МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ЕКОНОМІКО-ПРАВОВИЙ ФАКУЛЬТЕТ
КАФЕДРА СИСТЕМНОГО АНАЛІЗУ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Допустити до захисту

В.о. завідувача кафедри

_____ Мнацаканян М.С.

(підпис) *(ПІБ завідувача кафедри)*

«___»_____20__ р.

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ПО ПАРАМЕТРИЧНОМУ (ЕЛЕКТРО-МАГНІТНОМУ) КАНАЛУ

Кваліфікаційна робота
здобувача вищої освіти
першого (бакалаврського) рівня вищої освіти
освітньо-професійної програми
«____Комп'ютерні науки_____»
(назва освітньо-професійної програми)

_____
(прізвище, імя, по батькові здобувача вищої освіти)

Науковий керівник:
_Козловський В.В., д.т.н., професор __
(прізвище, ініціали, науковий ступінь, вчене звання)

Рецензент:
__Охріменко Т.О., к.т.н., НАУ_
(прізвище, ініціали, науковий ступінь, вчене звання, місце роботи)

Кваліфікаційна робота захищена
з оцінкою_____
Секретар ЕК_____
«____» _____20__ р.

Київ -2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ЕКОНОМІКО-ПРАВОВИЙ ФАКУЛЬТЕТ
КАФЕДРА СИСТЕМНОГО АНАЛІЗУ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Рівень вищої освіти *бакалавр*
Шифр та назва спеціальності *122 «Комп'ютерні науки»*
Освітньо-професійна програма *«Комп'ютерні науки»*

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри к.т.н.
(науковий ступінь, вчене звання)
_____ Мнацаканян М.С.
(підпис) *(ПІБ завідувача кафедри)*
«__» _____ 20__ р.

ПЛАН ВИКОНАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Кириченко Данило Миколайович
(прізвище, ім'я, по батькові)

1. Тема роботи: «Захист інформації від витоку по параметричному (електромагнітному) каналу»

керівник роботи_ Козловський В.В., д.т.н., професор_____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом Маріупольського державного університету від «___» _____20__ р. №__

2. Строк подання здобувачем роботи .

3. Вихідні дані до роботи (мета, об'єкт, предмет):

Об’єкт дослідження цифрова система адаптивного круїз-контролю автомобіля, вай-фай модуль.

Предмет дослідження – вай-фай модуль в цифровій системі адаптивного круїз-контролю автомобіля.

Мета кваліфікаційної роботи – Дізнатися по засоби захисту інформації від витоку по електро-магнитному каналу вай-фай модуля в цифровій системі адаптивного круїз-контролю автомобіля.

4. Зміст роботи

Розділ 1.Пошук інформації про параметричний канал.

Розділ 2.Аналіз вай-фай модуля в цифровій системі адаптивного круїз-контролю автомобіля.

Розділ 3. Знаходження засобів захисту ва-фай модуля.

5. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Аналіз предметної області, пошук даних про параметричний канал. Написання першого розділу.		
2.	Опис і надання інформації про вай фай модуль. Написання другого розділу		
3.	Наведення прикладів захисту вай фай модуля від витоку даних. Написання третього розділу		
4.	Редагування пояснювальної записки кваліфікаційної роботи.		
5.	Проходження перевірки на плагіат.		
6.	Підготовка презентації.		

Здобувач _____ _____
(підпис) *(прізвище та ініціали)*

Науковий керівник роботи _____ _____
(підпис) *(прізвище та ініціали)*

РЕФЕРАТ

Дипломна робота на тему «Захист інформації від витоку по параметричному (електро-магнітному) каналу».

Об'єкт дослідження: цифрова система адаптивного круїз-контролю автомобіля, вай-фай модуль.

Предмет дослідження: вай-фай модуль в цифровій системі адаптивного круїз-контролю автомобіля.

Мета проекту – Дізнатися по засоби захисту інформації від витоку по електро-магнитному каналу вай-фай модуля в цифровій системі адаптивного круїз-контролю автомобіля.

У роботі розглядаються питання захисту вай-фай модулю від витоку інформації по електро-магнитному каналу.

Ключові слова: АДАПТИВНИЙ КРУЇЗ-КОНТРОЛЬ, ACC, АЛГОРИТМ, ЦИФРОВІ СИСТЕМИ, DACC, МЕТОД, PILOT, ВАЙ-ФАЙ, МОДУЛЬ, ЕЛЕКТРО-МАГНИТНИЙ, КАНАЛ, ІНФОРМАЦІЯ, ЗАХИСТ, ЕЛЕКТРО-МАГНІТНИЙ, КАНАЛ, ВИТІК, КІБЕР-БЕЗПЕКА, АТАКИ, ХАКЕРИ.

ЗМІСТ

ВСТУП

Електромагнітні канали належать до властивостей матеріалів і систем, які впливають на їхню взаємодію з електромагнітним випромінюванням. Ці характеристики визначають, як матеріали і системи взаємодіють з електромагнітними полями, включно зі світлом, радіохвилями, мікрохвилями та іншими формами електромагнітного випромінювання.

Витік інформації означає несанкціоноване розкриття або доступ до конфіденційної чи захищеної інформації. Це може статися внаслідок різних чинників, включно з технічними властивостями, помилками в налаштуваннях системи, недоліками в процесах управління інформацією або зловмисними діями з боку зловмисників.

