**0Министерство науки и высшего образования Российской Федерации**

Федеральное государственное автономное образовательное учреждение

высшего образования

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ**

**ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Инженерная школа информационных технологий и робототехники

Отделение - ОИТ

Направление – Информатика и вычислительная техника

**Отчёт по лабораторной работе № 4**

**«Авторизация (идентификация, аутентификация)»**

по дисциплине: Защита информации

Выполнил:

студент гр. 8В7Б Мальцев М.Ю.

Проверил:

Доцент ОИТ Ботыгин И.А.

Томск 2020 г.

Оглавление

[Оглавление 2](#_Toc59453161)

[Результат работы 3](#_Toc59453162)

[1. Теоретический материал 3](#_Toc59453163)

[1.1 Введение 3](#_Toc59453164)

[1.2 Аутентификация и идентификация 3](#_Toc59453165)

[1.3 Биометрическая аутентификация 7](#_Toc59453166)

[1.4 Аутентификация по радужной оболочке глаз 11](#_Toc59453167)

[1.5 Аутентификация по геометрии лица 12](#_Toc59453168)

[1.6 Аутентификация по голосу и особенностям речи 14](#_Toc59453169)

[1.7 Биометрические технологии будущего 14](#_Toc59453170)

[2. Тест 17](#_Toc59453171)

[3. Пример аутентификации на собственной программе 20](#_Toc59453172)

[Вывод 24](#_Toc59453173)

Результат работы

1. Теоретический материал
   1. Введение

В настоящее время информационные системы (ИС) различного масштаба стали неотъемлемой частью базовой инфраструктуры государства, бизнеса, гражданского общества. Все больше защищаемой информации переносится в ИС. Современные информационные технологии не только обеспечивают новые возможности организации бизнеса, ведения государственной и общественной деятельности, но и создают значительные потребности в обеспечении безопасности для защиты информации.

Известно, что более 25 % злоупотреблений информацией в ИС совершаются внутренними пользователями, партнерами и поставщиками услуг, имеющими прямой доступ к ИС. До 70 % из них - случаи несанкционированного получения прав и привилегий, кражи и передачи учетной информации пользователей ИС, что становится возможным из-за несовершенства технологий разграничения доступа и аутентификации пользователей ИС. Совершенствование методов системы управления доступом и регистрации пользователей является одним из приоритетных направлений развития ИС.

Основными процедурами регистрации пользователей в ИС являются процедура идентификации - получение ответа на вопрос «Кто Вы?» и аутентификации - доказательства того, что «Вы именно тот, кем представляетесь». Несанкционированное получение злоумышленником доступа к ИС связано, в первую очередь, с нарушением процедуры аутентификации.

* 1. Аутентификация и идентификация

Идентификацию и аутентификацию можно считать основой программно-технических средств безопасности, поскольку остальные сервисы рассчитаны на обслуживание именованных субъектов. Идентификация и аутентификация - это первая линия обороны, "проходная" информационного пространства организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает. В качестве синонима слова "аутентификация" иногда используют словосочетание "проверка подлинности".

Аутентификация бывает односторонней (обычно клиент доказывает свою подлинность серверу) и двусторонней (взаимной). Пример односторонней аутентификации - процедура входа пользователя в систему.

В сетевой среде, когда стороны идентификации/аутентификации территориально разнесены, у рассматриваемого сервиса есть два основных аспекта:

1. что служит аутентификатором (то есть используется для подтверждения подлинности субъекта);

2. как организован (и защищен) обмен данными идентификации/аутентификации.

Субъект может подтвердить свою подлинность, предъявив, по крайней мере, одну из следующих сущностей:

. нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);

2. нечто, чем он владеет (личную карточку или иное устройство аналогичного назначения);

. нечто, что есть часть его самого (голос, отпечатки пальцев и т.п., то есть свои биометрические характеристики).

Этапы аутентификации:

Процесс аутентификации пользователя компьютером можно разделить на два этапа:

• подготовительный - выполняется при регистрации пользователя в системе. Именно тогда у пользователя запрашивается образец аутентификационной информации, например, пароль или контрольный отпечаток пальца, который будет рассматриваться системой как эталон при аутентификации;

• штатный - образец аутентификационной информации запрашивается у пользователя снова и сравнивается с хранящимся в системе эталоном. Если образец схож с эталоном с заданной точностью - пользователь считается узнанным, в противном случае пользователь будет считаться чужим, результатом чего будет, скажем, отказ в доступе на компьютер.

