УДК 004.056.5:004.9

Блинов Д. В.
студент
4 курс, Институт инженерных и цифровых технологий
НИУ «БелГУ»
Россия, г. Белгород
Научный руководитель: Мордовская О. С.
доцент

Blinov D. V.
Student
4th year, Institute of Engineering and Digital Technologies
National Research University "BelSU"
Russia, Belgorod
Scientific supervisor: Mordovskaya O. S.
Associate Professor

МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА И ЗАЩИТЫ УЧЁТНЫХ ЗАПИСЕЙ В АДМИНИСТРАТИВНОЙ ПАНЕЛИ ИНТЕРНЕТ-МАГАЗИНА

ACCESS CONTROL AND ACCOUNT PROTECTION MODEL FOR THE ONLINE STORE'S ADMINISTRATIVE PANEL

Аннотация:

В статье рассматривается модель разграничения доступа и защиты учётных записей в административной панели интернет-магазина строительного инструмента. Актуальность исследования обусловлена ростом числа кибератак на веб-приложения электронной коммерции и необходимостью надёжной защиты административного интерфейса от несанкционированного доступа. В работе предложена

ролевая модель доступа, разделяющая права администратора и пользователя, а также система мер противодействия основным угрозам. В статье приведены алгоритмы аутентификации и авторизации, схемы работы с сессиями, а также рекомендации по усилению безопасности учётных записей. Результаты исследования могут быть использованы при проектировании защищённых административных панелей интернет-магазинов и других веб-систем с разграничением прав доступа.

Abstract:

The article discusses an access control and account protection model for the administrative panel of a construction tools online store. The relevance of the study is driven by the growing number of cyberattacks on e-commerce web applications and the need for reliable protection of administrative interfaces against unauthorized access. The paper proposes a role-based access model separating administrator and user privileges, along with a set of countermeasures against major threats. The article presents authentication and authorization algorithms, session management schemes, and recommendations for strengthening account security. The findings can be applied in the design of secure administrative panels for online stores and other web systems with differentiated access rights.

Ключевые слова: разграничение доступа, административная панель, интернет-магазин, ролевая модель, безопасность веб-приложений, аутентификация, защита учётных записей, угрозы информационной безопасности.

Keywords: access control, administrative panel, online store, role-based model, web application security, authentication, account protection, information security threats.

Введение

Современный интернет-магазин представляет собой сложный программный комплекс, обеспечивающий не только витрину товаров и приём заказов, но и управление пользователями, контентом и заказами через административный интерфейс. Безопасность такого ресурса напрямую зависит от надёжности системы аутентификации и разграничения прав доступа. Несанкционированное проникновение в любую часть сайта, будь то личный кабинет покупателя или административная панель, может привести к утечке персональных данных, изменению цен, удалению информации и другим серьёзным последствиям. Поэтому разработка эффективной модели управления доступом и защиты учётных записей становится ключевой задачей при создании защищённого веб-приложения электронной коммерции.

Объектом исследования является процесс аутентификации и авторизации пользователей на веб-сайте интернет-магазина. Предметом исследования выступают методы и средства построения ролевой модели доступа, а также механизмы защиты учётных записей от основных угроз информационной безопасности.

Цель исследования – разработка и проверка модели разграничения доступа и защиты учётных записей для веб-сайта интернет-магазина, обеспечивающей надёжную идентификацию пользователей, строгое разделение прав между посетителями, зарегистрированными покупателями и администраторами, а также устойчивость к распространённым атакам.

Задачи: проанализировать типовые угрозы для пользовательских и административных учётных записей; спроектировать ролевую модель доступа с распределением прав между администратором и другими пользователями; разработать алгоритмы аутентификации и авторизации; предложить комплекс защитных мер против основных векторов атак; провести тестирование модели и оценить её эффективность.

