ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

П. П. Бескид, П. И. Силин

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ: БАЗОВЫЕ ПОНЯТИЯ, КЛАССИФИКАЦИЯ, СТАНДАРТИЗАЦИЯ

P. P. Beskid, P. I. Silin

INFORMATION RISK MANAGEMENT: BASIC CONCEPTS, CLASSIFICATION, STANDARDIZATION

В статье проанализировано понятие «информационный риск», представлена классификация информационных рисков организации, рассмотрены основные государственные стандарты в области управления рисками.

***Ключевые слова**: информационный риск, качество информации, классификация рисков, управление рисками.*

The article analyzes the concept of "information risk", classification of information risk organizations, the basic standards in the field of risk management.

***Keywords**: information risk, quality of information, risk classification, risk management.*

Введение

Успешная деятельность любых организаций связана с получением, передачей, хранением и обработкой информации. Современные корпоративные информационные системы позволяют сотрудникам использовать сервисы и приложения, работающие с едиными базами данных. Однако большинство существующих корпоративных информационных систем не проектировались с необходимым уровнем защищенности информации, что делает их уязвимыми к информационным рискам. Таким образом, одним из важнейших аспектов обеспечения нормального функционирования любой организации является задача анализа и управления информационными рисками.

Понятие «информационный риск» неоднозначно, обладает специфическими особенностями. Целью данной статьи является анализ и классификация информационных рисков в контексте информационной безопасности организации; обзор основных государственных стандартов в области управления рисками.

Анализ понятия «информационный риск»

Несмотря на то что в настоящее время термин «информационный риск» нашел широкое применение, пока не существует принятой большинством ученых и практиков

трактовки этого понятия. В аспекте информационной безопасности риск можно связать с событием реализации угрозы ресурсам информационной системы, вследствие которого произошло нарушение одной или более их базовых характеристик безопасности — конфиденциальности, целостности, доступности. Также информационный риск можно описать, как:

- вероятность события, которое привело к нарушению характеристик безопасности;
- событие, которое произошло с участием или без участия субъекта — деятельность или бездействие субъекта;
- выбор альтернативного варианта;
- событие, которое происходит с определенной частотой; характеристика этого события и т.д. [6].

Качественный анализ современных подходов к определению и характеристикам понятия «информационный риск» представлен в работах А.В. Шарапова [8]. Автор предлагает собственное определение: «Информационный риск — это возможность наступления случайного события в информационной системе предприятия, приводящего к нарушению ее функционирования, снижению качества информации ниже допустимого уровня, в результате которых наносится ущерб предприятию» [1].

Ключевым в данном определении является понятие «качество информации», которое в различных источниках определяется как: степень практической пригодности информации, используемой в процессе управления; определяемая совокупностью таких свойств, как полнота, плотность, полезность, достоверность, ценность информации; совокупность объективных свойств информации, обусловливающих ее пригодность удовлетворять потребности конечных пользователей [7].

Информация имеет ряд специальных свойств, входящих в состав ее качества. Их классификация приведена на рис. 1.

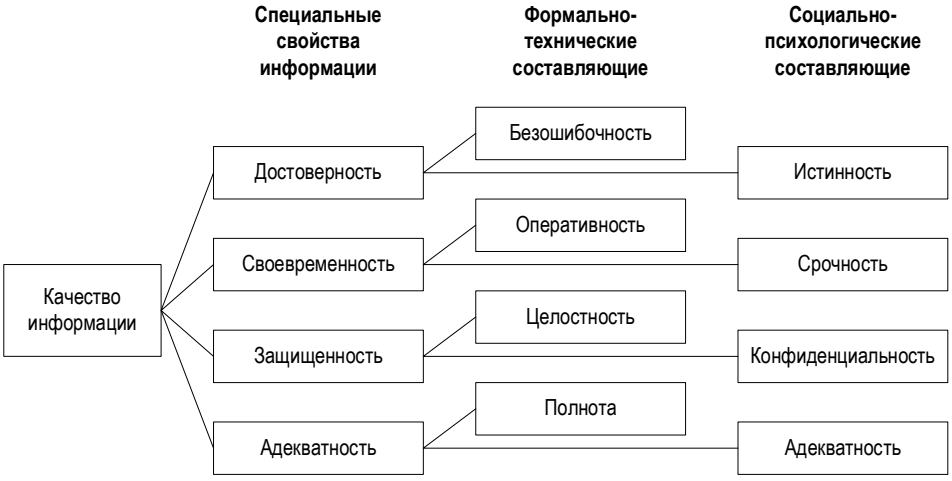

Рис. 1. Составляющие качества информации

Достоверность информации — это ее свойство не иметь скрытых ошибок.

Своевременность — свойство информации, состоящее в выполнении требований ее поступления потребителю не позднее предварительно установленного срока или через оговоренный промежуток времени после запроса.