Для аутентификации пользователя компьютер должен хранить некую таблицу имен пользователей и соответствующих им эталонов:

В наиболее простом варианте эталоном может быть просто пароль, хранящийся в открытом виде. Однако такое хранение защищает только от непривилегированных пользователей системы - администратор системы вполне сможет получить все пароли пользователей, хранящиеся в таблице, и впоследствии входить в систему от имени любого пользователя (скажем, для выполнения каких-либо злоумышленных действий, которые будут записаны на другого). Кроме того, известен факт, что подавляющее большинство пользователей используют 1-3 пароля на все случаи жизни. Поэтому узнанный злоумышленником пароль может быть применен и к другим системам или программам, в которых зарегистрирован его владелец. Наиболее часто эталон представляет собой результат какой-либо обработки аутентификационной информации, то есть Ei = f(Ai), где Ai - аутентификационная информация, а f(...) - например, функция хэширования (расчет контрольной суммы данных с использованием криптографических методов - хэша). Хэширование достаточно часто применяется в протоколах межсетевого обмена данными, а также необходимо для использования электронной цифровой подписи.

Есть и другие варианты хранения эталонов, например, такой:

Ei = f(IDi, Ai)

Этот вариант лучше предыдущего тем, что при одинаковых паролях двух пользователей их эталоны будут выглядеть по-разному. Впрочем, в данном случае вместо имен пользователей подойдет и любая случайная последовательность, ее лишь придется хранить в той же таблице для последующего вычисления эталонов в процессе аутентификации.

В любом случае функция вычисления эталона из аутентификационной информации должна быть однонаправленной, т. е. легко рассчитываться, но представлять собой вычислительную проблему при попытке вычисления в обратном направлении.

В открытой сетевой среде между сторонами идентификации / аутентификации не существует доверенного маршрута; это значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. Необходимо обеспечить защиту от пассивного и активного прослушивания сети, то есть от перехвата, изменения и/или воспроизведения данных. Передача паролей в открытом виде, очевидно, неудовлетворительна; не спасает положение и шифрование паролей, так как оно не защищает от воспроизведения. Нужны более сложные протоколы аутентификации.

Надежная идентификация и затруднена не только из-за сетевых угроз, но и по целому ряду причин. Во-первых, почти все аутентификационные сущности можно узнать, украсть или подделать. Во-вторых, имеется противоречие между надежностью аутентификации, с одной стороны, и удобствами пользователя и системного администратора с другой. Так, из соображений безопасности необходимо с определенной частотой просить пользователя повторно вводить аутентификационную информацию (ведь на его место мог сесть другой человек), а это не только хлопотно, но и повышает вероятность того, что кто-то может подсмотреть за вводом данных. В-третьих, чем надежнее средство защиты, тем оно дороже.

Современные средства идентификации/аутентификации должны поддерживать концепцию единого входа в сеть. Единый вход в сеть - это, в первую очередь, требование удобства для пользователей. Если в корпоративной сети много информационных сервисов, допускающих независимое обращение, то многократная идентификация/аутентификация становится слишком обременительной. К сожалению, пока нельзя сказать, что единый вход в сеть стал нормой, доминирующие решения пока не сформировались.

Таким образом, необходимо искать компромисс между надежностью, доступностью по цене и удобством использования и администрирования средств идентификации и аутентификации.

* 1. Биометрическая аутентификация

Помимо использования пароля в качестве аутентификационного контроля, существует ряд биометрических возможностей, которые обладают большей надежностью.

Биометрия - это методы автоматической аутентификации человека и подтверждения личности человека, основанные на физиологических или поведенческих характеристиках. Примерами физиологических характеристик являются отпечатки пальцев, форма руки, характеристика лица, радужная оболочка глаза. К поведенческим характеристикам относятся особенности или характерные черты, либо приобретенные или появившиеся со временем, то есть динамика подписи, идентификация голоса, динамика нажатия на клавиши. Биометрия - уникальная, измеримая характеристика человека для автоматической идентификации или верификации. Термин «автоматически» означает, что биометрические технологии должны распознавать или верифицировать человека быстро и автоматически, в режиме реального времени. Идентификация с помощью биометрических технологий предполагает сравнение ранее внесенного биометрического образца с вновь поступившими биометрическими данными.

