**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное ГОСУДАРСТВЕННОЕ бюджетное ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информатики

и вычислительной техники

Кафедра информационной

безопасности

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА К КУРСОВОЙ РАБОТЕ

по дисциплине «программно-аппаратные средства обеспечения информационной безопасности»

для направления (специальности) 10.05.03 информационная безопасность автоматизированных систем

на тему

«Разработка программы, защищенной от несанкционированного доступа и использующей различные способы аутентификации пользователей. Аутентификация пользователей по их «росписи» мышью.»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Выполнил: студент БИ-41 |  | | Домашевский А.Е. | |  |
|  | подпись | |  | | дата |
| Проверил: доцент кафедры ИБ | |  | | Пекунов А.А. |  |
|  | | подпись | |  | дата |

# Техническое задание

## Введение

Разработать программное средство (ПС) для аутентификации, основанной на росписи мышью.

Программу предполагается использовать как дополнительное средство аутентификации в компьютерных системах военного, энергетического и финансового назначения. Разработка является актуальной, так как намерена повысить безопасность идентификации и аутентификации пользователей в системе.

## Основания для разработки

Основанием для разработки является выбранная тема «Разработка программы, защищенной от несанкционированного доступа и использующей различные способы аутентификации пользователей», утвержденная заведующим кафедры.

## Назначение разработки

Назначением данной разработки является программное средство аутентификации. Программа должна предоставлять пользователю возможность входа в систему на основе росписи мышью.

Программное средство должно обеспечить удобство, быстроту и безопасность авторизации зарегистрированного в системе пользователя.

## Требования к программе или программному изделию

### Требования к функциональным характеристикам

Разрабатываемое ПС должно обладать следующими характеристиками:

1. Работать под управлением ОС Windows 7, OC Windows 8, OC Windows 10;
2. Программное средство должно обладать понятным пользовательским графическим интерфейсом;
3. В ПС должны быть реализованы:

* Аутентификация на основе росписи мышью;
* Менеджер пользователей;
* База данных пользователей и их биометрических характеристик;
* Администрирование данных.

1. При выполнении программной задачи должен показываться статус её выполнения.

### Требования к надежности

Надежность системы в целом зависит от выбранного алгоритма аутентификации или комбинации таких алгоритмов.

Алгоритм работы ПС должен соответствовать требованиям руководящего документа Гостехкомиссии России от 30 марта 1992 г. «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации».

Контроль отсутствия недекларированных возможностей должен осуществляться согласно руководящему документу Гостехкомиссии России РД № 114 от 04 июня 1999 г. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

### Требования к безопасности ПС

Программное средство должно обеспечивать надежность при возможных внешних попытках нарушить ее штатную работу.

Решения по использованию ПС должны приниматься с учетом обеспечения поддержки его функционирования производителем или поставщиком ПС.

### Условия эксплуатации

Стандартные условия эксплуатации программных продуктов.

### Требования к составу и параметрам технических средств

Для нормальной работы ПС рекомендуется следующая конфигурация ПК:

1. ОС Windows 7 и выше;
2. Компьютер с тактовой частотой 1.5 GHz и выше;
3. Оперативная память не менее 512 Мб;
4. Свободное дисковое пространство не менее 10 Гб.

### Требования к маркировке и упаковке

Не предъявляются.

### Требования к транспортированию и хранению

Не предъявляются.

### Специальные требования

Не предъявляются.

## Требования к программной документации

В процессе выполнения курсового проекта необходимо определить область применения ПС, составить блок-схему алгоритма работы программы.

На стадии разработки проекта рекомендуется выпустить следующий комплект документации:

1. Пояснительная записка к проекту;
2. Описание структуры программного продукта;
3. Инструкция по эксплуатации.

Виды, комплектность и содержание документов в части, определенной настоящим ТЗ, должны учитывать требования ГОСТ 34.201-89 и РД 50-34.698.

## Стадии и этапы разработки

|  |  |  |  |
| --- | --- | --- | --- |
|  | Содержание работы | Срок | Исполнитель этапа разработки |
| 1 | Исследование концепций современных стандартов | 1-2 неделя | Домашевский А.Е. |
| 2 | Анализ выбранных методов обработки информации | 3 неделя | Домашевский А.Е. |
| 3 | Разработка технического задания | 4 неделя | Домашевский А.Е. |
| 4 | Разработка эскизного проекта | 5 неделя | Домашевский А.Е. |
| 5 | Рабочий проект (написание кода) | 6-7 неделя | Домашевский А.Е. |
| 6 | Разработка документации | 8 неделя | Домашевский А.Е. |
| 7 | Испытание программы (отладка и тестирование) | 9 неделя | Домашевский А.Е. |

## Инструменты разработки

Программный продукт разрабатывается в среде Microsoft Visual Studio 2017 на языке программирования С# с использованием библиотек Microsoft .NET Framework.

Для создания БД используется Microsoft SQL Server Management Studio 2017.

## Прочие условия

Содержание отчетных материалов согласуется на уровне специалистов Заказчика, Пользователя и Исполнителя. Исполнитель должен быть заранее проинформирован Заказчиком и Пользователем о порядке и сроках согласования отчетных материалов, перечне вопросов, которые подлежат согласованию, составе согласующих подразделений и организаций и степени их компетенции при согласовании тех или иных разделов отчетной документации.

В случае необходимости может быть проведена защита предлагаемых решений в процессе технического совещания специалистов Исполнителя и Пользователя.

Настоящее ТЗ может быть уточнено или изменено в процессе работы. Уточнения и изменения ТЗ производятся по согласованию сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ТЗ.

Согласование и утверждение изменений производится в том же порядке и теми же должностными лицами, что и согласование, и утверждение ТЗ.

Замечания по отчетным материалам должны быть представлены Исполнителю с техническим обоснованием в письменной форме.