Це може мати серйозні наслідки, як-от фінансові втрати, порушення конфіденційності клієнтів, шкода репутації, порушення законодавства та інші негативні наслідки. Важливо вживати заходів для захисту інформації та запобігання витокам.

Зі звіту Державного центру кіберзахисту нам стало відомо, що за 2022 рік загалом було опрацьовано 19 млрд подій, зібраних за допомогою засобів моніторингу, аналізу та передавання телеметричної інформації про кіберінциденти та кібератаки. Кількість зареєстрованих і оброблених кіберінцидентів зросла до 64.

Як і раніше, основною метою хакерів є кібершпигунство, порушення доступності державних інформаційних сервісів і знищення інформаційних систем за допомогою програм-вайперів. У 2022 році зафіксовано суттєве зростання активності хакерських груп із розповсюдження шкідливого програмного забезпечення на 38% у категорії "Шкідливий програмний код". У зв'язку зі зростанням збільшення кібератак варто приділити велику увагу кіберзахисту, зокрема захисту від витоку інформації параметричним (електро-магнітному) каналом.

1.Основні електромагнітні характеристики

Деякі основні електромагнітні характеристики включають:

1. Пропускна здатність (прозорість): здатність матеріалу або середовища пропускати електромагнітне випромінювання без значного його поглинання або розсіювання. Матеріали з високою прозорістю забезпечують хорошу передачу світла або радіохвиль через себе.
2. Поглинання: Це здатність поглинати електромагнітне випромінювання. Поглинання може призводити до зміни інтенсивності або частоти випромінювання під час проходження через матеріал або середовище.
3. Відображення: Це здатність матеріалу відбивати електромагнітне випромінювання від своєї поверхні. Віддзеркалення може змінювати напрямок та інтенсивність випромінювання.
4. Розсіювання: зміна напрямку поширення електромагнітного випромінювання під час взаємодії з матеріалами або середовищем. Розсіювання може призводити до розсіяного випромінювання, яке поширюється в різних напрямках.
5. Заломлення: Це зміна напрямку поширення електромагнітного випромінювання під час переходу з одного середовища в інше з різними оптичними властивостями. Заломлення відбувається через різну швидкість поширення світла в різних середовищах.
6. Магнітна проникність: Це властивість матеріалу, що визначає його взаємодію з магнітним полем. Магнітна проникність описує, наскільки матеріал може "проникнути" в магнітне поле або сконцентрувати його всередині себе.
7. Діелектрична проникність речовини: властивість речовини, що визначає її взаємодію з електричним полем. Діелектрична проникність впливає на електричну поляризацію речовини під впливом зовнішнього електричного поля.
8. Індуктивність: Це властивість електричного ланцюга або компонента, що визначає його здатність створювати магнітне поле під час проходження електричного струму через нього. Індуктивність вимірюється в генрі і впливає на перехід електричної енергії в магнітну і назад.

2. Можливі причини та способи витоку інформації

Можливі причини та способи витоку інформації включають:

1. Несанкціонований доступ до системи або пристрою: Це може статися, якщо зловмисник отримує доступ до облікових даних, паролів або слабо захищених систем. Зловмисники можуть використовувати цей доступ для крадіжки або розкриття конфіденційних даних.
2. Фізичні загрози: Неконтрольований доступ до фізичних пристроїв або документів, таких як вкрадені ноутбуки, загублені USB-накопичувачі або неправильно утилізовані паперові документи, може призвести до витоку інформації.
3. Між мережеві атаки та хакерство: Зловмисники можуть використовувати різні техніки, як-от фішинг, шкідливі програми, атаки на слабкі місця системи або відмову в обслуговуванні (DDoS), щоб отримати доступ до системи та вкрасти конфіденційні дані.
4. Несанкціонований доступ до мережі: Якщо мережа недостатньо захищена, зловмисники можуть перехоплювати або підслуховувати мережевий трафік, щоб отримати доступ до переданої інформації.
5. Недоліки в процесах управління інформацією: Неправильне налаштування доступу до даних, відсутність контролю за обліковими записами, недостатні заходи безпеки або недостатнє навчання співробітників з питань інформаційної безпеки можуть призвести до витоку інформації.

