sqrt(-1)

команда
sqrt(-1)

Конкурс проектов по решению глобальных проблем информационной безопасности

Кейс: “Концепция системы гарантированной идентификации личности пользователя в Сети”

Участники команды:

Шеренешева Анастасия

[архитектор]

ГБОУ СОШ №17,10 класс,
г.Москва
n.schereneschewa2010@yandex.ru
+7 966 115 0304

Кабаченко Фёдор

[бизнес-менеджер]

МКОУ СОШ №3, 10 класс,
г.Нефтекумск
fkabachenko@gmail.com
+7 962 430 0117

Янченко Пётр

[программист]

МКОУ СОШ №3, 11 класс
г.Нефтекумск
petr.yanchenko@mail.ru
+7 906 469 8485

sqrt(-1)

команда sqrt(-1)

Исследование решений по идентификации личности

Сравнение и анализ действующих систем идентификации:

Проблема: В век информационных технологий никто не застрахован от кибератак. В связи с этим очень важно усилить защиту персональных данных пользователей.

Мы сравнили существующие системы идентификации личности по основным параметрам (см. таблицу).

Вывод: Наилучшими вариантами идентификации личности являются биометрические данные и специальные знания. Биометрия обеспечивает наивысшую защиту данных и максимальное удобство использования, а специальные знания – низкую стоимость и предельную простоту реализации.

Исходя из полученных данных, нашей задачей является создание системы идентификации личности, разработанной на основе синтеза биометрии и специфических знаний.

Использованные методы:
- сравнение (сопоставление нескольких объектов исследования, выделение общего и частного);
- анализ (рассмотрение отдельных сторон объекта);
- индукция и дедукция (рассуждение от частных фактов к общим выводам и наоборот);
- формализация (упрощенное представление объекта(-ов));
- обобщение (приведение всей информации к общему выводу).

sqrt(-1)

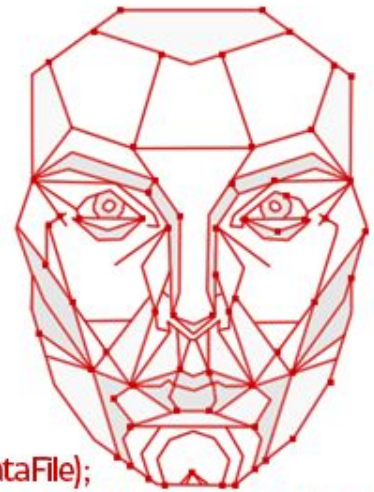
команда sqrt(-1)

Исследование решений по идентификации личности

Анализ собственного предложения:

Мы предлагаем систему идентификации личности, основанную на вводе пароля, отправке данных об об устройстве и последующем 3D распознавании контура лица.

Реализация системы предполагается в формате десктопного и мобильного приложения. Мы старались популяризировать систему, поэтому она доступна как для физических, так и для юридических лиц. Система может использоваться для совершения безопасных интернет-платежей, для контроля доступа в офисы, общественный транспорт и др.



```
Encrypt(DataFile);
SendToServer(DataFile,ServerAddress);
return 0;
```

Важнейшим критерием системы идентификации личности является *безопасность информации*. Наряду с нашим решением существуют и другие, способные качественно защитить данные.
НО! Создание системы по прототипу нашей необходимо, т.к. отсутствие дополнительного биометрического оборудования существенно упрощает использование и реализацию проекта.

Пользователь будет заинтересован в использовании нашей системы, потому что она надежна и удобна. Достаточно иметь устройство выход в Интернет и голову на плечах.

Преимуществами нашего предложения перед другими системами идентификации является:
- многоступенчатый уровень защиты данных;
- универсальность и простота использования (система работает в устройствах ежедневного пользования).

ВЫВОД: Опираясь на проведенное исследование, мы выяснили, что наилучшим вариантом системы идентификации личности станет решение, основанное на вводе пароля, инициализации параметров устройства и последующем 3D распознавании лица.

sqrt(-1)

команда sqrt(-1)

Описание функционала системы

- **Создание нового пользователя**

  Предоставляется возможность пользоваться новой системой

- **Безопасное хранение данных**

  Обеспечение безопасного хранения отправляемых данных

- **Аутентификация**

  Проверка подлинности предъявленного пользователем идентификатора

- **Восстановление потерянных данных**

  Откат к первоначальным настройкам пользователя, либо восстановление данных через BIP

sqrt(-1)

команда sqrt(-1)

Описание функционала системы

- **Усиленное шифрование данных**

  Усложнение шифрования для максимальной надежности хранения информации

- **Корректирование данных**

  Удаление или изменение существующей информации и дополнение к уже имеющейся

- **Универсальное использование**

  Возможность использования разного fixed key каждой организацией для идентификации личности

Вывод: Система идентификации обладает хорошим и многообразным функционалом, обеспечивающим удобство и надежность в использовании.

sqrt(-1)

команда sqrt(-1) | Технология реализации системы идентификации

Описание высокоуровневого алгоритма:

Основной функционал мы предлагаем реализовать через инициализацию параметров устройства*, а дополнительный через датчик внутри устройства**:

Наша система предполагает симметричный алгоритм блочного шифрования, использованиехэша алгоритма хэширования и randomseed для первичного шифрования координат. Конечное шифрование предполагает использование fixed key.

Используемые алгоритмы, действия и данные:

- HWID or UniquelD;
- (x;y;z);
- randomseed;
- md5 hash;
- AES256;
- SHA256;
- fixed key.

Вывод: Сочетание алгоритмов шифрования и дополнительных команд для изменения данных обеспечивает максимально безопасное хранение и лёгкую корректировку в случае утери или обновления данных.

sqrt(-1)

команда sqrt(-1)

Оценка рисков системы

Риски и пути их решения:

• Риски:	• Пути решения:
В любой биометрической системе существует вероятность возникновения зависимых друг от друга коэффициентов ложного пропуска: - FAR (False Acceptance Rate) – предоставление доступа незарегистрированному пользователю; - FRR (False Rejection Rate) – запрет доступа зарегистрированному в системе человеку.	Наилучшим решением является снижение вероятностей коэффициентов ложного пропуска: система тем лучше, чем меньше значение FRR при одинаковых значениях FAR.
Всегда существует шанс узнать fixed key, который упрощает расшифровку данных, а значит и увеличивает шанс взлома базы данных.	Создание более сложного fixed key (или сразу несколько).

Вывод: Риски есть во всех системах. И все риски имеют пути решения. Мы определили самые главные риски нашей системы (FAR,FRR и fixed key) и предположили лучшие пути их решения через снижение вероятностей коэффициентов ложного пропуска и создании усложнённого фиксированного ключа.