Виды, состав, объем и методы испытаний ПС определяются программой и методикой испытаний.

Испытания проводятся на площадках развертывания ПС.

Сроки приемки работ определяются календарными планами и сроками проведения соответствующих этапов в соответствии с техническими требованиями на создание ПС.

Прием и сдача проводимых работ осуществляются совместной комиссией на основе утвержденной программы и методики испытаний.

# Аннотация

В теоретической части данной курсовой работы рассматриваются методы биометрической аутентификации.

Программный продукт предназначен для аутентификации с помощью росписи мышью. Для разработки используется язык программирования C#. В соответствии с темой предоставлен алгоритм работы программы и инструкция по эксплуатации.

# Summary

The theoretical part of this course project describes biometric authentication methods.

The software product is designed for authentication using mouse-drawn signature. The C# programming language is used for the development. In accordance with the topic, the algorithm of the program and the instruction manual are provided.

# Оглавление

[Введение 10](#_Toc8521015)

[1. Теоретическая часть 11](#_Toc8521016)

[1.1. Основные понятия 11](#_Toc8521017)

[1.2. Методы биометрической аутентификации 13](#_Toc8521018)

[1.2.1. Статистические методы 13](#_Toc8521019)

[1.2.2. Динамические методы 15](#_Toc8521020)

[1.3. Функция хеширования 16](#_Toc8521021)

[1.3.1. Хеш-функция SHA-256 18](#_Toc8521022)

[1.4. Нормативные документы 20](#_Toc8521023)

[2. Практическая часть 21](#_Toc8521024)

[2.1. Анализ известных методов распознавания росписи мышью 21](#_Toc8521025)

[2.2. Модель нарушителя и модель угроз 24](#_Toc8521026)

[2.3. Снижение угроз 26](#_Toc8521027)

[2.4. Назначение программы и область применения 27](#_Toc8521028)

[2.5. Алгоритм работы программы 28](#_Toc8521029)

[2.6. Технико-экономический анализ 32](#_Toc8521030)

[2.7. Инструкция по эксплуатации 32](#_Toc8521031)

[Заключение 36](#_Toc8521032)

[Список литературы 38](#_Toc8521033)

# Принятые сокращения

БД – база данных

ЗИ – защита информации

ИБ – информационная безопасность

ИС – информационная система

НСД – несанкционированный доступ

ОС – операционная система

ПО – программное обеспечение

ПС – программное средство

РД – руководящий документ

РФ – Российская Федерация

ФСТЭК – Федеральная служба по техническому и экспортному контролю

ID – Identifier

KNN – k Nearest Neighbor

PIN – Personal Identification Number

SHA – Secure Hash Algorithm

# Введение

Сегодня информацию рассматривают как один из основных ресурсов развития общества, а информационные системы и технологии как средство повышения производительности и эффективности работы людей. Поэтому информация является ценнейшим и дорогостоящим ресурсом. Необходимость защиты информации является одной из самых актуальных проблем в области современных информационных систем – каждый пользователь персонального компьютера так или иначе сталкивался с этой проблемой, однако в системах, содержащих информацию, распространение которой может нанести ущерб человеку, обществу и даже государству, вопрос о важности обеспечения информационной безопасности является наиболее значительным.

Одним из существенных методов защиты информации является введение парольной защиты. Главный недостаток парольной аутентификации — это возможность передачи пароля другому лицу, что происходит довольно часто. И если в личной жизни страдает от таких поступков лично пользователь, то в корпоративных сетях это несет финансовую, юридическую и репутационную угрозу самой компании.

Намного эффективнее использование двухфакторной или строгой аутентификации, что намного снижает риск от передачи паролей другим пользователям, а вершиной безопасности является биометрическая аутентификация. В данной работе рассмотрена аутентификация при помощи росписи мышью.

# Теоретическая часть

## Основные понятия

Аутентификацией пользователя является проверка, действительно ли проверяемый пользователь является тем, за кого он себя выдает. Различные методы аутентификации необходимы, фактически во всех системах ограничения и разграничения доступа к данным. Для корректной аутентификации пользователя пользователь должен предъявить аутентификационную информацию — уникальную информацию, которой должен обладать лишь он один.

Существует 3 типа аутентификационных данных:

1. Парольная защита. В этом случае пользователь должен предъявить секретный PIN-код или пароль.
2. Ключи. Подразумевается физический носитель секретного ключа, который пользователь должен предъявить системе. Часто в этих целях используется пластиковая карта с магнитной полосой.
3. Биометрические данные. Чтобы получить доступ, пользователь должен предъявить параметр, который является частью его самого. При такой системе идентификации подвергается сама личность, а точнее, его индивидуальные характеристики. Например, радужная оболочка глаза, отпечатки пальцев, рисунок линий на ладони и т.д.

В каждом из данных случаев аутентификация выполняется в два этапа. Пользователь единожды дает эталонный образец аутентификационной информации, к примеру, запрашивается пароль. Этот образец хранится у субъекта системы, который проверяет аутентификацию — модуля аутентификации (это может быть, к примеру, сервер, выполняющий аутентификацию пользователей). Как правило, данный эталон действует определенное время, по завершении которого эталонный образец перезапрашивается.

Всякий раз, когда выполняется аутентификация, у пользователя запрашивается аутентификационная информация, которую затем сравнивают с эталоном. Исходя из результатов сравнения, делается вывод о подлинности пользователя.

Нередко процесс аутентификации неразрывно связан с процессом идентификации.

В процессе идентификации устанавливается взаимно однозначное соответствие между множеством сущностей системы и множеством идентификаторов. С помощью идентификации можно различать сущности системы при контроле доступа, аудите и т. д.

