применению методов защиты информации, принимая во внимание все возможные факторы, такие как: величина угроз, стоимость внедрения и обеспечения технической поддержки, а так же производительность системы и возможный ущерб.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Васильев С.В., Силкин А.Т., Тикменова И.В., Уткин А.В.* Организация противодействия техническим средствам разведки в автоматизированных системах управления с элементами радиочастотной идентификации // Научно-методические материалы исследований, труды семинаров и научно-технических конференций 3 ЦНИИ МО РФ. Книга 12. – М.: 3ЦНИИ МО РФ, 2008. – С. 38-41.
2. *Агафьин С. С.* LW-криптография: шифры для RFID-систем // Безопасность информационных технологий. – 2011. – № 1. – С. 30-33.
3. *Sanjay E. Sarma, Stephen A. Weis, Daniel W.* Engels RFID Systems and Security and Privacy Implications, Auto-ID Center, Massachusetts Institute of Technology, Cambridge, MA 02139 // B.S. Kaliski Jr. et al. (Eds.): CHES 2002, LNCS 2523. – 2003. – P. 454-469.
4. *Maricel O.* Balitanas and Taihoon Kim Review: Security Threats for RFID-Sensor Network Anti-Collision Protocol // International Journal of Smart Home. – 2010. – Vol. 4, № 1, January. – P. 23-36.
5. *Liang Y., Rong C.,* Strengthen RFID Tags Security Using New Data Structure // International Journal of Control and Automation. – 2008. – Vol. 1, № 1. – P. 51-58.

Статью рекомендовал к опубликованию к.т.н. С.К. Самогин.

Михеев Вячеслав Алексеевич – ОАО "ИМЦ Концерна "Вега"; e-mail: mikheev@imc-vega.ru; 125190, г. Москва, ул. Балтийская, 14; тел.: 84957874381, доб. 200; генеральный директор; к.т.н.

Уткин Андрей Владимирович – e-mail: a.utkin@rfidcenter.ru; тел.: 84957874381, доб. 295; начальник отдела радиочастотной идентификации; аспирант.

Виноградов Дмитрий Алексеевич – e-mail: d.vinogradov@rfidcenter.ru; тел.: 84957874381, доб. 318; начальник сектора разработки программного обеспечения.

Mikheev Vyacheslav Alekseevich – JSC "IMC of "Vega" Corporation"; e-mail: mikheev@imc-vega.ru; 14, Baltiyskaya street, Moscow, 25190, Russia; phone: +74957874381, ext. 200; director general; cand. of eng. sc.

Utkin Andrey Vladimirovich – e-mail: a.utkin@rfidcenter.ru; phone: +74957874381, ext. 295; pead of bepartment of radio frequency identification.

Vinogradov Dmitry Alekseevich – e-mail: d.vinogradov@rfidcenter.ru; phone: +74957874381, ext. 318; head of sector of software engineering.

УДК 004.056.5

В.Г. Миронова, А.А. Шелупанов

МЕТОДОЛОГИЯ ФОРМИРОВАНИЯ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В НЕОПРЕДЕЛЕННЫХ УСЛОВИЯХ ИХ ВОЗНИКНОВЕНИЯ*

В настоящее время организации используют электронный документооборот, при котором конфиденциальная информация циркулирует – хранится и обрабатывается в информационных системах. Информационные системы подвергаются всевозможным уг-

* Работа выполнена в соответствии с Госзаданием Министерства образования и науки проекты: № 7.701.2011; № 1/12.

розам, порождая угрозы безопасности государству, обществу и личности. В связи с этим необходимо обеспечить защиту конфиденциальной информации. В работе представлена методология формирования полного перечня угроз безопасности конфиденциальной информации (УБКИ), которая является основополагающей при создании модели УБКИ. Выявление полного перечня актуальных угроз позволяет создать модель угроз для построения надежной и эффективной системы защиты информации (СЗИ).

Угрозы; безопасность; информационная система; конфиденциальная информация.

V.G. Mironova, A.A. Shelupanov

METHODOLOGY OF FORMATION OF THREATS OF SAFETY OF CONFIDENTIAL INFORMATION IN UNCERTAIN CONDITIONS OF THEIR EMERGENCE

Currently, organizations use electronic document in which the confidential information circulates - is stored and processed in information systems. Information systems are all possible threats, causing security threats to the state, society and the individual. In this connection it is necessary to ensure the protection of confidential information. The paper presents the methodology for the a complete full list of threats to the security of confidential information (UBKI) which is fundamental to create the model UBKI. Identification of the full list of actual threats to create threats model for a reliable and effective information security system (SZI).

