Оглавление

[1. Введение 2](#_Toc406769141)

[1.1. Наименование работы 2](#_Toc406769142)

[1.2. Назначение и область применения 2](#_Toc406769143)

[2. Требования к программным обеспечениям 2](#_Toc406769144)

[2.1. Требования к функциональным характеристикам 2](#_Toc406769145)

[2.2. Требования к надёжности программных обеспечений 3](#_Toc406769146)

[2.2.1. Требования к обеспечению надёжного функционирования программ 3](#_Toc406769147)

[2.2.2. Время восстановление после отказа 3](#_Toc406769148)

[2.2.3. Отказы из-за некорректных действий пользователей системы 3](#_Toc406769149)

[3. Условия эксплуатации 3](#_Toc406769150)

[3.1. Климатические условия эксплуатации 3](#_Toc406769151)

[3.2. Требования к квалификации и численности персонала 4](#_Toc406769152)

[3.3.1. Перечень задач, выполняемых администратором сервера: 4](#_Toc406769153)

[3.3.2. Перечень задач, выполняемых оператором терминала: 4](#_Toc406769154)

[3.3. Требования к составу и параметрам технических средств 4](#_Toc406769155)

[3.4. Требования к информационной и программной совместимости 5](#_Toc406769156)

[3.4.1. Требования к информационным структурам и методам решения 5](#_Toc406769157)

[3.4.2. Требования к запросам пользователей данных из базы 5](#_Toc406769158)

[4. Требования к защите информации. 5](#_Toc406769159)

[4.1. Криптографический протокол обмена данными между сервером и «тонким клиентом». 5](#_Toc406769160)

[5. Требования к программной документации. 5](#_Toc406769161)

[6. Технико-экономические показатели 5](#_Toc406769162)

[6.1. Экономические преимущества разработки 6](#_Toc406769163)

[7. Стадии и этапы разработки 6](#_Toc406769164)

[7.1. Стадии разработки 6](#_Toc406769165)

[7.2. Этапы разработки 6](#_Toc406769166)

[8. Порядок контроля 7](#_Toc406769167)

[8.1. Анализ программного кода 7](#_Toc406769168)

# Введение

## Наименование работы

Наименование работы: «Система двухфакторной аутентификации пользователей».

## Назначение и область применения

Программные обеспечения предназначены:

* + 1. Для безопасной аутентификации пользователей на предприятии;
    2. Для доступа к рабочему месту;
    3. Для доступа к защищённым информационным ресурсам.

В состав программных обеспечений входит: приложение для администрирования и управления пользователями на сервере, приложение для тонкого клиента, считыватель смарт-карт, который подключается через USB интерфейс клиенту, скрипит для генерации таблиц реляционной базы данных на MS SQL Server 2012R2.

# Требования к программным обеспечениям

## Требования к функциональным характеристикам

Приложение администрирования и управление пользователями на сервера должна обеспечивать возможность выполнения перечисленных ниже функций:

* + 1. соединение с базой данных пользователей, если соединение невозможно установить, то сообщить об этом администратору;
    2. соединение с тонким клиентом, если соединение невозможно установить, то сообщить об этом администратору;
    3. поддержка безопасного протокола связи с тонким клиентом.
    4. создание нового пользователя;
    5. добавление информации о пользователе;
    6. привязка к пользователю смарт-карту с уникальным идентификатором;
    7. изменение данных пользователя;
    8. создание группы пользователей;
    9. ведения журнала аутентификации;
    10. возможность администратором отчистить журнал;

Приложение на тонком клиенте должна обеспечивать возможность выполнения следующих функций:

1. соединение со считывателем смарт-карт через USB интерфейс, если считыватель смарт-карт не подключён к тонкому клиенту, то вывести сообщение об этом;
2. поддержка криптографического протокола связи с сервером аутентификации пользователей.
3. возможность вывести результат аутентификации (аутентифицирован или не аутентифицирован);

## Требования к надёжности программных обеспечений

### 2.2.1. Требования к обеспечению надёжного функционирования программ

Надежное (устойчивое) функционирование программных обеспечений должно быть обеспечено выполнением совокупности организационно-технических мероприятий. Перечень организационно-технических мероприятий:

1. использование во время разработки программу контроля версий «git»;
2. использованием лицензионного программного обеспечения для разработки: Microsoft Visual studio 2012, Microsoft SQL Server 2012, SQL Managed studio и т. д. Программные обеспечения и библиотеки: ОС Linux Opensusse 13.2, qt creator, пакет компиляторов gcc и g++ и т. д.
3. регулярное выполнение ГОСТ 51188-98 защита информации, испытание программных средств на наличие программных вирусов.

### 2.2.2. Время восстановление после отказа

Время восстановления после отказа, вызванного сбоем электропитания технических средств (иными внешними факторами), не фатальным сбоем (не крахом) операционной системы, не должно превышать 30 минут при условии соблюдения условий эксплуатации технических и программных средств.

Время восстановления после отказа, вызванного неисправностью технических средств, фатальным сбоем (крахом) операционной системы, не должно превышать времени, требуемого на устранение неисправностей технических средств и переустановки программных средств.

Время восстановление после прекращение функционирования сетевого соединения, не должно превышать 1 минуты, при условии соблюдения условий эксплуатации программных обеспечений.

### 2.2.3. Отказы из-за некорректных действий пользователей системы

Отказы программы вследствие некорректных действий пользователя при взаимодействии с ПО через GUI недопустимы.

# Условия эксплуатации

## Климатические условия эксплуатации

Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики, должны удовлетворять требованиям, предъявляемым к техническим средствам, а именно ЭВМ.