В процессе идентификации и аутентификации пользователь или программа запрашивает доступ у системы (верификатора). В первую очередь осуществляется идентификация. Верификатор требует от претендента предъявить определенный идентификатор и выполняет проверку принадлежности предъявленного идентификатора ID множеству зарегистрированных в системе. Если идентификатор корректен, верификатор выполняет процедуру аутентификации (к примеру, запрашивает пароль), для того, чтобы убедиться, что претендент является именно тем, за кого себя выдает. Претендент допускается в систему при условии, что процедура аудентификации успешно завершена. В некоторых системах устанавливается дополнительное пороговое значение для числа попыток предъявления некорректного идентификатора и пароля, при превышении которого все дальнейшие попытки доступа данного претендента к системе блокируются.

Чаще всего аутентификационная информация не должна храниться в открытом виде и из соображений безопасности — к примеру, эталонные образцы паролей хранятся в модуле аутентификации либо в зашифрованном виде, либо в виде хеш-значений.

Хеш-функция — это математический алгоритм, преобразовывающий произвольный массив данных в состоящую из букв и цифр строку фиксированной длины. Причем при условии использования того же типа хеша длина эта будет оставаться неизменной, вне зависимости от объема вводных данных. Криптостойкой хеш-функция может быть только в том случае, если выполняются главные требования: стойкость к восстановлению хешируемых данных и стойкость к коллизиям, то есть образованию из двух разных массивов данных двух одинаковых значений хеша. Интересно, что под данные требования формально не подпадает ни один из существующих алгоритмов, поскольку нахождение обратного хешу значения — вопрос лишь вычислительных мощностей. По факту же в случае с некоторыми особо продвинутыми алгоритмами этот процесс может занимать чудовищно много времени.

Аутентификация может быть как односторонней, так и взаимной.

Помимо этого, для того, чтобы повысить стойкость аутентификации нередко применяют несколько методов аутентификации в одно время. Аутентификация на основе одновременного предъявления аутентификационной информации двух видов называется двухфакторной.

Также существуют примеры и трехфакторной аутентификации, определяемой аналогичным образом.

## Методы биометрической аутентификации

Биометрические данные являются очень удобным для людей способом аутентификации, так как их невозможно забыть или потерять. При этом, обеспечивается достаточно высокая степень защиты данных, так как подделать их очень сложно.

Все методы биометрической аутентификации делятся на два класса. Это статистические методы, основанные на физиологических характеристиках человека, которые присутствуют в каждом из нас всю жизнь, их нельзя потерять, скопировать или украсть. Второй класс – динамические методы. Они основываются на поведенческих особенностях людей (это, как правило, подсознательные движения в процессе повторения или воспроизведения какого-то конкретного обыденного действия).

### Статистические методы

**Аутентификация по отпечатку пальца**

Данный способ аутентификации является самым распространенной биометрической технологией. Для того, чтобы провести идентификацию, используется уникальность рисунка на пальцах. Отпечаток, который получают с помощью сканера, преобразуется в цифровой код и сравнивается с наборами эталонов, введенных раньше. У этого способа есть такие преимущества, как удобство в использовании и надежность.

Чтобы получить сведения об отпечатке пальцев, применяют специальные сканеры. Для отчетливого электронного представления рисунков необходимы специфические методы, так как отпечаток пальца имеет очень маленький размер, что затрудняет получение хорошо различимых папиллярных узоров.

**Аутентификация по радужной оболочке глаза**

В этой технологии биометрической аутентификации личности используется уникальность признаков и особенностей радужной оболочки человеческого глаза. Радужная оболочка – это тонкая подвижная диафрагма глаза у позвоночных с отверстием (зрачком) в центре. Радужная оболочка формируется еще до рождения человека и остается неизменной на протяжении всей жизни. Ее рисунок очень сложен, благодаря этому удается отобрать порядка 200 точек, которые обеспечивают высокую степень надежности аутентификации (при распознавании по отпечатку пальца используют 60-70 точек).

Данная технология эффективна потому, что, в отличие от сетчатки глаза, которая может меняться, радужка остается неизменной всю жизнь. Более того, не бывает двух абсолютно идентичных рисунков на радужной оболочке, даже у близнецов.

**Аутентификация по сетчатке глаза**

Этот метод аутентификации начал применяться на практике в 50-е годы прошлого века. Именно в тот период установили уникальность рисунка кровеносных сосудов глазного дна. Для сканирования сетчатки глаза применяют инфракрасное излучение. В настоящее время данный способ применяют значительно реже, так как он достаточно сложен, вызывает дискомфорт у человека, чьи данные идентифицируют. К тому же, как говорилось выше, исследователи обнаружили, что сетчатка глаза имеет свойство меняться в разные периоды жизни.

**Аутентификация по геометрии руки**

Чтобы провести аутентификацию по этой части тела нужно использовать несколько характеристик: изгибы пальцев, их толщину и длину, расстояние между суставами и структуру кости.

Столько параметров приходится учитывать в силу того, что по отдельности они не являются уникальными. Минус этого метода: ушибы и распухание тканей могут значительно исказить исходную структуру, а такое заболевание как «артрит» — сильно помешать сканированию. Надежность данного способа аутентификации сравнима с методом идентификации по отпечатку пальца.

**Аутентификация по геометрии лица**

Этот способ достаточно распространен. Построение трехмерного изображения лица заключается в выделении контуров глаз, губ, носа, бровей и других элементов лица, а также вычислении расстояния между ними. Чтобы определить уникальный шаблон, соответствующий конкретному человеку, необходимо от 12 до 40 характерных элементов. Здесь важно, чтобы шаблон мог учитывать множество разных вариаций изображения на случай изменения освещенности, положения и выражения лица.

### Динамические методы

**Аутентификация по голосу**

Этот биометрический метод очень прост в применении. Для его реализации не требуется дорогостоящая аппаратура, необходим только микрофон и звуковая плата. Существует много способов построения шаблонов по голосу: комбинации частотных и статистических характеристик голоса, модуляция, интонация, высота тона и другие.