Threats; safety; information system; confidential information.

В настоящее время деятельность современного предприятия невозможно представить без использования средств вычислительной техники (СВТ), поскольку электронный документооборот позволяет снизить как временные, так и финансовые затраты, а также значительно упростить обработку и хранение информации, которая циркулирует в ходе существования предприятия.

Электронный документооборот организован с использованием информационных систем (ИС), в которых хранится и обрабатывается конфиденциальной информации (КИ). Потеря или несанкционированное использование такой информации может привести к финансовым и репутационным рискам предприятия или физического лица. Поэтому обеспечение безопасности информации в ИС обработки КИ является важным фактором успешного функционирования экономических структур.

Безопасность информации обеспечивается путем построения системы защиты конфиденциальной информации (СЗКИ). Существует три основных этапа построения СЗКИ:

- предпроектное обследование ИС (аудит информационной безопасности (ИБ));
- проектирование СЗКИ;
- внедрение СЗКИ [1].

Первым этапом при построении СЗКИ является предпроектное обследование. Целью предпроектного исследование является получение ответов на ряд вопросов о функционировании ИС, технологии обработки и хранения КИ, об уязвимостях и угрозах безопасности информации. Ответы на эти вопросы позволяют четко сформулировать требования к СЗКИ, поэтому тщательное проведение предпроектного обследования ИС является не только важным, но и необходимым.

В ходе проведения предпроектного обследования:

- устанавливается необходимость обработки (обсуждения) КИ в ИС и организации в целом;
- анализируется перечень сведений конфиденциального характера, подлежащих защите от утечки по техническим каналам;

- определяются угрозы безопасности информации, строится модель угроз безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования;
- выявляются условия расположения объектов информатизации относительно границ контролируемой зоны (КЗ);
- определяются конфигурация и топология ИС в целом и их отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- анализируются технические средства (ТС) и системы, используемые или предполагаемые к использованию в ИС, условия их расположения, общесистемные и прикладные программные средства;
- определяются режимы обработки информации в ИС в целом и в отдельных компонентах;
- определяется класс защищенности [2];
- выявляется степень участия персонала в обработке (обсуждении, передаче, хранении) информации;
- формулируются требования к мероприятиям по обеспечению КИ в процессе проектирования СЗКИ [2].

Основной задачей, решаемой на этапе проведения предпроектного обследования, является определение угроз безопасности информации, построение модели угроз безопасности информации и модели вероятного нарушителя применительно к конкретным условиям функционирования ИС.

Идентификация угроз проводится с целью установления из всех возможных угроз безопасности КИ (УБКИ) тех, которые актуальны для данной ИС в процессах ее создания и функционирования. Полный перечень угроз безопасности информации используется для создания модели угроз безопасности ИС.

Составление полного перечня УБКИ и их проявлений проведем на основе анализа взаимодействия логической цепочки, представленной на рис. 1.

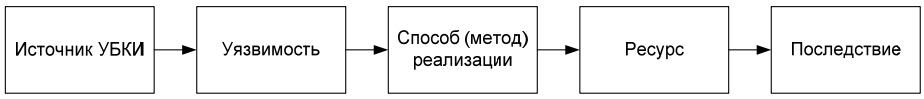

Рис. 1. Цепочка возникновения УБКИ

Понятия источника УБКИ, уязвимости, последствий приведены в [3].

Представим лишь частичное описание основных составляющих логической цепочки.

Для представления УБКИ нами использован подход применения элементов теории графов – ориентированные графы. Полный перечень УБКИ имеет вид

$$Y(A,B),$$

где $\mathbf{A} = \{a_c, a_{1,1}, a_{1,2}, \ldots, a_{i,j}, a_d\}$ – множество вершин графа **Y**; **B** – множество дуг графа **Y** – упорядоченных пар вершин $a \in \mathbf{A}$, вершина a_c – начало графа, вершина a_d – конец графа.

Вершины графа являются характеристиками УБКИ, которые разделены на уровни по критериям классификации, где i – количество критериев классификации УБКИ, j – количество признаков конкретного критерия.

Для определения множества $\mathbf{A^*} = \{a_{1,1}, a_{1,2}, \ldots, a_{i,j}\}$, $\mathbf{A^*} \in \mathbf{A}$ свойств УБКИ необходимо выявить их основные составляющие, табл. 1.

