**ЛАБОРАТОРНАЯ РАБОТА №4**

РАЗРАБОТКА ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ НА СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ

Цель: ознакомление с процессом разработки технического задания на создание автоматизированной системы (программного продукта).

Тема проект: разработка технический требований на создание автоматизированной системы аутентификации и авторизации в соответствии с СТП 09150.11.118-2009.

**Технические требования:**

- процесс аутентификации и авторизации должен осуществляться через запрос данных учетной записи (логин и пароль) пользователя.

- пароль пользователя должен быть не менее 8 символов и обязательно содержать цифры и символы разного регистра. Проверка пароля на соответствие требованиям должно осуществляться на стороне клиента;

- хранение пароля пользователя в системе должно осуществляться зашифрованном виде;

- при отсутствии активности пользователя в системе более 10 минут уничтожается сессия;

- предусмотреть подсистему сброса и восстановления данных учетной записи пользователя;

- предусмотреть UML-диаграмму процесса аутентификации и авторизации

пользователя в системе.**Контрольный вопрос**

1. В чем отличие аутентификации и авторизации?

Аутентификация — это процесс проверки личности пользователя. Система проверяет, действительно ли пользователь тот, за кого себя выдаёт. Для этого используются данные, предоставляемые пользователем, такие как:

* Логин и пароль;
* Биометрические данные (например, отпечаток пальца или распознавание лица);
* Одноразовые коды (OTP), отправляемые на телефон или email. Цель аутентификации — установить факт идентичности пользователя, чтобы убедиться, что доступ запрашивает именно он.

Авторизация — это процесс предоставления пользователю прав доступа к определённым ресурсам или действиям. Она происходит после успешной аутентификации и определяет, что именно пользователь может делать в системе. Например:

* Администратор может редактировать, удалять и добавлять данные.
* Обычный пользователь имеет доступ только к просмотру информации.

Ключевое отличие Аутентификация отвечает на вопрос «Кто вы?», а авторизация — «Что вам разрешено делать?». Первый этап проверяет личность, второй — права.

**1. Функциональные требования**

1.1 **Методы аутентификации**

* Поддержка как минимум трёх способов аутентификации:
  + Логин/пароль с настройкой минимальной длины (не менее 8 символов), обязательным использованием специальных символов и периодической сменой.
  + Одноразовые пароли (OTP), генерируемые через приложения (например, Google Authenticator) или SMS.
  + Биометрические методы аутентификации, включая отпечатки пальцев и распознавание лица.
* Реализация многофакторной аутентификации (MFA), комбинирующей различные методы для повышения безопасности.

1.2 **Ролевая модель доступа**

* Встроенная система ролевого разграничения доступа:
  + Администратор: полный доступ к функциям системы.
  + Пользователь: ограниченный доступ, только к данным, связанным с его учётной записью.
  + Гость: минимальный доступ к публичной информации без возможности вносить изменения.
* Возможность изменения и создания ролей через панель управления.

1.3 **Управление учётными записями пользователей**

* Создание, обновление, удаление и восстановление учётных записей.
* Функция автоматической блокировки пользователя после 5 неверных попыток ввода пароля.
* Возможность активации «гостевого» режима с ограниченным временем действия учётной записи.

1.4 **Мониторинг и отчётность**

* Ведение журнала действий пользователей, включая:
  + Даты входа в систему.
  + Попытки несанкционированного доступа.
  + Изменения настроек безопасности.
* Генерация отчётов о событиях для анализа работы системы.

#### ****2. Технические требования****

2.1 **Скорость работы**

* Максимальное время отклика при выполнении запроса (например, вход в систему) не должно превышать 1 секунды.
* Производительность системы рассчитана на 2000 активных пользователей одновременно.

2.2 **Совместимость и интеграция**

* Поддержка операционных систем Windows, macOS, Linux.
* Поддержка открытых API для интеграции с внешними системами.

2.3 **Безопасность данных**

* Все данные учётных записей должны храниться в зашифрованном виде с использованием стандарта AES-256.
* Использование SSL/TLS для шифрования данных при передаче.
* Реализация механизмов защиты от атак:
  + SQL-инъекции;
  + Межсайтовый скриптинг (XSS);
  + DDoS-атаки.

#### ****3. Требования к интерфейсу****

3.1 **Удобство и интуитивность**

* Веб-интерфейс с адаптивным дизайном для корректной работы на настольных компьютерах, планшетах и смартфонах.
* Интуитивный интерфейс для всех категорий пользователей: простота навигации и минимальные требования к обучению.

3.2 **Многоязычность**

* Поддержка как минимум двух языков интерфейса (например, русский и английский) с возможностью добавления дополнительных.

#### ****4. Внедрение и эксплуатация****

4.1 **Резервное копирование и восстановление**

* Ежедневное автоматическое создание резервных копий данных.
* Возможность восстановления данных из резервной копии в течение 30 минут.

4.2 **Служба технической поддержки**

* Наличие круглосуточной службы поддержки для решения проблем, связанных с работой системы.
* Время реакции на критические инциденты: не более 1 часа.