Основной недостаток аутентификации по голосу – низкая точность. Например, система может не опознать человека, с осипшим из-за простуды голосом. Также камнем преткновения в использовании этого метода является возможное многообразие голоса одного человека. Ведь голос имеет свойство изменяться в зависимости от возраста, настроения, состояния здоровья и под воздействием многих других факторов. Из-за вероятности неточностей и ошибок метод применяется для управления доступом в помещениях, где нужен средний уровень безопасности, например, в компьютерных классах.

**Аутентификация по рукописному почерку**

Метод биометрической аутентификации по рукописному почерку основывается на уникальном движении руки человека в момент подписания документов. Для сохранения подписи используются специальные ручки или восприимчивые к давлению поверхности. Для аутентификации этим способом необходима подпись человека. Шаблон создается в зависимости от необходимого уровня защиты. Как правило, подпись обрабатывается одним из двух способов: либо анализируется сам фрагмент, при установлении степени совпадения двух картинок, либо – динамические характеристики написания, для этого сверяют его временные и статистические параметры.

Кроме того, используют и комбинированную биометрическую систему аутентификации. В этом случае соединяются несколько типов биометрических технологий, которые позволяют одновременно учитывать разные характеристики человека. Например, аутентификацию по отпечатку пальцев можно сочетать со сканированием руки. Такой способ является более надежным с точки зрения возможности подделки

## Функция хеширования

Криптографические хеш-функции — незаменимый и повсеместно распространенный инструмент, используемый для выполнения целого ряда задач, включая аутентификацию, проверку целостности данных, защиту файлов и даже обнаружение зловредного ПО. Существует масса алгоритмов хеширования, отличающихся криптостойкостью, сложностью, разрядностью и другими свойствами.

Среди множества существующих хеш-функций принято выделять криптографически стойкие, применяемые в криптографии, так как на них накладываются дополнительные требования. Для того, чтобы хеш-функция считалась криптографически стойкой, она должна удовлетворять трём основным требованиям, на которых основано большинство применений хеш-функций в криптографии:

1. **Необратимость**: для заданного значения хеш-функции m должно быть вычислительно неосуществимо найти блок данных , для которого ;
2. **Стойкость к коллизиям первого рода**: для заданного сообщения должно быть вычислительно неосуществимо подобрать другое сообщение , для которого ;
3. **Стойкость к коллизиям второго рода**: должно быть вычислительно неосуществимо подобрать пару сообщений , имеющих одинаковый хеш.

Данные требования не являются независимыми:

1. обратимая функция нестойка к коллизиям первого и второго рода;
2. функция, нестойкая к коллизиям первого рода, нестойка к коллизиям второго рода; обратное неверно.

Следует отметить, что не доказано существование необратимых хеш-функций, для которых вычисление какого-либо прообраза заданного значения хеш-функции теоретически невозможно. Обычно нахождение обратного значения является лишь вычислительно сложной задачей.

Атака «дней рождения» позволяет находить коллизии для хеш-функции с длиной значений n битов в среднем за примерно вычислений хеш-функции. Поэтому -битовая хеш-функция считается криптостойкой, если вычислительная сложность нахождения коллизий для неё близка к .

Для криптографических хеш-функций также важно, чтобы при малейшем изменении аргумента значение функции сильно изменялось (лавинный эффект). В частности, значение хеша не должно давать утечки информации даже об отдельных битах аргумента. Это требование является залогом криптостойкости алгоритмов хеширования, хеширующих пользовательский пароль для получения ключа.

Хеширование часто используется в алгоритмах электронно-цифровой подписи, где шифруется не само сообщение, а его хеш-код, что уменьшает время вычисления, а также повышает криптостойкость. Также в большинстве случаев вместо паролей хранятся значения их хеш-кодов.

### Хеш-функция SHA-256

SHA-2 (англ. Secure Hash Algorithm Version 2 — безопасный алгоритм хеширования, версия 2) — семейство криптографических алгоритмов — однонаправленных хеш-функций, включающее в себя алгоритмы SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/256 и SHA-512/224.

Хеш-функции предназначены для создания «отпечатков» или «дайджестов» для сообщений произвольной длины. Применяются в различных приложениях или компонентах, связанных с защитой информации.

**Общее описание**

Хеш-функции семейства SHA-2 построены на основе структуры Меркла — Дамгора.

Исходное сообщение после дополнения разбивается на блоки, каждый блок — на 16 слов. Алгоритм пропускает каждый блок сообщения через цикл с 64 или 80 итерациями (раундами). На каждой итерации 2 слова преобразуются, функцию преобразования задают остальные слова. Результаты обработки каждого блока складываются, сумма является значением хеш-функции. Тем не менее, инициализация внутреннего состояния производится результатом обработки предыдущего блока. Поэтому независимо обрабатывать блоки и складывать результаты нельзя.

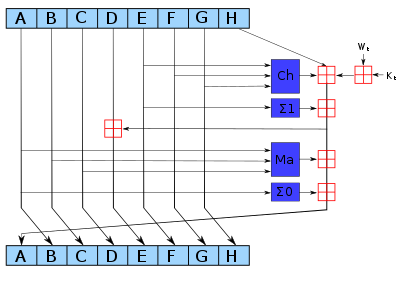
[](https://commons.wikimedia.org/wiki/File:SHA-2.svg?uselang=ru)

Рисунок 1. Схема одной итерации алгоритмов SHA-2

Алгоритм использует следующие битовые операции:

* ǁ — конкатенация,
* + — сложение,
* *and* — побитовое «И»,
* *xor* — исключающее «ИЛИ»,
* *shr* (shift right) — логический сдвиг вправо,
* *rotr* (rotate right) — циклический сдвиг вправо.