Методы и исследования

В основе разработанной модели разграничения доступа лежит каскадный протокол проверки учётных данных, реализованный на серверной стороне. Процесс авторизации представляет собой многоступенчатый алгоритм, каждый этап которого выполняет функцию фильтрации и завершается либо успешным созданием сессии, либо отклонением запроса с соответствующим уведомлением.

На входном шлюзе система сначала проверяет синтаксическую корректность введённого адреса электронной почты и соблюдение требований к сложности пароля, что предотвращает некорректные запросы на уровне приложения. Сразу после этого активируется защита типа CAPTCHA, которая отсеивает автоматизированные сценарии подбора паролей и брутфорс-атаки, повышая устойчивость системы к компрометации данных [3]. Затем выполняется криптографическая сверка введённого пароля с хешированным эталоном, хранящимся в базе данных; одновременно на этом этапе проверяется CSRF-токен, гарантирующий подлинность источника запроса и защиту от межсайтовой подделки [1].

После подтверждения корректности пары «логин–пароль» система анализирует флаг активности учётной записи. Если обнаруживаются признаки блокировки - административное отключение с выводом информационного сообщения. При успешной аутентификации инициируется создание защищённой сессии с генерацией уникального идентификатора, связанного с IP-адресом и User-Agent клиента, что позволяет надёжно идентифицировать пользователя на протяжении всего времени работы с ресурсом [2, 4]. Следующим обязательным шагом становится слияние гостевой корзины, хранящейся в локальном хранилище или временной сессии, с корзиной зарегистрированного пользователя - этот подход минимизирует потерю добавленных товаров

при переходе от гостевого режима к авторизованному. Завершающий этап алгоритма - проверка прав доступа: система определяет, имеет ли пользователь роль администратора, и на основании этого выполняет переадресацию либо в административную панель с расширенным набором CRUD-операций, либо в личный кабинет и каталог, что реализует модель управления доступом на уровне представлений и контроллеров.

Логическая структура данного процесса представлена на рисунках 1-2.