4.3 **Документирование и обучение**

* Предоставление технической и пользовательской документации, включая подробные инструкции по настройке и эксплуатации системы.
* Проведение обучения персонала по использованию ключевых функций системы.

Содержание

[1 ВВЕДЕНИЕ 5](#_Toc194567204)

[2 ОБЩИЕ СВЕДЕНИЯ 5](#_Toc194567205)

[3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ 6](#_Toc194567206)

[3.1 Назначение 6](#_Toc194567207)

[3.2 Цели создания 6](#_Toc194567208)

[4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ 7](#_Toc194567209)

[4.1 Объекты управления 7](#_Toc194567210)

[4.2 Пользователи системы 7](#_Toc194567211)

[4.3 Техническая инфраструктура 7](#_Toc194567212)

[5 ТРЕБОВАНИЯ К СИСТЕМЕ 9](#_Toc194567213)

[5.1 Требования к структуре 9](#_Toc194567214)

[5.2 Требования к процедурам доступа к системе 9](#_Toc194567215)

[5.3 Требования к функциональной безопасности 11](#_Toc194567216)

[5.4 Требования к информационной безопасности 12](#_Toc194567217)

[5.5 Требования к патентной чистоте 13](#_Toc194567218)

[6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ 14](#_Toc194567219)

[6.1 Требования к информационному обеспечению 14](#_Toc194567220)

[6.2 Требования к математическому обеспечению 15](#_Toc194567221)

[6.3 Требования к программному обеспечению 15](#_Toc194567222)

[6.4 Требования к техническому обеспечению 16](#_Toc194567223)

[6.5 Требования к организационному обеспечению 17](#_Toc194567224)

[7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ 17](#_Toc194567225)

[7.1 Этапы выполнения работ 17](#_Toc194567226)

[7.2 Основные виды работ 18](#_Toc194567227)

[8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ 18](#_Toc194567228)

[9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ 19](#_Toc194567229)

# 1 ВВЕДЕНИЕ

Развитие современных информационных технологий создало необходимость в обеспечении надёжной защиты данных и управления доступом в цифровых системах. Одной из ключевых задач является создание автоматизированных систем аутентификации и авторизации, которые позволяют безопасно идентифицировать пользователей, предоставлять доступ к ресурсам и защищать данные от несанкционированного использования.

Данный проект направлен на разработку технических требований к автоматизированной системе аутентификации и авторизации в соответствии с нормативным документом СТП 09150.11.118-2009. Основной целью является создание эффективного инструмента управления доступом, который обеспечивает высокий уровень безопасности, интеграцию с существующими информационными системами и удобство использования для всех категорий пользователей.

Проект охватывает процесс анализа текущих потребностей организации, определение ключевых функциональных и технических характеристик системы, а также разработку требований, которые будут основой для её создания. Внедрение данной системы позволит минимизировать риски несанкционированного доступа, оптимизировать управление учётными записями и повысить общую устойчивость информационной инфраструктуры.

# 2 ОБЩИЕ СВЕДЕНИЯ

2.1 Автоматизированная система аутентификации и авторизации предназначена для управления доступом пользователей к ресурсам, базам данных и информационным системам предприятия. Её внедрение позволяет повысить уровень информационной безопасности, оптимизировать процессы управления учетными записями и исключить возможность несанкционированного доступа.

2.2 Целью разработки системы является обеспечение надёжной и безопасной аутентификации пользователей, контроль доступа в зависимости от их полномочий, а также автоматизация процессов идентификации. Система должна гарантировать соответствие требованиям нормативных документов, таких как СТП 09150.11.118-2009.

2.3 Разработка системы осуществляется на основе следующих стандартов и нормативных документов:

* СТП 09150.11.118-2009;
* ISO/IEC 27001: управление информационной безопасностью;
* ГОСТ Р 57580-2017: защита персональных данных;
* Рекомендации OWASP по защите веб-приложений.

2.4 В рамках проекта используются следующие основные термины:

* **Аутентификация** — процесс проверки подлинности пользователя для предоставления ему доступа.
* **Авторизация** — определение прав доступа пользователя к ресурсам системы на основе его роли.
* **Роль** — набор привилегий, закреплённых за пользователем или группой.
* **Многофакторная аутентификация (MFA)** — использование нескольких методов проверки подлинности для повышения уровня безопасности.

# 3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ

## 3.1 Назначение

3.1 Автоматизированная система аутентификации и авторизации предназначена для обеспечения безопасного и эффективного управления доступом к информационным ресурсам организации. Основное назначение системы включает:

* Централизация аутентификации: предоставление единой платформы для проверки подлинности пользователей на основе различных методов (логин/пароль, двухфакторная аутентификация, биометрия).
* Управление доступом: автоматизация процессов предоставления и ограничения прав доступа на основе ролевой модели или других заданных правил.
* Обеспечение информационной безопасности: минимизация рисков несанкционированного доступа к данным и утечки конфиденциальной информации.
* Снижение нагрузки на администрацию: упрощение работы администраторов благодаря централизованному управлению учётными записями и политиками доступа.

## 3.2 Цели создания

3.2.1 Система должна минимизировать риски несанкционированного доступа к информационным ресурсам и защитить конфиденциальные данные от утечек, обеспечивая высокий уровень защиты в соответствии с действующими стандартами информационной безопасности.

