УДК 519.876.5

МЕТОДЫ ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ IT-ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

В. Е. СЕМЕНЕЦ, Т. П. ЗАЙКО, канд. пед. наук, доц. А. П. МАТЕЛЕНОК
(Полоцкий государственный университет
имени Евфросинии Полоцкой, Беларусь)

Аннотация. *Проанализированы наиболее значимые определения понятия «информационные риски». Рассмотрено понятие «качество информации». Произведена классификация ИТ-рисков. Представлен основные этапы методики качественной и количественной внутренних информационных рисков. Охарактеризованы основные правила минимизации ИТ-рисков.*

Ключевые слова: *ИТ-риски, качество информации, минимизации ИТ-рисков.*

В век информатизации автоматизация бизнес-процессов предприятия, использование разнообразных информационных сервисов и систем для ввода, обработки и защиты рабочей информации – это залог эффективности и конкурентоспособности на рынке. Однако, использование таких сложных и громоздких систем на предприятии сопровождается значительными трудностями по управлению информационной средой. Одним из важнейших параметров минимизация появляющихся рисков, связанных с информационными процессами на предприятии. Исходя из выше сказанного, управление рисками нарушения информационной целостности является основной задачей информационной безопасности компании, а ее обеспечение главным критерием качества выполнения информационных процессов в частности и информационной инфраструктурой предприятия в целом.

Термин «информационный риск (ИР)» широко используется в научной литературе, однако в настоящее время не существует общепринятой трактовки этого понятия. Отдельные специалисты в это понятие вкладывают следующий смысл: «информационный риск – это возможное событие, в результате которого несанкционированно удаляется, искажается информация, нарушается ее конфиденциальность или доступность» [1, с. 86]. В представленном определении ИР используется как синоним понятия угроза безопасности информации. Управление такими информационными рисками сводится к защите информации.

Д. Дьяков, рассматривает “информационный риск как угрозу безопасности информации в компьютерных системах” [2]. В работах других авторов рассматриваются под ИР рассматриваются в основном технические средства информационных технологий, исключая такой ключевой элемент информационных систем, как специалист. Заметим, что практически **отсутствуют подходы к трактовке понятия**

"информационный риск", в которых в качестве возможных нежелательных событий рассматривались бы события, приводящие к снижению достоверности, полноты и актуальности информации на стадии ее получения и ввода в информационную систему.

Однако, все приведенные подходы к пониманию термина "информационный риск" объединяет два обстоятельства: отсутствие комплексного системного взгляда на проблему и ясности понимания конечных результатов воздействия информационных рисков на предприятие.

Качественный анализ современных подходов к определению и характеристикам понятия «информационный риск» представлен в работах А.В. Шарапова [3]. 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» [3].

При этом указанное определение не затрагивает такое важное негативное явление, как нарушение авторского права на использование и распространение продукции интеллектуального труда, распространение заведомо ложной информации о предприятии, незаконное использование торговой или производственной марки. Тогда **информационный риск** – это возможность наступления случайного события, приводящего к нарушениям функционирования и снижению качества информации в информационной системе предприятия (ИСП), а также к неправомерному использованию или распространению информации во внешней среде, в результате которых наносится ущерб предприятию. Информационный риск оказывает отрицательное воздействие на результаты функционирования предприятия. Отметим, что это определение используются нами как наиболее полно характеризующие понятие «информационный риск» относительно нашего исследования и позволяющие рассматривать его с точки зрения и компьютерной и экономической безопасности.

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 [3].

Информация имеет ряд специальных свойств, входящих в состав ее качества. Их классификация приведена на рисунке [3].

Информационный риск вызывается внутренними или внешними причинами. Если причины информационного риска порождаются внутри предприятия, то такой

риск относится к внутренним. Внешним информационным риском считается риск, причины возникновения которого находятся за пределами предприятия.

