УДК 004.056

А.А. Шелупанов, О.О. Евсютин, А.А. Конев, Е.Ю. Костюченко, Д.В. Кручинин, Д.С. Никифоров

Актуальные направления развития методов и средств защиты информации

Представлены некоторые результаты работ, связанные с различными аспектами фундаментальных, прикладных научных исследований и реализацией производственных задач, выполненных научным коллективом Института системной интеграции и безопасности ТУСУРа. Подробно рассматривается комплексный подход к обеспечению информационной безопасности, позволяющий проводить исследования и создание методов оценки защищенности информационных систем. Приводятся некоторые достижения научной группы, которые связаны с фундаментальными исследованиями и программными реализациями для повышения качества следующих механизмов защиты: биометрической аутентификации пользователей; шифрования; защищенной передачи и определения аутентичности цифровых объектов; определения аутентичности элементов автоматизированных систем управления технологическими процессами и организации защищенных каналов связи при передаче информации между этими объектами.

Ключевые слова: модель системы защиты информации, модель угроз, биометрическая аутентификация, нейросети, шифрование, простые числа, аутентичность цифровых объектов, стеганография, автоматизированные системы управления, защищенные каналы связи.
doi: 10.21293/1818-0442-2017-20-3-11-24

В Томском государственном университете систем управления и радиоэлектроники (ТУСУР) с конца 90-х годов XX в. получило бурное развитие научное направление по исследованиям в области информационной безопасности и защиты информации. Структурным подразделением университета, курирующим данное направление, является Институт системной интеграции и безопасности.

За прошедшие два десятилетия выполнены и выполняются в настоящее время более ста проектов по различным аспектам фундаментальных, прикладных научных исследований и реализации производственных задач в интересах обеспечения информационной безопасности нашей страны. Эти проекты ориентированы на разработки в области аутентификации, криптографии, выявления сетевых атак, создания защищенных систем и защищенных протоколов передачи данных, внедрения технологии PKI в различных отраслях народного хозяйства, проведения компьютерно-технических экспертиз при расследовании киберпреступлений [1–8].

Накопленный в научной школе профессора А.А. Шелупанова опыт по применению комплексного подхода к обеспечению информационной безопасности позволяет проводить теоретические и прикладные исследования по созданию методов оценки защищенности информационных систем, включающих оригинальные способы построения моделей угроз информационной безопасности, систем защиты информации и т.п. [9–14].

В данной статье представлены лишь некоторые из научных исследований, поддержанных различными программами Министерства образования и науки РФ и индустриальными партнерами университета. Имеется и ряд перспективных инициативных исследований, поддержанных не только государственными источниками финансирования, но и частными фондами, крупными корпорациями и некоторыми ведомствами. Весь спектр развиваемых направлений является крайне актуальным и востребованным для обеспечения приоритета страны в научных исследованиях в интересах ее информационной безопасности.

Исследования в области проектирования системы защиты информации

Архитектура системы защиты информации (СЗИ) должна базироваться на следующих принципах:

– СЗИ рассматривается как комплекс средств защиты, направленных на обеспечение безопасности информационной системы и обрабатываемой в ней информации;

– каждое средство защиты информации является комплексом механизмов защиты, реализованных в данном средстве;

– механизмы защиты должны присутствовать на каждом из возможных информационных потоков типа «объект–субъект» и «субъект–субъект»;

– каждый механизм защиты призван нейтрализовать конкретную угрозу, существующую на заданном информационном потоке.

При построении СЗИ специалисты по информационной безопасности (ИБ) формируют перечень внедряемых средств защиты, основываясь на собственном опыте [15, 16]. На сегодняшний день не существует четкого перечня механизмов защиты, реализованных в отдельно взятом средстве защиты, и их сопоставления с конкретными угрозами. Описываемая в данном разделе методика позволяет представить средства защиты в виде перечня механизмов защиты информации.

Для анализа и оценки существующей в организации СЗИ необходимо [17]:

– построить схему защищаемых информационных потоков (схему документооборота);

– для каждого информационного потока определить перечень установленных средств защиты информации (СрЗИ);

– перечень угроз информации для каждого информационного потока.

Для составления схемы документооборота необходима модель документооборота, включающая перечень типовых информационных потоков. Таким образом, схема документооборота – это описание реальных информационных потоков в организации в виде структуры, состоящей из типовых элементов (объектов, хранящих или передающих информацию, и субъектов, обрабатывающих информацию) и типовых каналов связи между ними. Модель угроз содержит типовые угрозы для типовых информационных потоков. Классификация механизмов защиты напрямую зависит от угроз. При этом для каждой типовой угрозы существует собственный механизм защиты.

В рамках методики необходима конкретизация состава механизмов защиты, реализованных во внедренных и потенциально рекомендуемых специалистом по ИБ СрЗИ. Бизнес-процесс «Формирование рекомендуемого перечня СрЗИ» представлен на рис. 1 в нотации IDEF0.

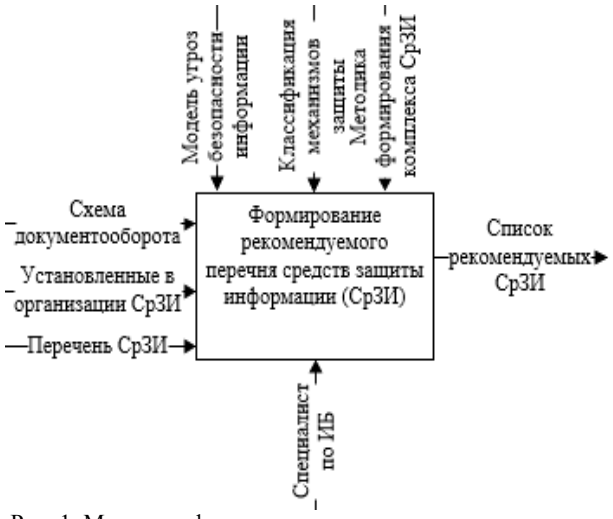

Рис. 1. Методика формирования рекомендуемого перечня средств защиты информации

Формирование рекомендуемого перечня СрЗИ происходит в три этапа (рис. 2):

1) определение перечня угроз для каждого существующего в организации информационного потока;

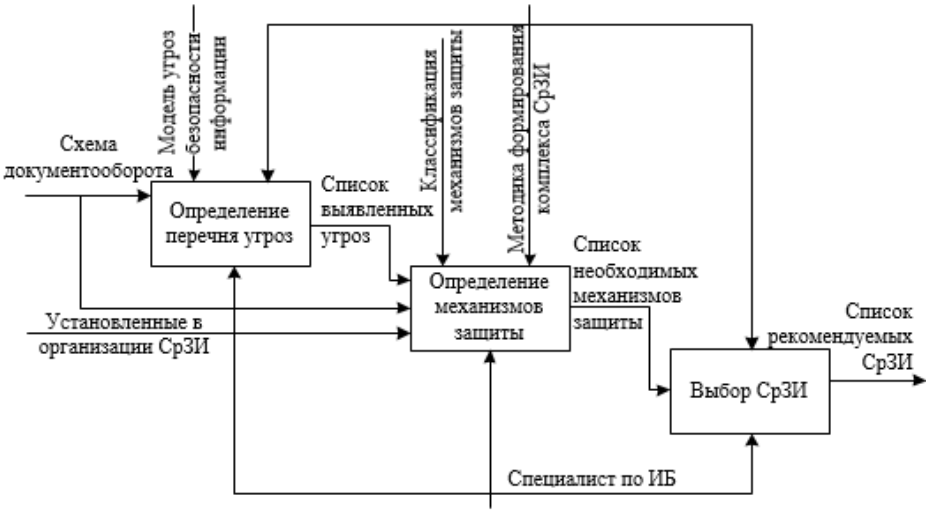

Рис. 2. Декомпозиция методики формирования рекомендуемого перечня средств защиты информации

2) определение для каждого существующего информационного потока функционирующих в организации механизмов защиты и их достаточности;

3) выбор для каждого существующего информационного потока рекомендуемых СрЗИ, позволяющих нейтрализовать «незакрытые» угрозы.