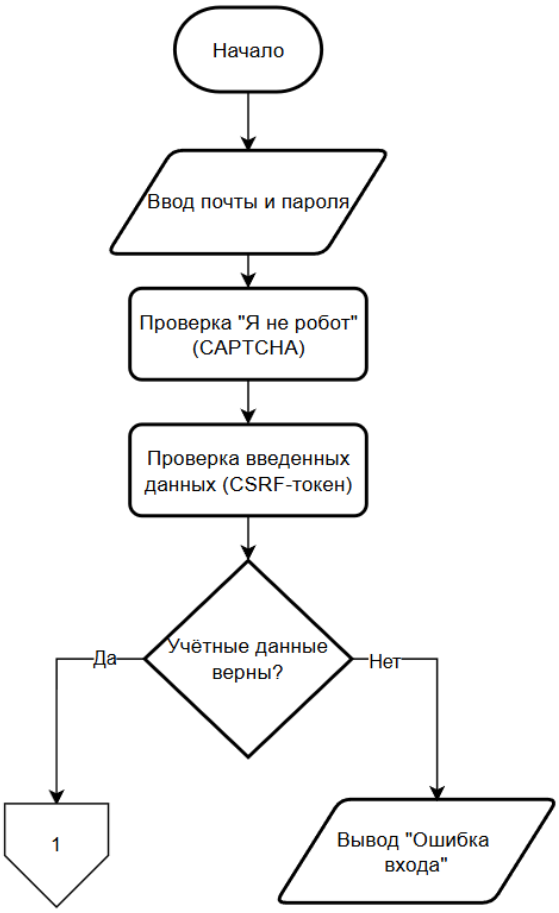

Рисунок 1 – Процесс авторизации пользователя

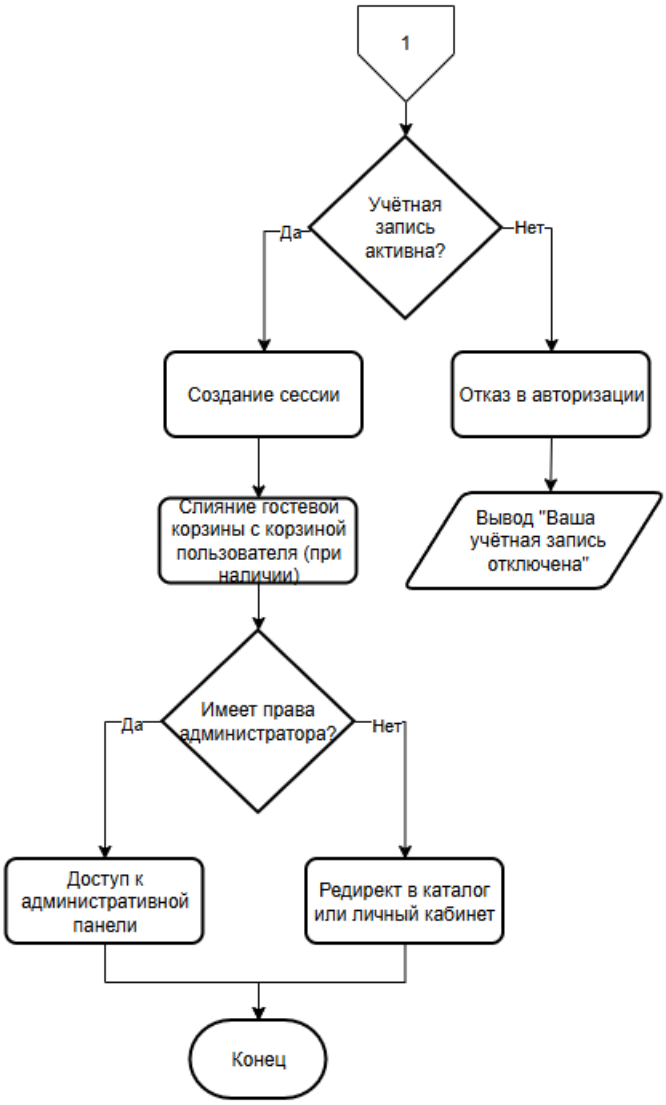

Рисунок 2 – Процесс авторизации пользователя (продолжение)

Процедура регистрации нового покупателя представляет собой симметричный по отношению к авторизации, но более расширенный алгоритм, поскольку включает этапы премодерации вводимых данных и обязательной верификации электронного адреса. На входном шлюзе пользователь заполняет форму, содержащую поля для имени, адреса электронной почты, номера телефона и пароля, причём последний должен удовлетворять требованию минимальной длины (не менее шести символов).

В момент отправки запроса активируется комплекс защитных мер: проверка CAPTCHA для отсечения ботов, валидация CSRF-токена, обеспечивающая защиту от межсайтовой подделки, а также валидация всех полей на соответствие ожидаемым форматам (например, корректность почты и телефонного номера). Завершающим этапом является проверка уникальности электронной почты - система гарантирует, что один адрес не может быть использован дважды, что предотвращает дублирование учётных записей.

Логическая структура данного процесса представлен на рисунке 3.