Свойство *защищенность* информации состоит в невозможности несанкционированного ее использования или изменения.

Кроме этого можно выделить социально-психологическое свойство — *конфиденциальность*, т.е. статус, предоставляемый информации, определяющий требуемую степень ее защиты и согласованный между пользователем и информационной системой.

Адекватность — свойство информации, заключающееся в верном отображении связей и отношений соответствующего объекта. В адекватности можно выделить составляющие: *полноту* — свойство, характеризующее степень отображения реальной действительности (описываемого объекта) в используемом конкретном сообщении, и *избирательность* — социально-психологическое свойство информации, состоящее в том, что она содержит наиболее полезные сведения для лица, принимающего решения.

Классификация информационных рисков

Анализ, оценка и управление рисками невозможны без их классификации. Существуют различные виды информационных рисков, основания и критерии, позволяющие их классифицировать. Среди всего многообразия оснований для классификации рисков выделяют [9] классификации по:

- источнику риска (внешний и внутренний);
- объему (локальный, глобальный);
- уровню новизны (повседневный, инновационный);
- мере опасности (катастрофический, допустимый, критический);
- срокам (кратковременный, стабильный);
- возможности преобразования (систематический, специфический);
- области применения (информационный, экологический, экономический и др.);
- степени риска (оправданный, неоправданный).

Традиционно для классификации информационных рисков выделяют внешние и внутренние риски [2] (табл. 1).

Таблица 1

Классификация информационных рисков

Внешние информационные риски	Внутренние информационные риски
Природно-естественные риски	Риски, связанные с управлением корпоративной инфраструктурой
Техногенные риски	Риски, связанные с деятельностью сотрудников
Социально-политические риски	Технические и технологические риски
Финансово-экономические риски	Имущественные риски
Риски, связанные с терроризмом (в т.ч. международным)	

Нужно отметить, что проблематика оценки и управления «внешними» рисками, а также техническими и технологическими рисками, достаточно исследована в специальной литературе. Стремительное развитие технологий защиты информации (программных, аппаратных и программно-аппаратных) позволило уменьшить число инцидентов безопасности технического характера. При этом число инцидентов, причиной которых в различных проявлениях служит человеческий фактор, остается велико. Персонал остается «слабым звеном», поэтому, наряду с техническими аспектами управления рисками, обеспечением согласованной работы большого количества разнородных составляющих корпоративной инфраструктуры, не меньшее внимание должно уделяться кадровым и организационным аспектами.

Государственные стандарты в области управления рисками

Оценка риска (risk assessment) в различных источниках рассматривается как: идентификация информационных ресурсов системы и угроз этим ресурсам, а также возможных потерь (потенциал потери), основанная на оценке частоты возникновения событий и размера ущерба; включающий идентификацию и анализ риска [4,5,9]; выявление риска и определение его влияния; составление списка рисков, ранжированных по цене и критичности; изучение уязвимостей, угроз, вероятности возможных потерь и теоретической эффективности контрмер [3].

В различных источниках под управлением риска понимают процессы идентификации, управления, устранения или уменьшения вероятности событий, способных негативно воздействовать на ресурсы информационной системы, уменьшения рисков безопасности при условии приемлемой стоимости средств защиты; выявления и оценки рисков и осуществления шагов по его снижению до приемлемого уровня [10]; осознания причин и границ нежелательных событий, определения приемлемого уровня риска, а также снижения его до приемлемого уровня [3].

Общее руководство по определению процесса менеджмента риска устанавливают Рекомендации по стандартизации Р 50.1.069-2009 в части 2 «Определение процесса менеджмента риска» (Determination of risk management process), утвержденные и введенные в действие Приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 г. № 1259-ст. Термины и определения, примененные в рекомендациях, соответствуют ГОСТ Р 51898 (Аспекты безопасности. Правила включения в стандарты) и ГОСТ Р 51897 (Менеджмент риска. Термины и определения). Подробная схема процесса менеджмента риска представлена на рис 2.

Заключение

В статье проведен анализ понятий «информационный риск» и «качество информации», рассмотрена классификация информационных рисков в контексте информационной безопасности организации.

Были рассмотрены основные государственные стандарты в области управления рисками; представлена схема процесса менеджмента риска, которая применяется на многих уровнях (стратегическом, тактическом, операционном) деятельности организации.

