8. *Шарай В.А., Андриуца М.В., Финько О.А.* Мониторинг состояния надежности безопасности структурно-сложных систем на основе логико-числовых моделей // Труды Международной научно-практической конференции «Передовые информационные технологии, средства и системы автоматизации и их внедрение на российских предприятиях» АІТА-2011. – М.: Институт проблем управления им. В.А. Трапезникова РАН, 2011. – С. 601- 612.

Статью рекомендовал к опубликованию д.т.н., профессор О.А. Финько.

Шарай Вячеслав Александрович:
Кубанский государственный технологический университет.
E-mail: wsharay@gmail.com.
350072, г. Краснодар, ул. Московская, 2А.
Тел.: +79298244416.
Аспирант.

Бурангулова Ольга Сергеевна
E-mail: superleka@rambler.ru.
Тел.: +79186702809.
Аспирантка.

Андриуца Максим Васильевич
ООО «Краснодаррегионгаз».
E-mail: alggaz@kubanol.ru.
353475, г. Геленджик, ул. Грибоедова, 60 А.
Тел.: 89886029541.
Начальник участка.

Sharaj Vyacheslav Aleksandrovich
Kuban State Technological University.
E-mail: wsharay@gmail.com.
2A, Moscow Street, Krasnodar, 350072, Russia.
Phone: +79298244416.
Postgraduate Student.

Burangulova Olga Sergeevna
E-mail: superleka@rambler.ru.
Phone: +79186702809.
Postgraduate Student.

Andriutsa Maxim Vasilevich
Open Company "Krasnodarregiongaz".
E-mail: alggaz@kubanol.ru.
60 A, Griboedov's Street, Gelendzhik, 353475, Russia.
Phone: +79886029541.
Chief of a Site.

УДК 004.056; 004.8

М.И. Тенетко, О.Ю. Пескова

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рассматриваются различные методы анализа рисков информационной безопасности, выделяются их особенности и недостатки. Сделан вывод, что наиболее эффективными из рассмотренных являются качественные методы. Предложен метод анализа рисков информационной безопасности на основе нечётких предикатов и нечёткого логического вывода,

позволяющего классифицировать риски и получать наилучшие рекомендации по рискам с помощью категорий естественного языка и с учётом оттенков категорий. Приведены результаты исследования возможных нечётких импликаций, обладающих свойством настройки оттенка заключения в зависимости от изменения оттенка посылки и пригодных для решения задач классификации рисков и выработки наилучших рекомендаций по рискам.

Управление информационной безопасностью; управление рисками; анализ рисков; нечеткая логика.

M.I. Tenetko, O.Yu. Peskova

RISK ANALYSIS OF INFORMATION SECURITY

In article various methods of the analysis of risks of information security are considered, their features and lacks are allocated. It is concluded that most effective are qualitative methods. We propose a method of information security risk assessment which allows to evaluate information security risks via fuzzy deduction, to classify information security risks, and to get optimal recommendations on risks treatment considering natural language entities and shades of meanings of entities. Results of investigation of possible fuzzy implication are suitable for the decision of problems of classification of risks and development of the best recommendations about risks are proposed.

Information security management; risk management; fuzzy deduction.

Процесс анализа рисков информационной безопасности. Сущность любого подхода к управлению рисками заключается в анализе факторов риска и принятии адекватных решений по обработке рисков. Факторы риска – это те основные параметры, которыми оперируют при оценке рисков [1]:

- Актив (Asset).
- Ущерб (Loss).
- Угроза (Threat).
- Уязвимость (Vulnerability).
- Мехнизм контроля (Control).
- Размер среднегодовых потерь (ALE).
- Возврат инвестиций (ROI).

Способы анализа и оценки этих параметров определяются используемой в организации методологией оценки рисков.

Процесс анализа рисков информационной безопасности в целом состоит из трёх этапов:

1. Подготовка к проведению анализа рисков информационной безопасности.
2. Анализ сценариев возможных инцидентов информационной безопасности.
3. Определение степени риска информационной безопасности и подбор рекомендаций по управлению рисками информационной безопасности.

