**МИНИСТЕРСТВО ТРАНСПОРТА И КОММУНИКАЦИЙ**

**РЕСПУБЛИКИ БЕЛАРУСЬ**

**УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ**

**«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**

**Автоматизированная система  
аутентификации и авторизации  
(СУДА «SecureAuth Pro»)**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**2022**

# СОДЕРЖАНИЕ

[СОДЕРЖАНИЕ 2](#_Toc132710187)

[1 ВВЕДЕНИЕ 3](#_Toc132710188)

[2 ОБЩИЕ СВЕДЕНИЯ 3](#_Toc132710189)

[3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ АС ТЕХКАРТА 3](#_Toc132710190)

[3.1 Назначение СУДА «SecureAuth Pro» 3](#_Toc132710191)

[3.2 Цели создания СУДА «SecureAuth Pro» 3](#_Toc132710192)

[3.2.1 Цели создания СУДА «SecureAuth Pro»: 3](#_Toc132710193)

[4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СУДА «SECUREAUTH PRO» И СУЩЕСТВУЮЩЕЙ СИСТЕМЫ РАЗРАБОТКИ ТЕХНОЛОГИЧЕСКОЙ КАРТЫ СТАНЦИИ 4](#_Toc132710194)

[4.1 Общая характеристика объектов СУДА SecureAuth Pro 4](#_Toc132710195)

[4.2 Существующая система разработки системы управления доступом и аутентификации 4](#_Toc132710196)

[5 ТРЕБОВАНИЯ К СУДА «SECUREAUTH PRO» 4](#_Toc132710197)

[5.1 Требования к структуре 4](#_Toc132710198)

[5.2 Требования к процедурам доступа системы управления доступом и аутентификации 5](#_Toc132710199)

[5.3 Требования к функциональной безопасности 7](#_Toc132710200)

[5.4 Требования к информационной безопасности 7](#_Toc132710201)

[5.5 Требования к патентной чистоте 7](#_Toc132710202)

[6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ 8](#_Toc132710203)

[6.1 Требования к информационному обеспечению 8](#_Toc132710204)

[6.2 Требования к математическому обеспечению 8](#_Toc132710205)

[6.3 Требования к программному обеспечению 8](#_Toc132710206)

[6.4 Требования к организационному обеспечению 8](#_Toc132710207)

[6.5 Требования к техническому обеспечению 9](#_Toc132710208)

[7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ 9](#_Toc132710209)

[8 ПОРЯДОК ПРИЕМКИ СУДА «SECUREAUTH PRO» В ЭКСПЛУАТАЦИЮ 10](#_Toc132710210)

[9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ 10](#_Toc132710211)

# 1 **ВВЕДЕНИЕ**

Данное техническое задание разработано с целью создания автоматизированной системы аутентификации и авторизации (СУДА «SecureAuth Pro») для обеспечения безопасного доступа пользователей к системе, контроля и управления их правами доступа.

# 2 ОБЩИЕ СВЕДЕНИЯ

2.1 Полное наименование: Система управления доступом и аутентификации: «SecureAuth Pro».

2.2 Сокращенное наименование: СУДА «SecureAuth Pro».

2.3 Заказчик: ИП Козлов В.Г., 246653, ул. Кирова, д. 34;

2.4 Выполнение работ по этапам и стадиям работ, оформление и предъявление Заказчику их результатов осуществляется Исполнителем согласно требованиям данного технического задания.

# 3 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ АС ТЕХКАРТА

## 3.1 Назначение СУДА «SecureAuth Pro»

3.1.1 СУДА «SecureAuth Pro» предназначена для обеспечения безопасного и эффективного контроля доступа пользователей к информационной системе или веб-приложению.

3.1.2 Назначение СУДА «SecureAuth Pro»:

– осуществление процесса аутентификации и авторизации;

– проверка пароля на соответствие требованиям;

– хранение пароля пользователя в системе;

– уничтожение сессии при отсутствии активности пользователя в системе более 10 минут;

– наличие подсистемы сброса и восстановления данных учетной записи пользователя;

– наличие UML-диаграммы процесса аутентификации и авторизации пользователя в системе.