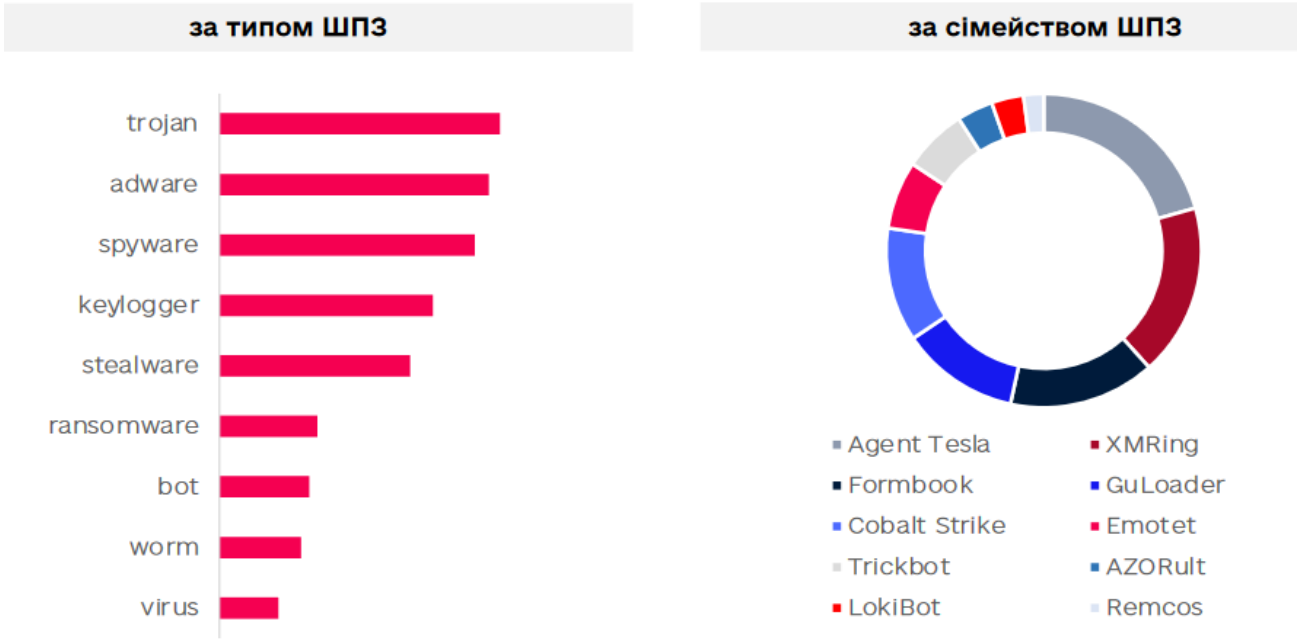

Рисунок 1 – «Шкідливе програмне забезпечення»

3. Адаптивний круїз-контроль

Адаптивний круїз-контроль (ACC) - це просунута система керування швидкістю автомобіля, яка дозволяє водієві встановити бажану швидкість та відстань до інших транспортних засобів, а потім підтримувати цю швидкість та відстань автоматично.

Коли ACC увімкнена, система використовує радар, лазерний датчик або камеру, щоб визначити відстань до транспортного засобу, що йде попереду, і швидкість цього транспортного засобу. Потім система налаштовує швидкість вашого автомобіля, щоб зберігати безпечну відстань до транспортного засобу попереду. Якщо водій автомобіля знаходиться на дистанції, яка може стати небезпечною, система автоматично зменшує швидкість або повністю зупиняє автомобіль.

Спочатку використовується набір даних, що містить інформацію про швидкість, відстань, прискорення, час реакції та інші параметри руху автомобіля в різних умовах. Цей набір даних може бути зібраний за допомогою калібрувальних тестів на автодромі або реальних дорожніх умовах.

Рисунок 2 – «Адаптивний круїз-контроль автомобіля»

4. Перехід до нових технологій

Цифрові системи адаптивного круїз-контролю (DACC) – це нове покоління систем ACC, які використовують цифрові датчики та алгоритми обробки даних для більш точного та ефективного керування автомобілем на дорозі.

Основна відмінність DACC від стандартних систем ACC полягає в тому, що вони використовують цифрові датчики, такі як камери, радари та лідери, які збирають більш точну інформацію про дорожню обстановку та навколишнє середовище. Ці дані передаються в комп'ютерну систему автомобіля, де вони обробляються алгоритмами машинного навчання прийняття більш точних рішень про керування автомобілем на дорозі.

Крім того, вони також можуть використовувати інформацію про трафік та погодні умови, що отримується через системи зв'язку та навігації автомобіля, для оптимального керування автомобілем та максимального використання можливостей системи.

З технічної точки зору до оснастити круїз-контролем можна будь-який автомобіль, проте в абсолютній більшості випадків ця операція здійснюється ще на етапі збирання транспортного засобу на конвеєрі.

Крім своєї основної функції (підтримання заданої швидкості), круїз-контроль чудово виконує ще одне завдання – економить паливо. На відміну від людини, електроніка дозує подачу палива грамотніше та плавніше, тим самим знижуючи споживання на 4–7%.

Система круїз-контролю може застосовуватись як на автомобілях з механічною трансмісією, так і на моделях з автоматом.

4.1 Переваги DACC перед стандартними системами ACC включають:

- Точніше та ефективніше керування автомобілем на дорозі, завдяки використанню цифрових датчиків та алгоритмів обробки даних.

-Швидша реакція на зміни дорожньої обстановки та навколишнього середовища завдяки більш швидкій обробці даних.

-Точне налаштування швидкості автомобіля та дистанції до попереднього автомобіля завдяки більш точному визначенню положення об'єктів на дорозі.

-Покращена безпека на дорозі завдяки більш точному та ефективному керуванню автомобілем на дорозі.

4.2 Винятки у використанні та непередбачені ситуації

Круїз-контроль не позбавляє автомобіліста необхідності контролю за дорожньою ситуацією. Більше того, в умовах неможливості підтримки постійної швидкості через щільний або рваний трафік його експлуатація практично повністю виключена.

В інструкціях з експлуатації до автомобілів прямим текстом говориться, що включати круїз-контроль не можна:

-При надто щільному дорожньому потоці.

-На аварійних ділянках доріг.

-На дорогах із поганим зчепленням.

-За будь-яких складних дорожніх умов.

-При недостатній видимості (вночі, під час дощу, снігопаду, туману).

-На звивистих дорогах.

-На з'їздах та під'їзних шляхах.