**Сравнение хеш-функций**

В таблице 1 показаны некоторые технические характеристики различных вариантов SHA-2. «Внутреннее состояние» обозначает промежуточную хеш-сумму после обработки очередного блока данных:

Таблица 1. Функции семейства SHA-2

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Хеш-функция** | **Длина дайджеста сообщения (бит)** | **Длина внутреннего состояния (бит)** | **Длина блока (бит)** | **Максимальная длина сообщения (бит)** | **Длина слова (бит)** | **Количество итераций в цикле** | **Скорость (MiB/s)** |
| SHA‑256, SHA‑224 | 256/224 | 256 (8 × 32) | 512 | 264 − 1 | 32 | 64 | 139 |
| SHA‑512, SHA‑384, SHA‑512/256, SHA‑512/224 | 512/384/256/224 | 512 (8 × 64) | 1024 | 2128 − 1 | 64 | 80 | 154 |

В данной работе использован алгоритм вычисления хеша SHA-256 для хранения хешированных паролей в БД с целью повышения защиты информации, включая защиту от атаки «человек посередине».

## Нормативные документы

1. Банк данных угроз безопасности информации, ФСТЭК России.
2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах, ФСТЭК России.
3. Приказ ФСБ РФ от 09.02.2005 № 66 (ред. от 12.04.2010) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
4. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
5. ГОСТ Р ИСО/МЭК 19794-7–2009 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 7. Данные динамики подписи»

# Практическая часть

## Анализ известных методов распознавания росписи мышью

На данный момент разработано несколько различных подходов к задаче верификации собственноручной подписи:

1. На основе нескольких статистических методов, в частности используются скрытые модели Маркова (СММ) в построении эталонной модели для каждого локального объекта.
2. Основанная на машинном обучении. Для применения машинного обучения при верификации подписи необходима обучающая выборка. В процессе исследования изучалась возможность применения таких алгоритмов, как KNN, метод опорных векторов и метод логистической регрессии.
3. Основанная на использовании нейронной сети. Для каждого объекта устанавливается специальный двухступенчатый перцептрон и внедрена структурная классификация. Технология применения нейронных сетей является широко распространённой для решения подобного рода задач.

Преимущества использования динамических признаков в том, что их гораздо сложнее подделать, так как они не видны при рассмотрении бумажной копии подписи. Результаты тестирования алгоритмов верификации подписи представляются в виде соотношения ошибок 1-го и 2-го рода. Ошибки 1-го рода связаны с отказами в доступе законному пользователю, ошибки 2-го рода — с ложной идентификацией. Используемые при дальнейшей обработке характеристики подписи:

* графическое изображение (в графической или векторной форме);
* количество отрывов пера от поверхности устройства;
* временные характеристики (минимальное, максимальное, среднее, полное время без отрыва пера от экрана);
* характеристики скорости перемещения пера (минимальные, максимальные значения проекций скоростей на оси и модуля скорости).

Проанализированы следующие подходы, позволяющие произвести верификацию собственноручной подписи:

* KNN-алгоритм;
* алгоритм Range Classifier;
* алгоритм на основе скрытой модели Маркова;
* простейшая перцептронная нейронная сеть

KNN-алгоритм классификации ( Nearest Neighbours, ближайших соседей) на вход принимает вектор, содержащий значения характеристик подписи, а на выходе выдаёт решение, подлинная подпись или подделка. Для классификации каждой из характеристик на основе обучающей выборки необходимо последовательно выполнить следующие операции:

* вычислить расстояние до каждого из объектов обучающей выборки;
* отобрать объектов обучающей выборки, расстояние до которых минимально.

Далее принимается положительное решение в случае, если характеристики находятся в пределах допустимого отклонения. Данный алгоритм имеет следующие недостатки:

* низкая точность;
* возникновение ошибок 1-го и 2-го рода при поворотах, масштабировании, сдвигах подписи.

Алгоритм верификации подписи Range Classifier состоит из следующих этапов:

* для каждого образца подписи рассчитывается центроид;
* для каждой подписи формируются векторы из углов и длин радиус-векторов от центроида до каждой точки;
* накладываются последовательности векторов тестируемой подписи и объектов обучающей выборки с учётом погрешности;
* определяется диапазон значений каждого вектора согласно обучающей выборке. Если пороговое число параметров попадает в указанный диапазон и наложение векторов совпадает, подпись признаётся подлинной.

Алгоритм на основе скрытой модели Маркова на вход также принимает вектор из характеристик подписи. Алгоритм состоит из следующих шагов:

* процесс подписания моделируется с несколькими состояниями, которые представляют собой цепь Маркова;
* каждое из этих состояний соответствует отдельной части подписи, которая не наблюдаются непосредственно (то есть скрыта);
* наблюдаемые данные связаны статистически с состояниями модели и условно независимы в каждом состоянии;
* при обучении параметры модели оцениваются по набору, содержащему достоверные подписи.

Во время верификации вычисляется вероятность того, что подпись подлинна. Если эта вероятность достигает установленного порогового значения, подпись принимается, в противном случае отвергается. Этот подход можно рассматривать как статистическое соответствие проверяемой подписи и подписи, построенной на основе скрытой модели Маркова.

Следующий алгоритм: нейронная сеть принимает на входы вектор, содержащий значения характеристик подписи. Сеть имеет 12 входов, 2 скрытых уровня по 6 нейронов каждый и 1 выход; функционирует по принципу «обучение с учителем». Обучение сети и верификация подписи происходит следующим образом:

1. на входы нейронной сети подаются характеристики подписи;
2. с помощью логистической функции активации задаются веса синапсов нейронной сети;
3. подпись признаётся верной, если на выходе нейронной сети значение превышает пороговое.

Данный алгоритм верификации отличается точностью распознавания и нечувствительностью к изменениям масштаба и сдвигах подписи.

