**ЛАБОРАТОРНАЯ РАБОТА №4**

**РАЗРАБОТКА ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ НА СОЗДАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ (АС АиА)**

На 10 листах

**СОДЕРЖАНИЕ**

**1 ОБЩИЕ СВЕДЕНИЯ3**

**2 ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ3**

**3 НАЗНАЧЕНИЯ И ЦЕЛИ СОЗДАНИЯ3**

3.1 Назначение3

3.2 Цели создания3

**4 ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ4**

**5 ТРЕБОВАНИЯ К СИСТЕМЕ5**

5.1 Требования к структуре5

5.2 Требования к процедурам доступа к системе5

5.3 Требования к функциональной безопасности5

5.4 Требования к информационной безопасности6

5.5 Требования к патентной чистоте7

**6 ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ7**

6.1 Требования к информационному обеспечению7

6.2 Требования к математическому обеспечению8

6.3 Требования к программному обеспечению8

6.4 Требования к техническому обеспечению8

6.5 Требования к организационному обеспечению8

**7 СОСТАВ И СОДЕРЖАНИЕ РАБОТ9**

**8 ПОРЯДОК ПРИЕМКИ В ЭКСПЛУАТАЦИЮ10**

**9 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ10**

1. ОБЩИЕ СВЕДЕНИЯ
   1. Наименование работы: разработка технических требований на автоматизированную систему аутентификации и авторизации в соответствие с СТП 09150.11.118-2009 (АС АиА).
   2. Заказчик АС и Ответственный по проекту: заказчик АС – Государственное объединение «Белорусская железная дорога»; Ответственный по проекту – Служба информационных технологий Государственного объединения «Белорусская железная дорога».
   3. Наименование Организации-пользователя АС: Государственное объединение «Белорусская железная дорога».
   4. Наименование объекта внедрения: службы и подразделения Белорусской железной дороги, информационная система Белорусской железной дороги.
2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ
   1. В изложенных технических требованиях применены термины, сокращения и определения в следующем значении:
      1. Аутентификация – проверка подлинности пользователя путём сравнения введённого им пароля с паролем, сохранённым в базе данных;
      2. Авторизация – процесс предоставления пользователю или группе пользователей определенных разрешений, прав доступа и привилегий;
      3. АС – автоматизированная система;
      4. ИС – информационная система;
      5. ЕСИА – Информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем»;
      6. ЕСПД – Единая система программной документации;
      7. ППО – прикладное программное обеспечение;
      8. ТЗ – техническое задание;
      9. ТП – технический проект;
      10. ПО – программное обеспечение.
      11. ТТ ­ технические требования
3. НАЗНАЧЕНИЯ И Цели создания
   1. Назначение
      1. Назначение разработки АС аутентификации и авторизации для сотрудников и пользователей информационной системы состоит в обеспечении безопасного доступа к информационным ресурсам компании.
      2. Разработка подобной системы способствует увеличению безопасности информационных ресурсов и защите конфиденциальных данных компании от несанкционированного доступа. Это также обеспечивает эффективное функционирование информационной системы.
   2. **Цели создания**
      1. Разработка преследует следующие цели и задачи:

* Обеспечение безопасности. Система должна гарантировать, что только авторизованные пользователи могут получить доступ к конфиденциальным данным и ресурсам компании, предотвращая несанкционированный доступ и потенциальные угрозы безопасности.
* Управление доступом. Автоматизированная система позволяет управлять правами доступа сотрудников и пользователей, определяя, к каким данным и функциям каждый из них имеет доступ в соответствии с их ролью и обязанностями.
* Удобство использования. Создание простого и удобного интерфейса для аутентификации и авторизации упрощает процесс работы с информационными системами, повышая эффективность работы и производительность сотрудников.
* Мониторинг и аудит. Система должна предоставлять возможность отслеживать действия пользователей, регистрировать входы и выходы, а также анализировать активность для контроля со стороны руководства, выявления аномалий и возможных угроз безопасности.
* Соблюдение нормативов. Разработка системы аутентификации и авторизации должна учитывать существующие в ИС Белорусской железной дороги технологии и соблюдение соответствующих нормативов и стандартов в области безопасности информации и защиты персональных данных, которые актуальны на момент разработки.