DACC зазвичай працює у поєднанні з іншими системами безпеки, такими як автоматичне гальмування та системи попередження про зіткнення. Якщо система визначає, що зіткнення є неминучим, вона може активувати аварійне гальмування, щоб зменшити швидкість і максимально знизити наслідки зіткнення.

5 Алгоритми

5.1 Розрахунок відстані до об'єктів

Головним алгоритмом можна назвати - розрахунку відстані до об'єктів під час використання адаптивного круїз-контролю можуть відрізнятися залежно від конкретної реалізації. Але в загальному випадку для розрахунку відстані між двома об'єктами в просторі можна використовувати формулу дистанції між двома точками.

Для розрахунку дистанції між двома точками у тривимірному просторі можна використовувати формулу:

$$d = \sqrt{(x_2 - x_{1)}{}^2 + (y_2 - y_{1)}{}^2 + (z_2 - z_{1)}{}^2} \quad (1.1)$$

де:

d - відстань між точками

x1, y1, z1 – координати першої точки

x2, y2, z2 - координати другої точки

У разі адаптивного круїз-контролю, одна з точок відповідає автомобілю, а інша - об'єкту, що знаходиться попереду автомобіля (наприклад, інший автомобіль чи перешкода на дорозі). За допомогою датчиків, встановлених на автомобілі, вимірюються координати об'єкта у просторі, і за цими даними розраховується відстань до нього.

5.2 Алгоритм розрахунку відстані до перешкоди

Формула розрахунку відстані до перешкоди на основі часу до зіткнення (Time-to-Collision, TTC) використовується в системах попередження про зіткнення та автоматичне гальмування, включаючи DACC.

Вона ґрунтується на оцінці часу, необхідного автомобілю для зіткнення з перешкодою, якщо він продовжить рух із поточною швидкістю та напрямком. Формула TTC обчислює відстань до перешкоди на основі різниці між поточною відстанню та швидкістю наближення.

Формально формула TTC може бути записана наступним чином:

$$TTC = \frac{D}{V} \quad (1.2)$$

де:

TTC – час до зіткнення

D – поточна відстань до перешкоди

V – швидкість наближення до перешкоди

У системах DACC TTC використовується для визначення критичних ситуацій, коли автоматичне гальмування має бути активоване, щоб уникнути зіткнення. Коли система виявляє, що TTC зменшується до певного порогового значення, вона автоматично застосовує гальма для запобігання зіткненню.

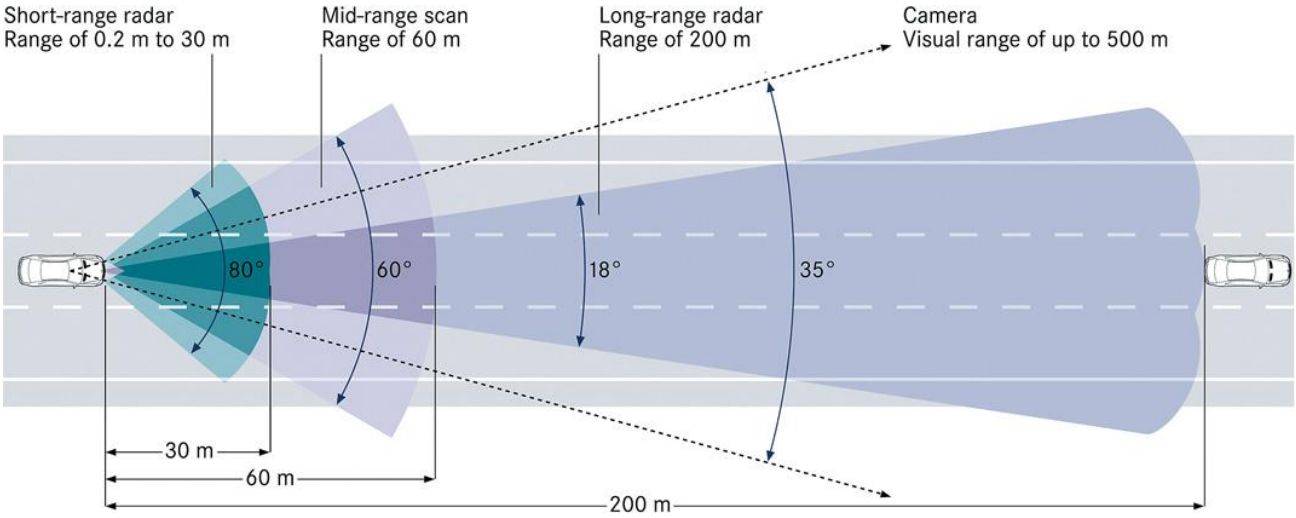

Рисунок 3 «Приклад роботи датчиків у адаптивному круїз контролі»

5.3 Формула для визначення оптимальної швидкості

Формула для визначення оптимальної швидкості з урахуванням відстані до перешкоди DACC може бути виражена наступним чином:

$$V_{opt} = \sqrt{(2 * a_{max} * d_c)} \quad (1.3)$$

де:

V_{opt} – оптимальна швидкість

a_{max} - максимальне прискорення автомобіля

d_c - відстань до перешкоди

Формула заснована на припущенні, що автомобіль може досягти максимального прискорення і потім уповільнити швидкість, необхідну для безпечного подолання перешкоди. Оптимальна швидкість розраховується таким чином, щоб мінімізувати час до наближення до перешкоди та забезпечити безпечну зупинку автомобіля перед перешкодою.