**Реализация и тестирование**

Алгоритмы реализованы в виде мобильного приложения для платформы Android на языке Java. В ходе тестирования на выборке из 100 подписей для рассмотренных алгоритмов получены результаты, приведённые в таблице.

Таблица 2. Результаты тестирования реализованных алгоритмов

|  |  |  |  |
| --- | --- | --- | --- |
| **Алгоритм** | **Ошибки 1-го рода, %** | **Ошибки 2-го рода, %** | **Время вычисления, мс** |
| KNN-алгоритм | 13 | 20 | 3,37 |
| Range Classifier | 4 | 20 | 5,17 |
| Алгоритм на основе СММ | 10 | 17 | 4,82 |
| Нейронная сеть | 8 | 12 | 2,16 |

В ходе исследования выявлено, что наиболее перспективными для дальнейшей работы являются алгоритм на основе СММ и нейронная сеть, так как доля ошибок этих алгоритмов меньше, чем других, однако в рамках дальнейшего исследования предполагается разработать упрощенный алгоритм верификации собственноручной подписи, учитывающий направления движения курсора и не предполагающий машинное обучение для простоты реализации, а также меньших затрат ресурсов ЭВМ и дискового пространства.

## Модель нарушителя и модель угроз

Модель нарушителя представляет собой описание возможных типов злоумышленников, которые намеренно или случайно, своим действием или бездействием способны нанести ущерб информационной системе, существующей в конкретной организации.

Всех возможных нарушителей информационной безопасности в организации условно разделяют на две категории:

1. Внешние нарушители – это нарушители, которые атакуют внутренние ресурсы организации из сетей общего пользования (изменение, удаление, хищение информации, рассылка спама и другое). Они обходят средства защиты такие как межсетевые экраны и системы обнаружения атак, чтобы проникнуть во внутреннюю сеть организации.
2. Внутренние нарушители – это сотрудники организации, вспомогательный персонал и временные работники, то есть те, кто находится внутри контролируемой зоны и имеет определенный доступ к оборудованию. Они находятся в преимущественном положении по сравнению с внешними нарушителями, так как уже владеют недоступной для внешних нарушителей конфиденциальной информацией об организации. Внутренние нарушители – это люди, которые знают, как работает организация, и понимают ее слабости.

Кроме того, все нарушители, независимо от их категории, могут обладать определённым потенциалом, характеризуемым возможностями нарушителей причинять ущерб безопасности информации. Краткие характеристики некоторых видов нарушителей, их потенциал и возможности указаны в таблице №3.

Таблица 3. Характеристики нарушителей

|  |  |  |
| --- | --- | --- |
| **Вид нарушителя** | **Потенциал** | **Возможности нарушителя** |
| Бывшие работники | низкий | Осуществление атаки за пределами организации из-за мести или финансовой выгоды. |
| Обслуживающий персонал | низкий | Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные действия. |
| Пользователи ИС | низкий | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Непреднамеренные, неосторожные действия. |
| Конкурирующие организации | средний | Поиск уязвимостей системы для получения конкурентных преимуществ. |
| Криминальные структуры | средний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. |
| Администратор ИС | средний | Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды, самореализация; нанесение ущерба из мести, непреднамеренные действия. |

Согласно Приказу ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" – угрозы безопасности информации определяются по результатам оценки возможностей нарушителей, анализа возможных уязвимостей информационной системы, способов реализации угроз и последствий от нарушения свойств безопасности информации: конфиденциальности, целостности, доступности.

В качестве опорных данных для определения возможных угроз безопасности информации использовался «Банк данных угроз безопасности информации», введенный ФСТЭК России.

В результате анализа записей указанного банка угроз были определены возможные угрозы безопасности. Их перечень приведён в таблице 4.

Таблица 4. Возможные угрозы безопасности

|  |  |  |
| --- | --- | --- |
| **Угрозы безопасности** | **Вероятность реализации угрозы** | **Опасность от применения угрозы** |
| Угрозы утечки защищаемой информации | Средняя | Высокая |
| Угроза анализа криптографических алгоритмов и их реализации | Средняя | Высокая |
| Угрозы несанкционированного или случайного воздействия на содержание защищаемой информации | Низкая | Высокая |
| Угрозы несанкционированного управления ПО | Низкая | Средняя |

Половина перечисленных в таблице угроз имеет вероятность их реализации – «Среднюю», и 75% угроз имеет уровень опасности – «Высокую». Следовательно, итоговый уровень безопасности информации будет считаться «Низким».

## Снижение угроз

Наиболее серьезной проблемой является угроза анализа криптографических элементов и утечки защищаемой информации. Для осуществления этих угроз нарушитель может получить несанкционированный доступ к БД или завладеть аутентификационными данными пользователя.

С целью снижения вероятности возникновения и опасности применения указанных угроз, необходимо разработать такое программное средство, которое будет включать в себя:

* Хеширование паролей;
* Использование динамических биометрических данных для аутентификации;
* Использование динамического хеширования вместо использования хеш-функций в самой БД;
* Распределение прав доступа к ПС;
* Наличие возможности оперативного ограничения доступа определенному пользователю.

Применение такого программного средства позволит противодействовать возникновению следующих угроз:

* Угрозы утечки защищаемой информации,
* Угроза анализа криптографических алгоритмов и их реализации,
* Угрозы несанкционированного управления ПО.

Это приведёт к повышению общего уровня обеспечения безопасности защищаемой информации ограниченного доступа с «Низкого» до «Среднего».

Таким образом, наиболее оптимальным решением задачи обеспечения противодействия возникновению возможных угроз обеспечения безопасности информации будет применение программного средства, использующего двухфакторную авторизацию с биометрическими данными с обязательным предварительным хешированием парольных данных.

