СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ КОМПАНИИ

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 рассмотрены понятия рисков и угроз в области обеспечения корпоративной безопасности компании. Определены угрозы корпоративной безопасности компании и их характер, рассмотрены принципы управления рисками. Предложены базовые действия по управлению корпоративной безопасностью компании. Обоснована необходимость создания системы управления рисками корпоративной безопасности.

Ключевые слова: корпоративная безопасность, риски и угрозы, управление рисками, реагирование и минимизация ущерба, методы управления рисками.

THE COMPANY'S CORPORATE SECURITY RISK MANAGEMENT SYSTEM

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: This article examines the concepts of risks and threats in the area of corporate security. It identifies threats to corporate security and their nature, and discusses risk management principles. Basic steps for managing corporate security are proposed, and the need for a corporate security risk management system is substantiated.

Keywords: Corporate security, risks and threats, risk management, response and damage minimization, risk management methods

В современном мире, где технологии развиваются с неимоверной скоростью, а бизнес-среда становится все более конкурентной и динамичной, корпоративная безопасность выходит на первый план в стратегии управления каждой компанией. Защита бизнеса – это не просто вопрос предотвращения финансовых потерь или утечки информации; это комплексная система мер, направленных на обеспечение устойчивости организаций в условиях неопределенности [1].

Корпоративная безопасность включает в себя множество аспектов – от физической охраны объектов до цифровой защиты информации, от правового обеспечения до формирования корпоративной культуры, ориентированной на безопасность. Эффективная стратегия защиты бизнеса должна учитывать не только внешние угрозы, такие как кибератаки, политический кризис, природные явления и техногенные аварии, коррупцию, но и внутренние риски, включая недовольство сотрудников и потенциальные конфликты интересов, неэффективное управление и неправильное использование технических средств [2]. Проблема обеспечения корпоративной безопасности является актуальной для любой компании вне зависимости от ее отраслевой принадлежности, формы собственности, размера и оборота.

Принципы корпоративной безопасности

Чтобы построить эффективную систему корпоративной безопасности, нужно помнить о главных основополагающих принципах[1]:

1. Комплексность: стратегия безопасности должна охватывать все направления и структурные подразделения компании: от рядовых сотрудников до топ-менеджеров. У каждого специалиста должна быть четкая инструкция и понимание своих действий для предотвращения рисков или минимизации ущерба от них. Важно обеспечить и наладить полное взаимодействие как между внутренними подразделениями компании, так и с внешними организациями, способными оказать помощь в решении вопросов безопасности.

2. Системность: необходимо рассматривать корпоративную безопасность как часть общей стратегии управления компанией, обеспечить эффективный контроль за системой защиты с гарантией максимальной безопасности.

3. Адаптивность: система должна быть гибкой и способной к быстрой реакции на изменения внешней среды.

4. Законность: безопасность должна обеспечиваться в рамках действующего законодательства, все применяемые методы и стратегии должны строго соответствовать нормам закона.

Ключевыми аспектами корпоративной безопасности являются управление рисками, соблюдение нормативных требований и обеспечение конфиденциальности информации. Данная область деятельности требует комплексного подхода и интеграции различных методов и технологий для устранения угроз и минимизации потенциального ущерба [3].

Важно понимать, что в условиях глобализации и интеграции новых технологий, риски становятся более сложными и разнообразными. Это обязывает компании адаптировать свои подходы к безопасности, внедряя инновационные решения и развивая комплексные программы, которые помогают не только выявлять и нейтрализовать угрозы, но и минимизировать их последствия. Главной задачей для обеспечения корпоративной безопасности предприятия является правильная оценка риска предполагаемой угрозы.

Для начала рассмотрим какие виды угроз существуют и классифицируем их. Под угрозами безопасности компании подразумеваются факторы и процессы, которые представляют или могут представлять опасность для успешного функционирования компании, её будущего потенциала, а также мешающие выполнению производственных и социальных функций [1].

Характер проявления угроз безопасности предприятия определяется по следующим параметрам и направлениям:

По месту возникновения:

- Внутренние угрозы: связаны с процессами, происходящими внутри предприятия (примеры: кражи, мошенничество, корпоративный шпионаж, саботаж, уход ключевых сотрудников, ошибки персонала, поломка оборудования) [2].

- Внешние угрозы: возникают за пределами предприятия (примеры: рейдерские атаки, недобросовестная конкуренция, действия конкурентов (промышленный шпионаж, переманивание персонала), кибератаки, экономические кризисы, изменения законодательства, незаконные проверки).

