ISSN 1818-0442

ДОКЛАДЫ

Томского государственного университета систем управления и радиоэлектроники

2(32) • 2014

Доклады ТУСУРа. №2(32), 2014

Министерство образования и науки Российской Федерации

ДОКЛАДЫ
ТОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ
2(32) • июнь 2014

Периодический научный журнал

Выходит 4 раза в год

Основан в 1997 г.

ISSN 1818-0442

Адрес редакции:

634050, г. Томск,
пр. Ленина, 40, ТУСУР,
тел. (382-2) 51-22-43

Свидетельство
о регистрации МНС РФ
1027000867068
от 13 октября 2004 г.

Подписной индекс 20648
в каталоге Агентства
«Роспечать»: газеты и журналы

Издательство
Томского государственного
университета систем управления
и радиоэлектроники
634050, Томск, пр. Ленина, 40,
тел. (382-2) 51-21-21

Оригинал-макет выпуска подготовлен
и отпечатан тираж ИП В.М. Бочкаревой
Техн. редактор В.М. Бочкарева
Корректор В.Г. Лихачева

Подписано в печать 28.05.2014.
Формат 60×84 $^{1}/_{8}$.
Усл. печ. л. 29,3
Тираж 500. Заказ 8.

Содержание

ЭЛЕКТРОТЕХНИКА

СООБЩЕНИЯ

ЭЛЕКТРОНИКА, ИЗМЕРИТЕЛЬНАЯ ТЕХНИКА, РАДИОТЕХНИКА И СВЯЗЬ

УДК 537.876.23

Ф.Н. Захаров, М.В. Крутиков

Сравнение точности оценки времени задержки навигационных сигналов при использовании различных моделей высотного профиля индекса преломления тропосферы

Статья посвящена точности оценки величины тропосферной задержки навигационных сигналов. Рассматриваются факторы, влияющие на точность этой оценки. Показано, что основной вклад в погрешность определения задержки вносят случайные флуктуации неоднородностей тропосферы в облаках и осадках. Оценены возможные значения ошибки определения времени задержки сигнала в тропосфере из-за расхождения реальных и модельных высотных профилей индекса преломления.

Ключевые слова: псевдодальность, задержка навигационного сигнала, тропосфера, индекс преломления, облачность, осадки.

Настоящая статья относится к области анализа точности работы спутниковых сетевых навигационных систем, таких как ГЛОНАСС (СССР/Россия), GPS (США), Galileo (Европа), COMPASS (Китай).

Как известно, координаты объекта в глобальной навигационной спутниковой системе определяются через измерение псевдодальностей от объекта до навигационных космических аппаратов (НКА). Псевдодальности, в свою очередь, вычисляются по измерениям времени задержки навигационных сигналов на трассах «НКА – потребитель» [1].

Погрешность измерения времени задержки определяется фактическим отношением сигнал/шум на входе приёмника, аппаратурными погрешностями и дополнительными задержками в радиоканале. Фактическое отношение сигнал/шум зависит от величин собственных и внешних шумов, помех, наличия рассогласования поляризации принимаемого сигнала с поляризацией приёмной антенны, значений ослабления сигнала при прохождении атмосферы. Аппаратурные погрешности определяются, главным образом, неучтёнными задержками в радиотрактах аппаратуры и расхождением частот опорных генераторов на НКА и приёмной станции. Дополнительные задержки навигационных сигналов определяются наличием многолучевого распространения, неточностью определения эфемерид НКА и задержкой сигнала в атмосфере из-за отличия скорости распространения электромагнитной волны от скорости света.

Использование малошумящих усилителей и высокостабильных стандартов частоты, применение калибровки приёмопередающих трактов и других технологий позволяют снизить среднеквадратическое отклонение (СКО) шумовых и аппаратурных погрешностей определения задержки сигнала до величины $\sigma_{ш} = (0{,}2…0{,}4)$ нс [1].

Для уменьшения влияния многолучёвости используют пространственно-избирательные методы подавления отражённых сигналов, а также цифровую обработку временных наблюдений принятых сигналов, что позволяет уменьшить СКО определения задержки вследствие влияния многолучёвости до величины $\sigma_{мл} = (0{,}3…0{,}5)$ нс. В работах Ю.С. Дубинко [2, 3] показано, что при исключении влияния отражённых сигналов можно получить СКО задержки навигационных сигналов менее 0,1 нс.

Основной вклад в атмосферную задержку вносят ионосфера и тропосфера. В случае спокойной ионосферы использование двух- или трёхчастотных методов компенсации ионосферной задержки позволяет получить СКО остаточной оценки задержки за счёт влияния ионосферы $\sigma_{и} = (0{,}3…0{,}5)$ нс [4]. В то же время принято считать [1, 5], что при использовании стандартных методов компенсации тропосферной задержки, основанных на модельных высотных профилях параметров тропосферы, остаточная ошибка компенсации составляет 10% от общей величины тропосферной задержки и равняется $\sigma_{т} = (1…10)$ нс.

Следовательно, общая остаточная случайная ошибка оценки времени задержки составит

$$\sigma_\tau = \sqrt{\sigma_{ш}^2 + \sigma_{мл}^2 + \sigma_{и}^2 + \sigma_{т}^2} = (1{,}1...10)\ \text{нс}. \quad (1)$$

Полученные оценки показывают, что основная ошибка определения времени задержки σ_τ определяется тропосферной составляющей. Если для обычного потребителя точности, достигаемой путём введения поправки, достаточно (при этом точность определения координат составляет несколько метров), то для метрологических измерений навигационных параметров, геодезических и других высокоточных измерений необходимо, чтобы СКО оценки общего времени задержки навигационного сигнала составляло (0,9…1,2) нс и менее [6]. При этом остаточное СКО оценки задержки сигнала в тропосфере должно быть не выше (0,3…0,8) нс.

Темой настоящей статьи является определение ошибок оценивания времени задержки навигационных сигналов в тропосфере в различных синоптических ситуациях и выбор моделей, наиболее точно описывающих изменения параметров тропосферы по высоте.

Дополнительное время задержки сигнала в тропосфере за счёт отличия скорости электромагнитной волны от скорости света пропорционально индексу преломления тропосферы на трассе прохождения сигнала [5]:

$$\tau_т = \frac{1}{c}\int_0^H 10^{-6} N(h)dh, \quad (2)$$

где $\tau_т$ – время задержки сигнала в тропосфере; c – скорость света; H – высота тропосферы (в средних широтах высота тропосферы составляет 10–12 км); $N(h)$ – высотный профиль индекса преломления в N-единицах. Данный интеграл вычисляется вдоль траектории радиолуча. Индекс преломления в соответствии с [5] определяется выражением

$$N = (n - 1)10^6, \quad (3)$$

где n – коэффициент преломления тропосферы.

В реальных условиях значения индекса преломления вдоль трассы получить крайне сложно [7]. Как правило, на практике для расчётов используют различные упрощённые модели вертикального профиля индекса преломления [8] и так называемые функции отображения, которые основаны на условии однородности тропосферы вдоль поверхности Земли. По вертикальному профилю вычисляется зенитная тропосферная задержка $\tau_т^z$, а задержка, соответствующая истинному углу возвышения КА α, вычисляется с помощью функции отображения $m(\alpha)$ [1, 5]:

$$\tau_т(\alpha) = \tau_т^z \cdot m(\alpha). \quad (4)$$

Существующие методы вычисления зенитной задержки и функции отображения основаны на условиях [9], при которых вертикальные распределения температуры, давления и влажности в тропосфере являются детерминированными функциями высоты, и предполагают локальное измерение метеорологических параметров вблизи поверхности Земли (обычно на высоте 2 м). При таком подходе точность оценки тропосферной задержки составляет от десятых долей до нескольких наносекунд [10], в зависимости от состояния тропосферы, что подтверждается данными из табл. 1. Приведённые в таблице величины ошибок показывают, что тропосфера существенно влияет на точность оценки общей задержки навигационного сигнала [11], особенно при сильной облачности и осадках. Это также подтверждается результатами работ [12, 13], в которых расчётным путём оценены флуктуации задержки на трассах по данным аэрологического зондирования за годовой период наблюдений.

Таблица 1

Флуктуации наблюдаемой дальности и времени задержки в тропосфере для радиолокационных измерений при малых углах места [14]

Состояние тропосферы	СКО показателя преломления тропосферы, *N*-ед.	СКО наблюдаемой дальности, м	СКО задержки сигнала, нс
Плотные кучевые облака	30	0,6	2
Рассеянные кучевые облака	10	0,15	0,5
Небольшие рассеянные кучевые облака	3	0,03	0,1
Чистый влажный воздух	1	0,006	0,02
Чистый нормальный воздух	0,3	0,0015	0,005
Чистый сухой воздух	0,1	0,0003	0,001

Кроме того, дополнительным фактором, влияющим на точность измерения задержки, являются пространственные неоднородности тропосферы, вызванные пространственными неоднородностями подстилающей поверхности [15]. В среднем значение горизонтальных градиентов индекса преломления незначительно (0,1–0,5 *N*-ед./100 м). Однако существуют особые условия (например, наличие границы суша – море), при которых будет наблюдаться увеличение флуктуаций индекса преломления вдоль земной поверхности. При этом возможны горизонтальные градиенты индекса преломления до 2 *N*-ед./100 м [16]. В этом случае флуктуации горизонтального градиента индекса преломления над неоднородной земной поверхностью оказывают дополнительное влияние на флуктуации задержки сигнала, которые могут составлять величину 0,3 нс [17].

Наличие атмосферных явлений приводит к заметным отклонениям высотного профиля индекса преломления от модельного. В частности, в работе [18] рассмотрены структуры неоднородностей индекса преломления, соответствующие различным метеорологическим образованиям, а также показаны примеры экспериментальных профилей индекса преломления, полученных с помощью рефрактометра при вертикальном зондировании различных метеорологических образований (рис. 1). В приведенных примерах наблюдаются сильные флуктуации индекса преломления, которые являются источником остаточной ошибки после введения поправки. Абсолютная величина остаточной ошибки компенсации тропосферной задержки может быть оценена по формуле

$$\Delta\tau_{\text{т}} = \frac{1}{c}\int_0^H 10^{-6}\left[N(h) - N_{\text{м}}(h)\right]dh, \qquad (5)$$

где $N_{\text{м}}(h)$ – модельный высотный профиль индекса преломления. В качестве модельного профиля $N_{\text{м}}(h)$ рассмотрим следующие высотные зависимости индекса преломления.

1. Линейная модель [19] $N_{\text{м}}(h) = N_S + g_N h$, где N_s – индекс преломления у поверхности Земли; $g_N = -40$ *N*-ед./км – градиент индекса преломления нормальной тропосферы [20].

2. Экспоненциальная модель [8, 14] $N_{\text{м}}(h) = N_S \exp(-b_1 h)$, где $b_1 = -0{,}1\ln\left(92/N_S\right)$ км$^{-1}$ – высотный коэффициент, который вычисляется из предположения, что на высоте 10 км индекс преломления постоянный и равен 92 *N*-ед. [21].

3. Биэкспоненциальная модель [20] $N_{\text{м}}(h) = N_{sd}\exp(-h/H_d) + N_{sw}\exp(-h/H_w)$, где N_{sd} = 275 *N*-ед. и $N_{sw} = N_s - N_{sd}$ – сухая и влажная компоненты индекса преломления, H_d = 9,5 км и H_w = 2,7 км – масштабы высоты для сухой и влажной компонент.

4. Модель Хопфилд [5] $N_{\text{м}}(h) = N_{sd}(1-h/H_d)^4 + N_{sw}(1-h/H_w)^4$, где H_d = 43 км и H_w = 12 км.

Рис. 1. Профили показателя преломления в различных метеорологических образованиях:
а – профиль в облаке; *б* – профиль в ливневых осадках; *в* – профиль в тумане

В работе [18] по результатам длительных экспериментальных рефрактометрических исследований тропосферы выделено три типа профиля индекса преломления (рис. 2), соответствующих трём различным синоптическим обстановкам на трассе распространения радиосигнала: циклонический без слоёв, антициклональный с мощным и устойчивым слоем и фронтальный раздел с локальными слоями, и предложены некоторые рекомендации по использованию моделей тропосферы.

Из табл. 1 и рис. 1, 2 видно, что сильные флуктуации вертикального профиля индекса преломления наблюдаются при облачности или осадках. Это также подтверждают экспериментальные данные, приводимые в работе [22]. Для примеров экспериментальных высотных профилей индекса

преломления, приведённых на рис. 2, величины остаточной ошибки определения времени задержки сигнала на радиотрассе оценены по формуле (5) для различных углов возвышения НКА. Результаты расчётов представлены в табл. 2. Приведённые значения СКО являются заниженными, так как рассчитаны в слое тропосферы толщиной 4 км. При учёте флуктуаций индекса преломления всей толщи тропосферы (до высоты 10–12 км) ошибка увеличится.

Рис. 2. Типы вертикальных профилей индекса преломления:
а – циклонический тип; *б* – антициклональный тип; *в* – фронтальный раздел с локальными слоями

Таблица 2

Ошибки определения задержки за счёт расхождения реального высотного профиля индекса преломления от модельного в слое тропосферы толщиной 4 км для трёх значений угла возвышения НКА

Состояние тропосферы	Модель профиля	СКО задержки сигнала, нс		
		90º	10º	3º
Циклон	Линейная	0,18	1,00	3,40
	Экспоненциальная	0,04	0,25	0,84
	Биэкспоненциальная	0,10	0,57	1,90
	Хопфилд	0,05	0,27	0,88
Антициклон	Линейная	0,17	0,96	3,20
	Экспоненциальная	0,05	0,27	0,90
	Биэкспоненциальная	0,02	0,12	0,40
	Хопфилд	0,07	0,42	1,40
Фронтальный раздел	Линейная	0,30	1,70	5,70
	Экспоненциальная	0,09	0,49	1,60
	Биэкспоненциальная	0,11	0,64	2,10
	Хопфилд	0,06	0,34	1,14

Данные табл. 2 показывают, что наиболее точно аппроксимируют реальные высотные профили индекса преломления три модели: экспоненциальная, биэкспоненциальная и Хопфилд. Для углов возвышения НКА от 90 до 10 градусов все три модели дают удовлетворительную точность оценки времени задержки. При углах возвышения НКА 3 градуса расчёты указывают на целесообразность использования модели Хопфилд и экспоненциальной модели в циклональных условиях (СКО менее 1 нс), в антициклональных условиях применимы экспоненциальная или (более предпочтительна) биэкспоненциальная модель. В условиях присутствия на радиотрассе фронтального раздела воздушных масс при углах возвышения НКА 3 градуса применение всех перечисленных моделей вертикального профиля дают ошибки более 1 нс, что недостаточно для высокоточных измерений.

Очевидно, что для точной оценки времени задержки целесообразно использовать зондирование всей толщи тропосферы. Однако существующие системы типа «Метеорит-МАРЗ» и «АВК-МРЗ» [23] не могут быть использованы в каждом пункте, где установлены наземные высокоточные средства приёма сигналов ГЛОНАСС. Поэтому на данный момент задача выявления физической или физико-статистической связи параметров тропосферы, в том числе облачности и осадков, с величиной задержки сигнала остаётся актуальной.

Выводы. Анализом ошибок различной природы, имеющих место при измерении задержек в аппаратуре потребителя после применения поправок, в условиях спокойной ионосферы и случая

отсутствия аэрологических данных о тропосфере показано преобладающее влияние тропосферы на точность измерений. Основной причиной погрешности являются отклонения в вертикальном профиле индекса преломления $N(h)$ от его модельных представлений, вызванные присутствием в тропосфере облачности и осадков.

Среди используемых обычно моделей профиля до углов возвышения 3 градуса для антициклонов наиболее пригодна биэкспоненциальная модель, а для циклонов более пригодны модель Хопфилд и экспоненциальная модель. Для условий фронтальных разделов воздушных масс рассмотренные модели дают неудовлетворительно большую погрешность.

При углах возвышения 10 градусов все перечисленные модели профиля дают ошибки величиной до 1 нс в условиях циклона и антициклона, но более предпочтительной является экспоненциальная модель. При фронтальном разделе наиболее пригодны модели Хопфилд и экспоненциальная, обеспечивающие ошибки до 0,5 нс.

Литература

1. Перов А.И. ГЛОНАСС. Принципы построения и функционирования / А.И. Перов, В.Н. Харисов. – М.: Радиотехника, 2010. – 800 с.

2. Дубинко Ю.С. Возможности повышения точностных характеристик при определении места по спутниковым навигационным системам / Ю.С. Дубинко, А.С. Селиверстов, М.И. Полтаржицкий // Труды ИПА РАН. – 2012. – Вып. 25. – С. 73–84.

3. Патент 2237256, Российская Федерация, МПК H04B1/06. Способ подавления ошибок многолучевости в приемниках спутниковой навигации / Ю.С. Дубинко, Т.Ю. Дубинко, С.В. Карпань. – № 2001104812/09; заявл. 21.02.2001; опубл. 20.05.2003. – 4 с.

4. Ким Б.-Ч. Влияние ионосферных неоднородностей на точность двухчастотных систем GPS / Б.-Ч. Ким, М.В. Тинин // Геомагнетизм и аэрономия. – 2007. – Т. 47, №2. – С. 254–259.

5. Антонович К.М. Использование спутниковых навигационных систем в геодезии: в 2 т. – Т. 1. – М.: ФГУП «Картгеоцентр», 2005. – 334 с.

6. Точность работы ГЛОНАСС пообещали повысить до 10 см [Электронный ресурс] // Российская газета [Офиц. сайт]. – Режим доступа: http://www.rg.ru/2012/12/27/glonass-site-anons.html, свободный (дата обращения: 27.12.2012).

7. Совместное измерение вертикальных профилей индекса рефракции и множителя ослабления сигнала 3-см диапазона над водной поверхностью / М.Е. Ровкин, Ю.П. Акулиничев, В.А. Хлусов, и др. // Доклады ТУСУРа. – 2005. – № 4 (12). – С. 61–67.

8. Госенченко С.Г. Алгоритм расчета и анализа тонкой структуры высотной зависимости индекса преломления // Доклады ТУСУРа. – 2005. – № 4 (12). – С. 15–20.

9. Рекомендация МСЭ-R P.835-4. Эталонные стандарты атмосферы [Электронный ресурс]. – Режим доступа: www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.835-4-200503-S!!PDF-R.pdf, свободный (дата обращения: 14.02.2014).

10. Бартон Д. Справочник по радиолокационным измерениям / Д. Бартон, Г. Вард. – М.: Сов. радио, 1976. – 392 с.

11. Антонович К.М. О моделировании тропосферы при GPS-измерениях / К.М. Антонович, Е.К. Фролова // Вестник СГГА. – 2002. – Вып. 7. – С. 11–17.

12. Мещеряков А.А. Применение численных моделей атмосферы для мониторинга условий распространения УКВ на приземных трассах / А.А. Мещеряков, Л.И. Кижнер, О.Н. Киселев // Сборник докладов междунар. науч.-техн. конф. «Радиолокация, навигация, связь». Секция «Электродинамика, распространение радиоволн, антенны. Техника СВЧ». – Воронеж, 2009. – С. 557–561.

13. Крутиков М.В. Тропосферная флуктуационная ошибка радиодальномерных измерений на наклонных морских трассах / М.В. Крутиков, Р.Р. Музафаров, М.И. Родионов // Радиотехника. – 1989. – № 7. – С. 6–8.

14. Бартон Д. Радиолокационные системы. – М.: Военное изд-во Министерства обороны СССР, 1967. – 480 с.

15. Киселёв О.Н. Мезомасштабные неоднородности коэффициента преломления в тропосфере и их влияние на распространение радиоволн УКВ-диапазона. – Томск: ТУСУР, 2007. – 199 с.

16. Кравцов Ю.А. Прохождение радиоволн через атмосферу Земли / Ю.А. Кравцов, З.И. Фейзулин, А.Г. Виноградов. – М.: Радио и связь, 1983. – 224 с.

17. Мещеряков А.А. Влияние изменчивости индекса преломления тропосферы на дальность прямой видимости и погрешности измерения координат радиолокационных целей / А.А. Мещеряков, С.Г. Госенченко, Л.И. Кижнер // Известия ТПУ. – 2011. – Т. 318, №2. – С. 59–63.

18. Павлова Л.В. Пространственная структура неоднородностей тропосферы по данным рефрактометрических измерений // Труды XX Всерос. науч. конф. «Распространение радиоволн». – Н. Новгород: Талам, 2002. – С. 352–353.

19. Радиоклиматический тропосферный атлас Тихого океана / под ред. Г.С. Шарыгина. – Томск: Томский гос. ун-т систем управления и радиоэлектроники, 2000. – 171 с.

20. Бин Б.Р. Радиометеорология / Б.Р. Бин, Е.Дж. Даттон. – Л.: Гидрометиздат, 1971. – 363 с.

21. Распространение радиоволн: учебник / О.И. Яковлев, В.П. Якубов, В.П. Урядов, А.Г. Павельев. – М.: ЛЕНАНД, 2009. – 496 с.

22. Roy A.L. Tropospheric Delay Measurement at Effelsberg with Water-Vapour Radiometry / A.L. Roy, U. Teuber, R. Keller // Proc. 16th Working Meeting on European VLBI for Geodesy and Astrometry. – Leipzig, 2003. – P 53–59.

23. Фридзон М.Б. Методология радиозондирования атмосферы и достоверность измерений вертикальных профилей температуры и влажности до высот 35–40 км: дис. ... д-ра техн. наук. – М., 2004. – 323 с.

Захаров Фёдор Николаевич
Аспирант каф. радиотехнических систем ТУСУРа
Тел.: 8-923-417-01-55
Эл. почта: fzakharov89@gmail.com

Крутиков Михаил Владимирович
Зав. лаб. распространения радиоволн НИИ РТС ТУСУРа
Тел.: (382-2) 41-39-69
Эл. почта: rwplab@sibmail.com

Zakharov F.N., Krutikov M.V.

Comparison of the accuracy of estimating the delay time of navigation signals by means of using different models of tropospheric refractivity profile

The paper deal with the accuracy of navigation signals` tropospheric delay estimation. The factors, which affect the estimation accuracy are discussed. To make it clear that random fluctuations of refraction coefficient in clouds and precipitations are major contributors of delay definition error. The error in determining the delay time of the signal in the troposphere is estimated. The error is arising from difference between real and simulated vertical profiles of the refraction coefficient.

Keywords: pseudorange, navigation signal delay, troposphere, refraction coefficient, cloud, precipitation.

УДК 621.317.35

Д.К. Отузбаева, Э.В. Семенов

Анализ искажений короткоимпульсных сигналов различной формы в свехширокополосных измерителях вольт-амперных и вольт-фарадных характеристик

Исследована возможность уменьшения систематической погрешности сверхширокополосного измерителя вольт-амперных и вольт-фарадных характеристик за счет оптимизации формы тестового сигнала. Проведено моделирование ожидаемой систематической погрешности, а также исследованы причины различий искажений для полученных импульсов.

Ключевые слова: нелинейные измерения, импульсные воздействия, нелинейные характеристики, систематическая погрешность.

Современные нелинейные измерители для получения нелинейных характеристик элементов производят измерения гармоническим сигналом [1]. При этом возникает методическая погрешность, если в последующем исследуемый элемент будет работать с импульсными сигналами [2]. В данной статье рассматривается альтернативный тип измерителя – характериограф (рис. 1), который позволяет одновременно измерять вольт-амперные (ВАХ) и вольт-фарадные (ВФХ) характеристики полупроводниковых элементов посредством воздействия сверхкоротким (100 нс и менее) видеоимпульсом [3]. Одна из проблем таких устройств: линейные искажения, возникающие из-за неравномерности передаточной характеристики и приводящие к систематической погрешности измерений. Существует несколько способов уменьшения влияния систематической погрешности: калибровка измерителя [4] или выбор для измерений тестового импульса, при котором систематическая погрешность будет минимальна. Настоящая статья посвящена исследованию второго способа.

Моделирование искажений регистрирующего устройства при воздействии сигналов разных форм. Сверхкороткоимпульсный характериограф состоит из шасси National Instruments PXI–1033, генератора тестовых сигналов Tabor Electronics 5201, аналогово-цифрового преобразователя PXI–5114, ЭВМ и измерительного преобразователя. Их назначение и технические характеристики приведены в [3].

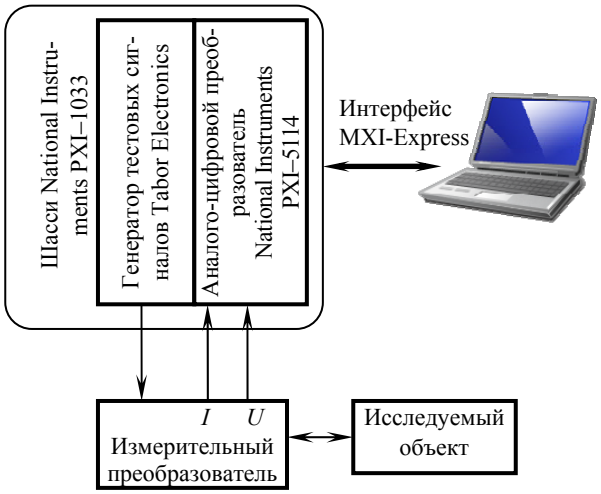


Рис. 1. Структурная схема системы для измерения вольт-амперных и вольт-фарадных характеристик сверхширокополосным импульсом

Линейные искажения, вносимые регистрирующим устройством PXI-5114, описываются его передаточной характеристикой. Для упрощения задачи моделирования представим передаточную характеристику регистрирующего устройства как передаточную характеристику фильтра нижних частот (ФНЧ) первого порядка, имеющую вид

$$H(\omega)=\frac{1}{1+i\omega/\omega_{\text{ср}}},$$

где $\omega=2\pi f$ (рад/с), $\omega_{\text{ср}}=2\pi f_{\text{ср}}$, $f_{\text{ср}}$ = 155 МГц – частота среза передаточной характеристики регистрирующего устройства PXI-5114. Тогда переходная характеристика этого фильтра имеет вид

$$h(t)=1-\exp\left[-\omega_{\text{ср}}t\right].$$

В качестве тестовых импульсов $u_{вх}(t)$ рассмотрим три формы импульсов длительностью 100 нс: трапециевидный, гауссовский и импульс экспоненциальными фронтами. Фронт импульса с экспоненциальными фронтами задается формулой

$$u_{вх}(t) = 1 - \exp\left(-\frac{t}{\tau_f}\right), \quad (1)$$

где τ_f – коэффициент, характеризующий длительность фронта. Гауссовский импульс задается соотношением

$$u_{вх}(t) = \exp\left[-\left(\frac{t}{\tau_e}\right)^2\right], \quad (2)$$

где τ_e – параметр, отвечающий за длительность импульса.

Импульсы были заданы с частотой дискретизации 5 Гвыб/с, соответствующей частоте дискретизации регистрирующего утройства. Отклик регистрирующего устройства $u_{вых}(t)$ на каждый из этих импульсов был найден согласно формулам:

$$S(\omega) = F\left[u_{вх}(t)\right]H(\omega), \quad (3)$$

$$u_{вых}(t) = F^{-1}\left[S(\omega)\right], \quad (4)$$

где $F\left[u_{вх}(t)\right]$ – прямое преобразование Фурье, $F^{-1}\left[S(\omega)\right]$ – обратное преобразование Фурье-спектра сигнала.

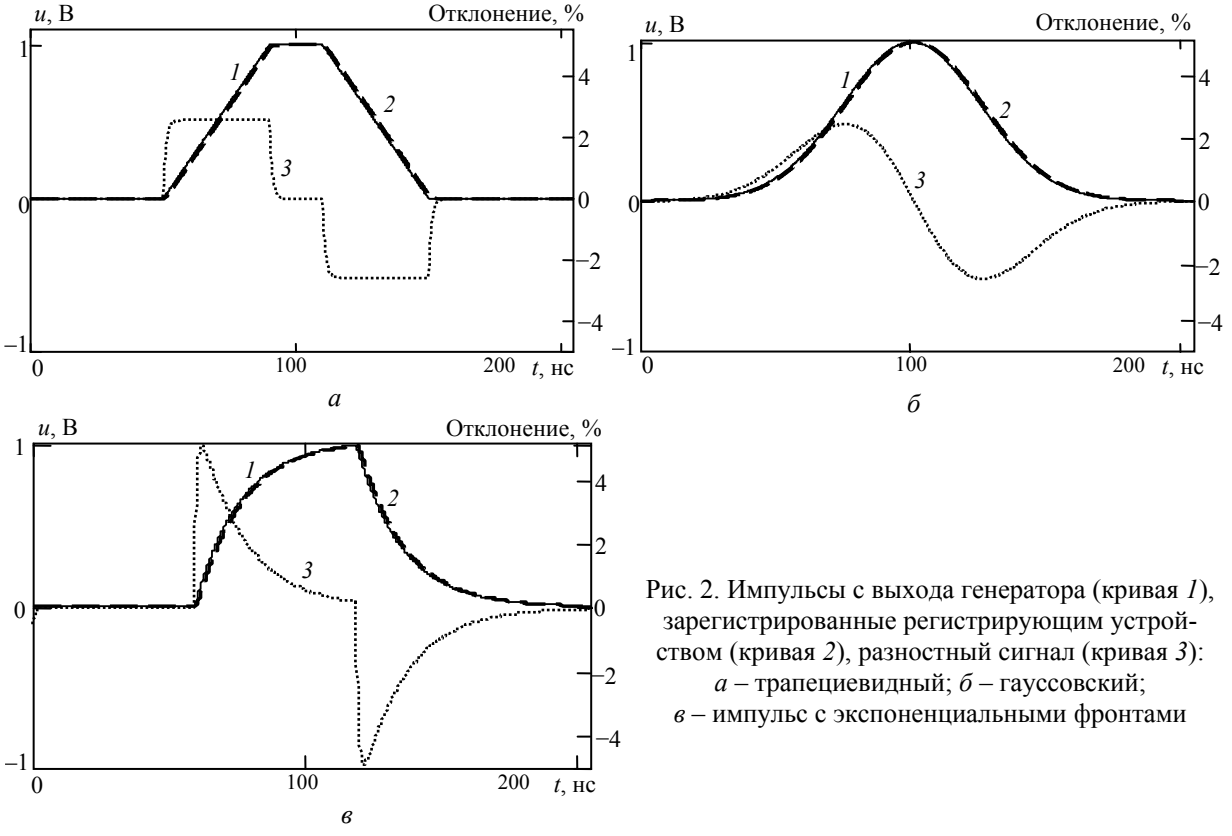


Рис. 2. Импульсы с выхода генератора (кривая *1*), зарегистрированные регистрирующим устройством (кривая *2*), разностный сигнал (кривая *3*): *а* – трапециевидный; *б* – гауссовский; *в* – импульс с экспоненциальными фронтами

Полученные отклики регистрирующего устройства и поданные на него импульсы приведены на рис. 2. Видно, что величина отклонения разностного сигнала для каждого импульса составляет приблизительно 2,5%, т.е. систематическая погрешность их регистрации примерно одинакова. Большая часть этой погрешности обусловлена некоторой задержкой сигнала регистрирующим устройством. На результаты измерений ВАХ и ВФХ она не влияет, поэтому рассмотрим остаточную систематическую погрешность после компенсации этой задержки.

Сигнал, принятый регистрирующим устройством, сдвинут во времени на величину вносимого им группового времени запаздывания τ:

$$\tau = -d\varphi / dt ,$$

для расчета отклика системы на входное воздействие вместо формулы (3) воспользуемся формулой

$$S(\omega) = F\left[u_{\text{вх}}(t)\right] H(\omega) \exp(i\omega\tau) .$$

Полученные в результате моделирования значения максимального отклонения зарегистрированного сигнала от сформированного, а также отклонения по переднему и заднему фронту приведены в таблице и на рис. 3. Оценка искажений приведена для участков, на которых переходные процессы, связанные с началом импульса и обусловленные конечной крутизной переходной характеристики, завершены. Конкретно в качестве такого участка выбран участок фронта 20...80% от амплитуды импульса.

Значение отклонения сформированного сигнала от зарегистрированного

Форма импульса	Значение отклонения, %	
	Передний фронт	Задний фронт
Трапециевидный импульс	0,0009	0,0009
Гауссовский импульс	0,036	0,038
Импульс с экспоненциальными фронтами	0,011	0,011

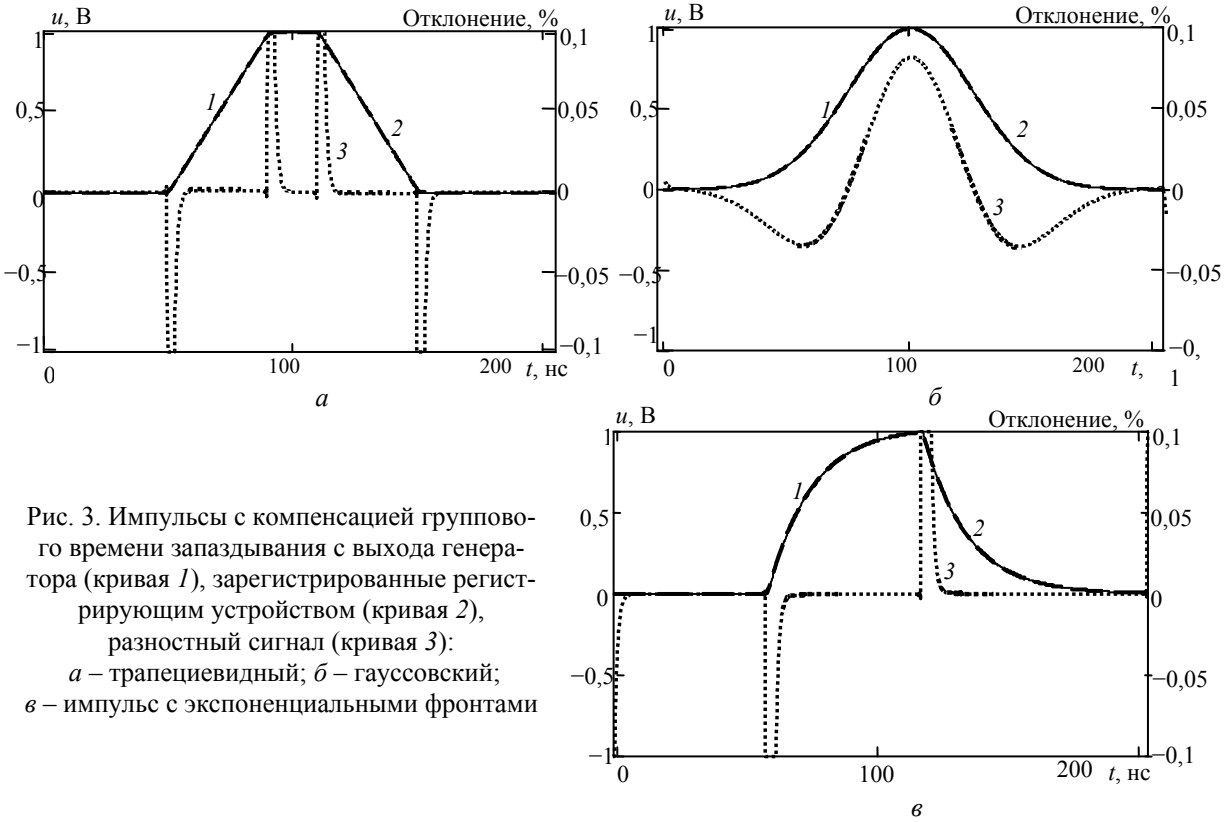


Рис. 3. Импульсы с компенсацией группового времени запаздывания с выхода генератора (кривая *1*), зарегистрированные регистрирующим устройством (кривая *2*), разностный сигнал (кривая *3*): *а* – трапециевидный; *б* – гауссовский; *в* – импульс с экспоненциальными фронтами

Согласно ранее проведенному математическому моделированию [5], а также результатам настоящего исследования, импульсы, имеющие участки линейного возрастания, имеют меньшее значение отклонения разностного сигнала, давая наименьшую систематическую погрешность измерений. При условии компенсации группового времени запаздывания импульс с экспоненциальными фронтами также дает малые искажения. Гауссовский импульс имеет гладкую форму, однако систематическая погрешность его регистрации достигает 0,08%. Таким образом, импульсы с фронтом, описываемым по линейному закону или имеющие экспоненциальное возрастание, имеют преимущество при регистрации регистрирующим устройством, в отличие от экспоненциальной функции квадрата времени.

Исследование причин различий в искажениях сигналов. Для установления причин различий в искажениях сигналов воспользуемся асимптотическими методами анализа, т.е. рассмотрим только участок фронта импульса, на котором переходные процессы, связанные с началом фронта, завершились.

Для нахождения отклика регистрирующего устройства на входное воздействие воспользуемся интегралом Дюамеля, применяемым для нахождения отклика системы на произвольно меняющееся во времени входное воздействие:

$$u_{\text{вых}}(t) = u_{\text{вх}}(0)h(t) + \int_0^t u'_{\text{вх}}(\tau)h(t-\tau)d\tau . \quad (5)$$

Фронт трапециевидного импульса описывается уравнением прямой

$$u_{\text{вх}}(t) = kt ,$$

где k – коэффициент наклона прямой. Таким образом, отклик регистрирующего устройства на линейно нарастающий фронт будет описываться выражением

$$u_{\text{вых}}(t) = 0 \cdot h(t) + \int_0^t k\left(1-\exp\left(\omega_{\text{ср}}\tau - \omega_{\text{ср}}t\right)\right)d\tau = kt - \frac{k\left(1-\exp(-\omega_{\text{ср}}t)\right)}{\omega_{\text{ср}}} . \quad (6)$$

После окончания переходных процессов, связанных с началом фронта, выражение $\exp(-\omega_{\text{ср}}t)$ стремится к нулю, так как $\left(-\omega_{\text{ср}}t\right)$ стремится к минус бесконечности. Таким образом, второе слагаемое в (6) стремится к $k/\omega_{\text{ср}}$. Следовательно прямая, описывающая фронт, сместится на величину $k/\omega_{\text{ср}}$, что можно рассматривать как задержку, так как наклон прямой не изменился. В таком случае, введя задержку, можно получить сигнал на выходе, идентичный исходному, т.е. сигнал с такой формой фронта обладает устойчивостью к влиянию систематической погрешности.

Экспоненциальный фронт импульса описывается выражением (1). С помощью интеграла Дюамеля (5) вычислили отклик регистрирующего устройства на входное воздействие

$$u_{\text{вых}}(t) = 0 \cdot \left[1-\exp\left(-\omega_{\text{ср}}t\right)\right] + \int_0^t \frac{1}{\tau_f}\exp\left(-\frac{\tau}{\tau_f}\right)\left[1-\exp\left(\omega_{\text{ср}}t - \omega_{\text{ср}}\tau\right)\right]d\tau .$$

После проведения некоторых математических преобразований выходное выражение принимает вид:

$$u_{\text{вых}}(t) = \frac{\exp\left(-\omega_{\text{ср}}t\right)}{\omega_{\text{ср}}\tau_f - 1} + 1 - \exp\left[-\frac{t}{\tau_f} + \ln\left(\frac{\omega_{\text{ср}}\tau_f}{\omega_{\text{ср}}\tau_f - 1}\right)\right] . \quad (7)$$

Так же, как и в прошлом примере, по окончании переходных процессов, связанных с началом фронта, выражение $\exp(-\omega_{\text{ср}}t)$ стремится к нулю, поэтому первое слагаемое в (7) стремится к нулю. Тогда выходная функция имеет вид входного воздействия за исключением наличия некоторой дополнительной величины в степени экспоненты, что можно рассматривать как задержку сигнала после регистрации. Таким образом, выходная функция стремится к

$$u_{\text{вых}} \Rightarrow 1 - \exp\left[-\frac{t}{\tau_f} + \ln\left(\frac{\omega_{\text{ср}}\tau_f}{\omega_{\text{ср}}\tau_f - 1}\right)\right] .$$

Найдем отклик регистрирующего устройства на входное воздействие в виде импульса гауссовской формы, описываемого выражением (2):

$$u_{\text{вых}}(t) = 1 \cdot \left[1-\exp\left(-\omega_{\text{ср}}t\right)\right] - \int_0^t \frac{-2t}{\tau_e^2}\exp\left(-\frac{t^2}{\tau_e^2}\right)\left[1-\exp\left(\omega_{\text{ср}}t - \omega_{\text{ср}}\tau\right)\right]d\tau =$$

$$= \frac{2}{\omega_{\text{ср}}\tau_e^2}\exp\left(-\frac{t^2}{\tau_e}\right)\left[t\exp\left(-\omega_{\text{ср}}t\right) - t^2\omega_{\text{ср}} - t\right] + 1 - \exp\left(-\omega_{\text{ср}}t\right) .$$

После окончания переходных процессов, связанных с началом фронта, выражение $\exp(-\omega_{\text{ср}}t)$ стремится к нулю, тогда выходная функция имеет вид: $u_{\text{вых}} \Rightarrow 1 - \frac{2}{\omega_{\text{ср}}\tau_e^2}\exp\left(-\frac{t^2}{\tau_e}\right)\left[t^2\omega_{\text{ср}} + t\right]$. Выражение $\exp\left(-\frac{t^2}{\tau_e{}^2}\right)$ соответствует входному воздействию, однако наличие перед ним множителя

$\left[t+t^2\omega_{\text{ср}}\right]$, зависимого от времени, указывает на то, что выходной сигнал не будет совпадать по форме с входным.

Заключение. Обнаружено, что систематическая погрешность для различных форм тестовых импульсов не одинакова. При длительности переходного процесса в регистрирующем или генерирующем устройстве, сопоставимой с длительностью фронта импульсного сигнала, меньшую систематическую погрешность дает гладкая форма сигнала (гауссовские импульсы), а при длительности переходного процесса в регистрирующем или генерирующем устройстве много меньшей длительности фронта импульса преимуществами обладают сигналы с линейным или экспоненциальным фронтом. Аналитически и в вычислительных экспериментах установлено, что если фронт меняется по линейному закону, либо описывается функцией экспоненты, то систематическая погрешность его регистрации устройством с передаточной характеристикой фильтра нижних частот с частотой среза реальной передаточной характеристикой регистрирующего устройства [5] минимальна. В случае если фронт возрастает как экспоненциальная функция квадрата времени (гауссовский импульс), то значение отклонения зарегистрированного сигнала от исходного имеет наибольшее значение.

Литература

1. *X*-параметры: новый принцип измерений ВЧ- и СВЧ- компонентов (X-parameters: The new paradigm for measurement, modeling, and design of nonlinear RF and microwave components) / D.E. Root, J. Horn, L. Bettset al. // Контрольно-измерительные приборы и системы. – 2009. – Т. 2. – С. 20.

2. Семенов Э.В. Виртуальный нелинейный импульсный измеритель характеристик цепей для САПР Microwave Office / Э.В. Семенов, Н.Д. Малютин, А.Г. Лощилов // СВЧ-техника и телекоммуникационные технологии (КрымиКо '2009): матер. 19-й Международ. конф. Севастополь, Украина, 14–18 сентября 2009 г. – Севастополь: Вебер, 2009. – Т. 1. – С. 103–104.

3. Семенов Э.В. Программно-аппаратный комплекс для сверхкороткоимпульсной характеризации полупроводниковых элементов // Инженерные и научные приложения на базе технологий National Instruments. – 2012: сборник трудов XI Международ. науч.-практ. конф. Москва, 6–7 декабря 2012 г. – М.: ДМК-пресс, 2012. – С. 10–12.

4. Назаров М.А. Абсолютная калибровка сверхкороткоимпульсного измерителя нелинейных характеристик цепей / М.А. Назаров, Э.В. Семенов // Докл. Том. гос. ун-та систем управления и радиоэлектроники. – 2013. – № 3, ч. 1. – С. 38–42.

5. Моделирование систематической погрешности сверхширокополосных нелинейных измерителей при различных параметрах тестовых / Д.К. Отузбаева, Э.В. Семенов // Современные техника и технологии: матер. 19-го Междунар. науч.-практ. конф., Томск 15–19 апреля 2014 г. – Томск: ТПУ, 2014. – Т. 1. – С. 133.

Отузбаева Дарина Кунтаевна
Магистрант каф. радиоэлектроники и защиты информации (РЗИ) ТУСУРа
Тел.: +7-905-990-63-71
Эл. почта: darina.otyz@gmail.com

Семенов Эдуард Валерьевич
Д-р техн. наук, профессор каф. РЗИ
Тел.: +7 (382-2) 41-33-65
Эл. почта: edwardsemyonov@narod.ru

Otuzbayeva D.K., Semyonov E.V.

Distortion analysis of various form short-pulse signal in UWB current-voltage and capacitance-voltage characteristics measuring system

The paper deals with the possibility of reducing the systematic inaccuracy in UWB current-voltage and capacitance-voltage characteristics measuring system by optimizing form of signal. Expected systematic inaccuracy was simulated, also causes of differences obtained pulse signal distortion were investigated.
Keywords: nonlinear measurements, pulse impact, non-linearity characteristic, video pulses, systematic error.

УДК 621.397: 621.384.3

Ю.Р. Кирпиченко

Динамический диапазон и число воспроизводимых градаций яркости высокочувствительных датчиков изображения

Получены аналитические выражения для оценки динамического диапазона и числа воспроизводимых градаций яркости высокочувствительных датчиков изображения с учетом зависимости шума выходного сигнала от интенсивности излучения.

Ключевые слова: прибор с зарядовой связью, электронно-оптический преобразователь, динамический диапазон, градации яркости.

Возможность обнаружить объект наблюдения на некотором фоне либо различить детали разной яркости ТВ-датчиком зависит от такой характеристики датчика, как количество воспроизводимых градаций яркости.

Увеличение числа воспроизводимых ТВ-датчиком градаций яркости увеличивает количество получаемой об объекте наблюдения информации.

При заданном контрасте входного изображения на выходе ТВ-датчика можно различить вполне определенное количество градаций яркости, которое зависит как от величины порогового контраста датчика, так и от его динамического диапазона.

Динамический диапазон будем определять отношением освещенности, при которой наступает насыщение, к освещенности, при которой отношение сигнал/шум на выходе ТВ-датчика равно пороговому.

Подход к оценке числа воспроизводимых градаций яркости зависит от назначения телевизионной системы. В телевизионной системе, где информация об объекте наблюдения воспринимается и анализируется посредством зрительного восприятия, число градаций яркости определяется особенностью такого восприятия, описываемого законом Вебера–Фехнера.

Для автоматических ТВ-систем аналогом различимого приращения яркости является приращение сигнала $\Delta N_{\text{с}}$, которое может быть обнаружено с требуемой вероятностью. Связь $\Delta N_{\text{с}}$ с пороговым отношением сигнал/шум $\Psi_{\text{пор}}$ устанавливается формулой [1]:

$$\Delta N_{\text{с}} = \sigma_{\text{ш}} \Psi_{\text{пор}}, \qquad (1)$$

где $\sigma_{\text{ш}}$ – среднеквадратическое отклонение шума ТВ-датчика.

Выражение (1) часто является исходным для расчета числа градаций яркости. При этом число градаций яркости определяется как отношение заряда насыщения к среднему квадратическому отклонению «шумового» заряда. Однако такой подход к определению числа различимых градаций яркости не учитывает тот факт, что в современных высокочувствительных ТВ-датчиках изображения шум выходного сигнала определяется квантовой природой регистрируемого оптического излучения и зависит от его интенсивности.

Выходной сигнал ТВ-датчика определим как разность между средним количеством фотонов $N_{\text{о}}$, попадающих на участок изображения объекта за время экспозиции, и средним количеством фотонов $N_{\text{ф}}$, попадающих на такой же участок изображения однородного фона.

Тогда отношение сигнал/шум Ψ разностного сигнала $\Delta N_{\text{сф}}$, выраженного в фотонах, попадающих за время накопления на элемент изображения ПЗС, с учетом квантового выхода $\eta_{\text{пзс}}$ можно записать в виде

$$\Psi = \frac{\Delta N_{\text{сф}} \sqrt{\eta_{\text{пзс}}}}{\sqrt{2N_{\text{ф}} + \Delta N_{\text{сф}} + N_{\text{т}}/\eta_{\text{пзс}}}}, \qquad (2)$$

где $N_{\text{т}}$ – среднее значение числа «темновых» электронов ПЗС; $N_{\text{ф}}$ – среднее значение числа фотонов, обусловленных фоновой засветкой; $\eta_{\text{пзс}}$ – квантовый выход ПЗС.

Решая уравнение (2) относительно различимого приращения входного сигнала, получим зависимость этого приращения от величины «фонового» сигнала $N_{\text{ф}}$

$$\Delta N_{\text{сф}1} = \frac{\Psi_{\text{пор}}^2 + \Psi_{\text{пор}}\sqrt{\Psi_{\text{пор}}^2 + 8\eta_{\text{пзс}}N_{\text{ф}} + 4N_{\text{т}}}}{2\eta_{\text{пзс}}}, \quad (3)$$

где $\Psi_{\text{пор}}$ – пороговое отношение сигнал/шум.

Для вычисления числа различимых градаций яркости $N_{\text{гр}}$ запишем выражение (3) в виде

$$\Delta N_{\text{сф}}^{n} = \frac{\Psi_{\text{пор}}^2 + \Psi_{\text{пор}}\sqrt{\Psi_{\text{пор}}^2 + 8\eta_{\text{пзс}}\text{N}_{\text{ф}}^{n} + 4N_{\text{т}}}}{2\eta_{\text{пзс}}},$$

где $N_{\text{ф}}^{n} = N_{\text{ф}} + \sum_{i=1}^{n-1}\Delta N_{\text{с}}^{i-1}$; $\Delta N_{\text{с}}^{i-1}$ – приращение яркости, предшествующее определяемому; n – номер определяемого приращения.

Величина n будет равна числу воспроизводимых ПЗС градаций яркости $N_{\text{гр}}$ при выполнении условия

$$N_{\text{ф}}^{n} \geq \eta_{\text{пзс}}N_{\text{нас}},$$

где $N_{\text{нас}}$ – максимально возможное число накопленных на элементе матрицы ПЗС фотоэлектронов.

Для обеспечения видения при низких уровнях освещенности (< 0,001 лк) и практически в полной темноте часто используется ПЗС-датчик изображения, сочлененный с электронно-оптическим преобразователем (ЭОП).

Среднее значение числа зарядов, накопленных на элементе ПЗС такого прибора за время кадра, и их дисперсия согласно [2] равны соответственно

$$N_{\text{з}} = \eta_{\text{эоп}}\eta_{\text{пзс}}K_{\text{ос}}G_{\text{эоп}}N_{\text{ф}}, \quad (4)$$

$$D[N_{\text{пзс}}] = \eta_{\text{эоп}}\eta_{\text{пзс}}K_{\text{ос}}^2F_{\text{ш}}^2G_{\text{эоп}}^2N_{\text{ф}}, \quad (5)$$

где $\eta_{\text{эоп}}$ – квантовый выход фотокатода ЭОП; $K_{\text{ос}}$ – коэффициент потерь в согласующей оптике; $F_{\text{ш}}$ – коэффициент шума микроканальных пластин; $G_{\text{эоп}}$ – коэффициент усиления ЭОП.

С учетом формул (4) и (5) выражение для различимого приращения яркости будет иметь вид

$$\Delta N_{\text{фс}2} = \frac{aF_{\text{ш}}^2\Psi_{\text{пор}}^2 + F_{\text{ш}}\Psi_{\text{пор}}\sqrt{a^2F_{\text{ш}}^2\Psi_{\text{пор}}^2 + 8a^2b\eta_{\text{эоп}}N_{\text{ф}} + 4N_{\text{т}}/F_{\text{ш}}^2}}{2ab}, \quad (6)$$

где $a = K_{\text{ос}}G_{\text{эоп}}$; $b = \eta_{\text{пзс}}\eta_{\text{эоп}}$.

Используя соотношение (6), можно определить число воспроизводимых градаций яркости ТВ-датчика (ПЗС) с усилителем яркости (ЭОП) по той же методике, что и для ПЗС.

На рис. 1 и 2 представлены расчетные зависимости числа воспроизводимых градаций яркости ПЗС и ПЗС, сочлененного с ЭОП. Расчет числа воспроизводимых градаций яркости ПЗС, сочлененного с ЭОП, проводился при следующих значениях параметров: $\eta_{\text{пзс}} = 0{,}5$; $\eta_{\text{эоп}} = 0$; $K_{\text{ос}} = 0$; $N_{\text{нас}} = 300000$ электронов; $N_{\text{т}} = 400$ электронов; $F_{\text{ш}} = 3$.

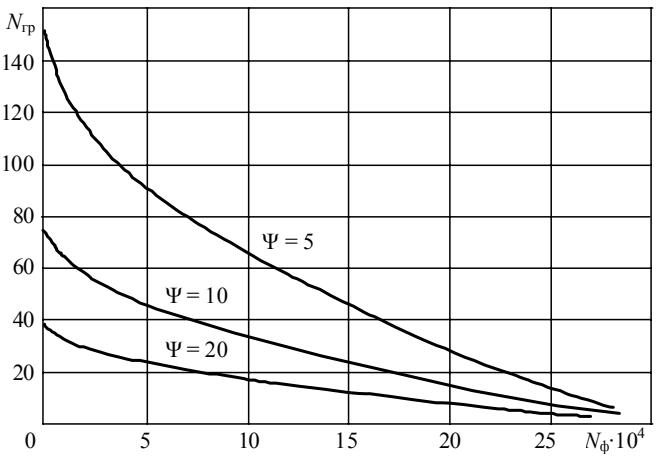


Рис. 1. Зависимость числа воспроизводимых ПЗС-датчиком градаций яркости от уровня фоновой засветки

Анализ результатов расчета и приведенных на рис. 1 и 2 зависимостей показывает, что число воспроизводимых градаций автоматической ТВ-системой на ПЗС уменьшается с ростом величины фоновой засветки и порогового отношения сигнал/шум. При $\Psi_{\text{пор}} = 20$, даже при уровне фоновой засветки равном нулю, число воспроизводимых градаций $N_{\text{гр}} < 40$.

При использовании усилителей яркости для повышения чувствительности ТВ-датчика, наряду с достижением поставленной цели, сопутствующим фактором является снижение качества изображения, выражающееся в уменьшении числа воспроизводимых градаций. Как видно из приведенных на рис. 2 кривых, особенно существенно число воспроизводимых градаций уменьшается с ростом коэффициента усиления ЭОП. Даже при коэффициенте усиления $G_{эоп}$ = 4000, значительно меньшем достигаемого в современных ЭОП, число воспроизводимых градаций равно единице в небольшом диапазоне изменения уровня фоновой засветки.

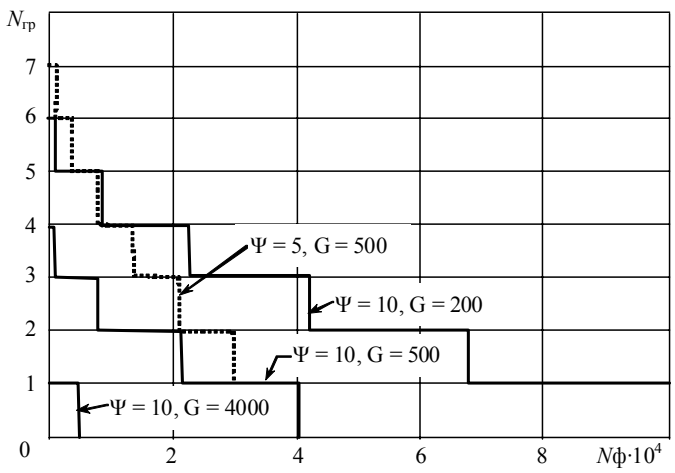


Рис. 2. Зависимость числа воспроизводимых градаций ТВ-датчиком с усилителем яркости

Уменьшение числа градаций с ростом $G_{эоп}$ означает, что чувствительность ТВ-датчика с усилителем яркости соответствует случаю регистрации отдельных квантов, а величина заряда на элементе ПЗС при попадании на фотокатод ЭОП одного кванта достигает величины, равной заряду насыщения.

Для определения динамического диапазона ПЗС рассчитаем число фотонов $N_{\phi max}$, при котором заряд на элементе матрицы ПЗС равен максимальному значению, и число фотонов $N_{\phi min}$, при котором отношение сигнал/шум на выходе ПЗС равно пороговому.

Число фотонов $N_{\phi max}$, соответствующее заряду насыщения элемента ПЗС с учетом квантового выхода $\eta_{пзс}$, будет равно

$$N_{\phi max} = N_{нас} / \eta_{пзс}.$$

Число фотонов $N_{\phi min}$, соответствующее пороговому отношению сигнал/шум, определим из выражения (3) при $N_{\phi} = 0$

$$N_{\phi min} = \frac{\Psi_{пор}^2 + \Psi_{пор}\sqrt{\Psi_{пор}^2 + 4N_т}}{2\eta_{пзс}}.$$

Тогда динамический диапазон матрицы ПЗС $D_{пзс}$ будет

$$D_{пзс} = \frac{N_{\phi max}}{N_{\phi min}} = \frac{2N_{нас}}{\Psi_{пор}^2 + \Psi_{пор}\sqrt{\Psi_{пор}^2 + 4N_т}}. \quad (7)$$

Определим динамический диапазон ТВ-датчика с усилителем яркости.

С учетом того, что $N_{\phi max}$ и $N_{\phi min}$ для такого датчика будут равны соответственно

$$N_{\phi max} = \frac{N_{нас}}{\eta_{эоп}\eta_{пзс}K_{ос}G_{эоп}}, \quad N_{\phi min} = \frac{aF_ш^2\Psi^2 + F_ш\Psi\sqrt{aF_ш^2\Psi^2 + 4N_т / F_ш^2}}{2ab},$$

запишем выражение для динамического диапазона $D_{пзс+эоп}$ в виде

$$D_{пзс+эоп} = \frac{2N_{нас}}{k\left(\Psi_{пор}^2 + \Psi_{пор}\sqrt{\Psi_{пор}^2 + 4\frac{N_т}{bk^2}}\right)}. \quad (8)$$

Из формулы (7) видно, что динамический диапазон матрицы ПЗС не зависит от величины квантового выхода и определяется только величиной заряда насыщения и числом «темновых» электронов.

Как видно из рис. 4, динамический диапазон датчика изображения, представляющего собой ПЗС, сочлененный с ЭОП, расширяется при увеличении квантового выхода ПЗС, потерь в согласующей оптике и уменьшении фактора шума микроканальной пластины. Динамический диапазон такого прибора значительно уже динамического диапазона ПЗС.

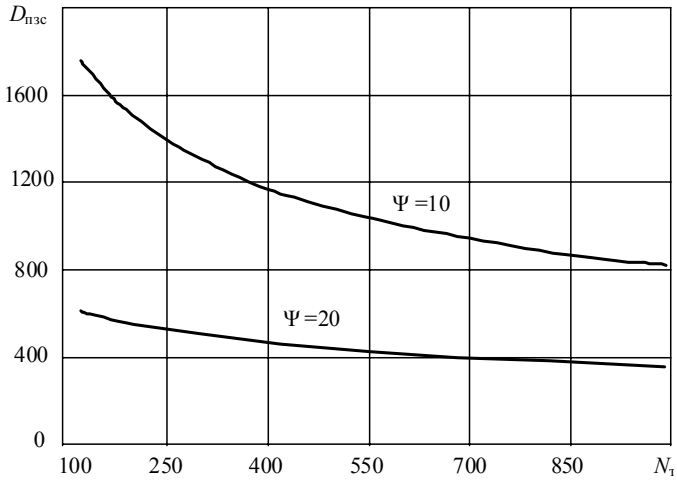


Рис. 3. Динамический диапазон ПЗС

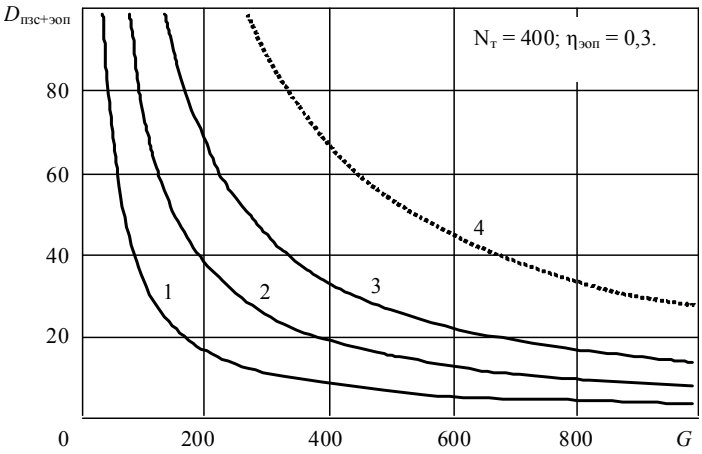


Рис. 4. Динамический диапазон ПЗС, сочлененного с ЭОП:
1 – $\eta_{пзс}$ =0,1; $F_ш$ = 3; $K_{ос}$ = 0,1;
2 – $\eta_{пзс}$ =0,5; $F_ш$ = 2; $K_{ос}$ = 0,1;
3 – $\eta_{пзс}$ =0,5; $F_ш$ = 1,5; $K_{ос}$ = 0,1;
4 – $\eta_{пзс}$ =0,5; $F_ш$ = 1,5; $K_{ос}$ = 0,05

Работа выполнена при финансовой поддержке Минобрнауки России в рамках базовой части государственного задания № 2014/225 по проекту 769.

Литература

1. Быков Р.Е. Основы телевидения и видеотехники: учеб. для вузов. – М.: Горячая линия–Телеком, 2006. – 399 с.

2. Дегтярев П.А. Исследование и разработка устройств получения видеосигнала в активно-импульсной телевизионной системе наблюдения: дис. … канд. техн. наук: 05.12.04. – Томск, 2005. – 233 с.

Кирпиченко Юрий Романович
Канд. техн. наук, доцент каф. телевидения и управления ТУСУРа
Тел.: (382-2) 42-33-87
Эл. почта: urkirp@gmail.com

Kirpichenko Yu.R.

The dynamic range and the number of brightness gradations of highly sensitive image sensors

An analytical formula for evaluation of dynamic range and the number of brightness gradations of highly sensitive image sensors were found considering the dependence of the output signal noise from the radiation intensity.

Keywords: charge-coupled device, dynamic range, image intensifier, gradations brightness.

УДК 621.397: 621.384.3

Ю.Р. Кирпиченко

Зависимость яркости свечения экрана ЭОП от напряжений на его электродах

Приведены результаты экспериментальных исследований влияния изменений напряжений на электродах на яркость свечения люминесцентного экрана ЭОП. Отмечается, что при малых освещенностях теоретические и экспериментальные результаты достаточно хорошо совпадают и что зависимость яркости свечения экрана ЭОП от напряжения на микроканальной пластине может быть аппроксимирована квадратичной функцией.

Ключевые слова: фотокатод, микроканальная пластина, люминесцентный экран ЭОП.

В активно-импульсных телевизионных системах (АИТВС) [1] ЭОП используется в большинстве своем в качестве быстродействующего ключа. Однако использование ЭОП в составе АИТВС предоставляет более широкие возможности для повышения качества изображения. К таким возможностям относится, например, расширение динамического диапазона [2], обеспечение равной яркости изображений объектов, находящихся на разных расстояниях от телевизионной камеры [3], и т.д.

В работе [2] приведены результаты исследования влияния режимов питания на динамический диапазон активно-импульсной телевизионной системы. Для эффективной работы телевизионной системы в условиях изменения освещенности объектов наблюдения требуется автоматическая регулировка ее чувствительности. Одним из способов управления чувствительностью телевизионной системы является регулировка коэффициента усиления ЭОП.

Для оценки чувствительности к управлению усилением при проектировании цепей автоматической регулировки яркости и выработки требований к стабильности источников питания необходимо знать закономерности изменения яркости от напряжений на электродах ЭОП.

В [4] приводится выражение, связывающее яркость свечения экрана ЭОП с напряжениями на его электродах

$$\Phi_{\text{изл}} = 2{,}7\cdot 10^{-2}\,\gamma S_{\text{инт}}\Phi_{\text{фк}}U_{\text{фк}}U_{\text{э}}\left(6\cdot 10^{-3}\frac{U_{\text{мкп}}^2}{\gamma_{\text{к}}^2}\right)^{\frac{4\gamma_{\text{к}}^2}{U_{\text{мкп}}}-1}, \qquad (1)$$

где γ – светоотдача люминесцентного экрана ЭОП; $S_{\text{инт}}$ – интегральная чувствительность фотокатода; $\Phi_{\text{фк}}$ – входной поток излучения; $U_{\text{фк}}$ – напряжение на фотокатоде; $U_{\text{э}}$ – напряжение между экраном и выходом МКП; $U_{\text{мкп}}$ – напряжение на микроканальной пластине; $\gamma_{\text{к}}$ – калибр канала МКП.

Из выражения (1) следует, что яркость свечения экрана ЭОП линейно зависит от освещенности фотокатода и напряжений на фотокатоде и экране. Зависимость яркости экрана от напряжения на микроканальной пластине более сложная.

В [3], например, для обеспечения равной яркости изображений объектов наблюдения по дальности используется квадратичный закон изменения коэффициента усиления ЭОП от напряжения на микроканальной пластине.

Ниже приведены результаты экспериментальных исследований влияния изменений напряжений на электродах ЭОП на яркость свечения люминесцентного экрана ЭОП 2^{+} поколения фирмы «Катод» (Новосибирск).

На рис. 1 показана экспериментальная зависимость яркости свечения экрана ЭОП в относительных единицах от напряжения на фотокатоде (пунктирная кривая). График, рассчитанный с допущением о линейной зависимости коэффициента первичного умножения от энергии первичного электрона на входе микроканала, показан на рис. 1 сплошной линией.

На рис. 2 приведена экспериментальная зависимость (кривая *2*) относительной яркости свечения экрана ЭОП от напряжения на экране.

Предположение о линейном характере такой зависимости, принятой в расчетах, подтверждается (кривая *1* и *2*). Однако экспериментальная кривая начинается не с нулевого значения напряжения на экране, а с некоторого значения (на рис. 2 примерно с 4,2 кВ – кривая *1*).

Такое поведение можно объяснить наличием алюминиевого экрана на поверхности люминофорного слоя экрана, обращенного в сторону фотокатода и предназначенного для снижения оптической обратной связи в ЭОП. Таким образом, на люминофор экрана могут попасть только те электроны, энергия которых достаточна для проникновения через алюминиевый экран.

На рис. 1 и 2 экспериментальные кривые получены для освещенности фотокатода, принятой за единицу, при которой разрешение изображения штриховой миры на экране монитора ограничено шумом (режим счета фотонов).

На рис. 3 приведены экспериментальные зависимости относительной яркости свечения экрана ЭОП от напряжения на МКП (штриховые кривые) и рассчитанная по формуле (1) (сплошная кривая).

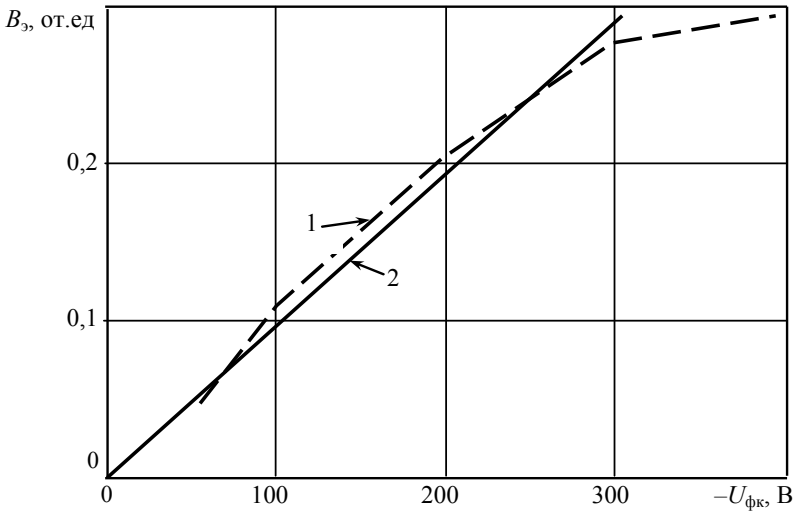


Рис. 1. Зависимость яркости свечения экрана ЭОП от напряжения на фотокатоде:
$U_{мкп}$ = 800 В; $U_э$ = 6 кВ; E_o = 1 (E_o – освещенность фотокатода ЭОП в относительных единицах)

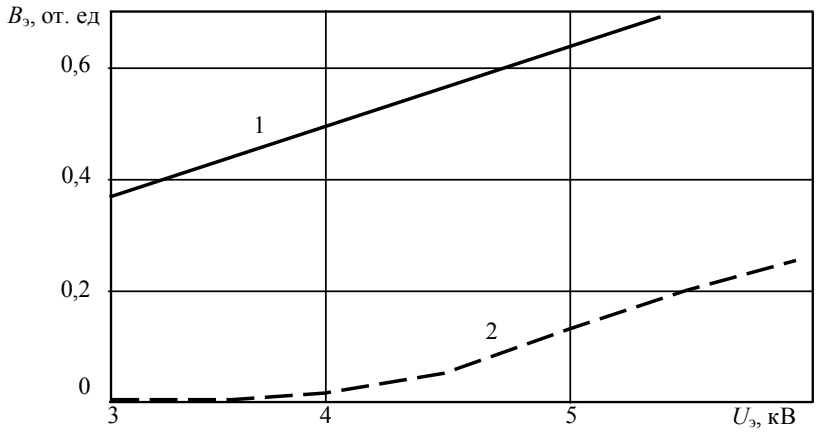


Рис. 2. Зависимость относительной яркости свечения экрана ЭОП от напряжения на экране:
$U_{фк}$ = – 200 В; $U_{мкп}$ = 800 В; E_o = 1

Из рис. 3 видно, что характер поведения расчетных и экспериментальных зависимостей (E_o = 1) при изменении $U_{мкп}$ достаточно хорошо совпадает. Следует отметить, что с увеличением освещенности фотокатода экспериментальные характеристики (кривые *1* и *2*) отличаются величиной показателя степени экспоненты в формуле (1). При этом, чем больше освещенность, тем больше отличие. Для выяснения такого отличия требуются дополнительные более тщательные исследования.

На рис. 3 штрихпунктирной линией показана аппроксимация зависимости яркости свечения экрана ЭОП от напряжения на микроканальной пластине квадратичной функцией

$$B_э = (U_{мкп} - 580)^2.$$

Из рис. 3 видно, что квадратичная аппроксимация (кривая *5*) достаточно хорошо совпадает с теоретической зависимостью, полученной из формулы (1).

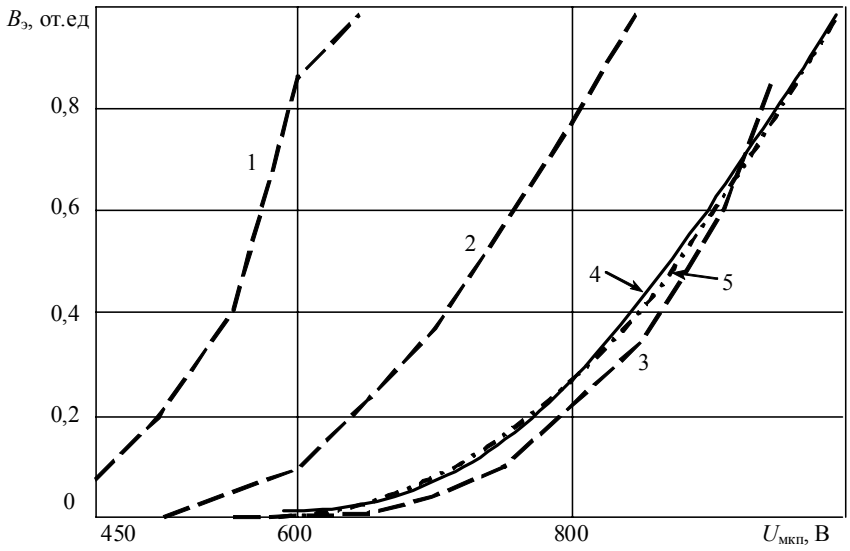


Рис. 3. Зависимость относительной яркости свечения экрана ЭОП от напряжения на микроканальной пластине: *1* – $E_o = 100$; *2* – $E_o = 10$; *3* – $E_o = 1$; *4* – расчетная кривая ($E_o = 1$); *5* – расчетная квадратичная зависимость

Проведенный анализ экспериментальных зависимостей и сравнение их с расчетными позволяет заключить, что полученные экспериментальные результаты достоверны и что при малых освещенностях зависимость яркости свечения экрана ЭОП от напряжения на МКП может быть аппроксимирована квадратичной функцией. Получено подтверждение вывода о том, что насыщение МКП в непрерывном режиме при достаточной накопительной емкости элемента ПЗС не ограничивает яркости свечения экрана ЭОП.

Работа выполнена при финансовой поддержке Минобрнауки России в рамках базовой части государственного задания № 2014/225 по проекту 769.

Литература

1. Активные ТВ-системы видения с селекцией фонов рассеяния / В.В. Белов, Г.Г Матвиенко, Р.Ю. Пак и др. // Датчики и системы. – 2012. – №3. – С. 25–30.

2. Кирпиченко Ю.Р. Исследование влияния режимов питания ЭОП на динамический диапазон активно-импульсной телевизионной системы // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2012. – №2 (26), ч. 1. – С. 100–104.

3. Пат. №2069885 РФ МПК G02B26/10, G02B23/12, G01S17/88. Способ наблюдения объектов при пониженной освещенности и устройство для его осуществления / Правообладатель Йелстаун Корпорейшн Н.В.; заявл. 01.03.1996; опубл. 27.11.1996.

4. Дегтярев П.А. Зависимость коэффициента преобразования электронно-оптического преобразователя с микроканальной пластиной от напряжений на электродах // Вестник СО АН ВШ. – 2002. №1 (8). – С. 35–39.

Кирпиченко Юрий Романович
Канд. техн. наук, доцент каф. телевидения и управления ТУСУРа
Тел.: (382-2) 42-33-87
Эл. почта: urkirp@gmail.com

Kirpichenko Yu.R.

The dependence of image intensifier screen brightness on the electric potential on its electrodes

The results of experimental investigation of the electric potential variation influence on image intensifier phosphor screen brightness voltage on a microchannel plate can be approximated by a quadratic function. It is noticed that theoretical and experimental results are similar at low illumination and the dependence of image intensifier screen brightness on voltage on a microchannel plate can be approximated by a quadratic function.
Key words: photocathode, microchannel plate, image intensifier phosphor screen.

УПРАВЛЕНИЕ, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА

УДК 681.3

О.С. Авсентьев, А.Н. Бабкин, С.А. Бабкин

Организационно-техническое и правовое обеспечение безопасности инфокоммуникационных систем объектов «критической инфраструктуры» в Российской Федерации

Рассматриваются вопросы обеспечения информационной безопасности объектов «критической инфраструктуры» в Российской Федерации. К подобным объектам относятся объекты электроснабжения, теплоснабжения, связи и телекоммуникаций, транспортной инфраструктуры, правоохранительной системы и др. Представлена обобщенная модель ключевой системы информационной инфраструктуры.

Ключевые слова: информационная безопасность, объект критической инфраструктуры, защита информации, автоматизированная система управления, инфокоммуникационная система.

Результатом научно-технического прогресса последних десятилетий, определившим основное направление мирового развития, является широкое применение инфокоммуникационных систем (ИКС) и технологий для повышения эффективности функционирования основных государственных структур и их объектов «критической инфраструктуры».

В соответствии с основными руководящими документами ФСТЭК России под «критически важным объектом» понимается объект, оказывающий существенное влияние на национальную безопасность Российской Федерации. Прекращение или нарушение функционирования такого объекта приводит к чрезвычайной ситуации или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики или другой сферы деятельности страны.

Территориальная распределенность элементов ИКС «критически важного объекта» обусловливает жесткие требования к оперативности принятия управленческих решений по обеспечению безопасности его функционирования.

Это особо актуально для объектов, функционирование которых тесно связано с соответствующими муниципальными объектами, что в значительной степени усложняет проведение мероприятий организационно-технического и правового обеспечения безопасности их ИКС в условиях воздействия различного рода негативных факторов.

Одним из наиболее существенных факторов снижения эффективности ИКС объектов «критической инфраструктуры» являются угрозы нарушения информационной безопасности.

В соответствии с Доктриной информационной безопасности Российской Федерации [1] одной из важнейших составляющих ее национальных интересов в информационной сфере считается «… защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России».

Решение данной задачи должно осуществляться системно, на основе всестороннего исследования как информационных процессов, реализуемых в ИКС рассматриваемого типа, так и механизмов реализации угроз их информационной безопасности и технологий защиты информации. То обстоятельство, что подобные процессы, механизмы и технологии реализуются с использованием средств, характеризующихся множеством разнородных параметров, относит вопросы организационно-технического и правового обеспечения безопасности информации объектов «критической инфраструктуры» к числу сложных как в методическом, так и в практическом плане.

Это требует разработки нового подхода к синтезу систем защиты информации (СЗИ) и оценке их эффективности на объектах «критической инфраструктуры» в условиях воздействия угроз информационной безопасности. Суть этого подхода должна состоять в разработке методов и алгоритмов формирования СЗИ и аппарата системной оценки защищенности ИКС.

В процессе реализации данного подхода целесообразно выделить следующие задачи:

– определение перечня объектов, функционирование которых существенно зависит от состояния безопасности информационной инфраструктуры (определение объекта защиты). При этом с це-

лью достижения необходимого и достаточного уровня защищенности информации, циркулирующей в ИКС объектов «критической инфраструктуры», целесообразно определение ее ценности (степени конфиденциальности);

– выявление возможных угроз, связанных с функционированием ИКС этих объектов;

– оценка существующего нормативного и правового обеспечения защиты объектов «критической инфраструктуры» от несанкционированного доступа в их ИКС и формулировка предложений по их совершенствованию;

– проработка организационно-технических и правовых вопросов защиты этих объектов от целенаправленных противоправных воздействий на их ИКС;

– определение перечня субъектов, которые должны участвовать в обеспечении информационной безопасности данных объектов, с анализом их возможностей и готовности принять участие в работе.

Соответственно, информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), считается ключевой (критически важной) системой информационной инфраструктуры (КСИИ).

В этом случае обрабатываемая в КСИИ информация о состоянии критически важного объекта (процесса), информация о КСИИ (о ее составе, характеристиках программного и программно-аппаратного обеспечения, размещении, коммуникациях и др.), которая в случае ее хищения (ознакомления с ней) может быть непосредственно использована для деструктивных информационных воздействий, а также иная информация, уничтожение, блокирование или искажение которой может привести к нарушению функционирования КСИИ, является критически важной.

Под обеспечением безопасности информации в ключевых системах информационной инфраструктуры понимается деятельность, направленная на ликвидацию угроз или на минимизацию ущерба от реализации угроз безопасности информации в ключевых системах информационной инфраструктуры.

В соответствии с приведенной выше терминологией в качестве ИКС объекта «критической инфраструктуры» Российской Федерации будем понимать КСИИ как инфокоммуникационную систему, которая осуществляет управление критически важным объектом (процессом) и (или) информационное обеспечение управления таким объектом (процессом), или официальное информирование общества (граждан), в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация и (или) будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

Типовая обобщенная модель КСИИ, осуществляющая управление критически важным объектом (процессом), представлена на рис. 1 и включает следующие основные компоненты:

– управляющую подсистему;

– информационно-измерительную подсистему (контроля, регистрации);

– информационно-исполнительную подсистему;

– подсистему внешнего управления и контроля.

Центральным звеном КСИИ является управляющая подсистема, которая предназначена для выполнения следующих основных задач:

– анализ актуальных данных об управляемом (контролируемом) критически важном объекте (процессе);

– анализ управляющей информации от внешних управляющих объектов (административной подсистемы);

– принятие (на основе результатов анализа) решений по управлению критически важным объектом (процессом) или компонентами;

– генерация команд управления критически важным объектом (процессом) или компонентами КСИИ.

Информационно-измерительная подсистема предназначена для выполнения следующих основных задач:

– формирование информационных сообщений о параметрах (состоянии) управляемого критически важного объекта (процесса) с использованием соответствующих датчиков (средств измерения, контроля);

– сбор и передача информации о параметрах (состоянии) управляемого критически важного объекта (процесса) от датчиков в управляющую подсистем) с использованием соответствующих средств связи и передачи данных.

Информационно-исполнительная подсистема отвечает за передачу (или) интерпретацию управляющей информации (команд управления) от управляющей подсистемы к исполнительным средствам и системам, оказывающим соответствующее воздействие на управляемый критически важный объект (процесс).

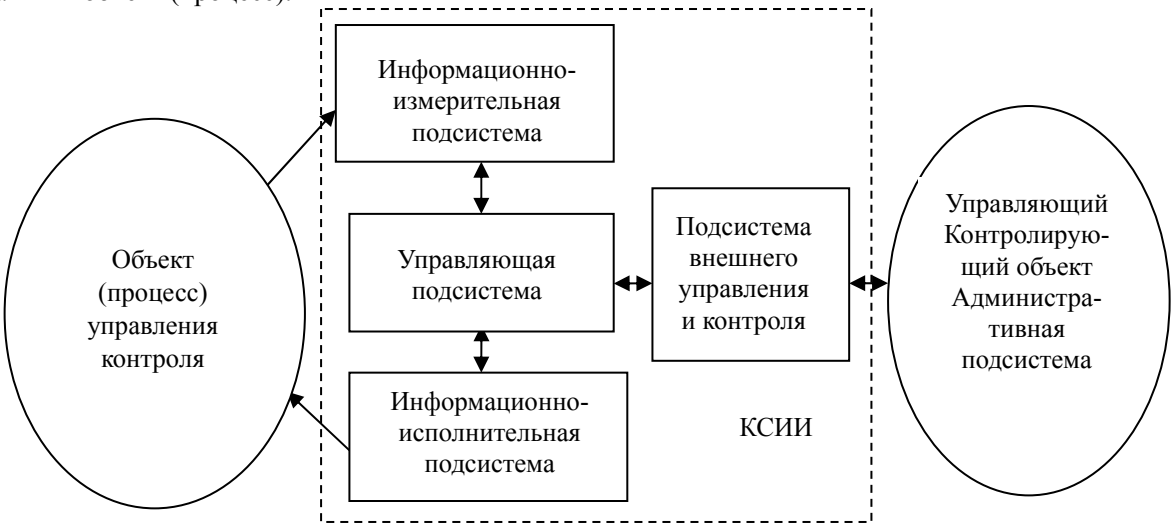


Рис. 1. Структурная схема ключевой системы информационной инфраструктуры

Подсистема внешнего управления и контроля обеспечивает взаимодействие управляющей подсистемы с внешним управляющим (контролирующим) объектом (процессом), осуществляющим администрирование КСИИ, и предназначена для выполнения следующих основных задач:

– сбор и передача управляющей подсистеме команд управления с внешних управляющих (контролирующих) объектов (процессов);

– передача статусной информации о состоянии КСИИ (ее компонентов) и (или) управляемого (контролируемого) критически важного объекта (процесса) от управляющей подсистемы внешним управляющим (контролирующим) объектам (процессам).

Подсистема внешнего управления может представлять собой автоматизированную систему (АС) «офисного типа» и (или) специализированные диспетчерские рабочие места.

В состав информационно-измерительной, информационно-исполнительной подсистем, а также подсистемы внешнего управления входит подсистема передачи данных, отвечающая за транспортировку всей циркулирующей в КСИИ информации. Эта подсистема включает средства, формирующие различные каналы передачи данных (проводные, оптоволоконные, радиоканалы и др.), а также средства, обеспечивающие интерфейс подсистемы передачи данных с основными подсистемами КСИИ.

Такие системы развернуты и функционируют в критически важных сегментах информационной инфраструктуры страны и включают [1, 2]:

- системы органов государственной власти;
- системы органов управления правоохранительных структур;
- системы финансово-кредитной и банковской деятельности;
- системы предупреждения и ликвидации чрезвычайных ситуаций;
- географические и навигационные системы;
- сети связи общего пользования на участках, не имеющих резервных или альтернативных видов связи;
- системы специального назначения;
- спутниковые системы, используемые для обеспечения органов управления и в специальных целях;
- системы управления добычей и транспортировкой нефти, нефтепродуктов и газа;
- системы управления водоснабжением;
- системы управления энергоснабжением;
- системы управления транспортом (наземным, воздушным, морским);

– системы управления потенциально опасными объектами;

– системы, которые не относятся к вышеуказанным, но нарушение штатного режима функционирования которых может привести к нарушению функций управления чувствительными для Российской Федерации процессами.

Как КСИИ, так и их элементы, а также обрабатываемая в них информация являются объектом воздействия различного рода угроз, а следовательно, и объектом защиты.

Указанные обстоятельства позволяют отнести КСИИ к сложным системам [4]. Используя аппарат теории множеств, определим их соответствия и композиции [3].

В качестве области отправления соответствия $\{O\}$ определим множество закономерностей функционирования КСИИ, ее демаскирующих признаков, каналов утечки информации, а в качестве области прибытия соответствия $\{П\}$ – множество закономерностей возникновения угроз, функционирования технических разведок (ТР), их возможностей по добыванию информации, циркулирующей в КСИИ, и сведений о ней.

Указанные соответствия представляются в виде композиции с областей интересов ТР к КСИИ в виде

$$c = (O, П, C), \quad (1)$$

где O – совокупность элементов, сопоставляемых с элементами $П$; $П$ – совокупность элементов, сопоставляемых с элементами O; $\{C \subset O \times П\}$ – множество, устанавливающее закон определения c, представляющий перечисление всех пар (o, n), участвующих в сопоставлении.

При этом допускается сопоставление ограниченного количества элементов множеств $\{O\}$, $\{П\}$, представляющих наиболее характерные закономерности воздействия угроз, функционирования КСИИ и ТР.

Содержание основных закономерностей функционирования КСИИ и ТР определяется их исключительным предназначением, разнообразием используемых технических средств и решаемых задач, обусловливающих свойства и признаки КСИИ, объективностью воздействия угроз и внимания со стороны ТР.

Данные закономерности могут быть представлены соответствующими областями отправления (2) и прибытия (3):

$$O=\{o_1, o_2, \ldots, o_n\}=\{o_i\}, \ i \in I, \ \ I=1,2, \ldots, n; \quad (2)$$

$$П=\{n_1, n_2, \ldots, n_m\}=\{n_j\}, \ \ j \in J, \ \ J=1,2,\ldots, m. \quad (3)$$

Содержательное описание законов соответствия, $C \subset O \times П$, может быть представлено произведением множеств:

$$O\&П=\{(o_i, n_j) | \ o_i \in O; \ n_j \in П\}; \ i = 1, 2, \ldots, n; \ j = 1, 2, \ldots, m. \quad (4)$$

Такое множество дает возможность получения ряда соответствий $c = (O, П, C)$, подтверждающих объективность усиленного внимания ТР к КСИИ.

Территориальная распределенность элементов КСИИ, увеличение объемов хранимой и передаваемой информации, жесткие требования к оперативности принятия управленческих решений для своевременного реагирования на нарушения безопасности функционирования объектов приводят к возрастанию количества преднамеренных и непреднамеренных угроз нарушения безопасности информации [5], возможных каналов ее утечки [6] и уязвимых звеньев несанкционированного доступа к информационным ресурсам этих объектов с целью чтения, копирования, подделки программного обеспечения, текстовой и другой информации [7].

С целью выявления возможных угроз, связанных с функционированием КСИИ объектов «критической инфраструктуры», целесообразно использовать базовую модель угроз безопасности информации, разработанную ФСТЭК России.

Нормативную правовую основу системы обеспечения безопасности объектов «критической инфраструктуры» составляют: Конституция Российской Федерации, Стратегия национальной безопасности Российской Федерации до 2020 года, законы Российской Федерации, указы Президента Российской Федерации, постановления Правительства Российской Федерации в сфере безопасности, защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, противодействия терроризму и экстремизму, обеспечения правопорядка, борьбы с преступностью.

Основными целями защиты информации в ИКС объектов «критической инфраструктуры» являются:

– достижение состояния защищенности информации во всех звеньях ИКС от внешних и внутренних угроз как в мирное время, так и в особый период, а также при возникновении чрезвычайных ситуаций;

− предотвращение нарушений прав личности, общества и государства на сохранение секретности и конфиденциальности информации, циркулирующей в ИКС.

На основании целей формируются и задачи защиты информации в ИКС объектов «критической инфраструктуры»:

− выявление и прогнозирование внутренних и внешних угроз информационной безопасности, разработка и осуществление комплекса адекватных и экономически обоснованных мер по их предупреждению и нейтрализации;

− формирование единой политики государственной власти и субъектов России по защите информации в ИКС;

− совершенствование и стандартизация применяемых методов и средств защиты информации в ИКС;

− создание и реализация механизма регулирования деятельности в области защиты информации объектов «критической инфраструктуры», а также обеспечение функционирования системы сертификации ИКС и входящих в их состав защищенных технических средств, средств защиты информации и средств контроля эффективности применяемых мер защиты.

Система обеспечения защиты информации в каждой конкретной ИКС, а также подход к ее построению и реализации - индивидуальны. Однако, во всех случаях для создания эффективной комплексной защиты информации необходимо:

1) выявить все возможные факторы, влияющие на уязвимость информации подлежащей защите, т.е. построить модель угроз информационной безопасности ИКС и выявить каналы утечки информации;

2) обосновать возможные методы защиты информации, направленные на устранение выявленных угроз;

3) создать комплексную систему, обеспечивающую качественное решение задач защиты информации в ИКС, основанную на минимизации ущерба от возможной утечки информации.

Литература

1. Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ № Пр-1895 от 9 сентября 2000 г.

2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. М.: Госстандарт России, 2008. – 9 с.

3. Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия–Телеком, 2006. – 544 с.

4. Советов Б.Я. Моделирование систем: учебник для вузов / Б.Я. Советов, С.А. Яковлев. – 3-е изд. – М.: Высш. шк., 2001. – 343 с.

5. Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. – Воронеж: Изд-во Воронежского гос. ун-та, 2002. – 408 с.

6. Заряев А.В. Источники и каналы утечки информации в телекоммуникационных системах: учеб. пособие для системы высшего профессионального образования МВД России / А.В. Заряев, В.Б. Щербаков и др. – Воронеж: Воронежский институт МВД России, 2003. – 94 с.

7. Защита информации в телекоммуникационных системах: учебник для вузов МВД России / С.В. Скрыль и др. – Воронеж: Воронежский институт МВД России, 2002. – 300 с.

Авсентьев Олег Сергеевич
Д-р техн. наук, профессор каф. информационной безопасности
Воронежского института МВД России (ВИ МВД России)
Тел.: (473) 200-52-40
Эл. почта: osaos@mail.ru

Бабкин Александр Николаевич
Канд. техн. наук, доцент, нач. каф. информационной безопасности ВИ МВД России
Тел.: (473) 200-52-40
Эл. почта: alex_babk@mail.ru., babkian@mail.vimvd.ru

Бабкин Сергей Александрович
Канд. техн. наук, доцент каф. физики
Воронежского института государственной противопожарной службы МЧС России
Тел.: (473) 277-86-53

Avsentjev O.S., Babkin A.N., Babkin S, A.

Organizational and technical and legal support of safety infocommunication systems of objects «critical infrastructure» in the Russian Federation

Questions of ensuring information security of objects of «critical infrastructure» in the Russian Federation are considered. Objects of power supply, heat supply, communication and telecommunications, transport infrastructure, law-enforcement system belong to similar objects, etc. The generalized model of key system of information infrastructure is presented.
Keywords: information security, object of critical infrastructure, information security, automated control system, infocommunication system.

УДК 519.4

М.И. Рожков

О некоторых характеристиках булевых функций без запрета от четырех переменных в связи с построением биективных отображений специального вида

Понижающие пары натуральных чисел $(h,t), h>t$, для функций без запрета $f=f(x_1,x_2,...,x_k)$ изучались ранее автором в связи с построением биективных отображений

$$B_{f,L}:(F_2)^n\to(F_2)^n, B_{f,L}(x)=(f(x),f(\delta(x)),...,f(\delta^{n-1}(x)),x\in(F_2)^n,$$

набор координатных функций которых задается преобразованием $\delta=\delta_L$ регистра сдвига длины n с функцией обратной связи L, существенно зависящей от ограниченного числа $s(1)$ начальных и $s(2)$ конечных аргументов, и нелинейной функцией съема $f=f(x_1,x_2,...,x_k)$ от k аргументов ($k<<n$). Наличие понижающей пары (h,t) сводит исходную задачу проверки биективности $B_{f,L}$ при больших значениях длины регистра n к проверке биективности соответствующих отображений применительно к регистрам сдвига ограниченной длины

$$n=n_0\in\{t+s(1)+s(2)-1,t+s(1)+s(2),...,h+s(1)+s(2)-2\},$$

что позволяет эффективно использовать для ее решения вычислительную технику. В настоящей работе рассматриваются алгоритмы нахождения понижающих пар (h,t) для функций без запрета от четырех переменных.

Ключевые слова: ортогональные системы функций, регистр сдвига, фильтрующий генератор, понижающее множество.

Основные понятия и обозначения. Далее в работе будем придерживаться следующих основных понятий и обозначений: F_2 – поле из двух элементов $\{0,1\}$; $(F_2)^n$ – пространство двоичных векторов длины n; $(f_1,f_2,...,f_m)$ – задание отображения $(F_2)^n\to(F_2)^m$ в виде системы координатных функций

$$L(x_1,x_2,...,x_n)=L(x_1,x_2,...,x_{s(1)},x_{n-s(2)+1},x_{n-s(2)+2},...,x_n),$$

$L(x_1, x_2, \ldots, x_n) = L(x_1, x_2, \ldots, x_{s(1)}, x_{n-s(2)+1}, x_{n-s(2)+2}, \ldots, x_n)$ – функция обратной связи регистра сдвига длины n, линейная по переменной x_1 (т.е. $L(x_1,x_2,...,x_n)=x_1+\lambda(x_2,x_3,...,x_n)$) и существенно зависящая от ограниченного числа крайних переменных ($s(1)\geq 1$, $s(2)\geq 0$, $n\geq s(1)+s(2)$ – заданные параметры); $\delta=\delta_L$ – преобразование векторов пространства $(F_2)^n$, осуществляемое регистром сдвига с функцией обратной связи $L=L(x_1,x_2,...,x_n)$, действующее на вектор $\mathbf{x}=(x_1,x_2,...,x_n)\in(F_2)^n$ по правилу

$$\delta(x_1,x_2,...,x_n)=(x_2,x_3,...,x_n,L(x_1,x_2,...,x_n));$$

$f(x_1,x_2,...,x_k)$ – функция от $k\geq 3$ аргументов без запретов (являющаяся фильтрующей функцией съема с соответствующего регистра сдвига); $B_{f,L}$ – преобразование двоичных векторов длины n, задаваемое следующей системой координатных функций:

$$B_{f,L}(x)=(f(x),f(\delta(x)),...,f(\delta^{n-1}(x)),x\in(F_2)^n.$$

Отметим, что преобразование $B_{f,L}$ можно рассматривать как отображение множества начальных заполнений двоичного регистра сдвига длины n с обратной связью L в множество наборов n символов выходной последовательности, снимаемой с данного регистра с помощью функции f.

В работах [1–4] рассматриваются вопросы выбора нелинейной функции съема $f:(F_2)^n\to F_2$, а также функции обратной связи L, при которых отображение $B_{f,L}$ является биективным. При этом биективность отображения $B_{f,L}$ равносильна ортогональности системы его координатных функций.

В работе [2] показано, что при $n \ge 2^{k-1}+k-1$ отсутствие запретов у функции $f(x_1,x_2,...,x_k)$ является необходимым условием биективности отображения $B_{f,L}$ (функции без запрета называют также функциями без потери информации, сильно равновероятными, а также совершенно уравновешенными [5, 6]).

Известно (см. [5]), что для функции без запретов $f(x_1,x_2,...,x_k)$ при любом фиксированном выходном слове $\mathbf{Y} = y(1), y(2),..., y(n)$ длины $n \ge 1$ существует ровно 2^{k-1} входных слов $x_1,x_2,...,x_k,x_{k+1},...,x_{n+k-1}$ (их множество обозначим $f^{-1}(\mathbf{Y})$), перерабатываемых данной функцией в **Y** по закону

$$y(j) = f(x_j,x_{j+1},...,x_{j+k-1}), j = 1,2,...,n.$$

Биективность отображения $B_{f,L}$ равносильна тому, что среди 2^{k-1} входных слов множества $f^{-1}(\mathbf{Y})$ ровно одно слово будет удовлетворять ограничениям

$$x_{n+1} = L(x) = L(x_1,x_2,...,x_n), x_{n+2} = L(\delta_L(x)),...,x_{n+k-1} = L((\delta_L)^{k-2}(x)). \quad (1)$$

При этом $x_{n+1},...,x_{n+k-1}$ как функции от независимых переменных $x_1,x_2,...,x_n$ (в силу ограничений на вид функции обратной связи *L*) зависят лишь от $k + s(1) - 2$ начальных переменных и от $s(2)$ последних переменных. Таким образом, выполняется ограничение (1) или нет (для данного входного слова $x_1,x_2,...,x_k,x_{k+1},...,x_{n+k-1}$) зависит только от его начального отрезка $x_1,x_2,...,x_{k+s(1)-2}$ длины $k+s(1) - 2$ и конечного отрезка $x_{n-s(2)+1},...,x_n,x_{n+1},...,x_{n+k-1}$ длины $k + s(2) - 1$.

Для заданных функции $f = f(x_1, x_2, ..., x_k)$, натуральных r, $s \ge k - 1$ и выходном слове $\mathbf{Y} = y(1), y(2),..., y(m)$ через $I = I(\mathbf{Y}) = I_{r,s}(\mathbf{Y})$ обозначим систему пар векторов

$$\{(\boldsymbol{\alpha}^{(i)}, \boldsymbol{\beta}^{(i)}) \mid i = 1,2,...,2^{k-1}\},$$

где $\boldsymbol{\alpha}^{(i)} = x_1, x_2,..., x_r$ и $\boldsymbol{\beta}^{(i)} = x_{m+k-s}, x_{m+k-s+1},..., x_{m+k-1}$ являются началом и концом входных слов $\mathbf{X} = x_1, x_2,..., x_k, x_{k+1},..., x_{n+k-1}$, перерабатываемых функцией *f* в выходное слово **Y**:

$$y(j) = f(x_j,x_{j+1},...,x_{j+k-1}), j = 1,2,...,m.$$

Так как число различных входов $X \in f^{-1}(\mathbf{Y})$, отвечающих заданному выходу **Y**, в точности равно 2^{k-1}, то полагаем, что $I(\mathbf{Y})$ состоит из 2^{k-1} элементов. При этом соответствующие системы $I(\mathbf{Y})$ и $I(\mathbf{Z})$ считаем равными ($I(\mathbf{Y}) = I(\mathbf{Z})$), если для любого $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in I(\mathbf{Y})$ данный элемент встречается в $I(\mathbf{Z})$ ровно столько раз, сколько он встречается в $I(\mathbf{Y})$.

Определение 1. Двоичные последовательности $\mathbf{Y} = y(1), y(2),..., y(n)$ и $\mathbf{Z} = z(1), z(2),..., z(m)$ назовем эквивалентными ($\mathbf{Y} \sim \mathbf{Z}$), если $I_{k-1,k-1}(\mathbf{Y}) = I_{k-1,k-1}(\mathbf{Z})$.

Определение 2. Пара натуральных чисел $(h,t), h > t$ называется понижающей парой для функции $f(x_1,x_2,...,x_k)$, если для любой последовательности **Y** длины *h* найдется эквивалентная ей последовательность **Z** длины *t*, причем каждая последовательность **Z** длины *t* эквивалентна некоторой последовательности **Y** длины *h*.

Известно [4], любая функция без запрета $f = f(x_1,x_2,...,x_k)$ обладает понижающей парой (*h, t*). Кроме того, если отображение $B_{f,L}$ биективно для

$$n = n_0 \in M = \{t + s(1) + s(2) - 1, t + s(1) + s(2),..., h + s(1) + s(2) - 2\},$$

тогда оно будет биективным при любом $n = n_0 + d \cdot (h - t), d = 0,1,...$. Тем самым вопрос о биективности отображений $B_{f,L}$ для всех достаточно больших n сводится к исследованию соответствующих отображений при ограниченных значениях n.

В работах [3–4] для некоторых функций f от $k \le 6$ переменных были найдены понижающие пары путем полного перебора всех выходных слов **Y** длины $n = h$ и слов **Z** длины $m = t$, вычисления множеств $f^{-1}(\mathbf{Y})$ и $f^{-1}(\mathbf{Z})$ с последующим поиском для слов **Y** эквивалентных им слов **Z**. Слож-

ность данного метода оценивается величиной $O(2^{h+t})$ операций, и на его основе могут быть найдены пары (h,t) при сравнительно небольшой величине $(h+t)\approx 40$.

В настоящей работе предложены алгоритмы, позволяющие для функций от четырех переменных вычислять понижающие пары (h, t) и при большей величине $(h + t)$.

Для заданной функции без запретов $f = f(x_1, x_2, ..., x_k)$ через $R(f)$ обозначим множество функций

$$R(f) = \{f(\mathbf{x}), f(\mathbf{x})+1, f(\mathbf{x}+\mathbf{e}), f(\mathbf{x}+\mathbf{e})+1, f(s(\mathbf{x})), f(s(\mathbf{x}))+1, f(s(\mathbf{x})+\mathbf{e}), f(s(\mathbf{x})+\mathbf{e})+1\},$$

где $\mathbf{e}$ – двоичный вектор с единичными координатами (преобразование $\mathbf{x}+\mathbf{e}$ заключается в инвертировании координат двоичного вектора $\mathbf{x}$), $s(\mathbf{x}) = s(x_1, x_2, ..., x_k) = (x_k, x_{k-1}, ..., x_1)$.

При экспериментальных расчетах понижающих пар полезным является следующее утверждение.

Теорема 1 [4, утв. 5]. *Пусть функция без запрета $f = f(x_1, x_2, ..., x_k)$ обладает понижающей парой (h,t). Тогда (h,t) будет понижающей парой для любой функции $\varphi \in R(f)$.*

Алгоритм 1 (определение понижающей пары для функции, линейной по крайней переменной). Пусть $f(x_1, x_2, ..., x_k) = \varphi(x_1, x_2, ..., x_{k-1}) + x_k$. Известно [3], двоичные последовательности $\mathbf{Y} = y(1), y(2), ..., y(n)$ и $\mathbf{Z} = z(1), z(2), ..., z(m)$ являются эквивалентными, если и только если при любом $\boldsymbol{\alpha} \in (F_2)^{k-1}$

$$\delta_{y(n)}\delta_{y(n-1)}...\delta_{y(1)}(\alpha) =, \delta_{z(m)}\delta_{z(m-1)}...\delta_{z(1)}(\alpha) \qquad (2)$$

где $\delta_\varepsilon(x_1, x_2, ..., x_{k-1}) = (x_2, x_3, ..., x_{k-1}, \varphi(x_1, x_2, ..., x_{k-1}) + \varepsilon)$.

Алгоритм расчета понижающих пар (h,t) для функций рассматриваемого вида основан на том, что в соответствии с равенством (2) множество окончаний длины k–1 векторов из множества $f^{-1}(\mathbf{Y})$ задается набором из 2^{k-1} двоичных векторов длины k–1 каждый, т.е. двоичным вектором длины $(k-1)\cdot 2^{k-1}$. Другими словами, для фиксации всех возможных элементов множества $I_s = \cup I_{k-1,k-1}(\mathbf{Y})$ (объединение проводится по всем словам $\mathbf{Y}$ длины s) достаточно иметь массив

$$\text{ARRAY}[\,\omega\,] \text{ бит}, \ \omega = 2^r, r = (k-1)\cdot 2^{k-1},$$

в который по соответствующему адресу ставится метка, если адрес принадлежит множеству I_s. При этом если массив ARRAY_1 заполнен для слов длины s, для вычисления множества I_{s+1} (т.е. заполнения массива ARRAY_2) достаточно перебрать адреса массива ARRAY_1, по которым установлена специальная метка. Из каждого такого адреса, интерпретируемого как набор 2^{k-1} двоичных векторов длины k–1, путем применения отображений δ_φ и $\delta_{\varphi+1}$ к его компонентам, вычисляется два новых вектора-адреса, по которым в массив ARRAY_2 заносятся соответствующие метки. Это позволяет вычислять множество I_s за $O(s\cdot\omega)$ операций. Данная сложность при фиксированном k и $s \to \infty$ существенно меньше величины $O(2^s)$, которой оценивается сложность вычисления элементов множества I_s путем прямой обработки всех 2^s слов длины s. И соответственно для проверки понижающей пары (h,t) потребуется $O((t+h)\cdot\omega)$ операций и $O(\omega)$ бит оперативной памяти.

Замечание. В силу теоремы 1 рассмотренный выше алгоритм применим и для функций, линейных по первой переменной $f(x_1, x_2, ..., x_k) = \varphi(x_2, x_3, ..., x_k) + x_1$. С помощью указанного алгоритма были найдены понижающие пары для всех нелинейных функций без запрета от 4 переменных $f(x_1, x_2, x_3, x_4)$, которые линейны по одной из крайних переменных. При этом для фиксации элементов каждого из множеств I_h и I_t требуется память объема 16 Мбит.

Алгоритм 2 (определение понижающей пары для функции общего вида). Пусть $f(x_1, x_2, ..., x_k)$ – произвольная булева функция без запрета, $\boldsymbol{\alpha}$ – заданный двоичный вектор длины k–1. Для заданном выходном слове $\mathbf{Y}$ длины s соответствующая система векторов

$$I_{k-1,k-1}(\mathbf{Y}) = \{(\boldsymbol{\alpha}^{(i)}, \boldsymbol{\beta}^{(i)}) \mid i = 1,2,...,2^{k-1}\},$$

однозначно задается видом векторов $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ и числом их вхождения в систему $I_{k-1,k-1}(\mathbf{Y})$.

Таким образом, число различных систем $I_{k-1,k-1}(\mathbf{Y})$ не более числа сочетаний с повторениями из $2^{2(k-1)}$ элементов по 2^{k-1}, т.е. величины [7]

$$\omega = \frac{(2^{2(k-1)} + 2^{k-1} - 1)!}{(2^{k-1}!) \cdot ((2^{2(k-1)} - 1)!)}.$$

Будем считать, что множеству различных систем $I_{k-1,k-1}(\mathbf{Y})$ поставлено во взаимно однозначное соответствие множество целых чисел $0 \le j \le \omega$. Следовательно, применительно к функциям от k переменных для фиксации всех наборов $I_s = \cup I_{k-1,k-1}(Y)$ (объединение проводится по всем словам $\mathbf{Y}$ длины s) достаточно иметь массив ARRAY[ω] объема ω бит. При этом по адресу j ставится метка (бит «1»), если система $\{(\alpha^{(i)},\beta^{(i)}) | i = 1,2,...,2^{k-1}\}$ принадлежит множеству I_s (в противном случае по адресу j находится «0»).

Если заполнен массив ARRAY_1 для слов длины s, для вычисления множества I_{s+1} (т.е. заполнения массива ARRAY_2) перебираются адреса массива ARRAY_1, по которым установлена метка. Из каждого такого адреса, интерпретируемого как система $I_{k-1,k-1}(\mathbf{Y}) = \{(\boldsymbol{\alpha}^{(i)}, \boldsymbol{\beta}^{(i)}) \mid i = 1,2,...,2^{k-1}\}$, вычисляются две новых системы и соответствующие им адреса, по которым в массив ARRAY_2 заносятся соответствующие метки. Новые две системы строятся следующим образом. Первая система отвечает слову длины s+1, у которого последний знак равен 0. Вторая система отвечает случаю, когда последний знак равен 1. Пусть $(\boldsymbol{\alpha},\boldsymbol{\beta})$ встречается в исходной системе $d = d_{\alpha,\beta}$ раз, $\boldsymbol{\alpha} = (\delta_1,\delta_2,...,\delta_{k-1})$, $\boldsymbol{\beta} = (\theta_1,\theta_2,...,\theta_{k-1})$. Пусть при этом $(\alpha,\gamma) = 0$, $f(\theta_1,\theta_2,...,\theta_{k-1},\varepsilon) = 1$. Тогда в первой новой системе вектор $(\boldsymbol{\alpha},\boldsymbol{\gamma})$ встречается d раз, где $\boldsymbol{\gamma} = (\theta_2,\theta_3,...,\theta_{k-1},\varepsilon)$. И одновременно во второй новой системе d раз встретится вектор $(\boldsymbol{\alpha},\boldsymbol{\gamma}^{\bullet})$, где $\boldsymbol{\gamma}^{\bullet} = (\theta_2,\theta_3,...,\theta_{k-1},\varepsilon+1)$.

Замечание. Отметим, что разные вектора $\boldsymbol{\beta}$ исходной системы могут приводить к одинаковым векторам $\boldsymbol{\gamma}$ и $\boldsymbol{\gamma}^*$ в новой системе. Если же $f(\theta_1,\theta_2,...,\theta_{k-1},0) = f(\theta_1,\theta_2,...,\theta_{k-1},1) = 0$, тогда в первой новой системе вектор $(\boldsymbol{\alpha},\boldsymbol{\gamma})$, $\boldsymbol{\gamma} = (\theta_2,\theta_3,...,\theta_{k-1},0)$ встретится d раз и d раз встретится вектор $(\boldsymbol{\alpha},\boldsymbol{\gamma}^{\bullet})$, $\boldsymbol{\gamma}^{\bullet} = (\theta_2,\theta_3,...,\theta_{k-1},1)$. При этом во второй новой системе исходный вектор $(\boldsymbol{\alpha},\boldsymbol{\beta})$ ничего не порождает. Аналогичная ситуация возникает и при $f(\theta_1,\theta_2,...,\theta_{k-1},0) = f(\theta_1,\theta_2,...,\theta_{k-1},1) = 1$.

Указанный алгоритм позволяет вычислять множество I_s за $O(s \cdot \omega)$ операций. Данная сложность при $s \to \infty$ и фиксированном k существенно меньше величины $O(2^s)$, которой оценивается сложность вычисления элементов множества I_s путем прямой обработки всех 2^s слов длины s.

В частности, применительно к функции от 4 переменных для фиксации элементов каждого из множеств I_h и I_t требуется память объема $\omega = (71!)/((7!)\cdot(64!)) \cong 10^{10}$ бит.

Случай функции $f(x_1,x_2,...,x_k)$ при $k = 3$. Так как функции без запрета от трех переменных $f = f(x_1,x_2,x_3)$ являются линейными по одному из крайних переменных, то с учетом теоремы 1 множество понижающих пар нелинейных функций без запрета от k = 3 переменных задается понижающими парами (h, t) функций $f_1 = x_1x_2 + x_2 + x_3$, для которой (h, t) = (6,4), и $f_2 = x_1x_2 + x_3$, для которой (h, t) = (11,8).

Случай функции $f(x_1,x_2,...,x_k)$ при k=4. С учетом теоремы 1 совокупность понижающих пар (h, t) для нелинейных функций ($\deg(f) \ge 2$) без запрета от k = 4 переменных, которые существенно зависят от крайних аргументов и одновременно линейны хотя бы по одному из них, задается парами (h, t) для нижеприведенных в таблице первых 62 функций вида $f(x_1,x_2,x_3,x_4) = \varphi(x_1,x_2,x_3) + x_4$. При этом функция f приводится в форме многочлена Жегалкина, а вспомогательная функция φ посредством целого числа $\varphi = c$, задающего ее значения на векторах $(x_1,x_2,x_3) = x = x_1 + 2\cdot x_2 + 4\cdot x_3$ по формуле $\varphi(x) = (c >> x)\%2$, (здесь правая часть задается соответствующими операторами языка программирования СИ). Понижающие пары (h, t) для этих функций

при $h + t > 40$ были найдены с использованием идей алгоритма 1. При этом для фиксации элементов каждого из множеств I_h и I_t требуется память объема 16 Мбит.

В таблице приведены также представители всех 8 классов $R(f)$ нелинейных функций без запрета, которые существенно зависят от крайних аргументов и одновременно не являются линейными ни по одному из крайних аргументов. Это функции с порядковыми номерами с 63 по 70. Соответствующие результаты были получены экспериментальными методами путем выделения функций $f(x_1,x_2,x_3,x_4)$ с равномерным распределением выходных $2^{k-1}= 8$ грамм. Кроме того, последние три функции таблицы являются линейными. Для всех этих функций понижающие пары вычислялись путем прямой обработки всех выходных слов длин h и t, т.е. без использования идей алгоритма 2.

Для трех функций из таблицы, для которых прямой метод не привел к нахождению понижающих пар, практическая сложность реализации идей алгоритма 2 связана с необходимостью использования памяти объема $\omega =(71!)/((7!)\cdot(64!))\cong 10^{10}$ бит (для фиксации элементов каждого из множеств I_h и I_t).

Перечень функций и их понижающих пар

п/п	φ	F	(h, t)
1	*2*	*3*	*4*
1	2	$x_1 + x_1x_2 + x_1x_3 + x_1x_2x_3 + x_4$	9,6
2	4	$x_2 + x_1x_2 + x_2x_3 + x_1x_2x_3 + x_4$	11,9
3	6	$x_1 + x_2 + x_1x_3 + x_2x_3 + x_4$	36,27
4	8	$x_1x_2 + x_1x_2x_3 + x_4$	8,5
5	10	$x_1 + x_1x_3 + x_4$	36,24
6	14	$x_1 + x_2 + x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_4$	12,10
7	18	$x_1 + x_1x_2 + x_3 + x_2x_3 + x_4$	50,46
8	20	$x_2 + x_1x_2 + x_3 + x_1x_3 + x_4$	51,27
9	22	$x_1 + x_2 + x_3 + x_1x_2x_3 + x_4$	49,45
10	24	$x_1x_2 + x_3 + x_1x_3 + x_2x_3 + x_4$	23,17
11	26	$x_1 + x_3 + x_2x_3 + x_1x_2x_3 + x_4$	74,68
12	28	$x_2 + x_3 + x_1x_3 + x_1x_2x_3 + x_4$	18,15
13	30	$x_1 + x_2 + x_1x_2 + x_3 + x_4$	50,46
14	34	$x_1 + x_1x_2 + x_4$	21,15
15	36	$x_2 + x_1x_2 + x_1x_3 + x_2x_3 + x_4$	59,55
16	38	$x_1 + x_2 + x_2x_3 + x_1x_2x_3 + x_4$	45,39
17	42	$x_1 + x_1x_2x_3 + x_4$	34,31
18	44	$x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_4$	19,16
19	46	$x_1 + x_2 + x_1x_2 + x_2x_3 + x_4$	20,17
20	50	$x_1 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_4$	25,21
21	54	$x_1 + x_2 + x_3 + x_1x_3 + x_4$	67,63
22	58	$x_1 + x_3 + x_1x_3 + x_2x_3 + x_4$	47,37
23	62	$x_1 + x_2 + x_1x_2 + x_3 + x_1x_3 + x_1x_2x_3 + x_4$	28,24
24	66	$x_1 + x_1x_2 + x_1x_3 + x_2x_3 + x_4$	20,17
25	70	$x_1 + x_2 + x_1x_3 + x_1x_2x_3 + x_4$	30,29
26	74	$x_1 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_4$	48,33
27	78	$x_1 + x_2 + x_1x_2 + x_1x_3 + x_4$	61,56
28	86	$x_1 + x_2 + x_3 + x_2x_3 + x_4$	23,21
29	94	$x_1 + x_2 + x_3 + x_1x_2 + x_2x_3 + x_1x_2x_3 + x_4$	44,40
30	110	$x_1 + x_2 + x_1x_2 + x_1x_2x_3 + x_4$	115,95
31	126	$x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_4$	59,55
32	142	$x_1 + x_2 + x_1x_2 + x_1x_3 + x_2x_3 + x_4$	21,15
33	158	$x_1 + x_2 + x_3 + x_1x_2 + x_1x_2x_3 + x_4$	29,28
34	166	$x_1 + x_2 + x_2x_3 + x_4$	11,9
35	174	$x_1 + x_2 + x_1x_2 + x_2x_3 + x_1x_2x_3 + x_4$	44,38

Продолжение таблицы

1	*2*	*3*	*4*
36	178	$x_1 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_4$	12,8
37	182	$x_1 + x_2 + x_3 + x_1x_3 + x_1x_2x_3 + x_4$	42,38
38	186	$x_1 + x_3 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_4$	65,35
39	190	$x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_4$	37,25
40	194	$x_1 + x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_4$	25,22
41	198	$x_1 + x_2 + x_1x_3 + x_4$	53,43
42	202	$x_1 + x_1x_3 + x_2x_3 + x_4$	47,32
43	206	$x_1 + x_2 + x_1x_2 + x_1x_3 + x_1x_2x_3 + x_4$	31,26
44	210	$x_1 + x_3 + x_1x_2 + x_4$	28,22
45	212	$x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_4$	18,15
46	214	$x_1 + x_2 + x_3 + x_2x_3 + x_1x_2x_3 + x_4$	65,53
47	218	$x_1 + x_3 + x_1x_2x_3 + x_4$	108,101
48	220	$x_2 + x_3 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_4$	15,13
49	222	$x_1 + x_2 + x_3 + x_1x_2 + x_2x_3 + x_4$	13,9
50	226	$x_1 + x_1x_2 + x_2x_3 + x_4$	23,20
51	228	$x_2 + x_1x_2 + x_1x_3 + x_4$	44,38
52	230	$x_1 + x_2 + x_1x_2x_3 + x_4$	82,75
53	232	$x_1x_2 + x_1x_3 + x_2x_3 + x_4$	12,8
54	234	$x_1 + x_2x_3 + x_1x_2x_3 + x_4$	63,53
55	236	$x_2 + x_1x_3 + x_1x_2x_3 + x_4$	31,27
56	238	$x_1 + x_2 + x_1x_2 + x_4$	61,56
57	242	$x_1 + x_3 + x_1x_2 + x_1x_3 + x_1x_2x_3 + x_4$	18,12
58	244	$x_2 + x_3 + x_1x_2 + x_2x_3 + x_1x_2x_3 + x_4$	12,11
59	246	$x_1 + x_2 + x_3 + x_1x_3 + x_2x_3 + x_4$	45,33
60	248	$x_3 + x_1x_2 + x_1x_2x_3 + x_4$	18,12
61	250	$x_1 + x_3 + x_1x_3 + x_4$	31,23
62	254	$x_1 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_4$	15,11
63		$g_1(x) = x_2 + x_3 + x_1x_3 + x_1x_4 + x_1x_2x_3 + x_1x_2x_4$	15,12
64		$g_2(x) = x_1 + x_2 + x_3 + x_1x_2 + x_2x_4 + x_1x_3x_4$	18,12
65		$g_3(x) = x_3 + x_1x_2 + x_2x_3 + x_2x_4 + x_1x_2x_3 + x_1x_2x_4$	14,8
66		$g_4(x) = x_2 + x_3 + x_1x_4 + x_2x_4 + x_3x_4 + x_1x_3x_4 + x_2x_3x_4$	Не найдено
67		$g_5(x) = x_2 + x_3 + x_4 + x_1x_4 + x_2x_4 + x_1x_3x_4 + x_2x_3x_4$	Не найдено
68		$g_6(x) = x_1 + x_3 + x_2x_4 + x_1x_2x_4$	Не найдено
69		$g_7(x) = x_2 + x_1x_3 + x_1x_3x_4$	9,7
70		$g_8(x) = x_2 + x_3 + x_1x_3 + x_3x_4 + x_1x_3x_4$	6,5
71		$l_1(x) = x_1 + x_4$	6,3
72		$l_2(x) = x_1 + x_2 + x_4$	10,3
72		$l_3(x) = x_1 + x_2 + x_3 + x_4$	7,3

Заключение. В настоящей работе предложены алгоритмы вычисления понижающих пар для булевых функций без запрета от четырех переменных. Данная характеристика имеет важное значение для построения биективных отображений $B_{f,L}$, задаваемых регистром сдвига большой длины n с функцией обратной связи $L(x_1,x_2,...,x_n)$, которая зависит от ограниченного числа крайних переменных, и нелинейной функцией-фильтром $f = f(x_1,x_2,...,x_k)$ от небольшого числа переменных $k << n$.

На основе данных алгоритмов найдены понижающие пары для почти всех функций без запрета от четырех переменных. Ранее аналогичные результаты были известны только для некоторых таких функций.

Полученные результаты могут быть полезны при построении и обосновании статистических свойств датчиков случайных последовательностей на основе фильтрующих генераторов.

Литература

1. Саранцев А.В. Построение регулярных систем однотипных двоичных функций с использованием регистра сдвига // Лесной вестник. – 2004. – № 1 (32). – С. 164–169.

2. Рожков М.И. К вопросу построения ортогональных систем двоичных функций с использованием регистра сдвига // Лесной вестник. – 2011. – № 3 (79). – С. 180–185.

3. Рожков М.И. Ортогональные системы булевых функций на выходе фильтрующего генератора // Промышленные АСУ и контроллеры. – 2014. – № 1. – С. 31–36.

4. Рожков М.И. Биективные отображения, порождаемые фильтрующим генератором // Прикладная дискретная математика. – 2014. – № 1 (23). – С. 27–39.

5. Сумароков С. Н. Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикл. и промышл. матем., сер. дискретн. матем. – 1994. – Т. 1, вып. 1. – С. 33–35.

6. Логачев О.А. Новые методы изучения совершенно уравновешенных булевых функций / О.А. Логачев, С.В. Смышляев, В.В. Ященко // Дискретная математика. – 2009. – Т. 22, № 2. – С. 51–74.

7. Холл М. Комбинаторика. – М.: Мир, 1970. – 424 с.

Рожков Михаил Иванович
Д-р техн. наук, канд. физ.-мат. наук, ст. науч. сотр., доцент каф. «Компьютерная безопасность» Национального исследовательского университета «Высшая школа экономики», Москва
Тел.: 8 (495) 916-35-04
Эл. почта: rozhkov.m.i@yandex.ru

Rozhkov M.I.

On some characteristics of Boolean functions without prohibition of four variables in connection with the construction of bijective mappings of a special type

In the work we consider the algorithms of lowering pairs finding for functions without prohibition of four variables. Lowering (or restrictive) pairs of natural numbers (h, t), $h > t$ for functions without prohibition was studied earlier by the author in connection with the construction of bijective mappings $B_{f,L}$ defined by the shift register of length n with feedback function L, essentially dependent on a limited number of initial and final arguments, and a nonlinear function of removal of k arguments ($k << n$).

Keywords: orthogonal system of Boolean functions, feedback shift register, filter generator, restrictive multitude.

УДК 004.051

Ю.В. Алейнов

Метод повышения эффективности обнаружения сетевых атак неизвестного типа путем внедрения ложных целей в состав сети

Рассмотрен метод повышения эффективности обнаружения вторжений неизвестного типа, основанный на внедрении в сеть ложных целей. Предложена модель, позволяющая в каждый момент времени связать вероятность атаки на ложную цель с параметрами ложных целей, защищаемой сети и внешней среды. Описан обобщенный метод получения оптимальной конфигурации ложных целей в сети в условиях меняющихся со временем входных параметров.
Ключевые слова: обнаружение вторжений, ложные цели, повышение эффективности.

Одним из важнейших направлений исследований в области информационной безопасности является обнаружение вторжений. В настоящее время существует много способов выявления фактов компьютерных атак разных типов. Среди них всегда особо выделялись те способы, которые позволяют обнаруживать атаки ранее неизвестного вида. Для обнаружения таких атак применяется, как правило, подход, основанный на идентификации аномального поведения в сети. Часто предлагается использовать различные эвристики для выявления заведомо отличного от нормального поведения [1, 2]. В частности, можно предложить эвристику, основанную на предположении о том, что легальный пользователь не будет обращаться к неизвестному для него объекту в сети. Для использования этой эвристики необходимо разместить в сети системы, не участвующие в других производственных процессах и не анонсируемые как работающие сетевые сервисы – так называемые ложные цели (ЛЦ). Любая сетевая активность такой ложной цели является подозрительной и должна рассматриваться как злонамеренная [3, 4]. В данной статье рассмотрена модель, позволяющая оценивать эффективность применения описанной эвристики в зависимости от параметров сети и ложных целей внутри нее, а также метод расчета параметров ложных целей в сети.

Модель сети, содержащей ложные цели. Отличительной особенностью рассматриваемой эвристики является то, что ее эффективность зависит от доли общего числа атак, приходящейся на ложные цели. В свою очередь, она определяется соотношением числа ложных и реальных целей в сети и другими их параметрами. Рассмотрим подробнее модель, позволяющую связать искомую эффективность с параметрами ложных и реальных целей.

Основным понятием рассматриваемой модели является понятие цели. Под целью будем понимать работающий на хосте в сети процесс, выполняющий определенный программный код. Так как очень часто сетевые атаки направлены на эксплуатацию уязвимостей в прикладном программном обеспечении, такое понимание цели можно считать обоснованным [5]. Атакой в рамках рассматриваемой модели будем называть следующую последовательность шагов, выполняемую атакующей стороной:

1) выбор по некоторому правилу цели для очередной атаки;
2) проверка наличия у цели подходящей уязвимости;
3) попытка эксплуатации уязвимости.

Как правило, любая атака ориентирована на некоторый набор уязвимостей программного кода. Таким образом, имеет смысл группировать цели в классы по признаку его совпадения (C_j на рис. 1). Каждый такой класс будет содержать как реальные, так и ложные цели.

Будем считать, что атакующая сторона представлена множеством копий вредоносного программного обеспечения, каждая из которых циклически осуществляет попытки атаки на сеть. Попытки атак совершаются в дискретные моменты времени. Можно предположить наличие большого количества независимых источников атак в каждый момент времени. Следовательно, можно рассматривать суммарный поток атак от этих источников, считая его простейшим. Очевидно, в условиях изменяющихся характеристик внешней среды будут меняться и параметры регистрируемого потока атак, но будем считать, что всегда можно выбрать такой промежуток времени, в течение

которого этот поток можно считать простейшим. В этом случае достаточно рассматривать состояние внешней среды в дискретные моменты времени, соответствующие промежуткам стационарности параметров регистрируемых потоков атак. При этом само состояние будет определяться параметрами этих потоков, а воздействие на защищаемую сеть атакующей стороны можно описать множеством независимых потоков атак, по одному на каждый класс целей (рис. 1).

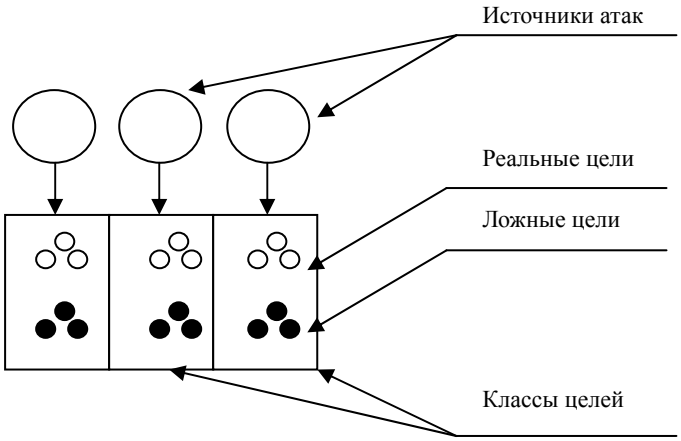


Рис. 1. Схема взаимодействия компонентов модели

Рассмотрим вероятность атаки на какую-либо ложную цель в сети на каждом промежутке стационарности параметров потоков атак. В силу введенных определений и предположений, эта вероятность равна сумме таких вероятностей по всем классам целей. Справедливо следующее выражение для указанной вероятности:

$$P = \sum_{i=1}^{k} P\{t \in C_i\} \frac{f_i}{f_i + r_i}, \qquad (1)$$

где $P\{t \in C_i\}$ – вероятность выбора на следующем шаге цели из класса C_i; f_i и r_i – количество ЛЦ и РЦ соответственно в классе C_i, а k – число классов целей.

Вероятность выбора цели из определенного класса на практике можно определить как отношение среднего числа атак на цели этого класса к общему количеству атак на все цели сети. Эти средние значения можно определить с помощью понятия интенсивности (I) потока атак. Наилучшей в смысле предложенной модели будет являться такая конфигурация параметров ЛЦ в сети, которая обеспечит максимальное значение P при заданных ограничениях на количество ЛЦ в каждом классе. Это справедливо для фиксированного момента времени.

Пусть теперь интенсивность атакующих воздействий для каждого класса целей меняется со временем. Если вычислять оптимальную конфигурацию ЛЦ на каждом шаге без учета внесенных ранее изменений, то есть опасность того, что некоторые ЛЦ, внедренные в сеть малое время назад, будут удалены на следующем шаге. Очевидно, это не даст им исполнить свою функцию и потенциально может привести к их раскрытию. Таким образом, рассматривая модель в динамике, необходимо учитывать такой значимый параметр цели, как время, прошедшее с момента ее появления, или время доступности. Каждый класс можно охарактеризовать распределением времени доступности целей этого класса. Можно сформулировать следующее ограничение: распределение времени доступности ЛЦ не должно отличаться от распределения времени доступности РЦ в этом же классе. Данное ограничение прямо следует из основного принципа внедрения ложных объектов в сеть: для того чтобы атакующий не смог раскрыть факт его дезинформации, ложный объект должен как можно меньше отличаться от реального.

Еще одно ограничение, связанное с этим же принципом, заключается в необходимости сохранять устойчивые наборы сервисов, находящихся на одном хосте при внедрении ложных целей. Кроме того, обычно присутствует ограничение на максимальное число хостов – «носителей» ложных целей.

Итак, можно перечислить следующие параметры целей, влияющие с точки зрения принятой модели на эффективность эвристики:

1) принадлежность цели к определенному классу с точки зрения совпадения исполняемого кода;

2) принадлежность цели к классу реальных или ложных целей;

3) момент времени, когда цель стала доступной в сети;

4) хост, на котором расположена цель.

Для сети в целом вычисляются такие параметры, как:

1) количество классов целей по признаку совпадения исполняемого кода;

2) распределение времени доступности цели в каждом классе;

3) множество комбинаций реальных целей, размещенных на каждом хосте;

4) количество реальных и ложных целей в каждом классе, а также максимально возможное число хостов, несущих ложные цели.

Формально модель можно записать следующим образом, учитывая (1):

$$\begin{cases} P = \sum\limits_{j=1}^{k} \dfrac{I_j}{I} \dfrac{f_j}{f_j + r_j} = \max, \\ \sum\limits_{i=1}^{k} \alpha_i x_i \le N, \\ P\left(\tau_j^F < \tau\right) = P\left(\tau_j^R < \tau\right), \end{cases} \quad (2)$$

где k – число классов целей в сети; I_j – интенсивность атак на цели класса C_j; I – интенсивность атак на цели всех классов; $x_j \in X$ – фиксированный набор типов целей (конфигурация хоста) из множества всех имеющихся конфигураций в сети; α_j – число хостов с ложными целями, соответствующих конфигурации x_j; N – максимальное число хостов с ложными целями; τ_j^F и τ_j^R – время доступности ложной и реальной целей соответственно (в классе целей C_j).

Метод определения оптимальных параметров ложных целей. В обобщенном виде метод заключается в итеративном выполнении следующих действий:

1. Получение входных параметров модели и исходной конфигурации ЛЦ.

2. Вычисление оптимальной конфигурации ЛЦ с помощью решения задачи оптимизации, задаваемой моделью (2).

3. На каждом шаге определение возможных управляющих воздействий для приближения текущей конфигурации ЛЦ к вычисленной на предыдущем шаге. При этом следует проводить оценку схожести распределений времени доступности РЦ и ЛЦ.

4. Среди возможных управляющих воздействий выбираются такие, которые обеспечивают максимальный рост вероятности выбора атакующим ЛЦ.

5. При изменении параметров модели оптимальная конфигурация должна быть вычислена вновь.

Данный метод позволяет поддерживать такую конфигурацию ложных целей в защищаемой сети, которая обеспечит максимальный поток атак на детекторы системы обнаружения вторжений (внедренные ложные цели) с учетом изменения характера внешнего воздействия на защищаемую сеть, а также с учетом изменения ее параметров.

Заключение. В данной статье предложена модель, описывающая работу системы обнаружения вторжений, использующей ложные цели, внедренные в адресное пространство защищаемой сети для повышения эффективности детектирования атак неизвестного типа. Предложен метод определения необходимых параметров ложных целей, обеспечивающий наибольший поток атак на ложные цели, что является условием максимальной эффективности применения данной эвристики. Отличительной особенностью предложенного метода является использование в качестве входных данных наиболее простых параметров сети, таких как размер адресного пространства, интенсивность потоков атак, количество ложных и реальных целей. В качестве основного направления дальнейших исследования в этой области можно назвать экспериментальную проверку предложенного метода и соотнесение результатов с расчетными.

Литература

1. Allen J. State of Practice of intrusion detection technologies : Technical Report / J. Allen, A. Christie, W. Fithen et al. – Pittsburgh: Carnegie Mellon Software Engineering Institute, 2000. – 242 с.

2. Милославская Н.Г. Интрасети: обнаружение вторжений: учеб/ пособие для вузов / Н.Г. Милославская, А.И. Толстой. – М.: Юнити-Дана, 2001. – 592 с.

3. Котенко И.В. Обманные системы для защиты информационных ресурсов в компьютерных сетях / И.В. Котенко, М.В. Степашкин // Труды СПИИРАН. – 2004. – Вып. 2, т. 1. – С. 211–230.

4. Правиков Д.И. Использование виртуальных ловушек для обнаружения телекоммуникационных атак / Д.И. Правиков, П.В. Закляков // Проблемы управления безопасностью сложных систем: труды междунар. конф. – М., 2002. – Ч. 1. – С. 310–314.

5. Боршевников А.Е. Сетевые атаки. Виды. Способы борьбы // Современные тенденции технических наук: материалы междунар. науч. конф., г. Уфа, октябрь 2011 г. – Уфа, 2011. – С. 8–13.

Алейнов Юрий Викторович
Аспирант каф. безопасности информационных систем Самарского государственного университета
Тел.: 8 (917) 812-9568
Эл. почта: aleinov@gmail.com

Aleinov Y.V.

The method for increasing the efficiency of unknown type intrusion detection by introducing false targets in the network

A method of increasing the efficiency of unknown type intrusion detection, based on using of decoys in the network, is suggested. A model that allows to tie likelihood of an attack on a decoy for each time with parameters of decoys, network and the external environment is described. A generalized method for obtaining the optimal configuration of decoys in the network in a time-varying input parameters is shown.
Keywords: intrusion detection, decoys, increasing efficiency.

УДК 621.396.41

С.К. Варлатая, Ю.С. Москаленко, С.В. Ширяев

Структурирование агентного множества оценки информационной безопасности корпоративных систем

Рассмотрены проблемы организации мультиагентной среды, предназначенной для оценки информационной безопасности системы. Предлагаются принципы формирования признакового пространства агентов и поиска их однородных функционально-ролевых групп.
Ключевые слова: агентное множество, агентный подход, мультиагентная система, типология агентов, архитектура агентов, кластерный анализ, оценка информационной безопасности.

Постановка задачи. Эффективность оценки информационной безопасности систем во многом зависит от степени автоматизации мероприятий по выработке политики безопасности и внедрению современных средств интеллектуальных информационных технологий.

Одно из перспективных направлений автоматизации оценки безопасности информационных систем связано с применением и внутренним развитием мультиагентных технологий [1]. При этом предполагается, что отдельный агент имеет лишь частичное представление об общей задаче оценки и способен решать некоторые её подзадачи в соответствии с делегированными ему функциями или ролью [2]. В рамках этой парадигмы эффективность мультиагентного подхода во многом предопределяется эффективностью взаимодействия агентов, которая неотделима от её организационной структуры. В развитие агентного подхода [3] в настоящей работе рассматриваются вопросы структурирования агентного сообщества на основе косвенной идентификации агентов и процедур кластеризации, инвариантных к топологическим особенностям агентных групп.

Предлагаемые решения. Необходимая и достаточная мощность агентного множества A определяется нормой подмножеств подзадач $|S|$, делегируемых агентам для оценки безопасности системы. Структурирование агентного сообщества осуществляется различными способами, но предпочтение всегда следует отдавать процедурам, не связанным, по крайней мере явно, с введением жестких классификационных критериев. Рассмотрим один из возможных вариантов такого принципа.

Пусть $a_j = (x_1, x_2, ..., x_n)$ – описание агента $a_j \in A$ в признаковом пространстве X. В качестве признаков будем использовать свойства агентов, измеренные в номинальной шкале. Напомним, что признак является номинальным, если множество его допустимых преобразований состоит только из взаимно однозначных преобразований. Хотя формирование признакового описания чаще всего происходит на интуитивном уровне, косвенная идентификация агентов представляется безальтернативной.

Рассматриваемое множество X предлагается определять по крайней мере четырьмя группами признаков: X_1, X_2, X_3 и X_4. Первая группа характеризует тип решаемых подзадач оценки безопасности и идентифицирует сервисы, предназначенные для их решения. При ориентации на CommonCriteria общей методологии оценки ОМО [3] эта группа должна включать в себя функциональную подгруппу (наличие аудита безопасности, наличие идентификации и аутентификации, использование ресурсов), подгруппу производных параметров (связи, приватности, защиты пользовательских данных и защиты функций безопасности объекта) и, наконец, подгруппу инфраструктурных атрибутов (криптографической поддержки, управления безопасностью, доступа к объекту, доверенного маршрута).

Вторая группа признаков X_2 отображает типы сред функционирования агентов, включая замкнутые и открытые, трансформируемые и нетрансформируемые, детерминированные, вероятностные, стационарные и нестационарные среды [4].

Третья группа X_3 характеризует типологию агентов. Обязательным является включение в эту группу следующих свойств агентов:

– поддержка автономности;

– поддержка социального поведения;

– поддержка активности;

– использование базовых знаний;

– использование убеждений;

– использование намерений, обязательств и желаний.

Четвертая группа признаков X_4 предназначена для идентификации типа архитектуры агентов: продукционной, Холланда, с трехуровневой базой знаний, BDI, коннекционистской, гибридной [4].

В общем случае глоссарий множества признаков X может быть иным.

Структурирование агентного множества A, представленного совокупностью описаний $\{a_j\}^k$, будем рассматривать как процедуру кластеризации – разбиения множества A на известное или не известное заранее число групп, с некоторыми неформальными требованиями:

– внутри групп описания агентов должны быть сильно связанными;

– между группами описания агентов должны быть слабо связными.

Под связностью понимается некоторая мера близости или расстояния. Эти требования отображают стандартную гипотезу компактности или «развала на кучи».

Нацеленность методов кластерного анализа на определенную структуру группировок агентов в пространстве признаков X может приводить к неоптимальным или даже неадекватным результатам, если гипотеза о типе группировок не верна. Традиционно в качестве критериев кластеризации используют два различных вида показателей [4]: оценочные индексы Мезиха (внешний критерий значимости, кофенетический коэффициент Сокала–Рольфа, меру воспроизводимости) и структурные характеристики кластеров (степень близости элементов внутри класса, среднюю длину ребер графа *i*-го кластера и т.п.). Это приводит, во-первых, к тому, что имеющейся совокупности данных фактов «навязывают» не присущую им структуру и тем самым искажают реальную интерпретацию группировки. Во-вторых, такой подход приводит к известным проблемам неоднозначности результатов (например к локальностям) при многопараметрической оптимизации.

Альтернативой описанной оценки решений может служить процедура, основная идея которой сводится к следующему. Пусть задано множество $A=(a_1,a_2,...,a_n)$, состоящее из *n* агентов. Система $R=(R_1,R_2,...,R_m)$ непустых множеств $R_i \in A$ называется разбиением множества A, если всякий элемент a_k содержится в одном и том же множестве $R_i\left(i=\overline{i,m}\right)$, т.е.

$$U_{i=1}^{m} R_i = A \text{ и } R_i \cap R_j = \otimes, i \neq j .$$

Множества $R_1,...,R_m$ являются классами разбиения R.

Во множестве всех разбиений на A можно определить разбиения, лежащие «между» другими. Например, если разбиение S получается из разбиения R объединением некоторых его классов, а разбиение T – аналогичным образом из S, то разбиение S лежит между R и T: [R, S, T].

С другой стороны, разбиениям R, S, T соответствуют отношения эквивалентности ρ,σ,τ. Исходя из этого, разбиение S лежит между разбиением R и T тогда и только тогда, когда

$$\rho \cap \tau \subset \sigma \subset \rho \cup \tau .$$

В терминах «между» крайними разбиениями будут: тривиальное, состоящее из одного агента, и универсальное, состоящее из всех агентов множества A. Идентификаторами отношений эквивалентности являются соответствующие им матрицы смежности [4]. Поэтому для оценки «похожести» разбиений естественно ввести расстояние между ними как некоторую индикаторную функцию, определяемую по величине разности сравниваемых матриц смежности. В этом случае вычислительная проблема упрощается вплоть до тривиальной и задача состоит в том, чтобы на множестве получаемых разбиений организовать процедуру последовательной оценки следующего разбиения по отношению к предыдущему с помощью найденного между ними расстояния. Если это расстояние ϑ сохраняет свое минимальное значение ε и

$$\vartheta = \varepsilon + \Delta ,$$

где Δ – константа, характеризующая устойчивость группировки на некотором наперед заданном интервале, то разбиения, попавшие в этот интервал, и есть исконные.

Нетрудно заметить, что предлагаемый подход инвариантен к характеру распределения агентов на множестве A и не опирается на какие-либо навязываемые извне топологические ограничения на группы агентов.

Заключение. Таким образом, в данной работе на основе современной технологии интеллектуальных агентов сформулированы и предложены решения, связанные с формированием признакового описания агентного сообщества оценки безопасности информационных систем и с явным определением его организационной структуры в теоретико-множественных терминах согласования разбиений.

Литература

1. Люгер Дж.Ф. Искусственный интеллект: стратегии и методы решения сложных проблем. – М.: Вильямс, 2005. – 864 с.

2. Рассел С. Искусственный интеллект. Современный подход / С. Рассел, П. Норвиг. – М.: Вильямс, 2005. – 1408 с.

3. Москаленко Ю.С. Агентный подход к оценке информационной безопасности корпоративных систем / Ю.С. Москаленко, С.К. Варлатая, С.В. Ширяев // Научный вестник НГТУ. – 2014. – № 1 (54). – С. 66–71.

4. Москаленко Ю.С. Организация систем, основанных на знаниях. – Владивосток: Изд. дом «Дальневосточный федеральный университет», 2013. – 242 с.

Варлатая Светлана Климентьевна
Канд. техн. наук, профессор каф. информационной безопасности школы естественных наук Дальневосточного федерального университета (ДВФУ ШЕН)
Тел.: 8-924-734-92-05
Эл. почта: sk-varl@yandex.ru

Москаленко Юрий Сергеевич
Канд. техн. наук, профессор каф. информационной безопасности ДВФУ ШЕН
Тел.: 8 (423) 224-20-74
Эл. почта: moskalenko.ys@dvfu.ru

Ширяев Сергей Вячеславович
Аспирант каф. проектирования безопасности компьютерных систем Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики
Тел.: 8-921-447-71-08
Эл. почта: ssv.88@inbox.ru

Varlataya S.K., Moskalenko Y.S., Shiryaev S.V.
Structuring agent-based set of corporate information security assessment systems.

The paper discusses the problems of the organization of multi-agent environment, designed to assess information security system. Offered principles of feature space agents and search their functional role of homogeneous groups.
Keywords: agent-based set, agent-based approach, multi-agent system, the typology of agents, agents architecture, cluster analysis, evaluation of information security.