Ця формула використовується у системах автоматичного гальмування та адаптивного круїз-контролю для визначення оптимальної швидкості автомобіля з урахуванням відстані до найближчої перешкоди.

5.4 Формула розрахунку оптимальної швидкості необхідного часу до прибуття

Формула розрахунку оптимальної швидкості на основі необхідного часу до прибуття (Time-to-Arrival, TTA) використовується в системах автоматичного керування транспортними засобами для визначення оптимальної швидкості, необхідної для досягнення заданого місця призначення в заданий час при врахуванні поточної швидкості та дистанції до точки призначення.

Формула виглядає так:

$$\mathrm{V_{opt}} = \frac{(\mathrm{D}-\mathrm{D_{cur}})}{\mathrm{t_{arr}}} \qquad (1.4)$$

де:

V_{opt}- оптимальна швидкість, м/с

D - відстань до місця призначення, м

D_{cur}- поточна відстань до місця призначення, м

t_{arr} – необхідний час до прибуття, секунди

Таким чином, формула враховує відстань, що залишилася, і необхідний час до досягнення точки призначення, щоб визначити оптимальну швидкість, з якою потрібно рухатися, щоб прибути вчасно. Ця формула часто використовується в системах навігації та автоматичного керування транспортними засобами, таких як автопілоти та системи керування швидкістю.

6. Вай-фай модуль

Wi-Fi модуль у DACC– це компонент, який дозволяє автомобілю отримувати та надсилати дані через бездротову мережу Wi-Fi.

Модуль використовується для зв'язку з іншими пристроями в автомобілі та зовнішніми джерелами даних, такими як сервери трафіку, карти та інші онлайн-ресурси. Це дозволяє автомобілю отримувати інформацію про поточну дорожню обстановку, пробки, погодні умови, стан дорожніх знаків та багато іншого, також може використовуватися для оновлення програмного забезпечення DACC та інших систем в автомобілі, що дозволяє виробникам автомобілів оновлювати та покращувати системи дистанційно, не потребуючи фізичної заміни компонентів.

Одним із прикладів використання Wi-Fi модуля в DACC є система оновлення карт, яка дозволяє автомобілю отримувати оновлення карт у режимі реального часу, що дозволяє водієві швидко адаптуватися до змін на дорозі.

6.1 Загрози Wi-Fi модулів

Як і будь-яка система, вай-фай модуль може стати об'єктом атак із боку зловмисників. Розглянемо деякі з можливих способів злому вай-фай модуля:

-Перехоплення трафіку. Зловмисник може перехоплювати трафік, що передається через вай-фай модуль, та отримувати доступ до конфіденційних даних.

-Атака на пароль. Зловмисник може використовувати методи перебору або підбору пароля для отримання доступу до вай-фай модуля.

-Вразливості у прошивці. У деяких випадках вай-фай модуль може містити вразливість у прошивці, які можуть бути використані зловмисником для отримання несанкціонованого доступу.

-Атака на систему захисту. Зловмисник може спробувати обійти систему захисту, що використовується у вай-фай модулі, наприклад, методом перехоплення та аналізу мережного трафіку.

Через вай-фай модуль у DACC можна спробувати отримати доступ і вкрасти різні типи даних.

Ось деякі приклади даних, які можуть бути скомпрометовані, якщо вай-фай модуль DACC не захищений належним чином:

-Користувацькі дані: Це включає особисту інформацію власника автомобіля, таку як імена, адреси, номери телефонів, адреси електронної пошти та фінансові дані. Витік цих даних може призвести до крадіжки особистої інформації та потенційного фінансового шахрайства.

-Дані автомобіля: Вай-фай модуль DACC може містити дані про стан автомобіля, включно з технічною інформацією, сервісними записами, GPS-координатами та історією поїздок. Витік цих даних може надати зловмисникам інформацію про місцезнаходження, приватні маршрути і навіть можливість віддаленого втручання в роботу автомобіля.

-Системні дані: Вай-фай модуль DACC може містити конфіденційну інформацію про систему та програмне забезпечення автомобіля. Це може включати коди доступу до системи, сертифікати безпеки та інші конфіденційні дані. Витік таких даних може дозволити зловмисникам обійти систему безпеки та отримати несанкціонований доступ до автомобіля.

-Мережеві дані: Якщо вай-фай модуль DACC під'єднано до зовнішніх мереж, як-от Інтернет, витік даних може містити мережеву активність, IP-адреси та іншу інформацію про під'єднання. Це може бути використано для проведення атак на мережу, вторгнення в інші пристрої або отримання додаткової інформації про власника автомобіля.

6.2 Система захисту Wi-Fi модуля в DACC

Захист інформації від витоку параметричним (електромагнітним) каналом є важливим завданням у сфері інформаційної безпеки.

Параметричний канал - це канал зв'язку, який використовує незвичайні канали передачі інформації, такі як зміна електромагнітних характеристик системи, наприклад електричної напруги або струму, для передачі інформації.

Захист даних вай-фай модуля DACC від електромагнітних перешкод здійснюється шляхом застосування екрануючих матеріалів та конструктивних рішень. Для запобігання витоку даних електромагнітним каналом використовуються такі методи:

У DACC можуть бути встановлені програми для моніторингу безпеки, які можуть визначати та запобігати спробам несанкціонованого доступу до системи. Ці програми можуть також аналізувати передачу даних та виявляти потенційні загрози безпеці.