На первом этапе эксперт собирает данные об информационной системе. Основные шаги первого этапа анализа информационных рисков показаны на рис. 1.

На втором этапе эксперт составляет сценарии возможных инцидентов информационной безопасности и анализирует их. Основные шаги второго этапа анализа рисков информационной безопасности показаны на рис. 2.

Количественные методы анализа рисков информационной безопасности. При использовании методов количественного анализа риска вычисляются числовые значения величин отдельных рисков и риска объекта в целом, выявляется возможный ущерб и дается стоимостная оценка от проявления риска. Результатом должна стать система мероприятий по снижению рисков и расчет их стоимостного эквивалента.

Количественный анализ можно формализовать, для чего используется инструментарий теории вероятностей, математической статистики, теории исследования операций.

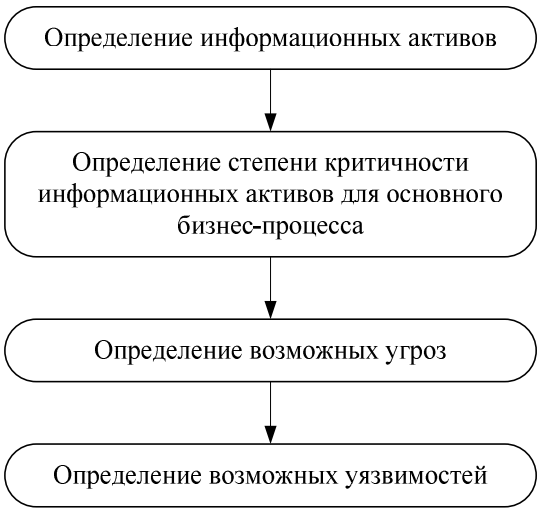

Рис. 1. Подготовка к проведению анализа рисков информационной безопасности

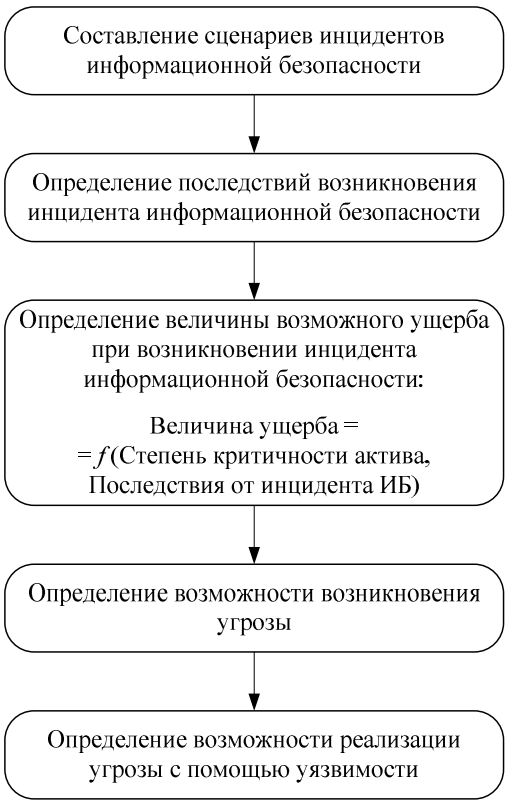

Рис. 2. Анализ сценариев возможных инцидентов информационной безопасности

Табличный метод анализа рисков. Одним из наиболее распространенных количественных методов анализа рисков является табличный метод. Этот метод опирается на таблицу, определяющую схему связей между угрозами, уязвимостями и ресурсами [2, 3]. Количественные показатели информационных ресурсов, как правило, оцениваются с помощью опроса сотрудников компании – владельцев информации, которые могут определить ценность информации, её характеристики и степень критичности, исходя из фактического положения дел. По результатам опроса производится оценивание показателей и степени критичности информационных ресурсов для наихудшего варианта развития событий, рассматриваются потенциальные воздействия на деятельность компании при возможном несанкционированном ознакомлении с конфиденциальной информацией, нарушении её целостности и доступности. В случаях, когда количественные оценки по ряду причин затруднены, допускается использование качественных оценок. Количественные и качественные показатели оцениваются при помощи фиксированных балльных шкал. К примеру, для количественных показателей возможна шкала от 1 до 10, для качественных показателей возможна шкала «высокий – низкий». Достаточно часто процесс получения количественных и качественных показателей дополняется методиками оценки других критичных показателей, учитывающих, например, требования по соблюдению законодательства, коммерческие и общественные отношения и т.д.

