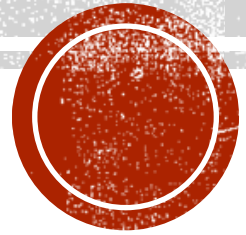
ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БЕЗДРОТОВИХ МЕРЕЖ ПЕРЕДАВАННЯ ДАНИХ ЗА РАХУНОК ГОЛОСОВОЇ АВТЕНТИФІКАЦІЇ

Оверченко Юрій УБ-19м



Мета роботи полягає в підвищенні захищеності інформаційної безпеки безпровідних мереж передавання даних за рахунок голосової автентифікації

Для досягнення вищевказаної мети необхідно виконати такі задачі:

- Проаналізувати недоліки захисту бездротових мереж передавання даних;
- Розглянути існуючі способи автентифікації;
- Вибрати найкращий спосіб автентифікації;
- Вибрати метод автентифікації;
- Вибрати мову програмування для розробки програмного забезпечння;
- Розробити програмне забезпечення для підвищення захищеності бездротових мереж передавання даних.

Об’єктом дослідження є процес захисту бездротових мереж передавання даних.

Предметом дослідження є методи захисту бездротових мереж передавання даних.

Wi-Fi Інтернет працює через радіохвилі. **Wi-Fi** використовує радіочастоти для передачі даних від роутера, який і є джерелом сигналу до пристрою або одержувачу. Ці частоти вимірюються в гігагерцах. Так, 1 герц дорівнює одній секунді, а один гігагерц - дорівнює 1 млрд. хвиль в секунду. Частоти, якими користуються роутери становлять п'ять гігагерц в секунду

Переваги **Wi-Fi**:

- Дозволяє розвернути мережу без прокладки кабелю, що може зменшити вартість розгортання і/або розширення мережі. Місця, де не можна прокласти кабель, наприклад, поза приміщеннями і в будівлях, що мають історичну цінність, можуть обслуговуватися безпровідними мережами.
- Дозволяє мати доступ до мережі мобільним пристроям.
- **Wi-Fi**-пристрої широко поширені на ринку. Гарантується сумісність устаткування завдяки обов'язковій сертифікації устаткування з логотипом **Wi-Fi.**
- Випромінювання від **Wi-Fi**-пристроїв у момент передачі даних на два порядки (у 100 разів) менше, ніж біля стільникового телефону.
- **Wi-Fi** — це набір глобальних стандартів. На відміну від стільникових телефонів, **Wi-Fi**-устаткування може працювати в різних країнах по всьому світу.

БЕЗПРОВІДНА МЕРЕЖА ПЕРЕДАЧІ ДАНИХ WI FI НЕ Є ДОСТАТНЬО ЗАХИЩЕНОЮ, ТАК ЯК ПРИ ПІДКЛЮЧЕНІ ПОТРІБНО ВВОДИТИ ЛИШЕ ПАРОЛЬ. ТОМУ НЕ СКЛАДАЄ ТРУДНОЩІВ ЩОБ ОТРИМАТИ КОНФІДЕНЦІЙНУ ІНФОРМАЦІЮ ТРЕТІЙ ОСОБІ.

Недоліки **Wi-Fi**:

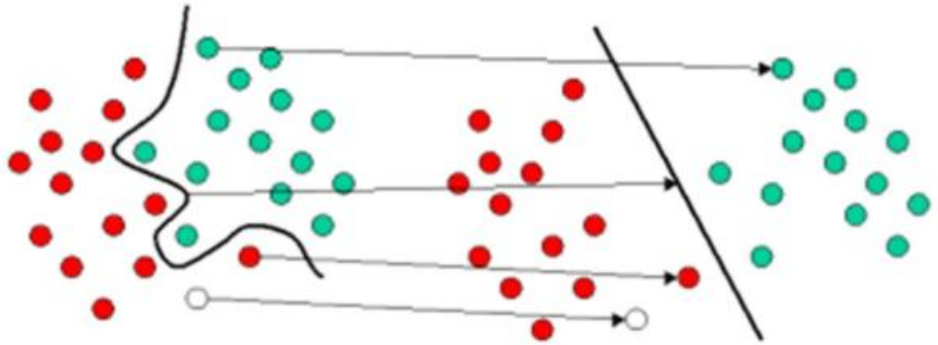
- Невелика ширина використовуваного спектра частот, відсутність можливостей роумінгу й авторизації не дозволяють **Wi-Fi**-пристроям потіснити на ринку мобільний зв'язок. Проте компанії **ZyXEL**, **SocketIP** і **Symbol Technologies** пропонують рішення з організації **Wi-Fi**-телефонії.
- Частотний діапазон і експлуатаційні обмеження в різних країнах неоднакові. У багатьох європейських країнах дозволено два додаткові канали, які заборонені в США; у Японії є ще один канал у верхній частці діапазону, а інші країни, наприклад Іспанія, забороняють використання низькочастотних каналів. Більш того, деякі країни, наприклад Росія, Білорусь і Італія, вимагають реєстрації всіх мереж **Wi-Fi** приміщень, що працюють зовні, або вимагають реєстрації **Wi-Fi**-оператора.
- Як було згадано вище, в Росії точки безпровідного доступу, а також адаптери **Wi-Fi** з ЕІВП, що перевищує 100 мВт (20 дБм), підлягають обов'язковій реєстрації.
- Найпопулярніший стандарт шифрування **WEP** може бути відносно легко зламаний навіть при правильній конфігурації (через слабку стійкість алгоритму). Не зважаючи на те, що нові пристрої підтримують досконаліший протокол шифрування даних **WPA** і **WPA2**, багато старих точок доступу не підтримують його і вимагають заміни. Ухвалення стандарту **IEEE 802.11i (WPA2)** в червні 2004 року зробило доступною безпечнішу схему, яка доступна в новому устаткуванні. Обидві схеми вимагають стійкіший пароль, ніж ті, які зазвичай призначаються користувачами. Багато організацій використовують додаткове шифрування (наприклад **VPN**) для захисту від вторгнення.

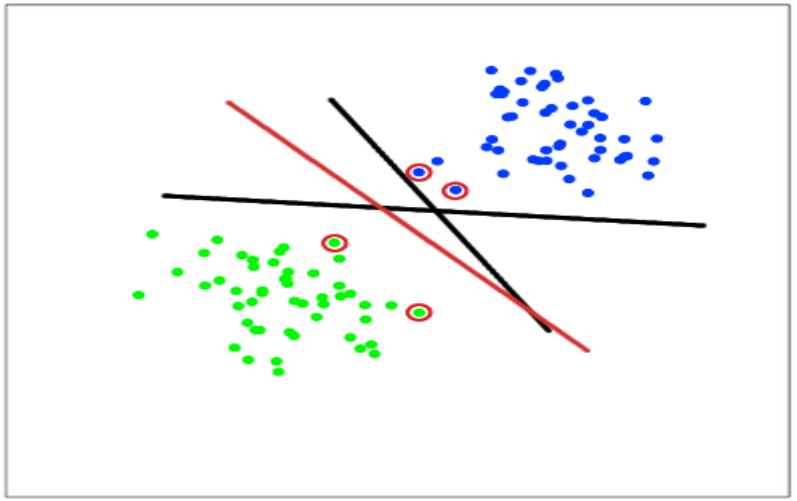
У дипломній роботі було проаналізовано різні форми біометричної автентифікації, та було визначено, що голосової автентифікації буде достатньо для захисту безпровідної мережі передачі даних **WI FI.**

Також голосова форма автентифікаціє є кращою ніж інші форми біометричної автентифікації особи. Тому що для її реалізації не потрібно багато складових, так як мікрофон є - влаштований в комп’ютер або ж в багатьох навушниках .

Було досліджено та проаналізовано різні методи голосової автентифікації та вибрано – метод опорних векторів.Він виявився найкращим з проаналізованих, так як він являється текстонезалежним.