3.2.2 Создание единой платформы для управления процессами аутентификации и авторизации, которая позволит администраторам эффективно контролировать доступ пользователей к ресурсам.

3.2.3 Система должна включать поддержку многофакторной аутентификации (MFA), биометрических технологий и других инновационных решений для повышения уровня надёжности проверки подлинности пользователя.

3.2.4 Автоматизация создания и управления учётными записями, включая предоставление прав доступа, блокировку пользователей и обновление политик безопасности.

3.2.5 Разработка интерфейса системы, который будет интуитивно понятным и удобным для пользователей, что снизит время на обучение и повысит продуктивность работы с системой.

3.2.6 Гарантия полного соответствия системы требованиям действующих стандартов и нормативных документов в области защиты персональных данных и управления доступом, таких как СТП 09150.11.118-2009.

# 4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ

## 4.1 Объекты управления

4.1.1 Учётные записи являются ключевым объектом управления, так как они содержат данные для аутентификации (логин, пароль, биометрические параметры), а также информацию о ролях и правах доступа. Каждая учётная запись имеет уникальный идентификатор, статус (активна, заблокирована, удалена) и историю действий, зафиксированных в системе.

4.1.2 Роли определяют, какие права доступа имеет пользователь. Например:

* Администратор: полный доступ к системе, возможность настройки её параметров, управления учётными записями и политиками безопасности.
* Пользователь: доступ только к своим данным и функциям, необходимым для выполнения задач.
* Гость: минимальные права, ограниченные просмотром определённых данных. Роли могут быть дополнительно настроены и изменены через административную панель.

4.1.3 Система предоставляет доступ к защищённым информационным ресурсам, таким как базы данных, файлы, журналы событий и конфиденциальная информация компании. Каждому ресурсу назначаются права доступа, основанные на ролях пользователей.

## 4.2 Пользователи системы

4.2.1 Администраторы выполняют управление системой, включая создание и удаление учётных записей, настройку ролей, мониторинг событий и решение вопросов безопасности. Они также отвечают за аудит и поддержку системы в соответствии с установленными политиками.

4.2.2 Это сотрудники или клиенты организации, которые используют систему для выполнения задач. Они проходят аутентификацию перед использованием ресурсов системы и работают с данными, доступ к которым определяется их ролями.

4.2.3 Гостевые пользователи получают временный или ограниченный доступ к информации. Например, это может быть предоставление доступа стороннему партнёру или подрядчику на период выполнения работ.

## 4.3 Техническая инфраструктура

4.3.1 Серверы обеспечивают обработку запросов пользователей, хранение данных и выполнение алгоритмов системы. Они должны быть надёжными, масштабируемыми и соответствовать высоким требованиям производительности.

4.3.2 Сетевое оборудование, включая маршрутизаторы и коммутаторы, отвечает за связь между компонентами системы. Оно должно поддерживать современные протоколы безопасности, такие как SSL/TLS, для защиты передаваемой информации.

4.3.3 Система может использовать облачные сервисы для хранения данных, резервного копирования и обработки запросов. Это обеспечивает высокую доступность, гибкость и возможность работы пользователей с любого устройства.

4.3.4 Рабочие места пользователей включают персональные компьютеры, ноутбуки и мобильные устройства, с которых осуществляется доступ к системе. Они должны поддерживать установленный веб-интерфейс и безопасность соединения.

4.4.1 Система должна быть интегрирована с внешними сервисами управления учётными записями, такими как Active Directory или LDAP. Это позволит использовать единую точку входа (SSO) для аутентификации пользователей, упрощая управление доступом и повышая уровень безопасности. Через такие системы можно централизованно управлять ролями, правами и статусами пользователей.

4.4.2 Интеграция с системами мониторинга (например, SIEM) необходима для анализа данных о действиях пользователей и выявления потенциальных угроз. Такие системы обеспечивают сбор логов, анализ событий, создание отчётов и уведомление о подозрительных действиях. Кроме того, возможно использование IDS/IPS (систем обнаружения и предотвращения вторжений) для блокировки вредоносной активности.

4.4.3 Система должна иметь открытый API, который позволяет внешним приложениям взаимодействовать с ней для обмена данными. Например, CRM-системы или ERP-платформы могут использовать API для получения информации о пользователях или выполнения операций по их авторизации. Это обеспечивает гибкость интеграции и расширяет функциональные возможности системы.

4.4.4 Поддержка взаимодействия с внешними платформами управления доступом (IAM-системами) обеспечивает единый контроль за всеми ресурсами. IAM-системы предоставляют централизованный подход к управлению доступом во всей организации, обеспечивая полное соответствие требованиям безопасности.

4.4.5 Интеграция с облачными системами (например, Azure, AWS или Google Cloud) позволяет использовать облачную инфраструктуру для хранения данных, масштабирования ресурсов или обеспечения работы системы в распределённой среде. Это создаёт возможности для удалённого доступа и повышения надёжности системы.