## Назначение программы и область применения

Программа предназначена для двухфакторной аутентификации с помощью росписи мышью в дополнении к парольной защите.

Общей особенностью способов аутентификации, основанных на клавиатурном почерке и росписи мышью является нестабильность их характеристик у одного и того же пользователя, которая может быть вызвана:

1. естественными изменениями, связанными с улучшением навыков пользователя по работе с клавиатурой и мышью или, наоборот, с их ухудшением из-за старения организма;
2. изменениями, связанными с ненормальным физическим или эмоциональным состоянием пользователя.

Изменения характеристик пользователя, вызванные причинами первого рода, не являются скачкообразными, поэтому могут быть нейтрализованы изменением эталонных характеристик после каждой успешной аутентификацией пользователя.

Изменения характеристик пользователя, вызванные причинами второго рода, могут быть скачкообразными и привести к отклонению его попытки входа в КС. Однако эта особенность аутентификации на росписи мышью может стать и достоинством, если речь идет о пользователях КС военного, энергетического и финансового назначения.

Поэтому областью применения является использование данной программы для аутентификации пользователей КС военного, энергетического и финансового назначения.

## Алгоритм работы программы

Данное ПС разрабатывается в среде программирования Visual Studio 2017 на языке C#. БД создана с помощью SQL Management Studio 2017.

Основой работы данной программы является распознавание росписи мышью. Для распознавания используется следующий алгоритм:

1. При изменении положения мыши на форме программы, вызывается функция определения направления движения курсора,
2. Данная функция вычисляет угол, тангенс которого равен отношению разниц координат и ,
3. Выбирается ближайшее к этому углу направление движения из заданных восьми,
4. Полученное направление записывается в список, заполнение прекращается после прекращения движения,
5. Список оптимизируется по длине и отсутствию повторений,
6. Чтобы проверить схожесть списков, используется функция Левенштейна для определения числа необходимых вставок и удалений с целью получения идентичных строк,
7. Вычисляется процентное соотношение похожести, и, если оно больше 70, подпись признается действительной и используется как эталон для следующей аутентификации.

Для хеширования данных перед отправкой в БД используется алгоритм хеширования SHA-256 за счет простоты реализации через встроенные библиотеки .NET.

В программе реализованы функции администрирования – создание пользователей, сброс паролей, ограничение доступа определенного пользователя к работе.

В БД реализованы поля: пользователь, пароль (в хешированном виде), подпись, блокировка пользователя, а также является ли пароль одноразовым.

Блок-схема работы программы представлена на рисунках 2 и 3.



Рисунок 2. Блок-схема программы, часть 1



Рисунок 3. Блок-схема программы, часть 2

## Технико-экономический анализ

Важной частью разработки ПС является технико-экономический анализ, так как позволяет оценить насколько разработанное ПС является востребованным по тем или иным причинам.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Разработанное ПС | Handwritten Signature SDK (Beta) | Gradiant Signature |
| Хеширование данных | + | - | + |
| Разграничение прав доступа | + | - | + |
| Наличие графического планшета не существенно | + | + | - |
| Русский интерфейс | + | - | - |
| Малые системные требования | + | + | - |
| Поддерживаемые операционные системы | Windows 7 и выше | Windows 7 и выше | Windows XP и выше |
| Стоимость лицензии (1 год) | Бесплатно | Бесплатно | Устанавливается при запросе |

Основываясь на таблице, можно сделать вывод о том, что основные преимущества данного ПС – ее стоимость. Кроме того, реализовано распределение прав, а также интерфейс на русском языке, что является плюсом данного ПС.

## Инструкция по эксплуатации

При запуске программы открывается форма аутентификации (Рисунок 4).

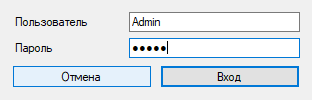


Рисунок 4. Аутентификация

Если данная пара логин-пароль существует в БД, то проверяется наличие доступа пользователя. В случае запрета будет выведено сообщение об ошибке (Рисунок 5).

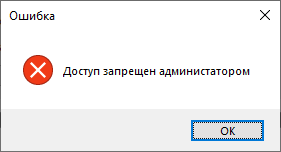


Рисунок 5. Доступ запрещен

Если пользователь был только что создан или пароль был сброшен, пользователю будет предложено создать новый пароль (Рисунок 6).

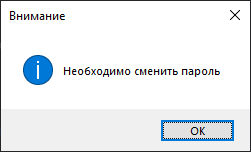


Рисунок 6. Пароль одноразовый

Для смены пароля необходимо просто заполнить предложенные поля (Рисунок 7).

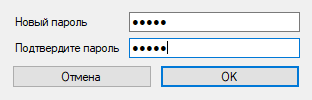


Рисунок 7. Новый пароль

После этого, в случае отсутствия подписи в БД, будет предложено внести новую подпись в БД (Рисунок 8).

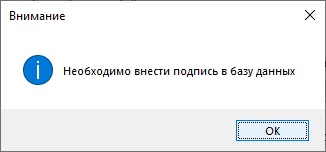


Рисунок 8. Подпись отсутствует в БД

После этого будет открыта форма для написания подписи (Рисунок 9).

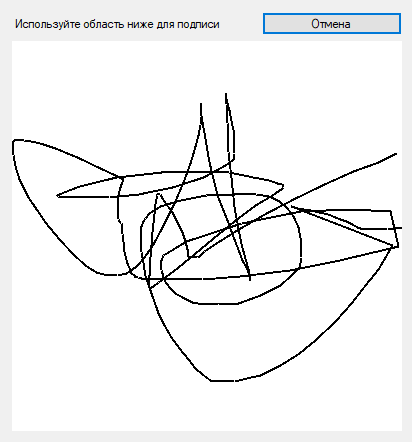


Рисунок 9. Написание подписи

В случае если подпись уже существует, при совпадении подписи более чем на 70% откроется форма для дальнейшей работы пользователя (Рисунок 10) или администратора (Рисунок 11).

