Евдущенко Елена Владимировна,
к.т.н., доцент, ВИТУ
Evdushchenko Elena Vladimirovna

Сулаберидзе Антон Дмитриевич,
курсант, ВИТУ
Sulaberidze Anton Dmitrievich

УПРАВЛЕНИЕ РИСКАМИ ПРИ РАЗРАБОТКЕ ВЕБ-ОРИЕНТИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ
RISK MANAGEMENT IN THE DEVELOPMENT OF WEB-ORIENTED INFORMATION SYSTEMS

Аннотация. В статье рассмотрен процесс управления рисками на этапах разработки веб-приложений и цифровых платформ. Дано описание внешних и внутренних ИТ-угроз. Угрозы возникающие при разработке веб-ориентированных информационных систем подразделяются на риски проектов и ИТ-риски, предвиденье которых позволяют вывести на рынок цифровой продукт в срок и сократить потери информации.

Abstract. The article examines the risk management process at the stages of developing web applications and digital platforms. A description of external and internal IT-threats is provided. The threats that arise during the development of web-oriented information systems are divided into project risks and IT risks; anticipating them makes it possible to launch a digital product on time and reduce information losses.

Ключевые слова: Веб-ориентированная информационная система, управление рисками, безопасность.

Keywords: Web-based information system, risk management, security.

Разработка веб-ориентированных информационных систем представляет собой сложный процесс, так как необходимо учитывать различные виды рисков, связанные с использованием веб-технологий для взаимодействия с пользователями [1, с. 21]. Управление рисками при разработке веб-приложений – это описание процессов, связанных с идентификацией, анализом рисков и принятием решений, которые включают максимизацию положительных и минимизацию отрицательных последствий наступления рисковых событий. Каждая организация формирует собственные внутренние стандарты по управлению рисками. Определенно, можно выделить основные этапы управления рискам (рисунок 1).

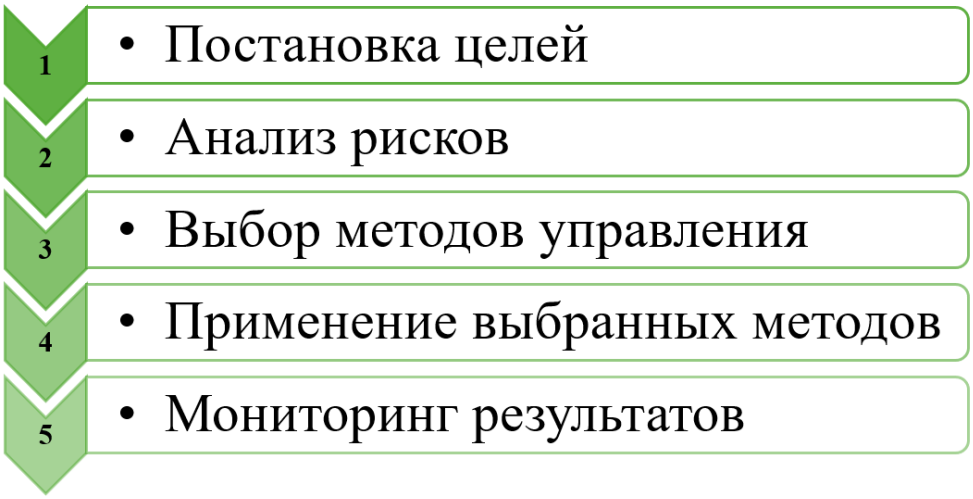


Рисунок 1. Основные этапы оправления рисками

После постановки целей в системе управления проводят анализ всех потенциальных рисков с целью их выявления. Для этого выбирают методы качественного и количественного анализа: методы сбора информации, моделирования деятельности предприятия, статистические и вероятностные.

На третьем этапе производится сопоставление эффективности различных методов воздействия на риск, которые позволяют минимизировать негативные последствия в случае его наступления. Методы воздействия могут быть направлены на:

– уклонение от риска,
– снижение риска,
– принятие риска на себя,
– передачу части или всего риска третьим лицам.

Завершением этапа является выбор метода или оптимального набора методов управления рисками.

Итогом применения выбранных методов является мониторинг результатов и совершенствование системы управления рисками. Данный этап включает оценку результатов, анализ эффективности принятых решений и корректировку целей управления рисками. Далее возникает новая итерация – переход к первому этапу.

Для разработки веб-приложений и цифровых платформ в настоящее время наиболее востребованным является «Жизненный цикл безопасной разработки» (SDL), представленный лидером в создании программного обеспечения – компанией Microsoft. Компания долгое время была сосредоточена на моделировании угроз для управление рисками [2]. В их протоколах определены пять шагов для моделирования угроз веб-приложений:

- определение требований безопасности к приложению;
- создание схемы приложения;
- выявление угроз;
- снижение угроз;
- подтверждение того, что угрозы были снижены до приемлемого уровня.

Компания Microsoft на протяжение 20 лет была сосредоточена на разработке методологии по созданию безопасного программного обеспечения, она описала принципы безопасности для каждого этапа проектирования, которые представлены в таблице 1.

