УДК 004.056.5

В.Г. Миронова, Е.Б. Белов, А.Ю. Крайнов

Формирование требований при проектировании системы защиты конфиденциальной информации

Представлен способ проведения анализа выполнения требований по информационной безопасности в информационных системах обработки конфиденциальной информации. Требования, предъявляемые к информационным системам обработки конфиденциальной информации, лежат в основе при проектировании и внедрении системы защиты информации.

Ключевые слова: система защиты, требования по безопасности информации, конфиденциальная информация.

Современные компании используют для автоматизации своей деятельности информационные системы (ИС). Все ключевые бизнес-процессы, такие как финансовый и бухгалтерский учет, управление кадрами, клиентами, товаром и складом, документооборот, автоматизируются соответствующими системами, а информация, циркулирующая в них, относится к информации ограниченного доступа (конфиденциальной информации (КИ)). При всей неоспоримой полезности внедрения все большего количества ИС этот процесс несет в себе новые издержки и риски для компании. Обязательным условием высокой конкурентоспособности компании становится защита информации в компании. Защита информации возможна путем создания системы защиты информации (СЗИ).

Разработка системы защиты информации производится подразделением организации или специализированными организациями, имеющими лицензии Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и(или) Федеральной службы безопасности (ФСБ России). Описание этапов создания СЗИ представлено в [1–4].

Основополагающим этапом создания СЗИ является предпроектное обследование ИС, в ходе проведения которого производится инвентаризация ресурсов ИС, построение моделей нарушителя и угроз безопасности информации, исследуются применяемые механизмы защиты информации. Подходы к анализу и оценке угроз безопасности информации описаны в [5, 6].

В ряде нормативных документов федеральных служб – ФСТЭК России и ФСБ России – предложен состав подсистем СЗИ от несанкционированного доступа (НСД):

– подсистема управления доступом;
– подсистема регистрации и учета;
– подсистема контроля целостности;
– подсистема безопасного межсетевого взаимодействия;
– подсистема антивирусной защиты;
– подсистема резервного копирования, восстановления и архивирования;
– подсистема криптографической защиты.

Подсистема управления доступом должна обеспечивать защиту от НСД серверов, автоматизированных рабочих мест (АРМ) пользователей и прикладных сервисов. Кроме того, должна быть обеспечена защита от НСД аппаратно-программных средств, влияющих на функционирование сегментов информационных сетей, в которых обрабатывается защищаемая информация. Основные механизмы реализации этой подсистемы – идентификация и аутентификация, подробно описанные в [7, 8].

В подсистеме регистрации и учета должны регистрироваться события, происходящие в ИС, касающиеся обработки информации ограниченного доступа в ней, например: запуск и останов средств регистрации; события, связанные со средствами безопасности, и др.

Подсистема обеспечения целостности должна осуществлять целостность программных средств защиты информации в составе СЗИ, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации.

Подсистема безопасного межсетевого взаимодействия предназначена для обеспечения безопасности информации при ее обработки в ИС, имеющих выход в сеть общего пользования и(или) международного информационного обмена.

Защиту от вредоносного программного обеспечения обеспечивает подсистема антивирусной защиты.

В [9, 10] описаны подходы, которые применяются при создании подсистемы криптографической защиты, которая обеспечивает конфиденциальность и целостность данных, хранимых в компонентах ИС и передаваемых между ними.

При разработке СЗИ определяются конкретные требования по защите информации, проводится аналитическое обоснование необходимости создания СЗИ и согласовывается выбор основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС), технических и программных средств защиты информации, организуются работы по выявлению возможных каналов утечки информации и нарушения целостности защищаемой информации, аттестация объекта информатизации.

Для проведения оценки уровня информационной безопасности ИС на соответствие требованиям стандартов и нормативных документов используются групповые и частные показатели.

Групповой показатель (GP_d) используется для оценки каждой группы требований к конкретной подсистеме СЗИ, d – номер группового показателя.

Оценка конкретного требования подсистемы СЗИ осуществляется с использованием частного показателя ($CP_{(d,f)}$), который детализирует общую оценку, f – номер частного показателя.

Оценка частного показателя ($CP_{(d,f)}$) формируется по результатам экспертного оценивания степени реализации требования подсистемы защиты информации в СЗИ.

При этом частному показателю $CP_{(d,f)}$ присваиваются следующие значения: 0 – не реализовано; 0,25, 0,5, 0,75 – частично реализовано; 1 – реализовано полностью.