Модель документооборота

При построении модели документооборота за основу было принято то, что действия, направленные на информацию и ее носители, могут происходить в разных средах. Среди них можно выделить такие среды, как:

– видовая – среда, где существует угроза визуального получения информации, т.е. возможность получения информации из документа без использования дополнительных преобразований;

– физическая – среда, где существует угроза получения доступа непосредственно к самому носителю информации;

– акустическая/виброакустическая – среда, где существует угроза утечки речевой информации;

– среда сигналов – среда, где существует угроза получения информации через побочные электромагнитные излучения носителей и средств ее передачи;

– виртуальная – среда, где существует угроза получения информации непосредственно из оперативной памяти.

На рис. 3 представлена разработанная модель документооборота. Элементы полученного графа представлены ниже.

Носители информации: V_1 – объект, хранящий аналоговую информацию, в том числе печатные до-

кументы; V_2 – человек; V_3 – объект, хранящий цифровую информацию; V_4 – процесс.

Каналы передачи информации: e_1 – в визуальной среде; e_2 – в акустической среде; e_3 – в электромагнитной среде; e_4 – в виртуальной среде.

Каналы удаленной передачи информации: e_3' – в электромагнитной среде; e_4' – в виртуальной среде.

На данной модели документооборота было построено множество документопотоков $G = \{V, e\}$, где $V = \{V_1, V_2, V_3, V_4\}$ – это множество состояний, а $e = \{e_1, e_2, e_3, e_4\}$ – множество каналов передачи информации. Под документопотоком понимается поток документов между пунктами обработки и создания информации (руководителями организации и структурных подразделений, специалистами) и пунктами технической обработки документов: экспедицией, секретариатом, канцелярией.

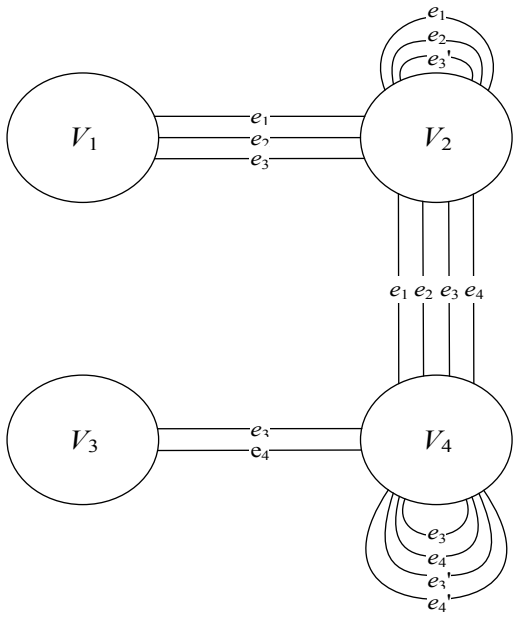

Рис. 3. Модель документооборота

Представленная модель является основой для построения схемы документооборота в организации. Любую схему документооборота можно представить как совокупность элементарных документопотоков (рис. 4).

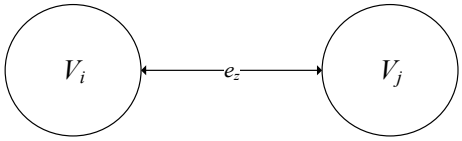

Рис. 4. Элементарный документопоток

Модель угроз обрабатываемой информации

Комплексная модель угроз информационной безопасности состоит из трех элементов:

– модель угроз обрабатываемой информации и её носителям [18];

– модель угроз безопасности информационной системы [19];

– модель угроз безопасности СЗИ.

При этом ко всем трем элементам существуют угрозы конфиденциальности и целостности, а к обрабатываемой информации – дополнительно угрозы доступности.

Например, применительно к обрабатываемой информации можно выделить 4 типовые угрозы конфиденциальности, применимые к каждому документопотоку:

– подмена получателя V_i;

– подмена получателя V_j;

– использование несанкционированного канала e_z;

– контроль злоумышленником канала e_z.

Примером подобных типовых угроз могут являться соответственно:

– отправка защищаемой информации ложному объекту в сети (из-за подмены IP-адреса, адреса вебсайта, электронной почты получателя при типе документопотока $\{V_4, e_4', V_4\}$) или запись информации ограниченного доступа в незащищенный файл (при типе документопотока $\{V_3, e_4', V_4\}$);

– несанкционированное считывание информации из защищаемого файла (при типе документопотока $\{V_3, e_4', V_4\}$);

– использование сетевых протоколов, не поддерживающих шифрование (при типе документопотока $\{V_4, e_4', V_4\}$);

– перехват сетевых пакетов за счет анализа сетевого трафика (при типе документопотока $\{V_4, e_4', V_4\}$).

Таким образом, при использовании разработанной модели можно получить типовой набор угроз для каждого элементарного документопотока в схеме документооборота, что приводит к формализации процесса составления перечня угроз и ликвидации субъективизма при получении искомого результата.

Модель системы защиты информации

Построение модели системы защиты информации основано на классификации механизмов защиты в зависимости от элементарного документопотока и типа угрозы.

Для каждого документопотока в каждой из сред были выбраны типовые механизмы защиты информации в соответствии с типовыми угрозами. Результаты классификации механизмов защиты от угроз конфиденциальности информации в виртуальной среде представлены в табл. 1.

Типы механизмов защиты, обозначенных в табл. 1:

– идентификация и аутентификация (ИА);

– управление доступом (УД);

– очистка памяти (ОП);

– регистрация событий (РС);

– шифрование (ШИ).

Если рассматривать элементарный документопоток между человеком (пользователем) и любым прикладным процессом по виртуальному каналу, то подобным каналом будут являться драйверы устройств ввода/вывода.

Перечень угроз конфиденциальности передаваемой информации и соответствующих механизмов защиты представлен в табл. 2.

Таблица 1

Соответствие механизмов защиты типовым угрозам в виртуальной среде на автоматизированном рабочем месте

Типы угроз	Типы механизмов защиты Виды документопотоков		
	Человек – процесс $\{V_2, e_4, V_4\}$	Носитель цифровой информации – процесс $\{V_3, e_4, V_4\}$	Процесс – процесс $\{V_4, e_4, V_4\}$
1-й тип	ИА УД РС ШИ	ИА УД РС ШИ	ИА УД РС ШИ
2-й тип	ИА УД РС ШИ	ИА УД РС ШИ	ИА УД РС ШИ
3-й тип	ИА УД РС	ИА УД РС	ИА УД РС
4-й тип	ОП РС	ОП РС	ОП РС

Таблица 2

Пример механизмов защиты для документопотока $\{V_2, e_4, V_4\}$

Угроза	Механизмы защиты
Получение несанкционированным пользователем данных, обрабатываемых прикладным процессом	ИА – аутентификация пользователя при запуске программы. УД – разграничение доступа пользователей к запуску программ. РС – регистрация работы пользователя с программой. ШИ – вывод пользователю только закодированной информации
Ввод защищаемой информации в несанкционированную программу	ИА – проверка аутентичности исполняемого файла. УД – реализация замкнутой программной среды. РС – регистрация работы пользователя с программой. ШИ – ввод пользователем только закодированной информации
Использование несанкционированного (некорректного) драйвера устройства при вводе/выводе данных	ИА – проверка аутентичности драйвера при запуске. УД – разграничение доступа пользователей к устройствам ввода/вывода в операционной системе. РС – регистрация событий, связанных с работой драйвера
Считывание обрабатываемой информации из буферов в оперативной памяти, закрепленных за устройством ввода/вывода	ОП – очистка буферов оперативной памяти. РС – регистрация событий, связанных с очисткой памяти

Построенная модель системы защиты информации имеет существенное достоинство по сравнению с аналогами. Заключается оно в детальной проработке конкретных элементов модели и взаимосвязи между ними, а именно: в данной модели учтены все типы угроз информации для всевозможных потоков передачи информации в виртуальной, электромагнитной, акустической и видовой средах, представлен перечень механизмов защиты, которые приведены в соответствие типовым угрозам, нейтрализацию которых они обеспечивают. Это позволяет повысить качество проектируемой системы защиты информации и минимизирует влияние субъективных аспектов, таких как уровень квалификации эксперта.