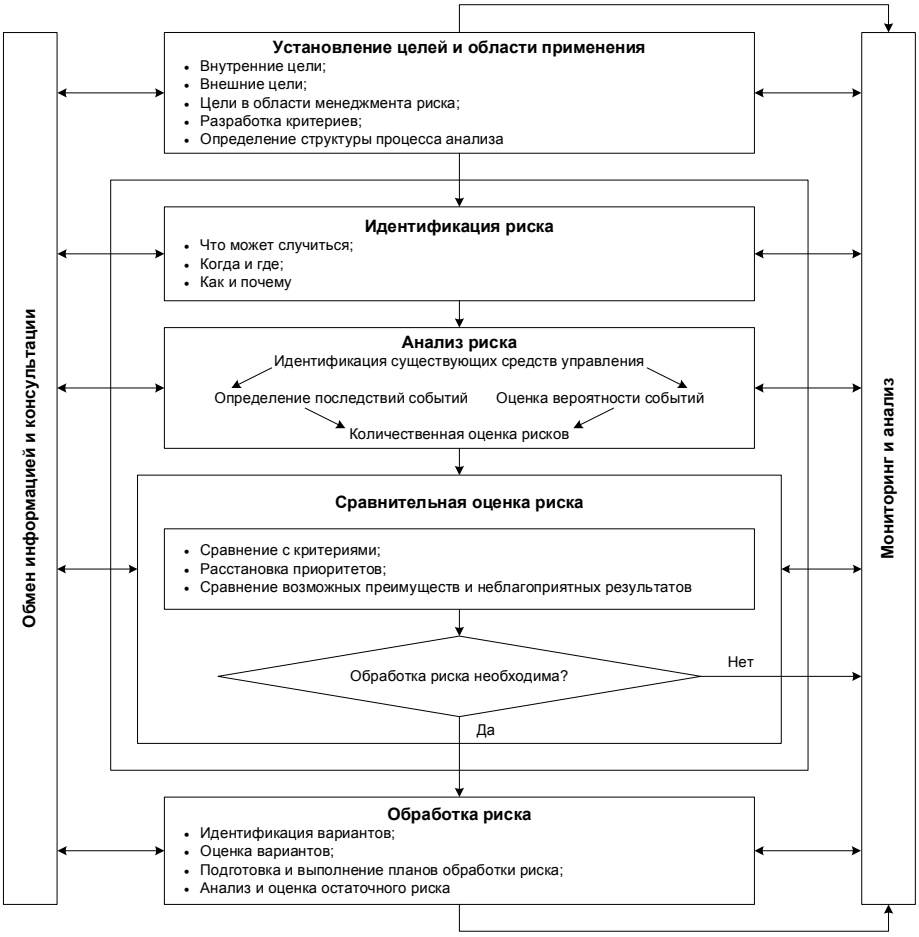

Рис. 2. Подробное описание процесса менеджмента риска

Проанализировав современные подходы к управлению информационными рисками, можно сделать вывод, что риски, связанные с человеческим фактором наиболее тяжело поддаются менеджменту. Это обусловлено тем, что большая часть видов рисков, указанных в классификации, возникает непосредственно из-за действий человека. Таким образом, для обеспечения информационной безопасности организаций особое внимание должно уделяться кадровым и организационным аспектам.

Литература

1. *Бескид П.П., Силин П.И.* Использование метода анализа иерархий для оценки информационных рисков в ГИС предприятий-перевозчиков бытовых отходов // Учен. зап. РГГМУ. 2015. № 40. — С. 276–283.

2. *Дьяконов Д.* Страхование информационных рисков как метод защиты информации [Электронный ресурс]. — URL: http://www.amulet-group.ru/page.htm?id=30
3. *Захаров А.И.* Информационные системы: оценка рисков // Information Security (Информационная безопасность). 2005. № 6. — С. 18–19.
4. *Информационная* технология. Уроки целостности систем и программных средств. ГОСТ Р ИСО/МЭК 15026-2002. Введ. 2003.06.30. — М.: ИПК «Издательство стандартов», 2–3. — 15 с.
5. *Информационные* технологии. Свод правил по управлению защитой информации: ISO/IES 27002:2005(E). — М.: Компания «Технорматив», 2007. — 117 с.
6. *Корченко А.Г., Иванченко Е.В., Казмирчук С.В.* Анализ и определение понятия риска для его интерпретации в области информационной безопасности // Ukrainian Information Security Research Journal. 2010. Т. 12, № 3(48). — С. 27–34.
7. *Леонтьев Е.А.* Надежность экономических информационных систем: учебное пособие. — Тамбов: Изд-во Тамб. гос. техн. ун-та, 2002. — 128 с.
8. *Шарапов А.В.* Проблема определения понятия информационных рисков // Безопасность информационных технологий. Bezopasnost Informatsionnykh Tekhnology. № 2010-2. — С. 44–48.
9. *International* standard Risk management. Principles and guidelines: ISO\FDIS-2009. — 24 p.
10. *Lichtensteir S.* Factors in the Selection of s Risk Assessment Method // Information Management & Computer Security. 1993. Vol. 4. Iss. 4. — P. 20–22.