Оценка группового показателя (GP_d) вычисляется как среднее из оценок входящих в него частных показателей ($CP_{(d,f)}$):

$$GP_d = \frac{\sum_{n=1} CP_{(d,f)}}{n}, \quad (1)$$

где n – количество частных показателей (требований к подсистеме защиты информации), входящих в групповой показатель (в подсистему защиты информации, функционирующую в составе СЗИ).

Оценки GP_d, полученные в результате оценивания групповых показателей ИБ, отображаются на диаграмме в соответствующих секторах d на величину, соответствующую значению оценок.

Примером может служить реализация подсистемы управления доступом субъектов доступа к объектам доступа в системе защиты персональных данных (ПДн) согласно [11] в ИС ПДн (ИСПДн), класс защищенности которой – 4.

Требования к подсистеме управления доступом субъектов доступа к объектам доступа для ИСПДн класса защищенности 4:

«УПД.1 – управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

УПД.2 – реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

…

УПД.6 – ограничение неуспешных попыток входа в ИС (доступа к ИС);

…

УПД.11 – разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;

…

УПД.13 – реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;

УПД.14 – регламентация и контроль использования в ИС технологий беспроводного доступа;

УПД.15 – регламентация и контроль использования в ИС мобильных технических средств;

УПД.16 – управление взаимодействием с ИС сторонних организаций (внешние ИС)…».

В таблице представлена экспертная оценка частных показателей подсистемы управления доступом субъектов доступа к объектам доступа для ИСПДн класса защищенности 4.

Экспертная оценка частных показателей

УПД 1	УПД 2	УПД 6	УПД 11	УПД 13	УПД 14	УПД 15	УПД 16
0,75	0,5	0,75	0,25	0,5	0	0	0,5

На рис. 1 показана диаграмма частных показателей подсистемы управления доступом субъектов доступа к объектам доступа для ИСПДн класса защищенности 4.

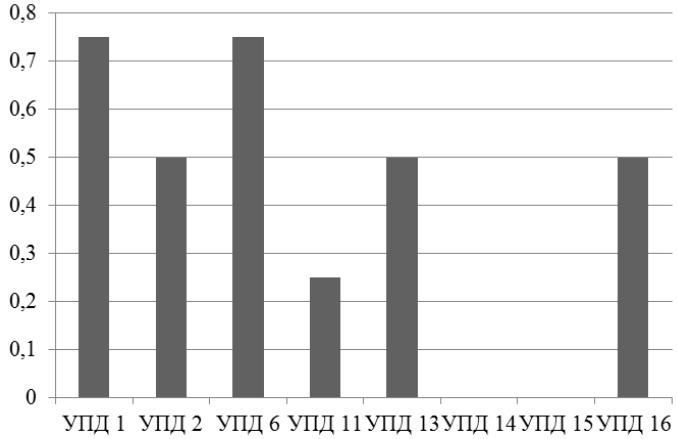

Рис. 1. Диаграмма частных показателей подсистемы управления доступом субъектов доступа к объектам доступа для ИСПДн класса защищенности 4

Исходя из полученных данных по частным показателям подсистемы управления доступом субъектов доступа к объектам доступа для ИСПДн класса защищенности 4 и формулы (1), групповой показатель будет равен 0,40625.

Таким образом, предложенный подход к оценке механизмов защиты информации позволяет выявить не только недействующие механизмы защиты информации, но и подсистемы СЗИ, которые являются слабыми относительно других реализованных в СЗИ подсистем.

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 Томского государственного университета систем управления и радиоэлектроники. – 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. 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.

11. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2013/06/26/gostajna-dok.html, свободный (дата обращения: 19.05.2014).

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

Белов Евгений Борисович
Зам. председателя Совета УМО по образованию в области информационной безопасности, Москва
Тел.: +7 (495) 931-06-09
Эл. почта: umoib@yandex.ru

Крайнов Алексей Юрьевич
Д-р физ.-мат. наук, доцент, профессор каф. математической физики физико-технического факультета Национального исследовательского Томского государственного университета
Эл. почта: office@keva.tusur.ru

Mironova V.G., Belov E.B., Krainov A.Yu.
Formation of requirements when designing a system to protect confidential information

The paper presents a method to analyze the requirements for information security in information systems for handling confidential information. Requirements for information systems processing sensitive information underlie the design and implementation of information security.
Keywords: system protection requirements for information security, confidential information.
