Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Шифрування даних для захисту автономних транспортних засобів від кібератак"

Виконав: студент
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Демчишин Максим Миколайович
підпис (прізвище та ініціали)

Керівник Оробчук О. Р.
підпис (прізвище та ініціали)

Нормоконтроль Тимощук Д. І.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Демчишину Максимові Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Шифрування даних для захисту автономних транспортних засобів від кібератак

Керівник роботи Оробчук Олександра Романівна, доктор філософії., старший викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «20» 11 2024 року № 4/7-1112

2. Термін подання студентом завершеної роботи 20.12.2024

3. Вихідні дані до роботи наукові публікації щодо шифрування даних для захисту від кібератак, інформаційної безпеки автономних транспортних засобів

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз предметної області. 1.1. Поняття автономного транспортного засобу. 1.2. Інформаційна безпека автономних транспортних засобів. 1.3. Автономні транспортні засоби як частина ІТС. 1.4. Вектори кібератак на автономні транспортні засоби. 1.5. Протоколи передачі та шифрування даних в АТЗ. 2. Криптографічні алгоритми в АТЗ. 2.1. Криптографічні алгоритми протоколу Bluetooth. 2.2. RSA та ECDSA. 2.3. Advanced Encryption Protocol. 2.4. Режими роботи AES. 3. Експериментальне дослідження. 3.1. Обгрунтування вибору інструментів експериментального дослідження. 3.2. Методика експерименту. 3.3. Аналіз результатів. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титульний слайд. 2. Вступ та актуальність. 3. Мета та завдання.
4. Режими шифрування AES. 5. Методика експерименту.
6. Результати (час шифрування). 7. Результати (споживання пам'яті).
8. Результати (завантаженість процесора). 9. Висновки.
10. Подальші напрями дослідження.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 23.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	23.09 – 25.09	Виконано
2.	Аналіз джерел та огляд літератури	26.09 – 11.10	Виконано
3.	Написання 1-го розділу	14.10 – 25.10	Виконано
4.	Розробка методики дослідження	28.10 – 15.11	Виконано
5.	Написання 2-го розділу	18.11 – 20.11	Виконано
6.	Проведення експериментальних досліджень	21.11 – 25.11	Виконано
7.	Написання 3-го розділу	26.11 – 29.11	Виконано
8.	Опрацювання питань охорони праці	02.12 – 03.12	Виконано
9.	Опрацювання питань безпеки в надзвичайних ситуаціях	04.10 – 05.12	Виконано
10.	Написання 4-го розділу	06.12 – 10.12	Виконано
11.	Оформлення пояснювальної записки	10.12 – 12.12	Виконано
12.	Нормоконтроль	12.12 – 13.12	Виконано
13.	Перевірка на плагіат	13.12 – 16.12	Виконано
14.	Попередній захист кваліфікаційної роботи	17.12 – 20.12	Виконано
15.	Захист кваліфікаційної роботи	26.12.2024	

Студент _____ Демчишин М. М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Оробчук О. Р.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Шифрування даних для захисту автономних транспортних засобів від кібератак // ОР «Магістр» // Демчишин Максим Миколайович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2024 // С. 75, рис. – 9, табл. – 3, кресл. – 10, додат. – 1.

Ключові слова: автономні транспортні засоби, AES, ITS, криптографія, симетричне шифрування.

У кваліфікаційній роботі досліджено вплив різних режимів шифрування AES на продуктивність систем з обмеженими ресурсами. Розглянуто переваги та недоліки режимі шифрування AES. Проведено експерименти з оцінки часу шифрування, споживання пам'яті та завантаження процесора для режимів ECB, CBC, CFB, OFB та CTR при різних розмірах чанків. Результати візуалізовано діаграмами з абсолютними та нормалізованими значеннями. На основі нормалізованих даних проведено порівняльний аналіз ефективності режимів.

ANNOTATION

Title // Thesis of educational level "Master"// Maksym Demchyshyn // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-61 // Ternopil, 2024 // P. 75, figs. 9, tables 3, drawings 10, annexes 1.

Keywords: autonomous vehicles, AES, ITS, cryptography, symmetric encryption.

The thesis investigates the impact of different AES encryption modes on the performance of systems with limited resources. The advantages and disadvantages of AES encryption modes were examined. Experiments have been conducted to evaluate the encryption time, memory consumption, and CPU load for ECB, CBC, CFB, OFB, and CTR modes with different chunk sizes. The results are visualized in diagrams with absolute and normalized values. Based on the normalized data, a comparative analysis of the efficiency of the modes was carried out.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АТЗ	—	Автономний транспортний засіб
ІТС	—	Інтелектуальна транспортна система
MTAI	—	Міжнародне товариство автомобільних інженерів
AES	—	Advanced Encryption Protocol
DDoS	—	Distributed Denial of Service
DES	—	Data Encryption Standard
ECDSA	—	Elliptic Curve Digital Signature Algorithm
IoT	—	Internet of Things
MITM	—	Man-in-the-Middle
SSL	—	Secure Sockets Layer
V2X	—	Vehicle-to-Everything
TLS	—	Transport Layer Security

ВСТУП

Автономні транспортні засоби (АТЗ) стрімко поширюються станом на сьогодні, обіцяючи докорінно змінити підходи до організації транспортної системи. Вони покладаються на складні системи датчиків, зв'язку та обробки даних для безпечної та ефективної навігації. Однак, ця складна цифрова інфраструктура також робить АТЗ вразливими до кібератак, які можуть призвести до серйозних наслідків, включаючи втрату контролю над транспортним засобом, викрадення даних та навіть загрозу життю пасажирів.

