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 X.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.