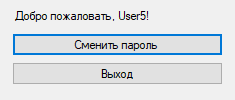


Рисунок 10. Форма пользователя

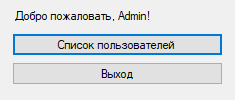


Рисунок 11. Форма администратора

При выборе работы со списком пользователей откроется следующая форма (Рисунок 12).

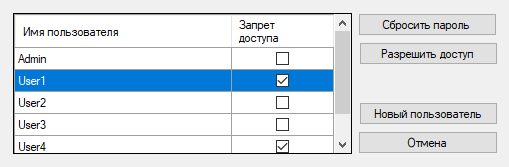


Рисунок 12. Список пользователей

При сбросе пароля определенного пользователя будет сгенерирован новый одноразовый пароль (Рисунок 13).

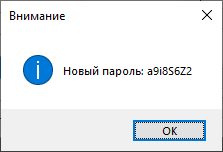


Рисунок 13. Пароль сброшен

Запрет и разрешение доступа мгновенно отобразится на таблице.

При создании нового пользователя будет предложено выбрать ему имя и одноразовый пароль (Рисунок 14), либо сгенерировать новый случайным образом, нажав на кнопку «Г».

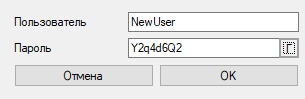


Рисунок 14. Новый пользователь

# Заключение

При выполнении курсовой работы изучен теоретический материал об аутентификации с помощью биометрических данных, описаны известные методы распознавания подписи. Проведен сравнительный анализ методов распознавания, разработана модель угроз и модель нарушителя и оценены способы уменьшения рисков ИБ.

В ходе выполнения данной работы разработано ПС, обеспечивающее аутентификацию пользователя с использованием росписи мышью. Также данное ПС включает в себя хеширование информации при помощи алгоритма SHA-256, функции администрирования данных о пользователях системы, а также возможность работы с базой данных, созданной в среде SQL Server.

Данный программный продукт может применяться как в организациях военного, энергетического и финансового назначения, так и в коммерческих организациях для повышения безопасности процесса аутентификации пользователей.

Использование хеширования паролей в ПС позволяет снизить риск анализа криптографических алгоритмов и их реализации, распределение прав доступа к ПС, использование биометрических данных и наличие возможности оперативного ограничения доступа определенному пользователю – риск утечки защищаемой информации.

Среди подобных продуктов разработанное ПС отличается сочетанием в себе наличия русского интерфейса, простотой реализации, хешированием данных и отсутствием необходимости использования графического планшета.

В заключение можно сказать, что разработки в области распознавания рукописной подписи имеют перспективы – могут быть разработаны усовершенствованные алгоритмы, учитывающие силу нажатия пера, могут быть сокращено количество ошибок при аутентификации. В таком случае распознавание подписи может стать достойной заменой верификации с помощью статических биометрических данных, так как оно позволяет не только быть реализовано без наличия аппаратных средств, но и позволит оценивать физическое и эмоциональное состояние пользователя.

# Список литературы

1. Жумагулова С. К., Есендаулетова Ж. Т., Токсеит Д. К. Некоторые аспекты использования методов аутентификации в программных системах // Молодой ученый. - 2016. - №5. - С. 184-186. - URL https://moluch.ru/archive/109/26276/ (дата обращения: 10.05.2019).
2. Епишкина А.В., Береснева А.В., Бабкин С.С., Курнев А.С. и др. О верификации собственноручной подписи // Прикладная дискретная математика. Приложение. - 2017. - №4. - URL https://cyberleninka.ru/article/n/o-verifikatsii-sobstvennoruchnoy-podpisi (дата обращения: 10.05.2019).
3. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью // irkat.ru: Иркутский Авиационный техникум URL: http://sdo.irkat.ru/UMM\_IZB/ЭУ%20по%20алгоритмизации/От\_Некипеловой/Защита\_информации/1/Лекция%202/23.html (дата обращения: 10.05.2019).
4. Биометрия и защита информации: человеческий признак vs человеческий фактор // okbsapr.ru: Сайт компании ОКБ САПР URL: http://www.okbsapr.ru/konyavskaya\_2013\_4.html (дата обращения: 10.05.2019).
5. Биометрическая защита информации // crime-research.ru: Центр исследования компьютерной преступности URL: http://www.crime-research.ru/library/biom\_systema\_zashiti.html (дата обращения: 10.05.2019).
6. Использование биометрических данных для защиты информации // inf74.ru: Информационное общество в Челябинской области URL: http://www.inf74.ru/safety/ofitsialno/ispolzovanie-biometricheskih-dannyih-dlya-zashhityi-informatsii/ (дата обращения: 10.05.2019).
7. SHA-2 // ru.wikipedia.org: Википедия – свободная энциклопедия URL: https://ru.wikipedia.org/wiki/SHA-2 (дата обращения: 10.05.2019).
8. Чудеса хеширования // kaspersky.ru: Блог Лаборатории Касперского URL: https://www.kaspersky.ru/blog/the-wonders-of-hashing/3633/ (дата обращения: 10.05.2019).
9. БДУ - Угрозы // fstec.ru: ФСТЭК России: https://bdu.fstec.ru/threat (дата обращения: 10.05.2019).
10. ГОСТ 34.201-89 от 01.01.1990 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».
11. Приказ ФСБ РФ от 09.02.2005 № 66 (ред. от 12.04.2010) «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».
12. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
13. РД Гостехкомиссии России от 30.03.1992 г. «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации».
14. РД Гостехкомиссии России № 114 от 04.06.1999 г. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».
15. РД 50-34.698-90 от 01.01.1992 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов».