**«Аутентификация личности по биометрическим данным»**

***Спирчина Яна Алексеевна***

*Студентка, Программная инженерия, Санкт-Петербургский политехнический университет Петра Великого, г.Санкт-Петербург*

*spirchina04@gmail.com*

Сегодня мы живем в мире, где передача и хранение данных являются неотъемлемой частью нашей повседневной жизни. Мы делаем покупки онлайн, общаемся с друзьями и коллегами через социальные сети, храним свои личные фотографии и документы в облачных сервисах. Но с возрастающим объемом данных, которые мы передаем и храним, возрастает и риск их утечки или кражи. В таких условиях биометрические технологии на телефонах стали ключом к защите личной информации. Давайте рассмотрим подробнее, какой бывает биометрия и как быстро она захватывает мир.

Биометрические технологии используют уникальные физиологические и поведенческие характеристики человека для идентификации и аутентификации. Сегодня большинство современных смартфонов оснащены датчиками отпечатков пальцев, сканерами лица и голоса, что позволяет пользователям быстро и безопасно разблокировать свои устройства. Если мы говорим про физические особенности человека, первое, что приходит на ум, это лицо. С этой уникальностью связана работа Face ID.

Face ID – это технология распознавания лица, которая использует передовые алгоритмы искусственного интеллекта для создания точной 3D-модели лица пользователя. Впервые, она была представлена американской компанией Apple и вызвала немало вопросов и дискуссий. Для разблокировки устройства достаточно просто посмотреть на экран.

В телефонах присутствуют специальные инфракрасные проекторы и детекторы, которые считывают форму лица (см. рис.1). Наши лица, действительно, уникальны. Например, даже у близнецов оно отличается в маленьких деталях. Однако, компьютерам необходимо много времени для повышения точности, чтобы различить эти маленькие детали. И тут для современных гаджетов важен баланс между точностью и временем срабатывания. Например, Apple для своих пользователей даёт шанс ошибки один к миллиону.

Изображение выглядит как человек, Человеческое лицо, снимок экрана, в помещении

Автоматически созданное описание

Рис.1. Работа Face ID

Однако, несмотря на все преимущества, Face ID также вызвал определенные опасения с точки зрения безопасности. Некоторые пользователи опасаются, что их лицевые данные могут быть украдены или использованы без их разрешения. Кроме того, возможны случаи, когда Face ID не распознает лицо пользователя, например, если он носит очки или шляпу.

Тем не менее, Face ID был разработан с учетом всех возможных угроз и обеспечивает максимальный уровень безопасности. Для защиты данных используется специальный чип Secure Enclave, который хранит биометрические данные пользователя в зашифрованном виде. Кроме того, Face ID не сохраняет фотографии или видео лица пользователя на устройстве.

Таким образом, Face ID – это новая технология аутентификации. Впервые представленная в 2017 году, она быстро захватывает мир и становится все более распространенной в повседневной жизни, защищая наши данные не только на телефонах, но и на планшетах и ноутбуках.

Но какие есть ещё способы защиты данных? Их оказывается гораздо больше, чем мы можем просто себе представить.

Оказывается, структура и расположение вен в наших ладонях и пальцах также является уникальной, так что можно просвечивать пальцы и таким образом подтверждать свою личность. Так, существуют специальные детекторы, которые способны распознать рисунок наших вен. Они просвечивают руку инфракрасным светом и регистрируют рисунок вен. Если говорить об ошибке точности, то она достигает уже один к трём миллиардам.

Также в современном мире есть ещё одна технология биометрической идентификации - распознавание подписей. Компьютер сравнивает не только саму форму подписи, но и как её делает человек включая даже скорость, с которой она была написана. Современные электронные планшеты ещё умеют и силу нажатия определять и угол наклона ручки.

Существует несколько методов распознавания подписей, включая ручное и автоматическое. Ручное распознавание подписей проводится экспертами-графологами, которые анализируют уникальные черты подписи и сравнивают их с образцами подписей, предоставленными клиентом. Этот метод является дорогостоящим и требует времени и опыта специалистов.