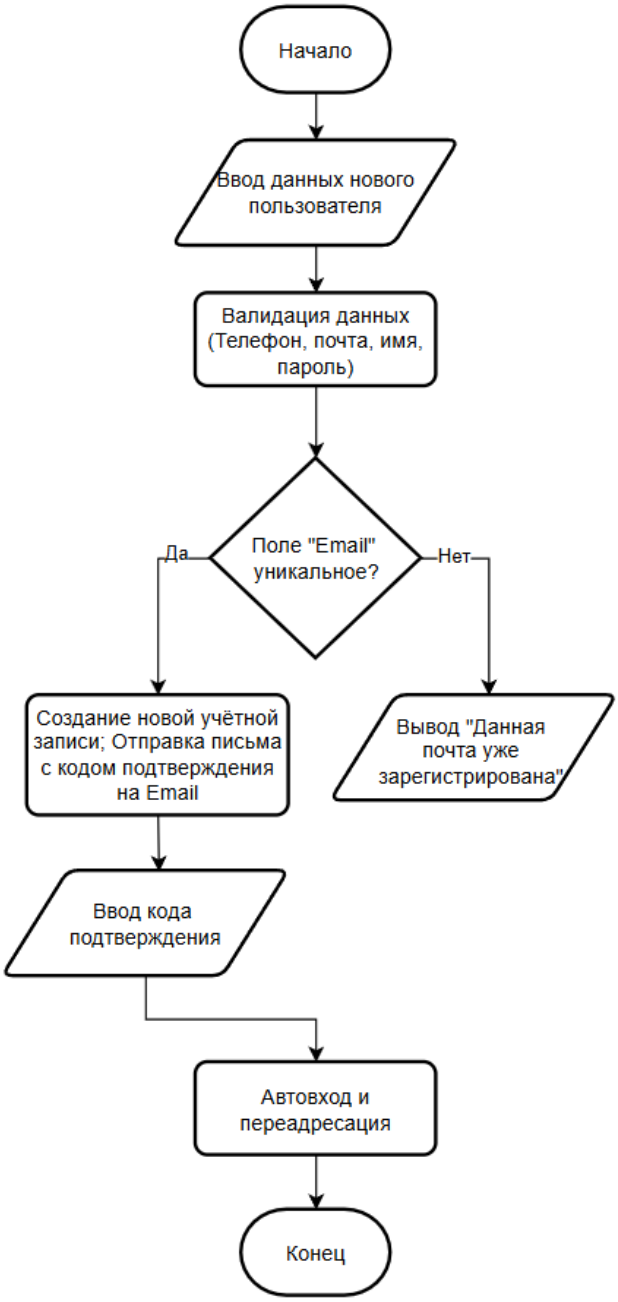

Рисунок 3 – Процесс регистрации нового пользователя

При успешном прохождении всех проверок в базе данных создаётся запись пользователя с предустановленными атрибутами: ролью «Клиент», что ограничивает доступ к административному интерфейсу и флажком «Учётная запись активна», означающим, что учётная запись сразу готова к использованию. Одновременно с этим формируется связанная запись в таблице «Покупатели», фиксирующая тип клиента как «Новый» и позволяющая в дальнейшем накапливать историю заказов и персональные настройки. Следующим обязательным шагом выступает генерация и отправка на указанную почту письма, содержащего одноразовый код для подтверждения адреса – данная мера, хотя и не блокирует немедленный вход, но служит важным элементом верификации личности и снижает риск регистрации с использованием чужих или временных почтовых ящиков.

Завершается алгоритм автоматическим входом в систему (авторизацией без повторного ввода пароля) и перенаправлением пользователя в его личный кабинет, что обеспечивает бесшовный переход от регистрации к активному использованию ресурса.

Процесс регистрации и этапы проверки представлены на рисунках 4-7.