УДК 004.056

Т.Т. Газизов, А.А. Мытник, А.Н. Бутаков

Типовая модель угроз безопасности персональных данных для информационных систем автоматизации учебного процесса

Рассмотрены информационные системы автоматизации учебного процесса ТГПУ: ИС E-Decanat и ИС Абитуриент. Выявлены типовые уязвимости и угрозы, сопряженные с обработкой персональных данных. Предложены анализ выявления угроз и методы решения по обеспечению безопасности персональных данных для каждой из рассмотренных систем.
Ключевые слова: информационная безопасность, уязвимость информационных систем, защита данных.

Сегодня обработка персональных данных является повседневной задачей, с которой сталкивается большинство работников всех сфер науки и образования [1, 2]. Работа приемной комиссии, кафедр, деканатов любого вуза всегда связана с обработкой и хранением персональных данных студентов. Как правило, для автоматизации действий обработки данных создаются информационные системы. Опыт внедрения и эксплуатации информационных систем показывает, что успешное использование программы для управления учебным процессом позволяет увеличить скорость принятия управленческих решений для большинства задач подразделения [3]. При этом одной из наиболее актуальных задач при проектировании автоматизированных информационных систем является обеспечение безопасности персональных данных при их обработке и защита от несанкционированного вмешательства. Цель данной работы – рассмотреть типовую модель угроз безопасности персональных данных для двух информационных систем автоматизации учебного процесса на примере Томского государственного педагогического университета (ТГПУ). Для описания типовой модели угроз рассмотрим описание и схему работы информационных систем автоматизации учебного процесса ТГПУ: ИС E-Decanat и ИС Абитуриент.

Информационная система E-DECANAT 2.0 предназначена для автоматизации управления учебным процессом ТГПУ. Целью разработки информационной системы E-Decanat является совершенствование деятельности учебных подразделений вуза – деканатов по учету и анализу движения контингента студентов для обеспечения эффективности управленческих решений. ИС E-Decanat 2.0 разработана в соответствие с построенной информационной моделью деканата и реализована с использованием технологии Java на основе клиент-серверной архитектуры. При разработке были использованы: IDE NetBeans, MS SQL Express Edition, СУБД MySQL. Предложенное решение является кроссплатформенным и опирается на открытые стандарты свободного программного обеспечения, что заметно расширяет сферу его применения для нужд высшего профессионального образования.

Совокупность данных в информационной системе подразделена на общие данные, т.е. те, которые обрабатывают различные подразделения вуза, и локальные, которые необходимы только для отдельного деканата с целью достижения баланса нагрузки при обработке и передаче данных. При решении этих задач используются две базы данных, одна из которых размещена в деканате, а другая – на одном из центральных серверов вуза. В центральной базе данных хранится общая информация, необходимая для работы всех факультетов вуза. В локальной базе данных хранится информация, необходимая для работы самого деканата: академические ведомости, учебные планы и другая сопутствующая информация. В роли СУБД используются два решения: MS SQL Server для общей БД и MySQL для локальной БД. Для обработки документов реализована интеграция с офисным пакетом OpenOffice.org с использованием экспорта данных в шаблоны.

Информационная система E-Decanat предназначена для автоматизации учебного процесса и не затрагивает экономическую и хозяйственную деятельность вуза. Информационная система не является изолированной от внешних систем и интегрирована в общую информационную инфраструктуру вуза (рис. 1), где взаимодействует с такими информационными системами, как «Электронная ка-

федра», «Абитуриент», информационная система учета студенческих кадров «A-Cadry», система автоматизации документооборота «A-Delo» [4].

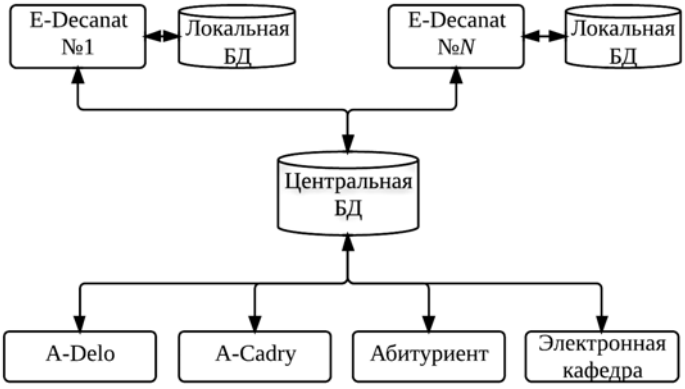


Рис. 1. Функциональная схема «E-Decanat» и «Абитуриент»

Информационная система «Абитуриент» предназначена для контроля знаний студентов ТГПУ. Целью создания информационной системы «Абитуриент» является автоматизация деятельности приемной комиссии ТГПУ [5]. Система располагает возможностями учета личных данных абитуриента и результатов вступительных испытаний, обеспечивает возможность выборки данных с использованием типовых запросов, генерацию отчетов в формате офисных приложений (например, таких, как OpenOffice.Org) [6], автоматическое зачисление и т.д. При разработке системы использовалось следующее программное обеспечение: MS Visual Studio 2008, СУБД MS SQL 2005. Информационная система обеспечивает гибкую настройку профилей и направлений подготовки на факультетах ТГПУ, различные формы конкурсных испытаний без внесения изменения в исходные модули системы. Обеспечивает механизм многопользовательского доступа к данным в соответствии с предопределенными привилегиями. База данных этой системы разделена на две части: информационную и наполняемую. Информационная часть используется для хранения наименований направлений и профилей, количества выделенных бюджетных и целевых мест, конкурсных предметов для каждого профиля. Наполняемая часть состоит из личных данных абитуриента и его конкурсной информации. Система «Абитуриент» интегрирована в общую информационную систему вуза, а также имеет связь с внешней информационной системой «ФИС ЕГЭ» (предназначенной для регистрации пользователей в информационных системах Федеральной службы по надзору в сфере образования и науки).

Рассмотренные информационные системы работают с персональными данными студентов. При обработке ПДн на автоматизированном рабочем месте, имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена, в соответствии с положением ФСТЭК России от 15 февраля 2008 г., возможна реализация следующих угроз безопасности ПД (УБПДн) [7–9]: угрозы утечки информации по техническим каналам; угрозы несанкционированного доступа (НСД) к ПДн, обрабатываемым на автоматизированном рабочем месте. Угрозы утечки информации по техническим каналам включают в себя: угрозы утечки акустической (речевой) информации; угрозы утечки видовой информации; угрозы утечки информации по каналу ПЭМИН. Угрозы НСД в ИСПДн связаны с действиями нарушителей, имеющих доступ к ИСПДн, включая пользователей ИСПДн, реализующих угрозы непосредственно в ИСПДн, а также нарушителей, не имеющих доступа к ИСПДн, реализующих угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена. Угрозы из внешних сетей включают в себя: угрозы «Анализа сетевого трафика» с перехватом передаваемой во внешние сети и принимаемой из внешних сетей информации; угрозы сканирования, направленные на выявление типа операционной системы АРМ, открытых портов и служб, открытых соединений и др.; угрозы выявления паролей; угрозы получения НСД путем подмены доверенного объекта; угрозы типа «Отказ в обслуживании»; угрозы удаленного запуска приложений; угрозы внедрения по сети вредоносных программ.

Функционирование рассмотренных выше информационных систем связано с обработкой персональных данных, отсюда возникает необходимость обеспечения безопасности информации о пер-

сональных данных. При этом, анализируя функциональные схемы представленных ИС, можем выделить наиболее типичные угрозы из типовой модели угроз: sql injection, разглашение служебной информации пользователями; получение удаленного доступа к СУБД; получение физического доступа к серверу СУБД; несанкционированный доступ к данным при передаче по сети. Проведя анализ построения и эксплуатации представленных ИС, а также исследуя особенности их использования в вузе, составим сводную таблицу возможных угроз, методов борьбы с ними а также зонами ответственности (таблица).

Возможные угрозы и методы борьбы с ними

Угроза	Меры предотвращения	Зона ответственности
SQL injection	Использование безопасных запросов, использование хранимых процедур	Разработчик
Разглашение служебной информации пользователями	Профилактическая беседа	Пользователь
Получение удаленного доступа к СУБД	Настройка сервера, ограничение сетевых подключений	Администратор БД, администратор сети
Получение физического доступа к серверу СУБД	Защита от несанкционированного доступа к оборудованию	Служба безопасности
Несанкционированный доступ к данным при передаче по сети	Защищенное соединение между клиентом и СУБД	Разработчик, поставщик СУБД, доверенный центр сертификации

В данной работе была рассмотрена типовая модель угроз безопасности персональных данных применительно к информационным системам автоматизации учебного процесса подразделений вуза, применяемых в автоматизации бизнес-процессов Томского государственного педагогического университета. Были выявлены типовые уязвимости и угрозы, сопряженные с обработкой персональных данных в рассмотренных информационных системах, выбраны методы борьбы с ними, указаны зоны ответственности. Результаты анализа представлены в виде таблицы. В этой связи цель данной работы была достигнута и применены соответствующие решения по обеспечению безопасности персональных данных для каждой из рассмотренных систем.

Литература

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_149747/, свободный (дата обращения: 24.04.2014).

2. Давыдова Е.М. Модель образовательного процесса с учетом требований работодателя // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2013. – № 4 (30). – С. 177–181.

3. Mytnik A.A. Business process automation in university using E-Decanat 2.0 software / A.A. Mytnik, A.P Klishin // The 1th International Global Virtual Conference–Workshop, April 2013. – Zilina: EDIS, 2013. – P. 308–310.

4. Мытник А.А. Опыт внедрения информационной системы E-Decanat для автоматизации управления учебным процессом в ТГПУ / А.А. Мытник, А.П. Клишин // Вестник ТГПУ. – 2013. – Вып. 1 (129). – С. 184–187.

5. Стась А.Н. Информационные системы. – Томск: Изд-во ТГПУ, 2010. – 186 с.

6. Пьяных Е.Г. Проектирование баз данных в среде OpenOffice.org (ПО для управления базами данных): учеб. пособие. – М., 2008. – 62 с.

7. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1. – С. 28–35.

8. Шелупанов А.А., Миронова В.Г., Ерохин С.С., Мицель А.А. Автоматизированная система предпроектного обследования информационной системы персональных данных АИСТ-П // Доклады ТУСУРа. – 2010. –№ 1. – С. 14–22.

9. Авсентьев О.С. Принципы моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности / О.С. Авсентьев, В.В. Александров, Г.И. Рябинин, С.В. Скрыль, Р.В. Мещеряков // Доклады ТУСУРа. – 2008. – Т. 2. – № 1. – С. 135–136.

Газизов Тимур Тальгатович
Доцент каф. информатики Томского государственного педагогического университета (ТГПУ)
Тел.: 8 (382-2) 52-11-26
Эл. почта: gtt@tspu.edu.ru

Мытник Антон Александрович
Магистрант каф. информатики ТГПУ
Тел.: 8 (382-2) 52-11-26
Эл. почта: mytnikAA@gmail.com

Бутаков Алексей Николаевич
Аспирант каф. информатики ТГПУ
Тел.: 8 (382-2) 52-11-26
Эл. почта: butakovan@tspu.edu.ru

Gazizov T.T. , Mytnik A.A., Butakov A.N.
Generic Model of Security Threats for Personal Data in regard of Information Systems Dedicated to Academic Planning

Information systems dedicated to automation of academic planning in TSPU called E-Decanat and IS Abiturient are reviewed in the article. Generic vulnerabilities and threats related to processing of personal data are revealed. Ways of analysis related to identifying threats and solutions related to security of personal data for each examined system suggested.
Keywords: Information security, vulnerability of information systems, protection of data.

УДК 681.322.067

С.М. Гончаров, А.Е. Боршевников

Построение нейросетевого преобразователя «Биометрия – код доступа» на основе параметров визуального вызванного потенциала электроэнцефалограммы

Рассматривается возможность построения нейросетевого преобразователя «Биометрия – код доступа» на основе ЭЭГ. Описывается структура нейросетевого преобразователя «Биометрия – код доступа». Предлагаются направления дальнейших исследований по разработке преобразователя «Биометрия – код доступа» на основе электроэнцефалограммы.

Ключевые слова: нейросетевой преобразователь «Биометрия – код доступа», секретный криптографический ключ, восстановление ключа, электроэнцефалограмма, визуальные вызванные потенциалы, биометрическая аутентификация.

В настоящее время идет активное развитие биометрических технологий. Одним из направлений развития данных технологий является биометрическая криптография. Основной задачей биометрической криптографии является привязка некоторой секретной информации (пароля или ключа) к определенной биометрической характеристике. Особенный интерес для использования в критических системах или приложениях, в которых используются элементы аутентификации или криптографической защиты информации, представляют характеристики деятельности мозга. Распространенной биометрией, характеризующей деятельность мозга, является электроэнцефалограмма, или ЭЭГ. Использование ЭЭГ в качестве биометрической характеристики дает несколько преимуществ. Данные электроэнцефалограммы конфиденциальны, их сложно подделать, а также они обеспечивают дополнительную меру защищенности от перехвата злоумышленником, заключающуюся в том, что снятие электроэнцефалограммы возможно на расстоянии не более 0,001 м от головы, что означает невозможность незаметного для пользователя съема данных. Помимо указанных преимуществ, внедрение технологии восстановления ключа из нечетких данных может обеспечить легкую смену «мысленного пароля» [1].

Один из эффективных подходов надежного хранения и восстановления секретного ключа был предложен в России. Для хранения секретных ключей (паролей) используются нейросетевые преобразователи «Биометрия – код доступа». Описанию данных преобразователей посвящена линейка стандартов ГОСТ Р 52633. Использование подобных преобразователей показывает хорошие результаты в вероятностях ошибок первого и второго рода [2].

В данной статье рассматривается нейросетевой преобразователь «Биометрия – код доступа» на основе электроэнцефалограммы с использованием бегущих цифр на экране, процедура восстановления ключа с помощью данного преобразователя, рассчитываются вероятности ошибок первого и второго рода.

Стимуляция на основе визуальных вызванных потенциалов. Опишем процедуру стимуляции деятельности мозга, при которой снимается электроэнцефалограмма для восстановления секретного ключа.

Используемая стимуляция для создания выглядит, как поочередно меняющиеся цифры от «0» до «9». Стимуляция для эксперимента вызывает визуальный вызванный потенциал [3]. Фрагмент стимуляции изображен на рис. 1.

Пользователи выбирают 1 или 2 символа и при их появлении на экране концентрируются на них. Данные символы являются «мысленным паролем».

Рис. 1. Фрагмент визуальной стимуляции

Съем ЭЭГ производился в течение 10 с. Для каждой секунды было использовано разбиение данной секунды на 128 частей, что соответствует синхронизации с нейрогарнитурой, используемой для съема ЭЭГ, и обеспечивает съем в реальном времени. Для случая когда пользователь запоминает 2 символа, съем ЭЭГ разбивается на два этапа по 5 с. В течение первого этапа пользователь концентрируется на одном символе, а в течение второго – на втором символе.

Биометрические характеристики визуального вызванного потенциала. В качестве биометрической характеристики a используется разница между уровнем ЭЭГ при стимуляции и усредненным значенем ЭЭГ в состоянии покоя. Обозначим уровень электроэнцефалограммы при стимуляции через $a_{\text{стим}}$, а усредненный уровень электроэнцефалограммы в состоянии покоя через $\overline{a}_{\text{покой}}$. Тогда

$$a = a_{\text{стим}} - \overline{a}_{\text{покой}}. \quad (1)$$

Однако в силу высокой сложности математического описания формы сигнала ЭЭГ [4] было принято решение производить выборку пятнадцати максимальных значений, вычисляемых по формуле (1). Целесообразно говорить об использовании характеристики a в векторном виде:

$$\overline{\mathbf{a}}_i = \{a_{ij}\}, \quad i = 1,...,14, \quad j = 1,...,15, \quad (2)$$

где $\overline{\mathbf{a}}_i$ – вектор биометрических данных, используемый в нейросетевом преобразователе; i – номер электрода, с которого снята электроэнцефалограмма; j – номер максимального значения a с канала i.

Построение и обучение нейросетевого преобразователя «Биометрия – код доступа» на основе ЭЭГ. В качестве структуры данного преобразователя выбрана двухслойная нейронная сеть сигмоидального типа.

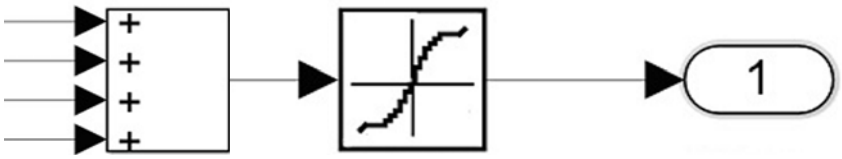
Для обучения выбрана стандартная процедура обучения нейросетевых преобразователей «Биометрия – код доступа», описанная в стандарте ГОСТ Р 52633.5–2011 [2]. Для обучения необходимо сформировать базу электроэнцефалограмм при воздействии стимуляции образов «Чужой», т.е. образов для которых нейросетевой преобразователь будет выдавать случайный криптографический ключ. Данную базу можно использовать для последующих процессов обучения преобразователя. Также необходимо сформировать базу электроэнцефалограмм образов «Свой» при состоянии покоя и при воздействии стимуляции. Данную базу необходимо удалить сразу после обучения преобразователя, в целях предотвращения её кражи и использования для компрометации секретного ключа. Результатом выполнения данной процедуры будут являться весовые коэффициенты нейронной сети:

$$\overline{\mathbf{M}}_i = \{M_{ij}\}, \quad i = 1,...,14, \quad j = 1,...,15, \quad (3)$$

$$\overline{\mathbf{M}} = \{M_k\}, \quad k = 1,...,320, \quad (4)$$

где $\overline{\mathbf{M}}_i$ – вектор весовых коэффициентов первого слоя нейронной сети, соответствующий вектору $\overline{\mathbf{a}}_i$; j – номер соответствующего компонента вектора $\overline{\mathbf{a}}_i$; $\overline{\mathbf{M}}$ – вектор весовых коэффициентов второго слоя нейронной сети; k – номер соответствующего нейрона первого слоя.

Нейроны первого и второго слоя сходны по строению (рис. 2), однако имеют различие в обрабатываемых данных и получаемых результатах.



Сумматор Передаточная функция Результат

Рис. 2. Строение нейрона нейросетевого преобразователя

Каждый нейрон первого слоя можно описать следующим образом:

$$x_1 = \sum \Delta \cdot \overline{\mathbf{M}}_i \cdot \overline{\mathbf{a}}_i = \sum \Delta \cdot \sum_{j=1}^{15} M_{ij} \cdot a_{ij}, \quad i = 1,...,14, \quad (5)$$

$$y_1 = y_1(x_1) = \frac{2}{1+e^{x_1}} - 1, \quad (6)$$

$$f_1(y_1) = \begin{cases} 1, & y_1 \geq 0, \\ -1, & y_1 < 0, \end{cases} \quad (7)$$

где x_1 – это результат работы сумматора нейрона первого слоя; Δ – коэффициент использования вектора $\overline{\mathbf{a}}_i$ в нейроне. Если $\overline{\mathbf{a}}_i$ используется в данном нейроне, то $\Delta = 1$ и $\Delta = 0$ в противном случае;

y_1 – передаточная функция первого слоя нейронной сети; $f_1(y_1)$ – решающее правило для нейрона первого слоя.

Используемые в сумматорах нейрона векторыбиометрических данных определяются следующим образом. В любом сумматоре обязательно используется 1 из 4 векторов, соответствующих векторам данных, снятых с электродов, расположенных на затылочной области головы. Данные электроды снимают ЭЭГ с области, в которой возникает наиболее сильный визуальный вызванный потенциал [4]. Для оставшихся трех входов сумматора используются 3 из 14 неиспользованных векторов биометрических данных.

Составим результирующий вектор работы первого слоя нейронной сети $\bar{t}$:

$$\bar{\mathbf{t}} = \{t_k\},\ k = 1,..., 320\ . \tag{8}$$

Каждый нейрон второго слоя можно описать следующим образом:

$$x_2 = \sum \Delta \cdot \overline{\mathbf{M}} \cdot \bar{t} = \sum \Delta \cdot M_k \cdot t_k,\quad k = 1,...,320\ , \tag{9}$$

$$y_2 = y_2(x_2) = \frac{2}{1+e^{x_2}} - 1\ , \tag{10}$$

$$f_2(y_2) = \begin{cases} 1, & y_2 \ge 0, \\ 0, & y_2 < 0, \end{cases} \tag{11}$$

где x_2 – это результат работы сумматора нейрона второго слоя; Δ – коэффициент использования компонента t_k в нейроне. Если t_k используется в данном нейроне, то $\Delta = 1$ и $\Delta = 0$ в противном случае; y_2 – передаточная функция второго слоя нейронной сети; $f_2(y_2)$ – решающее правило для нейрона второго слоя.

Используемые в сумматорах нейрона выходы первого слоя определяются согласно процедуре, описанной в ГОСТ Р 52633.5–2011 [2].

Результат работы каждого нейрона второго слоя является битом восстанавливаемого секретного криптографического ключа.

Полученные результаты работы нейросетевого преобразователя. Для проведения исследования построенного преобразователя была создана база из 10 различных биометрических образов, для каждого из которых было снято 20 примеров ЭЭГ в состоянии покоя и 80 примеров ЭЭГ под воздействием стимуляции. Один образ был выбран в качестве образа «Свой», остальные девять сформировали базу образов «Чужой».

Был проведен опыт по возможности получения злоумышленником секретного ключа при условии знания злоумышленником весовых коэффициентов. Наиболее интересными являются следующие результаты:

1. В случае, когда злоумышленник угадывает «мысленный пароль», расстояние Хэмминга от полученного злоумышленником ключа до секретного ключа пользователя было равно 7.

2. Во всех опытах по восстановлению ключа пользователем преобразователь безошибочно восстанавливал секретный ключ.

Приведем расчет ошибок первого и второго рода на основе результатов, полученных в ходе проведения опытов.

Для случаев, когда тестирующая выборка является небольшой и ошибка первого рода не была выбрана, данную ошибку можно вычислить по следующей формуле [4]:

$$P_1 \approx \int_1^{\infty} \frac{1}{2^{\frac{\Omega}{2}} \cdot \Gamma\left(\frac{\Omega}{2}\right)} \cdot x^{\frac{\Omega}{2}-1} \cdot e^{-\frac{x^2}{2}} \cdot dx\ , \tag{12}$$

где Ω – количество степеней свободы в распределении X^2.

В случае, когда в проведенной серии испытаний по предъявлению биометрической характеристики образа «Свой», состоящей из m опытов, не обнаружен факт отказа в доступе, число степеней свободы в распределении X^2 вычисляется по формуле

$$\Omega = \frac{1}{m+1}\ . \tag{13}$$

По формуле (12) получим ошибку первого рода: $P_1 = 6 \cdot 10^{-4}$.

Прогноз вероятности ошибок второго рода P_2 вычисляют приближенно, исходя из гипотезы нормального закона распределения значений вероятности ошибок по формуле [2]:

$$P_2 \approx \frac{1}{\sqrt{2\pi}} \int_{\sqrt{n}E(q(v))}^{\infty} e^{-\frac{x^2}{2}} dx, \qquad (14)$$

где n – число учитываемых преобразователем биометрических параметров; $E(q(v))$ – среднее качество всех учитываемых преобразователем биометрических параметров.

В построенном преобразователе использовалось 210 параметров, а среднее качество было получено равным 2,3. Тогда по формуле (14) получим ошибку второго рода: $P_2 \le 10^{-50}$.

Кроме описанных опытов, был проведен опыт по использованию в качестве «мысленного пароля» PIN-кода, состоящего из четырех символов. В ходе опыта было получено, что ошибка первого рода осталась на прежнем уровне, но среднее качество всех учитываемых параметров увеличилось до 3,6, и по формуле (14) было получено, что ошибка второго рода $P_2 \le 10^{-50}$. Полученный результат на порядки отличается от существующих средств биометрической аутентификации [5, 6].

Заключение. В данной работе описано построение нейросетевого преобразователя «Биометрия – код доступа» на основе данных электроэнцефалограммы и получены ошибки первого и второго рода для него.

Полученные результаты показывают, что необходимо дальнейшее исследование работы данного нейросетевого преобразователя. Необходимо:

1) увеличить размер базы электроэнцефалограмм не только по количеству биометрических образов в ней, но и по количеству биометрических образцов для каждого образа;

2) исследовать возможность увеличения расстояния Хэмминга от секретного ключа, получаемого злоумышленником, до ключа пользователя без утраты восстановительной способности преобразователя для пользователей;

3) оптимально подобрать коэффициенты обучения нейронной сети для преобразователя.

Однако уже сейчас полученные результаты показывают большие перспективы развития данной технологии.

Литература

1. Гончаров С.М. Идентификация пользователей на основе электроэнцефалографии с использованием технологий «Интерфейс мозг – компьютер» / С.М. Гончаров, М.С. Вишняков // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1 (25), ч. 2. – С. 166–170.

2. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрии. – М.: Стандартинформ, 2012. – 20 с.

3. Гнездицкий В.В. Обратная задача ЭЭГ и клиническая электроэнцефалография (картирование и локализация источников электрической активности мозга). – М.: МЕДпрессинформ, 2004. – 624 с.

4. Оценка вероятностей появления ошибок нейросетевых преобразователей биометрия-код на основе малых выборок / Б.С. Ахметов, А.И. Иванов, А.Ю. Малыгин, Т.С. Картбаев // Труды II Международной научной конференции «Высокие технологии – залог устойчивого развития». – Алматы, Казахстан. – 2013. – Т. 1. – С. 234–237.

5. Мещеряков Р.В. Биометрические методы идентификации / Р.В. Мещеряков, А.А. Шелупанов, В.П. Бондаренко // Известия Южного федерального университета. Технические науки. – 2003. – Т. 33, № 4. – С. 176–177.

6. Костюченко Е.Ю. Распознавание пользователя по клавиатурному почерку на фиксированной парольной фразе в компьютерных системах / Е.Ю. Костюченко, Р.В. Мещеряков // Известия Южного федерального университета. Технические науки. – 2003. – Т. 33, № 4. – С. 177–178.

Гончаров Сергей Михайлович
Канд. физ.-мат. наук, доцент, зав. каф. «Безопасность информации и телекоммуникационных систем» Морского государственного университета им. адм. Г.И. Невельского, Владивосток
Эл. почта: sgprim@smtp.ru, goncharov@msun.ru

Боршевников Алексей Евгеньевич
Инженер-программист Дальневосточного регионального учебно-научного центра по проблемам информационной безопасности, Владивосток
Тел.: 8 (924-1) 31-67-97
Эл. почта: LAdG91@mail.ru

Goncharov S.M., Borshevnikov A.E.
Construction of neural network transformer «Biometrics – access code» based on the parameters of the visual evoked potential electroencephalogram

The construction of neural network transformer «Biometrics – access code» based on EEG is researched. The structure of neural network transformer «Biometrics – access code» is described. The directions for further research of transformer «Biometrics – access code» based on electroencephalogram is offered.
Keywords: neural network transformer «Biometrics – access code», secret cryptographic key, key recovery, electroencephalogram, visual evoked potentials, biometric authentication.

УДК 004.056

О.Т. Данилова, Е.В. Широков

Анализ результатов аудита системы защиты информации с применением комплексной сравнительной оценки

Предлагается способ анализа результатов системы защиты информации (СЗИ) на базе метода комплексной сравнительной оценки. Преимущества рассматриваемого способа состоят в том, что, во-первых, анализ базируется на комплексном многомерном подходе в оценке такого сложного явления, как структурные изменения, происходящие в системе защиты; во-вторых, логика способа позволяет избежать субъективизма отдельных показателей; в-третьих, метод отличается простотой и универсальностью.

Ключевые слова: информационная безопасность, комплексная оценка, методика оценки.

Анализ системы информационной безопасности (СЗИ) ключевых систем информационной инфраструктуры должен позволить получить полную и объективную оценку защищенности информационных процессов, локализовать имеющиеся проблемы и разработать эффективную программу построения системы обеспечения информационной безопасности организации. К сожалению, существуют препятствия как методологического, так и организационного характера тому, чтобы комплексная оценка удовлетворяла этим требованиям. Поэтому нередко возникают ситуации, когда полученные тем или иным способом обобщающие оценки СЗИ ключевых систем не соответствуют действительности или на практике не оправдывают усилий, затраченных на сбор и обработку данных [1].

Для получения адекватного анализа комплекса применяемых мер защиты на объекте без привлечения сторонних экспертов и значительных финансовых затрат в данной работе представляется методика комплексной оценки результатов анализа защищенности, основанная на применении общеизвестных подходов оценивания рисков и методов, являющихся основой для расчета различных рейтингов [2]. К методам многомерного анализа (комплексной сравнительной оценки) относятся следующие:

1. Метод суммирования показателей – используют в случае одинаковой направленности исходных показателей и их общей сопоставимости. Наилучшим результатом по данному методу считается тот, который представляет собой максимальную сумму показателей-стимуляторов или минимальную сумму показателей-дестимуляторов.

2. Метод суммы мест – здесь анализируемые объекты ранжируются по показателям-стимуляторам в порядке возрастания и по показателям-дестимуляторам в порядке убывания. Наилучшим результатам соответствуют значения минимальной суммы мест. Метод прост и позволяет быстро получить необходимую оценку, но при этом является грубым и приблизительным, не учитывает значимость различных показателей.

3. Метод расстояний – преимущество метода расстояний перед другими методами обусловлено использованием приема нормирования, когда значения показателя всех сравниваемых объектов делятся на так называемое эталонное (другими словами, оптимальное) значение показателя.

4. Таксонометрический метод – не только учитывает абсолютные значения показателей, но и позволяет элиминировать их различную вариацию и является обобщением метода расстояний.

5. Метод суммы баллов с заданной непрерывной шкалой на выбранном отрезке – при оценке всех показателей по одинаковой шкале не учитываются их коэффициенты значимости, поэтому необходимо строить для каждого показателя свою шкалу с учетом его значимости**.**

Кроме исходных данных о значениях показателей, задаются шкалы для оценки каждого показателя. Этот метод требует разработки большого числа шкальных оценок, которые необходимо согласовывать между собой. Наиболее распространенными являются непрерывные шкалы и дискретные шкалы [3, 4].

Дискретная шкала задает определенное число уровней оценок (баллов), с помощью которых оценивается показатель. Как правило, в этом случае выбирают целочисленные балльные оценки: 0,

1, 2, 3 и т.д. или 0, 5, 10 и т.д. Обычно балльная оценка в этом случае исчисляется путем задания интервалов изменения показателя и соответствующих балльных оценок.

При применении непрерывной шкалы оценки могут принадлежать любой точке отрезка, который определяет шкалу данного показателя. Как правило, способ исчисления балльной оценки для непрерывной шкалы – непрерывное отображение отрезка, в пределах которого изменяется данный показатель, на заданную шкалу.

Ядро методики представляет собой классический подход к формированию режима безопасности и проектированию системы защиты объекта информатизации, включающий в себя три основных ключевых этапа:

1) идентификация, анализ и оценка рисков, охватывающих все активы организации;

2) оценка возможности уменьшения рисков;

3) оценка остаточных рисков и проведение комплексной оценки с выдачей заключения о достаточности принятых мер по защите.

Анализ качества оценки объектов СЗИ состоит из следующих этапов:

Этап 1. Определяются цели и условия функционирования организации – владельца информационных ресурсов, поскольку уровень информационной безопасности организации является одной из характеристик его жизнеспособности. При анализе СЗИ организации некоторые положения комплексной оценки соответственно будут пересекаться с определенными видами деятельности организации. В основном это затрагивает формирование стратегических интересов организации и соответственно их количественного толкования.

Этап 2. Здесь формируются данные об информационной системе организации, необходимая база системного анализа и выбирается исходная система показателей.

Этап 3. На этом этапе выбираются группы показателей или отдельного критерия, определенного как мера для сравнения количественных показателей исследуемой операции в отношении затрачиваемых усилий и получаемых результатов. Критерий должен отвечать следующим основным требованиям: иметь ясный физический смысл; быть определяющим и соответствовать основной цели функционирования системы, подсистемы или элемента; учитывать основные детерминированные и стохастические факторы, определяющие уровень безопасности системы; быть критичным к анализируемым параметрам и достаточно чувствительным к ним.

Необходимое условие: все показатели должны иметь одинаковую направленность – либо на увеличение, либо на уменьшение, т.е. увеличение любого частного показателя рассматривается как улучшение результатов деятельности и наоборот. Если имеются разнонаправленные показатели, то их приводят к одинаковой направленности путем ввода обратных чисел.

Оценка уровня защищенности определяется по каждому семейству на отрезке [0;1]. Так как все компоненты доверия, содержащиеся в конкретном семействе, имеют иерархическую последовательность, то оценка «1» выставляется, если объект соответствует максимальному компоненту доверия, а оценка «0» – если не выполняются требования самого низкого компонента. Объекты оценки соотносятся к соответствующим компонентам доверия на основе соответствующей анкеты.

Этап 4. По исходным данным строится вспомогательная матрица **P** по следующим правилам:

а) если показатель является стимулятором ($s_j = +1$), то элементы j-го столбца матрицы упорядочиваются по убыванию и элементу p_{ij} придается значение, соответствующее месту элемента x_{ij} среди упорядоченных элементов j-го столбца, элементам с одинаковыми значениями присваиваются одинаковые места;

б) если показатель является дестимулятором ($s_j = 1$), то элементы j-го столбца матрицы упорядочиваются по возрастанию и элементу p_{ij} придается значение, соответствующее месту элемента x_{ij} среди упорядоченных элементов j-го столбца.

Для расчета балльной оценки при использовании непрерывной шкалы можно задействовать следующие формулы:

– для показателей-стимуляторов: $b_{ij} = b_{\min j} + \dfrac{(b_{\max j} - b_{\min j})(x_{ij} - x_{\min j})}{(x_{\max j} - x_{\min j})}$;

– для показателей-дестимуляторов: $b_{ij} = b_{\max j} + \dfrac{(b_{\max j} - b_{\min j})(x_{ij} - x_{\min j})}{(x_{\max j} - x_{\min j})}$.

Здесь $b_{\max j}$ и $b_{\min j}$ – максимально и минимально возможные балльные оценки для j-го показателя по принятой для него шкале; $x_{\max j}$ и $x_{\min j}$ – соответственно максимальное и минимальное значения j-го показателя.

Этап 5. На этом этапе проводится операция стандартизации признаков (показателей), поскольку разные признаки могут иметь различную размерность.

Этап 6. Производится расчет точки-эталона P_0, обусловленный тем, что в одномерном пространстве происходит попарное сравнение показателей. Эталоном будет точка (вектор), образованная по правилу: среди признаков-стимуляторов отбираются признаки с максимальными значениями, а среди признаков-дестимуляторов – с минимальными.

Этап 7. Осуществляется ранжирование объектов по степени убывания характеристик. Этот этап занимает важное место в системе комплексного анализа в двух случаях:

1) когда требуется сопоставить состояния нескольких объектов на основе единой системы показателей;

2) когда нужно сопоставить результаты функционирования какого-либо объекта во времени.

Ранговое место служит обобщающим показателем, представляя собой «равнодействующую» всех признаков, что позволяет линейно упорядочить анализируемые объекты. Проведение оценки рангового места заключается в следующем:

– определяется расстояние C_{i0} между точками, характеризующими исследуемые объекты, и эталонной точкой P_0;

– формируется вектор значения расстояний $C = (C_{10} C_{20} ... C_{m0})$;

– определяется среднее арифметическое расстояний между i-м объектом и точкой P_0:

$$\overline{C}_0 = \frac{1}{m} \sum_{i=1}^{m} C_{i0};$$

– вычисляется среднеквадратическое отклонение σ_0 от точки P_0;

– рассчитывается показатель качества оценки i-го объекта $C_0 = \overline{C}_0 + 2\sigma_0$.

По расстоянию между i-м элементом C_{i0} и точкой P_0 можно сделать предварительные выводы о ранговом месте объекта при оценке качества системы. Чем меньше расстояние между C_{i0} и P_0, тем выше качество защиты объекта по данному признаку.

Этап 8. Расчеты уточняются через определение оценки $D = 1 - \dfrac{C_{i0}}{C_0}$, которая интерпретируется следующим образом: качество объекта тем выше, чем ближе значение показателя к единице.

Точность каждого применяемого метода в комплексе можно характеризовать соответствием средних удельных весов всех показателей в комплексной оценке (вкладов показателей в оценку) их коэффициентам значимости [5]. Количественно точность метода можно оценить как квадрат расстояния между двумя точками в n-мерном пространстве. Координаты одной точки – это значения средних удельных весов каждого показателя в комплексной оценке (w_j), координаты второй – коэффициенты значимости показателей (k_j). Отклонение, характеризующее точность применяемого метода комплексной сравнительной оценки, рассчитывается по формуле

$$O = \sum_{j=1}^{n} (k_j - w_j)^2,$$

где w_j – средний удельный вес каждого показателя.

Чем меньше значение отклонения, тем ближе значения средних удельных весов и коэффициентов значимости, тем точнее метод.

Полученные результаты позволяют сделать вывод о приемлемости использования методики комплексной сравнительной оценки для анализа результатов аудита системы обеспечения информационной безопасности организации. Однако следует учитывать, что осуществление этапов анализа связано со многими нерешенными проблемами, например при определении системы оцениваемых показателей и коэффициентов их сравнительной значимости, а также с затруднениями при разработке вычислительного алгоритма.

Литература

1. Конев А.А. Подход к описанию структуры системы защиты информации /А.А. Конев, Е.М. Давыдова // Доклады ТУСУРа. – 2013. – № 2 (28). – С.107–111.
2. Шеремет А.Д. Комплексный анализ хозяйственной деятельности. – М.: Инфра-М, 2006. – 415 с.
3. Евсютин О.О. Использование клеточных автоматов для решения задач преобразования информации / О.О. Евсютин, С.К. Росошек // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 173–174.
4. Мещеряков Р.В. Модель обработки информации в различных шкалах // Современные информационные технологии. – 2008. – № 8. – С. 101–103.
5. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с.

Данилова Ольга Тимофеевна
Канд. физ.-мат. наук, доцент каф. комплексной защиты информации
Омского государственного технического университета (ОмГТУ)
Тел.: 8 (381-2) 62-87-07
Эл. почта: olga.danlot@yandex.ru

Широков Егор Владимирович
Ст. преподаватель каф. комплексной защиты информации ОмГТУ
Эл. почта: 9785870@gmail.com

Danilova O.T., Shirokov E.V.

Analysis of results of audit of system of information security with application of a complex comparative assessment

In this article we propose a method based on a set of comparative evaluations, to analyze the data security system. The advantages of this method are as follows: firstly, It is based on an interdisciplinary approach to the assessment of such complex phenomena as the struct the system of protection, and secondly, the logic of this technique allows to overcome the shortcomings of methods for assessing structural changes and thus avoid the subjectivity of the individual indicators, and thirdly, the methods are simple and flexible.

Keywords: information security, complex assessment, methodology of evaluation.

УДК 519.713.4

О.О. Евсютин, А.А. Шелупанов

Основные подходы к использованию математического аппарата теории клеточных автоматов для решения задач кодирования информации

Рассматриваются некоторые свойства и характеристики процесса развития клеточного автомата, значимые при решении задач кодирования информации, и предлагается два подхода к решению данных задач с помощью математического аппарата теории клеточных автоматов. Вводится новое расширение классической модели клеточного автомата – клеточный автомат с кодовым множеством.

Ключевые слова: клеточный автомат, характеристики клеточного автомата, клеточный автомат с кодовым множеством, кодирование информации.

В настоящее время известны такие приложения математического аппарата теории клеточных автоматов, как симметричное шифрование [1, 2], генерация псевдослучайных последовательностей [3], хеширование [4], сжатие данных [5, 6], обработка цифровых изображений [7–10], стеганографическое кодирование [11] и некоторые другие. Необходимо отметить, что во всех перечисленных работах используются схожие подходы к решению возникающих частных задач кодирования информации с помощью клеточных автоматов. Однако общие теоретические положения, определяющие, каким образом должны использоваться клеточные автоматы для решения задач кодирования информации, на данный момент отсутствуют. Обобщение подобных подходов является целью настоящей работы.

Математическая модель клеточного автомата. Опишем математическую модель клеточного автомата как совокупность компонентов $\mathrm{CA} = \langle Z^n, \mathbf{L}, A, \mathbf{Y}, \sigma \rangle$, где Z^n – это пространство целочисленных координат клеток решетки; $\mathbf{L} = (l_1, \ldots, l_n)$, $l_i > 0$, $i = \overline{1,n}$ – вектор, задающий размеры решетки; A – алфавит внутренних состояний, определяющий конечное множество значений отдельно взятой клетки, представляющий собой отрезок ряда неотрицательных целых чисел; $\mathbf{Y}$ – окрестность клетки, в свою очередь, представляющая собой вектор относительных индексов, определяющий одинаковые для каждой клетки решетки количество и порядок расположения соседей, т.е. тех клеток, текущие значения которых повлияют на значение данной клетки в следующий момент времени; σ – локальная функция перехода, задаваемая аналитически или в виде множества параллельных подстановок, одновременное применение которой ко всем клеткам решетки определяет динамику клеточного автомата. Аргументы данной функции задаются окрестностью $\mathbf{Y}$ [12, 13].

Характеристики процесса развития клеточного автомата. Введем ряд характеристик процесса развития клеточного автомата, определяющих особенности его динамики.

Функция корреляции последовательных состояний истории развития клеточного автомата $k(c^t, c^{t-1})$, $t = 1, 2, \ldots$, для вычисления значений которой на каждом шаге развития клеточного автомата рассчитывается коэффициент корреляции между текущим и предыдущим состояниями решетки клеточного автомата, рассматриваемыми как слова в алфавите A, независимо от размерности клеточного автомата. Установлено, что с ростом t наблюдается стремление данной функции к некоторой постоянной величине, причем для нетривиальных обратимых клеточных автоматов характерно уменьшение корреляции, в то время как для необратимых клеточных автоматов в этом случае может наблюдаться значительная корреляция. Примеры рассматриваемой характеристики представлены на рис. 1.

В данном случае коэффициент корреляции состояний двумерных клеточных автоматов рассчитывался по формуле $k\left(c^t, c^{t-1}\right) = \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} c_{i,j}^t \oplus c_{i,j}^{t-1}$, где $c_{i,j}^t \in \{0,1\}$ – значение клетки решетки с координатами (i, j) в момент времени t.

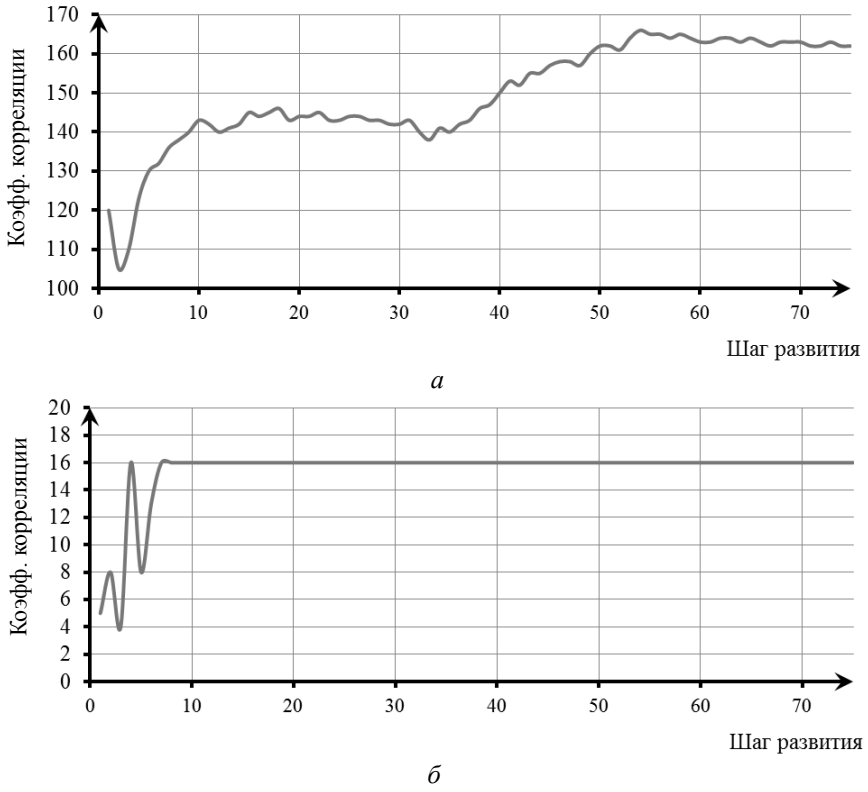


Рис. 1. Функция корреляции последовательных состояний решетки:
а – для обратимого клеточного автомата; *б* – для необратимого клеточного автомата

Функция рассеивания информации $r(t)$, определяющая максимальное расстояние, на которое распространилось влияние отдельно взятой клетки решетки в процессе развития клеточного автомата. Значения данной функции вычисляются с помощью подхода, основанного на сопоставлении двух историй развития заданного клеточного автомата, начинающихся с состояний, отличающихся значением одной клетки. Для n-мерных клеточных автоматов уместно рассматривать рассеивание информации в каждом из n возможных направлений. Пример для двумерного клеточного автомата представлен на рис. 2.

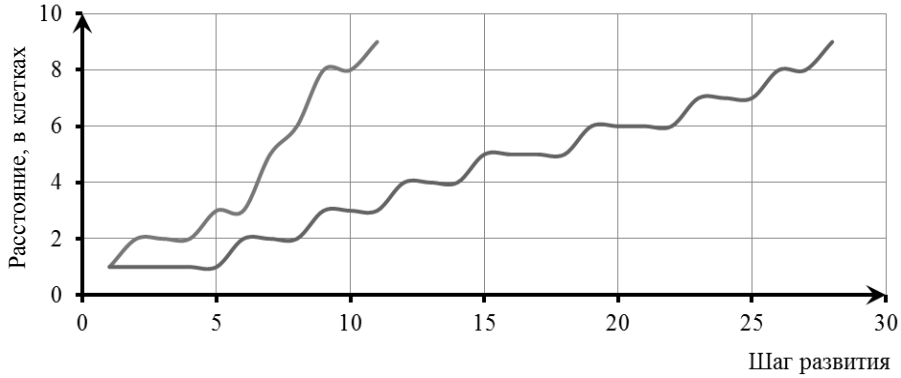


Рис. 2. Функция рассеивания информации:
в горизонтальном (больший рост) и вертикальном (меньший рост) направлении

Функция энтропии блока разбиения $h(t)$. Данная функция вводится для блочных клеточных автоматов: рассматривается множество возможных значений одного блока, на которые разбивается решетка клеточного автомата, и в каждый момент времени рассчитывается энтропия, приходящаяся на один блок разбиения для данного состояния развития клеточного автомата. Пример представлен на рис. 3. Соответствующий блочный клеточный автомат $\mathrm{CA_p} = \langle Z^n, \mathbf{L}, \mathbf{B}, A, \mathbf{P}, \psi \rangle$ [14] является дву-

мерным, $n=2$, причем алфавит внутренних состояний A выбран двоичным, вектор, задающий размеры блока разбиения, $\mathbf{B}=[2 \quad 2]$, набор схем разбиения $\mathbf{P}=[(0,0) \quad (1,1)]$ и блочная функция перехода ψ биективна. В этом случае с течением времени энтропия повышается, приближаясь к максимуму. Скорость роста энтропии зависит от вида блочной функции перехода, в частности, от числа циклов в ней.

Можно ввести обобщение данной характеристики для произвольного клеточного автомата, если по аналогии с блочным клеточным автоматом на каждом шаге развития рассматривать разбиение решетки на однородные части для вычисления локальной энтропии.

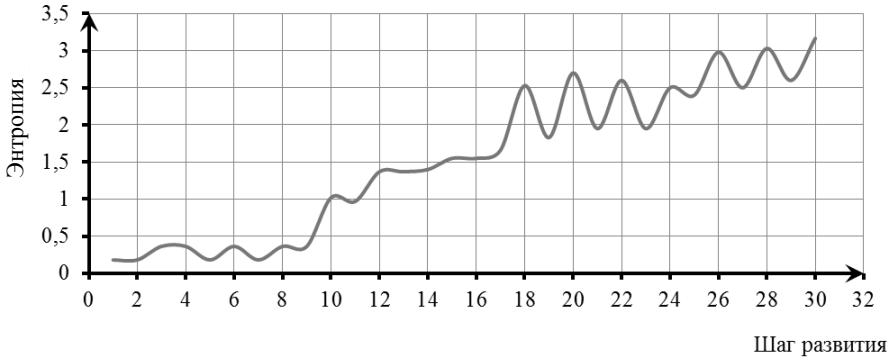


Рис. 3. Функция энтропии блока разбиения

Функция максимального количества одинаковых блоков разбиения $m(t)$, также вводящаяся для блочных клеточных автоматов и определяющая в каждый момент времени максимальное количество блоков разбиения, принимающих одинаковые значения. Пример для того же блочного клеточного автомата, что и в предыдущем случае, представлен на рис. 4. Можно увидеть, что функции $m(t)$ и $h(t)$ связаны между собой взаимообратной зависимостью: уменьшение $m(t)$ приводит к росту $h(t)$, что вполне соответствует определению энтропии.

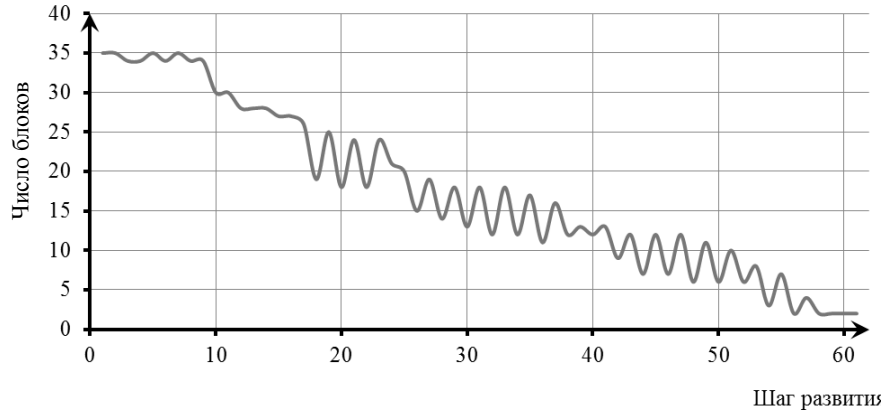


Рис. 4. Функция максимального количества одинаковых блоков разбиения

В результате исследования данных характеристик для различных клеточных автоматов сделан вывод, что наличие свойства обратимости у клеточного автомата вносит в его динамику принципиальные отличия по сравнению с необратимыми клеточными автоматами.

Кроме того, обратимые клеточные автоматы обладают следующим важным свойством, которое определяет предпочтительность их использования при решении некоторых конкретных задач (например, генерации псевдослучайных последовательностей) – их истории развития не содержат циклов неопределенной длины, когда в процессе развития клеточный автомат возвращается в одно из достигнутых им ранее состояний, не являющееся начальным. Наличие данного свойства у обратимых клеточных автоматов, в свою очередь, определяется тем, что они не обладают неконструируемыми (недостижимыми) состояниями развития.

Теорема. Множество неконструируемых состояний любого обратимого клеточного автомата является пустым.

Доказательство. Пусть задан некоторый обратимый клеточный автомат CA_1. Обозначим множество всех его состояний $\mathbf{C}(\mathrm{CA}_1)$ и выделим в данном множестве подмножество неконструируемых состояний $\tilde{\mathbf{C}}(\mathrm{CA}_1) \subset \mathbf{C}(\mathrm{CA}_1)$. Предположим, что множество $\tilde{\mathbf{C}}(\mathrm{CA}_1)$ не является пустым и содержит как минимум одно состояние c_0. Примем данное состояние в качестве начального состояния решетки клеточного автомата. Поскольку динамика обратимого клеточного автомата является детерминированной в обоих направлениях развития, существует некоторое состояние $c_0^{-1} \in \mathbf{C}(\mathrm{CA}_1)$ такое, что $c_0^{-1} = \tau' c_0$, где τ' – функция, обратная глобальной функции перехода τ клеточного автомата CA_1. Рассмотрим данный переход в обратном направлении, т.е. $c_0 = \tau c_0^{-1}$. Однако раз существует состояние, предшествующее состоянию c_0, состояние c_0 не может быть неконструируемым по определению, следовательно, $c_0 \notin \tilde{\mathbf{C}}(\mathrm{CA}_1)$. Пришли к противоречию, следовательно, множество $\tilde{\mathbf{C}}(\mathrm{CA}_1)$ является пустым.

Теорема доказана.

Клеточный автомат с кодовым множеством. Расширяя классическую модель клеточного автомата, введем понятие клеточного автомата с кодовым множеством $\mathrm{CA}_K = \langle \mathrm{CA}, K, \varphi \rangle$, где CA есть некоторый (базовый) клеточный автомат с алфавитом внутренних состояний A; K – упорядоченное множество значений, такое, что $|K| = |A|$, и отображение $\varphi: A \to K$ ставит в соответствие символам алфавита внутренних состояний A элементы кодового множества K.

Данное расширение предназначено для генерации кодовых последовательностей, записанных в алфавите K, с помощью динамики базового клеточного автомата CA. В отличие от алфавита внутренних состояний клеточного автомата A, представляющего собой некоторый отрезок ряда положительных целых чисел, на природу элементов кодового множества K таких ограничений не накладывается, и с помощью динамики заданного клеточного автомата, изменяя кодовое множество, можно генерировать кодовые последовательности различного вида, связанные различными отношениями между собой.

Общие теоретические положения по использованию клеточных автоматов для решения задач кодирования информации. Сформулируем два подхода к использованию математического аппарата теории клеточных автоматов для решения задач кодирования информации.

Первый из них служит для построения криптографических и стеганографических алгоритмов, а также для решения некоторых задач цифровой обработки изображений (например, фильтрации) и заключается в преобразовании входных данных, представляющих собой слово в алфавите A, соответствующее решетке клеточного автомата, непосредственно в процессе развития клеточного автомата, обладающего характеристиками заданного вида. Наиболее значимыми из этих характеристик будут следующие: локальное изменение энтропии в процессе развития клеточного автомата, скорость распространения информации по решетке клеточного автомата, изменение корреляции между соседними состояниями данной истории развития, а также между отдельными историями развития клеточного автомата.

Второй подход предлагает использовать динамику клеточного автомата для генерации кодовых последовательностей заданного вида, которые будут определять собственно кодирование элементов данных, для чего вводится понятие клеточного автомата с кодовым множеством.

В рамках данного подхода основными являются следующие свойства клеточного автомата: влияние начального состояния решетки с определенным образом упорядоченной структурой на историю развития клеточного автомата; способность порождать в ходе развития клеточного автомата последовательности (коды) заданного вида, цикличность истории развития клеточного автомата. Основное приложение данного подхода – это цифровая обработка сигналов, в частности изображений.

Заключение. Продолжением представленной работы будет развитие предложенных подходов к использованию математического аппарата теории клеточных автоматов для решения задач кодирования информации [15–18] и исследование введенного расширения классической модели клеточного автомата.

Работа выполнена при финансовой поддержке РФФИ (проект № 12-01-31378) и Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2014 год (проект № 1220).

Литература

1. Wuensche A. Cellular automata encryption: the reverse algorithm, Z-parameter and chain-rules // Parallel Processing Letters. – 2009. – Vol. 19, № 2. – P. 283–297.

2. Ключарёв П.Г. Блочные шифры, основанные на обобщённых клеточных автоматах / П.Г. Ключарёв // Наука и образование: электронное научно-техническое издание. – 2012. – № 12. – С. 27.

3. Сухинин Б.М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов / Б.М. Сухинин // Прикладная дискретная математика. – 2010. – № 2. – С. 34–41.

4. Mihaljevic M.J. A cellular automaton based fast one-way hash function suitable for hardware implementation / M.J. Mihaljevic, Y. Zheng, H. Imai // First International Workshop on Practice and Theory in Public Key Cryptography, PKC'98 Pacifico. – Yokohama, Japan. – 1998. – P. 217–233.

5. Lafe O. Data Compression and Encryption Using Cellular Automata Transforms / O. Lafe // Engineering Applications of Artificial Intelligence. – 1997. – Vol. 10, № 6. – P. 581–591.

6. Shaw C. Cellular automata based encoding technique for wavelet transformed data targeting still image compression / C. Shaw, S. Das, B.K. Sikdar. – 7th International Conference on Cellular Automata for Research and Industry. ACRI 2006. September 20–23. – Perpignan. France. – 2006. – P. 141–146.

7. Rosin P.L. Training cellular automata for image processing / P.L. Rosin // 14th Scandinavian Conference, SCIA 2005. – Joensuu, Finland, 2005. – P. 195–204.

8. Kauffmann C. Seeded ND medical image segmentation by cellular automaton on GPU / C. Kauffmann, N. Piché // International Journal of Computer Assisted Radiology and Surgery. – 2010. – Vol. 5, № 3. – P. 251–262.

9. Zagoris K. Scene text detection on images using cellular automata / K. Zagoris, I. Pratikakis // 10th International Conference on Cellular Automata for Research and Industry, ACRI 2012. – Santorini Island, Greece, 2012. – P. 514–523.

10. Sahoo G. Text extraction and enhancement of binary images using cellular automata / G. Sahoo, Tapas Kumar, B.L. Raina, C.M. Bhatia // International Journal of Automation and Computing. – 2009. – Vol. 6, № 3. – P. 254–260.

11. Wu H. A new JPEG image watermarking algorithm based on cellular automata / H. Wu, J. Zhou, X. Gong et al. // Journal of Information & Computational Science. – 2011. – Vol. 8, № 12. – P. 2431–2439.

12. Кудрявцев В.Б. Основы теории однородных структур / В.Б. Кудрявцев, А.С. Подколзин, А.А. Болотов. – М.: Наука, 1990. – 296 с.

13. Евсютин О.О. Разработка и тестирование вычислительного метода построения базисов декоррелирующих преобразований с использованием клеточных автоматов на разбиении / О.О. Евсютин, С.К. Росошек // Труды СПИИРАН. – 2012. – Вып. 4 (23). – С. 324–342.

14. Тоффоли Т. Машины клеточных автоматов / Т. Тоффоли, Н. Марголус. – М.: Мир, 1991. – 280 с.

15. Евсютин О.О. Приложения клеточных автоматов в области информационной безопасности и обработки данных / О.О. Евсютин, А.А. Шелупанов // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1 (25), ч. 2. – С. 119–125.

16. Исхаков С.Ю. Прогнозирование в системе мониторинга локальных сетей / С.Ю. Исхаков, А.А. Шелупанов, С.В. Тимченко // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2012. – № 1 (25), ч. 2. – С. 100–103

17. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

18. Кускова А.А. Оценка рисков информационной безопасности телекоммуникационной системы / А.А. Кускова, А.А. Шелупанов, Р.В. Мещеряков, С.С. Ерохин // Информационное противодействие угрозам терроризма. – 2009. – № 13. – С. 90–92.

Евсютин Олег Олегович
Канд. техн. наук, доцент каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8-923-403-09-21
Эл. почта: eoo@keva.tusur.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор, проректор по научной работе ТУСУРа
Тел.: 8 (382-2) 514-302
Эл. почта: saa@tusur.ru

Evsutin O.O., Shelupanov A.A.
Basic approaches to the use of mathematical apparatus of cellular automata theory for the tasks of encoding information

In the article we describe some properties and characteristics of the of evolution of a cellular automaton that are important in solving problems of encoding information. We propose the two approaches to the use of mathematical apparatus of cellular automata theory for solving of the given tasks. As extension of classical cellular automaton model we will introduce a notion of cellular automaton with code set.
Keywords: cellular automata, characteristics of the cellular automata, cellular automaton with code set, encoding information.

УДК 004.056

Б.И. Ефимов, Р.Т. Файзуллин

Устойчивость объективного решения экспертов при воздействии угроз по блокированию информации в системах принятия решений с привлечением экспертов

Предложено решение задачи вычисления вероятности принятия ложного решения в системах принятия решения с привлечением экспертов под воздействием угроз информационной безопасности, направленных на блокирование ответов экспертов.

Ключевые слова: информационная безопасность, системы принятия решений, эксперты, угрозы, теория вероятностей.

В настоящее время одними из наиболее динамично развивающихся информационных систем являются системы принятия управленческих решений. Одним из видов указанных систем являются системы, построенные на использовании знаний экспертов-аналитиков.

Данные системы могут использоваться во многих сферах жизнедеятельности. В ряде источников описано применение систем принятия управленческих решений в том числе и для эффективного регулирования уровня информационной безопасности. Так, в [1] приводится общая методология проведения так называемого SWOT-анализа, который может применяться в практике организаций по усилению безопасности; описаны сильные и слабые стороны данного вида анализа.

В настоящей статье рассмотрены некоторые частные вопросы обеспечения информационной безопасности самих систем принятия решений. Как показано в [2], обеспечение безопасности указанных систем является одной из важных задач при их разработке.

Для информационных систем в целом в [3] приводится классификация объектов угроз, позволяющая определить ресурсы, подлежащие защите. В перечень объектов включены: информация; элементы информационной системы (программные и аппаратные) и их настройки; элементы системы защиты (программные и аппаратные) и их настройки.

Угрозы безопасности систем принятия решений с привлечением экспертов в основном могут быть направлены на следующие объекты [4]: экспертов, принимающих участие в опросе, узлы коммутации, линии связи, лицо, принимающее решение.

Виды воздействий на объекты сети могут быть как преднамеренными, т.е. осуществляемыми злоумышленником, так и случайными, обусловленными отказами оборудования, программ и каналов связи. Преднамеренные угрозы направлены, в конечном итоге, на принятие «нужного» для злоумышленника решения. Отказы оборудования носят случайный, непредсказуемый характер и могут повлиять на принятие решения в пользу любой из существующих альтернатив.

В общем случае основной целью применения средств защиты информации является предотвращение ущерба, т.е. предотвращение реализации угроз информационной безопасности [5]. Однако в системах принятия решения для лица, принимающего решение, значимым является лишь конечный результат – выбор экспертами одной из предложенных альтернатив. Как показано в [2], система защиты информации должна быть построена таким образом, чтобы выполнялась единственная задача – решение, принимаемое экспертами при условии реализации возможных угроз, должно быть таким же, что и решение, которое было бы принято системой при полном отсутствии угроз информационной безопасности. Значение «перевеса», с которым побеждает одна альтернатива над другой, а также процентное распределение голосов экспертов между альтернативами не имеют никакого значения.

В [6] подробно рассмотрено поведение систем принятия решений с привлечением экспертов под воздействием угроз информационной безопасности по изменению ответов экспертов в пользу одной из альтернатив.

В данной статье рассмотрим частный случай, когда угрозы по изменению ответов экспертов отсутствуют, но существуют угрозы по блокированию ответов экспертов.

Исходные положения. Пусть опрос экспертов проводится по выбору одной из двух альтернатив: «0» и «1», общее количество экспертов, принимающих участие в голосовании, – m, количество экспертов, проголосовавших за альтернативу «1», – n.

Из всех возможных вариантов голосования экспертов рассмотрим только случаи голосования, когда количество экспертов, проголосовавших за альтернативу «1», равно или превышает количество экспертов, проголосовавших за альтернативу «0» ($n \geq m/2$), и определим, как угрозы информационной безопасности по блокированию ответов экспертов могут привести к выбору лицом, принимающим решение (ЛПР), другой альтернативы (альтернативы «0»).

Будем считать также, что вероятности блокирования ответов экспертов $P_{bloc\,i}$ одинаковы для всех экспертов.

Возможные варианты по выбору альтернативы ЛПР

Answ1 – количество дошедших до ЛПР ответов за альтернативу «1» больше, чем за альтернативу «0»; лицом, принимающим решение, выбирается альтернатива «1»;

AnswEq – количество дошедших до ЛПР ответов за альтернативы «1» и «0» равно, назначается повторное голосование;

Answ0 – количество дошедших до ЛПР ответов за альтернативу «1» меньше, чем за альтернативу «0»; лицом, принимающим решение, выбирается альтернатива «0».

Условия возникновения событий AnswEq, Answ0

Событие AnswEq возникает в случае, если ответов экспертов, отданных за альтернативу «1», блокируется ровно на $(2n - m)$ больше, чем ответов экспертов, отданных за альтернативу «0».

Событие Answ0 возникает в случае, если разница между количеством блокируемых ответов экспертов, проголосовавших за альтернативу «1», и количеством блокируемых ответов экспертов, проголосовавших за альтернативу «0», больше чем $(2n - m)$.

Вероятности наступления событий

Вероятность наступления события AnswEq:

$$P(AnswEq) = \sum_{k=0}^{m-n-1} P(B_k) \cdot P(D_{2n-m+k}), \tag{1}$$

где $P(B_k)$ – вероятность блокирования ровно k ответов экспертов из $(m–n)$ экспертов, проголосовавших за альтернативу «0»; $P(D_{2n-m+k})$ – вероятность блокирования ровно $(2\ m–n\ +k)$ ответов экспертов из n экспертов, проголосовавших за альтернативу «1».

$$P(B_k) = (P_{bloc})^k \cdot (1 - P_{bloc})^{(m-n-k)} \cdot C_{m-n}^k, \tag{2}$$

где C_{m-n}^k – число сочетаний из $m–n$ по k;

$$C_{m-n}^k = \frac{(m-n)!}{k! \cdot (m-n-k)!},$$

$$P(D_{2n-m+k}) = (P_{bloc})^{(2n-m+k)} \cdot (1 - P_{bloc})^{(n-(2n-m+k))} \cdot C_n^{2n-m+k}, \tag{3}$$

где C_n^{2n-m+k} – число сочетаний из n по $(2n - m + k)$;

$$C_n^{2n-m+k} = \frac{n!}{(2n-m+k)! \cdot (m-n-k)!}.$$

Подставляем в (1) формулы (2), (3):

$$P(AnswEq) = \sum_{k=0}^{m-n-1} \left((P_{bloc})^{(2n-m+2k)} (1 - P_{bloc})^{2(m-n-k)} \frac{n! \cdot (m-n)!}{k! \cdot (2n-m+k)! \cdot ((m-n-k)!)^2} \right). \tag{4}$$

Вероятность наступления события Answ0:

$$P(Answ0) = \sum_{k=0}^{m-n-1} P(E_k), \tag{5}$$

где $P(E_k)$ – вероятность появления события E_k.

Событие E_k – для конкретного значения k (количества заблокированных ответов экспертов, проголосовавших за альтернативу «0» ($k = \{0, 1, \ldots m - n - 1\}$), было заблокировано ответов экспертов, проголосовавших за альтернативу «1», более чем на $(2n - m)$ превышающее k ($l = \{2n - m+k+1, 2n–m+k+2, \ldots n\}$).

$$P(E_k) = P(B_k) \cdot P(F_{2n-m+k+1}), \quad (6)$$

где $P(B_k)$ – вероятность блокирования ровно k ответов экспертов из (m–n) экспертов, проголосовавших за альтернативу «0»; $P(F_{2n-m+k+1})$ – вероятность блокирования от ($2n$–m+k+1) до n ответов экспертов, проголосовавших за альтернативу «1».

$$P(F_{2n-m+k+1}) = \sum_{l=2n-m+k+1}^{n} P(D_l), \quad (7)$$

где $P(D_l)$ – вероятность блокирования ровно l ответов экспертов из n экспертов, проголосовавших за альтернативу «1».

$$P(B_k) = (P_{bloc})^k \cdot (1-P_{bloc})^{(m-n-k)} \cdot C_{m-n}^k, \quad (8)$$

где C_{m-n}^k – число сочетаний из m–n по k;

$$C_{m-n}^k = \frac{(m-n)!}{k! \cdot (m-n-k)!},$$

$$P(D_l) = (P_{bloc})^l \cdot (1-P_{bloc})^{(n-l)} \cdot C_n^l, \quad (9)$$

где C_n^l – число сочетаний из n по l;

$$C_n^l = \frac{n!}{l! \cdot (n-l)!}.$$

Подставляем в (6) формулу (7), полученную формулу подставляем в формулу (5):

$$P(Answ0) = \sum_{k=0}^{m-n-1} (P(B_k) \cdot \sum_{l=2n-m+k+1}^{n} P(D_l)). \quad (10)$$

В формулу (10) подставляем формулы (8), (9):

$$P(Answ0) = \sum_{k=0}^{m-n-1} \left((P_{bloc})^k \cdot (1-P_{bloc})^{(m-n-k)} \cdot \frac{(m-n)!}{k! \cdot (m-n-k)!} \cdot \sum_{l=2n-m+k+1}^{n} \left((P_{bloc})^l \cdot (1-P_{bloc})^{(n-l)} \cdot \frac{n!}{l! \cdot (n-l)!} \right) \right). \quad (11)$$

При возникновении события *AnswEq* должно назначаться повторное голосование до тех пор, пока не возникнет событие *Answ*1 или *Answ*0. При этом условная вероятность события *Answ*0 при условии, что произошло одно из этих событий, составляет:

$$P(Answ0 \mid Answ1 \cup Answ0) = \frac{P(Answ0)}{P(Answ1) + P(Answ0)}. \quad (12)$$

Необходимо отметить, что исключением является случай возникновения события *AnswEq*, когда угрозы ИБ отсутствуют и эксперты голосуют поровну за альтернативы «0» и «1». При дальнейшем описании указанный случай (n=m/2, m – четное) рассматриваться не будет.

Вероятность выбора альтернативы «0». Учитывая повторные голосования, назначаемые при возникновении события *AnswEq*, вычислим полные вероятности выбора альтернативы «0» (событие A0):

$$P(A0) = P(Answ0) + P(AnswEq) \cdot P(Answ0 \mid Answ1 \cup Answ0). \quad (13)$$

Вероятность события A0 – вероятность того, что действия злоумышленника приводят к изменению выбранной экспертами альтернативы.

Из формулы (13), используя формулу (12), получаем:

$$P(A0) = P(Answ0) + P(AnswEq) \cdot \frac{P(Answ0)}{P(Answ1) + P(Answ0)} = P(Answ0) \cdot (1 + \frac{P(AnswEq)}{P(Answ1) + P(Answ0)}). \quad (14)$$

Так как события *Answ*1, *AnswEq*, *Answ*0 образуют полную группу событий, получаем:

$$P(A0) = P(Answ0) \cdot (1 + \frac{P(AnswEq)}{1 - P(AnswEq)}) = \frac{P(Answ0)}{1 - P(AnswEq)}. \quad (15)$$

Вероятности $P(AnswEq)$, $P(Answ0)$ находятся по формулам (4), (11).

Программная реализация. Для вычисления вероятности события A0 в зависимости от вероятности блокирования ответов экспертов P_{bloc}, количества экспертов m и количества экспертов, проголосовавших за альтернативу «1», разработан модуль на языке программирования MATLAB.

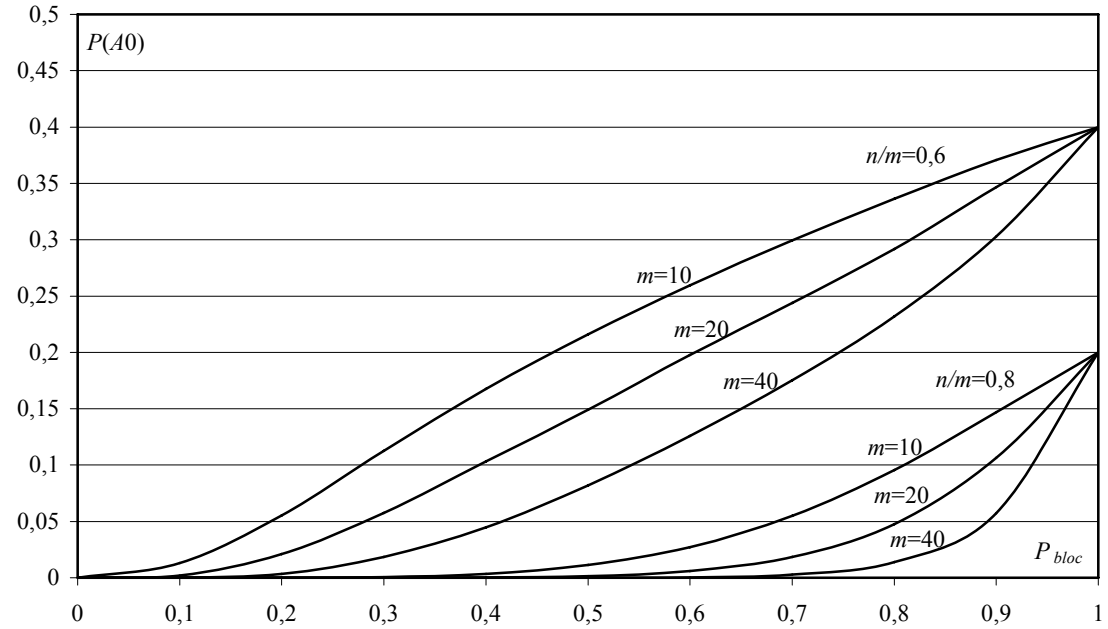


Рис. 1. Вероятность события $A0$ в зависимости от P_{blok} при разных значениях m и n/m

Результаты вычислений. На рис. 1 представлена зависимость вероятности $P(A0)$ от вероятности блокирования отдельного ответа эксперта P_{bloc} , при различных значениях количества экспертов m (m = {10, 20, 40}) и различных соотношениях ответов экспертов, поданных за альтернативы «0» и «1» (n/m = {0,6; 0,8}).

Из данного графика видно, что при $P_{bloc}\rightarrow 1$ значение вероятности $P(A0)$ стремится к значению доли экспертов, проголосовавших за альтернативу «0» ($1–n/m$), при любом значении m.

$$P_{bloc}\rightarrow 1;\ P(A0)\rightarrow 1–n/m.$$

То есть если доля экспертов, проголосовавших за альтернативу «0», равна ($1 – n/m$) и практически все ответы блокируются (кроме одного, так как нахождение $P(A0)$ при блокировании ответов всех экспертов не имеет смысла), то вероятность, что единственный незаблокированный ответ эксперта будет подан за альтернативу «0», также будет равна ($1 – n/m$).

Заключение. В статье показано, что так же, как и в случае воздействия угроз информационной безопасности, направленных на изменение ответов экспертов (подробно описано в [6]), при наличии угроз по блокированию ответов экспертов вероятность принятия ложного решения увеличивается при уменьшении относительного количества экспертов n/m, проголосовавших за альтернативу «1» (m – const, P_{bloc} – const).

При увеличении количества экспертов m, вероятность принятия ложного решения $P(A0)$ уменьшается при любых значениях вероятности блокирования ответов экспертов P_{bloc}, в отличие от случаев воздействия угроз по изменению ответов экспертов, при которых увеличение m приводит к уменьшению $P(A0)$ не при всех значениях P_{bloc}.

Таким образом, одним из способов повышения устойчивости объективного решения в системах принятия решений с привлечением экспертов при воздействии угроз по блокированию информации является увеличение числа экспертов.

Литература

1. Мицель А.А. Модель стратегического анализа информационной безопасности / А.А. Мицель, А.А. Шелупанов, С.С. Ерохин // Доклады ТУСУРа. – 2007. – № 2 (16). – С. 34–41.

2. Ефимов Б.И. Обеспечение информационной безопасности систем принятия решений с использованием теории графов / Б.И. Ефимов, Р.Т. Файзуллин // Динамика систем, механизмов и машин: матер. VII Междунар. науч.-техн. конф. – Омск: Изд-во ОмГТУ, 2009. – Кн. 1. – С. 280–284.

3. Ефимов Б.И. Применение алгоритмов теории графов для решения задач, связанных с обеспечением информационной безопасности в системах принятия решений // Системы управления и информационные технологии. – 2009. – № 1.3 (35). – С. 342–346.

4. Филькин К.Н. Информационно-управляющая система поддержки принятия решений при управлении информационной безопасностью территориально распределенной организацией / К.Н. Филькин, С.Н. Филькин, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 83–86.

5. Авсентьев О.С. Принципы моделирования механизмов воздействия вредоносных программ на защищенные информационные системы в интересах оценки угроз их безопасности / О.С. Авсентьев, В.В. Александров, Г.И. Рябинин, С.В. Скрыль, Р.В. Мещеряков // Доклады ТУСУРа. – 2008. – Т. 2. – № 1. – С. 135–136.

6. Ефимов Б.И. Вероятность принятия ложного решения под воздействием угроз информационной безопасности в системах принятия решений с привлечением экспертов / Б.И. Ефимов, Р.Т. Файзуллин // Доклады ТУСУРа. – 2013. – № 1 (27). – С. 69–74.

Ефимов Борис Игоревич
Аспирант каф. комплексной защиты информации
Омского государственного технического университета (ОмГТУ)
Тел.: 8 (381-2) 79-94-22
Эл. почта: b_efimov@mail.ru

Файзуллин Рашит Тагирович
Д-р техн. наук, профессор, зав. каф. комплексной защиты информации ОмГТУ
Тел.: 8 (381-2) 21-77-02
Эл. почта: r.t.faizullin@mail.ru

Efimov B.I., Faizullin R.T.

Stability of the objective decision of experts at influence of threats on blocking of information in decision-making systems with experts

The solution of a problem of calculation of probability of adoption of the false decision in decision-making systems with involvement of experts as a result of the threats of information security directed on blocking of answers of experts is proposed.

Keywords: information security, decision-making systems, experts, threats, probability theory.

УДК 004.021

Р.Ф. Жаринов

Исследование методов и средств решения задачи поиска вхождения символов в зашифрованные данные

Актуальность задачи поиска вхождений в зашифрованных данных обусловлена быстрым развитием рынка облачного хранения данных, тогда как на сегодняшний день не существует протоколов безопасной обработки данных на стороне облачного сервера, так как при обработке данных в зашифрованном виде либо необходимо передать серверу секретный ключ, либо каждый раз выкачивать всю базу данных. Решение задачи поиска вхождений над зашифрованными данными позволит безопасно хранить данные за пределами доверенной зоны. В настоящей статье рассмотрены общие методы безопасного поиска, а также приведен возможный инструментарий для создания протокола поиска вхождения в зашифрованных данных.
Ключевые слова: поиск в зашифрованных данных, гомоморфизм, метрики поиска вхождения.

В настоящее время среди компаний становится популярным строить информационную инфраструктуру с использованием облачных решений. Для малого и среднего бизнеса использование готовых аутсорсных решений по обработке данных позволяет уменьшить как штат сотрудников, обслуживающих информационные системы, так и сократить время внедрения и развертывания собственной инфраструктуры. Для крупных компаний использование облачных решений предоставляет возможность как горизонтального, так и вертикального масштабирования, в зависимости от изменяющихся условий рынка. Учитывая тот факт, что разглашение, потеря целостности и утечка данных могут разрушить основу для ведения бизнеса, они представляют большую ценность, но зачастую дублируются в открытом виде на многих внешних сервисах облачного хранения.

Компании, разрабатывающие инновационные решения или использующие конфиденциальную информацию, не могут позволить себе пользоваться преимуществами аутсорсных облачных решений ввиду возможности несанкционированного доступа со стороны сотрудников-администраторов внешних сервисов.

При выборе сервиса облачного хранения необходимо учитывать минимальный набор требований, предъявляемых к хранению и обработке информации, а именно:

- Авторизация – использование контроля доступа к собственным ресурсам.
- Безопасность на транспортном уровне – создание безопасного канала между пользовательским устройством и сервером.
- Схемы шифрования – позволяют хранить конфиденциальную информацию в виде, защищающем ее от несанкционированного доступа.
- Безопасный обмен файлами – возможность предоставления доступа к определенному множеству файлов сторонним пользователям, не являющимся клиентами данного сервиса.
- Дедубликация – возможность хранения уникальной информации на одной ноде облачного сервиса, исключая ее дублирование.

Существует достаточное количество сервисов, удовлетворяющих четырем из приведенных требований к хранению и обработке информации, но с использованием схем шифрования при хранении информации существует ряд проблем. В первую очередь это связано с обеспечением безопасной обработки данных в облачной структуре. Под безопасной обработкой понимается возможность производить операции над зашифрованными данными на стороне облачного сервера без передачи на его сторону дополнительной информации о хранимых данных, при этом также встает проблема комфортной работы с данными со стороны клиентов. Большинство предлагаемых решений для работы над зашифрованными данными значительно увеличивают время обработки запросов пользователя.

На сегодняшний день на рынке представлена только одна комплексная система обработки и хранения информации с использованием криптографических примитивов – система управления базой данных (СУБД) CryptDB [1]. Она позволяет производить конечный набор операций над зашиф-

рованными данными, без необходимости их расшифрования на стороне облачного сервера. К таким операциям относятся: сложение, объединение, сравнение, группировка, агрегирование данных, а также поиск по ключевым словам.

Как показывает практика, в современных автоматизированных системах неотъемлемой функцией является использование автодополнения, т.е. поиск вхождения по введенным данным в заданных полях базы данных (БД). В настоящее время не существует ни алгоритма, ни протокола, позволяющих производить операцию поиска вхождения в зашифрованных данных. Так, существует ряд решений для поиска ключевого слова, в случае идентичного совпадения введенного слова и слова в зашифрованном виде. Это не решает задачи успешного поиска, особенно в условии поиска в таких сложных языках, как русский, где у слов существует множество приставок, суффиксов и окончаний, что делает задачу корректной формулировки ключевого слова для поиска практически невыполнимой. Таким образом, настоящая статья будет посвящена поиску вхождений в зашифрованных данных.

Существующие решения. В 2000 г. была опубликована статья Сонга «Practical Techniques for Searches on Encrypted Data» [2], в которой авторы представили набор алгоритмов, позволяющих производить поиск в зашифрованных данных. Сложность поиска представленных алгоритмов была линейной $O(n)$ для каждого зашифрованного документа. Функции шифрования, поиска и расшифрования информации достаточно просты, поэтому будет описан лишь общий подход, используемый в алгоритме (рис. 1).

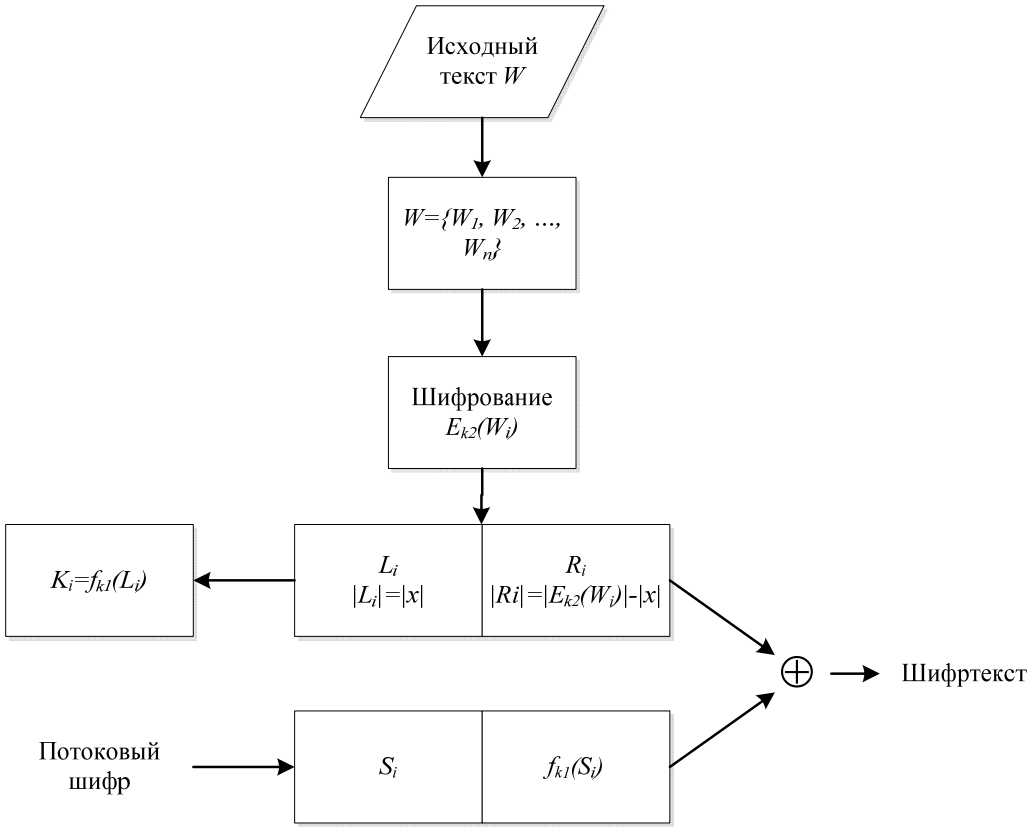


Рис. 1. Алгоритм шифрования в схеме Сонга

Алгоритм шифрования:

• На вход подается документ, который разбивается на слова по заранее заданному признаку (обычно выбирается разделение по расстоянию между словами), и удаляются все уникальные последовательности.

• Из одного мастер-ключа, предоставленного пользователем (MK), создается три подключа $KDF(MK)=<k_1,k_2,k_3>$, используемых в разных частях алгоритма и не позволяющих серверу расшифровать данные.

• Затем каждое слово шифруется стандартным блочным алгоритмом $E_{k_2}(W_i)$, разбивается на две неравные части $<L_i, R_i>$ (зависит от пользовательского параметра длины левой части зашифрованного сообщения x, $x<|W_i|$), дополнительно обрабатываются $S_i = G(k_3)$, $F_{k_i} = (S_i)$, где $k_i = f_{k_i}(L_i)$ и полученные значения складываются между собой (выполняется операция, исключающая или), образуя тем самым шифртекст $C =< L_i, R_i > \oplus < S_i, F_{k_i}(S_i) >$.

Алгоритм поиска:

• Для операции поиска необходимо зашифровать ключевое слово, согласно алгоритму шифрования и передать на сторону сервера $< E_{k_2}(W), f_{k_1}(L) >$.

• После этого сервер начинает обрабатывать каждую хранимую зашифрованную запись $C_i \oplus E_{k_2}(W_i)$, получая на выходе пару значений $< S_i, F_k(S_i) >$.

• И, так как значение длины исходного потокового шифрования известно, а именно x, из полученной пары мы сможем получить строку S_i.

• В итоге мы должны сравнить результат функции $F_{f_{k_i}(L)}(S_i)$ с оставшимися битами $F_k(S_i)$.

Вычислительная сложность приведенного алгоритма детерминированного поиска ключевого слова в зашифрованных данных экспоненциально растет с увеличением входных данных, что объясняет его неприменимость на практике. Подробного описания последующих разработанных схем поиска в зашифрованных данных приводить не будем, поскольку ни одна из них не находит вхождения в зашифрованных данных, а выполняет только поиск ключевых слов при полном совпадении. Ниже приведены некоторые особенности таких решений и их сравнительные характеристики (табл. 1, 2).

Таблица 1

Ключевые особенности существующих схем поиска в зашифрованных данных

Схема	Сложность поиска	Тип поиска	Требуется ли перевычисление предыдущих записей после вставки новых?
Song [2]	$O(n)$	Линейный	Нет
Goh [3]	$O(d)$	Использование предвычисления	Нет
Improved Index [4]	$O(1)$	Использование предвычисления	Да
PEKS [5]	$O(n)$	Линейный	Нет
Ranked [6]	$O(d)$	Использование предвычисления	Да

Таблица 2

Возможности выполнения различного вида поисков в схемах поиска в зашифрованных данных

Схема	Точное соответствие	Поиск вхождения	Регистронезависимый поиск	Регулярные выражения	Поиск стеммы
Song	Да	Нет	Нет	Нет	Нет
Goh	Да	Возможно	Возможно	Нет	Возможно
Improved Index	Да	Возможно	Возможно	Нет	Возможно
PEKS	Да	Возможно	Возможно	Нет	Возможно
Ranked	Нет	Нет	Да	Нет	Да

Впоследствии появилось много статей, которые, используя разные техники, уменьшали вычислительную сложность предложенных схем. Но в итоге задача поиска остановилась на возможности определения вхождения ключевого слова в зашифрованном множестве данных.

Какие же можно придумать решения для организации как минимум регистронезависимого поиска, а как максимум поиска вхождения?

Универсальное решение, конечно же, будет вводить избыточность, т.е. помимо шифрования основного теста, необходимо произвести его модифицирование (а именно привести к нижнему регистру) и так же зашифровать. Данный способ увеличит место хранения информации и увеличит скорость поиска необходимого ключевого слова как минимум в 2 раза. Исходя из данного заключения, можно подытожить, что метод поиска вхождения если и будет работать, то очень медленно (поэтому в табл. 2 используется слово «возможно»).

Возможный инструментарий для поиска вхождения в зашифрованных данных. Какие же существующие криптографические и математические протоколы можно взять за основу для протокола поиска вхождения? К сожалению, такого инструментария оказалось немного. Наиболее хорошо подходят: метрики вычисления расстояния между строками и использование скрытых вычислений. Рассмотрим подробнее каждый из перечисленных инструментариев.

Опишем основные метрики вычисления расстояния между строками как разной, так и одинаковой длины. Расстояние Хемминга [7] относится к метрике вычисления расстояния между множеством одинаковой длины и определяет количество бит (если рассматривать двоичные векторы) которые необходимо изменить, чтобы превратить одну строку в другую: $D_h(x,y)=\sum_{i=1}^{n} x\oplus y$.

Расстояние Левенштейна [7, 8] определяется как минимальное число требуемых операций преобразования (вставка, удаление и замена) для преобразования одной строки в другую. В качестве решения подобного рода задач используется алгоритм динамического программирования, который хранит в матрице количество операций изменения во всех возможных суффиксах и префиксах в обеих строках. Сложность вычисления данного алгоритма – $O(|x|\times|y|)$, а объем памяти для хранения матрицы – $O(\max|x||y|)$. Данное расстояние определяется рекуррентной формулой

$$D_i(x,y)=d(a,b),\ \text{где}\ a=|x|,b=|y|,$$

$$d(i,j)=\begin{cases} \begin{matrix} 0,\ \text{if}\ i=0,\ j=0,\\ i,\ \text{if}\ j=0,\ i>0,\\ j,\ \text{if}\ i=0,\ j>0, \end{matrix} \\ \min\begin{pmatrix} d(i,j-1)+1 \\ d(i-1,j)+1 \\ d(i-1,j-1)+\begin{cases}1,\ \text{if}\ x[i]=y[i]\\ 0,\ \text{if}\ x[i]\neq y[i]\end{cases}\end{pmatrix}, \ \text{if}\ \ i>0,\ j>0. \end{cases}$$

К недостаткам рассмотренного алгоритма можно отнести необходимость запоминания проделанных операций преобразования ввиду того, что результатом поиска вхождения является только операция «удаление».

Рассмотрим более сложную гибридную функцию вычисления расстояния Монг-Элкан (Monge-Elkan) [8], в которой используется рекурсивная схема сравнения для двух строк. Для начала строка x разбивается на подмножество $\{a_1,a_2,\ldots,a_{|x|}\}$, и строка y разбивается на $\{b_1,b_2,\ldots,b_{|y|}\}$, затем функция сравнения принимает вид $D_{me}(x,y)=\frac{1}{|x|}\sum_{i=1}^{|x|}\max_{j=1} D'(A_i,B_i)$, где D' – это некоторая второстепенная функция вычисления расстояния. Если в качестве второстепенной функции взять модифицированную функцию (при условии того, что для поиска вхождения нам необходима только операция удаления) расчета расстояния Левенштейна, получим итоговую формулу поиска вхождения, при $D_{mel}(x,y)=\begin{cases}1, & \text{если } x \text{ является вхождением в } y,\\ <1, & \text{если } x \text{ не является вхождением в } y:\end{cases}$

$$D_{mel}(x,y)=\frac{1}{|x|}\sum_{i=1}^{|x|}\max_{j=1}\begin{cases} \begin{matrix} 0,\ \text{if}\ \ i=0,\ j=0;\\ 0,\ \text{if}\ \ j=0,\ i>0;\\ 0,\ \text{if}\ \ i=0,\ j>0; \end{matrix} \\ d(i-1,j-1)+\begin{cases}1,\ \text{if}\ \ x[i]=y[i],\\ 0,\ \text{if}\ \ x[i]\neq y[i],\end{cases}\ \text{if}\ \ i>0,\ j>0. \end{cases}$$

В табл. 3 приведены результаты сравнения работы некоторых метрик при поиске вхождения слов «ell» и «all» в слове «hello».

Как видно из таблицы, модифицированный алгоритм Монг-Элкан выдает нужный нам результат, но с сокращением сложности алгоритма.

Что же касается использования критографических примитивов в применении скрытых вычислений, представляется возможным использование только двух способов: забывчивая передача (OT) [9] и гомоморфная криптосистема. Под OT-протоколом понимается тип передачи, в котором отправитель не запоминает, что было передано получателю и было ли передано вообще. В большинстве

случаев сложность такой передачи является полиномиальной. Использование гомоморфной криптосистемы с аддитивными свойствами позволяет взаимодействовать между отправителем и получателем более эффективно и с меньшей сложностью.

Таблица 3

Вычисления расстояний с использованием различных метрик

Метрика	Вычисленное расстояние Hello и ell	Вычисленное расстояние Hello и all
Levenshtein	2,0	3
MongeElkan	1,0	0,8(6)
SmithWaterman [7]	6,0	4,0
JaroWinkler [7]	0,8(6)	0,6(8)
Модифицированный MongeElkan	1,0	0,(6)

На сегодняшний момент криптосистема Пэйе [10] является одной из систем вероятностного шифрования, обладающая гомоморфным свойством аддитивности. Использование такой криптосистемы является наиболее перспективным с точки зрения решения задачи скрытых вычислений при поиске вхождения в зашифрованных данных.

Заключение. В настоящей статье приведен обзор существующих решений поиска в зашифрованных данных. На сегодняшний день не существует алгоритма, способного на практике продемонстрировать возможность поиска вхождения в зашифрованном тексте. В работе приведен обзор метрик, позволяющих вычислить минимальное расстояние для преобразования одной строки в другую, что необходимо для дальнейшей разработки двухстороннего протокола поиска вхождения в зашифрованных данных. В метрике было предложено использование гибридной функции подсчета расстояния, а в качестве второстепенной функции вычисления расстояния использовать модифицированное расстояние Левенштейна только с операцией удаления префиксов и суффиксов. В качестве основы безопасности дальнейшего протокола планируется использовать гомоморфную криптосистему Пэйе, которая поддерживает свойство аддитивности.

Литература

1. CryptDB: Protecting Confidentiality with Encrypted Query Processing / R.A. Popa, C.M.S. Redfield, N. Zeldovich, H. Balakrishnan // Proceedings of the 23-rd ACM Symposium on Operating Systems Principles. – Cascais, Portugal, 2011. – P. 85–100.

2. Song D.X. Practical Techniques for Searches on Encrypted Data / D.X. Song, D. Wagner, A. Perrig // Proceedings of IEEE Symposium on Security and Privacy, S&P 2000. – Berkeley, USA, 2000. – P. 44–55.

3. Secure indexes [Электронный ресурс]. – Режим доступа: http://crypto.stanford.edu/~eujin/papers/secureindex/secureindex.pdf, свободный (дата обращения: 20.05.2014).

4. Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions / R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky // Proceedings of the 13th ACM conference on Computer and communications security. – Alexandria, USA. – 2006. – P. 79–88.

5. Public Key Encryption with Keyword Search / D. Boneh, G.D. Crescenzo, R. Ostrovsky, G. Persiano // Proceedings of Eurocrypt 2004. – Interlaken, Switzerland, 2004. – P. 506–522.

6. Confidentiality-preserving rank-ordered search / A. Swaminathan, Y. Mao, G.M. Su et al. // Proceedings of the 2007 ACM workshop on Storage security and survivability. – N.Y., USA, 2007. – P. 7–12.

7. String Similarity Metrics for Information Integration [Электронный ресурс]. – Режим доступа: http://www.coli.uni-saarland.de/courses/LT1/2011/slides/stringmetrics.pdf, свободный (дата обращения: 25.04.2014).

8. Cohen W.W. A comparison of string distance metrics forname-matching tasks / W.W. Cohen, P. Ravikumar, S.E. Fienberg // Proceedings of the IJCAI-2003 Workshop on Information Integration on the Web. – Acapulco, Mexico, 2003. – P. 73–78.

9. Naor M. Oblivious transfer with adaptive queries / M. Naor, B. Pinkas // Proceedings of 19-th Annual International Cryptology Conference. – Santa Barbara, California, USA, 1999. – P. 573–590.

10. Paillier P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes // Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques. – Prague, Czech Republic, 1999. – P. 223–238.

Жаринов Роман Феликсович
Аспирант каф. технологий защиты информации
Санкт-Петербургского государственного университета аэрокосмического приборостроения
Тел.: 8 (812) 494-70-77
Эл. почта: roman@vu.spb.ru

Zharinov R.F.
Research of methods and instruments for searching entry in encrypted data

Problem of searching entry in encrypted data is relevant whereas the rapid development of cloud storage market. While today there is no security protocol processing on the server side of the cloud. For processing data in encrypted form it's need to pass secret key to server or download full database each time. Solution of the problem of searching entry in encrypted data will allow to store data outside the trusted zone in secure form. This article reviews the general methods of secure search, as well as instruments to create a protocol of searching entry in encrypted data.
Keywords: searching entry in encrypted data, homomorphism, string methods distance.

УДК 004.056

С.Л. Зефиров, А.Ю. Щербакова

Оценка инцидентов информационной безопасности

Рассматривается способ оценки инцидентов информационной безопасности, основанный на факторах событий информационной безопасности. Предложены алгоритм оценки инцидентов информационной безопасности и его программная реализация.

Ключевые слова: инцидент, информационная безопасность, фактор, первичная оценка, вторичная оценка, анализ.

С ростом числа информационных систем и совершенствованием информационных технологий растёт и число инцидентов информационной безопасности (ИБ), под которыми понимается одно или несколько нежелательных событий (событий ИБ), которые влияют на информационную безопасность активов систем и могут привести к негативным последствиям. Такими последствиями могут быть, например, нарушение конфиденциальности, целостности и доступности информационных активов, прерывание бизнес-процессов и др.

Международный стандарт ISO 27001:2005 [1] обращает особое внимание на необходимость создания процедуры управления инцидентами информационной безопасности – очевидно, что без своевременного реагирования на инциденты ИБ, устранения их последствий и возможных причин невозможно эффективное управление информационной безопасностью. В международном стандарте ISO/IEC 27035 [2] и национальном стандарте ГОСТ Р ИСО/МЭК 18044:2007 [3] приводятся процессы управления инцидентами информационной безопасности. Рассматриваются вопросы обеспечения нормативно-распорядительной документацией, ресурсами, даются рекомендации по необходимым процедурам для реализации этих процессов, в том числе по классификации инцидентов ИБ, распределению ролей при обработке инцидента ИБ, порядку обработки инцидентов ИБ. Схема управления обработкой инцидентов ИБ в соответствии с [2, 3] приведена на рис. 1.

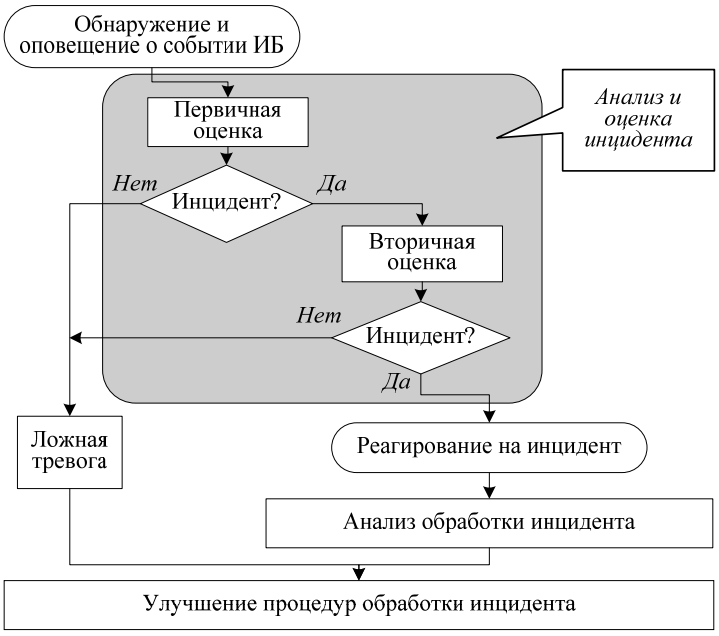


Рис.1. Управление обработкой инцидентов ИБ

Постановка задачи. Обнаружение, анализ и оценка инцидента ИБ являются определяющими этапами при управлении инцидентами ИБ, поскольку от своевременности и достоверности информации, полученной на этих этапах для принятия решения по реагированию на инцидент, зависит успешность его обработки.

Зачастую в организациях отсутствует методика обнаружения инцидентов ИБ, сотрудники не знают, какие события могут являться инцидентами ИБ, поскольку они не всегда связаны с прерываниями основной деятельности. Анализ и оценка инцидентов ИБ также могут быть затруднительны из-за недостаточности информации о произошедших инцидентах, их причинах и последствиях. Существует необходимость в создании и поддержке актуальной базы событий и инцидентов ИБ. База событий и инцидентов ИБ может быть создана на основе собственного опыта обработчиков инцидентов ИБ и сведений о произошедших инцидентах из различных источников. Сведения об инцидентах ИБ, произошедших в организациях, особенно в крупных фирмах, компаниях, обычно не публикуются, чтобы избежать риска повторных атак на их системы и потери репутации. Но аналитики ИБ при исследовании проблем обеспечения информационной безопасности, например на промышленных и других предприятиях [4], приводят обзоры обнаруженных уязвимостей информационных технологий, статистику инцидентов ИБ за определенный период, например [5,6], без указания организаций, в которых эти инциденты происходили. Подобные сведения позволяют регулярно обновлять базу инцидентов ИБ для поддержания её в актуальном состоянии.

Анализ и оценка инцидента ИБ представляют сложность ввиду большого объема информации, необходимой для идентификации событий ИБ как инцидентов, определения причин и источников этих событий, а также возможного развития их негативных последствий, поэтому эти процедуры должны быть формализованы и автоматизированы.

Задачей настоящей работы является разработка способа повышения оперативности анализа и оценки инцидентов ИБ с помощью их автоматизации и обеспечения адекватности принятия решения по обработке инцидентов ИБ за счет информационного обеспечения процедур их обнаружения, анализа и оценки на основе базы данных о произошедших событиях и инцидентах ИБ.

Оценка инцидентов информационной безопасности на основании их факторов. Первичная оценка идентификации события ИБ как инцидента ИБ может осуществляться на основании факторов событий ИБ, указывающих на определённый вид инцидента. Фактор события ИБ – признак события ИБ, указывающий на возможное нарушение ИБ или аварию защитных мер (средств), а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью. Факторы событий могут быть выявлены обработчиками инцидентов ИБ техническими средствами в процессе мониторинга систем и плановых проверок или сотрудниками организации в ходе выполнения ими основной деятельности.

Так как нежелательные события в системе, например замедление работы, отказы и сбои программного обеспечения и т.д., не всегда свидетельствуют об инциденте ИБ, необходимо подтверждение актуальности их факторов, для чего должна осуществляться вторичная оценка. По результатам вторичной оценки принимается решение, является ли инцидент ложным, реальным или потенциальным [7]. Для потенциальных инцидентов ИБ можно вычислить их вероятность, зная частость нежелательных событий в их сценариях и результативность защитных мер, направленных на предотвращение инцидентов ИБ, выбранных по результатам оценки рисков [8].

Для автоматизации процесса анализа и оценки инцидентов ИБ было разработано программное средство, алгоритм которого представлен на рис. 2.

С целью идентификации инцидентов ИБ обработчику необходимо на основе полученных от источника данных об обнаруженных событиях ИБ отметить в предустановленных списках соответствующие факторы инцидентов ИБ. Списки факторов инцидентов ИБ составляются на основе базы данных о произошедших событиях и инцидентах ИБ и регулярно обновляются. Затем обработчику необходимо выбрать вид инцидента для детального рассмотрения. В соответствии с выбранным видом инцидента ИБ программой строятся его сценарии.

В разработанном программном средстве предусмотрена функция вторичной оценки, которая представляет собой сбор дополнительной информации относительно обнаруженных факторов и соответствующих им событий для подтверждения их актуальности. В комментариях к каждому событию приводятся сведения о том, например, какая дополнительная информация нужна для подтверждения или опровержения факторов, и источник этой информации. Программа перестраивает сценарий инцидента в соответствии с подтвержденными при вторичной оценке факторами. Кроме того, программное средство позволяет построить все возможные сценарии инцидента, факторы которых отмечены не были (рис. 3). Эта функция позволяет обработчику инцидентов произвести сбор дополнительных сведений по рассматриваемому инциденту ИБ и повысить достоверность информации для принятия решения о мерах по реагированию на него.

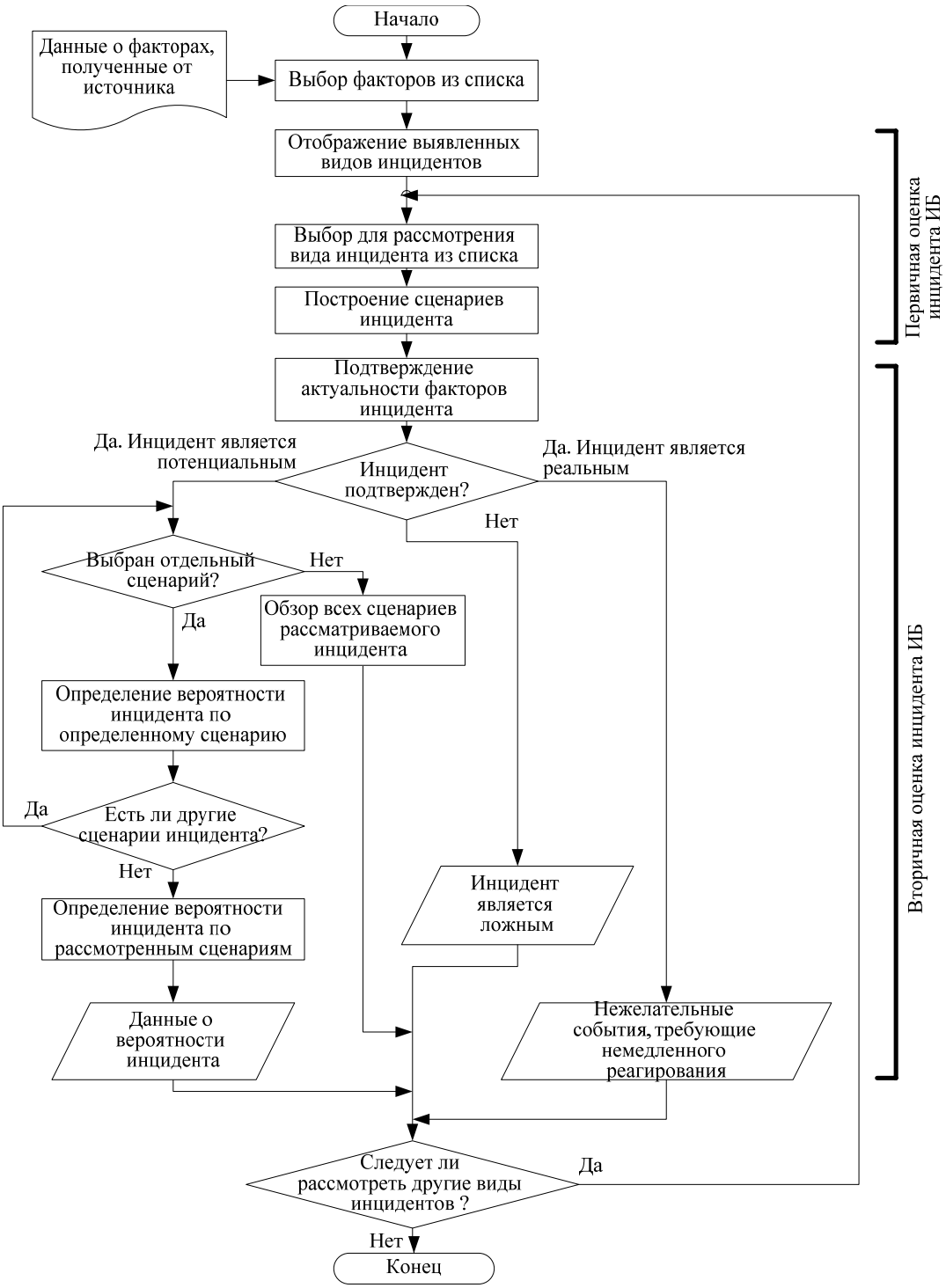


Рис. 2. Алгоритм работы программного средства

Программное средство позволяет оценить вероятность потенциального инцидента по отдельным его сценариям в соответствии с частотой нежелательных событий и уровнем защитных мер по их предотвращению. Для этого в программе установлено 5 уровней защитных мер – от 0 (защитные меры отсутствуют) до 4 (защитные меры предотвращают нежелательное событие в сценарии инцидента). Каждому уровню соответствует коэффициент результативности защитных мер – z. Например, если выбран «шаг» между уровнями, равный 0,25, то для защитных мер с уровнем 1 коэффициент результативности будет равен 0,75 (т.е. применение этих защитных мер снижает вероятность события инцидента на 0,25), а для защитных мер с уровнем 2 коэффициент будет равен 0,5 (т.е. применение этих защитных мер снижает вероятность события инцидента на 0, 5) и т.д. Вероят-

ность нежелательного события в сценарии инцидента в соответствии с [8] определяется следующим образом:

$$P_{HC} = h_i z_i \,, \tag{1}$$

где P_{HC} – вероятность нежелательного события; $i = \overline{1,n}$, где n – количество нежелательных событий в сценарии инцидента; h_i – частость события, являющегося причиной нежелательного события; z_i – коэффициент результативности защитных мер, направленных на предотвращение нежелательного события в сценарии инцидента.

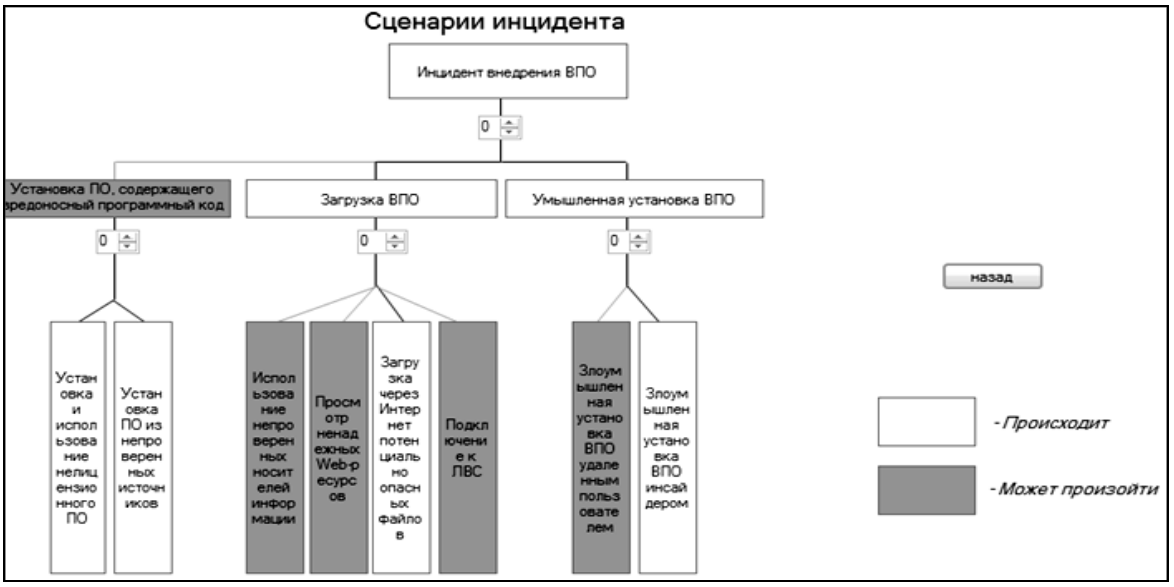


Рис. 3. Обзор сценариев инцидента внедрения ВПО

Вероятность инцидента по отдельному сценарию $P_И$ в соответствии с [8] определяется следующим образом:

$$P_И = \prod_{i=1}^{n} h_i z_i \,. \tag{2}$$

Результат определения вероятности инцидента ИБ по его отдельному сценарию на примере инцидента внедрения вредоносного программного обеспечения (ВПО) приведен на рис. 4.

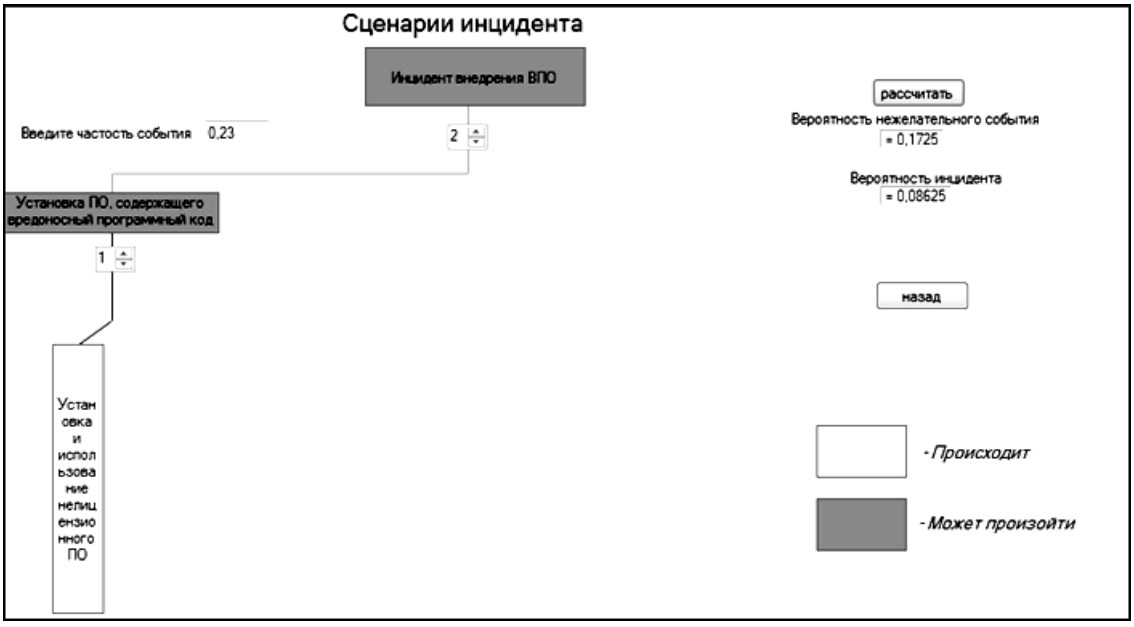


Рис. 4. Результат определения вероятности инцидента внедрения ВПО

Заключение. Таким образом, способ, реализуемый программным средством, позволяет по наблюдаемым факторам выделить соответствующий инцидент ИБ, рассмотреть наглядно его возможный сценарий, подсчитать вероятность инцидента, с учетом условных уровней защитных мер. Также программа даёт возможность просмотреть возможные нежелательные события инцидента, которые не были выявлены пользователем.

Разработанное программное средство дает возможность оценить происходящие в системе инциденты ИБ на основе актуальной базы данных о произошедших событиях и инцидентах ИБ, тем самым способствуя существенному уменьшению времени и повышению достоверности информации для адекватного принятия решения по обработке обнаруженных инцидентов ИБ.

Литература

1. ISO/IEC 27001:2005. Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. – 2005. – 54 с.

2. ISO/IEC 27035:2011. Информационные технологии. Метод обеспечения безопасности. Управление случайностями в системе информационной безопасности. – 2011. – 78 с.

3. ГОСТ Р ИСО/МЭК 18044:2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – М.: Стандартинформ, 2009. – 50 с.

4. Утечки конфиденциальной информации (итоги 2013 года) [Электронный ресурс]. – Режим доступа: http://www.banki.ru/news/research/?id=6242078, свободный (дата обращения: 19.06.2013).

5. Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств [Электронный ресурс]. – Режим доступа: http://www.securitylab. ru/analytics/398184.php, свободный (дата обращения: 19.06.2013).

6. ИБ инциденты СНГ 2011 г. [Электронный ресурс]. – Режим доступа: http://www. security-scripts.ru/download/books/ib-incidenty.pdf, свободный (дата обращения: 19.06.2013).

7. Щербакова А.Ю. Алгоритм обнаружения и анализа инцидентов информационной безопасности на основании их факторов // Открытые инновации – вклад молодежи в развитие региона: сб. матер. рег. молодежного форума (г. Пенза, 6 декабря 2013 г.). – Пенза: Изд-во ПензГУ, 2013. – Т. 1. – С. 225–226.

8. Щербакова А.Ю. Вероятностная оценка последствий инцидентов информационной безопасности // Труды междунар. симпозиума «Надежность и качество – 2013». – Пенза: Изд-во ПензГУ, 2013. – Т. 1. – С. 125–128.

Зефиров Сергей Львович
Канд. техн. наук, доцент, зав. каф. информационной безопасности систем и технологий
Пензенского государственного университета (ПензГУ)
Тел.: 8 (841-2) 36-82-23
Эл. почта: ibst@pnzgu.ru

Щербакова Анастасия Юрьевна
Аспирант каф. «Информационная безопасность систем и технологий» ПензГУ
Тел.: 8 (841-2) 36-82-23

Zefirov S.L., Shcherbakova A.Y.
Information security incidents assessment

A way of information security incidents assessment based on information security events' factors is considered in this paper. An algorithm and its program implementation are suggested.
Keywords: incident, information security, factor, first assessment, second assessment, analysis.

УДК 004.732

С.Ю. Исхаков, А.А. Шелупанов, А.Ю. Исхаков

Имитационная модель комплексной сети систем безопасности

Предложен подход к построению имитационной модели информационной безопасности комплексных сетей систем безопасности. Определены характерные особенности сетей данного типа и показана разница в подходах к обеспечению их защиты по сравнению с типовыми локально-вычислительными сетями. Предложена имитационная модель, учитывающая не только внешние, но и внутренние угрозы нарушения информационной безопасности системы.

Ключевые слова: комплексные сети систем безопасности, имитационная модель, инцидент безопасности, частная модель.

Проблемы мониторинга комплексных сетей систем безопасности. Решение задач, связанных с обеспечением безопасности жизни и здоровья человека на предприятиях, базируется на двух аспектах. С одной стороны, действующее законодательство обязывает работодателя обеспечить безопасность жизни и здоровья сотрудников во время исполнения ими своих служебных обязанностей. С другой стороны, любая организация является участником рыночных отношений и заинтересована в обеспечении сохранности своего имущества. Необходимо отметить, что системы безопасности априори не являются источником дохода для компании. Основной принцип таких систем – снижение рисков нанесения материального ущерба.

Для достижения баланса между затрачиваемыми экономическими ресурсами и стоимостью рисков реализации угроз безопасности большинство современных организаций оборудуют свои объекты системами безопасности. К ним относятся охранно-пожарные сигнализации, видеонаблюдение, системы контроля и управления доступом, системы автоматического пожаротушения и оповещения о пожаре, а также различные инженерные системы диспетчеризации.

В большинстве случаев перед администраторами систем безопасности возникает задача объединения их в единый комплекс с централизованным управлением. Широко распространенным подходом к решению подобных задач является объединение гетерогенного оборудования на базе технологий локальных сетей: все управляющие блоки задействованных систем связываются в комплексную сеть систем безопасности (КССБ).

Под КССБ понимается сложный гетерогенный комплекс аппаратного и программного обеспечения (ПО), различающегося по принципам действия и типу предоставляемой оператору информации, но объединенного общей задачей. Задача такого комплекса состоит в обеспечении безопасности человека на предприятии и снижении вероятности нанесения материального ущерба компании.

В качестве платформы для создания единой системы передачи информации используются технологии локально-вычислительных сетей (ЛВС). Эксплуатация таких комплексов связана с рядом исключительных особенностей:

1. *Гетерогенность оборудования и ПО.* Из-за чрезмерно большой области задач, решаемых с помощью КССБ, существует огромное количество производителей и решений для каждой из подсистем. Действующее законодательство не регламентирует создание таких комплексов. Государственные регуляторы контролируют проектирование, монтаж и эксплуатацию систем, связанных с обеспечением пожарной безопасности объектов. Все остальные слаботочные инженерные системы не являются обязательными и внедряются исключительно по желанию хозяйствующего субъекта. Это приводит к проблемам агрегирования информации, предоставляемой различными подсистемами.

2. *Апериодичность нагрузок.* Одной из наиболее характерных особенностей функционирования КССБ является отсутствие какой-либо периодичности в распределении нагрузки на элементы. Все системы безопасности направлены на выявление и предупреждение о возникновении внештатной ситуации. Большую часть времени они работают в режиме ожидания, и нагрузка на элементы минимальна. Так, например, в КССБ нередко используется видеосервер, к которому подключены аналоговые видеокамеры. Сервер собирает информацию и помещает ее в локальное хранилище. В данном режиме генерируемый им трафик минимален. В случае подключения к серверу клиентского

приложения с удаленной рабочей станции начинается передача информации. Особенностью трансляции видео в ЛВС является потребление всей свободной части канала передачи данных.

3. *Высокая степень приоритетности обслуживания.* В состав КССБ входят подсистемы обеспечения безопасности жизнедеятельности человека (системы пожарной безопасности, электронные проходные и т.д.), поэтому данная сеть требует повышенных мер по организации бесперебойной работы и приоритетности обслуживания.

4. *Наличие критически важной информации* [1]. Внутри КССБ хранится и передается информация, имеющая критическое значение для компании. К ней относятся не только оповещения о внештатных ситуациях, но и видеозаписи камер охранного наблюдения, журналы доступа к объектам, настройки средств противодействия шпионажу и т.д.

5. *Территориальная распределенность.* Из-за высокой стоимости внедрения и обслуживания КССБ обычно разворачивается на предприятиях среднего и крупного бизнеса. Основным инструментом снижения затрат на системы безопасности являются унификация структуры и объединение территориально удаленных объектов компании с созданием единого центра управления.

Несмотря на то, что в основе КССБ лежат технологии локальных сетей, подходы к обеспечению информационной безопасности (ИБ) [1, 2], используемые в типовых ЛВС, ограниченно применимы для КССБ. Это объясняется тем, что нарушение доступности или целостности таких сетей может привести к возникновению чрезвычайных ситуаций. Разница подходов к ИБ для типовых ЛВС и КССБ представлена в таблице.

Различия подходов к обеспечению ИБ в ЛВС и КССБ

Вопросы ИБ	ЛВС	КССБ
Средства антивирусной защиты	Широкое применение	Используются редко
Жизненный цикл системы	3–5 лет	8–10 лет
Установка исправлений безопасности	Регулярно	Нерегулярно
Управление изменениями	Систематически	При необходимости
Критически важная информация	Задержки допускаются	Задержки недопустимы
Доступность	Задержки допускаются	Задержки недопустимы
Аудит ИБ	Планируется и реализуется внешними организациями	Внутренний аудит

Из сравнительной таблицы видно, что типовые методы обеспечения ИБ ЛВС применимы для КССБ в малой степени. Это определяет необходимость защиты КССБ дополнительными средствами.

Многие из систем, входящих в КССБ, обладают собственными средствами защиты, которые необходимо согласовать между собой. Поскольку для обеспечения безопасности любой корпоративной информационной системы важно наличие общей платформы, то необходима эффективная политика безопасности [3] как основа для согласования всех компонентов защиты. Для обеспечения защиты КССБ проектировщиками и администраторами принимаются решения, направленные на максимальную изоляцию от общей сети передачи данных (СПД) компании, вплоть до разделения на физическом уровне. В точках соприкосновения с СПД внедряют системы обнаружения вторжений [5].

Основная проблема заключается в том, что при использовании такого подхода рассматриваются только риски [9, 10], связанные с внешними вторжениями в КССБ. Степень вероятности реализации внутренних угроз [3] нарушения доступности, целостности или конфиденциальности системы обычно принимают низкой. К таким угрозам можно отнести выход из строя видеокамеры либо архива видеозаписей, потерю питания станций пожарной сигнализации, отключение считывателей карт доступа, распространение вредоносных программ по причине человеческого фактора и т.д. В случае реализации таких угроз могут произойти как однозначно выявленные (явные), так и скрытые инциденты безопасности [1].

В случае КССБ под инцидентом безопасности (инцидентом) понимается любое незаконное, неразрешенное, неблагоприятное событие (НС), которое совершается в информационной системе.

К явным ИБ можно отнести, например, выход из строя видеосервера, и как следствие исчезновение сигнала с нескольких видеокамер. Если в организации имеется пост охраны, куда выводятся данные с видеокамер, то такое событие, вероятно, будет незамедлительно обнаружено и оперативно будут приняты меры по нейтрализации данной угрозы.

В случае выхода из строя сетевого хранилища камеры продолжат свою работу, видеосъемка будет продолжаться, но архива записей не будет. Время выявления такого инцидента может возрасти

до нескольких дней. Наступление такого события можно охарактеризовать как скрытый инцидент. Если в период окна опасности [1, 5], возникшего по причине скрытого инцидента, произойдет другой инцидент (например, кража имущества из помещения, контролируемого только видеокамерой), то стоимость риска кратно повысится, так как невозможно будет предпринять действия по идентификации нарушителя и провести расследование.

Таким образом, несмотря на изолированность КССБ и наличие средств защиты периметра, остается актуальной задача контроля текущего состояния КССБ и обеспечения выполнения основных функций всех систем безопасности. Для решения такой задачи необходимо организовать управление рисками реализации не только внешних, но и внутренних угроз. Учитывая приведенное ранее определение инцидента безопасности, в список угроз должны быть включены события, способные привести к аппаратным сбоям элементов системы.

Организация контроля текущего состояния системы сводится к проектированию и внедрению систем мониторинга ЛВС. Однако для сохранения принципа систем безопасности необходимы также средства прогнозирования инцидентов.

Определение нестабильного состояния системы на основе данных мониторинга. Задача обнаружения сбоев в работе ЛВС является весьма сложной из-за невозможности четкого определения критериев и разделения инцидентов безопасности и штатного изменения режима работы системы [7]. В данном случае наиболее обоснованным является подход к решению такой задачи с помощью мониторинга необходимого числа параметров с целью выявить отклонения в стабильной работе системы. В [8] рассмотрены основные аспекты использования подобных систем. Установлено, что принцип их работы основан либо на использовании сигнатур, либо на привлечении статистических методов.

Учитывая вышеописанные особенности КССБ, решение поставленных задач предпочтительно осуществлять с помощью статистических методов. Авторами была предложена методика [2], позволяющая определять необходимый и достаточный набор параметров для обнаружения инцидентов безопасности при заданном уровне детализации.

Полученные в результате использования предложенной методики частные модели сетевых элементов (СЭ) можно описать в виде (1)

$$\mathbf{E} = (p_1, p_2, \ldots, p_k), \tag{1}$$

где $p_1, \ldots, p_k$ – параметры СЭ, k – количество выбранных параметров для данной частной модели.

В текущий момент времени каждый из параметров СЭ характеризуется определенным значением δ. Текущее состояние СЭ есть совокупность текущих значений его параметров в данный момент времени. Если обозначить состояние СЭ как $\boldsymbol{\sigma}$, то

$$\boldsymbol{\sigma}_i = (\delta_1, \delta_2, \ldots, \delta_k), \tag{2}$$

где i – это текущий момент времени.

Задача выявления сбоев в работе системы сводится к определению, является ли текущее значение параметра δ_k свидетельством наступления инцидента безопасности.

Критерии выявления инцидентов безопасности могут быть представлены в виде логических функций

$$Criterion = (O, P, Z). \tag{3}$$

Функция (3) имеет булеву область значений и принимает значение ИСТИНА, когда параметр P объекта O находится в пределах допустимых значений Z, и ЛОЖЬ – в противном случае.

СЭ находится в безопасном состоянии, когда все связанные с ним функции Criterion принимают значение ИСТИНА.

Из предложенной в [4] методики следует, что если конкретный параметр СЭ входит в его частную модель (при заданном уровне детализации), то должно существовать правило, относящее его к данному СЭ (4).

$$r(O, P), \tag{4}$$

где O – конкретный СЭ; P – конкретный параметр СЭ.

Тогда $R = \{r = r(O, P)\}$ – множество правил r, сформированное в результате применения методики для определения необходимого и достаточного набора параметров для обнаружения инцидентов безопасности.

Имитационную модель информационной безопасности КССБ при заданном уровне детализации можно описать совокупностью СЭ, наборов параметров и критериев, разработанных для проверки соответствия состояния системы требованиям действующей политики безопасности (5):

$$\begin{aligned} &\forall O \in S, \\ &\forall P \exists r = r(O,P) \in R, \\ &\forall P \exists Criterion = (O,P,Z). \end{aligned} \tag{5}$$

Применение имитационной модели для оценки состояния системы. Полученную имитационную модель можно использовать для определения текущего состояния системы (рис. 1). На вход модели подаются текущие значения параметров СЭ, полученные на этапе сбора информации. В случае выполнения всех условий (5) вычисляется значение критерия для каждого из проверяемых показателей. Если в результате проверки все критерии имеют значение ИСТИНА, то система находится в безопасном состоянии, в противном случае – нет. Другими словами, система находится в безопасном состоянии, если текущие значения параметров всех СЭ соответствуют требованиям политики безопасности.

Рис. 1. Применение имитационной модели информационной безопасности КССБ

После получения имитационной модели нерешенным остается вопрос формирования критериев. Учитывая масштабы КССБ и особенности ее функционирования, множество *R* может содержать десятки и сотни критериев. На ранних стадиях исследования авторами предпринимались попытки решения данной задачи путем формирования критериев в виде пороговых значений для каждого параметра. Исследования показали, что такой подход не является эффективным.

Во-первых, количество контролируемых параметров прямо пропорционально количеству СЭ в системе, которое имеет тенденцию увеличиваться. Это приводит к увеличению времени и ресурсов, необходимых для формирования всех критериев.

Во-вторых, формирование критериев возможно только на основе экспертных оценок, построенных на базе продолжительных наблюдений.

В-третьих, особенности функционирования КССБ, связанные с апериодичностью в работе систем безопасности, являются причиной частого появления ложных сигналов о наступлении инцидентов безопасности.

Основываясь на вышеприведенных позициях, авторами были сформированы основные требования к процедуре формирования критериев:

– критерии должны формироваться регулярно для оценки каждого поступившего на вход модели значения;

– метод формирования критериев должен учитывать предыдущие значения показателя за некоторый предыдущий период с учетом их распределения во времени.

Одним из наиболее подходящих методов, удовлетворяющих поставленным условиям, является использование методов прогнозирования для оценки текущих значений параметров.

Заключение. Использование технологий локальных сетей для агрегирования информации, поступающей из гетерогенных систем, позволило сформировать понятие КССБ – специализированный вид ЛВС, обладающий характерными особенностями функционирования. Учитывая, что основное предназначение КССБ заключается в обеспечении безопасности жизни и здоровья человека, актуальным является вопрос моделирования работы таких систем и мониторинга состояния их систем защиты.

Предложенные авторами имитационная модель и подход к формированию критериев определения текущего состояния системы позволяют учитывать не только риски реализации внешних угроз, но и наступления событий, способных привести к аппаратным сбоям элементов системы. Отличительной особенностью данной имитационной модели является независимость от типа параметра объекта и его физического смысла.

Исходя из сформированных требований к процедуре формирования критериев, можно сделать вывод, что для оценки текущего состояния защищенности систем безопасности необходимо на ос-

нове оценки предыдущих значений исследуемого параметра формировать прогноз и сравнивать его с текущим значением. В [4] авторами был предложен подход к анализу данных мониторинга и формированию критериев оценки с помощью методов прогнозирования.

Литература

1. Мещеряков Р.В. Специальные вопросы информационной безопасности / Р.В. Мещеряков, А.А. Шелупанов. – Томск: Изд-во Института оптики атмосферы СО РАН, 2003. – 224 с.

2. Основы информационной безопасности: учеб. пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

3. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1. – С. 28–35.

4. Исхаков С.Ю. Разработка методического и программного обеспечения для мониторинга работы локальных сетей / С.Ю. Исхаков, А.А. Шелупанов // Телекоммуникации. – 2013. – № 6. – С. 16–21.

5. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 278 с.

6. Зайцев А.П. Технические средства и методы защиты информации: учебник / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2012. – 442 с.

7. Евсютин О.О. Приложения клеточных автоматов в области информационной безопасности и обработки данных / О.О. Евсютин, А.А. Шелупанов // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 119–125.

8. Исхаков С.Ю. Прогнозирование в системе мониторинга локальных сетей / С.Ю. Исхаков, А.А. Шелупанов, С.В. Тимченко // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 100–103.

9. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

10. Кускова А.А. Оценка рисков информационной безопасности телекоммуникационной системы / А.А. Кускова, А.А. Шелупанов, Р.В. Мещеряков, С.С. Ерохин // Информационное противодействие угрозам терроризма. – 2009. – № 13. – С. 90–92.

Исхаков Сергей Юнусович
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: frosty86@mail.ru

Шелупанов Александр Александрович
Д-р техн. наук, профессор, проректор по научной работе ТУСУРа
Тел.: 8 (382-2) 514-302
Эл. почта: saa@tusur.ru

Исхаков Андрей Юнусович
Аспирант каф. КИБЭВС ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: iay@keva.tusur.ru

Iskhakov S.Y., Shelupanov A.A., Iskhakov A.Y.
Engineering of imitation model of a complex network of security systems

Approach to creation of imitating model of information security of complex networks of systems of safety is offered. Characteristics of networks of this type are defined and the difference in approaches to ensuring their protection in comparison with standard local computer networks is shown. The imitating model considering not only external, but also internal threats of violation of information security of system is offered.
Keywords: complex networks of systems of safety, imitating model, safety incident, private model.

УДК 004.056

А.В. Иванов, В.А. Трушин

О модели речевого сигнала при оценке защищенности речевой информации от утечки по техническим каналам

Рассматривается модель речевого сигнала при оценке защищенности речевой информации от утечки по техническим каналам. Обсуждается целесообразность корректировки существующей модели с учетом возможностей как превышения уровня речи над средним уровнем, так и форсирования речи в реальных условиях защиты информации. Приводятся результаты расчетов и артикуляционных испытаний.

Ключевые слова: разборчивость речи, форсированная речь, артикуляционные испытания.

Применяемая в настоящее время методика оценки защищенности речевой информации от утечки по техническим каналам [1], основанная на методе Н.Б. Покровского [2], использует в качестве тестового сигнала (модели речевого сигнала) либо белый шум с огибающей, соответствующей усредненному спектру речи, либо соответствующий набор тональных сигналов со среднегеометрическими частотами октавных полос. При этом интегральный уровень тестового сигнала поддерживается постоянным и составляет 70 дБ, т.е. соответствует среднему уровню речи [3].

В реальных же условиях возможно как превышение уровня речевого сигнала по отношению к среднему [4], так и возникновение эффекта форсирования речи, который влечет за собой не только увеличение уровня сигнала, но и деформацию спектра речи.

Вероятность превышения среднего уровня речи. В исследованиях Н.Б. Покровского [2. С. 152] приводится зависимость (рис. 1) вероятности превышения определенного среднего уровня речевого сигнала от значения этого уровня (В).

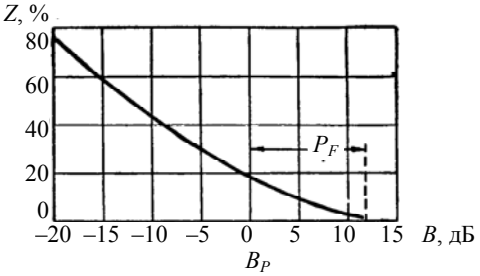


Рис. 1. Усредненная характеристика амплитудного состава речи: B_P – средний уровень речи; P_F – пикфактор русской речи (12 дБ)

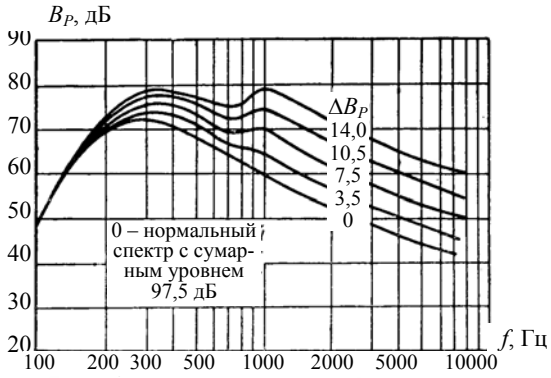
Исходя из данной зависимости, можно сделать вывод, что в 20% случаев уровень речи превышает средний уровень 70 дБ, следовательно, с такой же вероятностью проведенная оценка защищенности речевой информации будет ошибочна. В связи с этим для корректной оценки защищенности в работе [4] предлагается задавать требуемую вероятность непревышения порогового значения W и в соответствии с ней выбирать интегральный уровень тестового сигнала. Например, если заданная вероятность непревышения 95%, то необходимо установить уровень тестового сигнала 80 дБ.

Следует также отметить разницу в средних уровнях речи по Покровскому и используемых в методике [1]. У Покровского все измерения проводились на расстоянии 8 см от источника; в методике - на расстоянии 1 м. Затухание акустического сигнала в речевом диапазоне частот таково, что 93 дБ на 8 см приблизительно соответствуют 70 дБ на 1 м.

Внесение данных изменений в методику оценки защищенности позволит снизить вероятность утечки информации по техническим каналам.

Форсированная речь. В процессе проведения переговоров нередко возникают ситуации, в которых два или более дикторов начинают спорить друг с другом и стараться перекричать оппонента, что эквивалентно повышению уровня шума. Данные условия соответствуют форсированию речи.

Н.Б. Покровский объясняет это тем, что при повышении общего уровня шума говорящий непроизвольно повышает уровень голоса, чтобы слышать собственную речь, осуществляя тем самым самоконтроль. Количественно это явление харак-теризуется не только приращением суммарной интенсивности речи (в зависимости от суммарного уровня шума), но и искажением спектра речи



(перераспределением энергии речи в области высоких частот) (рис. 2) [2. С. 201].

При этом Покровский считает, что поправка на изменение спектра речи является одновременно и поправкой на изменение спектра формант. Эта гипотеза вытекает из рассмотрения физического процесса при форсировании речи и подтверждается практическими данными.

Рис. 2. Частотный спектр форсированной речи при различной степени форсирования (ΔB_p)

В соответствии с таким подходом были построены зависимости словесной разборчивости от соотношения сигнал/шум по классической методике [1] (для максимальной степени форсирования ΔB_p = 14 дБ, рис. 3–5).

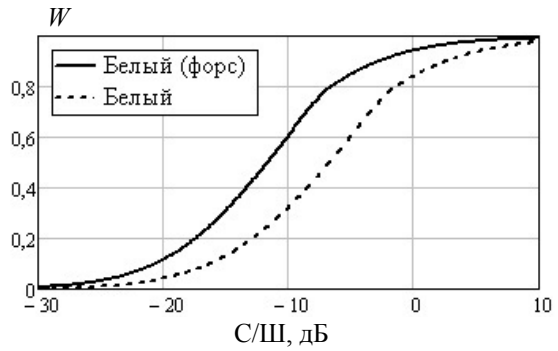


Рис. 3. Зависимость словесной разборчивости от соотношения сигнал/шум для белого шума при использовании стандартного спектра речи и форсированного

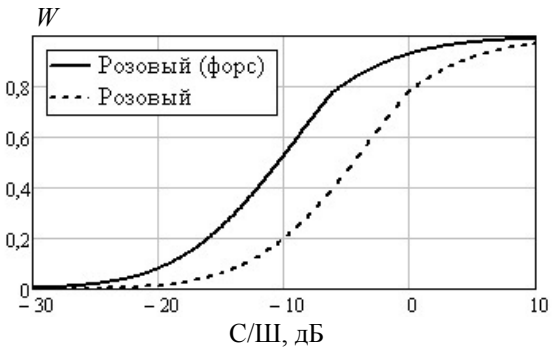


Рис. 4. Зависимость словесной разборчивости от соотношения сигнал/шум для розового шума при использовании стандартного спектра речи и форсированного

Видно, что во всех случаях изменение спектра речевого сигнала приводит к существенному увеличению показателя разборчивости речи.

Для получения достоверных данных о влиянии изменения спектра речевого сигнала в процессе форсирования были проведены соответствующие артикуляционные испытания, аналогичные изложенным в [5].

Полученные результаты для белого, розового и формантоподобного шумов приведены на рис. 6–8 соответственно.

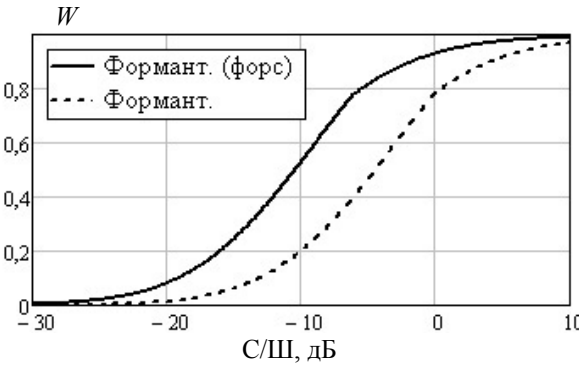


Рис. 5. Зависимость словесной разборчивости от соотношения сигнал/шум для формантоподобного шума при использовании стандартного спектра речи и форсированного

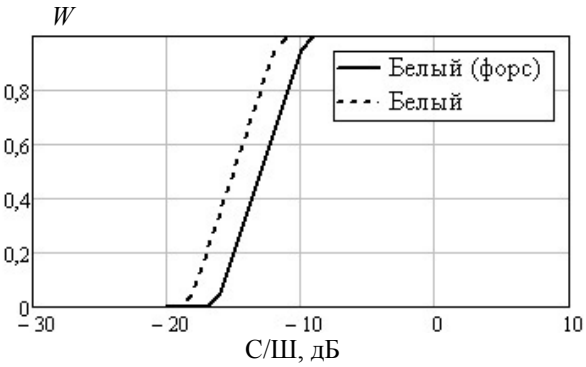


Рис. 6. Зависимость словесной разборчивости от соотношения сигнал/шум для белого шума при использовании стандартного спектра речи и форсированного по результатам артикуляционных испытаний

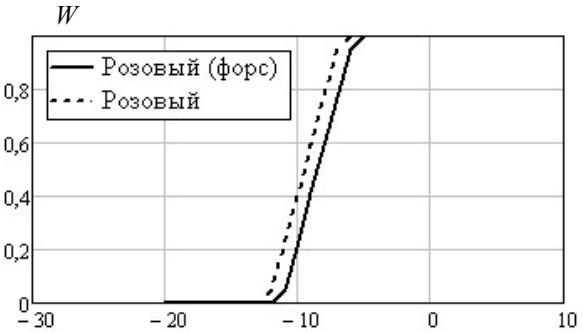


Рис. 7. Зависимость словесной разборчивости от соотношения сигнал/шум для розового шума при использовании стандартного спектра речи и форсированного по результатам артикуляционных испытаний

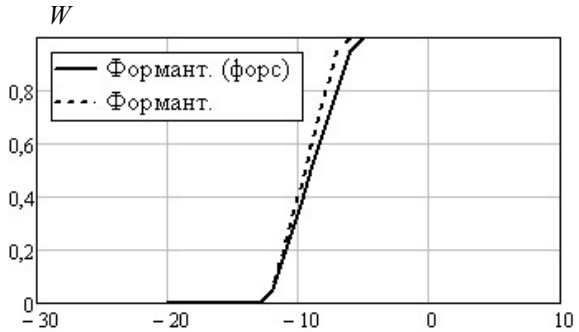


Рис. 8. Зависимость словесной разборчивости от соотношения сигнал/шум для формантоподобного шума при использовании стандартного спектра речи и форсированного по результатам артикуляционных испытаний

Эксперимент показал, что деформация спектра речевого сигнала при форсировании приводит к снижению показателя разборчивости речи, что полностью расходится с теоретическими расчетами.

