Электронный научный журнал "Математическое моделирование, компьютерный и натурный эксперимент в естественных науках" http://mathmod.esrae.ru/
URL статьи: **mathmod.esrae.ru/47-194**
Ссылка для цитирования этой статьи:
Кондратов Д.В., Володин Д.Н. Построение стратегий управления рисками в области информационной безопасности // Математическое моделирование, компьютерный и натурный эксперимент в естественных науках. 2024. №3

УДК 51-7 DOI:10.24412/2541-9269-2024-3-16-23

ПОСТРОЕНИЕ СТРАТЕГИЙ УПРАВЛЕНИЯ РИСКАМИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.Н. Володин[1], Д.В. Кондратов[2]
[1]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, danil3000200@mail.ru
[2]Саратовский государственный технический университет имени Гагарина Ю.А., Россия, Саратов, Институт проблем точной механики и управления Российской академии наук (ИПТМУ РАН), г. Саратов, Саратовский национальный исследовательский государственный университет имени Н.Г. Чернышевского, kondratovdv@yandex.ru.

BUILDING INFORMATION SECURITY RISK MANAGEMENT STRATEGIES

D.N. Volodin[1], D.V. Kondratov[2]
[1]Saratov State Technical University named after Yuri A. Gagarin, Russia, Saratov, danil3000200@mail.ru
[2] Yuri Gagarin State Technical University of Saratov, Russia, Saratov, Institute of Precision Mechanics and Control of the Russian Academy of Sciences, Saratov, Russia; Saratov State University, Saratov, Russia, kondratovdv@yandex.ru

Аннотация. В статье рассматривается процесс построения стратегий управления рисками в области информационной безопасности. Обсуждаются ключевые этапы: идентификация угроз и уязвимостей, оценка и приоритизация рисков, разработка и реализация защитных мер, а также мониторинг и совершенствование стратегии. Особое внимание уделено практическим методам управления рисками и их адаптации к динамически меняющейся среде угроз. Приводятся рекомендации по созданию эффективной системы защиты, минимизации вероятности инцидентов и снижению их последствий. Материал адресован специалистам в области информационной безопасности, стремящимся повысить устойчивость организаций к киберугрозам.

Ключевые слова: стратегии, риски информационной безопасности, анализ рисков, метод, рекомендации.

Abstract. This article explores the process of developing risk management strategies in the

field of information security. It discusses key stages, including the identification of threats and vulnerabilities, risk assessment and prioritization, the development and implementation of protective measures, as well as the monitoring and improvement of the strategy. Special attention is given to practical methods of risk management and their adaptation to the dynamically changing threat landscape. Recommendations are provided for creating an effective protection system, minimizing the likelihood of incidents, and reducing their impact. The material is aimed at information security professionals seeking to enhance organizational resilience against cyber threats.

Keywords: strategies, information security risks, risk analysis, method, recommendations.

Управление рисками в области информационной безопасности играет ключевую роль в защите цифровых активов и устойчивости организаций в условиях растущего числа угроз. Современные компании сталкиваются с широким спектром рисков от кибератак и утечек данных до случайных ошибок сотрудников и сбоев в работе оборудования. Пренебрежение этими рисками может привести к значительным потерям финансовым, репутационным и операционным.

Стратегическое управление рисками направлено на создание устойчивой системы защиты, которая позволяет не только минимизировать вероятность инцидентов, но и снизить их последствия. Для этого требуется системный подход, основанный на анализе текущих угроз, оценке их влияния и разработке эффективных методов противодействия.

В данном материале рассмотрены основные этапы построения стратегий управления рисками в информационной безопасности, начиная с идентификации угроз и заканчивая мониторингом и улучшением защитных механизмов. Цель статьи - подчеркнуть важность принципиального подхода к управлению рисками и предложить практические рекомендации для разработки эффективных стратегий.

Идентификация рисков является первым и наиболее важным этапом управления рисками в области информационной безопасности. Она направлена на выявление всех возможных угроз, уязвимостей и факторов, способных нанести ущерб организации. Эффективная идентификация рисков позволяет создать полный перечень потенциальных проблем, которые могут повлиять на конфиденциальность, целостность и доступность информационных активов.