Анализ иерархий. Применение другого метода – анализа иерархий – сводит исследование практически любых сложных систем к последовательности попарных сравнений компонент данных систем [4]. Иерархические структуры, которые используются в области информационной безопасности, могут относиться к различным классам иерархий, например физические иерархии (временные, пространственные, должностные и т.д.), специализированные иерархии (программные, аппаратно-технические, прав доступа и т.д.), исследовательские (структур данных, критериев, объектов и т.д.). Модель должна включать в себя и позволять измерять все важные количественные и качественные факторы. Однако метод работает лишь в том случае, когда практически все эти факторы измерены объективно и в полном объёме, значения показателей непротиворечивы, результаты задач принятия решений однозначны и соответствуют мнению эксперта. Иначе можно ожидать появления систематических и случайных ошибок в оценках [5].

Метод анализа рисков информационной безопасности на основе экспертных оценок. Данный метод представляет собой комплекс логических и математико-статистических методов и процедур по обработке результатов опроса группы экспертов в области информационной безопасности, причем результаты опроса являются основным источником информации. В основе метода лежит идея декомпозиции сложной и плохо поддающейся формализации задачи на последовательность более простых подзадач, соответствующих определённому числу элементарных экспертиз. Оценка параметров входит в число наиболее распространённых элементарных экспертиз. Как правило, под оценкой нечисловой информации понимается приписывание нечисловым характеристикам количественных или качественных значений по выбранной шкале измерений.

В общем случае оценка заключается в назначении вероятностей совершения событий, реализации угрозы, дат событий или весов. Определение весовых коэффициентов рисков используется для их упорядочения и определения первоочередных действий по защите. Затем для определения степени безопасности системы на основании уже определённых параметров используется линейный метод взвешивания и подсчёта [3, 6].

Метод анализа рисков информационной безопасности на основе оценки ожидаемых потерь и возврата от инвестиций. Этот метод был предложен Национальным Бюро Стандартов США в федеральном стандарте FIPS 65 “Guideline for Automatic Data Processing Risk Analysis” [7].

В соответствии с ним, оценка ожидаемого возможного ущерба от единичной реализации определённой угрозы (Single Loss Exposure, SLE) рассчитывается по формуле

$$SLE = AV \times EF, \quad (1)$$

где AV – стоимость ресурса (Asset Value); величина в фиксированном диапазоне, характеризующая ценность ресурса;

EF – мера уязвимости ресурса к угрозе; величина в фиксированном диапазоне, характеризующая степень уязвимости ресурса к данной угрозе.

Оценка годовых ожидаемых потерь (ALE, Annual Loss Expectancy) рассчитывается по формуле

$$ALE = SLE \times ARO, \quad (2)$$

где ARO – оценка вероятности реализации угрозы (Annual Rate of Occurrence); величина в фиксированном диапазоне, характеризующая насколько вероятна реализация данной угрозы в течение определённого периода времени[1].

Оценка возврата от инвестиций в информационную безопасность (ROSI, Return on Security Investment) рассчитывается по формуле

$$ROSI = ALE - CCC, \quad (3)$$

где CCC – инвестиции в СЗИ, защищающие от данной угрозы. В случае, если величина ROSI является положительной (или, по крайней мере, неотрицательной), можно говорить о том, что инвестиции в СЗИ оправданы [8].

Недостатки количественных методов анализа рисков информационной безопасности. Количественные методы анализа рисков информационной безопасности обладают серьёзными недостатками.

Существуют составляющие риска, которые никак не учитываются в количественных методах анализа рисков [9]:

- убыток в результате простоя бизнес-процесса;
- затраты на создание информации;
- приобретение активов;
- восстановительная стоимость;
- будущая стоимость;
- оплата сверхурочного труда работников;
- судебные издержки и некоторые другие составляющие.

