Использование фундаментальных положений алгебры логики, теории вероятностей, а также известных работ [1, 9, 10], делает удобным *алгоритм 2* для вычисления вероятности перехода в опасное состояние систем, описываемых как полностью определенными, так и неполностью определенными ФОС. Применение способов реализации ЧНФ позволяет получить преимущества при автоматизации процессов вычисления вероятности перехода исследуемых СЗИ в опасное состояние.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Рябинин И.А.* Надежность и безопасность структурно-сложных систем: Монография. – СПб.: Политехника, 2000. – 248 с.
2. *Яблонский, С.В.* Введение в дискретную математику: Учеб. пособие для вузов. – 2-е изд., перераб. и доп.: Монография. – М.: Наука. гл. ред. физ.-мат. лит., 1986. – 348 с.
3. *Логачёв О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. – М.: МЦНМО, 2004. – 470 с.
4. *Малюгин В.Д.* Применение алгебры кортежей логических функций // X Всесоюзное совещание по проблемам управления: Тез. докл. Кн. 1. – М.: Ин-т проблем управления, 1986.
5. *Финько О.А.* Модулярная арифметика параллельных логических вычислений: Монография / Под ред. В.Д. Малюгина. – М.: ИПУ РАН, 2003. – 224 с.
6. *Соколовский Е.П., Малашихин А.К., Финько О.А.* Применение числовой нормальной формы представления булевых функций в логико-вероятностном методе И.А. Рябинина // Материалы XIII Международной научно-практической конференции «Информационная безопасность», г. Таганрог, 9-13 июля 2013 г. Ч. II. – С. 113-118.
7. *Пухальский Г.И., Новосельцева Т.Я.* Цифровые устройства: Учебное пособие для втузов. – СПб.: Политехника, 1996. – 885 с.
8. *Вентцель, Е.С.* Теория вероятностей: Монография. – М., 1969. – 576 с.
9. *Черкесов, Г.Н., Можаев А.С.* Логико-вероятностные методы расчета надежности структурно-сложных систем. Качество и надежность изделий. – М.: Знание, 1991. – 340 с.
10. *Соложенцев, Е.Д.* Сценарное логико-вероятностное управление риском в бизнесе и технике: Монография. – СПб.: Изд. дом «Бизнес-пресса», 2004. – 432 с.

Статью рекомендовал к опубликованию д.т.н. В.Н. Марков.

Финько Олег Анатольевич – Филиал Военной академии связи (г. Краснодар). e-mail: ofinko@yandex.ru; 350063, г. Краснодар, ул. Красина, 4; тел.: +79615874848; профессор.

Соколовский Евгений Петрович – e-mail: Biryza_08@mail.ru; тел.: +79181744325; адъюнкт.

Finko Oleg Anatolievich – Branch of the Military Academy of Communications (Krasnodar); e-mail: ofinko@yandex.ru; 4, Krasina, Krasnodar, 350063, Russia; phone: +79615874848; professor.

Sokolovsky Evgeniy Petrovich – e-mail: Biryza_08 @mail.ru; phone: +79181744325; adjunct.

УДК 004.42

Е.Н. Тищенко, Е.Ю. Шкаранда

АЛГОРИТМИЗАЦИЯ ПРОЦЕССА ФОРМИРОВАНИЯ ЧАСТНОЙ МОДЕЛИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассматриваются подходы к алгоритмизации процесса формирования частной модели угроз безопасности персональных данных организаций и предприятий. Предложены решения для определения состава угроз, уязвимостей и последствий реализации угроз. Для этого использованы экспертные, вероятностные методы и формализованные процедуры анализа предметной области. Рассмотрены основные блоки алгоритма формирования модели угроз, описаны особенности каждого из блоков. Показано, что предложенные подходы и методы решают проблему формализации решаемой задачи, позволяют унифицировать и автоматизировать

процесс формирования модели угроз. При этом предложенный алгоритм может быть использован для реализации программной системы формирования модели угроз и предназначен для того, чтобы облегчить работу специалистов, занимающихся обеспечением информационной безопасности, и в частности, защитой персональных данных. Рассмотренная структура алгоритма может быть использована как универсальный шаблон, который применим для защиты информационных систем предприятий любого рода деятельности.