Таблица 1

Принципы обеспечение безопасности от компании Microsoft

Этап	**Предотвращение рисков**
Проектирование	Предлагаемый дизайн не должен позволить злоумышленникам легко получить несанкционированный доступ к данным или другим бизнес-ресурсам организации.
Разработка программы (кода)	Убедиться что, код не позволяет злоумышленникам получить контроль над приложением и выполнять несанкционированные действия, которые наносят ущерб клиентам, сотрудникам, системам, данным или другим бизнес-процессам. Разработчики также должны работать в безопасной среде, которая не позволяет злоумышленникам причинять вред.
Этап развертывания	Проверить, что процессы непрерывной интеграции и непрерывного развёртывания (CI/CD) не позволяют неавторизованным пользователям изменять код и взламывать его.
Запуск	Среда, в которой размещена программа (облако, серверы, мобильные устройства и т. д.), соответствует передовым методам обеспечения безопасности людей, процессов и технологий, чтобы злоумышленники не могли дискриминировать работу приложения и использовать её не по назначению. Включает в себя внедрение проверенных передовых методов, базовых конфигураций безопасности.

В целом, проектирование веб-ориентированных информационных систем должно строиться на принципах архитектуры с нулевым доверием. Это означает, что все эти этапы разработки должны соответствовать принципам нулевого доверия. Такая модель безопасности предполагает, что ни одному пользователю, устройству или сети по умолчанию не доверяют, будь то внутри или за пределами сети организации. В рамках данного подхода предусмотрено, что аутентификация и авторизация на ресурсах происходят динамически.

В процессе жизненного цикла разработки информационной системы на каждом из его этапов проводится анализ возможных негативных событий, рисков для разрабатываемого цифрового продукта.

Управление рисками в сфере информационных технологий (ИТ) – это направление снижения рисков, которые можно разделить на внешние и внутренние. Стратегия управления ИТ-рисками должна постоянно развиваться вместе с компанией и политической ситуацией в стране. Иначе возрастает риск потери данных или полного прекращения работы веб-приложений. Изучение внешней ситуации позволяет предвидеть появление новых, еще неизученных проблем. Процесс масштабирования должен быть применим не только для стратегии развития веб-ориентированной информационной системы в периоде быстрого технологического роста, но и к плану управления рисками.

И безопасность является одним из приоритетных направлений в управлении рисками при разработке онлайн-сервисов и цифровых платформ для B2B и B2C. Так требуется защищать персональные данные как пользователей, так и размещаемых на платформах цифровых продуктов, обеспечивать безопасность платежей

Наиболее распространёнными ИТ-рисками являются ошибки сотрудников, уязвимости программного обеспечения, сбои сети и устройств. К основным ИТ-рискам относятся: человеческие ошибки, аппаратный сбой, отключение сети/веб-сервера, утечка данных.

Анализ рисков, которые могут возникнуть при разработки цифровой платформы включают в себя мониторинг как внешних, так и внутренних угроз [3]. К внешним угрозам относятся:

- увеличение стоимости оборудования, аренды сервера;
- аппаратный сбой (выход из строя диска для хранения данных, серверного оборудования);
- отключения сети Интернет или веб-сервера;
- вирусная атака, взлом сети, взлом системы хранения данных.

Все возможные внутренние угрозы так же можно поделить на риски проекта и ИТ-риски [4, 5]. ИТ-риски при разработке веб-ориентированной информационной системы включают в себя:

– медленную работу функционала в условиях быстрого масштабирования и увеличение числа пользователей, при отстающих технических ресурсах;

– трудности при развертывании (разрывы в функциональной совместимости, недооценка вопросов безопасности);

– проблемы с работой серверной и клиентской частями в случае ошибок в коде;

– пользователи не могут выполнять основные функции приложения из-за проблем с UX-дизайном;

– непривлекательный дизайн (трудности восприятия из-за UI-дизайна).

Риски проекта в большей степени касаются увеличения длительности разработки продукта, изменения состава команды и несдачи проекта.

Управление разработкой веб-ориентированных информационных систем подразумевает не только знание процессов проектирования программных продуктов, но и владение методами управления рисками, которые позволяют не только реализовывать сложные проекты, но и контролировать процесс работы проектных команд.

Список литературы:

1. Лысенко, В. А. Системное проектирование информационных систем с веб-интерфейсом: монография: монография / В. А. Лысенко. – Архангельск: САФУ, 2016. – [Электронный ресурс]. – Режим доступа: https://e.lanbook.com/book/161705 (дата обращения: 09.12.2026).

2. Micrisoft Security Development Lefecycle Practices – [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/en-us/securityengineering/sdl/practices?oneroute=true (дата обращения: 10.01.2026).

3. Тихонов А. Г., Субботина Т. Н. Управление рисками при разработке программного обеспечения // Экономика и бизнес: теория и практика. 2022. №5-3.

4. Курочкина А. А., Максимова Т. Г., Смирнова А. В. Моделирование сценариев развития рисков проекта разработки программного обеспечения //Глобальный научный потенциал. – 2019. – №. 3. – С. 96.

5. Ряряева Е. С., Агапов А. В. Проблемы и перспективы разработки и применения программного обеспечения для управления рисками с позиции систем менеджмента качества // ОНВ. 2020. №6 (174)