Полученный результат может быть обоснован изменением функции коэффициента восприятия при увеличении уровня фонового шума (рис. 9) [2. С. 214], что методика [1] не учитывает.

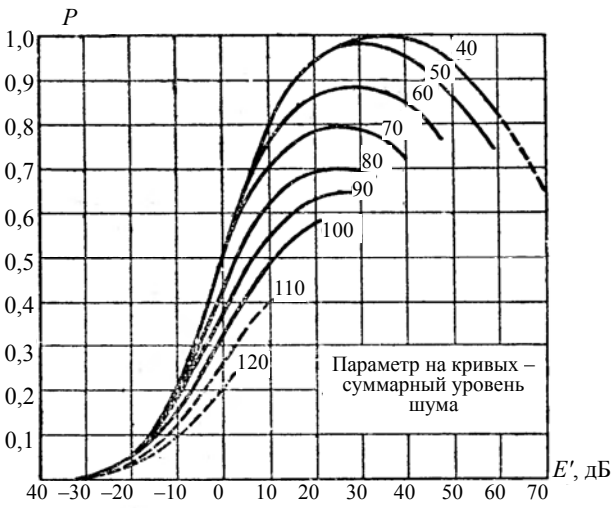


Рис. 9. Зависимость коэффициента восприятия от эффективного уровня ощущения формант при различных уровнях шума.

Также следует отметить, что влияние формантоподобной помехи как на обычную речь, так и на форсированную практически идентично, что позволяет предположить, что в результате форсирования спектр формант не претерпевает существенных изменений либо спектр формант меняется не так, как предполагает Покровский.

Заключение. Необходимо учитывать вероятностную зависимость превышения уровня речи над средним уровнем (70 дБ), в результате чего в 20% случаев уровень речи человека превышает уровень тестового сигнала, используемого при проведении оценки защищенности.

В реальных условиях могут возникать ситуации, при которых возникает форсирование речи. Исследовано влияние данного эффекта на разборчивость речи как со стороны увеличения уровня речи, так и со стороны изменения спектра речевого сигнала. Поставлен эксперимент по определению влияния изменения спектра речевого сигнала при форсировании на разборчивость речи. Оказалось что изменение спектра речевого сигнала оказывает обратный эффект, и разборчивость снижается.

Существующая методика [1] не учитывает данные обстоятельства. В связи с этим необходимо изменение методики с учетом в том числе корректировки кривой коэффициента восприятия для условий форсированной речи.

Литература

1. Железняк В.К. Некоторые методические подходы к оценке эффективности защиты речевой информации / В.К. Железняк, Ю.К. Макаров, А.А. Хорев // Специальная техника. – 2000. – № 4. – С. 39–45.

2. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Связьиздат, 1962. – 390 с.

3. Герасименко В.Г. Методы защиты акустической речевой информации от утечки по техническим каналам / В.Г. Герасименко, Ю.Н. Лаврухин, В.И. Тупота. – М.: РЦИБ «Факел», 2008. – 258 с.

4. Авдеев В.Б. О некоторых направлениях совершенствования методических подходов, применяемых при оценке эффективности технической защиты информации // Специальная техника. – 2013. – № 2. – С. 1–10.

5. О достоверности оценки защищенности речевой информации от утечки по техническим каналам / А.П. Бацула, А.В. Иванов, И.Л. Рева, В.А. Трушин // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 89–92.

Иванов Андрей Валерьевич
Ст. преподаватель каф. защиты информации
Новосибирского государственного технического университета (НГТУ)
Тел.: 8 (383) 346-08-53
Эл. почта: ivanov_av87@mail.ru

Трушин Виктор Александрович
Канд. техн. наук, ст. науч. сотр., зав. каф. защиты информации НГТУ
Тел.: 8 (383) 346-08-53
Эл. почта: rastr89@mail.ru

Ivanov A.V., Trushin V.A.

About model of a speech signal at an assessment of security of speech information by leaking from technical channels

The model of a speech signal is considered at an assessment of security of speech information by leaking from technical channels. Expediency of correction of existing model taking into account opportunities as excess of level of the speech over the average level, and force of speech in actual practice information security is discussed. Results of calculations and articulation tests are given.

Keywords: intelligibility of speech, forced speech, articulation tests.

УДК 004.9

К.В. Курносов, В.В. Селифанов

Разработка требований для оценки безопасности виртуальной инфраструктуры

В соответствии с руководящими и методическими документами в области технической защиты информации была разработана модель инфраструктуры, построенной с применением технологии виртуализации, в которой содержится информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну. Были определены виды потенциальных нарушителей безопасности, выделены актуальные угрозы и выработан набор требований для оценки безопасности таких инфраструктур.

Ключевые слова: виртуализация, виртуальная инфраструктура, виртуальная машина, гипервизор, информационная безопасность, требования информационной безопасности.

Обзор технологии виртуализации. Специфика современного рынка производства и услуг приводит к необходимости обработки огромных информационных потоков в реальном времени с повышенными требованиями к безопасности и надежности. Для продуктивной работы организаций требуется все больше и больше сервисов, предоставляемых как для клиентов, так и для собственных сотрудников. Запуск большого количества разнообразных служб и приложений на одном сервере ведет к увеличению финансовых потерь и иного ущерба, в случае выхода его из строя или реализации других возможных угроз.

Для обеспечения минимизации таких рисков очевидным представляется решение использовать для каждого сервиса отдельно выделенный сервер. Это делается в первую очередь для изоляции приложений друг от друга. Такой подход приводит к быстрому росту самих серверов, локальных сетей и инженерных коммуникаций. Следствием этого непременно становится неконтролируемый рост расходов на содержание информационной инфраструктуры, а также сложности с ее управлением и масштабируемостью.

Виртуализация является одной из ключевых технологий, позволяющих решить большинство этих проблем и перейти от экстенсивного развития инфраструктуры к интенсивному.

В проекте ГОСТа «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» [1. С. 2] под виртуализацией понимают создание программных систем на основе существующих аппаратно-программных комплексов, зависящих или не зависящих от них. Под виртуальной инфраструктурой (ВИ), в том же документе [1. С. 4], подразумевается сформированная совокупность физических компьютеров и серверов, виртуальных ресурсов и компонентов виртуальной платформы (ВП), развернутых на физических серверах, а также каналы связи.

Данная технология несет такие преимущества, как оптимальное использование вычислительных ресурсов, экономия ресурсов материальных, повышение возможностей масштабирования инфраструктуры и увеличение уровня отказоустойчивости.

Конечно, как и все технологии, технология виртуализации не совершенна и обладает своими недостатками. Технологии виртуализации порождают новые специфические угрозы. Примерами таковых могут являться угрозы гипервизору, угрозы образам виртуальной машины (ВМ) и виртуальным сетевым инфраструктурам.

Согласно статистике «Лаборатории Касперского» [2] 59% опрошенных российских компаний с локальными сетями от 100 компьютеров и выше уже внедрили или планируют внедрить виртуализацию серверов.

По данным исследований Cisco Systems, Inc [3], в качестве основных препятствий для использования технологий виртуализации в своих информационных системах (ИС) крупные компании чаще других упоминают вопросы безопасности (23% случаев). Таким образом, можно сделать вывод, что вопросы виртуализации и обеспечения ее безопасности на сегодняшний день довольно актуальны как в России, так и в мире в целом.

Анализ существующих информационных технологий реализующих ВИ показал, что для обеспечения их безопасности необходимо построение систем защиты информации, способных устранять специфичные угрозы, возникающие при использовании технологий виртуализации.

Постановка задачи. Ввиду отсутствия требований для технологий, реализующих ВИ, была поставлена цель по их разработке в соответствии с действующими в этой сфере нормативными и методическими документами. Для достижения поставленной цели необходимо было решить ряд задач. Во-первых, разработать модель ВИ, для которой будет строиться система защиты. Во-вторых, определить потенциальных нарушителей безопасности и выделить актуальные угрозы. В-третьих, проанализировать требования регуляторов, предъявляемые к системам, в которых могут быть использованы технологии виртуализации.

Модель виртуальной инфраструктуры. В случае если среда виртуализации используется для построения ИС, в которых содержится информация ограниченного доступа, то необходимо чтобы средства защиты информации прошли процедуру оценки соответствия. Документы, в которых определены меры по защите среды виртуализации, – проект ГОСТа «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения» [1. С. 14–28] и Приказы ФСТЭК России №17 [6. С. 19] и №21 [7. С. 6].

На основе указанных выше документов, описания архитектуры и выделенных объектов защиты, при использовании технологии виртуализации, существующих в этих документах, была разработана модель ВИ, включающая ее основные компоненты (рис. 1).

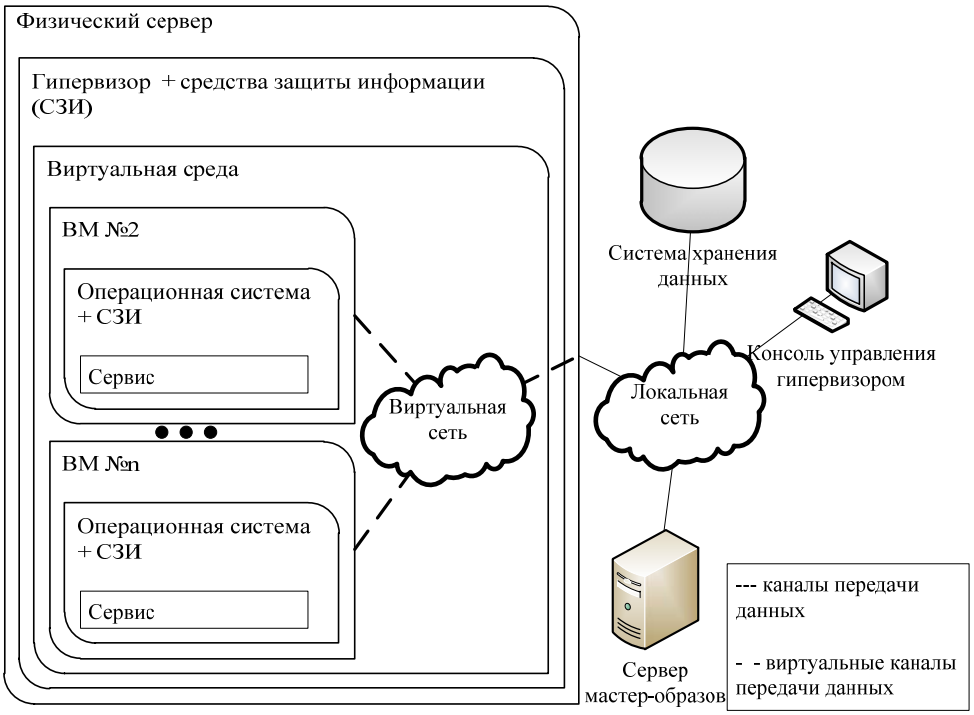


Рис. 1. Модель виртуальной инфраструктуры

Нарушитель и угрозы безопасности виртуальной инфраструктуры. Для определения угроз безопасности информации и разработки модели угроз в рамках данной статьи была разработана модель нарушителя безопасности ВИ.

В соответствии с методиками ФСТЭК России и ФСБ России [4, 5] все нарушители были поделены на внутренних и внешних. Внешние нарушители подразделяются на 2 категории: категория I (лица, не имеющие права доступа в контролируемую зону информационной системы) и категория II (лица, имеющие право постоянного или разового доступа в контролируемую зону информационной системы). К внешним нарушителям I категории относятся: бывшие сотрудники предприятия и посторонние лица, действующие в инициативном порядке. К внешним нарушителям II категории относятся представители преступных организаций. К внутренним нарушителям относятся: сотрудники организации, с разными правами доступа к компонентам системы, персонал, не имеющий легитимного доступа к компонентам системы, и лица из сторонних организаций, имеющие прямой или косвенный доступ к компонентам инфраструктуры.

Для каждого нарушителя были выделены возможные объекты атаки, средства атаки и используемые ими уязвимости. Общий перечень угроз, характерных для ВИ, приведен в проекте ГОСТа «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения»[1. С. 7–13].

Требования для оценки безопасности виртуальной инфраструктуры. Отталкиваясь от данных угроз и модели нарушителя, были разработаны требования безопасности для ВИ, являющихся частью ИС, в которых не ведется обработка сведений, составляющих государственную тайну. В соответствии с Приказом ФСТЭК России №17 [6. С. 6] устанавливаются четыре класса защищенности ИС, в том числе и ИС, реализованных на базе ВИ. Классы защищенности ранжируются по возрастанию требований от четвертого до первого. Ниже представлена таблица, в которой сведены воедино классы защищенности и требования, предъявляемые к ним.

Требования безопасности для ВИ, являющихся частью ИС

№	Требования	Класс защищенности			
		4	3	2	1
Т1	Требования к идентификации и аутентификации субъектов доступа и объектов доступа в ВИ, в том числе администраторов	+	+	++	++
Т2	Требования к управлению доступом субъектов доступа к объектам доступа в ВИ, в том числе внутри ВМ	+	++	++	++
Т3	Требования к регистрации событий безопасности в ВИ	–	+	+	+
Т4	Требования к управлению (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами ВИ, а также по периметру ВИ	–	–	+	++
Т5	Требования к доверенной загрузке серверов виртуализации (гипервизор), ВМ, серверов управления виртуализацией (консоль управления гипервизором)	–	–	–	–
Т6	Требования к управлению перемещением ВМ и обрабатываемых на них данных	–	–	+	++
Т7	Требования к контролю целостности ВИ и ее конфигураций	–	–	+	+
Т8	Требования к резервному копированию данных, резервированию технических средств, программного обеспечения ВИ, а также каналов связи внутри ВИ	–	–	+	++
Т9	Требования к реализации и управлению антивирусной защитой в ВИ	–	+	++	++
Т10	Требования к разбиению ВИ на сегменты (сегментирование ВИ) для обработки информации отдельным пользователем и (или) группой пользователей	–	–	+	++
Т11	Минимальный требуемый класс СВТ при построении ИС	5	5	5	5
Т12	Минимальный требуемый класс СОВ при построении ИС (в случае взаимодействия с сетями международного обмена)	5	5(4)	4	4
Т13	Минимальный требуемый класс МЭ при построении ИС (в случае взаимодействия с сетями международного обмена)	4	4(3)	4(3)	4(3)
Т14	Минимальный требуемый класс антивирусной защиты, при построении. ИС (в случае взаимодействия с сетями международного обмена)	5	5(4)	4	4
Т15	Минимальный требуемый уровень контроля отсутствия НДВ для используемого в ИС программного обеспечения	–	–	4	4

*+ требование предъявляется; ++ предъявляются усиленные требования; – требования не предъявляются.

В данной статье был сделан акцент на разборе требований, предъявляемых к системам защиты информации, разработанным для ВИ, построенных в соответствии с I классом защищенности как наиболее полном.

Т1. Требования к идентификации и аутентификации субъектов доступа и объектов доступа в ВИ, в том числе администраторов.

Идентификация и аутентификация субъектов и объектов доступа должна осуществляться в соответствии с требованиями ИАФ.1, ИАФ.2, ИАФ.3, ИАФ.4, ИАФ.5, ИАФ.6 и ИАФ.7 из методического документа ФСТЭК России «Меры защиты информации в государственных информационных системах» [5. С. 16–24].

В качестве объектов доступа в ВИ необходимо рассматривать программное обеспечение управления ВИ, гипервизор, хостовую операционную систему (для гипервизора 2-го типа), ВМ, виртуализированное программное обеспечение, СЗИ, используемые в рамках ВИ.

При реализации мер по идентификации и аутентификации субъектов доступа и объектов доступа в ВИ должны обеспечиваться:

– идентификация и аутентификация администраторов управления средствами виртуализации;

– идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в ВИ;

– блокировка доступа к компонентам ВИ для субъектов доступа, не прошедших процедуру аутентификации;

– защита аутентификационной информации в процессе ее ввода для аутентификации в ВИ от возможного использования лицами, не имеющими на это полномочий;

– идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления аппаратного обеспечения ВИ.

Внутри развернутых ВМ должна быть также обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с ИАФ.1–ИАФ.7 [5. С. 16–24].

Требования усиления. В ИС должны обеспечиваться взаимная идентификация и аутентификация пользователя и ВМ при удалённом доступе.

Т2. Требования к управлению доступом субъектов доступа к объектам доступа в ВИ, в том числе внутри ВИ.

Эту функцию в части управления доступом к ВИ выполняет гипервизор или СЗИ. Но управление доступа внутри ВМ эти средства выполнить не могут, в этом случае используются классические СЗИ от НСД, устанавливаемые на ВМ.

В ВИ должно обеспечиваться управление доступом субъектов доступа к объектам доступа, в том числе внутри ВМ, в соответствии с УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.11, УПД.12, УПД.13 из [Там же. С. 25–41].

При реализации мер по управлению доступом субъектов доступа к объектам доступа в ВИ должны обеспечиваться:

– контроль доступа субъектов доступа к средствам управления компонентами ВИ;

– контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, ВМ, файлам-образам ВМ;

– управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;

– контроль запуска ВМ на основе заданных оператором правил;

– разграничение доступа субъектов доступа, зарегистрированных на ВМ, к объектам доступа, расположенным внутри ВМ, в соответствии с правилами разграничения доступа пользователей данных ВМ;

– разграничение доступа субъектов доступа, зарегистрированных на ВМ, к ресурсам ВИ, размещенным за пределами ВМ, в соответствии с правилами разграничения доступа.

Требования усиления. В ВИ должен обеспечиваться доступ к операциям, выполняемым с помощью средств управления ВМ, в том числе к операциям создания, запуска, останова, создания копий, удаления ВМ, который должен быть разрешен только администраторам ВИ.

Т3. Требования к регистрации событий безопасности в ВИ.

Должна обеспечиваться регистрация событий безопасности в соответствии с РСБ.1, РСБ.2, РСБ.3, РСБ.4 и РСБ.5 [Там же. С. 62–69].

При реализации мер по регистрации событий безопасности в ВИ дополнительно к событиям, установленным в РСБ.1 [Там же. С. 62], должны подлежать регистрации: запуск и завершение работы компонентов ВИ, доступ субъектов доступа к компонентам ВИ, изменения в составе и конфигурации компонентов ВИ во время их запуска, функционирования и аппаратного отключения.

Для данных событий должны быть зафиксированы: дата и время события, результат события (успешный или неуспешный), идентификатор пользователя, инициировавшего событие.

Т4. Требования к управлению потоками информации между компонентами ВИ, а также по периметру ВИ.

В ИС должно осуществляться управление потоками информации между компонентами ВИ и по периметру ВИ в соответствии с УПД.3, ЗИС.3 [Там же. С. 29–31, 124], при этом должны обеспечиваться:

– фильтрация сетевого трафика между компонентами ВИ, в том числе между внешними и внутренними по отношению к ВМ сетями;

– наличие доверенных маршрутов внутри ВИ между администратором, пользователем и СЗИ (функциями безопасности);

– контроль передачи служебных информационных сообщений по составу и объёму;

– отключение неиспользуемых сетевых протоколов гипервизора, хостовой операционной системы, виртуальной вычислительной сети компонентами ВИ;

– обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри ВИ, в том числе для защиты от подмены сетевых устройств и сервисов;

– обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами ВИ и сетевых потоков виртуальной вычислительной сети;

– семантический и статистический анализ сетевого трафика.

Требования усиления. Должна быть обеспечена единая точка подключения к ВИ. В ИС должна обеспечиваться фильтрация сетевого трафика от (к) каждой гостевой операционной системы, в виртуальных сетях гипервизора и для каждой ВМ.

Т6. Требования к управлению перемещением ВМ и обрабатываемых на них данных.

Оператором должно обеспечиваться управление перемещением ВМ и обрабатываемых на них данных. При этом должны обеспечиваться:

– регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);

– управление размещением и перемещением данных, файлов-образов и исполняемых файлов ВМ.

Управление перемещением ВМ должно предусматривать возможность обеспечить:

– полный запрет перемещения ВМ;

– ограничение перемещения ВМ в пределах информационной системы;

– ограничение перемещения ВМ между сегментами ИС.

Требования усиления. Оператором должна осуществляться обработка отказов перемещения ВМ (контейнеров) и обрабатываемых на них данных.

Т7. Требования к контролю целостности ВИ и ее конфигураций.

В ИС должен обеспечиваться контроль целостности компонентов ВИ в соответствии с ОЦЛ.1 [5. С. 86–88]. При реализации мер по контролю целостности компонентов ВИ должны обеспечиваться:

– контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);

– контроль целостности состава и конфигурации виртуального оборудования;

– контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и ВМ;

– контроль целостности файлов-образов виртуализированного программного обеспечения и ВМ, файлов-образов, используемых для обеспечения работы виртуальных файловых систем;

– контроль целостности резервных копий ВМ.

Т8. Требования к резервному копированию данных, резервированию технических средств, программного обеспечения ВИ, а также каналов связи внутри ВИ.

В ИС должны обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения ВИ и каналов связи внутри ВИ в соответствии с ОДТ.2, ОДТ.4, ОДТ.5 [Там же. С. 96–102]. При реализации этих требований должны обеспечиваться:

– определение мест хранения резервных копий ВМ и данных, обрабатываемых в ВИ;

– резервное копирование ВМ;

– резервное копирование данных, обрабатываемых в ВИ;

– резервирование программного обеспечения ВИ;

– резервирование каналов связи, используемых в ВИ;

– периодическая проверка резервных копий и возможности восстановления ВМ и данных, обрабатываемых в ВИ с использованием резервных копий.

Требования усиления. В ИС должно выполняться резервное копирование конфигурации ВИ, программного обеспечения серверов управления виртуализацией, автоматизированного рабочего

места администратора управления средствами виртуализации, а также дистрибутивов средств построения ВИ.

Т9. Требования к реализации и управлению антивирусной защитой в ВИ.

В ИС должны обеспечиваться реализация и управление антивирусной защитой в ВИ в соответствии с АВЗ.1, АВЗ.2 [Там же. С. 73–74]. При реализации соответствующих мер должны обеспечиваться:

– проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;

– проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

Требования усиления. В информационной системе должно обеспечиваться разграничение доступа к управлению средствами антивирусной защиты.

Т10. Требования к разбиению ВИ на сегменты (сегментирование ВИ) для обработки информации отдельным пользователем и (или) группой пользователей.

В ИС должно обеспечиваться разбиение ВИ на сегменты (сегментирование ВИ) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с ЗИС.17 [Там же. С. 136–137].

Требования усиления. В ИС должно обеспечиваться выделение в отдельный сегмент (отдельные сегменты) серверов управления виртуализацией (автоматизированного рабочего места администратора управления средствами виртуализации).

Заключение. Результатом данной работы стали разработанные модель типовой ВИ, которая может быть использована при создании различных информационных систем, модель нарушителя и модель угроз и непосредственный перечень требований к системам защиты информации для таких информационных систем.

Таким образом, на основании проанализированных документов, проектов документов и приведенных в данной статье наработок можно построить информационную систему, с использованием технологий виртуализации, отвечающую требованиям основных регуляторов в сфере информационной безопасности на территории Российской Федерации.

Литература

1. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения [проект ГОСТ: разраб. ФСТЭК России]. – [Окончательная редакция]. – М., 2014. – 39 с.

2. Ледовской В.П. Виртуальным инфраструктурам – прогрессивная защита [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/analytics/Progressive_Defense_for_Virtual_Infrastructures, свободный (дата обращения: 28.04.2014).

3. Securing Virtual Applications and Servers [Электронный ресурс]. – Режим доступа: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-network-services-uns/white_paper_c11-652663.html, свободный (дата обращения: 28.04.2014).

4. Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в специальных информационных системах персональных данных отрасли: методический документ Министерства связи и массовых коммуникаций Российской Федерации: одобр. решением секции №1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» 21.04.2010. – 1-е изд. – М., 2010. – 50 с.

5. Меры защиты информации в государственных информационных системах: методический документ ФСТЭК России: утв. ФСТЭК России 11.03.2014. – М., 2014. – 176 с.

6. Российская Федерация. Приказы. Об утверждении требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России №17: издан ФСТЭК России 11.03.2013. – 1-е изд. – М., 2013. – 37 с.

7. Российская Федерация. Приказы. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России № 21: издан ФСТЭК России 18.03.2013. – 1-е изд. – М., 2013. – 20 с.

Курносов Кирилл Викторович
Студент каф. информационной безопасности НГУЭУ
Тел.: 8 (913) 753-21-81
Эл. почта: kursorkvk@mail.ru

Селифанов Валентин Валерьевич
Ст. преподаватель каф. информационной безопасности
Новосибирского государственного университета экономики и управления, начальник 6-го отдела
Управления ФСТЭК России по Сибирскому федеральному округу
Тел.: 8 (383) 264-04-84
Эл. почта: sfo1@mail.ru

Kurnosov K.V., Selifanov V.V.
Development of requirements for safety assessment virtual infrastructure

In accordance with the guiding and methodological documents in the field of technical protection of information, a model was developed infrastructure, built with the use of virtualization technologies, which contains information of restricted access, not containing information constituting state secrets. Were defined the types of potential offenders security, the urgent threats, and develop a set of requirements for safety assessment of such infrastructure.
Keywords: virtualization, virtual infrastructure, virtual machine, hypervisor, information security, requirements for information security.

УДК 621.391

А.Б. Лось

Исследование информационных характеристик преобразований замены и перестановки

Излагаются результаты исследования информационных характеристик преобразований замены и перестановки, являющихся основой построения криптографических алгоритмов. Получены оценки взаимной информации входных и выходных сообщений дискретного канала связи при применении указанных преобразований.

Ключевые слова: канал связи, взаимная информация, преобразование замены и перестановки.

В настоящей статье излагаются результаты исследования информационных характеристик преобразований замены и перестановки, являющихся основой построения криптографических алгоритмов [1−2]. Для указанных преобразований найдены верхние оценки взаимной информации входных и выходных сообщений дискретного канала связи. Полученные результаты позволяют оценивать эффективность данных преобразований в различных криптографических ситуациях.

Пусть знаки a_i входного сообщения $S_n \in \sigma(n)$ длины N: $\overline{a}_N = (a_1,...,a_N)$ дискретного канала связи, выбираются из алфавита $A = \{1,2,...,n\}$, $a_i \in A$, $i = 1,2,...,N$, а знаки b_i выходного сообщения $\overline{b}_N$, $\overline{b}_N = (b_1,...,b_N)$ образуются из знаков сообщения $\overline{a}_N$ путем применения преобразований замены и перестановки, выражаемых уравнениями:

$$b_i = a_i S, \tag{1}$$

$$b_i = a_{s(i)}, \quad i = 1,2,...,N, \tag{2}$$

где S_n − некоторая подстановка степени n, выбираемая из множества $\sigma(n)$ − всех подстановок степени n; а $S_N = \begin{pmatrix} 1, ..., N \\ s(1),...,s(N) \end{pmatrix}$ − некоторая подстановка степени N, выбираемая из множества $\sigma(N)$ всех подстановок степени N.

Обозначим через $M^N = \{\overline{a}_N\}$ и $E^N = \{\overline{b}_N\}$ множества входных и выходных сообщений длины N соответственно.

Зададим на множестве входных сообщений M^N и множествах подстановок $\sigma(n)$ и $\sigma(N)$ некоторые вероятностные распределения:

$$p(M^N) = \{p(\overline{a}_N), \overline{a}_N \in M^N\},$$
$$p(\sigma(n)) = \{p(S_n), S_n \in \sigma(n)\},$$
$$p(\sigma(N)) = \{p(S_N), S_N \in \sigma(N)\}.$$

Нетрудно видеть, что при этом в том и другом случае будут индуцироваться некоторые вероятностные распределения на множестве выходных сообщений E^N.

Назовем далее $H(A)$ − энтропию вероятностной схемы (ансамбля) A; $H(A/B)$ − условную энтропию ансамбля A при заданном ансамбле B, а $I(A,B)$ − взаимную информацию ансамблей A и B.

Пользуясь известными свойствами энтропии [3−4], получаем

$$H(M^N) + H(E^N/M^N) = H(E^N) + H(M^N/E^N),$$

откуда следует равенства:

$$H(M^N/E^N) = H(M^N) - H(E^N) + H(E^N/M^N), \tag{3}$$

$$I(A,B) = H(M^N) - H(M^N/E^N) = H(E^N) - H(E^N/M^N), \tag{4}$$

где

$$H(M^N) = -\sum_{\overline{a}_N \in M^N} p(\overline{a}_N) \cdot \log p(\overline{a}_N), \tag{5}$$

$$H(E^N)=-\sum_{\bar{b}_N\in M^N} p(\bar{b}_N)\cdot\log p(\bar{b}_N)\,, \tag{6}$$

а логарифм берется по основанию 2.

Рассмотрим вначале задачу оценки взаимной информации для преобразования замены.

В соответствии с определением условной энтропии получаем:

$$H(E^N/M^N)=-\sum_{\bar{a}_N\in M^N}\sum_{\bar{b}\in M^N} p(\bar{a}_N)\cdot p(\bar{b}_N/\bar{a}_N)\cdot\log p(\bar{b}_N/\bar{a}_N)\,, \tag{7}$$

где

$$p(\bar{b}_N)=\sum_{\bar{a}_N\in M^N} p(\bar{a}_N)\cdot p(\bar{b}_N/\bar{a}_N)\,, \tag{8}$$

$$p(\bar{b}_N/\bar{a}_N)=\sum_{S_n\in\sigma(n)} p(S_N)\cdot I\{b_i=a_iS_N,\ i=\overline{1,N}\}\,,$$

$I(R)$ – индикатор условия R.

Дальнейшие расчеты будем проводить в предположении, что рассматриваемый канал связи есть дискретный канал без памяти, при этом, очевидно,

$$p(\bar{a}_N)=p(a_1)\cdot\ldots\cdot p(a_N)\,,$$

а также в предположении, что подстановка S_n выбирается случайно и равновероятно из множества $\sigma(n)$ – всех подстановок степени n.

В этом случае:

$$p(\bar{b}_N/\bar{a}_N,S_n)=\sum_{S_n\in\sigma(n)} p(S_n)p(\bar{b}_N/\bar{a}_N,S_n)=\frac{1}{n!}\sum_{S_n\in\sigma(n)} p(\bar{b}_N/\bar{a}_N,S_n),$$

где $p(\bar{b}_N/\bar{a}_N,S_n)=1$, если $b_i=a_iS_n$, $i=1,2,\ldots,N$ и 0 – в противном случае.

Последнее соотношение можно переписать в виде условий:

$$p(\bar{b}_N/\bar{a}_N,S_n)=\frac{[n-\upsilon(b_1,\ldots,b_N)]!}{n!}, \tag{9}$$

если существует такая подстановка $S_n\in\sigma(n)$, что $b_i=a_iS_n$, $i=1,\ldots,N$; $p(\bar{b}_N/\bar{a}_N,S_n)=0$ в противном случае, где $\upsilon=\upsilon(b_1,\ldots,b_N)$ – число различных элементов в последовательности $(b_1,\ldots,b_N)$.

Пусть далее $(\alpha(1),\ldots,\alpha(n))$ – первичная спецификация последовательности $(b_1,\ldots,b_N)$, а именно: $\alpha(r)$ – число элементов последовательности $(b_1,\ldots,b_N)$, равных r, $r=1,\ldots,n$.

Тогда из (9) получаем:

$$p(\overline{\bar{b}_N})=\frac{[n-\upsilon(b_1,\ldots,b_N)]!}{n!}\sum_{\substack{r_1,\ldots,r_\upsilon=1\\ r_i\neq r_j,\,i\neq j}}^{n}\prod_{\ell=1}^{\upsilon}[p(r_l)]^{\alpha(r_l)}, \tag{10}$$

где $\alpha(r_k)>0$, $k=1,2,\ldots,\upsilon$, т.е. $\alpha(r_k)$ – элементы последовательности первичной спецификации, отличные от 0.

Подставляя (10) в (6) и (7), получаем

$$H(E^N/M^N)=-\sum_{\substack{l_1,\ldots,l_n=0\\ l_1+\ldots+l_n=N}}^{N}\frac{N!}{l_1!\ldots l_n!}p(1)^{l_1}\ldots p(n)^{l_n}\times\sum_{\substack{k(1),\ldots,k(\mu(l_1,\ldots,l_n))=1\\ k(i)\neq k(j),\,i\neq j}}^{n}\frac{[n-\mu(l_1,\ldots,l_n)]!}{n!}\cdot\log\frac{[n-\mu(l_1,\ldots,l_n)]!}{n!}. \tag{11}$$

$$H(E^N)=-\sum_{\substack{l_1,\ldots,l_n=0\\ l_1+\ldots+l_n=N}}^{N}\frac{N!}{l_1!\ldots l_n!}\frac{(n-\mu(l_1,\ldots,l_n))!}{n!}\sum_{\substack{r(1),\ldots,r(\mu)=1\\ r(i)\neq r(j)}}^{n}\prod_{k=1}^{\mu(l_1,\ldots,l_n)}[p(r(k))]^{l(r(k))}\times$$

$$\times\log_2\frac{(n-\mu(l_1,\ldots,l_n))!}{n!}\sum_{\substack{r(1),\ldots,r(\mu)=1\\ r(i)\neq r(j)}}^{n}\prod_{k=1}^{\mu(l_1,\ldots,l_n)}[p(r(k))]^{l(r(k))}, \tag{12}$$

где $\mu=\mu(l_1,\ldots,l_n)$ – число ненулевых элементов в последовательности $(l_1,\ldots l_n)$, $(l(r(1),\ldots,l(r(\mu))-$ последовательность самих ненулевых элементов.

Подставляя (11) и (12) в равенство (4), получаем выражение для взаимной информации входных и выходных сообщений рассматриваемого канала связи $I(M^N,E^N)$, явный вид которого, в силу громоздкости выражений, приведем для случая $p(a_i)=1/n,\ i=1,...,n$:

$$I(M^N,E^N)=N\log n-n^{-N}\cdot\sum_{\substack{l_1,...,l_n=0\\ l_1+...+l_n=N}}^{N}\frac{N!}{l_1!...l_n!}\log\frac{n!}{(n-\mu(l_1,...,l_n))!}. \tag{13}$$

В силу очевидных неравенств

$$H(M^N/E^N)>n^{-N}\cdot\begin{pmatrix}n\\N\end{pmatrix}N!\cdot\log\frac{n!}{(n-N)!},$$

$$-x>\ln(1-x)>\frac{x}{x-1},\quad 0<x<1,$$

из соотношения (12), в условиях $n>N$, получаем оценку для $I(M^N,E^N)$ – величины взаимной информации входных и выходных сообщений при применении преобразования простой замены:

$$\frac{1}{N}I(M^N,E^N)\le\frac{N^2}{n-N}\left[1+\log n\right]. \tag{14}$$

Рассмотрим теперь преобразование перестановки.

Заметим, что в соответствии с введенными выше предположениями, вероятность появления входного сообщения $\bar{a}_n=(a_1,...,a_n)$, где $a_i\in A=\{1,...,n\}$, равна

$$p(\bar{a}_N)=p(a_1)\cdot...\cdot p(a_N)=p_1{}^{r_1}...p_n{}^{r_n}, \tag{15}$$

где p_k – вероятность появления знака входного сообщения равного k, а вектор частот $\bar{r}=(r_1,...,r_n)$ – первичная спецификация последовательности $\bar{a}_N$, $r_к$ – число исходов, равных k. Будем также предполагать, что подстановка S_N выбирается случайно и равновероятно из множества $\sigma(N)$ – всех подстановок степени N.

Нетрудно видеть, что все множество входных сообщений M^N можно представить в виде объединения непересекающихся множеств $M^N(\bar{r})$, соответствующих первичным спецификациям векторов $\bar{r}$:

$$M^N=\underset{\bar{r}}{U}M^N(\bar{r}).$$

Аналогичным образом можно представить и множество выходных сообщений E^N:

$$E^N=\underset{\bar{r}}{U}E^N(\bar{r}).$$

Далее заметим, что условная вероятность $p(\bar{b}_N/\bar{a}_N)$ появления выходного сообщения $\bar{b}_N$ при заданном входном сообщении $\bar{a}_N\in M^N(\bar{r})$ имеет вид

$$p(\bar{b}_N/\bar{a}_N)=\frac{r_1!...r_n!}{N!},\ \text{если}\ \bar{b}_N\in E^N(\bar{r}),$$

$$p(\bar{b}_N/\bar{a}_N)=0,\ \text{если}\quad \bar{b}_N\notin E^N(\bar{r}). \tag{16}$$

Следовательно, при $\bar{b}_N\in E^N(\bar{r})$

$$p(\bar{b}_N)=\sum_{\bar{a}_N\in M^N}p(\bar{a}_N)\,p(\bar{b}_N/\bar{a}_N)=\sum_{\bar{a}_N\in M^N(\bar{r})}p_1{}^{r_1}...p_n{}^{r_n}\frac{r_1!...r_n!}{N!}=p_1{}^{r_1}...p_n{}^{r_n}. \tag{17}$$

Для энтропии $H(E^N)$ ансамбля выходных сообщений имеем

$$H(E^N)=-\sum_{\bar{b}_N\in E^N}p(\bar{b}_N)\log p(\bar{b}_N)=-\sum_{\substack{\bar{r}=(r_1,...,r_n)\\ r_1+...+r_n=N}}\ \sum_{\bar{b}_N\in E^N(\bar{r})}p_1{}^{r_1}...p_n{}^{r_n}\log(p_1{}^{r_1}...p_n{}^{r_n})=$$

$$=-\sum_{\substack{\bar{r}=(r_1...r_n)\\ r_1+...+r_n=N}}\frac{N!}{r_1!...r_n!}p_1{}^{r_1}...p_n{}^{r_n}\log[p_1{}^{r_1}...p_n{}^{r_n}]. \tag{18}$$

В соответствии с определением условной энтропии имеет место равенство

$$H(E^N/M^N)=-\sum_{\bar{a}_N\in M^N}p(\bar{a}_N)\sum_{\bar{b}_N\in E^N}p(\bar{b}_N/\bar{a}_N)\log p(\bar{b}_N/\bar{a}_N)=$$

$$=-\sum_{\substack{\bar{r}=(r_1,\dots r_n)\\ r_1+\dots r_n=N}}\sum_{\substack{\bar{a}_N\in M^N(\bar{r})\\ \bar{b}_N\in E^N(\bar{r})}}p_1^{r_1}\dots p_n^{r_n}\frac{r_1!\dots r_n!}{N!}\log\left(\frac{r_1!\dots r_n!}{N!}\right)=\sum_{\substack{\bar{r}=(r_1,\dots,r_n)\\ r_1+\dots+r_n=N}}p_1^{r_1}\dots p_n^{r_n}\frac{N!}{r_1!\dots r_n!}\log\left(\frac{N!}{r_1!\dots r_n!}\right). \tag{19}$$

С учетом (4), (18) и (19) получаем

$$H(E^N/M^N)-H(E^N)=\sum_{\substack{\bar{r}=(r_1,\dots r_n)\\ r_1+\dots r_n=N}}\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}\left[\log\left(\frac{N!}{r_1!\dots r_n!}\right)+\log(p_1^{r_1}\dots p_n^{r_n})\right]=$$

$$=\sum_{\substack{\bar{r}=(r_1,\dots r_n)\\ r_1+\dots r_n=N}}\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}\log\left[\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}\right]. \tag{20}$$

С учетом (20) из соотношения (4) получаем

$$I(M^N,E^N)=H_N(p_1,\dots p_n), \tag{21}$$

где

$$H_N(p_1,\dots,p_n)=-\sum_{\substack{\bar{r}=(r_1,\dots r_n)\\ r_1+\dots r_n=N}}\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}\log\left[\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}\right] \tag{22}$$

есть энтропия полиномиального распределения.

Далее в работе исследуется асимптотическое поведение величины $H_N(p_1,\dots,p_n)$ при $N\to\infty$ и $n/N\to 0$.

Рассмотрим полиноминальную схему с числом испытаний $N\to\infty$ и вектором вероятностей $P=(P_1,\dots,P_n)$, где P_k – вероятность появления исхода, равного k, $k=1,\dots,n$.

Обозначим через ξ_k случайную величину, равную числу исходов в данной полиноминальной схеме, равных k, $k=1,\dots,n$.

Тогда, очевидно,

$$P(\xi_k=k)=P_k,\ \ E\xi_k=NP_k,\ D\xi_k=NP_k(1-P_k),\ \ k=1,\dots,n,$$

$$P(\xi_1=r_1,\dots,\xi_n=r_n)=\frac{N!}{r_1!\dots r_n!}p_1^{r_1}\dots p_n^{r_n}. \tag{23}$$

Учитывая соотношение (23), величину $H_N(P_1,\dots,P_n)$ можно представить в виде

$$H_N(P_1,\dots,P_n)=-\log N!+\sum_{k=1}^{n}E\log(\xi_k!)-\sum_{k=1}^{n}E\xi_k\log P_k. \tag{24}$$

Нетрудно видеть, что

$$\sum_{k=1}^{n}E\xi_k\log P_k=N\cdot H_p, \tag{25}$$

где $H_p=\sum_{k=1}^{n}P_k\log P_k$.

Для оценки первого слагаемого в (24) используем формулу Стирлинга ([5]):

$$x!=\sqrt{2\pi}x^{x+1/2}e^{-x+\theta/12x}, \tag{26}$$

где $x>0$, $0<\theta<1$.

Тогда

$$\log N!=N\log N+\frac{1}{2}\log N-N\log e+\log\sqrt{2\pi}+\frac{\theta}{12N}\log e, \tag{27}$$

где $\frac{\theta}{12N}\log e=O\left(\frac{1}{N}\right)=o(1)$.

Оценим сумму $\sum_{k=1}^{n} E\log\xi_k!$ Применяя формулу (26), получаем

$$E\log\xi_k! = \sum_{S=0}^{N} \log S! C_N^S P_K^S (1-P_K)^{N-S} = \sum_{S=0}^{N} S\log S \cdot C_N^S P_K^S (1-P_K)^{N-S} + \frac{1}{2}\sum_{S=1}^{N} \log S \cdot C_N^S P_K^S (1-P_K)^{N-S} -$$

$$-\log e \sum_{S=0}^{N} S\, C_N^S P_K^S (1-P_K)^{N-S} + \log\sqrt{2\pi} + \frac{\theta \log e}{12}\sum_{S=1}^{N} \frac{1}{S} C_N^S P_K^S (1-P_K)^{N-S} . \quad (28)$$

Для первой суммы в (28) имеем:

$$\sum_{S=0}^{N} S\log S \cdot C_N^S P_K^S (1-P_K)^{N-S} = NB_N(P_K) + NP_K \log N , \quad (29)$$

где $B_{N(}P_K) = \sum_{S=0}^{N} \frac{S}{N} \log \frac{S}{N} C_N^S P_K^S (1-P_K)^{N-S}$.

Заметим, что функция $U(x) = x \cdot \log x$ непрерывна на отрезке [0,1] и имеет конечную производную 2-го порядка в точке $x = P_k > 0$.

Тогда, применяя теорему о порядке приближения с помощью полиномов Бернштейна [6], получаем

$$B_N(P_k) = U(P_k) + \frac{U''(x)|x=P_k}{2N} P_k(1-P_k) + \frac{\rho_N(k)}{N},$$

где $\rho_N(k) \to 0$ при $N \to \infty$ равномерно по $k = 1,...,n$.

Отсюда, определив $U''(x)|x=P_k$, получаем

$$\sum_{S=0}^{N} S\log S \cdot C_N^S P_K^S (1-P_K)^{N-S} = NP_K \log NP_K + \frac{(1-P_K)\log e}{2} + \rho_N(K) , \quad (30)$$

где $\rho_N(k) \to 0$ при $N \to \infty$.

Далее с учетом (24) получаем

$$\sum_{K=1}^{n}\sum_{S=0}^{N} S\log S \cdot C_N^S P_K{}^S (1-P_K)^{N-S} = N\log N - NH_P + (\frac{n-1}{2})\log e + \rho'_N(K) , \quad (31)$$

где $\rho'_N(K) = \sum_{K=1}^{n} \rho_N(K) \le n \max_K \rho_N(K) \to 0$ при $N \to \infty$.

Вторую и четвертую сумму в правой части (28) оценим с помощью неравенства Чебышева [7], положив $\varepsilon = N^{\frac{2}{3}} P_K^{\frac{1}{2}}$ и разбив область суммирования по S на 2 части:

$$(S - NP_K) \ge N^{\frac{2}{3}} P_K^{\frac{1}{2}} \quad \text{и} \quad (S - NP_K) < N^{\frac{2}{3}} P_K^{\frac{1}{2}} .$$

Для второй суммы в правой части (28) имеем

$$\sum_{S=1}^{N} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} = \sum_{|S-NP_K| \ge N^{\frac{2}{3}} P_K^{\frac{1}{2}}} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} + \sum_{|S-NP_K| < N^{\frac{2}{3}} P_K^{\frac{1}{2}}} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} . \quad (32)$$

Для первой суммы в (32) с учетом (23) имеем

$$\sum_{|S-NP_K| \ge N^{\frac{2}{3}} P_K^{\frac{1}{2}}} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} \le (\log N) P\{|\xi_K - NP_K| \ge N^{\frac{2}{3}} P_K^{\frac{1}{2}}\} \le N^{-1/3}(1-P_K)\log N = O(N^{-1/3}\log N) \to 0. \quad (33)$$

при $N \to \infty$.

Для второй суммы в (32) справедливы неравенства:

$$\log(NP_K - N^{\frac{2}{3}}P_K^{\frac{1}{2}})(1-\frac{1-P_K}{N^{\frac{1}{3}}}) \le \sum_{|S-NP_K|<N^{\frac{2}{3}}P_K^{\frac{1}{2}}} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} \le \log(NP_K + N^{\frac{2}{3}}P_K^{\frac{1}{2}}),$$

или при $N \to \infty$:

$$\log NP_K - o(1) \le \sum_{|S-NP_K|<N^{\frac{2}{3}}P_K^{\frac{1}{2}}} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} \le \log NP_K + o(1). \quad (34)$$

На основании (33) и (34) имеем асимптотическое равенство

$$\sum_{S=0}^{N} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} = \log NP_K + o(1). \quad (35)$$

Отсюда при условии $N \to \infty$ получаем

$$\frac{1}{2}\sum_{K=1}^{n}\sum_{S=0}^{N} (\log S) C_N^S P_K{}^S (1-P_K)^{N-S} = \frac{n}{2}\log N + \frac{1}{2}\sum_{K=1}^{n} \log P_K + o(1). \quad (36)$$

Вычислим четвертую сумму в правой части (28):

$$\sum_{S=1}^{N} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} = \sum_{|S-NP_K|\ge N^{\frac{2}{3}}P_K^{\frac{1}{2}}} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} + \sum_{|S-NP_K|<N^{\frac{2}{3}}P_K^{\frac{1}{2}}} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S}, \quad (37)$$

откуда при условии $N \to \infty$ получаем

$$\sum_{|S-NP_K|\ge N^{\frac{2}{3}}P_K^{\frac{1}{2}}} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} \le P\{|\xi_K - NP_K| \ge N^{\frac{2}{3}}P_K^{\frac{1}{2}}\} \le \frac{(1-P_K)}{N^{\frac{1}{3}}} = O(N^{-1/3}) \to 0$$

при условии $N \to \infty$, а для второй суммы в (37) имеет место неравенство

$$(NP_K + N^{\frac{2}{3}}P_K^{\frac{1}{2}})^{-1}(1-\frac{(1-P_K)}{N^{\frac{1}{3}}}) \le \sum_{|S-NP_K|<N^{\frac{2}{3}}P_K^{\frac{1}{2}}} \frac{1}{S} C_N^K P_K{}^S (1-P_K)^{N-S} \le (NP_K - N^{\frac{2}{3}}P_K^{\frac{1}{2}})^{-1},$$

откуда следует, что

$$\sum_{|S-NP_K|<N^{\frac{2}{3}}P_K^{\frac{1}{2}}} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} = O(N^{-1}). \quad (38)$$

Из (37)–(38) следует, что при $N \to \infty$

$$\frac{\theta \log e}{12}\sum_{S=1}^{N} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} = O(N^{-1}),$$

откуда

$$\frac{\theta \log e}{12}\sum_{K=1}^{n}\sum_{S=0}^{N} \frac{1}{S} C_N^S P_K{}^S (1-P_K)^{N-S} = o(1). \quad (39)$$

Третья сумма в правой части (28) равна:

$$(\log e)\sum_{S=0}^{N} S C_N^S P_K{}^S (1-P_K)^{N-S} = NP_K \log e,$$

откуда,

$$\log e \sum_{K=1}^{n}\sum_{S=0}^{N} S C_N^S P_K{}^S (1-P_K)^{N-S} = N \log e. \quad (40)$$

С учетом (28), (31), (36)−(40) получаем асимптотическое выражение для суммы $\sum_{K=1}^{n} E\log\xi_K!$ при условии $P_k = \text{const}$, $k = 1, \ldots, n$:

$$\sum_{K=1}^{n} E\log\xi_K ! = N\log N - N(H_P + \log e) + \frac{n}{2}\log N + \frac{1}{2}\sum_{K=1}^{n}\log P_K + n\log\sqrt{2\pi} + + \frac{n-1}{2}\log e + o(1). \quad (41)$$

Из (25), (27) и (41) получаем асимптотическое выражение для энтропии полиноминальной схемы $H_N(p_1,...,p_n)$:

$$H_N(p_1,...,p_n) = \frac{n-1}{2}\log N + \frac{1}{2}\sum_{K=1}^{n}\log P_K + \frac{n-1}{2}\log 2\pi e + o(1). \quad (42)$$

Окончательно для взаимной информации $I(M^N, E^N)$ получаем асимптотическое равенство:

$$I(M^N, E^N) = \frac{n-1}{2}\log_2 N - \frac{1}{2}\sum_{k=1}^{n}\log_2 P_k - \frac{n-1}{2}\log_2 2\pi e + o(1), \quad (43)$$

справедливое при условии $N \to \infty$, n=const, $P_k = \text{const}$, k=1,…, n.

Выражения (14) и (43) позволяют оценить значения параметров, в частности длину выходного сообщения N, при котором обеспечиваются важные криптографические качества рассматриваемых преобразований.

Литература

1. Алферов А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. − М.: Гелиос АРВ, 2001. − 479 с.

2. Бабаш А.В. Криптография / А.В. Бабаш, Г.П. Шанкин.− М.: СОЛОН-ПРЕСС, 2007. − 512 с.

3. Колесник В.Д. Курс теории информации / В.Д. Колесник, Г.Ш. Полтырев. − М.: Наука, 1982. − 416 с.

4. Духин А.А. Теория информации. − М.: Гелиос АРВ, 2009. − 248 с.

5. Сачков В.Н. Комбинаторные методы дискретной математики. − М.: Наука, 1966. − 384 с.

6. Березин И.С. Методы вычислений / И.С. Березин, Н.П. Жидков. − 3-е изд. − М.: Наука, 1966. − Т. 1. − 632 с.

7. Боровков А.А. Теория вероятностей. − 2-е изд. − М.: Наука, 1986. − 656 с.

Лось Алексей Борисович
Канд. техн. наук, доцент каф. компьютерной безопасности
Московского института электроники и математики
Национального исследовательского университета «Высшая школа экономики»
Тел.: 8-910-477-88-27
Эл. почта: alos@hse.ru

Los A.B.

The study of information characteristics transformations substitution and permutation

In the paper the results of the research information characteristics of conversion substitution and permutation, which is the basis for building cryptographic algorithms. The obtained value of the mutual information of the input and output messages of discrete communication channel in the application of these reforms.
Keywords: channel, mutual information, conversion substitution and permutation.

УДК 617.721 + 004.93

Н.Н. Минакова, И.В. Петров

Информационная система идентификации личности по слабо различимым текстурам радужной оболочки глаза в видимом диапазоне излучения

Предложен метод улучшения распознавания радужной оболочки глаза по снимкам в видимом диапазоне, основанный на выделении красной цветовой компоненты. Показана эффективность данного подхода на тестовой базе данных снимков.

Ключевые слова: идентификация личности, биометрия, радужная оболочка глаза.

В системах защиты информации для контроля доступа все чаще используются биометрические признаки, в том числе радужная оболочка глаза (РОГ). Значительный интерес представляет использование изображений радужной оболочки глаза, полученных в видимом диапазоне излучения. Одна из проблем, которая во многом препятствует использованию для идентификации снимков глаз в видимом диапазоне, – слабо различимая текстура РОГ у людей с темными глазами.

Была поставлена задача разработки и апробации подхода, позволяющего улучшить распознавание слабо различимых текстур радужной оболочки глаза.

Радужная оболочка глаза, как известно, обладает многослойной структурой. В ее передних слоях содержится меланин – темный пигмент, который определяется цвет радужной оболочки. Карие и черные глаза имеют высокую концентрацию меланина в передних слоях радужной оболочки глаза. Меланин характеризуется высокой степенью поглощения света в видимом диапазоне [1].

Анализ спектра поглощения меланина (рис. 1) позволил сделать вывод о том, что наименьшая степень поглощения меланина имеет место в красном спектральном диапазоне. Тогда можно предположить, что для улучшения качества распознавания текстуры целесообразно выделять из цветного изображения красный цветовой канал, который приближенно отвечает за красную спектральную компоненту получаемого при съемке изображения.

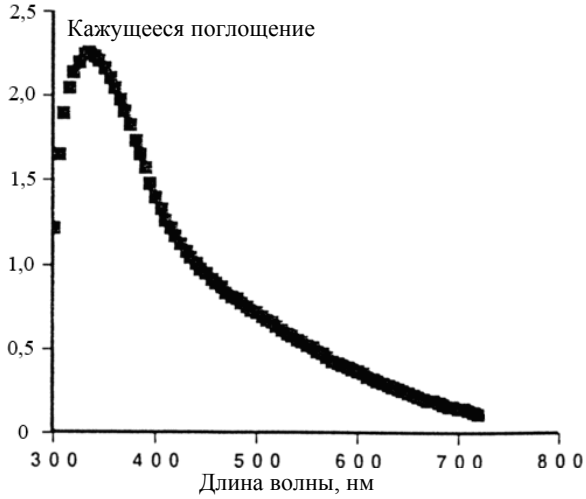


Рис. 1. Спектр поглощения меланина [1]

Для проверки правильности этой гипотезы был проведен численный эксперимент. Использована разработанная ранее информационная система, позволяющая сравнивать различные методы и алгоритмы распознавания радужной оболочки глаза [2].

Изображения из базы данных снимков в видимом диапазоне были разложены на три цветовые компоненты. Из изображений каждого цветового канала с использованием фильтра Габора выделялся вектор признаков. Построены внутриклассовые и внеклассовые распределения расстояний между векторами. По данным распределения вычислялись и сравнивались коэффициенты разделимости, которые выступали в качестве критерия эффективности распознавания [3]:

$$d' = \frac{|\mu_1 - \mu_2|}{\sqrt{\left(\sigma_1^2 + \sigma_2^2\right)/2}}, \quad (1)$$

где μ_1 и μ_2 – средние значения распределений; σ_1 и σ_2 – среднеквадратичные отклонения.

Результаты численных экспериментов для снимков в различных цветовых каналах представлены на рис. 2–4.

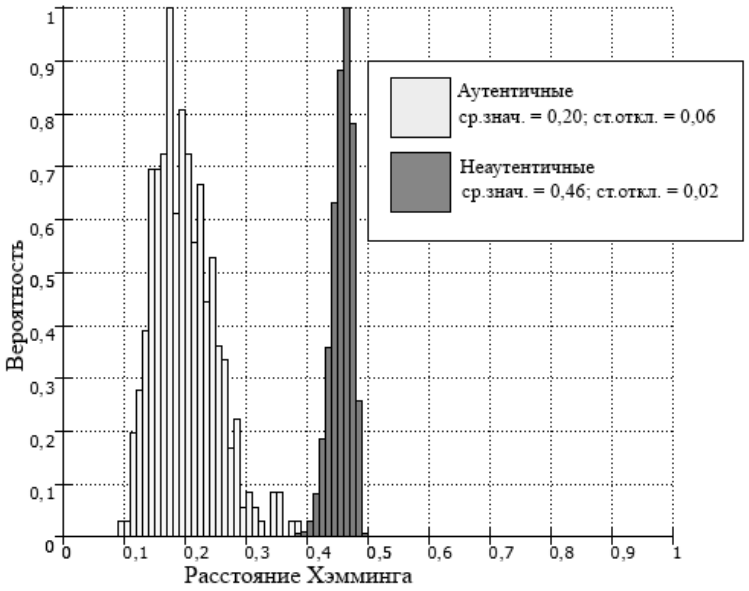


Рис. 2. Внутриклассовое и внеклассовое распределение расстояния Хэмминга для снимков в красном цветовом канале

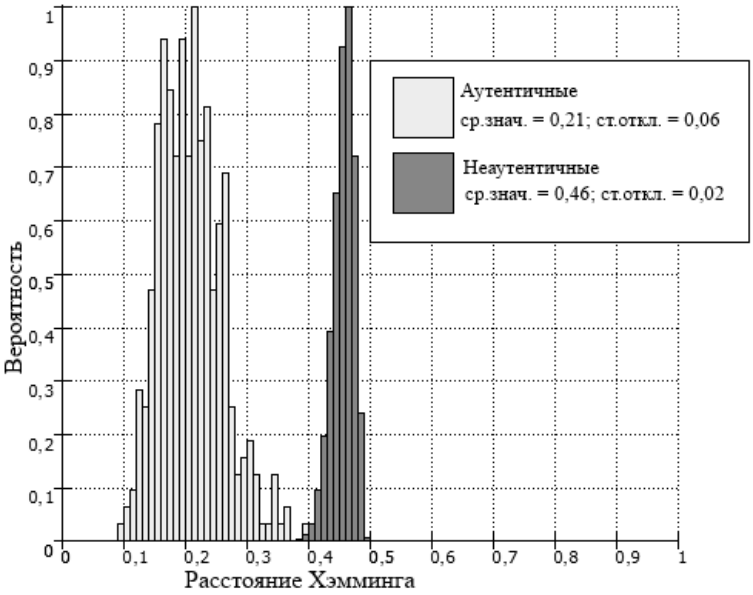


Рис. 3. Внутриклассовое и внеклассовое распределение расстояния Хэмминга для снимков в зеленом цветовом канале

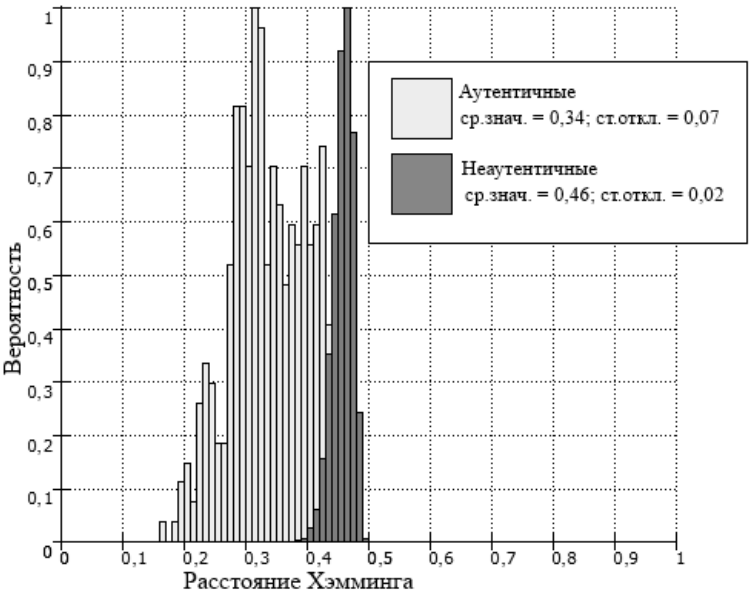


Рис. 4. Внутриклассовое и внеклассовое распределение расстояния Хэмминга для снимков в синем цветовом канале

Значения коэффициентов «разделимости», показывающих степень разделения внутри- и внеклассовых распределений расстояния между двумя кодами РОГ, представлены в таблице.

Коэффициенты разделимости для снимков РОГ в различных цветовых каналах

Канал	Коэффициент разделимости
Красный	**6,0**
Зеленый	5,7
Синий	2,4

Полученные данные показали, что наибольший коэффициент разделимости имеет место для изображений, выделенных из красной цветовой компоненты цветного изображения. Анализ внутриклассовых и внеклассовых распределений расстояний Хэмминга также показал, что наболее различимой текстурой обладает красная компонента (см. рис. 2). Синий канал практически не содержит полезной информации о структуре.

Проведенные численные эксперименты позволяют сделать вывод о том, что использование красной компоненты улучшает качество распознавания снимков со слабо различимой текстурой радужной оболочки глаза в видимом диапазоне излучения.

Литература

1. Absorption spectrum of melanin [Электронный ресурс]. – Режим доступа: http://www.cl.cam.ac.uk/~jgd1000/melanin.html, свободный (дата обращения: 19.04.14).

2. Минакова Н.Н. Информационная система анализа структуры радужной оболочки глаза / Н.Н. Минакова, И.В. Петров // Ползуновский вестник. – 2012. – № 3/2. – С. 230–234.

3. Daugman J. High confidence visual recognition of persons by a test of statistical independence // IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1993. – Vol. 15, № 11. – P. 1148–1161.

Минакова Наталья Николаевна
Д-р физ.-мат. наук, профессор каф. прикладной физики, электроники и информационной безопасности Алтайского государственного университета (АГУ), Барнаул
Тел.: +7(385-2) 36-48-09
Эл. почта: minakova@asu.ru

Петров Иван Васильевич
Аспирант каф. прикладной физики, электроники и информационной безопасности АГУ
Тел.: 8-981-773-58-13
Эл. почта: PetrovIV90@gmail.com

Minakova N.N., Petrov I.V.

Information system analysis barely visible texture of the iris in the visible range

A method to improve iris recognition from images in the visible range based on the selection the red color component is proposed. Effectiveness of this approach on a test database of images is shown.

Keywords: personal identification, biometrics, iris.

УДК 004.056.5

В.Г. Миронова, Е.Б. Белов, А.Ю. Крайнов

Формирование требований при проектировании системы защиты конфиденциальной информации

Представлен способ проведения анализа выполнения требований по информационной безопасности в информационных системах обработки конфиденциальной информации. Требования, предъявляемые к информационным системам обработки конфиденциальной информации, лежат в основе при проектировании и внедрении системы защиты информации.

Ключевые слова: система защиты, требования по безопасности информации, конфиденциальная информация.

Современные компании используют для автоматизации своей деятельности информационные системы (ИС). Все ключевые бизнес-процессы, такие как финансовый и бухгалтерский учет, управление кадрами, клиентами, товаром и складом, документооборот, автоматизируются соответствующими системами, а информация, циркулирующая в них, относится к информации ограниченного доступа (конфиденциальной информации (КИ)). При всей неоспоримой полезности внедрения все большего количества ИС этот процесс несет в себе новые издержки и риски для компании. Обязательным условием высокой конкурентоспособности компании становится защита информации в компании. Защита информации возможна путем создания системы защиты информации (СЗИ).

Разработка системы защиты информации производится подразделением организации или специализированными организациями, имеющими лицензии Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и(или) Федеральной службы безопасности (ФСБ России). Описание этапов создания СЗИ представлено в [1–4].

Основополагающим этапом создания СЗИ является предпроектное обследование ИС, в ходе проведения которого производится инвентаризация ресурсов ИС, построение моделей нарушителя и угроз безопасности информации, исследуются применяемые механизмы защиты информации. Подходы к анализу и оценке угроз безопасности информации описаны в [5, 6].

В ряде нормативных документов федеральных служб – ФСТЭК России и ФСБ России – предложен состав подсистем СЗИ от несанкционированного доступа (НСД):

– подсистема управления доступом;
– подсистема регистрации и учета;
– подсистема контроля целостности;
– подсистема безопасного межсетевого взаимодействия;
– подсистема антивирусной защиты;
– подсистема резервного копирования, восстановления и архивирования;
– подсистема криптографической защиты.

Подсистема управления доступом должна обеспечивать защиту от НСД серверов, автоматизированных рабочих мест (АРМ) пользователей и прикладных сервисов. Кроме того, должна быть обеспечена защита от НСД аппаратно-программных средств, влияющих на функционирование сегментов информационных сетей, в которых обрабатывается защищаемая информация. Основные механизмы реализации этой подсистемы – идентификация и аутентификация, подробно описанные в [7, 8].

В подсистеме регистрации и учета должны регистрироваться события, происходящие в ИС, касающиеся обработки информации ограниченного доступа в ней, например: запуск и останов средств регистрации; события, связанные со средствами безопасности, и др.

Подсистема обеспечения целостности должна осуществлять целостность программных средств защиты информации в составе СЗИ, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации.

Подсистема безопасного межсетевого взаимодействия предназначена для обеспечения безопасности информации при ее обработки в ИС, имеющих выход в сеть общего пользования и(или) международного информационного обмена.

Защиту от вредоносного программного обеспечения обеспечивает подсистема антивирусной защиты.

В [9, 10] описаны подходы, которые применяются при создании подсистемы криптографической защиты, которая обеспечивает конфиденциальность и целостность данных, хранимых в компонентах ИС и передаваемых между ними.

При разработке СЗИ определяются конкретные требования по защите информации, проводится аналитическое обоснование необходимости создания СЗИ и согласовывается выбор основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС), технических и программных средств защиты информации, организуются работы по выявлению возможных каналов утечки информации и нарушения целостности защищаемой информации, аттестация объекта информатизации.

Для проведения оценки уровня информационной безопасности ИС на соответствие требованиям стандартов и нормативных документов используются групповые и частные показатели.

Групповой показатель (GP_d) используется для оценки каждой группы требований к конкретной подсистеме СЗИ, d – номер группового показателя.

Оценка конкретного требования подсистемы СЗИ осуществляется с использованием частного показателя ($CP_{(d,f)}$), который детализирует общую оценку, f – номер частного показателя.

Оценка частного показателя ($CP_{(d,f)}$) формируется по результатам экспертного оценивания степени реализации требования подсистемы защиты информации в СЗИ.

При этом частному показателю $CP_{(d,f)}$ присваиваются следующие значения: 0 – не реализовано; 0,25, 0,5, 0,75 – частично реализовано; 1 – реализовано полностью.

Оценка группового показателя (GP_d) вычисляется как среднее из оценок входящих в него частных показателей ($CP_{(d,f)}$):

$$GP_d = \frac{\sum_{n=1} CP_{(d,f)}}{n}, \quad (1)$$

где n – количество частных показателей (требований к подсистеме защиты информации), входящих в групповой показатель (в подсистему защиты информации, функционирующую в составе СЗИ).

Оценки GP_d, полученные в результате оценивания групповых показателей ИБ, отображаются на диаграмме в соответствующих секторах d на величину, соответствующую значению оценок.

Примером может служить реализация подсистемы управления доступом субъектов доступа к объектам доступа в системе защиты персональных данных (ПДн) согласно [11] в ИС ПДн (ИСПДн), класс защищенности которой – 4.

Требования к подсистеме управления доступом субъектов доступа к объектам доступа для ИСПДн класса защищенности 4:

«УПД.1 – управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

УПД.2 – реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

…

УПД.6 – ограничение неуспешных попыток входа в ИС (доступа к ИС);

…

УПД.11 – разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;

…

УПД.13 – реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;

УПД.14 – регламентация и контроль использования в ИС технологий беспроводного доступа;

УПД.15 – регламентация и контроль использования в ИС мобильных технических средств;

УПД.16 – управление взаимодействием с ИС сторонних организаций (внешние ИС)…».

В таблице представлена экспертная оценка частных показателей подсистемы управления доступом субъектов доступа к объектам доступа для ИСПДн класса защищенности 4.

Экспертная оценка частных показателей

УПД 1	УПД 2	УПД 6	УПД 11	УПД 13	УПД 14	УПД 15	УПД 16
0,75	0,5	0,75	0,25	0,5	0	0	0,5

На рис. 1 показана диаграмма частных показателей подсистемы управления доступом субъектов доступа к объектам доступа для ИСПДн класса защищенности 4.

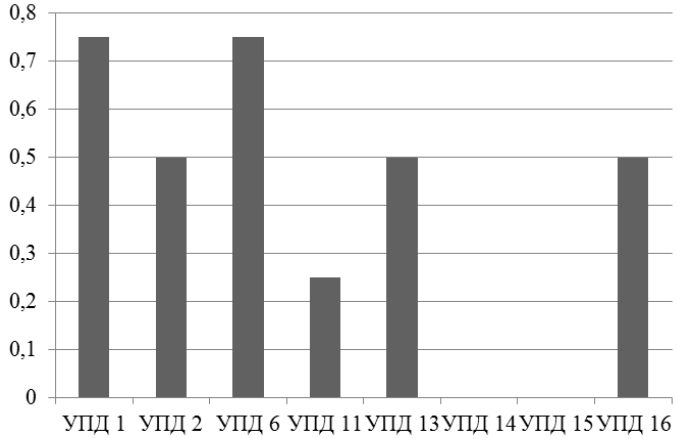


Рис. 1. Диаграмма частных показателей подсистемы управления доступом субъектов доступа к объектам доступа для ИСПДн класса защищенности 4

Исходя из полученных данных по частным показателям подсистемы управления доступом субъектов доступа к объектам доступа для ИСПДн класса защищенности 4 и формулы (1), групповой показатель будет равен 0,40625.

Таким образом, предложенный подход к оценке механизмов защиты информации позволяет выявить не только недействующие механизмы защиты информации, но и подсистемы СЗИ, которые являются слабыми относительно других реализованных в СЗИ подсистем.

Литература

1. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 278 с.

2. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» / А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – № 1 (21), ч. 1. – С. 14–22.

3. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1 (31). – С. 28–35.

4. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

5. Технология прямого поиска при решении задач прикладной математики / В.А. Архипов, С.С. Бондарчук, И.Г. Боровской, А.А. Шелупанов // Вычислительные технологии. – 1995. – Т. 4, № 10. – С. 19.

6. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях их возникновения / В.Г. Миронова, А.А. Шелупанов // Известия Южного федерального университета. Технические науки. – 2012. – Т. 137, № 12. – С. 39–45.

7. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия – Телеком, 2009. – 552 с.

8. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Т.Н. Югов // Доклады ТУСУРа. – 2011. – № 2 (24), ч. 3. – С. 206–211.

9. Криптографические протоколы в системах с ограниченными ресурсами / Р.В. Мещеряков, С.К. Росошек, А.А. Шелупанов, М.А. Сонькин // Вычислительные технологии. – 2007. – Т. 12, Спецвыпуск №1. – С. 51–61.

10. Встраивание криптографических функций в систему связи с ограниченными ресурсами / С.К. Росошек, Р.В. Мещеряков, А.А. Шелупанов, С.С. Бондарчук // Вопросы защиты информации. – 2004. – № 2. – С. 22–25.

11. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2013/06/26/gostajna-dok.html, свободный (дата обращения: 19.05.2014).

Миронова Валентина Григорьевна
Канд. техн. наук, мл. науч. сотр. каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: +7 (923) 415-16-08
Эл. почта: mvg@security.tomsk.ru

Белов Евгений Борисович
Зам. председателя Совета УМО по образованию в области информационной безопасности, Москва
Тел.: +7 (495) 931-06-09
Эл. почта: umoib@yandex.ru

Крайнов Алексей Юрьевич
Д-р физ.-мат. наук, доцент, профессор каф. математической физики физико-технического факультета Национального исследовательского Томского государственного университета
Эл. почта: office@keva.tusur.ru

Mironova V.G., Belov E.B., Krainov A.Yu.
Formation of requirements when designing a system to protect confidential information

The paper presents a method to analyze the requirements for information security in information systems for handling confidential information. Requirements for information systems processing sensitive information underlie the design and implementation of information security.
Keywords: system protection requirements for information security, confidential information.

УДК 004.056.5

В.Г. Миронова, С.С. Бондарчук, С.В. Тимченко

Угрозы безопасности конфиденциальной информации в различных условиях функционирования информационных систем

Представлен способ формирования угроз безопасности конфиденциальной информации, необходимый для создания модели угроз безопасности информации и проектирования системы защиты конфиденциальной информации.

Ключевые слова: угрозы информационной безопасности; конфиденциальная информация, информационная система.

В настоящее время информация становится одним из наиболее весомых и ценных продуктов человеческой деятельности. Эффективность работы любой компании в значительной степени зависит от наличия конфиденциальной информации (КИ), способов ее использования и надежности системы защиты информации (СЗИ).

На различных этапах функционирования информационных систем (ИС) обработки КИ могут возникнуть угрозы безопасности КИ (УБКИ) – такие явления или события, следствием которых могут быть нежелательные воздействия как на информацию, так и на компанию в целом.

В [1] представлены основные виды угроз безопасности:

– физической целостности;

– логической структуры;

– содержания;

– конфиденциальности;

– прав собственности на информацию.

Выявление потенциально существующих возможностей случайного или преднамеренного действия (бездействия), в результате которого могут быть нарушены основные свойства информации и систем ее обработки: доступность, целостность и конфиденциальность – является основной стадией проведения предпроектного обследования. На данной стадии разрабатывается модель угроз безопасности КИ, в которой формируются знания о потенциальных угрозах КИ, оценивается возможность их реализации и степень опасности. Основные этапы создания СЗИ описаны в [2–5].

Первым шагом при разработке модели УБКИ является формирование полного перечня УБКИ, обрабабатываемой в ИС. Формирование полного перечня УБКИ проведем на основе анализа взаимодействия логической цепочки согласно [6]:

источник угрозы – уязвимость – способ (метод) реализации – ресурс – последствие.

Понятия источника УБКИ, уязвимости, последствий приведены в [1]. Описание основных составляющих логической цепочки приведено в таблице.

Для представления УБКИ применим ориентированные графы. Представим полный перечень УБКИ в виде ориентированного графа $\mathbf{Y}(\mathbf{A},\mathbf{B})$, где $\mathbf{A} = \{a_c, a_{1,1}, a_{1,2}, \ldots, a_{i,j}, a_d\}$ – множество вершин графа $\mathbf{Y}$; $\mathbf{B}$ – множество дуг графа $\mathbf{Y}$ – упорядоченных пар вершин $a \in \mathbf{A}$; вершина a_c – начало графа; вершина a_d – конец графа.

Вершины графа представляют собой характеристики УБКИ, которые разделены на уровни по компонентам логической цепочки, где i – количество компонент логической цепочки УБКИ; j – количество признаков каждого компонента.

Для определения множества $\mathbf{A}^* = \{a_{1,1}, a_{1,2}, \ldots, a_{i,j}\}$, $\mathbf{A}^* \in \mathbf{A}$ УБКИ необходимо выявить основные составляющие УБКИ (см. таблицу).

На рис. 1 представлен граф для источника п. 1.2 из таблицы.

Основные составляющие УБКИ

№ п/п	Наименование	Обозначение
1	*2*	*3*
1	Источник угрозы	$\mathbf{A}_1$
1.1	Природные источники угроз	$a_{1,1}$
1.2	Антропогенные источники угроз (нарушители)	$\mathbf{A}_{1,2}$
1.2.1	Внешние (нарушитель ИБ территориально расположен за пределами контролируемой зоны (КЗ))	$a_{1,2,1}$
1.2.2	Внутренние	$a_{1,2,2}$
1.3	Техногенные источники угроз	$a_{1,3}$
2	Уязвимость	$\mathbf{A}_2$
2.1	Ошибки в программах, приводящие к их сбою, аварийному останову, неправильному режиму работы, «зависанию»	$a_{2,1}$
2.2	Закладки и недекларированные возможности программных средств ИС, позволяющие обойти СЗИ	$a_{2,2}$
2.3	Некорректная (ошибочная) схемная и/или микропрограммная (программная) реализация аппаратных, программно-аппаратных средств, используемых в ИС, приводящая к их сбою, отказу	$a_{2,3}$
2.4	Неправильная конфигурация и настройка программных, программно-аппаратных и аппаратных средств, включая СЗИ, приводящие к нарушению безопасности информации ИС	$a_{2,4}$
2.5	Отсутствие блокировки сеансов, оставленных без присмотра	$a_{2,5}$
2.6	Организационно-технические (технологические) уязвимости (непродуманная (небезопасная) технология обработки информации, отсутствие или ошибки в регламентах, отсутствие контроля доступа в помещения за обращением документов по СЗИ и ИС, отсутствие контроля несанкционированного физического подключения к линиям связи и коммуникационному оборудованию ИС и т.д.)	$a_{2,6}$
2.7	Отсутствие контроля целостности данных СЗИ	$a_{2,7}$
2.8	Отсутствие контроля за ИТ-средой ИС (за наличием в ИС только штатного санкционированного оборудования и программных средств: компьютеров, линий связи, периферийных устройств, системных и прикладных программ)	$a_{2,8}$
2.9	Назначение простых коротких или «пустых» паролей для входа в систему, отсутствие обеспечения их конфиденциальности	$a_{2,9}$
2.10	Хранение, отображение и передача данных об ИС либо из базы данных (БД) ИС в явном виде	$a_{2,10}$
3	Способ (метод) реализации	$\mathbf{A}_3$
3.1	Потеря, несанкционированное копирование, кража и вынос документов допущенными к ним лицами	$a_{3,1}$
3.2	Поиск и копирование документов о ИС и СЗИ, оставленных без присмотра, посторонними лицами	$a_{3,2}$
3.3	Поиск компьютеров ИС с оставленным без присмотра активным сеансом или создание условий для их возникновения	$a_{3,3}$
3.4	Подбор пароля	$a_{3,4}$
3.5	Добывание паролей персонала ИС путём общения с ним, подглядывания за его вводом, подслушивания и другими способами	$a_{3,5}$
3.6	Поиск и использование путей обхода СЗИ с помощью штатных программ ИС	$a_{3,6}$
3.7	Использование штатных программ и/или аппаратных, программно-аппаратных средств для поиска, несанкционированного просмотра и/или копирования незащищённых данных	$a_{3,7}$
3.8	Несанкционированное удаление, обнуление, перезапись данных ИС с помощью штатных программ и/или аппаратных, программно-аппаратных средств	$a_{3,8}$
3.9	Модификация (искажение) данных ИС с помощью штатных программ и/или аппаратных, программно-аппаратных средств	$a_{3,9}$
3.10	Случайное возникновение сбоев, отказов и ошибок вследствие старения, износа, неправильного технического обслуживания оборудования и некачественного проектирования программного обеспечения (ПО) ИС	$a_{3,10}$

Продолжение таблицы

1	*2*	*3*
4	Ресурсы (активы)	$\mathbf{A}_4$
4.1	Информация (вводимая в систему, содержащаяся в БД, выводимая из системы), подпадающая под действие Перечня сведений, подлежащих засекречиванию, иная информация с ограниченным доступом (служебная тайна, персональные данные) и другая чувствительная информация, воздействие на которую может привести к нарушению безопасности информации (к нарушению целостности и/или доступности)	$a_{4,1}$
4.2	Технические средства (ТС) (аппаратные и программно-аппаратные средства, накопители и носители информации, линии связи), содержащие КИ или обеспечивающие её передачу	$a_{4,2}$
4.3	Программные средства (общесистемные, прикладные), обрабатывающие КИ	$a_{4,3}$
4.4	Документация, раскрывающая КИ и технологию ее обработки	$a_{4,4}$
5	Последствия	$\mathbf{A}_5$
5.1	Нарушение конфиденциальности	$a_{5,1}$
5.2	Нарушение целостности	$a_{5,2}$
5.3	Нарушение доступности	$a_{5,3}$

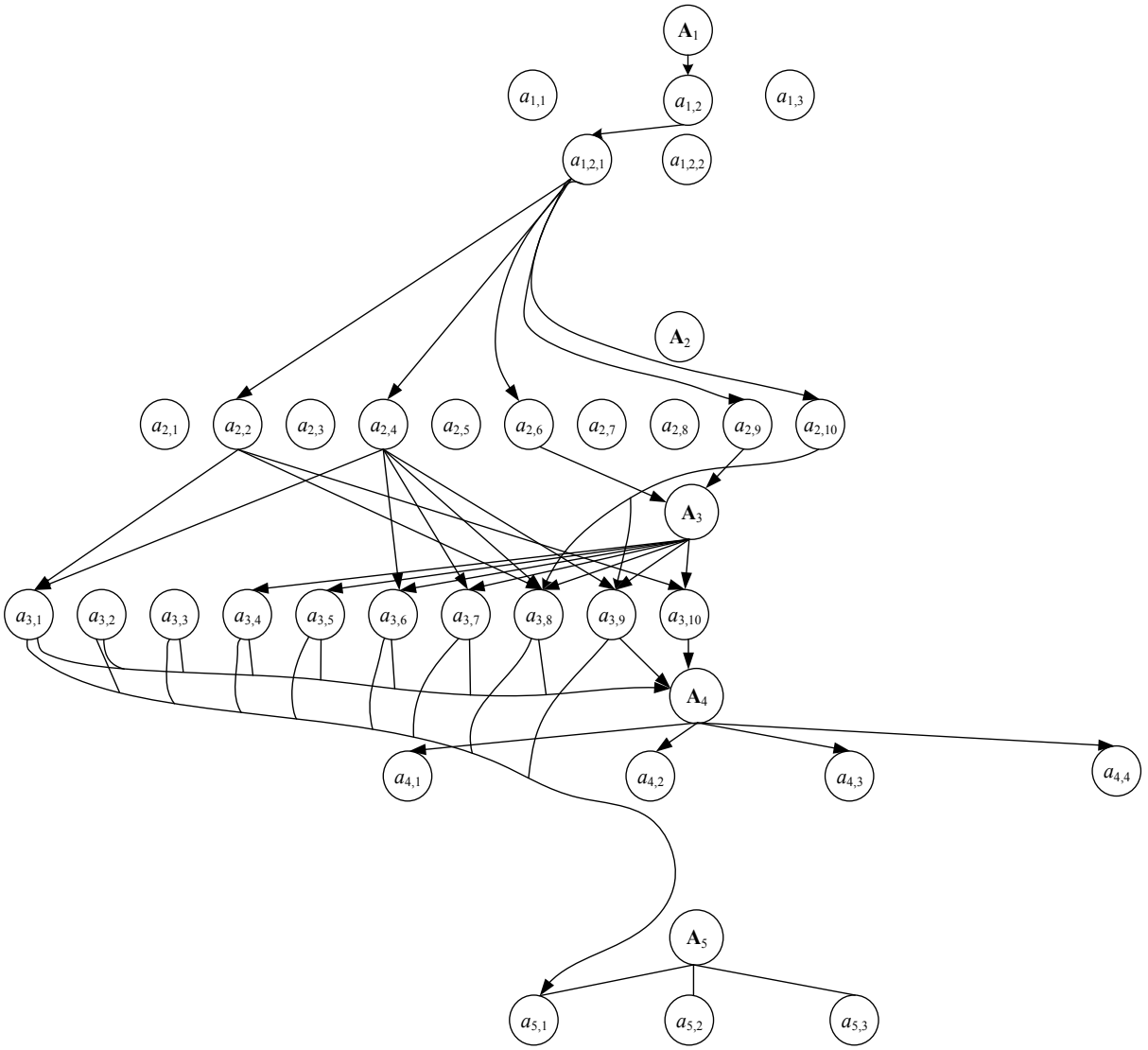


Рис. 1 Граф для источника п. 1.2 табл.1

Используя предложенный автором подход, можно сформировать перечень УБКИ, которые могут быть реализованы в заданных условиях функционирования, расположения ИС и конкретными

нарушителями информационной безопасности информации. Безусловно, после того как перечень будет установлен, специалисты должны определить среди этих угроз актуальные и спроектировать СЗИ. Подходы к созданию механизмов защиты КИ представлен в [7–10].

Литература

1. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 278 с.

2. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» / А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 14–22.

3. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1 (31). – С. 28–35.

4. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

5. Архипов В.А. Технология прямого поиска при решении задач прикладной математики / В.А. Архипов, С.С. Бондарчук, И.Г. Боровской, А.А. Шелупанов // Вычислительные технологии. – 1995. – Т. 4, № 10. – С. 19.

6. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях их возникновения / В.Г. Миронова, А.А. Шелупанов // Известия Южного федерального университета. Технические науки. – 2012. – Т. 137, № 12. – С. 39–45.

7. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия – Телеком, 2009. – 552 с.

8. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Т.Н. Югов // Доклады ТУСУРа. – 2011. – № 2 (24), ч. 3. – С. 206–211.

9. Криптографические протоколы в системах с ограниченными ресурсами / Р.В. Мещеряков, С.К. Росошек, А.А. Шелупанов, М.А. Сонькин // Вычислительные технологии. – 2007. – Т. 12, Спецвыпуск №1. – С. 51–61.

10. Встраивание криптографических функций в систему связи с ограниченными ресурсами / С.К. Росошек, Р.В. Мещеряков, А.А. Шелупанов, С.С. Бондарчук // Вопросы защиты информации. – 2004. – № 2. – С. 22–25.

Миронова Валентина Григорьевна
Канд. техн. наук, мл. науч. сотр. каф. комплексной информационной безопасности
электронно-вычислительных систем ТУСУРа
Тел.: +7-923-415-16-08
Эл. почта: mvg@security.tomsk.ru

Бондарчук Сергей Сергеевич
Д-р физ.-мат. наук, профессор Томского государственного педагогического университета
Эл. почта: office@keva.tusur.ru

Тимченко Сергей Викторович
Д-р техн. наук, ст. науч. сотр., профессор каф. математической физики
Национального исследовательского Томского государственного университета
Эл. почта: tsv@ftf.tsu.ru

Mironova V.G., Bondarchuk S.S., Timchenko S.V.

Threats to information security of confidential information in different contexts of information systems for handling confidential information

The paper presents a method for forming security threats confidential information needed to create the model information security threats and system design to protect confidential information.

Keywords: information security threats; confidential information, the information system.

УДК 004.056.5

В.Г. Миронова, Н.Т. Югов, А.А. Мицель

Методология проведения анализа режимов разграничения прав доступов пользователей к конфиденциальной информации и возможности осуществления несанкционированного доступа

Представлена методология проведения анализа режимов разграничения прав доступов пользователей к конфиденциальной информации и возможности осуществления несанкционированного доступа. В основе методологии лежит дискреционная модель разграничения прав доступа к информации модели Take-Grant.

Ключевые слова: разграничение прав, Take-Grant, конфиденциальная информация, несанкционированный доступ.

Основой любой системы защиты информации (СЗИ) является подсистема контроля и управления доступом, которая включает в себя процедуры идентификации и аутентификации. Эти процедуры защиты информации рассчитаны на работу с субъектами и объектами информационной системы (ИС) поименно. Определения этих понятий четко сформулированы в [1, 2].

Напомним, что в качестве субъектов ИС могут выступать как пользователи, так и процессы, а в качестве объектов ИС – информация и другие информационные ресурсы системы. Безусловно, при создании системы защиты проводится анализ существующих субъектов и объектов в ИС. Основные этапы построения СЗИ подробно описаны в [3].

Одним из этапов создания СЗИ является построение моделей нарушителя и угроз безопасности конфиденциальной информации (КИ). Порядок построения модели нарушителя безопасности изложен в [4], а подходы к проведению анализа угроз безопасности КИ – в [5–7].

На этапе построения модели нарушителя ИБ важно не только определить отличительные черты нарушителей – субъектов ИС, но и выявить возможные сговоры и случаи возможного предоставления доступа к КИ.

При проведении анализа режимов разграничения и распространения прав доступа аутентифицированных субъектов важно руководствоваться политикой ИБ. В [8] представлено описание существующих подходов к реализации политики ИБ. В настоящее время популярной является дискреционная политика ИБ (ДПИБ). Для проведения анализа режимов разграничения и распространения прав доступа при реализации ДПИБ была выбрана модель распространения прав доступа Take-Grant.

Формально описание модели Take-Grant выглядит следующим образом:

1. Множество объектов – **O**, где $o_j \in \mathbf{O}$, $\mathbf{O} = \{o_1, o_2, \ldots, o_j\}$, $j \in \mathbf{N}$;

2. Множество субъектов – **S**, где $s_n \in \mathbf{S}$, $\mathbf{S} = \{s_1, s_2, \ldots, s_n\}$, $n \in \mathbf{N}$;

3. Множество прав доступа **R**, где $r_i \in \mathbf{R}$, $\mathbf{R} = \{r_1, r_2, \ldots, r_j\} \cup \{t, g\}$, где t (take) – право брать права доступа, g (grant) – права давать права доступа.

G = (**S**, **O**, **E**) – конечный помеченный ориентированный без петель граф доступов, описывающий состояние системы. При этом вершинами графа **G** являются элементы **S** и **O**. Каждое ребро графа **G** имеет метку из множества видов прав доступа **R**.

Порядок перехода системы из состояния в состояние определяется правилами преобразования графа доступов, которые в классической модели носят название де-юре правил. Возможность передачи прав между двумя удаленными субъектами определяется с помощью предиката «Возможен доступ» (β, x, y, **G**), который будет истинным тогда и только тогда, когда существует цепочка преобразований графа **G** с помощью правил де-юре, в результате которых появляется дуга от объекта x к объекту y с правом β [8].

Граф доступов **G** = (**S**, **S**, **E**), все вершины которого представлены субъектами, является tg-связным или соединен tg-путем, когда без учета направления ребер в графе между ними существует путь такой, что каждое ребро этого пути помечено t или g.

Основным подходом к определению вероятности возникновения НСД в ИС является присваивание веса (стоимости) каждому ребру графа. Тогда возможность осуществления НСД будет складываться из суммы весов дуг доступов по соответствующим ребрам.

Обозначим множество вершин tg-графа $\mathbf{G_{tg}}$ через **V**, а множество дуг через **D**. Построим для выявления tg-путей новый не помеченный и не ориентированный граф $\mathbf{G_{tg}}$ на основе графа **G** по следующим правилам:

1) множество вершин графа $\mathbf{G_{tg}}$ совпадает с множеством вершин графа **G**;

2) если метка дуги в графе **G** включает в себя **t** или **g**, то добавляем в графе $\mathbf{G_{tg}}$ дугу между соответствующими вершинами. Граф $\mathbf{G_{tg}}$ характеризует связь вершин с помощью tg-путей.

В графе $\mathbf{G_{tg}}$ отношение инцидентности будем задавать с помощью матрицы смежности **E**. Матрицей смежности графа $\mathbf{G_{tg}}$ в этом случае является матрица **E** размерностью $n \times n$, (где n – число вершин графа), однозначно представляющая его структуру. А именно, если существует дуга из вершины v_i в вершину v_j, то существующий элемент матрицы смещения $\mathbf{E}_{ij} = 1$, в противном случае $\mathbf{E}_{ij} = 0$, также будем полагать, что в графе нет петель, и полагать $\mathbf{E}_{ij} = 0$. Поскольку граф $\mathbf{G_{tg}}$ будет рассматриваться как граф без петель, то в матрице смежности $\mathbf{G_{tg}}$ по главной диагонали будут стоять нулевые элементы.

Если **E** – матрица смежности графа $\mathbf{G_{tg}}$, то в графе существует маршрут между вершинами v_i и v_j тогда и только тогда, когда (i, j)-й элемент матрицы $\mathbf{E} + \mathbf{E}^2 + \ldots + \mathbf{E}^{n-1}$ не равен нулю.

Алгоритм поиска возможных путей доступа между субъектами:

1. Выделить количество участвующих субъектов.
2. Построить граф доступов **G**.
3. Построить матрицу доступов графа **G**.
4. Построить граф $\mathbf{G_{tg}}$.
5. Построить матрицу смежности **E**.
6. Определить веса дуг, построить матрицу меток дуг.
7. Определить маршруты по матрице смежности.
8. Определить стоимости полученных маршрутов.

Рассмотрим несколько типов графов доступов для разного количества участвующих субъектов. Пусть количество субъектов – 3.

1. Количество участвующих субъектов – s_1, s_2, s_3.
2. Граф доступов **G** (рис. 1).

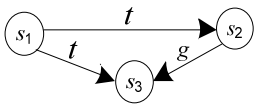


Рис. 1. Граф доступов **G**

3. Матрица доступов графа **G** (табл. 1).

Таблица 1

Матрица доступов графа G

	s_1	s_2	s_3
s_1	*F*	*t*	
s_2		*F*	
s_3	*t*	*g*	*F*

4. Построить граф $\mathbf{G_{tg}}$ (рис. 2).

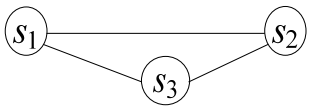


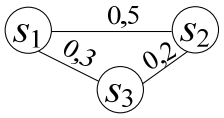
Рис. 2. Граф $\mathbf{G_{tg}}$

5. Построить матрицу смежности **E** (рис. 3).

$$\mathbf{E} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Рис. 3. Матрица смежности **E**

6. Веса дуг, матрица меток дуг (рис. 4).



$$\mathbf{E}=\begin{pmatrix} 0 & 0,5 & 0,3 \\ 0,5 & 0 & 0,2 \\ 0,3 & 0,2 & 0 \end{pmatrix}.$$

Рис. 4. Веса дуг, матрица меток дуг

7. Маршруты по матрице смежности. Максимальная длина маршрута $l = 3$ (рис. 5):
при длине пути 1

$$\mathbf{E}=\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix};$$

при длине пути 2

$$\mathbf{E}=\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

Рис. 5. Маршруты по матрице смежности

8. Стоимость полученных маршрутов (рис. 6):
при длине пути 1

$$\mathbf{S}=\begin{pmatrix} 0 & 0,5 & 0,3 \\ 0,5 & 0 & 0,2 \\ 0,3 & 0,2 & 0 \end{pmatrix};$$

при длине пути 2

$$\mathbf{S}=\begin{pmatrix} 0 & 0,5 & 0,7 \\ 0,5 & 0 & 0,8 \\ 0,7 & 0,8 & 0 \end{pmatrix}.$$

Рис. 6. Стоимость полученных маршрутов

Пусть количество субъектов равно 4, тогда:
1. Количество участвующих субъектов – s_1, s_2, s_3, s_4.
2. Граф доступов **G** (рис. 7).

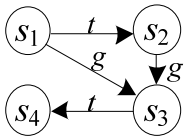


Рис. 7. Граф доступов **G**

3. Матрица доступов графа **G** (табл. 2).

Таблица 2

Матрица доступов графа G

	s_1	s_2	s_3	s_4
s_1	F	t	g	
s_2		F	g	
s_3			F	t
s_4				F

4. Построить граф $\mathbf{G_{tg}}$ (рис. 8).

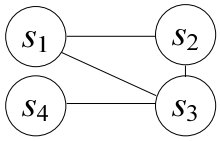


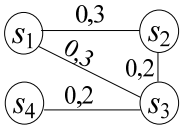
Рис. 8. Граф $\mathbf{G_{tg}}$

5. Построить матрицу смежности **E** (рис. 9).

$$\mathbf{E}=\begin{pmatrix}0&1&1&0\\1&0&1&0\\1&1&0&1\\0&0&1&0\end{pmatrix}.$$

Рис. 9. Матрица смежности **E**

6. Веса дуг, матрица меток дуг (рис. 10).



$$\mathbf{E}=\begin{pmatrix}0&0{,}3&0{,}3&0\\0{,}3&0&0{,}2&0\\0{,}3&0{,}2&0&0{,}2\\0&0&0{,}2&0\end{pmatrix}.$$

Рис. 10. Веса дуг, матрица меток дуг

7. Маршруты по матрице смежности. Максимальная длина маршрута $l = 3$ (рис. 11).

$$\mathbf{E}=\begin{pmatrix}0&1&1&0\\1&0&1&0\\1&1&0&1\\0&0&1&0\end{pmatrix}.$$

$$\mathbf{E}=\begin{pmatrix}2&1&1&1\\1&2&1&1\\1&1&3&1\\1&1&0&1\end{pmatrix}.$$

Рис. 11. Маршруты по матрице смежности

8. Стоимость полученных маршрутов (рис. 12):
при длине пути, равном 1

$$\mathbf{S}=\begin{pmatrix}0&0{,}3&0{,}3&0\\0{,}3&0&0{,}2&0\\0{,}3&0{,}2&0&0{,}2\\0&0&0{,}2&0\end{pmatrix};$$

при длине пути, равном 2

$$\mathbf{E}=\begin{pmatrix}0&0{,}5&0{,}5&0\\0{,}5&0&0{,}6&0\\0{,}5&0{,}6&0&0\\0&0&0&0\end{pmatrix};$$

при длине пути, равном 3

$$\mathbf{E}=\begin{pmatrix}0&0&0&0{,}7\\0&0&0&0{,}8\\0&0&0&1\\0{,}7&0{,}8&0&0\end{pmatrix}.$$

Рис. 12. Стоимость полученных маршрутов

Выявляя вероятностных нарушителей ИБ, важно не только знать их отличительные особенности, но и выявлять и оценивать возможные пути получения доступа к КИ нарушителем, проводить анализ путей распространения прав доступа.

С помощью предложенного подхода с использованием правил модели Take-Grant можно оценить возможные пути распространения прав доступа к КИ по длине и провести анализ их стоимости. Такой подход позволяет быстро и оперативно выявлять взаимодействия пользователей ИС с нарушителями ИБ, давать оценку таким взаимодействиям, формировать способы нейтрализации таких взаимодействий.

Литература

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия – Телеком, 2009. – 552 с.

2. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 278 с.

3. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» / А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 14–22.

4. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1 (31). – С. 28–35.

5. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

6. Технология прямого поиска при решении задач прикладной математики / В.А. Архипов, С.С. Бондарчук, И.Г. Боровской, А.А. Шелупанов // Вычислительные технологии. – 1995. – Т. 4, № 10. – С. 19.

7. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях их возникновения / В.Г. Миронова, А.А. Шелупанов // Известия Южного федерального университета. Технические науки. – 2012. – Т. 137, № 12. – С. 39–45.

8. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Т.Н. Югов // Доклады ТУСУРа. – 2011. – № 2 (24), ч. 3. – С. 206–211.

9. Криптографические протоколы в системах с ограниченными ресурсами / Р.В. Мещеряков, С.К. Росошек, А.А. Шелупанов, М.А. Сонькин // Вычислительные технологии. – 2007. – Т. 12, Спецвыпуск №1. – С. 51–61.

10. Встраивание криптографических функций в систему связи с ограниченными ресурсами / С.К. Росошек, Р.В. Мещеряков, А.А. Шелупанов, С.С. Бондарчук // Вопросы защиты информации. – 2004. – № 2. – С. 22–25.

Миронова Валентина Григорьевна
Канд. техн. наук, мл. науч. сотр. каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: +7-923-415-16-08
Эл. почта: mvg@security.tomsk.ru

Югов Николай Тихонович
Д-р физ.-мат. наук, профессор каф. математики ТУСУРа
Эл. почта: office@keva.tusur.ru

Мицель Артур Александрович
Д-р техн. наук, профессор каф. автоматизированных систем управления ТУСУРа
Тел.: +7 (382-2) 70-15-36
Эл. почта: maa@asu.tusur.ru

Mironova V.G., Ugov N.T., Mitsel A.A.

The methodology for the analysis of modes of differentiation of user access rights to confidential information and the possibility of unauthorized access

The article presents a methodology for the analysis of modes of differentiation of user access rights to confidential information and the possibility of unauthorized access . The methodology is discretionary model differentiation of access rights to information model Take-Grant.

Keywords: divestiture, Take-Grant, confidential information, unauthorized access.

УДК 004.722.2:621.391

В.Е. Митрохин, П.Г. Рингенблюм

Оценка влияния угроз информационной безопасности на доступность телекоммуникационной сети

Рассматривается оценка влияния угроз информационной безопасности на коэффициент готовности как на один из основных показателей телекоммуникационных сетей с использованием мнимого устройства, включаемого в состав оборудования узлов связи и отражающего влияние угроз информационной безопасности на сеть связи.

Ключевые слова: телекоммуникации, информационная безопасность, надежность, коэффициент готовности.

Под угрозой безопасности информации понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. По цели воздействия на информационную систему угрозы информационной безопасности делятся на угрозы целостности, конфиденциальности и доступности циркулирующей в ней информации.

Успешно реализованная угроза доступности информации в телекоммуникационной сети (ТКС), в отличие от угроз, направленных на другие свойства информации, приводит к простою атакованных информационных служб и как к крайнему варианту всей ТКС. Время простоя элементов ТКС возможно оценить количественно и включить его в расчет коэффициента готовности каждого рассматриваемого элемента как одну из составляющих времени восстановления работоспособности элемента, и далее – всей ТКС, что позволит в дальнейшем оценить ее защищенность от угроз этого типа.

В 2013 г. к широко распространенным фактическим угрозам информационной безопасности добавились хорошо известные исторически, но вследствие крайне малой распространенности не входящие в статистические выкладки и модели угроз, используемые коммерческими предприятиями угрозы доступности информации, связанные с паразитными электромагнитными излучениями и наводками (ПЭМИН). В результате скандальных публикаций Э. Сноуденом выдержек из каталогов программно-аппаратных средств, стоящих на вооружении АНБ США, достоянием общественности стала информация о программно-аппаратных закладках для слежения и деструктивных воздействий на оборудование, устанавливаемое на узлах связи ТКС. Были обнародованы программные и аппаратные закладки, предназначенные для скрытой установки в маршрутизаторы и межсетевые экраны, широко применяемые для построения ТКС, позволяющие производить полностью скрытое удаленное управление скомпрометированными устройствами и зеркалирование передаваемой информации. В силу этого появилась необходимость рассматривать эти угрозы при проектировании и оценке защищенных ТКС. В связи с отсутствием сложившейся практики моделирования угроз информационной безопасности такого рода предлагается использовать нижеследующий метод, хорошо зарекомендовавший себя для моделирования угроз информационной безопасности в сложных и разветвленных ТКС.

Для численной оценки влияния угроз информационной безопасности на доступность телекоммуникационной сети предлагается воспользоваться математическим аппаратом коэффициента готовности как наиболее гибкого и реалистичного стандартизованного показателя надежности. В этих целях введем в состав оборудования, расположенного на узле связи ТКС, мнимое устройство, влияние коэффициента готовности которого будет отражать влияние угроз информационной безопасности на доступность рассматриваемого узла связи.

Коэффициент готовности мнимого устройства ($K_{\Gamma}^{\text{В}}$) будет складываться из вероятности возникновения соответствующей угрозы информационной безопасности ($P_{\text{В}}$), вероятности ее реализации ($P_{\text{Р}}$) и коэффициента неготовности реализованной угрозы ($K_{\text{НГ}}^{\text{Р.У}}$), отражающего временной интервал, обусловленный простоем узла ТКС, вызванным устранением реализованной угрозы и ее

последствий. Исходя из того, что для оказания влияния на общий коэффициент готовности системы все три события (возникновение угрозы, успешная реализация угрозы, простой в результате реализации угрозы и устранения ее последствий) должны произойти одновременно, то согласно формулам определения полной вероятности коэффициент готовности элемента, отражающего влияние угроз информационной безопасности ($K_{\Gamma}^{\text{В}}$), определяется следующим образом:

$$K_{\Gamma}^{B} = 1 - K_{H\Gamma}^{P.У} \times P_B \times P_B \,. \quad (1)$$

Коэффициент неготовности реализованной угрозы ($K_{\text{НГ}}^{\text{Р.У}}$) отражает влияние реализованных угроз информационной безопасности на коэффициент готовности элемента телекоммуникационной системы. Тем не менее вероятность возникновения и успешной реализации угрозы информационной безопасности на определенном узле телекоммуникационной системы отлична от 1. Для учета этого фактора необходимо ввести в формулу расчета коэффициента готовности вероятность возникновения и реализации угрозы информационной безопасности.

Вероятность возникновения угрозы информационной безопасности ($P_{\text{В}}$) определяется на основании статистических данных, включающих в себя общую статистику по инцидентам информационной безопасности. Рассмотрим механизм оценки влияния угроз информационной безопасности на примере закладок АНБ. Вероятность возникновения описанной угрозы для коммерческого предприятия примем $P_{\text{В}} = 0{,}00001$. Вероятность принята минимальной в связи с нацеленностью данной угрозы информационной безопасности на стратегический и правительственный сегмент ТКС. Однако полностью исключить эту угрозу коммерческим предприятиям нельзя по причине отсутствия механизмов четкой таргетированности, т.е. возможно срабатывание закладки в оборудовании, изначально предназначенном для установки в критичных объектах сетевой инфраструктуры Российской Федерации, но установленном в коммерческом предприятии.

Вероятность реализации угрозы информационной безопасности ($P_{\text{Р}}$) зависит от применяемого для защиты телекоммуникационного оборудования и определяется на основании модели угроз, разработанной для конкретного узла в топологии сети и определенного оборудования, применяемого на этом узле. Для рассматриваемой в качестве примера угрозы вероятность реализации угрозы $P_{\text{Р}} = 1$ по причине отсутствия на сегодняшний день механизмов превентивной защиты от программно-аппаратных закладок.

Коэффициентом неготовности называется вероятность того, что рассматриваемый объект или система будет находиться в неработоспособном состоянии в период времени, когда предусматривается его или ее использование по назначению. Определить коэффициент неготовности для заданного периода времени можно по следующей формуле:

$$K_{\text{НГ}} = \frac{t_{\text{В}}}{t_{\text{П}}}, \quad (2)$$

где $t_{\text{П}}$ – общая продолжительность периода; $t_{\text{В}}$ – время восстановления работоспособности (простоя).

Для определения коэффициента неготовности реализованной угрозы необходимо задаться временным интервалом и определить время простоя, вызванного реализацией угрозы информационной безопасности и ее последствий на этом временном интервале.

Рассмотрим коэффициент неготовности, связанный с реализованной угрозой информационной безопасности, связанной с программно-аппаратными закладками в оборудовании узла связи ТКС. Примем среднее время восстановления после инцидента $t_{\text{В}} = 72$ ч. Это время обусловлено необходимостью получения с регионального склада поставщика нового оборудования, подготовки его к работе и установки на место инцидента. Для периода в 1 год $t_{\text{П}} = 8760$ ч в соответствии с (2) получаем

$$K_{\text{НГ}} = \frac{72}{87960} = 0{,}0082192 \,. \quad (3)$$

Исходя из (1) и (3), коэффициент готовности мнимого устройства узла связи, связанного с этой угрозой информационной безопасности, будет составлять

$$K_{\Gamma} = 1 - (0{,}00001 \times 1 \times 0{,}0082192) = 0{,}9999999 \,. \quad (4)$$

Аналогично рассчитываются коэффициенты готовности для остальных актуальных угроз информационной безопасности. Результаты расчетов сведены в таблицу.

Вероятности возникновения, реализации и коэффициент неготовности угроз информационной безопасности

№ п/п	Вид угрозы информационной безопасности	$P_{\text{В}}$	$P_{\text{Р}}$	$t_{\text{В}}$	$K_{\text{НГ}}^{\text{Р.У}}$
1	Атаки типа отказ в обслуживании	0,23667	0,6	4,6	0,00052476
2	Мошенничество в сфере телекоммуникаций	0,06	1	1	0,00011408
3	Вредоносное ПО	0,55667	0,2	24	0,0027379
4	Проникновение в систему извне	0,13667	0,1	2	0,00022816
5	Саботаж	0,03	1	48	0,0054758
6	Инциденты с беспроводными сетями	0,15	1	3,4	0,00038786
7	Ботнеты	0,205	0,4	24	0,0027379
8	Атаки на службу доменных имен	0,07	0,2	1	0,00011408
9	Внедрение закладок на оборудование ТКС	0,00001	1	72	0,0082192

Остальные актуальные угрозы информационной безопасности рассматриваются аналогично и рассчитываются по формулам (1)–(4) на основе данных из таблицы, которые затем последовательно объединяются в единый блок коэффициента готовности угроз информационной безопасности:

$$K_{\Gamma}^{B} = K_{\Gamma}^{\text{У1}} \times K_{\Gamma}^{\text{У1}} \times \cdots \times K_{\Gamma}^{\text{У9}}. \quad (5)$$

Подставив в (5) результаты предыдущих вычислений, получим

$$K_{\Gamma}^{B} = 0{,}9999255 \times 0{,}9999932 \times 0{,}9999969 \times 0{,}9998357 \times 0{,}9999418 \times 0{,}9997755 \times 0{,}9999984 \times \times 0{,}9999999 = 0{,}9991624. \quad (6)$$

Таким образом, в (6) получено значение коэффициента готовности мнимого устройства, отражающего влияние угроз информационной безопасности, направленных на доступность информации, на надежность ТКС. Для дальнейшей оценки защищенности ТКС от угроз такого рода можно воспользоваться методикой, предложенной в [2] и [4].

Литература

1. ГОСТ 27.002–89. Надежность в технике. Основные понятия. Термины и определения. – М.:Стандартинформ, 1990. – 24 с.

2. Митрохин В.Е. Влияние угроз информационной безопасности на коэффициент готовности телекоммуникационной сети с линейной топологией / В.Е. Митрохин, П.Г. Рингенблюм // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 156–160.

3. Миронова В.Г. Модель нарушителя безопасности конфиденциальной безопасности / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1. – С. 28–35.

4. Митрохин В.Е. Использование показателей, связанных с коэффициентом готовности для оценки защищенности телекоммуникационной сети от угроз информационной безопасности / В.Е. Митрохин, П.Г. Рингенблюм // Сб. матер. междунар. науч. конгресса и выставки «Интерэкспо Гео-Сибирь». – 2013. – Т. 5, № 2. – С. 102–106.

5. Сопов М.А. Модели повышения уровня информационной безопасности удостоверяющего центра / М.А. Сопов, А.Ю. Крайнов, А.А. Шелупанов // Доклады ТУСУРа. – 2011. – № 2 (24), ч. 3. – С. 211–216.

6. Жабина А.В. Коэффициент готовности развивающихся телекоммуникационных сетей / А.В. Жабина, Зо Зен Чхор // Матер. межрег. информ. конгресса «МИК-2004». – Омск: ОмГТУ, 2004. – Ч. 3. – С. 137–139.

Митрохин Валерий Евгеньевич
Д-р техн. наук, профессор, зав. каф. инфокоммуникационных системы и информационнй безопасности Омского государственного университета путей сообщения (ОмГУПС)
Тел.: 8 (381-2) 31-06-94
Эл. почта: mitrokhin@list.ru

Рингенблюм Павел Генрикович
Аспирант каф. инфокоммуникационных системы и информационной безопасности ОмГУПС
Эл. почта: win32conficker@gmail.com

Mitrokhin V.E., Ringenbljoum P.G.
Assessing the influence of information security threats to the availability of telecommunications network

The estimation of the influence of security threats on the availability factor, as one of the main indicators of telecommunication networks using imaginary device, included to the equipment of communication nodes, is reflecting the impact of security threats on the communication networks.
Keywords: telecommunications, information security, reliability, availability.

УДК 621.391.82, 621.396.6

В.Е. Митрохин, А.В. Ряполов

Защищенность радиоэлектронных систем к дестабилизирующему воздействию электромагнитных полей

Проведена оценка устойчивости элементов радиоэлектронной системы к дестабилизирующему воздействию внешних электромагнитных полей. Исследована эффективность использования экранирующих оболочек при наличии в них технологических отверстий. Исследовано появление наведенных токов и напряжений в кабельных соединениях от импульсного электромагнитного поля.

Ключевые слова: электромагнитная совместимость, экранирование, кабельные соединения, импульсные электромагнитные поля, наведенные напряжения.

Эксплуатация радиоэлектронных систем всегда сопряжена с проблемами, когда присутствует влияние мощных электромагнитных полей. Воздействие полей искусственного или естественного происхождения может приводить к нарушению обработки и передачи информации за счет создания помех в цепях устройства [1]. Нарушение нормальной работы выражается в нестабильности, сбоях, зависаниях, неправильно сформированных выходных сигналах и т.д. При взаимодействии с кабельными соединениями, которые являются неотъемлемой частью компьютерных сетей, систем управления и телекоммуникационных средств, возможно нарушение уровней сигналов, рост коэффициента ошибок, потеря трафика и т.п. В ряде случаев электромагнитные поля индуктируют в кабельных линиях напряжения, которые, достигая аппаратуры обработки информации, приводят к электрическим пробоям и термическим разрушениям. Для эксплуатируемых систем это значительно ухудшает такие показатели информационной безопасности, как целостность и доступность информации.

В этой статье мы кратко приводим результаты работы по расчету воздействия электромагнитных полей на элементы радиоэлектронной системы. В качестве объекта исследования выбрана пара экранированных блоков аппаратуры, соединенных симметричным кабелем передачи данных (рис. 1).

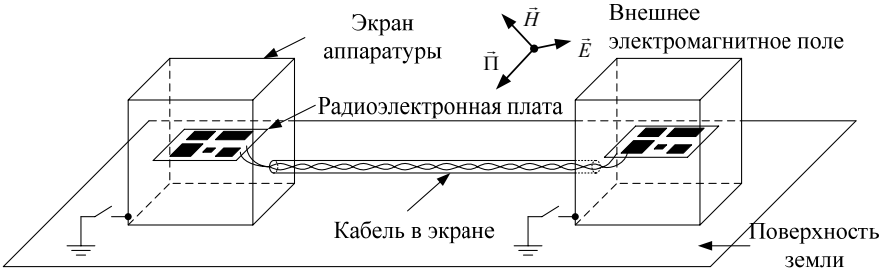


Рис. 1. Схема исследуемой радиоэлектронной системы

Исследование защищенности блоков аппаратуры. Оценка воздействия электромагнитного поля на блоки аппаратуры производилась с помощью метода конечных разностей во временной области (Finite Difference Time Domain, FDTD), широко используемого в решении электродинамических задач СВЧ-диапазона [2]. Метод позволяет исследовать распространение электромагнитных волн в диэлектрических и проводящих средах, но имеет ограничения при моделировании материалов с высокой проводимостью, например металлов. Эти ограничения преодолеваются внесением в стандартный метод FDTD дополнительных способов расчета [3, 4]. Благодаря возможности задавать в трехмерном объеме геометрические особенности исследуемых объектов, метод крайне эффективен при исследовании экранирующих оболочек. Аппаратура размещается в корпусах, где практически всегда присутствуют вентиляционные и технологические отверстия, которые являются путями проникновения электромагнитных полей. Точно воссоздав размеры экрана и отверстий в нем, метод FDTD позволяет еще на этапе разработки узнать, будут ли проникающие электромагнитные поля достигать опасных уровней.

В данном случае габаритные размеры исследуемой экранирующей оболочки взяты 20×40×40 см. Трехмерное счетное пространство, в котором располагается экран аппаратуры, было разбито на элементарные ячейки кубической формы со стороной 5 мм. Толщина стенки экрана соответствует размеру элементарной ячейки счетного пространства 5 мм. При такой толщине металла электромагнитное поле будет проникать внутрь экрана преимущественно через технологические отверстия. Были рассмотрены варианты экрана с отверстиями диаметром от 5 мм до 15 см. Внешнее электромагнитное поле задавалось двух типов: гармоническое с частотой от 1 МГц до 2 ГГц и импульсное с параметрами фронта и длительности 5/50 нс. Во всех случаях электромагнитное поле принималось как плоская волна с амплитудой напряженности электрического поля 100 В/м. Амплитуда напряженности магнитного поля, согласно соотношению между компонентами плоской волны 377 Ом, равнялась 0,265 А/м.

На рис. 2 представлены в качестве примера картины распределения напряженности электрического и магнитного поля вокруг и внутри экранирующей оболочки с отверстием диаметром 3 см, расположенным в верхней грани. На рис. 2, *а*, *б* показано воздействие гармонического сигнала с частотой 1600 МГц. Темные и светлые области показывают изменение напряженности поля в диапазоне от отрицательного до положительного амплитудного значения.

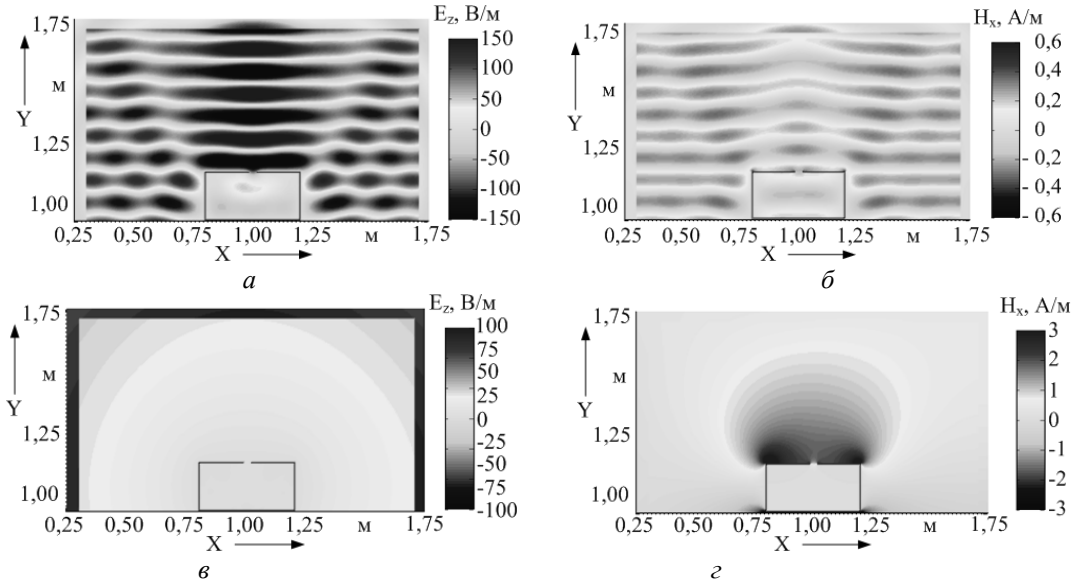


Рис. 2. Картины распределения электрического (слева) и магнитного (справа) полей при воздействии поля на экранирующую оболочку с отверстием: *а*, *б* – гармонического; *в*, *г* – импульсного

На рис. 3 показаны частотные зависимости напряженностей электрического и магнитного полей, которые были построены по значениям амплитуд, зафиксированных внутри экранирующей оболочки с отверстием 3 см. Можно заметить, что на обоих графиках присутствуют пики, начиная с частоты 800 МГц. Такой резкий рост значений напряженностей объясняется возникновением резонансных явлений внутри объема экрана, что является крайне опасным для работы аппаратуры внутри корпуса. Для приведенного примера меньший из габаритных размеров оболочки, равный 20 см, как раз составляет примерно половину длины волны для частоты 800 МГц. Сравнивая зависимости напряженностей электрического и магнитного полей, можно увидеть большую проникающую способность магнитного поля, в особенности на низких частотах.

Основным показателем эффективности работы экрана является экранное затухание, которое для электрического и магнитного полей рассчитывается на основе отношения значений напряженности при отсутствии и наличии экрана [5]:

$$A_{\text{Е}} = 20\lg\frac{E}{E_{\text{Э}}},\ A_{\text{Н}} = 20\lg\frac{H}{H_{\text{Э}}}. \qquad (1)$$

На рис. 4 приведены кривые экранного затухания для электрического и магнитного полей, построенные для экрана с отверстием диаметром 3 см. В расчете использованы значения, приведенные

на рис. 3, и амплитудные значения электрической и магнитной компонент воздействующей плоской волны.

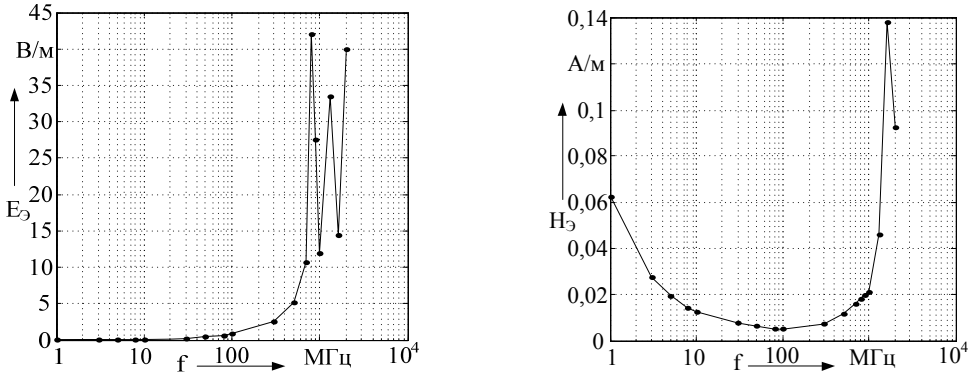


Рис. 3. Частотные зависимости электрического (слева) и магнитного (справа) полей в центре экранирующей оболочки с отверстием диаметром 3 см

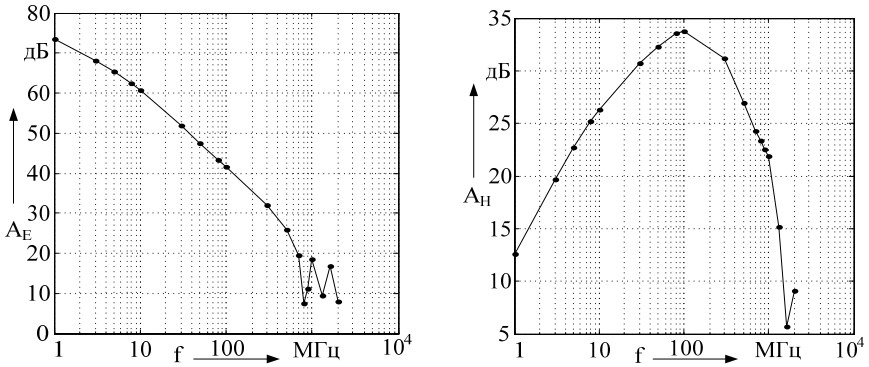


Рис. 4. Частотные зависимости экранного затухания для электрического (слева) и магнитного (справа) полей экранирующей оболочки с отверстием диаметром 3 см

Уменьшение защищенности к магнитному полю на низких частотах (см. рис. 4) приводит к тому, что внутренние цепи радиоэлектронной аппаратуры оказываются уязвимы к воздействию импульсных электромагнитных полей, у которых бóльшая часть энергии расположена в низкочастотной области. На рис. 5 показаны результаты моделирования проникновения импульсного электромагнитного поля с временными параметрами 5/50 нс внутрь экранирующей оболочки с отверстием. Зависимости построены для экранов, где диаметр отверстий изменяется от 5 мм до 15 см.

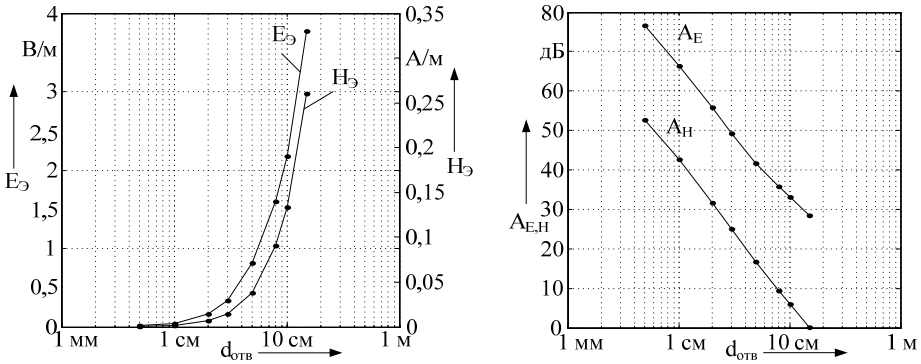


Рис. 5. Изменение электрического и магнитного полей (слева) и экранного затухания (справа) в зависимости от диаметра отверстия в экране

Из графиков на рис. 5 видно, что напряженность электрического и магнитного полей резко увеличивается, и при достижении диаметра отверстия в несколько сантиметров эти значения достигают того уровня, который способен привести к появлению помех во внутренних цепях. Экранное затухание для электрического поля снижается до значения менее 30 дБ, а защищенность от магнитного поля при отверстии диаметром 10 см и более пропадает практически полностью.

Исследование влияния на кабельные соединения. Источником нарушения целостности информации при передаче сигналов по кабелям в аппаратуре и между отдельными блоками выступают наведенные напряжения и токи. В экранированных цепях индуктированные напряжение и ток появляются, прежде всего, в цепи экрана [6]:

$$\dot{U}_{\text{экр}}(\omega,x)=\dot{E}(\omega)\left[\frac{\text{ch}\left(\ln\sqrt{p_{\text{н}}}\right)\text{ch}\left(\gamma_{\text{экр}}(\omega)\cdot\left(l_{\text{к}}-x\right)-\ln\sqrt{p_{\text{к}}}\right)-\text{ch}\left(\ln\sqrt{p_{\text{к}}}\right)\text{ch}\left(\gamma_{\text{экр}}(\omega)\cdot x-\ln\sqrt{p_{\text{н}}}\right)}{\gamma_{\text{экр}}(\omega)\cdot\text{sh}\left(\gamma_{\text{экр}}(\omega)\cdot l_{\text{к}}-\ln\sqrt{p_{\text{н}}p_{\text{к}}}\right)}\right]; \quad (2)$$

$$\dot{I}_{\text{экр}}(\omega,x)=\frac{-\dot{E}(\omega)}{Z_{\text{прод}}}\left[1-\frac{\text{ch}\left(\ln\sqrt{p_{\text{н}}}\right)\cdot\text{sh}\left(\gamma_{\text{экр}}(\omega)\cdot\left(l_{\text{к}}-x\right)-\ln\sqrt{p_{\text{к}}}\right)+\text{ch}\left(\ln\sqrt{p_{\text{к}}}\right)\cdot\text{sh}\left(\gamma_{\text{экр}}(\omega)\cdot x-\ln\sqrt{p_{\text{н}}}\right)}{\text{sh}\left(\gamma_{\text{экр}}(\omega)\cdot l_{\text{к}}-\ln\sqrt{p_{\text{н}}p_{\text{к}}}\right)}\right], \quad (3)$$

где $\dot{E}(\omega)$ – наведенная ЭДС, численно равная продольной электрической компоненте воздействующего электромагнитного поля, В/м; $\gamma_{\text{экр}}(\omega)$ – коэффициент распространения для цепи экрана кабеля, 1/м; $l_{\text{к}}$ – длина кабеля, м; x – координата вдоль длины кабеля, м; $p_{\text{н}}$ и $p_{\text{к}}$ – коэффициенты отражения, показывающие заземление или изолированность от земли начала и конца цепи экрана.

Протекание тока в экране в совокупности с воздействием внешнего поля вызывает появление в кабеле напряжений «жила–оболочка» и «жила–жила»:

$$\dot{U}_{\text{ж–об}}(\omega)=\dot{I}_{\text{экр}}(\omega)\cdot\dot{Z}_{\text{св}}(\omega); \quad (4)$$

$$\dot{U}_{\text{ж–ж}}(\omega)=\dot{U}_{\text{ж–об}}(\omega)\cdot\eta(\omega), \quad (5)$$

где $\dot{Z}_{\text{св}}(\omega)$ – сопротивление связи [7], показывающее проникновение электромагнитной энергии внутрь кабеля, Ом; η – коэффициент чувствительности двухпроводной цепи [8], наиболее точные его значения определяются экспериментально.

На рис. 6 приведены временные зависимости наведенных токов и напряжений в симметричном экранированном кабеле от импульса электрического поля с параметрами длительности 6,4/16 мкс и амплитудой 100 В/м. Экран кабеля соединен с корпусами блоков аппаратуры, но блоки не заземлены ($p_{\text{н}}$ = 0, $p_{\text{к}}$ = 0). Расчет проведен в частотной области, затем выполнено обратное преобразование Фурье.

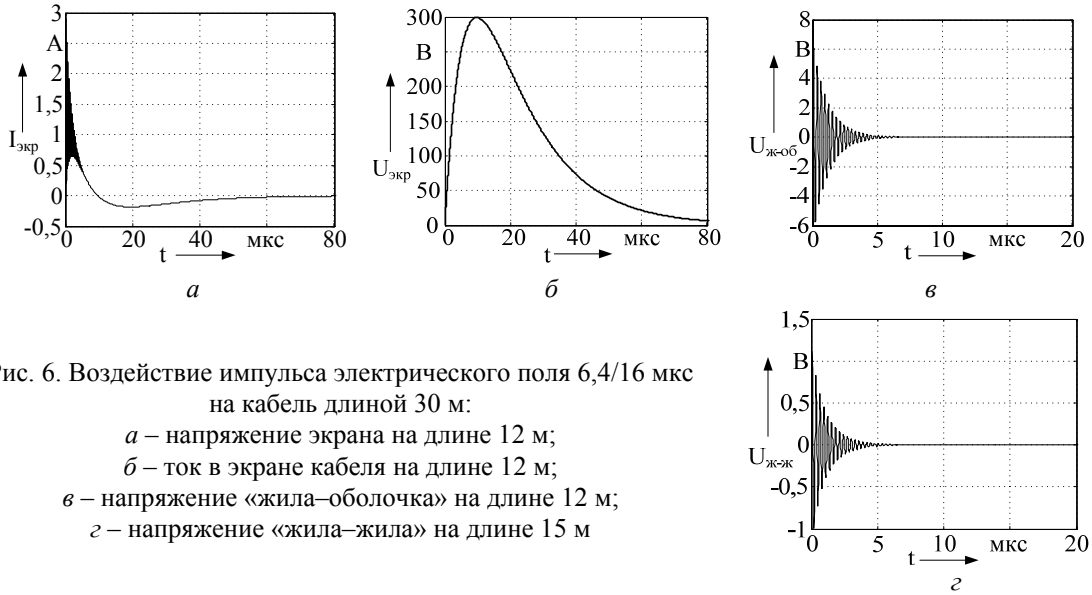


Рис. 6. Воздействие импульса электрического поля 6,4/16 мкс на кабель длиной 30 м:
а – напряжение экрана на длине 12 м;
б – ток в экране кабеля на длине 12 м;
в – напряжение «жила–оболочка» на длине 12 м;
г – напряжение «жила–жила» на длине 15 м

Графики на рис. 6 свидетельствуют о том, что напряжения «жила–оболочка» и «жила–жила» не достигают значений, способных вывести аппаратуру из строя, но могут повлиять на качество передачи информационных сигналов. Несмотря на небольшую длину кабеля 30 м, наведенное напряжение в экране достигает уровня, при котором возможно опасное воздействие на цепи, имеющие гальваническую связь с экраном кабеля или корпусом аппаратуры.

Заключение. Проведенная работа показала, что использованный подход в исследовании защищенности отдельных частей радиоэлектронных систем к электромагнитным полям позволяет опре-

делить эффективность применяемых защитных средств (экранирование), а также оценить степень дестабилизирующего воздействия, связанного с появлением мощных электромагнитных помех.

Литература

1. Кравченко В.И. Радиоэлектронные средства и мощные электромагнитные помехи / В.И. Кравченко, Е.А. Болотов, Н.И. Летунов. – М.: Радио и связь, 1987. – 256 с.

2. Taflove A. Computational electrodynamics: The finite-difference time-domain method. Second edition / A. Taflove, S.C. Hagness. – Boston: Artech House, 2000. – 866 p.

3. Методика расчета эффективности экранирования радиоэлектронной аппаратуры при воздействии импульсных электромагнитных полей / В.Е. Митрохин, А.В. Ряполов, А.Е. Гаранин // Известия Транссиба. – 2014. – № 1 (17). – С. 72–78.

4. Hybrid numerical technique to predict the electromagnetic field in penetrable conductive boxes / M. Feliziani, F. Maradei // Electromagnetics. – 2002. – Vol. 22. – P. 405–417.

5. Гроднев И.И. Электромагнитное экранирование в широком диапазоне частот. – М.: Связь, 1972. – 112 с.

6. Михайлов М.И. Электромагнитные влияния на сооружения связи / М.И. Михайлов, Л.Д. Разумов, С.А. Соколов. – М.: Связь, 1979. – 264 с.

7. Вэнс Э.Ф. Влияние электромагнитных полей на экранированные кабели. – М.: Радио и связь, 1982. – 120 с.

8. Ряполов А.В. Разработка методики расчета электромагнитного влияния на кабель конечной длины в широком диапазоне частот / А.В. Ряполов, В.Е. Митрохин // Радиотехника, электроника и связь: сб. докладов II Междунар. науч.-техн. конф. ВТТВ РЭиС–2013 (Омск). – 2013. – С. 214–220.

Митрохин Валерий Евгеньевич
Д-р техн. наук, профессор, зав. каф. инфокоммуникационных систем и информационнй безопасности Омского государственного университета путей сообщения (ОмГУПС)
Тел.: 8 (381-2) 31-06-94
Эл. почта: mitrokhin@list.ru

Ряполов Артём Владимирович
Аспирант, инженер каф. инфокоммуникационных систем и информационной безопасности ОмГУПС
Тел.: 8 (381-2) 31-06-94
Эл. почта: a.v.ryapolov@gmail.com

Mitrokhin V.E., Ryapolov A.V.

The immunity of the radio electronic system under impact of destabilizing electromagnetic field

The sustainability of the radio electronic system in presence of destabilizing external electromagnetic field is evaluated. The efficiency of the shielding enclosures with technological holes is investigated. The occurrence of induced voltages and currents in the cable connections from pulsed electromagnetic field is researched.

Keywords: electromagnetic compatibility, shielding, cable connection, pulsed electromagnetic field, induced voltage.

УДК 004.056.5

С.Н. Новиков

Методологические аспекты защиты информации с использованием ресурсов мультисервисных сетей связи

Предлагаются методологические основы комплексной защиты пользовательской информации (обеспечение конфиденциальности, целостности и доступности) на базе технологий сетевого уровня (протоколов маршрутизации и сигнализации) мультисервисных сетей связи.
Ключевые слова: конфиденциальность, целостность, доступность, маршрутизация.

Одним из путей обеспечения комплексной защиты информации (ЗИ) без снижения QoS является использование ресурсов мультисервисных сетей связи (МСС) (каналов связи, криптографических комплексов, баз данных и т.д.). В этом случае пользователь не обязательно должен обладать знаниями в области ЗИ и иметь специальное программно-аппаратное обеспечение. Ему достаточно определить свой профиль ЗИ (количественные оценки конфиденциальности, целостности и доступности). Система управления, проведя мониторинг свободных ресурсов МСС, реализует не только соединение, поддерживающее QoS для выбранного приложения, но и заявленный пользователем профиль. Реализация данного подхода возможна за счет протоколов маршрутизации и сигнализации.

Обеспечение комплексной ЗИ с использованием ресурсов МСС. В криптосистемах с открытым ключом отсутствует закрытый канал связи, и это упрощает проблему сеансовых ключей. Однако такие алгоритмы имеют особенности: для достижения аналогичной криптостойкости с симметричными алгоритмами требуется более длинный ключ; зависимость времени шифрования от длины ключа L_k имеет нелинейный характер и в общем случае определяется $t_{\text{ш}} = AL_k^c + B$, где $t_{\text{ш}}$ – время зашифрования; A, B и c – постоянные, значения которых определяются криптографическими алгоритмами. Оба фактора значительно ограничивают применение асимметричных криптосистем в МСС, так как существует критичная длина ключа $L_{k\ \text{кр}}$, превышение которой приведет к недопустимому увеличению $t_{\text{ш}}$ и как следствие к снижению QoS высокоскоростных приложений, функционирующих в реальном масштабе времени. *Конфиденциальность информации* и QoS высокоскоростных приложений предлагается обеспечить за счет многократного вложения асимметричных, криптографических алгоритмов шифрования [1]

$$y = E_{k_l}\left\{...E_{k_i}...[E_{k_1}(M)]\right\};\quad M = D_{k_1}\left\{...D_{k_i}[...D_{k_l}(y)]\right\}. \tag{1}$$

Здесь: $y = E_k(M)$, $M = D_k(y)$ – соответственно, зашифрование открытой информации M и расшифрование закрытой информации y с помощью независимых ключей $k_i; i = \overline{1,l}$; l – количество «вложенных» алгоритмов шифрования. Время шифрования (1) с учетом рис. 1 определяется

$$t_{\text{ш сост}} = l\left(\ A\frac{L_{k\ \text{сост}}}{l}\ \right)^c + B = \frac{A^c L_{k\ \text{сост}}^c}{l^{c-1}} + B, \tag{2}$$

при общей длине составного ключа $L_{k_{\text{сост}}} = \sum_{i=1}^{l} L_{k_i}$; $L_{k_i} = \text{const}$. Временной выигрыш применения «составного» ключа по отношению к зашифрованию одним «длинным» составит

$$\frac{t_{\text{ш}}}{t_{\text{ш сост}}} = \frac{AL_{k\ \text{сост}}^c + B}{l\left(A\left(\frac{L_{k\ \text{сост}}}{l}\right)^c + B\right)} = \frac{AL_{k\ \text{сост}}^c + B}{lA\left(\frac{L_{k\ \text{сост}}}{l}\right)^c + lB} = \frac{AL_{k\ \text{сост}}^c}{lA\left(\frac{L_{k\ \text{сост}}}{l}\right)^c} = l^{c-1}. \tag{3}$$

Результаты натурного эксперимента зашифрования алгоритмом RSA блока данных объемом 1 Кбайт при изменении длины ключа от 256 до 2048 бит; использовании составного 256-битного ключа подтвердили теоретическое предположение (3) [2].

Целостность и доступность информации предлагается обеспечить за счет организации n параллельных соединений между узлом-источником (УИ) и узлом-получателем (УП) в МСС [2]. Пусть передаются сообщения $M=\{M_1,M_2\}$ с априорными вероятностями $P(M_1)$ и $P(M_2)$; $P_{\text{м}}^{(i)}$ – вероятность модификации сообщения $M=\{M_1,M_2\}$ в i-м соединении ($i=\overline{1,n}$). Обеспечение целостности информации сводится к процессу принятия решения в точке приема по n одновременно принятым сообщениям $x=(x_1,...,x_i,...,x_n)$. Таким образом, на выходе решающего устройства (РУ) значение M^* будет соответствовать переданному сообщению $M=\{M_1,M_2\}$.

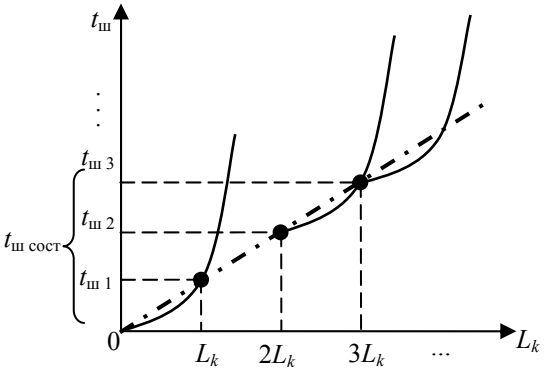


Рис. 1. Зависимости времени зашифрования от длины составного ключа

Условные вероятности, что на выходе РУ будет M_1 или M_2:

$$P\left(M_1/\left(x_i;i=\overline{0,n}\right)\right)=\frac{P(M_1)\left\{\prod\limits_{i\in x_i=M_1}\left(1-P_{\text{м}}^{(i)}\right)\prod\limits_{i\in x_i=M_2}P_{\text{м}}^{(i)}\right\}}{P\left(x_i;i=\overline{0,n}\right)};$$

$$P\left(M_2/\left(x_i;i=\overline{0,n}\right)\right)=\frac{P(M_2)\left\{\prod\limits_{i\in x_i=S_1}P_{\text{м}}^{(i)}\prod\limits_{i\in x_i=S_2}\left(1-P_{\text{м}}^{(i)}\right)\right\}}{P\left(x_i;i=\overline{0,n}\right)}.$$

Возьмем отношение этих выражений, прологарифмируем и обозначим

$$a_0=\ln\frac{P(M_1)}{P(M_2)};\quad a_i=\ln\frac{\left(1-P_{\text{м}}^{(i)}\right)}{P_{\text{м}}^{(i)}}. \tag{4}$$

В результате получим

$$\ln\frac{P\left\{M_1/\left(x_i;i=\overline{0,n}\right)\right\}}{P\left\{M_2/\left(x_i;i=\overline{0,n}\right)\right\}}=a_0+\sum_{i=1}^{n}x_ia_i. \tag{5}$$

Таким образом, правило принятия решения на выходе РУ имеет вид

$$a_0+\sum_{i=1}^{n}x_ia_i\begin{cases}\text{если}>0\Rightarrow M^*=M_1;\\ \text{если}<0\Rightarrow M^*=M_2.\end{cases} \tag{6}$$

Функциональная схема РУ представлена на рис. 2.

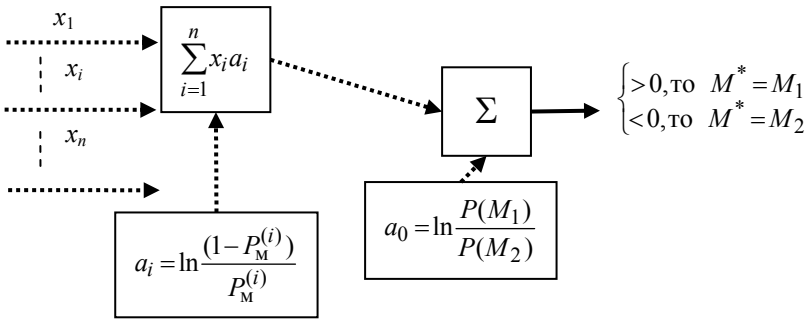


Рис. 2. Функциональная схема РУ

Вероятность целостности информации на выходе РУ при условии, что n – нечетно и $P_{\text{м}} = P_{\text{м}}^{(i)}$; $i = \overline{1,n}$ – независимые события, определяется

$$P_{\text{Ц РУ}} = 1 - \sum_{i=0}^{\frac{n-1}{2}} C_n^{\frac{n+1+2i}{2}} (1-P_{\text{м}})^{\frac{n-1-2i}{2}} P_{\text{м}}^{\frac{n+1+2i}{2}}. \quad (7)$$

Численные оценки целостности информации на выходе решающего устройства представлены на рис. 3. Статистическое моделирование работы РУ подтверждает теоретические расчеты (7).

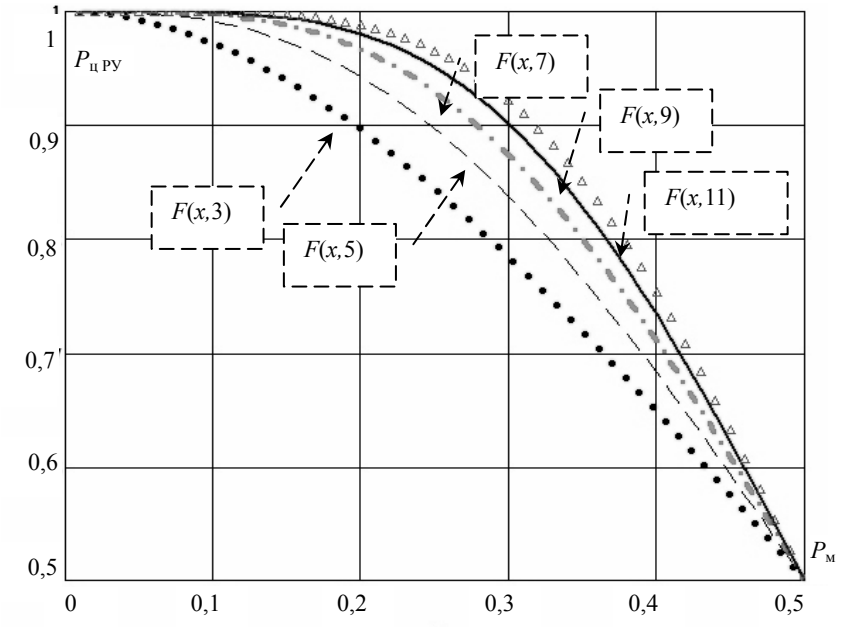


Рис. 3. График $P_{\text{ц РУ}} = f(P_{\text{м}})$ при различных n

Базовым методом обеспечения доступности информации является резервирование и дублирование как самих каналов связи, так и информации, к которой осуществляется доступ, т.е. за счет организации параллельных соединений между УИ и УП информации. В данном случае важно определить *критерий выбора минимальных по стоимости ресурсов МСС* для обеспечения требуемой пользователем доступности информации [3].