Основные шаги процесса идентификации рисков:

– Необходимо составить перечень всех активов организации, которые требуют защиты. Это могут быть серверы, базы данных, программное обеспечение, устройства пользователей, а также информационные ресурсы, включая персональные данные.

– Анализируются потенциальные угрозы, такие как кибератаки, вредоносное ПО, физические повреждения, человеческий фактор или природные катаклизмы. Также важно учитывать внутренние угрозы, включая инсайдерскую активность.

– Определяются слабые места в защите активов, например, устаревшее

программное обеспечение, незащищённые сетевые протоколы или недостатки в политике доступа.

– Для повышения эффективности используются специализированные инструменты, такие как сканеры уязвимостей, системы мониторинга, а также методики оценки, например, анализ угроз STRIDE или использование шаблонов сценариев угроз.

– Проведение опросов и рабочих встреч с ключевыми специалистами позволяет выявить риски, которые могут быть неочевидны на первый взгляд.

Результатом этапа идентификации является сформированный список угроз, уязвимостей и активов, подверженных рискам. Этот список становится основой для дальнейшего анализа и приоритизации, что позволяет направить ресурсы на защиту наиболее критичных элементов системы.[1]

После идентификации рисков важно оценить их значимость и определить порядок их обработки. Оценка рисков помогает определить вероятность наступления инцидента и его возможное влияние на организацию. Это позволяет сосредоточить усилия на тех рисках, которые представляют наибольшую угрозу для информационных активов.[2]

Основные шаги оценки и приоритизации рисков:

– Определение критериев оценки

Для оценки рисков используются два основных показателя: вероятность риска - как часто данный риск может реализоваться и влияние риска - степень ущерба, который риск может нанести.

Критерии оценки могут быть качественными (низкий, средний, высокий) или количественными (например, в денежном выражении).

– Методы оценки

Качественная оценка применяется для общего анализа, когда точные данные отсутствуют. Используются экспертные мнения, опросы и матрицы оценки. Количественная оценка базируется на статистических данных и моделировании, что позволяет определить точные финансовые потери или время простоя.

– Использование матрицы рисков

Матрица рисков (например, 5x5) помогает визуализировать соотношение вероятности и влияния. Риски распределяются по уровням важности: низкий уровень (приемлемые риски), средний уровень (требуют контроля) и высокий уровень (требуют немедленного вмешательства).

– Ранжирование рисков

Все риски распределяются по приоритету. Это позволяет сосредоточить ресурсы на тех из них, которые имеют высокую вероятность и значительное влияние. Риски с низкой значимостью могут быть приняты как часть операционных затрат.

– Документирование результатов

Итоги оценки заносятся в реестр рисков, который включает: описание

риска, вероятность и влияние, приоритет обработки.

Оценка и приоритизация рисков позволяет организации эффективно распределять ресурсы, избегая ненужных затрат на управление малозначительными рисками. На основании этих данных разрабатываются стратегии управления, направленные на минимизацию критических угроз.

Разработка стратегии управления рисками — это ключевой этап, направленный на определение конкретных действий, которые организация предпримет для минимизации воздействия рисков на свои информационные активы. Успешная стратегия должна быть гибкой, учитывающей как текущие угрозы, так и возможные изменения в ИТ-инфраструктуре и бизнес-процессах.[3]

Основные подходы к разработке стратегии управления рисками:

– Принципы управления рисками:

- исключение условий, при которых риск может реализоваться. Например, отказ от использования уязвимого программного обеспечения.
- уменьшение вероятности или воздействия риска за счёт внедрения защитных мер, таких как шифрование, брандмауэры или обучение сотрудников.
- осознанное решение принять риск, если его вероятность или воздействие минимальны.
- передача риска третьей стороне, например, через страхование или использование облачных сервисов с высокими стандартами безопасности.

