УДК 004.056.5

В.Г. Миронова, С.С. Бондарчук, С.В. Тимченко

Угрозы безопасности конфиденциальной информации в различных условиях функционирования информационных систем

Представлен способ формирования угроз безопасности конфиденциальной информации, необходимый для создания модели угроз безопасности информации и проектирования системы защиты конфиденциальной информации.

Ключевые слова: угрозы информационной безопасности; конфиденциальная информация, информационная система.

В настоящее время информация становится одним из наиболее весомых и ценных продуктов человеческой деятельности. Эффективность работы любой компании в значительной степени зависит от наличия конфиденциальной информации (КИ), способов ее использования и надежности системы защиты информации (СЗИ).

На различных этапах функционирования информационных систем (ИС) обработки КИ могут возникнуть угрозы безопасности КИ (УБКИ) – такие явления или события, следствием которых могут быть нежелательные воздействия как на информацию, так и на компанию в целом.

В [1] представлены основные виды угроз безопасности:

– физической целостности;

– логической структуры;

– содержания;

– конфиденциальности;

– прав собственности на информацию.

Выявление потенциально существующих возможностей случайного или преднамеренного действия (бездействия), в результате которого могут быть нарушены основные свойства информации и систем ее обработки: доступность, целостность и конфиденциальность – является основной стадией проведения предпроектного обследования. На данной стадии разрабатывается модель угроз безопасности КИ, в которой формируются знания о потенциальных угрозах КИ, оценивается возможность их реализации и степень опасности. Основные этапы создания СЗИ описаны в [2–5].

Первым шагом при разработке модели УБКИ является формирование полного перечня УБКИ, обрабабатываемой в ИС. Формирование полного перечня УБКИ проведем на основе анализа взаимодействия логической цепочки согласно [6]:

источник угрозы – уязвимость – способ (метод) реализации – ресурс – последствие.

Понятия источника УБКИ, уязвимости, последствий приведены в [1]. Описание основных составляющих логической цепочки приведено в таблице.

Для представления УБКИ применим ориентированные графы. Представим полный перечень УБКИ в виде ориентированного графа $\mathbf{Y}(\mathbf{A},\mathbf{B})$, где $\mathbf{A} = \{a_c, a_{1,1}, a_{1,2}, \ldots, a_{i,j}, a_d\}$ – множество вершин графа $\mathbf{Y}$; $\mathbf{B}$ – множество дуг графа $\mathbf{Y}$ – упорядоченных пар вершин $a \in \mathbf{A}$; вершина a_c – начало графа; вершина a_d – конец графа.

Вершины графа представляют собой характеристики УБКИ, которые разделены на уровни по компонентам логической цепочки, где i – количество компонент логической цепочки УБКИ; j – количество признаков каждого компонента.

Для определения множества $\mathbf{A}^* = \{a_{1,1}, a_{1,2}, \ldots, a_{i,j}\}$, $\mathbf{A}^* \in \mathbf{A}$ УБКИ необходимо выявить основные составляющие УБКИ (см. таблицу).

На рис. 1 представлен граф для источника п. 1.2 из таблицы.

