ОЦЕНКА РИСКОВ ОБЕСПЕЧЕНИЯ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Студент ФМО-24, Уколов Александр Александрович.

Научный руководитель д.э.н., профессор Салманов О.Н.

«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА» - ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГЕОДЕЗИИ И КАРТОГРАФИИ»

Аннотация. В статье рассматриваются подходы к оценке рисков корпоративной безопасности предприятия как основы построения эффективной системы защиты активов, информации и деловой репутации. Раскрыта сущность корпоративной безопасности, приведена классификация угроз и уязвимостей, описан риск-ориентированный подход к управлению безопасностью. Предложен алгоритм оценки рисков с использованием качественных и полуколичественных методов (матрица вероятности–ущерба, ранжирование, риск-профиль), а также рассмотрены меры реагирования: предотвращение, снижение, передача и принятие риска. Сделан вывод о необходимости интеграции оценки рисков в систему корпоративного управления и непрерывного мониторинга.

Ключевые слова: корпоративная безопасность, риск, угрозы, уязвимости, оценка рисков, матрица рисков, риск-ориентированный подход, управление рисками.

CORPORATE SECURITY RISK ASSESSMENT

Student of FMO-24, Ukolov Alexander Alexandrovich

Doctor of Economic Sciences, Professor Salmanov O.N.

Leonov Technological University named after Twice Hero of the Soviet Union, Pilot-Cosmonaut A.A. Leonov — Branch of the Federal State Budgetary

Educational Institution of Higher Education Moscow State University of Geodesy and Cartography

Abstract. The article examines approaches to assessing corporate security risks of an enterprise as the basis for building an effective system for protecting assets, information, and business reputation. The essence of corporate security is revealed, a classification of threats and vulnerabilities is provided, and a risk-oriented approach to security management is described. An algorithm for risk assessment using qualitative and semi-quantitative methods (probability-damage matrix, ranking, risk profile) is proposed, and response measures are considered: prevention, reduction, transfer, and acceptance of risk. The conclusion is made about the necessity of integrating risk assessment into the corporate governance system and continuous monitoring.

Keywords: corporate security, risk, threats, vulnerabilities, risk assessment, risk matrix, risk-oriented approach, risk management.

Современные предприятия функционируют в условиях высокой неопределённости, обусловленной усложнением цепочек создания ценности, цифровизацией управленческих и производственных процессов, ростом регуляторной нагрузки и усилением конкуренции. В данных условиях корпоративная безопасность трансформируется из вспомогательной охранной функции в системный фактор устойчивости организации. Практика показывает, что корпоративные инциденты (мошенничество, утечки данных, нарушения комплаенса, простои критичных ИТ-сервисов, инциденты физической безопасности) способны порождать мультипликативные последствия: прямые финансовые потери дополняются косвенными издержками, репутационным ущербом и снижением доверия контрагентов.

Вследствие ограниченности ресурсов предприятия возникает необходимость выбора приоритетов в сфере безопасности. Данный выбор рационально осуществлять на основе риск-ориентированного подхода, предполагающего систематическую идентификацию угроз, оценку

вероятности их реализации, определение тяжести последствий и принятие управленческих решений по обработке рисков. Таким образом, оценка рисков корпоративной безопасности представляет собой методологическую основу формирования и оптимизации защитных мер, а также обоснования затрат на безопасность.

Корпоративная безопасность в научно-прикладной трактовке может быть определена как совокупность организационных, правовых, кадровых, технических и информационных мероприятий, направленных на обеспечение защищённости активов предприятия, устойчивости бизнес-процессов и сохранения деловой репутации. Важным признаком корпоративной безопасности является межфункциональный характер: она затрагивает финансово-экономическую, информационную, кадровую, правовую, комплаенс- и физическую составляющие.

Формирование корпоративной безопасности целесообразно рассматривать в логике системного подхода: предприятие выступает сложной социально-экономической системой, в которой риск реализуется через взаимодействие внешней среды и внутренних характеристик (структуры управления, процессов, культуры, технологий) [2, с.65].

В контексте корпоративной безопасности риск представляет собой сочетание вероятности реализации угрозы и величины возможного ущерба. Концептуально риск формируется через триаду:

— угроза — потенциальное событие или действие, способное причинить ущерб;

— уязвимость — характеристика объекта, повышающая вероятность реализации угрозы;

— последствия — измеримые результаты инцидента для предприятия.