Все биометрические системы работают практически по одинаковой схеме. Во-первых, система запоминает образец биометрической характеристики (это и называется процессом записи). Во время записи некоторые биометрические системы могут попросить сделать несколько образцов для того, чтобы составить наиболее точное изображение биометрической характеристики. Затем полученная информация обрабатывается и преобразовывается в математический код.

Кроме того, система может попросить произвести еще некоторые действия для того, чтобы «приписать» биометрический образец к определенному человеку. Например, персональный идентификационный номер (PIN) прикрепляется к определенному образцу, либо смарт-карта, содержащая образец, вставляется в считывающее устройство. В таком случае, снова делается образец биометрической характеристики и сравнивается с представленным образцом.

Аутентификация по любой биометрической системе проходит четыре стадии: Запись - физический или поведенческий образец запоминается системой; Выделение - уникальная информация выносится из образца и составляется биометрический образец;

Сравнение - когда сохраненный образец сравнивается с представленным; «Совпадение/несовпадение» - система решает, совпадают ли биометрические образцы, и выносит решение.

Использование биометрии для аутентификации открывает ряд уникальных возможностей. Биометрия позволяет идентифицировать вас с помощью вас самих же. Смарт-карты, карточки с магнитной полосой, идентификационные карточки, ключи и подобные вещи, могут быть утеряны, украдены, скопированы или просто забыты дома. Пароли могут быть забыты, также украдены. Более того, постоянно развивающийся электронный бизнес и работа с информацией, представленной в электронном виде требует от человека запоминать множество паролей и персональных идентификационных номеров (PIN) для компьютерных счетов, банковских счетов, электронной почты, международных переговоров, веб - сайтов и т.п.. Биометрия предлагает быстрый, удобный, точный, надежный и не очень дорогой способ идентификации с огромным количеством самых разнообразных применений.

Нет такой единственной биометрической технологии, которая подошла бы для всех нужд. Все биометрические системы имеют свои преимущества и недостатки. Есть, однако, общие черты, которые делают биометрические технологии полезными. Во-первых, любая система должна быть основана на характеристике, которая является различимой и уникальной. Например, на протяжении века, правоохранительные органы использовали отпечатки пальцев для идентификации людей. Есть большое количество научных данных, подтверждающих идею, что не бывает двух одинаковых отпечатков пальцев. Технология, такая как идентификация, по руке, применялась долгие годы, а такие технологии как идентификации по радужной оболочке глаза или по характеристикам лица теперь получают достаточно большое распространение. Некоторые новые биометрические технологии могут быть очень точными, но могут потребовать дополнительных данных для подтверждения их уникальности. Другой аспект - насколько «дружелюбна» каждая технология. Процесс должен быть быстрым и простым, как, например, встать перед видеокамерой, сказать несколько слов в микрофон или дотронуться до сканера отпечатков пальцев. Основным преимуществом биометрических технологий является быстрая и простая идентификация без причинения каких-либо неудобств человеку.

Применения биометрических технологий разнообразны: доступ к рабочим местам и сетевым ресурсам, защита информации, обеспечение доступа к определенным ресурсам и безопасность. Ведение электронного бизнеса и электронных правительственных дел возможно только после соблюдения определенных процедур по идентификации личности. Биометрические технологии используются в области безопасности банковских обращений, инвестирования и других финансовых перемещений, а также розничной торговле, охране правопорядка, вопросах охраны здоровья, а также в сфере социальных услуг. Биометрические технологии в скором будущем будут играть главную роль в вопросах персональной идентификации во многих сферах. Применяемые отдельно или используемые совместно со смарт-картами, ключами и подписями, биометрия скоро станет применяться во всех сферах экономики и частной жизни.

В процессе биометрической аутентификации эталонный и предъявленный пользователем образцы сравнивают с некоторой погрешностью, которая определяется и устанавливается заранее. Погрешность подбирается для установления оптимального соотношения двух основных характеристик используемого средства биометрической аутентификации:(False Accept Rate) - коэффициент ложного принятия (т.е. некто успешно прошел аутентификацию под именем легального пользователя).(False Reject Rate) - коэффициент ложного отказа (т.е. легальный пользователь системы не прошел аутентификацию).