## 3.2 Цели создания СУДА «SecureAuth Pro»

## 3.2.1 Цели создания СУДА «SecureAuth Pro»:

* обеспечение безопасной аутентификации и авторизации пользователей: Система SecureAuth Pro разработана с целью гарантировать надежную аутентификацию и авторизацию пользователей на основе их учетных данных (логина и пароля) и обеспечивать соответствие паролей требованиям безопасности, таким как минимальная длина пароля, наличие цифр и символов разного регистра.
* защита от несанкционированного доступа: Система SecureAuth Pro использует современные методы шифрования и защиты паролей, что помогает предотвратить возможность несанкционированного доступа к системе и снижает риски утечки конфиденциальных данных.
* управление сессиями пользователей: Система SecureAuth Pro предусматривает управление сессиями пользователей, что позволяет автоматически завершать неактивные сессии после определенного периода времени (например, 10 минут), чтобы предотвратить несанкционированный доступ в случае пропуска пользователем системы.
* восстановление доступа: Система SecureAuth Pro предусматривает подсистему сброса и восстановления учетных записей пользователей, что помогает пользователям восстановить доступ к своей учетной записи в случае утери пароля или блокировки аккаунта.
* визуализация процесса аутентификации и авторизации: Система SecureAuth Pro предусматривает создание UML-диаграммы процесса аутентификации и авторизации пользователя, что помогает визуализировать этот процесс, облегчает понимание его работы и улучшает процесс разработки и отладки системы.

3.2.2 Решение комплекса задач по автоматизации процесса аутентификации и авторизации:

– позволяет обеспечить более высокий уровень безопасности за счет проверки учетных данных пользователей, использования современных методов шифрования, контроля сессий пользователей и других мер защиты;

– сокращает риски несанкционированного доступа, утечки конфиденциальных данных и других угроз безопасности;

– позволяет снизить ручные операции и упростить процедуры, связанные с проверкой учетных данных пользователей;

– увеличивает эффективность работы системы, так как она позволяет быстро и точно проверять учетные данные пользователей, управлять сессиями, восстанавливать доступ и выполнять другие операции без необходимости вручную вмешиваться в каждый случай;

– снижает затраты на обслуживание системы и улучшает общую производительность;

# 4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СУДА «SECUREAUTH PRO» И СУЩЕСТВУЮЩЕЙ СИСТЕМЫ РАЗРАБОТКИ ТЕХНОЛОГИЧЕСКОЙ КАРТЫ СТАНЦИИ

## 4.1 Общая характеристика объектов СУДА SecureAuth Pro

4.1.1 Объектами СУДА SecureAuth Pro являются учетные записи пользователей, методы аутентификации, а также правила авторизации.

4.1.2 Типовой перечень разделов для включения в технологическую карту промежуточной железнодорожной станции приведен в приложении А.

4.1.3 Перечень и содержание табличных видов форм в СУДА SecureAuth Pro приведены в приложении Б.

4.1.3 Описание разделов СУДА SecureAuth Pro приведено в приложении В.

## 4.2 Существующая система разработки системы управления доступом и аутентификации

4.2.1 Разработка системы управления доступом и аутентификации производится в соответствии с СТП 09150.11.118-2009 «Информационные технологии. Создание, эксплуатация и сопровождение автоматизированных систем. Правила документирования.».

# 5 ТРЕБОВАНИЯ К СУДА «SECUREAUTH PRO»

## 5.1 Требования к структуре

5.1.1 Структура и содержание основных разделов СУДА SecureAuth Pro устанавливается согласно требованиям СТП 09150.11.118-2009 «Информационные технологии. Создание, эксплуатация и сопровождение автоматизированных систем. Правила документирования.».