Введем обозначения: $c_{\text{Д}}^{(i)}$ – стоимость i-го соединения между УИ и УП, организованного для обеспечения доступности информации; $P_{\text{Д}}^{(i)}$ – вероятность обеспечения доступности информации i-го соединения ($i = \overline{1,n}$). Тогда общая стоимость организации параллельных соединений составит

$$c_{\text{Д}} = \sum_{i=1}^{n} c_{\text{Д}}^{(i)}. \quad (8)$$

Предположим, что атаки на каждое соединение независимы. Тогда результирующая вероятность обеспечения доступности определяется выражением

$$P_{\text{Д}}^{(\text{рез})} = 1 - \prod_{i=1}^{n} \left(1 - P_{\text{Д}}^{(i)}\right). \quad (9)$$

Обозначим

$$Q_{\text{Д}}^{(i)} = 1 - P_{Д}^{(i)},\ Q_{\text{Д}}^{(\text{рез})} = 1 - P_{\text{Д}}^{(\text{рез})}. \quad (10)$$

Тогда

$$Q_{\text{Д}}^{(\text{рез})} = \left[Q_{\text{Д}}^{(i)} \right]^n. \quad (11)$$

Прологарифмируем обе части выражения (11):

$$\ln Q_{\text{Д}}^{(\text{рез})} = n \ln Q_{\text{Д}}^{(i)}. \quad (12)$$

Допустим, что все параллельные соединения одинаковы по стоимости:

$$c_{\text{Д}} = n c_{\text{Д}}^{(i)}. \quad (13)$$

Разделим (12) на $c_{\text{Д}}$, с учетом (13) и (10) получим

$$\ln \frac{Q_{\text{Д}}^{(\text{рез})}}{c_{\text{Д}}} = \frac{\ln\left(1 - P_{\text{Д}}^{(i)}\right)}{c_{\text{Д}}^{(i)}}. \quad (14)$$

Из (14) следует вывод, что оптимальным соединением с точки зрения доступности информации при минимальной стоимости $c_{\text{Д}}^{(i)}$ будет то, у которого следующее отношение максимально:

$$k_{\text{Д}}{}^{(i)} = \left| \frac{\ln(1 - P_{\text{Д}}^{(i)})}{c_{\text{Д}}{}^{(i)}} \right|. \quad (15)$$

Методика комплексной ЗИ. Реализация вышеизложенного подхода, обеспечивающего комплексную ЗИ, возможна за счет механизмов сетевого уровня МСС [4, 7] (протоколов маршрутизации и сигнализации) (рис. 4).

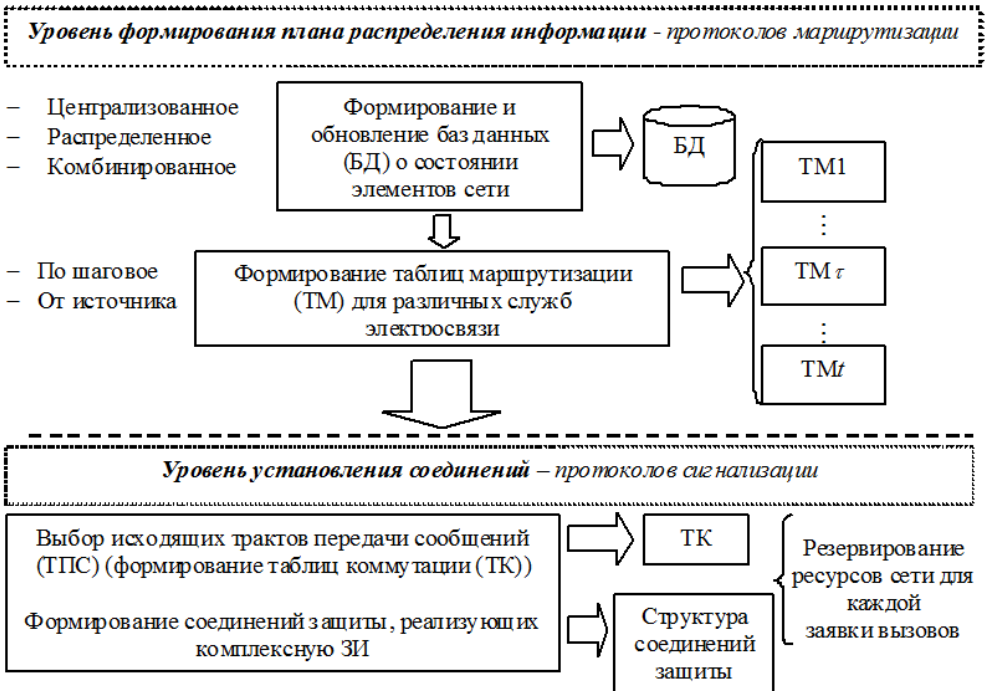


Рис. 4. Обобщенная функциональная модель маршрутизации в МСС

Основным продуктом уровня формирования ПРИ являются ТМ для каждой службы электросвязи $\left(\tau = \overline{1,t}\right)$ (приложения МСС). При этом применяются соответствующие методы мониторинга МСС, формирования и коррекции БД, которые по степени централизации можно классифицировать на централизованные, распределенные и комбинированные.

Уровень сигнализации, используя методы выбора исходящих ТПС, по сформированным ТМ формирует во всех транзитных узлах коммутации (УК), начиная с узла-источника (УИ):

– ТК для каждой заявки на установление соединения с требуемым QoS приложений МСС;

– структуру соединений защиты с целью выполнения требований пользователей к степени защищенности передаваемой информации (конфиденциальности, доступности, целостности).

Передача сообщений пользователей осуществляется по таблицам коммутации, которые сформированы на уровне системы сигнализации.

Таким образом, протоколы сетевого уровня (маршрутизации и сигнализации), проведя мониторинг свободных ресурсов МСС, реализуют не только соединение, поддерживающее QoS для выбранного приложения, но и заявленный пользователем профиль комплексной ЗИ.

Математическая модель анализа маршрутизации в МСС. В работе [4] проведена попытка систематизировать и обобщить известные решения, реализованные в технологиях IP, ATM и MPLS. В результате была предложена новая классификация методов маршрутизации, позволяющая, комбинируя известные методы формирования ПРИ и выбора исходящих ТПС, разработать новые методы маршрутизации.

«Логико-статистический» – сочетание «логического» и «статистического» методов формирования ПРИ. В условиях отсутствия внешних деструктурирующих воздействий на МСС формирование ПРИ осуществляется «статистическим» методом. В условиях резкого изменения структуры МСС (по каким-либо причинам) применяется «логический» метод.

«Логико-лавинный» – сочетание «лавинного» и «логического» методов состоит в том, что для установления оптимального соединения из УИ организуется «лавинный» поиск, но не во всех направлениях, а лишь в сторону УП. Волна поиска при этом распространяется в пределах некоторой зоны в виде полосы, охватывающей УИ и УП. Ширина, форма полосы зависят от приоритета пользователя, состояния элементов сети, требований приложений к QoS и могут устанавливаться в различных пределах. В частности, для пользователей низшей категории количество выбранных ТПС может не превышать одного, тогда поиск превращается в «чисто» последовательный.

«Логико-лавинно-статистический» – обобщение «логического», «лавинного» и «статистического». Применение одного из перечисленных методов зависит от условий функционирования МСС. В условиях отсутствия внешних деструктурирующих воздействий на МСС формирование ПРИ осуществляется «статистическим» методом. В условиях резкого изменения структуры МСС (по каким либо причинам) применяется «логико-лавинный» метод.

В этой связи с целью определения оптимальных методов маршрутизации возникает необходимость в разработке математической модели [5] функционирования МСС в условиях внешних деструктурирующих воздействий.

Структуру МСС представим в виде неориентированного графа $G[A_S, M_S]$ с множеством: вершин $A_S = \{a_i\};\ i = \overline{1,S}$ – УК; ребер $M_S = \{m_{ij}\};\ i,j = \overline{1,S};\ i \neq j$ – линий связи (ЛС). ПРИ в МСС задается в виде набора векторов

$$P^{(j)} = \left\| p_{i,v}^{(j)} \right\|_{(S-1),H_j} = \left(\overline{p_1^{(j)}}, \ldots, \overline{p_i^{(j)}}, \ldots, \overline{p_{j-1}^{(j)}}, \overline{p_{j+1}^{(j)}}, \ldots, \overline{p_S^{(j)}} \right), \quad (16)$$

где $P_i^{(j)} = (p_{i,v}^{(j)});\ \sum_{v=1}^{H_j} p_{i,v}^{(j)} v = \overline{1,H_j};\ i,j = \overline{1,S};$ H_j – степень a_j-го УК. Элементы вектора $\overline{p_i^{(j)}}$ определяют вероятность того, что на этапе поиска маршрута к a_j-му УП в a_i-м транзитном УК, начиная с УИ, будет выбрана v-я исходящая ЛС. Выражение (16) и процедура выбора исходящих ТПС определяют метод маршрутизации (M).

Поступающий в МСС поток данных τ-го приложения считается самоподобным

$$f(x) = \begin{cases} \dfrac{\lambda_{\tau,R,T}^{H_\tau} \cdot x^{H_\tau - 1} \cdot e^{-\lambda_{\tau,R,T} \cdot x}}{\Gamma(H_\tau)}; R,T = \overline{1,S}; R \neq T; \tau = \overline{1,t}; x \geq 0; \\ 0, \qquad x < 0, \end{cases}$$

где $\Gamma(H_\tau) = \int_0^\infty x^{H_\tau - 1} e^{-t} dx$ – гамма-функция с параметрами: $\lambda_{\tau,R,T}$ – интенсивность поступления потока данных τ-го приложения в a_R-й УИ для передачи в a_T-й УП; $0{,}5 < H_\tau \leq 1$ – параметр Херста. Интенсивность потока данных τ-го приложения составит $\lambda_\tau = \sum_{R,T=1}^{S} \lambda_{\tau,R,T}$. Вероятность поступления потока данных τ-го приложения в a_R-й УИ для его последующей передачи a_T-му УП будет

$$\Pi\tau=\left\|\pi_{\tau,R,T}\right\|_{S,S};\ \ 0\le\pi_{\tau,R,T}=\frac{\lambda_{\tau,R,T}}{\lambda_\tau}\le 1;\ \ \sum_{R,N=1}^{S}\pi_{\tau,R,T}=1;\ \ \tau=\overline{1,t}.$$

Длительность обслуживания входящего потока данных τ-го приложения подчиняется экспоненциальному закону с параметром μ_τ. Критерием оценки качества функционирования МСС принята

$$\{\hat{P}^{\tau}_{\text{отк}};\ \hat{p}^{(R,T)\tau}_{\text{отк}}\}=f\{G[A_S,M_S];\ \Pi_\tau;\ \lambda_\tau;\ \mu_\tau;\ M\};\ \ R,T=\overline{1,T};\ \ R\ne T;\ \ \tau=\overline{1,t}\ ; \qquad (17)$$

$\hat{P}^{(R,T)\tau}_{\text{отк}};\ R,T=\overline{1,T};\ R\ne T;\ \tau=\overline{1,t}$ – вероятность отказа в обслуживании τ-го приложения между УИ (a_R) и УП (a_T) – дифференциальная оценка; $\hat{P}^{\tau}_{\text{отк}}$ – вероятность отказа в обслуживании τ-го приложения в среднем по сети – интегральная оценка.

Методика оценки (17) состоит в решении следующей системы уравнений (18):

$$\begin{cases}
P^{(M)}_{(T)}=\left\|p^{(M)j}_{(T)i}\right\|_{S,S};\ \ i,j=\overline{1,S};\ \ i\ne j;\\
\lambda^{(M)j}_{0\ \tau,i}=\lambda_\tau\cdot\sum\limits_{T=1}^{S}p^{(M)j}_{(T)i}\cdot\pi_{\tau,i,j};\quad i,j=\overline{1,S};i\ne j;\\
p^{(M)j}_{\tau,i}=\dfrac{\left(1-\dfrac{\rho^{(M)}_{\tau,i,j}}{4}-\sqrt{\dfrac{\rho^{(M)}_{\tau,i,j}{}^2}{16}+\dfrac{\rho^{(M)}_{\tau,i,j}}{2}}\right)}{1-\left(\dfrac{\rho^{(M)}_{\tau,i,j}}{4}+\sqrt{\dfrac{\rho^{(M)}_{\tau,i,j}{}^2}{16}+\dfrac{\rho^{(M)}_{\tau,i,j}}{2}}\right)^2}\left(\dfrac{\rho^{(M)}_{\tau,i,j}}{4}+\sqrt{\dfrac{\rho^{(M)}_{\tau,i,j}{}^2}{16}+\dfrac{\rho^{(M)}_{\tau,i,j}}{2}}\right);\\
P^{\tau}_{\text{отк}}=\sum\limits_{k=1}^{2^n}Q^{(k)}_{\text{o}}\cdot\prod\limits_{\nu=1}^{n}\left(q_\nu^{\sigma_\nu}\cdot p_\nu^{1-\sigma_\nu}\right);\ \ R,T=\overline{1,S};\ \ \tau=\overline{1,t}\ ;\\
P^{(R,T)\tau}_{\text{отк}}=\sum\limits_{k=1}^{2^n}Q^{(k)}_{RT}\cdot\prod\limits_{\nu=1}^{n}\left(q_\nu^{\sigma_\nu}\cdot p_\nu^{1-\sigma_\nu}\right);\ \ R,T=\overline{1,S};\ \ \tau=\overline{1,t}\ .
\end{cases} \qquad (18)$$

Здесь $p^{(M)j}_{(T)i}$ – вероятность перехода из состояния a_i в a_j конечной цепи Маркова (КЦМ) для M-го метода маршрутизации при поиске a_T-го УК; a_T – поглощающее, т.е. $p^{(M)T}_{(T)T}=1$; $P^{(M)}_{(T)}=\left\|p^{(M)j}_{(T)i}\right\|_{S,S}$ – матрица переходных вероятностей (КЦМ); $\lambda^{(M)j}_{0\ \tau,i}=\lambda_\tau\cdot\sum\limits_{T=1}^{S}p^{(M)j}_{(T)i}\cdot\pi_{\tau,i,j}=\sum\limits_{T=1}^{S}\lambda^{(M)j}_{(T)\tau,i};\ \overline{1,S};\ i\ne j$ – общая интенсивность потоков τ-го приложения в $m_{i,j};\ i,j=\overline{1,S};\ i\ne j$; $\lambda^{(M)j}_{(T)\tau,i}=p^{(M)j}_{(T)i}\cdot\lambda_{\tau,i,T};\ i,j=\overline{1,S};\ i\ne j$ – интенсивность потока τ-го приложения в $m_{i,j};\ i,j=\overline{1,S};\ i\ne j$ при поиске a_T-го УК M-м методом маршрутизации; $p^{(M)j}_{\tau,i}$ – вероятность отказа в обслуживании τ-го приложения в $m_{i,j};\ i,j=\overline{1,S};\ i\ne j$ определяется по формуле, предложенной в [6]; n – количество ребер графа $G[A_S,M_S]$; $k=\overline{1,2^n}$ – количество состояний графа $G[A_S,M_S]$; $Q^{(k)}_o$ и $Q^{(k)}_{ij}$ переменные, принимающие значения 1, если граф, находясь в k-м, соответственно, будет «связен» – обеспечивает связность вершин a_i и a_j. В противном случае переменные равны 0.

Анализ результатов решения системы уравнений (18) методом статистического моделирования позволяет сделать вывод – в условиях выхода элементов МСС из строя более 30% параллельных методов маршрутизации показывают лучшую оценку параметра (17).

Заключение. На основе проведенных исследований возможно сделать следующие выводы:

– Разработаны методологические основы комплексной защиты пользовательской информации (обеспечение конфиденциальности, целостности и доступности) на базе технологий сетевого уровня (протоколов маршрутизации и сигнализации) мультисервисных сетей связи.

– Разработана математическая модель функционирования МСС в условиях внешних деструктурирующих воздействий и самоподобного трафика.

– В условиях выхода элементов МСС из строя более 30% параллельных методов маршрутизации дают лучшую оценку вероятности отказа в обслуживании приложений между УИ и УП.

Литература

1. Алгоритм, позволяющий обеспечить требуемый пользователем уровень конфиденциальности информации в мультисервисных сетях связи / С.Н. Новиков, О.И. Солонская: Свидетельство о регистрации электронного ресурса в объединенном фонде электронных ресурсов «Наука и образование» Института научной информации и мониторинга РАО, № 16462 от 6 декабря 2010 г., ВНТИЦ инв. № 50201050230 от 08.12.2010 г.

2. Пат. 2 513 725 РФ, МПК G 06 F 11/00. Способ обеспечения целостности передаваемой информации / С.Н. Новиков, О.И. Солонская (РФ). – № 2 012 122 695 / 08; заявл. 01.06.12; опубл. 20.04.14. – Бюл. № 11. – 17 с.

3. Алгоритм, позволяющий обеспечить требуемый пользователем уровень доступности информации / С.Н. Новиков, О.И. Солонская: Свидетельство о регистрации электронного ресурса в объединенном фонде электронных ресурсов «Наука и образование» Института научной информации и мониторинга РАО, № 16227 от 29 сентября 2010 г., ВНТИЦ инв. № 50201001615 от 05.10.2010 г.

4. Новиков С.Н. Классификация методов маршрутизации в мультисервисных сетях связи // Вестник СибГУТИ. – 2013. – № 2 (25). – С. 92–96.

5. Novikov S.N. The Analysis of Probability Time Characteristics of a Telecommunication Network / S.N. Novikov, A.A. Burov // The IEEE International Siberian Conference on Control and Communications (SIBCON-2005). – Russia, Tomsk, 2005. – P. 26–29.

6. Самоподобие в системах массового обслуживания с ограниченным буфером / М.Н. Петров, Д.Ю. Пономарев // Электросвязь. – 2002. –№ 2. – С. 35–39.

7. Исхаков С.Ю. Разработка методического и программного обеспечения для мониторинга работы локальных сетей / С.Ю. Исхаков, А.А. Шелупанов // Телекоммуникации. – 2013. – № 6. – С. 16–20.

Новиков Сергей Николаевич
Канд. техн. наук, доцент, зав. каф. безопасности и управления в телекоммуникациях СибГУТИ,
г. Новосибирск
Тел.: +7 (383) 269-82-45
Эл. почта: snovikov@ngs.ru

Novikov S.N.

Methodological aspects of data protection with the use of resources multiservice networks

The methodological basis of complex protection of user information (ensuring the confidentiality, integrity and availability) technology-based cross-tevogo level (routing and signaling protocols) multiservice networks are proposed.

Keywords: confidentiality, integrity, availability, routing.

УДК 004.056

С.И. Носков, А.А. Бутин, Л.Е. Соколова

Многокритериальная оценка уровня уязвимости объектов информатизации

Рассматривается формализованный способ оценки уязвимости объектов информатизации. Он предполагает построение агрегированного критерия уровня уязвимости в виде линейной свертки локальных критериев с применением методов теории принятия решений. При этом задача определения коэффициентов свертки сводится к поиску решения или квазирешения задачи линейного программирования. Предложен алгоритм оценки уровня компетентности привлекаемых экспертов.

Ключевые слова: информационная безопасность, уязвимость, линейное программирование, квазирешение, теория принятия решений, экспертная информация.

При создании инфраструктуры объектов информатизации (ОИ) на базе современных компьютерных систем и сетей неизбежно возникает вопрос их защищенности от различных угроз. Эти угрозы как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости, приводящие к нарушению безопасности информации на конкретном ОИ. Уязвимости неотделимы от ОИ и обусловливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и физического расположения.

Перечисленные обстоятельства диктуют настоятельную необходимость создания фундаментальной научной методологии комплексной оценки уровня безопасности ОИ. Представляется, что основой такой методологии могут и должны стать современные методы математического моделирования. Они являются признанным инструментом научного анализа сложных, с множеством внутренних и внешних взаимосвязей объектов различной природы, поскольку позволяют на модельном уровне формализовывать закономерности, присущие этим объектам, посредством разработки их качественных абстрактных образов. Это открывает широкие возможности в повышении эффективности вырабатываемых управляющих воздействий, поскольку при этом экспериментирование может проводиться не с «живой» системой, а с её математической моделью.

Этапом, предваряющим собственно настроение математической модели любого объекта, является выбор показателей (факторов, переменных), определяющих его функционирование. К сожалению, к настоящему времени как в научных, так и в нормативных изданиях не описан (не определен, не задан, не формализован) какой-либо один показатель (фактор), в полной мере отражающий уровень (степень, меру) уязвимости ОИ. Вместе с тем известны частные характеристики ОИ, «отвечающие» за те или иные локальные стороны в оценке такой комплексной уязвимости. Так, например, в работе [1] для удобства анализа отдельные уязвимости разделены на классы (они обозначаются заглавными буквами), которые, в свою очередь, распадаются на группы (обозначаются римскими цифрами), а последние – на подгруппы (обозначаются строчными буквами). Определено три класса: [A] объективные, [B] субъективные и [C] случайные уязвимости.

При этом объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-физическими методами парирования угроз безопасности информации.

К ним можно отнести:

[A.I] сопутствующие техническим средствам излучения:

- [A.I.a] электромагнитные (побочные излучения элементов и кабельных линий технических средств (ТС), излучения на частотах работы генераторов, на частотах самовозбуждения усилителей);
- [A.I.b] электрические (наводки электромагнитных излучений на линии и проводники, просачивание сигналов в цепи электропитания, в цепи заземления, неравномерность потребления тока электропитания);

• [A.I.c] звуковые (акустические, виброакустические);

[A.II] активизируемые:

• [A.II.a] аппаратные закладки (устанавливаемые в телефонные линии, в сети электропитания, в помещениях, в ТС);

• [A.II.b] программные закладки (вредоносные программы, технологические выходы из программ, нелегальные копии программного обеспечения (ПО));

[A.III] определяемые особенностями элементов:

• [A.III.a] элементы, обладающие электроакустическими преобразованиями (телефонные аппараты, громкоговорители и микрофоны, катушки индуктивности, дроссели, трансформаторы и пр.);

• [A.III.b] элементы, подверженные воздействию электромагнитного поля (магнитные носители, микросхемы, нелинейные элементы, подверженные высокочастотному навязыванию);

[A.IV] определяемые особенностями защищаемого объекта:

• [A.IV.a] местоположением объекта (отсутствие контролируемой зоны, наличие прямой видимости объектов, удаленных и мобильных элементов объекта, вибрирующих отражающих поверхностей);

• [A.IV.b] организацией каналов обмена информацией (использование радиоканалов, глобальных открытых информационных сетей, арендуемых каналов).

Субъективные уязвимости зависят от действий сотрудников и в основном устраняются организационными методами и программно-аппаратными средствами:

[B.I] ошибки:

• [B.I.a] при подготовке и использовании ПО (в том числе при разработке алгоритмов и ПО, его инсталляции, загрузке, эксплуатации, вводе данных);

• [B.I.b] при управлении сложными системами (при использовании возможностей самообучения систем, настройке сервисов универсальных систем, организации управления потоками информации);

• [B.I.c] при эксплуатации ТС (при включении/выключении ТС, использовании средств охраны и средств обмена информацией);

[B.II] нарушения:

• [B.II.a] режима охраны и защиты (доступа на объект и к ТС);

• [B.II.b] режима эксплуатации ТС (энергообеспечения, жизнеобеспечения);

• [B.II.c] режима использования информации (обработки и обмена информацией, хранения и уничтожения носителей, уничтожения производственных отходов и брака);

• [B.II.d] режима конфиденциальности (уволенными, а также сотрудниками в нерабочее время).

Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, малопредсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам информационной безопасности. К ним можно отнести:

[C.I] сбои и отказы:

• [C.I.a] отказы и неисправности ТС (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, охрану и контроль доступа);

• [C.I.b] старение и размагничивание носителей информации (дискет, съемных носителей, жестких дисков, элементов микросхем, кабелей и соединительных линий);

• [C.I.c] сбои ПО (операционных систем и СУБД, прикладных, сервисных и антивирусных программ);

• [C.I.d] сбои электроснабжения (оборудования, обрабатывающего информацию, обеспечивающего и вспомогательного оборудования);

[C.II] повреждения:

• [C.II.a] жизнеобеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации, кондиционирования и вентиляции);

• [C.II.b] ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий, корпусов технологического оборудования).

В рамках теории принятия решений разработан целый спектр методов, позволяющих объединять частные характеристики (критерии, показатели уязвимостей) объектов различной природы в некие ненаблюдаемые в реальности агрегаты (свертки), что позволяет оценивать обобщенные свойства объектов (в нашем случае уязвимость (ОИ) (см., например, [2–6]). Будем основывать дальнейшее изложение в основном на работах [5, 6], в которых представлена методика объединения локальных критериев в обобщенные агрегаты с использованием аппарата линейного программирования.

Итак, пусть в распоряжении исследования есть численная информация о g критериях уязвимости r элементов отдельного объекта информатизации, т.е. матрица $\mathbf{X}=\left\|x_{ij}\right\|,i=\overline{1,r},j=\overline{1,g}$.

Пусть к оценке уязвимости каждого элемента ОИ привлечены p экспертов. На основе использования их сравнительных высказываний и матрицы **X** необходимо построить линейную свертку частных критериев (агрегированный критерий) вида

$$R=\sum_{j=1}^{g}\alpha_j x_j, \tag{1}$$

где j – номер частного критерия.

Далее организуется процедура независимого опроса экспертов относительно сравнительной уязвимости пар ОИ. При этом каждый эксперт производит свою оценку только по отношению к парам, уязвимость ОИ в которых он может с уверенностью сравнить.

Каждый i-й эксперт строит индексное множество $M^i=\left\{(a_1^i,b_1^i),(a_2^i,b_2^i),...,(a_{l_i}^i,b_{l_i}^i)\right.$ пар объектов, в которых первый объект более (не менее) уязвим, чем второй, и множество $N^i=\left\{(c_1^i,d_1^i),(c_2^i,d_2^i),...,(c_{s_i}^i,d_{s_i}^i)\right\}$ пар объектов, уязвимость которых, по мнению эксперта, «примерно» одинакова, $i=\overline{1,p}$.

Здесь l_i и S_i – размерность множеств M_i и N_i соответственно. При этом не исключаются ситуации, когда какое-то из множеств N_i или M_i оказывается пустым, поскольку эксперт может затрудниться в указании требуемых пар.

В случае непротиворечивости экспертных высказываний должны быть совместны системы линейных равенств и неравенств

$$R(C_j^i)=R\left(d_j^i\right),i=\overline{1,p},j=\overline{1,l_i} \tag{2}$$

$$R(a_j^i)\geq R\left(b_j^i\right),i=\overline{1,p},j=\overline{1,S_i} \tag{3}$$

где через $R(k)$ обозначена уязвимость k-го объекта, $k=\overline{1,r}$.

Сделаем одну необходимую оговорку. А именно, чем больше значение $R(k)$, тем выше уязвимость k-го элемента объекта. Значит, для достижения однородности обобщенного и частных критериев необходимо полагать, что каждый фактор x_j позитивно влияет на уязвимость, т.е. усиливает (увеличивает) ее. А в приведенном выше перечне частных характеристик уязвимости ОИ есть такие, которые уязвимость снижают. Такие характеристики x_i необходимо преобразовывать, например, посредством использования переменных $1/x_i$. Поэтому в (1) естествен переход от переменных x_i к переменным $\tilde{x}_i$, задаваемым по правилу:

$\tilde{x}_i=x_i$, если i-й фактор увеличивает уязвимость объекта, и

$\tilde{x}_i=1/x_i$ в противном случае. Обозначим это правило цифрой (4).

Таким образом, свертка (1) заменится на следующую:

$$\tilde{R}=\sum_{j=1}^{g}\tilde{\alpha}_j\tilde{x}_j, \tag{5}$$

где, в соответствии с (4), $\tilde{x}_i\geq 0,j=\overline{1,g}$. Для агрегированного показателя уязвимости $\tilde{R}$ очевидным образом остаются справедливыми системы равенств (2) и неравенств (3).

Введем в рассмотрение переменные y_{ej}^{1i} и y_{ej}^{2i} следующим образом:

$$y_{ej}^{1i}=x_{a_e^i j}-x_{b_e^i j},(a_e^i,b_e^i)\in M^i,i=\overline{1,p},j=\overline{1,g},$$

$$y_{ej}^{2i}=x_{c_e^i j}-x_{d_e^i j},(c_e^i,d_e^i)\in N^i,i=\overline{1,p},j=\overline{1,g}.$$

Тогда равенства (2) и неравенства (3) примут соответственно вид

$$\sum_{j=1}^{g}\tilde{\alpha}_j y_{ej}^{1i}\geq 0,e=\overline{1,l_i},i=\overline{1,p}, \tag{6}$$

$$\sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{2i} = 0, e = \overline{1, l_i}, i = \overline{1, p}. \quad (7)$$

В соответствии с приемом, принятым в теории принятия решений, потребуем, чтобы так называемая разрешающая способность системы неравенств (6) была как можно выше. Формально это требование представимо в форме

$$\sum_{i=1}^{p} \beta_i \sum_{e=1}^{l_i} \sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{1i} \to \max. \quad (8)$$

Здесь β_i – уровень компетентности *i*-го эксперта, при этом $\beta_i > 0, i = \overline{1, p}, \sum_{i=1}^{p} \beta_i = 1$.

При отсутствии информации об оценках уровня компетентности экспертов будем полагать $\beta_i = 1$ для всех $i = \overline{1, p}$.

Учтем еще несколько важных соображений. Для обеспечения возможности сравнения степени уязвимости разных по характеру и масштабу элементов ОИ агрегированному показателю уязвимости $\tilde{R}$ необходимо придать относительный характер. Это можно делать, например, следующим образом.

Рассчитаем максимальные значения преобразованных значений частных критериев уязвимости: $\tilde{x}_j^+ = \max\limits_{j=1,g} \tilde{x}_j$.

Потребуем, чтобы уязвимость некоего объекта с максимальными значениями ее частных характеристик составляла 100%:

$$\sum_{j=1}^{p} \tilde{\alpha}_j \tilde{x}_j^+ = 100. \quad (9)$$

Требование строгой положительности параметров $\tilde{\alpha}_j$, а также то обстоятельство, что каждый частный показатель уязвимости обязательно должен обладать какой-то по крайне мере минимальной значимостью, можно формализовать следующим образом:

$$\tilde{\alpha}_j \tilde{x}_j^+ \geq \gamma_j, j = \overline{1, g}. \quad (10)$$

В качестве заданных заранее положительных чисел γ_j можно использовать, например, такие: $\gamma_j = \frac{10}{g}$, поскольку, если принять равными вклады каждой частной характеристики уязвимости в их агрегат, значения таких вкладов будут равны величине $\frac{100\%}{g}$.

Таким образом, задача построения агрегированного критерия уязвимости ОИ $\tilde{R}$ сводится к задаче линейного программирования (ЛП) с ограничениями (6), (7), (9), (10) и целевой функцией (8).

В том случае, если изначально уровень компетентности экспертов неизвестен ($\beta_i = \frac{1}{p}$ для всех *i*), то после решения указанной задачи ЛП этот уровень можно вычислить, рассчитав среднюю разрешающую способность высказываний каждого эксперта:

$$\beta_i = \sum_{e=1}^{l_i} \sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{1i} \Bigg/ \sum_{h=1}^{p} \sum_{e=1}^{l_h} \sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{1h}, \quad (11)$$

т.е. чем выше суммарная разрешающая способность ограничений (6), тем выше уровень компетентности соответствующего эксперта.

Разумеется, такой способ оценивания уровня компетентности экспертов является в определенной мере относительно условным, поскольку жестко привязан к виду функции, задающей свертку критериев. Если, в частности, вместо линейной функции (1) использовать более гибкую, например полином, результаты могут оказаться иными.

Предположим теперь, что задача ЛП (6)–(10), несовместна, т.е. экспертные высказывания взаимно противоречивы. В этом случае в соответствии с теорией решения некорректных задач

А.Н. Тихонова нужно искать квазирешение указанной задачи, использовав при этом прием, описанный в [4].

Введем в рассмотрение новые неотрицательные переменные u_e^i, v_e^i, t_e^i и преобразуем ограничения (6) и (7) к виду

$$\sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{1i} + t_e^i \geq 0, e = \overline{1, l_i}, i = \overline{1, p}, \quad (12)$$

$$\sum_{j=1}^{g} \tilde{\alpha}_j y_{ej}^{2i} + u_e^i - v_e^i = 0, e = \overline{1, l_i}, i = \overline{1, p}. \quad (13)$$

Введенные переменные представляют собой искажения, внесенные в ограничения (6) и (7), гарантирующие их совместность. Эти искажения необходимо минимизировать, заменив функционал (8) на

$$\sum_{i=1}^{p} \sum_{e=1}^{l_i} (t_e^i + u_e^i + v_e^i) \to \min. \quad (14)$$

Сформированная таким образом задача ЛП (9), (10), (12)–(14) также будет позволять рассчитывать коэффициенты линейной свертки (5).

Далее, при оценивании уровня компетентности каждого эксперта в этом случае следует исходить из соображения – чем меньше суммарное искажение ограничений, следующих из его экспертных высказываний, тем этот уровень выше, т.е. $\beta_i = 1 - \sum_{e=1}^{l_i} (t_e^i + u_e^i + v_e^i) \Big/ \sum_{i=1}^{p} \sum_{e=1}^{l_i} (t_e^i + u_e^i + v_e^i)$.

Для того чтобы обеспечить равенство единице суммарных уровней компетенции, полученные значения β_i необходимо соответствующим образом пронормировать.

Для оценки уровня компетентности экспертов, высказывания которых непротиворечивы, следует воспользоваться описанным выше приемом.

В следующей своей публикации авторы намерены описать практическое использование предложенной в работе методики для оценки уязвимости конкретных ОИ.

Литература

1. Классификация угроз информационной безопасности [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml, свободный (дата обращения: 11.04.2014).

2. Носков С.И. Управление системой обеспечения пожарной безопасности на региональном уровне / С.И. Носков, В.П. Удилов. – Иркутск: ВСИ МВД России, 2003. – 151 с.

3. Носков С.И. Газификация сельской местности: целевое программирование пожарной безопасности / С.И. Носков, В.Г. Подушко, В.П. Удилов. – Иркутск: ИрГТУ, 2001. – 150 с.

4. Носков С.И. Критериальная оценка обстановки с пожарами АТЕ Сибири и Дальнего Востока / С.И. Носков, В.П. Удилов, О.В. Бутырин // Проблемы деятельности правоохранительных органов и противопожарных служб: матер. II межвуз. науч.-практ. конф. – Иркутск: ИВШ МВД России, 1996. – С. 109–111.

5. Носков С.И. Технология моделирования объектов с нестабильным функционированием и неопределенностью в данных. – Иркутск: Облинформпечать, 1996. – 320 с.

6. Носков С.И. Оценка уровня уязвимости объектов транспортной инфраструктуры: формализованный подход / С.И. Носков, В.А. Протопопов // Современные технологии. Системный анализ. Моделирование. – 2011. – № 4. – С. 241–244.

Носков Сергей Иванович
Д-р техн. наук, профессор, профессор каф. информационных систем и защиты информации
Иркутского государственного университета путей сообщения (ИрГУПС)
Тел.: 8-914-902-24-94
Эл. почта: noskov_s@irgups.ru

Бутин Александр Алексеевич
Канд. физ.-мат. наук, доцент, доцент каф. информационных систем и защиты информации ИрГУПС
Тел.: 8-908-662-57-05
Эл. почта: butin_aa@mail.ru

Соколова Людмила Евгеньевна
Ассистент каф. информационных систем и защиты информации ИрГУПС
Тел.: 8-904-120-81-84
Эл. почта: LESokol1987@yandex.ru

Noskov S.I., Butin A.A., Sokolova L.E.
Multicriterial assessment of the level of vulnerability of the objects of informatization

The article considers a formalized way of assessing the vulnerability informatization objects. Itinvolves the construction of aggregated criterion of the level of vulnerability in the form of a linear convolution of local criteria with the use of methods of the theory of decision-making. The problem of determining the coefficients of the convolution is reduced to finding a solution or quasidecision of linear programming problems. An algorithm for evaluation of the level of competence of experts.
Keywords: information security, vulnerability, linear programming, quasidecision, theory of decision-making, expert information.

УДК 004.031, 004.056

А.П. Нырков, С.С. Соколов, А.С. Белоусов, Н.М. Ковальногова, В.А. Мальцев

Обеспечение безопасного функционирования мультисервисной сети транспортной отрасли

Рассмотрены предпосылки создания интегрированного информационно-коммуни-кационного пространства транспортной отрасли, постановка задачи передачи данных в мультисервисной сети транспортной отрасли и методы обеспечения помехозащищенности каналов передачи данных, предложена модель идентификации пользователя в мультисервисной сети.
Ключевые слова: мультисервисная сеть, модель индентификации пользователя, методы кодирования, помехозащищенность каналов, помехоустойчивость, передача данных, интегрированное информационно-коммуникационное пространство транспортной отрасли.

Транспортная стратегия Российской Федерации на период до 2030 г. предусматривает инновационный сценарий повышения конкурентоспособности транспортной системы за счет реализации транзитного потенциала страны. В соответствии с Рамочными стандартами безопасности и облегчения мировой торговли (ВТамО, 2005) требования по обеспечению безопасности теперь должны выполняться через безбумажный документооборот и предварительное информирование о перемещении товаров. Такой подход зафиксирован в Таможенном кодексе РФ и в «Концепции развития российской таможенной службы на период до 2020 года». Он распространяется на систему управления рисками, практику внедрения современных информационных технологий, предварительного информирования таможенных органов о перемещенных товарах и т.п.

Информатизация транспортной отрасли ввиду технического и технологического разнообразия имеет отличительной особенностью многообразие каналов передачи данных, прикладных программных решений и аппаратного обеспечения. Проблемы их безопасного функционирования подробно рассмотрены в работах [1–4].

В связи с повышенным вниманием Правительства и Президента Российской Федерации к развитию транспорта, необходимости качественной интеграции в международное транспортное пространство в рамках вступления России во Всемирную транспортную организацию, на первый план выходит решение вопросов, связанных со стандартизацией типовых операций, унификацией инструментария деятельности и оптимизацией ресурсов. Эти вопросы призваны решить продукты автоматизации основных видов деятельности, которые должны функционировать единым концептуальным информационным целым, образуя собой интегрированное информационно-коммуникационное пространство транспортной отрасли (ИИКП ТО).

Основные предпосылки создания интегрированного информационно-коммуникационного пространства транспортной отрасли. Основной целью создания ИИКП ТО является эффективный синтез имеющегося программно-аппаратного обеспечения процессов транспортной отрасли (ТО).

Основные задачи создания ИИКП ТО [5]:

1. Создание и поддержание бесперебойно функционирующих зарегистрированных и сопровождаемых информационных ресурсов, лицензионного программного обеспечения, а также территориально распределенной развитой вычислительной и коммуникационной инфраструктуры ТО.
2. Создание и внедрение новых форм и методов в управлении ТО в формате электронных регламентов (сервисов) на основе современных информационно-коммуникационных технологий.
3. Обеспечение функционирования ИИКП ТО на основе российских и международных стандартов менеджмента качества (ISO 9001, ISO 20000, ISO/IEC 38500 и др.).
4. Стандартизация и минимизация однотипных рутинных операций и повышение эффективности работы сотрудников ТО путем внедрения и интеграции специализированных приложений и средств коллективной деятельности.
5. Создание качественной инфраструктуры управления отраслевыми знаниями и иными нематериальными активами ТО.
6. Создание оптимальной транспортной среды маршрутизации потоков данных в рамках мультисервисной сети ИИКП ТО.

7. Формирование системы сервисов, поддерживаемых необходимой и достаточной вычислительно-коммуникационной инфраструктурой, для пользователей ИИКП ТО в соответствии с правами, установленными в матрицах доступа соответствующих информационных ресурсов.

8. Соблюдение требований по бесперебойности функционирования ИИКП ТО.

9. Снижение уровня потерь, связанных с принятием неэффективных управленческих решений, вызванных неточностями в служебной информации, несвоевременностью предоставления данных, нарушениями в регламентах использования информации и т.д.

10. Снижение уровня издержек на реализацию стандартных, рутинных, относительно редко изменяющихся служебных процедур и регламентов.

11. Организация системы контроля качества информационных продуктов, создаваемых в рамках работы пользователей и систем в ИИКП ТО.

12. Внедрение программно-целевого подхода при планировании, организации и аудите результатов мероприятий и программ в рамках функционирования ИИКП ТО.

13. Внедрение сервисов ИИКП ТО в рамках развития всех основных процессов, обеспечивающих стабильную работу ТО.

Мультисервисная сеть транспортной отрасли как основа существования интегрированного информационно-коммуникационного пространства транспортной отрасли. Ввиду наличия большого количества сервисов и разнородного программно-аппаратного обеспечения объектов транспортной инфраструктуры основой создания ИИКП ТО является мультисервисная сеть транспортной отрасли (МС ТО), которая по сути своей является сетью связи следующего поколения NGN (Next Generation Networks).

NGN применительно к транспортной сфере концептуально должна обеспечивать предоставление неограниченного объема услуг с гибкой системой управления трафиком, персонализацией (пользовательской или сервисной) и создание новых информационных услуг за счет унификации и эффективного синтеза сетевых решений. Данная сеть должна быть универсальной транспортной сетью с распределенной коммутацией, вынесением функций предоставления услуг в оконечные сетевые узлы, а также иметь возможность интеграции с использующимися традиционными сетями.

МС ТО – сеть связи, построенная в соответствии с концепцией NGN и обеспечивающая неограниченный набор услуг. Основные требования, предъявляемые к МС ТО:

- независимость технологий предоставления услуг от транспортных технологий;
- гибкое изменение скорости передачи в достаточно широком диапазоне для сервисов;
- передача многокомпонентной информации с синхронизацией всех компонент в реальном времени;
- участие нескольких операторов (сервисов) в формировании информационного контента;
- организация доступа к сервису единой транспортной сети вне зависимости от используемых технологий взаимодействия и расположения сервиса согласно матрице разграничения прав доступа ИИКП ТО [6].

Постановка задачи передачи данных в мультисервисной сети транспортной отрасли. Для постановки задачи представим сеть MPLS как неориентированный граф $G(V,E)$, где множество вершин V соответствует маршрутизаторам, а множество ребер E – сегментам сети. Определим множество $V_1 \subseteq V$, которое содержит вершины, соответствующие пограничным маршрутизаторам.

На рис. 1 представлен неориентированный граф сети МС ТО.

Для дальнейшей постановки задачи введем множество $R \subseteq V_1 \times V_1$, которое содержит пары вершин, соответствующие пограничным маршрутизаторам, между которыми передаются данные. Таким образом, если трафик передается от *LER 2* к *LER 1* и между *LER 2* и *LER 3* в обоих направлениях, то множество *R* будет иметь вид $R = \{(v_1, v_4), (v_1, v_9), (v_9, v_1)\}$.

Введем дополнительные обозначения: $w(x,y)$ – пропускная способность ребра (x,y) графа *G*; $l(s,t) = ((s,x_1),(x_1,x_2),...,(x_{\gamma(s,t)},t))$ – маршрут из вершины *s* в вершину *t* графа *G*, где $\gamma(s,t)$ – длина маршрута $l(s,t)$; $\tilde{A}(s,t)$ – максимально допустимая длина маршрута $l(s,t)$; $L(s,t) = \left\{ l(s,t) \in L \middle| \gamma(s,t) \le \tilde{A}(s,t) \right\}$ – множество маршрутов из *s* в *t*, длина которых не превышает $\tilde{A}(s,t)$; $l_i(s, t)$ – *i*-й маршрут из *s* в *t*, $l_i(s,t) \in L(s,t)$; $f(s, t)$ – поток из *s* в *t*; $f_i(s, t)$ – часть потока $f(s, t)$ по маршруту $l_i(s, t)$; $b(s, t)$ – требование к пропускной способности сети для пары (s, t); $\phi(x,y)$ – суммарный поток по ребру (x,y), где $0 \le \phi(x,y) \le w(x,y)$.

Для формулировки задачи передачи данных в сети МС ТО необходимы следующие исходные данные: неориентированный граф сети $G(V,E)$, множество вершин V_1, множество взаимодействующих вершин R, пропускные способности ребер w графа $G(V,E)$, требования к пропускной способности b и множество маршрутов L между взаимодействующими вершинами. Обозначим через $|L(s,t)|$ мощность множества $L(s,t)$. Следующие отношения должны выполняться согласно постановке задачи:

$$f(s,t)=\sum_{i=1}^{|L(s,t)|} f_i(s,t); \quad \varphi(x,y)=\sum_{(s,t)\in R}\ \sum_{\substack{i=1; \\ (x,y)\in l_i(s,t)}}^{|L(s,t)|} f_i(s,t).$$

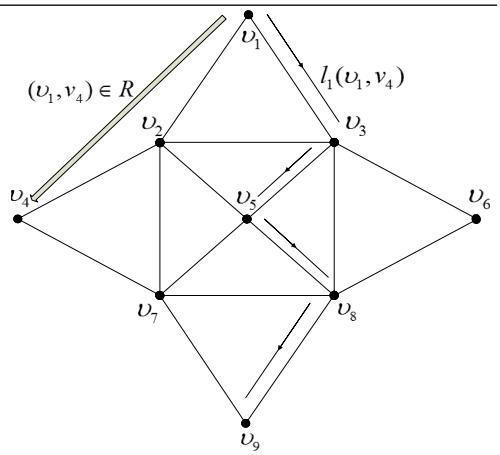


Рис. 1. Неориентированный граф сети МС ТО

Данная модель позволяет определить однокритериальные задачи согласно сформулированным выше принципам построения сетей МС ТО. При введении дополнительных параметров можно расширить модель и покрыть большее число критериев. Так, например, при известной стоимости передачи единицы потока по ребру $c(x,y)$ можно определить стоимость передачи потока по i-му маршруту в виде

$$c(l_i(s,t))=\sum_{(x,y)\in l_i(s,t)} \varphi(x,y)c(x,y),\ (s,t)\in R,\ i=\overline{1,|L(s,t)|}.$$

Задача минимизации стоимости передачи потоков будет заключаться в определении потоков $f_i(s,t)$, которые минимизируют функцию общей стоимости:

$$\sum_{(s,t)\in R}\ \sum_{i=1}^{|L(s,t)|} f_i(s,t)c(l_i(s,t))\to\min,$$

при выполнении ограничений

$$f_i(s,t)\ge 0,\ (s,t)\in R,\ i=\overline{1,|L(s,t)|};\quad \varphi(x,y)\le w(x,y),\ (x,y)\in R;\quad \sum_{i=1}^{|L(s,t)|} f_i(s,t)=b(s,t),\ (s,t)\in R.$$

Дальнейшее развитие модели позволит сформулировать большое число однокритериальных задач, таких как балансировка нагрузки в сети, минимизация числа маршрутов, задержек и пр. Также возможна постановка многокритериальной задачи, например задачи маршрутизации трафика [7].

Помехоустойчивость каналов передачи данных в мультисервисной сети транспортной отрасли. Под помехозащищенностью будем понимать возможность обеспечения надежной безошибочной работы сети передачи данных под действием внешних помех различного типа.

Современные методы обеспечения помехозащищенности условно можно разделить на четыре категории:

1. Изменение физических характеристик канала передачи данных.
2. Использование специальных средств подавления помех.
3. Изменение методов организации приема и/или передачи сигнала.
4. Кодирование передаваемой информации.

К первой категории можно отнести различные методы повышения качественных характеристик каналов передачи данных. Например, замену кабелей вида витая пара на кабели более высоких категорий, в которых используется дополнительное экранирование. Также в некоторых случаях проводные каналы передачи данных прокладывают в дополнительно защищенных кабельных трассах. В беспроводных каналах связи используются более сложные приемопередающие устройства, которые повышают помехозащищенность, например, за счет повышения отношения сигнал/шум.

К специальным средствам подавления помех можно отнести линейные и нелинейные генераторы шума и другие, отдельно используемые устройства.

Среди методов, которые позволяют увеличить помехозащищенность изменением организации приема/передачи сигнала, можно выделить такие, как метод разнесенного приема сигнала, исполь-

зование модуляции на меньшее количество состояний, использование различных методов принятия решения о передаваемом сигнале, использование сигналов с расширением спектра и другие методы.

Все вышеперечисленные методы имеют много субъективных факторов применения, накладывающих определённые ограничения на их использование. Каждый из этих методов применим только в конкретном классе задач, однако четвертая категория обладает отличительной особенностью – общностью применения, так как использование методов кодирования не зависит ни от канала передачи данных, ни от структуры сигнала.

Методы кодирования. История помехоустойчивых кодов или кодов, обнаруживающих и исправляющих ошибки, начинается в 1948 г. вместе со статьей Клода Элвуда Шеннона «Математическая теория связи». Шеннон в своей статье выразил главную мысль о том, что построение слишком хороших каналов является неоправданным, экономически выгоднее использовать кодирование. Именно с этого момента начинается активное изучение и разработка помехоустойчивых кодов.

На сегодняшний день насчитывается большое количество различных алгоритмов кодирования и декодирования информации для передачи по каналам связи. Однако основной идеей остается внесение избыточности. На этапе кодирования в информацию вносятся заранее определенным, специальным образом дополнительные символы или блоки символов, которые в дальнейшем могут быть использованы на этапе декодирования информации для обнаружения или исправления произошедших ошибок под действием внешних факторов и помех.

Алгоритмы можно группировать по различным признакам и категориям. По способу обработки информации коды можно разделить на 2 класса: блоковые и сверточные. Первый класс делит информацию на блоки определенной длины и обрабатывает каждый блок в отдельности, второй класс кодов обрабатывает и передает информацию в виде бесконечного потока.

Следует отметить методы комбинирования кодирования. Такие коды известны под названием каскадные коды. В таком коде информация кодируется сначала одним алгоритмом, а потом применяется другой алгоритм кодирования на уже кодированной информации. Таким образом, получается код-произведение. Для улучшения помехозащищенности каскадных кодов, часто после первого этапа кодирования, применяется операция перемежения, в результате которой символы, находящиеся на соседних позициях, располагаются на различном расстоянии друг от друга. При декодировании производят операцию, обратную перемежению, и символы расставляются по прежним местам в информационном потоке.

Популярной схемой каскадных кодов является алгоритм, который кодирует информацию блоковыми кодами Рида–Соломона, затем информация проходит операцию перемежения и кодируется сверточным кодом. На приемной стороне после декодирования сверточного кода происходит операция, обратная перемежению, при этом большие блоки ошибок рассортировываются и попадают в различные кодовые слова кода Рида–Соломона, тем самым еще более уменьшают вероятность ошибки при декодировании.

Отдельно следует обратить внимание на коды, использующие не только временной ресурс. При внесении избыточности количество полезной передаваемой информации снижается, а следовательно, снижается и скорость передачи данных. На сегодняшний день активно используются коды, использующие также и пространственный ресурс. Такие коды называются пространственно-временными. Суть их состоит в том, что информация передается не от одного источника, а одновременно от нескольких. Тем самым образуется пространственная избыточность. Принятый сигнал обрабатывается определенными алгоритмами и позволяет наиболее точно определить форму переданного сигнала, а следовательно, и произвести наиболее точное декодирование [8].

Идентификация пользователя в мультисервисной сети транспортной отрасли. Для успешной идентификации пользователя в мультисервисной сети транспортной отрасли необходимо выполнить следующую последовательность действий:

1. Произвести условное разбиение всей МС ТО на классы сервисов.
2. Для каждого класса МС ТО определить набор сервисов, входящих в него.

Будем различать два вида идентификации: полную и частичную.

Под полной идентификацией пользователя во всей МС ТО будем понимать совокупность успешных идентификаций пользователя во всех сервисах всех классов, в нее входящих. Под частичной идентификацией – совокупность успешных идентификаций пользователя во всех тех сервисах, в которых необходимо организовать доступ в рамках текущей сессии.

Также будем считать, что уровень корректности, полноты и качества идентификации с точки зрения уровня информационной защищенности активов МС ТО тем выше, чем больше атрибутов пользователя участвует в идентификации и чем сложнее степень их определения.

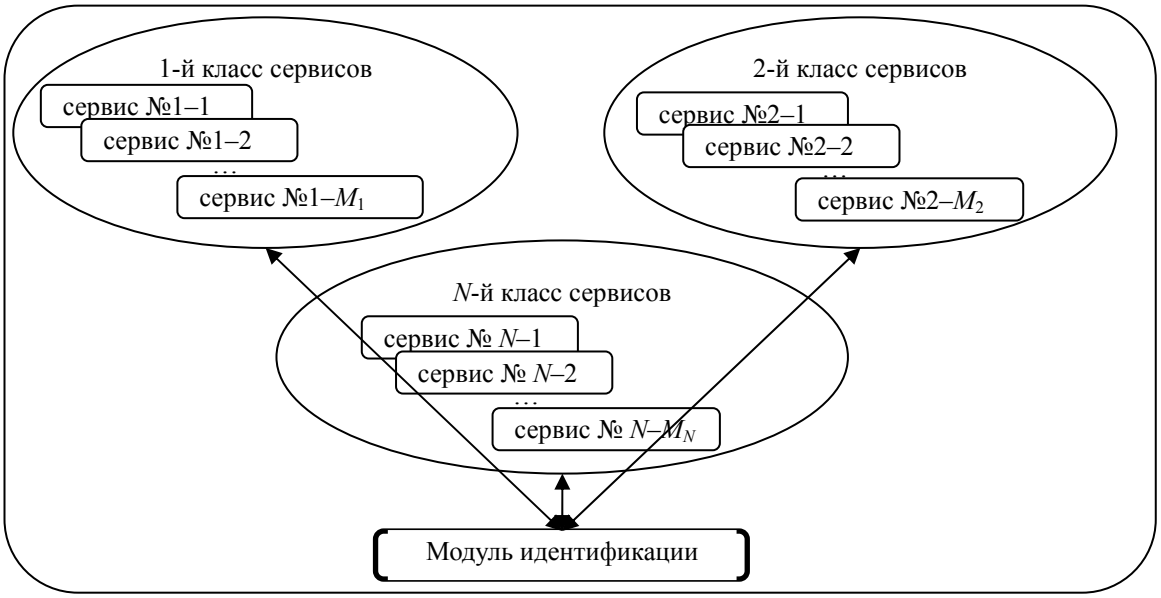


Рис. 2. Типовая схема взаимодействия модуля идентификации
как составного элемента МС ТО с классами сервисов

3. Провести процесс идентификации пользователя в МС ТО как поклассовую последовательность шагов по идентификации пользователя в каждом сервисе конкретного класса (для полной идентификации – все сервисы, для частичной – те, которые участвуют в идентификации).

За все процессы идентификации пользователя в МС ТО отвечает отдельный программно-аппаратный модуль, который обеспечивает эффективный синтез программных и аппаратных способов идентификации (рис. 2).

Для построения модели идентификации пользователя в МС ТО введем следующие обозначения: K_i – i-й класс сервисов; S_{ij} – j-й сервис в i-м классе; $a_{k_{ij}}$ – k-й идентификационный атрибут пользователя, определяемый в j-м сервисе i-го класса; $A_{ij} = \left\{a_{1_{ij}}, a_{2_{ij}}, ..., a_{k_{ij}}\right\}$ – множество идентификационных атрибутов пользователя, определяемое в j-м сервисе i-го класса.

Для каждого атрибута $a \in A$ определен домен V_a (для доменов допускается дискретность значений).

Множество 2^{V_a} – супердомен атрибута a $V = \bigcup\limits_{a \in A} V_a$. Таким образом, модель идентификации пользователя можно представить парой (A,V).

Для $\forall S \subseteq A$ определим следующие величины:

$$V_S = \bigcup_{s \in S} V_s, \quad \bar{2}^{V_S} = \bigcup_{s \in S} 2^{V_a}.$$

Под кортежем типа T будем понимать функцию следующего вида:

$$r : T \to \bar{2}^{V_T}$$

и $r(a) \subseteq V_a$ для всех $a \in T$, далее вместо $r(a)$ используем запись r_a, а для кортежа типа T – запись r_T, множество всех кортежей типа T обозначим как $U(T)$.

Под элементарным кортежем типа T будем понимать функцию

$$r : T \to V_T,$$

такую, что $r(a) \in V_a$ для любых $a \in T$, в случае если $V_a = \varnothing$, тогда $r(a) = null$ (это возможно в случает отсутствия оперативной необходимости идентификации пользователя в конкретном классе сервисов), множество кортежей типа T определим как $eU(T)$.

Для построения системы идентификации пользователей в МС ТО необходимо произвести классификацию сервисов (как было сказано ранее), категорирование пользователей и построение матри-

цы прав доступа, в которой по вертикали будут указаны категории пользователей, по горизонтали классы сервисов, а на пересечении – уровень доступа, определяемый для данной категории в рамках данного класса.

Пусть P – множество категорий пользователей. $D \subseteq A$ – набор атрибутов для категорирования. K_D – категорирование множества пользователей на основе атрибутов D. Категорию определим как элементарный кортеж:

$$r : D \to \bigcup_{a \in D} V_a ,$$

где $r(a) \in V_a$ для каждого $a \in D$. Множество всех элементарных кортежей типа D обозначим как $U(D)$. Таким образом, число категорий будет равно числу всех кортежей типа D; $K_D(r)$ – категория, определенная кортежем r.

Пользователь $p \in P$ принадлежит категории $K_D(r)$, если для каждого атрибута $a \in D$ значение идентификатора равно $r(a)$. Отсюда получаем следующее:

$$\bigcup_{r \in eU(D)} K_D(r) = L , \quad K_D \cap K_D(r') = \varnothing, \forall r, r' \in eU(D), r \neq r'.$$

Таким образом,

$$K_D = \{K_D(r) \mid r \in eU(D)\}$$

можно рассматривать как разбиение множества D. В результате некоторые категории могут оказаться пустыми (неактуальными в данный момент идентификации, например, при частичной идентификации) и их необходимо удалить из K_D.

Отметим также, что значения атрибутов модели идентификации пользователя могут изменяться в процессе функционирования МС ТО. Это определяется возможной миграцией и изменением состава сервисов, а также типом идентификации. При возникновении таких ситуаций необходимо произвести переклассификацию.

Также могут быть случаи идентификации по ряду альтернативных признаков.

Альтернативным признаком, например, может быть идентификация по отпечатку пальца или по сетчатке глаза и т.п.

Пусть a_i и a_{i^a} – попарно альтернативные признаки, а $\widetilde{a_j}$ – признаки, не имеющие альтернативных аналогов, тогда верная идентификация $True(I)$ возможна в случае истинности выражения:

$$True(I) \equiv \left(\widetilde{a_1} \,\&\, \widetilde{a_2} \,\&\, ... \,\&\, \widetilde{a_n}\right) \& \left(\left(a_1 \vee a_{1^a}\right) \& \left(\left(a_2 \vee a_{2^a}\right)\right) \& ... \& \left(a_m \vee a_{m^a}\right)\right),$$

где n – количество признаков, не имеющих альтернативных аналогов; m – количество признаков, имеющих альтернативные аналоги.

Заключение. Пространство информационного обмена, основой которого стала МС ТО, требует серьезно продуманной системы мер и правил по обеспечению должного уровня безопасности функционирования. В рамках одной статьи всего перечня мер не охватить. Предпосылками на будущее являются также существующие нормы законодательства РФ, которые дают четкие рекомендации по уровням защищенности и принципам категорирования информации. Именно хорошо продуманная система обеспечения информационной безопасности позволит, в том числе, стандартизировать многие процессы, что станет основой успешного развития всей отрасли как единого организма внутренних и международных отношений.

Литература

1. Нырков А.П. О проблемах защищенности беспроводных сетей передачи данных на внутренних водных путях / А.П. Нырков, А.В. Башмаков // Методы и технические средства обеспечения безопасности информации: матер. XIX науч.-техн. конф. – СПб.: Изд-во политехн. ун-та, 2010. – С. 43–44.

2. Каторин Ю.Ф. Защищенность информации в каналах передачи данных в береговых сетях автоматизированной идентификационной системы / Ю.Ф. Каторин, В.В. Коротков, А.П. Нырков // Журнал университета водных коммуникаций. – 2012. – № 1. – С. 98–102.

3. Нырков А.П. Методика проектирования безопасных информационных систем на транспорте / А.П. Нырков, С.С. Соколов, А.В. Башмаков // Проблемы информационной безопасности. Компьютерные системы. – 2010. – № 3. – С. 58–61.

4. Нырков А.П. Безопасность информационных потоков в АСУДС / А.П. Нырков, П.В. Викулин // Проблемы информационной безопасности. Компьютерные системы. – 2010. – № 4. – С. 78–82.

5. Соколов С.С. О создании единого интегрированного информационно-коммуникационного пространства транспортной отрасли // Региональная информатика РИ–2012: матер. Юбилейной XIII Санкт-Петербургской междунар. конф. 24–26 октября 2012 г. – СПб.: 2012. – С. 247–250.

6. Нырков А.П. Методы обеспечения доступа в ведомственных сетях на базе мультисервисных платформ / А.П. Нырков, А.А. Некрасов // Высокие технологии, фундаментальные исследования, образование: сб. тр. Восьмой Междунар. науч.-практ. конф. «Исследование, разработка и применение высоких технологий в промышленности». – СПб, 2009. – С. 68–71.

7. Нырков А.П. Мультисервисная сеть транспортной отрасли / А.П. Нырков, С.С. Соколов, А.С. Белоусов // Вестник компьютерных и информационных технологий. – 2014. – № 4. – С. 33–39.

8. Нырков А.П. Помехозащищенность как фактор обеспечения стабильной работы сети передачи данных на транспорте / А.П. Нырков, С.С. Соколов, А.С. Белоусов // Сборник научных трудов SWorld. – 2013. – Т. 8, № 1. – С. 5–9.

Нырков Анатолий Павлович
Д-р техн. наук, профессор, зав. каф. комплексного обеспечения информационной безопасности Государственного университета морского и речного флота (ГУМРФ) им. адм. С.О. Макарова
Тел.: 8 (812) 748-96-41
Эл. почта: NyrkowAP@gumrf.ru

Соколов Сергей Сергеевич
Канд. техн. наук, доцент, начальник управления информатизации ГУМРФ
Тел.: 8 (812) 748-97-20
Эл. почта: SokolovSS@gumrf.ru

Белоусов Андрей Сергеевич
Аспирант факультета информационных технологий ГУМРФ
Тел.: 8 (812) 748-97-20
Эл. почта: BelousovAS@gumrf.ru

Ковальногова Надежда Михайловна
Аспирант факультета информационных технологий ГУМРФ
Тел.: 8 (812) 748-97-50
Эл. почта: KovalnogovaNM@gumrf.ru

Мальцев Валерий Александрович
Аспирант факультета информационных технологий ГУМРФ
Тел.: 8 (812) 748-97-50
Эл. почта: MalcevVA@gumrf.ru

Nyrkov A.P., Sokolov S.S., Belousov A.S. , Kovalnogova N.M., Maltsev V.A.
Ensuring safe operation of multiservice network in transport industry

The article describes the prerequisites for the development of integrated information and communication space transportation industry, formulation of the problem of data transmission in multi-service transport industry and methods to ensure immunity of data transmission channels, a model of user identification in a multiservice network.

Key words: multiservice network, model proxy authentication user, coding techniques, channels immunity, immunity data, integrated information and communication space of transportation industry.

УДК 004.7

Т.М. Пестунова, З.В. Родионова, С.Д. Горинова

Анализ аспектов информационной безопасности на основе формальных моделей бизнес-процессов

Представлен подход к анализу аспектов информационной безопасности на основе формальных моделей процессов организации, разработанных в стандартных нотациях бизнес-моделирования. Процесс рассматривается как объект защиты информации. Проведён частичный анализ некоторых распространённых методик оценки рисков информационной безопасности в контексте объектов, содержащихся в EPC-модели.

Ключевые слова: информационная безопасность (ИБ), модели бизнес-процессов, права доступа, риски.

Согласно стандартам объектами защиты являются «информация или носитель информации или информационный процесс, которые надо защищать в соответствии с целью защиты» [1]. Анализ литературы и практика показывают, что при создании систем защиты информации в качестве объектов защиты, как правило, рассматриваются информация и её носители. В условиях, когда процессный подход к организации деятельности предприятия является основным принципом и при управлении, и при автоматизации, ограничиваться этим недостаточно. Цель защиты определяется целями деятельности организации, достижение которых обеспечивается, в частности, корректной реализацией основных и вспомогательных бизнес-процессов. Постановка задач ИБ в контексте бизнес-процессов позволяет соотнести аспекты безопасности с результатами бизнес-процессов, а значит, и с целями деятельности организации. Следует отметить, что бизнес-процессы организаций и предприятий не являются статичными. Их высокая изменчивость обусловлена многими причинами, в частности, слиянием фирм, оптимизацией организационной структуры, внедрением автоматизированных технологий и т.п., что требует постоянного отражения происходящих изменений в системе обеспечения ИБ. При этом изменения могут касаться всех элементов системы ИБ: от концептуальных документов, инструкций и регламентов до конфигурации программно-технических решений.

Анализ моделей бизнес-процессов даёт возможность отследить влияние происходящих изменений на многие аспекты ИБ. В частности, в [5, 6] и ряде последующих работ авторами был предложен автоматизированный подход к управлению правами доступа на основе анализа EPC-модели, основные этапы которого представлены на рис. 1. Говоря о целесообразности обращения к формальным моделям бизнес-процессов при решении задач ИБ, следует отметить, что эти модели обычно разрабатываются в ходе бизнес-планирования и реинжиниринга процессов предприятия, в частности, при автоматизации. Результаты таких работ приводят к необходимости внесения изменений в политики и (или) технологии ИБ, и если при моделировании бизнес-процессов предусмотреть анализ параметров, влияющих на ИБ, то можно снизить трудоёмкость работ по выявлению и обоснованию изменений в системе ИБ.

В данной работе исследуются модели бизнес-процессов в контексте решения задач анализа угроз и уязвимостей для последующей оценки рисков информационной безопасности. В современных условиях анализ рисков является основой обеспечения ИБ и проектирования систем защиты информации, что находит отражение не только в научно-методической литературе, но и закреплено в нормативно-правовых актах и стандартах [2, 3]. Важным документом при этом является модель угроз, в которой отражаются и актуализируются данные об источниках угроз, уязвимостях системы, объектах воздействия и ряде других параметров. Методы оценки рисков используются для анализа критичности выявленных угроз, обоснования множества актуальных угроз и выбора соответствующих контрмер.

Некоторые авторы [4] отмечают необходимость рассмотрения бизнес-процессов как основных активов организации, представляющих собой комбинацию из разнородных активов: информации, технических и программных средств, кадровых ресурсов и т. д. Но, несмотря на это, решение задач ИБ напрямую с моделями бизнес-процессов не связывается. Целесообразным считается получение

информации об основных бизнес-процессах от владельцев и участников этих процессов при помощи опросных листов. При этом цель сбора этих данных – выявление критичных информационных активов и технологических аспектов их обработки, на основе которых можно сделать выводы об угрозах и уязвимостях. Дальнейшая оценка не предполагает обращения к бизнес-процессам.

Рис. 1. Этапы процесса формализации и актуализации прав доступа на основе бизнес-процессов

Не подвергая сомнению данный метод, который используется и при описании бизнес-процессов, следует учесть три существенных обстоятельства. Во-первых, значительная часть информации, которая выявляется из ответов опросных листов, уже содержится в объектах формальных моделей бизнес-процессов. В качестве примера в табл. 1 приведено сопоставление элементов разработанной авторами модели формализации и актуализации прав доступа к графически отображаемым объектам бизнес-процессов для двух распространённых сред бизнес-моделирования, поддерживающих нотацию EPC. Указанные объекты также важны и с точки зрения задачи анализа угроз и уязвимостей. Схематично этот процесс изображён на рис. 2.

Во-вторых, получение актуальных данных о состоянии организации – это непрерывный процесс. После проведения аудита, который является периодическим процессом, в организации могут произойти разного рода изменения. Даже если используются автоматизированные системы управления рисками, при изменении бизнес-процессов информация об этих изменениях должна вручную отслеживаться и вноситься в соответствующую систему. Автоматизированное извлечение данных из модели бизнес-процесса позволяет упростить данную процедуру и повысить оперативность решения задач переоценки рисков не только по результатам аудита, но и на основе данных текущего мониторинга безопасности и в случаях реинжиниринга бизнес-процессов.

Анализ ряда распространённых моделей анализа рисков, краткие обобщённые результаты которого представлены в табл. 2, позволяет сделать вывод об их основных параметрах, многие из которых являются общими для разных методик. Выделяется методика ГРИФ, использующая понятие

«бизнес-процесс»: под ним подразумеваются производственные процессы, в которых обрабатывается ценная информация [8]. Они не оцениваются, и не детализируется обработка информации внутри этих процессов. Но при использовании бизнес-процесса для оценки рисков можно отследить путь информационного объекта внутри процесса, что даёт возможность выявить угрозы и уязвимости. В методике определения актуальных угроз в информационных системах персональных данных [7] существенным образом учитывается специфика обрабатываемой информации при оценке исходной защищённости системы (например, операции с обезличенными данными) и при экспертном определении опасности угроз (оцениваются последствия для субъекта персональных данных).

Таблица 1

Описание и графическое представление элементов модели бизнес-процессов для разных сред бизнес-моделирования в модели формализации и актуализации прав доступа

Элементы модели формализации и актуализации прав доступа	Графическое представление объектов модели бизнес-процесса в средах	
	Business Studio	ARIS
FF – множество функций, выполняемых участниками бизнес-процесса (исполнителями)	Функция	Функция
IS – множество информационных систем	Информационная система	Прикладная система
IO – множество информационных объектов	Информация	Кластер информации
PP – множество исполнителей		Должность
FI – ФИО исполнителя	Нет графического представления	ФИО
AT – множество типов доступа	——→	- - - - - - - - - - - - - - →

В-третьих, бизнес-процесс, представленный в виде модели, может быть рассмотрен как самостоятельный объект защиты информации. Он имеет определённые свойства, нарушение которых приводит к негативным последствиям с точки зрения достижимости целей (подцелей) организации, что лежит в основе оценки критичности процесса. Примерами таких свойств являются: своевременность результата (выхода процесса), соответствие результата установленным требованиям, соответствие затраченных на выполнение процесса ресурсов плановым значениям и др. Их нарушение возможно из-за ошибок исполнителя, ненадлежащего состояния ресурсов, нарушения своевременности входа процесса, излишних затрат времени исполнителей на реализацию предусмотренных процессом работ, несогласованности действий исполнителей и т.п. Причины многих факторов риска лежат в области организации и исполнения информационных процессов, следовательно, должны быть объектом внимания при выполнении работ по ИБ. Это позволяет соотнести информационные объекты и функции по их обработке с конкретными результатами бизнес-процесса, установив влияние нарушения одних процессов (подпроцессов) на другие, а в итоге – на цели деятельности. Отследить такие взаимосвязи можно, опираясь на формальную модель бизнес-процесса. Подобный подход рассматривается, в частности, в [11]. Основные объекты этой модели представлены в табл. 3.

Для организации процесса оценки рисков на основе модели бизнес-процесса необходимы:

1) правила построения модели бизнес-процессов, обеспечивающие наличие и однозначную интерпретацию содержащихся в ней данных для а) идентификации угроз и уязвимостей; б) оценки значимости информационного ресурса как с точки зрения последствий для результата процесса, так и с точки зрения влияния изменённого результата процесса на цели деятельности;

2) алгоритмы извлечения из бизнес-процесса данных, используемых в модели анализа рисков;

3) алгоритмы реагирования на изменения, отображающие изменения параметров модели бизнес-процесса в значения параметров модели оценки рисков.

Практическая реализация данного подхода осуществляется посредством создания информационной системы анализа безопасности процесса (далее – ИС АБП), место которой в системе ИБ показано на рис. 3: ИС АБП получает данные из бизнес-процесса, а далее может передавать их на ана-

лиз в системы управления информационными рисками (СУИР), которые могут быть основаны на разных методиках. Результаты работы СУИР используются традиционным образом для реализации мер защиты информации как в автоматизированных информационных системах (АИС), так и при неавтоматизированной обработке (ИС).

Рис. 2. Диаграмма процесса «Анализ угроз и уязвимостей»

Таблица 2

Сопоставление параметров оценки рисков для некоторых типовых методик

Наименование методики	CRAMM [4, 9]	Модель NIST [10]	ГРИФ [8, 9]
Схожие объекты (с учётом возможных различий в детализации)	*Модель ИС*: границы системы и функциональная спецификация; *ресурс* (физический, программный, информационный): ценность ресурса; *угроза*: уровень угрозы, ожидаемые финансовые потери; *уязвимость*: уровень уязвимости; *контрмера*	*Модель ИС*: границы и функции системы, важность системы и данных; *ресурс* (физический, программный, информационный); *угроза*: возможность реализации, величина ущерба для ИС; *уязвимость*: вероятность использования; *контрмера*;	*Модель ИС*: архитектура сети; *ресурс* (физический, программный, информационный): ценность; *угроза*: вероятность реализации, ущерб от реализации угрозы; *уязвимость*; *контрмера*
Отличительные объекты		*источник угрозы*: мотивация	*группа пользователей*: класс, доступ к информации; *аспекты ИБ ресурса*: конфиденциальность, целостность, доступность; *бизнес-процесс*

Таблица 3

Перечень данных модели оценки рисков Таубенбергера–Юрьенса [11]

Объекты модели	Примечание о содержании
Модель бизнес-процесса	Представляется в формальной нотации
Критичность бизнес-процесса	Высокая, средняя и низкая критичность для бизнеса оценивается на основе внешних правил
Информационный ресурс	Информационный объект, обрабатываемый бизнес-процессом
Аспект ИБ для ресурса	Конфиденциальность, доступность и/или целостность
Точка входа	Момент начала обработки информации бизнес-процессом
Точка завершения обработки	Момент передачи данных между пользователями, их изменения или сохранения
Канал связи	Канал передачи данных от одной точки обработки к другой
Цель безопасности	Задается по отношению к бизнес-процессу на основе внешнего правила (например, экспертным путем)

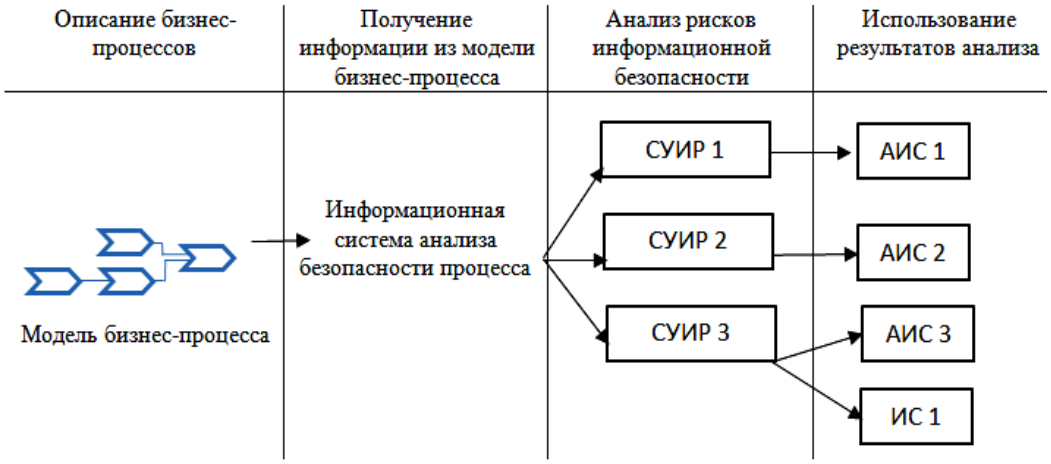


Рис. 3. Место ИС АБП в СУИБ

Сопоставление сведений, представленных в табл. 1 и 2, с данными в нотации EPC, показывает, что из модели бизнес-процесса можно извлечь данные для определения границ и особенностей ИС: содержание и носители обрабатываемой информации, пользователи, способы передачи данных внутри и вне ИС, используемые технологии. Эта информация является основой для идентификации защищаемых активов. Для автоматизированной идентификации возможных угроз в ИС АБП предусмотрена структура данных, содержащая используемые в методиках оценки рисков параметры угроз и уязвимостей во взаимосвязи с объектами бизнес-процесса, формируемая по следующим принципам:

1) каждой уязвимости должен быть поставлен в соответствие объект, определяющий, какому способу обработки, передачи и/или хранения присуща данная уязвимость;

2) каждой угрозе должны быть поставлены в соответствие аспекты ИБ, к нарушению которых может привести угроза: конфиденциальность, доступность и/или целостность;

3) каждой угрозе должен быть присвоен источник – источником может являться исполнитель бизнес-процесса, лицо, не принимающее участия в исполнении бизнес-процесса, стихия и проч.

Полная модель бизнес-процессов организации, представленная в формальной нотации, является иерархией моделей процессов и подпроцессов, которая отражает взаимосвязи процессов разного уровня детализации. При задании причинно-следственных связей между аспектами безопасности для информационных объектов, с одной стороны, и факторами и последствиями рисков для соответствующих подпроцессов, с другой стороны, можно, опираясь на взаимосвязи бизнес-процессов, отражаемые в формальной нотации, автоматизированным путём получить данные о степени влияния аспектов безопасности информационных объектов подпроцесса на результаты процессов более высокого уровня и в конечном итоге – на достижимость целей организации.

Заключение. В статье представлен подход к управлению аспектами ИБ на основе формальных моделей бизнес-процессов. В частности, на основе данных модели, представленной в терминах нотации EPC, разработана ИС формализации и актуализации прав доступа. Сформулирована концепция ИС АБП для автоматизированного анализа угроз и уязвимостей в ходе реинжиниринга бизнес-процессов, позволяющая оценивать планируемые изменения в организации бизнес-процессов с точки зрения возможных последствий ИБ и обоснованно принимать соответствующие решения.

Литература

1. ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – М.: Стандартинформ, 2006. – 18 с.

2. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. – М.: Стандартинформ, 2011. – 51 с.

3. ГОСТ Р ИСО/МЭК 27005–2010. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – М.: Стандартинформ, 2013. – 210 с.

4. Астахов А.М. Искусство управления информационными рисками. – М.: ДМК-Пресс, 2010. – 312 с.

5. Пестунова Т.М. Информационная система управления правами доступа на основе анализа бизнес-процессов / Т.М. Пестунова, З.В. Родионова // Доклады ТУСУРа. – 2010. – № 2 (22), ч. 2. – С. 253–256.

6. Родионова З.В. Управление процессом предоставления прав доступа на основе анализа бизнес-процессов / З.В. Родионова, Т. М. Пестунова // Прикладная дискретная математика. – 2008. – № 2. – С. 91–95.

7. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [методический документ ФСТЭК России: утв. ФСТЭК России 14.02.2008]. – М., 2008. – 10 с.

8. Методика оценки риска ГРИФ 2006 из состава Digital Security Office [Электронный ресурс]. – Режим доступа: http://dsec.ru/ipm-research-center/article/risk_assessment_method_vulture_2006_from_the_composition_of_the_digital_security_office/, свободный (дата обращения: 28.04.2014).

9. Лопарев С.А. Анализ инструментальных средств оценки рисков утечки информации в компьютерной сети предприятия / С.А. Лопарев, А.А. Шелупанов // Вопросы защиты информации. – 2003. – № 4. – С. 2–5.

10. Петренко С.А., Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: ДМК Пресс, 2004. – 384 с.

11. IT Security Risk Analysis based on Business Process Models enhanced with Security Requirements [Электронный ресурс]. – Режим доступа: http://ceur-ws.org/Vol-413/paper16.pdf, свободный (дата обращения: 20.04.2014).

Пестунова Тамара Михайловна
Канд. техн. наук, доцент, зав. каф. информационной безопасности
Новосибирского государственного университета экономики и управления (НГУЭУ)
Тел.: 8-913-922-53-05
Эл. почта: t.m.pestunova@nsuem.ru

Родионова Зинаида Валерьевна
Канд. техн. наук, доцент каф. информационной безопасности НГУЭУ
Тел.: 8-962-839-43-94
Эл. почта: z.v.rodionova@nsuem.ru

Горинова София Дмитриевна
Студентка НГУЭУ
Тел.: 8-953-792-63-27
Эл. почта: gsd0201@gmail.com

Pestunova T.M., Rodionova Z.V., Gorinova S.D.

Analysis of information security aspects based on the formal models of business processes

We outline an approach to analysis of information security aspects basing on formal models of company's business processes that are described in terms of standard business-modeling notations. Process is considered as a protected object. We partially analyzed some widespread risk evaluation methods in context of the objects used in EPC-model.

Keywords: information security, risks, models of business processes, access rights.

УДК 681.3.067

Е.Н. Пивкин, В.М. Белов, С.А. Белкин

К вопросу об анализе защищенности объектов информатизации с использованием нейронных сетей

Предложена общая схема оценки защищенности объектов информатизации с использованием нейронных сетей. Определены частные и общие показатели оценки защищенности объектов информатизации.

Ключевые слова: защищенность объектов информатизации, нейронные сети.

При эксплуатации объектов информатизации (ОИ) в организациях на всех этапах жизненного цикла ОИ возникают проблемы обеспечения безопасности информации. Одной из задач обеспечения безопасности информации на ОИ является оценка состояния защищенности ОИ, позволяющая выявить недостатки системы защиты ОИ и принять соответствующие меры по противодействию дестабилизирующим факторам [6]. Решение задачи оценки защищенности зависит от степени влияния множества факторов, а поскольку неизвестна взаимосвязь между исходными показателями защищенности, то функцию итогового показателя сложно определить формально.

В нашей работе для решения обозначенной выше задачи предлагается применять искусственные нейронные сети (НС), так как использование традиционных вычислений трудоемко и слабо отражает реальные физические процессы и объекты.

Нужно отметить, что выделяют следующие частные задачи анализа защищенности ОИ [1, 4, 7]:

– оценка уровня защищённости информационных систем (ИС);

– определение наиболее незащищённых мест в ИС;

– разработка моделей нарушителей информационной безопасности (ИБ);

– анализ возможных угроз ИБ;

– оценка рисков ИБ ИС;

– выработка рекомендаций по повышению эффективности систем защиты ИС от внешних и внутренних угроз;

– прогнозирование попыток несанкционированного доступа в компьютерную систему;

– моделирование противоборства злоумышленника и специалиста по защите информации.

По итогам рассмотрения различных нейропакетов для анализа защищенности ОИ был выбран нейропакет Neural Network Toolbox системы Matlab. Он обладает возможностью автоматизации процесса поиска оптимальной НС для решения поставленной задачи. Общий алгоритм оценки защищенности ОИ с применением НС представлен на рис. 1.

Решение задачи анализа защищенности ОИ с применением НС можно рассмотреть поэтапно [2, 3]:

1. Постановка задачи в терминах НС. Проверка гипотезы о разумности применения НС для решения задачи, представление ожидаемого результата работы НС и способ его дальнейшего использования.

2. Выбор топологии сети. Выбирают тип сети, исходя из постановки задачи и имеющихся данных для обучения.

3. Подбор характеристик сети. Экспериментально подбирают параметры сети: число слоев, число блоков в скрытых слоях, наличие или отсутствие обходных соединений, передаточные функции нейронов и т.д.

4. Отбор данных, формирование обучающей выборки. В обучающую выборку включают данные, которые описывают условия, близкие к условиям дальнейшего использования нейросистемы.

5. Подбор параметров обучения. Значения параметров обучения выбирают экспериментально, руководствуясь при этом критерием завершения обучения (например, минимизация ошибки или ограничение по времени обучения).

6. Обучение НС. Обучение НС заключается в процессе представления НС обучающих данных.

7. Проверка адекватности обучения. Тестирование качества обучения НС проводится на примерах, которые не участвовали в ее обучении. Если полученные результаты существенно отличаются от ожидаемых, то необходимо вернуться к постановке задачи [2, 3].

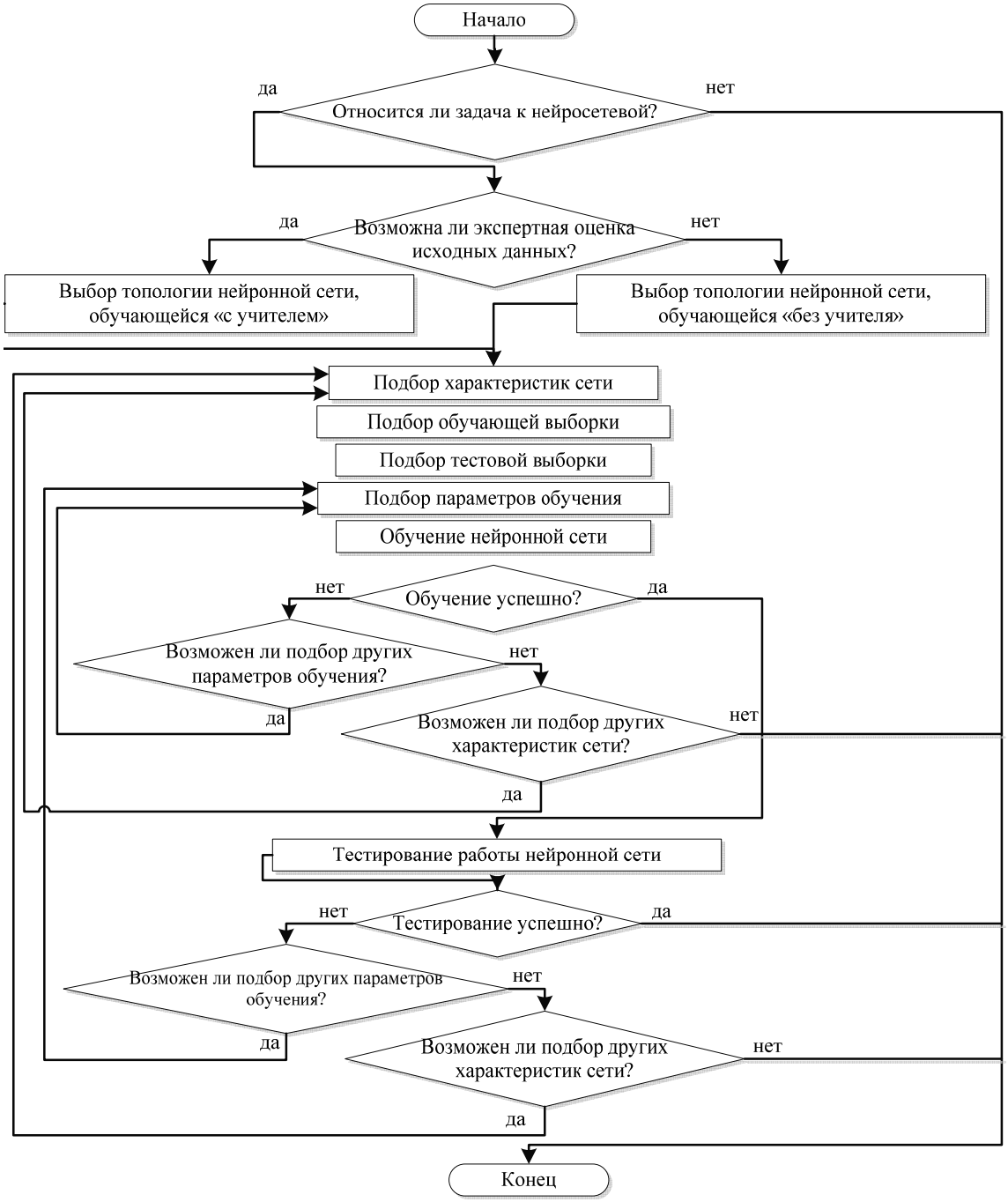


Рис. 1. Общий алгоритм оценки защищенности с использованием НС

Оценку защищенности ОИ выполняют с использованием отечественных и зарубежных методик, различных стандартов, в соответствии с которыми решение задачи сводят к анализу определенного количества показателей.

Предлагается осуществлять оценку уровня защищенности по следующим 8 групповым показателям: управление доступом; регистрация и учет; управление сетью; антивирусная защита; организация защиты персональных данных; контроль целостности и резервное копирование; физическая безопасность; криптографическая защита (при необходимости).

Для каждого направления оценки сформирован набор частных показателей. Всего выделено 79 частных показателей. Рассмотрим следующие частные показатели защищенности для направления «Контроль целостности и резервное копирование»:

1. Определены ли в документах организации, выполняются ли и контролируются ли процедуры контроля целостности?

2. Реализованы ли в системах, используемых в организации, защитные меры, обеспечивающие невозможность отказа от авторства проводимых сотрудниками операций и транзакций (например, электронная подпись (ЭП))?

3. Выполняется ли проверка целостности программного обеспечения, занимающегося обработкой критических данных (и самих данных)?

4. Определены ли в документации и осуществляются ли в организации процедуры регулярного резервного копирования информации?

5. Располагаются ли резервные копии вместе с инструкциями по восстановлению в месте, территориально отдаленном от основной копии информации?

6. Осуществляется ли регулярная проверка носителей, на которые осуществляется резервное копирование, на отсутствие сбоев?

7. Проводятся ли регулярные проверки процедур восстановления с целью поддержания возможности восстановления данных в установленном порядке и за гарантированный промежуток времени?

При оценке защищенности ОИ необходимо использовать экспертные оценки. Оценка должна основываться на свидетельствах, в качестве основных источников которых рекомендуется использовать:

– внутренние нормативные документы проверяемой организации и при необходимости документы третьих лиц, относящиеся к обеспечению ИБ организации;

– устные высказывания сотрудников проверяемой организации в процессе проводимых опросов;

– результаты наблюдений членов экспертной группы за деятельностью сотрудников проверяемой организации в области ИБ;

– результаты обследования экспертами ИС проверяемой организации;

– результаты использования экспертами инструментальных средств анализа защищенности.

Общая схема оценки защищенности ОИ представлена на рис. 2.

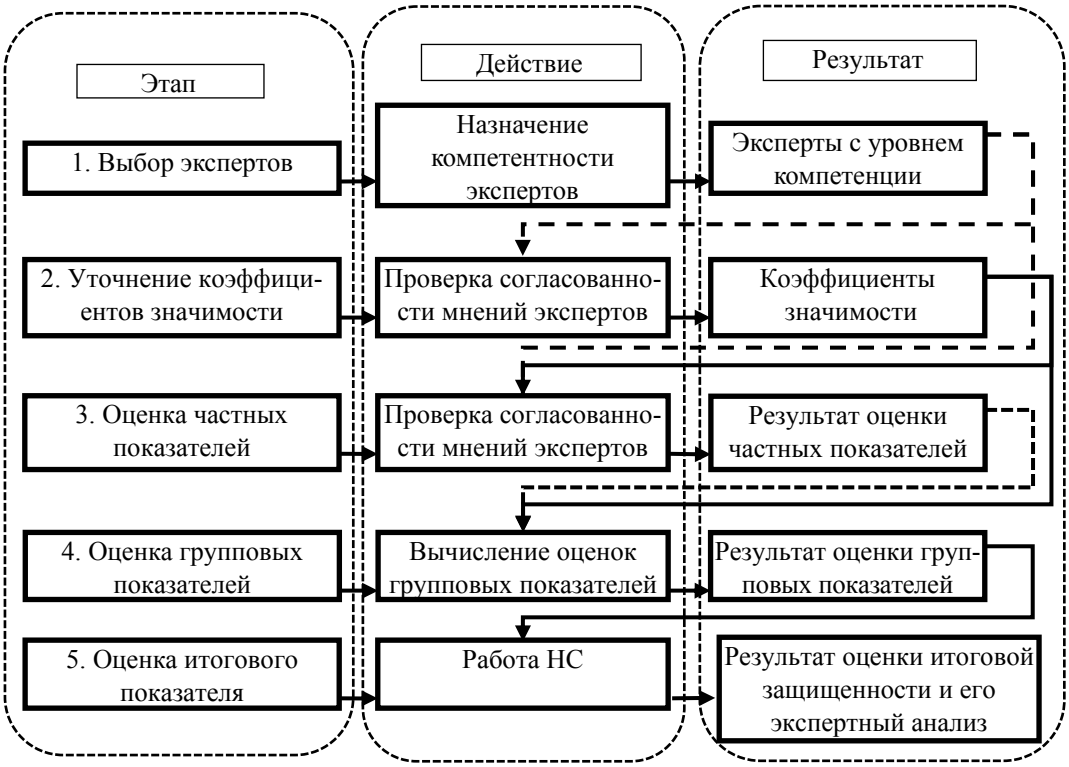


Рис. 2. Общая схема оценки защищенности ОИ с использованием НС

Сначала производят выбор экспертной группы. Формирование группы экспертов осуществляют из специалистов по обеспечению безопасности информации организации, обладающих достаточными знаниями. Эксперты имеют разную степень компетентности, которую учитывают при определении общей оценки частного показателя защищенности или коэффициента значимости частного показателя. Каждый эксперт независимо выставляет оценку каждому частному показателю (воз-

можные значения [0, 1]). После оценки согласованности мнений экспертов определяют итоговые оценки частных показателей с учетом степеней компетентности экспертов и оценки групповых показателей с учетом степеней коэффициентов значимости частных показателей. Групповые показатели оценивают как с использованием экспертных оценок, так и путем применения НС. Групповые показатели подают на вход НС и получают итоговый показатель оценки защищенности.

Предложена следующая архитектура НС [5]: полносвязная сеть прямого распространения «Многослойный персептрон», обучающаяся алгоритмом обратного распространения ошибки. Функция активации нейронов – логистическая. Количество слоев сети и число нейронов в каждом скрытом слое определялось экспериментально. Были смоделированы следующие НС:

– однослойная сеть с 8–16 скрытыми нейронами;

– двухслойная сеть с 8–24 нейронами в 1-м скрытом слое и с 8–20 нейронами во 2-м скрытом слое;

– трехслойная сеть с 12–24 нейронами в 1-м скрытом слое и с 12–20 нейронами во 2-м скрытом слое, с 8–16 нейронами в 3 скрытом слое.

Из рассмотренных НС была выбрана – двухслойная НС с 12 нейронами в 1-м скрытом слое, 8 нейронами во 2-м скрытом слое (ошибка обучения составляет 0,0862).

Результаты обучения нейронной сети: нейронная сеть обучена за 7 эпох, ошибка достигла 0,00862 при допустимой ошибке 0,01 на обучающей выборке.

Оценку защищенности ОИ организации проводили до и после применения мер по защите информации. Значения групповых показателей приведены в таблице.

Значения групповых показателей

Групповой показатель	Значения до применения защитных мер	Значения после применения защитных мер
Управление доступом	0,7786	0,909
Регистрация и учет	0,5403	0,777
Управление сетью	0,69	0,953
Антивирусная защита	0,9937	1
Организация защиты персональных данных	0,8897	0,9412
Контроль целостности и резервное копирование	0,4421	0,9671
Физическая безопасность	0,47525	0,667625
Криптографическая защита	0,8164	1

Значения групповых показателей были поданы на вход НС. В результате, значение итоговой защищенности, определенное с использованием НС без учета предложенных мер защиты, составляет 0,7344 и не является рекомендуемым. Защищенность с учетом предложенных мер защиты составляет 0,8765 и является рекомендуемой. Разность итоговых показателей определяет эффективность применения предложений защиты и составляет 0,1421, т.е. 14%.

На основе общей схемы оценки защищенности ОИ была разработана методика анализа защищенности ОИ, применение которой позволяет количественно оценить уровень защищенности ОИ, а также эффективность внедренных мер защиты. Методика позволяет выявить не поддающуюся формальному определению взаимосвязь между оцениваемыми показателями и степенью влияния каждого показателя на итоговую защищенность.

Методика может применяться для анализа защищенности ОИ уровня местного самоуправления города. Таким образом, методика анализа защищенности ОИ организации с использованием НС позволяет решить задачу количественной оценки защищенности и обосновать необходимость и (или) эффективность внедрения средств и мер защиты информации в организации.

Литература

1. Галушкин А.И. Нейрокомпьютеры в решении задач обеспечения информационной безопасности // Информационные технологии. – 2011. – № 1. – С. 34–38.

2. Крыжановский А.В. Применение искусственных нейронных сетей в системах обнаружения атак // Доклады ТУСУРа. – 2008. – Т. 2. – С. 104–105.

3. Нестерук Ф.Г. Основы организации адаптивных систем защиты информации: учеб. пособие. – СПб.: СПбГУ ИТМО, 2008. – 112 с.

4. Бахтин А.М. Возможные области применения нейронных сетей при оценке защищенности объектов информатизации / А.М. Бахтин, Е.Н. Пивкин // Измерение, контроль, информатизация: матер. XIV Междунар. науч.-техн. конф. / Под ред. Л.И. Сучковой. – Барнаул: Изд-во АлтГТУ, 2013. – Т. 2. – С. 172–174.

5. Бахтин А.М. Применение нейросетевого подхода для оценки защищенности объекта информатизации / А.М. Бахтин, Е.Н. Пивкин // Матер. X Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Наука и молодежь – 2013» [Электронный ресурс]. – Режим доступа: http://edu.secna.ru/media/f/vsib_tez_2013.pdf, свободный (дата обращения: 25.06.2013).

6. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 349 с.

7. Ерохин С.С. Модели и методы оценки защищенности информации и информационной безопасности объекта / С.С. Ерохин, Р.В Мещеряков, С.С. Бондарчук // Безопасность информационных технологий. – 2007. – № 4. – С. 39–46.

Пивкин Евгений Николаевич
Канд. техн. наук, главный специалист-эксперт отдела безопасности УФНС России по Московской обл.
Тел.: 8-906-942-02-17
Эл. почта: evpiv@yandex.ru

Белов Виктор Матвеевич
Д-р техн. наук, профессор каф. безопасности и управления в телекоммуникациях
Сибирского государственного университета телекоммуникаций и информатики
Тел.: 8 (383) 269-82-45
Эл. почта: vmbelov@mail.ru

Белкин Сергей Алексеевич
Аспирант каф. информационной безопасности
Новосибирского государственного университета экономики и управления «НИНХ»
Тел.: 8-913-772-86-23
Эл. почта: serega-box2011@yandex.ru

Pivkin E.N., Belov V.M., Belkin S.A.

On the issue of the analysis of the security of objects of informatization using neural networks

A general scheme of assessment of objects of informatization using neural networks is proposed. Private and global indicators for assessing the security object informatization are defined.

Keywords: protection of objects of informatization, neural networks.

УДК 343.983

В.В. Поляков, С.А. Лапин

Средства совершения компьютерных преступлений

С криминалистических позиций исследованы средства совершения компьютерных преступлений. Предложено их классифицирование по существенно различным критериям: по законности происхождения; по созданию; по техническому содержанию; по технологии использования; по стадии в преступлении. Типизация данных о средствах совершения компьютерных преступлений позволяет установить корреляционные связи между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений.

Ключевые слова: средства совершения компьютерных преступлений, расследование компьютерных преступлений, криминалистика.

Быстрое развитие компьютерных технологий сопровождается ростом компьютерной преступности и, что еще более важно, ее качественным изменением. Преступления совершаются более изощренными способами с применением специальных программно-аппаратных средств и сетевых технологий. Способы совершения компьютерных преступлений становятся высокотехнологичными за счет применения нетривиальных технических решений, а также принципиально новых или модифицированных программ [1]. Преступники творчески используют и модифицируют компьютерную технику и программное обеспечение. Результатом таких действий становится исключительно высокая латентность компьютерных преступлений [2].

Вопрос о средствах совершения компьютерных преступлений, рассматриваемых с криминалистических позиций, является малоизученным. От современной криминалистики требуется изучение причин, благодаря которым компьютерные преступления становятся возможными, анализ применяемых преступниками технологий, аппаратных и программных средств подготовки, совершения и сокрытия преступлений. Эти вопросы входят в криминалистическую характеристику компьютерных преступлений и являются предметом доказывания по данной категории уголовных дел. В настоящей работе проводится анализ средств совершения компьютерных преступлений и предлагается их возможная криминалистическая классификация.

Преступления в сфере компьютерной информации всегда совершаются с помощью средств компьютерной техники. Понятие этих средства является комплексным, включающим в себя компьютеры в различных вариантах их исполнения (ноутбуки, планшеты, смартфоны, и т.д.), компьютерные технологии (беспроводные Wi-Fi, Bluetooth, 3G, WiMAX и др.), а также компьютерное программное обеспечение, находящееся в открытом, запрещенном или ограниченном обороте и имеющее различное назначение (разрешенные и бесплатно распространяемые программы, например, Opera, Mozilla Firefox, вредоносные программы, например, SpyEye, Zeus, Carberp и т.д.). Следует отметить, что в настоящее время главную роль при совершении компьютерных преступлений выполняет программное обеспечение, а не аппаратные средства, которые сами по себе обычно не представляют опасности.

Как показывает современная практика, в большинстве случаев компьютерные преступления совершаются путем удаленного доступа по телекоммуникационным сетям с помощью обычной компьютерной техники, на которую устанавливается специальное программное обеспечение [3]. Это принципиальное обстоятельство имеет следствия, исключительно важные как для расследования, так и для предотвращения компьютерных преступлений. Так, в непосредственных (бессетевых) способах совершения преступлений аппаратные средства, например аппаратные кейлогеры или скиммеры для негласного съема информации, действуют лишь в отношении конкретного компьютерного устройства. Преступники хорошо знают, что при совершении преступления непосредственным образом остаются традиционные (материальные) следы, по которым можно будет их идентифицировать. Использование вредоносного программного обеспечения при удаленном доступе по информационным сетям позволяет осуществить преступление одновременно в отношении многих компьютеров. При таком доступе преступникам не нужно проникать в помещение, в котором нахо-

дится объект посягательства, при этом остаются не персонифицируемыми их электронно-цифровые следы. Электронно-цифровые следы всегда образуются и модифицируются в результате опосредованного воздействия компьютерных программ. Специфика этих следов проявляется в том, что они не имеют геометрической формы, цвета, запаха и иных характеристик, традиционно рассматриваемых криминалистикой, в которых могли бы отразиться отельные черты преступника, например его ДНК, запах, папиллярный узор и т.д. Таким образом, в механизме следообразования нет непосредственного следового контакта с преступником, его физическими и иными особенностями, так как компьютерная программа не несет на себе отпечатка конкретного человека, одни и те же электронно-цифровые следы-последствия могут быть образованы кем угодно. Несмотря на эту специфику, основным источником информации о средствах, применяемых в компьютерном преступлении, остаются именно конкретные следы и вся следовая картина в целом.

В настоящее время для совершения большинства компьютерных преступлений не требуется наличия средств преступления в виде дорогостоящей компьютерной техники. Практически каждый может найти в сети Интернет бесплатные вредоносные программы, включающие в себя необходимый для совершения преступления алгоритм действий. К таким программам могут прикладываться наглядные инструкции по их использованию. Эти обстоятельства в значительной степени способствуют росту числа совершаемых преступлений в сфере компьютерной информации [4]. Более того, помимо количества преступлений, меняется типичный портрет преступника в сторону лиц, не имеющих специального или высшего образования и постоянной работы [5–8].

Следственные органы, особенно на первоначальном этапе расследования компьютерных преступлений, редко располагают сведениями о средствах, используемых в преступлении. В отсутствие такой информации имеет важную роль для проведения расследования криминалистическая характеристика аналогичных преступлений. Ее практическое значение, проявляющееся в корреляционной взаимосвязи между структурными элементами преступления, дает основания строить следственные версии на основе использования имеющихся неполных данных. В компьютерных преступлениях выбор средств для их совершения обычно зависит от целого ряда факторов: объекта посягательства, принятого на нем режима охраны, применяемых технических и организационных средств охраны, программно-аппаратной защиты информации. Так как в большинстве случаев поводом для возбуждения уголовных дел являются заявления потерпевших, то следствию становится известен объект посягательства. Его исследование может пролить свет на способ совершения преступления или примененные преступником программно-аппаратные средства. Анализ судебно-следственной практики показывает, что типичные (относительно простые) или, наоборот, высокотехнологичные способы совершения преступлений могут осуществляться характерными для них программно-аппаратными средствами. Возможна также обратная ситуация, когда данные о средствах преступления известны и помогают строить следственные версии о других искомых элементах преступления. Например, конкретные средства совершения преступления могут указывать на применяемый преступниками способ совершения преступления, а также время и место его осуществления.

Средства, которые используются при совершении преступлений в сфере компьютерной информации, достаточно разнообразны. Важно также, что с криминалистических позиций их можно классифицировать по существенно различным критериям: по законности происхождения; по созданию; по техническому содержанию; по технологии использования; по стадии в преступлении и др. Это обусловливает необходимость разработки системы криминалистической классификации. В целях повышения эффективности расследования компьютерных преступлений разнообразные средства их совершения следует классифицировать, учитывая их основные особенности (таблица).

Как следует из таблицы, средства, предназначенные для полного или частичного управления компьютером и доступа к хранимой на нем информации предлагается прежде всего разграничить на две основные группы – законные и незаконные. Законные (разрешенные для использования) средства могут быть свободно распространяемыми, находиться в ограниченном обороте или быть изъятыми из оборота. Некоторые такие программные средства могут входить в состав операционной системы или устанавливаться самими пользователями дополнительного. Ограниченные в гражданско-правовом обороте средства, например, предназначенные для негласно получения информации путем видеоаудиозаписи, могут быть приобретены при наличии соответствующего разрешения. Использование изъятых из оборота специальных средств может быть разрешено органам оперативно-розыскной деятельности или иным государственным органам (например, следственному коми-

тету, прокуратуре, суду, экспертным учреждениям), однако создавать, владеть, пользоваться и распоряжаться такими средствами гражданам запрещено законом, т.е. их использование гражданами является незаконным.

Криминалистическая классификация средств совершения компьютерных преступлений

По законности происхождения		По созданию			По техническому содержанию			По технологии использования		По стадии в преступлении			
Законные	Незаконные	Готовые	Модифицированные	Собственной разработки	Аппаратные	Программно-аппаратные	Программные	Без удаленного доступа	С удаленным доступом	При подготовке	При совершении	При сокрытии	При противодействии следствию

Преступниками может применяться не только широкий перечень готового программно-аппаратного обеспечения, в том числе модифицированного, но и собственные уникальные разработки. Это наиболее характерно для высокотехнологичных способов совершения компьютерных преступлений, при которых используются компьютерные программы, созданные членами преступной группы или посторонними специалистами по заказу преступников. В этом случае речь идет прежде всего о так называемых шеллах (shell), которые позволяют преступнику выполнять ограниченный круг команд по управлению автоматизированным рабочим местом (например, выполнить какое-либо действие командной оболочки операционной системы и т.п.).

По техническому содержанию рассматриваемые средства могут быть условно разделены на аппаратные, программные и программно-аппаратные. При незаконном доступе к объекту посягательства использование чисто аппаратных средств мало распространено, так как современные компьютерные устройства обычно обладают каким-либо собственным программным обеспечением. Как показывает судебно-следственная практика, примерами программно-аппаратных устройств выступают скиммеры и кейлогеры. Скиммеры используют для кражи реквизитов банковских карт. Как правило, скиммер состоит из двух компонентов – устройства для считывания данных хранящейся на магнитной полосе банковской карты и устройства, позволяющего скопировать пин-код. Некоторые скиммеры оснащены инструментами беспроводной связи, с помощью которой злоумышленники получают информацию в реальном времени, а не хранят ее непосредственно на скиммере. Кейлогеры представляют собой устройства, которые позволяют перехватывать данные, вводимые с клавиатуры. Они выполняются в различных вариантах и могут хранить полученную информацию в собственной памяти или быть оснащены средствами беспроводной связи. Программное обеспечение, используемое для незаконного доступа к компьютерной информации, может быть признано вредоносным только судом. Отметим, что четкого определения вредоносного программного обеспечения в ст. 273 УК РФ не дается, что требует отдельного рассмотрения.

При проведении расследовании целесообразно учитывать, что конкретные средства совершения компьютерных преступлений могут использоваться только на определенных стадиях – подготовки к преступлению, непосредственно при его совершении, при сокрытии преступления, при противодействии следствию в условиях оперативно-розыскных мероприятий или следственных действий. Так, на стадии подготовки преступники изучают обстановку объекта посягательства, физический режим его охраны (замки, контроль сотрудниками, видеонаблюдение, сигнализацию), пытаются собрать информацию о действующих устройствах и программах информационной безопасности (системах идентификации и аутентификации), готовят хранилища для переноса охраняемой информации (flash носители, облачные хранилища и пр.), средства сокрытия и уничтожения следов своей деятельности (например, размагничивание жесткого диска). На этой стадии могут применяться специальные программы, исследующие и оценивающие объект посягательства с точки зрения его защищенности внешним угрозам (например, программы-шпионы типа Zeus). Непосредственно на этапе совершения преступления соответствующие средства направлены на получение преступником возможности управлять автоматизированным рабочим местом потерпевшего. Для получения неправомерного доступа преступники могут использовать программы, предназначенные для администраторов (TeamViewer, Radmin, TightVNC и т.п.), специализированные клиенты сетевых протоколов RDP (Remote Desktop Protocol) или VNC (Virtual Network Computing), имеющие собственный web-интерфейс для администрирования и управления, либо модификации вредоносного программ-

ного обеспечения, например Zeus, Carberp и т.п. Опасной разновидностью вредоносного программного обеспечения, позволяющего получить неправомерный доступ к автоматизированному рабочему месту, являются эксплойты, под которыми понимается программный код или его фрагмент, который через ошибки в каком-либо программном обеспечении, работающем на объекте посягательства, приводит к выполнению этим программным обеспечением действия, непредусмотренного разработчиками. При попытке массового заражения рабочих мест через использование web-сервисов применяются инструменты, которые включают в себя наборы эксплойтов, нацеленные на эксплуатацию ошибок в web-браузерах и различного рода расширений к ним (Adobe Flash, ActiveX и т.п.).

Сокрытие преступления, отдельных следов-последствий и участия в нем преступника может реализовываться во время совершения преступления и после него. Для этой цели могут применяться различные элементы маскировки, например: программно-аппаратный сбой, противоправные действия иных лиц и многое другое. Отметим, что для сокрытия электронно-цифровых следов может применяться не только вредоносное, но и законное программное обеспечение, например, позволяющее безвозвратно удалять информацию с носителя путем многократной ее перезаписи. Как правило, сокрытие сводится к попытке затруднить определение местонахождения преступников. Подобная цель может достигаться путем использования сервисов, позволяющих осуществить подмену реального IP-адреса на другой. Популярностью у преступников пользуются услуги предоставления доступа к сети, работающей по протоколу VPN. Современные VPN-сервисы предоставляют доступ к сети путем использования цепочки промежуточных серверов (Double/Triple-VPN), что значительно затрудняет определение реального IP-адреса преступника. В случаях, когда не требуется высокая пропускная способность канала связи, преступник может отдать предпочтение таким технологиям, как Tor, ввиду бесплатного предоставления анонимности при работе в телекоммуникационных сетях.

Исследование средств совершения компьютерных преступлений с позиций криминалистики, их типизация и классификация позволяют установить корреляционные связи между обстоятельствами, подлежащими установлению и доказыванию по уголовным делам, что способно повысить эффективность расследования подобных преступлений.

Работа выполнена по гранту Президента Российской Федерации для государственной поддержки молодых российских ученых МК7026.2013.6.

Литература

1. Поляков В.В. Характеристика высокотехнологичных способов совершения преступлений в сфере компьютерной информации: матер. ежег. Всерос. науч.-практ. конф., посвященной 50-летию юридического факультета и 40-летию Алтайского государственного университета «Уголовно-процессуальные и криминалистические чтения на Алтае». – Барнаул: Изд-во Алт. ун-та, 2012. – Вып. 11–12. – С. 123–126.

2. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями // Российский следователь. – 2012. – № 24. – С. 43–46.

3. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114–116.

4. Internet security threat report 2013 [Электронный ресурс]. – Режим доступа: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf, свободный (дата обращения: 01.05.2014).

5. Уголовное дело № 706/09 // Архив Железнодорожного районного суда г. Барнаула. – 2009.

6. Уголовное дело № 1-179/06 // Архив суда г. Алейска. – 2006.

7. Уголовное дело № 1-337/2011 // Архив суда г. Новоалтайска. – 2011.

8. Уголовное дело № 2-23/2011 // Архив суда г. Камень-на-Оби. – 2011.

Поляков Виталий Викторович
Канд. юрид. наук, доцент каф. уголовного процесса и криминалистики
Алтайского государственного университета (АлтГУ)
Тел.: 8 (385-2) 36-64-52
Эл. почта: vvpagu@rambler.ru

Лапин Сергей Александрович
Аспирант каф. прикладной физики, электроники и информационной безопасности АлтГУ
Тел.: 8 (385-2) 36-40-65
Эл. почта: lapinsa567@gmail.com

Polyakov V.V., Lapin S.A.
Means of committing computercrimes

In this paper means of committing computer crimes were investigated dealing with criminalistics. Autor made classification for their different criteria: legal emergence; development; technical content; technology use; stages of the crime. Typing information about means of committing computer crimes makes correlation between the established circumstances and evidence in the criminal cases. It can raise the effectiveness of the investigation of such crimes.
Keywords: means of committing computer crimes, computer crime investigation, criminalistics.

УДК 004.056

А.С. Поморцев

Методика оценки рисков нарушения информационной безопасности организации с учётом квалификации экспертов

Предложена методика учёта квалификации экспертов при проведении оценки рисков нарушения информационной безопасности (ИБ) организации. Предложен подход для расчёта количественной и качественной оценки рисков нарушения ИБ организации.
Ключевые слова: информационная безопасность, оценка рисков, квалификация экспертов.

Оценка рисков нарушения ИБ для организаций различных форм собственности и сфер деятельности позволяет:

– обеспечивать поддержание системы ИБ в актуальном состоянии;

– определять целесообразность экономических затрат на обеспечение ИБ;

– проводить оценку эффективности внедрения новых технических средств обеспечения ИБ;

– повышать имидж компании и доверие клиентов.

Для формирования оценки используются две составляющие – количественная и качественная. Количественная оценка необходима для определения конкретной величины риска, а качественная – для интерпретации полученного результата.

Поскольку эксперты, проводящие оценку, могут обладать различной квалификацией, необходимо её учитывать для повышения точности конечного результата. В этой связи актуальной задачей является разработка новой методики оценки рисков нарушения ИБ [1].

Количественная оценка. В работе [2, 3] была приложена система из 25 групповых параметров N, характеризующих инфраструктуру обеспечения ИБ. Каждый групповой параметр N_i включает в себя ряд частных показателей EV_{N_i} в виде конкретных требований по обеспечению ИБ. Перечень групповых параметров и частных показателей может меняться в зависимости от специфики конкретной организации.

Частные показатели EV_{N_i}, входящие в каждый групповой параметр N_i, неравнозначны. Это обусловлено тем, что на практике выполнение некоторых требований по обеспечению ИБ может быть намного важнее других. Например, обеспечение контроля доступа на территорию организации важнее, чем обеспечение контроля доступа к персональному компьютеру работника, так как, если злоумышленник не сможет попасть на территорию организации, то он не сможет получить физический доступ к компьютеру сотрудника. Важность группового показателя по сравнению с другими характеризуется коэффициентом значимости α_{ij}, при этом должно учитываться условие нормировки

$$\sum_{j=1}^{k} \alpha_{ij} = 1 . \qquad (1)$$

Степень выполнения частных показателей x_n определяется экспертом (или множеством экспертов) по шкале с 5 уровнями градации (0; 0,25; 0,5; 0,75; 1) в зависимости от степени фактического выполнения и документирования.

Особенностью данного подхода является то, что коэффициенты значимости α_{ij} и степень выполнения частных показателей x_n определяются экспертами. В этой связи предъявляются особые требования к квалификации экспертов, что существенно ограничивает сферу применения данного подхода.

Решение данной проблемы предлагается осуществить за счёт увеличения числа экспертов с проведением предварительной оценки их квалификации. Квалификация экспертов оценивается по двум составляющим:

– выполнение формальных признаков (стаж работы, число часов повышения квалификации за последние два года и т.д.);

– тестирование (на знание предметной области, действующей нормативно-технической документации и законодательства).

По результатам прохождения оценки квалификации предлагается разделять экспертов на 3 уровня, с присвоением соответствующего коэффициента y_n:

– эксперты с высокой квалификацией ($y=2$);

– эксперты со средней квалификацией ($y=1{,}5$);

– эксперты с низкой квалификацией ($y=1$).

Это означает, что при проведении оценки рисков нарушения ИБ мнение эксперта с высокой квалификацией будет иметь условный вес в 2 раза больше, чем эксперта с низкой квалификацией.

Таким образом, численное значение степени выполнения частного показателя S, с учётом квалификации экспертов, будет рассчитываться по следующей формуле:

$$S=\frac{\sum x_n y_n}{\sum y_n}. \tag{2}$$

Значение частного показателя EV_{N_i} будет рассчитываться как произведение численного значения степени его выполнения и коэффициента значимости:

$$EV_{N_i}=\alpha_{ij}\frac{\sum x_n y_n}{\sum y_n}. \tag{3}$$

Значение группового параметра N_i будет рассчитываться как сумма всех входящих в него частных показателей:

$$N_i=\sum_{i=1}^{k}\alpha_{ij}\frac{\sum x_n y_n}{\sum y_n}. \tag{4}$$

Среднее значение группового параметра D находится по формуле

$$D=\sum_{j=1}^{N}\sum_{i=1}^{k}\alpha_{ij}\frac{\sum x_n y_n}{\sum y_n}\Bigg/N. \tag{5}$$

Для дальнейших расчётов принимаем следующее условие – в случае полного выполнения всех требований по обеспечению ИБ, определённых множеством частных показателей, риск нарушения ИБ организации $R\to 0$. В таком случае формула для расчёта процентного значения величины риска нарушения ИБ будет иметь вид

$$R=(1-D)\times 100. \tag{6}$$

В результате расчёт количественной оценки рисков нарушения ИБ организации принимает вид

$$R=\left(1-\sum_{j=1}^{N}\sum_{i=1}^{k}\alpha_{ij}\frac{\sum x_n y_n}{\sum y_n}\Bigg/N\right)\times 100. \tag{7}$$

Качественная оценка рисков нарушения ИБ. Для перехода от количественной оценки к качественной предлагается использовать метод неравномерных шкал [4]. Пусть качественная шкала оценки рисков имеет 5 уровней градации («низкий», «ниже среднего», «средний», «выше среднего», «высокий»), затем устанавливается соотношение между количественной и качественной оценками, представленное в таблице.

Таблица соответствия между количественными и качественными оценками

Уровень риска	Риск нарушения ИБ, %
Низкий уровень риска	0–5
Уровень риска ниже среднего	5–15
Средний уровень риска	15–30
Уровень риска выше среднего	30–50
Высокий уровень риска	50–100

Графическое представление соотношения количественной и качественной оценок показано на рис. 1.

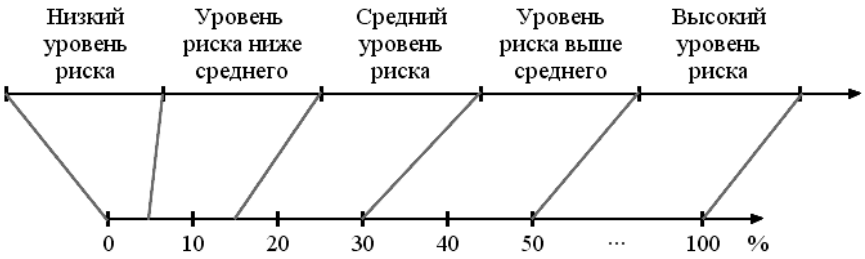


Рис. 1. Шкала соответствия качественных и количественных значений

В качестве апробации данной методики была проведена оценка рисков нарушения ИБ следующих организаций:

– ФГОБУ ВПО «СибГУТИ» (количественная оценка составила 66%, качественная – «высокий уровень риска»);

– ООО «Сибирский Центр Госзаказа» (количественная оценка риска составила 9,8%, качественная оценка – «уровень риска ниже среднего»). Данная оценка признана приемлемой, что подтверждается актом о проведении апробации.

По результатам проведения апробации были разработаны рекомендации в виде организационных и технических мер, направленных на снижение риска нарушения ИБ организации.

Заключение. В результате проведённых исследований можно сделать следующие выводы:

1. Поскольку эксперты могут обладать разной квалификацией, необходимо её учитывать при проведении оценки рисков нарушения ИБ.

2. Предложенная формула для расчёта количественной оценки риска нарушения ИБ позволяет учитывать квалификацию экспертов.

3. Для перехода от количественной оценки к качественной предложено использовать метод неравномерных шкал.

Литература

1. Поморцев А.С. Анализ методик оценки рисков предприятия // Материалы российской НТК «Современные проблемы телекоммуникаций», 25–26 апреля 2013 г. – Новосибирск: СибГУТИ, 2013. – С. 311–312.

2. Поморцев А.С. Об оценке рисков нарушений требований по обеспечению информационной безопасности предприятий телекоммуникационного профиля / А.С. Поморцев, А.А. Киселёв // Интернет-журнал «Технологии техносферной безопасности». – 2013. – № 3 (49). – С. 1–5.

3. Анализ и выбор параметров оценки рисков нарушения информационной безопасности организаций / С.Н. Новиков, А.А. Киселёв, А.С. Поморцев, О.В. Корзун // Ваш надежный партнер: информ. бюл. Новосиб. гор. торгово-пром. палаты. – 2013. – № 2 (69). – С. 11–12.

4. Сергеев А.Г. Метрология. Стандартизация. Сертификация: учеб. пособие для вузов / А.Г. Сергеев, М.В. Латышев, В.В. Терегеря. – М.: Логос, 2005. – 559 с.

Поморцев Антон Сергеевич
Аспирант каф. безопасности и управления в телекоммуникациях
Сибирского государственного университета телекоммуникаций и информатики (СибГУТИ), Новосибирск
Тел.: +7 (383) 2-69-82-45
Эл. почта: pomortsev.anton@gmail.com

Pomortsev A.S.

Risk assessment methodology violations of information security with regard to the qualifications of Experts

A method for accounting qualification of experts in risk assessment of information security violations is proposed. An approach for calculating the quantitative and qualitative assessment of risks of violation of information security is proposed.

Keywords: information security, risk assessment, qualification of experts.

УДК 004.056

А.С. Поморцев, С.Н. Новиков

Разработка системы параметров оценки рисков нарушения информационной безопасности организаций

Представлено решение проблемы оценки рисков нарушения информационной безопасности (ИБ) коммерческих организаций на основе нормативно-технических требований действующих стандартов и рекомендаций в области ИБ. Проведён обзор рынка программных продуктов по автоматизации оценки рисков, результаты которого указывают на необходимость разработки нового программного продукта, учитывающего чётко сформулированный перечень параметров оценки рисков нарушения ИБ.

Ключевые слова: информационная безопасность, оценка рисков.

На данный момент существует множество программных продуктов для оценки различных рисков организации. В этой связи возникает актуальная задача анализа возможностей данных программных продуктов применительно к современным требованиям обеспечения ИБ и оценки рисков её нарушения. В случае необходимости нужно разработать систему параметров оценки рисков нарушения ИБ организации.

Обзор рынка программных продуктов для оценки рисков. Из всего многообразия программных продуктов для оценки рисков активов организаций, которые представлены на отечественном рынке, можно выделить следующие:

– «Гриф 2006» [1] разработан с использованием международных стандартов ISO 17799–2000, ISO 17799–2005 и ISO 27001–2005;

– комплексная экспертная система управления информационной безопасностью «АванГард» [2] сочетает в себе положения ISO 15408–2002, ISO 17799, ISO 27001–2005, а также выборочные требования СТО БР ИББС-1.10–2007.

Многие из перечисленных стандартов на данный момент устарели или имеют новые версии. Поэтому использование основанных на них программных продуктов нецелесообразно.

Международные разработки (OCTAVE [3], CRAMM [4], RiskWatch [5], COBRA [6], «RA2 the art of risk» [7] и др.) редко используются отечественными организациями из-за:

– трудностей, связанных с русификацией интерфейса;

– отсутствия техподдержки на территории РФ;

– высоких требований к квалификации эксперта.

Перечисленные программные продукты предназначены для общей оценки рисков различных активов, а не для оценки рисков нарушения ИБ организаций.

Таким образом, актуальной задачей является разработка нового программного продукта для оценки рисков нарушения ИБ организаций.

Анализ нормативно-технической документации. В разрабатываемом программном продукте фундаментом для получения оценки являются параметры, по которым производится анализ состояния ИБ организации. В стандартах и нормативных документах, регламентирующих сферу ИБ в РФ, нет конкретного перечня параметров для проведения оценки. Поэтому первым этапом в создании нового программного продукта является формирование перечня параметров оценки рисков нарушения ИБ организаций.

Для формирования данного перечня проведён анализ международных, российских стандартов и рекомендаций [8–20]. Выбор документов осуществлялся на основе их актуальности и востребованности специалистами в области ИБ.

Проведенный анализ данных документов (с позиций обеспечения ИБ организаций) позволил сделать следующие выводы:

1) стандарты [8–17] носят общий, рекомендательный характер;
2) наибольшей практической значимостью обладают стандарты Банка России [18–20];

3) все стандарты и рекомендации, с учетом их характерных особенностей и практической значимости, можно разделить на три группы (табл. 1).

Таблица 1

Результаты анализа стандартов

Группа	Наименование стандартов/рекомендаций	Характерные особенности
Первая	ГОСТ Р ИСО/МЭК 17799–2005 ГОСТ Р ИСО/МЭК 13335-1–2006 ГОСТ Р ИСО/МЭК 13335-5–2006 ГОСТ Р 52448–2005 Рекомендация МСЭ-Т X.805–2003	– Поверхностное рассмотрение основных аспектов ИБ; – низкая практическая ценность; – отсутствие конкретных требований ИБ; – носят общий, рекомендательный характер
Вторая	ISO/IEC 27001–2006 ISO/IEC 27002–2007 ISO/IEC 27005–2008 ГОСТ Р ИСО/МЭК 13569–2007 ГОСТ Р ИСО/МЭК 15408–2008	– Хорошо структурированное представление информации; – сформирована чёткая концепция ИБ; – начинают выделяться конкретные требования и рекомендации для практического применения
Третья	СТО БР ИББС-1.0–2010 СТО БР ИББС-1.2–2010 РС БР ИББС-2.2–2009	– Высокая практическая ценность; – список конкретных требований и параметров для обеспечения ИБ; – наличие методики количественной оценки параметров ИБ

В результате проведенного анализа нормативно-технической документации в качестве базового стандарта для выбора параметров оценки рисков нарушения ИБ организаций был выбран СТО БР ИББС-1.0–2010.

Анализ и выбор параметров оценки рисков нарушения ИБ. Результаты сопоставительного анализа стандартов [8–17] с СТО БР ИББС-1.0–2010 сведены в табл. 2.

Условные обозначения к табл. 2:

да – групповой параметр освещён стандартом в полной мере;

ч-но – групповой параметр освещён стандартом частично;

нет – групповой параметр в стандарте не рассматривается.

Таблица 2

Результаты сравнения стандартов с базовым стандартом

№ параметр по ИББС	№ нового параметра	Стандарт/рекомендация								
		17799–2005	27001–2006	52448–2005	27005–2007	27002–2007	X.805	15408–2008	13335-1,5–2006	13569–2007
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
M1	N1	**да**	**нет**	**нет**	**нет**	**да**	**нет**	**нет**	**нет**	**ч-но**
M2	нет	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**	**ч-но**	**да**	**нет**
M3	N2	**ч-но**	**нет**	**нет**	**нет**	**да**	**нет**	**ч-но**	**ч-но**	**ч-но**
M4	N3	**да**	**нет**	**нет**	**нет**	**да**	**нет**	**нет**	**ч-но**	**нет**
M5	N4	**ч-но**	**нет**	**нет**	**нет**	**да**	**нет**	**нет**	**нет**	**ч-но**
M6	N5	**нет**	**нет**	**нет**	**нет**	**да**	**нет**	**да**	**нет**	**да**
M7	нет	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**	**ч-но**
M8	нет	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**	**ч-но**
M9	N6	**ч-но**	**нет**	**да**	**нет**	**ч-но**	**нет**	**ч-но**	**нет**	**нет**
M10	нет	**нет**	**нет**	**да**	**нет**	**ч-но**	**нет**	**ч-но**	**нет**	**нет**
M11	N7	**ч-но**	**ч-но**	**нет**	**нет**	**нет**	**нет**	**нет**	**да**	**нет**
M12	N8	**нет**	**нет**	**ч-но**	**ч-но**	**нет**	**нет**	**ч-но**	**нет**	**нет**
M13	N9	**нет**	**нет**	**да**	**да**	**ч-но**	**нет**	**нет**	**нет**	**ч-но**
M14	N10	**ч-но**	**нет**	**нет**	**да**	**да**	**нет**	**нет**	**нет**	**ч-но**
M15	N11	**ч-но**	**ч-но**	**нет**	**ч-но**	**ч-но**	**нет**	**нет**	**ч-но**	**ч-но**

Продолжение табл. 1

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
M16	N12	**нет**	**ч-но**	**ч-но**	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**
M17	N13	**ч-но**	**ч-но**	**нет**	**нет**	**нет**	**нет**	**нет**	**да**	**ч-но**
M18	N14	**да**	**нет**	**нет**	**нет**	**ч-но**	**нет**	**нет**	**нет**	**ч-но**
M19	N15	**ч-но**	**нет**	**нет**	**ч-но**	**ч-но**	**нет**	**нет**	**нет**	**ч-но**
M20	N16	**да**	**нет**	**нет**	**нет**	**да**	**нет**	**ч-но**	**нет**	**ч-но**
M21	N17	**нет**	**ч-но**	**нет**	**ч-но**	**ч-но**	**нет**	**да**	**нет**	**ч-но**
M22	N18	**ч-но**	**ч-но**	**нет**	**нет**	**ч-но**	**нет**	**нет**	**нет**	**нет**
M23	N19	**ч-но**	**ч-но**	**нет**	**нет**	**ч-но**	**нет**	**ч-но**	**нет**	**ч-но**
M24	N20	**нет**	**ч-но**	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**	**ч-но**
M25	N21	**нет**	**да**	**нет**	**нет**	**нет**	**нет**	**нет**	**ч-но**	**нет**
M26	N22	**нет**	**ч-но**	**нет**	**нет**	**ч-но**	**нет**	**нет**	**нет**	**ч-но**
M27	N23	**нет**	**ч-но**	**нет**	**нет**	**ч-но**	**нет**	**нет**	**нет**	**ч-но**
M28–M34	N24	**нет**	**ч-но**	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**	**нет**
нет	N25	**да**	**нет**	**нет**	**нет**	**да**	**нет**	**ч-но**	**нет**	**да**

В стандарте банка России [19] определено 34 групповых параметра, каждый из которых включает в себя от 4 до 32 показателей ИБ (M1–M34). В итоговом списке параметров оценки рисков нарушения ИБ:

– групповые параметры M2, M7, M8, M10 не включены, так как они носят банковскую специфику;

– групповые параметры M28–M34 объединены в параметр N24, так как все они ориентированы на оценку деятельности руководства организации;

– добавлен параметр, регламентирующий физическую безопасность предприятия (N25), так как он отсутствует в СТО БР ИББС-1.0–2010.

Таким образом, итоговый список параметров оценки рисков нарушения ИБ включает в себя 25 групповых параметров, представленных в табл. 3.

Таблица 3

Параметры оценки рисков нарушения ИБ

№ параметра	Наименование параметра
1	*2*
N1	Обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу
N2	Обеспечение ИБ при управлении доступом и регистрации
N3	Обеспечение ИБ средствами антивирусной защиты
N4	Обеспечение ИБ при использовании ресурсов сети Интернет
N5	Обеспечение ИБ при использовании средств криптографической защиты информации
N6	Общие требования по обработке персональных данных в организации
N7	Организация и функционирование службы ИБ организации
N8	Определение/коррекция области действия системы обеспечения ИБ
N9	Выбор/коррекция подхода к оценке рисков нарушения ИБ и проведению оценки рисков нарушения ИБ
N10	Разработка планов обработки рисков нарушения ИБ
N11	Определение/коррекция внутренних документов, регламентирующих деятельность в области обеспечения ИБ
N12	Принятие руководством организации решений о реализации и эксплуатации системы обеспечения ИБ
N13	Организация реализации планов внедрения системы обеспечения ИБ
N14	Разработка и организация реализации программ по обучению и повышению осведомлённости в области ИБ
N15	Организация реагирования на инциденты безопасности
N16	Организация обеспечения непрерывности бизнеса и его восстановления после прерываний

Продолжение табл. 4

1	*2*
N17	Мониторинг и контроль защитных мер
N18	Проведение самооценки ИБ
N19	Проведение аудита ИБ
N20	Анализ функционирования системы обеспечения ИБ
N21	Анализ системы обеспечения ИБ со стороны руководства организации
N22	Принятие решений по тактическим улучшениям системы обеспечения ИБ
N23	Принятие решений по стратегическим улучшениям системы обеспечения ИБ
N24	Оценка деятельности руководства организации
N25	Физическая безопасность

Заключение. В данный момент ведётся разработка программного продукта, который будет обладать следующими особенностями:

– автоматизация процедуры оценки рисков;

– оценка должна проводиться на основе сформированного перечня параметров (см. табл. 3);

– низкие требования к квалификации эксперта;

– представление итоговой оценки в наглядной форме;

– возможность лёгкой адаптации к требованиям новых или обновлённых нормативных документов по ИБ;

– формирование по результатам работы программы списка рекомендаций по улучшению системы обеспечения ИБ организации.

Обладая перечисленными особенностями, новый программный продукт позволит наиболее эффективно проводить оценку рисков нарушения ИБ организаций.

Литература

1. Современные методы и средства анализа и управление рисками информационных систем компаний [Электронный ресурс]. – Режим доступа http://dsec.ru/ipm-research-center/article/modern_methods_and_means_for_analysis_and_risk_management_of_information_systems_of_companies/, свободный (дата обращения: 09.04.2014).

2. Бурдин О.А., Кононов А.А. Комплексная экспертная система управления информационной безопасностью «АванГард» [Электронный ресурс]. – Режим доступа http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/5b998f309fa7de60c3256d5700403137, свободный (дата обращения: 09.04.2014).

3. OCTAVE [Электронный ресурс]. – Режим доступа http://www.cert.org/octave/, свободный (дата обращения: 09.04.2014).

4. CRAMM [Электронный ресурс]. – Режим доступа http://www.cramm.com/downloads/datasheets.htm, свободный (дата обращения: 09.04.2013).

5. Information Systems (ISO 27001 & NIST 800-53) [Электронный ресурс]. – Режим доступа http://www.riskwatch.com/, свободный (дата обращения: 09.04.2014).

6. Security Risk Analysis & Assessment, and ISO 27000 Compliance [Электронный ресурс]. – Режим доступа http://www.riskworld.net/, свободный (дата обращения: 09.04.2014).

7. RA2 art of risk [Электронный ресурс]. – Режим доступа http://xn----7sbab7afcqes2bn.xn--p1ai/content/ra2-art-risk, свободный (дата обращения: 09.04.2014).

8. ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Практические правила управления информационной безопасностью. – М.: Стандартинформ, 2006. – 56 с.

9. Международный стандарт ISO/IEC 27001–2005. Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования. – М.: Технорматив, 2006. – 54 с.

10. Международный стандарт ISO/IEC 27002–2007. Информационные технологии. Свод правил по управлению защитой информации. – М.: Технорматив, 2007. – 171 с.

11. Международный стандарт ISO/IEC 27005–2008. Информационные технологии. Методы защиты. Менеджмент рисков информационной безопасности. – ISO/IEC 2008. – 70 с.

12. ГОСТ Р 52448–2005. Защита информации. Обеспечение безопасности сетей электросвязи. – М.: Стандартинформ, 2006. – 20 с.

13. ГОСТ Р ИСО/МЭК 15408–2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – М.: Стандартинформ, 2006. – 41 с.

14. ГОСТ Р ИСО/МЭК 13335-1–2006. Информационная технология. Методы и средства обеспечения безопасности. Ч. 1: Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. – М.: Стандартинформ, 2007. – 19 с.

15. ГОСТ Р ИСО/МЭК ТО 13335-5–2006. Информационная технология. Методы и средства обеспечения безопасности. Ч. 5: Руководство по менеджменту безопасности сети. – М.: Стандартинформ, 2007. – 27 с.

16. ГОСТ Р ИСО/МЭК 13569–2007. Финансовые услуги. Рекомендации по информационной безопасности. – М., 2007. – 86 с.

17. Рекомендация МСЭ-Т Х.805. Безопасность. Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами. – Швейцария, Женева, 2004. – 21 с.

18. Стандарт Банка России. СТО БР ИББС-1.0–2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – М., 2010. – 42 с.

19. Стандарт Банка России. СТО БР ИББС-1.2–2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0.2010. – М., 2010. – 74 с.

20. Рекомендация в области стандартизации Банка России. РС БР ИББС-2.2–2009. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности. – М., 2009. – 23 с.

Поморцев Антон Сергеевич
Аспирант каф. безопасности и управления в телекоммуникациях
Сибирского государственного университета телекоммуникаций и информатики (СибГУТИ), Новосибирск
Тел.: +7 (383) 2-69-82-45
Эл. почта: pomortsev.anton@gmail.com

Новиков Сергей Николаевич
Канд. техн. наук, доцент, зав. каф. безопасности и управления в телекоммуникациях СибГУТИ
Тел.: +7 (383) 2-69-82-45
Эл. почта: snovikov@ngs.ru

Pomortsev A.S., Novikov S.N.

Develop a system for risk assessment of information security violations organizations

The paper presents a solution to the problem of risk assessment security breach commercial organizations on the basis of legal and technical requirements of existing standards and recommendations in the field of information security. A review of the market of software products for automating the risk assessment, the results of which indicate the need to develop a new software product, taking into account the clearly formulated list of parameters of risk assessment information security violations is considered.

Keywords: information security, risk assessment.

УДК 519.254

В.С. Русецкий, Е.А. Русецкая, Р.Т. Файзуллин, Р.Р. Файзуллин

Процедура отсроченного приема сообщения в задаче защиты продукции от фальсификации

Предложена процедура идентификации продукции несколькими кодами. Коды генерировались с помощью композиции 2 и 3 датчиков случайных чисел. Схема стойка к попыткам вскрытия. Проведенные тесты NIST показывают, что выдача удовлетворяет требованиям случайности.

Ключевые слова: случайная последовательность, имитовставка.

Защита от фальсификации. Переход на новый технологический уровень приводит к тому, что некоторые виды несанкционированной обществом деятельности становятся экономически невыгодными. Например, уход от оплаты наличными, кредитование, гарантийное обслуживание ограничивают уличную преступность эффективней, чем любые силовые методы.

Можно предположить, что имеющиеся нерегулируемые лакуны, используемые криминальными сетевыми структурами, можно элиминировать с помощью внедрения современных информационных технологий в повседневную жизнь. Одной из наиболее болевых точек является фальсификация различного рода продуктов.

Рассмотрим проблему фальсификации в криптографических терминах. У нас имеется два абонента: производитель (Алиса) и покупатель продукта (Боб). Сам продукт можно интерпретировать как сообщение P, пересылаемое от производителя продуктов покупателю по открытому каналу связи. Продавец априори выступает как атакующая сторона, задача которой – подменить сообщение имитовставкой [1].

Мы не будем рассматривать организационные и правовые меры по защите передачи, сводящиеся к защите канала связи, а будем считать, что производитель и покупатель как наиболее заинтересованные стороны производят процедуру аутентификации продукта при различного рода атаках со стороны продавца.

Очевидно, что первый и самый примитивный уровень аутентификации заключается в нанесении различного рода марок, кодов и т.п. на продукт, определяющих производителя.

Опыт применения такого рода меток показал, что атакующий легко справляется с задачей подмены сообщения. Так, попытки усложнить задачу подделки путем нанесения сложных технологических меток легко преодолеваются атакующим, причем иногда даже более быстро, чем защита реализуется самим производителем. Например, нанесение литеры М (Массандра) на дно бутылок было осуществлено нарушителями ранее, чем производителем.

Следующим шагом в усложнении процедуры аутентификации является нанесение различного рода уникальных кодов (номера, QR коды и т.п.) на упаковку и сам продукт, которые аутентифицируют не только производителя, но и сам продукт или упаковку партии продукта. В этом случае покупатель может обратиться непосредственно к производителю и узнать, что продукт с такой маркировкой действительно произведен Алисой. Насколько в этом случае высока защищенность? Очевидно, что возможно дублирование меток и без процедуры обратной связи, т.е. увеличения числа обменов сообщениями между Алисой и Бобом, защита не эффективна.

У Алисы имеется база данных с номерами продуктов и на обращение со стороны Боба с просьбой подтвердить N Алиса реагирует высылкой сообщения M_1 о том, что данный номер имеется в базе. Алиса может дополнить сообщение направлением продаж и любой другой сопутствующей информацией, что влияет на окончательное решение Боба о приеме сообщения (покупке). Но самое главное, что у Алисы нет информации о факте покупки данного продукта, что не позволяет полностью исключить имитовставку.

Мы имеем ситуацию, не совсем свойственную классической схеме. Алиса должна поощрить Боба в продолжении процедуры аутентификации и вынудить к формированию сообщения M_2 о факте приема P (покупки), не раскрывая информацию о предыдущем сеансе связи с другим поку-

пателем, завершившимся фактом приема. В ответ Алиса высылает сообщение M_3, которое несет информацию о том, был или не был куплен продукт ранее. Очевидно, что Боб решает задачу определения баланса между затратами на формирование сообщения M_2 и возможного риска приема имитовставки.

Так, предложенный в одном патенте [2] способ нанесения двух уникальных кодов на упаковку и сам продукт казалось бы полностью решает проблему. Но сама процедура вскрытия упаковки после покупки представляет собой затратную процедуру и ставит под сомнение доказательство факта имитовставки при разборе ситуации перед арбитром.

Возможно и другое решение задачи, т.е. неклассический отсроченный прием сообщения P. Боб фиксирует факт приема сообщения предъявлением Алисе сертификата, идентифицирующего продавца I, например фотографии чека. Алиса же хранит в базе данных не только поля под N_1, N_2, M_1, M_2, но и поле под I. Факт приема сообщения фиксирует факт продажи, а код N_2 уже может служить дополнительным аргументом для арбитра при доказательстве факта имитовставки. В случае если продажа или прием сообщения были осуществлены ранее другим получателем, Боб информируется об этом.

В данной ситуации Боб может выбирать между инициацией процедуры доказательства перед арбитром и быстрым отказом от приема сообщения. То есть Боб может осуществить возврат продукта, не отходя от кассы и не вскрывая упаковку, или предъявить иск продавцу за продажу фальсифицированного продукта. Заметим, что в этом случае код N_2 уже не является необходимым, а лишь достаточным, что существенно снижает затраты производителя при маркировке.

Включение в схему независимого арбитра и хранение у него I, обеспечивает юридическую поддержку в случае факта фальсификации и при атаке со стороны внутреннего нарушителя.

Насколько предложенная схема будет стойкой при попытке восстановления генератора кодов N_i при их наличии в ограниченном числе у Кларка?

Пусть даны два датчика ПСВ D_1, D_2. Будем считать, что период первого датчика равен 2^{N_1}, а период второго 2^{N_2}, $a_1,..,a_{2^{N_1}}$, $b_1,..,b_{2^{N_2}}$ – это строки из нулей и единиц, результат работы генераторов.