Обе величины измеряются в процентах и должны быть минимальны. Следует отметить, что величины являются обратнозависимыми, поэтому аутентифицирующий модуль при использовании биометрической аутентификации настраивается индивидуально - в зависимости от используемой биометрической характеристики и требований к качеству защиты ищется некая «золотая середина» между данными коэффициентами. Серьезное средство биометрической аутентификации должно позволять настроить коэффициент FAR до величин порядка 0,01 - 0,001 % при коэффициенте FRR до 3 - 5%.

В зависимости от используемой биометрической характеристики, средства биометрической аутентификации имеют различные достоинства и недостатки. Например, использование отпечатков пальцев наиболее привычно и удобно для пользователей, но, теоретически, возможно создание «искусственного пальца», успешно проходящего аутентификацию.

Общий же недостаток биометрической аутентификации - необходимость в оборудовании для считывания биометрических характеристик, которое может быть достаточно дорогостоящим.

В 21 веке н.э. есть достаточно много способов биометрической аутентификации. Все они делятся качественно на две большие группы, а именно: статические и динамические методы биометрической аутентификации.

Уникальные физиологические, или по другому статические, характеристики каждого человеческого организма, которые он получает от бога и природы и присущие только ему - составляют основу статических методов биометрической аутентификации. Статические характеристики человека не меняются на протяжении всей его жизни и являются неотъемлемыми от него.

* 1. Аутентификация по радужной оболочке глаз

Рисунок радужной оболочки глаза также является уникальной характеристикой человека, причем для ее сканирования достаточно портативной камеры со специализированный программным обеспечением, позволяющим захватывать изображение части лица, из которого выделяется изображение глаза, из которого в свою очередь выделяется рисунок радужной оболочки, по которому строится цифровой код для идентификации человека.

Время первичной обработки изображения в современных системах примерно 300-500мс, скорость сравнения полученного изображения с базой имеет уровень 50000-150000 сравнений в секунду на обычном ПК. Такая скорость сравнения не накладывает ограничений на применения метода в больших организациях при использовании в системах доступа. При использовании же специализированных вычислителей и алгоритмов оптимизации поиска становится даже возможным идентифицировать человека среди жителей целой страны.

Характеристики FAR и FRR для радужной оболочки глаза наилучшие в классе современных биометрических систем (за исключением, возможно, метода распознавания по сетчатке глаза).

Преимущества метода. Статистическая надёжность алгоритма. Захват изображения радужной оболочки можно производить на расстоянии от нескольких сантиметров до нескольких метров, при этом физический контакт человека с устройством не происходит. Радужная оболочка защищена от повреждений - а значит, не будет изменяться во времени. Так же, возможно использовать высокое количество методов, защищающих от подделки.

Недостатки метода. Цена системы, основанной на радужной оболочке выше цены системы, основанной на распознавании пальца или на распознавании лица. Низкая доступность готовых решений. Любой интегратор, который сегодня придёт на российский рынок и скажет «дайте мне готовую систему» - скорее всего, обломается. В большинстве своём продаются дорогие системы под ключ, устанавливаемые большими компаниями, такими как Iridian или LG.

* 1. Аутентификация по геометрии лица

Существует множество методов распознавания по геометрии лица. Все они основаны на том, что черты лица и форма черепа каждого человека индивидуальны. Эта область биометрии многим кажется привлекательной, потому что мы узнаем друг друга в первую очередь по лицу. Данная область делится на два направления: 2-D распознавание и 3-D распознавание. У каждого из них есть достоинства и недостатки, однако многое зависит еще и от области применения и требований, предъявленных к конкретному алгоритму.

**2-D распознавание лица**

2-D распознавание лица - один из самых статистически неэффективных методов биометрии. Появился он довольно давно и применялся, в основном, в криминалистике, что и способствовало его развитию. В последствие появились компьютерные интерпретации метода, в результате чего он стал более надёжным, но, безусловно, уступал и с каждым годом все больше уступает другим биометрическим методам идентификации личности. В настоящее время из-за плохих статистических показателей он применяется, в мультимодальной или, как ее еще называют, перекрестной биометрии, или в социальных сетях.

Преимущества метода. При 2-D распознавании, в отличие от большинства биометрических методов, не требуется дорогостоящее оборудование. При соответствующем оборудовании возможность распознавания на значительных расстояниях от камеры.