Автоматическое распознавание подписей, с другой стороны, основано на использовании компьютерных алгоритмов и машинного обучения. Оно позволяет быстро анализировать большое количество документов и сравнивать их подписи с сохраненными образцами. Однако, точность этого метода может быть ниже, чем у ручного метода. Распознавание подписей используется в различных областях, включая банковское дело, юридические услуги, государственные службы и т.д. Оно позволяет упростить и ускорить процесс проверки подлинности документов и сделок, а также уменьшить риски мошенничества и фальсификации (см.рис.2).

Изображение выглядит как человек, палец, гвоздь, большой палец

Автоматически созданное описаниеРис.2. Подпись

И наконец, рассмотрим самый популярный способ идентификации на сегодняшний день – сканер отпечатка пальца.

У каждого из нас уникальные отпечатки пальцев. У отпечатка есть два типа признаков: основные и локальные. Основные – это те, которые можно увидеть невооружённом глазом, такие как узор, форма и направление линий. Локальные отпечатки пальцев – это уникальные особенности, такие как вихри, островки, шипы и дуги, которые могут отличаться у каждого человека. Именно они используются для идентификации личности в системах биометрической аутентификации, а точнее в сканерах. Этот способ является самым распространённым, так как по научным данным совпадение отпечатков относится как 1 к 64 миллиардам (см.рис.3).

Принцип работы сканера отпечатка пальца основан на анализе уникальных черт папиллярных линий на пальцах человека. Когда палец помещается на сканер, он сканирует поверхность пальца и создает изображение его отпечатка. Затем компьютерный алгоритм анализирует изображение и сравнивает его с сохраненными образцами отпечатков в базе данных. Если отпечаток соответствует сохраненному образцу, то система разрешает доступ к защищенным данным или ресурсам.