Сформируем последовательность чисел $P_1,..,P_q$ по следующему правилу:

$$P_1 = \sum_{k=0}^{K} a_k 2^k, \quad P_i = \sum_{k=0}^{K} a_{k+m_i} 2^k, \quad m_i = \sum_{v=1}^{i} S_v, \quad S_v = \sum_{q=0}^{L} b_{q+L(v-1)} 2^q.$$

Первый датчик генерирует числа P_i, а второй – длины лакун S_v между P_i.

Числа P_i используются для маркировки некоторых объектов. Предложенная конструкция позволяет маскировать выход как первого датчика, так и второго и затрудняет восстановление структур генераторов ПСВ.

Попытаемся оценить снизу число операций, необходимых для восстановления структур генераторов в наиболее благоприятном для атакующего случае.

Пусть у атакующего имеется в наличии некоторое число Ω экземпляров $P_i, i = r_1,..,r_\Omega$. Очевидно, что порядок генерации не совпадает с порядком экземпляров P_i.

1) Будем считать, что генераторы представляют собой линейные регистры сдвига с обратной связью.

2) Будем считать, что какие-то два P_i из $P_i, i = r_1,..,r_\Omega$ генерируются последовательно, т.е. соответствующее S_v, определяющее лакуну между ними, равно нулю.

3) Будем считать, что длина первого регистра равна N_1, а второго N_2.

4) Будем считать, что значения каждых двух лакун S_v генерируются последовательно.

При всех этих условиях для восстановления D_1, D_2 необходимо рассмотреть все пары из $P_i, i = r_1,..,r_\Omega$ и в каждом случае получить $a_1,..,a_{2^{N_1}}$. Заметим, что последовательно генерируемые P_{i1}, P_{i2} позволяют полностью восстановить структуру линейного регистра сдвига.

Выделяя среди $a_1,..,a_{2^{N1}}$ остальные P_i, мы получим предполагаемые m_i. Число вариантов перебора пар будет равно C_2^{Ω}. Согласно 4 можно найти пару S_{v1},S_{v2}, которая позволяет получить именно такие m_i между $P_i, i = r_1,..,r_\Omega$. Число перебираемых пар S_{v1},S_{v2} равно $C_2^{\Omega-1}$.

Окончательно оценка на число операций, необходимых для восстановления структуры регистров, можно оценить величиной $C_2^{\Omega-1}C_2^{\Omega}2^{N_1}$. Минимальное значение Ω, при котором возможно восстановление регистров, равно 4.

Таким образом, число операций и память, необходимая для хранения промежуточных данных, для восстановления регистров сдвига, оценивается величиной $C2^{N_1}$ с небольшой по величине константой C. Любое изменение условий 1–4 приводит к существенному росту числа необходимых операций. Например, если для вычисления лакун использовать не весь выход второго регистра, а лишь некоторую часть, то значение Ω, необходимое для восстановления структуры регистров, растет факториально.

Ситуацию с датчиками ПСВ можно усложнить, добавив 3-й датчик, согласно которому последовательность $a_1,..,a_{2^{N1}}$ будет переставляться сгенерированной им перестановкой. Перестановка a_{k+m_i} и $a_{k+m_{i+1}}$ проводится, если датчик на данном шаге выдал 1, в противном случае не проводится. Для сгенерированных датчиками последовательностей битов были проведены тесты NIST [3, 4]. Кроме теста на равномерность в подпоследовательностях, все тесты были пройдены успешно.

Своё наглядное воплощение процедура отсроченного приёма сообщения получила в разработанном программном продукте «ПродМарка». Продукт предназначен для комплексного решения задачи защиты от фальсификации.

Архитектура продукта «ПродМарка» построена на клиент-серверном принципе, т.е. база данных продукции и обработчики обращений размещены на сервере владельца системы защиты, а клиенты, в данном случае покупатели, обращаются на сервер из различных коммуникационных сред.

Основой системы является база данных формата «MySQL», в которую посредством специального программного обеспечения производитель записывает информацию о поступающих в торговую сеть единицах продукции. Выбранный тип хранения данных – «InnoDB» позволяет при обновлении юридического статуса единицы продукции, в отличие от более распространённого «MyISAM», использовать блокировку на уровне строки, а не всей таблицы, что, в общем итоге, обеспечивает многократное повышение скорости работы клиентов с базой данных. К записываемой информации относятся наименование товара, изображение, описание и характеристики, направление распространения. Структура базы данных является оптимизированной, что позволяет отказаться от дублирования общей для видов или партий продукции информации. Стандартная сборка продукта позволяет без привлечения дополнительных средств распределённого хранения данных обрабатывать до десяти миллионов единиц продукции. При оценке быстродействия системы за расчётную нагрузку принимался месячный оборот продукции в количестве одного миллиона единиц, было смоделировано усреднённое значение 23 запроса в секунду, использован мобильный интернет-канал с пропускной способностью 200 кбит/с. Время ответа системы не превышало 4 с, а среднее чистое машинное время обработки запроса сервером составило 0,3 с. При этом система имеет возможность наращивания мощности с увеличением количества обрабатываемых единиц путём кластеризации.

Регистрацию продукции в базе данных выполняет комплекс программных средств, обеспечивающий валидацию и оптимизацию данных. Результатом регистрации, помимо непосредственной записи в базу данных, является генерация уникального номера и контрольного значения для каждой единицы. Уникальный номер используется для автоматизированного нанесения на упаковку продукции, в том числе в сочетании с машиночитаемым графическим кодом для быстрого распознавания портативными устройствами. Контрольные значения могут быть сгенерированы в том числе и с использованием генератора псевдослучайной последовательности. Тестирования, проведённые с применением стандарта программирования OpenMP [5], подтверждают возможность применения такой генерации.

Сценарий двусторонней связи с покупателем реализован посредством препроцессора гипертекста. Интерфейс служит для мгновенного обмена сообщениями с покупателями, обращений в базу данных, описания закрытых классов обслуживания датчиков ПСВ и связи с внешними библиотека-

ми. Обращения происходят на виртуальный хост системы, зарегистрированный в глобальном адресном пространстве.

После поступления продукции в торговую сеть покупатель приобретает возможность совершения первичных запросов характеристик товара в базу данных производителя, производя в ручном или автоматическом режиме отправку индивидуального номера упаковки в публичный интерфейс системы «ПродМарка». Ответом на запрос является текстово-графическая информация, содержащая наименование, описание, изображение и характеристики товара, служащая двум задачам: начальной идентификации и получению сведений о потребительских свойствах. При совпадении информации, отправленной системой, с информацией, нанесённой на упаковку, покупатель принимает решение о покупке.

Непосредственно в момент совершения покупки покупатель отправляет вторичный запрос в базу данных производителя, передавая либо фотографию кассового чека, либо контрольный код, скрытый внутри упаковки товара. После распознавания принятой от покупателя информации система возвращает юридический статус продукта: была ли вскрыта упаковка ранее или нет, одновременно совершая регистрацию покупки данной единицы продукции, вскрытия упаковки. Оперирование юридическим статусом является основополагающим инструментом системы, поскольку исключает возможность массового контрафактного дублирования продукции.

Литература

1. Дубнов И.А. Использование имитовставок для контроля целостности контента цифрового телевизионного вещания./ И.А. Дубнов, Ю.А. Дубнов // Труды НИИР. – 2013. – № 2. – С. 45–50.

2. Пат. 2463656 РФ, МПК G06F21/24, G06K9/00. Способ аутентификации продукта в контейнере и соответствующий способ для проверки аутентичности продукта и его контейнера / О. Дангманн (FR), Ж. Дешеро (FR). – Патентообладатель ОИ ЭРОП САРЛЬ (FR). – № 2011118612/08 ; заявл. 10.10.2008 ; опубл.: 10.10.2012.

3. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Электронный ресурс]. – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf, свободный (дата обращения: 24.04.14).

4. Вильданов Р.Р. Тесты псевдослучайных последовательностей и реализующее их программное средство / Р.Р. Вильданов, Р.В. Мещеряков, С.С. Бондарчук // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 108–111.

5. Вильданов Р.Р. Применение стандарта OpenMP для тестирования псевдослучайных последовательностей / Р.Р. Вильданов, В.В. Маркин, Р.В. Мещеряков // Сборник статей региональной научно-практической конференции «Многоядерные процессоры, параллельное программирование, ПЛИС, системы обработки сигналов» (28 февраля 2012 г. на базе Алтайского государственного университета). – 2012. – С. 153–158.

Русецкий Владимир Сергеевич
Инженер-программист центра телекоммуникаций и вычислительной техники Омского государственного технического университета (ОмГТУ)
Тел.: +7-983-117-15-51
Эл. почта: vladimir@omgtu.ru

Русецкая Елена Александровна
Начальник отдела АСУ–ВУЗ центра телекоммуникаций и вычислительной техники ОмГТУ
Тел.: +7-913-617-94-31
Эл. почта: elena@omgtu.ru

Файзуллин Рашит Тагирович
Д-р техн. наук, профессор, зав. каф. «Комплексная защита информации» ОмГТУ
Тел.: 8 (381-2) 21-77-02
Эл. почта: r.t.faizullin@mail.ru

Файзуллин Рамиль Рашитович
Ст. преподаватель каф. «Комплексная защита информации» ОмГТУ
Тел.: 8 (381-2) 72-17-19
Эл. почта: strannik11@list.ru

Rusetskiy V.S., Rusetskaya E.A., Faizullin R.T., Faizullin R.R.
Procedure of the delayed reception of the message in a problem of protection of production from falsification

A procedure for the identification of several product codes. Codes are generated using the compositions 2 and 3 random numbers. The scheme is resistant to tampering. NIST tests have shown that the issuance satisfies the requirements of randomness.
Keywords: random sequence, message authentication code.

УДК 004.089

А.Г. Сабанов

О проблеме достоверности идентификации пользователя при удаленном электронном взаимодействии

Рассмотрена задача исследования достоверности идентификации пользователя при удаленном электронном взаимодействии. Разработана методика определения ошибок идентификации. Показана необходимость использования биометрических методов идентификации для снижения уровня ошибок идентификации. Обоснована задача доработки нормативной базы в части регулирования идентификации пользователя при удаленном электронном взаимодействии.
Ключевые слова: идентификация, достоверность, проблема, пользователь, удаленное электронное взаимодействие.

Вопросы идентификации сторон при удаленном электронном взаимодействии (УЭВ) в связи с развитием информатизации общества [1] занимают одно из первых мест по актуальности. К числу особенно сложных и до сих пор не до конца решенных проблем безопасности относится надежная идентификация субъектов и объектов при УЭВ. Действительно, в целях противодействия нарастающему мошенничеству весьма важно знать, какой именно субъект находится на другой стороне сеанса взаимодействия. Несмотря на обилие западных нормативных документов, регулирующих процессы идентификации и аутентификации, рассмотренных в работе [2], вопросы достоверности идентификации до конца не решены. Под достоверностью идентификации будем понимать общую точность и полноту идентификационной информации об объекте. Достоверность идентификации обратно пропорциональна вероятности возникновения ошибок в информационной системе.

Схема идентификации должна быть удобной для применения пользователями и простой для организации онлайн-сервисов. Общие вопросы идентификации и аутентификации рассмотрены в работе [3], однако вопросы достоверности идентификации не вошли в данное исследование. В работе [4] изучены общие методы анализа надежности применительно к процессам аутентификации, которые были применены к задаче идентификации рисков в работе [5]. Одним из выводов перечисленных работ явилось установление факта отсутствия типовых схем, математических моделей и подходов к анализу надежности и достоверности идентификации при УЭВ. Мало того, как показано в работе [1], отечественная нормативная база по вопросам идентификации субъектов при УЭВ и доступе к онлайн-сервисам нуждается в серьезной доработке. Целью данной работы является разработка модели и методики оценки достоверности идентификации пользователя при УЭВ.

Модель исследования электронной идентификации. Формализуем процесс идентификации. Существующие системы идентификации (СИ), как правило, используют последовательные запросы на соответствие предъявленного субъектом идентификатора Id_i с занесенным ранее в базу данных. Типовая схема идентификации представлена на рис. 1.

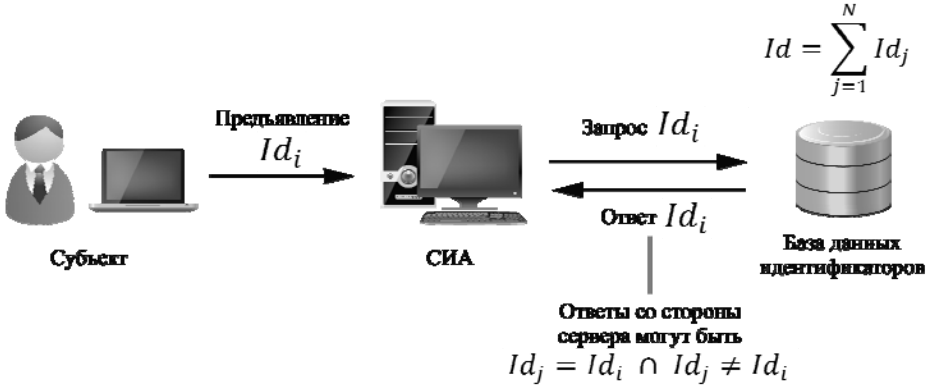


Рис. 1. Типовая схема идентификации субъекта

Предъявленный субъектом идентификатор принимается системой идентификации и аутентификации (СИА), которая высылает автоматический запрос в базу данных идентификаторов. Если предъявленный идентификатор Id_i совпадает с находящимся в базе Id_j, т.е. $Id_i = Id_j$, то идентифика-

ция считается пройденной успешно. В агрессивной к атакам среде сравниваться могут не сами значения Id_i, а их свертки (хеши). Современные СИА могут быть настроены на использование не одного, а нескольких идентификаторов – избыточность числа идентификаторов делается с целью повышения надежности процесса идентификации. Рассмотрим СИ – подсистему СИА, отвечающую только за процесс идентификации.

Модель процесса идентификации представлена на рис. 2.

Рис. 2. Модель предъявления идентификаторов субъектом, число идентификаторов $n = 3$

Количество идентификаторов в процессе их предъявления взаимодействующей стороне (чаще всего это информационной ресурс – сервер) может быть $n = 1, 2, 3$. Случаи $n > 3$ на практике встречаются весьма нечасто, однако покажем, что предлагаемые в данной работе подходы легко могут быть распространены на любое n. Предположим, что в базе данных находится N зарегистрированных идентификаторов: $Id = \sum_{j=1}^{N} Id_j$.

Ответы со стороны сервера могут быть $Id_j = Id_i \cap Id_j \neq Id_i$, где Id_i – предъявленный субъектом идентификатор.

В такой системе критерием успешной идентификации будет совпадение не одного, а заданного числа n предъявленных идентификаторов. Рассмотрим эту типовую модель процесса последовательного предъявления и проверки идентификаторов с точки зрения теории надежности информационных систем.

Согласно основным положениям теории структурной надежности [6] сначала определим условия работоспособности системы и сформулируем критерии отказа. Предполагается, что элементы (в рассматриваемом случае c_i – процедуры идентификации по Id_i, $i = 1, 2, 3$) отказывают независимо друг от друга, т.е. отказ любых элементов не изменяет надежности остальных элементов.

Пусть E будет событием элемента c_i, происходящего в определенный момент времени. Безотказность СИ для представленной на рис. 2 модели может быть представлена в виде

$$P_C = \prod_{i=1}^{n} P[E_i].$$

В случае известных распределений наработок до отказа отдельных элементов $F_i(t) = 1 - P_i(t)$ для независимых элементов вероятность безотказной работы СИ определяется выражением

$$P_C(t) = \prod_{i=1}^{n} [1 - F_i(t)] = \prod_{i=1}^{n} P_i(t) .$$

Принятым в большинстве работ по надежности подобных систем функцией распределения отказов в каждом элементе $F_i(t)$ является экспоненциальное распределение наработки до отказа

$$F_i(t) = 1 - P_i(t) = 1 - e^{-\lambda_i t}$$

с постоянной интенсивностью отказов $\lambda_i = \text{const}$, $i = 1, 2, 3$. Обозначим $\Lambda = \sum_{i=1}^{n} \lambda_i$. Тогда

$$P_C(t) = \exp(-\sum_{i=1}^{n} \lambda_i t) = \exp(-\Lambda t) .$$

При условии $\Lambda t \ll 1$ допустимы следующие приближенные выражения: $P_C(t) \approx 1 - \Lambda t$ и $Q(t) \approx \Lambda t$, где $Q(t) = 1 - P_C(t)$ – вероятность отказа.

Другими словами, вероятность безотказной работы системы идентификации в данном случае всегда меньше, чем вероятность отсутствия отказов самого ненадежного элемента. Она существенно возрастает при увеличении надежности самого ненадежного элемента.

При этом априори должны выполняться 2 условия:

- «доверенный» источник (база данных идентификаторов);
- «доверенные» процедуры идентификации.

На практике оба условия выполняются не в полной мере, лишь с какой-то долей вероятности.

В теории идентификации рассматривают ошибки первого и второго рода.

Ошибка первого рода состоит в том, что в результате проведенной идентификации пользователя не идентифицировали как легального зарегистрированного пользователя в системе. Это может случиться, например, в результате наличия «двойника» и/или сбоя при сравнении отдельного идентификационного параметра (параметров), превышения заданного уровня ошибок и сбоев в работе самой системы. В терминах теории надежности такое событие может трактоваться как отказ системы идентификации.

Ошибка второго рода применительно к задаче идентификации может быть сформулирована как идентификация злоумышленника под видом легального пользователя системы. Применительно к задаче оценки надежности системы такое событие определим как опасный отказ.

Оценки вероятности наступления отказа и опасного отказа лучше проводить для конкретной системы с заданными характеристиками. При этом можно воспользоваться математическими моделями надежности, разработанными в работе [7].

Приведем пример идентификации субъекта взаимодействия по двум представленным документам (идентификаторам). Предположим, что вероятность ошибки идентификации по первому идентификатору составляет 10^{-4}, по второму – 10^{-6}. Тогда суммарная вероятность ошибки идентификации составит $P = 10^{-10}$. С учетом того, что население Российской Федерации оценивается в 140 млн человек, т.е. $1{,}4\times10^{8}$, вероятная суммарная ошибка идентификации составит 1,4%. Однако эти примитивные оценки справедливы при условии так называемых «доверенных» источников и процессов идентификации. При недостаточной степени достоверности идентификации по выбранным параметрам необходимо вводить дополнительные идентификационные признаки, а в приведенную формулу добавлять поправочные коэффициенты.

Для проведения практических оценок этот процесс проще всего свести к рассмотрению вероятностных интервалов ожидаемых значений для всех (в том числе добавленных) p_i. Например, в условиях недостаточной достоверности в рассмотренном примере вероятность ошибки по первому идентификатору может оцениваться в пределах $10^{-4} – 10^{-3}$ или в более широких пределах в зависимости от степени «доверенности». Тогда суммарная ошибка может быть оценена как граница произведений наибольших значений p_i. Математически можно добиться желаемой (или заданной) точности идентификации введением одного или нескольких дополнительных идентификаторов даже в условиях недостаточной достоверности идентификации по каждому из рассматриваемых идентификационных признаков. На практике желательно в качестве идентификационных признаков вводить идентификаторы, зарегистрированные в различных ведомственных базах данных (например, ФМС, ФНС, ПФР). Для снижения рисков злоупотреблений также рекомендуется введение хотя бы одного неотчуждаемого от пользователя (например, биометрического) идентификатора. По логике общественной безопасности база данных биометрической идентификации граждан должна находиться в ведении МВД России. При этом эта база данных нуждается в современной системе управления доступом и должна быть обеспечена высокотехнологичным средством защиты конфиденциальности данных, например представленным в работе [8, 9].

Применение сертификата ключа проверки квалифицированной электронной подписи для идентификации субъектов. Одним из развивающихся способов идентификации сторон удаленного электронного взаимодействия является идентификация субъекта по его сертификату ключа проверки подписи (СКПП). Субъект получает свой СКПП по запросу в центре регистрации (ЦР) удостоверяющего центра (УЦ). На УЦ возлагаются следующие основные задачи:

- установление личности заявителя – будущего владельца СКПП;
- формирование по установленному алгоритму цифрового сертификата проверки подписи и заверение его электронной подписью УЦ;
- выдача под личную собственноручную подпись СКПП его владельцу;
- поддержка выданного сертификата на весь срок его действия.

Остановимся на первой задаче, которая на момент написания статьи фактически не регулируется. Из выданных на сегодня СКПП значительную часть представляют собой сертификаты должностных лиц предприятий и организаций. Заполненные без ошибок заданные поля СКПП (O, S, C, STREET, OID = 1.2.643.3.131.1.1 и 1.2.643.100.1) в абсолютном большинстве случаев позволяют однозначно идентифицировать юридическое лицо, в котором работает владелец сертификата. При этом, однако, для идентификации субъекта – владельца СКПП заполняются всего 3 поля: CN (ФИО), E (электронный адрес в произвольном формате), СНИЛС. Фактически для идентификации субъекта относительно пригодны только ФИО (вспомним число полных однофамильцев в крупных организациях) и СНИЛС, который является единственным уникальным идентификатором.

Поскольку СКПП является своего рода аналогом электронного паспорта, первая из перечисленных задач УЦ (установление личности заявителя) является одной из важнейших. Однако на текущий момент, несмотря на наличие ряда методических указаний по заполнению полей сертификата процесс установления личности не регламентирован. ЦР, действуя от лица УЦ, не протоколирует этапы представления заявителем идентификаторов и результаты их проверок и не хранит эти записи в своем защищенном архиве. Заметим, что в развитых странах ЦР обязан выполнять эти элементарные требования для разбора конфликтных ситуаций.

К сожалению, при выдаче СКПП физическим лицам дело с идентификацией владельца сертификата обстоит не лучше. Правила аккредитования УЦ (на момент написания данной статьи при Минкомсвязи России аккредитовано 317 УЦ) позволяют выдавать СКПП в удаленном режиме. Имеются УЦ, в рекламе которых говорится о выдаче СКПП за 15 мин в режиме удаленного электронного взаимодействия. Вопросы доверия к СКПП, выданным таким способом, остаются без ответа.

Заключение. Разработанная методика позволяет проводить оценки достоверности идентификации пользователя при УЭВ. Установлено, что вопросы идентификации участников электронного взаимодействия, в том числе по СКПП, нуждаются в дальнейшем исследовании и регулировании. Возможно, одним из путей решения проблемы станет принятие федерального закона об идентификации и аутентификации пользователей информационных систем. Однако обсуждение и принятие законов обычно длится достаточно долгое время. Независимо от появления такого закона Минкомсвязи России необходимо сформулировать и установить правила регистрации новых пользователей ИС и владельцев СКПП.

Литература

1. Распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р «О государственной программе Российской Федерации «Информационное общество (2011–2020 годы)». [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2010/11/16/infobschestvo-site-dok.html, свободный (дата обращения: 17.12.2013).

2. Сабанов А.Г. Обзор иностранной нормативной базы по идентификации и аутентификации // Инсайд. Защита информации. – 2013. – № 4 (52). – С. 82–88.

3. Аутентификация. Теория и практика / Под ред. А.А. Шелупанова. – М.: Горячая линия – Телеком, 2009. – 552 с.

4. Сабанов А.Г. Методы исследования надежности удаленной аутентификации // Электросвязь. – 2012. – № 10. – С. 20–24.

5. Сабанов А.Г. Методика идентификации рисков процессов аутентификации // Доклады ТУСУРа. – 2013. – № 4 (30). – С. 136–141.

6. Шубинский И.Б. Структурная надежность информационных систем. Методы анализа. – Ульяновск: Печатный двор, 2012. – 216 с.

7. Сабанов А.Г. Концепция моделирования процессов аутентификации // Доклады ТУСУРа. – 2013. – № 3(29). – С. 71–75.

8. Додохов А.Л. К вопросу о защите персональных данных с использованием СУБД Oracle / А.Л. Додохов, А.Г. Сабанов // Доклады ТУСУРа. – 2012. – № 2 (26). – С. 129–133.

9. Сабанов А.Г. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков // Ползуновский вестник. – 2012. – № 2–1. – С. 61–67.

Сабанов Алексей Геннадьевич
Канд. техн. наук, зам. генерального директора ЗАО «Аладдин Р.Д.», доцент МГТУ им. Н.Э. Баумана
Тел.: 8-985-924-52-09
Эл. почта: asabanov@mail.ru; a.sabanov@aladdin-rd.ru

Sabanov A.G.

On problem of user identification reliability for remote electronic interaction

The problem of reliability examination of user identification in remote electronic interaction is considered. An identification errors detection technique is developed. The necessity of use of biometric identification methods for lowering identification errors rate is shown. The task of modification of regulatory framework for user identification in remote electronic interaction is justified.

Keywords: identification, reliability, problem, user, remote electronic interaction.

УДК 004.056.5

В.Л. Токарев

Распознавание стратегии противодействующей стороны по текущим наблюдениям

Рассмотрен подход к распознаванию стратегии атаки на автоматизированную систему, основанный на предварительном построении нечетких моделей возможных стратегий, используемых для атак. Предложен метод, позволяющий по начальной последовательности действий атакующей стороны распознать выбранную ей стратегию и на этой основе прогнозировать её очередное действие с целью своевременного блокирования его реализации.

Ключевые слова: условия противодействия, стратегия атаки, прогнозирование.

Далеко позади те дни, когда весь арсенал средств обеспечения информационной безопасности составляли устройства защиты и системы обнаружения вторжения. Сложность того, что и когда нужно защищать, налагающиеся к тому же правила и требования создают потребность в новом типе систем защиты информации, основанных на методах искусственного интеллекта. Одним из назначений таких систем является распознавание стратегии злоумышленника, начавшего атаку на защищенную автоматизированную систему хранения, и обработки конфиденциальной информации с целью прогнозирования очередного его шага получения доступа к защищаемой информации. Надежное прогнозирование действий злоумышленника дает возможность компьютерной системе поддержки принятия решений своевременно, в автоматическом режиме, создать барьеры на пути «движения» злоумышленника, что позволит: 1) сэкономить силы и средства, которые бы потребовались при выстраивании системы защиты информации, блокирующей все возможные пути несанкционированного доступа; 2) излишне не осложнять получение доступа санкционированным пользователям.

Некоторые вопросы построения компьютерных систем поддержки принятия решений рассмотрены в монографии [1]. В этой статье рассматривается один из подходов к задаче прогнозирования действий противодействующей стороны (злоумышленника), основанный на оценивании в реальном времени стратегии, выбранной этой стороной для атаки на автоматизированную систему.

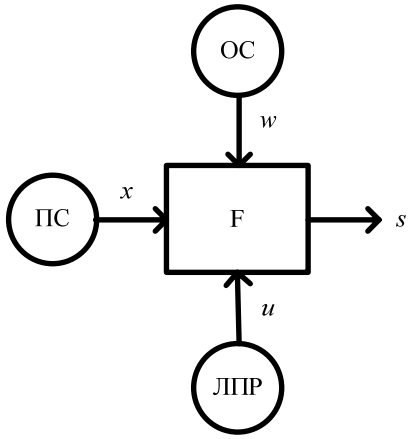


Рис. 1. Схема взаимодействие сторон

Для формализации задачи распознавания стратегии противодействующей стороны взаимодействие сторон можно представить схемой (рис. 1).

Процесс взаимодействия предлагается рассматривать как динамическую систему F, состояние s_k которой в каждый момент времени является функцией u_{k-1} – хода ЛПР (1-я сторона (1С)); x_k – хода ПС (2-я сторона (2С)); w_{k-1} – действия окружающей среды (ОС – 3-я сторона). Под ходом понимается какое-либо действие, способное повлиять на состояние s_k системы F в дискретный момент времени k. Эволюцию системы F_k под воздействием ходов сторон в пространстве состояний можно представить в виде

$$s_{k+1} = F_k(s_k, x_k, u_k, w_k), \quad s_k \in S, x_k \in X, u_k \in U, w_k \in W, k = 1,2,...,n, \qquad (1)$$

где S – множество возможных состояний системы F; X – множество возможных ходов стороной 2С; U – множество возможных действий 1С, направленных на защиту информации в автоматизированной системе; W – множество ограничений (правил игры), установленных стороной 3C.

Действия (ходы) конфликтующих сторон (1С и 2С) преследуют противоположные цели $\tau(j)=s_n^{(j)}$, j = 1С, 2С, $n \in K$. Момент времени n соответствует достижению цели одной из сторон (вы-

игрышу одной при поражении другой). 3-я сторона не имеет целью выигрыш, но она определяет правила взаимодействия и тем самым влияет на выбор пути достижения цели 1-й и 2-й сторон.

Предложена метрика $\rho(s_k, s_n^{(j)})$, $k,n \in K$, позволяющая оценивать достижение цели j-й стороной, отвечающая требованию

$$\rho\left(s_k, s_n^{(j)}\right) = \begin{cases} 1, & \text{если } s_n = \tau^{(j)}, \\ v \in [0,...,1], & \text{если } k \neq n, \\ 0, & \text{если } s_n = \tau^{(\neg j)}. \end{cases} \quad (2)$$

Процесс игры с точки зрения одного из игроков (1С) можно представить следующим образом:

$$\begin{aligned} & g_i^{(2C)}(s_o, u_1) \to x_1; \\ & h_1 : (s_o, u_1, x_1) \to s_1; \\ & g_i^{(2C)}(s_1, u_2) \to x_2; \\ & h_2 : (s_o, u_1, x_1) \to s_2; \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & g_i^{(2C)}(s_{n-1}, u_n) \to x_n; \\ & h_n : (s_{n-1}, u_n, x_n) \to s^{*(2C)}, \end{aligned} \quad (3)$$

где $g_i^{(2C)}$ – некоторая стратегия из множества G возможных стратегий, используемая 2С для достижения цели $\tau^{(2C)}$.

Задача заключается в том, что по некоторой начальной последовательности процесса (3) требуется выбрать $\hat{g}_i^{(2C)} \in G^{(2C)}$, наилучшим образом соответствующую полной последовательности (3).

Здесь $G^{(2C)}$ – множество возможных стратегий противодействующей стороны. Для четких множеств $(h_{i.1},...,h_{i.k},...,h_{i.n})$ – это траектория, которая определяется выбранной стратегией $g_i^{(2C)}$. Для нечетких множеств $(A_{i.1},...,A_{i.k},...,A_{i.n})$ – это стратегия, поскольку каждое $A_{i.k}$ содержит некоторое множество ходов $\{h_{i.k}\}$, соответствующих одной стратегии $g_i^{(2C)}$. Здесь $A_{i.k}$ – нечеткое множество, определяемое функцией принадлежности $\mu_{A_{i.k}}(h_{i.k})$.

Тогда стратегию стороны 2С можно определить по последовательности ходов x_k, сделанных в условиях $(s_{\kappa-1}, u_\kappa)$, и с учетом правил игры, установленных стороной 3С, при $k = 1,...,n$, т.е. в течение всего процесса (траектории).

Это позволяет определить путь достижения цели каждой стороной, как некоторую траекторию пар действий

$$\{(x_0,u_0),...,(x_k,u_k),...,(x_n,u_n);\ k,n \in K\} \text{ при } w_k \in W. \quad (4)$$

При этом каждой паре (x_k, u_k) соответствует k-е состояние s_k, а паре (x_n, u_n) – одно из состояний $s^*_{(j)} : j$ = 1С или 2С. Отсюда стратегия поведения участников 1С и 2С определена как желаемая последовательность

$$g_{(j)} = \{s_0,...,s_{(j)k},...s^*_{(j)}\},\ j = 1C, 2C. \quad (5)$$

Тогда модель стратегии $g_i^{(2C)}$ можно определить как динамическую нечеткую модель вида

$$\hat{s}_k = g_{i.k}^{(j)}(\hat{s}_{k-1}, (x_k, u_k)), \quad (6)$$

где $g_{i.k}^{(2C)}$ – функция перехода из состояния $\hat{s}_k$ в состояние $\hat{s}_{k+1}$, которая определяется выбранной стороной 2С стратегией g_i. То есть эта функция является отображением стратегии g_i на k-м шаге взаимодействия.

На основании этого предложено задачу оценивания стратегии свести к задаче оценивания функции g_i по имеющейся последовательности

$$\{h_0, h_1, ..., h_k, ..., h_m\},\ h_k = (\hat{s}_k, (x_k, u_k)),\ m < n. \quad (7)$$

Разнообразие ходов сторон $u_k \in U$, $x_k \in X$ на каждом шаге k взаимодействия приводит к «размытости» траекторий в рамках одной стратегии $g_i^{(2C)}$. При отсутствии такой «размытости» и ограничении числа шагов $k = m$, i-ю стратегию $g_i^{(2C)}$ можно определить как отображение, позволяющее определить (m+1)-е состояние:

$$g_i^{(2C)} \to s_{i.m+1}^{(2C)} \in S,\ i = 1, ..., p.$$

С учетом размытости каждую стратегию противодействующей стороны можно представить как множество $H_i^{(2C)}$ траекторий достижения цели $\tau^{(2C)}$:

$$\begin{aligned} H_i^{(2C)} &= \{(h_{i.1}, ..., h_{i.k}, ..., h_{i.n}),\ i = 1,2,..\}, \\ h_{i.1} &\in H_1, \cdots, h_{i.k} \in H_k, \cdots, h_{i.n} \in H_n. \end{aligned} \quad (8)$$

«Размытость» траекторий (8) предложено учесть с помощью нечеткой динамической модели вида

$$h_1 \in A_{i.1} \wedge \cdots \wedge h_k \in A_{i.k} \wedge \cdots \wedge h_m \in A_{i.m} \to s_{m+1} \in B_i, \quad (9)$$

где нечеткие множества $A_{i.k}$ определены на множестве значений $H_i^{(2C)}$, а нечеткое множество B_i – на множестве значений S.

Тогда в нечеткой модели (9) i-й стратегии вместо $s_к$ будем использовать $b_к$ – нечеткое множество с функцией принадлежности $\mu_{b_k}(s_k)$, вместо $u_к$ будем использовать $c_к$ – нечеткое множество с функцией принадлежности $\mu_{c_k}(u_k)$, а вместо $x_к$ будем использовать $d_к$ – нечеткое множество с функцией принадлежности $\mu_{d_k}(x_k)$, можем первый этап обработки последовательности $(A_{i.1}, ..., A_{i.k}, ..., A_{i.m})$, для которой $m < n$, свести к получению оценки по правилу:

Если истинна нечеткая импликация $(\mu_{b_k}(s_k), \mu_{c_k}(u_k)) \to \mu_{d_k}^{(i)}(x_k)$, то истинна оценка $\hat{g}_{i.k}^{(2C)}$, где истинность импликации соответствует $\max_i \{\mu_{d_k}^{(i)}(x_k)\}$.

Совокупность таких моделей, построенных для каждой цели $\tau^{(2C)}$, каждой ситуации, включающей исходное состояние s_0, имеющиеся ресурсы r_0 составляют базу знаний компьютерной системы оценивания нечеткого множества состояний системы F:

$$\begin{aligned} &g_1^{(2C)} : (A_{1.1}, ..., A_{1.k}, ..., A_{1.m}) \to b_{1.m+1}, \\ &g_2^{(2C)} : (A_{2.1}, ..., A_{2.k}, ..., A_{2.m}) \to b_{2.m+1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &g_p^{(2C)} : (A_{p.1}, ..., A_{p.k}, ..., A_{p.m}) \to b_{p.m+1}, \end{aligned} \quad (10)$$

где p – число возможных стратегий для каждой четверки $<\tau^{(2C)}, s_0, r_0^{(2C)}, h_0>$, $\tau^{(2C)} \in T$ – конечное множество возможных целей, $s_0 \in S$, $r_0^{(2C)} \in R$; $h_{i.k} \in H_i$: запятая внутри скобки означает конъюнкцию.

Тогда на всем множестве полученных оценок $\hat{g}_{i.k}^{(2C)}$, $k = 1, ..., m, i = 1, ..., p$, отыскивается стратегия, оценка которой определяется правилом

$$\hat{g}_i^{*(2C)} = \max_{\substack{k=1,...,m, \\ i=1,...,p}} \{N_i / m\},$$

где N_i – число оценок i-й стратегии.

Полученная оценка позволяет своевременно сделать прогноз следующего хода противодействующей стороны. Поскольку на момент прогноза известны значения (s_m, u_{m+1}), то можем использовать полученную оценку стратегии $\hat{g}_i^{(2C)}$, а обратившись к соответствующей записи

$\hat{g}_i^{(2C)}(s_m, u_{m+1}) \to \mu_{d_k}^{(i)}(x_k)$, хранящейся в базе знаний системы поддержки принятия решений [2], можем получить оценку $\hat{x}_k$, используя любой способ дефаззификации [3].

Рассмотрен подход к распознаванию стратегии атаки на автоматизированную систему, основанный на предварительном построении нечетких моделей возможных стратегий, используемых при атаках. Получен метод, позволяющий по начальной последовательности действий атакующей стороны распознать выбранную ей стратегию и на этой основе прогнозировать её очередное действие, с целью своевременного блокирования его реализации. На основе этого подхода можно создавать компьютерные системы поддержки принятия решений, позволяющие своевременно в автоматическом режиме выстраивать барьеры на пути «движения» злоумышленника к защищаемой информации, экономя при этом временные и материальные затраты.

Литература

1. Токарев В.Л. Компьютерная поддержка принятия решений. – М.: Изд-во СГУ, 2007. – 162 с.

2. Токарев В.Л. Интеллектуальная поддержка выбора решения по защите информации // Проблемы правовой и технической защиты информации: сб. научных статей. – Барнаул: Изд-во Алт. ун-та, 2008. – С. 141–144.

3. Борисов В.В. Нечеткие модели и сети / В.В. Борисов, В.В. Круглов, А.С. Федулов. – М.: Горячая линия – Телеком, 2007. – 284 с.

Токарев Вячеслав Леонидович
Д-р техн. наук, профессор каф. информационной безопасности Тульского государственного университета
Тел.: +7-910-943-74-36
Эл. почта: tokarev22@yandex.ru

Tokarev V.L.

Recognition of rival's strategy using actions detection

The approach to recognition of attack strategy to computerized system is considered. This approach is based on fuzzy models of possible attack strategy beforehand building. The method permitted on initial sequence of rival's actions to recognize strategy selected him for attack is suggested. That estimation of strategy makes it possible to forecast the next rival's operation and its implementation to block promptly.

Keywords: counteraction, attack strategy, forecasting.

УДК 004.04

Ю.В. Трифонова, Р.Ф. Жаринов

Возможности обезличивания персональных данных в системах, использующих реляционные базы данных

Рассматриваются вопросы обезличивания персональных данных, взгляд регулятора на требования к обезличиванию таких данных и проблемы, возникающие при применении методов обезличивания, предложенных Роскомнадзором. Вводится термин деперсонализации персональных данных. Предлагается кроссплатформенное решение для деперсонализации персональных данных в реляционных базах данных. Рассматриваются возможности использования инструментария CryptDB как надежного способа обезличивания персональных данных на стороне сервера.

Ключевые слова: обезличивание, деперсонализация, персональные данные, SQL, CryptDB.

Как только сложились требования к защите персональных данных в России, сразу же появились способы обхождения или уменьшения таких требований, и обезличивание персональных данных стало как раз одним из таких способов. Изначально обезличивание персональных данных позволяло самостоятельно оператору принимать решение о применяемых мерах и способах обеспечения безопасности персональных данных, после очередных изменений нормативных документов регуляторов обезличивание персональных данных стало значительно снижать требования к обработке таких данных, а как следствие – стоимость системы их защиты. До недавнего времени вопросы обезличивания постоянно обсуждались и являлись предметом ожесточенных споров, но в сентябре 2013 г. Роскомнадзор выпустил Приказ, который утвердил требования и методы по обезличиванию персональных данных, чем определил свою позицию в этом вопросе [1, 2]. Таким образом, Роскомнадзор предложил методику снижения обременений, позволяющую не применять в отношении обезличенных данных организационные и технические меры защиты, разработанные в свою очередь ФСТЭК и ФСБ. Хотя требования, предъявляемые сегодня к обработке персональных данных, позволяют достаточно гибко выбирать защитные мероприятия [3].

Обезличивание или деперсонализация. Итак, обезличивание персональных данных. Оказалось, что восприятие этого термина как представление персональных данных в виде, не позволяющем восстановить какую-либо информацию о субъекте персональных данных, является не совсем верным. Согласно ранее упомянутому Приказу Роскомнадзора обезличивание персональных данных должно обеспечивать не только защиту от несанкционированного использования, но и возможность их обработки, т.е. данные после обезличивания должны обладать рядом свойств, к которым относятся:

- Полнота – сохранение всей информации о конкретных субъектах или группах субъектов, которая имелась до обезличивания.
- Структурированность – сохранение структурных связей между обезличенными данными конкретного субъекта или группы субъектов, соответствующих связям, имеющимся до обезличивания.
- Релевантность – возможность обработки запросов по обработке персональных данных и получения ответов в одинаковой семантической форме.
- Семантическая целостность – сохранение семантики персональных данных при их обезличивании.
- Применимость – возможность решения задач обработки персональных данных, стоящих перед оператором, осуществляющим обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ (далее – оператор, операторы), без предварительного деобезличивания всего объема записей о субъектах.
- Анонимность – невозможность однозначной идентификации субъектов данных, полученных в результате обезличивания, без применения дополнительной информации.

Первым требованием к методу обезличивания Роскомнадзор поставил обратимость, т.е. возможность проведения деобезличивания. Таким образом, регулятор подтвердил возможность разбивания одной базы персональных данных на несколько с целью уменьшения требований к обработке части сведений, при этом используя возможность деобезличивания каждой конкретной записи для выполнения функций оператора. На наш взгляд, такой подход является неверным, поскольку данные обрабатываются в том же объеме у того же оператора. Если при этом снижаются требования к обработке, то возрастает вероятность атаки в момент деобезличивания персональных данных, и эта функция становится слабым звеном. Кроме того, уже неоднократно говорилось о том, что уникальность фамилии при определенных условиях является достаточным сведением для идентификации субъекта [4, 5], а по обезличенной базе данных при использовании простого метода перемешивания можно получить достаточно большое число сведений. Так, если в перемешанной базе данных будут храниться сведения о зарплате, то легко предположить, к кому относятся выбивающиеся из общего диапазона числа. Или же наличие известной фамилии в определенной базе данных может дать вам дополнительную информацию.

Однако часто возникают ситуации, когда необходимо полностью исключить обратимость. Из четырех предложенных регулятором методов обезличивания только один отвечает этому требованию – метод изменения состава или семантики, который предполагает обезличивание персональных данных путем замены их результатами статистической обработки, обобщения или удаления части сведений. Но в некоторых случаях такие изменения в базе данных абсолютно недопустимы, так, например, при разработке или доработке конкретной системы структура базы данных и ее наполнение играют важную роль, однако разработчиками являются сторонние работники или работники оператора, в чьи функциональные обязанности обработка персональных данных не входит. Кроме того, такой метод идеален при презентации системы посторонним людям: например, в рамках продажи или при прохождении проверки, он обеспечит возможность демонстрации системы, при этом исключив возможность нарушения конфиденциальности персональных данных, обрабатываемых в ней. Кто-то, возможно, скажет, что это можно сделать, заполнив базу данных случайными данными, однако для проверки всех функций базы данных необходим большой объем различных записей, отвечающих определенным требованиям, что невозможно легко создать и заполнить без использования исходных данных.

Таким образом, появляется задача обезличивания базы персональных данных, с исключением возможности получения каких-либо сведений о субъектах персональных данных по косвенным признакам, но с сохранением полноты, структурированности, релевантности и семантической целостности, условно назовем такой метод деперсонализацией.

Кроссплатформенное решение для деперсонализации в реляционных базах данных. Сегодня сложно представить автоматизированную обработку персональных данных без использования базы данных. Большинство баз данных строится с использованием SQL. Так, по данным профессионального сообщества Wikibon, на их долю приходится более 80% рынка (рис. 1) [6]. К наиболее популярным системам управления базами данных (СУБД) на языке SQL среди бесплатных относятся: MySQL, MariaDB, MongoDB и PostgreSQL (рис. 2) [7].

Рис. 1. Доля рынка реляционных баз данных на 2012 по данным Wikibon [6]

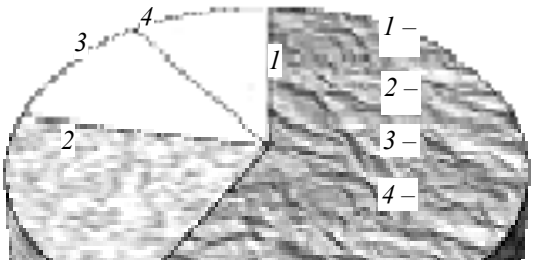


Рис. 2. Рынок реляционных баз дынных за 2013 г. по данным компании Infobox [7]

Выделяют два сегмента обезличивания персональных данных: статическое и динамическое. Статическое обезличивание применяется над копией промышленной версии базы данных и может беспрепятственно устанавливаться на внешние публичные носители информации без угрозы рас-

пространения реальных сведений о субъектах персональных данных. Такой подход мы и назвали деперсонализацией, поскольку он не предусматривает возможность обратного процесса – деобезличивания. Динамическое обезличивание работает в пределах защищенного периметра, используя дополнительные прокси-серверы, и работает путем перехвата и модификации ответов по заранее заданным алгоритмам. Объем передаваемых немодифицированных данных может зависеть от уровня полномочий запрашиваемого субъекта. В рамках настоящей работы подробно рассмотрим статистическое обезличивание, исходя из поставленной задачи.

Согласно магическому квадранту, приведенному в аналитическом отчете ведущей мировой исследовательской и консалтинговой компании Гартнер [8], на рынке присутствуют 3 лидирующих вендора: IBM с продуктом «InfoSphere Optim Data Privacy», Informatica с продуктом «Persistent Data Masking» и компания Oracle – «Data Masking Pack». Ввиду платности продуктов вышеуказанных вендоров оценить весь функционал не удалось. В табл. 1 приведено сравнение продуктов, использующих статическую деперсонализацию, по общедоступным параметрам.

Таблица 1

Сравнение продуктов, использующих статистическую деперсонализацию

Продукт / Характеристика	InfoSphere Optim Data Privacy [9]	Persistent Data Masking	Data Masking Pack
Предустановленные правила модификации данных	Да	Да	Да (алгоритм поиска отображения колонки к заданному правилу)
Возможность написание собственных правил-функций модификации данных	Да (C, C++, Lua, Assembler, VS COBOL II, PL/I, C)	Нет	Да (регулярные выражения)
Проверка целостности ссылок при модификации данных	Да	Да	Да
Возможность ускорения обработки при использовании кластеризации	Нет	Нет	Да (при использовании расширенной версии СУБД Oracle)

Как видно из отчета и сравнительной таблицы, продукты, способные провести как статическую, так и динамическую деперсонализацию на зарубежном рынке присутствуют в достаточном объеме. К сожалению, очень мало российских компаний из разряда малого бизнеса или государственных учреждений могут позволить себе столь дорогое решение. Поэтому большинство скриптов деперсонализации пишутся под себя без знания специфики, без анализа безопасности итогового решения (в качестве отрицательного примера можно привести скрипт использующий функцию реверсивности [10]) и как следствие на различных языках программирования.

Каким же образом можно унифицировать работу статической деперсонализации? Для начала необходимо выделить основные методы. К ним относятся:

- Перемешивание – перестановка значений в указанном множестве данных с удалением пиковой статистики данных.
- Обнуление/замыливание данных – возможность генерирования или установка одинаковых значений в поля с шаблонными данными (номер паспорта, пенсионного страхования и т.д.).
- Изменение семантики – удаление, замена или изменение части сведений какими-либо обобщенными значениями.
- Изменение итогового объема данных – увеличение объема модифицированной базы при помощи генерации или копирования данных либо удаление части зависимой информации.

В качестве универсального языка программирования будем использовать PL/SQL скрипты, предоставляющие мощный инструмент для обработки данных на сервере СУБД. В итоге алгоритм работы создания деперсонализированной базы данных будет выглядеть следующим образом:

- Для исходной базы данных необходимо настроить master-slave репликацию, тем самым при работе скрипта мы снимем нагрузку с основного сервера.
- Перед запуском скриптов необходимо остановить репликацию на вторичном сервере и произвести дублирование базы данных, тем самым актуализируя объем и сами данные БД.
- Завершающим шагом является запуск скриптов деперсонализации.

К основным недостаткам такого решения можно отнести необходимость адаптации хранимых процедур к БД организации. Связано это с отсутствием интуитивно понятного графического интерфейса, позволяющего соотносить поля с необходимыми методами деперсонализации данных.

Автоматизированная система обезличивания данных. Если подходить к вопросу обезличивания персональных данных по методике Роскомнадзора, т.е. сохраняя возможность обработки персональных данных в полном объеме, то можно предложить воспользоваться функционалом СУБД CryptDB, которая способна эффективно обслуживать запросы к реляционной базе данных – поиск, сортировка, математические функции и др. – без расшифровки записей. Таким образом, на стороне сервера база данных хранится в зашифрованном виде, что согласно Приказу регулятора [1] можно назвать обезличенным видом, поскольку это защищает данные от несанкционированного доступа и обеспечивает возможность их обработки. Обезличенные персональные данные за счет средств CryptDB позволяют сохранить такие свойства, как полнота, структурированность, релевантность, применимость и обратимость (описание свойств приведено выше), поскольку персональные данные в полном объеме могут обрабатываться легальным пользователем, а без дополнительной информации (секретного ключа) такая база данных будет представлять собой набор символов. Свойство семантической целостности в зашифрованной базе данных выполняться не будет, что полностью исключает возможность косвенного получения информации. Оценкой свойств такого способа обезличивания являются:

- Обратимость – позволяет провести процедуру деобезличивания.
- Вариативность – позволяет перейти от одной таблицы соответствия к другой без проведения процедуры деобезличивания.
- Изменяемость – позволяет вносить изменения в массив обезличенных персональных данных без предварительного деобезличивания.
- Стойкость – данный способ обезличивания является стойким к атакам на идентификацию субъекта персональных данных. Проведение такой атаки будет возможно только в случае раскрытия секретного ключа.
- Совместимость – возможно интегрирование записей, соответствующих отдельным атрибутам.
- Возможность косвенного деобезличивания – по зашифрованной базе данных невозможно провести косвенное деобезличивание персональных данных с использованием информации других операторов.
- Параметрический объем – объем зашифрованной базы данных в 4 раза больше объема исходной базы данных.
- Возможность оценки качества данных – проведение анализа качества обезличенных данных возможно.

Рассмотрим более подробно принципы работы CryptDB (схема работы с CryptDB представлена на рис. 3). Прокси-сервер хранит у себя мастер-ключ и схему базы данных. Сторонний сервер хранит у себя зашифрованную базу данных, хранимые процедуры и функции для работы CryptDB, а также служебные таблицы. Запросы с данными шифруются только от прокси-сервера и обратно. А все пользовательские запросы и ответы передаются в незашифрованном виде, поэтому прокси-сервер должен находиться в доверенной зоне [11–13].

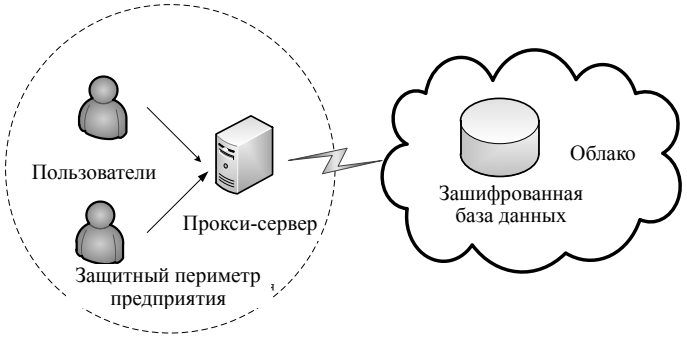


Рис. 3. Общая схема работы CryptDB

Из вышепредставленных криптографических алгоритмов детального рассмотрения заслуживает функция объединения данных разных таблиц по ключевым полям без необходимости их повторного шифрования. Итак, рассмотрим работу данного алгоритма на примере собственного приложения (табл. 2).

Таблица 2

Алгоритмы шифрования, функции и операции, используемые CryptDB

Схема	Алгоритм	Функция	Операции
RND	AES in CBC	нет	
DET	AES in CMC	Equality	=, !=, IN, COUNT, GROUP BY
OPE	OPSE [14]	Order	>, >=, <, <=, SORT, MAX, MIN
HOM	Paillier cryptosystem [15]	+,*	SUM
SEARCH	Song et al. [16]	Поиск по словам	LIKE
JOIN	ECC [17]	Join	LEFT JOIN, INNER JOIN, RIGHT JOIN, JOIN

Для реализации данного алгоритма необходимо реализовать следующие функции:

1. Генерация ключей.

а. Расчет параметров эллиптической кривой (генерация ключей, выбор кривой и фиксированной точки над нею).

б. Генерация секретных ключей для обращения к столбцу Sk_{col}, Sk_{msg}.

в. При генерации ключей используется алгоритм генерации псевдослучайного числа $PRP_{key}(\arg)$.

2. Шифрование сообщения m в виде точки C_i при обращении к столбцу i.

а. Рассчитываются секретные ключи для столбца: $csk_i = PRP_{Sk_{col}}(i)$, $csk_j = PRP_{Sk_{col}}(j)$.

б. Точка C_i вычисляется как $C_i = G \cdot csk_i \cdot PRP_{Sk_{msg}}(m)$, где G – фиксированная точка.

3. Вычисление токена $t_{i\to j}$ для операции обращения к столбцам выполняется следующим образом:

а. Используя значения из 2, *а* наш токен примет вид $t_{i\to j} = \frac{csk_j}{csk_i} \bmod n$, где n – это порядок эллиптической кривой.

4. Как результат мы можем продолжать выполнять операции шифрования на другой таблице без необходимости перешифрования:

а. Вычислим точку $C_{new} = C_i \cdot t_{i\to j}$.

Чтобы проверить правильность расчетов, необходимо доказать правильность работы алгоритма. Проверим, является ли точка C_{new} зашифрованной точкой другой таблицы:

$$C_i \cdot t_{i\to j} = C_i \cdot \frac{csk_j}{csk_i} \bmod n = G \cdot csk_i \cdot PRP_{Sk_{msg}}(m) \cdot \frac{csk_j}{csk_i} \bmod n = G \cdot PRP_{Sk_{col}}(j) \cdot PRP_{Sk_{msg}}(m).$$

Согласно алгоритму (п. 2, *а*), данное вычисление является зашифрованным обращением к столбцу j, из чего следует, что при использовании токена $t_{i\to j}$ можно обращаться к другой таблице зашифрованной на одном ключе Sk_{col}.

Дополнительно стоит отметить, что CryptDB шифрует все данные различными алгоритмами для обеспечения возможности выполнения операций над ними без расшифрования. Каждый столбец строки в зашифрованной базе данных представлен с 4-кратной избыточностью. Например, для хранения значения столбца ID, в зашифрованной базе данных хранится 4 столбца значений: вектор инициализации (IV) и 3 слоя (det, hom, ope) (рис. 4).

ID	NAME
1	Sasha

C1-IV	C1-Eq	C1-Ord	C1-Add	C2-IV	C2-Eq	C2-Ord	C2-Add
X27c3	X2b82	Xcb94	Xc2e4	X8a13	Xd1e3	X7eb1	X29b0

Рис. 4. Пример хранения исходной базы данных в зашифрованном виде CryptDB

Разработчики приложений, работающих с CryptDB, имеют возможность указывать для конкретных столбцов минимальный слой, в котором тот может находиться, таким образом, данные этого столбца не смогут находиться в слое, менее защищенном, чем установленный разработчиком ми-

нимальный слой. Если специфика работы с конкретными данными известна заранее, то для уменьшения времени обработки запросов можно удалить те слои, в которых нет необходимости.

Заключение. В настоящей статье рассмотрены различные подходы к обезличиванию персональных данных. Приведено кроссплатформенное решение для деперсонализации в различных реляционных базах данных, что позволит избежать необходимости написания скрипта для каждой СУБД и ошибок при их самостоятельном написании.

СУБД CryptDB рассмотрена с точки зрения надежного инструмента обезличивания персональных данных, иллюстрация свойств и характеристик такого обезличивания в рамках методических рекомендаций Роскомнадзора показывает возможность такого применения. Конечно, CryptDB является достаточно новой технологией, которая имеет ряд недостатков, в основном связанных со скоростью работы.

Какое-то время развитие CryptDB остановилось последняя версия проекта вышла в 2011 г., однако в 2013 году вышла статья об использовании описываемой СУБД [18]. Исходя из быстрого развития сервисов, предоставляющих облачное хранение данных, такой подход к обработке данных может стать лучшим решением для компаний малого бизнеса за счет низкой стоимости и универсальности такого решения.

Литература

1. Приказ Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (вместе с «Требованиями и методами по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ») [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=151882, свободный (дата обращения: 21.05.2014).

2. Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Роскомнадзором 13.12.2013) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_157082/, свободный (дата обращения: 21.05.2014).

3. Лукацкий А.В. Роскомнадзор выпускает неплохую методику по обезличиванию персональных данных // Бизнес без опасности [Электронный ресурс]. – Режим доступа: http://lukatsky.blogspot.ru/2013/12/blog-post_19.html, свободный (дата обращения: 21.04.2014).

4. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. – М.: Статут, 2011. – 134 с.

5. Является ли ФИО персональными данными в контексте ФЗ-152? // Форум информационной безопасности [Электронный ресурс]. – Режим доступа: http://www.itsecurity.groteck.ru/forum.php?sub=6788&from=0&format=printer-friendly, свободный (дата обращения: 21.04.2014).

6. Big Data Database Revenue and Market Forecast 2012–2017 / D. Floyer, J. Kelly, D. Vellante, S. Miniman // Professional community Wikibon [Электронный ресурс]. – Режим доступа: http://wikibon.org/wiki/v/Big_Data_Database_Revenue_and_Market_Forecast_2012–2017, свободный (дата обращения: 21.04.2014).

7. Какие стеки технологий используют чаще на платформе Jelastic? // Блог компании Infobox на Хабрахабр [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/company/infobox/blog/209792/, свободный (дата обращения: 21.04.2014).

8. Magic Quadrant for Data Masking Technology / Gartner. – 2013 [Электронный ресурс]. – Режим доступа: https://www.gartner.com/doc/2636081, свободный (дата обращения: 21.04.2014).

9. Compare IBM data masking solutions: InfoSphere Optim and DataStage [Электронный ресурс]. – Режим доступа: http://www.ibm.com/developerworks/data/library/techarticle/dm-1211maskingsolution/dm-1211maskingsolution-pdf.pdf, свободный (дата обращения: 21.04.2014).

10. On REVERSing comma-separated set of words [Электронный ресурс]. – Режим доступа: http://vbegun.blogspot.ru/2008/01/on-reversing-coma-separated-set-of.html, свободный (дата обращения: 21.04.2014).

11. CryptDB : HOWTO Compile on Ubuntu Linux 12.04 [Электронный ресурс]. – Режим доступа: http://whitehatty.wordpress.com/2012/09/30/cryptdb-howto-compile-on-ubuntu-linux-12-04/, свободный (дата обращения: 21.04.2014).

12. Документация CryptDB [Электронный ресурс]. – Режим доступа: http://people.csail.mit.edu/nickolai/papers/raluca-cryptdb.pdf, свободный (дата обращения: 21.04.2014).

13. Redfield C.M.S. Practical security for multi-user web application databases: partial fulfillment of the requirements for the degree of Master of engineering in electrical engineering and computer science / Massachusetts Institute of Technology. – 2012. – 68 p.

14. Orderpreserving symmetric encryption / A. Boldyreva, N. Chenette, Y. Lee, A. O'Neill // Proceedings of the 28-th Annual international conference on the theory and applications of cryptographic techniques. – Cologne, Germany, 2009. – P. 224–241.

15. Paillier P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes // Proceedings of the International conference on the theory and application of cryptographic techniques. – Prague, Czech Republic, 1999. – P. 223–238.

16. Song D.X. Practical Techniques for Searches on Encrypted Data / D.X. Song, D. Wagner, A. Perrig // Proceedings of IEEE Symposium on Security and Privacy, S&P 2000. – Berkeley, USA, 2000. – P. 44–55.

17. CryptDB: protecting confidentiality with encrypted query processing / R.A. Popa, C.M.S. Redfield, N. Zeldovich, H. Balakrishnan // Proceedings of the 23-rd ACM Symposium on Operating Systems Principles. – Cascais, Portugal, 2011. – P. 85–100.

18. Darrow B. You want to crunch top-secret data securely? CryptDB may be the app for that. – 2013. [Электронный ресурс]. – Режим доступа: http://gigaom.com/2013/04/05/you-want-to-crunch-top-secret-data-securely-cryptdb-may-be-the-app-for-that/, свободный (дата обращения: 21.04.2014).

Трифонова Юлия Викторовна
Ассистент каф. технологий защиты информации
Санкт-Петербургского государственного университета аэрокосмического приборостроения (ГУАП)
Тел.: 8 (812) 494-70-77
Эл. почта: ulia@guap.ru

Жаринов Роман Феликсович
Аспирант каф. технологий защиты информации ГУАП
Тел.: 8 (812) 494-70-77
Эл. почта: roman@vu.spb.ru

Trifonova U.V., Zharinov R.F.

Opportunities of depersonalization personal data in systems using relational databases

This article discusses depersonalization of personal data, Federal service for supervision of communications, information technology, and mass media (Roscomnadzor) point of view and the using problems of depersonalization methods. Cross-platform solution of depersonalization personal data in relational databases is offered. The possibilities of using CryptDB tools, as a reliable method of anonymization of personal data on the server side.

Keywords: depersonalization, personal data, SQL, CryptDB.

УДК 004.056.53:004.272

Р.Т. Файзуллин, Е.В. Щерба, Д.А. Волков

Схема реализации параллельных вычислений как инструмент защиты обрабатываемых данных

Предлагается схема разделения вычислений и хранения данных в центрах обработки данных, гарантирующая невозможность восстановления матрицы системы линейных уравнений на отдельных вычислительных узлах. Доказана применимость данного подхода в случае численного решения некоторых краевых задач для уравнений математической физики.
Ключевые слова: распределенные вычисления, разделение секрета, ЦОД, Грид-система.

Проблема защиты распределенных вычислений. Консолидация обработки и хранения больших массивов информации в центрах обработки данных – одно из самых перспективных направлений совершенствования корпоративных систем. Применение и внедрение ЦОД позволяют наиболее эффективно использовать коллективные вычислительные ресурсы, уменьшают общее число оборудования, снижают расходы на их поддержку [1, 2].

Необходимым элементом ЦОД является гарантированная защита информации. Основными направлениями защиты информации являются: защита от вирусных атак, обеспечение безопасности процесса взаимодействия информационных систем ЦОД с внешними источниками информации и, что наиболее важно, защита информации от несанкционированного доступа. Несмотря на все усилия у пользователей имеется определенная и обоснованная степень недоверия к уровню защиты ЦОД и к облачным вычислениям, основанная на угрозе атаки сговором (collusion attack). Даже наличие криптографических средств защиты информации и требуемых лицензий у поставщика облачных услуг не является для потенциальных потребителей достаточной гарантией защищенности процессов хранения и обработки информации.

Указанная практическая задача реализации защищенных распределенных вычислений (secure multi party computation, MPC) может быть решена с помощью различных схем разделения секрета (СРС). Традиционно в данных схемах присутствует постановщик задачи (клиент, input party, IP), распределяющий данные по вычислительным кластерам (computation parties, CP), и получатель результата (result party, RP) – зачастую клиент (IP). Классические СРС имеют ряд недостатков (высокие накладные расходы на коммуникации, отсутствие гарантии защищенности). Представляется возможным предложить такие СРС, в которых малая, но определяющая информативность часть секрета хранится или обрабатывается у клиента [3–5]. Данный подход позволяет добиться того, что в ЦОД хранятся данные, но не сама информация, и в каждом случае можно привести прозрачное для клиента доказательство того, что по большему массиву данных нельзя в принципе восстановить значимую информацию.

В качестве примера можно рассмотреть такую массовую задачу, как решение СЛАУ. Следует учесть, что структура матриц систем кодирует структуру моделируемых объектов, а задача декодирования и восстановления информации об объекте довольно проста. Поэтому возникает вопрос о правомерности передачи массовых вычислений в облако и об использовании неконтролируемых вычислительных ресурсов. В этом случае естественным выглядит использование распараллеливания вычислений в качестве инструмента разделения секрета со строгим доказательством сохранения секрета при использовании неполных данных.

Предлагаемые схемы параллелизации. Рассмотрим задачу решения большой системы линейных алгебраических уравнений $\mathbf{GX}=\mathbf{F}$, где квадратная матрица $\mathbf{G}$ не вырождена. Предположим, что некий достаточно большой главный минор $\mathbf{A}$ матрицы $\mathbf{G}$ также не вырожден. Тогда можно записать:

$$\begin{pmatrix}\mathbf{A} & \mathbf{B}\\ \mathbf{C} & \mathbf{D}\end{pmatrix}\begin{pmatrix}\mathbf{X}_1\\ \mathbf{X}_2\end{pmatrix}=\begin{pmatrix}\mathbf{F}_1\\ \mathbf{F}_2\end{pmatrix}$$

и привести систему к виду

$$\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{0} & \mathbf{D}-\mathbf{C}\mathbf{A}^{-1}\mathbf{B} \end{pmatrix}\begin{pmatrix} \mathbf{X}_1 \\ \mathbf{X}_2 \end{pmatrix}=\begin{pmatrix} \mathbf{F}_1 \\ \mathbf{F}_2-\mathbf{C}\mathbf{A}^{-1}\mathbf{F}_1 \end{pmatrix}.$$

Если размерность матрицы $\mathbf{D}$ намного меньше, чем размерность $\mathbf{A}$, клиент может получать значения $\mathbf{X}_2$ на своей вычислительной системе, а наиболее трудоемкие операции по вычислению $\mathbf{A}^{-1}, \mathbf{C}\mathbf{A}^{-1}\mathbf{B}$ передавать на общедоступные вычислительные ресурсы.

Обратим внимание, что это далеко не искусственная задача. Например, расчет сложных гидравлических систем сводится к решению систем нелинейных алгебраических уравнений, которые описывают два закона Кирхгофа применительно к графу системы: закон сохранения массы в узлах и закон сохранения энергии вдоль цикла. Размерность $\mathbf{D}$ в этом случае равна числу линейно независимых циклов в графе, что намного меньше числа узлов [6]. Расчет $\mathbf{A}^{-1}$, $\mathbf{A}^{-1}\mathbf{B}$, $\mathbf{A}^{-1}\mathbf{F}_1$ можно произвести только один раз, если граф не изменяется во время эксплуатации системы, так как нелинейность системы определяется матрицами $\mathbf{C}$ и $\mathbf{D}$ и правой частью $\mathbf{F}_2$. В случае массовых расчетов распараллеливание происходит по вариантам, определяемым различными $\mathbf{C}$, $\mathbf{D}$, $\mathbf{F}_2$, т.е. заданием регуляторов расхода и давления и напорами.

Другая массовая задача – вычисление обратной матрицы – может быть решена с помощью формулы Фробениуса [7]:

$$\begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{pmatrix}^{-1}=\begin{pmatrix} \mathbf{A}^{-1}+\mathbf{A}^{-1}\mathbf{B}\mathbf{H}^{-1}\mathbf{C}\mathbf{A}^{-1} & -\mathbf{A}^{-1}\mathbf{B}\mathbf{H}^{-1} \\ -\mathbf{H}^{-1}\mathbf{C}\mathbf{A}^{-1} & \mathbf{H}^{-1} \end{pmatrix},$$

где $\mathbf{H}=\mathbf{D}-\mathbf{C}\mathbf{A}^{-1}\mathbf{B}$ и $\mathbf{A}^{-1}$ существует.

Можно предложить много схем жесткого распараллеливания, но представляется возможным ввести простые правила:

1) два процессора передают данные промежуточных расчетов блоков на третий, если на третьем ранее не обрабатывался какой-либо из блоков матрицы;

2) вычисления следует распределять таким образом, чтобы на каждом процессоре в любой момент времени присутствовало не более чем два блока исходной или промежуточных матриц, причем не лежащих в одной «строке». Это позволяет избежать возможности попытки нахождения нормального решения, которое может дать некоторую информацию о точном решении.

Обратим внимание, что в этом случае мы получаем выигрыш в вычислениях в отличие от предыдущего случая, так как число операций для вычисления обратной матрицы $O(N^4)$, и, начиная с некоторого L, сравнимого с N, получается, что $O((N-L)^4)+O((N-L)^3)<O(N^4)$.

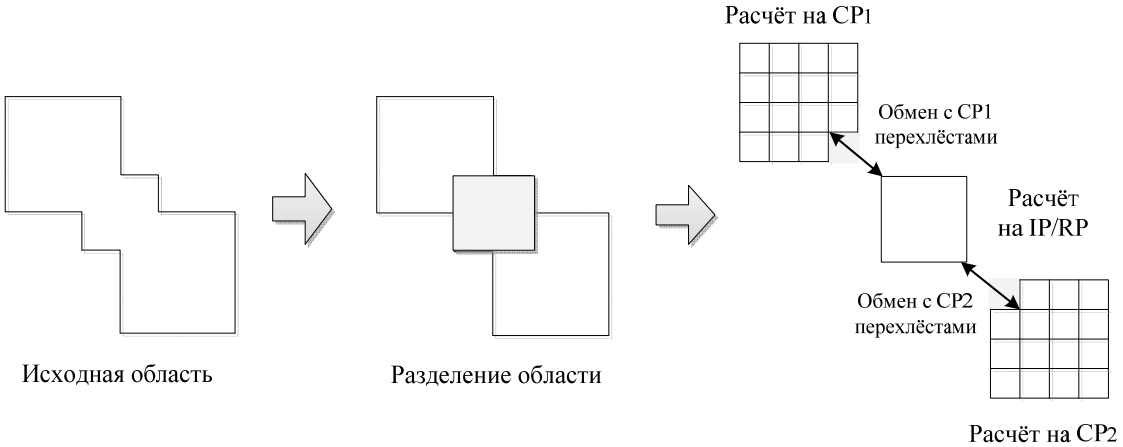


Рис. 1. Распределение вычислений

Если обратиться к итерационным методам и системам уравнений, ассоциированным с эллиптическими задачами, полученными с помощью метода конечных разностей или методом конечных элементов, то решение задачи разделения секрета можно получить с помощью альтернирующего метода Шварца. В этом случае на вычислительной системе клиента (IP) будут осуществляться опе-

рации, ассоциированные с границами подобластей (рис. 1). Основные вычислительные операции, например вычисления в областях сгущения расчетных точек, возлагаются на арендуемые кластеры (CP), а обмен осуществляется пересылкой граничных данных [8].

Общая организация схемы вычислений представлена на рис. 2. Обратим внимание на то, что в качестве управляющего сервера может и должен выступать компьютер клиента (IP/RP).

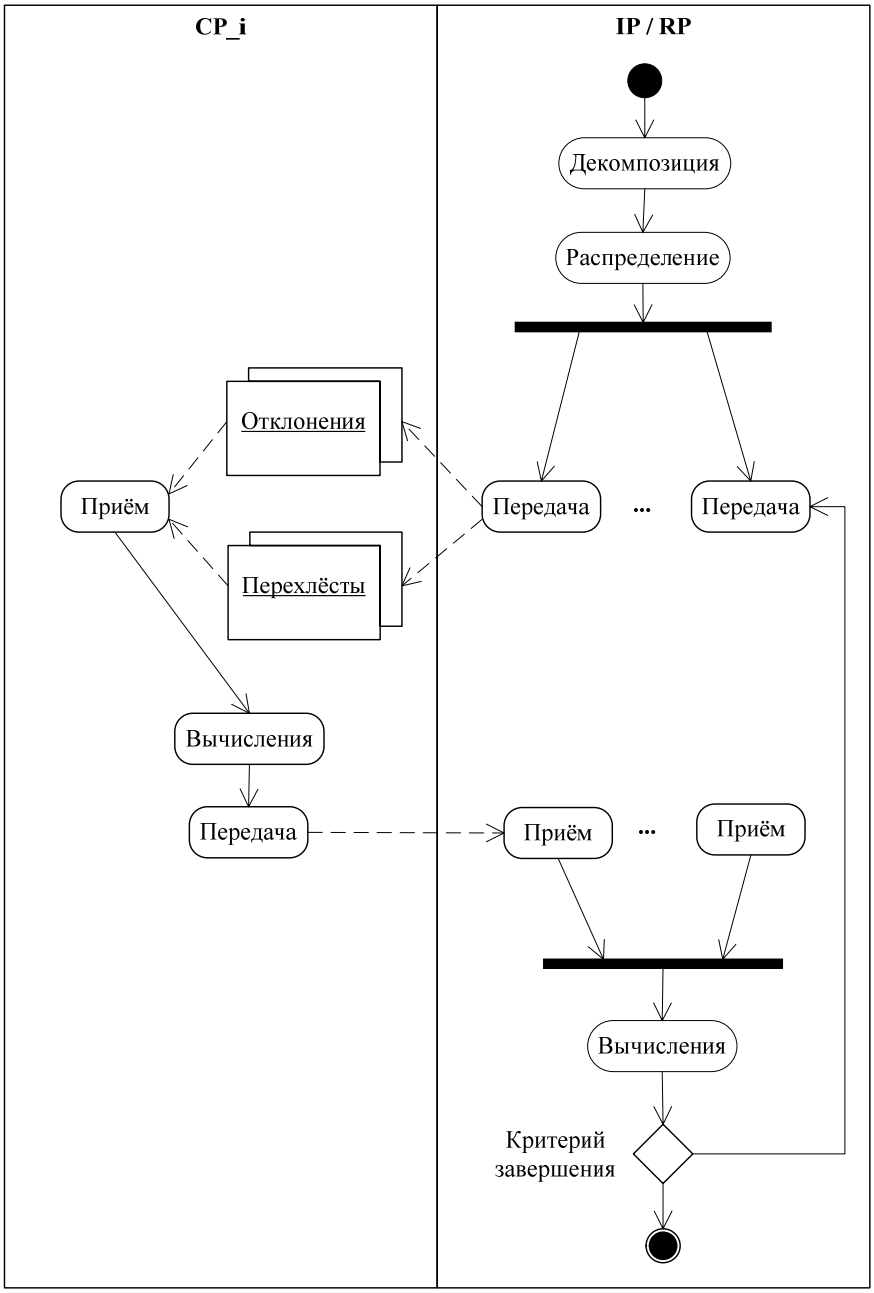


Рис. 2. UML-диаграмма управления вычислениями

Каким образом разделять области по вычислительным устройствам? На рис. 3 приведена постановка модельной задачи обтекания профиля с заданной линией разрыва потенциала.

Учитывая, что расчетные точки сгущаются в области, прилегающей к задней кромке и к точке торможения потоку, разделение областей можно выполнить так, как показано на рис. 4.

Реализация предложенной схемы возможна на базе вычислительной Грид-системы. Указанная Грид-система должна включать удаленные арендуемые кластеры (CP), сеть хранения данных SAN (Fibre Channel / 10 Gb Ethernet), сервер доступа и управления Грид-системой (IP/RP), а также вспомогательный локальный кластер для завершающих вычислений. Основную роль в такой системе играет сервер доступа и управления Грид-системой, отвечающий за постановку, декомпозицию,

диспетчеризацию и мониторинг задач. На текущем этапе исследований на основе разработанных схем разделения секрета ведётся разработка программного обеспечения и протоколов для управления сервером доступа, декомпозиции задач и взаимодействия элементов вычислительной системы.

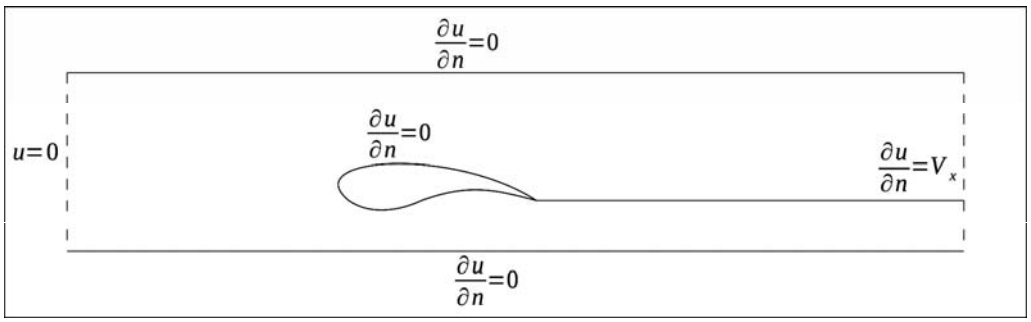


Рис. 3. Постановка задачи обтекания профиля в трубе

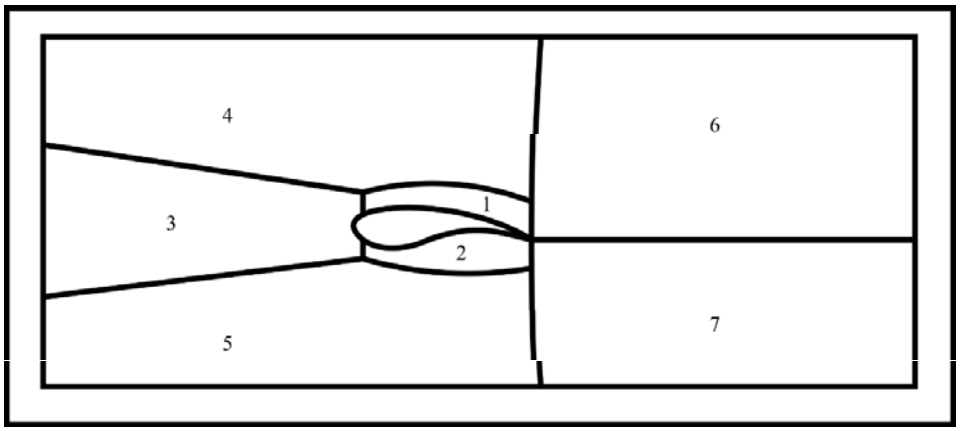


Рис. 4. Разделение областей ответственности между IP/RP (*1*, *2*) и CP (*3*–*7*)

На рис. 5 представлены результаты экспериментальных вычислений, отображающие эффективность вычислительных схем с пересылкой файлов границ. В качестве элементов вычислительной Грид-системы в ходе эксперимента были использованы не кластеры, а типовые бытовые вычислители. Видно, что с ростом размерности задачи эффективность растет и остается единственным способом решения задач большой размерности.

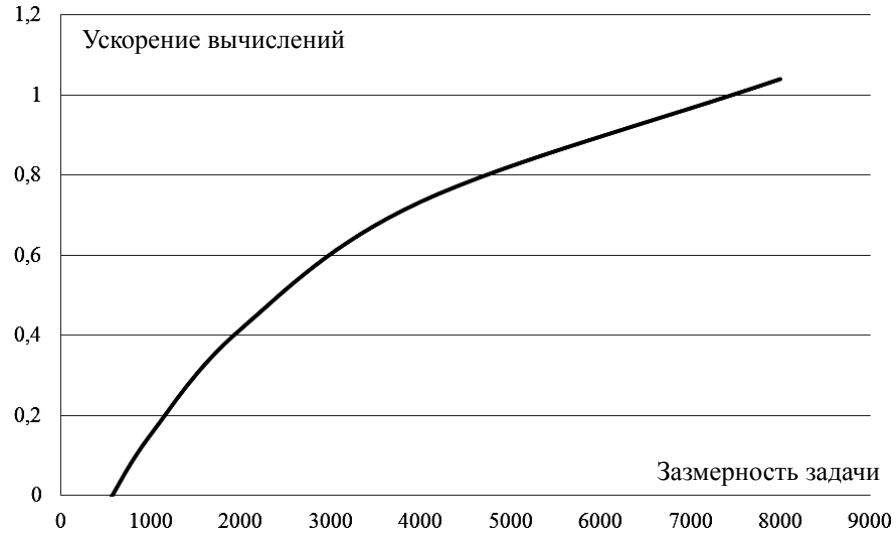


Рис. 5. Решение задачи Дирихле для уравнения Лапласа на расчетной сетке размера $N \times N$

Оценка трудоёмкости восстановления секрета. Естественным образом возникает вопрос о том, насколько надежно защищает предложенный способ разделения секрета от восстановления

секрета на основе знания данных, предоставляемых поставщикам облачных вычислений (СР). Представляется возможным использовать строго доказуемую неединственность решения, или единственность с точностью до широкого класса функций как инструмент в защите информации при решении краевых задач с привлечением неконтролируемых вычислительных ресурсов.

Указанный тезис можно пояснить на простейшем примере. Рассмотрим две односвязные области: $\Omega, \Xi \subset \Omega$ и задачу Дирихле для уравнения Лапласа:

$$\Delta u(x,y) = 0,\ (x,y) \in \Omega - \Xi, \quad u\big|_{\partial\Omega} = \varphi(x,y), \quad u\big|_{\partial\Xi} = \psi(x,y).$$

Решение этой задачи существует и единственно при достаточно слабых условиях на границы и рассматриваемые классы граничных функций. Предположим, что задача решается численно с помощью альтернирующего метода Шварца, где итерации последовательно проводятся на двух подобластях $\Theta_1, \Theta_2, \Theta_1 \cup \Theta_2 = \Omega - \Xi$, представляющих собой вложенные кольца. Кольцо Θ_1 примыкает к Ξ и контролируется вычислительным устройством *A*, а остальная часть Ω контролируется вычислительным устройством *B*. Возникает вопрос, можно ли обладая информацией о решении в области $\Omega - (\Theta_1 \cup \Xi)$, получить информацию о границе Ξ и значениях функции или ее производных на $\partial\Xi$? Если решение такой задачи будет неединственно или единственно с точностью до широкого класса функций, то подобную схему можно использовать для вычислений с арендой мощных вычислительных устройств и с гарантией сохранения секрета.

Рассмотрим три краевые задачи для уравнения Лапласа и покажем, насколько трудоемким является восстановление границы неизвестной области и значений функции на ней в том случае, когда известно решение на некоторой области, топологически эквивалентной кольцу. Тем обстоятельством, что функция сеточная и условной корректностью рассматриваемых задач будем пренебрегать. Покажем, что решение в каждом из этих случаев неединственно.

Рассмотрим задачу Коши для уравнения Лапласа:

$$\Delta u(x,y) = 0,\ (x,y) \in \Omega - \Xi,$$

где Ω – односвязная область, Ξ строго включена в Ω и ее граница не пересекается с границей Ω. Заданы

$$u\big|_{\partial\Omega} = \varphi(x,y), \quad u_n\big|_{\partial\Omega} = \psi(x,y).$$

Задача заключается в нахождении неизвестных функций $\zeta(s)$ и области Ξ:

$$u_{\partial\Xi} = \zeta(s), \Xi \subset \Omega.$$

Если выполнятся условия Неймана $\int\limits_{\partial\Omega} u_n = 0$, то область Ξ может быть пустым множеством, точнее, если сужение решения задачи Неймана на границу равно заданному значению: $v\big|_{\partial\Omega} = u_n\big|_{\partial\Omega} = \varphi$. Но оно может быть и не пустым, а любым, включенным в Ω. Таким образом, в этом, самом простом случае решение неединственно. Очевидно, что в случае выполнения условия Неймана, выполнения условий согласования между граничными значениями функции и ее нормальной производной область Ξ определяется неединственным образом. То есть вырезая из области Ω любое Ξ, не касающееся границы Ω, мы никак не влияем на решение вне Ξ и граничные условия.

Как поступать в более сложном случае, когда согласования между граничными условиями нет? Рассмотрим логарифмический потенциал по неизвестной площади и два нелинейных уравнения, выполняющихся на границе Ω, обозначим их *A*:

$$\sigma \iint\limits_{\Xi} \ln\left(\frac{1}{\sqrt{(x-x_s)^2 + (y-y_s)^2}}\right) ds = \varphi(x,y), \qquad \sigma \frac{\partial}{\partial n} \iint\limits_{\Xi} \ln\left(\frac{1}{\sqrt{(x-x_s)^2 + (y-y_s)^2}}\right) ds = \psi(x,y),$$

где σ – это неизвестная константа. Второе уравнение при выборе конкретного σ хорошо известно, это обратная задача гравиметрии определения формы области. Предположим, что решение второго уравнения единственно. Тогда, подставляя решение в первое уравнение, мы в общем случае не получим равенство. Надо будет подобрать такое σ и соответствующее ему решение, например, методом деления пополам, так, что оба уравнения обратятся в тождество. Таким образом, мы можем найти область и функцию $u_{\partial\Xi} = \zeta(s)$. Но обратим внимание на то, что, рассматривая разложения: $\varphi = \varphi_1 + \varphi_2, \psi = \psi_1 + \psi_2$, где слагаемые с индексом 1 отвечают согласованным краевым условиям задачи Неймана, мы можем получить решение в виде $u = u_1 + u_2$, где индекс *1* отвечает решению ранее

рассмотренной задачи Неймана, а индекс 2 отвечает решению задачи с помощью логарифмического потенциала. Рассматривая в качестве Ξ любую область Ξ_1, такую, что $\Xi \subset \Xi_1 \subset \Omega$, мы получим функцию, удовлетворяющую уравнению Лапласа в $\Omega - \Xi$ и заданным краевым условиям, что доказывает неединственность решения задачи.

Рассмотрим задачу продолжения функции, заданной на некоторой области K, гомеоморфной кольцу, через внутреннюю границу в область Ω, считая, что $\Delta u(x,y) = 0,\ (x,y) \in K,\ \Omega - \Xi$, где Ω – односвязная область, Ξ включена в Ω, и ее граница не пересекается с границей Ω. Значения функции в кольце известны: $u(x,y), (x,y) \in K$.

Задача заключается в нахождении неизвестной области Ξ и неизвестной нормальной производной на границе этой области:

$$u_n|_{\partial\Xi} = g(x,y), \Xi \subset \Omega \quad \text{с условием} \quad \int_{\partial\Xi} g(x,y)dl = 0.$$

Функция $V(x,y) = \frac{1}{\pi}\int_{\partial\Xi} g(x_s,y_s)\ln\left(\frac{1}{\sqrt{(x_s-x)^2+(y_s-y)^2}}\right)ds$ задает гармоническую функцию вне границы Ξ, удовлетворяющую условию Неймана на границе $V_n|_{\partial\Xi} = g(x,y)$.

Для любых двух замкнутых кривых в K, окаймляющих Ω, можно составить два интегральных уравнения первого рода, связывающих известные значения $u(x,y),\ (x,y) \in K$ и значения, индуцированные логарифмическим потенциалом простого слоя. Предположим, что решение этих уравнений существует и единственно вне зависимости от выбора кривых. Рассмотрим область $\Xi_1, \Xi \subset \Xi_1 \subset \Omega$. Функция V задает нормальную производную $V_n|_{\partial\Xi_1}$, с помощью которой можно также построить гармоническую функцию W вне и внутри Ξ_1. В самом деле, из-за отсутствия источников $\int_{\partial\Xi_1} V_n dl = 0$ и в качестве плотности можно взять $V_n|_{\partial\Xi_1}$. Внутри кольца $\Xi_1 - \Xi$ и вне его функция W совпадает с индуцированной ранее, так как их разность является гармонической функцией с нулевыми условиями Дирихле и Неймана на границе Ξ_1. В итоге мы получим неединственность Ξ при принятом допущении, что решение системы интегральных уравнений единственно задает Ξ.

Предположим, что на границе Ξ задано условие непротекания $u_n|_{\partial\Xi} = 0, \Xi \subset \Omega$. В этом случае построение потенциала V с помощью логарифмического потенциала простого слоя, как в предыдущем случае, невозможно. Как поступить в этом случае? Рассмотрим u решение смешанной задачи Неймана в кольце $\Omega - \Xi$

$$\Delta u(x,y) = 0,\ (x,y) \in \Omega - \Xi, \quad u|_{\partial\Omega} = \varphi(x,y),\ u_n|_{\partial\Xi} = 0$$

и покажем, что выбор Ξ не единствен. Функции u можно поставить в соответствие сопряженную гармоническую функцию v так, что $f = u + iv$ будет голоморфной. Если мы отступим от $\partial\Xi$ и выберем некоторую точку (x_0, y_0), лежащую во внутренности $\Omega - \Xi$, то через нее проходит Γ, линия уровня v, на которой также будет выполняться условие непротекания. Область, ограниченную Γ, можно рассматривать как Ξ_1, и u будет гармонической функцией в $\Omega - \Xi_1$.

Таким образом, практическая задача сводится только к методу подбора, который можно организовать, обладая некоторой априорной информацией и выбирая вид $\partial\Xi$ так, чтобы на внешней границе Ω происходила наиболее гладкая склейка с известным вне Ω решением и его производными. Оценим трудоемкость такого подхода. Если, например, сетка в подобласти $1 \cup 2$ представляет собой образ прямоугольной сетки размера $K \cdot N$, где K – число шагов сетки по нормали от Ξ, а N – число шагов сетки по поверхности, то число выборов «гладкой функции», описывающей $\partial\Xi$, будет равно $K \cdot 2^{N-1}$. Отсюда следует, что уже при $N \approx 80$ возникает комбинаторный взрыв и решение задачи продолжения методом подбора невозможно на современной и перспективной вычислительной технике.

Обратим также внимание на то, что неизвестными (секретом) являются не только Ξ и $\zeta(x,y)$ или $g(x,y)$, но и параметры сгущения или организации сетки внутри области Ω, что не только полностью исключает возможность решения задачи за приемлемое время, но и ставит вопрос об алгоритмической неразрешимости задачи *B*.

Заключение. Предложенные схемы организации защищенных параллельных вычислений (МРС), а также введенные простые правила позволяют решить вопрос о правомерности передачи массовых вычислений во внешние ЦОДы и об использовании неконтролируемых вычислительных ресурсов. Показано, что задача восстановления информации в этом случае сводится к задаче аналитического продолжения с неединственным решением. Реализация разработанных схем возможна на базе типовой Грид-системы и специализированного программного обеспечения.

Литература

1. BYTEmag. Центры обработки данных [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/articles/detail.php?ID=14070?ID=14070, свободный (дата обращения: 01.04.2014).

2. Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года [Электронный ресурс]. – Режим доступа: http://government.ru/docs/8024, свободный (дата обращения: 01.04.2014).

3. Файзуллин Р.Т. Приложение алгоритма префиксного кодирования массива данных в схеме разделения секрета / Р.Т. Файзуллин, Д.А. Сагайдак // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 136–140.

4. Файзуллин Р.Т. Алгоритмы разделения секрета с использованием принципиально малой части в качестве ключа / Р.Т. Файзуллин, И.Р. Файзуллин, О.Т. Данилова // Вестник Тюм. гос. ун-та. – 2011. – Вып. 7. – С. 175–179.

5. Кручинин В.В. Подходы к созданию защищенного архива на основе разделения секрета / В.В. Кручинин, А.А. Шелупанов // Доклады ТУСУРа. – 2008. – № 2 (18), ч. 1. – С. 67–72.

6. Логинов К.В. Расчет, оптимизация и управление режимами работы больших гидравлических сетей / К.В. Логинов, А.М. Мызников, Р.Т. Файзуллин // Математическое моделирование. – 2006. – Вып. 18 (9). – С. 92–106.

7. Bodewig E. Matrix calculus. – Amsterdam: North-Holland, 1956. – 334 p.

8. Мещеряков Р.В. Критерий структурной сложности информационных систем // Труды СПИИРАН. – 2010. – № 3 (14). – С. 76–90.

Файзуллин Рашит Тагирович
Д-р техн. наук, профессор, зав. каф. комплексной защиты информации
Омского государственного технического университета (ОмГТУ)
Тел.: 8 (381-2) 21-77-02
Эл. почта: r.t.faizullin@mail.ru

Щерба Евгений Викторович
Канд. техн. наук, доцент каф. комплексной защиты информации ОмГТУ
Тел.: 8 (381-2) 21-77-02
Эл. почта: evscherba@gmail.com

Волков Данил Андреевич
Студент Омского государственного университета им. Ф.М. Достоевского
Эл. почта: volkovdanil91@gmail.com

Faizullin R.T., Shcherba E.V., Volkov D.A.

A scheme for the implementation of parallel computing as a protection mechanism of processed data

In this paper we propose a scheme of separation of computing and storage in data centers. The scheme guarantees the impossibility of restoring the matrix system of linear equations on individual compute nodes. The applicability of this approach in the case of numerical solution of some boundary value problems for equations of mathematical physics has been proved.

Keywords: distributed computing, secret sharing, DPC, Grid-system.

УДК 004.056

И.А. Ходашинский, В.А. Дель, А.Е. Анфилофьев

Выявление вредоносного сетевого трафика на основе ансамблей деревьев решений

Рассматривается проблема обнаружения вредоносного трафика в компьютерных сетях. Для решения данной проблемы предлагается использовать ансамбль деревьев решений. Построение отдельного дерева ведется с помощью алгоритма C4.5. Предложены варианты объединения деревьев в ансамбли. Проведены эксперименты на данных репозиториев KEEL, KDD Cup 1999.

Ключевые слова: обнаружение вторжений, ансамбль деревьев решений, алгоритм C4.5.

Рост масштабов компьютерных сетей, усложнение их структуры и увеличение объема трафика, а также рост числа компьютерных злоупотреблений и сетевых атак диктуют необходимость повышения безопасности компьютерных сетей. Одним из средств выявления действий, направленных на нарушение конфиденциальности, целостности и доступности компьютерной системы или сети, является система обнаружения вторжений. Обнаружение вторжений – это процесс мониторинга и анализа событий, происходящих в компьютерной системе, с целью поиска признаков проблем безопасности.

В основе построения систем обнаружения вторжений лежат различные методы и подходы, в том числе методы интеллектуального анализа данных [1, 2]. Система обнаружения такого типа классифицирует данные аудита как нормальные и аномальные на основе набора шаблонов и правил. Преимущество использования правил заключается в их простоте и интерпретируемости. Предложено множество индуктивных алгоритмов генерации правил, популярным является подход на основе деревьев решений. Дерево решений состоит из трех основных компонентов: узлов, дуг и листьев. Узел имеет метку наиболее информативного признака, который еще не встречался в пути от корня до рассматриваемого узла. Дуга помечена значением узла-признака, из которого она выходит. Каждый лист имеет метку класса. Отдельные классификаторы в виде деревьев решений успешно применяются при построении систем обнаружения вторжений [3, 4]. Одним из путей повышения точности классификации является объединение отдельных классификаторов в ансамбль.

Цель работы – описание построения ансамбля классификаторов на основе деревьев решений.

Алгоритм C4.5. В алгоритме построения деревьев решений C4.5 с каждым узлом дерева ассоциировано подмножество обучающей выборки. Для каждого атрибута (признака) считается прирост информации, который будет обеспечен при разбиении подмножества по данному атрибуту [5]. Из всех возможных вариантов выбирается атрибут, дающий лучшее разбиение, после чего исходное подмножество в соответствии с выбранным атрибутом делится на несколько подмножеств, для каждого из которых описанная процедура вызывается рекурсивно.

Псевдокод алгоритма C4.5 представлен ниже:

```
procedure BUILD_TREE(T)
     best_attr ← null, best ← null
     for all a in attributes do
          s ← split_gain(T, split(T, a))
          if better(s, best) then
               best ← s, best_attr ← a
          end if
     end for
     for all T_i in split(T, best_attr) do
          build_tree(T_i)
          end for
     end procedure
```

В данном псевдокоде *split_gain* соответствует приросту информации после разбиения исходного множества *T* по атрибуту *a*

$$split\_gain = \frac{Info(X) - Info_a(X)}{-\sum_{i=1}^{n} \frac{|T_i|}{|T|} \log_2 \frac{|T_i|}{|T|}}.$$

Ансамбль деревьев решений. Для повышения точности классификации можно использовать несколько деревьев решений, объединенных в ансамбль. Ансамбль состоит из деревьев решений, количество которых указывается при создании ансамбля и агрегирующего модуля, задача которого заключается в объединении выводов одиночных деревьев решений.

На вход ансамбля классификаторов поступает обучающая выборка, которая впоследствии для каждого дерева решений случайным образом разделяется на две части в заданном отношении, собственно обучающая подвыборка и валидационная подвыборка. Обучающая подвыборка используется для обучения дерева решений, валидационная подвыборка – для оценки качества классификации и присвоения дереву определенного веса. Таким образом, деревья решений в ансамбле различны, так как они обучены на разных подвыборках. Соотношение размеров обучающей и валидационной подвыборок может варьироваться, пользователь указывает число *ratio* из отрезка [0, 1], в результате размер обучающей подвыборки составит $size = ratio \cdot size(train)$, в свою очередь, размер валидационной подвыборки составит $size = (1 - ratio) \cdot size(train)$.

Вес дерева в ансамбле – это характеристика, используемая агрегирующим модулем при объединении выводов одиночных деревьев, лежащая в отрезке [0, 1]. Интуитивно понятно, что если дерево качественно обучилось, у него будет больший вес, и данную информацию необходимо использовать при объединении ответов одиночных классификаторов.

После обучения ансамбль способен обрабатывать объекты контрольной выборки. Каждый объект контрольной выборки передается всем деревьям решений. Каждое дерево решений независимо друг от друга предсказывает класс, к которому принадлежит объект. Затем ответы всех деревьев решений объединяются в один с использованием агрегирующего модуля.

В работе рассмотрены две реализации агрегирующего модуля. Первая из них соответствует алгоритму простого голосования, ответом ансамбля является класс, за который проголосовало наибольшее количество деревьев решений. Вторая реализация агрегирующего модуля соответствует алгоритму взвешенного голосования. Данная реализация учитывает веса, присвоенные деревьям при обучении. Псевдокод данного подхода представлен ниже:

```
function WEIGHTED_MAJORITY_VOTING(sample)
  votes ← array[N]
  for all c in classifiers do
       class ← c.predict(sample)
       votes[class] ← votes[class] + c.weight
  end for
  return index_of_max(votes)
  end function
```

Алгоритмическая сложность обучения ансамбля составляет $O(MN^2K \log N)$, где M – количество деревьев решений в ансамбле, N – размер обучающей выборки, K – количество атрибутов у объекта. Алгоритмическая сложность классификации одного объекта составляет $O(M \log N)$, где M – количество деревьев решений в ансамбле.

Наборы данных. Для сравнения качества работы классификаторов были использованы наборы общеизвестных данных из репозитороев KDD Cup 1999 (http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html) и KEEL (http://www.keel.es). Описания наборов приведены ниже.

Bupa – набор данных, описывающий заболевания печени, возникающие от чрезмерного употребления алкоголя; задача заключается в определении наличия заболевания; количество атрибутов – 6, количество классов – 2, количество объектов – 345.

Набор данных *Glass* описывает виды стекол по их химическому составу; количество атрибутов – 9, количество классов –7, количество объектов – 24.

Набор данных *Wine* представляет собой результаты химического анализа вин, выращенных в одном регионе Италии, но полученных из трех различных сортов винограда; количество атрибутов – 13, количество классов – 3, количество объектов – 178.

Iris – набор данных, описывающий типы цветков ириса; количество атрибутов – 4, количество классов – 3, количество объектов – 150.

Набор данных *KDD Cup* описывает сетевые атаки; количество атрибутов – 41, количество классов – 23, количество объектов – 4898431.

Эксперимент. Эксперимент проводился на оборудовании следующей конфигурации: центральный процессор Intel Core i5 2,5 ГГц, оперативная память 16 Гб 1600 МГц DDR3, жесткий диск SSD 256 Гб, операционная система Mac OS X 10.9.2.

Для оценки эффективности классификаторов были проведены тесты на четырех наборах данных из репозитария KEEL. Сравнение проводилось с использованием метода кроссвалидации. Результаты проведенных экспериментов были сопоставлены с результатами из работы [6], где испытания проводились на тех же данных. В табл. 1 в столбце «Среднее» указаны усредненные значения процента правильной классификации, столбце «СКО» – среднеквадратическое отклонение.

Таблица 1

Результаты классификации данных из репозитория KEEL

Алгоритм	*Bupa*		*Glass*		*Iris*		*Wine*	
	Среднее	СКО	Среднее	СКО	Среднее	СКО	Среднее	СКО
Ant Miner	57,25	7,71	53,74	12,92	96,00	3,27	92,06	6,37
CORE	61,97	4,77	45,74	9,36	92,67	4,67	**94,87**	4,79
HIDER	65,83	10,04	64,35	12,20	**96,67**	3,33	82,61	6,25
SGERD	57,89	3,41	38,33	5,37	**96,67**	3,33	87,09	6,57
TARGET	65,97	1,41	44,11	5,37	92,93	4,33	82,24	7,57
CART	66,95	11,88	67,15	9,49	96,00	3,44	88,20	4,85
C4.5	67,00	8,66	67,44	12,27	96,00	4,66	94,90	6,19
Ensemble (10 C4.5)	**69,78**	9,67	**70,16**	16,24	94,67	4,21	93,34	5,51

Общеизвестно, что наборы данных *bupa* и *glass* являются трудными для классификации, однако каждый из ансамблей деревьев решений неплохо справился с этой задачей. Полученные результаты позволяют сделать вывод о достаточно высокой эффективности разработанных ансамблей классификаторов.

Работоспособность ансамблей деревьев решений была проверена на данных, связанных с сетевыми атаками. Набор KDD Cup 1999 содержит данные о 22 типах атак, которые могут быть разбиты по четырем классам: DOS (3883370 записей); R2L (1126 записей); U2R (52 записи); Probing (41102 записи). Кроме того, присутствует класс нормальных соединений (972781 запись).

Существует несколько различных подходов к формированию обучающей выборки на несбалансированных наборах данных. Согласно одному из них в обучающую выборку включаются заданный процент от количества объектов каждого класса. Однако достаточно очевидно, что в данном случае такой подход будет нерезультативен с точки зрения точности классификации, распределение классов в наборе данных KDD неравномерно, следовательно, при включении в обучающую выборки одинакового процента от разных классов получим ситуацию, когда наиболее часто встречающиеся классы (DOS и Normal) будут распознаваться отлично, в то время как менее встречающиеся классы (U2R и R2L) будут восприниматься как шумы и распознаваться очень плохо.

В связи с этим для формирования обучающей выборки был применен другой подход. Каждому типу атак в наборе данных KDD было сопоставлено значение класса этой атаки. После чего было произведено разбиение исходного набора данных KDD на пять наборов – по одному для каждого класса. Затем данные в каждом наборе были перемешаны. После этого обучающая выборку была сформирована следующим образом: было взято 25 записей класса U2R и по 200 записей из четырех классов: DOS, Normal, R2L, Probing. Записи, не включенные в обучающую выборку, были включены в контрольную выборку. Таким образом, размер обучающей выборки составил 825 записей, размер контрольной выборки составил 4897606 записей.

В ходе эксперимента в сравнении с другими алгоритмами [7, 8], ансамбль из 10 деревьев C4.5 со взвешенным голосованием на контрольной выборке показал результаты, приведенные в табл. 2. Здесь представлены проценты верно определенных классов атак от общего количества атак данного класса в наборе данных KDD.

Таблица 2

Результаты классификации атак из набора данных KDD

Алгоритм	Normal, %	U2R, %	R2L, %	DOS, %	Probing, %
FLS	10,00	95,00	85,00	80,00	80,00
ESC-IDS	98,20	14,10	31,50	99,50	84,10
Hybrid EFS	**98,50**	76,30	89,00	98,50	82,50
C4.5	95,90	21,10	30,20	97,10	76,30
5-NN	96,30	25,40	3,80	96,70	87,50
EFRID	92,78	88,13	7,41	98,91	50,35
NB	94,20	25,00	5,40	79,40	90,40
Naïve Bayesian	97,68	11,84	8,66	96,65	88,33
Ensemble (10 C4.5)	95,06	**100,00**	**98,7**	**99,88**	**99,57**

Производительность ансамбля классификаторов представлена в табл. 3.

Таблица 3

Производительность ансамбля классификаторов

Класс	Обучение, с	Классификация, мкс
Normal	2,384	7,10
U2R	2,567	37,03
R2L	2,532	14,04
DOS	2,747	4,51
Probing	2,535	13,21

Во втором столбце указано время обучения ансамбля классификаторов, состоящего из десяти деревьев решений, построенных алгоритмом C4.5. В третьем столбце указано среднее время классификации одного объекта. Обучение производилось на одной и той же обучающей выборке, описанной выше. Времена обучения различаются из-за разной загрузки центрального процессора. Различные времена классификации объясняются различными структурами получившихся деревьев решений.

Для подсчета ошибок первого и второго рода для всех атак была произведена замена меток класса на метку «attack», после чего было произведено повторное обучение и проверка на тех же обучающей и контрольной выборках. Результаты бинарной классификации (атака/нормальное соединение) представлены в табл. 4.

Таблица 4

Результаты бинарной классификации

Набор данных	Верно, %	Ошибка 1-го рода, %	Ошибка 2-го рода, %
KDD Cup 1999	98,88	1,08	0,04

Заключение. В работе представлена процедура построения ансамблей классификаторов на основе деревьев решений, обученных алгоритмом C4.5. Работоспособность ансамблей классификаторов проверена на четырех наборах данных из репозитария KEEL. Полученные классификаторы на основе ансамбля деревьев решений легко обучаются и имеют хорошие прогностические способности. Эксперименты на наборах данных о сетевых атаках позволили сделать вывод о том, что перспективным является применение ансамблей классификаторов на основе деревьев решений для обнаружения вторжений. При использовании ансамбля классификаторов получен выигрыш в проценте правильной классификации всех классов атак. В бинарной классификации был получен достаточно высокий процент правильной классификации, ошибки второго рода порядка 0,04% свидетельствуют о том, что разработанный прототип может быть реализован в качестве системы обнаружения вторжений в межсетевом экране.

Однако, при реализации в межсетевом экране нужно отказаться от использования Java в качестве языка программирования в пользу C++ из-за наличия сборщика мусора. В случае недостаточного количества памяти сборщик мусора запускается очень часто, что в свою очередь приводит к замедлению работы системы обнаружения вторжений.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (гранты 12-07-00055а, 14-07-00449а).

Литература

1. Lee W. Adaptive intrusion detection: a data mining approach / W. Lee, S.J. Stolfo, and K.W. Mok // Artificial Intelligence Review. – 2000. – Vol. 14. – P. 533–567.

2. Patcha A. An overview of anomaly detection techniques: existing solutions and latest technological trends / A. Patcha, J.-M. Park // Computer Networks. – 2007. – Vol. 51. – P. 3448–3470.

3. An intrusion detection and alert correlation approach based on revising probabilistic classifiers using expert knowledge / S. Benferhat, A. Boudjelida, K.Tabia, H. Drias // Applied Intelligence. – 2013. – Vol. 38. – P. 520–540.

4. Ohta S. Minimizing False Positives of a Decision Tree Classifier for Intrusion Detection on the Internet / S. Ohta, R. Kurebayashi, K. Kobayashi // Journal of Network and Systems Management. – 2008. – Vol. 16. – P. 399–419.

5. Quinlan J.R. C4.5: Programs for Machine Learning. – San Francisco: Morgan Kaufmann Publishers, 1993. – 299 p.

6. KEEL Data-Mining Software Tool: Data Set Repository, Integration of Algorithms and Experimental Analysis Framework / J. Alcala-Fdez, A. Fernandez, J. Luengo et al. // Journal of Multiple Valued Logic and Soft Computing. – 2011. – Vol. 17. – P. 255–287.

7. Boughaci D. A Fuzzy Local Search Classifier for Intrusion Detection / D. Boughaci, S. Bouhali, S. Ordeche // Proceedings of the International Arab Conference on Information Technology, ACIT, Zarqa, 2011 [Электронный ресурс]. – Режим доступа: http://www.nauss.edu.sa/acit/PDFs/f2988.pdf (дата обращения: 20.04.2014).

8. Корниенко И.С. Программно-инструментальный комплекс идентификации нечетких систем / И.С. Корниенко, О.А. Серебрянникова, И.А. Ходашинский // Жоклады ТУСУРа. – 2012. – №1 (25), ч. 1. – С. 60–64.

Ходашинский Илья Александрович
Д-р техн. наук, профессор каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: hodashn@rambler.ru

Дель Владимир Александрович
Инженер каф. КИБЭВС ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: rush.vr@gmail.com

Анфилофьев Александр Евгеньевич
Студент каф. КИБЭВС ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: yowwi00@gmail.com

Hodashinsky I.A., Del V.A.
Intrusion detection using an ensembles of decision trees

In this paper, we propose ensembles of decision trees for intrusion detection. Verification tests have been carried out by using KEEL data set and the benchmark 1999 KDD Cup data set. The results are encouraging and demonstrate the benefits of our approach.
Keywords: intrusion detection, ensemble approaches, decision trees, algorithm C4.5.

УДК: 621.394.6

А.А. Хорев

Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера

Рассмотрены вопросы, связанные с перехватом побочных электромагнитных излучений (ПЭМИ), возникающих при выводе изображения на экран монитора, оптимальным приемником. Предложены математическая модель и методика оценки возможностей перехвата ПЭМИ видеосистемы компьютера техническими средствами разведки (ТСР).

Ключевые слова: видеосистема, побочные электромагнитные излучения, технический канал утечки информации, перехват информации.

К одной из основных угроз безопасности информации ограниченного доступа, обрабатываемой техническими средствами (ТС), относится *утечка информации по техническим каналам*, под которой понимается неконтролируемое распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего перехват информации.

При обработке информации ПЭВМ технические каналы утечки информации образуются за счет побочных электромагнитных излучений (ПЭМИ), а также вследствие наводок информационных сигналов в линиях электропитания ПЭВМ, соединительных линиях вспомогательных технических средств и систем, цепях заземления и посторонних проводниках.

Наиболее опасным (с точки зрения утечки информации) режимом работы ПЭВМ является вывод информации на экран монитора.

Исследования по перехвату побочных электромагнитных излучений (ПЭМИ) видеомониторов ПЭВМ начались практически одновременно с их созданием и носили закрытый характер.

В зарубежной литературе вместо термина ПЭМИ используются термины «compromising electromagnetic emanations» (компрометирующие электромагнитные излучения) или TEMPEST (сокращение от «transient electromagnetic pulse emanation standard» – стандарт на электромагнитные импульсные излучения, вызванные переходными процессами в электронной аппаратуре).

Первые открытые публикации по перехвату ПЭМИ ПЭВМ появились в начале 80-х годов прошлого века. Наибольшее внимание из них привлекла статья голландского ученого Вима Ван Эйка (Wim van Eck) «Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?», опубликованная в журнале «Computers and Security» в декабре 1985 г. [1].

С тех пор многое изменилось. Переход на интерфейсы VGA и DVI значительно усложнил задачу перехвата ПЭМИ.

Наиболее подробно исследование проблемы перехвата ПЭМИ видеомониторов с интерфейсами VGA и DVI проведено в диссертации М.Г. Кюн (Markus G. Kuhn)) [2]. Для перехвата ПЭМИ он использовал цифровой супергетеродинный приемник Dynamic Sciences R1250 с логопериодической антенной.

Сигнал с демодулятора приемника подавался на цифровой запоминающий осциллограф Tektronix TDS 7054, а затем обрабатывался с использованием специального программного обеспечения и преобразовывался в растровые изображения, которые выводились на монитор компьютера в реальном масштабе времени. Для синхронизации изображения использовался внешний высокостабильный генератор импульсов R-1160C.

Эксперименты проводились в здании, расположенном в полугородской среде. Несмотря на то, что в здании находилось более 100 работающих компьютеров, при экспериментах удавалось перехватывать текстовые изображения на расстояниях 10 м через два офисных помещения (три гипсокартонные стены), расположенных на том же этаже здания [2].

Использование цифрового запоминающего осциллографа позволило М.Г. Кюну реализовать метод некогерентного накопления импульсов, что существенно повысило качество перехваченных изображений. Время усреднения (количество усредняемых кадров) ограничивалось памятью цифрового запоминающего осциллографа.

При проведении исследований М.Г. Кюн установил, что частота обновления яркости (цвета) каждого пикселя изображения F_n (*pixel clock frequency*) зависит от размеров изображения, частоты обновления экрана $F_к$ и особенностей видеокарты, что позволяет, «подстроившись» под тактовую частоту F_n конкретного компьютера, выделять изображение, выводимое на экран его монитора, на фоне побочных электромагнитных излучений других компьютеров.

В открытой отечественной литературе публикации, связанные с техническими каналами утечки информации, вызванными побочными электромагнитными излучениями, стали появляться в конце прошлого – начале этого века. Основное внимание в этих работах уделено средствам измерений и методам измерений ПЭМИ в целях оценки эффективности защиты средств вычислительной техники от утечки информации по техническим каналам, однако вопросы, связанные с теоретической оценкой возможностей перехвата ПЭМИ средствами разведки, практически не рассматривались.

Целью данной статьи является разработка математической модели обнаружения побочных электромагнитных излучений видеосистемы компьютера оптимальным приемником, позволяющей проводить оценку возможностей перехвата ПЭМИ средствами разведки.

Проведенный анализ показал, что в качестве показателя оценки возможности перехвата ПЭМИ СВТ наиболее часто используется вероятность правильного обнаружения информативного сигнала приемным устройством средства разведки P_O при фиксированной ложной тревоге $P_{лт}$ (критерий Неймана–Пирсона).

При перехвате изображения, выводимого на экран монитора, необходимо учитывать, что оно стабильно в течение некоторого времени (T_a), которое зависит от характера действий оператора ПЭВМ и может варьировать от нескольких секунд (при наборе текста) до нескольких минут (при чтении текста). Данный факт позволяет использовать методы цифровой корреляционной обработки принимаемых импульсных сигналов, что существенно повышает отношение сигнал/шум. Следовательно, для расчета вероятности правильного обнаружения пачки одинаковых слабых некогерентных нефлюктуирующих импульсов можно использовать формулу [3]

$$P_O \approx \Phi\left(q \cdot \sqrt{N} - \Phi^{-1}\left(1 - P_{\text{лт}}\right)\right), \tag{1}$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} \exp\left(-\frac{t^2}{2}\right) dt$ – интеграл вероятности; $\Phi^{-1}(x)$ – функция, обратная $\Phi(x)$;

q – энергетическое отношение сигнал/шум на входе разведывательного приемника; N – количество осредненных импульсов, $N = F_{\text{к}} \cdot T_a$; $F_{\text{к}}$ – частота кадровой развертки монитора, Гц; T_a – время стабильности перехватываемого изображения, с.

Учитывая, что для оптимального приемника полоса пропускания фильтра $\Delta F = 1/\tau$, и допуская, что форма импульса прямоугольная, энергетическое отношение сигнал/шум на входе разведывательного приемника q будет равно

$$q = \frac{P_{\text{и}}}{N_{\text{ш}}}, \tag{2}$$

где $P_{\text{и}}$ – мощность одиночного импульса на входе разведывательного приемника, Вт; $N_{\text{ш}}$ – мощность шума, приведенная ко входу разведывательного приемника в полосе пропускания ΔF, Вт.

Мощность шума, приведенная к входу разведывательного приемника, будет определяться как собственными шумами приемника, так и шумами антенны

$$N_{\text{ш}} = \sqrt{N_{\text{ш.п}}^2 + N_{\text{ш.а}}^2}, \tag{3}$$

где $N_{\text{ш.п}} = \int\limits_{\Delta F} N_{\text{ш.п}}(f) df$ – мощность собственных шумов приемника в полосе пропускания ΔF; $N_{\text{о.п}}(f)$ – спектральная плотность мощности собственных шумов приемника; $N_{\text{ш.а}} = \int\limits_{\Delta F} N_{\text{ш.а}}(f) df$ – мощность шумов антенны, приведенная ко входу разведывательного приемника в полосе пропускания ΔF; $N_{\text{ш.а}}(f)$ – спектральная плотность мощности шумов антенны, приведенная ко входу разведывательного приемника.

Из-за большого количества случайных факторов рассчитать мощность ПЭМИ не представляется возможным. Поэтому оценку возможностей по перехвату ПЭМИ для каждой ПЭВМ проводят инструментально-расчетным методом, предполагающим изменение уровней напряженности поля ПЭМИ на расстоянии d = 1 м и измерение или расчет затухания сигнала на трассе «ПЭВМ – средство разведки» (рис. 1).

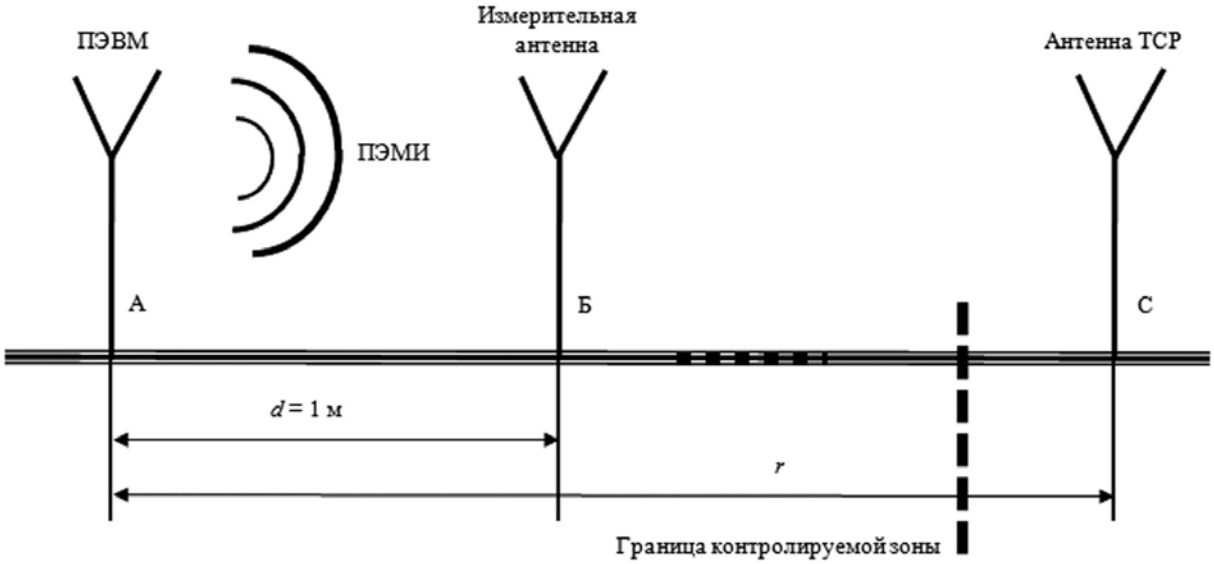


Рис. 1. Схема расчетно-инструментального метода оценки защищенности ПЭВМ от утечки информации, возникающей за счет ПЭМИ

Учитывая, что при выводе на экран монитора реального изображения побочные электромагнитные излучения видеосистемы ПЭВМ анализатором спектра не обнаруживаются, измерения рекомендуется проводить при выводе на экран монитора тестового сигнала «точка – через точку», представляющего собой чередование «белых» и «черных» пикселей.

При таком виде тестового изображения спектр ПЭМИ носит дискретный характер, уровень излучаемых ПЭМИ максимален.

Например, проведенные исследования ПЭМИ ПЭВМ с интегрированной видеокартой Intel (R) HD Graphis Family с интерфейсом VGA [4] показали, что для теста «точка – через точку» для разрешения монитора 1280×1024×60:

– спектральные составляющие ПЭМИ видеосистемы ПЭВМ выявлены в диапазоне частот от 54 до 2322 МГц (вплоть до 43-й гармоники);

– частота первой гармоники ПЭМИ составляет: $F_{\text{с}} = F_{\text{п}}/2 \approx 54$ МГц, где $F_{\text{п}}$ – частота обновления яркости (цвета) каждого пикселя;

– длительность импульсов цветности $\tau \approx 8{,}95$ нс ($\tau \approx 0{,}97/ F_{\text{п}}$), а и их период следования $T \approx 18{,}6$ нс (т.е. $Q = T/\tau \approx 2$).

Учитывая, что наиболее вероятно роль случайных антенн при излучении ПЭМИ выполняют проводники, соединяющие выход цифроаналогового преобразователя видеоадаптера с разъемом VGA, и кабель, соединяющий системный блок с монитором, будем полагать, что в излучении ПЭМИ доминирует электрическая составляющая электромагнитного поля $E_{\text{с}}$.

Уровни напряженности поля информативных сигналов ПЭМИ измеряются на всех обнаруженных частотах f_i в режиме среднеквадратичного детектора (RMS) при включенном и выключенном тесте.

С учетом погрешностей измерений максимально возможный уровень напряженности поля информативного сигнала ПЭМИ за период измерений рассчитывается по формуле

$$E_{\text{с}.i} = \sqrt{(\varepsilon_{\text{и}} E_{\text{и}.i})^2 - (E_{\text{п}.i}/\varepsilon_{\text{и}})^2}\ , \qquad (4)$$

где $E_{\text{с}.i}$ – максимально возможный уровень напряженности поля информативного сигнала ПЭМИ за период измерений на i-й частоте, мкВ/м; $E_{\text{и}.i}$ – измеренное значение напряженности поля информативного сигнала ПЭМИ на i-й частоте при включенном тесте, мкВ/м; $E_{\text{п}.i}$ – измеренное

значение напряженности поля на i-й частоте при выключенном тесте, мкВ/м; $\varepsilon_{\text{и}} = 1 + \sqrt{\left(10^{0{,}05\cdot\varepsilon_a} - 1\right)^2 + \left(10^{0{,}05\cdot\varepsilon_{\text{ип}}} - 1\right)^2}$ – среднеквадратическая погрешность измерительного тракта; ε_a – среднеквадратическая ошибка калибровки измерительной антенны, дБ; $\varepsilon_{\text{ип}}$ – среднеквадратическая ошибка измерения амплитуды сигнала измерительным приемником, дБ.

Измерив напряженность электромагнитного поля информативных составляющих ПЭМИ $E_{c.i}$ и полагая, что полоса пропускания входного фильтра $\Delta F = 1/\tau$, отношение сигнал/шум на входе разведывательного приемника для каждого частотного диапазона, в котором обнаружены информативные составляющие ПЭМИ, можно рассчитать по формуле

$$q_j = \frac{Q\cdot U_{\text{с}.j}^2/Z}{\sqrt{N_{\text{ш.п}.j}^2 + N_{\text{ш.а}.j}^2}} \approx \frac{2\cdot\sum\limits_{\Delta F_j}\left(\dfrac{E_{\text{с}.i}}{K_{\text{а}.i}\cdot V_{r.i}}\right)^2}{Z\cdot\sqrt{\left(\sum\limits_{m=1}^{M_j} N_{\text{о}.j.m}(f)\cdot\Delta F_{\text{и}}\right)^2 + \left(\sum\limits_{m=1}^{M_j}\dfrac{\left(E_{\text{ш.а}.j.m}(f)/K_{a.j.m}(f)\right)^2}{Z}\cdot\Delta F_{\text{и}}\right)^2}}, \qquad (5)$$

где $E_{\text{с}.i}$ – напряженность электрической составляющей электромагнитного поля i-й спектральной составляющей, входящей в состав j-го частотного интервала, В/м; $K_{\text{а}}(f)$ – спектральный калибровочный коэффициент антенны средства разведки, 1/м; $K_{\text{а}.i}$ – значение калибровочного коэффициента антенны средства разведки на i-й частоте, 1/м; $V_{r.i}$ – коэффициент ослабления сигнала на i-й частоте на трассе «ПЭВМ – средство разведки»; ΔF_j – j-й частотный интервал; $E_{\text{ш.а}.n}(f)$ – спектральная чувствительность антенны, измеренная на m-й частоте, входящей в состав j-го частотного интервала, при отношении сигнал/шум $q = 1$, $\text{В}/(\text{м}\cdot\sqrt{\text{Гц}})$; $N_{\text{о}.n}(f)$ – спектральная плотность мощности собственных шумов приемного устройства, измеренная на m-й частоте, входящей в состав j-го частотного интервала, $\text{В}/(\text{м}\cdot\sqrt{\text{Гц}})$; $\Delta F_{\text{и}}$ – ширина полосы пропускания измерительного приемника при измерении $E_{\text{с}.i}$, Гц; $M_j \approx \Delta F_j/\Delta F_{\text{и}}$; $Q = T/\tau$ – скважность тестового сигнала (при тесте «точка – через точку» $Q \approx 2$); T – период следования пиксельных импульсов, с; τ – длительность пиксельных импульсов, с; Z – входное сопротивление приемного устройства, Ом.

Расчет значений граничных частот частотных интервалов ΔF_j осуществляется по формулам

$$\Delta F_j = f_{\text{в}.j} - f_{\text{н}.j} = \Delta F; \quad f_{\text{н}j} = \frac{10^{-6}(j-1))}{\tau}; \quad f_{\text{в}j} = \frac{10^{-6}\cdot j}{\tau}, \qquad (6)$$

где $f_{\text{н}j}$ – нижняя частота j-го частотного интервала, МГц; $f_{\text{в}j}$ – верхняя частота j-го частотного интервала, МГц; τ – длительность импульсов передачи оттенка цвета в тестовом режиме, с.

Полагая, что шумы антенны значительно выше собственных шумов приемного устройства средства разведки, формулу (5) запишем в виде

$$q_j \approx \frac{2\cdot\sum\limits_{\Delta F_j}\left(\dfrac{E_{\text{с}.i}}{K_{\text{а}.i}\cdot V_{r.i}}\right)^2}{Z\cdot\sum\limits_{m=1}^{M_j}\dfrac{\left(E_{\text{ш.а}.j.m}(f)/K_{\text{а}.j.m}(f)\right)^2}{Z}\cdot\Delta F_{\text{и}}} \approx \frac{2\cdot n_j}{\Delta F_j}\cdot\sum_{\Delta F_j}\left(\frac{E_{c.i}}{E_{\text{ш.а}.i}\cdot V_{r.i}}\right)^2, \qquad (7)$$

где $E_{\text{с}.i}$ – напряженность электрической составляющей электромагнитного поля i-й спектральной составляющей, входящей в состав j-го частотного интервала, мкВ/м; $V_{r.i}$ – коэффициент ослабления сигнала на i-й частоте на трассе «ПЭВМ – средство разведки»; $E_{\text{ш.а}.i}$ – спектральная чувствительность антенны на i-й частоте, измеренная при отношении сигнал/шум $q = 1$ и $\Delta F = 1$ Гц, $\text{мкВ}/(\text{м}\cdot\sqrt{\text{Гц}})$; ΔF_j – j-й частотный интервал, Гц; n_j – количество измеренных спектральных составляющих, попадающих в j-й частотный интервал.

При измерении уровней напряженности поля сигналов ПЭМИ в зависимости от длины волны измерительная антенна может оказаться в ближней, средней или дальней зонах. Ближняя зона ограничена расстоянием от излучателя $r \le \lambda/2\pi$. Дальняя зона начинается с расстояния $r > (3...10)\lambda$. Будем полагать, что границей дальней зоны является расстояние $r = 6\lambda$.

В ближней зоне электрическая составляющая электромагнитного поля E_c убывает обратно пропорционально кубу расстояния (~ $1/r^3$), а дальней – обратно пропорционально расстоянию (~ $1/r$). Предположим, что в средней зоне электрическая составляющая электромагнитного поля E_c убывает обратно пропорционально квадрату расстояния (~ $1/r^2$).

Тогда затухание на трассе «ПЭВМ – средство разведки» V_r (безразмерная величина) можно рассчитать по формулам [5]:

А. Для частоты сигнала ПЭМИ ниже $f \le 47{,}75$ МГц

$$V_r \approx \begin{cases} r^3 \quad \text{если} \quad r \le \dfrac{47{,}75}{f}; \\ \dfrac{47{,}75 \cdot r^2}{f} \quad \text{если} \quad \dfrac{47{,}75}{f} < r \le \dfrac{1800}{f}; \\ \dfrac{8{,}59 \cdot 10^4 \cdot r}{f^2} \quad \text{если} \quad r > \dfrac{1800}{f}. \end{cases} \tag{8}$$

Б. Для частоты сигнала ПЭМИ $47{,}75 \text{ МГц} < f \le 1800$ МГц

$$V_r \approx \begin{cases} r^2 \quad \text{если} \quad r \le \dfrac{1800}{f}; \\ \dfrac{1800 \cdot r}{f} \quad \text{если} \quad r > \dfrac{1800}{f}. \end{cases} \tag{9}$$

В. Для частоты сигнала ПЭМИ $f > 1800$ МГц

$$V_r \approx r, \tag{10}$$

где f – частота измеренного сигнала, МГц; r – расстояние от ПЭВМ до средства разведки, м.

Выбор нормативного (порогового) значения вероятности правильного обнаружения сигнала целесообразно осуществлять с точки зрения минимизации вероятности полной ошибки $P_{\text{ош}}$.

Проведенный анализ показал, что при априорной вероятности появления сигнала $P^* = 0{,}5$ значения вероятностей полной ошибки $P_{\text{ош}}$ значительно превышают значения вероятностей правильного обнаружения сигнала $P_{\text{о}}$ ($P_{\text{ош}} >> P_{\text{о}}$) при $P_{\text{о}} < 0{,}05$, становятся соизмеримы с ними ($P_{\text{ош}} \approx P_o$) при $P_{\text{о}} \approx 0{,}33 \cdot (1 + P_{\text{лт}})$ и становятся значительно их меньше ($P_{\text{ош}} << P_{\text{о}}$) при $P_{\text{о}} > 0{,}83 \cdot (1 + P_{\text{лт}})$ [6].

Случай, когда вероятность ошибки соизмерима с вероятностью правильного обнаружения сигнала, является случаем наибольшей неопределённости при принятии решения о наличии или отсутствии сигнала. Поэтому в качестве порогового значения *при решении задачи обнаружения сигнала* целесообразно принять значение вероятности правильного обнаружения $P_n \approx 0{,}3$.

Задаваясь пороговыми значениями вероятности правильного обнаружения сигнала P_n и вероятности ложной тревоги $P_{\text{лт}}$ из формулы (1) легко получить предельно допустимое (пороговое) значение энергетического отношения сигнал/шум на входе приёмного устройства средства разведки δ

$$\delta \approx \frac{\Phi^{-1}(P_n) + \Phi^{-1}(1 - P_{\text{лт}})}{\sqrt{N}}. \tag{11}$$

Например, для вероятностей $P_n = 0{,}3$ и $P_{\text{лт}} = 10^{-3}$ пороговое значение отношения сигнал/шум на входе приёмного устройства средства разведки будет равно $\delta \approx 2{,}68/\sqrt{N} = 2{,}68/\sqrt{F_{\text{к}} \cdot T_{\text{а}}}$.

Пространство вокруг ПЭВМ, в пределах которого отношение сигнал/шум q на входе разведывательного приемника превышает пороговое значение δ ($q \ge \delta$), называется *опасной зоной* 2 ($R2$). Следовательно, перехват ПЭМИ ПЭВМ возможен при выполнении двух условий (рис. 2 [6]):

– первое – расстояние от ПЭВМ до границы контролируемой зоны должно быть менее зоны $R2$ ($R_{\text{кз}} \le R2$);

– второе – в пределах зоны $R2$ возможно размещение средств разведки ПЭМИН.

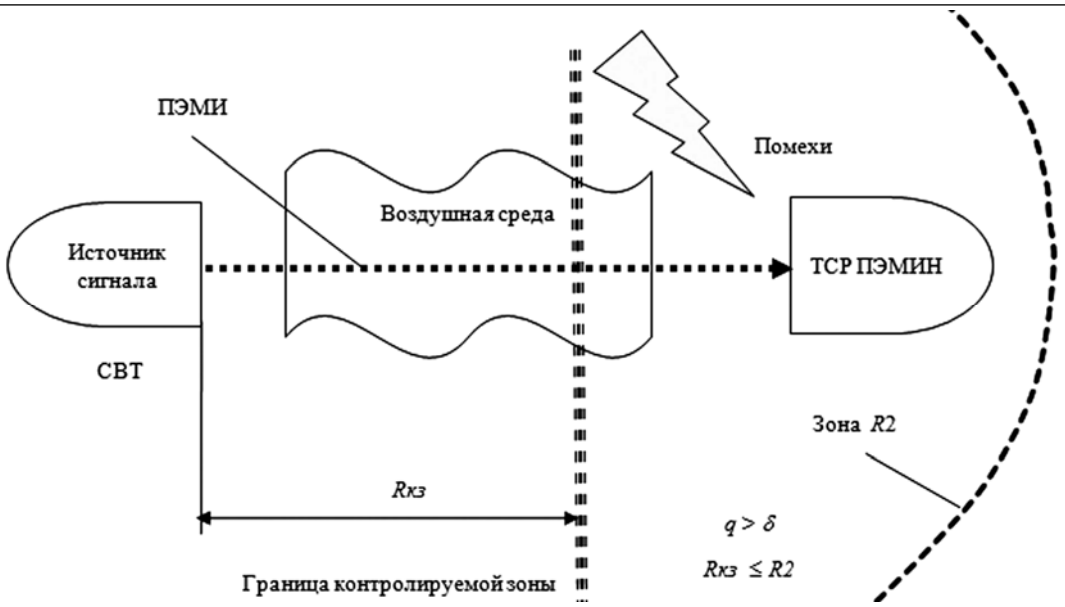


Рис. 2. Схема перехвата побочных электромагнитных излучений ПЭВМ (электромагнитный технический канал утечки информации)

Обычно зону $R2$ рассчитывают применительно к стационарным, перевозимым и переносимым средствам разведки.

Расчет зоны $R2$ проводится в следующей последовательности.

Начиная с расстояния $r = 1$ м с шагом 1 или 5 м по формуле (5) или (7) рассчитывается отношение сигнал/шум q_j для каждого частотного диапазона, в котором обнаружены информативные составляющие ПЭМИ. Полученные значения q_j сравниваются с рассчитанным по формуле (11) пороговым отношением сигнал/шум δ. За значение зоны $R2$, м, принимается то минимальное расстояние r, при котором для всех частотных диапазонов выполняется условие $q_j \le \delta$, т.е. $R2 = \min\{r\} | q_j \le \delta$.

Таким образом, предложенная математическая модель обнаружения побочных электромагнитных излучений видеосистемы компьютера оптимальным приемником позволяет оценить возможность перехвата ПЭМИ ПЭВМ средствами разведки и обосновать целесообразность использования на объектах информатизации тех или иных технических средств защиты информации.

Литература

1. Wim van Eck. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? [Электронный ресурс]. – Режим доступа: http://cryptome.org/emr.pdf, свободный (дата обращения: 03.12.2013 г.).

2. Kuhn G. Compromising emanations: eavesdropping risks of computer displays: This technical report is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the University of Cambridge, Wolfson College. [Электронный ресурс]. – Режим доступа: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf, свободный (дата обращения: 03.12.2013 г.).

3. Теоретические основы радиолокации: учеб. пособие для вузов. – 2-е изд., перераб. и доп. / А.А. Коростылев, Н.Ф. Клюев, Ю.А. Мельник и др. / Под ред. В.Е. Дулевича. – М.: Сов. радио, 1978. – 608 с.

4. Исследование побочных электромагнитных излучений видеосистем средств вычислительной техники. Шифр «107-ИПП-ИБ»: отчет о НИР «заключ.» / МИЭТ; рук. А.А. Хорев – М., 2013. – 167 с.

5. Хорев А.А. Оценка возможности по перехвату побочных электромагнитных излучений видеосистемы компьютера. Ч. 2 // Специальная техника. – 2011. – № 4. – С. 51–62.

6. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов: в 3 т. – Т. 1: Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

Хорев Анатолий Анатольевич
Д-р техн. наук, профессор, зав. каф. «Информационная безопасность»
Национального исследовательского университета «МИЭТ», Москва
Тел.: 8-916-500-01-64
Эл. почта: horev@miee.ru

Horev A.A.
Evaluation of the possibility of detection side compromising electromagnetic emanations video PC

One of the most dangerous channels of the leakage of information with restricted access, on-cultivated PC channel is the leakage arising from side within the compromising electromagnetic emanations video PC. In the article development of a mathematical model for discovering compromising electromagnetic emanations video PC optimal receiver and instrumental calculation method for evaluation of power interception compromising electromagnetic emanations means of intelligence. Developed the mathematical model takes into account the possibility of improving the signal to noise due to digital signal processing with the interception of multiple «frames» image.
Keywords: video system, compromising electromagnetic emanations, technical channel of information leakage, the interception of information.

УДК 004.491.22

М.Е. Бурлаков

Модель многослойной универсальной системы обнаружения вторжений

Проектируется модель универсальной системы обнаружения вторжений. Вводятся требования по проектированию базы данных универсальной системы обнаружения вторжений, а также определяется общий принцип работы в многоступенчатых информационных системах и описывается процесс безотрывного обучения и тренировки. Обосновывается актуальность и новизна созданной модели.

Ключевые слова: универсальная система обнаружения вторжений; многоступенчатые информационные системы.

Под системой обнаружения вторжений (СОВ) понимается программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную / информационную систему или сеть либо несанкционированного управления ими злоумышленником. СОВ включает в себя: сенсорную подсистему, подсистему анализа, хранилище и консоль управления.

Как следует из определения, СОВ – это пассивная система. Существует множество классификаций СОВ в зависимости от области и вариантов применения в информационных системах [1]. Например, существует классификация в зависимости от использования на том или ином уровне сетевой модели *OSI* [2], на основании этого выделяют следующие типы СОВ:

1) сетевые. Например, *Snort* [3]. Уровень *OSI*: транспортный и сеансовый;

2) основанные на протоколе. Например, модуль *Nginx*. Уровень *OSI*: представление;

3) основанные на прикладных протоколах. Например, компилятор *MySQL*. Уровень *OSI*: прикладной;

4) узловые. Например, *OSSEC*. Уровень *OSI*: транспортный и сетевой;

5) гибридные. Например, *Prelude*. Уровень *OSI*: транспортный, сетевой и сеансовый.

Существенным недостатком всех современных систем обнаружения вторжений является либо их строгая направленность на решение задач в конкретном уровне сетевой модели, либо небольшая вариативность в плане работы с несколькими уровнями передачи информации [4]. Под уровнем передачи информации (УПИ) будем понимать программно-аппаратный блок, принимающий и впоследствии передающий данные другим(ому) блокам(у). В настоящее время отличительной особенностью УПИ является отсутствие универсальной программно-аппаратной реализации обнаружения вторжений в информационных системах.

В данной работе предлагается теоретическая модель универсальной системы обнаружения вторжений, которая может быть подключена к любому типу УПИ. Под универсальностью понимается единая структура СОВ, единая методика обработки данных вне зависимости от выбранного уровня передачи информации.

Теоретическая модель универсальной системы обнаружения вторжений. Основополагающим элементом универсальной системы обнаружения вторжений является база данных (БД). В предлагаемой модели с целью обеспечения проектируемой универсальности БД должна состоять из следующего набора элементов:

1. Блок хранения единого реестра срабатываний (ЕРС). ЕРС хранит в себе информацию обо всех угрозах, на которые сработали все СОВ в рамках информационной системы. Структура хранения данных в ЕРС имеет вид «Набор угроз» – «СОВ*i*», где «Набор угроз» – множество найденных угроз, СОВ*i* – *i*-я система обнаружения вторжений, перехватившая угрозу. Для дальнейшего анализа получаемых данных в предлагаемой системе ЕРС должны содержаться следующие типы сортировок:

а) сортировка по дате занесения записи, позволяющая отслеживать интенсивность детектирования угроз, поступающих на все УПИ;

б) сортировка по СОВ*i*, отслеживающая количество угроз на конкретный УПИ;

в) сортировки, определяемые оператором в зависимости от решаемой задачи.

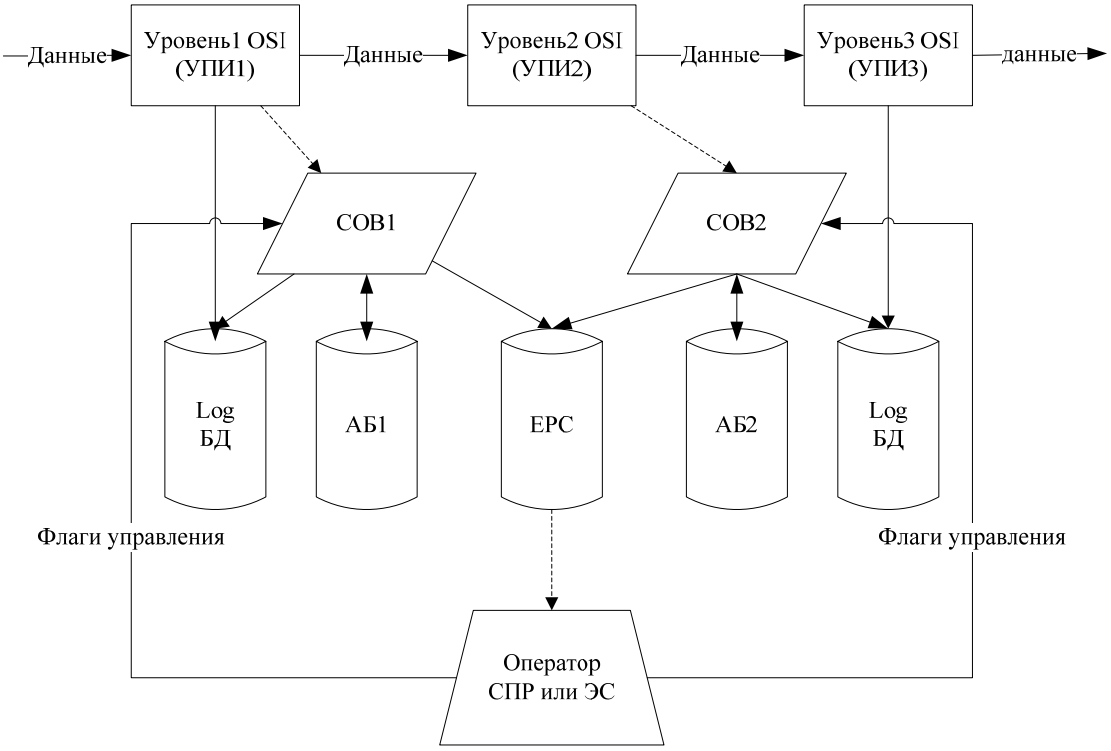
2. Блоки актуальных библиотек (АБ) по УПИ. Для каждого УПИ предполагается наличие своей библиотеки с хранимыми векторами угроз.

3. Блоки инициализационных библиотек (ИБ). Инициализационные библиотеки предполагают наличие первоначальных данных для начала работы СОВ, а также для обеспечения корректного процесса ее обучения. В предлагаемой модели ИБ – полный аналог АБ по структуре строения.

4. Блоки тренировки (ТБ). Создаются после инициализации на стороне СОВ процесса тренировки. Вся структура создания ТБ описывается в инициализационном файле (ИФ), который формируется оператором либо сторонней системой.

5. Блок логирования (*Log* блок). Данный блок отвечает за сбор потока данных. *Log* блок может как накапливать информацию, присланную с УПИ, так и информацию уже обработанную СОВ. В первом случае структура хранения данных в этом блоке эквивалентна структуре передаваемых данных в СОВ. *Log* блок может формироваться как самой СОВ, так и УПИ. Для разных систем может быть создана единая *Log* БД вида «*Log* БД УПИ» – «Тип УПИ». Наличие *Log* блока не является обязательным для УПИ.

Общая структурная модель предлагаемой универсальной системы обнаружения вторжений представлена на рис. 1. Пунктирная линия от УПИ к СОВ подразумевает возможность исключения СОВ из процесса передачи данных.



СПР – система принятия решений, ЭС – экспертная система

Рис. 1. Модель работы универсальной системы обнаружения вторжений

Рассмотрим работу предлагаемой универсальной системы обнаружения вторжений пошагово.

1. Данные поступают в уровень *OSI* (УПИ1).

