УДК 004

УПРАВЛЕНИЕ РИСКАМИ В СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д. А. Исак, М. А. Ганжур
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Аннотация. Информационная безопасность является важным аспектом деятельности любого современного предприятия или организации. Конфиденциальная информация, хранящаяся и передаваемая внутри компании, может стать мишенью для злоумышленников, а ее утрата — привести к серьезным финансовым, юридическим и репутационным потерям. Риски информационной безопасности относятся к потенциальным угрозам или уязвимостям, которые зачастую приводят к утере или неправильному использованию конфиденциальных данных. Целью публикации является анализ различных типов рисков, существующих в области информационной безопасности, а также методов и стратегий, используемых для снижения их количества.

Ключевые слова: риск, информационная безопасность, контроль, мониторинг, управление рисками.

RISK MANAGEMENT IN INFORMATION SECURITY SYSTEM

Daniil A. Isak, Marina A. Ganzhur
Don State Technical University, (Rostov-on-Don, Russian Federation)

Abstract. Information security is an important aspect of the activities of any modern enterprise or organization. Confidential information stored and transmitted within the company can become a target for intruders, and its loss can lead to serious financial, legal and reputational losses. Information security risks refer to potential threats or vulnerabilities that often lead to the loss or misuse of confidential data. The work objective is to analyze various types of risks existing in the field of information security, as well as methods and strategies used to reduce their number.

Keywords: risk, information security, control, monitoring, risk management.

Введение. Безопасная работа информационной системы предполагает идентификацию, оценку, обработку, мониторинг на регулярной основе рисков выхода ее из строя, а также контроль за эффективностью и постоянным совершенствованием, своевременное предоставление руководству предприятия или организации полной и достоверной информации, необходимой для принятия управленческих решений по данному вопросу.

Риск нарушения работоспособности системы — это риск реализации угроз безопасности информации, которые обусловлены недостатками систем информационной безопасности, прикладного программного обеспечения, а также несоответствием указанных процессов деятельности организации [1].

Угроза — потенциально возможное событие, действие (воздействие), которое может нарушить бизнес-процесс или состояние защищенности актива.

Уязвимость — недостаток актива или мер его защиты, который может быть использован одной или несколькими угрозами [2].

Существуют следующие подпроцессы управления рисками информационной безопасности:

1. Идентификация риска кибербезопасности.
2. Оценка риска.
3. Обработка риска.
4. Сбор, регистрация и оценка потерь от событий риска.
5. Мониторинг и контроль.

6. Формирование отчетности.
7. Риск-культура [1, 3].

Необходимо оценить риск информационной безопасности для расчета и анализа последующих действий. Оценка должна быть независимой, чтобы иметь возможности для определения дополнительных рисковых зон, не выявленных во время разработки их подразделениями, непосредственно занимающимися данной проблемой.

Основная часть. Идентификация риска кибербезопасности. Для идентификации риска информационной безопасности могут использоваться различные инструменты (способы) его выявления. Например, анализ новых продуктов (процессов) включает в себя организацию и выполнение действий по идентификации рисков кибербезопасности (КБ) в них непосредственно при разработке или перед запуском.

При разработке новых продуктов (процессов) на предприятии осуществляется их анализ на предмет выполнения требований информационной безопасности. В случае выявления экспертом невыполненных требований информационной безопасности или отсутствия возможности их выполнения по объективным причинам (сроки, ресурсы) определяются возможные риски кибербезопасности в соответствии с картой присущих рисков (таблица 1).

Таблица 1

Карта рисков (составлено авторами)

Группа риска	Описание	Риск
Риск утечки конфиденциальной информации	Раскрытие конфиденциальной информации предприятия, а также нарушение обязательств по соблюдению конфиденциальности данных клиентов и работников	Утечки: – коммерческой тайны; – персональных данных; – иной охраняемой законом информации (например тайны связи, врачебной тайны и т. д.); – информации для внутреннего использования
Риск внешнего (внутреннего) мошенничества	Кибермошенничество, приводящее к хищению денежных средств клиентов или предприятия третьими лицами (работниками предприятия) с помощью информационных систем	Кибермошенничество – в каналах обслуживания клиентов; – с использованием автоматизированных систем (например дистанционное банковское обслуживание и иные финансовые системы и сервисы)
Риск нарушения целостности активов	Искажение или уничтожение информации при помощи информационных технологий и (или) неавторизованных действий третьих лиц либо работников предприятия	Модификация информации. Уничтожение информации
Риск недоступности активов	Нарушение работы систем (процессов) в результате намеренных действий третьих лиц и (или) работников предприятия	Недоступность систем компании. Сбой в работе систем информационной безопасности. Недоступность облачных сервисов

Риск несоответствия регуляторным требованиям	Невыполнение требований регуляторов в части компьютерной безопасности, приводящее к штрафам (предписаниям, приостановке деятельности предприятия)	Несоответствие требованиям законодательства в области защиты персональных данных. Несоответствие требованиям законодательства в области защиты объектов критической информационной инфраструктуры
		Несоответствие требованиям регулятора при работе со средствами криптографической защиты информации
		Несоответствие требованиям регулятора при работе с электронной подписью и удостоверяющими центрами и т. д.
Риск нарушения процессов управления КБ	Нарушение финансового состояния предприятия по кибербезопасности либо некорректное выполнение требований по безопасности	Невыполнение требований безопасности предприятия. Некорректное выполнение процессов безопасности

Владелец риска (эксперт безопасности) направляет полную информацию по идентифицированным рискам риск-менеджеру (работнику) для проведения оценки рисков [4].