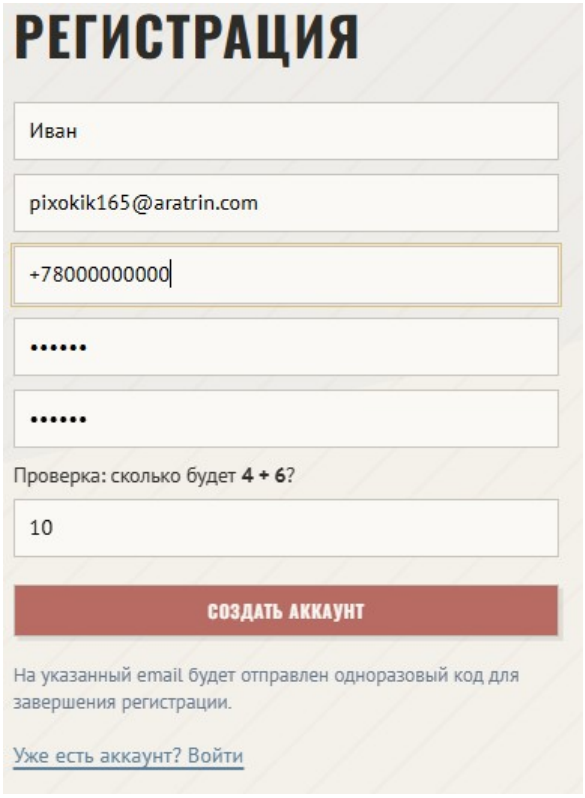

Рисунок 4 – Ввод данных нового пользователя

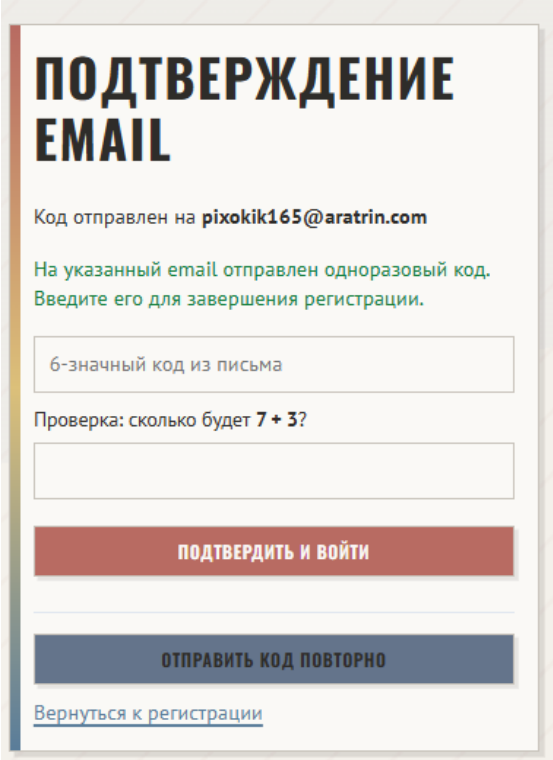

Рисунок 5 – Поле ввода кода для подтверждения почты

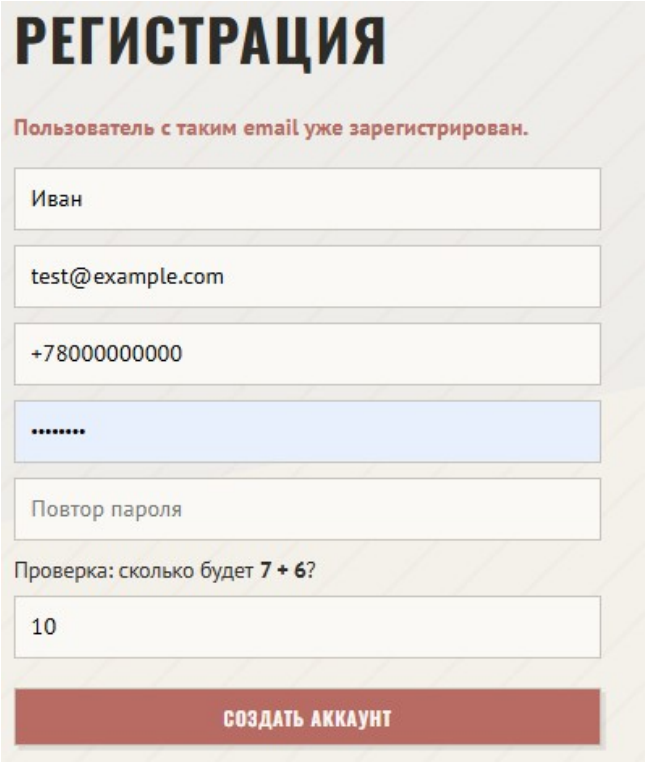

Рисунок 6 – Вывод в результате проверки уникальности почты

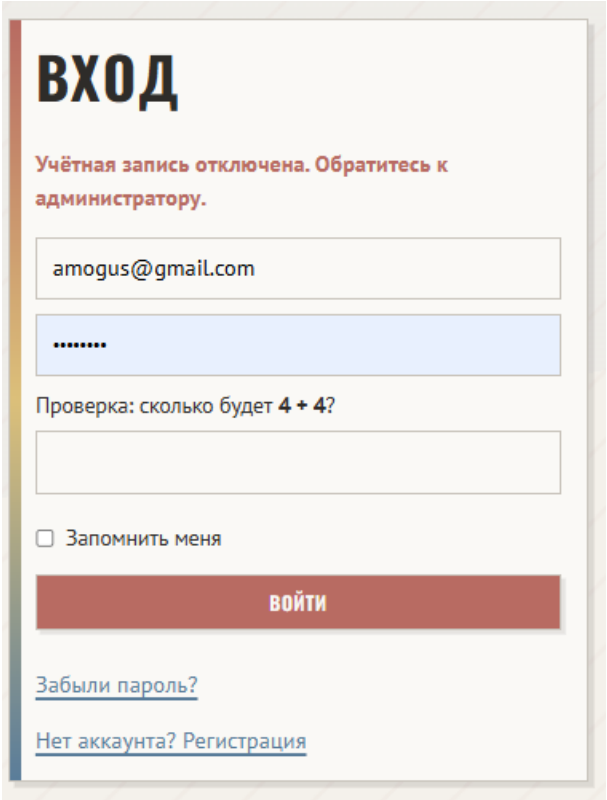

Рисунок 7 – Вывод в результате входа деактивированной учётной записи

Архитектура разграничения доступа по ролевому принципу реализована в виде трёх логически изолированных зон, каждая из которых имеет собственный набор маршрутов, контроллеров и промежуточных слоёв проверки прав. Публичная зона объединяет страницы, доступные любому посетителю без аутентификации: каталог товаров, карточки продуктов, корзину, информационные страницы, а также формы входа, регистрации и восстановления пароля. Эта часть интерфейса не требует идентификации пользователя и служит точкой входа для всех категорий посетителей, включая неавторизованных.

Зона покупателя, напротив, защищена промежуточным слоем к личному кабинету. Доступ к оформлению заказов, списку желаний, генерации PDF-документов (чеков и накладных) и функционалу отзывов разрешён только после успешной аутентификации, причём система допускает в эту зону как обычных клиентов, так и администраторов, поскольку их роли не исключают возможности совершения покупок.

Наиболее строгие ограничения накладываются на административную зону, которая помимо обязательной аутентификации требует наличия роли «Администратор» – проверка выполняется на уровне маршрутизатора, и при отсутствии соответствующих прав пользователь перенаправляется на страницу каталога или получает сообщение об ошибке доступа. Административный интерфейс включает панель с ключевыми метриками, полноценное управление товарной номенклатурой (категории, единицы измерения, остатки на складе), обработку заказов с возможностью экспорта в CSV, формирование управленческих отчётов и актов списания, администрирование пользователей и промокодов, а также модерацию отзывов, что обеспечивает весь цикл операционного управления интернет-магазином.

Архитектура разграничения прав представлена на рисунке 8.