5.1.2 Для реализации функций СУДА SecureAuth Pro предусматриваются следующие функциональные подсистемы:

* подсистема аутентификации: отвечает за процесс проверки подлинности пользователей при попытке входа в систему. Может включать различные методы аутентификации, такие как пароли, двухфакторная аутентификация, одноразовые пароли, биометрическая аутентификация и другие;
* подсистема авторизации: отвечает за определение прав доступа пользователей на основе их аутентификации. Может включать правила авторизации, определение ролей, групп доступа, а также настройку разрешений на уровне ресурсов или функций системы.
* подсистема управления учетными записями: отвечает за создание, управление и администрирование учетных записей пользователей. Может включать функции создания учетных записей, установки паролей, блокирования и разблокирования учетных записей, управления ролями и правами доступа, а также синхронизации с другими источниками идентификации, такими как каталоги LDAP или каталоги корпоративных ресурсов;
* подсистема самообслуживания пользователей: отвечает за предоставление возможностей самообслуживания пользователям, таких как сброс пароля, разблокировка учетной записи, обновление профиля и другие операции без необходимости обращения в службу поддержки. Может включать веб-интерфейс или мобильное приложение для пользователей, а также механизмы безопасной идентификации пользователя при выполнении операций самообслуживания;
* подсистема мониторинга угроз и защиты от атак: отвечает за обнаружение, мониторинг и защиту от различных угроз и атак на систему SecureAuth Pro. Может включать систему обнаружения вторжений (IDS), защиту от атак на основе анализа поведения, защиту от фишинговых атак, антивирусную защиту и другие меры для обеспечения безопасности системы;
* подсистема поддержки и обновлений: отвечает за предоставление технической поддержки, обновлений системы SecureAuth Pro и решения проблем пользователей. Может включать доступ к базе знаний, системе тикетов для поддержки, обновлениям системы и другим ресурсам для поддержания надлежащей работы системы.

## 5.2 Требования к процедурам доступа системы управления доступом и аутентификации

5.2.1 Функции доступа к СУДА «SecureAuth Pro» реализуются с различными уровнями доступа к информации.

5.2.2 Пользователи:

* аутентификация: Пользователи должны успешно пройти процедуру аутентификации, чтобы получить доступ к системе. Это может включать ввод учетных данных, таких как логин и пароль, использование многофакторной аутентификации (например, одноразовых паролей, SMS-кодов, биометрических данных и др.) или других методов, которые гарантируют, что пользователь является действительным и авторизованным пользователем;
* авторизация: После успешной аутентификации пользователю могут быть назначены соответствующие права доступа в системе на основе его роли, обязанностей и функций в организации. Например, администраторы могут иметь полные права доступа для управления настройками системы, а обычные пользователи могут иметь ограниченные права доступа только к определенным функциям или ресурсам;
* управление идентификационными данными: Пользователи могут иметь возможность управлять своими идентификационными данными, такими как смена пароля, обновление контактной информации, управление настройками безопасности и др., в рамках политик и правил организации.

5.2.3 Разработчики:

* создание и управление приложениями: разработчики могут иметь возможность создавать и управлять приложениями в системе СУДА «SecureAuth Pro». Это может включать регистрацию новых приложений, настройку и управление настройками безопасности, авторизацией, аутентификацией и другими настройками приложений;
* управление пользователями и ролями: разработчики могут иметь возможность управлять пользователями и их ролями в системе СУДА «SecureAuth Pro». Это может включать создание, редактирование и удаление учетных записей пользователей, присвоение и изменение ролей, определение прав доступа и других настроек пользователей;
* управление доступом: разработчики могут иметь возможность управлять правами доступа пользователей к ресурсам и сервисам в системе СУДА «SecureAuth Pro». Это может включать определение прав доступа на уровне ролей или на уровне конкретных ресурсов, настройку прав доступа к API, управление разрешениями на чтение, запись, удаление и другими действиями с данными и ресурсами;
* аутентификация и авторизация: разработчики могут иметь доступ к настройкам аутентификации и авторизации в системе СУДА «SecureAuth Pro». Это может включать настройку многофакторной аутентификации, установку и управление сертификатами безопасности, настройку методов аутентификации, таких как OAuth, SAML, LDAP и других, а также настройку правил авторизации и контроля доступа;
* мониторинг и аудит доступа: разработчики могут иметь возможность мониторинга и аудита доступа в системе СУДА «SecureAuth Pro». Это может включать просмотр журналов действий, анализ аудит-логов, мониторинг событий безопасности и другие меры для обнаружения и предотвращения несанкционированного доступа.