Недостатки. Низкая статистическая достоверность. Предъявляются требования к освещению (например, не удается регистрировать лица входящих с улицы людей в солнечный день). Для многих алгоритмов неприемлемость каких-либо внешних помех, как, например, очки, борода, некоторые элементы прически. Обязательно фронтальное изображение лица, с весьма небольшими отклонениями. Многие алгоритмы не учитывают возможные изменения мимики лица, то есть выражение должно быть нейтральным.

**3-D распознавание лица**

Реализация данного метода представляет собой довольно сложную задачу. Несмотря на это в настоящее время существует множество методов по 3-D распознаванию лица. Методы невозможно сравнить друг с другом, так как они используют различные сканеры и базы. далеко не все из них выдают FAR и FRR, используются абсолютно различные подходы.

Переходным от 2-d к 3-d методом является метод, реализующий накопления информации о лицу. Этот метод имеет лучшие характеристики, чем 2d метод, но так же как и он использует всего одну камеру. При занесении субъекта в базу субъект поворачивает голову и алгоритм соединяет изображение воедино, создавая 3d шаблон. А при распознавании используется несколько кадров видеопотока. Этот метод скорее относится к экспериментальным и реализации для систем СКУД я не видел ни разу.

Наиболее классическим методом является метод проецирования шаблона. Он состоит в том, что на объект (лицо) проецируется сетка. Далее камера делает снимки со скоростью десятки кадров в секунду, и полученные изображения обрабатываются специальной программой. Луч, падающий на искривленную поверхность, изгибается - чем больше кривизна поверхности, тем сильнее изгиб луча. Изначально при этом применялся источник видимого света, подаваемого через «жалюзи». Затем видимый свет был заменен на инфракрасный, который обладает рядом преимуществ. Обычно на первом этапе обработки отбрасываются изображения, на котором лица не видно вообще или присутствуют посторонние предметы, мешающие идентификации. По полученным снимкам восстанавливается 3-D модель лица, на которой выделяются и удаляются ненужные помехи (прическа, борода, усы и очки). Затем производится анализ модели - выделяются антропометрические особенности, которые в итоге и записываются в уникальный код, заносящийся в базу данных. Время захвата и обработки изображения составляет 1-2 секунды для лучших моделей.

Так же набирает популярность метод 3-d распознавания по изображению, получаемому с нескольких камер. Примером этого может являться фирма Vocord со своим 3d сканером.

Преимущества метода. Отсутствие необходимости контактировать со сканирующим устройством. Низкая чувствительность к внешним факторам, как на самом человеке (появление очков, бороды, изменение прически), так и в его окружении (освещенность, поворот головы). Высокий уровень надежности, сравнимый с метом идентификации по отпечаткам пальцев.

Недостатки метода. Дороговизна оборудования. Имеющиеся в продаже комплексы превосходили по цене даже сканеры радужной оболочки. Изменения мимики лица и помехи на лице ухудшают статистическую надежность метода. Метод еще недостаточно хорошо разработан, особенно в сравнении с давно применяющейся дактилоскопией, что затрудняет его широкое применение.

* 1. Аутентификация по голосу и особенностям речи

Одна из старейших технологий, в настоящее время ее развитие ускорилось - так как предполагается ее широкое использование в построении «интеллектуальных зданий». Существует достаточно много способов построения кода идентификации по голосу, как правило, это различные сочетания частотных и статистических характеристик голоса.

Ее внедрение вызвано постоянным ростом и распространением телефонных линий различного типа. Данный вид биометрии основан на анализе характеристик голоса: громкости, скорости, манере речи и др.

Основные проблемы данного вида аутентификации:

. изменение голоса (эмоции, состояние здоровья);

. помехи в микрофоне и линиях связи;

. перехват конфиденциальной информации нарушителем.

* 1. Биометрические технологии будущего

Спектр технологий, которые могут использоваться в системах безопасности, постоянно расширяется. В настоящее время ряд биометрических технологий находится в стадии разработки, причем некоторые из них считаются весьма перспективными. К ним относятся технологии на основе:

) термограммы лица в инфракрасном диапазоне излучения;

) характеристик ДНК;

) клавиатурного почерка;

) анализ структуры кожи и эпителия на пальцах на основе цифровой ультразвуковой информации (спектроскопия кожи);

) анализ отпечатков ладоней;

) анализ формы ушной раковины;

) анализ характеристик походки человека;

) анализ индивидуальных запахов человека;

) распознавание по уровню солености кожи;

) распознавание по расположению вен.