– Определение приоритетов

Основываясь на результатах оценки, необходимо сосредоточиться на управлении критическими рисками, которые представляют наибольшую угрозу. Менее значимые риски могут быть отложены или приняты.[4]

– Разработка планов управления

Для каждого значимого риска создаётся план управления, включающий: меры по снижению или устранению риска, ответственных за выполнение и сроки реализации.

– Интеграция с нормативной базой

Стратегия должна учитывать требования нормативно-правовых актов и стандартов, таких как: Федеральный закон № 152-ФЗ «О персональных данных»; Федеральный закон № 187-ФЗ «О безопасности КИИ»; Международные стандарты ISO/IEC 27001 и 31000.

– Обеспечение ресурсов

Эффективная реализация стратегии требует достаточного финансирования, кадров и технических средств. Организация должна выделить необходимые ресурсы для выполнения всех запланированных мероприятий.

– План действий в случае инцидента

Включает разработку процедур реагирования, чтобы минимизировать ущерб в случае реализации риска. Это может быть активация резервных копий, информирование сотрудников или восстановление систем.

Разработанная стратегия управления рисками должна быть документирована, одобрена руководством и доведена до всех заинтересованных сторон. Она является основой для систематического подхода к снижению рисков и обеспечения информационной безопасности в организации.

После разработки и внедрения стратегии управления рисками необходимо организовать её постоянный мониторинг и улучшение. Угрозы в области информационной безопасности постоянно эволюционируют, поэтому даже самая продуманная стратегия требует регулярной адаптации к новым условиям.[5]

Основные шаги мониторинга и улучшения стратегии:

– Регулярный анализ текущей ситуации в области безопасности, использование инструментов мониторинга (IDS/IPS, SIEM) для выявления новых угроз, сбор и обработка данных о произошедших инцидентах.

– Анализ показателей эффективности (например, количество предотвращённых атак, время реакции на инциденты) и сравнение реального уровня безопасности с целевыми показателями.

– Проведение повторных аудитов для выявления новых угроз и уязвимостей, учет изменений в ИТ-инфраструктуре и бизнес-процессах.

– Проведение периодических тренингов для повышения осведомлённости сотрудников о новых угрозах. Имитация атак (Red Team/Blue Team) для проверки готовности к инцидентам.

– Улучшение существующих мер защиты (например, обновление программного обеспечения, оптимизация политики управления доступом). Добавление новых методов или технологий в соответствии с актуальными угрозами.

– Фиксация в реестре рисков и связанных документах. Регулярное обновление плана управления рисками.

Постоянный мониторинг и улучшение стратегии управления рисками обеспечивают её актуальность и эффективность. Такой подход позволяет организации оставаться устойчивой перед лицом новых угроз и быстро адаптироваться к изменениям во внутренней и внешней среде.

Эффективное управление рисками в области информационной безопасности является неотъемлемой частью устойчивой работы любой организации. Построение стратегии, включающей идентификацию, оценку, приоритизацию и управление рисками, позволяет минимизировать вероятность инцидентов и снизить их последствия.

Ключевым фактором успеха является постоянный мониторинг и регулярное обновление стратегии в соответствии с изменениями в

инфраструктуре и ландшафте угроз. Это требует не только применения современных технологий, но и вовлечённости сотрудников, их осведомлённости и готовности противостоять вызовам.

Следование изложенным подходам помогает создать надёжную систему защиты, которая обеспечивает безопасность информационных активов, снижает финансовые и репутационные потери и способствует долгосрочной стабильности и конкурентоспособности организации.

