МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»
Кафедра математической кибернетики и компьютерных наук

РАЗРАБОТКА МЕТОДОЛОГИИ ВЫБОРА АСПЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СОЗДАНИЕ КОМПЛЕКТА ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ ДЛЯ ИНТЕРНЕТ-МАГАЗИНА

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

Студентки 5 курса 551 группы
направления 09.03.04 — Программная инженерия
факультета КНиИТ
Хлебниковой Анастасии Алексеевны

Научный руководитель
доцент, к. т. н. _____ В. М. Соловьев

Заведующий кафедрой
к. ф.-м. н., доцент _____ С. В. Миронов

Саратов 2025

ВВЕДЕНИЕ

Информационная безопасность (ИБ) является одним из ключевых аспектов функционирования современных информационных систем. Особенно актуальна эта проблема для интернет-магазинов, которые обрабатывают значительные объёмы персональных данных, а также совершают финансовые транзакции в режиме онлайн. Повышенное внимание к ИБ обусловлено ростом количества кибератак, появлением новых уязвимостей и ужесточением законодательства в области защиты информации. В условиях ограниченных ресурсов, характерных для малого бизнеса, возникает необходимость в разработке адаптированных методик обеспечения информационной безопасности. Цель настоящей работы — разработать методологию выбора приоритетных аспектов защиты информации для интернет-магазина и создать комплект организационно-распорядительной документации.

Цель работы: разработка методологии выбора аспектов информационной безопасности и создание комплекта организационно-распорядительной

документации для интернет-магазина.

Задачи:

- Изучить современные угрозы информационной безопасности в электронной коммерции;
- Проанализировать действующее законодательство и стандарты в области ИБ;
- Определить критерии выбора приоритетных направлений защиты;
- Разработать методику оценки рисков;
- Создать комплект регламентирующей документации по ИБ;
- Оценить эффективность предложенных решений с точки зрения практического применения.

Научная новизна и практическая значимость. Научная новизна работы заключается в следующем:

1. Адаптация существующих моделей оценки рисков к специфике интернет-магазинов с учётом микросервисной архитектуры;
2. Формализация критериев приоритезации аспектов ИБ для малых предприятий;
3. Разработка практико-ориентированной документации, сочетающей

нормативные и технические подходы.

Практическая значимость состоит в том, что разработанная методология может быть внедрена малыми компаниями без существенных затрат на внешних консультантов. Комплект документации обеспечивает выполнение требований ФЗ-152, GDPR и рекомендаций ФСТЭК.

Структура и объём работы. Выпускная квалификационная работа состоит из введения, трёх глав, заключения, списка использованных источников (21 наименование) и приложений. Общий объём работы — 93 страницы, включая 7 таблиц и 6 приложений. Работа сопровождается программным проектом, реализованным на Java, приведенным в приложениях.

Краткое содержание работы

Первая глава “Теоретические основы информационной безопасности интернет-магазина” посвящена теоретическим основам информационной безопасности, раскрывая ключевые понятия, классификацию угроз, стандарты и методологии оценки рисков, а также современные тенденции и особенности защиты информации в малом бизнесе.

Информационная безопасность определяется как состояние защищённости информации от несанкционированного доступа, использования, раскрытия, разрушения или модификации. Основные характеристики защищаемой информации — конфиденциальность, целостность, доступность и аутентификация. Конфиденциальность обеспечивает доступ к данным только уполномоченным лицам, целостность гарантирует неизменность и точность информации, доступность — своевременный доступ к данным и ресурсам, а аутентификация подтверждает подлинность пользователей и систем.

Для построения эффективной системы защиты информации выделяют несколько ключевых подходов. Технический подход базируется на использовании аппаратных и программных средств (антивирусы, межсетевые экраны, системы обнаружения вторжений, шифрование), обеспечивая базовый уровень защиты. Управленческий подход ориентирован на разработку политик безопасности, оценку рисков и обучение персонала, способствуя системному управлению. Правовой подход предусматривает соблюдение национального и международного законодательства, что минимизирует юридические риски. Организационный подход связан с формированием внутренней структуры и культуры безопасности, включая распределение ответственности и контроль. Интегрированный подход объединяет все перечисленные методы для создания комплекс- ной и устойчивой системы защиты.

Угрозы информационной безопасности классифицируются по характеру воздействия (нарушение конфиденциальности, целостности, доступности), источнику (внутренние и внешние), преднамеренности (умышленные и случайные) и способу реализации (технические, социальные, физические). Источниками угроз выступают как сотрудники и пользователи, так и внешние злоумышленники.

Важным элементом управления безопасностью является оценка рисков,

включающая идентификацию угроз и уязвимостей, анализ вероятности и последствий, оценку уровня риска и выбор стратегии реагирования. Методы оценки делятся на качественные, основанные на экспертных суждениях и описательных категориях, и количественные, использующие статистические модели и математический анализ. Качественные методы просты и оперативны, но обладают субъективностью и меньшей точностью. Количественные методы дают более объективные и воспроизводимые результаты, однако требуют значительных ресурсов и экспертных знаний.