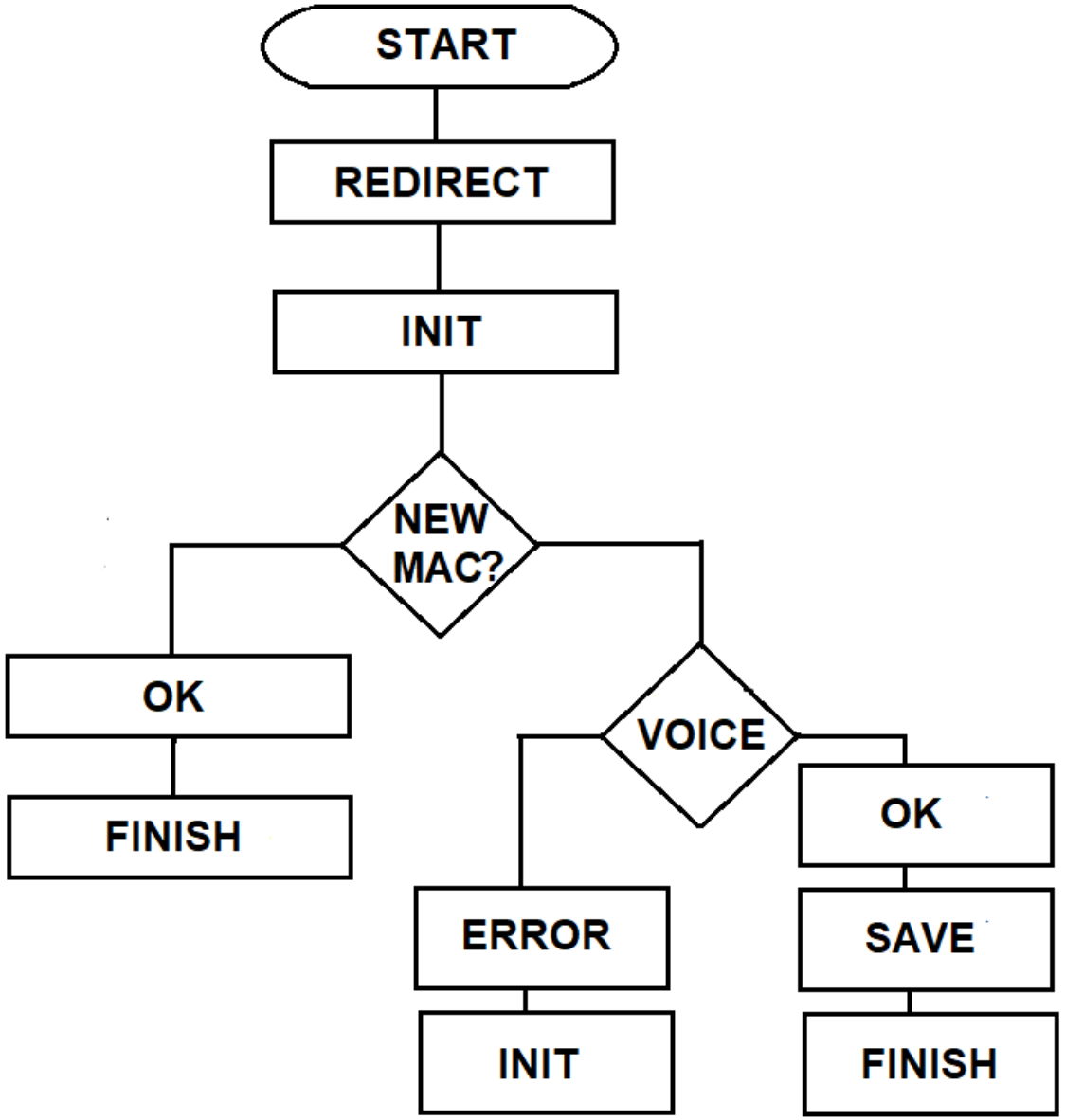
Цей алгоритм створює лінію або гіперплощину, яка ділить дані на класи. Як у дитячій задачі, де треба однією лінією розділити червоні і сині кружечки, алгоритм повинен знайти найбільш правильну лінію. Але таких ліній може бути дуже багато. Комп'ютер шукає такі точки на графіку, які розташовані найближче до лінії поділу. Ці точки називаються опорними векторами. Потім алгоритм обчислює відстань між опорними векторами і розділяє площиною. Основна мета алгоритму - знайти таке місце, де це відстань буде максимально велика.





Для досягнення мети, яка була поставлена в даній роботі. Було створено сайт для автентифікації, програмне забезпечення для автентифікації по голосу та налаштування до роутера , для перепосилання користувача на потрібний сайт.

При підключені до мережі WI-FI, відповідно від завантажених налаштувань в систему роутера, користувача відразу буде перенаправляти на сайт на якому буде проводитись авторизація.За допомогою створеного ПЗ на сайті з’явиться вікно авторизації, яке повідомить, що для авторизації потрібно проговорити фразу, якщо голос користувача співпаде, авторизація пройде успішно і вхід в мережу буде здійснено.



При підключенні до мережі **Wi FI** , користувача буде перенаправлено на сайт для голосової автентифікації, коли користувач натисне кнопку «Авторизуватись по голосу» , ПЗ запуститься та визначить чи це вже зареєстрований користувач чи ні, якщо користувач вже зареєстрований тоді його підключить до мережі **WI FI**, якщо ж це новий користувач він проходить автентифікацію по голосу, якщо голос не співпадає тоді система видасть помилку, якщо ж голос співпадає тоді система збереже мак адресу та підключення до мережі **WI FI** буде проведено.