Отметим, что последствия в корпоративной безопасности не сводимы к финансовым потерям. Они включают также правовые санкции, снижение

операционной устойчивости, ухудшение репутации и утрату доверия стейкхолдеров. Следовательно, при оценке риска требуется учитывать многокритериальный характер ущерба.

Риск-ориентированный подход обеспечивает переход от реактивной модели («реагирование на инциденты») к проактивной («предупреждение и снижение вероятности»). Он позволяет:

1. Устанавливать приоритеты защиты в условиях ограниченных ресурсов;
2. Обосновывать выбор мер безопасности экономической логикой;
3. Согласовывать деятельность по безопасности со стратегическими целями предприятия;
4. Оценивать эффективность внедрённых контролей посредством динамики риск-показателей [6, с. 29].

Классификация угроз является необходимым условием формализации оценки рисков и построения риск-карты. В прикладных исследованиях целесообразно выделять следующие группы угроз.

1.Экономические и финансовые угрозы: внутреннее и внешнее мошенничество, конфликт интересов, злоупотребления полномочиями, манипуляции с финансовой отчётностью и платежами.

Уязвимости: недостаточная сегрегация обязанностей, слабый внутренний контроль, непрозрачность закупок, низкая дисциплина исполнения регламентов.

2. Информационные и киберугрозы: несанкционированный доступ, утечки конфиденциальных сведений, вредоносное ПО, атаки на доступность.

Уязвимости: слабая аутентификация и управление доступами, отсутствие сегментации сети, недостаточный уровень актуализации систем, дефицит обучения персонала.

3. Кадровые угрозы: инсайдерские действия, ошибки персонала, снижение лояльности, высокая текучесть кадров.

Уязвимости: дефицит процедур проверки при найме, слабая адаптация, недостаток обучения, непрозрачность мотивации, неразвитая культура безопасности [1, с.77].

4. Правовые и комплаенс-риски: нарушения законодательства, санкции регуляторов, судебные споры, коррупционные проявления.

Уязвимости: недостаточность договорной работы, отсутствие комплаенс-процедур, слабая документация, неформализованные правила взаимодействия с контрагентами.

5. Физические угрозы: проникновения, хищения, повреждение имущества, аварии и ЧС.

Уязвимости: низкий уровень контроля доступа, устаревшие технические средства охраны, отсутствие планов реагирования и тренировок.

Данная классификация позволяет построить «каталог угроз» и применять его как основу для разработки риск-сценариев.

Процедура оценки рисков должна быть воспроизводимой, сопоставимой по периодам и обеспечивать управленческую интерпретируемость результатов. В практике корпоративной безопасности часто отсутствует достаточная статистика инцидентов; поэтому наиболее применим полуколичественный подход, сочетающий экспертную оценку с формализованными шкалами.

К принципам оценки рисков относятся:

— системность и полнота охвата активов;

— доказательность (опора на данные инцидентов, аудитов, интервью);

— сопоставимость (единые шкалы вероятности и ущерба);

— ориентация на принятие решений (связь риска и мер контроля).

Методология оценки рисков корпоративной безопасности включает в себя несколько этапов:

Этап 1. Определение контекста и критериев.

На данном этапе формируется рамка оценки: определяются активы и процессы, включаемые в анализ, горизонты планирования и критерии ущерба. Практически значимо заранее установить параметры «допустимого риска» (risk appetite), отражающие готовность предприятия принимать определённый уровень угроз при сохранении экономической целесообразности.

Этап 2. Идентификация активов и построение риск-сценариев.

Ключевым методическим шагом является переход от абстрактных угроз к конкретным риск-сценариям вида: актив → угроза → уязвимость → инцидент → последствия.

Источники идентификации:

— ретроспективный анализ инцидентов и потерь;

— внутренние аудиты, обследование процессов;

— интервью с владельцами процессов и ответственными за безопасность;

— анализ контрагентов и логистических цепочек;

— технические обследования (ИТ-контуры, контроль доступа, инфраструктура).

Этап 3. Оценка вероятности и последствий.

Для обеспечения сопоставимости применяются шкалы, например 1–5.

Вероятность (P): от «практически исключено» до «очень вероятно».

Последствия (I): от «незначительные» до «критические».

Тогда интегральный показатель риска определяется как:

$$R = P \times I$$

При необходимости многокритериальности ущерба используется агрегирование: выбирается максимальная оценка по критериям (финансовые потери, правовые санкции, репутация, простои) либо применяется взвешивание. В условиях ВКР допустимо обосновать выбор агрегирования как методическое допущение, повышающее надёжность интерпретации.

Этап 4. Ранжирование и риск-профиль (матрица рисков).