Технология построения и анализа термограммы является одним из последних достижений в области биометрии. Как обнаружили ученые, использование инфракрасных камер дает уникальную картину объектов, находящихся под кожей лица. Разные плотности кости, жира и кровеносных сосудов строго индивидуальны и определяют термографическую картину лица пользователя. Термограмма лица является уникальной, вследствие чего можно уверенно различать даже абсолютно похожих близнецов. Из дополнительных свойств этого подхода можно отметить его инвариантность по отношению к любым косметическим или косметологическим изменениям, включая пластическую хирургию, изменения макияжа и т. п., а также скрытность процедуры регистрации.

Технология, построенная на анализе характеристик ДНК (метод геномной идентификации) является, по всей видимости, хотя и самой продолжительной, но и наиболее перспективной из систем идентификации. Метод основан на том, что в ДНК человека имеются полиморфные локусы (локус -положение хромосомы (в гене или аллели), часто имеющие 8-10 аллелей. Определение набора этих аллелей для нескольких полиморфных локусов у конкретного индивида позволяет получить своего рода геномную карту, характерную только для этого человека. Точность данного метода .определяется характером и количеством анализируемых полиморфных локусов и на сегодняшний день позволяет достичь уровня 1 ошибки на 1 млн человек.

Динамику ударов по клавиатуре компьютера (клавиатурный почерк) при печатании текста анализирует способ (ритм) печатания пользователем той или иной фразы. Существуют два типа распознавания клавиатурного почерка. Первый предназначена для аутентификации пользователя при попытке получения доступа к вычислительным ресурсам. Второй осуществляет мониторинговый контроль уже после предоставления доступа и блокирует систему, если за компьютером начал работать не тот человек, которому доступ был предоставлен первоначально. Ритм работы на клавиатуре, как показали исследования ряда фирм и организаций, является достаточно индивидуальной характеристикой пользователя и вполне пригоден для его идентификации и аутентификации. Для измерения ритма оцениваются промежутки времени либо между ударами при печатании символов, расположенных в определенной последовательности, либо между моментом удара по клавише и моментом ее отпускания при печатании каждого символа в этой последовательности. Хотя второй способ считается более эффективным, наилучший результат достигается совместным использованием обоих способов. Отличительной особенностью этого метода является его дешевизна, так как для анализа информации не требуется никакого оборудования, кроме клавиатуры. В литературе описаны 4 математических подхода к решению задачи распознавания клавиатурного почерка пользователя ЭВМ: статистический, вероятностно-статистический (на базе теории распознавания образов) и нечеткой логики (на основе нейросетевых алгоритмов).

Следует отметить, что в настоящий момент данная технология находится в стадии разработки, и поэтому сложно оценить степень ее надежности, особенно с учетом высоких требований, предъявляемых к системам безопасности.

Технология анализа формы ушной раковины является одной из самых последних подходов в биометрической идентификации человека. С помощью даже недорогой Web-камеры можно получать довольно надежные образцы для сравнения и идентификации. Этот способ недостаточно изучен, в научно-технической литературе достоверная информация о текущем состоянии дел отсутствует.

В настоящее время ведутся разработки систем «электронного носа», реализующих процесс распознавания по запаху. Наличие генетического влияния на запах тела позволяют считать эту характеристику перспективной для использования в целях биометрической аутентификации личности. Как правило, «электронный нос» представляет собой комплексную систему, состоящую из трех функциональных узлов, работающих в режиме периодического восприятия пахучих веществ: системы пробоотбора и пробоподготовки, линейки или матрицы сенсоров с заданными свойствами и блока процессорной обработки сигналов матрицы сенсоров. Этой технологии, как и технологии анализа формы ушной раковины, еще предстоит пройти долгий путь развития, прежде чем она станет удовлетворять биометрическим требованиям.

1. Тест

Авторизацией называется

* Процесс, посредством которого идентификация предполагаемой личности проверяется на основе документа, удостоверяющего личность.
* Аутентификация основанная на двух разных типах идентификации.
* Часть идентичности, которая отражает определенную врожденную особенность личности, то есть то что связано с конкретной личностью.
* **Процесс, который дает (или отключает) право доступа к (сетевым) ресурсам.**

Какие из следующих действий идентифицируют вашу личность (выберите два)?

