УДК 004.056

В.М. Нечунаев

Методика описания корпоративной информационной системы для процедуры управления рисками информационной безопасности

Приведена методика описания корпоративной информационной системы как первоначальный этап процедуры управления рисками информационной безопасности. С использованием методов системного анализа производится декомпозиция структуры системы, вводится постановка проблемы обеспечения информационной безопасности в отношении системы.

В настоящее время управление рисками информационной безопасности является одной из самых актуальных тенденций в области решения вопросов информационной безопасности. Первоначальным этапом любой процедуры управления рисками является описание (характеристика) системы.

Корпоративная информационная система (КИС) определяется как система, состоящая из персонала, информации и комплекса средств автоматизации, реализующая информационную технологию установленных функций. Исходя из определения, в КИС выделяются четыре уровня:

- технические средства;
- программное обеспечение;
- информационные ресурсы;
- организационныя структуры – сотрудники, отделы, рабочие группы, сторонние организации, с которыми ведется работа в рамках КИС.

Минимально определяемой единицей, к которой применимы процедуры управления рисками, является элемент КИС. В результате КИС можно представить как совокупность элементов различных уровней.

Для элементов КИС определяются свойства, характерные с точки зрения информационной безопасности. Перечислим основные свойства:

- конфиденциальность (К);
- целостность (Ц);
- доступность (Д);
- надежность (Н).
- уровень доверия (УД).

Для всех свойств элементов КИС задаются количественно-качественные шкалы, позволяющие характеризовать значимость элементов в структуре КИС и для работы организации в целом.

Взаимосвязь элементов и работа КИС в целом моделируются заданием связей между элементами разным уровней. Дадим определение связи.

Связь – это отношения между элементами КИС. Анализ функционирования КИС позволяет определить два вида связей:

- *Связь физического соединения* – канал связи между двумя серверами; администратор, имеющий физический доступ к серверу.
- *Связь логического соединения* – пользователь, имеющий доступ к базе данных под определенной учетной записью; информационные ресурсы, находящиеся на сервере.

Связь может быть однонаправленной или двунаправленной.

Однонаправленная связь – это связь от элемента Э1 к Э2, при которой реализация угрозы на Э2 ставит под угрозу элемент Э1, и, напротив, реализация сценария угрозы на Э2 не ставит под угрозу элемент Э1.

Двунаправленная связь – это связь от элемента Э1 к Э2, при которой реализация сценария угрозы на одном из элементов ставит под угрозу другой элемент.

В результате перечисления элементов КИС и связей между ними получаем граф следующего вида:

- Вершины графа – элементы КИС с набором свойств.
- Ребра графа – виды связей между элементами КИС.

Пример простейшего графа приведен на рис. 1.

Постановка проблемы обеспечения информационной безопасности в отношении КИС достигается моделированием системы управления информационной безопасностью (СУИБ). В структуре системы управления информационной безопасностью можно выделить следующие компоненты: инженерно-технические, программно-аппаратные, организационные, правовые, морально-этические [1].

Единственным типом элементов СУИБ являются защитные меры. Защитные меры – это различные способы решения задач информационной безопасности.

В контексте взаимодействия КИС и СУИБ защитные меры применяются к элементам КИС, воздействуя на определенные свойства. К примеру, защитная мера «резервирование» может быть применена к свойству «доступность» элемента типа «роутер». Одна и та же защитная мера может применяться как к одному элементу, так и к группе элементов, причем типы элементов могут быть различными.

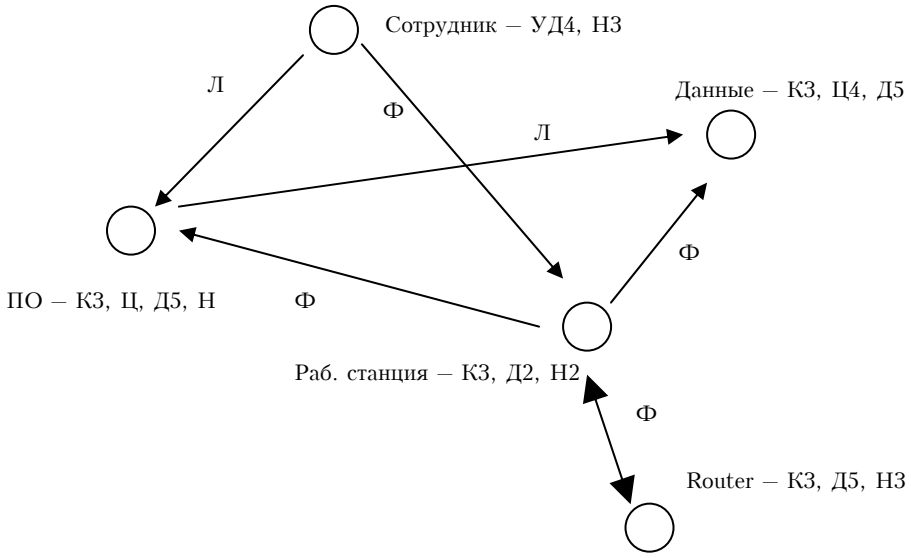

Рис. 1. Пример описания КИС

Модель действия защитной меры в целом идентична общей модели управления безопасностью [2]. Воздействие защитной меры может быть прямое, опосредованное или защитная мера никак не может воздействовать на задачу обеспечения информационной безопасности. Полный список защитных мер и их достаточность выходят за рамки данной работы.

Связи между элементами КИС и СУИБ определяются свойствами элементов СУИБ. Если защитная мера прямо воздействует на свойство «конфиденциальность» и опосредованно на свойство «доступность» какого-либо элемента КИС, то связь между элементом КИС и элементом СУИБ определяется как «К 2, Ц 0, Д 1, О 0, УД 0, Н 0».

Связь между элементами КИС и СУИБ является однонаправленной и всегда направлена от элемента СУИБ к элементу КИС.

Резюмируя, совокупность защитных мер, применяемых к элементам КИС, можно представить как несвязный граф.

Общую характеристику системы можно представить как граф №1, определяющий КИС, и граф №2, определяющий СУИБ. Два графа связаны между собой связями, которые определяют воздействие элементов графа №2 на элементы графа №1.

Таким образом, представленная методика описания корпоративной информационной системы является основой для процедуры управления рисками и в дальнейшем позволяет:

1. Производить оценку уровня потенциального ущерба.
2. Производить оценку уровня риска информационной безопасности как по системе в целом, так и по отдельным элементам.

Литература

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Основы защиты информации. – Ч. 1. – Томск: В-Спектр, 2007. – 152 с.

2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия – Телеком, 2004. – 280 с.

3. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. – М.: Гелиос АРВ, 2005. – 224 с.

Нечунаев Вадим Михайлович
Ижевский Государственный Технический Университет
Аспирант кафедры «Системы и технологии информационной безопасности»
Тел.: 8(3412) 63 03 57
Эл. почта: nvm@019.pfr.ru

V.M. Nechunaev

Description methodology of corporate information system for information security risk managment procedure

In present work the description methodology of corporate information system is given as a first stage of information security risk managment procedure. Using system analysis methods the decomposition of system structure is produced, the problem of supplying with information security regarding system is set.