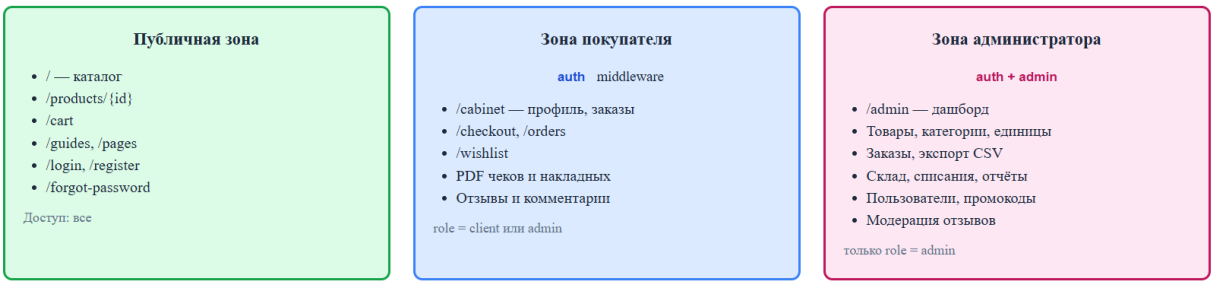

Рисунок 8 – Разграничение зон сайта по ролям

Результаты

В результате исследования разработана и внедрена модель разграничения доступа и защиты учётных записей в административной панели интернет-магазина, реализованная в виде полнофункционального веб-приложения. Основой модели служит каскадный протокол аутентификации, включающий многоступенчатую проверку вводимых данных: валидацию логина и пароля с почтой, криптографическую сверку, а также проверку CSRF-токена для гарантии подлинности запроса.

Дополнительные уровни безопасности обеспечиваются анализом статуса учётной записи (активна/отключена) и сессионным менеджментом с привязкой к IP-адресу и User-Agent, что предотвращает перехват сессий. Процедура регистрации новых покупателей дополнена проверкой уникальности электронной почты и обязательной отправкой письма с кодом подтверждения, что снижает риск создания фиктивных учётных записей. Для повышения удобства пользователей реализовано автоматическое слияние гостевой корзины с корзиной авторизованного покупателя, что сохраняет выбранные товары при переходе между режимами.

Архитектура разграничения доступа построена по трёхуровневому ролевому принципу, где публичная зона открыта для всех посетителей и содержит каталог, карточки товаров, корзину, информационные страницы

и формы входа/регистрации; зона покупателя защищена промежуточным слоем и предоставляет доступ к личному кабинету, оформлению заказов, списку желаний, PDF-документам и функционалу отзывов; административная зона дополнительно проверяет наличие роли «Администратор» и включает панель с ключевыми метриками, управлением товарами, категориями, складскими остатками, заказами с экспортом в CSV, пользователями, промокодами и модерацию отзывов. Такое разделение обеспечивает чёткое распределение функций и надёжную изоляцию критических операций от неавторизованных субъектов.

Функциональное тестирование разработанной системы подтвердило корректность всех реализованных сценариев. Авторизация успешно пропускает только активные учётные записи с правильными паролями и блокирует попытки входа при неверных данных, отключённом статусе или отсутствии CSRF-токена; регистрация валидирует все поля, предотвращает дублирование и отправляет подтверждающее письмо; ролевая модель строго ограничивает доступ к административной панели, перенаправляя покупателей в каталог при попытке перехода по защищённым маршрутам.

Модуль управления заказами корректно резервирует товары при оформлении, обновляет остатки после подтверждения оплаты и восстанавливает их при отмене, а подсистема генерации документов формирует счета, договоры, товарные чеки и акты передачи в формате HTML, пригодном для просмотра, печати и отправки покупателю. Все эти результаты подтверждают эффективность предложенной модели разграничения доступа и её пригодность для промышленной эксплуатации в составе интернет-магазина.

Возможные угрозы, риски, которые они представляют, а также способы противодействия им представлены в таблице 1.