Модель угроз; уязвимость; персональные данные; информационная безопасность; защита данных.

E.N. Tishchenko, E.Yu. Shkaranda

ALGORITHMIZATION OF THE FORMATION OF INDIVIDUAL SECURITY THREAT MODEL OF PERSONALLY IDENTIFIABLE INFORMATION

The article discusses approaches to algorithmization of the formation of individual security threat model of personally identifiable information of companies and businesses. The solutions for the determination of threats, vulnerabilities, and consequences of threats carried out are proposed. To do this the authors used the expertise, probabilistic methods and formalized procedures of subject area analysis. The basic blocks of the algorithm of the formation of the threat model are considered, the features of each of the blocks are described. It is shown that the proposed approaches and methods solve the problem of formalization of the goal, unify and automate the process of formation of the threat model. In this case, the proposed algorithm can be used to implement a software system of formation threat model and is designed to facilitate the work of professionals engaged in information security, and in particular the protection of personally identifiable information. Considered structure of the algorithm can be regarded as a universal pattern, which is applicable for the protection of corporate information systems of any type of business.

Threat model; vulnerability; personally identifiable information; information security; data protection.

Постановка задачи. Реальные положительные достижения в деле эффективного обеспечения защиты информации может дать только построение комплексной системы. Её результативность зависит, прежде всего, от степени осознания рисков и угроз, которым подвергаются или могут подвергаться информационные активы компании. С этой целью разрабатывается модель угроз нарушения информационной безопасности.

Под моделью угроз понимается абстрактное (формализованное или неформализованное) описание основных (актуальных) угроз безопасности, которые должны учитываться в процессе организации защиты информации, проектирования и разработки системы защиты информации, проведения проверок (контроля) защищенности системы защиты информации.

При формировании перечня угроз необходимо учитывать назначение, условия и особенности функционирования информационной системы. Модели угроз могут разрабатываться для защиты различных видов конфиденциальной информации, информации, относящейся к государственной тайне, для построения системы физической защиты и т.п. В связи с ростом практики правоприменения законодательства в области персональных данных, специалисты по защите информации всё чаще сталкиваются с задачей разработки модели нарушителя и угроз безопасности персональных данных. Создание модели угроз – зачастую довольно трудоёмкий процесс, требующий большого числа затрат. Следовательно, актуальным становится алгоритмизация такого процесса, проектирование и разработка программного продукта, учитывающего совокупность условий и факторов, создающих опасность для информационных активов.

Модель угроз безопасности персональных данных разрабатывается на основе следующих нормативно-правовых документов:

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная 15 февраля 2008 года заместителем директора ФСТЭК России;
- «Методика определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных», утвержденной 14 февраля 2008 года заместителем директора ФСТЭК России;
- ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на информацию. Общие положения».

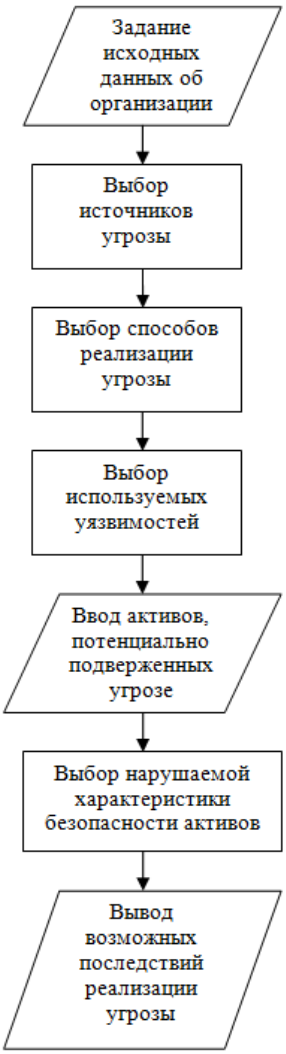

Рис. 1. Блочная структура одного цикла программной системы формирования модели угроз