Исследования, связанные с реализацией механизмов защиты информации

Научной группой под руководством А.А. Шелупанова проводятся исследования, направленные на реализацию и улучшение различных типов механизмов защиты. Основной упор делается на защиту информации, циркулирующей в виртуальной среде – автоматизированных системах и сетях передачи данных.

В данном разделе приводятся основные достижения научной группы, которые связаны с фундаментальными исследованиями и программными реализациями, направленными на повышение качества следующих механизмов защиты:

– механизмов биометрической аутентификации пользователей за счет использования нейросетей и их комплексирования с общепринятыми методами;

– механизмов шифрования за счет улучшения алгоритмов определения простоты числа;

– механизмов защищенной передачи и определения аутентичности цифровых объектов за счет разработки стеганографических методов преобразования данных;

– механизмов определения аутентичности элементов автоматизированных систем управления технологическими процессами (АСУТП) и организации защищенных каналов связи при передаче информации между этими объектами за счет адаптации типовых сетевых протоколов под специфику функционирования АСУТП.

Исследования в области аутентификации

Классическим подходом к аутентификации пользователей является использование традиционной парольной защиты. В рамках данного подхода производится сопоставление пары идентификатор–аутентификатор (логин–пароль) с аналогичной информацией, в том или ином виде хранящейся на стороне. При этом это не обязательно будет такая же пара логин–пароль – информация может храниться в зашифрованном виде, или же храниться могут только хэш-функции от данной информации [20].

Очевидным плюсом такого подхода является простота реализации, отсутствие необходимости приобретения для этого каких-либо дополнительных аппаратных средств и сложного программного обеспечения.

Однако наряду с этим такой подход имеет и ряд существенных недостатков:

1) пароль может быть легко передан другому лицу, причем такая передача может носить как случайный характер, так и преднамеренный (который, в свою очередь, может быть добровольным или осуществленным под воздействием различных угроз);

2) после такой передачи факт разглашения пароля остается совершенно не очевидным и до момента нанесения ущерба после такого разглашения сам его факт, в подавляющем большинстве случаев, остается незамеченным, что не дает прямых поводов к смене пароля;

3) возможность обыкновенного забывания пароля пользователем, приводящее к потенциальной потере доступа к информации;

4) возможность подбора пароля методами перебора;

5) возможные атаки на место хранения пар логин–пароль на стороне, проводящей непосредственное сравнение при аутентификации [21].

Выявленные слабые стороны требуют дополнительных мер по усилению традиционной парольной защиты за счет использования многофакторной аутентификации.

Многофакторная аутентификация – это такая технология контроля доступа, при которой помимо ввода логина и пароля к аккаунту пользователя просят подтвердить свою личность дополнительными способами. В качестве таких способов могут использоваться способы, основанные на обладании определенным предметом, имеющимся в наличии только у легального пользователя. Причем это может быть как отдельным физическим предметом (токен, смарт-карта и т.д.), так и частью самого пользователя, неотделимой или сложно отделимой от самого пользователя (ладонь, палец, манера работы на клавиатуре и т. д.). Во втором случае речь идет о биометрических характеристиках.

Биометрические характеристики – это набор некоторых физических или поведенческих черт, позволяющих осуществлять подтверждение личности пользователя.

Все биометрические характеристики человека могут быть разделены на две большие группы:

– статические характеристики пользователи;

– динамические характеристики пользователя.

Статические биометрические характеристики пользователя

Статические методы биометрической аутентификации основаны на физиологических характеристиках человека, присутствующих от рождения и до смерти, находящихся при нём в течение всей его жизни, которые не могут быть потеряны, украдены и скопированы [22].

В качестве традиционно используемых статических характеристик можно выделить следующие:

1) отпечаток пальца [23–25];

2) геометрия руки [26, 27];

3) геометрия лица [28];

4) радужная оболочка глаза [29];

5) сетчатка глаза [30].

В качестве недостатка такого рода характеристик можно выделить тот факт, что при большом желании они могут быть физически отделены от владельца, принудительно использованы или подделаны.

Эти недостатки могут быть компенсированы использованием динамических биометрических характеристик.

Динамические биометрические характеристики пользователя

Динамические методы биометрической аутентификации основываются на поведенческих характеристиках людей, т.е. на характерных подсознательных движениях в процессе воспроизведения или повторения какого-либо обыденного действия [22].

В качестве традиционно используемых статических характеристик можно выделить следующие:

1) образ подписи [31];

2) динамика подписи [32];

3) голос [33];

4) клавиатурный почерк [34].

При этом следует отметить, что использование динамических биометрических характеристик не является панацеей, поскольку практически все они имеют существенную вероятность ошибки первого и второго рода, что не позволяет говорить об их самостоятельном использовании. В свою очередь, их комплексирование с другими методами в рамках построениям многофакторной аутентификации при системе «И» (пройти все подсистемы) приводит к существенному росту вероятности ошибок первого рода, опять же снижающую работоспособность системы. Рассмотрим некоторые подходы, реализованные, в частности, на факультете безопасности Томского государственного университета систем управления и радиоэлектроники.

Клавиатурный почерк пользователя на фиксированной парольной фразе

Основными параметрами, по которым можно построить такую характеристику, являются продолжительность нажатия (промежуток времени между нажатием на клавишу и отпусканием этой клавиши) и интервал между нажатиями (промежуток времени между нажатием текущей клавиши и нажатием следующей клавиши).

Идентификация по фиксированной фразе основана на анализе характеристик клавиатурного почерка пользователя, полученных благодаря вводу заранее заданной фразы в определенной точке системы. Например, во время выполнения входа в систему, когда пользователь вводит свой логин и пароль. Также данный метод может включать в себя использование определенной фразы, общей для всех пользователей. Статический анализ обычно применяется в системах, в которых пользователи вводят с клавиатуры лишь небольшой объем текста, например, в различных онлайн-сервисах, таких как банки, магазины и т.д. [35].

По итогам тестирования методов, основанных на использовании нейронных сетей, получены оцен-

ки вероятности ошибок первого рода 3–4% при соответствующей вероятности ошибок второго рода 2–3% [36]. Эти высокие значения не позволяет говорить о самостоятельной применимости данного подхода.

Лучшие значения можно получить при использовании подхода, основанного на нечеткой логике [37], а именно 4–5% вероятность ошибок первого рода при 1–2% вероятности ошибок второго рода, однако самостоятельное применения такого подхода для аутентификации также проблематично.

Клавиатурный почерк пользователя в рамках аутентификации по произвольному тексту

При аутентификации пользователя по клавиатурному почерку по произвольному тексту можно, считывая нажатия клавиш и записывая информацию о них в базу данных прозрачно для пользователя и не привлекая внимание злоумышленника, который может занять место авторизированного пользователя за компьютером, предотвратить несанкционированный доступ к рабочему месту.

При этом параметры для аутентификации (вышеупомянутые временные интервалы) измеряются на наиболее часто встречающихся сочетаниях знаков (биграммах, триграммах и т. д.). Применение такого подхода в рамках собственной реализации позволяет говорить о безошибочной различимости 8 пользователей на обучающей выборке более 100 000 знаков от пользователя при применении наивного классификатора Байеса, однако такой объем выборки является неприменимым на практике. Кроме того, в других источниках [34] можно найти аналогичные оценки вероятностей ошибок при различных используемых методах анализа характеристик аутентификации, однако ни один из них опять же не позволяет говорить о самостоятельной применимости рассматриваемого подхода.

Аутентификация по динамике проставления подписи

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 [32]. При подготовке параметров, участвующих в проведении процедуры аутентификации, выполнялись следующие действия:

1) съем зависимостей положения пера на планшете $x(t)$ и $y(t)$, высоты $z(t)$, давления на планшет $p(t)$, угла наклона пера к планшету $\alpha(t)$ и угла между пером и плоскостью, образованной осями y и z, и пером $\beta(t)$ от времени t (итого 6 характеристик);

2) проведение нормировки подписи к фиксированному размеру, ограниченному максимальными значениями характеристик путем линейного преобразования, перерасчет зависимостей шага 1 с учетом нормировки;

3) расчет зависимостей скоростей и ускорений изменения характеристик от времени (итого вместе с исходными получаем после этого шага 18 характеристик);

4) применение преобразования Фурье и выделение амплитуд постоянной составляющей и первых семи гармоник временных зависимостей из шага 1 – итого 8 амплитуд – получаем на выходе параметра, записываемых в БД и используемых классификаторами при анализе [38].