2. Далее информация передается на следующий уровень УПИ2. Параллельно данные передаются в блок СОВ (СОВ1), и осуществляется запись данных в *Log* блок средствами УПИ, в случае если это предусмотрено конфигурацией работы системы.

3. Используя блок АБ (на рис. АБ1 или АБ2), СОВ принимает решение о легитимности или нелегитимности принятых данных. В случае если данные не легитимны (угроза), происходит запись в единый реестр срабатываний, который в свою очередь анализируется оператором или сторонней системой. В качестве активной сторонней системы может быть рассмотрена экспертная система (ЭС) или система принятия решений (СПР).

4. Оператор может влиять на СОВ через флаги управления. В предлагаемой модели флаги управления СОВ включают в себя:

а) флаг включения/выключения. Данный флаг позволяет включать или выключать СОВ между УПИ при анализе потока данных в информационной системе;

б) флаг обучения и тренировки. Флаг позволяет активировать режим обучения и тренировки. При активации данного режима система использует определенный конфигурационный файл (КФ), позволяющий автоматически формировать среду обучения и тренировки. Данные для последующего обучения и тренировки берутся из *Log* блока. Также создаются инициализационные и тренировочные блоки (запись данных), а единый реестр срабатываний используется только для чтения с целью дальнейшего анализа эффективности СОВ. Обучение и тренировка СОВ также описываются КФ, созданным оператором, либо сторонней системой.

Режим обучения и тренировки универсальной системы обнаружения вторжений. Для начала корректной работы СОВ необходимы ее предварительное обучение и тренировка. Введем ряд определений элементов обучения и тренировки:

БД конфигураций – база данных конфигураций с типом хранения вида «конфигурация» – «СОВ», позволяющая сохранять конфигурацию СОВ в определенный момент времени. В рамках процесса обучения и тренировки СОВ используется оператором либо другой системой с целью дальнейшего анализа наиболее оптимальных конфигураций СОВ.

Загрузчик конфигураций (ЗК) – программно-аппаратное решение, обеспечивающее подготовку конфигураций для СОВ с последующим ее обновлением. Загрузчик конфигураций обладает функцией считывания текущей конфигурации СОВ с возможностью последующего ее сохранения в БД конфигураций.

Конфигурационный файл (КФ) – файл с определенной структурой, с помощью которого производится управление выбранной СОВ. Под управлением СОВ понимается либо определение и инициализация режима обучения и тренировки, либо текущая настройка его работы.

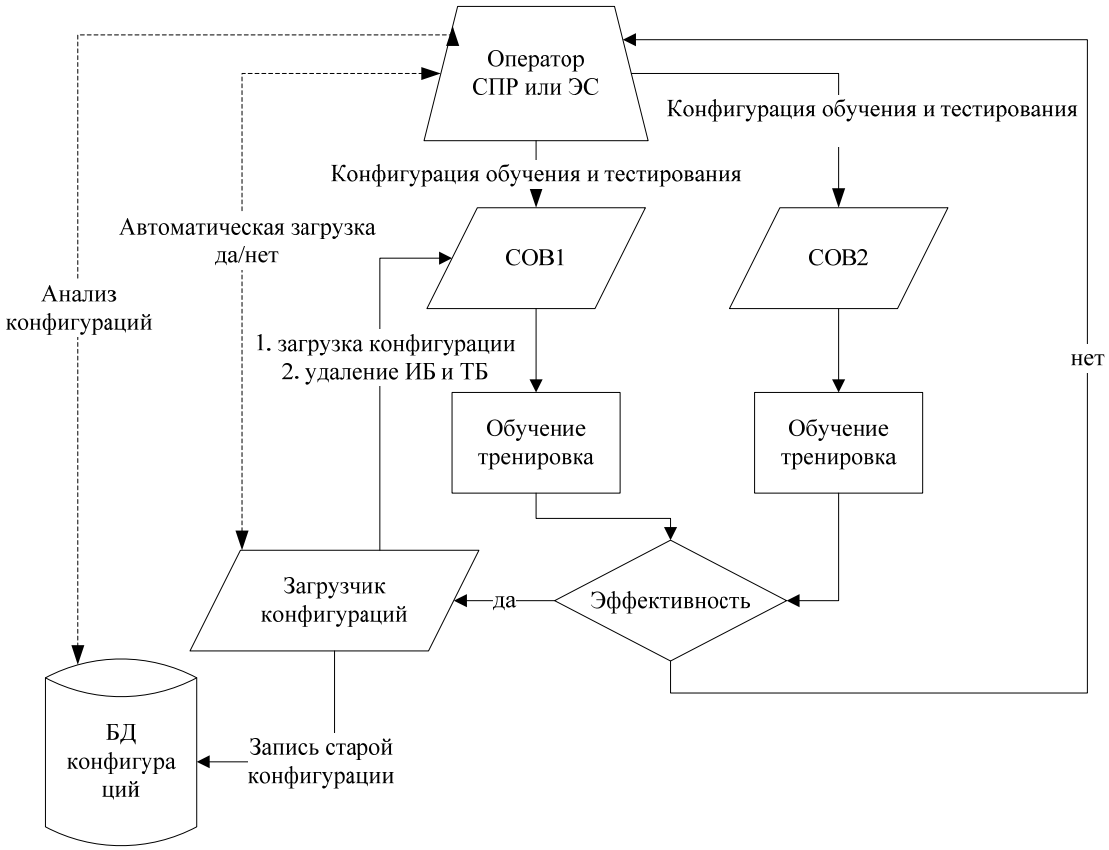


Рис. 2. Упрощенная структурная модель обучения и тренировки функционирующей СОВ

Структурная схема обучения и тренировки двух СОВ в рамках работающих УПИ представлена на рис. 2. На рис. 2 представлен только участок информационной системы с конечным числом блоков УПИ и соответствующим им СОВ. В общем случае количество блоков СОВ в рамках ИС не регламентируется.

Рассмотрим процесс обучения и тренировки системы обнаружения вторжений пошагово.

1) включение флага тренировки;

2) загрузка конфигурационного файла обучения и тренировки в СОВ и создание инициализационного и тестового блоков;

3) обучение и тренировка;

4) определение меры эффективности:

а) «Эффективно». Новые параметры отправляются в загрузчик конфигураций. Параллельно в базе данных конфигураций сохраняется старая конфигурация СОВ. Загрузчик конфигураций в зависимости от определенных настроек либо оператором, либо автоматически загружает новые параметры в рабочую версию СОВ;

б) «Не эффективно». Отчет отправляется либо оператору, либо в другую систему для последующего анализа.

В предложенной модели конфигурационный файл процесса обучения и тренировки универсальной системы обнаружения вторжений имеет следующие параметры: параметр настройки формирования инициализационного блока (ИБ) на основе блока актуальных библиотек (АБ), параметр настройки формирования тестового блока (ТБ) и параметр работы процесса обучения и тренировки СОВ с использованием единого реестра срабатываний и *Log* блока.

Детальный процесс обучения для системы обнаружения вторжений представлен на рис. 3.

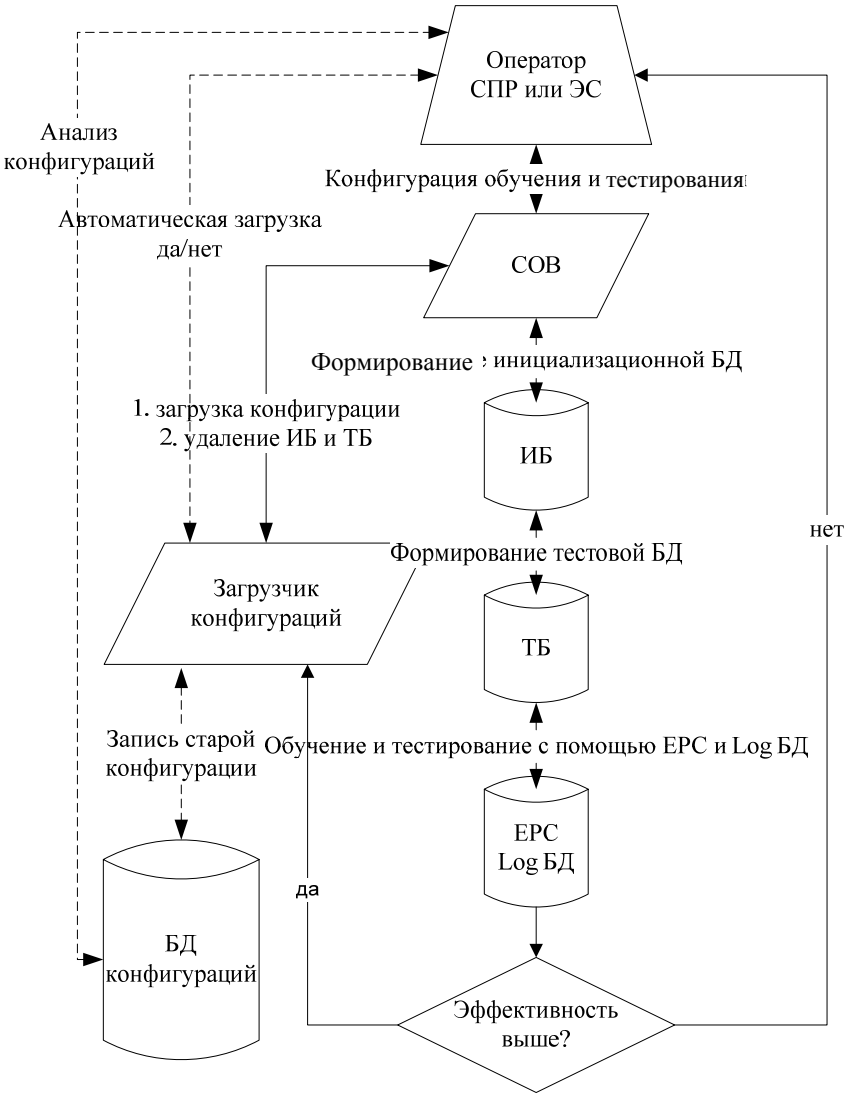


Рис. 3. Подробная модель обучения и тренировки универсальной СОВ

Рисунок 3 отличается от рис. 2 в части детального описания процесса обучения и тестирования, которые состоят из следующих шагов:

1) включение флага тренировки;

2) формирование инициализационного блока (ИБ);

3) формирование тестового блока (ТБ);

4) обучение и тестирование СОВ с использованием единого реестра срабатываний и Log базы данных;

5) оценка эффективности работы.

В результате представленных выше пошаговых алгоритмов, реализована теоретическая модель универсальной системы обнаружения вторжений, включающая в себя процессы обучения и тренировки. Предложенная модель позволяет универсализировать использование системы обнаружения вторжений в разных типах УПИ в отличие от известных моделей, которые подразумевают выполнение конкретных задач.

Заключение. В данной статье была предложена теоретическая модель универсальной системы обнаружения вторжений. К основным плюсам описанной системы можно отнести:

Динамичность и актуальность. За счет наличия единого реестра срабатываний и процесса безотрывного обучения и тренировки СОВ обеспечиваются актуальность данных и ее постоянная адаптация к текущей среде передачи информации.

Независимость. За счет наличие флага управления «включение/выключение» СОВ и параллельности обработки данных с УПИ предложенная модель обеспечивает независимость и параллельность к информационной системе.

Унификация. Обеспечивается за счет универсальности хранения (баз данных) и обработки информационных потоков СОВ.

К потенциальному недостатку можно отнести возможную большую нагрузку на блок реализации СОВ. Недостаток может быть исключен путем внедрения процесса распараллеливания комплекса СОВ на многопроцессорных информационных системах.

Литература

1. Бурлаков М.Е. Аудит безопасности локальной вычислительной сети с помощью динамической системы на нейронах с реакцией на последовательности / М.Е. Бурлаков, М.Н. Осипов // Матер. XIII Междунар. науч.-практ. конф. «ИБ-2013». – Таганрог: Изд-во ЮФУ, 2013. – Ч. 1. – С. 85–91.

2. ГОСТ Р ИСО/МЭК 7498-1–99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Введ. 1999-03-18. – М.: Гостстандарт, 2006. – 62 с.

3. Everett F. Snort IDS and IPS Toolkit / F. Everett, C. James, M. Jonkman. – Kohlenberg: Syngress, 2007. – 41 p.

4. Бурлаков М.Е. Метод фильтрации входящего трафика на основе двухслойной рекуррентной нейронной сети // Ползуновский вестник. – 2012. – № 3/2. – С. 215–219.

Бурлаков Михаил Евгеньевич
Аспирант каф. безопасности информационных систем Самарского государственного университета
Тел.: 8-929-703-33-38
Эл. почта: knownwhat@gmail.com

Burlakov M.E.

The common model of intrusion detection system

A common model of intrusion detection system (IDS) is described in the article. There are requirements for designing a database of IDS, as well as the general principle of operations are determined in multi-information systems and there is description of the process of education and training IDS. The usefulness of model is justified.

Keywords: universal intrusion detection system, multi-information systems.

УДК 004.93

Т.Ю. Дорошенко, Е.Ю. Костюченко

Система аутентификации на основе динамики рукописной подписи

Реализованы программное обеспечение и база данных для проведения исследования идентификации пользователя по рукописной подписи, проставляемой при помощи графического планшета. Собрана база подписей для проведения исследования. Сформированы и выделены параметры для проведения аутентификации. Полученные результаты позволяют осуществить реализацию системы для идентификации пользователя по подписи на основе комбинированного подхода, использующего аппараты математической статистики и искусственных нейронных сетей.

Ключевые слова: аутентификация пользователей, динамическая рукописная подпись, графический планшет.

Постановка задачи. Среди систем аутентификации большими перспективами в настоящее время обладают биометрические системы, основанные на поведенческой (динамической) характеристике человека и учитывающие особенности, характерные для подсознательных движений человека в процессе воспроизведения какого-либо действия. К таким методам относится аутентификация по рукописному/клавиатурному почерку, голосу и др. В этом случае дорогостоящее оборудование не является неотъемлемой частью системы, невозможен обход системы за счет изготовления муляжей, а сам способ привычен для человека и не вызывает отторжения. Принципиально важным преимуществом динамических биометрических систем контроля доступа является возможность для личности сохранять в тайне свой биометрический образ (парольную фразу), что на 4–6 десятичных порядков повышает степень защиты, предоставляемой динамическими БСКД относительно статических [1–3].

Разрабатываемое программное обеспечение представляет собой прототип системы аутентификации компьютерной системы по динамике подписи пользователя на графическом планшете. Цель работы – повышение надежности традиционной парольной защиты за счет использования многофакторной аутентификации на основе анализа динамики проставления подписи, проводимого с использованием аппаратов математической статистики и искусственных нейронных сетей.

Основой аутентификации личности по почерку и динамике написания контрольных фраз (подписи) являются уникальность и стабильность динамики этого процесса для каждого человека, характеристики которой могут быть измерены, переведены в цифровой вид и подвергнуты компьютерной обработке. Таким образом, при аутентификации для сравнения выбирается не продукт письма, а сам процесс.

Биометрическую аутентификацию по подписи можно разделить на следующие этапы:

– предъявление пользователем биометрического образа – ввод пароля (подписи) на графическом планшете;

– оцифровка входных электрических сигналов – измерение заданных биометрических параметров в предъявленном образе;

– нормализация входных сигналов, приводящая их к некоторому эталонному значению;

– сохранение в базе данных системы биометрического эталона идентифицируемой личности – построение шаблона (или профиля) пользователя;

– обучение системы;

– сравнение предъявляемого пользователем профиля с сохраненными;

– предсказание уровня ошибок первого и второго рода для полученного биометрического профиля, принятие решения.

Программное обеспечение для съема образа подписи. Важным этапом решения задачи подтверждения подлинности динамической подписи являются получение, анализ и хранение динамических характеристик (первичных параметров) подписей, проставляемых на графическом планшете. В связи с этим создан программный модуль для съема образа подписи.

Основные задачи, решаемые модулем:

– фиксация перемещений пера относительно чувствительной зоны планшета и перехват потока входных данных;

– динамическая отрисовка подписи на специальной панели в режиме реального времени;

– нормализация первичных параметров подписи;

– сохранение нормализованных первичных параметров подписи в базе данных.

Для обеспечения корректного функционирования системы съема подписи с множеством графических планшетов, представленных на рынке, а также для получения всех данных, которые позволяет снимать аппаратное обеспечение, использован стандартизированный программный интерфейс для графических планшетов, датчиков трехмерного положения и других указывающих устройств в Windows – WinTab.

Алгоритм снятия подписи:

1) при вызове функции подписи – открытие контекста устройства ввода, передающего данные в цифровой форме непосредственно к приложению, без подготовки курсора;

2) каждый раз при возникновении события «Приход пакета» (каждые 5 мс, если перо находится в области действия планшета) вызвать обработчик событий, выполнить пункты 3–8;

3) получение серийного номера пакета, вызвавшего событие;

4) получение пакета с серийным номером пакета, вызвавшего событие;

5) нормализация данных пакета;

6) сохранение пакета в массив WintabPacket;

7) изображение точки на специальной панели;

8) при вызове функции сохранения подписи – закрытие контекста устройства ввода, увеличение счетчика массива.

По серийному номеру пакета извлекаются требуемые показатели: координаты положения пера, сила давления пера на поверхность планшета, угол пера по часовой стрелке и угол наклона пера относительно поверхности графического планшета, время снятия показателей.

Анализ снятых первичных характеристик показал, что в некоторых пакетах некорректно устанавливается штамп времени. Об этой же погрешности говорится и в статье П.С. Ложникова, А.В. Еременко [4]. Рассмотрим суть проблемы на примере используемого дигитайзера WACOM Intuos 3, имеющего частоту дискретизации, равную 200 Гц. Это означает, что когда перо находится в области чувствительности дигитайзера, все поступающие от него пакеты должны иметь штамп времени, кратный 5 мс. Однако в единичных случаях наблюдается отклонение этого значения (в отдельных случаях даже нарушается порядок следования пакетов по штампу времени). При этом можно заметить, что ошибка появляется именно в проставлении штампа – все остальные снимаемые характеристики не имеют скачков. Решено пренебречь данным параметром и при вычислении скоростей на отрезках дискретизации использовать заданную производителем частоту дискретизации, равную 5 мс; для упорядочивания пакетов использовать идентификатор пакета pktID.

Еще одной ошибкой (уже аппаратной части графического планшета) является периодическое одновременное (в одном пакете) проставление значений, больших, чем нуль, для параметров давления и координаты положения кончика пера над планшетом по оси Z. Это буквально бы значило, что перо не касается планшета, но оказывает на него давление, что невозможно.

Также особое внимание уделено искажениям, вызванным невозможностью точного воспроизведения подписи одним человеком. К таким искажениям относятся:

– изменение геометрических размеров подписи;

– нестабильность времени воспроизведения подписи;

– изменение угла наклона подписи относительно системы координат.

Используемые алгоритмы для компенсации изменений описаны в автореферате диссертации [5].

При нормализации подписей перед их сохранением в базу данных решаются следующие задачи:

1) удаление нулевых (по параметру давления) значений пакетов в начале и в конце подписи, что предотвращает хранение «мусора» в базе данных, которое впоследствии может снизить информативность сигналов;

2) исправление ошибки «координата Z – давление»;

3) поворот подписи таким образом, чтобы она располагалась параллельно оси абсцисс;

4) нормализация по размеру.

Интерфейс главного окна программы и внешний вид проставляемой подписи для проведения исследования представлены на рис. 1.

Рис. 1. Интерфейс главного окна программы

Реализованный модуль работает под операционной системой Windows, выполнен с использованием среды разработки Microsoft Visual Studio 2010, языка программирования C# и платформы .NET, MySQL Connector, библиотеки WintabDN. Шаблоны для работы с библиотекой WintabDN взяты с электронного ресурса [6].

Формирование вектора биометрических параметров. Точность работы системы аутентификации зависит от размера пространства первичных и вторичных характеристик подписи. Количество первичных характеристик зависит от возможностей аппаратной составляющей системы и определяется количеством степеней свободы, которое описывает число квазинепрерывных характеристик взаимного положения планшета и пера.

Для формирования вектора биометрических параметров (вторичных характеристик) первичные параметры часто подвергаются преобразованию путем вычисления линейных функционалов по полной реализации подписи или по ее фрагментам. Распространенным методом получения вектора биометрических параметров является вычисление дискретного преобразования Фурье с последующим выделением амплитуд гармоник [9, 10].

Таким образом, для получения вторичных характеристик выполняется следующий алгоритм:

1) удаление постоянной составляющей из спектра;
2) увеличение количества точек для получения гладкой кривой;
3) быстрое преобразование Фурье для спектров каждого из параметров;
4) выделение первых семи гармоник – получение амплитуд и частот для каждой гармоники от каждого первичного параметра;
5) нормализация вторичных характеристик по амплитуде максимальной гармоники;
6) проведение статистического анализа, отсев подписей с грубыми отклонениями от среднего значения более чем на 3σ.

База данных для хранения параметров динамической подписи. Для обеспечения хранения характеристик эталонных подписей в одном месте и возможности удобного доступа к ним выполнено инфологическое проектирование и реализована база данных в СУБД MySQL [7]. База данных размещена на сервере кафедры КИБЭВС (93.91.166.75:3306).

Таблицы базы данных и атрибуты:

– пользователи: идентификатор пользователя (PK), фамилия, имя, отчество, дата рождения;

– подписи: идентификатор подписи (PK), идентификатор пользователя (FK), дата и время проставления подписи (проставляется в момент сохранения подписи по времени на сервере), комментарий;

– пакеты: идентификатор подписи (FK, PK), серийный номер пакета (PK), трехмерные координаты *X*, *Y*, *Z* кончика пера относительно планшета, сила нажатия (давление) пера на планшет, угол наклона пера относительно планшета и угол пера по часовой стрелке, временной штамп;

– нормализованные пакеты: идентификатор подписи (FK, PK), серийный номер пакета (PK), нормализованные трехмерные координаты *X*, *Y*, *Z* кончика пера относительно планшета, сила нажатия (давление) пера на планшет, угол наклона пера относительно планшета и нормализованный угол пера по часовой стрелке;

– названия параметров: идентификатор параметра (PK), имя параметра, описание параметра;

– значения параметров: идентификатор подписи (FK, PK), идентификатор параметра (FK, PK), номер гармоники (PK), значение амплитуды гармоники, значение частоты гармоники.

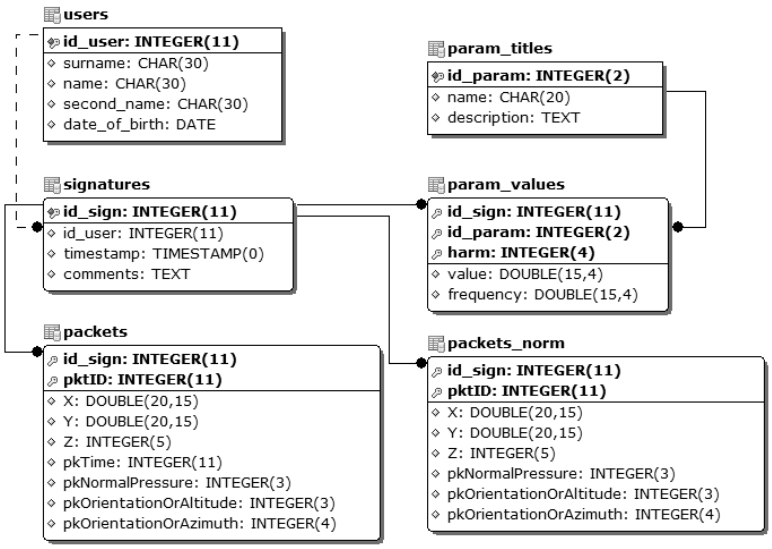


Рис. 2. Концептуальная модель данных

Концептуальная модель данных представлена на рис. 2.

Предоставленные на уровне СУБД права доступа к базе данных: администраторам – полный доступ, пользователям – только INSERT.

Планирование эксперимента. В качестве основных характеристик любой биометрической системы принимают ошибки первого (FAR) и второго (FRR) рода. Первое число характеризует вероятность ложного совпадения биометрических характеристик двух людей, а второе – вероятность отказа доступа человеку, имеющему допуск. Таким образом, встает задача предварительной оценки точности определения ошибок первого и второго рода при идентификации пользователей по динамической подписи.

Из теории вероятностей доверительный интервал для оценки неизвестных вероятностей может быть построен по следующей формуле [8]:

$$p = \frac{n}{t^2 + n}\left(\omega + \frac{t^2}{2n} \pm t\sqrt{\frac{\omega(1-\omega)}{n} + \frac{t^2}{4n^2}}\right). \quad (1)$$

Здесь параметр t определяется уровнем доверительной вероятности на основе функции Лапласа. При уровне доверительной вероятности 0,95 параметр t = 1,96. Кроме того можно воспользоваться методом, изложенным в [12].

Предварительная оценка частоты ошибок первого и второго рода может быть найдена исходя из анализа ошибок аналогов и составляет $\omega_1 = 0{,}01$ для ошибок первого рода и $\omega_2 = 0{,}01$ для ошибок второго рода.

Количество экспериментов по идентификации определяется объемом базы подписей и предварительно составляет 1300 экспериментов по оценке ошибок первого рода и 11700 экспериментов по оценке ошибок второго рода. На настоящий момент в базе содержится 1203 подписи, число ненулевых точек подписи составляет 600–1000.

Подставляя эти данные в формулы, получаем предварительные границы доверительных интервалов для ошибок первого и второго рода: $p_1 \in [0{,}006;\ 0{,}017]$ и $p_2 \in [0{,}008;\ 0{,}012]$. Эти значения позволяют определять вероятность ошибок первого и второго рода с точностью до 0,0055 и 0,002 соответственно. Данный расчет является прикидочным, поскольку самих оцениваемых вероятностей пока нет, однако порядок оценки точности этих значений не изменится.

Заключение. В ходе проделанной работы были получены следующие результаты:

1. Реализован модуль для снятия образа динамической подписи, проставляемой на графическом планшете.
2. Собрана база подписей 12 пользователей суммарным объемом более 1200 подписей.
3. Получены вторичные характеристики для каждой подписи.
4. Получены предварительные оценки, позволяющие спрогнозировать порядок размаха доверительного интервала вероятностей ошибок первого и второго рода при дальнейшем эксперименте, а по сути – точность получаемых оценок вероятностей ошибок.

Следующим этапом исследования является получение оценки информативности параметров для задачи идентификации на основе метода накопленных частот [10], реализованного ранее и адаптированного для возможности идентификации нескольких пользователей, а также с применением подхода оценки информативности параметров при решении задач с использованием искусственных нейронных сетей [11].

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2014 год (проект № 1220).

Литература

1. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: ПГУ, 2000. – 188 с.
2. Брюхомицкий Ю.А. Параметрический метод биометрической аутентификации пользователей информационных систем // Информационное противодействие угрозам терроризма. – 2003. – № 1. – С. 42–48.
3. Костюченко Е.Ю. Идентификация по биометрическим параметрам при использовании аппарата нейронных сетей / Е.Ю. Костюченко, Р.В. Мещеряков // Нейрокомпьютеры: разработка, применение. – 2007. – № 7. – С. 39–50.
4. Ложников П.С. Идентификация личности по рукописным паролям / П.С. Ложников, А.В. Еременко // Мир измерений. – 2009. – № 4 (98). – С. 11–17.
5. Сорокин И. А. Формирование системы признаков для идентификации личности по динамике воспроизведения подписи: автореф. дис. ... канд. техн. наук: 05.13.01. – Пенза, 2005. – 22 с.
6. WintabDN-шаблоны [Электронный ресурс]. – Режим доступа: http://sourceforge.net/projects/wintabdn, свободный (дата обращения: 10.02.2014).
7. Кузнецов М.В. MySQL 5 / М.В. Кузнецов, И.В. Симдянов. – СПб.: БХВ-Петербург, 2006. – 1024 с.
8. Гмурман В.Е. Теория вероятностей и математическая статистика: учеб. пособие для вузов. – М.: Высшая школа, 2004. – 479 с.
9. Ложников П.С. Разработка метода идентификации личности по динамике написания слов: автореф. дис. ... канд. техн. наук: 05.13.01. – Омск, 2004. – 22 с.
10. Еременко А.В. Повышение надежности аутентификации пользователей компьютерных систем по динамике написания пароле: автореф. дис. ... канд. техн. наук: 05.13.19. – Омск, 2011. – 20 с.
11. Костюченко Е.Ю. Критерии информативности при обработке биометрических сигналов при помощи нейронных сетей / Е.Ю. Костюченко, Р.В. Мещеряков, А.Ю. Крайнов // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 118–120.
12. Архипов В.А. Технология поиска при решении задач прикладной математики / В.А. Архипов, С.С. Бондарчук, И.Г. Боровской, А.А. Шелупанов // Вычислительные технологии. – 1995. – Т. 4, № 10. – С. 51–62.

Дорошенко Татьяна Юрьевна
Инженер каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8-923-408-31-47
Эл. почта: tankem@mail.ru

Костюченко Евгений Юрьевич
Канд. техн. наук, доцент каф. КИБЭВС ТУСУРа
Тел.: 8-923-444-42-24
Эл. почта: key@keva.tusur.ru

Doroshenko T.Y., Kostyuchenko E.Y.

The authentication system based on dynamic handwritten signature

Implemented software and database for the research of user identification, based on handwritten signature, stamped with a tablet. Base of signatures collected for a future research. Formed and isolated characteristics for authentication. The obtained results allow produce the implementations of the system for identify the user by their signatures. Process of identification will be based on combination of approaches using mathematical statistics and artificial neural networks.

Keywords: user authentication, dynamic handwritten signature, graphically tablet.

УДК 004.89

А.В. Ахаев, И.А. Ходашинский, А.Е. Анфилофьев

Метод выбора программного продукта на основе интеграла Шоке и империалистического алгоритма

Рассматривается проблема выбора программного продукта по функциональным возможностям. Данную проблему предлагается решать на основе интеграла Шоке, а для извлечения нечеткой меры использовать империалистический алгоритм оптимизации. Предложен вариант выбора программных продуктов по интегральной оценке. Проведен эксперимент.

Ключевые слова: интегральная оценка, программные продукты, интеграл Шоке, империалистический алгоритм.

Повсеместное применение и постоянное совершенствование информационных технологий, наличие большого количества программных продуктов (ПП) на рынке, а также отсутствие у лиц, принимающих решения, технических знаний и опыта для выбора программного обеспечения делают необходимой разработку методов и средств выбора подходящих программных продуктов из множества аналогов. Данная проблема требует нахождения компромисса между техническими характеристиками, функциональными возможностями и финансовыми вопросами и может быть сформулирована как многокритериальная проблема принятия решений.

Наиболее часто применяемым инструментом для оценки качества программного обеспечения является метод анализа иерархий в различных его модификациях. В работе [1] выбор пакета программного обеспечения для имитационного моделирования основан на нечетком методе анализа иерархий; здесь по семи основным критериям проводится оценка шести программных продуктов. Метод анализа иерархий предложено использовать в работе [2] для выбора одной из двух систем *ERP* (*Enterprise Resource Planning*) по восьми критериям. Методология анализа среды функционирования применена в работе [3] для выбора программного обеспечения системы маршрутизации, отличительной особенностью применённого подхода является описание характеристик программных продуктов в порядковых (ранговых) шкалах.

В реальных задачах принятия решений критерии взаимозависимы, следовательно, традиционные операторы агрегации на основе аддитивных мер для объединения таких критериев не применимы. Для моделирования субъективного процесса принятия решений используются нечеткие меры, а в качестве оператора агрегации многими авторами применяется интеграл Шоке [4–6], в том числе и для оценки качества программного обеспечения [7–9]. В качестве оценочных характеристик авторы используют такие понятия, как удобство использования, эффективность, надежность, гибкость, портативность, повторное использование.

Постановка задачи выбора программного продукта. Пусть имеется множество программных продуктов (альтернатив) S, задаваемых на множестве функциональных возможностей (атрибутов, признаков) A и оцениваемых G экспертами, тогда трехмерная матрица вида продукт–атрибут–эксперт

$$\mathbf{F} = \| f_{ijk} \|, (i = 1, 2, \ldots, m; j = 1, 2, \ldots, n; k = 1, 2, \ldots, N)$$

определяет степень выраженности атрибута j в программном продукте i, определенную экспертом k, $0 \le f_{ijk} \le 1$. Тогда для каждого программного продукта i существует срез вида $\| f_{kj} \|$.

Нечеткая мера выражает значимость каждого подмножества атрибутов и определяется для каждого i следующим образом [10]:

$$\mu_i : 2^A \to \Re,$$

где 2^A – множество всех подмножеств множества индексов функциональных возможностей A. Функция μ удовлетворяет следующим условиям:

1) $\mu_i(\varnothing) = 0, \mu_i(A) = 1;$
2) $\forall B, C \subseteq A, B \subseteq C \Rightarrow \mu_i(B) \le \mu_i(C).$

Тогда применительно к нашей задаче значение интеграла Шоке по нечеткой мере есть интегральная оценка программного продукта i

$$\tilde{y}_i = (c)\int_A f d\mu = \sum_{j=1}^{n} (f(k,\sigma(j)) - f(k,\sigma(j-1)))\mu(A_{(i)}),$$

где σ является перестановкой индексов для ранжирования

$$f(k,\sigma(1)) \le \cdots \le f(k,\sigma(n)),\ A_{(i)} = \{\sigma(j),\ldots,\sigma(n)\} \text{ и } f(k,\sigma(0)) = 0.$$

Для применения интеграла Шоке необходимо задать нечеткую меру. Однако данная задача затруднена не только сложностью задания всех 2^n значений коэффициентов, но и пониманием экспертом смысла нечеткой меры [11].

Для того чтобы применить интеграл Шоке, предлагается решить задачу извлечения нечеткой меры на основе обучающей выборки. Пусть экспертные предпочтения по каждому программному продукту выражены в виде матрицы обобщенных интегральных оценок:

$$\mathbf{Y} = \| y_{ki} \|, (k = 1, 2, \ldots, N;\ i = 1, 2, \ldots, m).$$

Зная вектор экспертных предпочтений $\| y_k \|$ для программного продукта i, можно найти значения $\mu(A_{(i)})$, минимизируя выражение суммы разности квадратов:

$$e = \sum_{k=1}^{N} (y_k - \tilde{y}_i)^2 \to \min,$$

$$e = \sum_{k=1}^{N} \left(y_k - \sum_{j=1}^{n} (f(k,\sigma(j)) - f(k,\sigma(j-1)))\mu(A_{(i)}) \right)^2 \to \min.$$

Оптимальное решение должно удовлетворять ограничениям: нечеткие меры должны быть монотонными и всегда принадлежать интервалу [0, 1]. Таким образом, извлечение нечеткой меры является проблемой оптимизации ошибки e с ограничениями.

Для минимизации приведенного выражения будем использовать популяционный империалистический алгоритм. После извлечения нечетких мер $\mu(A_{(i)})$ для каждого программного продукта можно выбрать наилучший по требованиям пользователя.

Пусть требования пользователя представляют собой вектор

$$\mathbf{T} = \| t_j \|,$$

который определяет степень потребности атрибута j, $0 \le t_j \le 1$, а yt_i – интегральная оценка требований пользователя, вычисленная с использованием значений $\mu(A_{(i)})$ по интегралу Шоке. Для определения наилучшего программного продукта необходимо найти ближайшую к требованиям оценку ПП:

$$\min(|y_k - yt_i|).$$

Таким образом, метод решения задачи выбора ПП (после задания экспертных предпочтений) состоит из следующих этапов:

1) извлечение нечеткой меры на основе империалистического алгоритма;
2) определение наилучшего программного продукта по методу ближайших соседей.

Ниже предлагается более подробно рассмотреть первый этап.

Извлечение нечеткой меры с использованием империалистического алгоритма. Империалистический алгоритм основан на соперничестве стран в мировой истории [12]. Все страны разделены на две группы: империалистические государства и колонии. Основной частью данного алгоритма является империалистическое соперничество, которое должно приводить колонии к схождению к глобальному экстремуму целевой функции. Описание алгоритма минимизации ошибки e представлено ниже:

Вход: матрица $\| f_{kj} \|$ экспертных оценок функциональных возможностей программного продукта i, вектор $\| y_k \|$ обобщенных экспертных предпочтений.

Выход: нечеткая мера $\mu(A_{(i)})$.

Интерпретация нечеткой меры и ошибки в данном алгоритме: $\mu(A_{(i)})$ – позиция (координата) i-й страны; $c = e$ – стоимость i-й страны.

Шаг 1. Инициализация империй. Процесс инициализации империй начинается со случайной генерации N_{pop} количества стран. Из них выбирается N_{imp} наиболее сильных стран (империалистов), которые будут формировать империи.

Сила определяется через нормализованную стоимость C_i каждого империалиста:

$$C_i = c_i - \max_{j=\overline{1,N_{imp}}} c_j,$$

где c_i – стоимость i-го империалиста ($c = e$). Тогда сила p_i:

$$p_i = \left| \frac{C_i}{\sum_{j=1}^{N_{imp}} C_j} \right|.$$

Оставшиеся N_{col} стран распределяются в качестве колоний между империалистами пропорционально их силе. То есть количество колоний в i-й империи определяется как

$$NC_i = round\ (p_i N_{col}).$$

После определения количества колоний в каждой империи, колонии случайным образом распределяются среди них.

Шаг 2. Ассимиляция колоний. Процесс ассимиляции колоний моделируется их перемещением к империалисту. Направление перемещения совпадает с вектором, устремленным от колонии к империалисту. Расстояние перемещения x является случайной величиной, распределенной по нормальному закону

$$x \sim U(0, \beta \cdot d),$$

где d – текущее расстояние между колонией и империалистом, а β – число, большее единицы, которое позволяет колониям сближаться с империалистом равновероятно со всех сторон. В большинстве реализаций алгоритма используется значение $\beta \approx 2$ [12].

Шаг 3. Обмен позициями между империалистом и колонией. Если после ассимиляции новая позиция одной или нескольких колоний империи является более выгодной, чем позиция самого империалиста, тогда империалист перемещается на позицию этой колонии, а колония – на позицию империалиста. Иначе переход к Шагу 4.

Шаг 4. Расчет стоимости империи. Стоимость империи складывается из двух показателей: стоимость империалистического государства и стоимость колоний, входящих в нее. При этом наибольшее влияние оказывает империалист, в то время как влияние колоний незначительное:

$$TC_i = c_i + \xi \overline{c_i},$$

где TC_i – сила i-й империи; c_i – стоимость империалиста i-й империи; $\overline{c_i}$ – средняя стоимость колоний империи; ξ – положительное число меньше 1. Малое значение ξ позволяет обеспечить минимальное влияние колоний на стоимость империи. В большинстве реализаций алгоритма 0,1 является подходящим значением константы ξ [12].

Шаг 5. Империалистическое соперничество. Процесс соперничества моделируется выбором некоторого числа колоний (как правило, одной) самой слабой империи и инициированием борьбы между другими империями за право обладания колониями (колонией). При этом возможность выиграть соперничество имеет каждая из империй. То есть колонии не обязательно будут захвачены самой сильной империей, но она имеет наибольшую вероятность обладания ими.

Перед началом соперничества необходимо вычислить силу (вероятность победы) для каждой империи. Сила i-й империи определяется через нормализованную стоимость NTC_i каждой империи (аналогично Шагу 1):

$$NTC_i = TC_i - \max_{j=\overline{1, N_{imp}-1}} TC_j.$$

Здесь максимальная стоимость империи вычисляется за исключением самой слабой империи, за обладание колонии которой осуществляется соперничество. Тогда сила (вероятность победы) определяется как

$$P_{p_i} = \left| \frac{NTC_i}{\sum_{j=1}^{N_{imp}-1} NTC_j} \right|.$$

Затем формируется вектор **P** вида

$$\mathbf{P} = [P_{p_1}, P_{p_2}, ..., P_{p_{N_{imp}-1}}]$$

и вектор **R** такой же размерности, его элементы случайно распределены по равномерному закону

$$\mathbf{R} = [r_1, r_2, ..., r_{N_{imp}-1}],\ r_1,\ r_2,\ \ldots,\ r_{N_{imp}-1} \sim U(0, 1),$$

и вычисляется вектор **D** как разница между **P** и **R**:

$$\mathbf{D} = \mathbf{P} - \mathbf{R} = [D_1, D_2, ..., D_{N_{imp}-1}] = [P_{p_1} - r_1, P_{p_2} - r_2, ..., P_{p_{N_{imp}-1}} - r_{N_{imp}-1}].$$

Таким образом, колонии, за которые идет борьба, передаются империи, для которой соответствующее значение вектора **D** максимально.

Шаг 6. Уничтожение слабых империй. Если империя не содержит ни одной колонии, то уничтожить империю. Иначе переход к Шагу 7.

Шаг 7. Условие останова. Если осталась только одна империя, то закончить выполнение алгоритма. Позиция $\mu(A_{(i)})$ империалиста оставшейся империи является выходным значением алгоритма. Иначе переход к Шагу 2.

В [7] утверждается, что генетические алгоритмы могут застревать в локальных оптимумах. В [12] указано, что империалистический алгоритм быстрее сходится к своему оптимальному значению в сравнении с классическим генетическим алгоритмом и оптимизацией по методу роящихся частиц.

Эксперимент. Целью эксперимента является проверка адекватности данных, полученных с помощью представленного метода, соотнесение результатов с рекомендациями экспертов.

Эксперимент проводился на реальных данных по 11 программным продуктам системы «1С:Предприятие 8» из одной области применения. Множество входных данных состоит из 11 таблиц экспертных оценок по 10 функциональным возможностям ПП, а также 11 векторов предпочтений экспертов. Каждая таблица содержит оценки пяти экспертов по одному ПП (табл. 1).

Таблица 1

Оценки программного продукта

Эксперт	Функциональная возможность										Общая оценка
	УП	КФ	МУ	РО	УО	СУ	П	ВК	РЗП	УП	
Э1	1	0,75	1	0,75	0,5	0,5	0,75	0,75	0,5	0,5	0,8
Э2	1	0,75	1	0,5	0,75	0,75	0,75	0,75	0,5	0,5	0,7
Э3	1	0,75	1	0,75	0,5	0,5	0,5	1	0,75	0,5	0,85
Э4	1	0,5	0,75	0,75	0,75	0,75	0,75	0,75	0,5	0,5	0,75
Э5	1	0,75	1	0,75	0,75	0,5	0,75	0,5	0,5	0,75	0,65

где УП – учет пациентов, КФ – коечный фонд, МУ – медицинские услуги, РО – регламентированные отчеты, УО – управленческие отчеты, СУ – складской учет, П – планирование, ВК – взаиморасчеты с клиентами, РЗП – расчет заработной платы, УП – управление персоналом.

При извлечении нечеткой меры в империалистическом алгоритме использовалось 592 страны и 5 империй. Результаты извлечения нечеткой меры представлены в табл. 2.

Таблица 2

Нечеткая мера программных продуктов

	ПП1	ПП2	ПП3	ПП4	ПП5	ПП6	ПП7	ПП8	ПП9	ПП10	ПП11
Нечеткая мера	0,89119	0,91705	0,56071	0,55743	0,32565	0,50426	0,83727	0,27791	0,41013	0,32046	0,81047
Ошибка	0,06365	0,06621	0,02248	0,023	0,0161	0,02245	0,09301	0,01625	0,03509	0,03105	0,02032

Здесь ПП1 – 1С:Медицина. Поликлиника, ПП2 – 1С:Медицина. Больница, ПП3 – 1С:Медицина. Больничная аптека, ПП4 – 1С:Медицина. Клиническая лаборатория, ПП5 – 1С:Медицина. Больничные, ПП6 – 1С:Медицина. Федеральные регистры, ПП7 – 1С:Розница 8. Аптека, ПП8 – 1С:Кабинет здоровья образовательного учреждения, ПП9 – 1С:Управление аптечной сетью, ПП10 – 1С:Паспорт здоровья ребенка, ПП11 – Аналит:учет медицинских услуг.

Метод апробирован на пяти пользователях-экспертах, уже работающих с программными продуктами «1С:Предприятие 8». Предлагалось сформировать оценки функциональных возможностей желаемого программного продукта (табл. 3).

По данным требованиям и с использованием полученных нечетких мер формировались интегральные оценки желаемых ПП. В результате сравнения интегральных оценок требований пользователей с интегральными оценками ПП определялся наилучший программный продукт для каждого пользователя (см. табл. 3).

Полученные результаты совпали с рекомендациями экспертов, а также с реальным выбором пользователей, сделанным ранее. Проведенное тестирование позволяет сделать вывод о том, что

данный подход способен оказать объективную поддержку пользователю в вопросе выбора программного продукта.

Таблица 3

Требования пользователей и результаты выбора

Пользователь	Функциональные возможности										Результат
	УП	КФ	МУ	РО	УО	СУ	П	ВК	РЗП	УП	
П1	1	0,5	1	1	0,25	0,5	0,05	0,75	0,5	0,5	ПП9
П2	1	0,75	1	0,75	0,75	0,5	0,25	0,75	0,5	0,5	ПП11
П3	1	1	1	0,75	0,75	0,75	0,05	0,05	0,05	0,05	ПП8
П4	0,5	0,75	0,5	1	0,5	0,05	0,75	0,05	0,75	0,75	ПП4
П5	0,75	0,5	0,75	0,25	0,05	0,05	0,5	0,75	1	1	ПП5

Заключение. Предложенный метод позволяет анализировать программные продукты по функциональным возможностям для выбора наиболее подходящего варианта. На основе представленного метода разработана подсистема, которая является частью экспертной системы [13, 14] и позволяет подобрать программный продукт по требованиям пользователя.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (гранты 12-07-00055а, 14-07-00449а).

Литература

1. Azadeh A. A robust decision-making methodology for evaluation and selection of simulation software package / A. Azadeh, S.N. Shirkouhi, K. Rezaie // International Journal of Advanced Manufacturing Technology. – 2010. – Vol. 47. – P. 381–393.

2. Karaarslan N. An application for modular capability-based ERP software selection using AHP method / N. Karaarslan, E. Gundogar // International Journal of Advanced Manufacturing Technology. – 2009. – Vol. 42. – P. 1025–1033.

3. Smirlis Y.G. Data envelopment analysis models to support the selection of vehicle routing software for city logistics operations / Y.G. Smirlis, V. Zeimpekis, G. Kaimakamis // Operational Research. 2012. – Vol. 12. – P. 399–420.

4. Tan C. Intuitionistic fuzzy Choquet integral operator for multi-criteria decision making / C. Tan, X. Chen // Expert Systems with Applications. – 2010. – Vol. 37. – P. 149–157.

5. Grabisch M. The application of fuzzy integrals in multicriteria decision making // European Journal of Operation Research. – 1996. – № 89. – P. 445–456.

6. Meyer P. On the use of the Choquet integral with fuzzy numbers in multiple criteria decision support / P. Meyer, M. Roubens // Fuzzy Sets and Systems. – 2006. – Vol. 157. – P. 927–938.

7. A Hybrid Algorithm to Extract Fuzzy Measures for Software Quality Assessment / X. Wang, M. Ceberio, S. Virani et al. // Journal of Uncertain Systems. – 2013. – Vol. 7, № 3. – P. 219–237.

8. Pasrija V. Assessment of Software Quality: Choquet Integral Approach / V. Pasrija, S. Kumar, P.R. Srivastava // Procedia Technology. – 2012. – Vol. 6. – P. 153–162.

9. Yang H. Measuring Software Product Quality with ISO Standards Base on Fuzzy Logic Technique // Affective Computing and Intelligent Interaction, AISC 137. – Berlin: Springer-Verlag, 2012. – P. 59–67.

10. Sugeno M. Theory of fuzzy integrals and its applications: Ph.D. Thesis. – Tokyo. – 1974. – 237 p.

11. Сакулин С.А. К вопросу о практическом применении нечетких мер и интеграла Шоке / С.А. Сакулин, А.Н. Алфимцев // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. – 2012. – С. 55–63.

12. Atashpaz-Gargari E. Imperialist Competitive Algorithm: An Algorithm for Optimization Inspired by Imperialistic Competition / E. Atashpaz-Gargari, C. Lucas // IEEE Congress on Evolutionary Computation. – 2007. – P. 4661–4667.

13. Ахаев А.В. Алгоритмы и программные средства построения экспертных систем выбора программных продуктов на примере «1С:Предприятие 8» / А.В. Ахаев, И.А. Ходашинский // Информатика и системы управления. – 2013. – № 4. – С. 70–79.

14. Ахаев А.Е. Алгоритм оценивания функционального наполнения программных продуктовна основе нечеткого логического вывода // Доклады ТУСУРа. – 2013. – № 2 (28). – С. 169–174.

Ахаев Александр Валерьевич
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: AkhaevAV@gmail.com

Ходашинский Илья Александрович
Д-р техн. наук, профессор каф. КИБЭВС
Тел.: 8 (382-2) 41-34-26
Эл. почта: hodashn@rambler.ru

Анфилофьев Александр Евгеньевич
Студент каф. КИБЭВС ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: yowwi00@gmail.com

Akhaev A.V., Hodashinsky I.A.
Method for software selection on the basis of Choquet integral and imperialist algorithm

A problem of software selection on functionality is discusses. To solve based on the Choquet integral, and to extract the fuzzy measure used imperialist optimization algorithm is suggested. Variant of software selection on integrated assessment is offered. The experiment was conducted.
Keywords: integral evaluation, software, Choquet integral, imperialist algorithm.

УДК 504.064.37

М.Ю. Катаев, А.К. Лукьянов

Восстановление общего содержания углекислого газа методом эмпирических ортогональных функций из спутниковых данных

Рассматривается описание метода эмпирических ортогональных функций (ЭОФ) и его модификации для решения задачи восстановления общего содержания углекислого газа по реальным данным измерений спутниковым прибором GOSAT. Обсуждается структура программного комплекса, предназначенного для обучения метода ЭОФ и обработки данных измерений. Приводятся результаты обработки данных измеренных спутниковых спектров отраженного от поверхности солнечного излучения в ближней ИК-области спектра для станции Lamont наземной сети TCCON измерения общего содержания CO_2 в атмосфере.

Ключевые слова: атмосфера Земли, газовый состав, дистанционные спутниковые методы, отраженное от поверхности солнечное излучение, Фурье-спектрометр, эмпирические ортогональные функции.

Естественные природные факторы и хозяйственная деятельность человека вносят существенные изменения в состав атмосферы за счет изменения содержания аэрозольных примесей и газовых компонент. Замеченные в последнее время существенные изменения погоды привлекают внимание широкого круга исследователей в связи с актуальными оценками ожидаемых последствий различных воздействий (антропогенных и естественных) на климат Земли. Для решения всех возникающих при этом задач необходимо разрабатывать модели пространственно-временного поведения различных компонент атмосферы, в том числе и углекислого газа. Несмотря на то, что измерительных станций в мире работает более двух тысяч [http://www.wmo.int], они расположены неравномерно пространственно и проводят не синхронизированные по времени измерения. Этих измерений достаточно, чтобы построить качественную модель, однако совсем недостаточно для детальной количественной модели, для которой более приемлемы равномерная пространственная и временная сетки. Единственным способом, который максимально полно позволяет проводить регулярные по пространству и времени измерения, является спутниковый метод. Среди спутниковых приборов, а соответственно и подходов к обработке, позволяющих проводить измерения общего содержания CO_2 можно выделить Sciamachy [www.sciamachy.org], GOSAT [www.gosat.nies.go.jp], AIRS [airs.jpl.nasa.gov], IASI [smsc.cnes.fr/IASI]. Эти приборы различаются по спектральным и пространственным характеристикам измерений, что, естественно, приводит при обработке данных измерений к различной точности определения общего содержания CO_2. Среди указанных спутниковых приборов выделяется прибор GOSAT, который начал измерения с середины 2009 г. и предназначен для мониторингового режима измерений общего содержания CO_2 и CH_4.

В данной статье нами рассматривается метод эмпирических ортогональных функций (ЭОФ) [1] и его модификация, который применяется для целей обработки данных спутникового мониторинга общего содержания CO_2.

Описание составляющих спутникового сигнала. Спутниковый прибор GOSAT представляет собой Фурье-спектрометр среднего разрешения (0,2 $см^{-1}$), для которого диаметр пятна обзора составляет около 8 км. Собранное прибором с пятна обзора отраженное солнечное излучение измеряется с соотношением сигнал/шум = 1000/1. Спектральные каналы прибора расположены в ближней ИК и ИК-области спектра: канал *1* – 0,757–0,775 мкм (12900–13200 $см^{-1}$), канал *2* – 1,56–1,72 мкм (5800–6400 $см^{-1}$), канал *3* – 1,92–2,08 мкм (4800–5200) и канал *4* – 14,28–5,55 мкм (700–1800 $см^{-1}$). Для восстановления общего содержания CO_2 применяются данные измерений второго канала, в котором расположены полосы поглощения углекислого газа (рис. 1).

Основные составляющие спутникового сигнала связаны с отражением солнечного излучения от поверхности, расположенным в пятне обзора, однократно и многократно рассеянным излучением в атмосфере, а также переотраженным излучением от поверхности вне пятна обзора и зарегистриро-

ванным спутниковым прибором. Наиболее значимым по величине является отраженный от поверхности сигнал, который составляет от 70 до 90% всего сигнала в зависимости от угла падения солнечного излучения. Вторым по величине сигналом является однократно рассеянное излучение [2].

В статье [1] нами рассматривалось применение метода ЭОФ для целей восстановления общего содержания углекислого газа, когда сигналы прибора были модельными. Было показано, что при отсутствии помех разного класса, присутствующих в реальных измерениях, точность восстановления общего содержания CO_2 высокая (средняя относительная погрешность = 0,032%).

Применимость разработанного подхода к решению обратной задачи восстановления общего содержания CO_2 из реальных данных рассматривается в данной статье.

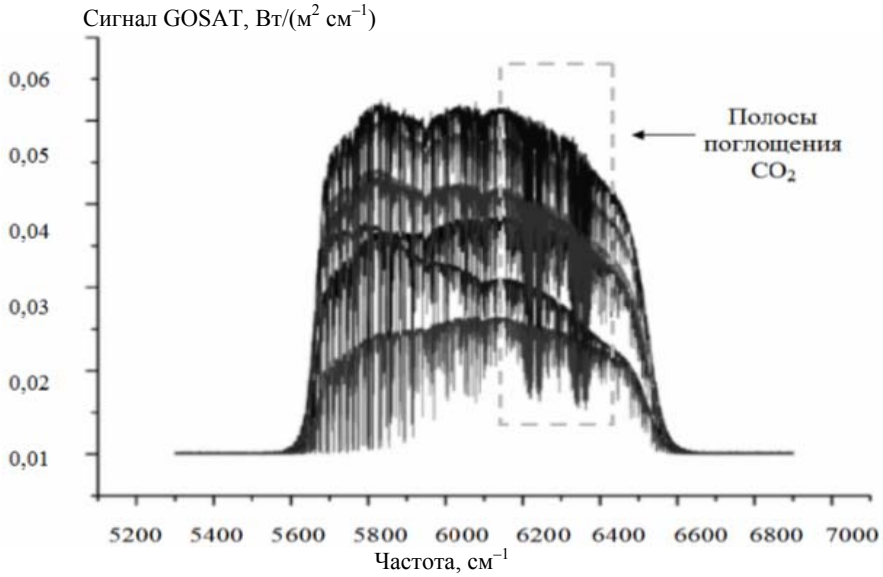


Рис. 1. Реально измеренные спектры отраженного солнечного излучения

Метод эмпирических ортогональных функций. Описание различных составляющих измеренного сигнала необходимо было для того, чтобы пояснить специфику подходов (метод дифференциального поглощения, метод оптимального оценивания, DOAS и др. [3–14]) к решению обратной задачи и предлагаемого подхода. Традиционно применяются параметрические подходы, когда измеренный сигнал (см. (1)) сравнивается с физической моделью:

$$\mathbf{y}_{obs} = f(\mathbf{p},\mathbf{b}) + \boldsymbol{\xi}, \tag{1}$$

где $f(\mathbf{p},\mathbf{b})$ – соответствующая физическая модель (в нашем случае это уравнение переноса излучения в атмосфере); $\mathbf{p}$ – искомый параметр (общее содержание CO_2); $\mathbf{b}$ – мешающие параметры (например, оптические толщи водяного пара и аэрозоля); $\boldsymbol{\xi}$ – ошибки измерения; $\mathbf{y}_{obs}$ – полученные измерения.

Решение относительно искомого параметра ищется из выражения невязки:

$$\Delta(\mathbf{p}) = \left\|\mathbf{y}_{obs} - f(\mathbf{p},\mathbf{b})\right\|^2_{\mathbf{S}_y} + \alpha\left\|\mathbf{p} - \mathbf{p}_a\right\|^2_{\mathbf{S}_\mathbf{p}} + \beta\left\|\mathbf{p}\right\|^2_{\mathbf{Z}}, \tag{2}$$

где $\mathbf{p}_\alpha$ – априорная оценка искомого параметра; $\mathbf{S}_y$ – матрица ковариации случайной ошибки измерений; α, β – параметры; $\mathbf{S}_p$ – матрица ковариации ошибок априорной информации и $\mathbf{Z}$ – матрица сглаживания Тихонова–Туоми (Tikhov–Twomey). Во многих алгоритмах [6, 9–13] последний член с матрицей $\mathbf{Z}$ опускают.

Представим один из вариантов расчета матрицы $\mathbf{Z}$:

$$\mathbf{Z} = \begin{pmatrix} 2 & -1 & \dots & 0 \\ -1 & 2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & -1 & 2 \end{pmatrix}.$$

Решение уравнения (2), приводит к выражению:

$$\mathbf{p}^{i+1} = \mathbf{p}^i + \mathbf{A}^{-1}(\mathbf{K}_i^T \mathbf{S}_y^{-1}(y_{obs} - f(\mathbf{p}^i,\mathbf{b})) + \mathbf{S}_p^{-1}(\mathbf{p}^i - \mathbf{p}_a) - \mathbf{Z}\mathbf{p}^i), \tag{3}$$

здесь $\mathbf{K}$ – матрица Якоби ($\mathbf{K} = \partial \mathrm{f} / \partial \mathbf{p}$), содержащая частные производные, а матрица $\mathbf{A}$ равна $\mathbf{A} = \mathbf{K}_i^T \mathbf{S}_y^{-1} \mathbf{K}_i + \mathbf{S}_p^{-1} + \mathbf{Z}$.

Как видно из (3) найденное решение зависит от многих составляющих, которые определяют физическую модель, точность формирования матрицы Якоби, знание априорной информации и различного рода погрешности. Эти составляющие определяют точность решения. Сложностью решения (3) является тот аспект, что в случае сильных изменений сигнала по величине, изменения вектора *b* решение может сильно меняться (свойство некорректности), а также, при больших размерностях (сотни или тысячи точек) измеряемого сигнала, время решения (3) сильно возрастает. Это обстоятельство побудило нас исследовать возможности другого подхода, более быстрого и при этом без потери точности, который относится к классу непараметрических, а именно метод эмпирических ортогональных функций.

Для непараметрических подходов характерно сравнение измеренных сигналов и решения. Статистические или иные характеристики взаимосвязи этих элементов позволяют построить алгоритм решения обратной задачи.

Пусть имеется набор измерений $\mathbf{Y}$, который содержит в себе информацию об искомом параметре (общем содержании CO_2 на оптической трассе формирования сигнала). Между сигналом и искомым параметром существует некоторая функциональная связь вида (1).

Принцип метода эмпирических ортогональных функций (ЭОФ) широко представлен в литературе в основном для анализа рядов наблюдений, сжатия информации, выявления закономерностей проявления физических процессов во времени и пространстве [15–19]. При решении обратных задач этот подход практически не используется.

Метод решения обратной задачи восстановления общего содержания CO_2 на основе ЭОФ связан с набором типичных математических операций:

1. Вычисление ковариационной функции *R*:

$$R = \Delta Y (\Delta Y)^T, \ \Delta Y = (Y - < Y >), \tag{4}$$

где $\mathbf{Y}$ – измеренный (или модельный) сигнал из *N* точек.

2. Разложение в ряд по собственным векторам и значениям ковариационной матрицы

$$\mathbf{R} = \mathbf{U} \Lambda \mathbf{U}^T, \tag{5}$$

здесь $\mathbf{U}$ – матрица собственных векторов и $\mathbf{\Lambda}$ – собственные значения.

3. На основе элементов (4) и (5) можно построить эмпирические ортогональные функции (ЭОФ)

$$\mathbf{E} = \mathbf{U} \Delta \mathbf{Y}. \tag{6}$$

4. Определение искомого параметра

Для решения обратной задачи необходимо учитывать тот факт, что сигналы связаны с общим содержанием газов, поглощающих солнечное излучение в выбранном канале длин волн. В предположении линейной зависимости искомой величины от измеренных сигналов можно получить выражение

$$\Delta \mathbf{P} = \mathbf{P} - < \mathbf{P} >= \mathbf{A} \mathbf{E}, \tag{7}$$

где вектор $\mathbf{A}$ является искомым из решения системы алгебраических уравнений:

$$\mathbf{A} = (\Delta \mathbf{P} \Delta \mathbf{P}^T)^{-1} \Delta \mathbf{P}^T \mathbf{E}. \tag{8}$$

Решение системы линейных алгебраических уравнений (8) позволяет найти коэффициенты $\mathbf{A}$ и тем самым построить алгоритм для обработки данных измерений, который мы назвали базовым:

$$\mathbf{P} = \mathbf{A} \mathbf{E} + <\mathbf{P}_o>, \tag{9}$$

где $\mathbf{P}_o$ – среднее, полученное на стадии расчета коэффициентов $\mathbf{A}$.

Численное тестирование этого подхода на модельных данных [1], позволило выявить характерную особенность алгоритма, которая выражалась в смещении решения от точного значения. Из анализа результатов численного моделирования было обнаружено, что смещение обусловлено отсутствием учета априорной информации, например зенитного угла Солнца, в зависимости от которого меняется амплитуда сигнала.

Нами была выполнена модификация данного подхода за счет добавления априорной информации. Известно, что при спутниковом зондировании атмосферы необходимо знать положение Солнца относительно пятна наблюдения. Область атмосферы над пятном наблюдения зависит от рельефа и

типов поверхности, содержания аэрозольной составляющей и распределения влажности воздуха. Учет этих компонент в матрице измерений **Y** позволил избежать смещения решения и получить более точное решение. Все выполняемые действия, связанные с решением обратной задачи, были воплощены в программный комплекс.

Описание программного комплекса. Блок-схема программного комплекса приведена на рис. 2. Особенностью непараметрических подходов обработки является обязательное выполнение двух этапов: 1) обучения и 2) обработки. Впоследствии, когда обучение было произведено, остается один этап – обработка. На этапе обучения были использованы разнообразные наборы данных (модельные и реальные). Модельные спутниковые сигналы рассчитываются на основе программы, написанной нами [20]. Программа позволяет рассчитывать спутниковый сигнал для любой точки поверхности Земли и времени в течение года (это время циклов изменения концентрации CO_2, CH_4 и других атмосферных газов). Далее выбиралась точка на поверхности Земли, для которой проводились расчеты спутниковых сигналов GOSAT (см. рис. 1) для нескольких лет (2009–2013 гг.), с шагом 6 ч (1460 сигналов в год и каждый сигнал 8000 спектральных точек в диапазоне второго канала). Часть сигналов из общей выборки формирует обучающую выборку (50%), другая часть тестовую (50%) по правилу, представленному в [21]. Соотношение между обучающей и тестовой выборкой может быть изменено в зависимости от точности обучения на первом шаге. Если заданная точность 0,1% не достигнута, обучающая выборка увеличивается (в нашем случае на 5%) и т.д., пока не будет достигнута заданная точность. Есть ограничение на соотношение между обучающей и тестовой выборками, которое выражается в условии, что тестовая выборка не может быть менее 10% от общей выборки. В работе [1] нами были представлены результаты обучения и обработки модельных данных, которые показали результат, достаточный для того, чтобы перейти к обработке реальных сигналов. Реальные сигналы для общей выборки, для того же промежутка времени и географической точки, для уровня L1B (сигналы после радиометрической калибровки) были получены на сайте [www.gosat.nies.go.jp].

Для расчета спутниковых сигналов использовалась модельная информация об общем содержании CO_2 в атмосфере, а также реальные данные GOSAT, уровня L2, восстановленные из сигналов GOSAT значения общего содержания параметрическим методом (3)). Спутниковые сигналы и данные общего содержания являются основой для обучения, при котором формируются коэффициенты обратной задачи **A** и **E** в нами разработанном программном комплексе (см. рис. 2).

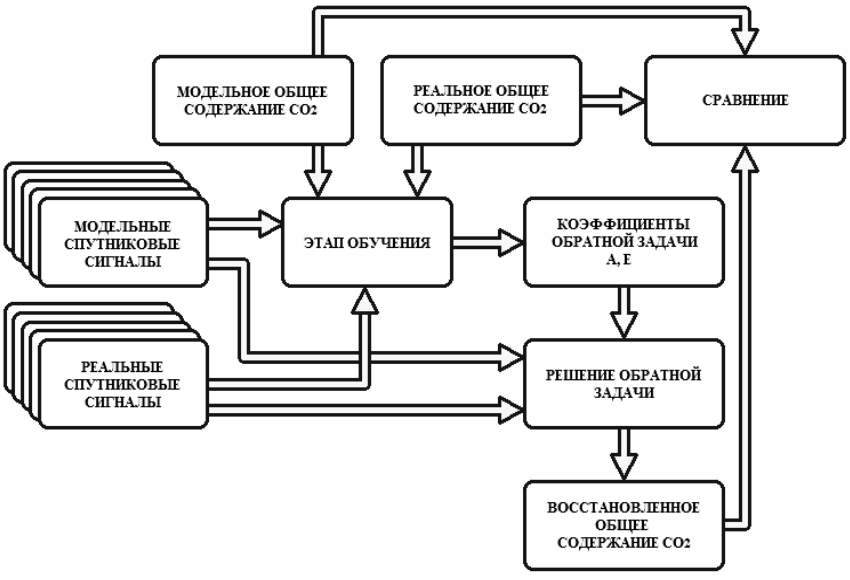


Рис. 2. Блок-схема программного комплекса

Таким образом, процесс обучения связан с расчетами по формулам (4)–(8), а процесс обработки в использовании формулы (7), где матрица **E** связана с измеренным сигналом. Более детально алгоритм представлен в [1].

После того как обработаны сигналы и получены значения общего содержания CO_2, эти значения сравниваются с известными значениями, которые были известны априори при получении модельных сигналов или получены для того же времени, географического места независимым прибором.

Результаты решения обратной задачи для реальных данных. Точность определения газового состава атмосферы по данным спутниковых измерений обусловлена совокупностью разнообразных факторов: погрешность измерений прибора, абсолютная и спектральная калибровка, погрешности телеметрии, особенности алгоритма интерпретации, исходная спектроскопическая и априорная информация. Практическое использование данных о состоянии атмосферы возможно после тщательного анализа их соответствия предъявляемым требованиям точности, пространственного и временного разрешения, на основе интенсивных согласованных исследований по валидации спутниковых данных.

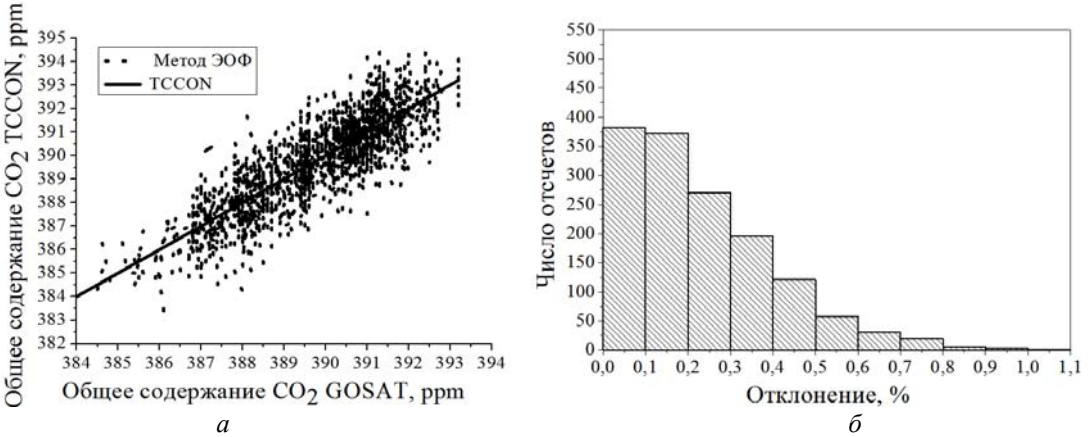
Для целей проверки возможности применения метода эмпирических ортогональных функций при обработке реальных сигналов нами были использованы данные измерений международной сети станций TCCON (Total Carbon Column Observing Network) [http://www.tccon.caltech.edu]. На этих станциях проводится измерение общего содержания CO_2 и CH_4 и других атмосферных параметров. При этом общее содержание CO_2 и CH_4 проводится прибором (Фурье-спектрометр среднего разрешения), по своим возможностям близком к прибору, который установлен на спутнике.

Для подготовки выборки данных, нами была выбрана станция Lamont (36.604 С, 97,486 В), находящаяся практически в центре Северной Америки. Данные станции в течение практически каждого дня (исключение составляют облачные дни, когда измерения не выполняются) были получены для временного интервала 2000–2013 гг. Спутниковые измерения были собраны за этот же промежуток времени из области размером 2×2 градуса, с центром в точке стояния станции Lamont. Всего было получено 5785 сигналов. Далее нами было выполнено согласование данных измерений GOSAT с данными измерений на станции Lamont по времени.

Каждый сигнал GOSAT представляет собой набор спектральных точек, получаемых Фурье-спектрометром в четырех каналах (около 20 тыс. точек), записанных в формате HDF. Нами выбирались данные второго канала (около 8000 точек), из которых для обработки отбирались данные (1800 точек), в которых расположены полосы поглощения углекислого газа (см. рис. 1). Далее все оставшиеся спектральные точки сигналов за весь временной промежуток времени, проходили оценку на вариабельность. Для дальнейшей работы были оставлены наиболее изменчивые по величине спектральные точки сигнала, которых осталось всего 780. Таким образом, для обучения и тестирования нами было получено для станции Lamont 5785 реальных сигналов GOSAT, в каждом из которых было 780 спектральных точек.

Для проверки работоспособности алгоритма ЭОФ нами выполнялось два варианта решения обратной задачи. Первый вариант связан с обучением и обработкой данных GOSAT для выборки в течение одного года, а второй вариант – когда обучение остается первоначальным, а выборка для обработки поступает полностью (за 2009–2013 гг.).

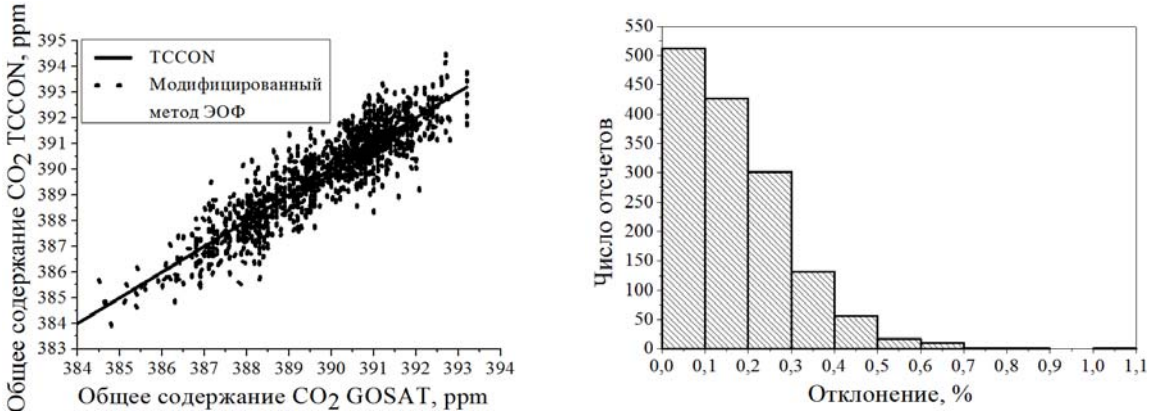
После обучения и решения обратной задачи стандартным подходом ЭОФ, для тестовой выборки результаты восстановленного общего содержания CO_2 сравнивались со значениями для станции Lamont, которые показаны на рис. 3. Такая же процедура выполнялась для модифицированного подхода ЭОФ, когда матрица измерений дополнялась априорными значениями (зенитный угол Солнца, при котором получен сигнал, общее содержание аэрозольной составляющей атмосферы и водяного пара, на основе данных GOSAT уровня L2), и показана на рис. 4.



а *б*

Рис. 3. Результаты сравнения обработки измерений GOSAT методом ЭОФ стандартным подходом [на основе формул (4)–(7)]

Сравнение результатов, представленных на рис. 3, *а*, *б* и 4, *а*, *б*, показывает, что учет априорной информации позволяет получить более близкую информацию об общем содержании CO_2 к данным измерений на наземной станции. В первом случае (см. рис. 3, *б*) отличие сигналов не превышает 0,9%, а во втором случае – 0,6% (см. рис. 4, *б*).



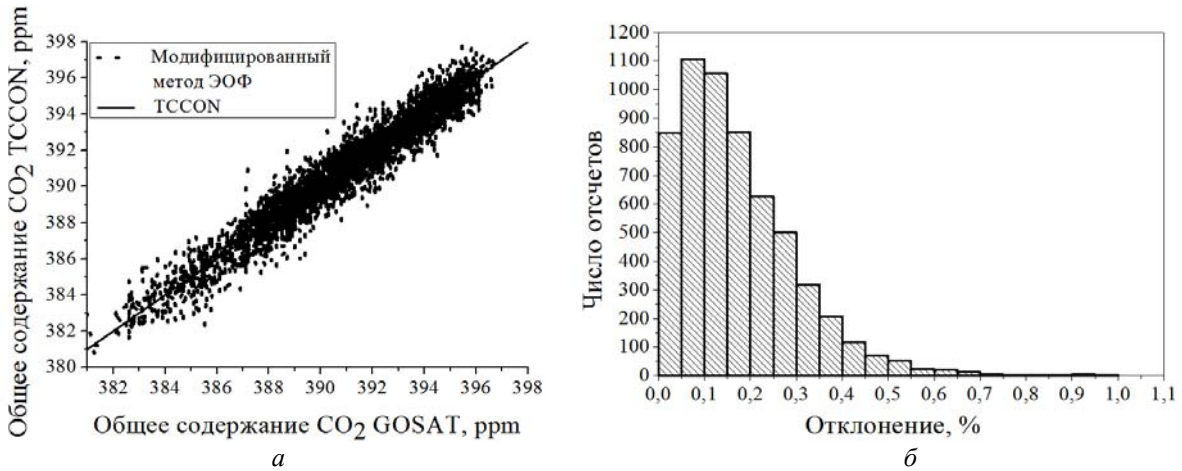
а *б*

Рис. 4. Результаты сравнения обработки измерений GOSAT методом ЭОФ модифицированным подходом (в матрице измерений добавлена априорная информация)

Далее нами была проведена обработка всей совокупности данных (рис. 5) за несколько лет модифицированным методом ЭОФ, и результаты представлены на рис. 6, *а*, *б*.

Рис. 5. Значения общего содержания CO_2 для полной выборки TCCON за 2009–2012 гг.

Из рис. 6 видно, что даже при обучении метода ЭОФ на выборке для одного года использование полученных на этой стадии коэффициентов [**A, E**, см. (9)] для обработки результатов измерений за четыре года отличается от данных наземного измерения общего содержания CO_2 с отклонением не более 0,7%. Таким образом, отклонение практически не выросло (см. рис. 3 и 4), что говорит об устойчивости и эффективности метода ЭОФ. Данное свойство хорошо объясняется тем, что метод ЭОФ основан на учете статистической информации.



а *б*

Рис. 6. Результаты сравнения обработки измерений GOSAT методом ЭОФ модифицированным подходом (в матрице измерений добавлена априорная информация)

Заключение. Проведенные исследования показывают возможность восстановления общего содержания CO_2 по космическим гиперспектральным измерениям отраженного солнечного излучения при решении задач мониторинга окружающей среды. Рассмотренный метод эмпирических ортогональных функций обработки данных измерений может быть применен для получения достоверной информации о пространственно-временном поведении углекислого газа на больших территориях. Основанием для этого является согласование, с отклонением не более одного процента, данных восстановленных значений общего содержания CO_2 и данных подспутниковой станции TCCON Lamont за длительный промежуток времени. Представлено описание программной системы для хранения и обработки данных, получаемых с спутника GOSAT.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №13-05-01036.

Литература

1. Катаев М.Ю. Непараметрические математические методы восстановления общего содержания CO_2 из данных спутникового мониторинга / М.Ю. Катаев, С.Г. Катаев, А.Г. Андреев и др. // Доклады ТУСУРа. – 2011. – № 2 (24), ч. 3. – С. 181–186.

2. Зуев В.Е. Распространение видимых и инфракрасных волн в атмосфере. – М.: Советское радио, 1970. – 496 с.

3. Huang H. Application of Principal Component Analysis to High-Resolution Infrared Measurement Compression and Retrieval / H. Huang, P. Antonelli // J. Appl. Meteorol. – 2001. – №40. – P. 365–388.

4. Airborne observations of spatial and temporal variability of tropospheric carbon dioxide / B.E. Anderson, G.L. Gregory, J.E. Collins et al. // J. Geophys. Res. – 1996. – Vol. 101. – P. 1985–1997.

5. Buchwitz M. A near infrared optimized DOAS method for the fast global retrieval of atmospheric CH_4, CO, CO_2, H_2O, and N_2O total column amounts from SCIAMACHY/ENVISAT-1 nadir radiances / M. Buchwitz, V.V. Rozanov, J.P. Burrows // J. Geophys. Res. – 2000. – Vol. 105. – P. 15231–15246.

6. Dufour E. Spaceborne estimate of atmospheric CO_2 column by use of the differential absorption method: error analysis / E. Dufour, F. Breon // Appl. Opt. – 2003. – № 42. – P. 3595–3609.

7. Frankenberg C. Iterative maximum a posteriori (IMAP)-DOAS for retrieval of strongly absorbing trace gases: Model studies for CH_4 and CO_2 retrieval from near infrared spectra of SCIAMACHY onboard ENVISAT / C. Frankenberg, U. Platt, T. Wagner // Atmos. Chem. Phys. – 2005. – № 5. – P. 9–22.

8. Mao J. Sensitivity studies for space-based measurement of atmospheric measurement of atmospheric total column carbon dioxide by reflected sunlight / J. Mao, S.R. Kawa // Appl. Opt. – 2004. – № 43. – P. 914–927.

9. Zhiming K. Spaceborne measurements of atmospheric CO_2 by high-resolution NIR spectrometry of reflected sunlight: An introductory study / K. Zhiming, J. Marglois, G. Toon et al. // Geophysical research letters. – 2002. – Vol. 29, № 15. – P. 111–114

10. Three years of greenhouse gas column-averaged dry air mole fractions retrieved from satellite. Part 1: Carbon dioxide / O. Schneising, M. Buchwitz, J.P. Burrows et al. // Atmos. Chem. Phys. – 2008. – № 8. – P. 3827–3853.

11. Park J.H. Atmospheric CO2 monitoring from space // Appl. Opt. – 1997. – Vol. 36. – P. 2701–2712.

12. Connor B. Orbiting Carbon Observatory: Inverse method and prospective error analysis / B. Connor, H. Boesch, G. Toon et al. // J. Geophys. Res. – 2008. – Vol. 113. – P. 20903–20919.

13. Boesch H. Global Characterization of CO_2 Column Retrievals from Shortwave-Infrared Satellite Observations of the Orbiting Carbon Observatory-2 Mission / H. Boesch, D. Baker, B.J. Connor et al. // Remote Sens. – 2011. – Vol. 23. – P. 270–304.

14. Butz A. Retrievals of atmospheric CO_2 from simulated space-borne measurements of backscatteres near-infrared sunlight: accounting for aerosol effects / A. Butz, O.P. Hasekamp, C. Frankenberg, I. Aben // Applied Optics. – 2009. – Vol. 48. – P. 3322–3336.

15. Обухов А.М. О статистически ортогональных разложениях эмпирических функций // Известия АН СССР. Сер. геофиз. – 1960. – № 3. – С. 432–439.

16. Естественные составляющие метеорологических полей / А.В. Мещерская, Л.В. Руховец, М.И. Юдин, Н.И. Яковлева. – Л.: Гидрометеоиздат, 1970. – 199 с.

17. Айвазян С.А. Прикладная статистика: Исследование зависимостей / С.А. Айвазян, И.С. Енюков, Л.Д. Мешалкин. – М.: Финансы и статистика, 1985. – 487 с.

18. Фортус М.И. Эмпирические ортогональные функции случайного временного ряда, заданного на конечном отрезке // Известия РАН. Физика атмосферы и океана. – 2002. – Т. 38, №1. – С. 64–70.

19. Чувашина И.Е. Применение аппарата разложения в двойные ряды по ЭОФ координат и времени для исследования временной структуры полей средних суточных температур // Труды ГГО. – 1976. – Вып. 367. – С.81–86.

20. Kataev M.Yu. Information-processing software for satellite signal modeling in global scale / M.Yu. Kataev, A.K. Lukianov // International Conference on Environmental Observations, Modeling and Information Systems (ENVIROMIS-2010), 5–11 July 2010, Tomsk, Russia. – Tomsk, 2010. – P. 71.

21. Хайкин С. Нейронные сети: полный курс. – М.: Вильямс, 2006. – 1104 с.

Катаев Михаил Юрьевич
Д-р техн. наук, профессор каф. автоматизированных систем управления (АСУ) ТУСУРа,
профессор Юргинского технологического института (филиала)
Национального исследовательского Томского политехнического университета
Тел.: 8-960-975-2785, (382-2) 70-15-36
Эл. почта: kataev.m@sibmail.com

Лукьянов Андрей Кириллович
Аспирант каф. АСУ ТУСУРа
Тел.: 8 (382-2) 70-15-36

Kataev M.Yu., Lukyanov A.K.
Retrieving of the total carbon dioxide by using an empirical orthogonal functions from satellite data

The article describes the method of empirical orthogonal functions and its modifications for the solution of recovery tasks of the total content of carbon dioxide in the real measured from satellite instrument GOSAT. The results of data processing model calculations of spectra of reflected from the surface solar radiation in the near infrared spectral range, as well as real satellite data for the station Lamont terrestrial network TCCON.
Keywords: Earth's atmosphere, gas composition, remote satellite methods, reflected from the surface solar radiation, Fourier spectrometer, empirical orthogonal functions.

УДК 004.724

А.И. Савельев, М.В. Прищепа

Архитектура обмена данными без потерь в пиринговом веб-приложении видеоконференц-связи

Поднимается проблема соединения клиентов и передачи аудио- и видеопотоков данных в пиринговых веб-приложениях видеоконференц-связи. При взаимодействии нескольких клиентских и серверной частей приложения видеоконференц-связи на основе протокола WebRTC возможна частичная или полная потеря «сигнальных» данных, препятствующая соединению клиентов. Предложенная архитектура передачи и хранения «сигнальных» данных на клиенте и сервере обеспечивает буферизацию и последующую обработку «сигнальных» данных, исключая их потерю и поддерживая взаимодействие между группами клиентов.

Ключевые слова: пиринговые соединения, peer-to-peer протоколы, видеоконференц-связь, веб-приложения, передача мультимедийных данных.

Анализ способов передачи данных в пиринговых веб-приложениях видеоконференц-связи. В настоящее время, несмотря на большие темпы развития интернет-технологий, существует множество проблем, связанных с потоковой передачей видео- и аудиоинформации. Во многом эти проблемы возникают по причине недостаточной пропускной способности каналов связи. Поскольку системы видеосвязи требуют больших сетевых ресурсов даже для передачи видео между двумя участниками, то поддержка многопользовательских видеоконференций является крайне затруднительной задачей.

Сейчас сотни тысяч пользователей могут одновременно использовать пиринговые (peer-to-peer (P2P)) сети [1, 2]. Обычной практикой в P2P-системах потокового видео на сегодняшний день является объединение участников, просматривающих один и тот же контент в «рой» (swarm), и перераспределение частей видеоконтента исключительно между участниками этого роя. Для такой канально-изолированной структуры P2P-видеосистем характерны задержки переключения каналов и отставание воспроизведения контента, связанные с оттоком абонентов канала и дисбалансом числа принимающих и ретранслирующих узлов. В целом глобальные P2P-сети с канально-изолированной структурой в настоящее время имеют серьезные проблемы с производительностью, которые будут становиться все более серьезными с ростом числа пользователей каналов.

Кроме того, в сетях потоковых систем P2P существуют проблемы, связанные с задержками каналов коммутации и низкой производительностью систем для каналов с небольшим числом участников. В работе [3] для решения этих проблем предлагается многоканальная потоковая P2P платформа View-Upload Decoupling (VUD), разделяющая выполняемые пользователем операции загрузки и просмотра данных, а также совместного использования ресурсов перекрестных каналов. За счет этого, обеспечиваются стабильность для многоканальных систем и качественное распределение ресурсов сети. Кроме того, для повышения производительности передачи данных учитывается географическое местоположение клиентов сети, и связь устанавливается между наиболее близко расположенными пользователями, имеющих необходимые данные.

В работе [4] представлена архитектура многопользовательской распределенной пиринговой системы видеоконференций, в которой предполагается, что каждый участник может создавать, отправлять и получать видеосигнал в любой момент времени, но во время видеоконференции участник передает либо видеосигнал, создаваемый его устройством, либо ретранслирует принимаемый видеосигнал другому участнику. Таким образом, участник, который посылает свой собственный видеосигнал, не может действовать в качестве промежуточного узла для прохождения видеосигнала от другого партнера. Данная распределенная архитектура может быть использована для реализации видеоконференций системы P2P, чтобы позволить каждому участнику видеть другого участника. Архитектура данной системы видеоконференц-связи P2P определяется на основе так называемой «цепи». Конфигурация цепи во время сеанса связи формируется на основе конфигурационных (служебных) сообщений, рассылаемых между приложениями видеоконференц-связи участников.

Для уменьшения объема данных, передаваемых в ходе видеоконференц-связи, в работе [5] используется автоматический способ определения текущего говорящего, и его потокам мультимедийных данных выставляется наибольший приоритет при передаче остальным участникам. Идентификация, диаризация дикторов, а также другие методы обработки речи и анализа лица человека широко применяются для автоматизации телекоммуникационных сервисов [6–8].

В работе [9] предложена «бессерверная» архитектура распределительного узла для передачи видео высокой четкости в многопользовательской системе видеоконференц-связи. В основе архитектуры заложен многопользовательский управляющий блок, интегрированный в клиентское приложение, который служит для установления множественных канальных соединений, кодирует и декодирует клиентские видеопотоки и распределяет видео другим участникам сеанса связи.

Производительность способов передачи потокового видео в P2P-сетях зависит также от конфигурации самой сети, ее топологии, неоднородности сетевых ресурсов абонентов, пропускной способности их каналов связи [10]. В отличие от совместной загрузки файлов, где малая пропускная способность канала просто приводит к медленной загрузке, при передаче потокового видео низкая скорость подключения становится настоящей проблемой. Также остаются актуальными вопросы компрессии видеосигнала, позволяющей снизить загруженность канала без значительного увеличения нагрузки на устройство конечного пользователя при кодировании/декодировании сигнала.

В работах [11, 12] представлены полученные авторами результаты предварительных исследований по сокращению передаваемого объема данных между пользователями в приложениях видеоконференц-связи. Описаны алгоритмы и программные средства, позволившие провести оптимизацию разработанного кроссплатформенного приложения видеоконференц-связи на этапах создания и удаления аудио- и видеопотоков данных, их передачи от сервера к клиенту и обратно, создания цепочек потоков и их поиска на сервере. В ходе исследований были выполнены упрощение клиентской части приложения и реорганизация структуры серверной части приложения.

На основе предложенных принципов оптимизации способов обмена мультимедийными данными в приложении видеоконференц-связи была разработана новая пиринговая архитектура прямой передачи аудио- и видеоданных между клиентскими частями, представленная в следующем разделе. Затем описан процесс формирования клиентских веб-страниц и установления связи с сервером по протоколу WebSocket. В последнем разделе обсуждаются разработанные алгоритмы установления соединений между клиентами с использованием протокола WebRTC.

Основные элементы разработанной пиринговой архитектуры взаимодействия модулей веб-приложения видеоконференц-связи. Разработанная архитектура, представленная на рис. 1, позволяет предотвратить потерю «сигнальных» данных при соединении трех и более участников видеоконференц-связи. Основными структурными элементами архитектуры являются: *1* – клиентская часть приложения; *2* – серверная часть приложения; *3* – блок протоколов передачи данных. Клиентская часть подразделяется на две независимые составляющие – устройство пользователя и веб-страница. Устройство пользователя в приложении необходимо для создания аудио- и видеопотоков с камеры и микрофона, подключенных или являющихся частью устройства.

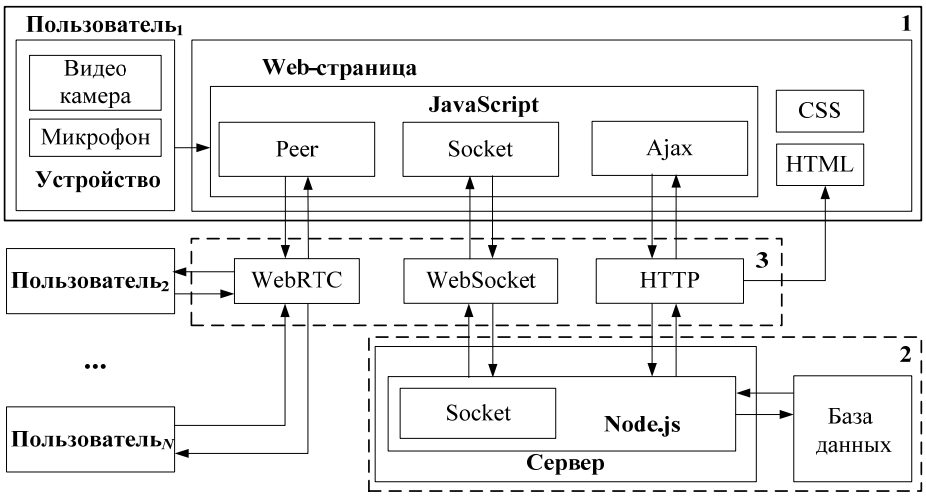


Рис. 1. Разработанная архитектура обмена данными в приложении видеоконференц-связи

Веб-страница клиентской части приложения состоит из классов, написанных на языке программирования JavaScript, необходимых для создания соединений с сервером и другими клиентами с помощью различных протоколов и обработки данных. Средства CSS и HTML служат для построения графического интерфейса, отображения данных и управления клиентской частью приложения. Средства JavaScript, использующиеся на веб-странице видеочата, включают в себя три различных типа инструкций, позволяющих организовать передачу данных по трем протоколам: WebRTC, WebSocket и HTTP. Также средства JavaScript служат для захвата и обработки потоков данных с микрофона и видеокамеры.

Следующим основным элементом архитектуры приложения является серверная часть, она выполняет несколько различных функций: формирование клиентской части приложения; регистрация клиента; авторизация клиента; обмен «сигнальными» данными между клиентами; создание комнат чата и работу с базой данных. Сам сервер работает на платформе Node.js, транслирующей JavaScript в машинный код, и имеет такую же асинхронную архитектуру, как и клиентская часть, разработанная средствами языка программирования JavaScript. База данных MongoDB, расположенная в серверной части приложения, имеет NoSQL-архитектуру, которая подходит для упрощения реализации серверной части. Взаимодействие с базой данных MongoDB происходит с помощью JavaScript и специальной библиотеки драйвера, предназначенной для этой базы данных.

Третий элемент архитектуры, представленной на рис. 1, состоит из протоколов – HTTP, WebSocket и WebRTC. Эти протоколы обеспечивают обмен данными на различных этапах работы приложения, с их помощью осуществляется создание соединения клиентских частей по протоколу WebRTC для передачи потоковых аудио- и видеоданных между ними. Существуют проблемы, возникающие при создании соединения, исходящие из асинхронной архитектуры приложения и протокола WebRTC, не предусматривающего стандартную реализацию соединения множества клиентов. Также необходимо отметить сложность процедуры установления связи между клиентами по протоколу WebRTC, требующую обмена «сигнальными» данными между ними и особого внимания при создании соединения.

В данной работе описано решение вышерассмотренной проблемы потери сигнальных данных при множественном соединении клиентов видеоконференц-связи с помощью внедрения новых алгоритмов взаимодействия клиентских и серверной частей и использования различных протоколов для организации обмена данными. Такая архитектура позволяет создать полноценное пиринговое приложение видеоконференц-связи, которое может работать в режиме группового чата. В следующем разделе рассмотрены основные протоколы и программные средства, использующиеся для создания клиентской веб-страницы и ее функционирования при проведении видеоконференции.

Процесс формирования клиентских веб-страниц и установления связи с сервером по протоколу WebSocket. Чтобы ясно представлять проблему потери «сигнальных» и предложенные в данном исследовании программно-алгоритмические решения данных, вначале рассмотрим основные этапы функционирования клиентской и серверной частей разработанного приложения видеоконференц-связи.

Клиентская часть приложения начинает работу с формирования веб-страницы регистрации или авторизации, позволяющих взаимодействовать клиенту с сервером посредством отправления или получения данных по HTTP-протоколу.

HTTP – это протокол прикладного уровня для передачи произвольных данных. Данный протокол используется в приложении для передачи клиенту графического интерфейса в виде html и css данных, логики клиентской части приложения, написанной на языке программирования JavaScript, а также для обмена данными клиента с сервером, при регистрации и авторизации клиента с помощью технологии Ajax, позволяющей обмениваться данными с сервером по протоколу HTTP без перезагрузки веб-страницы.

Авторизация клиента позволяет пользователю получить доступ к персональным данным и странице видеоконференц-связи. Для авторизации пользователь вводит данные в формы: логин и пароль. Затем происходит сбор данных из форм и отправка этих данных на сервер с помощью технологии Ajax. Далее сервер обрабатывает полученные данные: проверяет на соответствие определенному набору символов и на превышение максимального размера данных в запросе, выполняет поиск пары логин–пароль по базе данных. При успешном завершении всех операций сервер сформирует страницу видеоконференц-связи с пользовательскими данными и отправит ее по протоколу HTTP-клиенту. В случае несоответствия данных определенным требованиям или возникновения

ошибки сервер отправит клиенту информационное сообщение, способствующее устранению возникшей ситуации, используя протокол HTTP.

Регистрация клиента, так же как и авторизация, предполагает заполнение форм данными и их отправку на сервер по протоколу HTTP. Далее сервер обрабатывает данные, присланные клиентом. В случае положительного результата обработки сервер сохранит все полученные данные в базе данных, проведет в автоматическом режиме регистрацию клиента, сформирует и отправит ответ на запрос клиента в виде страницы видеоконференц-связи с пользовательскими данными. В случае ошибочных данных сервер вернет уведомление об ошибке клиенту по протоколу HTTP.

Таким образом, приложение использует HTTP-протокол для надежной передачи HTML, CSS и javascript данных между сервером и клиентом. Преимущество использования этого протокола в том, что он специально предназначен для передачи веб-страниц и их логики, а также хорошо поддерживается всеми существующими браузерами. Протокол HTTP имеет набор стандартных команд, среди которых есть две основные команды: «GET» и «POST», входящие в состав Ajax технологии, соответственно позволяющие осуществлять запросы на выдачу страниц к серверу и запрос на обмен различным типом данных между сервером и клиентом при авторизации или регистрации клиента.

После получения клиентом веб-страницы видеоконференц-связи средствами JavaScript, создается сокет на клиенте, который устанавливает соединение с сервером с помощью протокола WebSocket. WebSocket – это протокол полнодуплексной связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером в режиме реального времени. Протокол WebSocket открывает сокеты на клиенте и сервере, позволяющие обмениваться любыми типами данных. В случае успешного соединения по протоколу WebSocket сервер создаст у себя сокет с данными клиента и начнет его авторизацию: попытается получить http cookie данные клиента, которые хранят необходимую информацию для авторизации, произведет распаковку cookie данных, попытается загрузить из базы данных сессию, соответствующую данным из http cookie, по загруженной сессии определит пользователя, принадлежащего сессии, привяжет пользовательские данные к сокету, создаст уникальный номер для сокета, сгенерирует и отправит событие «connection» внутри сервера. Если одно из действий при авторизации сокета сгенерирует ошибку, то сокет на сервере будет автоматически отключен и удален, а клиентский сокет получит сообщение о разрыве соединения. Событие «connection», возникающее на сервере, привязывает к сокету, созданному на сервере – «слушателей» событий, посылаемых сокетом клиента. Сокет клиента еще при его создании формирует набор «слушателей» событий, посылаемых сокетом сервера. Таким образом, устанавливается связь между клиентом и сервером через протокол WebSocket, которая позволяет им быстро обмениваться сообщениями различного типа, не требующими их идентификации, так как для каждого вида сообщений существует отдельный «слушатель».

Данный протокол при построении архитектуры обмена данными позволяет достичь высокой скорости обмена информации и уменьшение нагрузки на клиента и сервер за счет отсутствия затрат на идентификацию данных. В разработанном приложении видеоконференц-связи протокол WebSocket играет важную роль – он занимается передачей «сигнальных» данных браузеров клиентов, которые позволяют создать соединение по протоколу WebRTC. Таким образом, данный протокол является основой для создания соединения по протоколу WebRTC и упрощает процесс передачи данных, необходимых для пирингового соединения.

Алгоритмы установления соединений между клиентами по протоколу WebRTC. После установления связи с сервером по протоколу WebSocket для совершения видеозвонков пользователю необходимо включить видеокамеру и микрофон и дать к ним доступ браузеру. Браузер, получивший доступ к камере и микрофону пользователя, используя средства JavaScript, сформирует медиапотоки данных с подключенных устройств. Полученные аудио- и видеопотоки можно будет передать по протоколу WebRTC между браузерами клиентов напрямую. WebRTC – интернет-протокол, предназначенный для организации передачи потоковых данных между браузерами или другими поддерживающими его приложениями по технологии точка–точка. Для соединения двух клиентов по протоколу WebRTC необходим следующий набор JavaScript инструкций: создание пира для каждого из клиентов, назначение одного из клиентов как «вызывающего», назначение другого клиента как «отвечающего», формирование «сигнальных» данных, обмен «сигнальными» данными, завершение установки соединения.

Для передачи «сигнальных» данных между клиентами используется сервер и протокол WebSocket. Ранее созданные сокеты в клиентской части приложения позволяют передавать «сигналь-

ные» данные по определенным каналам серверу, сервер в свою очередь транслирует эти данные другим клиентам, для которых они предназначены. Для соединения клиентов по протоколу WebRTC необходимо три типа данных: «call offer», «call answer» и «candidate». «Call offer» служит для инициализации сессии WebRTC, он формируется на одном из клиентов и с помощью WebSocket-протокола пересылается серверу, сервер в свою очередь передает данное сообщение «отвечающему» клиенту. «Call offer» имеет формат SDP (Session Description Protocol). Сообщение SDP, передаваемое от одного узла другому, может указывать: адреса места назначения, служащие для медиа-потоков мультикастинг-адресами, номера UDP портов для отправителя и получателя, медиа-форматы (например, кодеки), применяющиеся во время сессии, время старта и остановки. Сообщение SDP используется для широковещательных сессий, например телевизионных, радиопрограмм или видеоконференций. Клиент, получивший «call offer», сформирует и отправит ответ по протоколу WebSocket в виде данных «call answer», которые также имеют формат SDP. Как только клиент, отправлявший «call offer», получит SDP-сообщение типа «call answer», между клиентами начнется обмен данными типа «candidate» по протоколу WebSocket. Данные типа «candidate» имеют формат – ICE (Interactive Connectivity Establishment) Candidate. Создание интерактивного подключения (ICE) – это метод, используемый в компьютерных сетях, включающий в себя передачу сетевых адресов (NATs) в таких интернет-приложениях, как ip-телефония (VoIP), приложениях пиринговой передачи данных (peer-to-peer communications), видеоприложениях, системах мгновенного обмена сообщениями (instant messaging) и других интерактивных медиа-приложениях. Данные типа «candidate» используются для соединения клиентов, устанавливая путь между ними, по которому будут передаваться медиа-потоки. При успешном обмене данными типа «candidate» каждый из клиентов откроет канал для передачи различного типа данных по протоколу WebRTC, в том числе аудио- и видеопотоков.

Протокол WebRTC имеет особенности, которые создают сложности при соединении пользователей: для создания соединения между клиентами требуется выполнить операцию «handshake», которая состоит из обмена различным типом «сигнальных» данных между браузерами, но одновременно клиент может устанавливать только одно соединение по протоколу WebRTC.

Данная специфика протокола влечет за собой ряд проблем, при создании полноценной видеоконференц-связи. Проблемы возникают из-за асинхронной архитектуры приложения в ситуациях соединения одного клиента со множеством, множества с одним, множества со множеством. Такие ситуации приводят к нарушению алгоритма соединения – полной или частичной потере данных, требующихся для установления связи между клиентами. Чтобы решить сложившуюся проблему, было предложено несколько дополнительных подходов к построению архитектуры обмена данными в приложении: буферизация «сигнальных» данных протокола WebRTC на клиенте и сервере, объединение сокетов, соединяемых клиентов в «комнату» на сервере. «Комната» – это массив, находящийся на сервере, состоящий из нескольких сокетов, позволяющий обмениваться данными только с сокетами, находящимися в данном массиве. Таким образом, «комнаты» изолируют группы сокетов друг от друга, способствуя распространению данных только внутри определенных групп. Такие подходы помогают исключить потерю данных, позволяют создать все необходимые соединения между клиентами и управлять процессами соединения клиентов на различных этапах работы приложения. Далее рассмотрим алгоритмы, основанные на разработанных подходах, позволяющие создать соединение по протоколу WebRTC, контролировать обработку «сигнальных» данных, осуществлять буферизацию «сигнальных» данных и группировать сокеты клиентов в отдельные «комнаты».

Алгоритм, представленный на рис. 2, описывает этап соединения клиентов до формирования «сигнальных» данных. Сначала «вызывающий» клиент подает запрос на сервер для соединения с «отвечающим» клиентом по протоколу WebSocket. Далее сервер производит поиск «отвечающего» клиента среди подключенных. Если клиента нет, то сервер завершит звонок «вызывающего» клиента, если «отвечающий» клиент найден, то ему отправляется запрос на соединение по протоколу WebSocket. «Отвечающий» клиент формирует и отправляет ответ на запрос. Если ответ отрицательный, то сервер завершает звонок «вызывающего» клиента, в случае положительного ответа сервер получит id сокетов «вызывающего» и «отвечающего» клиентов, по id сокетов найдет «комнату», в которых сокеты находятся в данный момент. После завершения данного алгоритма происходит создание и обработка буферов сокетов на сервере посредством алгоритма, изображенного на рис. 3.

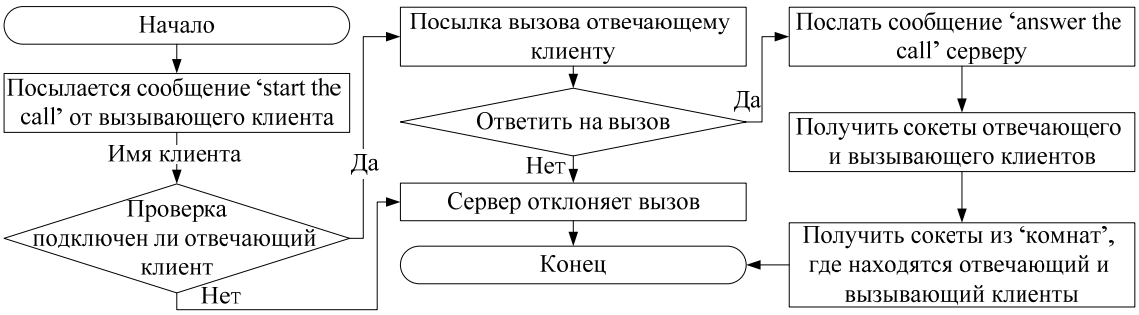


Рис. 2. Алгоритм подготовки клиентских частей перед формированием сигнальных данных

После того как «комната», где находятся сокеты каждого из клиентов, получены, начинает работать алгоритм, представленный на рис. 3. Сначала извлекается сокет из «комнаты» «отвечающего» клиента, для него создается буфер для хранения сокетов, ожидающих соединения по протоколу WebRTC. Затем сокет из «комнаты» «отвечающего» клиента добавляет в уже существующий буфер – сокет, взятый из «комнаты» «вызывающего» клиента. Если взятый сокет из «комнаты» «вызывающего» клиента был не последним, то операция извлечения сокета из «комнаты» «вызывающего» клиента и его добавление в буфер повторяется со следующим сокетом из этой комнаты. После того как будет взят последний сокет из «комнаты» «вызывающего» клиента, сокет из «комнаты» «отвечающего» клиента отсоединяется от своей «комнаты» и добавляется в «комнату» «вызывающего» клиента.

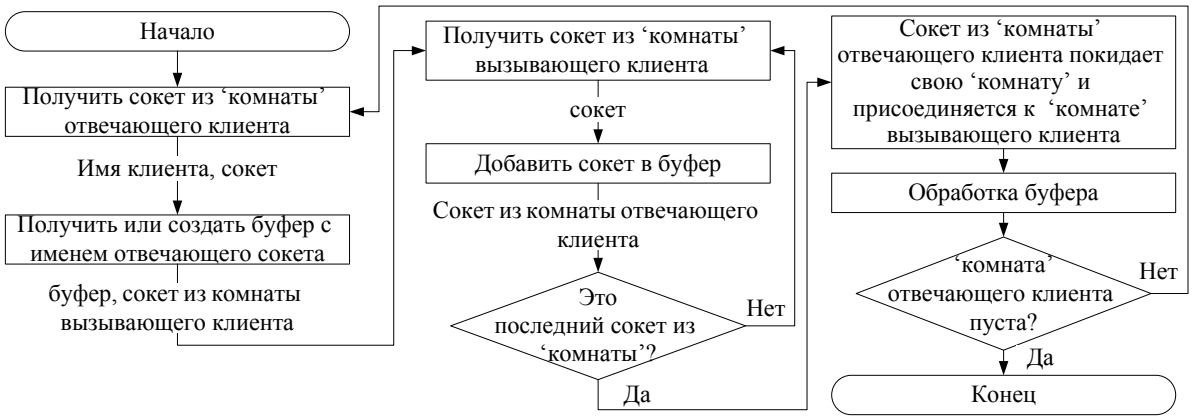


Рис. 3. Алгоритм распределения сокетов и обработки их буферов на сервере

Далее происходит вызов функции обработки буфера сокета, которая выполнит запрос на формирование сигнальных данных для всех клиентов, находящихся в очереди данного буфера. В конце алгоритма выполняется проверка на пустоту «комнаты» «отвечающего» клиента, если «комната» не пуста, то алгоритм повторит все действия с самого начала, в ином случае алгоритм считается завершенным. Как можно заметить, данный алгоритм добавляет в «комнату» «вызывающего» клиента клиентов из «комнаты» «отвечающего» клиента, и при каждом обращении к «комнате» «вызывающего» клиента в данном алгоритме «комната» должна увеличиваться. Но это не так по причине того, что перед началом алгоритма происходит дублирование всех пользователей из «комнаты» «вызывающего» клиента в отдельный массив, таким образом, алгоритм работает правильно, и каждый раз он использует не основную «комнату», а заранее подготовленный массив.

Алгоритм, представленный на рис. 4, является общим для обработки запросов от сервера на формирование сигнальных данных «call offer» или на обработку пришедших от другого клиента сигнальных данных «call answer». В клиентской части приложения видеоконференц-связи существует два отдельных буфера для каждого типа данных.

Приходящий запрос или «сигнальные» данные сначала добавляются в соответствующий им буфер. Затем происходит проверка обоих буферов, не обрабатывается ли один из них в данный момент. Если один из буферов занят обрабатывающей функцией, то алгоритм завершается, а новые данные в буфере будут обработаны позже. Если ни один из буферов не занят, они проверяются на

пустоту. В случае если оба буфера пусты, клиент по протоколу WebSocket отправит серверу уведомление, что он готов получать новые данные для установления соединения с другими клиентами. Если какой-то из буферов содержит данные, то будут извлечены первые в очереди данные и обработаны соответствующим образом для установления подключения. Как только подключение будет установлено, алгоритм продолжит свою работу с места опроса занятости буфера.

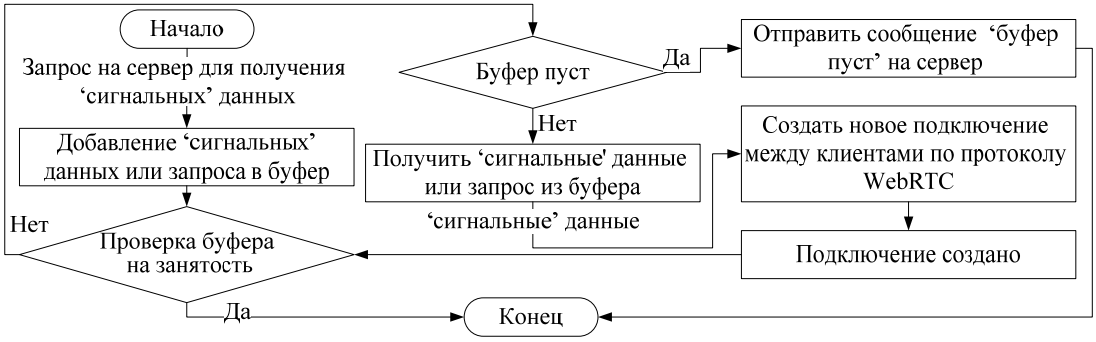


Рис. 4. Алгоритм работы с буфером данных на клиенте

Стоит отметить, что сигнальные данные типа «candidate» не имеют специальных буферов для их хранения ни на клиенте, ни на сервере, так как их обработка происходит сразу же, как только клиент их получит. Во время обработки «сигнальных» данных типа «candidate» буферы, принадлежащие данным типа «call answer» или «call offer», в зависимости от ситуации обработки продолжают быть заняты обрабатывающей функцией. Таким образом, остальные данные типа «call answer» или «call offer» продолжают добавляться в буферы, не нарушая алгоритма соединения клиентов по протоколу WebRTC.

Три приведенных выше алгоритма составляют одну из главных частей приложения, которая осуществляет создание видеоконференц-связи с другими пользователями посредством peer-to-peer протокола WebRTC. Алгоритмы позволяют контролировать асинхронную архитектуру клиентской и серверной частей приложения, осуществляя обработку данных по необходимости, препятствуя возникновению ситуаций перемешивания данных и прерывания выполняющихся соединений по протоколу WebRTC. Таким образом, в приложении достигается возможность создавать групповые видеоконференции и контролировать их состояние с помощью объединенных в «комнаты» клиентов на сервере.

Заключение. Предложенная архитектура обмена данными в приложении видеоконференц-связи позволяет распределить каналы передачи данными по соответствующим протоколам и разделить задачи между ними. Так как изначально архитектура приложения видеоконференцсвязи является асинхронной, то были выполнены разработка и внедрение новых алгоритмов по управлению данными, необходимых для соединения клиентских приложений по протоколу WebRTC. В итоге было получено полноценное приложение видеоконференц-связи, способное производить групповые звонки и контролировать состояние клиентов, связанных в общие группы – «комнаты» на сервере во время проведения группового чата.

Стоит отметить, что на данный момент существуют еще некоторые проблемы, ограничивающие использование протокола WebRTC на устройствах: 1) всего три браузера (Opera, Mozilla Firefox, Google Chrome) поддерживают данный протокол; 2) требуется наличие мощного процессора и достаточного количества памяти для обработки аудио- и видеопотоков данных. Кроме того, указанные браузеры не работают с графическими сопроцессорами, в результате нагружается основной процессор. Дальнейшие исследования будут направлены на упрощение способа передачи и улучшение обработки аудио- и видеоданных с использованием пиринговых связей для распределения нагрузки по обработке данных между клиентами.

Работа выполнена при частичной финансовой поддержке РФФИ (проект № 13-08-0741-а).

Литература

1. X. Hei, A measurement study of a large-scale P2P IPTV system / X. Hei, C. Liang, J. Liang et al. / IEEE Transactions on Multimedia, 2007.

2. Hei X. Inferring network-wide quality in P2P live streaming systems / X. Hei, J. Liang, Y. Liu, K.W. Ross / IEEE Journal on Selected Areas in Communications, 2007.

3. Di Wu. Redesigning multi-channel P2P live video systems with View-Upload Decoupling / Di Wu, C. Liang, Y. Liu, K.W. Ross / Computer Networks. – 2010, №54. – P. 2007–2018.

4. Civanlar M.R. et al. Peer-to-peer multipoint videoconferencing on the Internet // Signal Processing: Image Communication. – 2005, №20. – P.743–754.

5. Volfin I. Dominant speaker identification for multipoint videoconferencing / I. Volfin, I.l Cohen / Computer Speech and Language. – 2013. – Vol. 27. – P. 895–910

6. Ronzhin A. Speaker Turn Detection Based on Multimodal Situation Analysis / A. Ronzhin, V. Budkov // Springer International Publishing Switzerland. M. Zelezny et al. (Eds.): SPECOM–2013, LNAI 8113. – 2013. – P. 302–309.

7. Ronzhin A. PARAD-R: Speech Analysis Software for Meeting Support / A. Ronzhin, V. Budkov, I. Kipyatkova / In Proc. of the 9th International Conference on Information, Communications and Signal Processing ICICS-2013. Tainan, Taiwan. – 2013.

8. Ronzhin A. Context-Aware Mobile Applications for Communication in Intelligent Environment / A.L. Ronzhin, A.I. Saveliev, V.Yu. Budkov // Springer-Verlag Berlin Heidelberg, S. Andreev et al. (Eds.): NEW2AN/ruSMART–2012, LNCS 7469. – 2012. P. 307–315.

9. Meshcheryakov R.V. Dialogue as a basis for construction of speech systems / Meshcheryakov R.V., Bondarenko V.P. // Cybernetics and Systems Analysis. – 2008. – Т. 44. № 2. – С. 175–184.

10. Бондаренко В.П. Обработка речевых сигналов в задачах идентификации / В.П. Бондаренко, А.А. Конев, Р.В. Мещеряков / Изв. высш. учебных заведений. Физика. – 2006. – Т. 49, № 9. – С. 207.

11. Мещеряков Р.В. Структура систем синтеза и распознавания речи // Известия Томского политехнического университета. – 2009. – Т. 315, № 5. – С. 127–132.

12. Vishnu Monn. Software-based serverless endpoint video combiner architecture for high-definition multiparty video conferencing / Vishnu Monn Baskaran, Yoong Choon Chang, Jonathan Loo, KokSheik / Journal of Network and Computer Applications. – 2013. – Vol. 36. – P. 336–352.

13. Ramzan N. et al. Video streaming over P2P networks: Challenges and opportunities // Signal Processing: Image Communication. – 2012. – № 27. – P. 401–411.

14. Савельев А.И. Оптимизация алгоритмов распределения потоков мультимедийных данных между сервером и клиентом в приложениях видеоконференц-связи // Труды СПИИРАН. – 2013. – Вып. 31. – С. 61–79.

15. Ronzhin A.L. Context-Aware Mobile Applications for Communication in Intelligent Environment / A.L. Ronzhin, A.I. Saveliev, V.Yu. Budkov // Springer-Verlag Berlin Heidelberg, S. Andreev et al. (Eds.): NEW2AN/ruSMART. – 2012. – LNCS 7469. – P. 307–315.

Савельев Антон Игоревич
Мл. науч. сотр. лаборатории речевых и многомодальных интерфейсов
Санкт-Петербургского института информатики и автоматизации РАН (СПИИРАН)
Тел.: 8 (812) 328-70-81
Эл. почта: saveliev@iias.spb.su

Прищепа Мария Викторовна
Канд. техн. наук, науч. сотр. лаборатории речевых и многомодальных интерфейсов СПИИРАН
Тел.: 8 (812) 328-70-81
Эл. почта: prischepa@iias.spb.su

Saveliev A.I., Prischepa M.V.

Architecture of lossless data exchange in pear-to-pear web application of videoconference

The problem of client connection and audiovisual data transmission in pear-to-pear web application of videoconference are discussed. At the interaction of several clients and server parts of the videoconference application based on WebRTC protocol the partial or complete loss of signal data that hampers the client connection. The proposed architecture of data transmission and storage on client and server provides buffering and following processing of the signal data with the exception of their loss and support of interaction between client groups.

Keywords: peer-to-peer connection, peer-to-peer protocols, videoconferencing, web applications, media stream distribution.

УДК 681.322

С.В. Беззатеев, Н.В. Волошина, К.А. Жиданов

Система формирования фингерпринта статических изображений с использованием взвешенной метрики Хэмминга и модели взвешенного контейнера

Рассматривается алгоритм вычисления фингерпринта для статических изображений с учетом значимости различных областей (компонент, элементов) изображения с точки зрения влияния вносимых в них искажений на восприятие полученного в результате изображения – модели взвешенного контейнера. Алгоритм использует в качестве базового компонента помехоустойчивые коды, совершенные во взвешенной метрике Хэмминга.

Ключевые слова: фингерпринтинг, цифровой водяной знак, модель взвешенного контейнера, коды во взвешенной метрике Хэмминга, совершенные коды, защита авторских прав.

При распространении цифровых мультимедиа данных особо актуальной является задача защиты авторских прав на такую информацию (DRM – digital right management). Для решения этой задачи используют методы цифровых водяных знаков (DWM – digital watermarking) и цифровых фингерпринтов (DFP – digital fingerprinting) [1–5]. В первом случае для защиты в исходные мультимедиа-данные, например изображение, внедряется информация о владельце. Эта информация должна сохраняться при различных искажениях помеченного изображения, пока уровень его качества не упадет ниже некоторого порога. Второй подход подразумевает формирование некоторой дополнительной информации (фингерпринт) на базе исходного изображения с использованием специфических свойств изображения (например, опорных точек). Объем фингерпринта значительно меньше исходного изображения. Полученный фингерпринт используется для поиска копий изображений, незаконно распространяемых в сети. Метод построения фингерпринта должен обеспечивать его воспроизведение при различных искажениях исходного изображения до тех пор, пока они не достигнут определенного уровня.

Существенным различием этих методов является следующее.

При встраивании DWM часть мультимедиаданных меняется (например, метод LSB подразумевает изменения младших битов). А при построении DFP никаких изменений в исходный контейнер не вносится, а записывается только дополнительная информация об особенных свойствах изображения.

Встраиваемая при DWM-метка формируется пользователем и может иметь различный вид, по существу представляя собой некую информацию владельца. DFP получают на основе исходного изображения. Никаких пользовательских данных он не содержит.

В работе предлагается DRM метод, использующий оба подхода с использованием кодовых методов и модели взвешенного контейнера, позволяющий подготовить структуру исходного изображения (других мультимедийных данных) к дальнейшему формированию устойчивого цифрового фингерпринта, при условии внесения минимальных искажений в исходные данные.

Описание предлагаемого метода. Основными задачами любой системы DRM является построение такого метода получения (добавления) данных об авторе, который будет устойчивым к различного рода искажениям до определенного их уровня (например, сильные визуально заметные искажения), внося минимальные искажения либо совсем не внося их в исходные данные.

Метод DFP не вносит искажений. Он базируется на выделении специальных свойств (характеристик) исходных данных с дальнейшей их фиксацией. Проблема метода заключается в том, что для некоторого класса данных такие свойства, обладающие устойчивостью к искажениям, трудно найти. В то же время требование абсолютного отсутствия искажений для этих данных не является актуальным (например, фотореалистические изображения).

Для таких данных можно использовать методы DWM. В этом случае информация об авторе (метка) внедряется в исходные данные (например, в изображение), внося при этом некоторые иска-

жения. Однако из-за несогласованности метки и структуры изображения не всегда удается произвести внедрение с приемлемым уровнем искажений.

В статье предлагается метод построения DFP по свойству наличия в изображении кодовых слов (концепция F5 [3]), а при их отсутствии – создания этого свойства, т.е. внесения искажений методом DWM [1, 4, 5]. Рассмотрим суть метода на примере статических изображений. Исходное изображение или его часть преобразуется в битовый поток. Этот поток разделяется на блоки a длиной n. Эти блоки рассматриваются как кодовые слова c некоего кода C, искаженные вектором ошибок **e**. Если блок a является кодовым словом c кода C, то $e=0$ и синдром $s=0$, т.е. данный блок обладает требуемым свойством. Если $s\neq 0$, то блок не обладает требуемым свойством и для его создания необходимо исправить ошибки, т.е. произвести декодирование $a\Rightarrow c$. Если использовать совершенные коды, то задача получения $s=0$ для любого блока решается при внесении минимального числа ошибок [2], а следовательно, и искажений. Для минимизации вносимых искажений будем использовать несколько кодов, имеющих одинаковые параметры и построенных во взвешенной метрике Хэмминга. При таком подходе фингерпринтом будем считать полученную в результате декодирования последовательность кодов ($\lambda_1,\lambda_2,...\lambda_i,...$), кодовые слова $c_j\in C_i=\Gamma(L_{\lambda_i},G_{\lambda_i})$ которых являются наиболее близкими к построенным по исходному изображению блокам a_j; $\Gamma(L_{\lambda_i},G_{\lambda_i})$ – соответствующим образом выбранный код Гоппы во взвешенной метрике Хэмминга [6].

Следует отметить, что поскольку при таком подходе используются коды, исправляющие ошибки, согласованные с взвешенной метрикой Хэмминга, то и формируемые из битового потока блоки должны иметь взвешенную структуру. Подобная задача решается при построении взвешенного контейнера при реализации метода WDWM (взвешенного цифрового водяного знака) [1]. Для построения взвешенных блоков необходимо предварительно разделить исходные данные (например, изображение) на несколько зон. Деление производится исходя из степени влияния искажений, происходящих в зоне, на результирующее качество (например, воспринимаемое качество изображения, значение PSNR и т.д.). Таким образом, блоки a формируются посредством комбинирования частей из различных зон, найденных в процессе построения взвешенного контейнера.

Обобщенна схема метода построения взвешенного фингерпринта приведена на рис. 1.

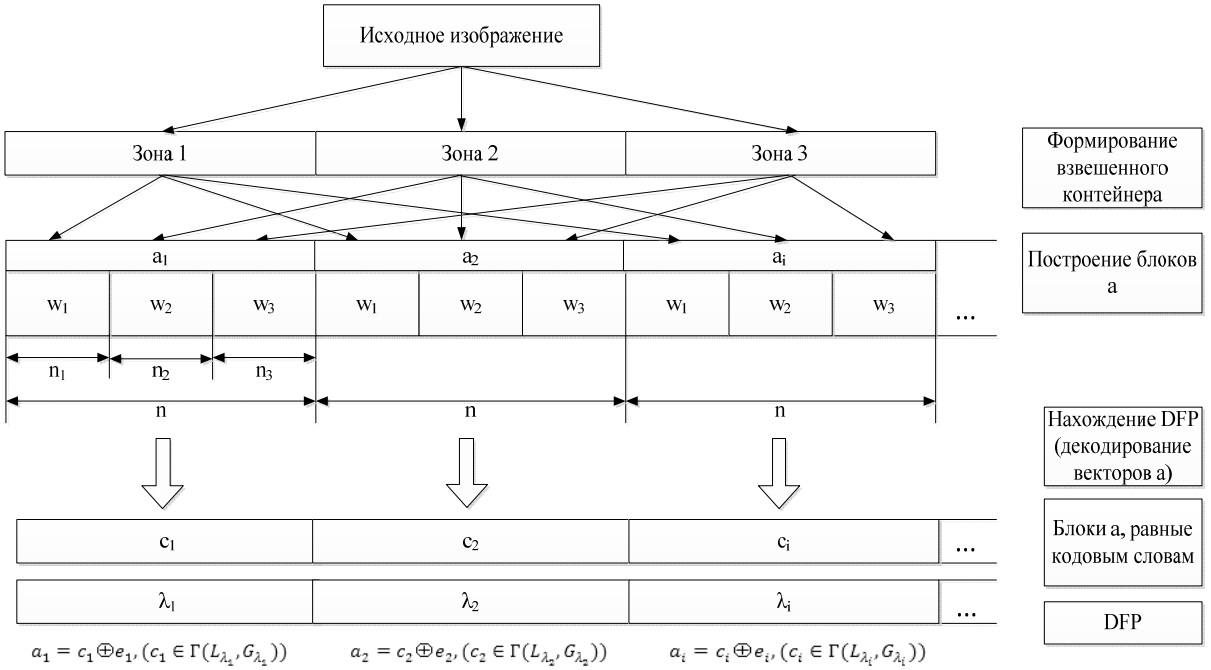


Рис. 1. Обобщенная схема построения взвешенного фингерпринта для контейнера с тремя зонами значимости

Коды во взвешенной метрике Хэмминга. Совершенные коды. Помехоустойчивые коды во взвешенной метрике Хэмминга [6] определяются следующим образом:

Длина кодового слова n задается набором длин $n_1, n_2, ..., n_l, n = \sum_{i=1}^{l} n_i$. Каждая позиция кодового слова $a = (a_1^1 a_2^1 \dots a_{n_1}^1 a_1^2 \dots a_{n_2}^2 \dots a_1^l \dots a_{n_l}^l)$ имеет свой вес ω_j. Будем считать, что эти веса упорядочены по возрастанию, т.е. $\omega_1 < \omega_2 < \dots \omega_j < \dots < \omega_l$. Вес слова a во взвешенной метрике Хэмминга определяется следующим образом:

$$wt_{WHM}(a) = \sum_{a_i^j \neq 0} \omega_j .$$

Очевидно, аналогичным образом определяется расстояние Хэмминга во взвешенной метрике Хэмминга между двумя векторами $\mathbf{a} = (a_1^1 a_2^1 \dots a_{n_1}^1 a_2^1 \dots a_{n_2}^2 \dots a_l^1 \dots a_{n_l}^1)$ и $\mathbf{b} = (b_1^1 b_2^1 \dots b_{n_1}^1 b_2^1 \dots b_{n_2}^2 \dots b_l^1 \dots b_{n_l}^1)$:

$$d_{WHM}(\mathbf{a}, \mathbf{b}) = \sum_{a_i^j \neq b_i^j} \omega_j .$$

Для двоичных кодов во взвешенной метрике Хэмминга, как и для кодов в обычной метрике, можно выписать границу Хэмминга, связывающую параметры кода n, M, d_{WHM}:

$$M \cdot W_n^{\tau} \leq 2^n,$$

где M – количество кодовых слов в коде (для двоичного линейного кода $M = 2^k$); W_n^{τ} – число векторов длины n в шаре радиуса τ во взвешенной метрике Хэмминга.

$$W_n^{\tau} = \sum_{\sum_{j=1}^{l} \tau_j \omega_j \leq \tau} \prod_{i=1}^{l} \binom{n_i}{\tau_i},$$

где $\tau = \dfrac{d_{WHM} - 1}{2}$.

Соответственно можно определить совершенный код, т.е. код, параметры которого лежат на этой границе. Для линейного двоичного кода это соотношение будет выглядеть следующим образом:

$$2^{n-k} = \sum_{\sum_{j=1}^{l} \tau_j \omega_j \leq \tau} \prod_{i=1}^{l} \binom{n_i}{\tau_i}.$$

Совершенные коды во взвешенной метрике Хэмминга могут быть построены с использованием хорошо известных методов построения оптимальных кодов (например, граница Варшамова-Гилберта). Однако такой метод построения является вычислительно трудоемким и главное не дает конструктивного метода декодирования построенных таким образом кодов. Использование специальных классов кодов Гоппы во взвешенной метрике Хэмминга позволяет решить обе эти задачи.

Специальный класс кодов Гоппы для взвешенной метрики Хэммига. Для построения кодов Гоппы, согласованных с взвешенной метрикой Хэмминга, используется конструкция обобщенных (L,G) кодов с нумераторами позиций различных степеней [6]. То есть $L = \left\{ \dfrac{v_i^j(x)}{u_i^j(x)} \right\}_{j=1,l;i=1,n_j}$, $v_i^j(x)$ – формальная производная соответствующего знаменателя $u_i^j(x)$, $\deg u_i^j(x) = \omega_j$ и $u_i^j(x)$ – многочлен, не приводимый над $F_{2^m}[x]$. Многочлен Гоппы для такого кода задается неприводимым многочленом

$$G(x), G(x) \in F_{2^m}[x], \deg G(x) = \tau \geq \omega_l, (G(x), u_i^l(x)) = 1, \forall i : i = 1, n_l .$$

Число различных кодов Гоппы из этого класса с одинаковыми параметрами (n, k, d_{WHM}) определяется числом различных неприводимых многочленов степени τ над $F_{2^m}[x]$.

Алгоритм вычисления фингерпринта на базе семейства кодов Гоппы, совершенных во взвешенной метрике Хэмминга $\Gamma_{WHM}(n,k,d)$. Опишем здесь простейший вариант алгоритма

вычисления фингерпринта для статических изображений, использующий различные по значимости области изображения и семейство кодов Гоппы, совершенных во взвешенной метрике Хэмминга.

Без потери общности будем рассматривать здесь статическое изображение, в котором определены три зоны значимости:

- Третья зона не предполагает внесения каких-либо искажений, т.е. $\omega_3 = \infty$.
- Вторая зона имеет относительный вес ω_2 вносимых искажений, равный 2.
- Первая зона позволяет вносить максимальное число искажений без существенных последствий для качества результирующего изображения и соответственно имеет минимальный относительный вес $\omega_1 = 1$.

Для такого изображения выберем семейство кодов Гоппы, совершенных во взвешенной метрике Хэмминга $\Gamma_{WHM}(n,k,d)$, со следующими параметрами:

$$n = n_1 + n_2 = 2^{2m-1} + 2^{m-1} - 1, n_1 = 2^m, n_2 = 2^{2m-1} - 2^{m-1} - 1, k = 2^{2m-1} + 2^{m-1} - 2m, d_{WHM} = 5.$$

Как указывалось в предыдущем разделе, число различных кодов в этом семействе определяется количеством неприводимых многочленов второй степени с коэффициентами из $GF(2^m)$:

$$I_{GF(2^m)}(2) = 2^{2m-1} - 2^{m-1}.$$

Очевидно, что, так как рассматриваемые коды совершенные, то любой вектор $\mathbf{a} = (a_1^1\ a_2^1 \ldots a_{n_1}^1\ a_1^2 \ldots a_{n_2}^2)$, полученный из изображения при разбиении его на зоны, может быть представлен во взвешенной метрике Хэмминга следующим образом:

$$(a_1^1\ a_2^1 \ldots a_{n_1}^1\ a_1^2 \ldots a_{n_2}^2) = (c_1^1\ c_2^1 \ldots c_{n_1}^1\ c_1^2 \ldots c_{n_2}^2)_i \oplus (e_1^1\ e_2^1 \ldots e_{n_1}^1\ e_1^2 \ldots e_{n_2}^2)_i,$$

где $(c_1^1\ c_2^1 \ldots c_{n_1}^1\ c_1^2 \ldots c_{n_2}^2)_i \in \Gamma(L_i, G_i), wt_{WHM}(e_1^1\ e_2^1 \ldots e_{n_1}^1\ e_1^2 \ldots e_{n_2}^2)_i = t_i \le 2$.

Таким образом, используя при декодировании вектора **a** различные $\Gamma(L_i, G_i)$ коды семейства $\Gamma_{WHM}(n,k,d)$, мы будем получать векторы ошибки с различными весами $0 \le t_i \le 2$.

Фингепринтом будем считать набор номеров $\lambda_1, \lambda_2, \ldots, \lambda_R$ кодов из семейства, соответствующих векторам, полученным из изображения при разбиении его на зоны следующим образом.

Вектору $\mathbf{a} = (a_1^1\ a_2^1 \ldots a_{n_1}^1\ a_1^2 \ldots a_{n_2}^2)$ поставим в соответствие наименьший номер λ такого $\Gamma(L_i, G_i)$ кода, для которого полученный при декодировании вектор ошибки $\mathbf{e} = (e_1^1\ e_2^1 \ldots e_{n_1}^1\ e_1^2 \ldots e_{n_2}^2)_i$ оказался наименьшего веса.

То есть $\lambda = \min_i i : wt_{WHM}(e_1^1\ e_2^1 \ldots e_{n_1}^1\ e_1^2 \ldots e_{n_2}^2)_i = \min_j wt_{WHM}(e_1^1\ e_2^1 \ldots e_{n_1}^1\ e_1^2 \ldots e_{n_2}^2)_j$.

Тогда алгоритм вычисления фингерпринта на базе семейства кодов $\Gamma(L_i, G_i)$ описывается следующим образом:

1. Изображение разбивается на зоны различной значимости.

2. В соответствии с разбиением изображения формируются блоки и выбираются подходящие параметры семейства кодов.

3. Фингерпринт $\lambda_1, \lambda_2, \ldots, \lambda_M$ формируется следующим образом:

Найденные векторы ошибок $\mathbf{e} = (e_1^1\ e_2^1 \ldots e_{n_1}^1\ e_1^2 \ldots e_{n_2}^2)_i$ исправляются, и соответственно блоки $\mathbf{a} = (a_1^1\ a_2^1 \ldots a_{n_1}^1\ a_1^2 \ldots a_{n_2}^2)$ исходного изображения преобразуются в кодовые слова кодов Гоппы из семейства $\Gamma_{WHM}(n,k,d)$. Например, первый блок превращается в кодовое слово $(c_1^1\ c_2^1 \ldots c_{n_1}^1\ c_1^2 \ldots c_{n_2}^2) \in \Gamma(L_{\lambda_1}, G_{\lambda_1})$. Согласно описанному ранее алгоритму получения номеров λ_i, искажения, вносимые при этом в исходное изображение, будут минимальны.

Проверка фингерпринта и его устойчивость к случайным и преднамеренным искажениям изображения. В соответствии с описанным алгоритмом создания фингерпринта $\lambda_1, \lambda_2, \ldots, \lambda_R$ в обработанном в результате получения фингерпринта изображении P имеется R блоков

$(c_1^1 c_2^1 \ldots c_{n_1}^1 c_1^2 \ldots c_{n_2}^2)_i \in \Gamma(L_{\lambda_i}, G_{\lambda_i}), i = 1,\ldots,R$. То есть каждый такой блок является кодовым словом соответствующего кода Гоппы из семейства $\Gamma_{WHM}(n,k,d)$. При проверке фингерпринта $\lambda_1,\lambda_2,\ldots,\lambda_R$ для изображения осуществляется декодирование блоков a с использованием $\Gamma(L_{\lambda_i}, G_{\lambda_i})$ кодов, соответствующих фингерпринту, и если для любого блока синдром $s = 0$, то фингерпринт считается соответствующим заданному, а изображение – равным P.

Наличие несущественных искажений изображения P может приводить к появлению ошибок в этих блоках. То есть будем считать, что в искаженном изображении P^* имеются блоки

$$(b_1^1 b_2^1 \ldots b_{n_1}^1 b_1^2 \ldots b_{n_2}^2)_i = (c_1^1 c_2^1 \ldots c_{n_1}^1 c_1^2 \ldots c_{n_2}^2)_i \oplus (e_1^1 e_2^1 \ldots e_{n_1}^1 e_1^2 \ldots e_{n_2}^2)_i = (\hat{c}_1^1 \hat{c}_2^1 \ldots \hat{c}_{n_1}^1 \hat{c}_1^2 \ldots \hat{c}_{n_2}^2)_i \oplus (\hat{e}_1^1 \hat{e}_2^1 \ldots \hat{e}_{n_1}^1 \hat{e}_1^2 \ldots \hat{e}_{n_2}^2)_i,$$

$$wt_{WHM}(\hat{e}_1^1 \hat{e}_2^1 \ldots \hat{e}_{n_1}^1 \hat{e}_1^2 \ldots \hat{e}_{n_2}^2)_i = wt_i \le 2,$$

$$(c_1^1 c_2^1 \ldots c_{n_1}^1 c_1^2 \ldots c_{n_2}^2)_i, (\hat{c}_1^1 \hat{c}_2^1 \ldots \hat{c}_{n_1}^1 \hat{c}_1^2 \ldots \hat{c}_{n_2}^2)_i \in \Gamma(L_{\lambda_i}, G_{\lambda_i}), i = 1,\ldots,R.$$

Используя фингерпринт $\lambda_1,\lambda_2,\ldots,\lambda_R$ и искаженное изображение P^*, легко найти соответствующий вектор ошибки $(\hat{e}_1^1 \hat{e}_2^1 \ldots \hat{e}_{n_1}^1 \hat{e}_1^2 \ldots \hat{e}_{n_2}^2)_i$ и соответствующий ему вес wt_i. Очевидно, что при небольших искажениях $(c_1^1 c_2^1 \ldots c_{n_1}^1 c_1^2 \ldots c_{n_2}^2)_i = (\hat{c}_1^1 \hat{c}_2^1 \ldots \hat{c}_{n_1}^1 \hat{c}_1^2 \ldots \hat{c}_{n_2}^2)_i$ и соответственно $(e_1^1 e_2^1 \ldots e_{n_1}^1 e_1^2 \ldots e_{n_2}^2)_i = (\hat{e}_1^1 \hat{e}_2^1 \ldots \hat{e}_{n_1}^1 \hat{e}_1^2 \ldots \hat{e}_{n_2}^2)_i$.

Определим теперь штрафную функцию $F = \sum_{i=1}^{R} wt_i \cdot f_{wt_i}$. В простейшем случае можно считать весовые коэффициенты $f_{wt_i} \in \{f_1, f_2\}$ штрафной функции одинаковыми и равными 1. Однако возможен и более гибкий вариант $f_1 \ne f_2$, учитывающий природу искажений и их влияние на восприятие результирующего изображения, т.е. его качество.

Принятие решения о наличии данного фингерпринта в имеющемся изображении P^* осуществляется по значению штрафной функции F и пороговым значениям B_1 и B_2, определяющим соответственно события «ложной тревоги» и «пропуска цели».

Заключение. Предложен новый метод вычисления фингерпринта, использующий особенности исходного контейнера, связанные с различной степенью его чувствительности к искажениям, вносимым в различных зонах контейнера. Для того чтобы воспользоваться таким свойством контейнера, предлагается применять для его описания взвешенную метрику Хэмминга в отличие от используемой в известных ранее схемах обычной метрики Хэмминга. Для эффективного использования такой метрики в работе предлагается брать семейство обобщенных кодов Гоппы, совершенных во взвешенной метрике Хэмминга. Благодаря использованию такого семейства кодов удается обеспечить внесение минимального числа искажений при создании фингерпринта. Кроме того, кодовые конструкции позволяют исправлять случайные искажения, возникающие при хранении или передаче контейнера. Открытым остается вопрос оптимального выбора коэффициентов в штрафной функции, обеспечивающих минимальные вероятности «ложной тревоги» и «пропуска цели» при принятии решения о наличии фингерпринта в анализируемом контейнере.

Работа выполнена при финансовой поддержке Минобрнауки РФ в рамках базовой части государственного задания СПбГУАП на 2014 год (проект № 2452).

Литература

1. Беззатеев С.В. Специальный класс кодов для стеганографических систем / С.В. Беззатеев, Н.В. Волошина, К.А. Жиданов // Доклады ТУСУРа. – 2012. – № 1 (25), ч. 2. – С. 112–118.

2. Neeta D. Implementation of LSB steganography and its evaluation for various bits / D. Neeta, K. Snehal, J. Daisy // Proc. of digital information management: 1st International conference. – India, 2006. – P. 173–178.

3. Westfeld A. F5–A steganographic algorithm high capacity despite better steganalysis / Information hiding. 4th International workshop. Lecture notes computer science. – 2001. – Vol. 2137. – P. 289–302.

4. Bezzateev S. Steganographic method on weighted container / S. Bezzateev, N. Voloshina, K. Zhidanov // Proc. of XIII Int. symposium on problems of redundancy in information and control system. – Saint-Petersburg, Russia, 2012. – P. 10– 12.

5. Anfinogenov S. Robust digital watermarking system for still images // S. Anfinogenov, V. Korshik, G. Morales-Luna // Proc. of Federated conference on computer science and information systems (FedCSIS). – Wrocław, Poland, 2012. – P. 85–689.

6. Беззатеев С.В. Двоичные обобщенные (L,G)-коды, совершенные во взвешенной метрике Хэмминга / С.В. Беззатеев, Н.А. Шехунова // Проблемы передачи информации. – 2012. – Т. 48, № 4. – С. 47–51.

Беззатеев Сергей Валентинович
Д-р техн. наук, зав. каф. технологий защиты информации
Санкт-Петербургского государственного университета аэрокосмического приборостроения (ГУАП)
Тел.: 8 (812) 494-70-52
Эл. почта: bsv@aanet.ru

Волошина Наталия Викторовна
Канд. техн. наук., доцент каф. технологий защиты информации ГУАП
Тел.: 8 (812) 494-70-52
Эл. почта: natali@vu.spb.ru

Жиданов Константин Александрович
Ассистент каф. технологий защиты информации ГУАП
Тел.: 8 (812) 494-70-52
Эл. почта: konstantin.zhidanov@gmail.com

Bezzateev S.V., Voloshina N.V., Zhidanov K.A.

The method of digital fingerprinting for static images based on weighted Hamming metric and on weighted container model

An algorithm of digital fingerprinting is proposed. The specific feature of this algorithm is that it takes into account different significance of different parts of the image according to their influence on the resulting image quality if any distortions have been occurred. The weighted container model is used for this purpose. This algorithm uses the ECC in weighted Hamming metric as a base approach.

Keywords: fingerprinting, digital watermarking, weighted container model, ECC in weighted Hamming metric, perfect codes, digital right management.

УДК 681.322.067

С.М. Гончаров, М.Е. Маркин

«Интерфейс мозг–компьютер» как нестандартная технология управления и передачи информации

Рассматривается использование «интерфейса мозг–компьютер» в качестве нестандартной технологии управления движущимися объектами, позволяющей отслеживать аутентичность источника сигналов в постоянном режиме. Описываются проведение эксперимента по управлению имитатором надводного судна, оптимальные способы обработки сигнала ЭЭГ, обучение классификатора. Предлагаются направления дальнейшего развития.

Ключевые слова: электроэнцефалография, ИМК, линейный дискриминантный анализ, воображаемое движение, визуально вызванные потенциалы, управление подвижными объектами, защита информации, биометрическая аутентификация.

Одним из методов защиты информации является использование нестандартных методов передачи информации. В данной работе в качестве такого нестандартного метода рассматривается технология «интерфейс мозг–компьютер». Вопросы аутентичности источника сигналов рассматриваются в других работах авторов [3].

В последнее время направление человеко-компьютерного взаимодействия (Human-Computer Interaction) значительно расширилось и включает в себя как уже привычные, так и весьма экзотические примеры. Одним из таких проявлений является интерфейс мозг–компьютер, или ИМК (Brain-Computer Interface, BCI), созданный для обмена информацией между мозгом и электронным устройством (например, компьютером). Первые исследования в этой области были проведены ещё в середине 70-х годов [1], и в настоящее время существует множество различных способов и областей применения интерфейса мозг–компьютер.

Принцип работы заключается в распознавании активности областей головного мозга. Разные области мозга отвечают за разные виды активности. Например, реакция на зрительные раздражители отражается в затылочной доле, а именно зрительной коре (visual cortex)[2]. Основываясь на активности зон мозга можно, так или иначе, интерпретировать получаемые данные.