Основные составляющие УБКИ

№ п/п	Наименование	Обозначение
1	*2*	*3*
1	Источник угрозы	$\mathbf{A}_1$
1.1	Природные источники угроз	$a_{1,1}$
1.2	Антропогенные источники угроз (нарушители)	$\mathbf{A}_{1,2}$
1.2.1	Внешние (нарушитель ИБ территориально расположен за пределами контролируемой зоны (КЗ))	$a_{1,2,1}$
1.2.2	Внутренние	$a_{1,2,2}$
1.3	Техногенные источники угроз	$a_{1,3}$
2	Уязвимость	$\mathbf{A}_2$
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 СЗИ	$a_{2,2}$
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	Неправильная конфигурация и настройка программных, программно-аппаратных и аппаратных средств, включая СЗИ, приводящие к нарушению безопасности информации ИС	$a_{2,4}$
2.5	Отсутствие блокировки сеансов, оставленных без присмотра	$a_{2,5}$
2.6	Организационно-технические (технологические) уязвимости (непродуманная (небезопасная) технология обработки информации, отсутствие или ошибки в регламентах, отсутствие контроля доступа в помещения за обращением документов по СЗИ и ИС, отсутствие контроля несанкционированного физического подключения к линиям связи и коммуникационному оборудованию ИС и т.д.)	$a_{2,6}$
2.7	Отсутствие контроля целостности данных СЗИ	$a_{2,7}$
2.8	Отсутствие контроля за ИТ-средой ИС (за наличием в ИС только штатного санкционированного оборудования и программных средств: компьютеров, линий связи, периферийных устройств, системных и прикладных программ)	$a_{2,8}$
2.9	Назначение простых коротких или «пустых» паролей для входа в систему, отсутствие обеспечения их конфиденциальности	$a_{2,9}$
2.10	Хранение, отображение и передача данных об ИС либо из базы данных (БД) ИС в явном виде	$a_{2,10}$
3	Способ (метод) реализации	$\mathbf{A}_3$
3.1	Потеря, несанкционированное копирование, кража и вынос документов допущенными к ним лицами	$a_{3,1}$
3.2	Поиск и копирование документов о ИС и СЗИ, 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	Добывание паролей персонала ИС путём общения с ним, подглядывания за его вводом, подслушивания и другими способами	$a_{3,5}$
3.6	Поиск и использование путей обхода СЗИ с помощью штатных программ ИС	$a_{3,6}$
3.7	Использование штатных программ и/или аппаратных, программно-аппаратных средств для поиска, несанкционированного просмотра и/или копирования незащищённых данных	$a_{3,7}$
3.8	Несанкционированное удаление, обнуление, перезапись данных ИС с помощью штатных программ и/или аппаратных, программно-аппаратных средств	$a_{3,8}$
3.9	Модификация (искажение) данных ИС с помощью штатных программ и/или аппаратных, программно-аппаратных средств	$a_{3,9}$
3.10	Случайное возникновение сбоев, отказов и ошибок вследствие старения, износа, неправильного технического обслуживания оборудования и некачественного проектирования программного обеспечения (ПО) ИС	$a_{3,10}$

Продолжение таблицы

1	*2*	*3*
4	Ресурсы (активы)	$\mathbf{A}_4$
4.1	Информация (вводимая в систему, содержащаяся в БД, выводимая из системы), подпадающая под действие Перечня сведений, подлежащих засекречиванию, иная информация 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	Технические средства (ТС) (аппаратные и программно-аппаратные средства, накопители и носители информации, линии связи), содержащие КИ или обеспечивающие её передачу	$a_{4,2}$
4.3	Программные средства (общесистемные, прикладные), обрабатывающие КИ	$a_{4,3}$
4.4	Документация, раскрывающая КИ и технологию ее обработки	$a_{4,4}$
5	Последствия	$\mathbf{A}_5$
5.1	Нарушение конфиденциальности	$a_{5,1}$
5.2	Нарушение целостности	$a_{5,2}$
5.3	Нарушение доступности	$a_{5,3}$