Решение задачи. Для составления алгоритма модели угроз необходимо использовать следующие параметры:

- Аннотацию угрозы;
- Возможные источники угрозы;
- Способ реализации угрозы;
- Используемые уязвимости;
- Вид активов, потенциально подверженных угрозе;
- Нарушаемые характеристики безопасности активов;
- Возможные последствия реализации угроз.

Функционирование программной системы формирования модели угроз можно рассмотреть на примере блочной структуры (рис. 1).

Рассмотрим подробнее каждый блок.

Задание исходных данных об организации. Первый блок подразумевает ввод данных, по которым специалист, разрабатывающий модель, может идентифицировать организацию, а именно её полное название, юридический адрес и т.п. Также вводятся технические характеристики информационной системы персональных данных, на основании которых экспертным методом проводится оценка уровня исходной защищенности информационной системы персональных данных. Подробно проведение оценки описано в методике, разработанной ФСТЭК России.

Выбор источников угрозы. Под источниками угрозы будем понимать возможные носители угрозы информационной безопасности. Они могут быть вызваны:

- «человеческим фактором»;
- техническими средствами;
- непредвиденными обстоятельствами, такими как пожар, землетрясение и т.д.

Если у рассматриваемой угрозы антропогенный источник, формируется модель нарушителя безопасности персональных данных. В первую очередь необходимо указать, является нарушитель

внешним или внутренним по отношению к организации и информационной системе. Затем из предложенных характеристик и возможностей нарушителя выбрать необходимые.

При указании второго источника угрозы предусмотрен выбор технического канала утечки информации.

Непредвиденные обстоятельства (стихийные бедствия) практически невозможно спрогнозировать, но для каждого из вероятных необходим комплекс защитных мероприятий.

Выбор способов реализации угрозы. Для каждой указанной ранее угрозы указывается способ её реализации. Так, например, для угрозы целостности персональных данных способом реализации может выступать использование вредоносного программного обеспечения, а для угрозы утечки информации по каналам побочных электромагнитных излучений и наводок – осуществление доступа к информационной системе с использованием аппаратных средств съема информации (рис. 2).

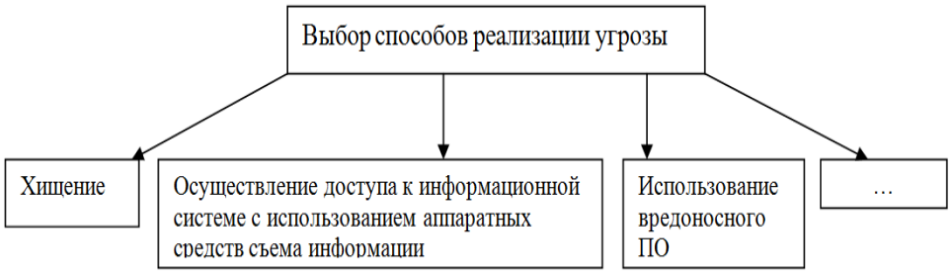

Рис. 2. Пример содержания блока «Выбор способов реализации угрозы»

В процессе проведенных исследований был сформирован перечень угроз, отличающийся полнотой и универсальностью по отношению к конкретной реализации информационной системы.

Данный перечень является частью формализованного представления модели угроз. В процессе его формирования определяются ключевые угрозы, формируются из них группы, ранжируются группы по степени важности, что позволяет оценивать модель угроз по одному из основных показателей – критерию полноты. Данный критерий определяется путем сравнения сформированной модели с полным перечнем угроз.