5.2.4 Руководство:

* управление политиками безопасности: руководство может иметь возможность определения и управления политиками безопасности в системе СУДА «SecureAuth Pro». Это может включать определение требований к паролям, установку правил авторизации, настройку политик блокировки аккаунтов и других мер безопасности;
* управление аудитом и мониторингом: руководство может иметь доступ к мониторингу и аудиту доступа в системе СУДА «SecureAuth Pro». Это может включать просмотр журналов действий, анализ аудит-логов, мониторинг событий безопасности и другие меры для обнаружения и предотвращения несанкционированного доступа;
* управление пользователями и ролями: руководство может иметь возможность управления пользователями и их ролями в системе СУДА «SecureAuth Pro». Это может включать создание, редактирование и удаление учетных записей пользователей, присвоение и изменение ролей, определение прав доступа и других настроек пользователей;
* мониторинг и управление ресурсами: руководство может иметь возможность мониторинга и управления ресурсами и сервисами в системе СУДА «SecureAuth Pro». Это может включать просмотр и управление правами доступа к ресурсам, контроль использования ресурсов, управление доступом к API и другими мерами для обеспечения безопасности и эффективного использования ресурсов;
* отчетность и аналитика: руководство может иметь доступ к отчетам и аналитике в системе СУДА «SecureAuth Pro». Это может включать генерацию отчетов о правах доступа, анализ данных о доступе и использовании ресурсов, оценку рисков безопасности и другие аналитические функции для оценки эффективности политик безопасности и обеспечения соответствия требованиям.

5.2.5 Администраторы:

* создание и управление пользователями: администраторы могут создавать, редактировать и удалять учетные записи пользователей в СУДА «SecureAuth Pro». Они также могут назначать и изменять роли и права доступа для пользователей;
* управление ролями и группами: администраторы могут создавать, редактировать и удалять роли и группы пользователей в СУДА «SecureAuth Pro». Они могут также определять права доступа, настройки политик безопасности и другие настройки для ролей и групп;
* управление правами доступа: администраторы могут определять и настраивать права доступа к ресурсам и приложениям в СУДА «SecureAuth Pro». Это может включать определение разрешенных действий (например, чтение, запись, удаление) и областей доступа (например, определенные каталоги, файлы, функции приложений) для пользователей, ролей и групп.

5.2.6 Доступ к СУДА «SecureAuth Pro» осуществляется на основании ввода имени пользователя и пароля, которые назначаются Администраторами СУДА «SecureAuth Pro».

5.2.7 Пароль должен состоять из 8 символов и более и содержать в себе цифры и буквы различного регистра.

5.2.8 В случае неправильного ввода пароля от учетной записи более 3 раз учетная запись блокируется.

5.2.9 Учет и хранение паролей выполняется администраторами СУДА «SecureAuth Pro». Пароли хранятся в базе данных СУДА «SecureAuth Pro» в зашифрованном виде.

5.2.10 При отсутствии активности пользователя в системе более 10 минут уничтожается сессия;

5.2.11 Должен быть предусмотрена возможность входа через протокол авторизации OAuth.