* **Показываю чиновнику удостоверение личности, и он его проверяет.**
* Называю чиновнику своё имя.
* Звоню чиновнику и сообщаю своё имя и личный код, после чего он проверяет данные в базы данных.
* **Когда я нахожусь на приеме у чиновника, сообщаю своё имя и личный код, после чего он проверяет данные в базы данных.**

Двойной защитой называется

* Аутентификация на основе двух идентификаторов.
* **Аутентификация основана на двух разных типах идентификации.**
* Аутентификация, основанная на двух или более различных типах идентификации.

Идентификатор — это…

* **уникальный набор символов, однозначно соответствующий объекту или субъекту в данной системе.**
* распознавание участника процесса информационного взаимодействия (ИВ) перед тем, как к нему будут применены какие-либо аспекты ИБ.
* секретный набор символов, позволяющий подтвердить соответствие субъекта предъявленному им идентификатору.
* обеспечение уверенности в том, что участник ИВ идентифицирован верно.

Как называется процесс предоставления определенных полномочий лицу или группе лиц на выполнение некоторых действий в системе?

* Аутентификация
* **Авторизация**
* Идентификация
* Мандатный контроль доступа

Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от (выберите два):

* перехвата;
* **воспроизведения;**
* **атак на доступность.**

В качестве аутентификатора в сетевой среде могут использоваться:

* год рождения субъекта;
* фамилия субъекта;
* **секретный криптографический ключ**

Какой вид идентификации и аутентификации получил наибольшее распространение?

* Системы PKI
* **Постоянные пароли**
* Одноразовые пароли

Какой способ аутентификации самый небезопасный?

* **Однофакторная аутентификация**
* Двухфакторная аутентификация
* Многофакторная аутентификация

Какого варианта реализации системы аутентификации по одноразовым паролям не существует?

* Метод «запрос-ответ»
* Метод «только ответ»
* **Метод «только запрос»**
* Метод «синхронизация по времени»

1. Пример аутентификации на собственной программе

В данном разделе представлен пример аутентификации при помощи языка Kotlin для операционной системы Android.

При реализации примера был использован только класс кодировки Base64, чтобы реализовать базовый тип аутентификации (basic auth). Для демонстрации примера работы был создан класс AuthExample, имеющий метод авторизации и регистрации, а также поле, хранящее массив пользователей.

**class** **AuthExample** {

**private** **val** users = mutableMapOf("user" to "1234", "test" to "test")

**fun** **login**(name: String, password: String): String {}

**fun** **register**(name: String, password: String): String {}

}

Для авторизации используется метод login(), параметрами которого являются имя и пароль пользователя. Метод возвращает либо текст с ошибкой при неуспешной авторизации, либо строку с указанием типа авторизации (basic) и зашифрованную строку, которая является ключом авторизации, если имя и пароль совпадают. Ключ формируется путем шифрования данных пользователя с помощью алгоритма Base64 в виде <login:password>.

**fun** **login**(name: String, password: String): String {

**return** **try** {

**if** (users.getValue(name) == password) {

"Authorization: Basic " + Base64.getEncoder()

.encodeToString("$name:$password".toByteArray())

} **else** {

"Неправильный пароль."

}

} **catch** (e: NoSuchElementException) {

"Такого пользователя не существует"

}

}

Регистрация пользователя реализована в методе register(). Входными параметрами являются имя пользователя и пароль. При вызове метода, регистрация может считаться успешной, если введенное имя пользователя не совпадает с уже имеющимся. Метод возвращает только статус выполнения операции.

**fun** **register**(name: String, password: String): String {

**return** **if** (users.containsKey(name)) {

"Такой пользователь уже существует"

} **else** {

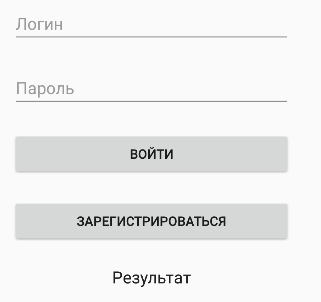
users[name] = password

**return** "Пользователь успешно зарегистрирован"

}

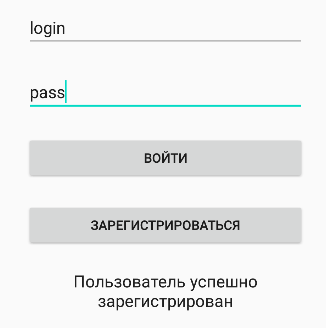
}

Для выполнения приведенного выше примера был создан простой интерфейс в приложении android, представленный на рисунках ниже.