Регистрация ЭЭГ производится специальными электродами. Каждый электрод подключен к усилителю. Для записи ЭЭГ может использоваться бумажная лента, или сигнал может преобразовываться с помощью АЦП и записываться в файл на компьютере (рис. 1).

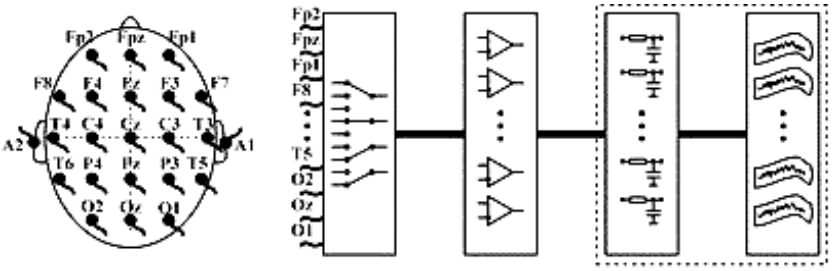


Рис. 1. Типичная схема энцефалографа (исследуемый объект и электроды – коммутатор – усилители – фильтры – регистрирующие устройства)

Однако, кроме регистрирующего энцефалографа, в составе интерфейса мозг–компьютер присутствуют и другие компоненты (рис. 2).

Применение, в силу своих особенностей, возможно весьма разнообразное – от набора текста на экране компьютера до управления сложными видами протезов.

Мгновенные данные ЭЭГ являются результатом многолетнего совершенствования, развития и обучения головного мозга человека. Поэтому снимки ЭЭГ во многом (за исключением некоторых полностью физиологических процессов) являются индивидуальными, в некоторой мере идентифицирующими характеристиками индивида.

Широкий спектр применения ИМК не мог не затронуть такую область ИБ как биометрические системы аутентификации [5]. Систему аутентификации по характеристикам сигналов мозга можно отнести к динамическому методу биометрической аутентификации. И хотя этот вид биометрической аутентификации не столь распространен, как, например, аутентификация по отпечатку пальца, исследования в этом направлении ведутся весьма обширные.

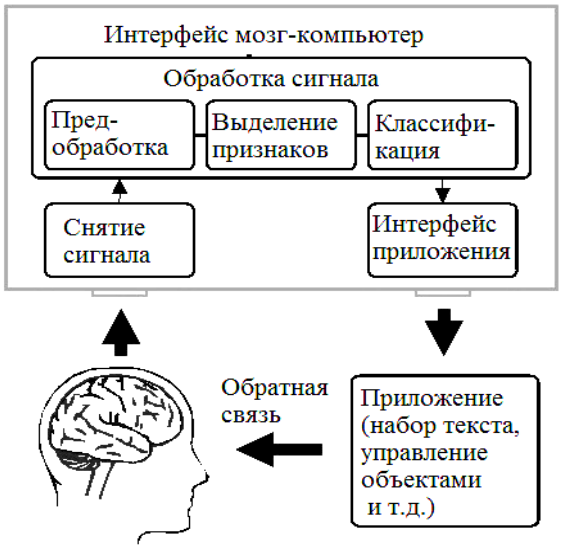


Рис. 2. Схема устройства ИМК

Основной проблемой в применении сигналов мозга для аутентификации является поиск и приведение этих сигналов в некоторый удобный или более статичный вид, поскольку они имеют особенность меняться под действием опыта. Кроме непосредственно биометрической аутентификации существует подход, предполагающий использование ИМК для парольной аутентификации. В этом случае ИМК используется как устройство ввода пароля вместо клавиатуры или другого иного способа. В таком применении ИМК имеет некоторые преимущества перед обычными методами ввода данных, например отсутствие акустического и оптического каналов утечки информации. Это объясняется отсутствием необходимости вводить информацию, которую можно неким образом подсмотреть либо подслушать.

Вообще обработанные сигналы с прибора снятия ЭЭГ можно использовать в качестве управляющих внутри некой программной среды. Следовательно, используя биологическую обратную связь, можно управлять практически любым техническим средством. Данное направление исследований весьма популярно в последнее время и развивается бурными темпами.

Существует несколько наиболее распространенных технологий управления объектами через интерфейс мозг–компьютер:

1) P300;

2) Motor Imagery;

3) SSVEP (Steady State Visually Evoked Potential).

P300 – реакция на единичный визуальный раздражитель, которая проявляется с задержкой в среднем 300 мс [4].

Motor Imagery – мыслительная активность, сопровождающая реальные или воображаемые движения конечностями.

SSVEP – реакция на зрительный раздражитель повторяющийся с частотой от 3,5 до 75 Гц, выраженная в электрической активности зрительной области мозга с той же или кратной частотой. Для снятия электрических потенциалов коры головного мозга в эксперименте используется периферийное устройство Emotiv Epoc с 14 электродами. В качестве программной среды выбрано свободно распространяемое ПО OpenViBE.

Схема эксперимента. В ходе эксперимента производилось управление имитатором надводного судна. В данной работе используется имитатор «ИС-2005» ЗАО «Инженерный центр информационных и управляющих систем». Имитатор предназначен для имитации сигналов приемника ГЛОНАСС/DGPS, лага, компаса и датчика положения руля для проверки и настройки современных

авторулевых. Имитатор моделирует: корпус судна (подводная и надводная части), гребной винт фиксированного и регулируемого шага, руль, главный двигатель судна (модель только по частоте вращения), рулевую машину постоянной или переменной производительности (с двумя насосами) со следящей системой; действующие возмущения (постоянный ветер, порывы ветра, двухмерное нерегулярное морское волнение, постоянное течение); датчики (лаг с NMEA-выходом, приемник ГЛОНАСС/DGPS с NMEA-выходом, компас с NMEA-выходом, датчик обратной связи руля и др.)

На вход имитатора подавались сигналы положения руля, сформированные в процессе работы интерфейса мозг–компьютер.

Работа интерфейса проходит в несколько последовательных этапов.

Этап 1. Подготовительный. Следует удостовериться в корректном расположении считывающего устройства, наличии соединения клиент-сервер в среде разработки. На этом этапе обеспечивается штатный режим снятия данных ЭЭГ и/или вносятся изменения в параметры сервера, указывается специальная информация (пол, возраст и т.д.).

Этап 2. Снятие первоначальных данных. Первоначальные данные необходимы для последующих выработки фильтра и тренировки классификатора. К данному этапу следует подойти ответственно и минимизировать факторы, отвлекающие и рассеивающие внимание пользователя, поскольку обучающая выборка с точки зрения классификатора всегда достоверна. Также этот этап может использоваться и для многократной тренировки самого пользователя интерфейса. Тренировка пользователя необходима для улучшения способности концентрироваться на текущем задании.

Этап 3. Выработка фильтра. Непосредственное участие пользователя не требуется. На этом этапе вырабатывается пространственный фильтр, использование которого позволяет увеличить качество принимаемого сигнала за счет использования других электродов, кроме непосредственно расположенных над рабочей областью головного мозга.

Этап 4. Обучение классификатора. На данном этапе также используются записанные ранее первоначальные данные. Классификатор, основанный на описанном выше методе линейного дискриминантного анализа, разделяет выборку на 2 класса.

Этап 5. Финальный. Интерфейс работает в режиме «реального времени». Данные снимаются периферийным устройством, фильтруются, обрабатываются классификатором, и в виде управляющих импульсов подаются на внешнее устройство.

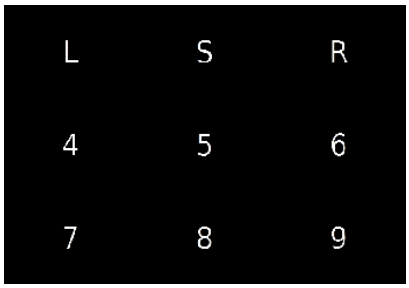


Рис. 3. Таблица символов для визуальной стимуляции

Снятие первоначальных данных. В то время как данные об активности головного мозга фиксируются периферийным устройством ЭЭГ, оператору представляется рабочее поле на мониторе, через которое осуществляется визуальная стимуляция. Оно представляет собой таблицу символов с попеременно подсвечивающимися строками и столбцами (рис. 3).

На стадии первоначального сбора данных предполагается фиксировать взгляд на символах из таблицы. Однако на стадии управления значимыми являются столбцы таблицы (правый отвечает за поворот вправо, левый – влево, центральный – за остановку). У вспышек, выделяющих строки и столбцы, фиксируется время, после которого во временном окне в 300 мс ожидается реакция на предъявленный стимул.

Данные, собранные на этом этапе, используются далее для формирования пространственного фильтра и классификатора.

Классификатор. Важным этапом работы интерфейса является обучение классификатора, который выделяет значимые раздражители на финальной стадии эксперимента.

Используемый классификатор представляет собой модуль, выполняющий множественное обучение по выделению единственного характеристического вектора из множества векторов и дальнейшей проверки этого вектора на обучаемом классификаторе. В качестве математического аппарата используется линейный дискриминантный анализ.

Линейный дискриминантный анализ (LDA) является алгоритмом классификации, который разделяет входное множество на два класса.

Пусть исходная выборка $\mathbf{X}$ разделяется на две подвыборки $\mathbf{X}^1$ и $\mathbf{X}^2$, где $\mathbf{X}^1$ – выборка, состоящая из n_1 векторов первого класса, $\mathbf{X}^2$ – выборка, состоящая из n_2 векторов второго класса. Пусть также (1) – центр первого класса, (2) – центр второго класса, (3) и (4) – несмещённая i-я координата векторов первого и второго класса соответственно.

Для дальнейших вычислений необходимо построить корреляционную матрицу **S**, которая определяет степень корреляции между различными координатами. Данная матрица разбивается на две части – $\mathbf{S}^1$ и $\mathbf{S}^2$, соответствующие двум классам:

$$\overline{\mathbf{X}}^1 = \frac{\sum_{i=1}^{n_1} \mathbf{x}_i^1}{n_1}, \tag{1}$$

$$\overline{\mathbf{X}}^2 = \frac{\sum_{i=1}^{n_2} \mathbf{x}_i^2}{n_2}, \tag{2}$$

$$\dot{\mathbf{X}}^1 = \mathbf{X}_i^1 - \overline{\mathbf{X}}_i^1,\ 1=1\ldots n, \tag{3}$$

$$\dot{\mathbf{X}}^2 = \mathbf{X}_i^2 - \overline{\mathbf{X}}_i^2,\ 1=1\ldots n, \tag{4}$$

$$S_{i,j}^1 = \frac{\dot{\mathbf{X}}_i^1 \dot{\mathbf{X}}_j^1}{n_1 - 1}, \tag{5}$$

$$S_{i,j}^2 = \frac{\dot{\mathbf{X}}_i^2 \dot{\mathbf{X}}_j^2}{n_2 - 1}, \tag{6}$$

$$\mathbf{S} = \mathbf{S}^1 + \mathbf{S}^2. \tag{7}$$

Результат классификации **y** на некотором входном векторе **x** вычисляется следующим образом:

$$\mathbf{y} = \left(\mathbf{x} - \frac{\overline{\mathbf{X}}_1 + \overline{\mathbf{X}}_2}{2} \right) \mathbf{S} \left(\overline{\mathbf{X}}_1 - \overline{\mathbf{X}}_2 \right). \tag{8}$$

Вектор **y** содержит действительные значения, причём если вектор **x** принадлежал первому классу, то выход будет положительным, а в противном случае – отрицательным.

Результаты. Результаты проведения эксперимента отражены на рис. 4.

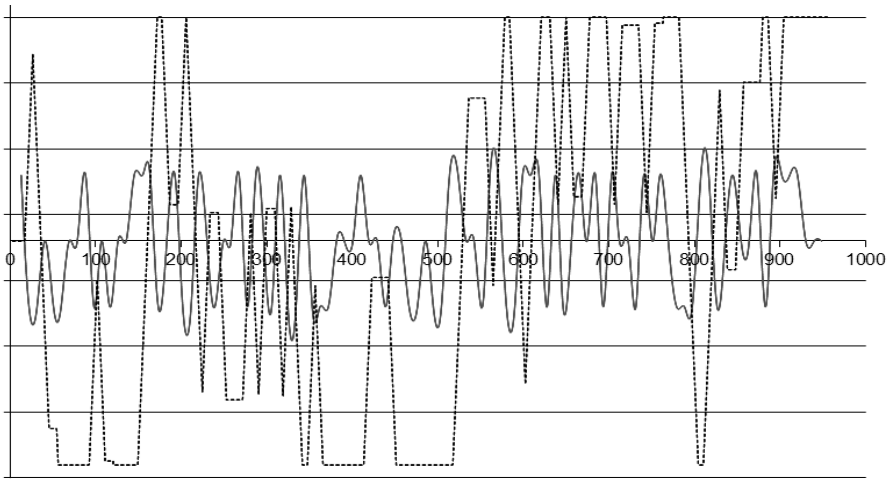


Рис. 4. Графики, демонстрирующие ход проведения эксперимента

Сплошной линией отмечено изменения угла положения руля по времени, пунктиром – сигналы, поступающие с выхода интерфейса (влево/стоп/вправо). И хотя достижимая точность распознавания удовлетворительна, а именно 78%, были выявлены некоторые недостатки. Как видно из графиков (см. рис. 4), сигнал на смену состояния руля приходит через фиксированные промежутки времени – это особенность выбранного метода генерации стимулов. Однако у данного метода есть потенциал развития, применительно к системам управления: возможно использование гораздо большего числа состояний, управление не только положением руля, но и другими показателями. Кроме того, предполагаемое в ближайшем времени использование методов классификации нейросетевыми алгоритмами позволит существенно увеличить точность распознавания действий [6].

Таким образом, на данном этапе развития применение этому комплексу может быть найдено в управлении некими вспомогательными системами, не требующими высокой точности действий. Отметим, что использование интерфейса мозг–компьютер в качестве побочного результата позволяет решать задачу аутентичности источника сигналов управления.

Литература

1. Vidal J. Real-Time Detection of Brain Events in EEG // Proceedings of the IEEE. – 1977. – Vol. 65, № 5. – P. 633–641.
2. Шмидт Р. Физиология человека / Р. Шмидт, Г. Тевс. – М.: Мир, 1996. – Ч. 3. – 323 с.
3. Вишняков М.С. Использование потенциалов коры головного мозга для парольной идентификации на основе технологии «ИМК» / М.С. Вишняков, М.Е. Маркин, С.М. Гончаров // Информация и безопасность. – 2012. – Т. 15, № 3. – С. 404–409.
4. Decety J. Brain structures participating in mental simulation of motor behavior: A neuropsychological interpretation / J. Decety, D.H. Ingvar // Acta Psychologica. – 1990. – Vol. 73. – P. 13–24.
5. Мещеряков Р.В. Биометрические методы идентификации / Р.В. Мещеряков, А.А. Шелупанов, В.П. Бондаренко // Известия Южного федерального университета. Технические науки. – 2003. – Т. 33, № 4. – С. 176–177.
6. Костюченко Е.Ю. Идентификация по биометрическим параметрам при использовании аппарата нейронных сетей / Е.Ю. Костюченко, Р.В. Мещеряков // Нейрокомпьютеры. – 2007. – № 7. – С. 39–50.

Гончаров Сергей Михайлович
Канд. физ.-мат. наук, доцент, зав. каф. безопасности информации и телекоммуникационных систем Морского государственного университета им. адм. Г.И. Невельского
(МГУ им. адм. Г.И. Невельского), Владивосток
Эл. почта: sgprim@smtp.ru, goncharov@msun.ru

Маркин Михаил Евгеньевич
Мл. науч. сотр. сектора информационной безопасности
НИИ морского транспорта МГУ им. адм. Г.И. Невельского
Тел.: +7-914-652-66-79
Эл. почта: markin_1941@mail.ru

Goncharov S.M., Markin M.E.
«Brain-computer interface» as new technology of control and information transfer

Researched the applying of brain-computer interface as new non-standart technology for control of moving object and information transfer. This technology allow to verify authenticity of signal source at every turn. Describes the experiment for control of marine surface vessel simulator, optimal ways for EEG data processing and training classifiers. Offered the directions for further research.
Keywords: Brain-Computer Interface, motor imagery visual evoked potentials, control of moving objects, information security, biometric authentication.

УДК 771.53

Н.Е. Проскуряков, С.Ю. Борзенкова, Е.Е. Евсеев, О.В. Чечуга

Современные технологии создания страховых фондов документации

Рассмотрены перспективные технологии создания страховых фондов документации в современных условиях. Определены основные технологии записи и воспроизведения бинарных данных с использованием микрофильма и штрихового кодирования. Приведены варианты оценки эффективности гибридных технологий микрофильмирования.
Ключевые слова: исходный электронный документ, микрофильм, методы записи и воспроизведении бинарных данных, сканирование, декодирование, штрих-код.

Задача создания страховых фондов документации. В настоящее время в России стремительными темпами растут объемы сканирования и оцифровки бумажной документации предприятий и организаций, библиотечных и архивных фондов. Утверждены различные государственные документы, концепции и программы, нацеленные на увеличение электронного документооборота. Практически во всех федеральных органах исполнительной власти и органах исполнительной власти субъектов Российской Федерации завершается переход на использование в своей деятельности электронных документов.

Вместе с тем часть документов, относящихся к особо ценным и особо важным, требует обеспечения их длительного и надежного хранения. Эта задача в настоящее время решается системой Единого российского страхового фонда документации (далее – ЕР СФД) с применением традиционного для этих целей носителя информации – микроформы. Ежегодно увеличивающийся объем электронных документов уже сегодня ставит перед системой ЕР СФД решение вопросов по разработке принципов и методов долговременного сохранения электронных массивов информации.

Положение о ЕР СФД, утвержденное Постановлением Правительства Российской Федерации от 26.12.1995 г. №1253-68, допускает фиксацию массивов конструкторской, технологической, проектной, нормативной, научной, историко-культурной и другой документации, относящейся к ЕР СФД, не только на микроформах, но и на других компактных носителях информации.

Как показали информационные исследования, проводимые регулярно на протяжении последних лет ФГУП «НИИ Репрографии» (г. Тула), в настоящее время для долгосрочного сохранения различных видов информации в ведущих зарубежных странах применяется два основных подхода – микрофильмирование и оцифровка [1].

Между сторонниками и противниками этих направлений ведутся горячие научные споры. Особую актуальность приобретает вопрос долгосрочного сохранения электронной информации.

Информационное страхование бумажных документов с помощью классических технологий оптического микрофильмирования, несмотря на некоторый спад объемов, по-прежнему продолжает осуществляться практически во всех странах. Но объективное возрастание в жизни общества роли электронного документооборота и стремительное нарастание объема документов, создаваемых, обрабатываемых и хранимых в электронной форме, диктуют необходимость развития новых подходов и технологических решений, таких как гибридные электронно-микрографические технологии.

Внедрение данных технологий в практику создания долговременно хранимых страховых информационных ресурсов происходит практически повсеместно. Преимущества электронного документооборота хорошо известны – это высокая оперативность поиска и доступа к документам, экономия времени и расходных материалов, возможность обмена документами по различным электронным каналам связи, снижение бюрократической волокиты и т.д.

Однако повсеместное внедрение электронного документооборота влечет за собой ряд серьезных проблем, важнейшей из которых является проблема долгосрочной сохранности электронных документов в целях их информационного страхования и архивирования. Без решения этого вопроса невозможно гарантировать сохранение и доступность для потомков цифрового интеллектуального, научного и культурного наследия цивилизации.

Возможности долгосрочного хранения электронных документов ограничены частой сменой поколений цифровых носителей и поддерживающих их аппаратно-программных платформ, которые склонны к быстрому устареванию и исчезновению. В поисках выхода из сложившейся ситуации мировым научным сообществом предлагаются различные варианты обеспечения длительности существования электронных документов в цифровой среде.

Самыми распространенными решениями являются миграция документов в новые программные среды и форматы, периодическая многократная перезапись на новые носители, а также эмуляция, т.е. имитация старой программной оболочки на новых операционных системах и оборудовании.

Однако оба данных подхода (миграция и эмуляция) принципиально не выходят за рамки цифровой среды, которая по самой своей природе достаточно динамична, изменчива и нестабильна. Для обеспечения постоянной миграции и эмуляции требуются большие финансовые, организационные и трудовые ресурсы. Кроме этого, проведенные эксперименты показали, что указанные процессы не обеспечивают защиты информации от потерь при частой перезаписи и переформатировании, т.е. не дают гарантии того, что она сохранится в неизменном оригинальном виде.

Поэтому в настоящее время ученые и специалисты обращаются к исследованию и разработке других, более надежных и экономичных стратегий архивирования важнейшей электронной информации с использованием таких технологий долговременного хранения, которые не требуют постоянного обновления и поддержки. И здесь на помощь человечеству снова приходит микрофильм, проверенный и испытанный аналоговый носитель, обладающий огромным потенциалом.

Разработка гибридных способов сохранения информации. В международном стандарте по микрографии долгосрочное сохранение цифровой информации определяется в широком смысле как «действия, необходимые для поддержания доступа к цифровым данным после отказа носителя или смены технологии». По сути, управление хранением цифровых данных состоит в управлении рисками утраты цифровой информации со временем.

Цель управления хранением – обеспечить долговечность цифровой информации в приемлемой форме и гарантировать ее целостность. Для достижения этой цели лучше всего подходит архивный микрофильм как технологически независимый носитель, обеспечивающий гарантированное хранение информации сроком до 500 лет, а также ее неизменность и устойчивость за счет минимального вмешательства в процесс хранения.

Но как совместить аналоговый носитель – микрофильм, и цифровое содержание электронных документов? Для этого в микрографии необходимо осуществить интеграцию цифровых и аналоговых технологий. Принципиальная возможность такой интеграции появилась в начале 70-х годов прошлого века с изобретением COM-систем – устройств, позволяющих экспонировать электронную текстовую и графическую цифровую информацию из компьютера на микроформы. Сейчас на современном мировом рынке насчитывается около 20 моделей COM-систем ведущих мировых производителей.

Эти системы различаются по принципу записи, типам микроформ, с которыми работают, форматам принимаемых исходных файлов и другим техническим характеристикам, однако все они способны записывать цифровую информацию из компьютера на пленочные носители. Последним достижением в производстве COM-систем стала разработка лазерной цветной системы, способной качественно и с высокой скоростью вести запись цифровой информации на цветной микрофильм.

При этом продолжают совершенствоваться и существующие, хорошо зарекомендовавшие себя на рынке COM-системы. Так, фирмой Microbox была представлена новая версия изделия Polycom, способная работать с электронными образами документов до формата А0 включительно и в связи с этим являющаяся наиболее пригодным аппаратом для создания СФД для различных отраслей промышленности.

COM-системы вместе со сканерами микрофильмов по праву можно назвать ключевым звеном современных электронно-микрографических технологий, своего рода мостом между цифровым и аналоговым мирами. Несколько лет назад несовершенства и недостатки отдельных моделей, а также общая увлеченность стремительным развитием технологий оцифровки дали повод некоторым ученым считать, что микрофильм как носитель безнадежно устаревает, а COM-системы необходимы только для локального применения при сохранении специфических видов электронных документов.

Однако неудачи различных стратегий долгосрочного цифрового сохранения заставили исследователей пересмотреть свои взгляды и снова обратиться к традиционному микрофильму, теперь уже

как к носителю для сохранения цифровой информации, долгосрочный и стабильный потенциал которого может быть усилен возможностями современных COM-систем.

COM-устройства коренным образом изменили способ создания архивных микрофильмов. Вместо использования для создания изображения оптической съемки эта технология считывает бинарные данные оцифрованного изображения и записывает положение каждого пикселя на пленку с помощью лазера (напрямую) или подобных устройств. Вариантом этой технологии являются записывающие устройства, способные переносить на микрофильм изображение с монитора – это стало возможным благодаря разработкам новых графических карт и специальных мониторов с очень высоким разрешением экрана. Современные COM-устройства могут принимать большую часть распространенных электронных текстовых и графических форматов, а новые аппараты позволяют улучшить качество вывода при работе с самыми различными оригинальными вводимыми изображениями.

Важная роль COM-систем в современном сохранении цифровых материалов подтверждается официальным принятием и введением в действие в 2009 г. международного стандарта ISO 11506 «Архивирование электронных данных. Компьютерный вывод на микрофильм (COM) и запись на оптический диск (COLD)». Данный стандарт впервые в мировой практике нормативно закрепляет стратегию долгосрочного архивного сохранения цифровой информации с помощью компьютерной записи на микрофильм для долгосрочного сохранения и на лазерный оптический диск для оперативного использования. Данный стандарт приобретен нашим институтом, переведен на русский язык и используется в работе.

В настоящее время в мире реализуется множество проектов сохранения цифровой информации с использованием COM-систем. Известно, что данные устройства широко применяются в библиотеке Конгресса США, различных отраслях Германии, Японии, Швеции, Франции и Великобритании и множестве других инновационных проектах по долгосрочному сохранению цифровой информации в ведущих странах мира.

Что касается России, то, по приблизительным подсчетам, в настоящее время в нашей стране находится в эксплуатации около 50 COM-систем различных типов и производителей. Основными потребителями этих устройств являются организации и учреждения, участвующие в создании и наполнении единого российского страхового фонда документации, а также другие организации, осознающие важность долгосрочного страхового сохранения своих информационных активов.

Российский рынок такого рода оборудования представляется достаточно развитым. На нем представлены практически все основные мировые производители COM-оборудования, включая «большую тройку» ведущих немецких компаний – SMA, Zeutschel и Microbox.

Российская наука не стоит в стороне от указанных проблем. Так, в нашей стране именно ФГУП «НИИ Репрографии» на протяжении последних лет в интересах национальной безопасности государства теоретически обосновывает, нормативно и методически закрепляет, а также внедряет современные гибридные электронно-микрографические технологии создания, сохранения и использования ЕР СФД, которые позволяют интегрировать традиционные (микрографические) и современные (электронные) способы создания страховых фондов документации различного назначения.

Данные гибридные технологии позволяют долгосрочно сохранять на микрофильме определенные виды цифровой информации, в частности текстовую, фотографическую и чертежно-графическую документацию, созданную как путем оцифровки бумажных оригиналов, так и непосредственно в ЭВМ. Исследования, проводимые в данной области, опираются на твердую государственную поддержку, высокую научную квалификацию сотрудников НИИ Репрографии, передовой зарубежный опыт и парк современного электронно-микрографического оборудования (COM-системы, сканеры микроформ), позволяющего проводить различные эксперименты, отрабатывать технологические схемы и моделировать цепочки взаимодействия новых устройств в условиях функционирования системы СФД. При этом сотрудниками НИИ Репрографии осуществляется регулярный мониторинг зарубежной информации по проблеме исследований, осуществляется ее сбор, накопление и анализ.

Благодаря COM-системам открываются новые возможности в области долгосрочного сохранения цифровой информации. Современные инновации в сфере COM-систем существенно расширяют сферу их применения.

Так, по результатам последних зарубежных исследований теоретически обоснован и экспериментально подтвержден новый подход к сохранению цифровой информации на микрофильмах. Идея такого подхода заключается в следующем.

Любой цифровой документ состоит из набора двоичных данных – битовой информации. Эта битовая информация может быть закодирована в виде двухмерного штрих-кода, состоящего из информационных точек, а далее представлена в виде двухмерного растрового изображения.

Изображение при помощи COM-системы сохраняется на микрофильме. При необходимости восстановления информации штрих-кодовые данные считываются с микрофильма сканирующим устройством, а затем декодируются, в результате чего происходит восстановление оригинального электронного документа.

Значение этой технологии заключается в том, что впервые появилась теоретически обоснованная и технологически реализуемая возможность долгосрочно сохранять на микрофильме любую цифровую информацию и документацию.

При этом тип электронного документа не имеет значения, так как все цифровые файлы состоят из набора двоичных данных и соответственно могут быть представлены в виде двухмерных графических штрих-кодов.

Помимо уже осуществляемого сохранения цифровой цветной и черно-белой чертежно-графической, текстовой и фотографической документации, применение данного метода открывает казавшиеся ранее невозможными перспективы сохранения на микрофильмах цифровой аудиовизуальной документации, программных продуктов, трехмерной документации CAD-приложений и др., т.е. любого типа цифровых данных.

Сейчас предлагаются различные варианты этого подхода, такие как гибридное хранение, т.е. совместная запись на микрофильм как самого оригинала изображения документа, так и его цифрового штрих-кода, использование цветного микрофильма, что позволит повысить объем записываемых кодированных данных благодаря использованию трех цветных слоев и т.д. Однако принципиальная схема технологии остается такой, как на рис. 1.

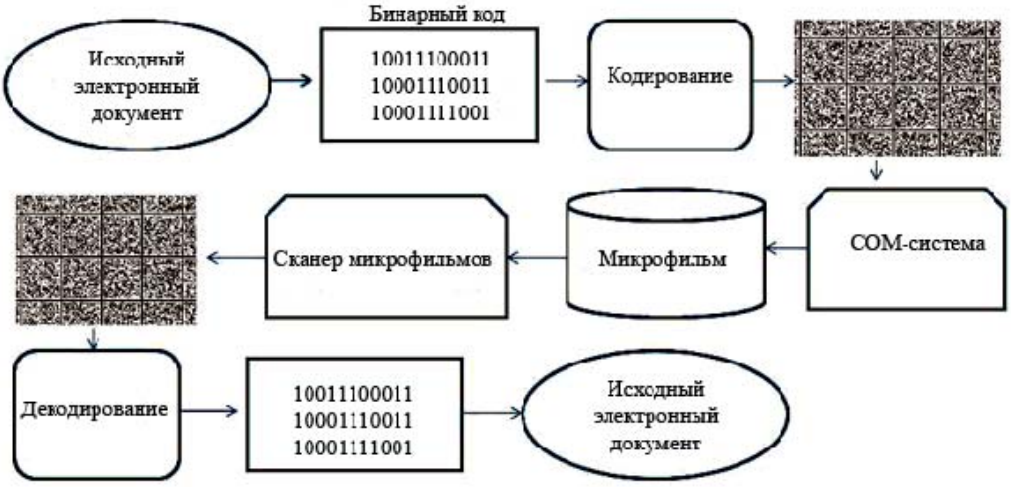


Рис. 1. Схема сохранения бинарной информации на микрофильме

Исходный цифровой документ любого типа с помощью программных алгоритмов представляется в виде двухмерного штрих-кодового растрового изображения, которое может восприниматься COM-системой. Затем данное изображение экспонируется COM-системой на микрофильм, который направляется на хранение. Далее с использованием сканера микрофильмов микрофильм сканируется, отсканированное штрих-кодовое изображение декодируется и происходит восстановление оригинального электронного документа (файла).

Необходимо заметить, что алгоритм кодирования / декодирования снабжен механизмом коррекции ошибок Рида–Соломона, аналогичным тому, который используется при записи / считывании оптических дисков, что повышает надежность считывания и декодирования штрих-кодовой информации.

Предлагается использовать для этих целей следующий вариант такого подхода. Хранение должно осуществляться гибридным способом, т.е. на микрофильм записываются как само аналоговое изображение, так и его цифровой код. По своей природе микрофильм позволяет считывать информацию и человеку, и машине, поэтому он может использоваться как гибридный носитель, сочетая аналоговую и цифровую информацию.

В качестве конкретного носителя предлагается цветной микрофильм производства Ilfochrome Micrographic [2]. Для хранения данных на цветной пленке есть свои основания, главное из которых заключается в том, что при хранении можно использовать все три цветовых слоя, благодаря чему увеличится объем сохраняемых данных. Двухмерный штрих-код, в который преобразовываются оригинальные документы, – это растровое изображение, в котором каждая растровая точка представляет собой состояние. Одна растровая точка служит бинарным описанием состояния (максимальная или минимальная оптическая плотность) или описанием состояния более высокого порядка (несколько уровней плотности).

По данным экспериментальных исследований, в которых для записи цветного микрофильма использовалась цветная лазерная COM-система нового поколения Archive Laser Recorder, была достигнута достаточно высокая плотность записи информации. Так, при размере точек 15 мкм на шестисотметровом рулоне цветной пленки 35 мм можно сохранить 22 гигабайта данных. При размере точки 12 мкм – 38 гигабайт. При 9 мкм – примерно 70 гигабайт на одном рулоне.

Кажется, что такой объем не составляет конкуренции таким носителям, как, например, жесткий диск. Но не стоит забывать, что при хранении цифровой информации вместимость не всегда является определяющим фактором, особенно по сравнению с долговечностью и стабильностью.

Однако такая технология является достаточно затратной, так как для записи требуются цветная пленка, цветной лазер (цветные COM-устройства) и химико-фотографическая обработка цветной пленки, что достаточно дорого. Сканирующее оборудование, необходимое для считывания цветной пленки, также является более сложным и дорогим, чем аналогичное оборудование для черно-белых материалов.

Соответственно если цвет решающего значения не имеет, рациональнее использовать черно-белый микрофильм. Тогда в качестве носителя используется обычный черно-белый микрофильм, а исходные электронные документы (их бинарные данные) кодируются с помощью двухмерного черно-белого графического штрих-кода. Затем эти данные трансформируются в изображение и сохраняются (экспонируются) на микропленку (рис. 2). При воспроизведении бинарных данных микрофильм сканируется, а изображение декодируется с помощью расшифровки отсканированного штрих-кода. В результате снова получается поток бинарных данных, из которых восстанавливается исходный электронный документ.

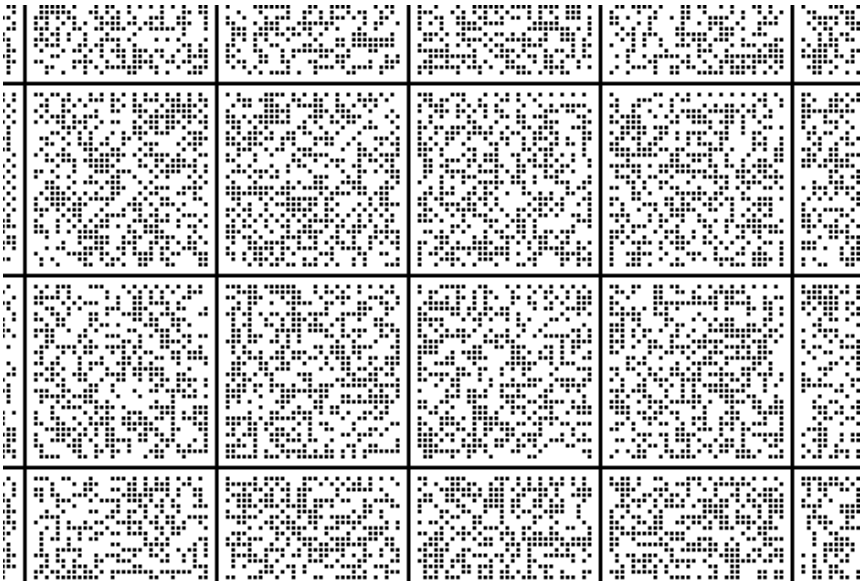


Рис. 2. Увеличенный фрагмент черно-белого штрих-кодового изображения

Черно-белые штрих-коды позволяют добиться относительно высокой плотности записи информации. Выяснилось, что на одном 16-мм микрофильме длиной 30,5 м в штрих-кодах можно сохранить 7200 изображений формата А4 или 45,32 мегабайт информации (на 35-мм микрофильме соответственно в 2 раза больше). В данном случае стоимость хранения 1 мегабайта составит $0,28, что в долгосрочной перспективе хранения представляется наиболее оптимальной по сравнению с дру-

гими системами, особенно в сравнении ее со стоимостью миграции каждые 5–7 лет, необходимой для других форматов, и стоимостью их технической поддержки.

Так, например, хранение на современных жестких дисках обходится 0,1…0,3 доллара за 1 гигабайт, но эти технологии требуют значительных затрат в процессе хранения, так как большое количество жестких дисков должно постоянно функционировать, чтобы поддерживать систему в рабочем состоянии. Это требует значительных затрат на электроэнергию, инфраструктуру и техобслуживание на протяжении относительно короткого срока службы.

К тому же в отличие от других носителей, таких как жесткие диски, флеш-карты, CD- или DVD-диски, технологии считывания микрофильма очень просты и универсальны. Тогда как для воспроизведения данных с популярных электронных носителей необходимы специализированные интерфейсы и сложные технологии (оптические диски с лазерной технологией, высокоточное расположение считывающих устройств для магнитных носителей, контролирующие программы и оборудование и т.д.), для считывания данных с микрофильма необходимы только простые оптические устройства. Это выгодно отличает данный носитель от IT-систем. Если найти в будущем устаревший привод для DVD или лент, или USB-порт, совместимый с новыми компьютерными системами, будет очень сложно, то для микрофильма будет достаточно любого современного оптического устройства для формирования изображения – это может быть сканер, камера или другой аппарат.

Заключение. На основе проведенных исследований можно сделать следующие выводы:

1) В свете последних достижений науки технологический потенциал микрофильма и COM-систем в деле долгосрочного сохранения цифровой информации представляется очень существенным. Разумеется, что новые технологии требуют совершенствования, исследований и экспериментов по подбору параметров записи, отработке режимов, синхронизации оборудования, оптимизации настроек элементов системы, технико-экономические расчетов и т.д. Однако первые шаги уже сделаны, и дальнейшие исследования возможности применения данного перспективного метода обязательно будут продолжены как за рубежом, так и в нашей стране.

2) Основными моментами, определяющими направления развития работ по информационному страхованию различных видов информации за рубежом, являются следующие:

– Рост тенденции архивирования цифровой информации на микрофильме.

– Снижение доли классического оптического микрофильмирования.

– Развитие технологий цветного микрофильмирования.

– Совершенствование возможностей и улучшение технических характеристик современного микрографического оборудования, такого как COM-системы и сканеры микроформ.

3) Сегодня специалисты ведущих стран мира опять обратились к апробированной технологии обработки и сохранения информации – микрографии; правда, это теперь существенно усовершенствованная и обогащенная новыми возможностями технология.

Литература

1. Мировой опыт создания и хранения информационных ресурсов в современных условиях / А.К. Талалаев, Е.Е. Евсеев, П.Е. Завалишин, Н.Е. Проскуряков // Изв. Тул. гос. ун-та. Технические науки. – 2013. – № 3. – С. 408–421.

2. Ilfochrome Micrographic Film [Электронный ресурс]. – Режим доступа: http://www.yumpu.com/et/document/view/549624/ilfochrome-micrographic-film, свободный (дата обращения: 07.04.2013).

Проскуряков Николай Евгеньевич
Д-р техн. наук, профессор каф. технологии полиграфического производства и защиты информации Тульского государственного университета (ТулГУ)
Тел.: 8 (487-2) 35-24-93
Эл. почта: tppzi@tsu.tula.ru

Борзенкова Светлана Юрьевна
Канд. техн. наук, доцент каф. технологии полиграфического производства и защиты информации ТулГУ
Тел.: 8 (487-2) 35-24-93
Эл. почта: tehnol_sb@tsu.tula.ru

Евсеев Евгений Евгеньевич
Канд. техн. наук, доцент, директор ФГУП НИИ Репрографии, Тула
Тел.: 8 (487-2) 56-97-27
Эл. почта: info@reprograf.ru

Чечуга Ольга Владимировна
Канд. техн. наук, доцент каф. технологии полиграфического производства и защиты информации ТулГУ
Тел.: 8 (487-2) 35-24-93
Эл. почта: sourie_1@mail.ru

Proskuryakov N.E., Borzenkova S.Y., Evseev E.E., Chechuga O.V.
The modern technology of insurance funds documentation

Promising technologies for creating documentation of insurance funds in modern conditions. The basic technology of recording and playback of binary data using microfilm and barcoding. Variants of evaluating the effectiveness of hybrid technology microfilming.
Keywords: original electronic document, microfilm, recording and playback methods of binary data, scanning, decoding, barcode.

УДК 519.25 ; 004.8

А.С. Романов, Р.В. Мещеряков, З.И. Резанова

Методика проверки однородности текста и выявления плагиата на основе метода опорных векторов и фильтра быстрой корреляции

Проведен анализ существующих средств и подходов поиска плагиата в тексте, обоснована необходимость дополнительной проверки текста на однородность. Приводятся описание и результаты работы методики проверки текста на однородность и выявления плагиата на основе кроссвалидации, одноклассового классификатора машины опорных векторов и фильтра быстрой корреляции для определения наиболее информативных признаков текста.
Ключевые слова: плагиат, однородность текста, быстрая корреляция, кроссвалидация, одноклассовая классификация, машина опорных векторов.

Типичная система для выявления плагиата [1] представляет собой программу, сравнивающую два текста на наличие общих подстрок и предполагающую использование базы данных возможных источников заимствований. В зависимости от расположения базы данных программы для выявления плагиата можно разделить на три группы [2]:

1. «Онлайновые» системы. Позволяют производить поиск оригинальных источников в сети Интернет благодаря интеграции с поисковыми системами.

2. «Оффлайновые» системы. Позволяют проводить поиск дубликатов в пределах локальной коллекции.

3. Универсальные. Позволяют формировать собственные коллекции текстов, проводить поиск в этих коллекциях, а также использовать сеть Интернет для поиска источников заимствований.

В случае если источник заимствования не найден, любая из трех описанных систем однозначно расценивает текст как оригинальный. Однако причиной этому может служить недостаточный объем базы данных, банальное отсутствие текстового слоя в документе-«доноре» и др. Поэтому всё чаще можно слышать о фактах публикации текстов, частично заимствованных из других источников, полного плагиата [3] и даже полностью искусственно сгенерированных текстов [4]. Выявление и пресечение подобных случаев является актуальной междисциплинарной практической задачей, затрагивающей области лингвистики, криминалистики, информационной безопасности, интеллектуального анализа данных и др.

Одним из способов повышения качества работы сервисов поиска плагиата и аналогичных систем в других областях нам видится добавление проверки текста на однородность: в случае если какой-либо из фрагментов явно отличается от общего авторского стиля текста, то велика вероятность того, что этот фрагмент заимствован из другого источника.

Для проведения таких проверок можно адаптировать уже известные методы идентификации автора текста [5]:

– использовать методы статистического анализа и теории информации: методы сжатия информации, проверку статистических гипотез о равенстве средних на основе критерия Стьюдента, критерий Колмогорова–Смирнова, меру Кульбака и хи-квадарт (на использовании последней меры основан алгоритм определения плагиата в работе [6]);

– использовать методы машинного обучения. При этом нужно интерпретировать задачу поиска неоднородностей как задачу одноклассовой классификации [7], а возможное заимствование определять путем обучения и тестирования на фрагментах текста методом кроссвалидации [8]. Другой вариант – заранее обучить несколько разных классификаторов, способных определять пол автора, возраст, образование, собственно стиль конкретного автора и т.д. Подавая на вход обученных моделей вектор признаков для отдельных фрагментов, можно, например, выявить в тексте с явно мужским стилем отдельные фрагменты, написанные женщиной; в тексте, соответствующем возрастной группе 18–25 лет, – группы предложений, характерные для пожилых людей, и т.д., как это делалось в работе [9];

– использовать специализированные методы, такие как, например, метод накопительных сумм (QSUM) [10–12]. Для проведения анализа выбирается пара характеристик, являющихся функциями предложения. Затем производится подсчет этих характеристик для каждого предложения и вычисляется среднее значение для всего текста. После считаются отклонения от средних значений для каждого предложения и строится накопительная сумма отклонений: начиная с нуля и затем последовательно прибавляя отклонения остальных предложений. Для каждой характеристики строится масштабированный график, на котором отображаются значения сумм для каждого этапа вычисления накопительной суммы. Графики однородного стиля должны практически совпадать. Неоднородный текст покажет их несовпадение. Главным преимуществом метода QSUM является то, что он дает отклонения хронологически, отображая их накопленную сумму. Основной недостаток метода – интерпретация полученных графиков. Для объективного вынесения решения об однородности текста можно использовать регрессионный анализ и методы машинного обучения, как это сделано в работе [2], – точность такого модифицированного метода доходит до 75% даже без тонкой настройки параметров, однако сильно зависит от позиции «вставки» и общего размера текста.

В данной работе предлагается комбинированная методика проверки однородности текста и выявления плагиата, включающая последовательное использование:

1) метода отбора информативных признаков, основанного на быстрой корреляции (FCBF);

2) метода машинного обучения машина опорных векторов (SVM).

Выбор информативных признаков текста. Как уже было сказано, ключевую роль в вопросе проверки однородности текста играет выбор признаков. Характеристика должна слабо контролироваться автором на сознательном уровне, быть устойчивой к изменению стиля внутри текстов одного и того же автора и быть способной статистически разделить двух и более авторов с заданной точностью. Сложность заключается как в выборе этих характеристик, так и в методике их сравнения.

Для отбора информативных признаков текста в работе используется метод многомерного отбора-FCBF (Fast Correlation-Based Filter) [13]. Метод начинает работать с полным множеством доступных для анализа признаков, использует меру симметричной неопределенности для определения зависимостей между признаками и позволяет найти подмножество, лучше всего описывающее данную предметную область, путем поиска и последовательного исключения малоинформативных признаков.

Мера симметричной неопределенности рассчитывается как

$$SU(X,Y)=2\left[\frac{H(X)-H(X|Y)}{H(X)+H(Y)}\right]=SU(Y,X),$$

где $H(X)$, $H(Y)$ – энтропии случайных величин, имеющих соответственно *i* и *j* состояний:

$$H(X)=-\sum_i P(x_i)\log_2(P(x_i)),$$

$H(X|Y)$ – условная энтропия:

$$H(X|Y)=-\sum_j P(y_j)\sum_i P(x_i|y_i)\log_2(P(x_i|y_j)),$$

$P(x_i)$, $P(y_i)$ – априорные вероятности для всех значений *X* и *Y*, $P(x_i|y_j)$ – апостериорная вероятность *X* при известных *Y*.

Значение *SU*, равное единице, свидетельствует о том, что, используя первый признак, можно точно предсказать значение второго, тогда как нулевое значение означает полную независимость признаков.

Пусть имеется набор данных *S*, состоящий из *C* классов и описывающийся *N* признаками. Для получения итогового подмножества признаков выполняются следующие действия:

1. Путем последовательного расчета меры для всех признаков и сравнения с заданным пороговым значением δ получают множество S' релевантных классу *C* признаков $\forall F_i \in S'$, $i=\overline{1,N}$, $SU_{i,c}>\delta$, где $SU_{i,c}$ обозначает корреляцию признака F_i и класса *C*.

2. Определение доминантных признаков таких, что для F_i ($F_i \in S$, $SU_{i,c}>\delta$) не существует $F_j \in S'$ ($j \neq i$), для которого $SU_{j,i}>SU_{i,c}$, где $SU_{j,i}$ – количественная оценка степени корреляции

признака F_i и других релевантных признаков из множества S'. Признак с самым большим значением $SU_{i,c}$ является доминантным признаком всегда.

3. Если найден F_j, для которого условие из п. 2 не выполняется, то считаем его избыточным по отношению к F_i. Обозначим S_{P_i} как множество, содержащее все возможные избыточные признаки по отношению к F_i.

4. Пусть $F_i \in S'$ и множество S_{P_i} не пустое. Разделим S_{P_i} на два класса: $S_{P_i}^{+} = \{F_j \mid F_j \in S_{P_i}, SU_{j,c} > SU_{i,c}\}$ и $S_{P_i}^{-} = \{F_j \mid F_j \in S_{P_i}, SU_{j,c} \le SU_{i,c}\}$.

5. Если $\left|S_{P_i}^{+}\right| = 0$, то F_i можно считать доминантным признаком, не продолжать поиск избыточных признаков для элементов множества $S_{P_i}^{-}$, а удалить их.

6. Если $\left|S_{P_i}^{+}\right| \neq 0$, то необходимо проверить его элементы: если среди них не найдено доминантных признаков, то следовать п. 5, иначе – удалить признак F_i, а решение относительно удаления признаков $S_{P_i}^{-}$ принимать на основе других признаков S'.

Проверка текста на однородность. Итоговый алгоритм проверки текста на однородность представлен на рис. 1.

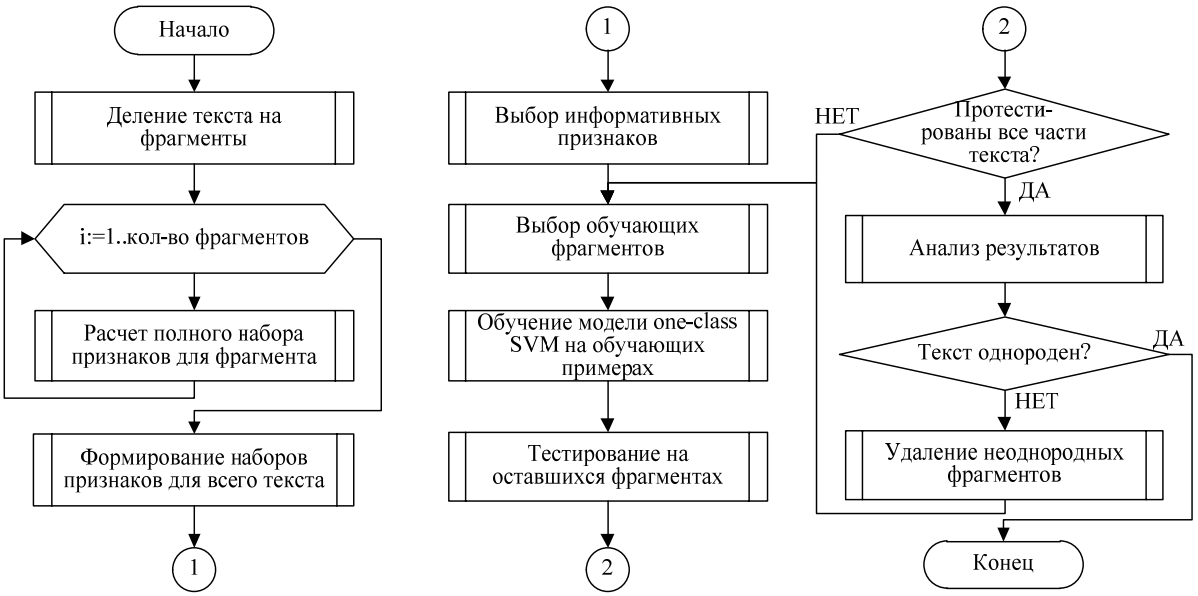


Рис. 1. Алгоритм проверки текста на однородность

Решение относительного того, отличается ли текст от общего авторского стиля, принимается классификатором на основе машины опорных векторов (SVM), показавшей отличные результаты при решении ряда смежных задач [14–16]. Однако учитывая специфику задачи, используется модификация метода – одноклассовый SVM и его реализация в libsvm [17], позволяющие проводить обучение только на основе примеров одного класса.

Для выделения неоднородных фрагментов из текста используется метод кроссвалидации – фрагменты текста делятся в определенной пропорции на обучающие и тестовые примеры, производится обучение классификатора и проверка, далее тестовая часть берется другая, после чего процедура повторяется. Найденные неоднородные фрагменты удаляются, и поиск начинается сначала. Критерием останова может служить, например, максимальная доля фрагментов, которые можно удалить из текста, или другая эвристика. Следует отметить, что метод не чувствителен к позиции «вставки» относительно начала текста.

При делении текста на фрагменты в случае, если в тексте присутствует явное членение на предложения, предпочтительно использовать их границы. Если границы предложения явно не

обозначены, используется набор слов между двумя знаками препинания, либо фрагменты фиксированной длины.

Экспериментальная часть. В исследовании использовались следующие корпуса текстов:

1) корпус прозаических текстов русских писателей XVIII–XX вв. (всего 215 текстов 50 авторов);

2) научные статьи по филологии, истории, праву, экономике и другим общественным и гуманитарным наукам, взятые из электронного архива журнала «Вестник Томского государственного университета» [18] (всего 500 текстов, написанных без соавторства).

Все тексты были предварительно размечены: в автоматическом режиме определены границы предложений и проведен морфологический анализ. Большие тексты были разбиты на более мелкие (по 100 предложений). Для имитации плагиата в каждый из полученных текстов было добавлено единым блоком от 1 до 10 предложений, взятых из текстов другого автора. Для корпуса статей, по возможности, дополнительно учитывалось научное направление. Всего было получено порядка 1000 таких примеров с заранее известными позициями и объемами вставок для каждого из корпусов.

В качестве сравниваемых характеристик использовались единицы символьного уровня текста, элементы грамматики, идиосинкразические и специальные признаки текста, в том числе:

– признаки, предложенные Мортоном: длина предложения (в словах) и комбинация слов, начинающихся с гласной буквы, и коротких слов из двух-четырех букв;

– наборы биграмм и триграмм символов, разделенные по частотному признаку;

– наборы слов и сочетаний слов, разделенные по частотному признаку;

– грамматические классы слов и сочетания грамматических классов;

– словари соответствующих научных дисциплин;

– словари мужских и женских признаков текста и др.

Для оценки качества работы метода использовалась *F*-мера, представляющая собой гармоническое среднее между точностью *P* и полнотой классификации *R*:

$$F = 2\frac{P \cdot R}{P + R},$$

Полученные результаты приведены в таблице.

Результаты экспериментов

Корпус	Объем «вставки»									
	1	2	3	4	5	6	7	8	9	10
Произведения русских авторов XVIII–XX вв., %	64	75	89	85	85	84	79	80	82	78
Статьи по общественным и гуманитарным наукам, %	55	70	76	73	73	77	68	67	73	65

Более точные результаты для первого корпуса можно объяснить тем, что писатели обладают ярко выраженным авторским стилем, поэтому вставка «чужеродного» текста может быть обнаружена сравнительно легко. Данный вывод подтверждается предыдущими результатами исследований [5] и экспертами-лингвистами. В корпусе научных статей авторский инвариант выражен в меньшей степени. Свои особенности накладывают также лексические, морфологические и синтаксические особенности научного стиля. В целом следует отметить достаточно высокие результаты для обоих корпусов, из которых следует, что предложенный подход является перспективным и требует более тщательной проверки.

Заключение. В данной статье рассмотрена важная междисциплинарная практическая задача – выявление неоднородных фрагментов в тексте и плагиата. Обоснована необходимость использования методов проверки текста на однородность авторского стиля наряду с классическими алгоритмами текстового поиска. Предложена методика поиска неоднородных фрагментов в тексте, основанная на использовании кроссвалидации и одноклассовой классификации методом машины опорных векторов. Выбор информативных критериев предлагается делать автоматически на основе фильтра быстрой корреляции. Полученные экспериментальные результаты позволяют сделать вывод о достаточно высокой точности работы метода и перспективности предложенного подхода для решения поставленной задачи.

Полученные результаты не являются окончательными для данной работы. Мы планируем базироваться на них в своих будущих исследованиях. Как возможные направления развития темы рассматриваются следующие задачи:

1. Расширение корпуса научных статей и апробация методики на статьях, относящихся к естественным и техническим наукам.

2. Создание специального корпуса, объединяющего тексты, в которых вставка инородных предложений производится человеком осмысленно с учетом жанра, темы, контекста и прочих особенностей конкретного текста: как реальные примеры плагиата, так и специальные тексты, подготовленные экспертами. Апробация методики на этом корпусе.

3. Экспертная лингвистическая оценка полученных результатов и усовершенствование методики за счет добавления полученной дополнительной информации.

4. Полная автоматизация предложенного подхода и создание автоматизированной системы для проверки текста на однородность и определения плагиата.

Литература

1. Дягилев В.В. Архитектура сервиса определения плагиата, исключающая возможность нарушения авторских прав / В.В. Дягилев, А.А. Цхай, С.В. Бутаков // Вестник НГУ. Сер.: Информационные технологии. – 2011. – Т. 9, вып. 3. – С. 23–29.

2. Романов А.С. Модификация метода накопительных сумм для проверки однородности текста и выявления плагиата // Электронные средства и системы управления: матер. докл. IX Междунар. науч.-практ. конф. (30–31 октября 2013 г.): в 2 ч. – Ч. 2. – Томск: В-Спектр, 2013. – С. 30–38.

3. Экспертизы. Вольное сетевое сообщество «Диссернет» [Электронный ресурс]. – Режим доступа: http://www.dissernet.org/expertise, свободный (дата обращения: 19.04.2014).

4. Шумская А.О. Выбор параметров для идентификации искусственно созданных текстов // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2013. – № 2 (28). – С. 126–128.

5. Романов А.С. Разработка и исследование математических моделей, методик и программных средств информационных процессов при идентификации автора текста / А.С. Романов, А.А. Шелупанов, Р.В. Мещеряков. – Томск: В-Спектр, 2011. – 188 с.

6. Седов А.В. Анализ неоднородностей в тексте на основе последовательностей частей речи [Электронный ресурс] / А.В. Седов, А.А. Рогов // Современные проблемы науки и образования. – 2013. – № 1. – Режим доступа: www.science-education.ru/107-8339, свободный.

7. Stein B. Intrinsic plagiarism analysis with meta learning / B. Stein, S. Meyer zu Eissen [Электронный ресурс]. – Режим доступа: http://www.uni-weimar.de/medien/webis/research/events/pan-07/pan07-papers-final/stein07-intrinsic-plagiarism-analysis-with-meta-learning.pdf, свободный (дата обращения: 19.04.2014).

8. Воронцов К.В. Комбинаторный подход к оценке качества обучаемых алгоритмов // Математические вопросы кибернетики. – М.: Физматлит, 2004. – Т. 13. – С. 5–36.

9. Mechti S. A framework for plagiarism detection based on author profiling / S. Mechti, M. Jaoua, H. Belghith // Notebook for PAN at CLEF 2013 [Электронный ресурс]. – Режим доступа: http://www.clef-initiative.eu/documents/71612/c7a0e432-dd82-46b1-ab9e-5d0dd98c3a8d, свободный (дата обращения: 19.04.2014).

10. Morton A.Q. Literary Detection: How to prove authorship and fraud in literature and documents. – New York : Scribner's, 1978. – 221 p.

11. Farringdon J.M. Analyzing for authorship / J.M. Farringdon with contributions by A.Q. Morton, M.G. Farringdon, M.D. Baker. – Cardiff : University of Wales Press, 1996. – 324 p.

12. Holmes D. Forensic stylometry: A review of the qsum controversy / D. Holmes, F.J. Tweedie // Revue informatique et statistique dans les sciences humanies. – 1995. – № 31. – P. 19–47.

13. Yu L. Feature Selection for High-Dimensional Data: A Fast Correlation-Based Filter Solution / L. Yu, H. Liu // Proceedings of The Twentieth International Conference on Machine Leaning (ICML-03). – 2003. – P. 856–863.

14. Романов А.С. Идентификация автора текста с помощью аппарата опорных векторов / А.С. Романов, Р.В. Мещеряков // Компьютерная лингвистика и интеллектуальные технологии: матер. ежегод. междунар. конф. «Диалог–2009» (Бекасово, 27–31 мая 2009 г.). – М.: РГГУ, 2009. – Вып. 8 (15). – С. 432–437.

15. Романов А.С. Идентификация авторства коротких текстов методами машинного обучения / А.С. Романов, Р.В. Мещеряков // Компьютерная лингвистика и интеллектуальные технологии: по

матер. ежегод. междунар. конф. «Диалог» (Бекасово, 26–30 мая 2010 г.). – М.: Изд-во РГГУ, 2010. – Вып. 9 (16). – С. 407–413.

16. Романов А.С. Определение пола автора короткого электронного сообщения / А.С. Романов, Р.В. Мещеряков // Компьютерная лингвистика и интеллектуальные технологии: матер. ежегод. Междунар. конф. «Диалог» (Бекасово, 25 – 29 мая 2011 г.). – М.: Изд-во РГГУ, 2011. – Вып. 10 (17). – С. 620–626.

17. Chang C.-C. LIBSVM: a library for support vector machines / C.-C. Chang, C.-J. Lin // ACM Transactions on Intelligent Systems and Technology [Электронный ресурс]. – 2011. – Режим доступа: http://www.csie.ntu.edu.tw/~cjlin/papers/libsvm.pdf, свободный (дата обращения: 19.04.2014).

18. Резанова З.И. Задачи авторской атрибуции текста в аспекте гендерной принадлежности (к проблеме междисциплинарного взаимодействия лингвистики и информатики) / З.И. Резанова, А.С. Романов, Р.В. Мещеряков // Вестник Том. гос. ун-та. – 2013. – № 370. – С. 24–28.

19. Давыдова Е.М. Модель образовательного процесса с учетом требований работодателя // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2013. – № 4 (30). – С. 177–181.

Романов Александр Сергеевич
Канд. техн. наук, доцент каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: alexx.romanov@gmail.com

Мещеряков Роман Валерьевич
Д-р техн. наук, профессор каф. КИБЭВС ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: mrv@ieee.org

Резанова Зоя Ивановна
Д-р фил. наук, зав. каф. общего, славяно-русского языкознания и классической филологии
Национального исследовательского Томского государственного университета,
профессор каф. русского языка и литературы
Национального исследовательского Томского политехнического университета
Тел.: 8 (382-2) 52-67-89
Эл. почта: resso@rambler.ru

Romanov A.S., Meshcheryakov R.V., Rezanova Z.I.

Plagiarism detection and text homogeneity checking technique based on one-class support machine and fast correlation-based filter

The article provides an analysis of the existing tools and approaches for identifying text plagiarism, justifying the need for additional verification of the text homogeneity. The article presents the description and results of the technique for the purpose of determining the plagiarism in the text, based on cross-validation, one-class SVM classifier and fast correlation-based filter.

Keywords: plagiarism, text homogeneity, fast correlation based filter, cross-validation, one-class classification, support vector machine.

УДК 519.688:622.276

В.Л. Сергеев, К.С. Гаврилов

Адаптивная идентификация и интерпретация нестационарных газодинамических исследований скважин газовых и газоконденсатных месторождений

Рассматриваются модели и алгоритмы адаптивной идентификации и интерпретации результатов газодинамических исследований скважин газовых и газоконденсатных месторождений на неустановившихся режимах фильтрации на основе интегрированной системы моделей кривой восстановления давления с учетом дополнительной априорной информации. Приводятся результаты анализа качества алгоритмов идентификации и интерпретации кривой восстановления давления скважин газового месторождения.

Ключевые слова: идентификация, адаптация, интерпретация, газодинамические исследования скважин, кривая восстановления давления, интегрированные системы моделей, априорная информация, газовые и газоконденсатные месторождения.

Нестационарные гидродинамические исследования (ГДИ) скважин по кривой восстановления давления (КВД) являются наиболее информативным методом определения параметров пластов нефтяных и газовых месторождений, на основании которых осуществляются процессы добычи нефти, составляются технологические проекты разработки месторождений, создаются геолого-технологические модели процессов нефтегазодобычи.

Особенностью КВД полученных в результате заранее спланированных ГДИ газовых скважин (рис. 1) является достаточно быстрый, в пределах одного часа, процесс восстановления забойного давления и далее медленных рост забойного давления до пластового в пределах от 30 мин до 20–50 ч. Причем большая часть КВД однородно-пористого пласта представляет линейную зависимость квадрата забойного давления от логарифма времени.

На способе выделения прямолинейного участка КВД с использованием при необходимости производной забойного давления основан широко используемый в нефтегазовых компаниях метод обработки результатов исследований [1]. Аналогичный метод реализован в зарубежных программах PanSystem, Saphir. Следует отметить, что недостатком традиционных методов интерпретации КВД [1–3] является их затратный характер, поскольку обработка результатов производится после завершения заранее спланированных по времени проведения исследований, что связано с простоями скважин и значительной потерей добычи газа.

В настоящее время в связи с возможностью получения информации в режиме реального времени стационарными информационными измерительными системами требуется иная технология, позволяющая определять фильтрационные параметры и энергетическое состояние залежей в процессе гидродинамических исследований, не планируя заранее время их завершения.

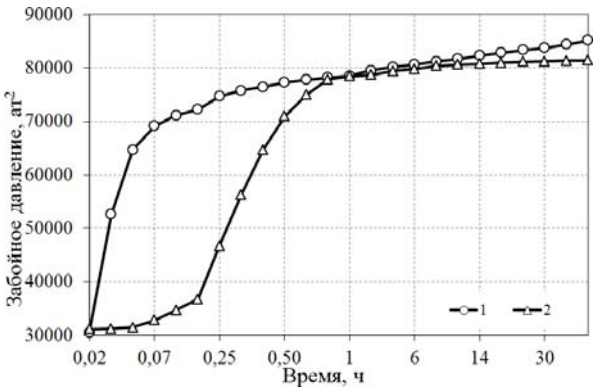


Рис. 1. Кривая восстановления давления скважин № 1046, № 1054

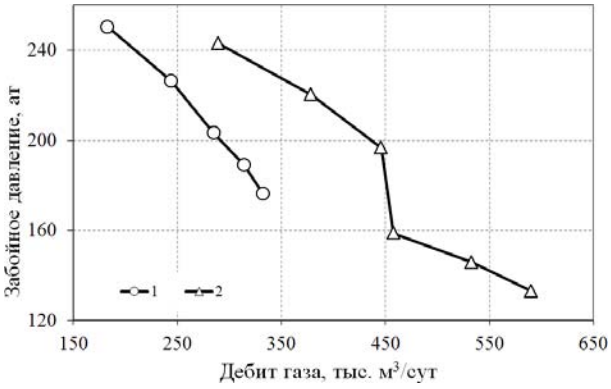


Рис. 2. Индикаторные кривые скважин № 1046, № 1054

В данной работе на основе технологии адаптивной идентификации [4, 5] рассматриваются модели и алгоритмы интерпретации КВД газовых скважин, позволяющие определять параметры пластов и время завершения исследований в процессе получения данных о забойном давлении.

Модели и алгоритмы адаптивной идентификации и интерпретации. Решение задачи адаптивной идентификации и интерпретации КВД рассмотрим на примере определения параметров однородно-пористого нефтяного пласта представленной моделью [1]

$$P_з^2 = \alpha_1 + \alpha_2 \lg(t), \quad \alpha_1 = P_{з0}^2 + \alpha_2 \lg(\frac{2{,}25\chi}{r_{с,пр}^2}) + bq_0^2, \quad \alpha_2 = \frac{2{,}3q_0\mu T_{пл} z\rho}{2\pi khT_c}, \quad \chi = kP_{пл}/m\mu_{пл}, \qquad (1)$$

где $P_з(t)$, $P_з(t_0) = P_{з0}$ – текущее и начальное перед остановкой скважины забойные давления; q_0 – дебит скважины в момент ее остановки t_0; m – пористость; h – эффективная мощность пласта; χ –коэффициент пьезопроводности; $r_{с,пр}^2$ – приведенный радиус скважины; $z_г$ – коэффициент сверхсжимаемости газа при пластовом давлении и пластовой температуре $T_{пл}$ ($T_с = 293$ K); ρ – атмосферное давление; k – проницаемость пласта; $P_{пл}$ – пластовое давление; μ – вязкость газа в пластовых условиях; b – параметр модели индикаторной кривой.

$$P_з^2 = P_{пл}^2 - aq - bq^2. \qquad (2)$$

При использовании модели (1), технологии интегрированных моделей и метода адаптивной интерпретации [4–6] оценки параметров пласта – проводимости $\sigma = kh/\mu$, пьезопроводности χ и пластового давления $P_{пл}$ в моменты времени t_k, $k = 1,2,3,...$, рассчитываются по формулам:

$$\sigma^*(t_k, u_k^*) = \frac{42{,}4\, q_0 \rho T_{пл} z_г}{\alpha_2^*(t_k, u_k^*) T_с}, \qquad (3)$$

$$\chi^*(t_k, u_k^*) = 0{,}445\, r_c^2 \exp(\frac{\alpha_1^*(t_k, u_k^*) - P_{з0}^2 - b^* q_0^2}{\alpha_2^*(t_k, u_k^*)}), \qquad (4)$$

$$P_{пл}^*(t_k, u_k^*) = \sqrt{\alpha_1^*(t_k, u_k^*) + \alpha_2^*(t_k, u_k^*)\lg(t_p)}, \; u_k^* = (\omega^*, h^*, \bar{z}_k), \qquad (5)$$

где $\alpha^*(t_k, u_k^*) = (\alpha_1^*(t_k u_k^*,), \alpha_2^*(t_k, u_k^*))$ – оптимальные оценки параметров модели КВД (1), управляющих параметров $\omega^*(t_k) = (\omega_1^*(t_k), \omega_2^*(t_k), \omega_3^*(t_k))$ и параметра h^*, полученные путем решения трех оптимизационных задач:

$$\alpha^*(t_k, \omega, \bar{z}_k) = \arg\min_{\alpha} \Phi(\alpha(t_k), \omega(t_k), h(t_k), \bar{z}_k), \qquad (6)$$

$$\omega^*(t_k) = \arg\min_{\omega} J(\alpha^*(t_k, \omega), W((t_k - t_{k-i}/h))), \qquad (7)$$

$$h^*(t_k) = \arg\min_{h} JK(\alpha^*(t_k, \omega_k^*), W((t_k - t_{k-i}/h))). \qquad (8)$$

Здесь запись $\arg\min_x f(x)$ означает точку минимума x^* функции $f(x)$ ($f(x^*) = \min_x f(x)$); Φ – показатель качества интегрированной системы моделей КВД с учетом экспертных оценок гидропроводности, пьезопроводности и пластового давления $\bar{z}_k = (\bar{\sigma}_k, \bar{\chi}_k, \bar{P}_{пл,k})$, известных к моменту времени t_k [4]; $W((t_k - t_{k-i}/h)$ – весовая функция с параметром h для обеспечения процесса адаптивной интерпретации [5, 6]; J, JK – показатели качества модели КВД (1) для определения оценок управляющих параметров $\omega^*(t_k) = (\omega_1^*(t_k), \omega_2^*(t_k), \omega_3^*(t_k))$ и параметра $h^*(t_k)$; t_p – экспертная оценка времени восстановления забойного давления до пластового; b^* – оценка параметра модели индикаторной кривой (2).

Момент времени завершения исследований t_k^* может быть определен по критерию стабилизации оценок $\alpha^*(t_k, u_k^*)$ [5, 6]:

$$\left|\alpha_j^*(t_{k-i},u_k^*)-\alpha_j^*(t_k,u_k^*))/\alpha_j^*(t_k,u_k^*)\right|\le\varepsilon_j,\ j=1,2,k=1,2,3,\ldots\ (\varepsilon_j-\text{заданная точность}),\qquad(9)$$

где за t_k^* принимается то значение времени t_k, при котором выполняется неравенство.

Отметим, что для линейной по параметрам $\boldsymbol{\alpha}_n$ интегрированной системы моделей КВД (1), представленной в матричном виде

$$\begin{cases}\mathbf{Y}_n^*=\mathbf{F}_0\boldsymbol{\alpha}_n+\boldsymbol{\xi}_n,\\ \overline{\mathbf{Z}}_n=\mathbf{F}_a\boldsymbol{\alpha}_n+\boldsymbol{\eta}_n,\end{cases}\qquad(10)$$

и комбинированного показателя качества, выбранного в виде суммы частных квадратичных показателей качества

$$\Phi(\boldsymbol{\alpha}_n,\omega_n,h_n)=\left\|\mathbf{Y}_n^*-\mathbf{F}_0\boldsymbol{\alpha}_n\right\|^2_{\mathbf{K}(h(n))}+\left\|\overline{\mathbf{Z}}_n-\mathbf{F}_a\boldsymbol{\alpha}_n\right\|^2_{\mathbf{W}(\omega(n))},\qquad(11)$$

оптимизационная задача (6) сводится к решению систем линейных алгебраических уравнений вида

$$(\mathbf{F}_0^T\,\mathbf{K}(h_n)\mathbf{F}_0+\mathbf{F}_a^T\mathbf{W}(\omega_n)\mathbf{F}_a)\boldsymbol{\alpha}_n=(\mathbf{F}_0^T\,\mathbf{K}(h_n)\mathbf{Y}_n^*+\mathbf{F}_a^T\mathbf{W}(\omega_n)\overline{\mathbf{Z}}_n),\qquad(12)$$

где запись $\|\mathbf{X}\|^2_{\mathbf{W}}$ означает квадратичную форму $\mathbf{X}^T\mathbf{W}\mathbf{X}$; $\mathbf{Y}_n^*=(q_i^*,i=\overline{1,n})$ – вектор фактических значений дебита скважин; $\overline{\mathbf{Z}}_n=(\bar{a}_{1,n},\bar{a}_{2,n},\bar{p}_n^{-2})$ – дополнительные априорные данные и экспертные оценки параметров модели КВД (1) $\bar{a}_{1,n}$, $\bar{a}_{2,n}$ и квадрата пластового давления $\bar{p}_n^{-2}$, известные к моменту времени t_n; $\mathbf{F}_0=(1,p_{3,i},i=\overline{1,n})$ – матрица размерности $(2\times n)$; $\mathbf{F}_a^T=\begin{bmatrix}1,0,1\\ 0,1,\lg(t_p)\end{bmatrix}$ – матрица размерности (2×3); $\mathbf{W}(\omega_n)=\mathrm{diag}(\omega_{1,n},\omega_{2,n},\omega_{3,n})$ – диагональная матрица управляющих параметров ω_n; $\mathbf{K}(h_n)=\mathrm{diag}(w_i((t_n-t_{n-i}))/h_n,i=\overline{1,n-i})$ – диагональная матрица значений весовой функции $w(x/h)$ с параметром h_n. Для получения системы линейных уравнений (12) достаточно взять частные производные по параметрам $\boldsymbol{\alpha}_n$ от комбинированного функционала $\Phi(\boldsymbol{\alpha}_n,\omega_n,h_n)$ и приравнять их к нулю.

Следует отметить, что оптимизационные задачи (7), (8) не имеют аналитического решения и определяются с использованием методов последовательных приближений.

Результаты интерпретации КВД скважин газового месторождения. Результаты интерпретации КВД газовых скважин № 1046 и № 1054 месторождения Тюменской области приведены на рис. 3–6 и в табл. 2, 3.

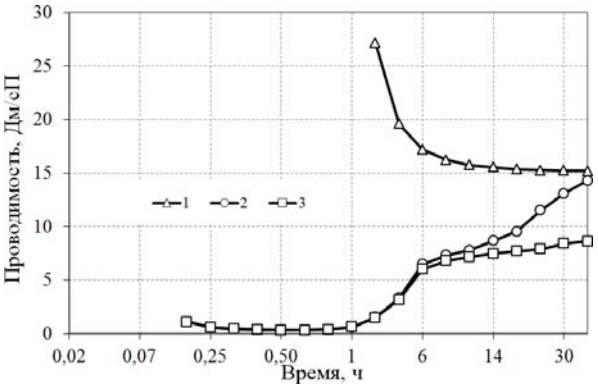


Рис. 3. Оценки проводимости пласта скважины № 1046

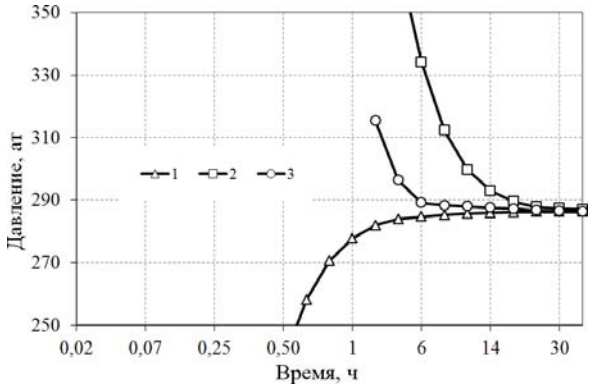


Рис. 4. Оценки пластового давления скважины № 1046

На рис. 3–6 (линия *1*) приведены оценки проводимости $\sigma^*(t_k,u_k^*)$ (3) и пластового давления $P_{\text{пл}}^*(t_k,u_k^*)$ (5) в различные моменты времени t_k, полученные при интерпретации КВД скважин

№ 1046 и № 1054 методом интегрированных моделей (6), (7) (АИ_ИМ) и модели КВД (1) (линия *1*). Оценки вектора управляющих параметров $\omega_k^* = (\omega_{1k}^*, \omega_{2k}^*, \omega_{3k}^*)$ и параметра h_k^* весовой функции $w(x/h) = \exp(-x/h)$ определялись путем решения оптимизационных задач (7), (8) методами деформированного многогранника и золотого сечения соответственно [8].

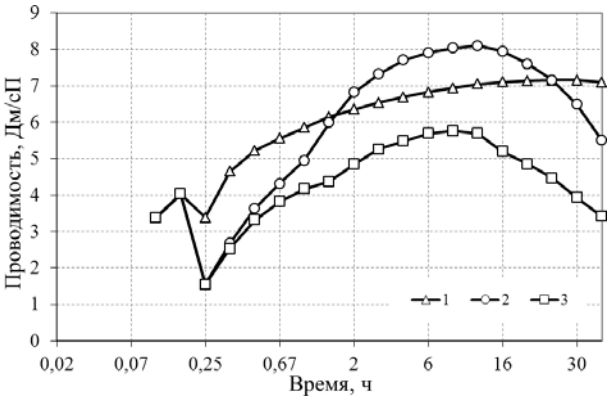


Рис. 5. Оценки проводимости пласта скважины № 1054

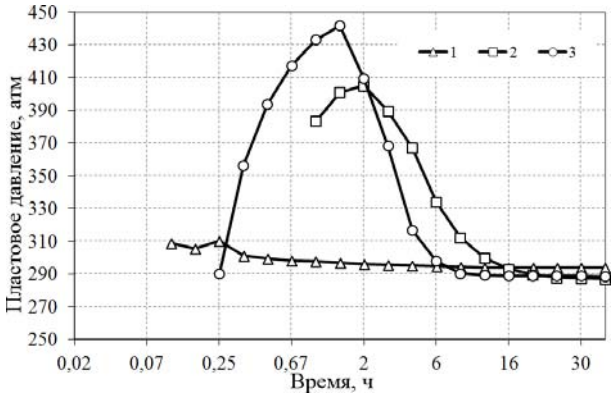


Рис. 6. Оценки пластового давления скважины № 1054

Линией *2* приведены оценки проводимости $\sigma^*(t_k, 0, h_k^*, \bar{z}_k)$ и пластового давления $P_{\text{пл}}^*(t_k, 0, h_k^*, \bar{z}_k)$, полученные адаптивным методом наилучшего совмещения (АМ_НС) путем решения СЛУ (12) при значениях управляющих параметров, равных нулю ($\omega_k = 0$). Линией *3* приведены оценки проводимости $\sigma^*(t_k, \omega_k^*, h_k^*, 0)$ и пластового давления $P_{\text{пл}}^*(t_k, \omega^*, h^*, 0)$, полученные адаптивным методом наилучшего совмещения с регуляризацией (АМ_НСР) путем решения СЛУ (12) при значениях экспертных оценок проводимости, пьезопроводности и пластового давления, равных нулю ($\bar{z}_k = 0$) [6]. Корректировка экспертных оценок $\bar{z}_i$ проводилась по схеме

$$\bar{a}_{k-1} = \alpha_k^*(t_k, \omega_k^*, h_k^*, \bar{z}_k),\ \bar{p}_{k-1}^2 = (P_{\text{пл}}^*(t_k, \omega_k^*, h_k^*, \bar{z}_k))^2,\ k = 2,3,4,\ldots .$$

Исходные данные и экспертные оценки параметров пласта и скважины, известные к моменту времени t_0, приведены на рис. 1 и в табл. 1.

Таблица 1

Исходные данные и дополнительные априорные сведения

Исходные данные и экспертные оценки	Скважины	
	1046	1054
1. Пластовая температура, К	356,66	357
2. Радиус контура питания скважины, м	650	650
3. Радиус скважины, м	0,108	0,5
4. Атмосферное давление, атм	1,033	1,033
5. Температура при нормальных условия (+20 °С) К	293	293
6. Коэффициент сжимаемости газа при пластовых условиях	0,9198	9058
7. Пористость	0,19	0,096
8. Эффективная мощность, м	11,8	17,6
9. Динамическая вязкость, сП	0,02	0,02
10. Дебит скважины до остановки, тыс. м^3/сут	332,25	589,83
11. Экспертная оценка проводимости пласта, Дм/сП	30	12
12. Экспертная оценка пьезопроводности пласта, см^2/с	3500	2000
13. Экспертная оценка пластового давления, атм	300	300
14. Экспертная оценка времени восстановления забойного давления, ч	50	50
15. Оценки параметра *a* модели ИК (2)	7,71	4,12
16. Оценки параметра *b* модели ИК (2)	0,405	0,19
17. Оценки пластового давления модели ИК (2)	300	296

Оценки параметров модели индикаторной кривой a^*, b^* и пластового давления $P^*_{\text{пл}}$ (2) определялись методом наименьших квадратов

$$\boldsymbol{\beta}^* = \arg\min_{\boldsymbol{\beta}} \left\| \mathbf{Y}^*_n - \mathbf{F}_u \boldsymbol{\beta} \right\|^2$$

с использованием данных забойного давлении P^*_{3i} и дебита q^*_i скважин № 1046 ($i=\overline{1,5}$) и № 1054 ($i=\overline{1,6}$), приведенных на рис. 2. Здесь $\boldsymbol{\beta}^* = (P^*_{\text{пл}}, a^*, b^*)$; $\mathbf{Y}^*_n = ((P^*_{3i})^2,\ i=\overline{1,n})$ – вектор; $\mathbf{F}_u = (1, q^*_i, (q^*_i)^2, i=\overline{1,n})$ – матрица размерности ($n\times 3$), n=5,6.

В табл. 2, 3 для скважин № 1046 и № 1054 приведены результаты сравнительного анализа оценок проводимости, пьезопроводности и пластового давления с использованием программного комплекса Sapir и метода адаптивной интерпретации с учетом экспертных оценок, адаптивного метода наилучшего совмещения и метода адаптивной интерпретации с регуляризацией за разные периоды исследований, в том числе и оценки момента времени завершения исследований t^*_k (9), полученные при $\varepsilon_j = \varepsilon = 0{,}02,\ \ j=1,2,3$.

Таблица 2

Результаты интерпретации скважины 1046

Методы	Время исследований, ч	Проводимость, Дм/сП	Пьезопроводность, см^2/с	Пластовое давление, атм	Моменты времени завершения исследований t^*_k, ч
Saphir	38	10,92	2280	282,2	38
АИ_ИМ	6	17,23	2588	284,4	10
	14	15,82	2352	285,8	
	30	15,24	2305	286,2	
	38	15,21	2305	286,2	
АИ_НС	6	6,53	989	289,1	38
	14	8,65	1316	287,5	
	30	13,14	1745	286,4	
	38	14,36	2166	286,2	
АИ_НСР	6	6,02	921	289,7	38
	14	7,53	1141	288,1	
	30	8,47	1273	287,4	
	38	8,62	1309	287,2	

Таблица 3

Результаты интерпретации скважины 1054

Методы	Время исследований, ч	Проводиость, Дм/сП	Пьезопроводность, см^2/с	Пластовое давление, атм	Время завершения исследований t^*_k, ч
Saphir	36	6,52	1195	288,3	36
АИ_ИМ	6	6,82	1190	294,7	8
	12	7,04	1226	294,1	
	20	7,14	1241	293,8	
	30	7,15	1243	293,8	
	36	7,10	1235	294,1	
АИ_НС	6	7,96	1369	334,6	36
	12	8,13	1401	299,8	
	20	7,64	1317	289,4	
	30	6,49	1129	287,3	
	36	5,51	960	287,1	
АИ_НСР	6	5,70	1000	298,1	36
	12	5,69	997	289,7	
	20	4,85	852	288,7	
	30	3,93	694	288,6	
	36	3,41	603	288,2	

Из рис. 3–6 и табл. 2, 3 видно, что метод адаптивной интерпретации обеспечивает получение более точных оценок фильтрационных параметров и пластового давления на коротких КВД в пределах от 8 до12 ч исследований, что позволяет существенно сократить время простоя скважин.

Выводы. Для определения параметров газовых пластов по результатам нестационарных гидродинамических исследований по кривой восстановления предлагается использовать метод адаптивной интерпретации, позволяющий проводить обработку данных в процессе проведения исследований, определять время завершения исследований и учитывать дополнительную априорную информацию.

На примере гидродинамических исследований газовых скважины месторождения Тюменской области показано, что метод адаптивной интерпретации с учетом и корректировкой экспертных оценок обеспечивает получение более точных оценок проводимости пласта, пьезопроводности и пластового давления, позволяет значительно сократить время простоя скважины по сравнению с традиционным методом наилучшего совмещения и метода интерпретации, реализованного в программе Saphir.

Литература

1. Гриценко А.И. Руководство по исследованию скважин / А.И. Гриценко, З.С. Алиев и др. – М.: Наука, 1995. – 523 с.

2. Шагиев Р.Г. Исследование скважин по КВД. – М.: Наука, 1998. – 304 с.

3. Bourdet D. Use of pressure derivative in well test interpretation / D. Bourdet, J.A. Ayoub, Y.M Pirard // SPE. – 1984. – № 12777. – P. 293–302.

4. Сергеев В.Л. Интегрированные системы идентификации. – Томск: Изд-во Том. политех. ун-та, 2011. – 198 с.

5. Сергеев В.Л. Метод адаптивной идентификации гидродинамических исследований скважин с учетом априорной информации / В.Л.Сергеев, А.С. Аниканов // Известия Том. политех. ун-та. – 2010. – Т. 317, № 5. – С. 50–52.

6. Сергеев В.Л. Адаптивная интерпретация нестационарных гидродинамических исследований скважин в системе «пласт–скважина» методом интегрированных моделей / В.Л. Сергеев, К.С. Гаврилов // Известия Том. политех. ун-та. – 2012. – Т. 321, № 5. – С. 72–75.

7. Тихонов А.Н. Методы решения некорректных задач / А.Н. Тихонов, В.Я. Арсенин. – М.: Наука, 1979. – 392 с.

8. Пантелеев А.В. Методы оптимизации в примерах и задачах / А.В. Пантелеев, Т.А. Летова. – М.: Высшая школа, 2002. – 544 с.

Сергеев Виктор Леонидович
Д-р техн. наук, профессор каф. геологии и разработки нефтяных месторождений
Института природных ресурсов
Национального исследовательского Томского политехнического университета
Эл. почта: SergeevVL@ignd.tpu.ru
Тел.: 8-905-992-92-31

Гаврилов Константин Сергеевич
Аспирант каф. геологии и разработки нефтяных месторождений
Института природных ресурсов
Национального исследовательского Томского политехнического университета
Эл. почта: gavrilovks@gmail.com

Sergeev V.L., Gavrilov K.S.

Adaptive identification and interpretation of non-stationary well test gas fields

The models and adaptive algorithms for the identification and interpretation of well test gas fields in transient mode filtering based on the integrated model system pressure recovery curve in light of additional a priori information. The results of quality analysis algorithms of identification and interpretation of pressure recovery curve gas exploration wells.

Keywords: identification, adaptation, interpretation, well test, pressure build-up curve, integrated systems models, a-priori information, gaz and gas condensate fields.

УДК 528.88

И.Н. Шишкин, А.А. Скугарев

Использование геоинформационных технологий для мониторинга и оценки последствий чрезвычайных ситуаций

Предложены способы мониторинга чрезвычайных ситуаций с использованием геопорталов с визуализацией и анализом данных из источников оперативной информации: данных дистанционного зондирования, данных гидрометеорологического мониторинга, камер наблюдения. Рассмотрены источники данных по весенним паводкам и лесным пожарам.

Ключевые слова: геопортал, геоинформационные технологии, данные дистанционного зондирования Земли, чрезвычайная ситуация.

Проблема мониторинга чрезвычайных ситуаций (ЧС) для нашей страны является крайне актуальной. Сложно переоценить востребованность оперативной информации о развитии и последствиях чрезвычайных ситуаций службами, занимающимися наблюдением за ЧС и ликвидацией последствий ЧС.

К наиболее важным данным о ЧС относится не только информация о местоположении ЧС, но и такие параметры, как размеры опасных проявлений, направление и скорость распространения, наличие в зоне развития ЧС населенных пунктов, инженерных коммуникаций и т.д. Визуализацию и анализ данной информации целесообразно выполнять с использованием геоинформационных технологий. Однако для работы с пространственными данными, требуется использование специализированного геоинформационного программного обеспечения. В данной ситуации на помощь могут прийти геопорталы – электронные географические ресурсы, расположенные в сети Интернет. Использование геопорталов не требует наличия специального программного обеспечения и специальных знаний пользователей. Помимо этого, доступ к представляемым данным получают широкие группы пользователей, имеющих доступ к сети Интернет. Это, на наш взгляд, является огромным преимуществом такого способа визуализации и анализа данных о чрезвычайных ситуациях.

Современные геоинформационные технологии позволяют объединить множество источников информации в рамках единого информационного ресурса – геопортала. Использование геопорталов позволяет работать со специально подготовленными данными различных типов и источников. Однако информация, представляемая на геопортале, требует специальной предварительной обработки. Так, использование геопорталов дает возможность визуализации обработанных данных оперативной спутниковой съемки, получаемых как с различных спутников дистанционного зондирования, так и, например, с беспилотных аппаратов. Однако, требуется предварительная обработка данных, в том числе с использованием автоматизированных алгоритмов обработки. Автоматизация обработки данных ДЗЗ позволяет существенно сократить время от получения данных до их размещения на геопортале и проведения их анализа [1].

Мониторинг паводков. Для мониторинга паводковой обстановки возможно использование различных источников данных: снимков с искусственных спутников Земли (ИСЗ) (рис. 1), информации с системы гидропостов Росгидромета (рис. 2), видео с камер наблюдения, установленных в прибрежных зонах рек (рис. 3), и т.д. Геопорталы позволяют объединить данные источники информации в рамках единого информационного ресурса и представляют собой средство не только визуализации данных, но и их анализа и получения новых видов данных (векторные слои).

Использование веб-камер позволяет наблюдать ситуацию в режиме реального времени и при наличии облачности, что позволяет дополнить информацию, получаемую с данных ДЗЗ, и провести их верификацию.

Наличие приемной станции спутниковой информации является существенным фактором, повышающим оперативность получения данных дистанционного зондирования. Использование данных оперативной спутниковой съемки в видимом и инфракрасном диапазонах спектра с ИСЗ Terra, Aqua, NPP, «Метеор-М» №1 позволяет получать данные на участки развития ЧС многократно в те-

чение одних суток. Время, с момента получения данных на приемную станцию до момента их размещения на геопортале составляет около 1 ч. Как следствие, появляется возможность получения результатов анализа и интерпретации как данных спутниковой съемки, так и всего комплекса информации, представленной на геопортале в оперативном режиме.

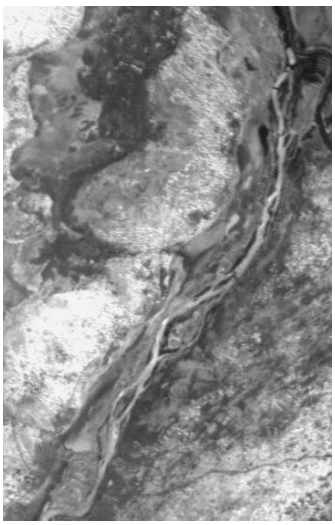


Рис. 1. Ледовая обстановка на участке реки Обь от с. Победа до впадения р.Томь по состоянию на 7.04.2014 на снимке с ИСЗ «Метеор-М» №1

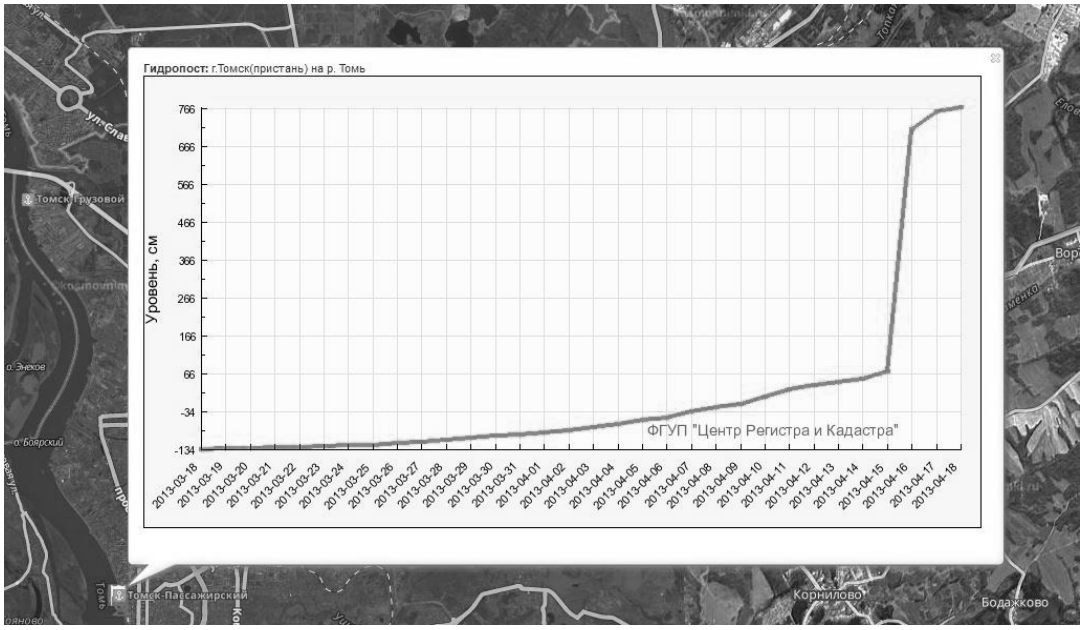


Рис. 2. Данные гидропоста на пристани г. Томск с 18.03.2013 по 18.04.2013

Рис. 3. Просмотр видео с веб-камеры на геопортале

Благодаря наличию географической привязки данных ДЗЗ возможны осуществление подсчета площади подтопленных территорий, наблюдение за динамикой развития ЧС, составления прогноза развития ЧС и его визуализации средствами геопортала. Данные можно предоставлять как с ограничением доступа [2–5, 7], так и в открытом виде для информирования не только заинтересованных служб, но и населения. Хранение данных ДЗЗ можно осуществлять в сжатом виде [6] для экономии ресурсов вычислительной системы.

Мониторинг и оценка последствий лесных пожаров. Современные технологии позволяют обнаруживать лесные пожары с помощью данных ДЗЗ (рис. 4), а также проводить оценку последствий пожаров (оценка площадей гарей). Для оперативного мониторинга целесообразно использовать данные низкого пространственного разрешения, так как они имеют наибольшую повторяемость съемки одной и той же территории. Обнаружение пожаров с помощью снимков с радиометра MODIS (ИСЗ Terra и Aqua) возможно выполнять как в автоматическом режиме с помощью алгоритма MOD14 [4] , так и визуально.

Обнаружение лесных пожаров основано на детектировании температурных аномалий. Кроме того, алгоритм MOD14 [4] предоставляет возможность оценки вероятности обнаружения лесного пожара, а также построения маски пожаров и анализа площадей выгоревших территорий.

Недостатком алгоритма является наличие ложных срабатываний из-за антропогенных источников температурных аномалий, а также использование каналов с пространственным разрешением 1000 м. Из-за этого снижается точность локализации пожара и определения численных характеристик пожара.

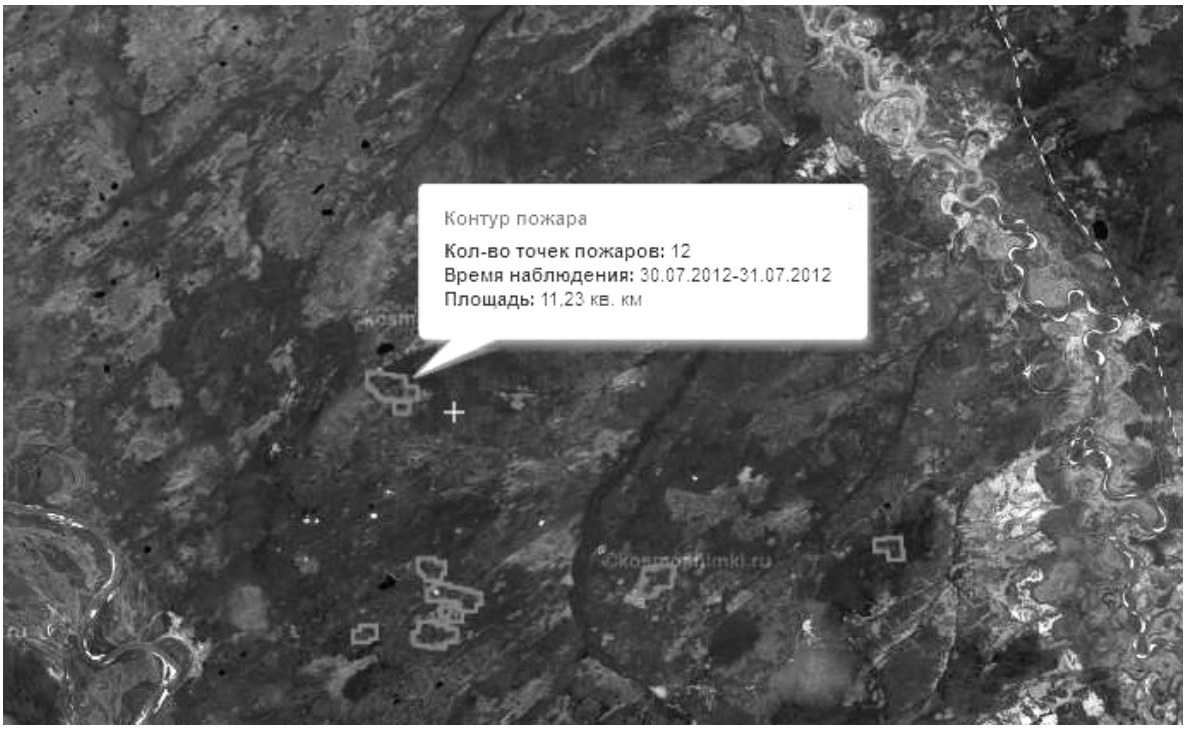


Рис. 4. Результаты автоматического детектирования пожаров

Для визуального обнаружения пожаров возможно использование определенного синтеза каналов (таблица).

Каналы для детектирования пожаров

Составляющая	Длина волны, мкм	Пространственное разрешение, м
R	2,155–2,105	500
G	0,876–0,841	250
B	0,67–0,62	250

При использовании данного синтеза возможно визуально обнаружить очаг пожара, и используемые каналы с более высоким пространственным разрешением, по сравнению с алгоритмом MOD14, позволяют локализовать очаг пожара с большей точностью.

Для увеличения информативности изображения возможно использование алгоритмов паншарпинга, что увеличивает пространственное разрешение с 500 до 250 м.

Для верификации и оценки последствий возможно дополнение данными среднего и высокого пространственного разрешения (рис. 5).

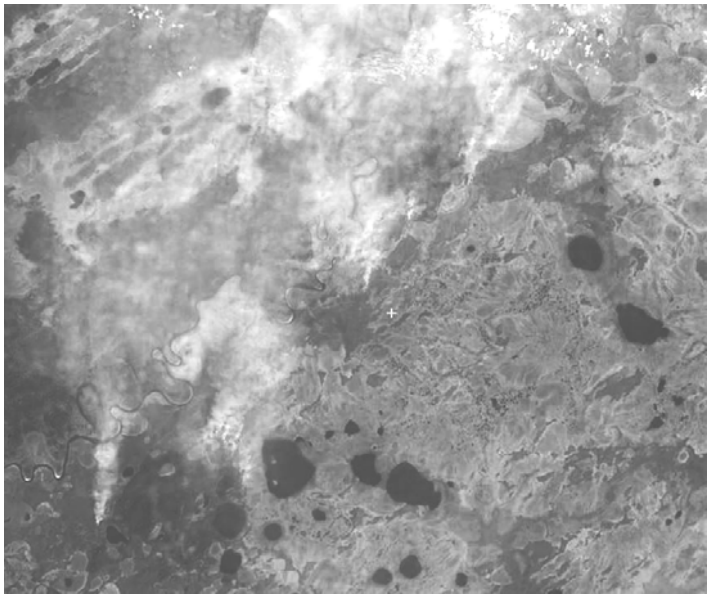


Рис. 5. Снимок очагов лесных пожаров ИСЗ SPOT-4

Данные, полученные в результате автоматической обработки, размещаются на геопортале в виде векторных слоев, объединяющих очаги пожаров в кластер (см. рис. 4). Кроме того, при накоплении данных за длительный период возможно проведение статистического анализа как средствами геопортала, так и с помощью другого программного обеспечения.

Кроме векторных слоев, на геопортале размещаются данные автоматической обработки снимков радиометра MODIS с параметрами из таблицы и для верификации данных снимки, полученные другими съемочными системами среднего и высокого пространственного разрешения.

Заключение. Геоинформационные приложения, решающие вопросы комплексирования оперативных данных из различных источников, являются эффективным средством в сфере мониторинга и оценки последствий ЧС. Использование в данной сфере геоинформационных технологий, геопорталов позволяет с большей точностью прогнозировать и проводить мониторинг ЧС, а также более оперативно реагировать на них.

Дополнение данных ДЗЗ изображениями с веб-камер позволяет получать информацию в реальном времени и вне зависимости от погоды. Целесообразно также дополнять перечень оперативных данных материалами всепогодной радиолокационной спутниковой съемки и материалами съемки беспилотными летательными аппаратами (БПЛА).

Использование геопорталов позволяет объединить в единую информационную систему различные источники данных, которые дополняют друг друга и в целом представляют собой эффективное средство мониторинга ЧС. Размещение подобных ресурсов в сети Интернет позволяет оперативно информировать как заинтересованные службы, так и население.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2014 год (проект № 1220).

Литература

1. Шишкин И.Н. Автоматизация обработки спутниковых снимков // Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2013». – 2013. – Ч. 4. – С. 111–113.

2. Сабанов А.Г. Требования к системам аутентификации по уровням строгости / А.Г. Сабанов, А.А. Шелупанов, Р.В. Мещеряков // Ползуновский вестник. – 2012. – № 2/1. – С. 61–67.

3. Исхаков А.Ю. Двухфакторная аутентификация на основе программного токена / А.Ю. Исхаков, Р.В. Мещеряков, И.А. Ходашинский // Вопросы защиты информации. – 2013. – № 3 (102). – С. 23–28.

4. Ходашинский И.А. Технология усиленной аутентификации пользователей информационных процессов / И.А. Ходашинский, М.В. Савчук, И.В. Горбунов, Р.В. Мещеряков // Доклады ТУСУРа. – 2011. – № 2–3. – С. 236–248.

5. Савчук М.В. Методы усиленной аутентификации пользователей / М.В. Савчук, Р.В. Мещеряков, Е.М. Давыдова // Безопасность информационных технологий. – 2007. – № 4. – С. 60–68.

6. MODIS Collection 5 Active Fire Product User`s Guide Version 2.5 [Электронный ресурс]. – Режим доступа: http://modis-fire.umd.edu/Documents/MODIS_Fire_Users_Guide_2.5.pdf, свободный (дата обращения: 18.04.2014).

7. Евсютин О.О. Сжатие цифровых изображений, используемых в геоинформационной системе электронного генерального плана промышленного предприятия / О.О. Евсютин, М.М. Милихин // Доклады ТУСУРа. – 2012. – № 2 (26), ч. 1. – С. 224–229.

Шишкин Илья Николаевич
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: 8-923-423-08-60
Эл. почта: sin@keva.tusur.ru

Скугарев Андрей Анатольевич
Руководитель Центра космического мониторинга Земли ТУСУРа
Тел.: 8-913-889-98-03
Эл. почта: skugarev@inbox.ru

Shishkin I.N., Skugarev A.A.
Using GIS technologies for monitoring and evaluating the effects of emergencies

The article includes methods of monitoring emergencies using geoportals with data visualization and analysis from sources of operative information: remote sensing data, hydrometeorological data, surveillance cameras. Article shows sources of data for spring floods and forest fires.
Keywords: geoportal, GIS technology, remote sensing data, emergency situation.

УДК 004.724

М.И. Мельников, А.С. Ковтун

Самоорганизующаяся сеть оперативного взаимодействия для нужд населения и специальных служб

Рассмотрена возможность организации системы информационного взаимодействия в районах, подвергшихся влиянию разрушительных факторов техногенного или природного характера, при помощи самоорганизующихся сетей. Предлагаемый комплекс являет собой совокупность разрабатываемых решений, таких как информационная среда, построенная на базе технологии Wireless Mesh IEEE 802.11s, а также информационного и коммуникационного порталов, выполняющих роль служб взаимодействия и оповещения.

Ключевые слова: ячеистая топология, mesh-сеть, самоорганизующиеся сети, SIP, XMPP, локальный информационный портал.

Проблема обеспечения информационного обеспечения населения при ЧС. В настоящее время все большее значение получает проблема оперативного обеспечения доступа к информационной среде населения в любых условиях, особенно это актуально в условиях чрезвычайных ситуаций (далее ЧС), когда существующая инфраструктура, образующая информационную среду, получает повреждения, не позволяющие ей нормально функционировать на какой-либо территории, что, безусловно, создаёт ряд дополнительных проблем, связанных с оперативным устранением данной ЧС.

Надо признать, что в России в рамках данной проблемы активно ведутся работы по обеспечению населения информацией о ЧС [1], но основной вектор данных работ – это оповещение населения через существующую инфраструктуру GSM- и CDMA-сетей (Общероссийская комплексная система информирования и оповещения населения в местах массового пребывания людей) [2], но работа данной системы невозможна в местах где нарушено нормальное функционирование существующих беспроводных сетей связи. А также в данной ситуации возникают не только технические, но и организационные проблемы, связанные с согласованием рассылки в местах ЧС [3].

Проблемы обеспечения информацией населения в условиях чрезвычайных ситуаций весьма актуальны. В этой связи вполне обоснованной является разработка программно-аппаратного комплекса, призванного организовать локальное информационное пространство в рамках зоны ЧС с возможностью взаимодействия её с внешними информационными сетями.

Постановка проблемы. Сложно предопределить географические масштабы того или иного ЧС, соответственно практически невозможно загодя определить потребности в связи. Согласно наставлению по организации управления и оперативного (экстренного) реагирования при ликвидации чрезвычайных ситуаций [4], утверждённому Правительственной комиссией по предупреждению и ликвидации чрезвычайных ситуаций и обеспечению пожарной безопасности, основным видом связи при разрешении систем проводной связи является радиосвязь. Но в рамках современного информационного общества недостаточно просто организовать радиосвязь для взаимодействия оперативных служб и обеспечить население возможностью доступа к информации и линиям ТФоП.

Соответственно в районе ЧС силами служб, занимающихся устранением последствий бедствия, требуется оперативно развернуть инфраструктуру беспроводной сети передачи данных.

Оптимальным решением в плане доступности для обывателя было бы развернуть своеобразную «открытую» GSM-сеть, но данная технология требует сложных расчётов по расположению передатчиков и перекрытия ими частотных диапазонов [5], что не позволяет развернуть сеть в сроки адекватные ситуации.

Поэтому был сформирован ряд требований к инфраструктуре сети:

1) необходимость быстрого развертывания сети без сложных расчётов зон покрытия и радиочастотного перекрытия;

2) динамическая реконфигурация сети в соответствии с изменением оперативной обстановки;

3) возможность подключения и работы наиболее распространённых мобильных устройств.

Рассмотрим более подробно каждый из пунктов.

Необходимость быстрого развертывания сети обусловлена тем, что в рамках ЧС ощущается острый недостаток времени на мероприятия, собственно, не связанные с устранением последствий.

Возможность динамической реконфигурации позволит решить вопрос несоответствия ёмкости сети возросшим потребностям зоны ЧС. То есть в случае увеличения зоны или количества абонентов развёртываемой инфраструктуры легко можно увеличить диапазон и ёмкость беспроводной сети.

Ключевым требованием системы является возможность подключения и работы с ней наиболее распространённых мобильных устройств. По итогам исследования Gartner, в 4-м квартале 2013 г. в мире было продано 1,8 млн мобильных телефонов, из них 0,97 млн – это смартфоны, в стандарт оснащения которых входят такие беспроводные интерфейсы, как GSM, Bluetooth и WiFi [6]. Как рассматривалось выше, GSM-сети сложны в развертывании, а Bluetooth ограничен по скорости передачи данных и диапазону. Таким образом, оптимальным решением в данном случае становится применение технологии беспроводного доступа семейства протоколов IEEE 802.11 (WiFi), а в частности протокол IEEE 802.11s (WiFi Mesh).

Общая информация о Mesh-сетях. Mesh-сеть – это распределенная одноранговая ячеистая сеть.

Идея Mesh-сети предложена ещё в 1962 г. Полом Бэраном [7], одним из основоположников сегодняшнего Интернета [8]. Эта сеть имела название Ricochet и просуществовала вплоть до 2008 г.

Технология Mesh (ячеистые сети, multi-hop сети) расширяет функциональность беспроводного доступа к сетевым сервисам и позволяет реализовывать точки доступа с охватом и порогом снижения пропускной способности на порядок более высоким, чем у привычных хот-спотов. Благодаря возможности обеспечения защищенного беспроводного покрытия на улицах, в городской местности или в крупных населенных пунктах и районах, Wireless Mesh может быть использована для быстрого развертывания, в частности сети связи для целей внутренней безопасности или в случаях чрезвычайных ситуаций в городе [10].

Топология данной сети, построенной по стандарту 802.11s, представлена рис. 1. Mesh-сеть – это сеть, в которой каждый элемент сети связан с несколькими другими элементами этой же сети, что позволяет достичь возможности варьировать маршруты через сегменты с лучшими показателями связи [9, 11–13].

Если ближайшая точка доступа перегружена, данные перенаправляются к ближайшему незагруженному узлу. Блок данных продолжает перемещаться от одного узла к другому, пока не достигнет места назначения.

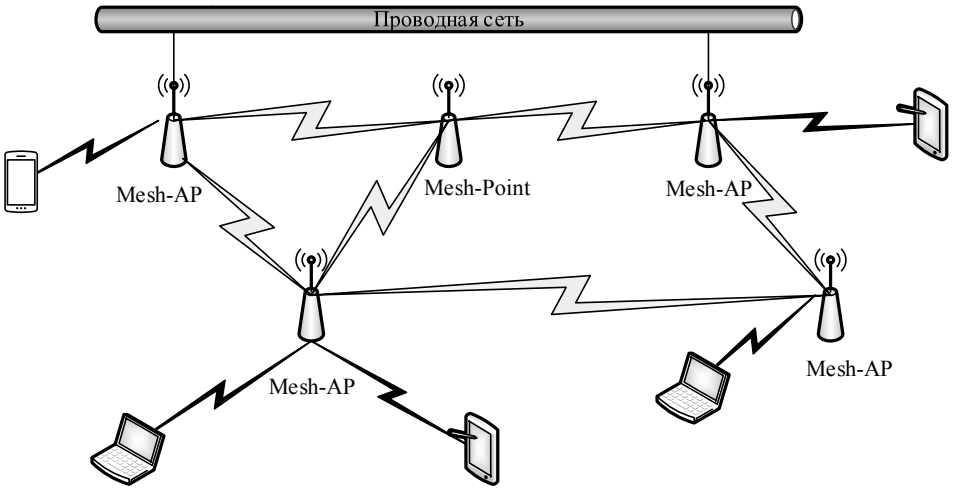


Рис. 1. Топология беспроводной Mesh-сети

Mesh-сети позволяют организовать надежное покрытие сети в определённой локальной зоне, данная технология позволяет организовать высокоскоростную беспроводную сеть в зоне чрезвычайной ситуации. Ключевым функционалом, определяющим предпочтение данных сетей в кризисных ситуациях, является функционал самоорганизации, т.е. выход из строя промежуточных узлов или добавление новых узлов в сеть не приведет к разрушению сети, а только снизит (или увеличит) её зону покрытия и пропускную способность. Благодаря особенностям протокола время разворачивания данной сети ограничивается только скоростью распределения точек доступа по зоне планируемого покрытия.

Для решения поставленной задачи организации взаимодействия предлагается рассматривать указанную реализацию протокола IEEE 802.11s.

Предлагаемая структура комплекса. Предлагается реализовать программно-аппаратный комплекс самоорганизующейся сети передачи данных в районах ЧС.

Разрабатываемый комплекс включает в себя следующие элементы: оборудование для создания информационной среды, информационный и коммуникационный порталы.

Информационный портал предназначен для размещения оперативной информации о происходящих событиях, а также для осуществления координации действий различных подразделений. Он представляет собой веб-ресурс, доступ к которому автоматически получает любое устройство, способное подключиться к информационной среде.

Коммуникационный портал предназначен для осуществления связи между участниками сети и за её пределы, построен по принципу клиент-серверной коммуникации. Порталом обеспечивается голосовая, а также текстовая связь в режиме реального времени, основанная на протоколе SIP и XMPP (Jabber). Эти технологии достаточно распространены и поддерживаются большинством устройств изначально. Однако, для унификации системы доступа, возможен доступ к этим сервисам при помощи специального приложения, разработанного для основных операционных систем смартфонов: Android, Windows Phone, а также iOS. Такое приложение можно будет скачать с информационного портала и начать им пользоваться без дополнительных настроек. Доступ же к ресурсам с персональных и мобильных компьютеров осуществляется напрямую через сервисы информационного порта. После подключения к коммуникационному порталу информация о новом абоненте автоматически вносится в единую телефонную книгу.

Информационная среда обеспечивается точками доступа Wireless Mesh. Технологически это устройства, призванные обеспечивать территорию устойчивым сигналом сети стандарта IEEE 802.11s. Точки доступа подразделяются на ряд видов:

1. Стационарные точки доступа. Это устройства с отдельным питанием и мощным передатчиком, предназначенные для обеспечения сигналом больших территорий при наличии источника гарантированного электропитания. Такими устройствами предлагается оснащать места временного пребывания населения или штаба ЧС. Эти точки доступа оборудованы возможностью подключения к порталам и интерфейсам доступа.

2. Мобильные точки доступа не имеют возможности подключения к порталам, т.е. являются по своей сути репитерами, тем самым выигрывая в массе и размере. Они оснащены разнообразными средствами крепления и защиты, что позволяет использовать их в полевых условиях при наличии источника электропитания, а также оснащать ими транспортные средства, участвующие в ликвидации ЧС.

3. Автономный ретранслятор предназначен для использования в качестве носимого и/или автономно установленного. Он имеет независимый источник питания, который позволяет организовывать доступ к информационному порталу в любой точке зоны ЧС.

Для обеспечения возможности связи с прочими сетями в комплексе предусмотрен интерфейс доступа к информационным сетям общего пользования. Таковыми сетями могут быть сеть Интернет, а также телефонная сеть общего пользования (ТфОП). Возможность доступа к этим сетям ограничивается правами доступа, устанавливаемыми на коммуникационном портале.

Для контроля состояния развёрнутой сети в комплексе присутствует система управления и мониторинга, которая подразумевает возможность оповещения о возможной потере связности (например, ввиду перемещения точек доступа относительно друг друга). Также существует возможность перераспределять трафик между точками доступа, выявляя и устраняя наиболее загруженные участки.

Полная структурная схема комплекса приведена на рис. 2. Данный комплекс обладает следующими ключевыми особенностями:

1. Простота развёртывания сети. Устройства не будут требовать никакой дополнительной настройки. Основное условие обеспечения связности сети – нахождение в пределах видимости как минимум одного устройства из сети.

2. Возможность быстрого развёртывания сети на большой территории за счёт носимых/возимых мобильных точек доступа.

3. Устройства возможно устанавливать в транспортные средства (ТС), что позволит организовывать оперативную связь внутри автоколонн или же при расстановке ТС на территории – охват этой территории сетью.

4. Реализация полностью функциональных внутренних ресурсов (информационного и коммуникационного портала), доступ к которым осуществляется через веб-интерфейс.

5. Подключение к сети осуществляется посредством любого устройства с возможностью подключения к WiFi. С точки зрения пользователя сеть представляется обычной открытой Wi-Fi-сетью. Разница только во внутренней структурной организации.

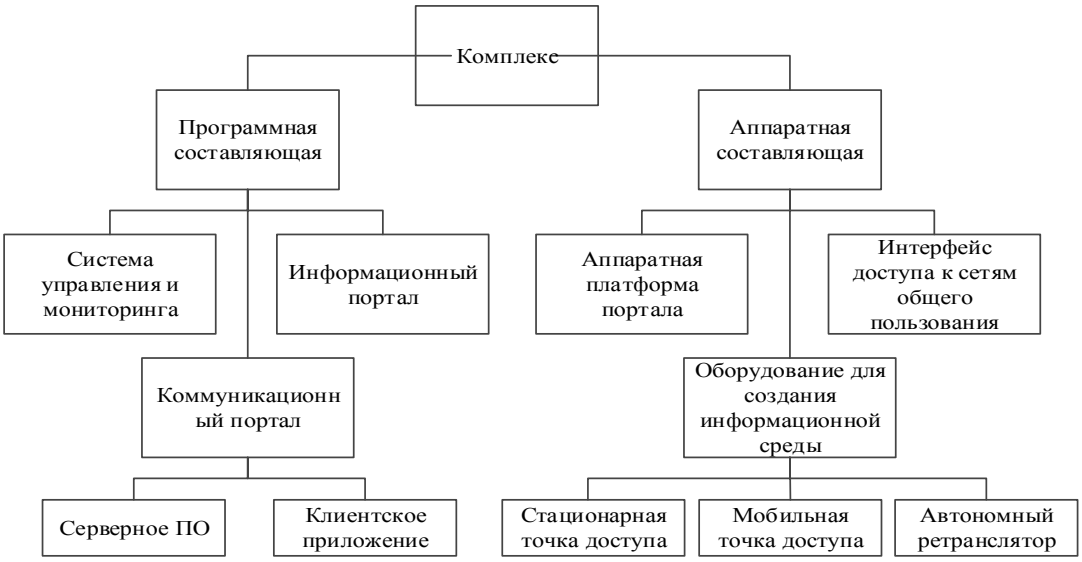


Рис. 2. Структурная схема предлагаемого комплекса

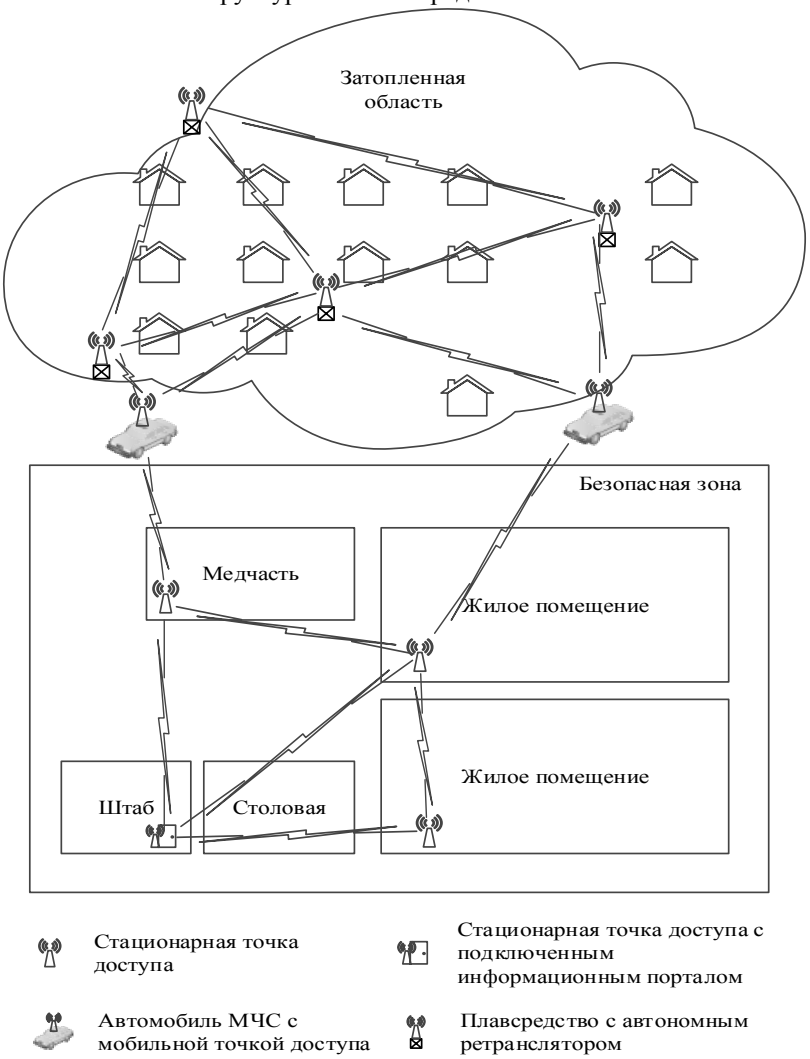


Рис. 3. Схема развёртывания комплекса

Пример использования комплекса. В качестве примера реального использования комплекса можно привести ЧС, возникшую в результате затопления жилой местности (рис. 3).

На рис. 3 приведена возможная схема реализации комплекса в случае затопления жилой местности. Затопленной оказалась территория с несколькими жилыми домами. Недалеко от зоны бедствия была образована безопасная зона, в которой временно размещаются жильцы затопленных домов, а также штаб ЧС и подсобные помещения. Используя предлагаемый комплекс, возможно развернуть сеть с общим доступом на территории бедствия. В штабе устанавливается стационарная точка доступа, к которой подключаются информационный, а также коммуникационный порталы. Эти порталы обеспечивают информирование населения о событиях, а также обеспечивают связь между оперативными службами. При использовании интерфейса подключения к внешним линиям возможно использование GSM-сети для связи с иными сетями (при наличии таковой). В каждом подсобном помещении также устанавливается стационарная точка доступа таким образом, чтобы в зоне радиочастотной видимости каждой точки находились ещё две. Таким образом, обеспечивается покрытие территории безопасной зоны устойчивым сигналом стандарта IEEE 802.11a/b/g/n (WiFi). Покрытие сетью затопленной территории обеспечивается за счёт автономных ретрансляторов, установленных на плавсредствах, а также выданных личному составу группы спасателей. Находясь в зоне видимости друг друга, такие ретрансляторы обеспечивают покрытие сетью большую территорию зоны.

Заключение. В статье представлен комплекс, позволяющий оперативно развёртывать информационную сеть в районе ЧС либо в районе проведения спецоперации. Комплекс базируется на беспроводных самоорганизующихся Mesh-сетях (стандарт IEEE 802.11s). Дано обоснование возможности реализации такого комплекса. Приведена и описана структура комплекса, включающая в себя как аппаратные, так и программные решения. Показан пример развёртывания и использования предлагаемого комплекса в конкретной ситуации, связанной с затоплением жилой местности.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2014 год (проект № 1220).

Литература

1. Указ Президента РФ от 13.11.2012 № 1522 «О создании комплексной системы экстренного оповещения населения об угрозе возникновения или о возникновении чрезвычайных ситуаций» [Электронный ресурс]. – Режим доступа: http://graph.document.kremlin.ru/page.aspx?1633290, свободный (дата обращения: 14.04.2014).

2. Разработка методологии информирования и оповещения населения в местах массового пребывания людей: отчет о работе (заключит.) / Центр исследования экстремальных ситуаций; МЧС России. – М., 2006.

3. Первая попытка SMS-оповещений о ЧС в Костроме провалилась [Электронный ресурс]. – Режим доступа: http://news.mail.ru/inregions/center/44/incident/11544067/, свободный (дата обращения: 14.04.2014).

4. Наставление по организации управления и оперативного (экстренного) реагирования при ликвидации чрезвычайных ситуаций [Электронный ресурс]. – Режим доступа: http://www.mchs.gov.ru/upload/site1/library/TJut65rrGG.doc, свободный (дата обращения: 14.04.2014).

5. Энциклопедия GSM-связи. Ч. 2 [Электронный ресурс]. – Режим доступа: http://www.3dnews.ru/editorial/gsm_part2, свободный (дата обращения: 14.04.2014).

6. Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013 [Электронный ресурс]. – Режим доступа: http://www.gartner.com/newsroom/id/2665715, свободный (дата обращения 14.04.2014).

7. On distributed communications networks [Электронный ресурс]. – Режим доступа: http://pages.cs.wisc.edu/~akella/CS740/F08/740-Papers/Bar64.pdf, свободный (дата обращения: 14.04.2014).

8. Paul Baran Invents Packet Switching [Электронный ресурс]. – Режим доступа: http://www.livinginternet.com/i/ii_rand.htm, свободный (дата обращения: 14.04.2014).

9. Mesh-сети: технологии, приложения, оборудование [Электронный ресурс]. – Режим доступа: http://www.tssonline.ru/articles2/fix-op/mesh_seti_techn_prilozh_oborud, свободный (дата обращения: 14.04.2014).

10. Ячеистые сети [Электронный ресурс]. – Режим доступа: http://citforum.ru/nets/wireless/mesh/, свободный (дата обращения: 14.04.2014).

11. Мещеряков Р.В. Характеристики надежности распределенных криптографических информационно-телекоммуникационных систем с ограниченными ресурсами / Р.В. Мещеряков, А.А. Шелупанов, Т.Ю. Зырянова // Вычислительные технологии. – 2007. – Т. 12. – № S1. – С. 62–67.

12. Росошек С.К. Встраивание криптографических функций в систему связи с ограниченными ресурсами / С.К. Росошек, Р.В. Мещеряков, А.А. Шелупанов, С.С. Бондарчук // Вопросы защиты информации. – 2004. – № 2. – С. 22–25.

13. Росошек С.К. Криптографические протоколы в системах с ограниченными ресурсами / Р.В. Мещеряков, С.К. Росошек, А.А. Шелупанов А.А., М.А. Сонькин // Вычислительные технологии. – 2007. – Т. 12. – № S1. – С. 51–61.

Мельников Максим Игоревич
Вед. инженер центра технологий безопасности ТУСУРа
Тел.: (382-2) 90-01-11 доб. 29-03
Эл. почта: mmi@keva.tusur.ru

Ковтун Александр Сергеевич
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел. (382-2) 90-01-11, доб. 29-01
Эл. почта: kas@isib.su

Melnikov M.I., Kovtun A.S.

Self-organizing network for operational information cooperation for the needs of the population and special purposes

The possibility of organizing a system of information exchange in the areas affected by the devastating impact of man-made or natural factors, using self-organizing networks. The proposed complex consist of the information environment hardware that is based on technology Wireless Mesh IEEE 802.11s and the information and communication portals that serve as the collaborative services and alert.

Keywords: cell topology, mesh networks, self-organized networks, SIP, XMPP, local information portal.

УДК 681.3:629.7

В.Х. Ханов

Сетевые технологии для бортовых систем космического аппарата: опыт разработки

Дан обзор проведенных разработок в области реализации сетевых технологий для бортовых систем космического аппарата. Приведены сведения по основным проведенным разработкам. Представлены результаты разработки резервируемой сетевой архитектуры бортового комплекса управления, маршрутизирующего коммутатора SpaceWire, аппаратного контроллера протокола RMAP. Определены варианты создания сетевой архитектуры и направления дальнейших исследований и разработок.

Ключевые слова: SpaceWire, сетевая архитектура, малые космические аппараты.

Сетевые технологии для использования в космической аппаратуре. Сетевые технологии, получившие повсеместное распространение во всех сферах жизни человечества, тем не менее, довольно трудно внедряются в космическое приборостроение. Оказалось, что «земные» сетевые технологии, отличающиеся полнотой областей применения, не отвечают требованиям космического электронного приборостроения к простоте реализации, надежности, низкому энергопотреблению. Специализированные интерфейсы, несколько десятков лет назад специально разработанные для авиакосмического применения, например MIL-STD-1533 [1], не позволяют создать сложноструктурированные сети и к тому же отличаются невысокой скоростью. Ситуация начала изменяться с появлением сетевой технологии SpaceWire, специально разработанной для космического применения под руководством Европейского космического агентства (ESA). На сегодняшний день технология SpaceWire (SpW) отвечает всем требованиям для эксплуатации в составе бортовых космических систем, поэтому она быстро получила распространение в зарубежной космической практике.

В России также проводятся активные работы по внедрению SpW. И хотя космических миссий с применением SpW пока нет, большинство ведущих отечественных разработчиков бортовых космических систем включают SpW в свои разработки. В данной статье приведен обзор некоторых проведенных исследований и разработок в области SpW в лаборатории космического электронного приборостроения СибГАУ.

Постановка задачи. Сетевая идеология построения космических систем уже давно развивается за рубежом. Координатором этого процесса является Международный консультативный комитет по космическим информационным системам (CCSDS). Он рассматривает все информационные процессы взаимодействия наземных и бортовых систем как интеграцию сетевых уровней, подобно модели OSI. ESA, следуя руководящим документам CCSDS, разработало в начале 2000-х годов стандарт SpaceWire ECSS-E-ST-50-12C [2] для построения бортовой сети космического аппарата (КА). В настоящее время стандарт SpaceWire используют не только предприятия ESA, но и США (NASA), Японии (JASA), Китая. В мире насчитывается более 20 успешных космических миссий, в которых использовался SpW.

В Роскосмосе создана рабочая группа по внедрению стандарта SpW. Уже несколько лет ожидается первая версия российского SpW стандарта. Однако до сих пор в России нет ни одного КА, ни полномасштабных прототипов космических систем с применением SpW. Объясняется это высокой консервативностью отечественной аэрокосмической отрасли при внедрении данной технологии. К основным причинам этой ситуации можно отнести:

– существенные отличия технологии SpW от применяемых в настоящее время на КА централизованных, аппаратно-резервируемых структур со сложной системой связей на базе нескольких информационных интерфейсов. Количество требуемых изменений настолько велико, что связанные с внедрением сетевой технологией высокие технические риски выступают в качестве главного сдерживающего фактора;

– отсутствие положительных примеров апробирования технологии SpW в отечественных космических системах. В настоящее время трудно ожидать, что в России технология SpW сразу будет

использована на большом КА. Скорее всего, отечественные разработки в области SpW впервые будут использованы на малых КА (МКА);

– отставание в создании отечественной электронной компонентной базы (ЭКБ) SpW. Номенклатура отечественной ЭКБ весьма ограничена. Нет сообщений об ее апробировании в космических миссиях.

Учитывая приведенные обстоятельства, общая задача исследований в области SpW сформулирована следующим образом: на примере МКА отработать и продемонстрировать на практике основные технические решения по созданию бортовых систем космического аппарата с использованием SpW, в том числе резервируемую сетевую архитектуру бортового комплекса управления (БКУ), варианты создания сетевой архитектуры, маршрутизирующий коммутатор SpW, аппаратный контроллер протокола RMAP. В качестве элементной базы реализации использовать перепрограммируемые FPGA ПЛИС, применяемые СФ-блоки должны быть открытыми.

Сетевая резервируемая архитектура бортового комплекса управления. Особенностью сетевой архитектуры является создание инфраструктуры передачи данных, позволяющей легко дублировать основные и инфраструктурные компоненты сети, иметь несколько альтернативных путей передачи данных, масштабировать или модифицировать сеть под имеющееся оборудование на борту КА [3].

За основу в качестве базовой взята топология типа «звезда» с быстродействующим коммутатором (маршрутизирующим коммутатором в случае технологии SpW) в качестве центрального узла. Как наиболее вероятный кандидат на сетевую архитектуру БКУ для МКА определена топология «двойная звезда», представленная на рис. 1.

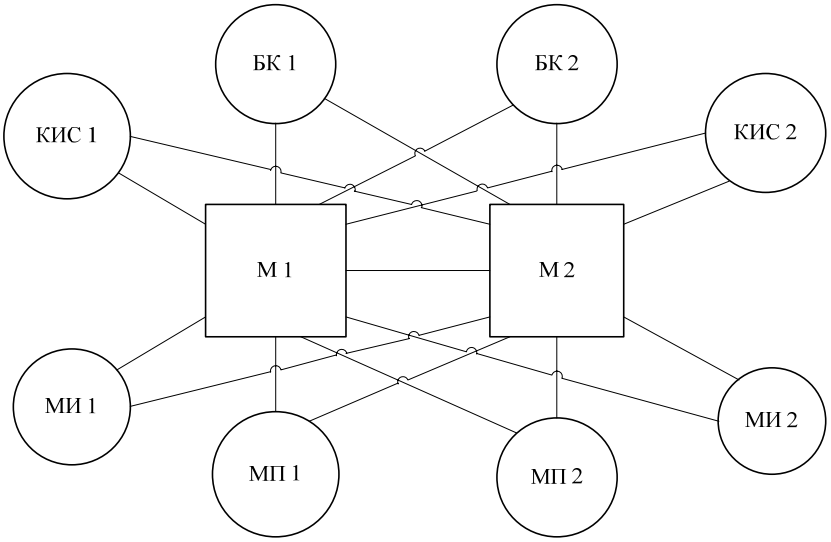


Рис. 1. Сетевая резервируемая архитектура БКУ

Сетевая архитектура предполагает использование в качестве инфраструктурных компонентов «связку» двух маршрутизаторов (М), один из которых является активным, другой находится в «холодном» резерве. Маршрутизаторы связаны отдельным физическим линком. Для повышения надежности связь маршрутизаторов может обеспечиваться 2 физическими линками. К каждому маршрутизатору подключается свой полукомплект устройств, составляющих БКУ. Кроме того, каждое устройство из одного полукомплекта подключается к маршрутизатору другого полукомплекта. В текущий момент времени один полукомплект находится в активном режиме, другой – в «холодном» резерве. При отказе устройства из одного полукомплекта автоматически включается аналогичное устройство из другого полукомплекта.

Рассмотренная архитектура отличается простотой реализации механизмов резервирования и отвечает современным тенденциям в развитии космического приборостроения. Последние исследования показали, что аппаратура, находящаяся в «горячем» резерве, в большей степени подвержена отказам по накопленной дозе радиации, чем находящаяся в «холодном» резерве. Поэтому в настоящее время производители КА, учитывая современный уровень надежности ЭКБ, в большей степени отдают предпочтения «холодному» резерву относительного «горячего».

Рассмотренную сетевую архитектуру можно определить как наиболее оптимальную для МКА, имеющего небольшие значения для срока активного существования (САС) КА (от 2 до 5 лет). Он обеспечивает достаточную для МКА надежность при приемлемом уровне аппаратного резервирования. Для аппаратов со сроком САС более 5 лет представленная архитектура хорошо масштабируется до более высоких значений кратности резервирования: 2 или 3. Для аппаратов с совсем малым САС (1–2 года) и малым бюджетом разработки от второго маршрутизатора и резервного полукомплекта можно отказаться.

Маршрутизирующий коммутатор SpaceWire. Для построения разветвленных сетей SpaceWire используются маршрутизирующие коммутаторы. В настоящее время существует несколько различных реализаций коммутаторов SpW, выполненных в виде законченных микросхем или конфигурируемых СФ-блоков. Но применение этих решений в небольшом проекте затруднено из-за их высокой стоимости, к тому же не все реализации поддерживают такие функции, как адаптивная маршрутизация и широковещательные пакеты. Поэтому было решено создать свою реализацию СФ-блока коммутатора SpW.

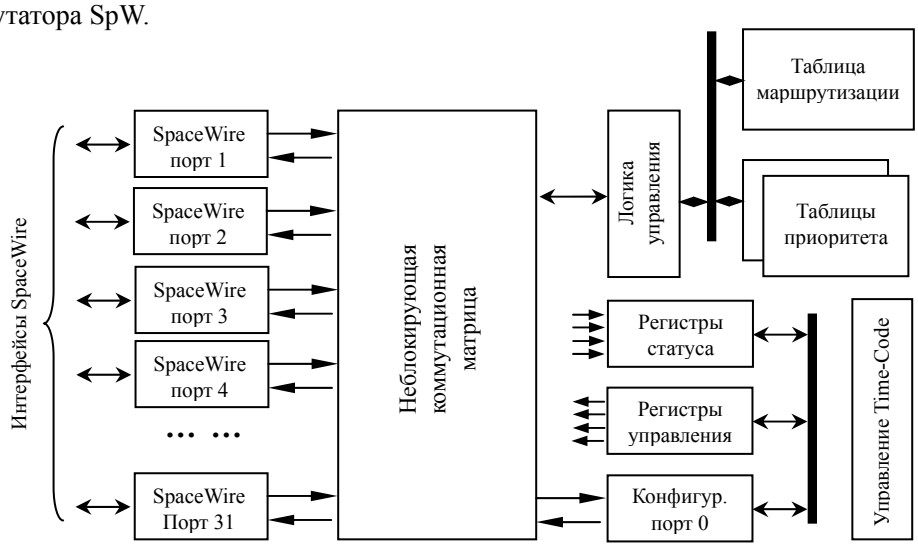


Рис. 2. Структурная схема маршрутизирующего коммутатора SpaceWire

На рис. 2 представлена структурная схема коммутатора с настраиваемым количеством портов SpW от 2 до 31. Все порты соединяются друг с другом с помощью неблокирующей коммутационной матрицы, которая позволяет установить прямой канал между ними. Причем уже установленные соединения не препятствуют созданию новых, если коммутируемые порты свободны.

Для коммутации пакетов с логической адресацией используется таблица маршрутизации и две таблицы приоритетов, доступ к которым производится последовательно с учетом приоритета запрашивающего порта (чем меньше номер порта, тем выше его приоритет). Это позволяет иметь только одну копию таблицы маршрутизации, но поскольку на определение адреса порта уходит всего 3 системных такта, то на производительность это существенно не влияет. Две таблицы приоритетов позволяют реализовать 3 уровня приоритета для каждого порта, что используется при адаптивной маршрутизации.

Реализованный алгоритм адаптивной маршрутизации имеет установку, разрешающую или запрещающую использовать порты с наименьшим приоритетом в случае, если имеются активные занятые порты с высоким приоритетом. В общем случае из таблицы маршрутизации будет выбран активный незанятый порт с наивысшим приоритетом (при нескольких свободных портах одного приоритета будет выбран с наименьшим номером). Использование регионально-логической адресации предусматривает необходимость удаления первого байта пересылаемого пакета. Для этого используется регистр, в котором устанавливаются номера региональных портов.

Дополнительно SpW-коммутатор поддерживает функцию широковещательного распространения пакета по сети. Эта функция может быть установлена для одного или нескольких логических адресов. При приходе пакета он будет отправлен на все порты, указанные в таблице маршрутизации для данного логического адреса.

Для конфигурирования используется внутренний нулевой порт, который поддерживает протокол RMAP в соответствии со стандартом ECSS-E-ST-50-52C [4]. RMAP позволяет читать и записывать данные непосредственно в регистры коммутатора.

Коммутатор позволяет собирать статусную информацию о количестве ошибок, связанных с ошибками маршрутизации пакета, превышением времени ожидания порта, разрывами SpW соединения. Кроме того, каждый порт имеет свой статусный регистр, в котором отражается более детальная информация о его состоянии.

Разработанный СФ-блок маршрутизирующего коммутатора SpW был использован в нескольких проектах, демонстрирующих разные варианты реализации сетевой архитектуры для МКА.

Аппаратный контроллер протокола RMAP. Протокол RMAP является протоколом для передачи служебных и информационных пакетов для конфигурации и взаимодействия сетевых устройств в сети SpW. Аппаратный в виде СФ-блока контроллер протокола RMAP позволяет упростить процедуры взаимодействия по данному протоколу узлов сети SpaceWire – бортовых систем КА.

RMAP-контроллер спроектирован как СФ-блок для включения в проекты типа система на кристалле с помощью внутрисистемной шины AMBA 2.0. Структура RMAP-контроллера показана на рис. 3.

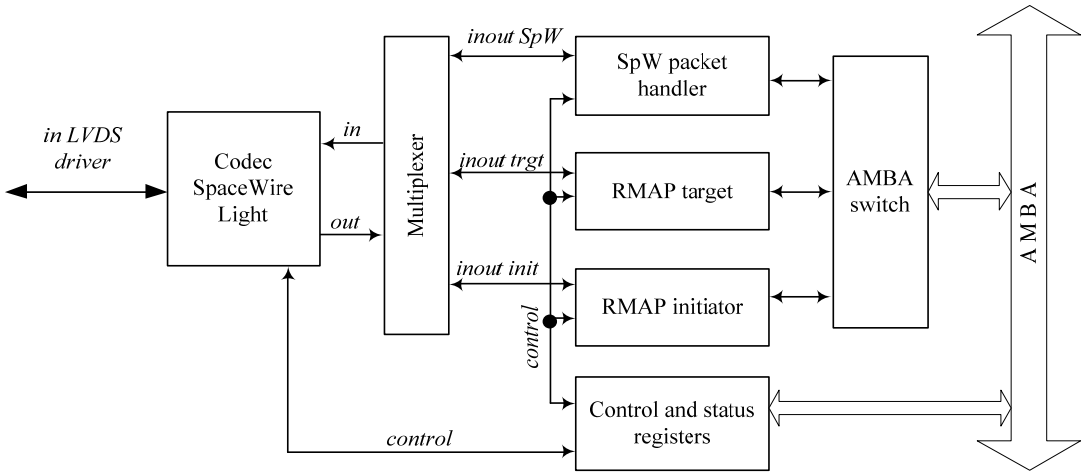


Рис. 3. Структура RMAP-контроллера

Входные и выходные сигналы присоединяются к драйверу LVDS физического уровня сети SpW. В качестве кодека сети SpaceWire использован открытый свободно распространяемый СФ-блок SpW Light [5]. RMAP-контроллер предназначен не только для обработки RMAP-пакетов, но и обычных пакетов сети SpW с помощью блока обработчика SpW-пакетов. Обработчик RMAP-пакетов состоит из блока приемника RMAP-target и блока передатчика RMAP-initiator. Переключение данных, поступающих из кодека SpW Light или в кодек SpW Light, осуществляется с помощью блока мультиплексора. Управление работой RMAP-контроллера осуществляется с помощью блока управляющих и статусных регистров.

По завершении верификационных испытаний СФ-блок контроллера RMAP будет использован в нескольких устройствах бортовой аппаратуры для малых и полноразмерных КА.

Варианты реализации сетевой архитектуры для малых космических аппаратов. Практические исследования заключались в реализации двух вариантов исполнения сетевой архитектуры для МКА, имеющих условные названия – сосредоточенная и распределенная.

В распределенной архитектуре устройства сети связаны традиционным способом – посредством кабельной сети. Сосредоточенная архитектура представляет собой моноблок, в котором взаимодействие составляющих устройств осуществляется не с помощью кабельной сети, а посредством межплатных разъемов. Обе архитектуры могут представлять интерес для разных групп заказчиков, тяготеющих к различным принципам построения бортовых систем. На рис. 4–5 представлен пример сосредоточенной сетевой архитектуры; на рис. 6 – пример распределенной архитектуры.

Первый пример является полнофункциональным бортовым комплексом управления (БКУ) для малого космического аппарата с резервируемой сетевой архитектурой, соответствующей схеме на рис. 1.

БКУ состоит из двух полукомплектов. Устройствами, входящими в каждый полукомплект, являются:

– модуль бортового компьютера, реализующий основные вычислительные и управляющие действия на борту МКА; в качестве процессора использован софт-процессор LEON 3, встраиваемый в ПЛИС типа flash-FPGA Actel;

– модуль низкочастотной части командно-измерительной системы, предназначенный, с одной стороны, для сбора телеметрических данных от систем КА, преобразования их в телеметрические пакеты и передачи пакетов в высокочастотную часть командно-измерительной системы (ВЧ КИС) для их передачи по радиоканалу; с другой стороны, для приема от ВЧ КИС телекоманд управления, их дешифрации и передачи по адресуемым системам КА, в основном в БК;

– модуль преобразования интерфейсов имеет чисто технологическую функцию; он предназначен для преобразования некоторого множества интерфейсов (RS232, CAN и др.), используемых системами космического аппарата, к интерфейсу SpW; кроме того, он может принимать аналоговые сигналы с датчиков и передавать сигналы на исполнительные устройства (ИУ);

– модуль питания предназначен для стабилизации напряжения, поступающего в БКУ от внешней бортовой питающей сети.