Риски ранжируются по значению R и размещаются в матрице «вероятность–последствия». Матрица позволяет выделить зоны риска (критическая, значимая, умеренная, низкая) и сформировать приоритетный перечень мероприятий. Итогом этапа является риск-профиль предприятия — совокупность наиболее существенных риск-сценариев, требующих управленческого реагирования.

Этап 5. Обработка риска и выбор контролей

Управление риском предполагает выбор одной из стратегий:

— избежание (устранение деятельности/условий, порождающих риск);

— снижение (внедрение контролей: организационных, технических, кадровых);

— передача (страхование, договорная ответственность, аутсорсинг);

— принятие (если риск укладывается в допустимый уровень).

Рациональность мер оценивается через соотношение «стоимость контроля — ожидаемое снижение ущерба». Научная значимость данного положения состоит в том, что безопасность рассматривается как экономическая категория: её эффективность определяется не максимизацией контроля, а оптимизацией риска при заданных ресурсных ограничениях [3, с.10].

Этап 6. Мониторинг и пересмотр.

Оценка рисков должна носить циклический характер. Основания для пересмотра:

— изменения организационной структуры и процессов;

— внедрение новых ИТ-решений;

— смена контрагентов и логистических схем;

— существенные инциденты и выявленные нарушения;

— изменения нормативной среды.

Практическая применимость методики обеспечивается формированием документов корпоративной безопасности.

Реестр рисков целесообразно оформлять таблицей со следующими полями:

— риск-сценарий и затронутый актив;

— источник угрозы и уязвимость;

— оценка вероятности, последствий, интегрального риска;

— существующие и рекомендуемые меры контроля;

— ответственные лица и сроки внедрения.

Карта рисков (risk map) визуализирует распределение рисков по матрице, обеспечивая управленческую наглядность и облегчая коммуникацию с руководством [5, с.106].

Практика внедрения риск-ориентированного подхода показывает, что его результативность определяется не только корректностью расчётов, но и институциональными условиями:

— закреплением ответственности (владельцы рисков и владельцы процессов);

— наличием внутреннего контроля и комплаенс-процедур;

— регламентированностью управления доступами и полномочиями;

— культурой безопасности и регулярным обучением персонала;

— информационной поддержкой (инцидент-менеджмент, журналы событий, аналитика) [4, с. 362].

Следовательно, оценка рисков выступает не самостоятельной процедурой, а элементом системы корпоративного управления, обеспечивающим согласованность между целями бизнеса и задачами защиты.

Оценка рисков обеспечения корпоративной безопасности предприятия является методологически обоснованным и управленчески значимым инструментом повышения устойчивости организации. Риск-ориентированный подход позволяет систематизировать угрозы и уязвимости,

сформировать риск-профиль предприятия, определить приоритеты защитных мероприятий и обеспечить обоснование затрат на безопасность. Наиболее применимой в условиях ограниченной статистики является полуколичественная методика, основанная на шкалах вероятности и последствий, риск-матрице и реестре рисков.

Перспективным направлением развития корпоративной безопасности следует считать интеграцию оценки рисков с системами внутреннего контроля, комплаенса и непрерывного мониторинга, что обеспечивает переход к циклической модели управления безопасностью и повышает адаптивность предприятия к изменяющейся среде.

Список литературы:

1. Балалыкин Н. Д. Оценка внешних угроз экономической безопасности хозяйствующих субъектов на примере ООО «Компания Металл Профиль» // Молодой ученый. — 2022. — № 47 (442). — С. 75–79.

2. Минаков Д. А. Оценка модели рисков информационной безопасности: характеристика проблемы и перспективы развития // Экономика и бизнес: теория и практика. — 2023. — № 10-2 (104). — С. 63–69.

3. Головкова Е. А., Котанджян А. В., Загребина А. А. Риски экономической безопасности организации // Вектор экономики. — 2024. — № 4. — 10 с.

4. Николаенко В. С. Комплаенс-риски эксплуатации ИТ-продуктов // Стратегические решения и риск-менеджмент. — 2024. — Т. 15. — № 4. — С. 360–367.

5. Гурина Л. А. Оценка рисков кибербезопасности энергетического сообщества микросетей // Вопросы кибербезопасности. — 2024. — № 1. — С. 101–107.

6. Прокуда М. В. Основные подходы к анализу и оценке рисков информационной безопасности: состояние и перспективы развития в

России // Актуальные исследования. — 2025. — № 42 (277). — Ч. I. — С. 26–30.