УДК 004

Е. В. Кошелев

ПОДХОДЫ К ОЦЕНКЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Информационная безопасность стала важнейшей областью в современном мире, так как информационные системы играют ключевую роль в жизни организаций и общества в целом. С развитием технологий и расширением сферы цифровизации, ростом объема хранимой и обрабатываемой информации, а также появлением новых угроз, вопросы оценки и управления рисками информационной безопасности стали более актуальными и сложными. Вот несколько ключевых аргументов, подчеркивающих актуальность данной темы:

1. Увеличение объема данных. Различные государственные и негосударственные, коммерческие и некоммерческие организации хранят и обрабатывают огромные объемы информации, включая личные данные клиентов, бизнес-процессы и государственные тайны. Угрозы по утечке и недоступности этой информации стали значительными.

2. Развитие киберугроз. С появлением киберпреступников, хакерских групп и государственных кибератак, уровень угроз информационной безопасности значительно возрос. Оценка этих рисков стала важной задачей для защиты информации.

3. Законодательные требования. Множество стран, в том числе и Россия, ввели строгие нормативы и законы, обязывая организации соблюдать стандарты информационной безопасности и сообщать о нарушениях. Оценка рисков помогает организациям соответствовать этим требованиям.

4. Повышение осведомленности. Осознание важности информационной безопасности растет среди бизнес-лидеров и общества. Оценка рисков помогает лучше понимать уязвимости и разрабатывать эффективные стратегии защиты.

5. Технологический прогресс. Постоянное развитие информационных технологий создает новые возможности, но также усиливает риски. Оценка рисков позволяет адаптироваться к этим изменениям.

Исходя из вышеперечисленных факторов, понимание и применение подходов к оценке рисков информационной безопасности становятся неотъемлемой частью деятельности организаций, государственных институтов и частных лиц. Актуальность этой темы подчеркивает

необходимость постоянного исследования и разработки новых методов и подходов для эффективного управления рисками в сфере информационной безопасности.

Риском в сфере информационной безопасности называется потенциальная возможность понести убытки из-за нарушения безопасности информационной системы.

В статье В. Н. Максименко и Е. В. Ясюка под названием «Основные подходы к анализу и оценке рисков информационной безопасности» [1] говорится, что идеи управления рисками в сфере информационной безопасности, возникли еще в 1970-х годах, когда была разработана модель модель Клементса–Хоффмана (рис. 1) [2].

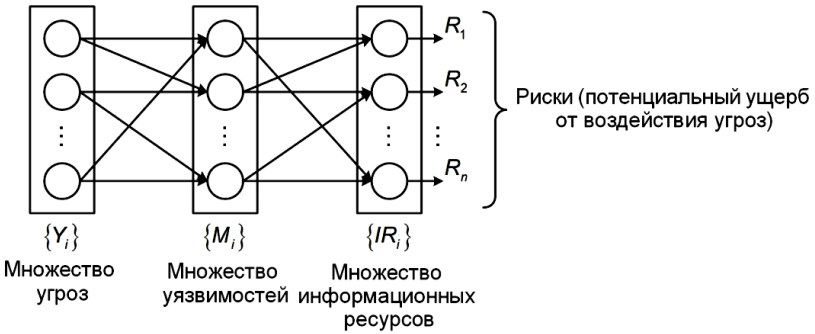

Рис. 1. Общая схема формирования рисков информационной безопасности (модель Клементса–Хоффмана)

Риск для информационной безопасности в модели Клементса–Хоффмана рассчитывается по формуле:

$$\text{Риск} = \text{Угроза} * \text{Уязвимость} * \text{Информационный ресурс}. \quad (1)$$

Из общей модели Клементса–Хоффмана можно сформировать модель с полным перекрытием (рис. 2). Данная модель описывает систему, в которой имеются средства защиты на каждый возможный путь проникновения [3].

Все известные методики оценки и анализа рисков можно разбить на три группы.

Качественные методы оценки рисков информационной безопасности:

1. Экспертные оценки – основаны на мнениях экспертов, которые оценивают вероятность и последствия рисков на основе своего опыта и знаний.

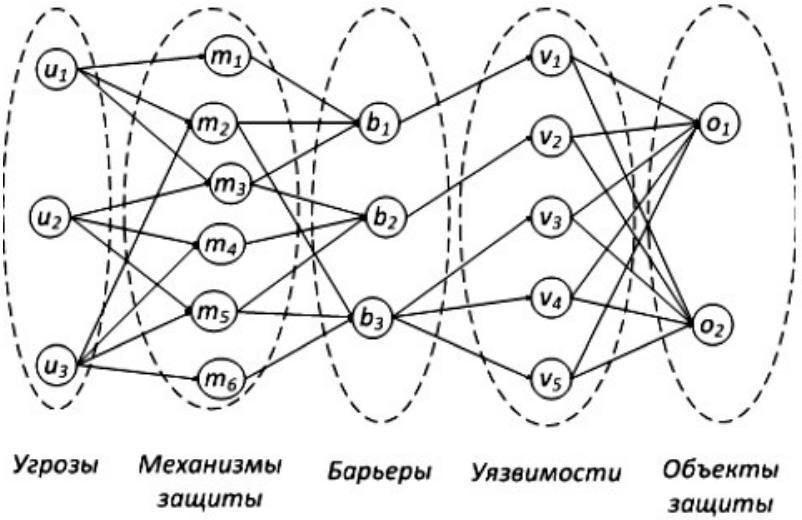

Рис. 2. Модель безопасности с полным перекрытием

2. Матрицы рисков – позволяют оценивать риски с использованием категорий, как правило, на основе цветовой кодировки или числовых шкал.