-Екранування корпусу модуля: корпус вай-фай модуля виготовляється з матеріалів, що мають високу електромагнітну екрануючу здатність, таких як алюміній, мідь, нікель. Це дозволяє запобігти проникненню електромагнітних сигналів усередину корпусу та забезпечує захист даних.

-Використання фільтрів: для захисту від електромагнітних перешкод, які можуть впливати на роботу вай-фай модуля, застосовуються спеціальні фільтри. Вони дозволяють придушувати небажані сигнали та захищають від перешкод.

-Тестування на витоку: вай-фай модуль проходить спеціальне тестування на витік даних електромагнітним каналом. Це дозволяє виявляти та усувати можливі вразливості у системі захисту.

-Періодичне оновлення ПЗ: важливим фактором захисту даних вай-фай модуля є періодичне оновлення програмного забезпечення. Це дозволяє усувати виявлені вразливості та забезпечувати більш високий рівень безпеки.

Крім того, для захисту Wi-Fi з'єднання можуть використовуватися алгоритми хешування для перевірки цілісності даних. Наприклад, протокол WPA2 використовує алгоритм HMAC-SHA1 для перевірки цілісності даних, що передаються.

-Резервне копіювання та відновлення: Регулярне створення резервних копій даних, що передаються через модуль Wi-Fi DACC, та наявність механізмів відновлення допомагають мінімізувати втрати даних у разі їх витоку або зміни. Резервні копії повинні зберігатися в безпечному місці та регулярно оновлюватись.

-Навчання та обізнаність користувачів: Важливо проводити навчання та підвищувати обізнаність користувачів, які взаємодіють із модулем Wi-Fi DACC. Це включає навчання за правилами безпечного використання Wi-Fi мереж, розпізнавання потенційних загроз та звітування про підозрілі активності.

-Шифрування даних: дані, що передаються між вай-фай модулем та іншими пристроями, шифруються за допомогою алгоритму AES. Це забезпечує конфіденційність інформації, що передається, і захищає її від перехоплення.

AES– це симетричний метод шифрування, який використовується для захисту передачі даних у різних додатках, включаючи Wi-Fi, Bluetooth та інші мережні технології.

AES був розроблений в 2001 році і він замінив старий стандарт шифрування DES (Data Encryption Standard) і став одним із найнадійніших і найпоширеніших методів шифрування.

Основний принцип роботи AES полягає у використанні ключа для перетворення вихідного тексту на шифрований вигляд, який може бути переданий по мережі. Розмір ключа може бути різним, але зазвичай використовуються ключі завдовжки 128, 192 чи 256 біт.

Перетворення виконується за допомогою декількох циклів, кожен з яких включає чотири етапи: заміну байтів, перемішування байтів, перемішування стовпців і перемішування рядків. Ці етапи повторюються багато разів, щоб отримати остаточний зашифрований текст.

Рисунок 4 – «Приклад роботи шифрувальної системи AES»

Однією з головних переваг AES є високий рівень безпеки. Шифрований текст, дуже важко розшифрувати без знання ключа. Крім того, AES є дуже ефективним методом шифрування, який може бути використаний в реальному часі на багатьох пристроях, включаючи мобільні пристрої та комп'ютери.

Система захисту Wi-Fi модуля в DACC може бути налаштована для визначення та запобігання спробам несанкціонованого доступу до системи. Наприклад, система може реєструвати всі спроби входу в систему та сповіщати адміністратора системи про будь-які підозрілі дії.

Також, автовиробники, оснащені DACC, зазвичай проводять внутрішні тести, щоб переконатися в ефективності захисту системи. Вони можуть використовувати різні методи, такі як пентестинг (тестування на проникнення), щоб перевірити вразливість та оцінити рівень безпеки.

6.3 Сертифікація безпеки та критерії захищеності

Зазвичай виробники проводять сертифікацію своїх продуктів відповідно до певних стандартів безпеки, таких як FIPS (Federal Information Processing Standard) або Common Criteria.

FIPS – це стандарт, встановлений урядом США, який визначає вимоги до захисту інформації та інформаційних систем. Відповідно до стандарту FIPS, для захисту конфіденційних даних необхідно використовувати алгоритми шифрування, такі як AES. Виробники можуть проводити тести та сертифікацію своїх систем, щоб переконатися, що вони відповідають вимогам стандарту.

Common Criteria – це міжнародний стандарт, який визначає вимоги до безпеки інформаційних технологій та продуктів. Виробники можуть також проводити сертифікацію своїх систем відповідно до цього стандарту.

Захищеність DACC (системи адаптивного круїз-контролю) оцінюється за рядом критеріїв, включаючи:

Стійкість до атак: оцінка стійкості DACC до різних атак, наприклад, до злому вай-фай модуля або впровадження шкідливого програмного забезпечення.

Реакція на непередбачені ситуації: здатність DACC адекватно реагувати на несподівані чи непередбачені ситуації на дорозі, наприклад, на швидку появу перешкоди чи зміну погодних умов.

Точність та ефективність: оцінка точності та ефективності системи, наприклад, наскільки точно DACC підтримує задану швидкість та безпечну відстань між машинами.

Надійність та безпека: оцінка надійності та безпеки DACC в екстремальних умовах, наприклад, при високих швидкостях або сильному гальмуванні.

Відповідність стандартам: перевірка відповідності DACC міжнародним стандартам безпеки та якості, наприклад, стандарту ISO 26262, який визначає вимоги щодо функціональної безпеки автомобілів.