## 5.3 Требования к функциональной безопасности

5.3.1 Требования к функциональной безопасности СУДА "SecureAuth Pro" включают следующие аспекты:

* аутентификация и авторизация: СУДА должна обеспечивать надежную и безопасную аутентификацию пользователей, проверку их идентификации, а также авторизацию на основе ролей и прав доступа. Должны быть применены сильные механизмы аутентификации, такие как двухфакторная аутентификация (2FA) или множественные факторы безопасности, чтобы защитить от несанкционированного доступа;
* шифрование данных: данные, передаваемые между компонентами СУДА, должны быть защищены с использованием криптографических алгоритмов и протоколов, обеспечивающих конфиденциальность и целостность информации. Это может включать шифрование передаваемых данных по сети, хранение паролей и других конфиденциальных данных в зашифрованном виде, а также защиту ключей шифрования;
* управление правами доступа: СУДА должна обеспечивать гибкое и точное управление правами доступа пользователей на основе ролей, групп или других параметров. Это позволяет предоставлять минимально необходимые привилегии (принцип наименьших привилегий) и ограничивать доступ пользователей только к тем функциям и ресурсам, которые им действительно необходимы;
* защита от атак: СУДА должна включать меры защиты от различных видов атак, таких как атаки на перехват данных, внедрение злонамеренного кода, подделку данных и другие.

5.3.2 Программное обеспечение СУДА «SecureAuth Pro» должно обеспечивать во всех регламентированных условиях и режимах его эксплуатации требуемый уровень качества функционирования и требуемые уровни безопасности и надежности. Указанные требования должны достигаться выполнением модели качества соответственно ГОСТ 27.003-90.

## 5.4 Требования к информационной безопасности

5.4.1 При разработке СУДА «SecureAuth Pro» должны быть учтены следующие требования к информационной безопасности:

* конфиденциальность: СУДА должна обеспечивать защиту конфиденциальности информации, предотвращая несанкционированный доступ к данным пользователей, правам доступа, а также другим конфиденциальным данным, хранящимся в системе;
* целостность: СУДА должна гарантировать целостность информации, предотвращая несанкционированное изменение данных, прав доступа и других настроек системы. Все изменения должны быть отслеживаемы и подлежать контролю;
* доступность: СУДА должна быть доступной и функциональной для авторизованных пользователей в тех случаях, когда это необходимо. Должны быть предприняты меры для защиты от отказа в обслуживании (DoS) или других атак на доступность системы;
* физическая безопасность: СУДА должна быть защищена от несанкционированного физического доступа, включая защиту серверов, сетевого оборудования, баз данных и других физических ресурсов, на которых функционирует система.

## 5.5 Требования к патентной чистоте

5.5.1 При выполнении работ исполнителем обеспечивается патентная чистота результатов работ. Данная работа не должна содержать патентов, зарегистрированных в Республике Беларусь и других странах.

5.5.2 По требованию Заказчика Исполнитель представляет сведения о рыночной стоимости созданных при выполнении работ объектов интеллектуальной собственности.

# 6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ

## 6.1 Требования к информационному обеспечению

6.1.1 Информационное обеспечение должно выполнять все функции и задачи, для которых оно предназначено, соответствовать требованиям бизнес-процессов и быть удовлетворительным для пользователей.

6.1.2 Информационное обеспечение должно быть надежным, то есть обеспечивать стабильную и безотказную работу в течение требуемого времени, минимизировать возможность ошибок и сбоев, а также иметь механизмы резервного копирования и восстановления данных.

6.1.3 Информационное обеспечение должно быть защищено от несанкционированного доступа, взломов, утечек данных и других угроз безопасности. Это может включать механизмы аутентификации, авторизации, шифрования данных, мониторинга безопасности и другие меры.

6.1.4 Информационное обеспечение должно соответствовать требованиям законодательства, нормативных актов, стандартов и регуляторных требований в отношении защиты данных.

6.1.5 Информационное обеспечение должно иметь механизмы резервного копирования данных и возможности их восстановления в случае потери или повреждения, чтобы обеспечить защиту от потери данных и непрерывность бизнес-процессов.

6.1.6 Информационное обеспечение должно обеспечивать адекватную защиту конфиденциальности данных, включая механизмы шифрования, контроля доступа, аудита и другие технические и организационные меры, чтобы предотвращать несанкционированный доступ к конфиденциальным данным.

