УДК 519.95

ИНФОРМАЦИОННЫЕ РИСКИ

© М.В. Чириков

Ключевые слова: информация; защита информации; информационные риски.

Статья посвящена методике оценки информационных рисков. Описаны задачи, которые необходимо решить для построения процесса управления рисками организации.

Из-за стремительного внедрения информационных технологий во всем мире и постоянно растущего числа сфер, где информация является стратегически ценной единицей организации, охрана этой информации занимает одно из главенствующих позиций. Сегодня информация, будучи нематериальной по своей природе, становится предметом товарно-денежных отношений и объектом нормативно правового регулирования.

Как перед государственными структурами, так и перед коммерческими организациями, заинтересованными в охране сведений, имеющих в своем составе информацию, которая могла бы каким-либо образом повлиять на прибыль или интересы учреждения, встают вопросы, какую сумму нужно потратить на защиту информации, что будет в случае, если информация, которая представляет интерес для злоумышленника или конкурента, попадет к нему в руки, и какие последствия при этом могут наступить [1]. Требуется также обоснованность защиты информации. На эти вопросы призвана дать ответ методика оценки информационных рисков.

При построении процесса управления рисками организациям необходимо решить несколько задач. В первую очередь, формализовать процесс, который связан с политикой управления рисками или политикой безопасности. Основными ключевыми моментами являются определение объектов процесса, основных составляющих процесса, распределение ответственности между подразделениями организации, определение минимально допустимого уровня приемлемого риска и т. д.

Следующая задача, стоящая перед организацией, – это построение модели угроз. В этом может участвовать не только отдел информационной безопасности, но и другие подразделения организации. Модель угроз – ключевой элемент в построении процесса обеспечения безопасности. Исходя из определения угрозы, угрозу можно декомпозировать на три основных части – источник, действие, объект воздействия. Часто необходимо доказать, что создаваемая модель полна, т. е. описывает все возможные угрозы. Самый простой путь – это разделить каждый компонент на классы. Например, источники поделить на природные, техногенные и антропогенные; человеческие действия – на случайные и неслучайные; объекты воздействия – на типы информационных ресурсов: ПО, оборудование, персонал, процессы и т. д. Для наглядности можно воспользоваться графами. При этом любая новая угроза может быть декомпозирована вышеописанным способом, и ее элементы попадут в тот или иной класс [2].

И, наконец, последней задачей, с точки зрения построения процесса обеспечения безопасности, является создание методики по управлению информационным рисками.

Таким образом, решение вышеобозначенных задач позволяет значительно снизить информационные риски организации.

ЛИТЕРАТУРА

1. *Петренко С.А., Симонов С.В.* Управление информационными рисками. Экономически оправданная безопасность. Компания АйТи; ДМК Пресс, 2004. С. 11-15.
2. *Голов А.* Методы оценки информационных рисков // Информационно-издательский центр «CONNECT!». 2007. № 11. URL: http://www.ec-group.ru/press/public/detail.php?ID=56&print=Y. Загл. с экрана.

Поступила в редакцию 16 ноября 2011 г.

Chirikov M.V. INFORMATION RISKS

The article is devoted to the assessment methodics of information risks. The tasks which are necessary to solve for constructing the process of management of organization risks are described.

Key words: information; information protection; information risks.