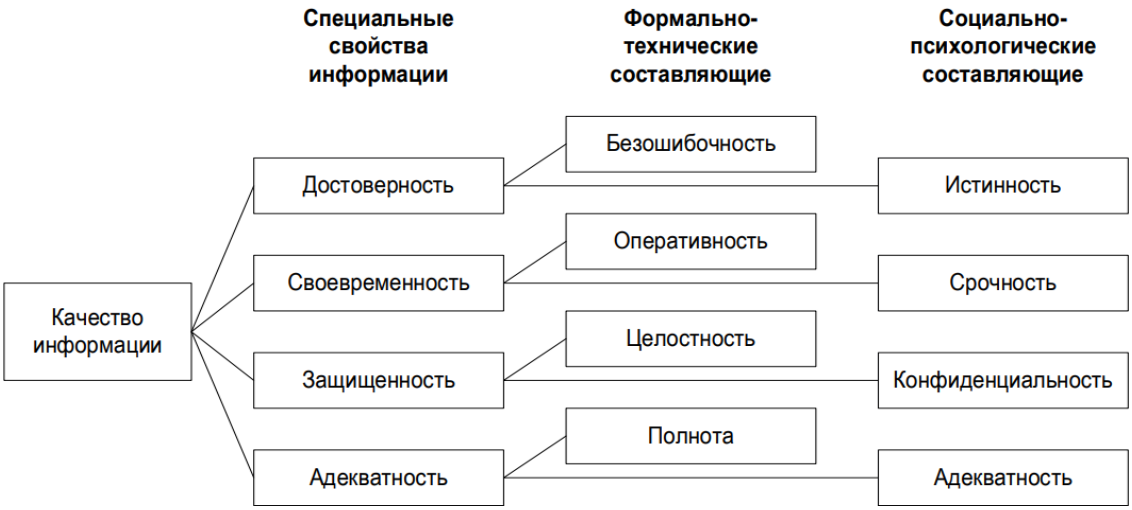

Рисунок. – Составляющие качества информации

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 [1] 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] (таблица).

Таблица. – 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

Основные этапы методики количественной оценки внутренних информационных рисков.

Для возможности проведения количественной оценки и построения риск-модели облачной среды необходимо решить следующие задачи.

1. Определить и описать возможные технические риски использования облачных сред в их взаимосвязи с уязвимостями и активами организации.

2. Сформировать перечень уязвимостей для каждого риска, построить для них базовые векторы системы общего учета уязвимостей (CVSS).

3. Разработать методику по оценке уровня риска. Показатели частоты и урона будут рассчитываться на основе показателей CVSS метрик: базовой, временной и инфраструктурной.

4. Определить риск-модель на основе полученных уровней влияния рассматриваемых уязвимостей. Группировка уязвимостей по принципу принадлежности одному уровню влияния позволит ввести новый показатель – сервисный уровень. Совокупное представление возможных сервисных уровней и интенсивности переходов между ними позволит прогнозировать уровни риска в определенный момент времени.

Основные этапы методики качественной оценки внутренних информационных рисков.

Главные задачи качественного подхода:

1) выявить и классифицировать возможные виды рисков, которые присущи проекту;

2) определить и описать причины и факторы, влияющие на уровень данных видов риска;

3) описать и дать оценку всех возможных последствий гипотетической реализации выявленных рисков;

4) предложить мероприятия по минимизации и (или) компенсации последствий, рассчитав стоимостную оценку этих мероприятий.

Результаты качественного анализа служат важной исходной информацией для осуществления количественного анализа. Факторы, влияющие на рост степени риска, можно условно разделить на объективные и субъективные. Объективные факторы непосредственно не зависят от самого проекта: это инфляция, конкуренция, политические и экономические кризисы, экология, налоги и т.д. Субъективные факторы характеризуют непосредственно данный проект или фирму: это производственный потенциал, техническое оснащение, уровень производительности труда, проводимая финансовая политика и т.д.

Целью обоих методик является понимание реальных рисков информационной безопасности компании, определение перечня актуальных угроз, а также выбор эффективных контрмер и средств защиты. Каждый метод оценки рисков

имеет свои преимущества и недостатки. Количественный метод требует значительно больше времени, так как каждому фактору риска присваивается конкретное значение. Однако в большинстве случаев дополнительная точность не требуется или просто не стоит лишних усилий. Например, если для оценки фактора риска надо потратить четыре месяца, а решение проблемы займет только два, ресурсы используются неэффективно.

Качественный метод позволяет проводить анализ за считанные минуты. Он позволяет выполнить оценку рисков быстрее, однако оценки и результаты носят более субъективный характер и не дают наглядного понимания ущерба, затрат и выгод от внедрения средств защиты информации. Выбор метода следует делать исходя из специфики конкретной компании и задач, поставленных перед специалистом.

Следует констатировать, что единой методики, по которой можно было бы определить количественную величину риска, на сегодняшний день не существует. Во-первых, это обусловлено отсутствием необходимого объема статистической информации о возможности возникновения какой-либо конкретной угрозы. Во-вторых, играет немаловажную роль тот факт, что определить величину стоимости конкретного информационного ресурса порой очень трудно.

Таким образом, снижение рисков информационной безопасности относится к одной из первоочередных задач бизнеса. Управление рисками, сокращение ущерба от их реализации помогают компании сохранить свое положение на рынке, конкурентное преимущество, избежать финансовых и репутационных издержек. Хорошей практикой для предотвращения инцидентов безопасности является использование комбинированных методик сочетающих как количественную оценку так и качественную.

ЛИТЕРАТУРА

6. Спильниченко В. К. Информационные риски в банкинге // Экономический журнал. – 2013. – № 3. – URL: https://cyberleninka.ru/article/n/informatsionnye-riski-v-bankinge (дата обращения: 30.05.2024).
7. Дьяконов Д. Страхование информационных рисков как метод защиты информации [Электронный ресурс]. – URL: http://www.amulet-group.ru/page.htm?id=30.
8. 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.
9. Царегородцев А.В., Логинова А.О., Блохина О.В. Методика количественной оценки риска информационной безопасности для облачной инфраструктуры организации [Электронный ресурс]. – URL: https://journal.mrsu.ru/wp-content/uploads/2018/08/tsaregorodtsev.pdf.