УДК 004.056

Какабьян К.С.,
студент
4 курс, факультет №1 Кибербезопасности и управления
Поволжский государственный университет
телекоммуникаций и информатики
Россия, г. Самара

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ПОДХОДЫ И МЕТОДЫ

Аннотация: *В современном мире всё больше организаций и частных лиц сталкиваются с проблемами в области информационной безопасности. С каждым годом угрозы становятся более сложными и утонченными, и организации должны принимать меры, чтобы защитить свою конфиденциальную информацию от киберпреступников. В этой статье рассматриваются подходы и методы анализа рисков в информационной безопасности, которые помогут организациям определить потенциальные угрозы и принять соответствующие меры для их предотвращения.*

Ключевые слова: *методы анализа, управление рисками, риски, угрозы, уязвимости, информационная безопасность.*

INFORMATION SECURITY RISK ANALYSIS: APPROACHES AND METHODS

Abstract: *In today's world, more and more organizations and individuals are facing information security challenges. Every year, threats become more complex and sophisticated, and organizations must take measures to protect their confidential information from cybercriminals. This article discusses approaches and*

methods for analyzing risks in information security that will help organizations identify potential threats and take appropriate actions to prevent them.

Keywords: *analysis methods, risk management, risks, threats, vulnerabilities, information security.*

Анализ рисков в информационной безопасности — это процесс идентификации, оценки и управления рисками, связанными с конфиденциальностью, целостностью и доступностью информации. Целью анализа рисков является выявление потенциальных угроз для информационной безопасности и разработка стратегии для их предотвращения.

Подходы к анализу рисков

Существует несколько подходов к анализу рисков в информационной безопасности. Рассмотрим некоторые из них.

1. Качественный анализ рисков (Qualitative Risk Analysis)

Качественный анализ рисков — это метод, основанный на экспертном мнении. Он используется для определения вероятности наступления угроз и степени их воздействия на организацию. Для проведения квалифицированного анализа рисков используются определенные методы, такие как SWOT-анализ (анализ сильных и слабых сторон, возможностей и угроз) и PESTLE-анализ (анализ политических, экономических, социальных, технологических, правовых и экологических факторов). Квалифицированный анализ рисков позволяет оценить вероятность наступления угроз и определить их воздействие на организацию.

2. Количественный анализ рисков (Quantitative Risk Analysis)

Количественный анализ рисков — это метод, основанный на математических моделях. Он используется для определения вероятности наступления угроз и

количественной оценки их воздействия на организацию. Для проведения количественного анализа рисков используются различные математические методы, такие как анализ Монте-Карло, анализ рисков в проектах и другие. Количественный анализ рисков позволяет более точно определить вероятность наступления угроз и их воздействие на организацию.

3. Комбинированный анализ рисков (Combined Risk Analysis)

Комбинированный анализ рисков — это метод, который объединяет количественный и качественный анализ рисков. Он используется для более точного определения вероятности наступления угроз и их воздействия на организацию. Для проведения комбинированного анализа рисков используются как математические модели, так и экспертные оценки. Комбинированный анализ рисков позволяет получить более точную и надежную оценку рисков.

Методы анализа рисков

Основными методами анализа рисков в информационной безопасности являются:

1. Анализ уязвимостей (Vulnerability Analysis) — это метод, который используется для определения уязвимостей в системе безопасности организации. Для проведения анализа уязвимостей используются различные инструменты и технологии, такие как сканеры уязвимостей, тестирование на проникновение и другие. Метод анализа уязвимостей позволяет выявить уязвимости в системе безопасности и принять меры для их устранения.

2. Анализ угроз (Threat Analysis) — это метод, который используется для определения потенциальных угроз для системы безопасности организации. Для проведения анализа угроз используются различные методы, такие как анализ требований к безопасности, анализ критических узлов и другие. Метод

анализа угроз позволяет выявить потенциальные угрозы для системы безопасности и принять меры для их предотвращения.

3. Анализ рисков в проектах (Project Risk Analysis) — это метод, который используется для определения рисков и их воздействия на выполнение проекта. Для проведения анализа рисков в проектах используются различные методы, такие как метод дерева решений, анализ событий и другие. Метод анализа рисков в проектах позволяет определить риски, связанные с проектом, и принять меры для их устранения.

4. Анализ воздействия рисков (Impact Analysis) — это метод, который используется для определения меры воздействия рисков на организацию. Для проведения анализа воздействия рисков используются различные методы, такие как анализ потерь, анализ воздействия на бизнес-процессы и другие. Метод анализа воздействия рисков позволяет определить воздействие рисков на организацию и принять меры для их минимизации.

5. Анализ и управление рисками (Risk Management Analysis) — это метод, который используется для определения эффективности системы управления рисками в организации. Для проведения анализа управления рисками используются различные методы, такие как анализ процессов управления рисками, анализ компетенции сотрудников и другие. Метод анализа управления рисками позволяет определить эффективность системы управления рисками в организации и в дальнейшем совершенствовать её.

Применение методов анализа рисков

Рассмотрим несколько примеров применения методов анализа рисков в информационной безопасности.

1. Анализ угроз в компьютерной сети.

При анализе угроз в компьютерной сети используются методы анализа угроз и анализа уязвимостей. Например, проводится анализ возможных угроз, таких

как вирусы, черви, несанкционированный доступ и другие. После этого проводится анализ уязвимостей компьютерной сети, который позволяет выявить уязвимые места в системе безопасности. На основе результатов анализа рисков принимаются меры по устранению уязвимостей и предотвращению угроз.

2. Анализ рисков при разработке программного обеспечения.

При разработке программного обеспечения используются методы анализа рисков, чтобы определить возможные риски и принять меры для их устранения. Например, проводится анализ возможных ошибок программного кода, который может привести к некорректной работе программы или нарушению безопасности данных. После этого принимаются меры по устранению выявленных рисков.

3. Анализ рисков при выборе поставщика услуг информационной безопасности.

При выборе поставщика услуг информационной безопасности проводится анализ рисков, связанных с данным поставщиком. Например, проводится анализ квалификации сотрудников, наличия необходимых сертификатов и лицензий. На основе результатов анализа рисков принимается решение о выборе наиболее подходящего поставщика услуг информационной безопасности.

Заключение

Методы анализа рисков являются важным инструментом в области информационной безопасности. Они позволяют определить риски, связанные с информационной безопасностью, и принять меры для их устранения.

Важно понимать, что анализ рисков — это процесс, который должен проводиться регулярно и включать в себя все аспекты информационной

безопасности. Только так можно обеспечить защиту информации и минимизировать возможные риски.

Использованные источники:

1. Нестеров С.А. Основы информационной безопасности: учебное пособие — 3-е изд., стер. — Санкт-Петербург : Лань, 2017. — 324 с.
2. Маслова М. А. Анализ и определение рисков информационной безопасности // Научный результат. Информационные технологии. 2019. № 1, С. 31-37.
3. Петренко С.А., Симонов С.В. Управление информационными рисками. Экономически оправданная безопасность. Москва, ДМК Пресс, 2004, 392 с.
4. Вострецова Е.В. Основы информационной безопасности : учебное пособие для студентов вузов — Екатеринбург: Уральский федеральный университет, 2019. - 204 с.
5. Шарапов А.В. Проблема определения понятия информационных рисков. Безопасность информационных технологий, 2010, № 2, С. 44–48.