При этом рассчитывается показатель полного поглощения моделью возможных угроз [1, 2]:

$$H_{ej} = \frac{P_{ej}^{(11)}}{P_{ej}^{(11)} + P_{ej}^{(10)}}, \quad (1)$$

где $P_{ik}^{(11)}$ – число угроз, входящих, как в формируемую модель, так и в полный перечень; $P_{ik}^{(10)}$ – число гроз, входящих в полный перечень, но не входящих в формируемую модель.

Выбор используемых уязвимостей. По аналогии с третьим блоком, на основании уже перечня уязвимостей, выбираем соответствующую уязвимость. Таким образом, для способа реализации «хищение» уязвимостью могут являться недостатки механизмов охраны.

В свою очередь, перечень уязвимостей может быть определен методом тестирования информационной системы. При этом информационная система обработки персональных данных имеет определенные особенности [3]:

- отсутствие заранее заданного эталона, с которым сопоставляются результаты тестирования;
- значительная сложность составляющих системы и, поэтому, невозможность разработки исчерпывающего тестирующего алгоритма;
- сложность формализации показателей качества процесса тестирования и качества тестируемых объектов;
- присутствие логических и вычислительных составляющих, которые характеризуются динамической структурой.

В литературных источниках, рассматриваемых данную проблему, приведены математические модели построения системы обработки персональных данных, которые могут быть приняты как абстрактные эталоны. Однако в конкретных условиях многие показатели неоднозначны.

Рассматриваемые системы, как правило, функционируют в условиях, когда факторы, возникающие в процессе работы, практически не формализуются. В связи с этим практически невозможно реализовать их полное тестирование, гарантирующее исчерпывающую проверку. Поэтому тестирование необходимо проводить в объемах, ограниченно необходимых, в определенных заранее заданных интервалах модификации факторов и условий функционирования. Поэтому появляется необходимость скрупулезного отбора моделей тестирования и контролируемых параметров.

Показатели качества систем обработки персональных данных весьма трудно формализуются и измеряются. В связи с этим анализ результатов тестирования в значительной степени носит относительно субъективный характер. О глубине тестирования можно говорить только после продолжительной их эксплуатации в конкретных условиях.

В большинстве систем имеются компоненты, представляющие собой изменяющиеся структуры, вырабатывающие логические решения, зависящие от случайной модификации входных данных и конкретных условий функционирования. В связи с этим практически невозможно выработать универсальный тест и приходится использовать различные методы тестирования, которые различаются конечными задачами, контролируемыми компонентами и подходами к оценке.

Последовательность тестирования включает:

- формализованное описание алгоритма тестирования;
- тестирование системы с ее реальным функционированием и разными уровнями детализации;
- выявление проблемных мест и условий их проявления.

Для формализованного описания алгоритма тестирования нужно выработать правила формализации. Эти правила необходимо четко сформулировать, и их количество не должно быть большим. Систему обработки персональных данных можно рассматривать как совокупность относительно независимых модулей, реализующих конкретные функции и обладающих замкнутой структурой. Как правило, они характеризуются независимым режимом работы. В связи с этим тестирование нужно проводить с учетом не менее, чем трех уровней:

- оценка каждого отдельного модуля для обнаружения расхождений между результатами работы, а также интерфейса с основными правилами;
- одновременное тестирование взаимозависящих модулей с целью обнаружения несоответствий между результатами работы этих модулей и общими определенными правилами;

- системное тестирование с целью обнаружения несоответствий между системой и ее целями.

На каждом уровне необходимо провести три вида тестирования:

- тестирование в реальном масштабе времени;
- случайное тестирование;
- детерменированное тестирование.

В случае детерменированного тестирования необходимо проверить каждую комбинацию вероятных действий и взаимозависящую с ей комбинацию результатов работы. При таком подходе возможно выявление отклонений результатов работы от первоначально заданных с учетом сочетаний типа: входящий сигнал – отклик системы.

В связи с тем, что достаточно сложно перебрать каждые возможные варианты происходящих событий, становится возможным применение случайного тестирования.