По направленности:

- Угрозы экономической безопасности: направлены на финансовые и хозяйственные интересы предприятия (проявления: снижение прибыли, падение рентабельности, потеря финансовой устойчивости и платежеспособности, устаревание финансовых инструментов).

- Угрозы информационной безопасности: направлены на данные и информационные системы (проявления: неправомерный доступ к информации (угроза конфиденциальности), изменение данных (угроза целостности), блокировка доступа к системе (угроза доступности)).

- Другие типы угроз: кадровая, производственная, маркетинговая, экологическая и т.д.

По характеру действий:

- Преднамеренные: злоумышленные действия (примеры: взлом системы, кража, нападение, мошенничество).

- Непреднамеренные: случайные или ошибочные действия (примеры: ошибки в работе персонала, сбои оборудования, природные катаклизмы).

По характеру проявления угрозы безопасности организации можно разделить на три основные группы:

- статические – данный тип угроз реализуется с некоторой достаточно высокой и устойчивой по значению частотой;

- вероятностные – проявления этих угроз осуществляется с некоторой вероятностью;

- уникальные – носят преимущественно гипотетический характер, имеют единичный характер реализации и допускаются в возможной перспективе возникновения.

По вероятности наступления угрозы могут быть: потенциальными, реализуемыми в данный момент времени и уже фактически реализованный инцидент [4].

Ущерб от перечисленных выше угроз может быть прямым – возникать непосредственно при реализации риска возникновения угрозы, косвенным – возникать как побочный эффект наступления какого-либо события, отложенным – оценить ущерб не представляется возможным, поскольку риск наступления угрозы является отложенным.

Чтобы предотвратить неблагоприятные инциденты или минимизировать их последствия была создана система, которая позволяет предвидеть появление проблем и заранее спланировать план действий на случай нештатной ситуации. Это риск-менеджмент – система выявления, анализа, оценки, контроля и профилактики потенциальных внешних и внутренних угроз.

Оценка рисков корпоративной безопасности предприятия — это комплекс мероприятий, включающий идентификацию угроз, анализ уязвимостей, оценку вероятности и последствий инцидентов, а также ранжирование рисков для выработки мер по их снижению [4]. Процесс помогает предвидеть

проблемы и заранее спланировать план действий на случай внештатной ситуации, принимать осознанные решения, экономически обосновывать бюджеты на безопасность и защищать активы, персонал и репутацию компании.

Процесс управления рисками включает в себя пять основных этапов:

1.Постановка цели- **определение** всех потенциальных угроз предприятия - проводим тщательный анализ текущей ситуации на предприятии, анализируем все возможные потенциальные угрозы, определяем активы предприятия, подлежащие защите.

2.**Идентификация рисков** – выявление потенциальных угроз, определение существующих уязвимостей и слабых мест, которые могут привести к нежелательным инцидентам или которыми могут воспользоваться злоумышленники и недобросовестные конкуренты. Это имеет ключевое значение, поскольку позволяет определить, где улучшения наиболее необходимы.

3. **Оценка вероятности и степень воздействия риска**.

На данном этапе выполняется количественный анализ для принятия решения о дальнейших действиях. В ходе данного этапа могут выявляться новые факторы риска и вносится коррективы и поправки в уже выявленные риски. Риски классифицируются по уровню вероятности как низкие, средние или высокие, а по степени воздействия на незначительные, умеренные или критические. Есть и альтернативные варианты оценок степени вероятности и воздействия риска, часто используется шкала от 1 до 5 [4].

Для оценки рисков используются различные методы:

- **Метод экспертных оценок:** Привлечение специалистов и экспертов для субъективного определения вероятности и воздействия рисков.
- **Метод контрольных списков (чек-листов):** Использование заранее определенных списков потенциальных угроз и уязвимостей для систематической проверки.
- **Матричный метод:** Визуализация рисков на матрице, где по одной оси — вероятность, по другой — последствия.
- **Метод анализа сценариев ("что, если..."):** Проигрывание различных гипотетических ситуаций для оценки их потенциального влияния.
- **Метод анализа чувствительности:** Оценка влияния изменений отдельных факторов на общий уровень риска.