1. ХАРАКТЕРИСТИКА ОБЪЕКТОВ СИСТЕМЫ РАЗРАБОТКИ
   1. Автоматизация процессов авторизации и аутентификации представляет собой внедрение специализированных программных средств для обеспечения безопасности доступа к информационным ресурсам.
   2. Объекты автоматизации – процессы аутентификации и авторизации пользователей в ИС Белорусской железной дороги.
   3. Участники данных процессов – это: ­

* пользователи информационно-телекоммуникационной сети «Интернет», незарегистрированные в ЕСИА; ­
* работники структурных подразделений Белорусской железной дороги; ­
  1. Автоматизированные системы аутентификации, такие как одноразовые пароли, биометрическая идентификация или многофакторная аутентификация, повышают уровень безопасности за счет точности и сложности проверки подлинности.
  2. Автоматизация процесса авторизации позволяет быстро и точно определить права доступа пользователя к различным ресурсам, что снижает вероятность ошибок и угроз безопасности утечки и потери информационных ресурсов.
  3. ИС подразумевает доступ пользователей к системе в режиме «клиент-сервер», с использованием Web технологий.

1. Требования к системе
   1. **Требования к структуре**
      1. В качестве платформы для построения АС должно использоваться программное обеспечение с открытым исходным кодом, для дополнительной безопасности. Проектирование АС должно базироваться на сервисно-ориентированной архитектуре:

* уровень представления информации;
* уровень прикладной бизнес логики;
* уровень транспортировки сервисов;
* уровень хранения и обработки данных (сервер базы данных).
  + 1. Система должна быть построена с использованием модульной архитектуры, позволяющей легко добавлять новые методы аутентификации и авторизации и новых пользователей, а также интегрировать её с другими уже существующими информационными системами и сервисами.
  1. **Требования к процедурам доступа к системе**
     1. Пользователи должны проходить процедуру регистрации, включающую проверку личности и установку уникального идентификатора (логина) и пароля. Пароль пользователя должен быть не менее 8 символов и обязательно содержать цифры и латинские символы разного регистра, также допускается возможность содержания специальных символов. Такие же требования используются при аутентификации.
     2. Проверка пароля на соответствие требованиям должна осуществляться на стороне клиента.
     3. Система должна поддерживать различные методы аутентификации, включая парольные, биометрические, одноразовые пароли и многофакторную аутентификацию.
     4. Администраторы должны иметь возможность управлять правами доступа пользователей в соответствии с их ролями и обязанностями в организации.
     5. Процедуры управления доступом должны быть оперативными, прозрачными и гибкими, позволяя быстро реагировать на изменения в структуре организации и потребности пользователей.
     6. Пользователи, обладающие доступом к конфиденциальным данным или критическим ресурсам, должны проходить многофакторную аутентификацию для повышения уровня безопасности.
     7. Пользователи должны быть ознакомлены с политиками безопасности, регламентирующими правила использования системы и обязанности пользователей по обеспечению безопасности информации.
     8. Максимальный период неактивности пользователя – 10 минут. После этого сессия уничтожается, пользователь должен вновь проходить процедуру авторизации.
  2. **Требования к функциональной безопасности**
     1. Система должна обеспечивать защиту от несанкционированного доступа путем эффективного управления аутентификацией и авторизацией пользователей.
     2. Должны быть реализованы меры по предотвращению атак перебора паролей, подбора идентификаторов и других типов атак на аутентификацию.
     3. Система должна обеспечивать гранулярный контроль доступа к ресурсам на основе ролей, прав и политик безопасности.
     4. Должны быть предусмотрены механизмы аудита и мониторинга, позволяющие отслеживать действия пользователей и выявлять подозрительную активность.
     5. Система должна обеспечивать шифрование паролей, чтобы защитить пользователей от несанкционированного доступа.
     6. Должны использоваться современные алгоритмы шифрования и протоколы безопасности для обеспечения надежной защиты паролей и информации.
     7. Система должна обрабатывать ошибки и исключения безопасным образом, чтобы предотвращать утечку чувствительной информации и иные нарушения безопасности.
     8. Должны быть предусмотрены механизмы резервного копирования и восстановления данных для обеспечения доступности информации в случае аварийных ситуаций или сбоев. При наличии резервных копий данных возможно полное восстановление информации. Это позволяет минимизировать потери информации, обеспечивает бесперебойную работу организации и способствует быстрому восстановлению после возникновения проблем.
     9. Должны быть предусмотрены варианты сброса пароля, либо же восстановления данных по заранее введенной информации. Должны использоваться логин, адрес электронной почты или номер телефона.
  3. **Требования к информационной безопасности**
     1. Данные пользователей, включая учетные записи и пароли, должны храниться и передаваться в зашифрованном виде.
     2. Должны быть приняты меры для защиты информации от несанкционированных изменений или полного удаления.
     3. Должны использоваться методы хэширования для обеспечения целостности хранимых данных и их защиты от подмены или искажения.
     4. Система должна обеспечивать доступность информации для авторизованных пользователей в том случае, если это необходимо для нормального функционирования бизнес-процессов, соответствующих их ролям в системе.
     5. Система должна защищаться от различных угроз, включая внешние атаки (например, DDoS-атаки, SQL-инъекции), внутренние угрозы (например, утечки данных) и другие типы атак.
     6. Должны быть приняты меры по обнаружению и предотвращению угроз, а также механизмы быстрого реагирования на инциденты безопасности.
     7. Система должна регулярно обновляться и мониториться на наличие уязвимостей и потенциальных угроз безопасности.
     8. Должны быть приняты меры по оперативному реагированию на обнаруженные уязвимости и обновлению системы для их исправления.
  4. **Требования к патентной чистоте**
     1. При проектировании системы следует предпочтительно использовать открытые стандарты и протоколы, которые не защищены патентами и свободно доступны для использования.
     2. Если необходимо использовать патентно-защищенные методы или технологии, следует убедиться в наличии соответствующих лицензий или разрешений на их использование.
     3. Если в ходе разработки системы ведется сотрудничество с третьими сторонами или исполнителями, необходимо заключить с ними соглашения о неразглашении, чтобы предотвратить возможные споры относительно интеллектуальной собственности.
     4. Все этапы проверки патентной чистоты и принятые меры по обеспечению соблюдения патентного законодательства должны быть документированы для последующего аудита и подтверждения соответствия.