Далее проводился анализ полученных параметров с применением методов нейронных сетей и наивного классификатора Байеса. По его итогам наилучшие оценки качества для отдельных классификаторов составили менее 5% для вероятности ошибки аутентификации, при минимальных значениях более 1%, что опять же очевидно не говорит в пользу самостоятельного использования такого подхода.

Комплексирование нескольких методов аутентификации с гарантией неснижения характеристик лучшего из методов

Очевидным подходом к повышению производительности отдельных методов является их комплексирование. Однако при прямом комплексировании по методу «И», в рамках которого необходимо одновременное прохождение всех отдельных применяемых методов, возникает проблема, что вероятности успешной аутентификации легального пользователя в рамках разных подходов будут перемножаться. Это, в свою очередь, приведет к быстрому росту вероятности ошибки первого рода и снижению применимости такого подхода. Необходимо разработать такой подход комплексирования, который гарантировал бы неснижение любых отдельных показателей качества подхода относительно лучшего из комплексируемых подходов.

Такой подход может быть сформулирован следующим образом:

1) проводится свертка выходных значений нейронной сети и классификатора Байеса с применением монотонной функции. Данная функция дополнительно содержит несколько коэффициентов – параметров проведения свертки. Применение такой функции гарантирует, что существует такой набор коэффициентов, который вырождает эту свертку в отдельный классификатор с его параметрами качества;

2) проводится оптимизация полученной свертки с точки зрения подборов оптимальных параметров свертки и порогов принятия решения при классификации. Пороги классификации подбираются независимо для каждого пользователя и могут отличаться между собой. Так как отдельные классификаторы являются фрагментами свертки, то по итогам оптимизации гарантируют результат не хуже, чем их отдельные показатели качества на основе вероятностей ошибок, независимо от конкретного вида этого критерия.

Для реализации данного подхода вся выборка делится на 3 части – обучающую для классификаторов (в рамках эксперимента 60%), обучающую для

оптимизации (20%) и тестовую для оценки качества полученного комбинированного классификатора (20%) [39].

Применение такого подхода позволило достигнуть статистически значимого снижения вероятности ошибки аутентификации при комплексировании подходов на основе нейронной сети и наивного классификатора Байеса. Применение такого подхода принципиально возможно и при построении системы многофакторной аутентификации и объединении различных факторов, например аутентификации по голосу и по динамике подписи, гарантируя итоговый показатель качества не хуже, чем у отдельно взятого подхода.

Направления дальнейших исследований

В рамках данного раздела представлен обзор методов аутентификации с рассмотрением их сильных и слабых сторон. Подробное рассмотрена аутентификация по динамическим биометрическим характеристикам, с использованием методов, реализованных в Институте системной интеграции и безопасности Томского государственного университета систем управления и радиоэлектроники. Сделано заключение, что хотя применение таких методов и позволяет получить результаты, сопоставимые с мировыми аналогами в области самостоятельного анализа отдельных характеристик, ни один из рассматриваемых подходов не может быть применен без дополнения, поскольку не обеспечивает приемлемого на практике уровня качества аутентификации с точки зрения вероятностей ошибок первого и второго рода.

Прямое комплексирование таких подходов при объединении результатов на основе оператора «И» приводит к существенному росту вероятности ошибок первого рода и затрудняет практическое применение подобной системы.

Предложен подход к комплексированию результатов разных методов анализа, гарантирующий результаты не хуже, чем лучший из них, независимо от используемого критерия оценки, основанного на точности. Показана его применимость при аутентификации по динамике проставления подписи на основе методов наивного классификатора Байеса и нейронной сети. Возможно применение такого подхода для комплексирования нескольких факторов при составлении многофакторной системы аутентификации, однако выбор функций для объединения более двух параметров остается темой для дальнейшего исследования.

Исследования в области криптографии

Многие современные криптографические системы строятся на базе простых чисел. Так, в известной криптографической системе с открытым ключом RSA потребность в выборе простых чисел имеет основополагающую позицию и от выбора простых чисел во многом определяется стойкость шифрования [40]. Поэтому важным направлением развития методов и систем защиты информации является разработка эффективных методов и алгоритмов генерации простых чисел. Одна из ключевых задач, связанных с генерацией простых чисел, заключается в проверке на простоту сгенерированного числа.

Все алгоритмы проверки простоты (тесты простоты) делятся на два больших класса: детерминированные и вероятностные алгоритмы. Детерминированные алгоритмы позволяют гарантированно точно определить простое число, но имеют большую вычислительную сложность. Вероятностные алгоритмы позволяют установить простоту числа с некоторой вероятностью ошибки, но за гораздо меньшее время. Для уменьшения вероятности ошибки алгоритм повторяется, но с другими параметрами. Если число не удовлетворяет условиям проверки вероятностным алгоритмом, то оно гарантированно является составным числом.

Существует большое количество тестов простоты. Обзором различных тестов простоты числа занимались такие ученые, как А.А. Балабанов [41], О.Н. Василенко [42], А.В. Черемушкин [43], P. Ribenboim [44] и др. Исходя из проведенных обзоров, можно выделить следующие ключевые моменты:

– в настоящее время широко используются вероятностные проверки простоты. Так, объединенный алгоритм Рабина–Миллера широко используется в криптосистемах с открытым ключом для построения простых ключей длиной 512, 1024 и 2048 бит;

– в основе (в качестве критерия простоты) большинства современных применяемых на практике тестов простоты числа лежит малая теорема Ферма [44]. Под критерием простоты числа понимается такое необходимое условие, выполнение которого обязательно для простых чисел.

Поэтому исследования в области разработки критериев простоты и на их основе алгоритмов проверки натуральных чисел на простоту имеют большое значение для повышения качества криптографических систем при шифровании.

Результаты исследования по поиску новых критериев простоты числа

Для поставленных задач был разработан метод генерации критериев простоты на основе использования аппарата производящих функций [45]. Метод основывается на следующем свойстве композиции производящих функций: для двух обыкновенных производящих функций с целыми коэффициентами $B(x)=\sum_{n\geq 0} b_n x^n$ и $F(x)=\sum_{n>0} f_n x^n$, и композиты $F^{\Delta}(n,k)$ производящей функции $F(x)$ значение выражения

$$\sum_{k=1}^{n-1} \frac{F^{\Delta}(n,k) b_{k-1}}{k}$$

является целым для всех простых чисел n.

На основе указанного метода были построены различные критерии простоты числа, например, если в качестве внешней производящей функции использовать $R(x)=\operatorname{arctg}(x)$, а внутренней функции $F(x)=ax+bx^2$, то можно вывести выражение

$$(-1)^{n+1}\frac{\left(a+\sqrt{4b-a^2 i}\right)+\left(a-\sqrt{4b-a^2 i}\right)-(2a)^n}{n2^n},$$

значение которого при произвольных a, b является целым для простых n.

Используя разработанный метод, становится возможным создание большого набора новых критериев простоты числа. Поэтому данный процесс был автоматизирован путем создания специализированного программного обеспечения – генератор критериев простоты числа (Primality Criterion Generator – PCG) [46].

Использование разработанного программного обеспечения приводит к накоплению большого количества критериев простоты поэтому были разработаны методы оценивания полученных критериев [47]. В качестве основных критериев эффективности критерия простоты было выделено следующее: универсальность теста простоты, достоверность получаемого результата, вычислительная сложность. Для автоматизации оценки также был реализован инструментарий для анализа тестов и критериев простоты числа в виде специализированного программного обеспечения – Primality Test Analyser – PTA [48]. Разработанные программы PCG и PTA составляют комплекс программ и являются удобным средством исследования критериев простоты числа для дальнейшего поиска эффективного теста простоты числа.