4.4.6 Система должна поддерживать подключение к внешним платформам биометрической аутентификации, которые используют технологии отпечатков пальцев, распознавания лиц или голосовых данных. Это увеличивает надёжность аутентификации и снижает зависимость от традиционных методов, таких как логин и пароль.

4.4.7 Внешние системы должны соответствовать требованиям международных стандартов безопасности и законодательства, включая GDPR, HIPAA и другие регулирующие документы. Интеграция с такими системами обеспечивает юридическую защиту данных пользователей и компании.

# 5 ТРЕБОВАНИЯ К СИСТЕМЕ

## 5.1 Требования к структуре

5.1.1 Система должна иметь модульную архитектуру, разделённую на независимые компоненты, которые можно разрабатывать, тестировать и обновлять отдельно. Такой подход обеспечивает гибкость системы, позволяет легко добавлять новые функции и упрощает её техническое обслуживание.

5.1.2 Серверная часть должна быть спроектирована так, чтобы поддерживать высокую производительность и надёжность. Она обязана обеспечивать обработку всех запросов пользователей и управление данными, включая их хранение, модификацию и доступ. Важным требованием является возможность горизонтального масштабирования, чтобы система могла справляться с увеличением нагрузки. Серверная часть должна поддерживать современные стандарты безопасности и включать механизмы резервного копирования данных.

5.1.3 Клиентская часть системы должна предоставлять интуитивно понятный интерфейс для работы с пользователями. Она должна поддерживать адаптивный дизайн, чтобы корректно работать как на настольных компьютерах, так и на мобильных устройствах.

5.1.4 База данных должна быть организована централизованно, обеспечивая высокую скорость доступа к информации и её надёжное хранение. Для обеспечения безопасности данные должны быть зашифрованы, а также необходимо реализовать регулярное резервное копирование для предотвращения их утраты. Структура базы данных обязана поддерживать обработку больших объёмов информации и позволять проводить транзакции без снижения производительности.

5.1.5 Система должна быть способна работать в распределённой сетевой среде. Для защиты данных требуется использование протоколов SSL/TLS. Система должна обеспечивать стабильность передачи данных между компонентами независимо от количества пользователей.

5.1.6 Поддержка стандартов API (REST или SOAP) для интеграции системы с внешними платформами, такими как Active Directory, CRM, ERP и другими корпоративными решениями.

5.1.7 Система должна вести журналы действий пользователей, системных событий и ошибок. Логирование необходимо для анализа инцидентов, обнаружения угроз и обеспечения прозрачности работы системы. Также требуется инструмент мониторинга для отслеживания состояния компонентов системы и быстрого реагирования на неполадки.

5.1.8 Система должна включать механизмы резервирования данных и ресурсов, а также функции автоматического восстановления после сбоев.

## 5.2 Требования к процедурам доступа к системе

5.2.1 Процедура аутентификации должна быть организована так, чтобы обеспечивать надёжную проверку личности пользователя перед предоставлением доступа к системе. Для этого необходимо использовать многофакторную аутентификацию, которая включает комбинацию нескольких методов, таких как логин и пароль, одноразовые пароли (OTP), или биометрические данные (отпечаток пальца, распознавание лица). В случае использования паролей должны быть предусмотрены требования к их длине, сложности, а также регулярная их смена.

5.2.2 Авторизация должна быть основана на заранее определённой ролевой модели, где каждому пользователю назначаются права доступа в зависимости от его роли и уровня полномочий. Процедура должна включать проверку соответствия введённой информации с правами, предоставленными пользователю, и ограничение доступа к ресурсам в случае отсутствия необходимых привилегий. Также должны быть предусмотрены механизмы автоматической блокировки доступа при нарушении правил безопасности или истечении срока действия учётной записи.

5.2.3 Администраторы должны иметь отдельную процедуру доступа к системе с расширенными привилегиями. Доступ к административным функциям должен быть ограничен и защищён дополнительными уровнями проверки, например, обязательным использованием многофакторной аутентификации. Все действия, выполняемые администраторами, должны фиксироваться в журнале событий для анализа и аудита.

5.2.4 Для временных пользователей должна быть предусмотрена отдельная процедура гостевого доступа, которая включает минимальные права. Доступ к системе в данном случае предоставляется на ограниченный срок и автоматически прекращается по завершении установленного времени.

5.2.5 Создание, модификация и удаление учётных записей должны выполняться через административный интерфейс с проверкой прав доступа. Каждой операции должен предшествовать процесс аутентификации администратора, чтобы исключить вероятность несанкционированного изменения данных. Должен быть реализован механизм восстановления удалённых или заблокированных учётных записей.

5.2.6 Все процедуры доступа должны быть документированы в виде записей в журнале событий. Логи должны содержать информацию о времени и типе операции, устройстве, с которого был выполнен доступ, и результате аутентификации.

5.2.7 Пароли пользователей должны удовлетворять строгим требованиям безопасности, включая минимальную длину, обязательное использование заглавных букв, цифр и специальных символов. Система должна обеспечивать возможность регулярного обновления паролей и автоматическую блокировку устаревших или скомпрометированных. Пользователь должен получать уведомление об истечении срока действия пароля заранее, с возможностью его изменения.