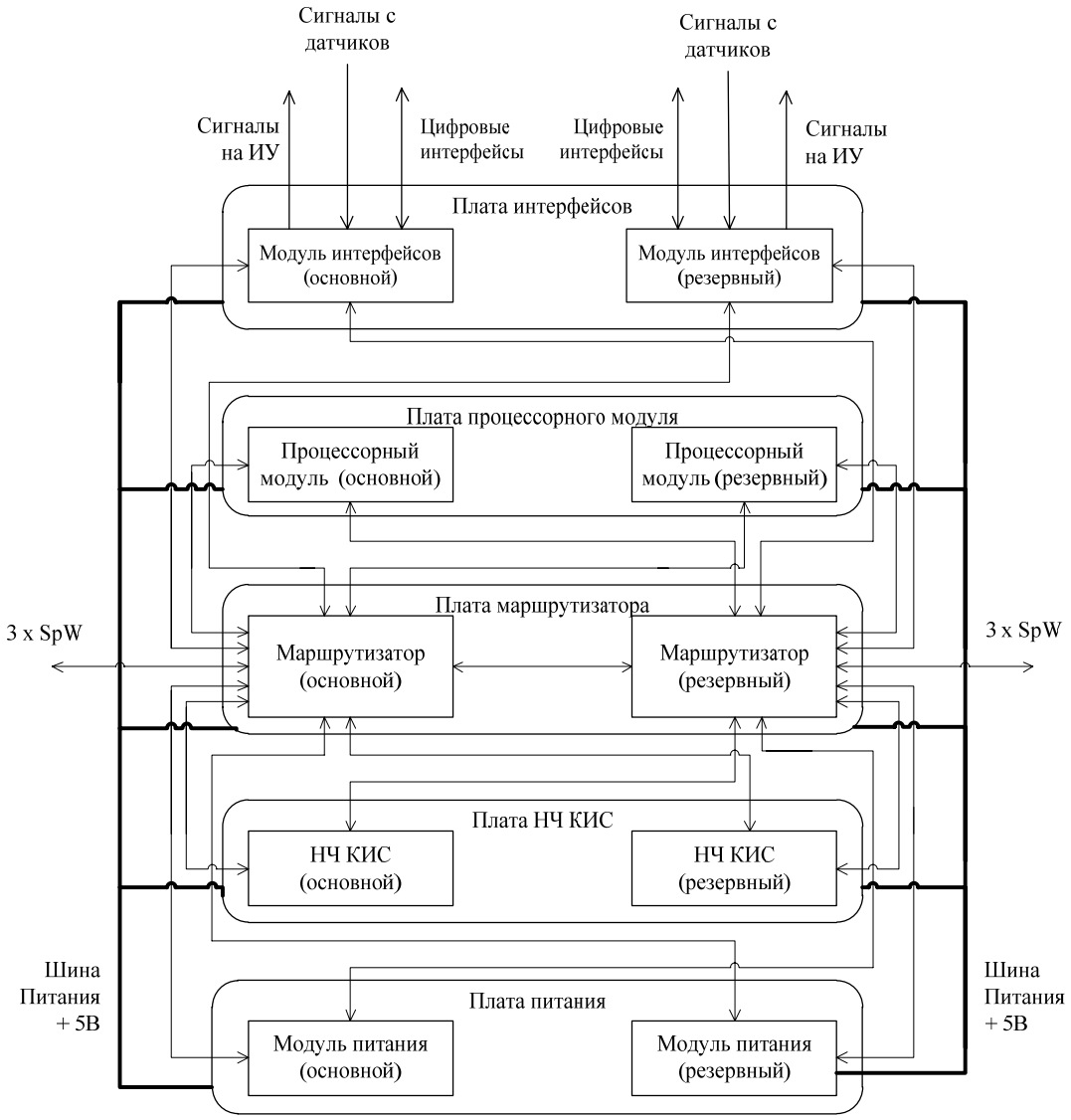


Рис. 4. Пример сосредоточенной сетевой архитектуры: структурная схема

Пример, представленный на рис. 6, является аппаратурой информационного обмена (АИО) для создания бортовых систем, распределенных по пространству МКА. АИО предназначена для создания сетевой инфраструктуры для различных подсистем МКА как служебных, так и подсистем по-

лезной нагрузки. Таким образом, АИО позволяет создавать структурированную по подсистемам (U-блокам) МКА бортовую сеть. АИО состоит из следующих устройств:

– маршрутизирующего коммутатора SpW на 4 внешних порта с функцией коммутации питания подключаемых к коммутатору устройств;

– однокристального процессорного модуля (бортового компьютера), состоящего из процессора Leon 3, встроенного коммутатора SpW с 4 внешними портами, интерфейсами CAN и Ethernet в одной ПЛИС;

– модуля расширения интерфейсов (многофункционального моста), SpW<>CAN, SpW<>SPI, SpW<>I2C.

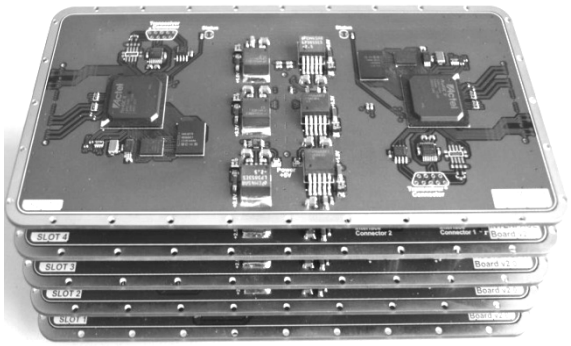
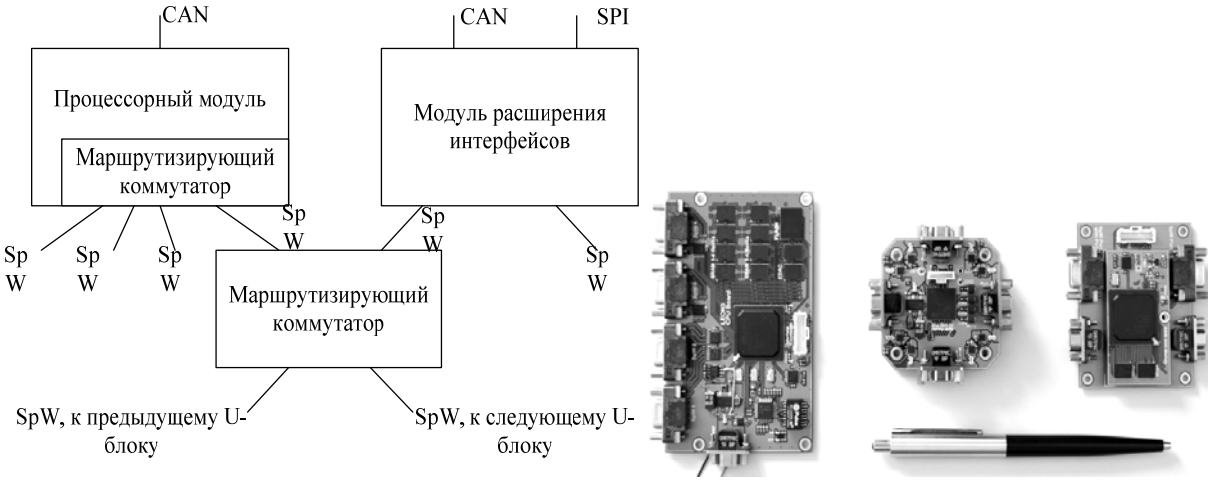


Рис. 5. Пример сосредоточенной сетевой архитектуры: внешний вид

АИО предназначена для МКА, не рассчитанных на длительные сроки активного существования. Поэтому резервирование устройств, составляющих АИО, не предусмотрено. Чтобы устройства АИО имели экстремально низкие размеры, часть устройств имеет мезонинную конструкцию.



а *б*

Рис. 6. Пример распределенной сетевой архитектуры: *а* – структурная схема; *б* – внешний вид устройств

Рассмотренные примеры исполнения сетевой архитектуры на основе SpW были реализованы в виде опытных образцов; работы по верификации проектов продолжаются. АИО к настоящему времени имеет летную реализацию для одного из отечественных МКА.

Направления дальнейших исследований и разработок. Дальнейшие работы в области сетевых космических технологий можно разделить на две группы: ближнесрочные и дальнесрочные. В ближнесрочной перспективе, учитывая накопленный опыт и переход разработок к практическому применению, требуется провести реинжиниринг разработанных СФ-блоков, а также продолжить работы по созданию комплексной системы функциональной верификации. В частности, уже сейчас начаты работы по созданию анализатора трафика (сниффера) сети SpW. Сниффер сети SpW, помимо других возможностей, будет внедрять одиночные ошибки в передаваемые по сети пакеты, что позволит отработать сбоеустойчивость устройств сети SpW к потерям данных вследствие неблагоприятных факторов космического пространства (ионизирующее излучение).

В отдаленной перспективе планируется разработка транспортного протокола передачи данных для структурированных сетей SpW. Система стандартов SpW не определяет транспортный уровень, поэтому разработчики космических систем вынуждены сами заниматься разработкой этого протокола. Известны несколько открытых спецификаций на протокол транспортного уровня, разработчиками которых являются известные зарубежные компании, занимающиеся сетью SpW. В России подобные работы также проводятся. Хотя сеть МКА имеет малый масштаб относительно полноразмерных КА, накопленный опыт показывает, что и для МКА простой и надежный протокол транспортного уровня необходим.

Заключение. В результате проведенных работ проведены исследования и разработки по созданию инфраструктурных устройств для сетевой резервируемой архитектуры взаимодействия бортовой аппаратуры малого космического аппарата на основе сетевой технологии SpaceWire.

Литература

1. MIL-STD-1533. Tutorial [Электронный ресурс]. – Режим доступа: http://www.aim-online.com/pdf/OVW1553.PDF, свободный (дата обращения: 24.05.2014).

2. ECSSE-ST-50-12C SpaceWire – Links, nodes, routers and networks. – European Cooperation for Space Standardization (ECSS), 2008 – 129 c.

3. Сетевая архитектура сопряжения комплексов бортового оборудования космического аппарата / В.Х. Ханов, А.В. Шахматов, М.Ю. Вергазов, С.А. Чекмарев // Вестник Сибирского государственного аэрокосмического университета. – 2012. – № 4 (44). – С. 148–151.

4. ECSSE-ST-50-52C SpaceWire – Remote memory access protocol. – European Cooperation for Space Standardization (ECSS), 2010. – 109 c.

5. Joris van Rantwijk, SpaceWire Light v20110709 [Электронный ресурс]. – Режим доступа: http://opencores.org/project,spacewire_light, свободный (дата обращения: 24.05.2014).

Ханов Владислав Ханифович
Доцент каф. безопасности информационных технологий
Сибирского государственного аэрокосмического университета им. акад. М.Ф. Решетнёва, Красноярск
Тел.: 8 (391) 2-62-18-47
Эл. почта: khvkh@sibsau.ru

Khanov V.Kh.

Network technologies for on-board systems spacecraft: development experience

A review conducted by developments in the implementation of network technologies for on-board systems of the spacecraft. Provides information on key developments conducted. Presents the results of a redundant network architecture onboard control complex, routing switch SpaceWire, RMAP controller. Identified options for creating network architecture and directions for further research and development.
Keywords: paceWire, network architecture, micro-spacecraft.

УДК 380.10

Н.Б. Голованова

Формирование подходов к оценке экономической безопасности субъекта хозяйствования

Рассмотрены теоретико-методические вопросы оценки экономической безопасности субъекта хозяйствования, исследованные в рамках выделенных автором подходов к оценке. Предложены критерии сравнения сформированных подходов, позволяющие оценить потенциал выделенных подходов.

Ключевые слова: экономическая безопасность, оценка экономической безопасности, классификация подходов к оценке безопасности объекта, системный, функциональный, процессный, ресурсный, причинный подходы, инструменты измерения и оценки экономической безопасности.

Вопросы безопасности вообще и экономической безопасности в частности в настоящее время вызывают повышенный интерес, став как самостоятельным направлением научных исследований, так и объектом практической, прежде всего управленческой, деятельности. Многообразие окружающей нас объективной реальности позволяет выделить множество объектов безопасности, к числу которых могут быть отнесены и субъекты хозяйственной деятельности, ключевой функцией которых является осуществление экономической деятельности, т.е. производство материальных благ и оказание услуг, необходимых человеку и обществу в целом.

Если обратиться к официальным документам, то, строго говоря, ни в одном из них непосредственного выделения субъекта хозяйствования как объекта безопасности нет. Так, в Законе РФ «О безопасности» от 5 марта 1992 г. [1], в Стратегии национальной безопасности РФ до 2020 г. [2] в качестве объектов безопасности выделены личность, общество и государство. В новом ФЗ № 390-ФЗ от 28.12.2010 «О безопасности», который признал утратившим силу Закон «О безопасности» 1992 г., указание на объекты безопасности вообще отсутствует, а вместо объектов безопасности в законе названы ее виды: безопасность государства, общественная безопасность, экологическая безопасность, безопасность личности и иные виды безопасности [3]. Лишь в принятой Стратегии экономической безопасности Российской Федерации, одобренной указом Президента РФ от 29 апреля 1996 г., в числе уже объектов экономической безопасности, помимо личности, общества и государства, выделены и основные элементы экономической системы [4], к которым, очевидно, могут быть отнесены и хозяйствующие субъекты.

Отсутствие легитимного признания субъекта хозяйствования как объекта безопасности вовсе не означает, что такое выделение неправомерно и необоснованно. Напротив, именно субъект хозяйствования является базовым, первичным элементом любой экономической системы, в том числе, рыночного типа. А это значит, что качество и уровень развития экономической системы в значительной степени определяются качеством составляющих ее элементов, т.е. выделение субъекта хозяйствования как объекта безопасности не только возможно, но и целесообразно и необходимо.

Принимая во внимание положения ГК РФ, под субъектом хозяйствования будем понимать юридическое лицо – организацию, которая имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество и отвечает по своим обязательствам этим имуществом, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде, функционирует в определенной организационно-правовой форме, предусмотренной ГК РФ [5].

За период становления и развития рыночных отношений в российской научной, учебной литературе, в диссертационных исследованиях и методических разработках детально рассмотрены вопросы менеджмента организации в новых условиях хозяйствования, построения организационных структур предприятия и систем управления, систем бухгалтерского и управленческого учета, антикризисного управления и риск-менеджмента. Однако в большинстве случаев все перечисленные вопросы исследуются без учета проблем экономической безопасности такого сложного комплекса,

каким является современный хозяйствующий субъект, что требует обстоятельной проработки широкого спектра проблем, начиная от определения сущности самого понятия – экономическая безопасность и заканчивая построением систем обеспечения экономической безопасности организации. Правда, справедливости ради надо заметить, что в исследовании систем, осуществляющих экономическую деятельность, изучение безопасности как системного свойства является относительно новым направлением, ставшим реакцией научного сообщества на проблему их сохранения и выживания в связи с повышением сложности и динамичности среды функционирования. Поэтому это в определенной степени объясняет и оправдывает недостаток теоретических разработок, еще больше повышая их актуальность и значимость.

Одним из наименее изученных, но вместе с тем имеющих практическую значимость и ценность является вопрос оценки экономической безопасности субъектов хозяйствования. Именно результаты оценки ложатся в основу выработки мер управленческих воздействий по стабилизации деятельности субъекта хозяйствования. И очевидно, что чем достовернее и своевременнее будет оценка экономической безопасности, тем более обоснованными и действенными будут меры по ее обеспечению.

Рассмотрение изложенных в научных публикациях взглядов на экономическую безопасность как свойства субъекта хозяйствования и ее оценку позволяет выделить следующие негативные факторы:

1) узкое понимание экономической безопасности как способности субъекта хозяйствования противодействовать противоправным действиям субъектов внешней среды;

2) сведение экономической безопасности к характеристике финансового состояния и результатов хозяйственной деятельности и как следствие сужение диапазона характеристики хозяйствующего субъекта;

3) отождествление оценки экономической безопасности с процедурой традиционного мониторинга состояния хозяйствующего субъекта;

4) использование традиционного инструментария, не учитывающего новые тенденции в развитии и управлении хозяйствующими субъектами;

5) использование при оценке в качестве базы сравнения внутренних организационных ориентиров вместо объективно содержательных, повышающих качество оценки;

6) сведение оценки экономической безопасности к инструментальному средству антикризисного управления и выработке антикризисных мер для выполнения аналитической, информационной и контрольной функции при минимизации мотивирующей функции оценки.

Недостаточная разработанность вопросов оценки экономической безопасности и многообразие существующих взглядов на понимание сущности экономической безопасности, с одной стороны, и необходимость их обобщения и систематизации как основы эффективной реализации оценки экономической безопасности – с другой, актуализирует вопрос о формировании основных подходов к ее оценке.

По своему содержанию оценка экономической безопасности представляет собой целенаправленный процесс установления соотношения характеристик предмета оценки определенным, заранее установленным критериям, а задача оценки может быть определена как вынесение обоснованного суждения о защищенности хозяйствующего субъекта и возможности достижения им организационных целей в условиях внутренних и внешних возмущений, представляющих опасность для выживания.

В результате проведенного исследования было выделено пять подходов, каждый из которых основан на определенном понимании того, что оценивается [6–11], т.е. в качестве классификационного признака использовался предмет оценки: системный, функциональный, процессный, ресурсный и причинный. Первые четыре подхода относятся к онтологическим, т.е. исследование сосредоточено на самом объекте исследования – субъекте хозяйствования; последний – к казуальным, т.е., предполагающим изучение факторов, воздействующих на объект.

Выделение предмета оценки в качестве основы формирования подходов к оценке является не случайным, так как от этого зависят все последующие действия. Несмотря на общее признание значимости вопросов обеспечения безопасности, как это ни странно, до сих пор в официальных документах РФ отсутствует определение безопасности вообще и экономической безопасности в частности. Так, в уже упоминавшемся Законе РФ 1992 г. безопасность была определена как защищенность жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Однако в дальнейшем этот закон утратил силу, и был введен Закон РФ «О безопасности» 2010 г., в

котором понятие безопасности отсутствует. Это привело к появлению различных толкований понятия экономической безопасности, а значит, и подходы к оценке могут быть разные.

Остановимся на краткой характеристике предлагаемых подходов.

Системный подход. Выделение и формирование данного подхода является наиболее очевидным, ибо системное представление хозяйствующего субъекта представляется на сегодняшний день наиболее логичным и структурированным инструментом его изучения. Данный подход основан на понимании экономической безопасности субъекта хозяйствования как такого его состояния, при котором использование ресурсов эффективно и обеспечивает устойчивое функционирование хозяйствующего субъекта в настоящем и будущем. При этом состояние рассматривается как совокупность параметров, характеризующих его функционирование, как результирующая реакция субъекта хозяйствования на возмущения внешней среды и внутренние изменения [12].

Так как реакция на одни и те же возмущения может быть различной, то существует множество состояний, а значит, многовариантность развития хозяйствующего субъекта. Это возможное множество включает как область опасных, так и безопасных состояний, разделенных границей безопасности, каждая точка которой определяет параметры порогового, критического состояния хозяйствующего субъекта. Таким образом, с позиции теории систем экономическая безопасность субъекта хозяйствования – это его нахождение в пространстве безопасных состояний. В этом случае оценка экономической безопасности заключается в определении положения субъекта хозяйствования относительно границы безопасности, а показателем безопасности будет расстояние от текущего (фактического) состояния хозяйствующего субъекта до границы безопасности. В идеале оценка экономической безопасности путем сравнения текущего и критического состояния субъекта хозяйствования требует построения обобщающего показателя состояния, которое может быть осуществлено путем аддитивной или мультипликативной свертки частных показателей состояния.

Реализация системного подхода к оценке экономической безопасности, таким образом, предполагает решение двух основных вопросов:

- описание состояния хозяйствующего субъекта с использованием какого-либо инструмента;
- установление границы, отделяющей множество безопасных состояний от опасных, т.е. пороговых значений состояния хозяйствующего субъекта.

При ясности и очевидности теоретических положений оценки экономической безопасности через состояние хозяйствующего субъекта при переходе к практической реализации возникает ряд проблем как при характеристике текущего состояния, так и при определении границ безопасности:

- проблема доступности измерения всех аспектов функционирования хозяйствующего субъекта, достаточного для идентификации состояния;
- отсутствие эффективного метода построения границ экономической безопасности;
- запаздывающий характер оценки безопасности, приводящий к задержке принятия решения: факт наличия опасности устанавливается по уже сложившемуся состоянию, что позволяет использовать только меры реактивного характера и исключает возможность превентивных мер;
- отсутствие шкалы оценивания значения показателя экономической безопасности.

В основе **функционального подхода** лежит понимание экономической безопасности как совокупности внутренних условий и факторов, создающих опасность жизненно важным интересам субъекта хозяйствования. Возможность формирования функционального подхода связана с тем, что безопасность является комплексным понятием, в рамках которого могут быть выделены функциональные направления, каждое из которых отражает определенную сторону функционирования системы: производственная, информационная, финансовая, технологическая, социальная и другая безопасность. Осуществляя декомпозицию общей безопасности на составляющие, мы тем самым разбиваем общую задачу оценки (каковой она является при использовании системного подхода), снимая имеющиеся затруднения (в частности, выделения области безопасных состояний). В этом случае логично считать, что экономическая безопасность отражает экономическую составляющую. Но главная функция хозяйствующего субъекта состоит именно в осуществлении экономической деятельности, вступление, прежде всего, в экономические отношения, что и определяет сам факт создания и функционирования хозяйствующего субъекта [12]. То есть для хозяйствующего субъекта экономическая составляющая является определяющей, подчиняющей все другие аспекты безопасности, результирующей все ее функциональные аспекты. Если наши рассуждения верны, то в этом случае экономическая безопасность обретает статус общей безопасности; а все аспекты безопасно-

сти выступают как факторы, влияющие на экономическую безопасность, и эта зависимость при желании может быть выражена аналитически.

Учитывая, что теоретически может быть выделено много аспектов общей, экономической, безопасности, при проведении оценки можно ограничиться лишь отдельными ее видами, которые характеризуют наиболее значимые и критичные факторы безопасности, т.е. выстроить приоритеты факторов по их влиянию на общую безопасность. В этом случае, оценивая экономическую безопасность, во внимание будут приняты только наиболее существенные аспекты, для которых и определяется область допустимых значений.

Оценка безопасности в данном случае заключается в нахождении частных показателей безопасности, которые могут быть получены как отклонение фактического текущего значения определенной составляющей деятельности хозяйствующего субъекта от нормативного значения.

Процессный подход к оценке экономической безопасности предполагает характеристику процесса обеспечения безопасности и опирается на понимание экономической безопасности как непрерывного процесса обеспечения на предприятии, находящемся в определенном внешнем окружении и подверженном внутренним изменениям, стабильности его функционирования и созданию возможностей для его развития. В данном случае оценка экономической безопасности сводится фактически к определению эффективности мер по обеспечению безопасности.

Ресурсный подход концентрирует внимание на выявлении и оценке сильных сторон хозяйствующего субъекта, которые обеспечиваются наличием и, что более важно, использованием имеющихся ресурсов и способностей. Выделение данного подхода соответствует современным представлениям о хозяйствующем в условиях высококонкурентной рыночной экономики субъекте: именно ресурсы и способности становятся основными детерминантами эффективной деятельности, основным фактором получения прибыли. Смещение центра тяжести при изучении хозяйствующего субъекта с анализа воздействия внешней среды на изучение внутренних возможностей связано с тем, что в условиях высокой неопределенности среды стратегия адаптации к происходящим изменениям становится малоэффективной. И только усилия самого субъекта хозяйствования, обладающего некой совокупностью ресурсов и способностей, обеспечивает устойчивое основание для своего функционирования. Вообще чем сильнее размах изменений во внешней среде, тем выше вероятность того, что именно внутренние ресурсы и способности станут фундаментом для долгосрочного развития [14].

С позиций ресурсного подхода экономическая безопасность субъекта хозяйствования – это такое состояние и использование его материальных, нематериальных и человеческих ресурсов, которое обеспечивает хозяйствующему субъекту устойчивые конкурентные позиции. Иными словами, экономическая безопасность – это способность хозяйствующего субъекта, эффективно используя свои организационные ресурсы, удерживать и наращивать свои конкурентные позиции. Следует обратить внимание, что безопасность субъекта хозяйствования обеспечивается не просто наличием ресурсов (это лишь производственные активы хозяйствующего субъекта), а способностью их согласованного и продуктивного использования: по отдельности ресурсы не создают конкурентного преимущества; они должны быть задействованы все вместе, только тогда они формируют организационную способность, обеспечивающую эффективную деятельность субъекта хозяйствования.

В соответствии с ресурсным подходом задача оценки экономической безопасности сводится к оценке организационных ресурсов и способностей и их влияния на положение хозяйствующего субъекта во внешней среде. Показателем экономической безопасности будет в данном случае изменение рыночной позиции.

Оценка ресурсов проводится по двум основным критериям: во-первых, это важность, т.е. понимание того, какие ресурсы и способности наиболее важны для приобретения устойчивого конкурентного преимущества; во-вторых, какие у ресурсов и способностей есть слабые и сильные стороны по сравнению с конкурентами. Существующая практика, как правило, ориентирована на выделение и оценку лишь финансовых и материальных ресурсов, размер которых отражается в бухгалтерском балансе. Однако в современных условиях более сильное влияние на экономическую безопасность оказывают нематериальные ресурсы, прежде всего технологические.

В качестве инструмента оценки организационных ресурсов и способностей могут быть использованы экспертные оценки, где субъектами оценки являются топ-менеджеры. Но в этом случае возникает большой риск получения необъективной оценки, переоценки собственных возможностей. Минимизация влияния субъективного фактора, с одной стороны, с другой – переход к количествен-

ной оценке организационных способностей, могут быть реализованы с использованием такого инструмента как бенчмаркинг. Это инструмент представляет собой процесс идентификации лучших практик любых организаций мира, которые помогут организации повысить эффективность своей деятельности [14]. Показателем экономической безопасности хозяйствующего субъекта при использовании бенчмаркинга будет величина разрыва, существующего между организационными способностями хозяйствующего субъекта и организации (организаций), принятых за базу сравнения. В конечном итоге оценка экономической безопасности посредством организационных способностей заключается не столько в точных количественных значениях, сколько в идеях и понимании происходящего.

Наконец, одним из подходов к оценке экономической безопасности хозяйствующего субъекта может стать **причинный (каузальный) подход**. Основой его выделения является понимание экономической безопасности как совокупности внешних условий и факторов, создающих опасность для функционирования хозяйствующего субъекта и реализации организационных интересов.

Принципиальное отличие последнего от ранее рассмотренных состоит в том, что при оценке экономической безопасности происходит переход от изучения внутренней среды к наблюдению за внешней средой, а точнее, возмущениями, идущими от внешней среды, т.е. происходит замена изучения и оценки следствия анализом и оценкой причин. Оценка экономической безопасности будет состоять в определении влияния существующих и потенциальных опасностей на поведение субъекта хозяйствования.

В принципе, причинный подход следует оценить как достаточно позитивный, так как его реализация позволяет выявить и проанализировать причины нарушения экономической безопасности, т.е. выявить существующие и потенциальные угрозы для хозяйствующего субъекта. Такой подход обеспечивает выигрыш во времени, позволяя осуществлять меры не реактивного характера, а превентивного. Проблемы, возникающие при его реализации, связаны с двумя обстоятельствами. Во-первых, поскольку среда функционирования субъекта хозяйствования разнообразна, то существует достаточно много областей безопасности, что существенно осложняет обеспечение экономической безопасности хозяйствующего субъекта. Диагностика всего диапазона внешних воздействий сделает анализ среды малоэффективным, как с точки зрения затрат, так и с точки зрения информационной перегрузки. При большом количестве и широком диапазоне внешних воздействий анализ окружающей среды, а значит, и оценка угроз, становятся весьма затруднительными. Второй проблемой являются трудности, а порой недоступность измерения воздействий внешней среды, что усложняет построение системы предотвращения угроз.

Отправной точкой для анализа и оценки внешних воздействий с точки зрения опасности для хозяйствующего субъекта может стать определенная систематизация информации о внешней среде. Например, в качестве одного из инструментов такой систематизации является известный в стратегическом анализе PEST (или в другой интерпретации – STEP) – анализ, позволяющий классифицировать внешние возмущения по источникам на политические, экономические, социальные и технологические. Другим вариантом является разделение внешней среды по степени «близости» к хозяйствующему субъекту. Предпосылкой эффективной оценки экономической безопасности может стать выделение жизненно важных для хозяйствующего субъекта факторов внешнего воздействия, к числу которых следует отнести клиентов, поставщиков и конкурентов, которое позволит сузить перечень угроз, ограничив их факторами прямого, непосредственного воздействия.

Если в качестве отправной точки оценки экономической безопасности принять уровень прибыли, то оценка в рамках причинного подхода будет состоять в определении отклонения потенциальной прибыли (значение которой может быть получено путем моделирования зависимости прибыли хозяйствующего субъекта от внешних негативных воздействий) либо от значения точки безубыточности, либо, что предпочтительнее с точки зрения эффективности оценки, от среднего уровня прибыли в отрасли, к которой относится хозяйствующий субъект.

Обобщение рассмотренных теоретико-методических вопросов оценки экономической безопасности субъекта хозяйствования позволяет провести сравнительную характеристику предложенных подходов, что позволит лицу, принимающему решение, оценить потенциал каждого из подходов (таблица).

Очевидно, что все рассмотренные подходы имеют как определенные достоинства, так и недостатки, а качество получаемой на их основе оценки экономической безопасности зависит от большо-

го числа факторов. В конечном счете выбор подхода зависит от лица, принимающего решение, от его профессиональной квалификации и определяется прагматическими соображениями.

Сравнительный анализ подходов к оценке экономической безопасности

Признак сравнения	Системный подход	Функциональный подход	Процессный подход	Ресурсный подход	Причинный подход
Первичное понятие	ЭБ – состояние	ЭБ – совокупность функциональных видов безопасности	ЭБ – непрерывный процесс обеспечения безопасности	ЭБ – совокупность ресурсов и организационных способностей	ЭБ – совокупность опасных факторов и условий внешней среды
Предмет оценки	Состояние СХ	Отдельные виды безопасности	Процесс обеспечения безопасности	Организационные ресурсы и способности	Угрозы внешней среды
Стратегическая цель оценки	Повышение устойчивости СХ	Повышение устойчивости СХ	Повышение устойчивости СХ	Развитие и укрепление конкурентной позиции	Выживание СХ
Инструментарий оценки	Ключевые показатели деятельности СХ. Модели деятельности, методы корреляционно-регресионного анализа	Показатели функциональных элементов деятельности СХ, функциональная модель безопасности	Показатели результативности принимаемых мер, критерии эффективности мер	Методы стратегического анализа	Методы факторного анализа
Характер оценки	Показатель ЭБ – апостериорная	Апостериорная	Априорная и апостериорная	Априорная	Априорная

ЭБ – экономическая безопасность; СХ – субъект хозяйствования.

В заключение отметим, что в задачи нашего исследования не входил вопрос критической оценки существующих определений экономической безопасности и выделения предпочтительных подходов ее оценки. Вместе с тем считаем необходимым высказать авторскую позицию, которая заключается в понимании экономической безопасности как характерном свойстве – свойстве сопротивляемости хозяйствующего субъекта, выражающем его способность поддерживать свое нормальное функционирование и обеспечивать развитие без нарушения целостности в условиях внешних и внутренних возмущений и воздействий независимо от них. И с этой точки зрения наиболее адекватным предложенному толкованию экономической безопасности является использование ресурсного подхода к ее оценке как имеющего четкую стратегическую направленность и отражающую специфические особенности функционирования субъекта хозяйствования в условиях современной рыночной экономики.

Литература

1. Закон РФ от 5 марта 1992 г. № 2446-I «О безопасности» (с изменениями и дополнениями) [Электронный ресурс]. – Режим доступа: http://base.garant.ru/10136200/, свободный (дата обращения: 20.05.2014).

2. Указ Президента РФ от 12 мая 2009 г. № 537 «О стратегии национальной безопасности Российской Федерации до 2020 года» [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2009/05/19/strategia-dok.html, свободный (дата обращения: 20.05.2014).

3. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2010/12/29/bezopasnost-dok.html, свободный (дата обращения: 20.05.2014).

4. Указ Президента РФ от 29 апреля 1996 г. № 608 «О государственной стратегии экономической безопасности Российской Федерации (основных положениях)» [Электронный ресурс]. – Режим доступа: http://base.garant.ru/106503/, свободный (дата обращения: 20.05.2014).

5. Гражданский кодекс Российской Федерации (ГК РФ) [Электронный ресурс]. – Режим доступа: http://base.garant.ru/10164072/, свободный (дата обращения: 20.05.2014).

6. Бельков О.А. Понятийно-категориальный аппарат концепции национальной безопасности // Безопасность. – 1994. – № 3. – С. 91–94.

7. Бизнес и безопасность. Толковый терминологический словарь / Под ред. О.Г. Румянцева. – М.: Бек, 1995. – 336 с.

8. Ващекин Н.П. Безопасность предпринимательской деятельности: учеб. пособие / Н.П. Ващекин, М.И. Дзлиев, А.Д. Урсул. – М.: Экономика, 2002. – 334 с.

9. Клейнер Г. Системная парадигма и теория предприятия // Вопросы экономики. – 2002. – № 10. – С. 47–69.

10. Основы экономической безопасности (Государство, регион, предприятие, личность) / Под ред. Е.А. Олейникова. – М.: ЗАО «Бизнес-школа «Интел-синтез», 1997. – 288 с.

11. Половнев К.С. Механизм обеспечения экономической безопасности промышленного предприятия: дис. ... канд. экон. наук: 08.00.05. – Екатеринбург, 2002. – 134 с.

12. Могилевский В.Д. Методология систем (вербальный подход). – М.: Экономика, 1999. – 251 с.

13. Ковалев В.В. Финансовый учет и анализ: концептуальные основы. – М.: Финансы и статистика, 2004. – 720 с.

14. Грант Р.М. Современный стратегический анализ. – 5-е изд. – СПб.: Питер, 2008. – 560 с.

Голованова Наталия Борисовна
Д-р экон. наук, профессор, декан экономического факультета
Московского государственного университета приборостроения и информатики
Тел.: +7 (495) 964-91-54
Эл. почта: Golovanova_NB@mgupi.ru

Golovanova N.B.

Formation approaches to assessing the economic security of the economic entity

The article considers the theoretical and methodological issues of assessing the economic security of the economic entity researched within the allocated approaches of evaluation. Comparative description of via dedicated characteristics comparison allows to estimate the potential of each of the generated approaches.

Keywords: economic security, economic security assessment, classification of economic security evaluation approaches, system approach, the functional approach, process approach, resource-based approach, the causal approach, measurement tools and safety assessment.

ЭЛЕКТРОТЕХНИКА

УДК 629.7.054

П.Е. Гавриш, Г.Я. Михальченко

Построение системы управления частотой вращения бесконтактного двигателя постоянного тока

Рассматривается система управления частотой вращения бесконтактного двигателя постоянного тока. Отличительной особенностью системы является снижение запаздывания и накопления вычисляемой ошибки регулирования, позволяющее увеличить точность и быстродействие системы.

Ключевые слова: стабилизация частоты вращения, широтно-импульсная модуляция, двухфазный преобразователь частоты.

Одной из главных задач скоростных подсистем силовых гироскопических приборов космических аппаратов является реализация системы управления частотой вращения бесконтактного двигателя постоянного тока. Одним из доминирующих требований к такого рода электроприводам является обеспечение плавности вращения в районе нулевой частоты вращения и стабилизация угла положения ротора двигателя [1–3]. Среди множества решений практическое применение на борту космических аппаратов нашли системы с импульсным частотно-фазовым дискриминатором, на одном из входов которого формируется импульсный сигнал повышенной частоты по отношению к задающему сигналу, а на другом входе формируется сигнал повышенной частоты с датчика положения ротора [2]. Преобразование низкочастотных задающих сигналов в высокочастотные осуществляется в соответствии с выражениями:

$$U_0(\sin\Omega_з t\cos\omega_0 t+\cos\Omega_з t\sin\omega_0 t)=U_0\sin(\Omega_з+\omega_0)t\ ;$$

$$U_0(\cos\Omega_з t\cos\omega_0 t-\sin\Omega_з t\sin\omega_0 t)=U_0\cos(\Omega_з+\omega_0)t\ ,$$

где $\Omega_з$ – частота задающего воздействия, ω_0 – промежуточная повышенная частота.

Аналогично формируются сигналы текущей частоты вращения ротора в области повышенной частоты ($\Omega_{тек}+\omega_0$). Разность между этими сигналами и определяет ошибку регулирования угла положения ротора [4].

Такой путь построения системы регулирования характеризуется и рядом недостатков. Во-первых, использование однополосной модуляции [5] для преобразования низкочастотных аналоговых сигналов $\Omega_з$ и $\Omega_{тек}$ по двум координатам в сигналы высокой частоты $\Omega_з+\omega_0$ и $\Omega_{тек}+\omega_0$ в цепи формирования задающего сигнала и в цепи обратной связи неоправданно усложняет системы управления. Каждая из этих цепей включает по четыре умножителя и по два сумматора для получения сигнала ошибки на выходе фазового дискриминатора, что сопровождается снижением надежности.

Во-вторых, большое количество математических операций в цифровых системах управления сопровождается накоплением запаздывания в контуре регулирования и накопления вычисляемой ошибки регулирования, что приводит к ограничению быстродействия.

В-третьих, дискретное считывание информации о разности фаз по углу и обработка импульсной информации фазовым дискриминатором исключает возможность построения астатической системы регулирования с нулевой ошибкой в статическом режиме.

Для минимизации всех вышеперечисленных негативных факторов предлагается иной путь обработки сигналов задания и обратной связи по частоте вращения, исключающий использование однополосной модуляции. Структурная схема электропривода, реализующая этот путь, приведена на рис. 1. В целом система содержит бесконтактный двигатель постоянного тока (БДПТ) с двумя фазными обмотками, ротор которого связан с синусно-косинусным датчиком положения ротора ДПР. Двухфазный преобразователь частоты ДПЧ представляет собой два инвертора, формирующих на фазных обмотках переменные напряжения с широтно-импульсной модуляцией. Обработка информации с выходов ДПР реализуется двухвходовыми умножителями $УМ_1$ и $УМ_2$ и сумматором Σ_1. Сигнал ошибки регулирования на выходе пропорционально-интегрально-дифференциального регулятора (ПИД) является заданием для синусно-косинусного формирователя управляющих сигналов

($ФУС_1$ и $ФУС_2$) и через широтно-импульсный модулятор ШИМ синхронизирует моменты коммутации ключевых элементов БДПТ.

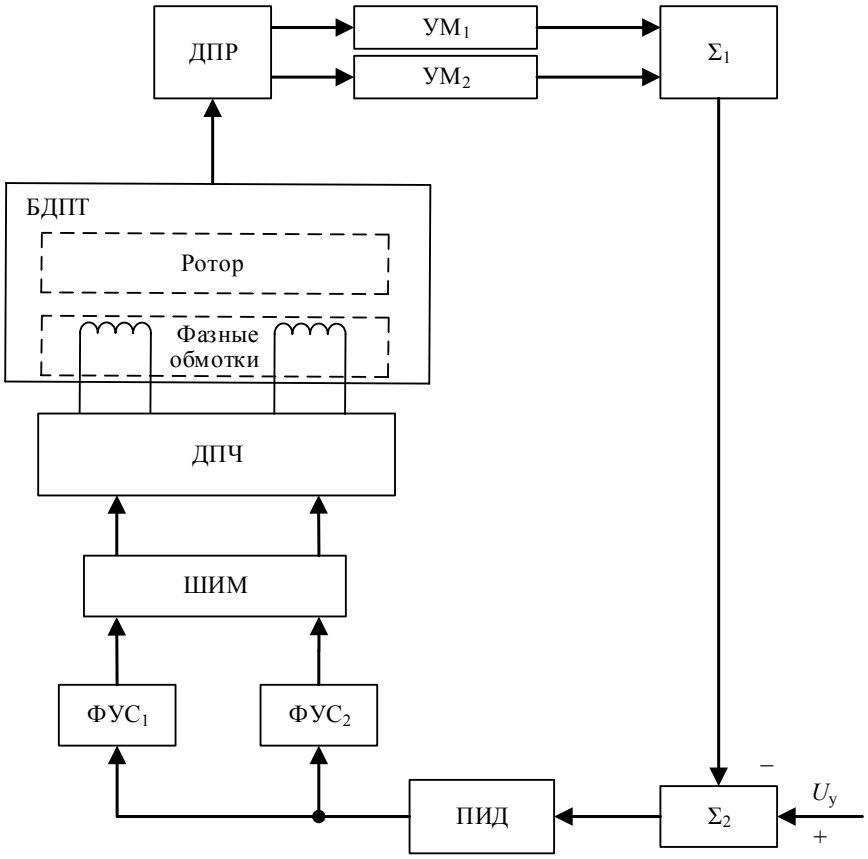


Рис. 1. Структурная схема системы регулирования частоты вращения бесконтактного двигателя постоянного тока

Система управления частотой вращения бесконтактного двигателя постоянного тока работает следующим образом.

На вход сумматора $\sum_2$ подается напряжение управления $U_у$, являющееся заданием на частоту вращения ротора двигателя. На второй вход этого сумматора подается постоянное выходное напряжение сумматора $\sum_1$ с отрицательным знаком. Напряжение на выходе сумматора $\sum_2$ поступает на вход ПИД-регулятора и представляет собой сигнал ошибки регулирования по частоте вращения ротора. Скорректированный сигнал ошибки поступает на входы синусно-косинусных формирователей управляющих сигналов $ФУС_1$, $ФУС_2$. Формирователи преобразуют напряжение сигнала ошибки в два низкочастотных сигнала $\sin\Omega_з t$ и $\cos\Omega_з t$, мгновенные значения частоты которых определяются в соответствии с выражением

$$\Omega_з = 2\pi \cdot 1{,}41 \frac{U_{ош}}{\text{const}}$$

и являются заданием по углу поворота ротора двигателя.

Эти сигналы поступают на управляющие входы широтно-импульсного модулятора ШИМ, который преобразуют их в сигналы управления транзисторами двухфазного преобразователя частоты ДПЧ. На статорных обмотках двигателя действуют напряжения, длительность импульсов которых изменяется пропорционально низкочастотным сигналам, и в этих обмотках протекают токи $I_m \sin(\Omega_з t + \psi)$ и $I_m \cos(\Omega_з t + \psi)$. При вращении ротора в установившемся режиме на выходах синусно-косинусного датчика положения ротора ДПР действуют два напряжения: $U_{ДПР1} = U_m \sin\Omega_{вр} t$ и $U_{ДПР2} = U_m \cos\Omega_{вр} t$. Эти напряжения поступают на попарно объединенные входы умножителей $УМ_1$, $УМ_2$, на выходах которых действуют напряжения:

$$U_1 = U_m \sin^2 \Omega_{вр} t = U_m(0{,}5 - 0{,}5\cos 2\Omega_{вр} t);$$

$$U_2 = U_m \cos^2 \Omega_{вр} t = U_m(0{,}5 + 0{,}5\cos 2\Omega_{вр} t).$$

Напряжения U_1, U_2, в свою очередь поступающие на входы первого сумматора $\sum_1$, преобразуются в постоянное напряжение

$$U_\Sigma = U_m(0{,}5 - 0{,}5\cos 2\Omega_{вр} t + 0{,}5 + 0{,}5\cos 2\Omega_{вр} t) = U_m,$$

которое является напряжением обратной связи, а его величина пропорциональна текущему значению частоты вращения ротора $\Omega_{вр}$. Астатизм системы регулирования достигается в устройстве интегральной составляющей ПИД-регулятора разностного сигнала ошибки регулирования $U_У - U_\Sigma$.

Для реализации однополярной реверсивной модуляции широтно-импульсный модулятор (рис. 2) выполнен в виде задающего генератора ЗГ, двух генераторов треугольных развертывающих напряжений $Г_{р.1}$, $Г_{р.2}$, фазы выходных напряжений которых смещены относительно друг друга на 180 электрических градусов, и четырех компараторов $К_1 – К_4$. Одни входы компараторов объединены и образуют управляющие входы модулятора, а каждый из генераторов развертывающих напряжений определяет длительность управляющих импульсов каждой стойки инверторов двухфазного преобразователя частоты.

Выходы компараторов широтно-импульсного модулятора осуществляют управление двухфазным преобразователем частоты.

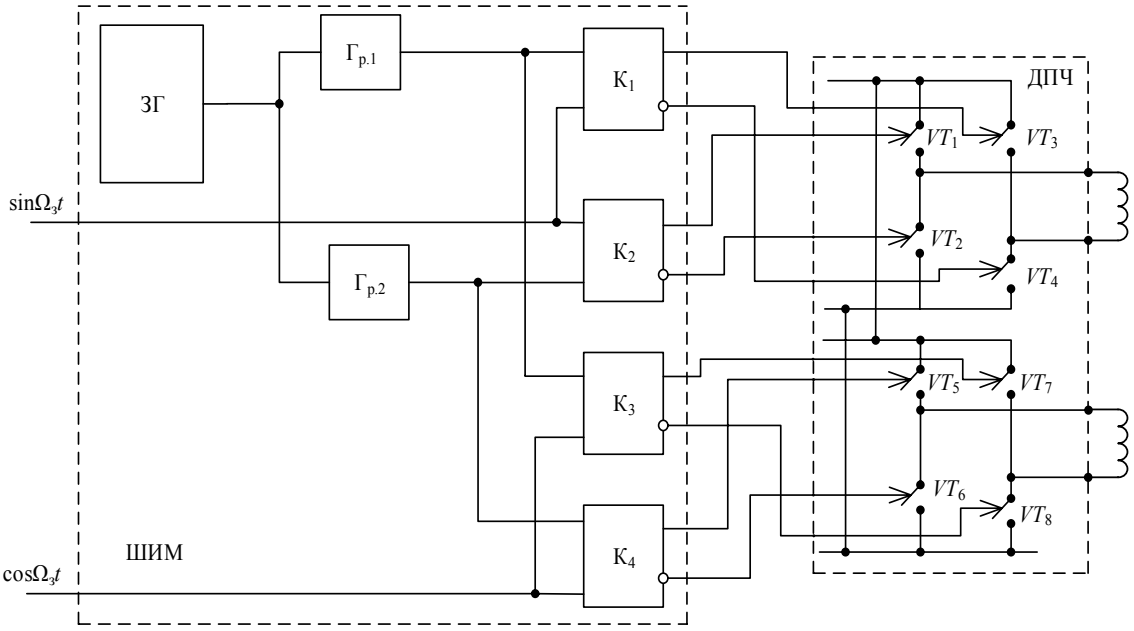


Рис. 2. Структурная схема ШИМ и ДПЧ

Структура двухфазного преобразователя частоты (см. рис. 2) представляет собой два мостовых инвертора на транзисторах $VT_1 – VT_4$ и $VT_5 – VT_8$, входные зажимы которых подключены к источнику постоянного напряжения, а к выходам подключены фазные обмотки БДПТ.

Работу широтно-импульсного модулятора и инверторов двухфазного преобразователя частоты поясняют временные диаграммы на рис. 3. Выходные импульсы U_1 задающего генератора синхронизируют работу генераторов треугольных развертывающих напряжений $Г_{р.1}$, $Г_{р.2}$ так, что на их выходах и на одних из входов компараторов $К_1$, $К_3$ и $К_2$, $К_4$ действуют напряжения U_2, U_3, фазы которых смещены относительно друг друга на 180 электрических градусов. На вторые объединенные входы компараторов $К_1$, $К_2$ и $К_3$, $К_4$ подается низкочастотный сигнал $\sin\Omega_з t$ или $\cos\Omega_з t$, сформированный из скорректированного сигнала ошибки регулирования. Рассмотрим работу инверторов.

На рис. 3 приняты следующие обозначения: U_1 – импульсная последовательность задающего генератора; U_2 – треугольное развертывающее напряжение; U_3 – смещенное по фазе треугольное развертывающее напряжение; U_4 – сигнал управляющих входов широтно-импульсных модуляторов $К_1$, $К_2$; U_5, U_6 – напряжение на прямых выводах компараторов; U_7, U_8 – напряжение на инверсных выводах компараторов; U_9 – выходное напряжение одного из инверторов.

Пусть с 0-го по 3-й тактовый период коммутации ШИМ действует положительное напряжение U_4, тогда на прямых выходах компараторов будут действовать импульсные последовательности U_5 и U_6, а на инверсных выходах – импульсные последовательности U_7, U_8 соответственно. Условимся, что низкий (нулевой) уровень этих последовательностей соответствует выключенному состоянию транзисторов VT_1–VT_4, а высокий уровень – включенному состоянию. При таком алгоритме проводящего состояния транзисторов: VT_3, $VT_1 – VT_1$, $VT_4 – VT_4$, $VT_2 – VT_4$, $VT_1 – VT_1$, VT_3 – на выходе инвертора будет действовать напряжение U_9 положительной полярности.

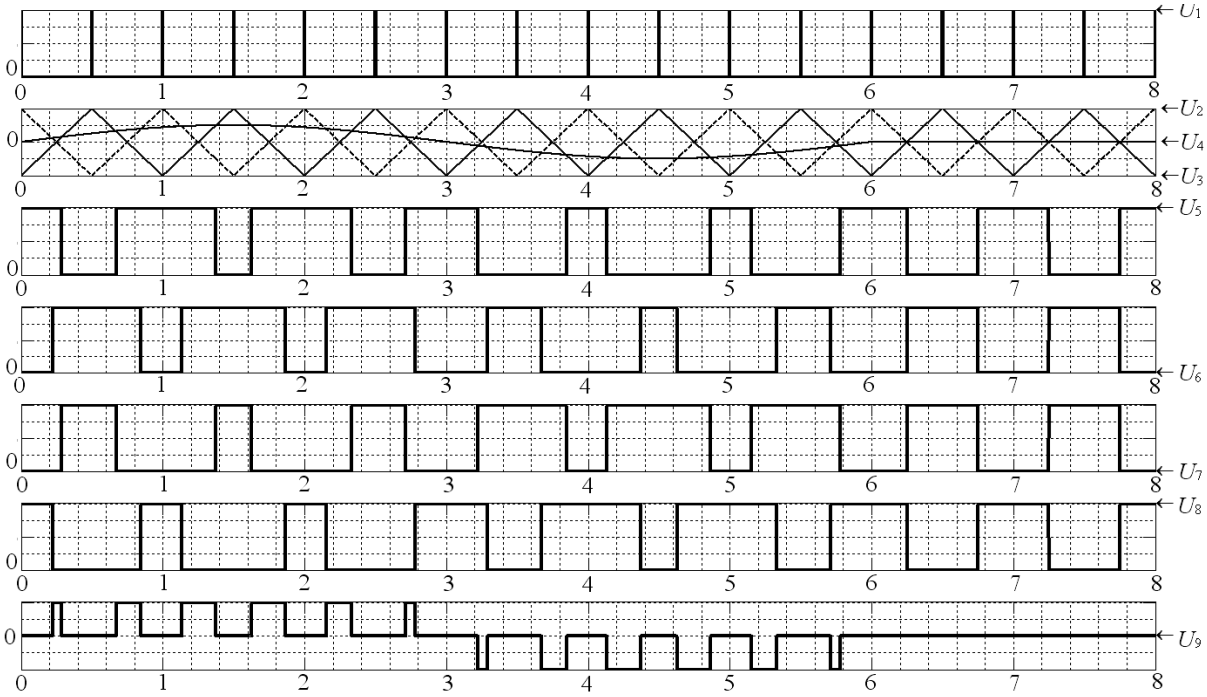


Рис. 3. Диаграмма работы широтно-импульсного модулятора при положительном управляющем сигнале

Когда сигнал U_4, действующий на управляющем входе широтно-импульсного модулятора, имеет отрицательное значение (3–6-тактовый период коммутации ШИМ), тогда на прямых выходах компараторов $К_3$, $К_4$ будут действовать импульсные последовательности U_5 и U_6, а на инверсных выходах – импульсные последовательности U_7, U_8 соответственно. При таком алгоритме проводящего состояния транзисторов: VT_1, $VT_3 – VT_3$, $VT_2 – VT_2$, $VT_4 – VT_2$, $VT_3 – VT_1$, VT_3 – на выходе инвертора будет действовать напряжение отрицательной полярности U_9.

Когда сигнал управляющего входа широтно-импульсного модулятора U_4 имеет нулевое значение (6–8-тактовый период коммутации ШИМ), то на управляющие входы транзисторов будут поступать импульсные последовательности U_5, U_6 и инверсные им последовательности U_7, U_8. При этом одновременно будут включены транзисторы VT_1, VT_3 или транзисторы VT_2, VT_4. Выходное напряжение инвертора при этом равно нулю U_9, поскольку фазные обмотки будут закорочены либо верхними ключами инвертора, либо нижними.

В системе регулирования частоты вращения ротора БДПТ на управляющие входы широтно-импульсного модулятора поступают низкочастотные сигналы $\sin\Omega_з t$ и $\cos\Omega_з t$, которые и определяют выходные напряжения инверторов двухфазного преобразователя частоты положительной и отрицательной полярности в соответствии с рассмотренным алгоритмом формирования выходного напряжения (рис. 3). В обмотках двигателя будут протекать токи $I_m \sin(\Omega_з t + \psi)$ и $I_m \cos(\Omega_з t + \psi)$. Таким образом, реализуется однополярная реверсивная модуляция фазных напряжений БДПТ.

Полученная замкнутая система регулирования по мгновенному значению частоты вращения является астатической за счет интегральной составляющей на выходе ПИД-регулятора, а регулирование угла поворота достигается фиксированием мгновенных значений низкочастотных сигналов управления $\sin\Omega_з t$ и $\cos\Omega_з t$ так, чтобы в фазных обмотках протекали постоянные токи необходимого уровня. Изменение направления вращения достигается изменением порядка чередования фаз на выходе синусно-косинусного формирователя управляющих сигналов ($\cos\Omega_з t$, $\sin\Omega_з t$).

Заключение. Исключение из системы управления избыточного количества умножителей и сумматоров, реализующих функции однополосной модуляции, позволяет повысить надежность системы. Снижение запаздывания и накопления вычисляемой ошибки регулирования позволяет увеличить точность и быстродействие системы регулирования частоты вращения бесконтактного двигателя.

Литература

1. Трахтенберг Р.М. Импульсные астатические системы электропривода с дискретным управлением. – М.: Энергоатомиздат, 1982. – 168 с.

2. Пат. 2291552 РФ, МПК H 02 P 6/08. Устройство для регулирования частоты вращения электродвигателя / Ю.Е. Муравяткин, С.В. Редькин, А.С. Авдиевич; заявл. 09.11.04; опубл. 10.01.07. Бюл. № 1. – 6 с.

3. Якимовский Д.О. Повышение точности управления моментом двигателя-маховика // Гироскопия и навигации. – 2008. – №3 (62). – С. 46–52.

4. Гавриш П.Е. Математические модели скоростных подсистем электроприводов силового гироскопического прибора / П.Е. Гавриш, Г.Я. Михальченко // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2013. – №4(30). – С. 103–109.

5. Гоноровский И.С. Радиотехнические цепи и сигналы: учебник для вузов. – М.: Радио и связь, 1986. – 512 с.

Гавриш Павел Евгеньевич
Аспирант каф. промышленной электроники (ПрЭ) ТУСУРа, инженер-электроник ОАО «НПЦ «Полюс»
Тел.: 8 (382-2) 55-40-29
Эл. почта: POLUS@online.tomsk.net, gavrish_pasha@mail.ru

Михальченко Геннадий Яковлевич
Д-р техн. наук, профессор каф. ПЭ
Тел.: 8 (382-2) 41-32-32
Эл. почта: kpe-tusur@yandex.ru, mail@comprel.ru

Gavrish P.E., Mikhalchenko G.Ya.

The control system by frequency of drive rotation construction

The control system by frequency of drive rotation is considered. The distinctive feature of the system are decrease in delay and accumulation of a regulation mistake, increase in accuracy and speed.

Keywords: rotation frequency stabilization, pulse-width modulation, biphase converter of frequency.

УДК 62-83: 621.313.392

А.Г. Гарганеев, Д.А. Падалко, А.В. Черватюк

Перспективы развития мехатронных систем с синхронно-гистерезисными электрическими машинами

На основе теории гистерезисного преобразования энергии и свойств магнитных материалов типа Fe-Cr-Co и Fe-Co-V анализируется перспективность применения в электрических машинах мехатронных систем материала типа Fe-Cr-Co. Приведены примеры мехатронных систем с импульсным намагничиванием материала ротора.

Ключевые слова: электрическая машина, полупроводниковый преобразователь, инвертор, постоянный магнит.

Интенсификация научно-технического прогресса предопределяет широкое применение в различных сферах человеческой жизни постоянных магнитов. Магнитные материалы на основе редкоземельных металлов в большой степени определяют развитие энергетики и энергосберегающих технологий, экологически чистых видов транспорта и модернизации традиционных его видов, а также бытовой техники, медицины и т.п. [1]. По различным экспертным оценкам, основной рост объёмов потребления магнитов на основе структуры Nd-Fe-B во многом будет определяться потребностями производителей электромашинных генераторов и электродвигателей.

Производство редкоземельных постоянных магнитов на основе сплавов системы Nd-Fe-B в мире является одной из наиболее динамично развивающихся отраслей промышленности. С момента освоения их промышленного выпуска (1987 г.) темпы среднегодового прироста объёмов их производства до 2000 г. составляли не менее 30%. Планируемые объёмы выпуска до 2020 г. приведены на рис. 1 [2]. В этой связи становится актуальным не только развитие отечественного производства магнитов на основе структур, в частности Nd-Fe-B и Sm_nCo_m, но и поиск альтернативных путей создания эффективных мехатронных систем (МС) с электрическими машинами на основе иных магнитотвердых материалов.

Рис. 1. Динамика роста мирового выпуска постоянных магнитов

Постановка задачи. При всей своей привлекательности «традиционные» постоянные магниты имеют и ряд недостатков, основными из которых являются:

1) высокая стоимость (особенно для структур $Sm_n Co_m$);
2) зависимость от иностранного производителя;
3) низкая механическая прочность и проблемы механической обработки;
4) старение;
5) возможность размагничивания при высоких температурах (низкая точка Кюри);
6) критичность к влаге (особенно для структур Nd-Fe-B);

7) сложность организации защит электродвигателя и генератора от короткого замыкания, прежде всего ввиду большого запаса электромагнитной энергии во вращающемся роторе (индукторе). В аварийных ситуациях «неисчезаемый» запас электромагнитной энергии ротора потенциально опасен;

8) проблемы применения во взрывоопасных средах ввиду потенциального запаса электромагнитной энергии в индукторе;

9) сложность технологического оборудования при сборке или ремонте электрических машин ввиду больших механических усилий, вызываемых взаимодействием магнитов с металлическими частями машины;

10) сложность управления электрической машиной по магнитной составляющей тока при скоростях выше синхронной.

Определенной альтернативой применению в МС постоянных магнитов вышеуказанных структур являются магнитотвердые материалы «гистерезисного типа». До настоящего времени гистерезисные электрические машины (ГМ) применялись в специальных технологиях: разделение изотопов урана (газовые ультрацентрифуги) и гироскопическая техника инерциальных систем навигации. Однако замечательные свойства гистерезисного материала позволяют создавать синхронные машины с «естественным» пусковым моментом, а применение режима «перевозбуждения» приближает эти машины по энергетическим показателям к машинам с постоянными магнитами. Область применения таких электрических машин может быть чрезвычайно обширной: от бытовой техники до промышленного применения. Из наиболее известных до настоящего времени структур следует отметить структуру типа Fe-Co-V («викаллой»), впрочем, недостатком которого является наличие дорогостоящего ванадия. Таким образом, задачей данной статьи является выявление технико-экономических аспектов применения ГМ с магнитными материалами, альтернативными викаллою.

Теоретические основы применения мехатронных систем с гистерезисными машинами на основе материала Fe-Cr-Co. Особенность ГМ состоит не только в природе образования момента, предусматривающего работу в синхронных и асинхронных режимах, но и в том, что магнитная «податливость» материала ротора делает ее полностью управляемой. Полная управляемость (помимо регулирования напряжения и частоты) достигается периодическим импульсным намагничиванием, позволяющим регулировать намагниченность материала ротора по амплитуде и фазе относительно синхронной системы координат. При этом на напряжение питания U_1 машины накладывают редкие импульсы с частотой $f_и$, фазой $\alpha_и$, длительностью $t_и$ и амплитудой $U_и$ (рис. 2). Импульсы создают дополнительное намагничивание материала ротора, не только приближая коэффициент мощности машины, близкий к единице, но и эффективно демпфируя угловые колебания ротора [4].

При скольжении машины (например, в режиме запуска) такое регулирование является «квазисинхронным», поскольку ротор в промежутках времени между импульсами намагничивания работает на участках угловых характеристик. Дополнительно следует отметить, что гистерезисная машина с инерционным ротором может работать при сверхнизких положительных или отрицательных скольжениях. В принципе, ГМ может работать и без импульсов, однако при этом ее энергетические характеристики невысоки. Разработано много способов и устройств дополнительного намагничивания ГМ, которые могут применяться в сочетании как с обычной сетью, так и в составе инверторных электроприводов.

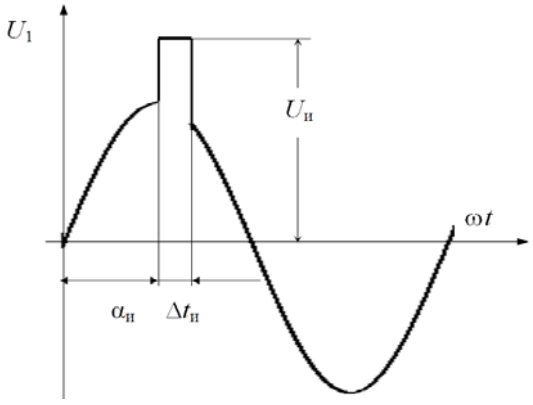


Рис. 2. Параметры импульсного намагничивания гистерезисной машины

Теория гистерезисных электроприводов разработана в ряде работ [8]. Однако представляет теоретический и практический интерес также применение ГМ в автономных системах генерирования электроэнергии (СГЭЭ) на основе режима самовозбуждения [9]. В качестве примера на рис. 3 представлена схема мехатронной СГЭЭ переменного тока. Согласно представленной схеме полупроводниковый преобразователь (ПП) образует необходимый уровень реактивного тока, поддерживающий процесс самовозбуждения в диапазоне регулирования. Для синхронно-гистерезисного генератора (СГГ) в ПП дополнительно предусмотрено наличие устройства импульсного подмагничивания ротора, как это используется у синхронно-гистерезисных двигателей (СГД). При возникновении ава-

рийных ситуаций, приводящих к перегрузке СГЭЭ, процесс самогенерации прекращается («срыв генерации») с принудительным управляемым размагничиванием материала ротора, не приводя к катастрофическим последствиям.

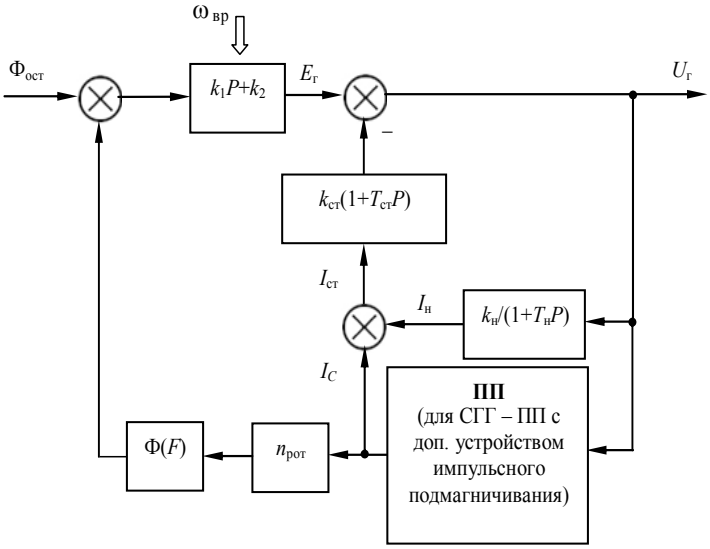


Рис. 3. Мехатронная СГЭЭ переменного тока с гистерезисным генератором

Перспективным магнитотвердым материалом с высоким уровнем механических свойств, как альтернатива викаллою, может стать, а фактически уже и является, сплав системы Fe-Cr-Co, о котором впервые было заявлено в 1936 г. В. Кёстером [10]. Поскольку в послевоенное время активно велись работы по внедрению в промышленное производство сплавов типа «алнико», потенциальные возможности магнитотвёрдых материалов структуры Fe-Cr-Co отошли на второй план. В 1971 г. в Японии были получены сплавы системы Fe-Cr-Co, содержащие 23–25% кобальта, 30–35% хрома с максимальным энергетическим произведением $(BH)_{макс.} > 40$ кДж/м^3 при остаточной индукции $B_r > 1{,}1$ Тл и коэрцитивной силе $H > 62$ кА/м, т.е. были получены постоянные магниты, по своим магнитным свойствам близкие к магнитам из наиболее широко используемого в технике сплава ЮНДК24 или Алнико 5. Также было сообщено, что сплавы Fe-Cr-Co являются пластичными, в частности, поддаются обработке давлением и режущим инструментом [11].

Как показывает литературный обзор [12, 13], современные новые российские промышленные сплавы 25Х15КА и 22Х15КА в зависимости от режима термической обработки заменяют не только все применяемые ранее промышленные сплавы для гистерезисных машин, но и обладают достоинствами, которые обеспечивают им неоспоримые конкурентные преимущества перед ними.

Магнитотвёрдые сплавы системы Fe-Cr-Co по сравнению с викаллоем содержат в 3–5 раз меньше кобальта и примерно в 2,5–3 раза дешевле его. Путём подбора соответствующей термообработки им можно придать магнитные свойства, не уступающие свойствам викаллоя. По уровню полей (2–30 кА/м), например, сплав 25Х15КА, имеющий высокие гистерезисные свойства, может заменить все существующие гистерезисные материалы. Результаты применения сплава 25Х15КА в девяти типоразмерах гистерезисных двигателей, где он заменил сплав викаллой, показали, что электромеханические характеристики двигателей улучшаются на 10–30%, при этом трудозатраты при механической обработке и сборке роторов, а также брак по термообработке уменьшаются в 3 раза (!) [12].

По данным [11–13] опытные испытания роторов из сплава 25Х15КА в электродвигателях постоянного тока ДПМ-35 взамен роторов из ЮНДК24, проведенные в ОАО «Псковэлектромаш», показали, что без ухудшения качества двигателя себестоимость изготовления снижается на 20–25%.

Примеры реализации мехатронных систем на основе гистерезисных машин и устройств импульсного намагничивания. Известно довольно много схем гистерезисных МС с устройствами импульсного намагничивания (УИН), отличающихся вариантами соединения основного и импульсного источников. При проектировании конкретных УИН необходимо таким образом выбирать алгоритмы управления ими, чтобы, выполняя задачу повышения энергетических показателей МС, не внести дополнительных возмущений по моменту и скорости машины, если это не требуется по каким-либо другим соображениям.

На рис. 4 представлена одна из схем, позволяющая производить форсированный пуск СГД с последующим перевозбуждением или, в принципе, формировать импульсы напряжения на двигателе в процессе его работы [14]. УИН выполнено в виде трехфазного трансформатора *TV*. Первичная обмотка *1* имеет отпайки, к которым может подключаться либо двигатель, либо напряжение сети. Концы фаз первичной и вторичной обмоток трансформатора подключены соответственно через выпря-

мители *VD*1 и *VD*2 к бесконтактным тиристорным ключам *VS*1, *VS*2. При подключении СГД к отпайкам первичной обмотки его запуск происходит при включенном тиристоре *VS*2 и выключенном *VS*1. При этом СГД подключен на полное напряжение сети, а трансформатор работает в режиме трансформатора тока. При окончании запуска тиристор *VS*1 включается, а тиристор *VS*2 выключается, напряжение на двигателе резко снижается, так как оно определяется работой трансформатора в режиме понижающего автотрансформатора.

В случае если напряжение сети подведено к отпайкам первичной обмотки, а СГД подключен к сетевым контактам, пуск производится при включенном тиристоре *VS*1 и выключенном тиристоре *VS*2, а трансформатор работает в качестве повышающего автотрансформатора. По окончании пуска происходит обратное переключение тиристорных ключей, и напряжение на СГД понижается примерно до напряжения сети. В принципе, алгоритм переключения тиристорных ключей может реализовывать и импульсный режим намагничивания СГД. Схему можно рекомендовать при питании СГД непосредственно от промышленной сети.

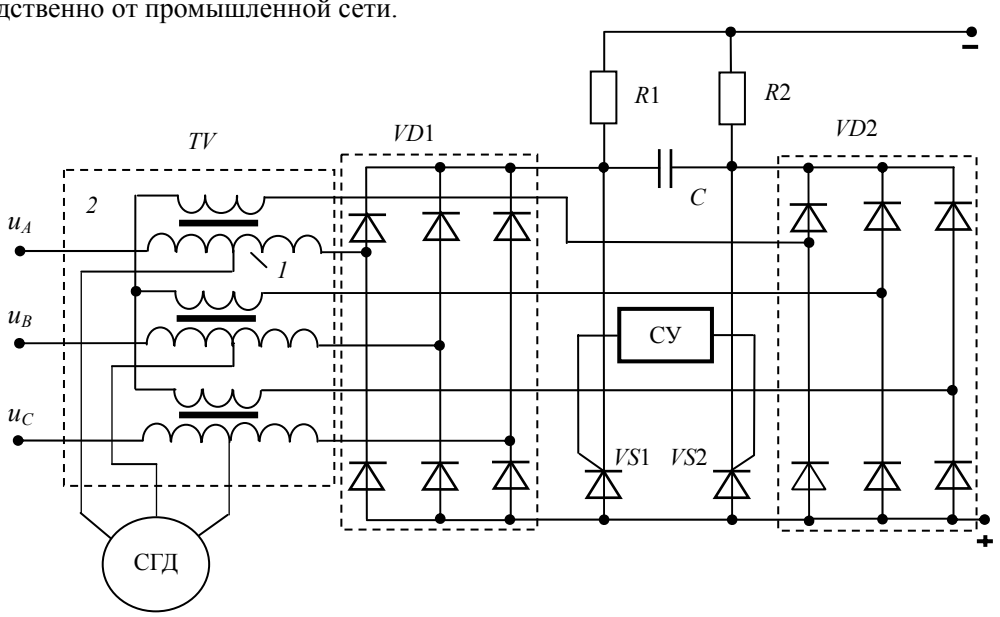


Рис. 4. Устройство намагничивания СГД с автотрансформатором
(СУ – схема управления)

Рисунок 5 иллюстрирует схему МС на основе нулевого инвертора напряжения, используемого в качестве вольтодобавки [15]. При отсутствии импульса намагничивания полупроводниковые ключи *S*1 и *S*2 замкнуты, а ключ *S*3 разомкнут и трансформатор *5* работает как трансформатор тока закороченной вторичной обмоткой. При формировании импульса намагничивания посредством схем управления *3* и *4* периодически замыкается полупроводниковый ключ *S*3 и размыкается один из ключей *S*1 или *S*2. Таким образом, на выходной обмотке трансформатора *5* образуется двуполярное выходное импульсное напряжение, которое суммируется с напряжением питания СГД, поступающим от сети. При этом нет одностороннего подмагничивания статора СГД. Импульсы намагничивания формируются по фазе и длительности в блоке *2*, синхронизируясь с напряжением сети через датчики блока *1*. Достоинство данной схемы состоит в том, что при вероятном выходе из строя полупроводниковых ключей УИН не нарушается целостность фазных проводников СГД.

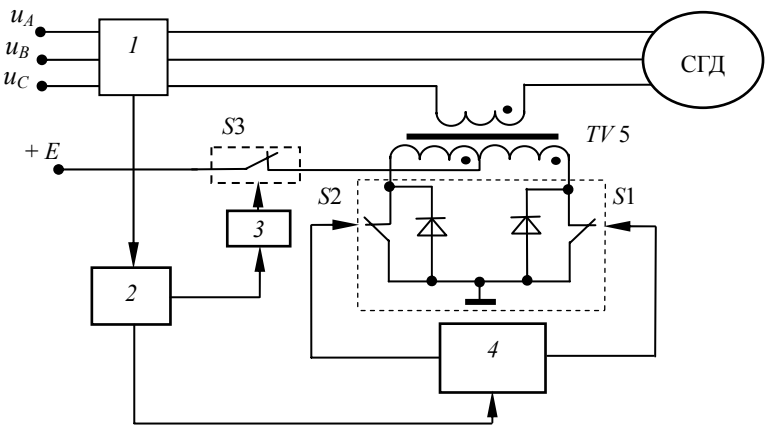


Рис. 5. Реализация МС с УИН
на основе нулевого инвертора в фазе СГД

Источник постоянного тока может быть как дополнительным, так и основным – от звена постоянного тока автономного инвертора, поскольку может иметь общую точку с общей шиной постоянного тока статического преобразователя. Кроме того, такой УИН способен работать с любым основным источником питания – автономными инверторами напряжения или тока, генератором или промышленной сетью. Схема может быть рекомендована для питания СГД, входящих в состав инерциальных систем навигации, а также многодвигательных электроприводов ультрацентрифуг или веретен.

На рис. 6 представлены варианты реализации бестрансформаторных схем импульсного намагничивания на выходе основного источника – автономного инвертора или сети [5]. Схема, представленная на рис. 6, *а*, формирует импульс намагничивания при размыкании полупроводникового ключа *S*2 и замыкании ключа *S*1. Недостатком схемы является необходимость пропускания импульсного тока через основной источник. От этого недостатка свободна схема, представленная на рис. 6, *б*. В момент формирования импульса намагничивания полупроводниковые ключи *S*1, *S*2 отключают основной источник питания, и ток импульсного источника замыкается только через фазы СГД.

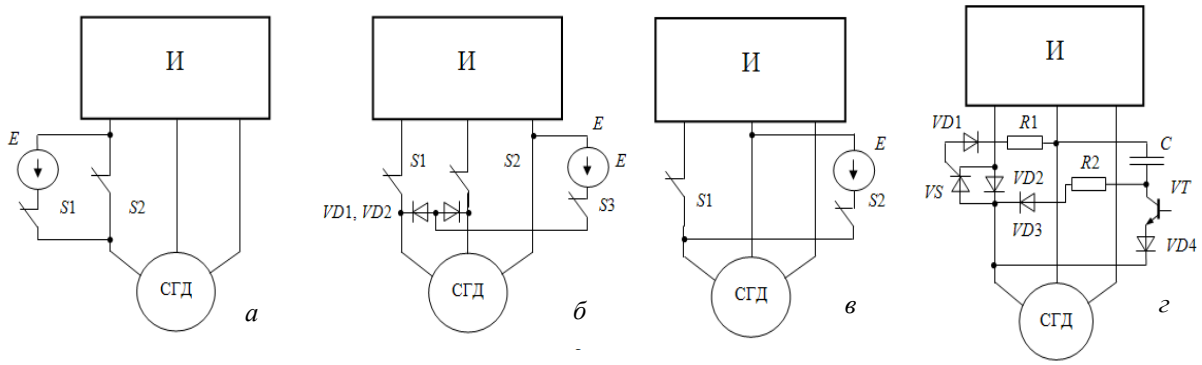


Рис. 6. Бестрансформаторные варианты схем УИН на выходе инвертора

Схема на рис. 6, *в* является фактически частным случаем предыдущей схемы. Общим недостатком схем на рис. 5 и 6 является наличие большого количества полупроводниковых ключей в цепях питания СГД. На рис. 6, *г* представлен вариант практической реализации схемы рис. 6, *в*. УИН содержит последовательный полупроводниковый ключ переменного тока, выполненный на тиристоре *VS* и диодах *VD*1, *VD*2. В качестве импульсного источника применен конденсатор *C* с цепью заряда *R*2, *VD*3. Работа транзисторного ключа *VT* синхронизирована с работой ключей инвертора И. В исходном состоянии транзисторный ключ *VT* выключен, ключ на тиристоре *VS* и диодах *VD*1, *VD*2 включен. При формировании импульса намагничивания включается транзистор *VT* и выключается тиристор *VS*.

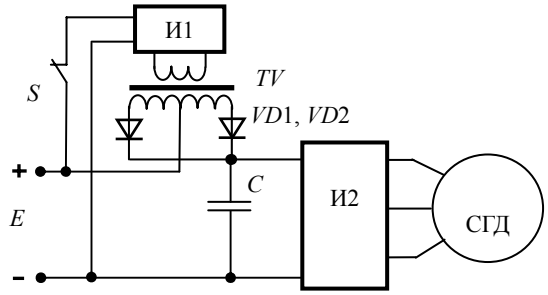


Рис. 7. УИН с дополнительным вольтодобавочным инвертором в цепи постоянного тока основного инвертора

На рис. 7 представлена схема МС с УИН в виде вольтодобавочного инвертора И1, расположенного в цепи постоянного тока основного инвертора И2 и способного выполнять функцию форсажа при запуске СГД. Схема формирует повышенное напряжение на входе основного инвертора при замыкании переключателя *S*. Следует отметить, что в представленной схеме ввиду наличия компенсирующего конденсатора *C* на входе основного инвертора затруднено формирование узких импульсов намагничивания [5]. Схема может быть рекомендована для применения в МС, не требующих информации о положении ротора, например в электроприводах топливных насосов.

Если в инверторе реализуется закон широтно-импульсной модуляции (ШИМ) выходного напряжения, то, вводя задержку в работу ключей инвертора, т.е. «вырождая» на время номинальный алгоритм ШИМ, можно получить возрастание тока на интервале задержки. Таким образом также достигается режим перевозбуждения двигателя.

Заключение. Проведенный технико-экономический анализ показывает, что в ряде МС машины на основе материала Fe-Cr-Co способны заменить дорогостоящие электрические машины с материалом Nd-Fe-B. Разработчикам следует обратить пристальное внимание на изучение регулировочных свойств и эксплуатационных возможностей МС с электрическими машинами гистерезисного типа.

Литература

1. Савченко А.Г. Магниты Nd-Fe-B и перспективные технологии их производства // Научно-практический семинар «Научно-технологическое обеспечение деятельности предприятий, институтов и фирм» // МИСиС. – М., 2003.– С. 510–545.

2. Применение РЗМ для производства постоянных магнитов [Электронный ресурс]. – Режим доступа: http://cniti-technomash.ru/assets/files/Doklad_konferencia_RZM.pdf, свободный (дата обращения: 11.05.2014).

3. Гарганеев А.Г. Экспериментальное исследование режима скольжения синхронно-гистерезисного двигателя // Изв. вузов. Электромеханика. – 2002. – № 2.– С. 35–42.

4. Гарганеев А.Г. Мехатронные системы с синхронно-гистерезисными двигателями / А.Г. Гарганеев, С.В. Брованов, С.А. Харитонов. – Томск: Изд-во Том. политех. ун-та, 2012. – 227 с.

5. Делекторский Б.А. Управляемый гистерезисный привод / Б.А. Делекторский, В.Н. Тарасов. – М.: Энергоатомиздат, 1983. – 128 с.

6. Делекторский Б.А. Регулирование гистерезисного гиродвигателя в процессе запуска / Б.А. Делекторский, В.Н. Тарасов // Труды МЭИ. 1974. – Вып. 187. – С. 37–41.

7. Мастяев Н.З. Гистерезисные электродвигатели. Ч. I / Н.З. Мастяев, И.Н. Орлов. – М.: МЭИ, 1963. – 220 с.

8. Гарганеев А.Г. Режим скольжения в гистерезисном электроприводе // Изв. вузов. Электромеханика. – 1989. – № 5. – С. 95–98.

9. Garganeev A.G. Autonomous electric power generation system based on self-excited electrical machine / A.G. Garganeev, S.A. Kharitonov // Tekhnichna elektrodynamika. – 2013. – № 4. – P. 56–58.

10. Ervens W. Chrom–Eisen–Cobalt–Werkstoffe: Neue Verformbare Dauermagnete // Techn. Mitt. Krupp Forsch. Berichte. – 1982. – B. 40, № 3. – P. 109–116.

11. Kaneko H. New Ductile Permanent Magnet of Fe–Cr–Co System / H. Kaneko, M. Homma, K. Nakamura // AIP Conference Proceedings «Magnetism and Magnetic Materials». – 1971. – № 5. – P. 1088–1092.

12. Прецизионные сплавы: справочник под ред. Б.В. Молотилова. – 2-е изд., перераб. и доп. – М., Металлургия, 1983. – 439 с.

13. Сплавы для гистерезисных двигателей / Л.А. Кавалерова, И.А. Малько, И.М. Миляев и др. // Электронная промышленность. – 1987. – Вып. 6(164). – С. 40–42.

14. А.с. 179370 СССР, МКИ, НО2Р 1/00. Устройство для перевозбуждения гистерезисного электродвигателя / В.Л. Бунаков, С.Н. Стоборов (СССР). – № 927287/24-7; заявлено 28.10.64; опубл. 26.03.66. Бюл. № 5. – 3 с.

15. А.с. 1145443 СССР, МКИ4, НО2Р 7/36. Электропривод гироприбора / В.И. Авдзейко, А.Г. Гарганеев, А.С. Сухин и др. (СССР). – № 3649804/24-07; заявлено 06.010.83; опубл. 15.03.85. Бюл. № 10. – 7 с.

Гарганеев Александр Георгиевич
Д-р техн. наук, профессор, зав. каф. электротехнических комплексов и материалов
Национального исследовательского Томского политехнического университета (НИТПУ)
Тел.: (382-2) 70-17-77 (доп. 1956)
Эл. почта: garganeev@rambler.ru

Падалко Дмитрий Андреевич
Аспирант каф. электротехнических комплексов и материалов НИТПУ
Тел.: (382-2) 70-17-77 (доп. 1956)
Эл. почта: padalko.da@gmail.com

Черватюк Александр Владимирович
Магистрант каф. электротехнических комплексов и материалов НИТПУ
Тел.: (382-2) 70-17-77 (доп. 1956)
Эл. почта: alexandrgs13@mail.ru

Garganeev A.G., Padalko D.A., Chervatyuk A.V.
Future Development of Hysteresis Synchronous Electrical Machine Mechatronic Systems

Based on the theory of hysteretic conversion of energy and magnetic material properties of Fe-Cr-Co and Fe-Co-V, it was concluded that the Fe-Cr-Co system materials are perspective to be applied in the electrical machines of mechatronic systems. Some examples of mechatronic systems with impulse excitation of rotor material are provided.
Keywords: Electrical machine, semiconductor converter, inverter, rectifier, magnetic materials.

УДК 621.313.333.2

А.А. Голдовская, Е.С. Дорохина, О.Л. Рапопорт, Р.О. Асланян

Актуальность создания и применения системы теплового контроля асинхронных тяговых электродвигателей

Представлены результаты расчета теплового поля асинхронного тягового двигателя двумя методами: графическим методом в среде ELCAD и с помощью тепловой математической модели, реализованной в среде Matlab. Построены температурные поля тягового электродвигателя при номинальных условиях работы и при повышенном значении тока статора. Показана необходимость регистрации температуры не только пазовых, но и лобовых частей обмотки электродвигателя. Результаты представленных расчетов показали необходимость использования системы теплового контроля температуры электродвигателя во время эксплуатации.

Ключевые слова: асинхронный тяговый двигатель, модернизация, температурное поле, математическая модель, контроль теплового состояния.

Одним из факторов повышения экономического роста страны является эффективное функционирование железнодорожного транспорта. В связи с этим в 2013 г. ОАО «РЖД» была разработана Программа модернизации и инновационного развития сети железных дорог ОАО «РЖД» и разработан проект «Стратегия развития железнодорожного транспорта РФ до 2030 года» [1, 2]. Одним из основных направлений модернизации и инновационных технологий в транспорте предусматривает увеличение доли тяжеловесных поездов массой 9–12 тыс. т и более с использованием систем дистанционного управления распределенной тягой, а также технические и технологические решения, обеспечивающие повышение скоростей движения не менее чем на 25%. Другим направлением модернизации является внедрение асинхронного тягового электропривода как на пассажирские, так и на грузовые электровозы.

Следствием всего вышесказанного является повышение нагрузок на подвижной состав. Таким образом, условия эксплуатации как всего оборудования, так и, в частности, тягового электропривода происходит в режимах перегрузки относительно номинальных условий эксплуатации. С учетом того, что тяговые электродвигатели являются наиболее нагруженным оборудованием электровоза, повышение нагрузки приведет к увеличению температурного поля электрической машины. Длительная эксплуатация электродвигателя в таких режимах является опасной за счет возможного наступления предельного теплового состояния и внезапного выхода его из строя.

С учетом ориентации ОАО «РЖД» на развитие тягового электропривода переменного тока остановимся на рассмотрении асинхронных тяговых электродвигателях. Обоснованием перехода на тяговые асинхронные электродвигатели является простота их обслуживания, эксплуатации, простота конструкции, низкая стоимость и высокая надежность машины. К недостаткам данных электродвигателей можно отнести большой пусковой ток, чувствительность к изменениям параметров в сети и необходимость применения преобразователя частоты для плавного регулирования скорости. В настоящее время в эксплуатации ОАО «РЖД» находятся двигатели серий НТА-1200, ДАТ-1200 и др. Данные серии электродвигателей для контроля их теплового состояния оборудованы датчиком температуры, в частности тяговый электродвигатель НТА-1200 оборудован датчиком температуры, вмонтированным в сердечник стали статора. Таким образом, в период эксплуатации электродвигателя имеется информация о температуре пазовой части обмотки статора. Но температура других частей: обмоток ротора, лобовых частей обмотки статора и др. – для оценки теплового состояния недоступна.

Другим путем получения информации о температурном поле машины является использование тепловой математической модели (ТММ) электродвигателя, которая позволяет производить расчет температур элементов конструкции электродвигателя по его входным параметрам [3, 4]. Такая модель позволяет получить информацию не только о температуре пазовой части обмотки статора, но и о температурах лобовых частей обмоток статора и температуре узлов ротора.

Разработанная тепловая математическая модель была создана на основе двигателя НТА-1200. Апробация ее адекватности проходила на электровозе 2ЭС10 «Гранит» № 062. Электровозы данной марки оснащены асинхронными тяговыми электродвигателями марки Siemens мощностью 1200 кВт. Приведение параметров математической модели для исследуемого двигателя к двигателю, установленному на электровозе, позволило экспериментально исследовать разработанную модель.

Эксплуатируемые электровозы «Гранит» оснащены системой определения температур узлов двигателя: пазовой части обмотки статора, сердечника статора и расчетной усредненной температуры ротора. Для оценки погрешности определения температур с использованием предлагаемой матмодели было проведено сравнение значений температур узлов тягового электродвигателя, полученные при эксплуатационных ходовых испытаниях электровоза 2ЭС10 № 062.

Эта погрешность не превышает 8%. При этом наибольшая погрешность была получена для узла ротора за счет того, что в экспериментальных данных его температура определяется как средняя.

В таблице приведены значения температур, полученные с помощью разработанной тепловой математической модели, для двух режимов работы двигателя. В первой столбце представлены значения температур узлов электродвигателя при работе с параметрами, близкими к номинальным по значению тока статора: напряжение сети U = 3320 В, фазный ток статора I_f = 336 А, температура окружающей среды t = 20 °С, частота вращения n = 796 об/мин, расход охлаждающего воздуха q = 90 м^3. Во втором столбце представлены значения температур узлов электродвигателя при двукратном увеличении тока статора: напряжение сети U =3000 В, фазный ток статора I_f= 600 А, температура окружающей среды t = 20 °С, частота вращения n = 1300 об/мин, расход охлаждающего воздуха q = 90 м^3.

Результаты расчета теплового поля машины с помощью ТММ

Наименование узла электродвигателя	Температура узлов электродвигателя, °С	
	U =3320 В, I_f = 336 А, t = 20 °С, n = 796 об/мин, q = 90 м^3	U = 3000 В, I_f = 600 А, t = 20 °С, n = 1306 об/мин, q = 90 м^3
Лобовая часть обмотки статора со стороны подачи воздуха	91,45	121,77
Пазовая часть обмотки статора	103,01	121,34
Лобовая часть обмотки статора со стороны, противоположной подаче воздуха	97,31	128,85
Сердечник статора	104,82	104,80
Лобовая часть обмотки ротора со стороны подачи воздуха	84,57	105,22
Пазовая часть обмотки ротора	88,04	98,17
Лобовая часть обмотки ротора со стороны, противоположной подаче воздуха	88,84	113,74
Сердечник ротора	84,01	95,75
Короткозамкнутое кольцо со стороны подачи воздуха	84,56	105,15
Короткозамкнутое кольцо со стороны, противоположной подаче воздуха	88,83	113,69
Выходная температура воздуха	41,21	56,47

В первом случае, когда ток статора имеет номинальное значение, полученное температурное поле имеет классическое распределение температуры в электродвигателе [5, 6]. Пазовые части обмотки двигателя имеют максимальное значение, лобовые части – менее нагреты. Моделирование температурного поля, проведенное в среде ELCAD (рис. 1), также подтвердило данное распределение. Погрешность между всеми результатами (экспериментальные значения, расчет с помощью тепловой математической модели, моделирование в среде ELCAD) не превышает 10%.

В случае двукратного увеличения тока статора (I_f = 600 А) при максимально возможном сохранении остальных параметров наблюдается увеличение температур лобовых частей обмоток статора и ротора. Моделирование данного режима работы в среде ELCAD также подтвердило полученное распределение температур в двигателе.

Погрешность расчетов в среде ELCAD и расчетов с помощью тепловой математической модели связана с тем, что разработанная ТММ производит расчет температур электродвигателя с учетом подогрева охлаждающего воздуха вдоль машины. Программирование в среде ELCAD не дает возможности учитывать подогрев воздуха при его движении вдоль машины.

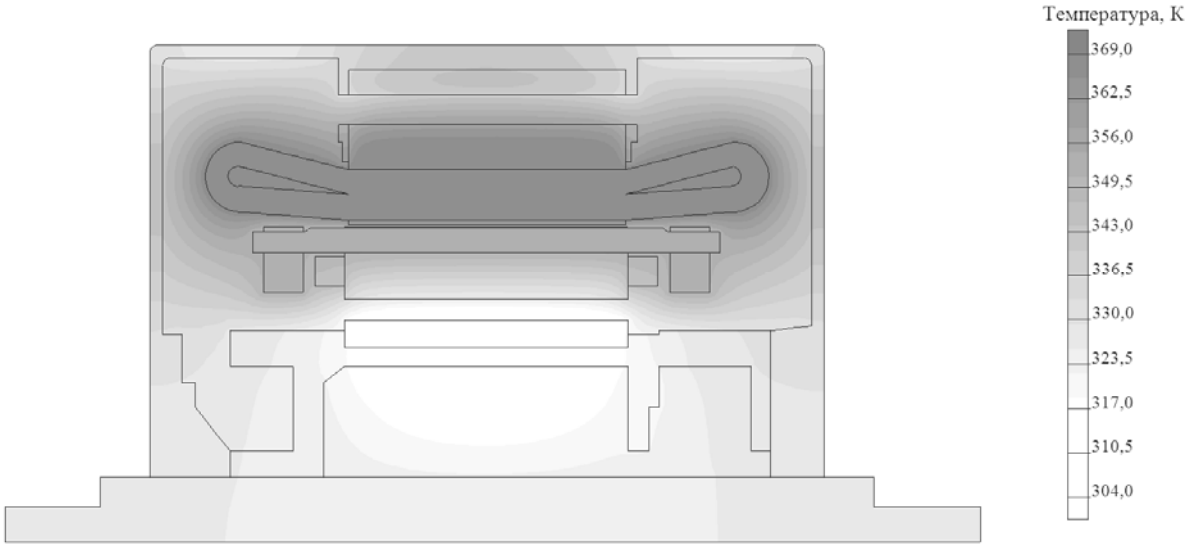


Рис. 1. Моделирование теплового состояния тягового асинхронного электродвигателя в среде ELCAD при U = 3320 В, I_f = 336 А, t = 20 °С, n = 796 об/мин

Заключение. В результате проведенных исследований можно сделать следующие выводы:

1. Повышение токовых нагрузок выше номинальных при одних и тех же условиях охлаждения приводит к большему увеличению температур лобовых частей обмоток статора и ротора, чем в пазовой части. Данное явление можно объяснить тем, что теплоотдача лобовых частей обмоток статора и ротора в большой степени зависит от количества охлаждающего воздуха. При постоянном значении расхода охлаждающего воздуха теплоотвод с лобовых частей остается практически таким же при увеличенных примерно в 4 раза потерях в обмотке.

2. Полученные результаты моделирования показывают, что производимый контроль температуры только пазовой части обмотки электродвигателя во время эксплуатации электровоза не является достаточным. Показано, что наиболее нагретыми частями являются лобовые части обмоток. Именно по этим наиболее нагретым частям можно судить о ресурсе ТЭД по тепловому состоянию изоляции.

Литература

1. Стратегия развития железнодорожного транспорта в Российской Федерации до 2030 года [Электронный ресурс]. – Режим доступа: http://www.mintrans.ru/documents/detail.php? ELEMENT_ID=13009, свободный (дата обращения: 14.04.2014).

2. Стратегические направления научно-технического развития ОАО «Российские железные дороги» на период до 2015 г. («Белая книга» ОАО «РЖД») [Электронный ресурс]. – Режим доступа: http://doc.rzd.ru/doc/public/ru?STRUCTURE_ID=704&layer_id=5104&id=4038, свободный (дата обращения: 14.04.2014).

3. Дорохина Е.С. Система мониторинга теплового состояния тяговых электродвигателей постоянного тока / Е.С. Дорохина, О.Л. Рапопорт, А.А. Хорошко // Изв. высш. учебных заведений. Электромеханика. – 2012. – № 4. – С. 16–21.

4. Дорохина Е.С. Тепловая модель асинхронного тягового двигателя / Е.С. Дорохина, А.А. Хорошко // XVII Междунар. науч.-практ. конф. студентов и молодых ученых «Современные техника и технологии» СТТ 2011. – Томск, 2011. – Т. 1. – С. 455–456.

5. Тихонов Ф.В. Разработка методов выбора параметров асинхронного тягового двигателя с учетом теплового состояния обмоток: дис. … канд. техн. наук. – М., 2008. – 136 с.

6. Сипайлов Г.А. Тепловые, гидравлические и аэродинамические расчеты в электрических машинах: учеб. пособие / Г.А. Сипайлов, Д.И. Санников, В.А. Жадан. – М.: Высшая школа, 1989. – 239 с.

Голдовская Анастасия Александровна
Ассистент каф. электромеханических комплексв и материалов (ЭКМ)
Энергетического института Национального исследовательского Томского политехнического университета
Тел.: 8-960-978-29-66
Эл. почта: Horoshko@tpu.ru

Дорохина Екатерина Сергеевна
Ассистент каф. ЭКМ
Тел.: 8-913-845-03-39
Эл. почта: dorohina@tpu.ru

Рапопорт Олег Лазаревич
Канд. техн. наук, доцент каф. ЭКМ
Тел.: 8-913-820-37-79
Эл. почта: raol46@mail.ru

Асланян Роксана Ованесовна
Магистрант 6-го курса каф. ЭКМ
Тел.: 8-913-856-39-15
Эл. почта: rassvetik5@mail.ru

Goldovskaya A.A., Dorokhina E.S., Rapoport O.L., Aslanyan R.O.
The importance of establishing and applying the thermal control system of traction induction motors

The calculation results of the traction induction motor thermal field are presented by two methods: graphical method in the environment ELCAD and using thermal mathematical model implemented in the environment Matlab. Traction electric motor temperature fields are constructed at nominal operating conditions and at increased value of stator current. The registration necessity of temperature not only grooving, but also winding front parts of the electric motor is shown. The calculation results showed the necessity of using motor temperature monitoring during operation.
Keywords: traction induction motors, modernization, temperature field, mathematical model, thermal monitoring.

УДК 621.313.333.2

О.С. Качин, С.И. Качин, А.В. Киселев, А.Б. Серов

Конструкция однофазного асинхронного электродвигателя с повышенным пусковым моментом

Описана конструкция однофазного асинхронного электродвигателя с повышенным пусковым моментом, рассмотрены принципы его функционирования. Предложены пути модернизации однофазных асинхронных электродвигателей в направлении снижения энергопотребления. Приведены экспериментальные механические характеристики электродвигателя предложенной конструкции в сравнении с электродвигателем стандартного исполнения. Приведены расчетные значения показателей энергоэффективности для различных вариантов исполнения однофазных асинхронных электродвигателей на базе предложенной конструкции.

Ключевые слова: однофазный асинхронный электродвигатель, энергоэффективность, пусковой момент, пусковая обмотка.

Однофазные асинхронные электродвигатели (ОАД) малой мощности широко используются в самых различных сферах современной жизни в составе электроприводов, питаемых от однофазной сети переменного тока. Массовое распространение они получили благодаря использованию в бытовой технике. Данный класс электродвигателей относится к изделиям массового производства и выпускается десятками миллионов штук в год, что определяет повышенный интерес производителей к совершенствованию их конструкций и технологий производства. При этом в мировых тенденциях последних десятилетий наблюдается устойчивое предпочтение параметра энергоэффективности электроприводов.

В этой связи одним из основных эксплуатационных показателей однофазных электродвигателей для бытовой техники является уровень их энергопотребления. Согласно оценкам Министерства экономического развития РФ (доклад Президиуму Госсовета РФ «О повышении энергоэффективности российской экономики»), основным потенциалом снижения потребления электрической энергии в «лучших» домохозяйствах обладают холодильные компрессоры (до 50% всего потенциала). До последнего времени задача снижения электропотребления в жилищном секторе сравнительно успешно решалась путем «импортирования энергоэффективности» из-за рубежа, путем закупки «крупных» бытовых электроприборов (в первую очередь холодильников) с повышенной энергоэффективностью. Так, например, замена устаревших конструкций холодильников на современные энергоэффективные модели может позволить сэкономить до 10 млрд кВт·ч электрической энергии по РФ в год. В связи со стратегической важностью данного показателя Министерством экономического развития РФ планируется к 2020 г. снизить расход электроэнергии на холодильник до 250–280 кВт·ч/год (аналогичный показатель в 2000 г. составлял 387 кВт·ч/год, а в 2007 г. – 325 кВт·ч/год). Государственной программой Российской Федерации «Энергосбережение и повышение энергетической эффективности на период до 2020 года» (утверждена Распоряжением Правительства Российской Федерации от 27 декабря 2010 г. №2446-р) предусматривается замена устаревших холодильников и морозильников в 2013–2020 гг. на энергетически высокоэффективные в количестве 125,78 млн штук. При этом планируется обеспечить значительную экономию электрической энергии в жилищном секторе на протяжении 10–30 лет (средний срок службы бытовых холодильников в России).

Достижение существенного снижения расхода электроэнергии бытовыми холодильниками возможно, если использовать новые материалы, технологии и технические решения, в первую очередь, применительно к электроприводу холодильных компрессоров, в качестве электродвигательного устройства которого, как правило, берутся однофазные асинхронные электродвигатели с пусковой обмоткой. Данный тип однофазных электродвигателей отличается тем, что пусковая обмотка подключается к сети лишь на время пуска, имеет малое сечение провода в сравнении с основной обмоткой и занимает менее 1/3 пазового объема статора.

Постановка задачи. Одним из главных направлений совершенствования однофазных асинхронных электродвигателей с пусковой обмоткой является улучшение их пусковых характеристик, а

именно, увеличение пускового момента [1–6]. Данный параметр особенно актуален для электродвигателей, приводящих во вращение компрессоры. Наличие определенного превышения пускового момента электродвигателя над максимальным моментом нагрузки необходимо также из соображений сохранения условий пуска электропривода при снижении напряжения питающей сети, что наиболее часто имеет место в условиях перегрузки энергосистем в пригородной, а также в сельской местности Российской Федерации. Указанная проблема актуальна, так как наличие запаса по пусковому моменту в ряде случаев позволяет снижать проектную мощность электродвигателя, что обеспечивает большую его загрузку в номинальном режиме и уменьшение потребления электроэнергии. Таким образом, цель работы заключается в повышении пускового момента однофазных асинхронных электродвигателей с пусковой обмоткой, а также анализе путей повышения их энергоэффективности.

Разработка новых конструкций однофазных асинхронных электродвигателей. Коллективом Томского политехнического университета была разработана конструкция однофазного асинхронного электродвигателя, позволяющая повысить пусковой момент, защищенная патентом РФ на изобретение №2510120 [7]. Согласно предложенной конструкции в статоре в области пазов, расположенных в зонах магнитных осей основной обмотки, выполнены сквозные немагнитные зазоры или с воздушным заполнением, или с немагнитными вставками (рис. 1).

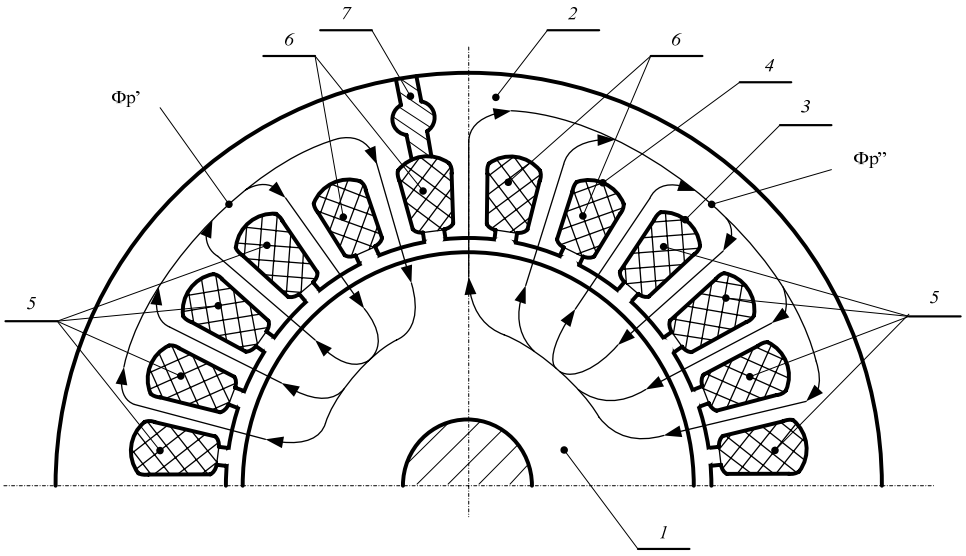


Рис. 1. Активная часть однофазного асинхронного электродвигателя предлагаемой конструкции с отображением силовых линий магнитного поля ротора Фр: *1* – ротор; *2* – статор; *3* и *4* – пазы основной и вспомогательной обмоток; *5* – основная обмотка; *6* – вспомогательная обмотка; *7* – сквозной немагнитный зазор

Полюсное деление каждой из систем полюсов составляет 180°, соответственно сдвиг основной и вспомогательной систем полюсов выполнен на 90° относительно друг друга. Возможно выполнение предлагаемой конструкции электродвигателя с большим числом полюсов в каждой из фаз, например с четырьмя полюсами. Вспомогательные обмотки *6* имеют большее по сравнению с основными обмотками *5* соотношение активного и индуктивного сопротивлений либо включены последовательно с конденсатором.

При выполнении в предложенной конструкции (см. рис. 1) сквозных немагнитных зазоров в статоре в области пазов, расположенных в зонах магнитных осей основной обмотки, магнитный поток поперечной реакции ротора представляет совокупность двух магнитных потоков Фр’ и Фр”. Причем каждый из указанных магнитных потоков почти в два раза меньше магнитного потока Фр электродвигателя традиционной конструкции, поскольку они создаются уменьшенной (ориентировочно в два раза) магнитодвижущей силой ротора. Каждый из магнитных потоков Фр′ и Фр″ охватывает меньшее число проводников ротора в сравнении с прототипом (см. рис. 1). В результате величина индуктивности ротора в конструкции предлагаемого однофазного асинхронного электродвигателя уменьшается почти в два раза по сравнению с однофазным электродвигателем, выполненным в соответствии с традиционной конструкцией.

Выполнение сквозных немагнитных зазоров *7* в предложенной конструкции статора однофазного асинхронного электродвигателя практически не влияет на величину основного магнитного потока, создаваемого основной обмоткой, и на электромагнитные параметры основной фазы статора.

Таким образом, уменьшение индуктивности обмотки ротора сопровождается снижением величины индуктивного сопротивления фазы ротора и, соответственно, повышением пускового момента электродвигателя, поскольку критический момент и критическое скольжение при этом возрастают [8]. Следовательно, предложенная конструкция однофазного асинхронного электродвигателя позволяет улучшать его пусковые характеристики в сравнении с известными техническими решениями в данной области техники.

Однофазный электродвигатель предложенной конструкции работает следующим образом. При включении основной фазы с основными обмотками *5* и вспомогательной фазы с вспомогательными обмотками *6* в сеть переменного напряжения создаются два пульсирующих магнитных потока, сдвинутых в пространстве и во времени. Суммарное магнитное поле статора *2*, действующее на ротор *1*, будет вращаться в пространстве и наводить в короткозамкнутой обмотке ротора *1* ЭДС, под действием которых в короткозамкнутой обмотке ротора *1* будут протекать токи и создавать магнитный поток ротора *1*. Взаимодействие магнитных потоков статора *2* и ротора *1* создает вращающий момент на роторе *1*. Причем наличие сквозных немагнитных зазоров *7* в статоре в области пазов *4* вспомогательной обмотки *6*, расположенных в зонах магнитных осей основной обмотки *5*, приводит к уменьшению индуктивного сопротивления обмотки ротора *1*, что сопровождается изменениями во взаимодействии магнитных потоков статора *2* и ротора *1* и увеличением пускового момента однофазного асинхронного электродвигателя. В результате пуск электродвигателя при заданной нагрузке осуществляется за более короткий промежуток времени либо может быть выполнен с увеличенной нагрузкой на валу. После выхода электродвигателя в рабочий режим вспомогательная фаза с вспомогательными обмотками *6* может быть отключена, поскольку при рабочей скорости вращения может обеспечиваться достаточный вращающий электромагнитный момент при работе лишь основной фазы с основными обмотками *5*.

Работоспособность предлагаемой конструкции проверена экспериментально на однофазном асинхронном электродвигателе электроточила «Томск 1У4.2» с пусковой обмоткой ТУ 16-539.533-72, в конструкции статора которого были выполнены сквозные немагнитные зазоры. Из приведенных зависимостей момента *M* от скольжения *S* однофазных асинхронных электродвигателей (рис. 2) следует, что пусковой момент в электродвигателе предложенной конструкции повышен на 23% (кривая *2*) в сравнении с традиционной конструкцией (кривая *1*), а его частота вращения на рабочем участке механической характеристики несколько снижена.

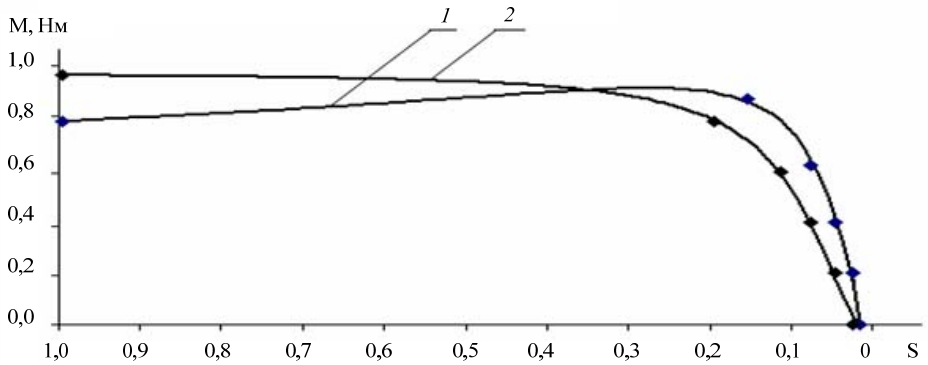


Рис. 2. Зависимости момента *M* от скольжения *S* однофазных асинхронных электродвигателей, выполненных по традиционной (кривая *1*) и предложенной (кривая *2*) конструкции

Таким образом, применение предлагаемого однофазного асинхронного электродвигателя позволяет повысить пусковой момент, что может обеспечить надежный пуск электродвигателя при наличии нагрузки на валу, близкой по величине к номинальной или даже превышающей ее, а также при снижении напряжения питающей сети относительно номинального значения.

Предлагаемый путь повышения величины пускового момента ОАД с пусковой (вспомогательной) обмоткой благодаря снижению индуктивности короткого замыкания вследствие конструктивных изменений в магнитопроводе статора позволяет осуществлять как проектирование новых элек-

тродвигательных устройств с улучшенными техническими характеристиками и эксплуатационными параметрами, так и модернизацию существующих конструкций данного типа электродвигателей.

Одним из направлений модернизации ОАД с пусковой обмоткой для холодильных агрегатов может быть повышение их устойчивости к понижению напряжения питания в сравнении с его номинальным значением. Для решения этой задачи не требуется каких-либо дополнительных изменений в элементах ОАД, помимо описанных выше изменений в конструкции магнитопровода статора. При этом величина пускового момента (по расчетным данным) может быть увеличена на 20–28%, что позволяет иметь дополнительный 11% запас на снижение напряжения питающей сети (превышает предельно допустимое значение установившегося отклонения напряжения в системах электроснабжения общего назначения), что позволит распространить использование модернизированных подобным образом электродвигателей в ранее недоступные сферы.

Следующим направлением модернизации ОАД с пусковой обмоткой является снижение потребления электрической энергии при заданной величине механической энергии, отдаваемой на нагрузку. Решение данной задачи имеет несколько путей реализации. Возможен вариант, когда одновременно с предлагаемыми изменениями конструкции статора уменьшается удельное сопротивление элементов беличьей клетки до величины, обеспечивающей сохранение пускового момента электродвигателя на заданном уровне. В этом случае можно ожидать снижения электрических потерь в ОАД на 10–16% и повышения выходной мощности на 4–6% (вследствие уменьшения скольжения в рабочем режиме). Экономия потребляемой холодильным компрессором электрической энергии, по предварительным оценкам, только от реализации указанных конструктивных изменений может составить порядка 13%. Это несколько больше, чем суммарное плановое снижение расхода электроэнергии на холодильник к 2020 г. (около 11% с учетом всех предполагаемых усовершенствований его составных элементов, включая повышение теплоизоляционных свойств корпуса холодильника).

Более радикальным вариантом модернизации ОАД является выполнение беличьей клетки ротора из меди или из сплавов с близким к ней удельным сопротивлением (латунь, бронза) наряду с описанными выше изменениями конструкции статора и, при необходимости, другими усовершенствованиями, обеспечивающими сохранение пускового момента электродвигателя на требуемом уровне. В этом случае мощность на валу электродвигателя, по расчетам, может быть увеличена на 8–10%, а экономия потребляемой электроэнергии составит около 22%.

Заключение. На основе проведенных исследований возможно сделать следующие выводы:

1. Предлагаемые конструкторские решения, направленные на изменение индуктивных параметров ОАД, имеют теоретическое обоснование их технической эффективности и открывают новые возможности для улучшения основных эксплуатационных показателей электроприводов для бытовой техники.

2. В предложенной конструкции однофазного асинхронного электродвигателя удалось достигнуть повышения пускового момента за счет снижения величины индуктивного сопротивления фазы ротора на 23%. Таким образом, применение предлагаемого однофазного асинхронного электродвигателя с повышенным пусковым моментом может обеспечить надежный пуск электродвигателя при наличии нагрузки на валу, близкой к номинальной или даже превышающей ее, а также при снижении напряжения питающей сети относительно номинального значения.

3. Проведенный анализ на примере компрессора холодильного оборудования показывает, что при оптимизации электромагнитной части возможно повысить энергоэффективность до 22%.

Литература

1. Абрамов А.Д. Однофазный асинхронный электродвигатель с повышенным пусковым моментом / А.Д. Абрамов, А.Р. Куделько // Электричество. – 1990. – № 12. – С. 67–69.

2. Пат. 2 028 024 РФ, МПК Н 02 К 17/08. Однофазный электродвигатель / Е.И. Ефименко (РФ). – № 5 000 293/07; заявл. 16.08.91; опубл. 27.01.95. Бюл. № 3. – 6 с.

3. А. с. 1 410 203 РФ, МПК Н 02К 17/04. Статор однофазного асинхронного электродвигателя / Б.Ф. Ковалев (СССР). – № 4167693; заявл. 26.12.86; опубл. 15.07.88. Бюл. № 20. – 3 с.

4. Пат. 2 010 410 РФ, МПК Н 02К 17/04. Однофазный асинхронный электродвигатель / Б.Ф. Ковалев (РФ). – № 4 948 371/07; заявл. 24.06.91; опубл. 30.03.94. Бюл. № 9. – 4 с.

5. Веларде Н.М. Исследование однофазных асинхронных двигателей с пусковой ферромагнитной обмоткой в установившихся и переходных режимах: автореф. дис. … канд. техн. наук: 05.09.01 / Моск. энергетический ин-т. – М., 1995. – 20 с.

6. Коротков Л. Асинхронные двигатели: перспективы совершенствования // Рынок электротехники. – 2006. – № 4. – С. 171–176.

7. Пат. 2 5101 20 РФ, МПК Н 02К 17/08. Однофазный электродвигатель / С.И. Качин, О.С. Качин (РФ). – № 2 012 139 937/07; заявл. 18.09.12; опубл. 20.03.14. Бюл. № 8. – 8 с.

8. Москаленко В.В. Автоматизированный электропривод / В.В. Москаленко. – М.: Энергоатомиздат, 1986. – 196 с.

Качин Олег Сергеевич
Доцент каф. электропривода и электрооборудования
Национального исследовательского Томского политехнического университета (НИТПУ)
Тел.: 8 (382-2) 56-37-59
Эл. почта: kos@tpu.ru

Качин Сергей Ильич
Д-р техн. наук, профессор каф. электропривода и электрооборудования НИТПУ
Тел.: 8 (382-2) 70-63-30
Эл. почта: ksi@tpu.ru

Киселев Александр Викторович
Ассистент каф. электромеханических комплексов и материалов НИТПУ
Тел.: 8 (382-2) 56-34-53
Эл. почта: kiselev_av@mail2000.ru

Серов Александр Борисович
Магистрант каф. электромеханических комплексов и материалов НИТПУ
Тел.: 8 (382-2) 56-34-53
Эл. почта: sabtpu@gmail.com

Kachin O.S., Kachin S.I., Kiselev A.V., Serov A.B.

Single phase induction motor

The design of the single-phase induction motor with increased starting torque is described. The principles of motor functioning are considered. Ways of modernization of single-phase induction motors in the direction of energy efficiency are offered. Experimental mechanical characteristics of the proposed electric motor in comparison with the standard electric motor are provided. Values of energy efficiency for various proposed design options of single-phase induction motors are given.

Keywords: single-phase induction motor, starting torque, energy efficiency, starting winding.

СООБЩЕНИЯ

УДК 338.28

Е.Б. Белов, В.П. Лось

О разработке профессиональных стандартов в области информационной безопасности

Принятие Национального плана развития профессиональных стандартов определено майскими указами Президента, цель которых – создание прочной экономической базы социального развития общества.

Ключевые слова: информационная безопасность, специалист по информационной безопасности, профессиональный стандарт, обобщенные трудовые функции, уровни квалификации.

Общая характеристика вида профессиональной деятельности, трудовых функций. Минтруд России в плане разработки профессиональных стандартов (ПС) определил одну позицию для разработки ПС «Специалист по информационной безопасности». Это вызвало определенные трудности для разработчиков, поскольку охватить все области деятельности таких специалистов в рамках одного ПС не представлялось возможным. Оставив неизменным наименование ПС, разработчики пошли по пути уточнения вида профессиональной деятельности и привязки к нему содержания стандарта.

Вид профессиональной деятельности – деятельность по обеспечению защищенности компьютерных систем (КС) от вредоносных технических воздействий. Первоначально проблема обеспечения безопасности данных в КС возникла при расширении круга пользователей ЭВМ и вычислительных систем. Увеличение количества ЭВМ и областей их применения объективно создало предпосылки для модификации, хищения и уничтожения данных. Появление автоматизированных информационных систем еще более усугубило проблему обеспечения безопасности данных.

Описание обобщенных трудовых функций, входящих в вид профессиональной деятельности, и обоснование их отнесения к конкретным уровням квалификации. Деятельность по обеспечению защищенности компьютерных систем (КС) от вредоносных технических воздействий включает обобщенные трудовые функции (ОТФ) и соответствующие им уровни квалификации, представленные в табл. 1.

Таблица 1

Обобщенные трудовые функции и уровни квалификации

Обобщенные трудовые функции (ОТФ)	
Наименование	Уровень квалификации
Эксплуатация защищенных КС и применение методов и средств обеспечения их безопасности	5
Администрирование и эксплуатация аппаратно-программных средств защиты информации в компьютерных системах	6
Разработка и применение методов оценивания уровня безопасности компьютерных систем, сертификация программного обеспечения, аттестация объектов информатизации	7
Проектирование и разработка специальных технических и программно-математических средств защиты информации компьютерных систем	7 8

ОТФ «Эксплуатация защищенных КС и применение методов и средств обеспечения их безопасности» предусматривает 5-й уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

ОТФ «Администрирование и эксплуатация аппаратно-программных средств защиты информации в компьютерных системах» предусматривает 6-й уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда Рос-

сии как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

Аналогично обосновывается соответствие остальных ОТФ приведенным в табл. 1 уровням квалификации.

Описание состава трудовых функций и обоснование их отнесения к конкретным уровням (подуровням) квалификации. ОТФ «Эксплуатация защищенных КС и применение методов и средств обеспечения их безопасности» включает трудовые функции (ТФ) и соответствующие им уровни квалификации, показанные в табл. 2.

Таблица 2

Трудовые функции и уровни квалификации

Трудовые функции	Уровень квалификации
Применение программно-аппаратных средств обеспечения информационной безопасности (ИБ) в КС	5
Применение технических средств обеспечения ИБ защищенных КС	5
Эксплуатация комплексных систем обеспечения ИБ в компьютерных системах	5

ТФ «Применение программно-аппаратных средств обеспечения информационной безопасности (ИБ) в КС» предусматривает 5-й уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

Аналогично обосновывается соответствие остальных ТФ приведенным в табл. 2 уровням квалификации.

ОТФ «Администрирование и эксплуатация аппаратно-программных средств защиты информации в компьютерных системах» включает трудовые функции (ТФ) и соответствующие им уровни квалификации, представленные в табл. 3.

Таблица 3

Трудовые функции и уровни квалификации

Трудовые функции	Уровень квалификации
Администрирование систем ИБ компьютерных систем	6
Организация профилактических проверок, регламентов технического обслуживания и текущего ремонта систем безопасности КС	6
Приемка и освоение программно-аппаратных средств защиты информации	6

ТФ «Администрирование систем ИБ компьютерных систем» предусматривает 6-й уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

Аналогично обосновывается соответствие остальных ТФ приведенным в табл. 3 уровням квалификации.

ТФ «Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации» предусматривает 7-й уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

Аналогично обосновывается соответствие остальных ТФ приведенным в табл. 4 уровням квалификации.

ОТФ «Проектирование и разработка специальных технических и программно-математических средств защиты информации компьютерных систем» включает следующие трудовые функции (ТФ) и соответствующие им уровни квалификации, представленные в табл. 5.

Таблица 4

Трудовые функции и уровни квалификации

Трудовые функции	Уровень квалификации
Проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	7
Разработка требований по защите, формирование политик безопасности КС	7
Применение методов и методик оценивания безопасности компьютерных систем при проведении контрольного анализа системы защиты	7
Выполнение экспериментально-исследовательских работ при проведении сертификации программно-аппаратных средств защиты и анализа результатов	7
Проведение экспериментально-исследовательских работ при аттестации объектов с учетом требований к обеспечению защищенности компьютерной системы	7
Проведение инструментального мониторинга защищенности компьютерных систем	7
Проведение экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	7

Таблица 5

Трудовые функции и уровни квалификации

Трудовые функции	Уровень квалификации
Разработка требований к средствам защиты информации компьютерных систем с учетом действующих нормативных и методических документов	7
Проектирование программных и аппаратных средств защиты информации компьютерных систем	7
Разработка, отладка и тестирование средств защиты информации компьютерных систем	7
Сопровождение разработки средств защиты информации компьютерных систем	8

ТФ «Разработка требований к средствам защиты информации компьютерных систем с учетом действующих нормативных и методических документов» предусматривает 7-й уровень квалификации, поскольку это соответствует «Уровням квалификации в целях подготовки профессиональных стандартов» Минтруда России как по показателям уровней квалификации (широта полномочий и ответственность; характер умений; характер знаний), так и по минимальным требованиям к уровню образования и основным путям достижения уровня квалификации.

Аналогично обосновывается соответствие остальных ТФ приведенным в табл. 5 уровням квалификации.

Основные этапы разработки проекта профессионального стандарта. Организации, на базе которых проводились исследования:

1. Учебно-методическое объединение (УМО) по образованию в области информационной безопасности.
2. Академия информационных систем.
3. МОО «Ассоциация защиты информации».
4. ЗАО «АВАНГАРД ЦЕНТР».
5. НП «Союз защитников информации».

Выбор этих организаций основывался на следующих требованиях:

1. Большой опыт в организации подготовки специалистов в области информационной безопасности в целом и компьютерной безопасности в частности.
2. Содействие организациям, предприятиям и органам государственной власти Российской Федерации в реализации государственной политики в области обеспечения защиты информации.

14 организаций участвовало в разработке проекта профессионального стандарта.

К разработке проекта профессионального стандарта «Специалист по информационной безопасности» были привлечены эксперты трех категорий:

− представители организаций-заказчиков/потребителей услуг в области информационной безопасности;

− представители образовательных организаций, реализующих специальности (направления подготовки) в области информационной безопасности;

− представители организаций-работодателей отрасли информационной безопасности, осуществляющих не менее 5 лет деятельность в области информационной безопасности, предприятий различных форм собственности.

В экспертную группу разработки проекта профессионального стандарта вошли руководители и специалисты-эксперты в данном виде профессиональной деятельности, специалисты в области управления, обучения и развития персонала, другие специалисты.

Требования к квалификации экспертов-разработчиков проекта профессионального стандарта:

1) должность – не ниже руководителя подразделения или ведущего специалиста;

2) стаж – не менее 5 лет работы в области информационной безопасности в организации, которая является работодателем в отрасли либо представителем системы профессионального образования, оказывающей образовательные услуги в области информационной безопасности.

К разработке ПС были привлечены более 20 экспертов, представляющих различные организации, в том числе ассоциации и объединения.

Этапы разработки проекта профессионального стандарта «Специалист по информационной безопасности»:

− анализ международных и отечественных стандартов;

− составление классификатора функциональных областей на основе международных и отечественных стандартов и прототипа перечней трудовых функций и трудовых действий;

− индивидуальные устные интервью с работниками данной профессии разных квалификационных уровней;

− проведение конференций и круглых столов;

− сбор замечаний и пожеланий участников конференций и круглых столов, выступления, ответы на вопросы, обсуждение индивидуальное и в группах;

− анализ полученных замечаний и пожеланий, обобщение результатов;

− подготовка первой версии проекта профессионального стандарта и публикация для начала общественного обсуждения;

− обсуждение первой версии проекта профессионального стандарта на Экспертном совете Минтруда России;

− подготовка второй версии проекта профессионального стандарта на основе рекомендаций Экспертного совета Минтруда России;

− сбор, анализ замечаний и пожеланий, обобщение результатов;

В ходе экспертизы проекта профессионального стандарта использовались следующие методы работы:

− составление и использование обобщенного (типового) классификатора трудовых функций и трудовых действий, сгруппированных по функциональным областям;

− рабочие совещания (очные, по телефону, по другим каналам телекоммуникационной связи);

− сбор замечаний и пожеланий по электронной почте.

При подготовке ПС использовались нормативные правовые документы и ГОСТы, регулирующие вид профессиональной деятельности, для которого разработан проект профессионального стандарта.

Обсуждение проекта профессионального стандарта. Обсуждение проекта ПС проходило на конференциях и круглых столах. К основным из этих мероприятий относятся:

− Конференция Минтруда России «Разработка и принятие профессиональных стандартов – стратегическая реформа кадрового обеспечения. Профессиональный стандарт – Специалист информационной безопасности» (Москва).

− 12-я всероссийская конференция «Информационная безопасность. Региональные аспекты. ИнфоБЕРЕГ–2013» (Сочи).

− VII Всероссийская конференция научно-технической школы-семинара «Информационная безопасность – актуальная проблема современности», проведенная в филиале Военной академии связи (Краснодар).

Замечания и предложения к проекту ПС обсуждались на заседаниях экспертной группы и принимались решения о соответствующих корректировках.

Ближайшие перспективы. На совещании по вопросу разработки профессиональных стандартов 9 декабря 2013 г. Президент Российской Федерации В.В. Путин отметил: «Профстандарты должны задать чёткие и ясные требования к компетенции специалистов, служить ориентиром для людей, какими знаниями, навыками они должны обладать, чтобы быть востребованными на современном рынке труда.

В руках государства система профессиональных стандартов призвана стать одним из главных инструментов модернизации экономики, обеспечения высокого качества жизни людей через достойно оплачиваемый, высокопродуктивный производительный труд».

С учетом этих требований нашему сообществу предстоит определиться с ПС, охватывающими не только область компьютерной безопасности. К числу таких стандартов можно отнести профессиональные стандарты со следующими наименованиями:

1. Руководитель по обеспечению безопасности информации.
2. Специалист по обеспечению безопасности информации.
3. Специалист в области информационной безопасности бизнеса.
4. Специалист (инженер) по безопасности связи.
5. Специалист по противодействию техническим разведкам.
6. Специалист по безопасности информационных технологий, информационных ресурсов и информационных систем.
7. Специалист по криптографической защите информации.

Белов Евгений Борисович
Зам. пред. Совета УМО по образованию в области информационной безопасности, Москва
Тел.: +7 (495) 931-06-09
Эл. почта: umoib@yandex.ru

Лось Владимир Павлович
Д-р воен. наук, профессор, проректор по научной работе
Московского государственного университета приборостроения информатики
Тел.: +7 (499) 269-46-96
Эл. почта: los_vp@mgupi.ru

Belov E.B., Los V.P.

On Developing Professional Standards in Information Security

The National Plan of Developing Professional Standards adopted by RF President's decree has the main purpose to create solid economic foundations for social development of society.

Keywords: information security, specialist in information security, professional standard, average summed working duties, qualification levels.

УДК 338.27

Н.Л. Журавлева

Анализ финансовых рисков при планировании НИОКР вуза

Рассмотрены основные финансовые риски при планировании НИОКР вуза. Выделены факторы, способствующие уменьшению финансовых рисков. Определены перспективы роста объемов финансирования.

Ключевые слова: анализ рисков, научно-исследовательская деятельность, финансирование НИОКР.

Современная глобальная парадигма диктует новые вызовы к организации планирования научно-исследовательских и опытно-конструкторских работ (НИОКР) вуза. Уже недостаточно просто выполнять НИОКР в рамках государственного задания – сегодня требуется эффективная бюджетная система и ориентация на стимулирование роста объемов НИОКР. Поэтому вопрос анализа финансовых рисков является актуальным и востребованным. В логике нашей работы определим финансовые риски как вероятность потери денежных средств.

Целью представленной работы выступает комплексный анализ бюджета НИОКР Томского государственного университета систем управления и радиоэлектроники за период 2009–2013 гг. Анализ необходим для формирования эффективной финансовой системы, способствующей росту объемов НИОКР.

При проведении анализа бюджета НИОКР вуза были поставлены и решены следующие задачи:

– оценка состояния и динамики финансирования НИОКР ТУСУРа;

– выявление основных проблем и недостатков в области государственного и внебюджетного финансирования НИОКР ТУСУРа;

– выработка конкретных рекомендаций по повышению эффективности планирования НИОКР ТУСУРа.

В ТУСУРе научно-исследовательская деятельность строится на сочетании бюджетного и внебюджетного финансирования. В таблице приведены данные по объемам финансирования НИОКР из различных источников с 2009 по 2013 г.

Финансирование научно-исследовательской деятельности (тыс. руб.)

Источники финансирования	2009 г.	2010 г.	2011 г.	2012 г.	2013 г.
Бюджетное финансирование	58336,7	75505,8	93 074,5	181 911,8	166 666,2
Внебюджетное финансирование (вкл. Постановление 218)	257508,1	452512,9	524 878,6	547 772,0	494 465,7
Итого по ТУСУР	315844,8	528018,7	617 953,1	729 683,8	661 131,9
Удельный вес бюджетной составляющей в общем объеме финансирования научно-исследовательской деятельности (в %)	18,47	14,3	15,06%	24,93%	25,21%

Анализ таблицы позволяет сделать следующие выводы:

1. Стабильное увеличение доли бюджетного финансирования приводит к качественным сдвигам показателей по научной деятельности, а именно: повышению эффективности управления проектами, развитию и модернизации материально-технической базы и инфраструктуры вуза. Однако доля бюджетных НИОКР относительно невелика (25,21% в 2013 г.), что характеризует недостаточную активность участия отдельных подразделений в конкурсах на выполнение НИОКР и получение грантов различных фондов.

2. Университет по своему инновационно-коммерческому потенциалу, т.е. по возможности существовать и развиваться в рыночных условиях, занимает ведущие позиции в российском образовательном пространстве согласно данным информационно-коммуникационной площадки Министерства образования и науки РФ (http://www.innoedu.ru).

Внебюджетная составляющая в консолидированном научном бюджете принадлежит, в основном, промышленно-предпринимательскому сектору (рис. 1). Доля его участия стабильно высока и составляет более 80%. Участие промышленных, индустриальных партнеров выступает в современной системе финансирования научных исследований приоритетным показателем, определяющим место вуза в научном пространстве.

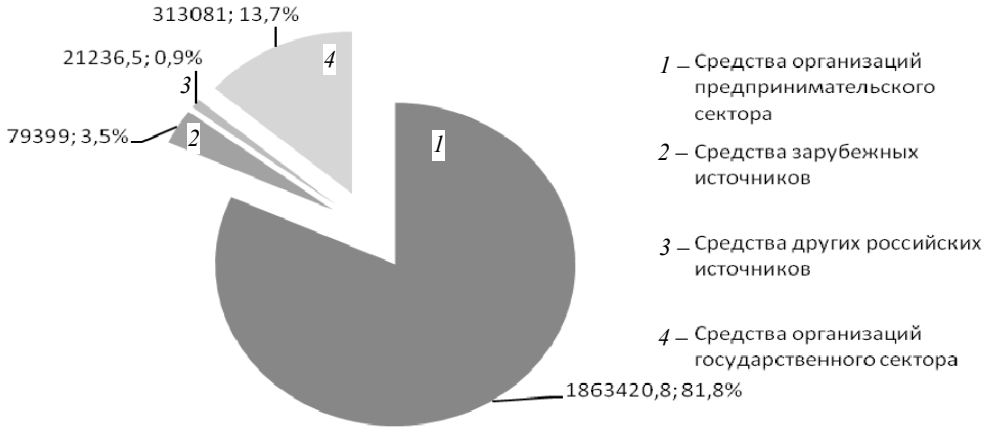


Рис. 1. Соотношение источников внебюджетного финансирования за период 2009–2013 гг.

Заметим, что зарубежные инвесторы не проявляют должного интереса к научно-производственной продукции университета. Доля зарубежных заказчиков в объеме доходов от науки составляет в среднем 2–5%.

Сформулируем перспективы роста объемов финансирования НИОКР с участием зарубежных партнеров и с увеличением доли бюджетных инвестиций:

1) активизация деятельности научных подразделений по увеличению бюджетной составляющей за счет участия в конкурсах, в том числе в кооперации с индустриальными партнерами и предприятиями наукоемкого бизнеса;

2) повышение эффективности использования научного оборудования и приборов, приобретенных при выполнении федеральных целевых программ, программ государственных и негосударственных научных фондов и др.;

3) разработка и реализация согласованных с научными подразделениями планов маркетинговых работ по продвижению научной продукции университета на зарубежные рынки.

Представим график динамики бюджетного и внебюджетного финансирования (рис. 2).

Незначительный спад объемов, выполняемых НИОКР, является индикатором уязвимости финансовой устойчивости вуза и требует детального анализа причин.

Изменение условий и факторов развития вузовской науки обусловило ситуацию сокращения объемов финансирования государственного задания и необходимость поиска внешних дополнительных источников финансирования НИОКР, в том числе в рамках федеральных целевых программ (в том числе в области кадрового потенциала), национальных технологических платформ, государственного оборонного заказа и др.

Выделим факторы, способствующие уменьшению финансовых рисков вуза:

– тенденция к росту доли исследователей, имеющих ученую степень;

– тенденция к росту доли молодых (до 39 лет) исследователей;

– тенденция к росту публикационной активности исследователей в изданиях с высоким импакт-фактором.

Так, сегодня фактором, влияющим на уменьшение финансовых рисков вуза, является необходимость осуществлять профессиональное образование молодежи непосредственно в лабораториях, в процессе проведения современных научных исследований, образование должно строиться на базе актуальных, значимых и перспективных достижений науки.

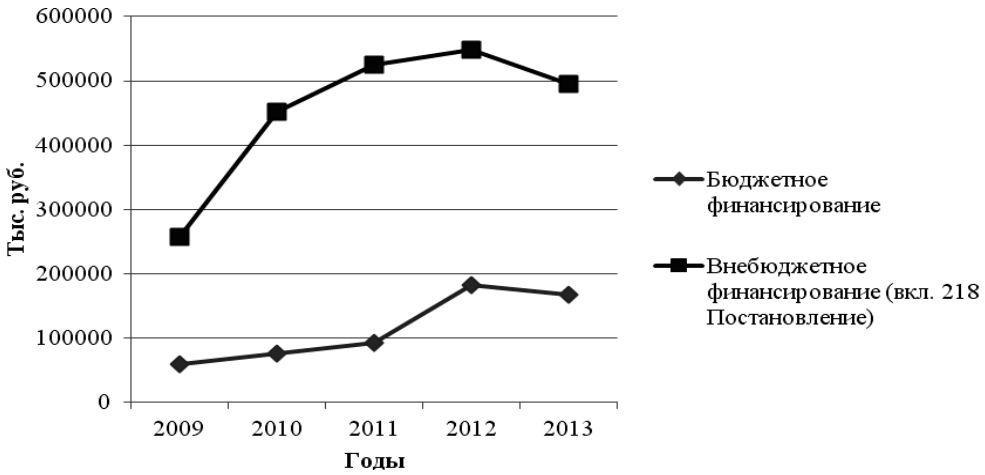


Рис. 2. Динамика бюджетного и внебюджетного финансирования

Для участия в хоздоговорных и госбюджетных НИР в ТУСУРе активно привлекаются студенты старших курсов, главным образом, дипломники. Так, в качестве исполнителей НИР на платной основе в 2009–2013 гг. приняли участие 1367 студентов, что составляет более 5 % от общего числа студентов очной формы обучения.

Понятие науки многокомпонентно. Этот тезис позволяет сказать, что в 2009–2013 гг. в НИР приняло участие более 5500 студентов университета (5656 чел.) Основное развитие получили следующие формы студенческой научной работы: участие в научных конференциях, конкурсах научных работ, рефератов, участие в выполнении НИР в группах ГПО, выставках, изобретательская деятельность. В университете создана комплексная система приобщения молодежи к участию во всевозможных научных мероприятиях, конкурсах, грантах (в том числе международного уровня). Создана система льготного налогообложения студенческих конструкторских бюро, финансирования студенческих грантов из собственных средств университета. На рис. 3 представлена диаграмма участия студентов очной формы обучения в научной работе. Около 40 % студентов-очников задействованы в научном процессе университета.

Исходя из непрерывности образовательной траектории «студент–аспирант–научный сотрудник», к участию в НИР на платной основе в 2009–2013 гг. были привлечены 420 аспирантов (50,2% от общего контингента аспирантов очной формы обучения). Если учитывать все формы участия аспирантов в научно-исследовательской деятельности, а именно: как авторов патентов, актов внедрения, публикаций, участие в выполнении научных проектов в организациях инновационного пояса, то в 2013 г. доля аспирантов составила 98%.

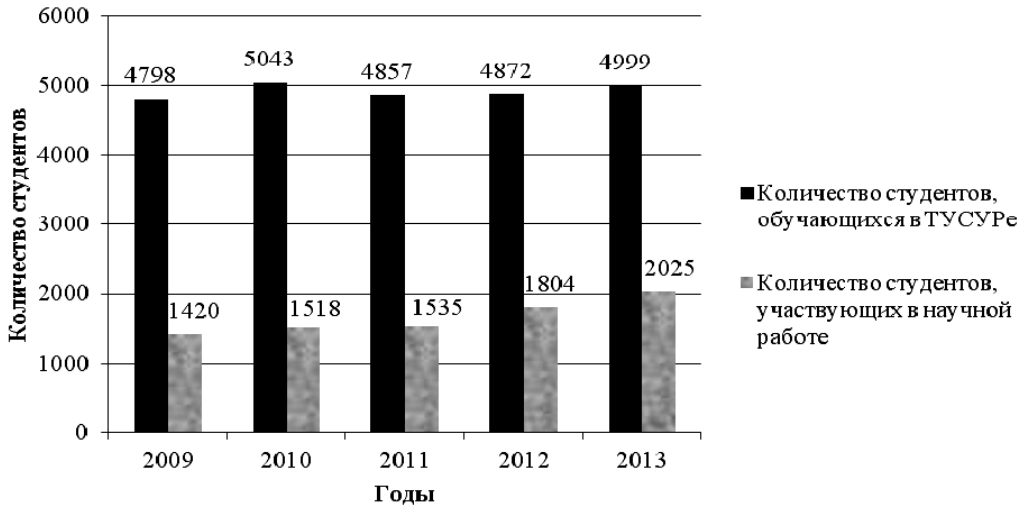


Рис. 3. Участие студентов очной формы обучения в научной работе

Таким образом, в университете сформирована инфраструктура, обеспечивающая обслуживание и сопровождение научно-исследовательской деятельности студентов и аспирантов. Реализация на-

учных проектов позволяет обеспечить дополнительной квалифицированной работой студентов и аспирантов, что является немаловажным фактором сохранения кадрового потенциала университета.

Проведенный анализ позволяет выделить следующие устойчивые тенденции по преодолению финансовых рисков при планировании НИОКР вуза:

1) увеличение доли бюджетного финансирования по государственному заданию, федеральным целевым программам;

2) увеличение доли бюджетного финансирования по зарубежным грантам;

3) обеспечение высокой доли участия предпринимательского сектора, промышленного (индустриального) партнера;

4) повышение роли внебюджетных фондов (особенно в части фундаментальных исследований).

В заключение отметим, что при анализе финансовых рисков в процессе планирования НИОКР вуза важно учитывать не только внешние изменения политического и экономического характера, но и внутренние ресурсы, в том числе кадровый потенциал и системную работу по стимулированию и закреплению молодых исследователей в сфере науки и образования.

Журавлева Наталья Леонидовна
Нач. отдела организации и планирования НИОКР ТУСУРа
Тел.: 8 (382-2) 51-20-93
Эл. почта: pnl@main.tusur.ru

Zhuravleva N.L.

Financial risk analysis in planning research and development at university

The article considers the main financial risks when planning R&D at university. Factors contributing to reduction of financial risks are defined. The prospects of growth of R&D amount are shown.

Keywords: risk analysis, research activities, R&D funding.

Требования к подготовке рукописей статей, представляемых для публикации в журнале «Доклады Томского государственного университета систем управления и радиоэлектроники»

1. Оригинал на бумажном носителе должен полностью соответствовать электронному варианту.

2. Электронный вариант должен быть представлен в виде файла, названного по-русски фамилией первого автора, на дискете или диске в формате Word **2003**. Предпочтительнее представить его по электронной почте.

3. Текст статьи должен быть набран без принудительных переносов через один интервал (множитель 1,05) шрифтом Times New Roman 10,5 кегля; распечатан на одной стороне листа белой писчей бумаги формата А4 с полями шириной 25 мм, без помарок и вставок. Шаблон статьи размещен на сайте: http://www.tusur.ru/ru/science/tusur_reports_magazine/template.dot. Размер статьи со всеми атрибутами должен быть, как правило, не более пяти страниц.

4. Одни и те же ***символы и обозначения переменных, векторов, функций и т.д. в тексте, формулах, таблицах и рисунках должны быть единообразными по написанию***. Русские и греческие символы, а также цифры и все математические знаки: скобки, плюсы, минусы и т.д. – набираются прямым шрифтом; переменные, обозначенные латинскими буквами – курсивом, кроме слов, их сокращений, имен функций (const, input; U_{in}; $I_{\text{вх}}$; T_z; β_1; $\sin x_t$), программ, названий фирм и химических формул (H_2O).

5. Все употребляемые обозначения и сокращения должны быть пояснены.

6. Единицы измерения физических величин должны соответствовать Международной системе единиц (СИ) и пишутся по-русски.

7. Таблицы и рисунки должны иметь тематические заголовки (не повторяющие фразы-ссылки на них в тексте). (Рис. 1. Название рисунка; Таблица 1. Название таблицы). Большие блоки с расшифровкой условных обозначений лучше приводить в тексте. Подписи и надписи – Times New Roman, 10 пт. На все рисунки и таблицы должны быть ссылки в тексте (… на рис. 3, … в табл. 2).

8. ***Рисунки и фотографии должны быть черно-белыми***, четкими, контрастными, аккуратными, сгруппированными. Графики – не жирно, сетка – четко. Единицы измерения и название осей – на русском, шрифт – не жирным. Для десятичных чисел использовать запятую (не точку).

Рисунки могут быть выполнены в программах CorelDraw, Illustrator, Word, Visio и должны давать возможность внесения исправлений, не использовать на рисунках заливки желтым, голубым цветами и т.п., при переводе в ч/б они теряют информативность – сливаются в одинаковый серый. Применять штриховки различного вида.

9. Иллюстрации, разрешением не менее 300 dpi, дублируются отдельными файлами. Если это невозможно, должны быть предоставлены оригиналы иллюстраций, пригодные для полиграфического исполнения. Масштаб изображения – наиболее мелкий (при условии читаемости).

10. Формулы должны быть набраны в формульном редакторе (Equation, MathType) программы Word.

11. На все источники, указанные в списке литературы, должны быть ссылки по тексту (нумерация в порядке упоминания, например, [1, 2], [5–7]). Описание источников должно соответствовать ГОСТ 7.1-2003 и ГОСТ Р 7.0.5-2008 и содержать всю необходимую для идентификации источника информацию, а именно: *для непериодических изданий* – фамилию и инициалы автора, полное название работы, место издания, название издательства, год издания, количество страниц; *для периодических изданий* – фамилию, инициалы автора, полное название работы, название журнала, год выпуска, том, номер, номера страниц.

12. Статья должна иметь (в порядке следования): УДК; И.О. Фамилии авторов; заглавие; аннотация (не реферат); ключевые слова; основной текст статьи; список библиографий под подзаголовком "Литература"; сведения об авторах; далее на английском языке: Фамилии авторов И.О., заглавие статьи, аннотацию, ключевые слова. Сведения об авторах включают в себя фамилию, имя, отчество, ученую степень, ученое звание, должность, место работы, телефон, электронный адрес.

Бумажный вариант рукописи статьи должен быть подписан авторами и иметь сопроводительное письмо на бланке организации (для сторонних авторов).

Плата за публикацию статей не взимается.

Материальные претензии авторов, связанные с распространением материалов их статей после опубликования, не принимаются.

Авторы несут полную ответственность за содержание статей и за последствия, связанные с их публикацией.

Примечание. Адрес для переписки: vnmas@tusur.ru. Тел.: (7–382–2) 51-21-21.