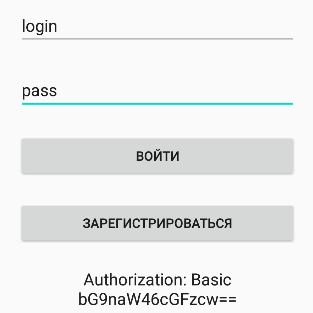
1. – Изначальный интерфейс

На рисунке выше представлены поля ввода логина и пароля, кнопки для входа в учетную запись и ее регистрации, а также поле, выводящее результат операции.



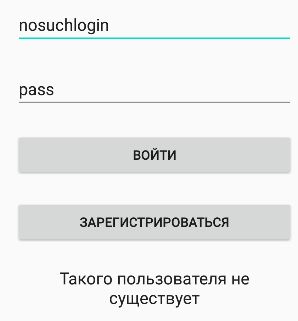
1. – Регистрация

При нажатии кнопки «Зарегистрироваться» будет вызвать метод register, берущий значение полей логина и пароля. На рисунке регистрация прошла успешно, о чем оповестило поле под кнопкой регистрации.



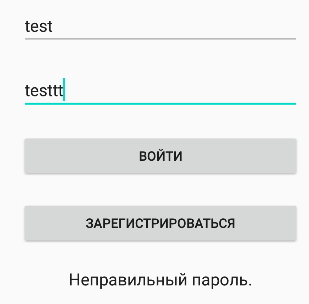
1. – Вход в учетную запись

После регистрации пользователя, можно войти в созданную учетную запись. При нажатии кнопки «войти» вызывается метод login(), возвращающий результат операции в поле результата. На рисунке видно, что пользователь успешно авторизовался и получил заголовок авторизации базового типа (Authorization Basic). Такая строка должна быть использована в качестве заголовка каждого запроса в систему, требующего авторизации. Несмотря на то, что базовый способ авторизации не безопасен, он подходит для того, чтобы показать принцип работы.



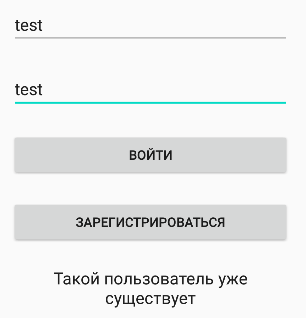
1. – Попытка войти в несуществующую учетную запись

Далее, были проверены ошибки. Так, на приведенном выше рисунке, введен несуществующий пользователь, о чем оповещает система.



1. – Попытка войти с неправильным паролем

Также при входе в учетную запись проверяется пароль пользователя. В данном случае, был введен неправильный пароль, что отображается в поле результата.



1. – Попытка зарегистрировать такую же учетную запись

На данном рисунке, была осуществлена попытка зарегистрироваться с таким же именем пользователя. Метод register возвращает статус операции, означающий, что регистрация не была завершена.

Из приведенных выше рисунков можно сделать вывод, что программа корректно выполняет свою работу.

Вывод

В процессе выполнения лабораторной работы было проведено исследование на тему авторизации. Теоретические знания подкреплены практическим примером авторизации, реализованной на языке программирования Kotlin с графическим интерфейсом операционной системы Android.

Приложение А. Исходный код приложения

AuthExample:

**class** **AuthExample** {

**private** **val** users = mutableMapOf("user" to "1234", "test" to "test")

**fun** **login**(name: String, password: String): String {

**return** **try** {

**if** (users.getValue(name) == password) {

"Authorization: Basic " + Base64.getEncoder()

.encodeToString("$name:$password".toByteArray())

} **else** {

"Неправильный пароль."

}

} **catch** (e: NoSuchElementException) {

"Такого пользователя не существует"

}

}

**fun** **register**(name: String, password: String): String {

**return** **if** (users.containsKey(name)) {

"Такой пользователь уже существует"

} **else** {

users[name] = password

**return** "Пользователь успешно зарегистрирован"

}

}

}

Android View:

**val** authExample = AuthExample()

loginButton.setOnClickListener {

**val** result = authExample.login(

userNameInputView.text.toString(),

passwordInputView.text.toString()

)

authResultView.text = result

}

registerButton.setOnClickListener {

**val** result = authExample.register(

userNameInputView.text.toString(),

passwordInputView.text.toString()

)

authResultView.text = result

}