Ступінь автоматизації: оцінка ступеня автоматизації DACC та здатності системи працювати без участі водія у різних умовах.

7. Приклади захисту інформації від витоку в різних сферах

Розглянемо кілька конкретних прикладів захисту інформації від витоку при зміні електромагнітних характеристик у різних сферах:

1 Інформаційна безпека комп'ютерних систем:

1.1 Застосування екранування у вигляді фарафаритових матеріалів для запобігання витоку даних через електромагнітні випромінювання з комп'ютерних компонентів.

1.2 Використання криптографічного шифрування для захисту даних під час їхньої передачі через мережу, щоб запобігти несанкціонованому доступу до інформації, навіть у разі перехоплення сигналу.

2 Бездротові комунікації та радіозв'язок:

2.1 Застосування шифрування даних під час передавання бездротовими каналами зв'язку, як-от Wi-Fi або Bluetooth, щоб забезпечити конфіденційність переданої інформації.

2.2 Використання фільтрів і підсилювачів сигналу для зменшення впливу електромагнітних перешкод на якість зв'язку та запобігання витоку даних.

3 Системи управління доступом і безпеки:

3.1 Застосування методів фізичної ізоляції та екранування для захисту електромагнітних характеристик системи контролю доступу, щоб запобігти несанкціонованому доступу та витоку інформації про доступ.

3.2 Використання протоколів шифрування та аутентифікації для забезпечення безпечного передавання даних між компонентами системи безпеки.

4 Медичні пристрої та системи:

4.1 Застосування екранування та фільтрації електромагнітних сигналів у медичних пристроях для запобігання впливу зовнішніх перешкод і захисту конфіденційності медичної інформації.

4.2 Використання методів криптографії та протоколів безпеки під час передавання даних між медичними пристроями, щоб запобігти витоку чутливої інформації про пацієнтів.

Як мі бачимо у кожній із цих сфер застосовуються відповідні технології та методи для захисту даних від витоку при зміні електромагнітних характеристик. Однак, конкретні рішення і методи можуть відрізнятися залежно від конкретних вимог. У багатьох з них використовуються одні й ті ж самі методи, це використовується для поліпшення захисту системи.

8 Захист інформації у автопілотах

Компанії використовують кілька методів для захисту вай-фай модуля у своїх автомобілях:

1. Шифрування: використовується шифрування WPA2 для захисту мережі. WPA2 є найбезпечнішим протоколом шифрування Wi-Fi, який є на сьогоднішній день. Цей протокол використовує алгоритм AES який ми обговорювали раніше. Це робить мережу практично незламною.

2. Криптографічний ключ: Кожен автомобіль має унікальний криптографічний ключ, який використовується для захисту зв'язку між автомобілем та сервером. Цей ключ створюється при виробництві автомобіля та використовується для шифрування та розшифрування даних, що передаються через мережу.

Безпека ПЗ: також приділяє велику увагу безпеці ПЗ своїх автомобілів. Вони використовують криптографічні алгоритми та інші методи захисту, щоб захистити свої системи від злому та зловживання.

Оновлення програмного забезпечення: регулярно випускається оновлення програмного забезпечення для своїх автомобілів, які виправляють вразливості та покращують захист. Ці оновлення автоматично завантажуються на автомобіль через Wi-Fi, що допомагає підтримувати його захищеним.

Крім того компанії рекомендують своїм користувачам використовувати лише офіційні Wi-Fi мережі, а не відкриті мережі, щоб зменшити ризик злому. Також важливо використовувати пароль для захисту своєї Wi-Fi мережі та змінювати його регулярно.

9. Перспективи розвитку

Autopilot – це система автоматичного керування автомобілем. Вона була введена в 2015 році і швидко стала однією з найвідоміших систем DACC на ринку.

Основна функція Autopilot – це можливість автоматичного керування автомобілем на автострадах та інших типах доріг. Система використовує безліч

датчиків та камер, щоб визначати відстань до інших автомобілів та запобігати зіткненням. Вона також може стежити за дорожніми знаками та смугами руху, щоб підтримувати безпечну швидкість та рух автомобіля.

Крім основної функції автоматичного керування має інші функції, такі як Summon, що дозволяє автомобілю самостійно переміщатися на короткі відстані, та Autosteer, яка дозволяє автомобілю автоматично перебудовуватися між смугами руху.

Автопілот постійно оновлюється та покращується. Компанії випускають нові версії програмного забезпечення, щоб покращити функціональність та безпеку системи. Наприклад, в 2018 році була випущена версія Autopilot 2.5, яка мала більш точні датчики і розширену функціональність, а в 2020 році була випущена версія Full Self-Driving, яка включає ще більш передові функції, такі як автоматичне перебудова на з'їздах і використання світлофорів .

Перспективи розвитку DACC включають:

1. Поліпшення функцій автоматичного гальмування та прискорення - майбутні версії DACC можуть використовувати більш точні датчики та більш складні алгоритми машинного навчання для покращення функцій автоматичного гальмування та прискорення.

2. Покрашення системи розпізнавання об'єктів – розвиток технологій та алгоритмів розпізнавання об'єктів може допомогти збільшити точність та ефективність системи DACC. Це може включати покращення розпізнавання об'єктів у поганих погодних умовах та у темряві.