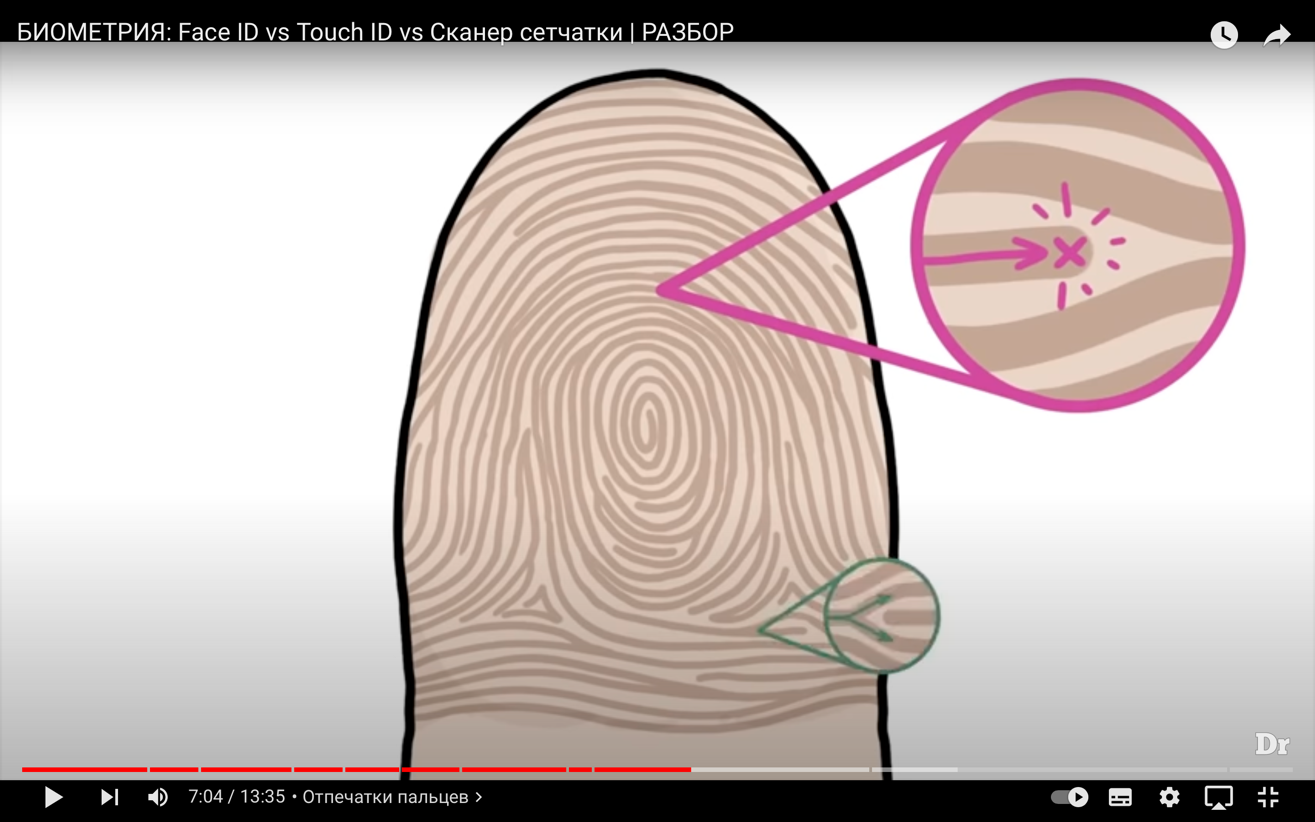


Рис.3. Отпечаток пальца

Сканеры отпечатков пальцев могут быть различных типов, включая оптические, емкостные и ультразвуковые. Они также могут быть интегрированы в различные устройства, такие как смартфоны, ноутбуки, планшеты, дверные замки и т.д.

Сканеры отпечатков пальцев имеют множество преимуществ по сравнению с традиционными методами аутентификации, такими как пароли и PIN-коды. Во-первых, они более безопасны, так как отпечаток пальца является уникальной и неизменяемой биометрической характеристикой человека. Во-вторых, они более удобны в использовании, так как не требуют запоминания сложных паролей или кодов доступа. В-третьих, они более быстры в работе, что позволяет ускорить процессы аутентификации и авторизации.

Однако, они также имеют свои недостатки. Например, они могут быть менее точными в случае повреждения или изменения папиллярных линий на пальцах. Кроме того, злоумышленники могут использовать различные методы для обмана системы, такие как копирование отпечатка или использование поддельных пальцев.

Таким образом, сканер отпечатка пальца является важной технологией для защиты данных и обеспечения безопасности в различных областях. Однако, он также имеет свои недостатки и требует дополнительных мер безопасности для защиты от злоумышленников. В будущем ожидается, что технологии сканеров отпечатков пальцев будут становиться все более точными и надежными, что позволит использовать их в более широком спектре областей.

Подводя итог, хочется сказать, что биометрические технологии не являются абсолютно надежными. Возможны случаи подделки отпечатков пальцев или использования масок для обмана сканеров лица. Кроме того, хакеры могут получить доступ к базам данных с биометрической информацией, что повышает риск утечки личных данных.

Тем не менее, биометрические технологии на телефонах являются эффективным инструментом для защиты данных. Они позволяют пользователям быстро и безопасно разблокировать свои устройства, не прибегая к использованию сложных паролей или пин-кодов. Более того, биометрические технологии могут быть использованы для защиты не только телефонов, но и других устройств и сервисов, таких как банковские счета или облачные хранилища.

**Ссылки**

1. Биометрия: Face ID vs Touch ID vs Сканер сетчатки | РАЗБОР – YouTube [Электронный ресурс] – URL: <https://www.youtube.com/watch?v=jqo5EGmQYY0> (Дата обращения: 12.07.2023).
2. Face ID – Википедия[Электронный ресурс]. URL: <https://ru.wikipedia.org/wiki/Face_ID> (Дата обращения: 11.07.2023).