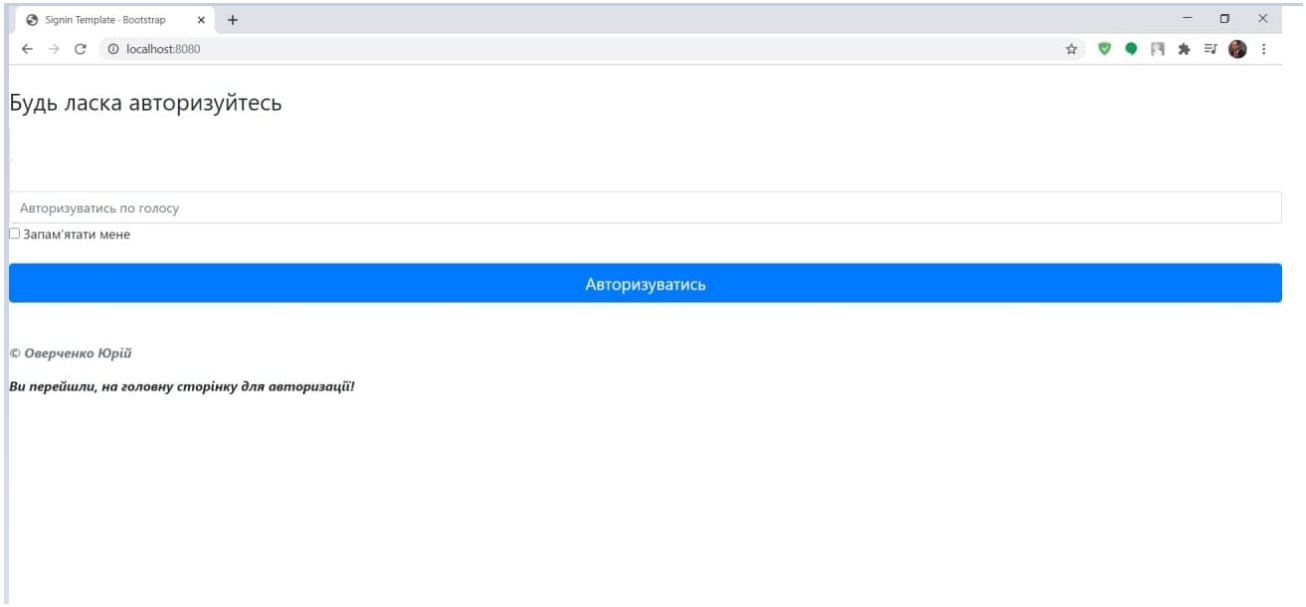
При створенні сайту та ПЗ було вибрано мови програмування:

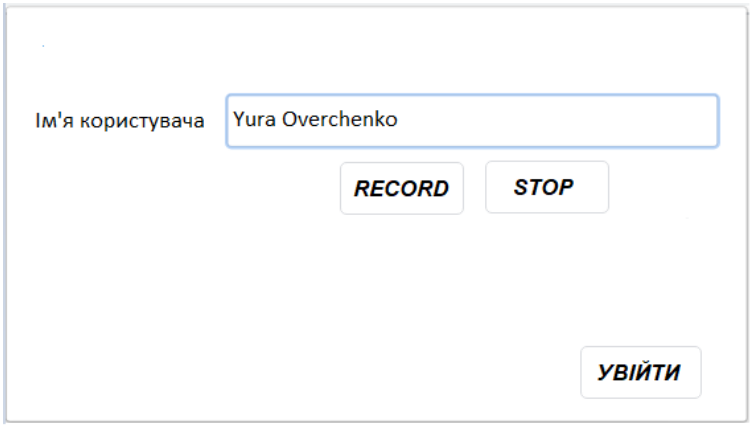
Java має переваги над іншими мовами програмування, так як на даній мові програмування можна написати як і сайт так і ПЗ до нього.

Також було вибрано фреймворк для роботи з сайтом **Java Spring Boot.**

Для розробки зручного та привабливого інтерфейсу було обрано мови програмування **HTML** і **CSS.**

Та для розробки було вибрано середовище IntelliJ IDEA.





Вигляд головної сторінки , вікна для автентифікації та помилки при не успішній автентифікації

ДЯКУЮ ЗА УВАГУ!