5.2.8 Система должна автоматически фиксировать все попытки несанкционированного доступа, включая попытки подбора пароля. В случае превышения установленного лимита попыток входа учётная запись пользователя должна блокироваться, а администратор системы должен получать соответствующее уведомление. Эти события также должны записываться в журнал для последующего анализа.

5.2.9 Для предотвращения несанкционированного использования доступа система должна автоматически завершать сеанс пользователя при отсутствии активности в течение установленного времени. Администратор должен иметь возможность настраивать допустимый период бездействия, а пользователь должен быть уведомлён перед завершением сеанса.

5.2.10 Для повышения уровня безопасности входа в систему должна быть реализована поддержка многофакторной аутентификации. Пользователь обязан подтвердить свою личность, используя не только пароль, но и дополнительные способы проверки, например, одноразовые пароли (OTP), биометрические данные или специальные аппаратные устройства.

5.2.11 Система должна предоставлять безопасную процедуру сброса учётных данных в случае их утери. Для этого требуется подтверждение личности пользователя через зарегистрированный email-адрес, номер телефона или другие методы. Процесс сброса должен быть защищён от несанкционированного вмешательства.

5.2.12 В системе должна быть предусмотрена возможность предоставления временного доступа для определённых пользователей или групп с автоматическим ограничением срока действия. По истечении указанного времени доступ должен прекращаться автоматически без необходимости дополнительных действий со стороны администратора.

5.2.13 Политики доступа и управления учётными записями должны регулярно пересматриваться и обновляться в соответствии с современными требованиями безопасности. Администраторы должны быть уведомлены о необходимости обновления политик, включая сроки их актуализации

## 5.3 Требования к функциональной безопасности

5.3.1 Система должна исключать возможность несанкционированного доступа к своим компонентам. Это достигается использованием надёжных процедур аутентификации и авторизации, шифрования данных, а также блокировкой учётной записи при многократных неверных попытках входа. Необходимо проводить регулярный аудит безопасности для выявления и устранения потенциальных уязвимостей.

5.3.2 Все персональные и конфиденциальные данные, передаваемые и хранящиеся в системе, должны быть защищены от несанкционированного доступа. Для этого используется шифрование, основанное на современных алгоритмах, таких как AES-256 для хранения данных и SSL/TLS для их передачи.

5.3.3 Система обязана обеспечивать защиту целостности данных от случайных или преднамеренных изменений. Для этого реализуются механизмы контрольных сумм и журналирования изменений. В случае выявления несоответствий система должна уведомлять администратора и блокировать подозрительные операции.

5.3.4 Система должна быть устойчива к кибератакам, таким как DDoS, SQL-инъекции, XSS и другие. Для этого применяются механизмы защиты, включая фильтрацию входящих запросов, брандмауэры и системы предотвращения вторжений (IPS). Система должна проходить регулярное тестирование на проникновение для проверки её устойчивости.

5.3.5 Система должна обеспечивать непрерывную работу, исключая случаи простоев, которые могут повлиять на выполнение критических задач. Для этого предусмотрены механизмы отказоустойчивости, такие как резервные серверы и автоматическое переключение между ними в случае сбоя.

5.3.6 Система должна поддерживать безопасное создание, изменение и удаление учётных записей. Администраторы обязаны следовать строгим процедурам контроля изменений, чтобы исключить возможность несанкционированного создания или изменения учётных данных.

5.3.7 В системе должны быть предусмотрены процедуры реагирования на инциденты безопасности. Это включает автоматическое уведомление администратора о подозрительных действиях, подробное логирование событий и восстановление данных из резервных копий в случае нарушения.

5.3.8 Система должна включать инструменты мониторинга, которые обеспечивают постоянный контроль за её состоянием. Эти инструменты обязаны отслеживать возможные аномалии, вести сбор данных о поведении пользователей и предоставлять аналитические отчёты для предотвращения угроз.

5.3.9 Система должна поддерживать возможность регулярного обновления, направленного на устранение выявленных уязвимостей и добавление новых средств защиты. Обновления должны проходить тестирование перед их развёртыванием, чтобы избежать негативного влияния на текущую работу системы.

## 5.4 Требования к информационной безопасности

5.4.1 Система должна обеспечивать защиту всех данных пользователей от несанкционированного доступа. Для этого необходимо использовать шифрование данных как при их хранении, так и при передаче. Должны применяться современные криптографические алгоритмы, такие как AES-256 для хранения данных и протоколы SSL/TLS для защиты сетевого взаимодействия. Особое внимание должно уделяться защите персональных данных и другой конфиденциальной информации.

5.4.2 Все данные, передаваемые между компонентами системы, должны быть защищены от перехвата или модификации. Для этого обязательным требованием является использование зашифрованных каналов передачи данных, включая HTTPS. Также требуется защита от атак типа "человек посередине" (Man-in-the-Middle).

5.4.3 Каждый пользователь должен проходить процесс идентификации и аутентификации перед доступом к системе. Механизмы аутентификации должны включать поддержку многофакторной аутентификации для повышения уровня безопасности. Кроме того, система должна блокировать доступ после нескольких неудачных попыток входа.