В итоге в ходе исследования были рассмотрены 117 различных пар функций. Для каждой функции рассматривались простые целочисленные параметры в пределах от –5 до 5 (итого: 9 608 пар функций), а также учитывалось не только суммирование до $(n-1)$-го элемента, но и полное суммирование с учетом n-го элемента (итого: 19 216 пар функций). В результате исследования были найдены 930 потенциальных критериев простоты числа, на основе которых можно строить новые тесты простоты.

Исследования в области цифровой стеганографии

Одно из современных направлений защищенной передачи данных в информационных системах основано на использовании методов цифровой стеганографии, реализующих встраивание в цифровые объекты скрытых информационных последовательностей различного назначения.

Стеганографические методы защиты информации позволяют решать такие задачи, как обеспечение конфиденциальности информации и обеспечение аутентификации цифровых объектов [49]. Кроме того, методы цифровой стеганографии используются в областях, непосредственно не связанных с информационной безопасностью. В качестве примера можно привести встраивание служебной информации в медицинские изображения для удобства их хранения и обработки.

В данном разделе будут рассмотрены научно-технические результаты, полученные исследовательским коллективом факультета безопасности в области цифровой стеганографии.

Помимо решаемых задач методы цифровой стеганографии классифицируют по типам данных, с которыми они работают. В основном это аудио-, видеоданные и цифровые изображения. Далее речь пойдет о встраивании информации в цифровые изображения.

В этом случае следующий уровень классификации определяется наличием сжатия: методы и алгоритмы, работающие со сжатыми изображениями и изображениями без сжатия, рассматривают как два разных класса.

Встраивание информации в несжатые цифровые изображения осуществляется в пространственную или частотную область. Пространственной областью называется матрица пикселей цифрового изображения, а частотная область – это матрица значений, полученных из цифрового изображения при применении к нему какого-либо частотного преобразования. Данные значения называют также коэффициентами частотного преобразования [50]. Встраивание информации в частотную область позволяет обеспечить незаметность или робастность встраивания в зависимости от конкретной задачи, а также совместить встраивание информации с форматами представления цифровых изображений.

Стеганографические методы, работающие со сжатыми цифровыми изображениями, в большинстве случаев являются частотными. Наиболее распространенный метод сжатия цифровых изображений с потерями JPEG основан на дискретном косинусном преобразовании (ДКП) [50], и при работе с JPEG-изображениями встраивание осуществляется посредством внесения изменений в квантованные коэффициенты дискретного косинусного преобразования (далее – ДКП-коэффициенты или просто коэффициенты).

Авторами настоящей статьи были получены оригинальные стеганографические методы и алгоритмы во всех перечисленных направлениях. Они представлены в нижеследующих разделах.

Пространственное встраивание информации в несжатые цифровые изображения

Существует большое количество алгоритмов пространственного встраивания информации в цифровые изображения. Наиболее широкий класс составляют алгоритмы, основанные на методе наименее значимых битов (LSB), согласно которому для записи битов секретного сообщения используются младшие один–два бита пикселей цифрового изображения, несущие в себе наименьшее количество информации, воспринимаемой зрением человека [49].

Основная проблема LSB-подобных алгоритмов заключается в том, что в результате встраивания младшие биты пикселей цифрового изображения приобретают статистические характеристики, присущие секретному сообщению, что является демаскирующим признаком, указывающим на наличие в изображении встроенного сообщения.

Существуют разные подходы к решению данной проблемы. Одним из таких подходов является

предварительное преобразование секретного сообщения перед встраиванием, направленное на сокрытие его статистических характеристик.

В [51] в качестве такого преобразования предлагается использовать динамику обратимого клеточного автомата. Примером клеточного автомата, обладающего свойством обратимости, является блочный клеточный автомат [52, 53]. Проведено исследование, направленное на установление способности блочного клеточного автомата к перемешиванию и рассеиванию информации, и определены параметры автомата, позволяющие обеспечить надежное сокрытие статистических характеристик встраиваемого сообщения в ходе предварительного преобразования.

Для решения данной задачи можно было использовать иные обратимые преобразования, например шифрование, однако преимуществом клеточно-автоматного преобразования являются простота реализации и высокое быстродействие.

Классическое LSB-подобное встраивание информации в пиксели цифрового изображения не позволяет впоследствии восстановить исходные значения измененных пикселей. Однако существуют алгоритмы, реализующие обратимое сокрытие данных, когда при извлечении встроенного сообщения из изображения-контейнера исходное изображение восстанавливается без каких-либо потерь.

Примером алгоритмов, обладающих подобным свойством, являются алгоритмы, основанные на интерполяции, когда секретное сообщение встраивается не в само оригинальное изображение, а в изображение-контейнер, полученное путем увеличения оригинала.

В статье [54] представлено исследование широкого класса подобных алгоритмов и получен собственный алгоритм, основанный на использовании интерполяционного полинома Лагранжа второй степени. В результате проведенного исследования установлено, что данный класс алгоритмов не обеспечивает высокого визуального качества стегоизображений, однако к преимуществам относятся высокая емкость, устойчивость к небольшим изменениям яркости, а также обратимость встраивания.

Частотное встраивание информации в несжатые цифровые изображения

Исследования в области частотного встраивания представлены алгоритмом, описанным в работе [55].

Данный алгоритм осуществляет встраивание секретного сообщения в фазовый спектр дискретного преобразования Фурье (ДПФ). Выбор фазового спектра для встраивания связан с тем, что в отличие от амплитуд фазы элементов Фурье-образа принимают значения из точно определенного интервала $(-\pi,\pi]$ независимо от изображения-контейнера. Это свойство удобно использовать для задания операции встраивания.

Изображение-контейнер разбивается на неперекрывающиеся блоки равного размера, к каждому из которых применяется ДПФ и рассчитывается фазовый спектр. Для встраивания одного бита секретного сообщения используется один элемент фазового спектра.

Процедура встраивания определена следующим образом. В интервале $(-\pi,\pi]$ выбирается два непересекающихся интервала $(\varphi_0-\varepsilon,\varphi_0+\varepsilon)$ и $(\varphi_1-\varepsilon,\varphi_1+\varepsilon)$, называемых интервалами встраивания. Фазовые значения, попадающие в интервал $(\varphi_0-\varepsilon,\varphi_0+\varepsilon)$, принимаются как соответствующие нулевому биту, а фазовые значения, попадающие в интервал $(\varphi_1-\varepsilon,\varphi_1+\varepsilon)$, – как соответствующие единичному биту. Для встраивания сообщения фазовые значения блоков изображения-контейнера последовательно обходятся и проверяются на принадлежность заданным интервалам встраивания. Если значение очередного элемента фазового спектра принадлежит одному из интервалов встраивания, то в него записывается очередной бит секретного сообщения следующим образом: если необходимо записать 0, то фазовому элементу присваивается значение φ_0, если 1 – значение φ_1. Низкочастотные элементы фазового спектра исключаются из обхода, чтобы избежать существенных искажений блока изображения-контейнера.

Важной особенностью представленного в [55] исследования является решение характерной для частотного встраивания проблемы искажения встроенного сообщения при восстановлении пикселей цифрового изображения из частотных коэффициентов. В известных исследованиях, посвященных робастным стеганографическим методам, рассматривается только устойчивость стеганографических вложений по отношению к внешним воздействиям на стегоконтейнер. Однако при встраивании информации в частотную область цифровых объектов и отсутствии внешних воздействий искажения вносятся на этапе восстановлении цифрового объекта из измененного частотного спектра в связи с округлением вещественных величин до целых.

В работе [55] данная проблема решается за счет оригинального подхода, заключающегося в организации итеративной процедуры встраивания. После встраивания части сообщения в блок изображения происходит проверка, возможно ли извлечь все вложенные биты без ошибок. Для этого выполняется обратное ДПФ, происходит формирование значений пикселей блока, а затем заново применяется ДПФ, т.е. имитируется ситуация извлечения сообщения. Если возникают ошибки, они исправляются путем повторного встраивания битовой строки в блок коэффициентов, полученный после последнего ДПФ. Потеря и инверсия бита корректируются повторным встраиванием, для устранения ложного бита происходит возврат к первоначальному фазовому значению. Если безошибочного извлечения не удается достичь за заданное число итераций, то количество информации, встраиваемой в блок, уменьшается на один бит, и вся процедура повторяется заново.