Таблица 1 - Угрозы, риски и меры противодействия им

Название угрозы	Возможные риски	Способ противодействия
Перебор пароля	Компрометация учётной записи путём массового перебора паролей	Внедрение CAPTCHA на этапе входа, ограничение количества неудачных попыток входа с временной блокировкой IP-адреса
Подделка запроса (CSRF)	Выполнение несанкционированных действий от имени аутентифицированного пользователя	Использование CSRF-токенов во всех формах изменения данных (регистрация, вход, настройки профиля) с проверкой на серверной стороне
Перехват сессии	Угон идентификатора сессии и получение несанкционированного доступа	Привязка сессии к IP-адресу клиента, регенерация сессионного идентификатора при входе и смене уровня прав
Несанкционированный доступ	Внесение изменений в каталог, заказы, цены; утечка данных пользователей и заказов	Многоуровневая проверка: обязательная аутентификация и дополнительная ролевая фильтрация на всех маршрутах административной зоны
Создание фальшивых учетных записей	Искусственное увеличение базы пользователей, накрутка отзывов, спам	Валидация уникальности почты на сервере, обязательная верификация адреса электронной почты через ссылку или одноразовый код
Внедрение вредоносного кода (SQL-инъекции)	Чтение или изменение данных в базе, повышение привилегий	Использование Eloquent ORM с параметризованными запросами, что исключает прямое экранирование; дополнительная валидация всех входных параметров
Атака на форму ввода (XSS)	Исполнение скрипта в браузере администратора	Экранирование вывода всех пользовательских данных с помощью Blade-шаблонизатора, санитизация HTML-тегов в отзывах и комментариях
Изменение данных через прямой несанкционированный доступ к API	Обход интерфейса и выполнение операций без проверки прав	Использование политик доступа на уровне контроллеров, проверка прав на каждое действие в административной панели

Приведённая таблица демонстрирует, что разработанная модель разграничения доступа обеспечивает комплексную защиту учётных записей и административной панели интернет-магазина от основных

классов угроз, характерных для веб-приложений. Каждая потенциальная уязвимость перекрывается соответствующим техническим решением, встроенным непосредственно в архитектуру системы на уровне промежуточного программного обеспечения, политик доступа. При этом защитные меры не являются изолированными, а образуют взаимосвязанную цепочку: например, многоступенчатая аутентификация сочетается с ролевой фильтрацией, а валидация входных данных дополняется параметризацией запросов и экранированием вывода. Такой подход минимизирует риски несанкционированного доступа, утечки конфиденциальной информации и нарушения целостности данных, что подтверждает практическую надёжность предложенной модели и её готовность к эксплуатации в реальных условиях.

Заключение

В ходе исследования была разработана и реализована модель разграничения доступа и защиты учётных записей в административной панели интернет-магазина. Предложенная модель построена на основе каскадного протокола аутентификации, объединяющего многоступенчатую проверку реквизитов, верификацию паролей и анализ статуса учётной записи, а также трёхуровневую ролевую архитектуру, чётко разделяющую публичную зону, зону покупателя и административную панель.

Практическим результатом работы стала полнофункциональная система, обеспечивающая регистрацию и верификацию новых покупателей, безопасную авторизацию с автоматическим слиянием гостевой корзины, управление каталогом товаров, обработку заказов с резервированием остатков и корректировкой складских запасов, генерацию первичных документов, а также административную панель для

управления ассортиментом, пользователями, промокодами, заказами и отзывами с разграничением доступа на основе ролей.

Функциональное тестирование подтвердило корректную работу всех реализованных сценариев: система успешно пропускает только активные учётные записи с верными паролями, блокирует попытки входа при неверных данных или отключённом статусе. Анализ потенциальных угроз показал, что предложенные механизмы защиты – CSRF-токены, сессионная привязка к IP, параметризованные ORM-запросы, экранирование вывода и ролевые политики – комплексно перекрывают основные векторы атак, характерные для веб-приложений.

Полученные результаты могут быть использованы малыми и средними предприятиями, нуждающимися в специализированном интернет-магазине с надёжной системой разграничения доступа и защитой учётных записей, без избыточного функционала крупных платформ и без высоких комиссионных отчислений.

Использованные источники:

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие для вузов [Текст] / П. Н. Девянин. – 2-е изд., испр. и доп

2. Хоффман, Э. Безопасность веб-приложений. Разведка, защита, нападение [Текст] / Эндрю Хоффман. – 2-е изд. – Астана: Спринт Бук, 2025. – 432 с.

3. Google reCAPTCHA – Documentation [Электронный ресурс]. – URL: https://developers.google.com/recaptcha. – (дата обращения: 07.06.2026).

4. Макдональд, М. Грокаем безопасность веб-приложений [Текст] / Малькольм Макдональд; пер. с англ. А. Денисова. – Санкт-Петербург:

Питер: Прогресс книга, 2025. – 334 с