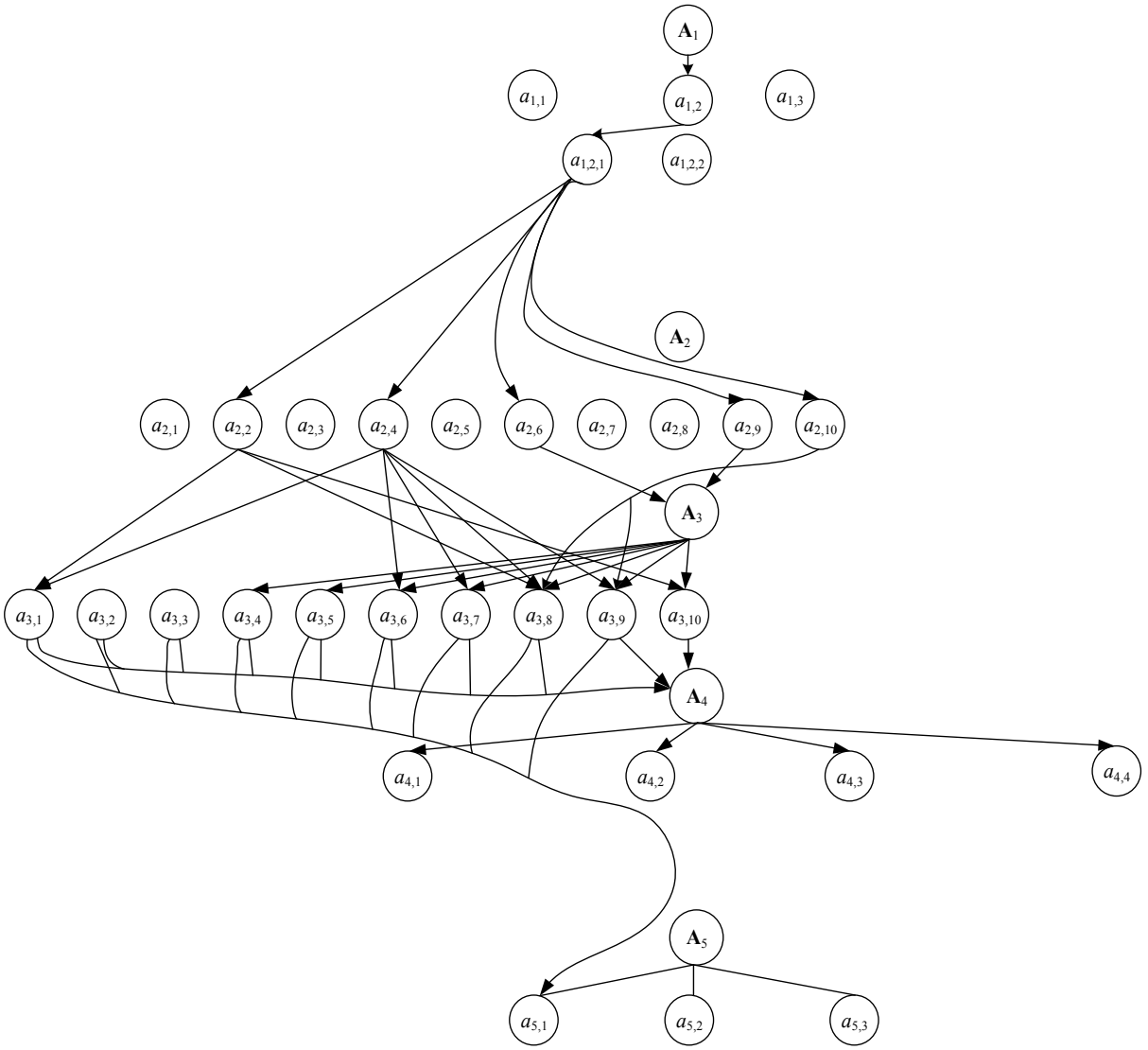

Рис. 1 Граф для источника п. 1.2 табл.1

Используя предложенный автором подход, можно сформировать перечень УБКИ, которые могут быть реализованы в заданных условиях функционирования, расположения ИС и конкретными

нарушителями информационной безопасности информации. Безусловно, после того как перечень будет установлен, специалисты должны определить среди этих угроз актуальные и спроектировать СЗИ. Подходы к созданию механизмов защиты КИ представлен в [7–10].

Литература

1. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 278 с.

2. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» / А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 14–22.

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

4. 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.

5. Архипов В.А. Технология прямого поиска при решении задач прикладной математики / В.А. Архипов, С.С. Бондарчук, И.Г. Боровской, А.А. Шелупанов // Вычислительные технологии. – 1995. – Т. 4, № 10. – С. 19.

6. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях их возникновения / В.Г. Миронова, А.А. Шелупанов // Известия Южного федерального университета. Технические науки. – 2012. – Т. 137, № 12. – С. 39–45.

7. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия – Телеком, 2009. – 552 с.

8. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Т.Н. Югов // Доклады ТУСУРа. – 2011. – № 2 (24), ч. 3. – С. 206–211.

9. Криптографические протоколы в системах с ограниченными ресурсами / Р.В. Мещеряков, С.К. Росошек, А.А. Шелупанов, М.А. Сонькин // Вычислительные технологии. – 2007. – Т. 12, Спецвыпуск №1. – С. 51–61.

10. 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.

Миронова Валентина Григорьевна
Канд. техн. наук, мл. науч. сотр. каф. комплексной информационной безопасности
электронно-вычислительных систем ТУСУРа
Тел.: +7-923-415-16-08
Эл. почта: mvg@security.tomsk.ru

Бондарчук Сергей Сергеевич
Д-р физ.-мат. наук, профессор Томского государственного педагогического университета
Эл. почта: office@keva.tusur.ru

Тимченко Сергей Викторович
Д-р техн. наук, ст. науч. сотр., профессор каф. математической физики
Национального исследовательского Томского государственного университета
Эл. почта: tsv@ftf.tsu.ru

Mironova V.G., Bondarchuk S.S., Timchenko S.V.

Threats to information security of confidential information in different contexts of information systems for handling confidential information

The paper presents a method for forming security threats confidential information needed to create the model information security threats and system design to protect confidential information.

Keywords: information security threats; confidential information, the information system.