Расширение числа событий может возникнуть при использовании тестирования в реальном масштабе времени. Такого тестирование проверяет работу с учетом процесса изменения объемов оперативной памяти, параметров вычислительной системы и т.д.

Анализ структуры реализуемых системой обработки персональных данных функций показывает, что вполне возможно моделирование вариантов их реализации с определением вероятности наличия уязвимости и ее несанкционированного использования за заданное время [4].

Алгоритм обнаружения и использования уязвимости системы может рассматриваться как последовательность элементарных операций с определением временных параметров их реализации. При имитационном моделировании с применением стандартных программных средств установлен факт того, что закон распределения всего времени реализации обнаружения и использования уязвимости является нормальным и, следовательно, корректно применить вероятностную функцию Лапласа.

При этом расчет вероятности осуществляется по формуле:

$$P_{t \le T} = 0,5 + \Phi_0\left(\frac{T - M_t}{t}\right), \qquad (2)$$

где $\Phi_0(z)$ – функция Лапласа; P(t) – вероятность обнаружения и использования уязвимости за время T; M_t, D_t – математическое ожидание и дисперсия.

Ввод активов, потенциально подверженных угрозе. Специалист по защите информации вводит в программу перечень информационных активов, которых коснется конкретная угроза.

Выбор нарушаемой характеристики безопасности активов. Характеристиками безопасности информации являются:

- конфиденциальность;
- целостность;
- доступность.

Вывод возможных последствий реализации угрозы. Каждая реализованная угроза влечет за собой определённые последствия. Важно понимать, какие именно. Ими могут стать, к примеру, нарушение режима функционирования информационной системы, несанкционированное ознакомление и разглашение персональных данных, финансовый ущерб организации.

При этом, для определения состава возможных последствий угрозы вполне корректным является применение экспертных методов [5, 6].

Пусть W_i – весовой коэффициент значимости последствия угрозы F_i, присвоенный экспертом. Пусть G_i – степень возможности последствия. При этом, $0 \le G_i \le 1$ и $W_i > 0$ для $1 \le i \le n$.

В такой постановке можно применить линейный метод для надежности системы защиты персональных данных SR (s), оцениваемой экспертом r. Надежность может быть определена по формуле:

$$SR(s,r) = \frac{1}{n} \sum_{i=1}^{n} W_i G_i \cdot \quad (3)$$

Алгоритм процесса формирования частной модели нарушителя и угроз безопасности персональных данных должен строиться с учетом определённых принципов. Вводимые исходные данные об организациях сохраняются в базу данных для упрощения дальнейшей работы. Позиции, предполагающие выбор, должны содержать данные, в первую очередь основанные на руководящих документах ФСТЭК России и ФСБ. Также должна быть предусмотрена возможность ввода специалистом в области информационной безопасности, работающим с программой, дополнительных данных. По окончанию работы одного цикла программы на основе полученной информации о защищаемом объекте должен формироваться список возможных последствий реализации угрозы. После формирования первой угрозы, программа должна возвращаться на этап выбора источников угрозы. В итоге формируется перечень всех прогнозируемых угроз нарушения безопасности персональных данных объекта.

Выводы. Предложенный алгоритм может быть положен в основу программной системы формирования модели угроз и призван облегчить работу специалистов, занимающихся защитой персональных данных. Описанная структура является универсальным шаблоном, который можно применять для защиты информационных систем предприятий любого рода деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Хубаев Г.Н.* Экономика проектирования и применения банков данных: Текст лекций. – Ростов-на-Дону: РИСХМ, 1989. – 69 с.
2. *Тищенко Е.Н., Степанов Д.П.* Определение эффективности распределенных межсетевых экранов в зависимости от функциональной полноты // Экономические науки. – 2008. – № 41. – С. 151-156.
3. *Шураков В.В.* Надежность программного обеспечения систем обработки данных: Учебник. – 2-е изд., перераб. и доп. – М.: Финансы и статистика, 1987. – 272 с.
4. *Тищенко Е.Н., Строкачева О.А.* Модель аудита информационной безопасности систем электронной коммерции // Научная мысль Кавказа. – 2006. – № 14. – С. 134-141.
5. *Тищенко Е.Н., Строкачева О.А.* Оценка параметров надежности защищенной платежной системы в электронной коммерции // Вестник РГЭУ (РИНХ). – 2006. – № 22. – С. 115-122.
6. *Тищенко Е.Н.* Инструментальные методы защищенности распределенных экономических информационных систем: дис. …д-ра. экон. наук. – Росто-на-Дону, 2003.