Таблица 1

Основные составляющие логической цепочки

№ п/п	Наименование	Обозначение
1.	Источник угрозы	a_1
1.1	Природные источники угроз	$a_{1,1}$
1.1.1	пожары	$a_{1,1,1}$
1.1.2	землятресения	$a_{1,1,2}$
1.1.3	наводнения	$a_{1,1,3}$
1.2	Антропогенные источники угроз (нарушители)	$a_{1,2}$
1.2.1	внешние (нарушитель ИБ территориально расположен за пределами КЗ)	$a_{1,2,1}$
1.2.2	внутренние	$a_{1,2,2}$
1.2.2.1	нарушитель ИБ (лицо, имеющее санкционированный доступ к ИС, но не имеющее доступ к КИ)	$a_{1,2,2,1}$
1.2.2.2	нарушитель ИБ (зарегистрированный пользователь ИС, осуществляющий ограниченный доступ к ресурсам ИС с рабочего места)	$a_{1,2,2,2}$
1.2.2.3	нарушитель ИБ (зарегистрированный пользователь ИС, осуществляющий удаленный доступ к КИ по локальным и (или) распределенным ИС)	$a_{1,2,2,3}$
1.2.2.4	нарушитель ИБ (зарегистрированный пользователь ИС с полномочиями администратора безопасности сегмента (фрагмента) ИС)	$a_{1,2,2,4}$
1.2.2.5	нарушитель ИБ (зарегистрированный пользователь с полномочиями системного администратора ИС)	$a_{1,2,2,5}$
1.2.2.6	нарушитель ИБ (зарегистрированный пользователь с полномочиями администратора безопасности ИС)	$a_{1,2,2,6}$
1.2.2.7	нарушитель ИБ (программист-разработчик (поставщик) прикладного программного обеспечения и лицо, обеспечивающее его сопровождение на защищаемом объекте)	$a_{1,2,2,7}$
1.2.2.8	нарушитель ИБ (разработчик и лицо, обеспечивающее поставку, сопровождение и ремонт ТС для ИС)	$a_{1,2,2,8}$
1.3	техногенные источники угроз	$a_{1,3}$
1.3.1	средства и линии связи	$a_{1,3,1}$
1.3.2	средства инженерных коммуникаций	$a_{1,3,2}$
1.3.3	технические средства обработки информации	$a_{1,3,3}$
1.3.3.1	некачественные технические средства обработки КИ	$a_{1,3,3,1}$
1.3.3.2	аппаратные закладки	$a_{1,3,3,2}$
1.3.4	программные средства обработки КИ	$a_{1,3,4}$
1.3.4.1	некачественное программное обеспечение	$a_{1,3,4,1}$
1.3.4.2	программные закладки	$a_{1,3,4,2}$
1.3.4.3	программно-аппаратные закладки	$a_{1,3,4,3}$
1.3.4.4	программные вирусы	$a_{1,3,4,4}$
1.3.4.5	вредоносные программы, распространяющиеся по сети (черви)	$a_{1,3,4,5}$
2.	Уязвимость	a_2
2.1	ошибки в программах, приводящие к их сбою, аварийному останову, неправильному режиму работы, «зависанию»	$a_{2,1}$

2.2	закладки и недекларированные возможности программных средств ИС, позволяющие обойти СЗКИ	$a_{2,2}$
2.3	некорректная (ошибочная) схемная и/или микропрограммная (программная) реализация аппаратных, программно-аппаратных средств, используемых в ИС, приводящая к их сбою, отказу	$a_{2,3}$
2.4	другие	$a_{2,4}$
3	Способ (метод) реализации	a_3
3.1	потеря, несанкционированное копирование, кража и вынос из КЗ документов допущенными к ним лицами	$a_{3,1}$
3.2	поиск и копирование документов об ИС и СЗКИ, оставленных без присмотра, посторонними лицами	$a_{3,2}$
3.3	поиск компьютеров ИС с оставленным без присмотра активным сеансом или создание условий для их возникновения	$a_{3,3}$
3.4	подбор пароля	$a_{3,4}$
3.5	другие	$a_{3,5}$
4	Ресурсы (активы)	a_4
4.1	информация (вводимая в систему, содержащаяся в БД, выводимая из системы), подпадающая под действие перечня сведений, подлежащих засекречиванию, иная информации с ограниченным доступом (служебная тайна, персональные данные) и другая чувствительная информация, воздействие на которую может привести к нарушению безопасности информации (к нарушению целостности и/или доступности)	$a_{4,1}$
4.2	ТС (аппаратные и программно-аппаратные средства, накопители и носители информации, линии связи), содержащие КИ, указанную в п.п 1.5.2, или обеспечивающие её передачу	$a_{4,2}$
4.3	программные средства (общесистемные, прикладные), обрабатывающие КИ, указанную в п.п 1.5.2	$a_{4,3}$
4.4	другие	$a_{4,4}$
5	Последствия	a_5
5.1	нарушение конфиденциальности	$a_{5,1}$
5.2	нарушение целостности	$a_{5,2}$
5.3	нарушение доступности	$a_{5,3}$