6.1.7 Информационное обеспечение должно быть удобным в использовании, иметь интуитивно понятный интерфейс, быть дружественным к пользователю и обеспечивать удовлетворение потребностей пользователей.

## 6.2 Требования к математическому обеспечению

6.2.1 Специальных требований к применению в подсистеме математических моделей, методов или типовых алгоритмов не предъявляется.

## 6.3 Требования к программному обеспечению

6.3.1 Программное обеспечение должно быть разработано и реализовано с соблюдением современных стандартов безопасной разработки, включая проверку на наличие уязвимостей, предотвращение инъекций, межсайтового скриптинга (XSS) и других уязвимостей, а также защиту от возможных атак на стороне сервера и клиента. 6.3.2 Программное обеспечение должно поддерживать механизмы шифрования данных, как в состоянии передачи, так и в состоянии хранения, чтобы обеспечить конфиденциальность и целостность данных.

6.3.3 Программное обеспечение должно предоставлять возможности для ведения аудита, то есть записи и мониторинга действий пользователей, с целью обнаружения и реагирования на потенциальные нарушения безопасности.

6.3.4 Программное обеспечение должно иметь механизмы управления правами доступа, позволяющие администраторам системы настраивать права доступа пользователей на основе их ролей, обязанностей и ограничений.

## 6.4 Требования к организационному обеспечению

6.5.1 Функционирование СУДА «SecureAuth Pro» не требует дополнительного оперативного эксплуатационного персонала.

6.5.2 Сопровождение СУДА «SecureAuth Pro» осуществляется специалистом Козловым В.Г.

## 6.5 Требования к техническому обеспечению

6.9.1 Техническое обеспечение должно обеспечивать защиту сетей и коммуникаций организации, включая использование защищенных протоколов, шифрования данных, виртуальных частных сетей (VPN), брандмауэров и других механизмов защиты сетевых ресурсов.

6.9.2 Техническое обеспечение должно быть защищено от несанкционированного доступа физическими мерами, такими как ограниченный доступ в помещения с техническим оборудованием, видеонаблюдение, контроль доступа и другие меры физической безопасности.

6.9.3 Техническое обеспечение должно иметь механизмы защиты от вредоносного программного обеспечения, такие как антивирусные программы, антишпионские программы и фаерволы, для обнаружения и предотвращения атак со стороны вредоносного ПО.

# 7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ

7.1 Состав, содержание и этапность выполнения работ определяются согласно календарному плану к договору.

7.2 Заказчик организует поставку необходимого оборудования и лицензионного программного обеспечения.

7.3 Состав и перечень документов, предъявляемых по окончании соответствующих стадий и этапов, определяется в соответствии с договором на разработку СУДА «SecureAuth Pro».

7.4 Основные этапы разработки выполняются в соответствии с нормативными документами.

# 8 ПОРЯДОК ПРИЕМКИ СУДА «SECUREAUTH PRO» В ЭКСПЛУАТАЦИЮ

8.1 Проверка наличия всех необходимых компонентов.

8.2 Проверка конфигурации системы.

8.3 Тестирование функциональности.

8.4 Подготовка документации.

8.5 Подписание акта приемки.

8.6 Последующее обслуживание.

# 9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

9.1 Вся разрабатываемая документация оформляется в соответствии с действующими нормативными документами.

9.2 К СУДА «SecureAuth Pro» должна прилагаться инструкция пользователю. Рабочая документация должна соответствовать действующим стандартам и ГОСТ, ЕСКД и ЕСПД.

**НАСТОЯЩЕЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ МОЖЕТ УТОЧНЯТЬСЯ И КОРРЕКТИРОВАТЬСЯ ПО ВЗАИМНОЙ ДОГОВОРЕННОСТИ МЕЖДУ ИСПОЛНИТЕЛЕМ И ЗАКАЗЧИКОМ В РАБОЧЕМ ПОРЯДКЕ.**