Можно допустить существование математического метода, представляющего эти составляющие в виде некоторых численных показателей. Однако для этого необходимо проанализировать большое количество разнородных параметров состояния бизнеса. Исчерпывающее и актуальное количественное описание состояния бизнеса в этом случае получить вряд ли возможно, поскольку за время, необходимое для его получения, обстановка внутри и вне бизнеса может значительно измениться. Даже в случае получения такого описания оно может представлять собой огромный объём информации, требующий большого количества времени для обработки и осознания.

Кроме того, есть составляющие риска, принципиально не поддающиеся подсчёту [10, 11, 13]:

- репутация компании или организации;
- престиж и ценность торговой марки;
- нанесённый моральный ущерб;
- влияние риска на сотрудников;

[1] В данном примере указана величина за год (“annual”), но вполне допускается использование другого, более подходящего к ситуации периода времени.

- влияние риска на акционеров или владельцев бизнеса;
- влияние риска на потребителей;
- влияние риска на поставщиков и партнёров;
- влияние риска на агентства кредитных рейтингов и прочие финансовые структуры.

В частности, если реализация угрозы повлияет на моральное состояние сотрудников, последствия могут выразиться в потере производительности, уходе высококвалифицированных сотрудников и сдерживании притока новых сотрудников, производственным конфликтам.

Реализация угрозы может заставить акционеров или владельцев бизнеса задуматься о том, что бизнес не соответствует ожиданиям, и перевести инвестиции в другой бизнес.

Реализация угрозы может вызвать потерю доверия и отток потребителей, которые будут обеспокоены плохой репутацией бизнеса и неспособностью бизнеса защитить персональные данные потребителей.

Агентства кредитных рейтингов могут снизить показатели кредитоспособности пострадавшего от угрозы бизнеса, а поставщики товаров – сократить объёмы поставок, что впоследствии помешает пострадавшему бизнесу привлечь новые инвестиции и восстановить своё положение на рынке.

Как видно, неполучение прибыли от удара по престижу и снижения репутации может в некоторых случаях существенно превысить затраты на создание системы информационной безопасности.

Анализ рисков информационной безопасности, основанный на аудите информационной безопасности. Количественный анализ рисков информационной безопасности может быть совмещён с аудитом на соответствие политики информационной безопасности рекомендациям, отражающим наиболее успешную практику управления информационной безопасностью. Эти рекомендации изложены в специально разработанных международных и национальных стандартах:

- ISO/IEC FDIS 17799:2005 и основанный на нём ГОСТ Р ИСО/МЭК 17799-2005 [12, 13];
- стандарты Банка России СТО БР ИББС–1.0–2008, СТО БР ИББС–1.1–2007 и СТО БР ИББС–1.2–2009 [14-16];
- стандарт безопасности данных индустрии платёжных систем (PCI DSS) [17];
- прочие национальные и правительственные стандарты.

Стандарты управления информационной безопасностью содержат лишь рекомендации (или требования) по применению определённых мер защиты преимущественно технических. Стандарты предназначены прежде всего для формальной сертификации информационной системы и системы управления информационной безопасностью. Применение стандартов для анализа рисков информационной безопасности основывается на следующем допущении: можно утверждать, что риски информационной безопасности отсутствуют, если информационная система сертифицирована на соответствие требованиям стандарта.

При этом требования стандартов не учитывают целого ряда составляющих информационного риска, перечисленных в предыдущем подразделе. Более того, формальное соответствие требованиям стандарта и успешное прохождение сертификации вовсе не означает наличия действующей и эффективной системы управления информационной безопасностью.

Подтверждением тому может служить утечка данных в платёжной системе Heartland Payment Systems, Inc., обнаруженная в январе 2009 г. и повлёкшая за собой компрометацию миллионов транзакций по банковским картам. В результате

утечки злоумышленникам стали известны номера банковских карт, даты окончания действия карт и имена владельцев карт. Этой информации достаточно для создания поддельных банковских карт и совершения нелегитимных транзакций от имени легитимных владельцев карт [18, 19].