Данный подход позволяет избежать искажения передаваемого в стегоизображении сообщения и впоследствии извлечь его в исходном виде.

Встраивание информации в сжатые JPEG-изображения

Встраивание информации в сжатые JPEG-изображения представлено рядом алгоритмов, опубликованных в работах [56, 57].

Данное направление в цифровой стеганографии отличается наибольшей практической значимостью в связи с повсеместностью использования сжатых JPEG-изображений.

Алгоритмы, работающие с JPEG-изображениями, при встраивании оперируют отдельными ДКП-коэффициентами или группами ДКП-коэффициентов. Во втором случае встраивание заключается в установлении определенных соотношений между коэффициентами в зависимости от встраиваемых битов.

Помимо этого, такие алгоритмы различаются по используемым операциям над элементами данных. В случае непосредственного встраивания битов сообщения в отдельные ДКП-коэффициенты можно выделить два основных класса операций: аддитивные операции и операции замены.

Аддитивное встраивание информации в сжатые JPEG-изображения преимущественно представлено различными алгоритмическими реализациями метода PM1. Данный метод оперирует ненулевыми ДКП-коэффициентами JPEG-изображения, встраивая в каждый из них один бит секретного сообщения. Встраивание заключается в изменении четности коэффициентов в зависимости от значений встраиваемых битов.

В исследовании [56] показано, что эффективность встраивания по методу PM1 зависит от порядка обхода блоков JPEG-изображения и порядка обхода ДКП-коэффициентов в каждом блоке. Встраивание равного количества информации в блоки с разным количеством по-разному расположенных ненулевых коэффициентов приводит к разному уровню искажений. Поэтому при частичном заполнении стегоконтейнера повышение качества встраивания может быть достигнуто за счет целенаправленного выбора ДКП-коэффициентов, в которые будут записаны биты секретного сообщения.

На основе проведенного исследования в [56] предложен оригинальный подход к построению стегопути при встраивании сообщения в ДКП-коэффициенты JPEG-изображения по методу PM1. Суть данного подхода заключается в том, что для каждого блока изображения-контейнера рассчитывается вес, зависящий от того, в каких частотных областях располагаются составляющие данный блок ДКП-коэффициенты, и порядок обхода блоков при встраивании зависит от полученных весовых значений.

Алгоритм встраивания, реализующий предложенный подход, относится к классу полуадаптивных алгоритмов, поскольку веса блоков рассчитываются до начала встраивания. После этого биты сообщения последовательно распределяются по блокам изображения таким образом, что ни в один блок не встраивается два бита подряд. При этом ДКП-коэффициенты в каждом блоке обходятся в порядке от высокочастотных областей к низкочастотным.

Данный подход позволяет существенно повысить качество встраивания по сравнению со случайным распределением битов сообщения по блокам изображения-контейнера.

Другой класс стеганографических алгоритмов, работающих с ДКП-коэффициентами сжатых изображений, основан на операциях замены. Замене могут подвергаться ДКП-коэффициенты либо отдельные биты ДКП-коэффициентов. В работе [57] представлены результаты исследования оригинальной схемы встраивания на основе операции замены отдельных ДКП-коэффициентов.

Основным элементом данной схемы является малое целочисленное значение x, называемое величиной замены. При встраивании в один ДКП-коэффициент записывается один бит секретного сообщения следующим образом: если бит равен единице, то ДКП-коэффициент заменяется значением x, в противном случае – значением $–x$. Для исключения неоднозначности при извлечении вводится дополнительная операция: все ДКП-коэффициенты, по абсолютному значению совпадающие с величиной замены, но не используемые для записи битов сообщения, увеличиваются или уменьшаются на единицу.

В [57] предлагается четыре алгоритмических реализации описанной стеганографической схемы. Их особенностью является использование генетического алгоритма для повышения качества встраивания. Отличие отдельных алгоритмов друг от друга заключается в постановке задач оптимизации.

Роль генетического алгоритма во всех случаях состоит в том, чтобы наилучшим образом разместить подстроку встраиваемой двоичной строки в ДКП-блоке.

Если взять определенное значение величины замены x и считать, что ДКП-коэффициенты с данным значением соответствуют единичному биту, а ДКП-коэффициенты с противоположным по знаку значением – нулевому биту, то можно увидеть, что любой блок ДКП-коэффициентов исходного изображения уже содержит некоторую двоичную строку. Поэтому встраивание можно рассматривать как переход от уже имеющейся в блоке строки к строке, подлежащей встраиванию. Данный переход можно совершить разными способами, каждый из которых требует разного количества изменений, вносимых в ДКП-коэффициенты. При этом решение об использовании отдельно взятого коэффициента (запись в данный коэффициент нуля или единицы, корректирующая операция, отсутствие изменений) приводит к появлению множества вариантов использования прочих коэффициентов. И задача оптимизации заключается в выборе лучшего варианта для всего блока.

Важным преимуществом введенной схемы встраивания и реализующих ее алгоритмов является

возможность произвольного выбора ДКП-коэффициентов для встраивания, что позволяет обеспечить неравномерное распределение битов сообщения по блокам ДКП-коэффициентов изображения-контейнера. Данное решение позволяет адаптировать встраивание к свойствам изображения-контейнера.

Направления дальнейших исследований

Дальнейшее развитие рассмотренного направления будет заключаться в синтезе новых алгоритмов встраивания информации в цифровые изображения, обладающих улучшенными показателями эффективности встраивания.

В частности, предлагается использовать биоинспирированные методы оптимизации для повышения эффективности стеганографического встраивания информации. Будут поставлены и решены новые задачи оптимизации как для непосредственного встраивания информации, так и для формирования пространства сокрытия.

Исследования в области защищенной передачи данных

В настоящее время активно развиваются системы, автоматизирующие процесс учета потребляемых ресурсов, таких как вода, газ, электроэнергия и т.д. Такие системы называются автоматизированными системами коммерческого учета энергоресурсов (АСКУЭ). Структурная схема АСКУЭ представлена на рис. 5.

Рис. 5. Структурная схема АСКУЭ

Центральный сервер обрабатывает всю информацию, поступающую от устройств учета (УУ). Устройства сбора и передачи данных (УСПД) являются посредниками между УУ и центральным сервером. В задачи УСПД входит опрос счетчиков и контроль их работоспособности.

Изначально АСКУЭ разрабатывались для использования на предприятиях, но с развитием технологий стали внедряться и в сферу ЖКУ. Использование промышленных АСКУЭ в жилых домах связано с рядом проблем. Необходимо обеспечить связь между компонентами системы, также необходимо противодействовать несанкционированному доступу к системе, например несанкционированной замене УУ и другим угрозам [58].

Существующие устройства, входящие в состав АСКУЭ, не имеют надежных механизмов защиты, так как предназначены для использования на промышленных объектах и служат для контроля использования ресурсов, а не для их коммерческого учета.

Для обеспечения надежной аутентификации устройств в АСКУЭ предложено решение, основанное на рекомендациях ITU-T G.9903 02.2014. В качестве протокола аутентификации используется протокол EAP-PSK, работающий поверх протокола EAP, возможности которого были расширены для работы в сетях с гетерогенными каналами связи [59].

Во время прохождения процедуры аутентификации устройства получают ключи шифрования для обмена данными с остальными участниками сети (при условии, что аутентификация пройдена успешно). В качестве алгоритма шифрования используется AES-CCM, который является связкой двух алгоритмов:

– AES-CTR – потоковый режим шифрования AES;

– AES-CBC – алгоритм подсчета кода аутентификации сообщения.

Такой подход позволяет контролировать устройства, подключаемые к АСКУЭ, а также обеспечить контроль целостности и аутентичность данных, получаемых УСПД от УУ.