Современные тенденции в информационной безопасности связаны с применением искусственного интеллекта, облачных технологий и Интернета вещей (IoT). Искусственный интеллект повышает эффективность обнаружения и предотвращения угроз за счёт анализа больших объёмов данных и автоматизации процессов. Облачные технологии обеспечивают гибкость и масштабируемость инфраструктуры, но требуют комплексного подхода к безопасности данных и доступа. Интернет вещей расширяет возможности автоматизации, но создаёт новые уязвимости из-за ограниченных ресурсов устройств и необходимости строгого контроля конфиденциальности.

Особое внимание уделено информационной безопасности малого бизнеса, где ограничения ресурсов и менее формализованные процессы создают дополнительные риски. Малые предприятия часто испытывают недостаток финансовых и кадровых ресурсов, что ограничивает внедрение комплексных решений. Рекомендуется повышение осведомлённости сотрудников через обучение, использование облачных сервисов с встроенной защитой, формализация простых политик безопасности и регулярное резервное копирование данных. Эти меры позволяют существенно повысить уровень защиты при ограниченных возможностях.

Таким образом, глава 1 формирует системное представление о теоретических основах информационной безопасности, подчёркивая необходимость комплексного подхода, учитывающего технические, управленческие, правовые и организационные аспекты. В современных условиях динамично меняющихся угроз и технологий эффективная защита информации требует постоянного совершенствования и адаптации мер безопасности с учётом специфики организации и её ресурсов.

Вторая глава “Проектирование системы защиты интернет-магазина” посвящена рассмотрению методики выбора приоритетных аспектов

информационной безопасности (ИБ) в условиях малого бизнеса с учётом особенностей микросервисной архитектуры интернет-магазинов. Основное внимание уделено критериям выбора защитных мер, процессу оценки рисков, моделированию сценариев атак и определению приоритетных направлений защиты.

Выбор аспектов защиты информации базируется на международных и национальных стандартах ISO/IEC 27001 и ГОСТ Р 57580.1-2017, предусматривающих объективную оценку рисков и целесообразность применения мер ИБ. Для распределённых систем с микросервисной архитектурой характерно увеличение числа потенциальных точек уязвимости, что требует учёта как классических критериев ИБ, так и специфики взаимодействия сервисов через API.

Ключевым критерием является важность информации, подлежащей защите, которая классифицируется на критически важную, ограниченно важную и общедоступную. В интернет-магазине к критичным относятся персональные данные клиентов, платёжная информация, учётные данные и служебные секреты микросервисов. Для каждого типа данных предусмотрены соответствующие меры защиты: шифрование, строгая аутентификация, разграничение доступа и резервное копирование.

Оценка вероятности реализации угроз проводится с учётом уязвимостей инфраструктуры, квалификации персонала и активности нарушителей. В микросервисной архитектуре распространены угрозы, связанные с ошибками кон- фигурации API Gateway, недостаточной изоляцией сервисов, уязвимостями в сторонних библиотеках и атаками на входные точки. Для снижения рисков рекомендованы регулярные аудиты, внедрение Zero Trust, мониторинг и оповещения.

Анализ последствий инцидентов учитывает финансовые потери, репутационные риски и юридические последствия, что обосновывает необходимость защиты даже при низкой вероятности атак. Важным аспектом является экономическая обоснованность мер — затраты на безопасность не должны превышать потенциальный ущерб.

Процесс оценки рисков включает идентификацию активов (информационных, технических, программных, человеческих и процедурных), анализ уязвимостей (проверка ПО, настройка сервисов, анализ бизнес-логики) и количественную или качественную оценку вероятности и последствий угроз.

Приведены примеры рисков с их классификацией и рекомендациями по снижению.

Моделирование сценариев атак охватывает типичные угрозы: атаки на открытые API, SQL-инъекции, кражу JWT-токенов через XSS и компрометацию CI/CD пайплайнов. Для каждого сценария описаны уязвимости и меры защиты, включая аутентификацию, фильтрацию ввода, аудит и контроль доступа.

Определение приоритетных направлений защиты базируется на риск-ориентированном подходе с фокусом на критичные сервисы (auth, payment, orders), контроле разработки и доставки кода, устойчивости к отказам, обучении персонала и мониторинге безопасности. Особое внимание уделено реализации ограничений частоты обращений (rate limiting) для предотвращения перебора паролей с помощью библиотеки Bucket4j и алгоритма token bucket.

Для повышения безопасности аутентификации реализована двухфакторная аутентификация на основе временных одноразовых паролей с использованием библиотеки Google Authenticator. Описана архитектура решения, хранение секретных ключей и интеграция с фронтендом.

Внедрение аудита действий пользователей позволяет централизованно регистрировать ключевые события (входы, неудачные попытки, обновления токенов, регистрацию), что обеспечивает трассируемость, расследование инцидентов и соответствие требованиям стандартов GDPR и ISO/IEC 27001. Аудит реализован как отдельный слой с хранением логов в защищённой базе данных PostgreSQL и механизмами ограничения доступа.

В итоге предложенная методика обеспечивает комплексный подход к выбору и реализации мер информационной безопасности в малом бизнесе с микросервисной архитектурой, позволяя эффективно управлять рисками, минимизировать потенциальные ущербы и соблюдать нормативные требования при оптимальных затратах ресурсов.

Третья глава “Разработка документации по информационной безопасности” описывает процесс разработки комплекта организационно-распорядительной документации (ОРД) как ключевого элемента построения эффективной системы информационной безопасности (СИБ) в условиях малого бизнеса с микросервисной архитектурой интернет-магазина. ОРД представляет собой совокупность локальных нормативных актов, регламентирующих деятельность организации в области защиты информации, обеспечивающих формализацию процедур, распределение ответственности и соответствие

требованиям действующего законодательства и международных стандартов, включая Федеральный закон №152-ФЗ, приказы ФСТЭК России, ГОСТ Р 57580 и ISO/IEC 27001.

В работе представлен перечень обязательных документов, необходимых для внедрения системы защиты информации: политика информационной безопасности, положение о доступе к микросервисам, модель угроз нарушителя, регламент управления уязвимостями, журналы информационной безопасности и акт оценки соответствия. Каждый документ имеет чётко определённое назначение, обеспечивая комплексный охват процессов ИБ — от стратегического планирования до контроля и аудита.

Особое внимание уделено структуре и содержанию ключевых документов. Например, политика информационной безопасности формирует основные цели, принципы и направления деятельности, определяет объекты и субъекты защиты, роли и зоны ответственности, а также процедуры контроля и обучения. Паспорт информационной системы персональных данных (ИСПДн) описывает технические и организационные характеристики системы, требования к защите обрабатываемых данных и архитектуру микросервисов. Модель угроз систематизирует возможные риски и источники атак, что позволяет планировать эффективные меры защиты. Методика проведения аудитов регламентирует порядок и периодичность оценки соответствия фактического состояния требованиям безопасности.

Важным аспектом является интеграция системы информационной безопасности с существующими бизнес-процессами и функциональными подразделениями предприятия. Кадровая служба участвует в обеспечении безопасности на этапах найма, адаптации и увольнения сотрудников, включая проверку благонадёжности и проведение инструктажей. Финансовая служба контролирует доступ к платёжным данным и взаимодействует с ИБ-отделом для соблюдения нормативных требований. Техническая служба (ИТ/DevOps) реализует и поддерживает технические меры защиты, отвечает за инфраструктуру и процессы обновления программного обеспечения.

Распределение ответственности между сотрудниками различных уровней подробно регламентировано, что обеспечивает подотчётность и минимизацию рисков, связанных с человеческим фактором. В работе приведена таблица зон ответственности для руководителя организации, специалистов по ИБ, ИТ-службы, кадровиков, финансовых менеджеров и пользователей.

Особое внимание уделено обучению и повышению осведомлённости персонала. Рекомендуется комплекс программ — вводные инструктажи для новых сотрудников, периодические тренинги, тематические семинары и имитационные учения (tabletop-exercises), адаптированные под различные категории персонала. Это способствует формированию культуры безопасности и снижению вероятности инцидентов.

Для поддержания актуальности и эффективности системы информационной безопасности предусмотрена регулярная пересмотр и обновление документации, с учётом изменений в законодательстве, инфраструктуре и угрозах. Эффективность стратегии оценивается с помощью мониторинга ключевых показателей безопасности (KSI), проведения внутренних и внешних аудитов, а также сбора обратной связи от сотрудников.

В работе приведена оценка затрат на внедрение и сопровождение СИБ, включающая расходы на технические средства, лицензии, обучение, разработку документации и аудит. Анализ экономической целесообразности показывает, что предотвращение инцидентов позволяет существенно сократить потенциальные убытки, обеспечивая окупаемость проекта в течение двух лет.

В заключение рассмотрены перспективы развития системы информационной безопасности с акцентом на автоматизацию процессов мониторинга и реагирования, а также внедрение современных технологий защиты: Zero Trust Architecture, контейнерная безопасность, SASE и интеграция искусственного интеллекта. Эти направления позволяют повысить адаптивность и устойчивость системы к новым вызовам и угрозам, что особенно актуально для динамично развивающейся микросервисной среды интернет-магазина.

Таким образом, разработанный комплект организационно-распорядительной документации и предложенный комплекс мер обеспечивают системный и эффективный подход к управлению информационной безопасностью в микросервисных ИТ-средах малого бизнеса, способствуя защите критичных данных, снижению рисков и соблюдению нормативных требований.

В заключении подводится итог проведённого исследования по организации информационной безопасности в микросервисной ИТ-инфраструктуре, включая анализ угроз и разработку нормативной базы. Отмечается важность интеграции ИБ с бизнес-процессами и постоянного

повышения квалификации персонала для адаптации к изменяющимся условиям. Также даны рекомендации по дальнейшему развитию системы защиты для обеспечения её надёжности и соответствия современным требованиям.