## Требования к квалификации и численности персонала

Минимальное количество персонала, требуемого для работы функционирования программно-аппаратного комплекса безопасной аутентификации пользователей, должно составлять не менее 2 штатных единиц: администратор сервера и оператор терминала «тонкий клиент». Администратор сервера должен иметь высшее профильное образование. Оператор терминала должен иметь не ниже среднее профессиональное образование и должен обладать навыками использования ЭВМ на уровне пользователя.

### 3.3.1. Перечень задач, выполняемых администратором сервера:

1. задача поддержания работоспособности технических средств;
2. задачи установки (инсталляции) и поддержания работоспособности системных программных средств — операционной системы;
3. задача установки (инсталляции) программного обеспечения безопасной аутентификации пользователей, установка и настройка ОС Linux, входящих в комплекс «тонкий клиент»;
4. задача подержание сетевого подключения между сервером и тонким клиентом;
5. задача создания резервных копий базы данных.

### 3.3.2. Перечень задач, выполняемых оператором терминала:

1. следить за правильным использованием считывателя смарт-карт;
2. предоставить возможность ввода пароля пользователям;

## Требования к составу и параметрам технических средств

В состав технических средств должен входить IВМ-совместимый персональный компьютер (ПЭВМ), выполняющий роль сервера, включающий в себя:

1. процессор Intel core i3 и выше, или процессор с аналогичными характеристиками;
2. оперативную память (ОЗУ) объём 4ГГб, не менее;
3. HDD объём 60 ГГб, не менее;
4. операционную систему Windows Server 2012 R2;
5. Microsoft SQL Server 2012R2;

Допускается использование отдельного сервера для базы данных на базе MS SQL Server 2012 R2.

В состав «тонкого клиента» должен сходить ПЭВМ c минимальным набором компонентов:

1. процессор Intel Pentium IV и выше, или процессор с аналогичными характеристиками;
2. оперативную память (ОЗУ) объём 2 Гб и выше;
3. HDD 60Гб;
4. ОС Linux специальной сборки (предоставляется вместе со всем ПО);
5. USB считыватель смарт-карт.

## Требования к информационной и программной совместимости

### 3.4.1. Требования к информационным структурам и методам решения

База данных работает под управлением Microsoft SQL Server. Базу данных может редактировать только администратор сервера.

## 3.4.2. Требования к запросам пользователей данных из базы

Администратор сервера безопасной аутентификации, с базой данных работает только через приложение администрирования. Имеются возможности выполнять действия, относящиеся к базе данных, перечисленные в п. 2.1.

**3.4.3. Требования к программным средствам, используемым программой**

Системные программные средства, используемые программой администрирования, должны быть предоставлены лицензионной локализованной версией операционной системы Windows Server 2012R2 и Microsoft SQL Server 2012R2.

# Требования к защите информации.

## Криптографический протокол обмена данными между сервером и «тонким клиентом».

Все основные операции необходимо выполняться на сервере аутентификации пользователей. Терминал «тонкий клиент» должен взаимодействовать с сервером через специальный криптографический протокол. Протокол реализован на основе стеков TCP/IP, криптографическим алгоритмом ГОСТ 28147-89 и протокол обмена ключами Диффи-Xеллмана. При начале каждой сессии, сервер и клиент обмениваются ключами для шифрования. Для сравнения пароля используется однонаправленная хэш-функция. Криптографический алгоритм ГОСТ 28147-89 должен быть реализован максимально эффективно и безопасно.

# Требования к программной документации.

В состав программных документаций должно входить:

1. техническое задание;
2. программы и методики испытаний;
3. руководства администратора сервера безопасной аутентификации пользователей;
4. руководства оператора терминала «тонкого клиента»;
5. руководство аутентифицируемых пользователей.

# Технико-экономические показатели

## Экономические преимущества разработки

Данный проект имеет ряд преимуществ по экономическим показателям:

1. так как в качестве терминала доступа к серверу аутентификации используется «тонкий клиент», то требование к аппаратному обеспечению терминала минимальное, стоимость которого значительно ниже;
2. на клиенте используется ОС Linux, данная операционная система относиться к программным обеспечениям свободного распространения.

# Стадии и этапы разработки

## Стадии разработки

Разработка должна быть проведена в 4 стадии:

1. разработка технического задания;
2. разработка программных обеспечений;
3. тестирование по методикам испытаний:
4. внедрение продуктов.

## Этапы разработки

Разработка должна быть проведена в нескольких этапах. На стадии разработки технического задания должно быть поставлены основные требования к аппаратно-программному комплексу:

1. функциональные возможности ПО;
2. требования к аппаратным составляющим;
3. требования к защите информации и криптографическому протоколу;
4. сроки разработки.

На стадии разработки ПО должны быть проведены следующие основные работы:

1. разработка архитектуры программного обеспечения с применением соответствующих паттернов проектирования;
2. реализация ядра серверной части;
3. реализации ядра клиентской части;
4. реализации криптографического протокола;
5. проектирование базы данных;
6. разработки GUI серверной части;
7. написание документации;

На этапе тестирования ПО следует:

1. написать консольные приложения для автоматического тестирования;
2. провести все методики испытания c помощью программ автоматического тестирования;
3. корректировка документации;
4. быть готовым для демонстрации работы системы;

# Порядок контроля

## Анализ программного кода

Каждый файл программного кода должна быть исследован с помощью статистического анализа кода для выявления возможных ошибок на стадии разработки. Так же статический анализ кода позволит выявить потенциально небезопасный код на этапе написания программы. Это позволит допускать как можно меньше программных ошибок.