Однако в силу того, что решение предназначено для сетей с гетерогенными каналами связи, его использование не всегда целесообразно. Если есть возможность подключения всех устройств АСКУЭ по одному каналу связи, то использование протоколов, рассчитанных на сети с гетерогенными каналами, приведет к лишним нагрузкам на оборудование и генерации паразитного трафика.

Для снижения нагрузки на оборудование и уменьшения объема паразитного трафика в сети предложено решение, основанное на протоколе IPsec. Данное решение целесообразно, так как все устройства в АСКУЭ поддерживают протокол 6loWPAN (стандарт взаимодействия по протоколу IPv6 поверх маломощных беспроводных персональных сетей).

Протокол IPsec, портированный на устройства в составе АСКУЭ, обеспечивает взаимную аутентификацию устройств в сети с использованием протокола IKEv2. При этом возможны варианты работы, при которых сеть настраивается по протоколу EAP-PSK. Во время настройки устройства получают сетевые адреса и ключи аутентификации, после чего EAP-PSK завершает работу, и передача данных происходит по протоколу IPsec. Второй вариант работы – использование предустановленных на устройства сертификатов. В таком случае первичная настройка проводится вручную, но сети не требуется использование протокола EAP-PSK.

Контроль целостности и шифрование данных при их передаче обеспечиваются протоколом ESP, который используется в IPsec на транспортном уровне. Данный протокол обеспечивает защиту не только передаваемых данных, но и заголовков пакетов сетевого уровня.

Данный подход позволяет обеспечить надежную аутентификацию устройств в АСКУЭ, обеспечить защиту передаваемых данных и предоставляет большое количество опций для настройки режима работы сети, но не применим для сетей с гетерогенными каналами связи. Подход, основанный на EAP-

PSK, не столь гибок, но применим для сетей с гетерогенными каналами связи.

Заключение

В данной статье представлен обзор нескольких основных из десятков существующих направлений научных исследований в области информационной безопасности, развиваемых в Томском государственном университете систем управления и радиоэлектроники в научной школе профессора А.А. Шелупанова.

Комплексный подход к проведению научных исследований, практикуемый в Институте системной интеграции и безопасности, и необходимость параллельно решать производственные задачи позволяет органично развивать фундаментальные и прикладные направления работ. Результаты прикладных разработок стабильно внедряются в практическую деятельность организаций, использующих новые методики и технологии защиты информации, в различных секторах экономики по всей России.

Актуальность представленных научных результатов подтверждается востребованностью публикаций коллектива в высокоуровневых отечественных и зарубежных журналах.

Одним из факторов поступательного развития научных направлений является широкое вовлечение студентов в исследовательские проекты и проекты по внедрению средств защиты информации на реальных объектах. Так, например, созданы и успешно работают группы проектного обучения по проведению компьютерных экспертиз, по автоматическому определению авторства сообщений в сети Интернет, по разработке программного комплекса для проведения соревнований в области информационной безопасности и т.п. В интересах индустриальных партнеров – ведущих разработчиков средств защиты информации – действуют проекты по разработке защищенного мессенджера и исследованиям в области определения сетевых атак в реальном времени.

Главным приоритетом развития заявленных направлений в ближайшие годы будет являться более тесное взаимодействие с индустриальными партнерами и приближение достижений фундаментальных исследований к практической реализации в целях повышения обороноспособности страны при защите от киберугроз.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУРа на 2017–2019 гг. (проект № 2.8172.2017/8.9).

Литература

1. 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.

2. 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.

3. Криптографические протоколы в системах с ограниченными ресурсами / Р.В. Мещеряков, С.К. Росошек, А.А. Шелупанов, М.А. Сонькин // Вычислительные технологии. – 2007. – Т. 12, № S1. – С. 51–61.

4. 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.

5. 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.

6. Мещеряков Р.В. Концептуальные вопросы информационной безопасности региона и подготовки кадров / Р.В. Мещеряков, А.А. Шелупанов // Труды СПИИРАН. – 2014. – № 3(34). – С. 136–159.

7. Смолина А.Р. Классификация методик производства компьютерно-технической экспертизы с помощью подхода теории графов / А.Р. Смолина, А.А. Шелупанов // Безопасность информационных технологий. – 2016. – № 2. – С. 73–77.

8. Смолина А.Р. Методика проведения подготовительной стадии исследования при производстве компьютерно-технической экспертизы / А.Р. Смолина, А.А. Шелупанов // Доклады ТУСУРа. – 2016. – Т. 19, № 1. – С. 31–34.

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. 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.

11. 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.

12. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Н.Т. Югов // Доклады ТУСУРа. – 2011. – № 2(24), ч. 3. – С. 206–210.

13. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1(31). – С. 28–35.

14. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях их возникновения / В.Г. Миронова, А.А. Шелупанов // Изв. ЮФУ. Технические науки. – 2012. – № 12(137). – С. 39–45.

15. Мещеряков Р.В. Специальные вопросы информационной безопасности / Р.В. Мещеряков, А.А. Шелупанов. – Томск: Изд-во Института оптики атмосферы СО РАН, 2003. – 224 с.

16. Зайцев А.П. Технические средства и методы защиты информации / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2012. – 442 с.

17. Конев А.А. Подход к описанию структуры системы защиты информации / А.А. Конев, Е.М. Давыдова // Доклады ТУСУРа. – 2013. – № 2(28). – С. 107–111.

18. Конев А.А. Подход к построению модели угроз защищаемой информации // Доклады ТУСУРа. – 2012. – № 1(25), ч. 2. – С. 34–39.

19. Novokhrestov A. Mathematical model of threats to information systems / A. Novokhrestov, A. Konev // AIP Conference Proceedings. – 2016. – Vol. 1772(1). – P. 060015-1–060015-4.

20. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам: учеб. пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др.; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – 2-е изд., стереотип. – М.: Горячая линия – Телеком, 2012. – 550 с.

21. Безмалый В. Парольная защита: прошлое, настоящее, будущее // КомпьютерПресс. – 2008. – № 9. – С. 37–45.

22. Попов М. Биометрические системы безопасности [Электронный ресурс]. – Режим доступа: http://www.bre.ru/security/12571.html, свободный (дата обращения: 30.06.2017).

23. Ross A. A deformable model for fingerprint matching / A. Ross, S. Dass, A.K. Jain // Journal of Pattern Recognition. – 2005. – Vol. 38, № 1. – P. 95–103.

24. Matsumoto T. Impact of artificial gummy fingers on fingerprint systems / T. Matsumoto, H. Hoshino, K. Yamada, S. Hasino // Proceedings of SPIE. – 2002. – Vol. 4677. – P. 275–289.

25. Jain A.K. Biometric: A Tool for Information Security / A.K. Jain, A. Ross, S. Pankanti // IEEE Transactions on Information Forensics and Security. – 2006. – Vol. 1, № 2. – P. 125–144.

26. Kukula E. Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance / E. Kukula, S. Elliott // Proceedings of 35th Annual International Carnahan Conference on Security Technology. – London, 2001. – P. 83–88.

27. Kumar A. Personal Verification using Palmprint and Hand Geometry Biometric / A. Kumar, D.C. Wong, H.C. Shen, A.K. Jain // Proceedings of 4th International Conference on Audio- and Video-based Biometric Person Authentication. – Guildford, 2003. – P. 668–678.

28. Колесник А.В. Распределенная система распознавания лиц на основе геометрических характеристик / А.В. Колесник, Ю.В. Ладыженский [Электронный ресурс]. – Режим доступа: http://masters.donntu.org/2010/fknt/kolesnik/library/tez1.htm, свободный (дата обращения: 29.12.2015).

29. Ganorkar S.R. Iris Recognition: An Emerging Biometric Technology / S.R. Ganorkar, A.A. Ghatol // Proceedings of the 6th WSEAS International Conference on Signal Processing, Robotics and Automation. – Elounda, 2007. – P. 91–96.

30. Marino C. Personal authentication using digital retinal images / C. Marino, M.G. Penedo, M. Penas, M.J. Carreira, F. Gonzalez // Journal of Pattern Analysis and Application. – 2006. – Vol. 9, № 1. – P. 21–33.

31. Favata J.T. Handprinted character/digit recognition using a multiple feature/resolution philosophy / J.T. Favata, G. Srikantan, S.N. Srihari // Proceedings of IWFHR-1994. – 1994. – P. 57–66.