4. **Выбор метода управления рисками. Создание и внедрение мер по уменьшению вероятности и минимизации последствий рисков.**

На этом этапе мы определяем список наиболее критичных рисков, требующих незамедлительного решения, разрабатываем и внедряем меры для снижения их вероятности и последствий. На основании оценки риска и возможностей предприятия выбираем один из методов управления рисками: предотвращение, смягчение, перенос, принятие риска [4].

Методы управления рисками:

- Предотвращение: устранение возможности возникновения угрозы, полный отказ от деятельности, связанного с риском, чтобы избежать его полностью.

Иногда затраты или операционные потери , связанные с предотвращением определенного риска , могут перевесить выгоды, тогда необходимо рассмотреть другие методы .

- Смягчение: снижение вероятности возникновения риска или уменьшение его потенциального негативного воздействия. Профилактика, диверсификация. Когда полностью избежать риска невозможно , наилучшим шагом является снижение его вероятности или минимизация его последствий.

- Перенос: передача ответственности за управление риском третьей стороне или страхование риска. Суть страхование заключается в готовности компании отказаться от части прибыли, чтобы уклониться от риска или снизить риск до минимума.

- Принятие риска: Осознанное согласие с риском, когда предполагаемые выгоды превышают возможные убытки, или просто принятие риска, когда нет возможности его снизить или передать. Для этих целей предприятия создают собственные фонды для покрытия возможных убытков. Принятие риска – это взвешенное решение , и важно очень тщательно оценить вероятность и последствия , прежде чем выбрать такой метод.

В большинстве случаев перечисленные методы применяются в совокупности. После выбора методов управления рисками формируется стратегия их комплексной реализации, выделяются необходимые финансовые, материальные, трудовые ресурсы, распределяются обязанности конкретных исполнителей.

5.**Мониторинг и контроль выполнения и анализ эффективности принятых решений.**
Составляется отчетность по выявленным рискам, информация о динамике их показателей. Основываясь на полученной отчетности, оценивается эффективность работы риск-менеджмента, использования отдельных его инструментов и затрат на его реализацию. Готовятся рекомендации,

разрабатываются меры по снижению или контролю рисков. Процесс оценки должен быть регулярным, поскольку условия и угрозы постоянно меняются. Неэффективные методы подлежат замене.

Главная цель управления рисками – минимизация последствий, которые связаны с данным риском. Потери оцениваются в денежном выражении, оцениваются также шаги по их предотвращению.

Управление рисками — это непрерывный, циклический процесс, который требует систематического анализа, оценки промежуточных результатов и корректировки стратегий и методов. Грамотная работа с рисками — один из ключевых инструментов для достижения успехов в бизнесе.

Систематическая работа с рисками помогает компании улучшить отношения с контролирующими органами, повысить степень доверия клиентов и партнеров, стать более привлекательной для инвесторов и даже оптимизировать расходы на страхование.

Заключение

Оценка рисков обеспечения корпоративной безопасности – это важнейший процесс для любого предприятия, стремящегося защитить свои активы. Компании сталкиваются с разнообразными рисками и угрозами, которые могут серьезно повлиять на их репутацию, финансовые показатели и стабильность. Проблема обеспечения корпоративной безопасности является актуальной для любой компании [1, 3]. Управление рисками позволяет предвидеть проблемы, принимать осознанные решения и защищать активы. Внедрение комплексной системы корпоративной безопасности минимизирует риски и обеспечивает устойчивое развитие компании. Выбор правильной методики оценки рисков зависит от многих факторов, включая размер бизнеса, специфику отрасли и доступные ресурсы. Правильная оценка риска корпоративной безопасности помогает своевременно выявить угрозы и внедрить соответствующие меры защиты. Регулярный мониторинг рисков, пересмотр системы безопасности и усовершенствование защитных мер помогают оставаться на шаг впереди потенциальных угроз.

Список литературы

1. Кириллова О. Ю., Васин С. Г. Корпоративная безопасность как объект управления: причинно-следственные связи возникновения и развития // Вестник Российского экономического университета им. Г. В. Плеханова. — 2024. — № 5. — С. 200–209.
2. Машкова Е. В. Business ethics and management of internal threats in companies // Journal of Monetary Economics and Management. — 2024. — № 25.

3. Жокабине Н. Ф., Пархоменко И. А. Анализ комплаенс-рисков предприятия // Вестник Академии права и управления. — 2024. — № 2. — С. 106–112.
4. Криштаносов В. Б. Методология оценки и управления цифровыми рисками // Труды БГТУ. Серия 5: Экономика и управление. — 2021. — № 2 (250). — С. 15–36.