5.4.4 Система должна обеспечивать разграничение доступа к ресурсам на основе ролевой модели или других гибких методов управления доступом. Пользователи могут видеть и изменять только те данные, которые разрешены их уровнем доступа. Любая попытка получить доступ к запрещённым ресурсам должна фиксироваться в журнале событий.

5.4.5 Система должна быть защищена от распространённых киберугроз, включая DDoS-атаки, SQL-инъекции, XSS, брутфорс и другие. Для этого необходимо внедрить межсетевые экраны, системы предотвращения вторжений (IPS) и настроить фильтры безопасности. Регулярное сканирование на уязвимости и тестирование на проникновение помогут поддерживать высокий уровень защиты.

5.4.6 Система должна фиксировать все события, связанные с доступом пользователей, изменением данных и системными сбоями. Журналы событий должны быть защищены от несанкционированного изменения и доступны только администраторам.

5.4.7 Система должна поддерживать регулярное обновление программного обеспечения с целью устранения уязвимостей и обеспечения соответствия современным стандартам безопасности. Обновления должны быть протестированы перед их развёртыванием в рабочей среде.

5.4.8 Необходимо реализовать процедуру регулярного резервного копирования всех критически важных данных. Резервные копии должны храниться в зашифрованном виде на изолированных носителях. В случае утраты данных процедура восстановления должна быть быстрой и надёжной.

5.4.9 Доступ к данным и системным функциям со стороны сотрудников организации должен быть ограничен на основании их должностных полномочий. Все действия, выполняемые пользователями с расширенными правами, должны фиксироваться в журнале событий для последующего аудита.

5.4.10 Система должна соответствовать актуальным нормативным требованиям в области защиты информации, таким как GDPR, ISO/IEC 27001 и локальные законы о защите персональных данных.

## 5.5 Требования к патентной чистоте

5.5.1 Система должна быть разработана таким образом, чтобы её функциональность, технологии и архитектура не нарушали патентные права третьих лиц.

5.5.2 На этапе проектирования и разработки системы должна быть выполнена проверка уникальности используемых технологий, алгоритмов и методов. Для этого требуется провести предварительный поиск зарегистрированных патентов в соответствующих областях, чтобы убедиться в отсутствии совпадений. Уникальность технологий подтверждается документально.

5.5.3 При разработке предпочтение должно отдаваться открытым стандартам и технологиям, которые свободно доступны и не защищены патентами.

5.5.4 Если в системе предполагается использование стороннего программного обеспечения, библиотек или инструментов, необходимо обеспечить строгое соблюдение условий их лицензий. Должны быть учтены ограничения, накладываемые лицензионными соглашениями, чтобы исключить нарушение интеллектуальных прав.

5.5.5 На каждом этапе разработки необходимо вести документальный учёт проведённых проверок на патентную чистоту. Должен быть составлен отчёт, подтверждающий, что разработка не нарушает патентные права третьих лиц. Этот отчёт предоставляет заказчику гарантию безопасности использования системы.

5.5.6 Для проверки патентной чистоты рекомендуется привлекать юридических специалистов, обладающих экспертным знанием в области интеллектуальной собственности.

5.5.7 Все результаты работ, включая программный код, алгоритмы и документы, должны быть переданы заказчику с гарантией исключительных прав на их использование. Это включает обеспечение отсутствия скрытых обязательств перед третьими лицами или зависимости от патентов, которые могут ограничить эксплуатацию системы.

# 6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

## 6.1 Требования к информационному обеспечению

6.1.1 Информационное обеспечение системы должно предусматривать централизованное хранение всех данных, необходимых для её функционирования. Это включает учётные записи пользователей, роли, права доступа и журналы событий. Централизованное хранилище исключает дублирование данных и упрощает управление информацией.

6.1.2 Данные должны быть классифицированы в зависимости от уровня их важности и конфиденциальности. Конфиденциальные данные, такие как персональная информация пользователей и настройки системы, подлежат шифрованию для предотвращения их утечки.

6.1.3 Входная информация системы включает данные аутентификации пользователей и параметры их действий. Она должна быть обработана в реальном времени, чтобы обеспечить своевременный доступ к ресурсам системы.

6.1.4 Выходные данные включают отчёты о действиях пользователей, результаты аналитики и журналы изменений. Они предоставляются администраторам для анализа, принятия решений и выявления угроз безопасности.

6.1.5 Система должна поддерживать механизм автоматического обновления данных для обеспечения их соответствия текущей ситуации. Это включает синхронизацию информации о пользователях и настройках безопасности.

6.1.6 Резервное копирование информации должно быть автоматизированным и проводиться регулярно в заранее установленные периоды. Хранение резервных копий требуется организовать на защищённых носителях или в облачных сервисах.

6.1.7 Документация должна содержать описание структуры информационной базы, форматы входных и выходных данных, а также протоколы их передачи. Администраторы и разработчики должны иметь доступ к документации для упрощения сопровождения и модернизации системы.