3. Збільшення швидкості і точності системи - майбутні версії DACC можуть працювати швидше і точніше, що дозволить автомобілям швидше реагувати на умови дорожнього руху, що змінюються, і поліпшити загальну продуктивність системи.

4. Збільшення дальності виявлення - майбутні версії DACC можуть мати більш дальні датчики, що дозволить автомобілям виявляти об'єкти та перешкоди на більшій відстані та з більш високою точністю.

Додаткові функції - майбутні версії DACC можуть включати додаткові функції, такі як автоматичне паркування та автоматична зміна смуги.

В цілому, DACC - це технологія, яка продовжуватиме розвиватися та покращуватись, щоб забезпечити більш безпечне, зручне та ефективне водіння автомобілів у майбутньому.

Висновок

Захист інформації від витоку за зміни електромагнітних характеристик є важливим аспектом забезпечення інформаційної безпеки. Для цього застосовуються різні методи та заходи, включаючи:

1. Шифрування даних: Використання криптографічних алгоритмів і протоколів шифрування забезпечує конфіденційність і цілісність даних, що передаються, захищаючи їх від несанкціонованого доступу або зміни.

2. Електромагнітне екранування: Застосування екранувальних матеріалів та дизайну, які мінімізують електромагнітні випромінювання або перешкоди, допомагає запобігти несанкціонованому доступу до електромагнітних характеристик системи.

3. Фізична безпека: Обмеження фізичного доступу до системи та пристроїв допомагає запобігти несанкціонованій зміні електромагнітних характеристик. Це може включати фізичні бар'єри, контроль доступу, відеоспостереження та інші методи фізичної безпеки.

4. Моніторинг та виявлення інцидентів: Реалізація системи моніторингу та виявлення допомагає виявляти підозрілі активності, включаючи спроби зміни електромагнітних характеристик системи. Це може включати системи моніторингу мережного трафіку, інтегровані системи безпеки та аналіз поведінки користувачів.

5. Навчання та поінформованість співробітників: Навчання персоналу в галузі інформаційної безпеки та підвищення їх поінформованості про можливі загрози дозволяє запобігти несанкціонованим змінам електромагнітних характеристик. Співробітники повинні бути ознайомлені з політиками безпеки, процедурами обробки даних та регулярно проходити навчання з безпеки.

Щодо DACC, який є комплексною системою з функціями автоматичного гальмування та попередження про зіткнення, захист даних від витоку та змін має ключове значення. Впровадження відповідних методів і протоколів захисту даних у модулі Wi-Fi DACC відіграє важливу роль у запобіганні несанкціонованому доступу та захисту конфіденційності даних користувача.

Деякі основні аспекти захисту даних у модулі Wi-Fi DACC включають:

1. Шифрування даних: Використання криптографічних алгоритмів забезпечує конфіденційність даних, що передаються за Wi-Fi, і захист від прослуховування.

2. Аутентифікація та ідентифікація: Застосування механізмів аутентифікації та ідентифікації дозволяє перевіряти легітимність учасників комунікації через Wi-Fi та запобігати несанкціонованому підключенню або заміні даних. Це може включати використання протоколів автентифікації, паролів чи сертифікатів.

3. Фільтрування та контроль доступу: Встановлення механізмів фільтрації та контролю доступу визначає, які пристрої чи користувачі мають дозвіл на підключення до модуля Wi-Fi DACC. Це забезпечує запобігання несанкціонованому доступу та захист від вторгнень.

4. Виявлення та запобігання атакам: Реалізація систем виявлення та запобігання атакам дозволяє реагувати на підозрілі дії або спроби злому Wi-Fi модуля. Це може включати моніторинг мережного трафіку, виявлення аномалій або використання інтелектуальних алгоритмів виявлення підозрілих активностей.

5. Регулярні оновлення та патчі: Регулярне оновлення програмного забезпечення та встановлення патчів безпеки для модуля Wi-Fi DACC допомагають виправляти вразливості та забезпечувати захист від відомих загроз.

Інтеграція цих заходів безпеки та постійне оновлення системи захисту даних у модулі Wi-Fi DACC дозволяють мінімізувати ризик витоку інформації. Однак важливо розуміти, що захист даних є безперервним процесом, що потребує постійного моніторингу, оцінки ризиків та вжиття відповідних заходів безпеки.

Загалом захист даних від витоку при зміні електромагнітних характеристик потребує комплексного підходу, що включає технічні, фізичні та організаційні заходи безпеки. Ефективний захист ґрунтується на постійному моніторингу та оновленні системи безпеки, а також на обізнаності та активній участі всіх учасників процесу.

Список використаних джерел

1. Вікіпедія - Адаптивний круїз-контроль [Ел.ресурс]. - Режим доступу: https://uk.wikipedia.org/wiki/Адаптивний_круїз-контроль.
2. Робокрафт - Адаптивний круїз-контроль [Ел.ресурс]. - Режим доступу: https://auto.ria.com/uk/news/articles/253393/adaptivnyj-kruiz-kontrol-chto-on-umeet-i-stoit-li-pereplaty.html.
3. Autonews - Адаптивний круїз-контроль [Ел.ресурс] https://www.autonews.ru/news/624bede59a79473e81395838
4. ITC Community - Кібер безпека [Ел.ресурс] https://itc.ua/news/gosspetssvyazi-obnarodoval-otchet-tsentra-kiberzashhity-za-2-kvartal-2022-goda-aktivnost-hakerskih-grupp-v-ukraine-sushhestvenno-vozrosla/