Компания Heartland прошла сертификацию на соответствие требованиям стандарта безопасности данных индустрии платёжных систем PCI DSS. Сертификация была выполнена компанией Trustwave, квалифицированным оценщиком безопасности[2], надёжность которого не вызывает сомнений. Причины утечки данных в Heartland не разглашаются, но подчёркивается, что они не связаны с невыполнением требований стандарта PCI DSS [18].

С учётом этого факта случай с Heartland создаёт опасный прецедент, ставящий под сомнение результативность формальной сертификации на соответствие требованиям стандартов управления информационной безопасностью.

Качественный анализ рисков информационной безопасности. Альтернативой рассмотренным методам является качественный метод анализа рисков информационной безопасности – это процесс оценивания рисков, основанный на сценариях инцидентов информационной безопасности и определении влияния инцидента на активы (рассматривается, в частности, [9, 10, 11, 20]).

При проведении качественного анализа рисков эксперт составляет краткое описание сценариев возможных инцидентов информационной безопасности, которые затем разрабатываются и исследуются для поиска областей деятельности и активов организации, которые могут быть затронуты инцидентом, и для определения рамок ущерба, нанесённого всем возможным областям деятельности и активам. Вместо численной интерпретации понятия риска, свойственной количественным методам анализа рисков, выполняется классификация рисков информационной безопасности в соответствии с затрагиваемыми областями деятельности и активами.

Основываясь на сведениях о внешней среде бизнеса, эксперт в области информационной безопасности определяет возможные инциденты информационной безопасности в виде сценариев. Раскрывая сценарий и изменяя переменные сценария, влияющие на события, эксперт идентифицирует области деятельности и активы бизнеса, потенциально затронутые инцидентом и определяет воздействие на эту область или актив в виде категории естественного языка: «воздействие выше среднего», «ущерб неприемлем», «низкий ущерб» и т.п.

Основное достоинство этих категорий заключается в том, что они не требуют дополнительной интерпретации и интуитивно понятны как специалисту в области информационной безопасности, так и неспециалистам, заинтересованным в построении системы безопасности (акционерам, совету директоров и т.п.). Эксперт интуитивно, исходя из сценария рисковой ситуации и своего профессионального опыта, понимает, какая категория естественного языка наилучшим образом описывает тот или иной параметр сценария рисковой ситуации.

Кроме того, эксперт может образовывать более сложные категории с помощью определённых синтаксических правил, например, «не очень высокая возможность возникновения угрозы», «степень риска ближе к высокой, чем к средней», «данная рекомендация по риску скорее уместна, чем нет». Сложные категории либо содержат некоторый оттенок, видоизменение смысла исходной категории, либо являются объединением или пересечением двух и более исходных категорий. Сложные категории применяются в тех случаях, когда тот или иной параметр сценария рисковой ситуации невозможно однозначно отнести к одной из исходных категорий.

[2] Qualified Security Assessor, QSA.

Без использования сложных категорий анализ риска сводится к выявлению линейной зависимости оценок риска и уместности рекомендаций по риску от показателей ценности ресурса, величины ущерба, возможности угроз и уязвимостей. Категории, описывающие степень риска и уместности рекомендаций по риску, в этом случае определяются простой суммой баллов, полученных за определённые значения параметров рисковых ситуаций, а шкала, состоящая из категорий естественного языка, при этом ничем не отличается от шкалы с численными значениями.

Кроме того, эксперт может образовывать более сложные категории с помощью определённых синтаксических правил, например, «не очень высокая возможность возникновения угрозы», «степень риска ближе к высокой, чем к средней», «данная рекомендация по риску скорее уместна, чем нет». Сложные категории либо содержат некоторый оттенок, видоизменение смысла исходной категории, либо являются объединением или пересечением двух и более исходных категорий. Сложные категории применяются в тех случаях, когда тот или иной параметр сценария рисковой ситуации невозможно однозначно отнести к одной из исходных категорий.

Без использования сложных категорий анализ риска сводится к выявлению линейной зависимости оценок риска и уместности рекомендаций по риску от показателей ценности ресурса, величины ущерба, возможности угроз и уязвимостей. Категории, описывающие степень риска и уместности рекомендаций по риску, в этом случае определяются простой суммой баллов, полученных за определённые значения параметров рисковых ситуаций, а шкала, состоящая из категорий естественного языка, при этом ничем не отличается от шкалы, имеющей от трёх до пяти численных значений.

