УДК 159.99

ОЦЕНКА И АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИТ-ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ

В.Е. СЕМЕНЕЦ, И. А. ШПАКОВ
(Представлено: канд. пед наук, доц. А. П. МАТЕЛЕНОК)

В статье обоснована необходимость проведения оценки и анализа рисков информационной безопасности ИТ-инфраструктуры организации с целью адаптации базового набора мер защиты. Проведен анализ методов количественной и качественной оценки рисков информационной безопасности, определен смешанный подход к оценке рисков как компромиссный между ними. Приведены примеры количественной и качественной оценки рисков информационной безопасности ИТ-инфраструктуры.

Риски информационной безопасности являются одними из самых значимых и вероятных рисков, с которыми сталкиваются современные организации. Информационные риски охватывают широкий спектр угроз и уязвимостей, которые могут негативно повлиять на информационные системы и данные организаций.

Термин «информационный риск» широко используется в научной литературе, однако в настоящее время не существует общепринятой трактовки этого понятия. Информационный риск (ИР) – это возможное событие, в результате которого несанкционированно удаляется, искажается информация, нарушается ее конфиденциальность или доступность. В представленном определении ИР используется как синоним понятия угроза безопасности информации. Управление такими информационными рисками сводится к защите информации. Представим определение, данное Комитетом организаций-спонсоров Комиссии Тредвея (The Committee of Sponsoring Organizations of the Treadway Commission, COSO): "Risk is defined by COSO as the possibility that events will occur and affect the achievement of strategy and business objectives". Отметим, что 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. На наш взгляд наиболее точное определение информационного риска – 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 организации. 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.

Информация имеет ряд специальных свойств, входящих в состав ее качества. Их классификация приведена на рисунке 1.1.

Рисунок 1.1. – Составляющие качества информации

Разработка методики оценки риска - достаточно трудоемкая задача. Во-первых, такая методика должна всесторонне описывать информационную систему, ее ресурсы, ее угрозы и уязвимости. Сложность заключается в том, чтобы построить максимально гибкую модель информационной системы, которую можно было бы настраивать в соответствии с реальной системой. Во-вторых, методика оценки рисков должна быть предельно прозрачна, чтобы владелец информации, использующий ее, мог адекватно оценить ее эффективность и применимость к своей конкретной системе.

Под оценкой и анализом рисков понимается процедура выявления факторов рисков и оценки их значимости. Анализ рисков включает оценку ИР и методы снижения рисков или уменьшения связанных с ним неблагоприятных последствий.

Анализ и оценку рисков можно подразделить на два взаимно дополняющих друг друга вида: качественный и количественный. Качественные методы оценки рисков не оперируют числовыми данными, представляя результат в виде описаний, сценариев угроз ИБ и рекомендаций. К основным недостаткам качественных методов оценки рисков можно отнести отсутствие числового представления результатов, невысокую точность и приближенный характер результатов [1]. С применением качественного подхода возможно учесть те риски, которые нельзя характеризовать количественно, с другой стороны, качественная оценка усложняет принятие точных решений по снижению рисков. Методы количественной оценки рисков ИБ используют фактические данные, которые можно измерить математически или с помощью других вычислительных методов. Количественные методы оценки рисков учитывают только те риски, что могут быть количественно выражены. Благодаря измеримости и воспроизводимости данных количественная оценка рисков является надежным и эффективным методом, но его недостатком является возможность игнорирования рисков, возникающих из нетехнических аспектов. Как качественная, так и количественная оценка являются ключевыми факторами успешной деятельности по управлению рисками, и обычно их используют совместно. Например, на этапе установления контекста риска первым используют качественный подход [2], выявляя приоритетные риски, которые после будут уточнены с помощью количественного подхода. Компромиссом между подходами качественной и количественной оценки может быть смешанный подход к оценке рисков, также называемый гибридной оценкой рисков. Смешанный подход объединяет качественный и количественный методы: например, путем перевода качественно определенного значения риска в количественный по соответствующей числовой шкале или наоборот. С использованием смешанного подхода к оценке рисков сохраняются достоинства обоих методов (точность оценок, полученных из количественного метода и возможность всестороннего анализа, получаемого с использованием качественного метода оценки) и нивелируются их недостатки[3].

Приведем один из примеров получения количественной оценки о состояни ИТ-инфраструктуры в учреждениях общего среднего образования получается путем математической обработки ответов на анкетные вопросы (каждому ответу анкеты поставлена в соответствие весовая величина(%)) и оценки защиты физического оборудования. После обработки полученных данных формируется отчет, фрагмент которого представлен в таблице 1.

Таблица 1

Риск	Последствия в случае наступления	Вероятность наступления (%)	Возможные меры защиты
Взлом паролей пользователей	Доступ к данным. Изменение данных. Копирование данных. Потеря репутации.	30	Установка комплексной системы защиты компьютерной сети, которую обеспечат специализированные программы, выявляющие все возможные угрозы безопасности и применяющие меры по борьбе с ними.
Разрушение данных из-за сбоя питания	Потеря данных. Сбой в работе системы.	15	Использование источников бесперебойного питания. Резервное копирование данных.
Утрата / порча данных (литературы, контрольных работ) по неосторожности	Потеря данных без возможности восстановления.	35	При загрузки новых данных воспользоваться помощью специалиста.
Раражение компьютерным вирусом IT - инфраструктуры	Заражение компьютерным вирусом. Потеря данных. Сбой в работе системы.	10	Установка лицензионных антивирусных программ. Соблюдение правил «сетевой гигиены».
…	…	…	…

Для получения качественной оценки о состоянии ИТ-инфраструктуры необходимо проанализировать защищенность и архитектуру построения информационной системы описывается и оценивается ИТ-инфраструктуры организации:

- все ресурсы, на которых хранится ценная информация;
- сетевые группы, в которых находятся ресурсы системы (то есть физические связи ресурсов друг с другом);
- отделы, к которым относятся ресурсы;
- виды ценной информации;
- ущерб для каждого вида ценной информации по трем видам угроз;
- бизнес-процессы, в которых обрабатывается информация;
- группы пользователей, имеющих доступ к ценной информации;
- класс группы пользователей;
- доступ группы пользователей к информации;
- характеристики этого доступа (вид и права);
- средства защиты информации;
- средства защиты рабочего места группы пользователей.

Таким образом, методика оценки и анализа информационных рисков ИТ-инфраструктуры организации должна содержать количественную и качественную составляющую. Она должна иметь возможность всесторонне описывать информационную систему, ее ресурсы, ее угрозы и уязвимости. При этом методика должна позволять владельцу информации или эксперту ее применяющему, адекватно оценить ее эффективность и применимость к конкретной системе. Риск реализации угрозы информационной безопасности в разработанной методике для каждого вида информации должен рассчитываться по трем основным угрозам: конфиденциальность, целостность и доступность и быть направленным на одну основную цель — идентификацию неприемлемых рисков и их своевременную обработку.

ЛИТЕРАТУРА

1. Минаков А. В. Оценка модели рисков информационной безопасности: характеристика, проблемы и перспективы // Экономика и бизнес: теория и практика. 2023. № 10–2 (104). С. 63–69.
2. Canbolat S., Elbez G., Hagenmeyer V. A new hybrid risk assessment process for cyber security design of smart grids using fuzzy analytic hierarchy processes // Automatisierungstechnik. 2023. № 71 (9). Pp. 779-788.
3. Харченко А. Ю., Харченко Ю. А. Анализ и определение рисков информационной безопасности // Вестник науки и образования. 2020. № 6–1 (84). С. 18–21.