Для наглядности процесс управления рисками в информационной безопасности представлен на блок-схеме, которая отражает основные этапы.(Рисунок 1)

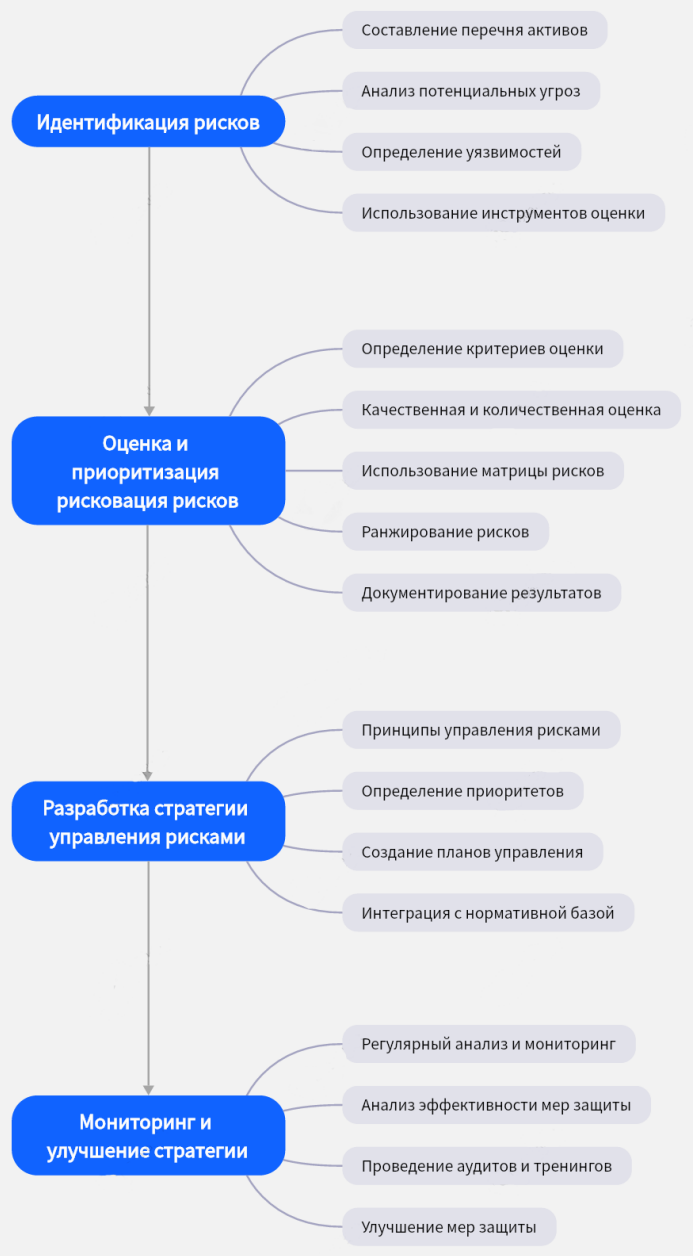

Рисунок 1

Управление рисками в информационной безопасности требует системного подхода, включающего идентификацию угроз, оценку и приоритизацию

рисков, разработку и реализацию стратегии, а также постоянный мониторинг. Этот процесс позволяет снизить вероятность инцидентов и минимизировать их последствия, что способствует защите информационных активов и устойчивости организации в условиях динамично меняющихся угроз.

Литература

1. Андрианов, В. И. Инновационное управление рисками информационной безопасности : учебное пособие / В. И. Андрианов, А. В. Красов, В. А. Липатников. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2012. — 396 с. — ISBN 978-5-91891-092-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/181472 (дата обращения: 14.12.2024). — Режим доступа: для авториз. Пользователей.
2. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 17.12.2024). — Режим доступа: для авториз. Пользователей.
3. Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182299 (дата обращения: 12.12.2024). — Режим доступа: для авториз. Пользователей.
4. Риск-контроллинг информационной и экономической безопасности : монография / Г. И. Золотарева, С. В. Филько, И. В. Филько, И. В. Федоренко. — Красноярск : СибГУ им. академика М. Ф. Решетнёва, 2018. — 192 с. — ISBN 978-5-86433-759-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/147582 (дата обращения: 20.12.2024). — Режим доступа: для авториз. Пользователей.
5. Давыдов, А. И. Управление информационной безопасностью : учебное пособие / А. И. Давыдов, Д. А. Елизаров. — Омск : ОмГУПС, 2023. — 91 с. — ISBN 978-5-949-41321-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/419255 (дата обращения: 14.12.2024). — Режим доступа: для авториз. пользователей.