В настоящее время не существует метода анализа рисков информационной безопасности, позволяющего оценивать степень риска и уместность рекомендации по данному риску с помощью категорий естественного языка и оттенков категорий, который мог бы лечь в основу системы поддержки принятия решений при управлении рисками информационной безопасности. Такой метод может быть основан на нечёткой логике и нечётких множествах, в частности, на основе нечётких предикатов и нечёткого логического вывода, позволяющего классифицировать риски и получать наилучшие рекомендации по рискам с помощью категорий естественного языка и с учётом оттенков категорий.

Было проведено исследование возможных нечётких импликаций, обладающих свойством настройки оттенка заключения в зависимости от изменения оттенка посылки и пригодных для решения задач классификации рисков и выработки наилучших рекомендаций по рискам, а также исследование их возможностей. Анализ результатов экспериментов показал следующее.

Наиболее удобные для интерпретации заключения получены с помощью импликаций Gaines and Rescher, Gödel, Goguen (при всех композициях), а также с помощью почти всех импликаций при композициях Max-Bounded и Max-Drastic. Заключения, отражающие любые изменения посылок, можно получить при помощи импликации Goguen при композициях Max-Min и Max-Prod. Все импликации дают вывод «неизвестно», если оказываются не в состоянии определить правильный вывод (иными словами, если наблюдение является отрицанием или дополнением посылки нечёткого правила). Импликация Goguen обладает свойством настройки оттенка заключения в зависимости от изменения оттенка посылки. Для решения задач классификации рисков и выработки наилучших рекомендаций по рискам выбрана нечёткая импликация Goguen.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Астахов А.* CISA, 2006. Как управлять рисками информационной безопасности? [Электронный ресурс]. – Режим доступа: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/kak-upravlyat-riskami-informacionnoi-bezopasnosti, свободный. – Загл. с экрана. – Яз. Рус.
2. ISO/IEC FDIS 27005:2008. Information technology. Security techniques. Information security risk management. – Geneva: ISO, 2008. – 55 p.
3. *Саати Т.* Принятие решений. Метод анализа иерархий / Томас Саати: Пер. с англ. Р. Вачнадзе. – М.: Радио и связь, 1993. – 320 с. – Перевод изд.: The analytic hierarchy process: planning setting priorities, resource allocation / Thomas L. Saaty. New York, 1980.
4. *Харитонов Е.В.* Согласование исходной субъективной информации в методах анализа иерархий // Математическая морфология. –1999. – Т. 3. – Вып. 2. – С. 41-51.
5. *Петренко С.А., Петренко А.А.* Аудит безопасности Intranet.– М.: ДМК Пресс, 2002. – 416 с.
6. *Корченко А.Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения – К.: МК-Пресс, 2006.
7. Federal Information Processing Standards Publication 65. Guideline for Automatic Data Processing Risk Analysis. – Washington, DC: U.S. General Printing Office, 1979. – 56 p.
8. *Endorf C.F.* Measuring ROI on security / Carl F. Endorf // Information security management handbook / Edited by Harold F. Tipton and Micki Krauze. – 6th edition. – Boca Raton: Auerbach Publications, 2007. – Part 1, Section 1.1, Ch. 12. – P. 133-137.
9. *Henry K.* Risk management and analysis / Kevin Henry // Information Security Management Handbook / Edited by Harold F. Tipton, Micki Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2007. – Part 1, Section 1.4, Ch. 28. – P. 321-329.
10. *Rittinghouse J.W.* Business continuity and disaster recovery for infosec managers / John W. Rittinghouse, James F. Ransome. – Oxford: Elsevier, 2005. – 408 p.
11. *Spedding L.* Business risk management handbook: a sustainable approach / Linda Spedding, Adam Rose. – Oxford: Elsevier, 2008. – 768 p.
12. ISO/IEC FDIS 17799:2005. Information technology. Security techniques. Code of practice for information security management. – Geneva: ISO, 2005. – 115 p.
13. ГОСТ Р ИСО/МЭК 17799–2005. Информационная технология. Практические правила управления информационной безопасностью. – Введ. 2006–01–01. – М.: Стандартинформ, 2006. – 61 с.
14. СТО БР ИББС–1.0–2008. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения [Электронный ресурс]. – Введ. 2009–05–01. – М.: Банк России, 2008. – Режим доступа: http://www.cbr.ru/credit/Gubzi_docs/st10-08.pdf, свободный. – Загл. с экрана. – Яз. рус.
15. СТО БР ИББС–1.1–2007. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности [Электронный ресурс]. – Введ. 2007–05–01. – М.: Банк России, 2007. – Режим доступа: http://www.cbr.ru/credit/Gubzi_docs/st11.pdf, свободный. – Загл. с экрана. – Яз. рус.
16. СТО БР ИББС–1.2–2009. Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации. Требованиям СТО БР ИББС–1.0–2008 [Электронный ресурс]. – Введ. 2009–06–01. – М.: Банк России, 2009. – Режим доступа: http://abiss.ru/upload/iblock/749/sto_br_ibbs-1.2-2009.pdf, свободный. – Загл. с экрана. – Яз. рус.
17. Payment Card Industry (PCI) Data Security Standard . Requirements and Security Assessment Procedures. Version 1.2. [Электронный ресурс]. – Effective date October 1 2008. – Wakefield, MA: PCI Security Standards Council, 2008. – 73 p. – Режим доступа: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml, свободный. – Загл. с экр. – Яз. англ.
18. *Ragan S.* Does the Heartland breach prove PCI useless? [Электронный ресурс] / Steve Ragan // The Tech Herald. – 2009. – January, 26. – Режим доступа: http://www.thetechherald.com/article.php/200905/2849/Does-the-Heartland-breach-prove-PCI-useless, свободный.
19. Events unfold after Heartland breach // Computer Fraud & Security. – 2009. – Vol. 2. – P. 2, 20.
20. *Landoll D.* The security risk assessment handbook: a complete guide for performing security risk assessments / Douglas J. Landoll. – Boca Raton: Auerbach Publications, 2006. – 504 p.