## 6.2 Требования к математическому обеспечению

6.2.1 Математическое обеспечение системы должно включать набор алгоритмов, обеспечивающих корректную обработку данных, поступающих от пользователей. Это включает алгоритмы для проверки подлинности данных, шифрования, декодирования и анализа активности пользователей. Особое внимание должно быть уделено алгоритмам, которые используются для шифрования конфиденциальной информации, таким как AES или RSA.

6.2.2 Система должна поддерживать математические методы для анализа данных и прогнозирования потенциальных угроз.

6.2.3 Математическое обеспечение должно включать модели, позволяющие эффективно управлять правами доступа.

6.2.4 Система должна включать алгоритмы, обеспечивающие контроль целостности данных.

6.2.5 Математическое обеспечение должно включать методы оптимизации для повышения производительности системы. Это может включать алгоритмы кэширования, распределения нагрузки между серверами и минимизации времени обработки запросов.

6.2.6 Должны быть реализованы алгоритмы для восстановления данных в случае их утраты. Это включает модели реконструкции информации из резервных копий и методы проверки их корректности.

6.2.7 Для оценки устойчивости системы и её поведения под нагрузкой необходимо использовать математическое моделирование.

6.2.8 Документация должна содержать полное описание используемых моделей и алгоритмов, включая их математические основы, предположения и ограничения.

## 6.3 Требования к программному обеспечению

6.3.1 Программное обеспечение системы должно обеспечивать выполнение всех необходимых функций, включая аутентификацию пользователей, управление доступом, мониторинг событий и обработку данных. Оно должно быть гибким и адаптируемым для интеграции с внешними платформами и облачными сервисами, а также поддерживать работу в распределённых сетях.

6.3.2 В программное обеспечение необходимо внедрение механизмов автоматического восстановления и резервного копирования данных.

6.3.3 Все компоненты программного обеспечения должны соответствовать современным стандартам информационной безопасности.

6.3.4 Программное обеспечение должно быть разработано с учётом возможности масштабирования.

6.3.5 Программное обеспечение должно быть совместимо с различными операционными системами и устройствами. Это включает поддержку Windows, Linux, macOS, а также работу на мобильных платформах, таких как Android и iOS.

6.3.6 Интерфейс программного обеспечения должен быть интуитивно понятным и доступным для пользователей с различным уровнем подготовки. Все основные функции должны быть легко доступны и сопровождаться инструкциями.

6.3.7 Все компоненты программного обеспечения должны быть подробно документированы. Документация должна включать описание архитектуры, функций, интерфейсов и требований к установке.

6.3.8 Программное обеспечение должно поддерживать регулярное обновление, направленное на устранение выявленных ошибок, повышение уровня безопасности и добавление новых функций. Процесс обновления должен быть автоматизированным и минимально влияющим на работу системы.

6.3.9 Программное обеспечение должно включать встроенные инструменты для интеграции с внешними системами и приложениями. Это включает API и возможности взаимодействия с корпоративными платформами, такими как ERP и CRM.

## 6.4 Требования к техническому обеспечению

6.4.1 Серверы должны быть оснащены высокопроизводительными процессорами, достаточным объёмом оперативной памяти и системами хранения данных высокой ёмкости.

6.4.2 Необходимо использование современного сетевого оборудования, которое поддерживает высокоскоростную передачу данных и защищённые протоколы связи.

6.4.3 Техническое обеспечение должно предусматривать наличие резервных серверов, которые будут включаться в работу в случае отказа основного оборудования.

6.4.4 Система должна быть оборудована специализированными аппаратными средствами защиты информации, такими как аппаратные шифраторы, брандмауэры и устройства предотвращения атак.

6.4.5 Резервное копирование данных должно осуществляться на отдельные серверы или в облачные хранилища. Техническое обеспечение должно включать оборудование, необходимое для автоматизации процесса резервного копирования и восстановления данных.

## 6.5 Требования к организационному обеспечению

6.5.1 Для эффективного функционирования системы требуется чёткое распределение обязанностей между всеми участниками процесса. Администраторы системы отвечают за управление доступом, мониторинг безопасности и сопровождение программного обеспечения.

6.5.2 Должны быть разработаны и утверждены регламенты, определяющие правила использования системы, порядок аутентификации, ограничения для пользователей и меры реагирования на инциденты безопасности. Регламент должен быть доступен всем сотрудникам и регулярно обновляться.

6.5.3 Все пользователи системы, включая администраторов, должны пройти обязательное обучение, направленное на изучение принципов работы системы, правил безопасного использования и управления доступом. Обучение должно проводиться регулярно и включать обновления при внедрении новых функций системы.

6.5.4 На организационном уровне должна быть реализована строгая система управления доступом к ресурсам.

6.5.5 Организация обязана разработать и внедрить план реагирования на инциденты, связанный с угрозами безопасности системы.

# 7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ

## 7.1 Этапы выполнения работ

7.1.1 На этом этапе проводится сбор и анализ всех требований к системе, включая технические, функциональные, организационные и информационные аспекты. Осуществляется консультация с заинтересованными сторонами, уточнение целей и задач системы, а также формулирование требований к её архитектуре и компонентам.

7.1.2 Разрабатывается проект системы, включающий её архитектуру, структуру модулей, взаимодействие между компонентами и описание используемых технологий. Подготавливается техническое задание, а также проводится выбор программных и аппаратных средств.