32. Дорошенко Т.Ю. Система аутентификации на основе динамики рукописной подписи / Т.Ю. Дорошенко, К.Ю. Костюченко // Доклады ТУСУРа. – 2014. – № 2(32). – С. 219–223.

33. Рахманенко И.А. Исследование формант и мелкепстральных коэффициентов в качестве вектора признаков для задачи идентификации по голосу // Матер. XI Междунар. науч.-практ. конф. «Электронные средства и системы управления». – Томск: ТУСУР, 2015. – С. 188–192.

34. Banerjee S.P. Biometric Authentication and Identification Using Keystroke Dynamics: A Survey / S.P. Banerjee, D.L. Woodard // Journal of Pattern Recognition Research. – 2012. – Vol. 7, № 1. – P. 116–139.

35. Широчин В.П. Динамическая аутентификация на основе анализа клавиатурного почерка / В.П. Широчин, А.В. Кулик, В.В. Марченко // Вестник Нац. техн. ун-та Украины «Информатика, управление и вычислительная техника». – 1999. – № 32. – С. 1–16.

36. 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.

37. Горбунов И.В. Алгоритмы и программные средства идентификации Парето-оптимальных нечетких систем на основе метаэвристических методов: дис. … канд. техн. наук: 05.13.18. – Томск, 2014. – 192 с.

38. Костюченко Е.Ю. Показатели качества систем распознавания пользователей по динамике подписи на основе наивного классификатора Байеса и нейронной сети / Е.Ю. Костюченко, М.А. Гураков, Е.О. Кривоносов // Труды МАИ. – 2016. – № 2(86). – С. 1–15.

39. Gurakov M.A. Integration of Bayesian classifier and perceptron for problem identification on dynamics signature using a genetic algorithm for the identification threshold selection / M.A. Gurakov, E.O. Krivonosov, M.D. Tomyshevet al. // Lecture Notes in Computer Science. – 2016. – Vol. 9719. – P. 620–627.

40. Rivest R. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems / R. Rivest, A. Shamir, L. Adleman // Communications of the ACM. – 1978. – Vol. 21, № 2. – P. 120–126.

41. Балабанов А.А. Алгоритм быстрой генерации ключей в криптографической системе RSA / А.А. Балабанов, А.Ф. Агафонов, В.А. Рыку // Вестник научно-технического развития. – 2009. – № 7(23). – С. 11–17.

42. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МНЦМО, 2003. – 326 с.

43. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. – М.: МНЦМО, 2002. – 104 с.

44. Ribenboim P. The little book of bigger primes. – New York: Springer-Verlag, 2004. – 356 p.

45. Кручинин Д.В. Метод построения алгоритмов проверки простоты натуральных чисел для защиты информации / Д.В. Кручинин, В.В. Кручинин // Доклады ТУСУРа. – 2011. – № 2(24). – С. 247–251.

46. Шабля Ю.В. Генератор критериев простоты натурального числа / Ю.В. Шабля, Д.В. Кручинин, А.А. Шелупанов // Доклады ТУСУРа. – 2015. – № 4(38). – С. 97–101.

47. Мельман В.С. Методы анализа тестов простоты числа / В.С. Мельман, Ю.В. Шабля, Д.В. Кручинин // Матер. XII Междунар. науч.-практ. конф. «Электронные средства и системы управления». – Томск: ТУСУР, 2016. – С. 54–55.

48. Кручинин Д.В. Программное обеспечение для анализа тестов простоты натурального числа / Д.В. Кручинин, Ю.В. Шабля // Доклады ТУСУРа. – 2014. – № 4(34). – С. 95–99.

49. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. – Cambridge: Cambridge University Press, 2010. – 437 p.

50. Salomon D. Data compression: the complete reference, 4th Edition. – London: Springer-Verlag, 2007. – 1111 p.

51. Евсютин О.О. Модификация стеганографического метода LSB, основанная на использовании блочных клеточных автоматов // Информатика и системы управления. – 2014. – № 1(39). – С. 15–22.

52. Евсютин О.О. Исследование дискретных ортогональных преобразований, получаемых с помощью динамики клеточных автоматов // Компьютерная оптика. – 2014. – Т. 38, № 2. – С. 314–321.

53. 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.

54. Евсютин О.О. Алгоритмы встраивания информации в цифровые изображения с применением интерполяции / О.О. Евсютин, А.С. Кокурина, Р.В. Мещеряков // Доклады ТУСУРа. – 2015. – № 1(35). – С. 108–112.

55. An Adaptive algorithm for the steganographic embedding information into the discrete Fourier transform phase spectrum / O.O. Evsutin, A.S. Kokurina, R.V. Mescheryakov, O.O. Shumskaya // Advances in Intelligent Systems and Computing. – 2016. – Vol. 451. – P. 47–56.

56. Улучшенный алгоритм встраивания информации в сжатые цифровые изображения на основе метода PM1 / О.О. Евсютин, А.С. Кокурина, А.А. Шелупанов, И.И. Шепелев // Компьютерная оптика. – 2015. – Т. 39, № 4. – С. 572–581.

57. Алгоритм встраивания информации в сжатые цифровые изображения на основе операции замены с применением оптимизации / О.О. Евсютин, А.А. Шелупанов, Р.В. Мещеряков, Д.О. Бондаренко // Компьютерная оптика. – 2017. – Т. 41, № 3. – С. 412–421.

58. Модель угроз безопасности автоматизированной системы коммерческого учета энергоресурсов / А.К. Новохрестов, Д.С. Никифоров, А.А. Конев, А.А. Шелупанов // Доклады ТУСУРа. – 2016. – Т. 19, № 3. – С. 111–114.

59. Организация защищенной гетерогенной сети в автоматизированных системах коммерческого учета энергоресурсов / М.М. Антонов, А.А. Конев, Д.С. Никифоров, С.А. Черепанов // Доклады ТУСУРа. – 2016. – Т. 19, № 3. – С. 107–110.

Шелупанов Александр Александрович
Д-р техн. наук, ректор ТУСУРа, зав. каф.
комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: +7 (382-2) 70-15-29
Эл. почта: saa@tusur.ru

Евсютин Олег Олегович
Канд. техн. наук, доцент каф. безопасности
информационных систем (БИС) ТУСУРа
Тел.: +7 (382-2) 70-15-29
Эл. почта: eoo@keva.tusur.ru

Конев Антон Александрович
Канд. техн. наук, доцент каф. КИБЭВС
Тел.: +7 (382-2) 70-15-29
Эл. почта: kaa1@keva.tusur.ru

Костюченко Евгений Юрьевич
Канд. техн. наук, доцент каф. КИБЭВС
Тел.: +7 (382-2) 70-15-29
Эл. почта: key@keva.tusur.ru

Кручинин Дмитрий Владимирович
Канд. физ.-мат. наук, научный сотрудник каф. КИБЭВС
Тел.: +7 (382-2) 70-15-29
Эл. почта: kdv@keva.tusur.ru

Никифоров Дмитрий Сергеевич
Аспирант каф. КИБЭВС
Тел.: +7 (382-2) 70-15-29
Эл. почта: nds@csp.tusur.ru

Shelupanov A.A., Evsutin O.O., Konev A.A.,
Kostychenko E.Yu., Kruchinin D.V., Nikiforov D.S.

Modern trends in development of methods and means for information protection

In this article authors present the results related to the various aspects of fundamental or applied scientific research and the implementation of production tasks that are made by the research team of TUSUR Institute of System Integration and Security. An integrated approach to the information security is considered in detail that allowed to conduct research on the development of methods for assessing the security of information systems. The article contains the main achievements of the scientific group, related to fundamental research and program implementations that aimed to improve the quality of the following mechanisms of security: biometric user authentication; encryption; secure transmission and authentication of digital objects; identification of the elements' authenticity in automated process control systems, and development of secure communication channels for the information transfer.

Keywords: model of information security system, threat model, biometric authentication, neural networks, encryption, primes, authenticity of digital objects, steganography, automated systems of control, secure channels of communication.