Статью рекомендовал к опубликованию к.т.н. Г.В. Карайчев.

Тенетко Михаил Иванович
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: tenetko@gmail.com.
347928, г. Таганрог, пер. Некрасовский, 44.
Тел.: 88622535982.
Независимый специалист.

Пескова Ольга Юрьевна
E-mail: poy@tsure.ru.
Тел.: 88634371905.
К.т.н.; доцент.

Tenetko Mikhail Ivanovich
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: tenetko@gmail.com.
44, Nekrasovskiy, Taganrog, 347928, Russia.
Phone: +78622535982.
Independent Specialist.

Peskova Olga Yur’evna
E-mail: poy@tsure.ru.
Phone: +78634371905.
Cand. of Eng. Sc.; Associate Professor.

УДК 004.056.5, 004.89

А.М. Цыбулин

АРХИТЕКТУРА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

Количество атак на информационные системы предприятий неуклонно растет. В связи с этим возрастают количество анализируемых событий безопасности, разнообразие механизмов защиты, а также вероятности ошибок при конфигурировании аппаратного, программного обеспечения и анализе инцидентов безопасности. Целью исследования является разработка архитектуры автоматизированной системы управления информационной безопасностью предприятия. Использование автоматизированной системы управления позволяет разрешить указанные проблемы за счет решения следующих задач: автоматизация централизованного и децентрализованного мониторинга и аудита управления информационной безопасностью, синтез оптимального решения по повышению уровня информационной безопасности для предприятия.

Атака, интеллектуальный агент; многоагентная система; информационная безопасность; управление информационной безопасностью; мониторинг; аудит; катастрофоустойчивость; информационная система.

A.M. Tsybulin

AUTOMATED INFORMATION SECURITY MANAGEMENT SYSTEM OF ENTERPRISE ARCHITECTURE

The total amount of attacks on enterprise’s information system more and more increases. Therefore analyzed security events, security incidents, the variety of security mechanisms and also error’s probability during hardware’s and software’s configuration are increased too. The main