7.1.3 На следующем этапе разрабатываются модули программного обеспечения в соответствии с утверждённым проектом. Включает в себя программирование, написание алгоритмов и интеграцию отдельных компонентов. Также осуществляется разработка интерфейса для конечных пользователей.

7.1.4 Выполняется проверка всех модулей системы на соответствие требованиям, функциональность и стабильность работы. Проводится тестирование на наличие ошибок, оценка производительности, а также тестирование безопасности и устойчивости к внешним воздействиям.

7.1.5 После завершения тестирования система устанавливается на серверное оборудование и настраивается для работы в реальной инфраструктуре. Производится интеграция с внешними системами и обучение сотрудников организации работе с новой системой.

7.1.6 Обеспечивается сопровождение системы после её внедрения, включая обновление программного обеспечения, исправление ошибок, мониторинг безопасности и предоставление консультаций пользователям. Также осуществляется регулярный аудит системы для её оптимизации и модернизации.

## 7.2 Основные виды работ

7.2.1 Интервью с заинтересованными сторонами, анализ текущей инфраструктуры и документов для формирования четкого перечня требований.

7.2.2 Создание подробного описания функций, модулей и компонентов системы, её архитектуры, интерфейсов и методов взаимодействия.

7.2.3 Написание исходного кода, создание алгоритмов, настройка модулей и реализация интерфейса пользователя.

7.2.4 Проведение функционального, нагрузочного, интеграционного и безопасности тестирования, включая моделирование возможных угроз.

7.2.5 Настройка взаимодействия с внешними платформами, такими как Active Directory, CRM или другие корпоративные системы.

7.2.6 Подготовка обучающих материалов и проведение тренингов для сотрудников, которые будут работать с системой.

7.2.7 Разработка полного комплекта документации, включая пользовательские инструкции, отчёты по тестированию, архитектурные схемы и эксплуатационные регламенты.

7.2.8 Проведение регулярных проверок на соответствие системы требованиям, а также её доработка для повышения производительности и безопасности.

# 8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ

8.1 На этапе подготовки к приёмке в эксплуатацию должна быть завершена установка и настройка всех компонентов системы, включая серверное оборудование, программное обеспечение и интеграцию с внешними системами. Также необходимо провести обучение персонала, который будет работать с системой, и предоставить доступ к документации, необходимой для её эксплуатации.

8.2 Перед передачей системы в эксплуатацию проводится проверка её соответствия всем установленным требованиям. Это включает оценку её функциональности, надёжности, безопасности и производительности в соответствии с техническим заданием. Проверка осуществляется на основании заранее утверждённого перечня критериев приёмки.

8.3 Система должна быть протестирована в условиях, максимально приближённых к реальной эксплуатации. Это включает проверку всех основных функций, взаимодействие с внешними системами, выполнение процедур аутентификации и авторизации, а также моделирование возможных отказов и нагрузок.

8.4 По результатам тестирования выявленные ошибки и несоответствия требованиям должны быть устранены. После внесения корректировок проводится повторное тестирование для подтверждения исправления проблем.

8.5 Все этапы проверки и тестирования системы должны быть документированы. Итоговый отчёт включает описание проведённых тестов, выявленных проблем, способов их решения и оценки соответствия системы требованиям.

8.6 По итогам успешного завершения всех проверок и тестирований составляется приёмочный акт, который подписывается представителями заказчика и исполнителя. После подписания акта система считается принятой в эксплуатацию.

# 9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

9.1 Документация должна включать полный перечень всех документов, необходимых для сопровождения, эксплуатации и модернизации системы. Это включает техническую документацию, пользовательские инструкции, отчёты по тестированию, схемы архитектуры системы и регламенты использования.

9.2 Техническая документация должна содержать описание архитектуры системы, её компонентов, взаимодействия модулей, используемых алгоритмов и технологий. Также в ней должны быть указаны требования к аппаратному и программному обеспечению.

9.3 Должны быть разработаны подробные инструкции для всех категорий пользователей системы, включая администраторов, конечных пользователей и сотрудников технической поддержки. Инструкции должны содержать описание основных функций и процедур, таких как вход в систему, управление доступом и работа с интерфейсом.

9.4 Документация должна включать регламенты эксплуатации системы, определяющие правила использования, порядок обновления, резервного копирования и восстановления данных. Регламенты также должны включать процедуры реагирования на инциденты и порядок взаимодействия с технической поддержкой.

9.5 Результаты всех проведённых тестов должны быть оформлены в виде отчётов. Эти отчёты должны содержать описание целей и методов тестирования, выявленных проблем, их устранения и итоговой оценки системы.

9.6 Документация должна регулярно обновляться по мере внесения изменений в систему. Это касается обновлений программного обеспечения, модификации функций и добавления новых компонентов. Обновлённая версия документации должна своевременно предоставляться пользователям и администраторам.

9.7 Все документы должны храниться в электронном и бумажном виде. Доступ к документации должен быть организован таким образом, чтобы пользователи имели возможность быстро получить необходимые сведения при работе с системой.