Статью рекомендовал к опубликованию д.т.н., профессор С.В. Соколов.

Тищенко Евгений Николаевич – Ростовский государственный экономический университет (РИНХ); e-mail: brann@mail.ru; 344007, г. Ростов-на-Дону, ул. Б. Садовая, 69; тел.: +78632402123; кафедра информационных технологий и защиты информации; зав. кафедрой; д.э.н.; доцент.

Шкаранда Екатерина Юрьевна – e-mail: ekaterinashkaranda@yandex.ru; 344016, г. Ростов-на-Дону, ул. Горшкова 9/1, кв. 34; тел.: +79289882829; кафедры информационных технологий и защиты информации; аспирантка.

Tishchenko Evgeniy Nikolayevich – Rostov State Economic University; e-mail: brann@mail.ru; 69, B. Sadovaya Street, Rostov-on-Don, 344007, Russia; phone: +78632402123; the department information technologies and information security; head of department; dr of ec. sc.; associate professor.

Shkaranda Ekaterina Yurievna – e-mail: ekaterinashkaranda@yandex.ru; apt. 34, 9/1 Gorshkova street, Rostov-on-Don, 344016, Russia; phone: +79289882829; the department information technologies and information security; postgraduate student.

УДК004.056

В.С. Аткина

МОДЕЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Цель исследования: разработкамодели оценки защищенности информации в организациях банковской системы Российской Федерации. В рамках данного исследования решены следующие задачи: рассмотрена проблема обеспечения информационной безопасности организаций банковской системы Российской Федерации. Проанализированы требования регуляторов к уровню защищенности информации в организациях, принадлежащих банковской системе. Определены цели, задачи и этапы обеспечения информационной безопасности в банковской сфере. Проанализирована модель автоматизированной банковской информационной системы, на основании которой выделены уровни иерархииинформационной инфраструктуры, ключевые бизнес-процессы, элементы структуры и виды связей между ними. Предложена и формально описана модель оценки защищенности информации в организациях банковской системы Российской Федерации. Сделан вывод о возможности автоматизации предложенного подхода к оценке защищенности и использовании его в качестве программного обеспечения автоматизированного рабочего места специалиста по защите информации.

Банковская система; угроза; информационная безопасность; риск; оценка защищенности.

V.S. Atkina

MODEL ASSESSMENT OF THE BANKING SYSTEM PROTECTION ORGANIZATIONS OF THE RUSSIAN FEDERATION

The purpose of the study is development the model of evaluation information security in organizations of the banking system of the Russian Federation. The present study addressed the following tasks: the problem of information security organizations of the banking system of the Russian Federation was discussed. Analyze the requirements of regulators to the level of information security in organizations of the banking system. Were defined goals, objectives and stage to ensure information security in the banking sector.The author analyzed the model of the automated banking information system , the analysis were identified levels of the hierarchy of the information infrastructure , business processes , the structure and types of connections between them. Proposed and formally described model estimation of information security in the organization of the banking system of the Russian Federation. It is concluded that the possibility of automating the proposed approach to security assessment and its use as a software workstation specialist in information security.

Banking system; threats; information security; risk; assessment of security.

В настоящее время одной из значительных и активно развивающихся отраслей экономики Российской Федерации (РФ) является банковская деятельность. Одной из составляющих успешного развития которой является обеспечение информационной безопасности (ИБ). И это связано не только с задачами обеспече-