На рис. 2 представлен граф формирования УБКИ например, для источника $a_{1,2}$.

Можно выделить (рис. 2) множество УБКИ для источника $a_{1,2}$ – Антропогенные источники угроз (нарушители), например:

угроза, реализованная $a_{1,2,2,1}$ – нарушителем ИБ (лица, имеющего санкционированный доступ к ИС, но не имеющего доступ к КИ) с использованием уязвимости $a_{2,1}$ – ошибки в программах, приводящие к их сбою, аварийному останову, неправильному режиму работы; методом $a_{3,3}$ поиска компьютеров ИС с оставленным без присмотра активным сеансом или создание условий для их возникновения. Эта угроза воздействует на ресурсы (активы) предприятия – a_4 и нарушает такую характеристику ИБ, как $a_{5,3}$ – нарушение доступности.

После того, как был сформирован полный перечень УБКИ, необходимо построить модель УБКИ. Результатом модели УБКИ является перечень актуальных угроз, на основании которых формируются требования к СЗКИ.

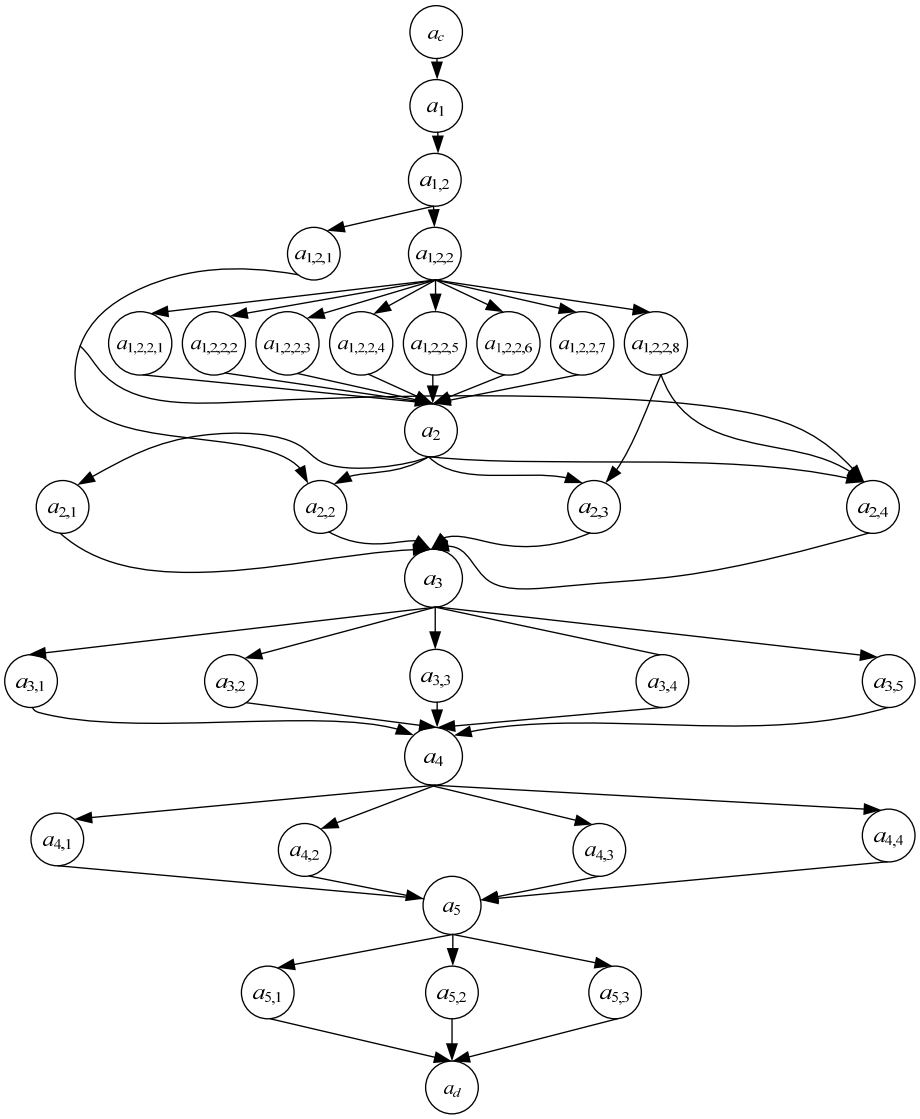

Рис. 2. Граф формирования УБКИ для источника

Выводы. Таким образом, предложенная методология позволяет строить полную матрицу перечня УБКИ. Определив актуальные из них, можно построить модель угроз безопасности информации, учитывающую особенности объекта и ИС. Это дает основания для формирования требования к СЗКИ.

Следует отметить, что формирование полного перечня УБКИ является основополагающим при создании модели УБКИ, поскольку именно на данном этапе производится оценка всех угроз и вероятности их возникновения, что весьма актуально для реализации прочной и эффективной СЗИ.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

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

2. «Специальные требования по технической защите конфиденциальной информации (СТР-К)» / Утверждена Гостехкомиссией 2002 г.
3. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждёна ФСТЭК от 15.02.2008 года.
4. *Миронова В.Г., Шелупанов А.А.* Сети Петри как инструмент анализа системы защиты конфиденциальной информации // Известия ЮФУ. Технические науки. – 2011. – № 12 (125). – С. 64-70.
5. *Шелупанов А.А., Миронова В.Г. и др.* Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – Ч. 1. – 2010. – № 1 (21). – С. 14-22.