3. SWOT-анализ – используется для определения сильных и слабых сторон, возможностей и угроз в контексте информационной безопасности.

Количественные методы оценки рисков информационной безопасности:

1. Вероятностный анализ – основан на математических моделях и статистике, позволяет количественно измерить вероятность и воздействие рисков.

2. Методы Монте-Карло – используются для моделирования вероятностей событий и их воздействия, учитывая случайные факторы.

3. Экономический анализ рисков – учитывает финансовые аспекты, позволяя количественно оценить потенциальные потери и выгоды.

Качественные методы оценки рисков информационной безопасности ориентированы на экспертное мнение и качественные характеристики (например, по шкале «высокий», «средний», «низкий»), в то время как количественные методы используют численные данные и математические модели для более точной количественной оценки

рисков. Комбинирование этих методов может обеспечить более полное понимание и управление рисками информационной безопасности.

Методы смешанной оценки рисков информационной безопасности:

1. Анализ важности и вероятности – комбинируют качественные и количественные аспекты, учитывая как вероятность, так и важность рисков, чтобы определить их приоритеты.

2. FMEA (Failure Modes and Effects Analysis) – оценивает риски с использованием качественных и количественных данных, а также определяет последствия сбоев и их вероятность.

Методы смешанной оценки информационной безопасности позволяют учесть разные аспекты рисков, включая их качественное и количественное измерение, что способствует более глубокому и комплексному анализу безопасности и помогает в разработке более эффективных стратегий управления рисками.

С постоянно возрастающей сложностью угроз и уязвимостей, программные продукты для оценки рисков информационной безопасности стали необходимостью. Ниже приведен перечень нескольких таких программных решений, которые помогают выявлять уязвимости, анализировать безопасность сети и приложений, и обеспечивать надежную защиту от потенциальных угроз. Они представляют собой мощные инструменты в борьбе с угрозами и обеспечении цифровой безопасности организаций.

1. Nessus – этот инструмент обеспечивает сканирование уязвимостей, помогая выявить потенциальные уязвимости в сетевых устройствах и приложениях.

2. Qualys – предоставляет облачное решение для оценки безопасности, сканируя сети на наличие уязвимостей и предоставляя рекомендации по их устранению.

3. Burp Suite – популярное приложение для тестирования на проникновение, которое позволяет обнаруживать уязвимости в веб-приложениях.

4. OpenVAS – этот открытый источник программного обеспечения предоставляет возможности сканирования уязвимостей и оценки безопасности сети.

5. Wireshark – данный инструмент является мощным средством анализа сетевого трафика, позволяя выявлять аномалии и потенциальные угрозы.

6. Snort – является системой обнаружения вторжений и позволяет мониторить сетевой трафик на предмет злонамеренной активности.

7. Metasploit – этот инструмент предоставляет широкий спектр эксплойтов и уязвимостей для тестирования на проникновение и обеспечивает информацию о безопасности.

8. Nmap – этот инструмент для сканирования сети обнаруживает активные устройства и службы на сети, помогая выявить потенциальные уязвимости.

9. Acunetix – предоставляет веб-сканер для обнаружения уязвимостей в веб-приложениях и предоставляет детальные отчеты о безопасности.

10. SolarWinds Security Event Manager – решение для управления журналами и мониторинга безопасности, обнаруживающее и реагирующее на аномалии в сети.

Эти программные продукты помогают организациям оценивать риски информационной безопасности, обнаруживать уязвимости и обеспечивать более надежную защиту от потенциальных угроз.

Однако важно помнить, что оценка рисков – это не статичный процесс, а непрерывный цикл, который требует постоянного обновления и адаптации к изменяющимся условиям и угрозам.

Список литературы

1. Максименко, В. Н. Основные подходы к анализу и оценке рисков информационной безопасности / В. Н. Максименко, Е. В. Ясюк // Экономика и качество систем связи. – М. : Изд-во ЗАО «Национальный институт радио и инфокоммуникационных технологий». – 2017. – Вып. 2(4). – С. 42 – 48.

2. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт / В. И. Васильев, А. М. Вульфин, М. Б. Гузаиров и др. // Информационные технологии. – 2020. – Вып. 4. – С. 213 – 221.

3. Янников, И. М. Особенности реализации системы оценки защищенности критически важных и потенциально опасных объектов на основе метода Клементса–Хоффмана / И. М. Янников, М. В. Телегина // Интеллектуальные системы в производстве. – 2018. – Вып. 4, Т. 16. – С. 169 – 175.

Кафедра «Информационные системы и защита информации»
ФГБОУ ВО «ТГТУ»