1. **ТРЕБОВАНИЯ К ВИДАМ ОБЕСПЕЧЕНИЯ**
   1. **Требования к информационному обеспечению**
      1. Состав, структура и способы организации данных в АС должны быть определены на этапе рабочего проектирования. Информационный обмен данными в системе должен осуществляться с помощью разработанного защищенного коммуникационного протокола передачи данных. Хранение данных в системе должно быть построено на основе СУБД, использующихся в ИС Белорусской железной дороги. Срок хранения данных устанавливается дополнительно
      2. Для обеспечения целостности данных должны использоваться встроенные механизмы СУБД. Средства СУБД. Структура базы данных должна поддерживать шифрование хранимой и обрабатываемой пользовательской информации.
      3. Доступ к данным должен быть предоставлен только авторизованным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации. Средства СУБД, а также средства используемых операционных систем, сервера приложений и веб-сервера должны обеспечивать документирование и протоколирование (логирование) циркулирующей в системе информации, защиту данных от разрушений при авариях и сбоях в электропитании системы, контроль, хранение, обновление и восстановление данных.
   2. **Требования к математическому обеспечению**
      1. Описание и содержание алгоритмов, исполняемых в ИС, определяется в процессе разработки программного обеспечения.
   3. **Требования к программному обеспечению**
      1. Прикладное программное обеспечение должно отвечать следующим требованиям:

* высокая степень готовности для решения поставленных задач;
* совместимость программных продуктов в части используемых технических средств, системного ПО и общесистемной инфраструктуры в пределах требований к техническому обеспечению, а также их информационная совместимость в пределах требований к информационному обмену.
  + 1. ПО должно быть разработано с учетом технологии, обеспечивать реализацию всех функций системы и решение всех поставленных задач для автоматизации процессов авторизации и аутентификации.
    2. ПО должно осуществлять аутентификацию пользователей различными методами – пароль, биометрия, вход через почтовый клиент или социальные сети.
    3. В случае возникновения ошибки при обработке данных, система должна известить об этом оператора немедленно. ПО должно быть построено в виде программных модулей, унифицированных для каждого пользователя.
  1. **Требования к техническому обеспечению**
     1. В состав технических средств должны входить следующие основные виды:
* сервер баз данных;
* рабочее место администратора БД;
* сетевое оборудование.
  + 1. Для функционирования системы у пользователя необходимо следующее техническое обеспечение со следующими минимальными характеристиками:
* Процессор: Intel Core i3 или эквивалентный процессор с тактовой частотой не ниже 2.4 ГГц.
* • Оперативная память: 3 Гб RAM или более.
* • Жесткий диск: 64 Гб SSD или HDD.
  1. **Требования к организационному обеспечению**
     1. Организационное обеспечение АС должно быть достаточным для эффективного функционирования у пользователей АС.
     2. Организационная структура АС должна позволять выполнять все функции АС с учетом их распределения по уровням управления.
     3. Инструкции организационного обеспечения АС должны определять действия пользователей, необходимые для выполнения каждой автоматизированной функции, во всех режимах функционирования АС, с учетом заданных требований по безошибочности и быстродействию. Требования к содержанию инструкций – по СТП 09150.11.118-2009.

1. состав и содержание работ
   1. Разработка должна быть проведена в три стадии:

* разработка технического задания;
* рабочее проектирование;
* внедрение.
  1. На стадии разработки технического задания должен быть выполнен этап разработки, согласования и утверждения настоящего технического задания. На стадии рабочего проектирования должны быть выполнены перечисленные ниже этапы работ:
* разработка программы;
* разработка программной документации;
* испытания программы.

На стадии внедрения должен быть выполнен этап разработки, подготовки и передачи программы.

* 1. На этапе разработки технического задания должны быть выполнены перечисленные ниже работы:
* постановка задачи;
* определение и уточнение требований к техническим средствам;
* определение требований к программе;
* определение стадий, этапов и сроков разработки программы и документации на неё;
* согласование и утверждение технического задания и всех требований в него входящих.
  1. На этапе разработки программы должна быть выполнена работа по программированию (кодированию) и отладке программы (тестированию).
  2. На этапе разработки программной документации должна быть выполнена разработка программных документов в соответствии с требованиями к составу документации.
  3. На этапе испытаний программы должны быть выполнены перечисленные ниже виды работ:
* разработка, согласование и утверждение и методики испытаний;
* проведение приемо-сдаточных испытаний;
* корректировка программы и программной документации по результатам испытаний.
  1. На этапе подготовки и передачи программы должна быть выполнена работа по подготовке и передаче программы и программной документации в эксплуатацию на объектах Заказчика.

1. порядок приемки в эксплуатацию
   1. Приемо-сдаточные испытания должны проводиться на объекте Заказчика в оговоренные сроки.
   2. Приемо-сдаточные испытания программы должны проводиться согласно разработанной Исполнителем и согласованной Заказчиком Программы и методик испытаний.
   3. Ход проведения приемо-сдаточных испытаний Заказчик и Исполнитель документируют в Протоколе проведения испытаний.
   4. На основании Протокола проведения испытаний Исполнитель совместно с Заказчиком подписывает акт приемки-сдачи программы в эксплуатацию.
2. требования к документированию
   1. В состав технической документации, разрабатываемой при доработке компонентов АС, должны входить следующие документы:

* Спецификация;
* Инструкция по установке АС (в составе Руководства Администратора АС);
* Общее описание разработанной АС;
* Программа и методика испытаний разработанной АС;
* Руководство пользователя разработанной АС;
* Руководство Администратора разработанной АС.
  1. Руководство пользователя должно содержать описание принципов и функций АС, а также способов работы на автоматизированных рабочих местах оператора. Руководство Администратора должно включать:
* Инструкции по разворачиванию системы;
* Описание принципов организации системы (на уровне Администратора);
* Описание способов работы АС;
* Описание способов ведения справочников в базе данных системы.
  1. Вся документация должна предоставляться Заказчику в 2-х экземплярах на бумажном и электронном (компакт-диск, флеш) носителях. Документы на электронном носителе должны предоставляться в формате Microsoft Word.
  2. АС должна передаваться Заказчику на электронных носителях (компакт-диск и флеш) в двух копиях.
  3. Комплекты документации должны быть предоставлены на государственном языке (допускается использование английского языка в тех местах, где его присутствие необходимо).