Анализ актуальных угроз безопасности в инфраструктуре включает в себя организацию и выполнение деятельности по анализу ландшафта угроз, внешних источников, данных об уязвимостях в организации.

Риск-менеджер (работник) анализирует источники информации — TIP (при наличии), результаты инструментального контроля (сканирования) уязвимостей, экспертные заключения (внутренние, внешние аудиты), Банка данных угроз Федеральной службы по техническому и экспертному контролю (БДУ ФСТЭК), отраслевые порталы, новостные сайты и т. д. — с целью выявления потенциальных рисков безопасности информационной системы и оценки их применимости к инфраструктуре предприятия. На основании информации об активах и их состоянии определяется применимость рисков к инфраструктуре предприятия с целью дальнейшей оценки.

Риски кибербезопасности могут быть идентифицированы:

– при выполнении сотрудниками должностных обязанностей, в том числе при проведении регулярных и внеплановых проверок;

– при проведении аудита бизнес-процессов организации;

– при проведении внешнего независимого аудита [2].

Работники, проводившие внутренний аудит и выявившие риски, направляют полную информацию для проведения оценки риск-менеджеру (работнику).

При аудите бизнес-процессов организации, внешнего аудита в случае выявления рисков информационной безопасности системы результаты направляются риск-менеджеру (работнику).

Самооценка рисков — это инструмент идентификации риска, позволяющий через опрос работников структурных подразделений организации выявить и оценить риски, проанализировать эффективность и достаточность существующих контрольных процедур с целью предупреждения

угроз в будущем. Самооценка включает в себя организацию и деятельность по проведению периодической (ежегодной) самооценки риска.

В ходе проведения такой самооценки анализируются следующие аспекты:

– уровень риска. Общее воздействие риска (прямое и косвенное) на предприятие. Учитываются данные базы реализованных рисков, оценивается полнота данных с учетом внешних данных (внешней применимой статистики), влияние изменений процессов, внешней среды на уровень риска;

– эффективность контролей. Оценка степени эффективности и достаточности имеющихся в организации механизмов контроля риска;

– рейтинг риска. Определение общего рейтинга риска и эффективности контролей;

– стратегии реагирования на риск. Выбор стратегии реагирования на риск с учетом общего рейтинга риска, составление плана мероприятий с указанием сроков устранения рисков и ответственных.

Заключение (выводы). Риски информационной безопасности могут нести значительную угрозу современным предприятиям и организациям. Кибератаки, человеческие ошибки, физическая безопасность и социальная инженерия — это лишь некоторые из потенциальных уязвимостей, которые организации должны учитывать при разработке своих стратегий безопасности. Применение надежных мер кибербезопасности, комплексных программ обучения и повышения осведомленности сотрудников, а также внедрение систем контроля доступа — это эффективные и проверенные способы снижения рисков информационной безопасности. Если сотрудники будут сохранять бдительность и проявлять инициативу в устранении рисков информационной безопасности, организации смогут защитить себя от их потенциально разрушительных последствий.

Библиографический список

1. Бабаш, А. В. Информационная безопасность. Лабораторный практикум: учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. — Москва : КноРус, 2016. — 136 с.

2. Гафнер, В. В. Информационная безопасность : учебное пособие / В. В. Гафнер. — Ростов-на-Дону : Феникс, 2017. — 324 с.

3. Громов, Ю. Ю. Информационная безопасность и защита информации : учебное пособие / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. — Старый Оскол: ТНТ, 2017. — 384 с.

4. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт : моногр. / Л. Л. Ефимова, С. А. Кочерга. — Москва : Юнити-Дана, 2016. — 239 с.

Об авторах:

Исак Даниил Алексеевич, магистрант кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), momo11132@rambler.ru

Ганжур Марина Александровна, старший преподаватель кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), mganzhur@yandex.ru

About the Authors:

Isak, Daniil A., Master's degree student of the Computing Systems and Information Security Department, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), momo11132@rambler.ru

Ganzhur, Marina A., senior lecturer of the Computing Systems and Information Security Department, Don State Technical University (1, Gagarin sq., Rostov-on-Don, 344003, RF), mganzhur@yandex.ru