6. *Миронова В.Г., Шелупанов А.А.* Предпроектное проектирование информационных систем персональных данных как этап аудита информационной безопасности // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – Ч. 1. – 2010. – № 2 (22). – С. 257-259.
7. *Миронова В.Г., Шелупанов А.А.* Анализ этапов предпроектного обследования информационной системы персональных данных // Вестник СибГАУ им. М.Ф. Решетнева. – 2011. – № 2 (35). – С. 45-48.
8. *Миронова В.Г., Шелупанов А.А., Югов Т.Н.* Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях // Доклады Том. гос. ун-та систем управления и радиоэлектроники. – 2011. – № 2 (24), Ч. 3. – С. 206-211.

Статью рекомендовал к опубликованию к.ф.-м.н. Г.И. Афонин.

Миронова Валентина Григорьевна – Томский государственный университет систем управления и радиоэлектроники; e-mail: mvg@security.tomsk.ru; 634050, г. Томск, пр. Ленина, 40; тел.: 89234151608; руководитель аттестационного цента института системной интеграции и безопасности ТУСУРа.

Шелупанов Александр Александрович – e-mail: saa@udcs.ru; тел.: +83822514302; проректор по научной работе ТУСУРа; д.т.н.; профессор.

Mironova Valentina Grigor'evna – "Tomsk State University of Control Systems and Radio Electronics"; e-mail: mvg@security.tomsk.ru; 40, Lenin avenue, Tomsk, 634050, Russia; phone: +79234151608; the head of the appraisal institute cents systems integration and security TUSUR.

Shelupanov Alexander Alexandrovich – e-mail: saa@udcs.ru; phone: +73822514302; vice-rector TUSUR; dr. of eng. sc.; professor.

УДК 004.056

А.П. Стефаров, В.Г. Жуков

ФОРМИРОВАНИЕ ТИПОВОЙ МОДЕЛИ НАРУШИТЕЛЯ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ*

Рассмотрено решение задачи построения типовой модели нарушителя правил разграничения доступа в автоматизированных системах. Проанализированы существующие подходы к построению неформальной модели нарушителя правил разграничения доступа в автоматизированных системах. Описаны критерии классификации нарушителей и оригинальная методика классификации нарушителей. На основе выявленных критериев предложены семь категорий нарушителей правил разграничения доступа в автоматизированных системах. Сформирована таблица, показывающая наличие угроз информационной безопас-

* Работа выполнена при поддержке Минобрнауки в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2007-2013 годы», ГК № 07.514.11.4047 от 06.10.2011 г.