З огляду на зростаючу кількість кіберзагроз, забезпечення кібербезпеки АТЗ є критично важливим завданням. Одним із ключових методів захисту даних в АТЗ є шифрування, яке перетворює інформацію в нечитабельний формат, що унеможливлює її використання зловмисниками. Серед різноманітних алгоритмів шифрування, симетричний блочний шифр AES (Advanced Encryption Standard) отримав широке визнання завдяки своїй високій надійності та ефективності.

Проте, застосування AES в умовах обмежених обчислювальних ресурсів, характерних для вбудованих систем АТЗ, ставить певні виклики. Різні реалізації AES можуть мати різну продуктивність та споживання ресурсів, що необхідно враховувати при їх виборі для конкретного застосування. Особливо важливим є дослідження впливу обсягу даних, що шифруються, на продуктивність різних реалізацій AES в умовах обмежених обчислювальних потужностей [1,2].

Метою даної роботи є дослідження ефективності використання обмежених обчислювальних ресурсів автономного транспортного засобу різними режимами роботи криптографічного шифру AES.

Щоб досягнути мети, необхідно виконати наступні задачі:

– дослідити та проаналізувати джерела предметної області дослідження;

– реалізувати програмний скрипт для проведення експерименту з використанням зовнішніх інструментів;

– провести дослідження ефективності використання обчислювальних ресурсів різними режимами роботи криптографічного шифру AES;

– визначити перспективні напрямки подальшого дослідження шифрування в системах АТЗ.

Об’єкт дослідження – режими роботи криптографічного шифру AES.

Предмет дослідження – використання обчислювальних ресурсів криптографічним шифром AES.

У кваліфікаційній роботі використовувалися такі методи дослідження: експеримент та вимірювання, аналіз та синтез.

Науковою новизною роботи є дослідження використання обмежених обчислювальних ресурсів шифром AES в ізольованому середовищі.

Практичною цінністю одержаних результатів є можливість використання дослідження для оптимального вибору режиму роботи AES на АТЗ з обмеженими обчислювальними потужностями.

Основні положення і результати роботи були представлені на XII науковотехнічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18-19 грудня 2024 р.).

РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Поняття автономного транспортного засобу

Автономні транспортні засоби (АТЗ) – це транспортні засоби, здатні здійснювати навігацію і приймати рішення незалежно від втручання людини, є революційним досягненням у транспортних технологіях. Ці транспортні засоби функціонують завдяки синтезу низки складних технологій, включаючи датчики, камери, GPS, радари, системи виявлення і визначення дальності за світловим зображенням та багато інших (див. рис. 1.1). Ці компоненти працюють разом, щоб точно сприймати навколишнє середовище транспортного засобу, забезпечуючи здатність приймати оптимальні рішення в режимі реального часу.

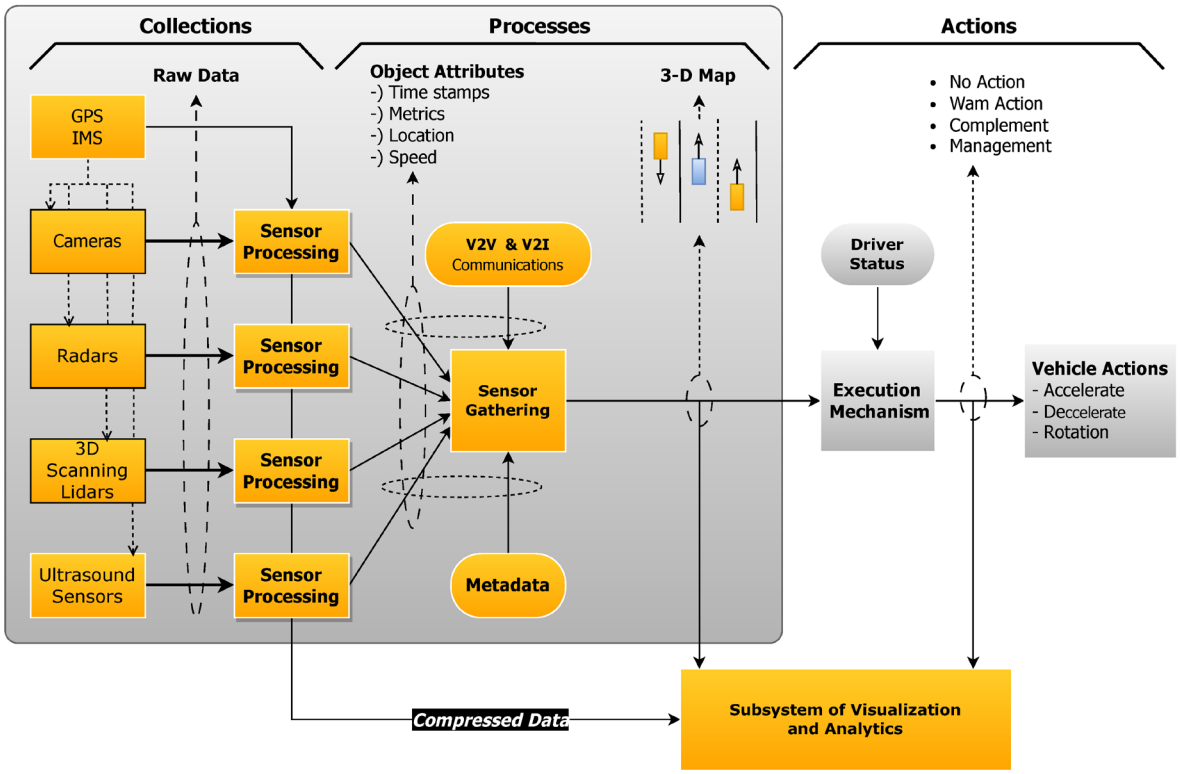

Рисунок 1.1 – Схема функціональних систем АТЗ

В основі функціональності АТЗ лежить здатність полегшувати взаємодію між транспортними засобами та з критично важливою дорожньою інфраструктурою -

характеристика, яка, будучи ключовою для їхньої ефективності, також робить їх вразливими до кіберзагроз. Потенційне проникнення в системи АТЗ становить серйозну загрозу, оскільки відкриває можливості для крадіжки особистої інформації або зараження шкідливим програмним забезпечення, яке може поставити під загрозу безпеку транспортного засобу.

Міжнародне товариство автомобільних інженерів (MTAI) класифікує автоматизацію транспортних засобів на шість рівнів - від повного керування людиною до повної автоматизації. Транспортні засоби перших трьох рівнів (рівні від 0 до 2) вимагають від водія виконання основних завдань водіння, тоді як автоматизовані системи водіння останніх трьох рівнів (рівні від 3 до 5) можуть виконувати основні завдання водіння з обмеженою участю або без участі водія. Кожен рівень окремо можна характеризувати наступним чином:

– рівень 0, без автоматизації: транспортний засіб не має жодної автоматизації, і водій несе відповідальність за виконання всіх завдань;\

– рівень 1, допомога водієві: транспортним засобом керує переважно водій з деякими доступними автоматизованими функціями, такими як адаптивний круїз;

– рівень 2, часткова автоматизація: у транспортному засобі встановлено кілька комбінованих автоматизованих функцій, але водій повинен виконувати всі завдання і стежити за навколишнім середовищем;

– рівень 3, умовна автоматизація: транспортний засіб може працювати з автоматизованою системою водіння в умовах низькошвидкісного щільного руху на автомагістралі. Водієві не потрібно спостерігати за навколишнім середовищем, але він повинен бути готовим замінити систему в будь-який момент;

– рівень 4, високий рівень автоматизації: транспортний засіб може виконувати всі завдання за певних умов (наприклад, у географічно огородженому місці), і водієві не потрібно контролювати транспортний засіб взагалі;

– рівень 5, повна автоматизація: транспортний засіб може виконувати всі завдання за будь-яких умов, і водієві не потрібно контролювати транспортний засіб.

Технології автоматизації на різних рівнях можуть по-різному змінити транспортні системи і за рахунок цьому створювати абсолютно різні стани інформаційної безпеки АТЗ.

1.2 Інформаційна безпека автономних транспортних засобів

Функціонування автономних транспортних засобів нерозривно пов'язане з обробкою значних обсягів даних, що робить інформаційну безпеку ключовим фактором їхньої надійності, а основними її складовими є забезпечення трьох основних принципів:

– конфіденційність: цей принцип підкреслює важливість запобігання несанкціонованому доступу до даних. Дотримання конфіденційності має вирішальне значення для запобігання потенційному привласненню або використанню конфіденційної інформації, яка в разі неправильного поводження може поставити під загрозу безпечну та надійну роботу аудіо-відео систем;

– цілісність: цей принцип забезпечує автентичність, точність і узгодженість даних протягом усього їхнього життєвого циклу. Це передбачає не лише виявлення несанкціонованого доступу до даних, але й запобігання несанкціонованій модифікації даних. Збереження цілісності даних має вирішальне значення для підтримки надійності системи та її здатності приймати правильні рішення;

– доступність: ефективність системи залежить від постійної доступності її функціональних можливостей та здатності працювати відповідно до очікувань. Для прикладу, у контексті безпілотних літальних апаратів будь-який компроміс у доступності може мати негайні та серйозні наслідки для безпеки.

Окрім цих фундаментальних концепцій, безпека інформаційних систем може також залежати від додаткових характеристик, від конкретних обставин і застосування, включаючи автентичність, логування, неможливість спростування і надійність. Ці характеристики, якщо їх розглядати разом, допомагають створити інтегровану і всеосяжну систему безпеки для автономних транспортних засобів, яка

допомагає захистити такі транспортні засоби від широкого спектру можливих загроз.

Порушення безпеки сенсорних систем в АТЗ викликають значне занепокоєння через те, що вони можуть поставити під загрозу безпеку транспортного засобу та благополуччя його пасажирів. Автомобілі використовують складний набір датчиків, включаючи камери, світлові сенсори і радари, але не обмежуючись ними. Ці датчики необхідні для інтерпретації навколишнього середовища і полегшення процесів прийняття важливих рішень. Порушення роботи цих сенсорних систем може призвести до викривленого розуміння навколишнього середовища, що, в свою чергу, може підвищити ризик нещасних випадків і загроз безпеці.

Історично уже існують різні приклади, що підкреслювали потенціал таких атак на аудіо-візуальні датчики. До них відносяться точні атаки підміни, здатні обдурити датчики, змусивши їх визнати неіснуючі перешкоди, і атаки глушінням, які ефективно переривають здатність датчиків точно виявляти об'єкти. Небезпечним є те, що обладнання, необхідне для здійснення цих атак, часто може бути простим і легкодоступним, наприклад, лазерна указка або радіопередавач, що збільшує множину потенційних зловмисників.

Оскільки аудіо- та відеотехніка стає все більш звичним явищем у нашому транспортному контексті, важливість усунення вразливостей безпеки аудіо- та відеосенсорів стає все більш очевидною. Це підкріплює необхідність розробки та впровадження суворих заходів безпеки, пристосованих для виявлення та нейтралізації атак на аудіо- та відеодатчики. Поряд із цими заходами безпеки, дуже важливо підвищувати обізнаність громадськості про потенційні ризики, пов'язані з атаками на ці датчики.

Повертаючись до контексту атак на датчики, не можна не згадати також атаки, метою яких є перехоплення інформації з сенсорі з метою отримання приватної інформації або модифікації чи підміни таких даних. Саме тому шифрування даних, в тому числі з сенсорів, є невід'ємною частиною забезпечення безпеки автономних транспортних засобів.

Проте, важливо усвідомлювати, що сучасні автономні транспортні засоби вже не є ізольованими системами. Вони все більше інтегруються в складну екосистему, що складається з інших транспортних засобів, дорожньої інфраструктури, хмарних сервісів та різноманітних пристроїв, формуючи тим самим складну мережу, відому як Інтелектуальну Транспортну Систему (ITC). Ця інтеграція відкриває нові можливості для оптимізації руху, покращення безпеки та надання додаткових сервісів, але водночас створює нові виклики для кібербезпеки, які потребують окремого розгляду в контексті концепції ITC.

1.3 Автономні транспортні засоби як частина ITC

Інтернет речей (IoT) є наслідком об’єднання ряду системних функціоналів, таких як: аналітика в реальному часі, машинне навчання, вбудовані системи, бездротові мережі, системи управління, автоматизація будинків і будівель. З точки зору споживача, IoT є синонімом продуктів, що відносяться до концепції «розумного будинку», «розумної охорони здоров'я», «розумного міста» тощо. Багато з цих сфер мають схожі характеристики і стикаються зі схожими проблемами. Запозичення технологій між підгалузями Інтернету речей є поширеним явищем, але його потрібно добре обміркувати і дослідити на практиці. Незважаючи на схожість, навіть в межах однієї галузі вимоги до дальності зв'язку та швидкості передачі даних, роботи в режимі реального часу, надійності та безпеки відрізняються. Інтелектуальні транспортні системи (ITC), як підгалузь розумного міста, характеризуються багатьма рисами Інтернету речей. Їх відмінними рисами є: жорсткі часові вимоги, динаміка і великі обсяги даних. Однією з головних характерних властивостей ITC є високі вимоги до кібербезпеки. Можна назвати такі напрямки застосування ITC: транспортна безпека, ефективність дорожнього руху та інформаційно-розважальні системи. Застосування ITC для безпеки дорожнього руху мають дуже високі вимоги до кібербезпеки в поєднанні з жорсткими обмеженнями в реальному часі. Хоча додатки для підвищення ефективності дорожнього руху та інформаційно-розважальні додатки безпосередньо не пов'язані

з фізичною безпекою учасників дорожнього руху, вимоги до кібербезпеки залишаються високими, оскільки порушення в будь-якому з них може вплинути на ефективність всієї ІТС. Наприклад, перевантаження каналу зв'язку для інформаційно-розважальних додатків може перешкоджати нормальній роботі додатків безпеки, що може бути критично важливим .

Транспортні спеціальні мережі (VANET) є ключовим компонентом усіх сучасних розробок для ІТС. Вузли (транспортні засоби) в VANET обмінюються короткими повідомленнями, які називаються маячками, протягом певних періодів часу. Маячки містять важливу інформацію про транспортні засоби та навколишнє середовище, наприклад, напрямок, прискорення, швидкість, стан дороги, погодні умови тощо. Підключення транспортних засобів до бездротового зв'язку в один стрибок ставить багато завдань, таких як аутентифікація нових транспортних засобів, необхідність захисту ідентичності користувача, переривання, забезпечення багатострибкового зв'язку, висока неоднорідність (в залежності від того, чи автомобілі перевантажені у великому місті або в приміській зоні). Значна частина досліджень з кібербезпеки ІТС зосереджена на мережевій безпеці .

ІТС можна розглядати як підтип IoT, тому її можна розробляти з використанням подібних підходів та архітектур. На рисунку 1.2 зображено контури архітектури більшості розробок IoT. Вона також може бути застосована в ІТС.

Представлена архітектура складається з чотирьох рівнів, що відповідають за різні функції IoT. Застосування цієї схеми в ІТС надає кожному рівню більш специфічні функції.

Рівень сприйняття ІТС охоплює смартфони користувачів, датчики в транспортних засобах та інфраструктурні пристрої. Багато питань безпеки на рівні сприйняття пов'язані з конфігурацією та ініціалізацією пристроїв під час виробництва та проектуванням внутрішньої автомобільної мережі, оскільки в більшості випадків вона не призначена для підключених автомобілів.

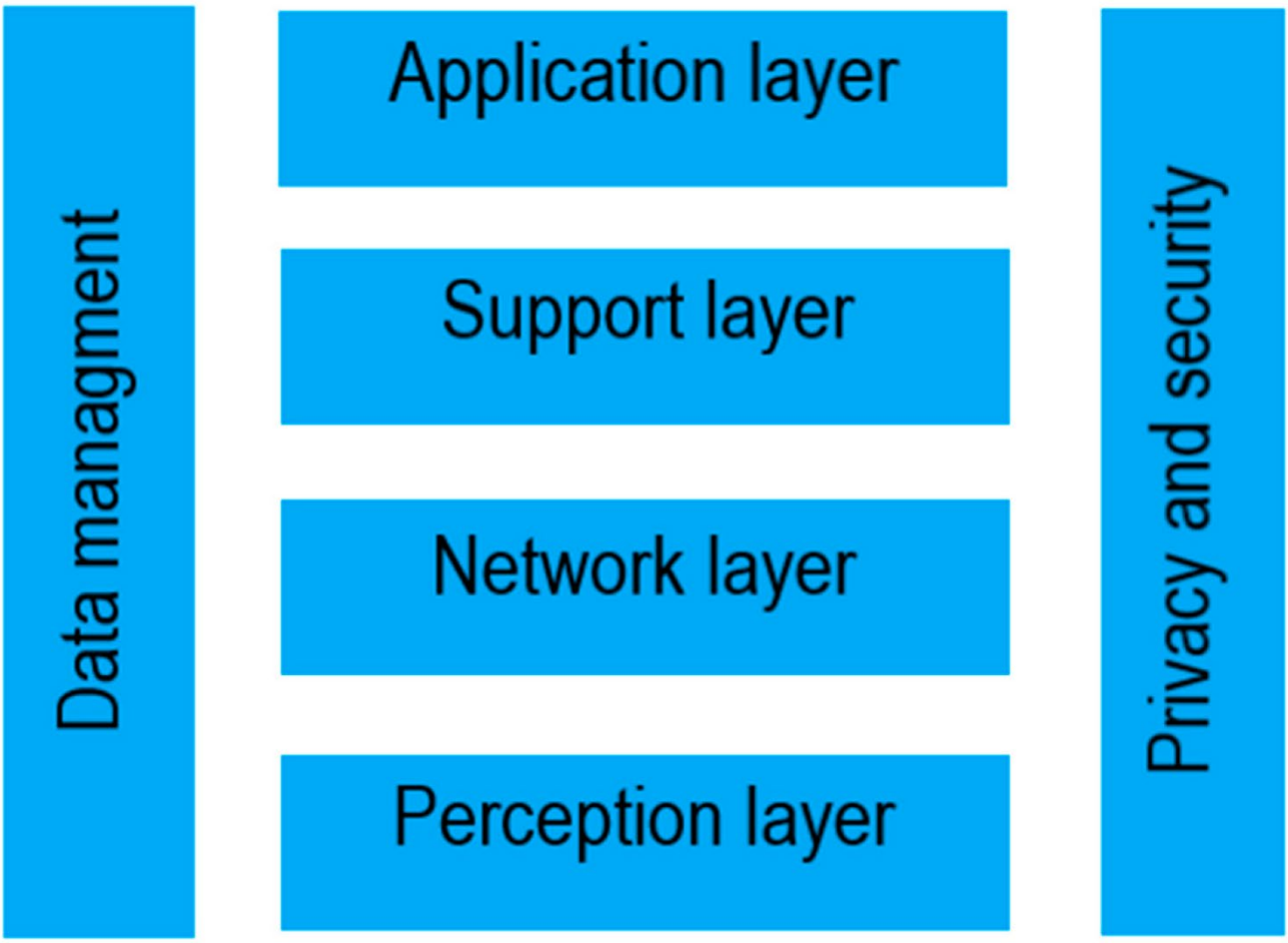

Рисунок 1.2 – Контури архітектури IoT

Мережевий рівень є складним сплавом дротових і бездротових технологій. Одним з важливих питань кібербезпеки на цьому рівні є забезпечення автентифікації вузлів у VANET. Через необхідність захисту персональних даних автентифікація повинна бути анонімною. Обмежена кількість вузлів та жорсткі часові вимоги створюють додаткові труднощі .

Серед розробок стандартів архітектури VANET можна виділити дві мережеві технології - сімейство стандартів IEEE 1609 (Wireless Access in Vehicle Environment-WAVE), засноване на стандарті 802.11, і стандарт 3GPP (застосовується для мереж 4G і 5G LTE-Long Term Evaluation під назвою Cellular Vehicle to Everything-C-V2X).

WAVE описує механізм автентифікації на основі списку ієрархічних сертифікатів. Він визначає чіткі вимоги до конкретних криптографічних примітивів і не надає альтернативи. Проблема полягає в тому, що в динамічній ситуації та

завантаженій мережі процедура, описана в стандарті, не задовольняє часовим обмеженням. Вона вимагає: алгоритм еліптичної кривої цифрового підпису (ECDSA) і конкретні еліптичні криві P-256 і P256r1; максимальний розмір закритого ключа - 32 байти; AES-CCM (Advanced Standard Encryption in Counter Mode) - симетричний алгоритм шифрування і хеш-функція SHA-256 .

Технологія C-V2X визначає два режими роботи - режим 4 (некерований режим) і режим 3 (керований режим). У керованому режимі застосовуються стандартні механізми безпеки стандартів LTE. У некерованому режимі питання безпеки залишаються невирішеними. Стандарт встановлює вимоги до захисту від дублювання, цілісності, конфіденційності та передбачає використання псевдонімів. Він окреслює вимоги, але не дає рекомендацій щодо конкретних механізмів .

Філософія 5G орієнтована на надання послуг. Slicing Security as-a-Service, або SSaaS, дозволяє операторам надавати диференційовані та індивідуальні пакети безпеки, включаючи алгоритми шифрування, параметри шифрування, можливості конфігурації чорних і білих списків, методи аутентифікації та міцність ізоляції тощо.

На рівні підтримки дані обробляються в тумані або хмарі, залежно від їх часових і просторових особливостей та міркувань безпеки. Як нова технологія, структури на основі туману створюють нові виклики для безпеки, оскільки робоче середовище розподілених систем туману складніше захистити, ніж централізовану хмару. Існуючі вимірювання безпеки і конфіденційності для хмарних обчислень не можуть бути безпосередньо застосовані до туманних обчислень через їх особливості, такі як мобільність, гетерогенність і великомасштабний георозподіл .

Прикладний рівень відображає кінцеву взаємодію з користувачем, яка може виражатися в інформуванні, попередженні і навіть активації певної системи в транспортному засобі (у випадку безпілотних транспортних засобів). Перш ніж потрапити до користувача, дані, отримані на сенсорному рівні, можуть бути оброблені в декількох місцях. Залежно від семантики даних, вимог безпеки та часових обмежень обчислення можуть виконуватися локально, в самому транспортному засобі, в придорожніх пристроях (RSU), в тумані або хмарі. Дані в

ІТС відповідають усім характеристикам великих даних, що є передумовою для застосування штучного інтелекту (ШІ). Його застосування в таких критично важливих для безпеки системах, як ІТС, має бути ретельно продуманим, оскільки вони дуже вразливі до низки кібератак .

Хоча ІТС є відносно новим явищем, багато технологій, які вони інтегрують, були випробувані на практиці, і набутий досвід можна використовувати повторно. З точки зору безпеки, деякі з класичних підходів, безумовно, відіграватимуть ключову роль. Ефективними підходами до захисту рівня підтримки є: надійна автентифікація, зашифрований зв'язок, управління ключами, регулярний аудит, приватна мережа та безпечна маршрутизація [3].

Криптографічні методи є основою кібербезпеки. Застосування криптографічних методів в автомобільній промисловості має історію з 90-х років. Традиційні алгоритми та стандарти шифрування не повністю підходять для ІТС, оскільки вони не можуть задовольнити вимоги високої пропускної здатності, низької затримки та надійності. Легке шифрування стало основною вимогою в ІТС.

Сегментація мережі є ще одним класичним підходом, який покращує як безпеку, так і ефективність мережі. Говорячи про сегментацію мережі ІТС, слід враховувати, що деякі з вузлів є мобільними, динамічно приєднуються і мають вимоги до анонімності. У VANET важливу роль відіграватиме відокремлення кластерів від машин, що спілкуються між собою, таким чином будуючи ієрархію в мережі. Залежно від цілей і ситуації, можна враховувати різні метрики - поведінкові характеристики, засновані на історичних даних, ресурси, місцезнаходження і так далі.

ІТС - це складна багатокомпонентна система, яка є чутливою до кібербезпеки та вразливою у всіх своїх підсистемах. У представленому документі показана чотирирівнева модель архітектури IoT, яка була адаптована для більш чіткого розмежування проблем.

На рівні сприйняття Spoofing-атаки призводять до некоректного збору даних. Відмова в обслуговуванні може призвести до виходу з ладу будь-якої з систем. Основною проблемою на цьому рівні є конфігурація та ініціалізація пристроїв під

час виробництва та проектування внутрішньої мережі транспортного засобу, що не відповідає підключенню транспортних засобів у динамічних мережах.

Концепція безпеки за контрактом є перспективною технологією на рівні сприйняття, особливо щодо питань, пов'язаних зі змінами та вдосконаленням стратегій безпеки. Об'єднання сенсорів успішно застосовується на практиці для усунення неточної інформації.

На мережевому рівні можливі численні кібератаки через динамічну топологію VANET. Іноді атакуюча сторона може діяти пасивно, наприклад, підслуховувати. Атаки «чорних» та «сірих» дір опускають повторну передачу пакетів і таким чином порушують комунікацію. Атака «зловмисник посередині» поширює модифіковані дані. Атаки на синхронізацію затримують передачу даних і таким чином завдають шкоди системам, які покладаються на реакцію в реальному часі. Sybil покладається на підміну ідентифікаційних даних вузлів, що може спричинити глушіння або відмову в обслуговуванні. Через можливість атаки на ідентифікаційні дані автентифікація вузлів обов'язково повинна бути анонімною.

Для зменшення мережевих та обчислювальних ресурсів, необхідних для безперервного обміну псевдонімами у VANET, шукаються різні рішення щодо анонімної автентифікації.

Однією з найбільш швидкозростаючих технологій, яка експериментується в цій галузі, є блокчейн. Крім анонімної аутентифікації, блокчейн в безпеці ITC може знайти застосування на верхніх рівнях архітектури в якості захищеного сховища даних. Ще однією відповіддю на питання зменшення ресурсів при анонімній автентифікації є туманні обчислення (Fog computing). Зберігання вразливої ідентифікаційної інформації вузлів на периферії системи обмежить ризик атак. Використання декількох взаємодоповнюючих технологій є можливим вирішенням питання ресурсоефективної автентифікації. Хорошим прикладом цього є фільтр цвітіння як основний метод, а також чорний список і запит до легітимної сторони як допоміжні методи.

На рівні підтримки основною проблемою є захист туманних структур.

Традиційні методи безпеки, такі як криптографія та сегментація мережі, є найбільш підходящим рішенням для захисту туману. Вони повинні бути адаптовані до потреб ІТС.

На прикладному рівні основними питаннями, на яких повинна зосередитися безпека, є опис і стандартизація складної моделі даних і метаданих, а також захист систем, заснованих на ШІ.

Можливими атаками на цьому рівні є отруєння даних, збурення середовища та маніпулювання політиками.

Через складність ІТС необхідна інтелектуальна стратегія безпеки. ШІ, машинне навчання, онтології та теорія ігор - це інструменти, які знайшли застосування в рішеннях з кібербезпеки. Їх застосування та адаптація до ІТС потребує детального вивчення. Інтелектуальна безпека часто базується на співпраці між фахівцями з кібербезпеки та різноманітними інтелектуальними рішеннями для забезпечення безпеки.

1.4 Вектори кібератак на автономні транспортні засоби

Будь-яка зловмисна дія, спрямована на компрометацію або зміну систем або даних транспортного засобу, вважається кібератакою на АТЗ. Фішингові атаки, впровадження шкідливого програмного забезпечення, атаки на відмову в обслуговуванні та прямі фізичні напади на апаратне забезпечення автомобіля - ось лише деякі з багатьох прикладів різноманітних способів прояву кібератак. Успішна кібератака на автономний автомобіль може мати руйнівні наслідки, включаючи втрату керування, системні збої і навіть фізичні травми інших водіїв і пасажирів. Впровадження ретельної стратегії безпеки, яка включає такі функції, як контроль доступу, мережева безпека, шифрування та автентифікація, а також часте тестування та аудит безпеки, має вирішальне значення для запобігання кібератакам на безпілотні автомобілі. Крім того, дуже важливо бути в курсі останніх загроз і вразливостей у сфері кібербезпеки, а також регулярно оновлювати та посилювати заходи безпеки, щоб протистояти новим загрозам у міру їх появи.

Перехоплення дистанційного керування - це серйозна кібератака, яка може бути спрямована на АТЗ. Під час такої атаки зловмисник віддалено перебирає на себе функції керування, гальмування та прискорення автомобіля. Потенційно зловмисник може скерувати автомобіль у небезпечному напрямку або навіть спричинити аварію. Незахищені маршрути бездротового зв'язку або неякісні процедури автентифікації в програмному забезпеченні автомобіля можуть призвести до викрадення пульта дистанційного керування. З огляду на те, наскільки сильно безпечне функціонування АТЗ залежить від програмного забезпечення та мереж зв'язку, цей вид атак повинен викликати особливе занепокоєння. Щоб уникнути перехоплення пульта дистанційного керування, необхідно вживати надійних заходів безпеки, зокрема шифрування, брандмауери та регулярне оновлення програмного забезпечення для виправлення будь-яких відомих недоліків. Крім того, виробники повинні розглянути можливість встановлення відмовостійких систем, які дозволять автомобілю зупинитися або сповільнити рух у разі нападу .

Підробка датчиків - це ще один вид кібератаки, який може бути застосований проти безпілотних автомобілів. Мета цієї атаки - змусити автомобіль приймати неправильні рішення або, можливо, вийти з ладу, обдуривши його датчики фальшивими даними. Наприклад, зловмисник може використовувати інструмент для передачі помилкових сигналів на радар або лідарні датчики автомобіля, створюючи враження, що на дорозі є фальшива перешкода, хоча її немає. Це може призвести до викривлення або різкого гальмування автомобіля, що може спричинити аварію. Сприйняттям транспортним засобом сигналів світлофора та інших дорожніх індикаторів можна маніпулювати за допомогою підміни датчиків, що призводить до ігнорування або неправильної інтерпретації важливих повідомлень. Щоб запобігти підміні датчиків, необхідно встановити безпечні протоколи зв'язку між датчиками на транспортному засобі та іншими системами. Крім того, важливо використовувати різні датчики для перехресної перевірки даних і виявлення розбіжностей. Алгоритми ML також можуть бути використані для виявлення потенційних атак шляхом виявлення аномалій у даних датчиків .

Кібератака на відмову в обслуговуванні - це різновид кібератаки, яка може бути використана для націлювання на антивірусні системи. У цій атаці зловмисник перевантажує системи або мережі транспортного засобу трафіком або запитами, роблячи систему недоступною або такою, що не реагує на запити. Це може перешкоджати нормальній роботі транспортного засобу або призвести до його повного вимкнення. Наприклад, зловмисник може здійснити DoS-атаку на навігаційну систему транспортного засобу, позбавивши її доступу до життєво важливих даних про місцезнаходження, що призведе до того, що автомобіль загубиться або заплутається. Для запобігання DoS-атакам вкрай важливо застосовувати заходи мережевої безпеки, такі як брандмауери та системи виявлення вторгнень, для виявлення та блокування шкідливого трафіку. Крім того, впровадження методів резервування та обходу відмов може допомогти переконатися, що важливі системи продовжують функціонувати, навіть якщо одну з них зламано. Регулярне тестування та аудит безпеки також може допомогти у виявленні та усуненні можливих недоліків, які можуть бути використані в DoS-атаці .

Зараження шкідливим програмним забезпеченням - це різновид кібератаки, яка може бути застосована проти автономних автомобілів. У цій атаці шкідливе програмне забезпечення вставляється в бортові комп'ютерні системи автомобіля, надаючи зловмиснику доступ до контролю або викрадення інформації. Використовуючи вразливість програмного забезпечення, зловмисник може, наприклад, імплантувати шкідливе програмне забезпечення в інформаційно-розважальну систему автомобіля, яке потім може поширитися на інші системи, такі як рульове управління або гальмівна система. Отримавши такий доступ, зловмисник може заволодіти автомобілем, викрасти конфіденційну інформацію або навіть спричинити зіткнення. Шкідливі завантаження, інфіковані оновлення програмного забезпечення або прямий фізичний доступ до систем автомобіля - це лише кілька способів проникнення шкідливого програмного забезпечення. Щоб уникнути ін'єкції шкідливого програмного забезпечення, дуже важливо запровадити надійні заходи безпеки, включаючи безпечні процедури завантаження,

підписання коду та регулярне оновлення програмного забезпечення для виправлення будь-яких відомих недоліків. Крім того, атаки шкідливого програмного забезпечення можна виявити та обробити за допомогою систем виявлення вторгнень та реагування на них .

Фізична кібератака - це вид кібератаки, який передбачає фізичний доступ до апаратного забезпечення або систем транспортного засобу з метою їх зламу або зміни. У цьому типі атаки зловмисник отримує доступ до фізичних частин транспортного засобу, таких як датчики, процесори або комунікаційні модулі, і використовує цей доступ, щоб змінити поведінку транспортного засобу або викрасти приватну інформацію. Наприклад, фізичне втручання зловмисника в гальмівну систему автомобіля може призвести до відмови системи та аварії. Впровадження заходів фізичної безпеки, таких як захищене від несанкціонованого доступу обладнання та безпечні процедури завантаження, для запобігання несанкціонованому доступу до компонентів транспортного засобу має вирішальне значення для запобігання фізичним кібератакам. Крім того, навіть якщо фізичний доступ отримано, встановлення надійних процедур шифрування та автентифікації може допомогти захистити дані та комунікації. Регулярне тестування та аудит безпеки також можуть допомогти у виявленні та усуненні можливих недоліків, які можуть бути використані в реальній кібератаці.

Глушіння GPS - це різновид кібератаки, який може бути використаний для націлювання на АТЗ. Під час такої атаки зловмисник втручається в GPS-сигнал транспортного засобу, що ускладнює навігацію або нормальне функціонування автомобіля. Використання обладнання, яке випромінює радіосигнали на тій самій частоті, що й GPS-сигнали, може призвести до глушіння GPS, що заважає автомобілю отримувати точну інформацію про місцезнаходження. Це може призвести до того, що автомобіль загубиться або розгубиться, що може поставити під загрозу безпеку інших людей або спричинити зіткнення. Оскільки для навігації та безпечного функціонування автомобілі значною мірою покладаються на дані GPS, глушіння GPS може бути для них дуже проблематичним. Для запобігання глушіння GPS дуже важливо використовувати резервні системи позиціонування,

наприклад, кілька GPS-приймачів або інші технології позиціонування, зокрема інерційну навігацію або системи на основі камер. Ще одним способом зменшення впливу спроб глушіння GPS є використання систем фільтрації сигналу та виявлення глушіння [4].

Фішингові атаки є прикладом кібератаки, яка може бути спрямована на відеореєстратори. У цій атаці зловмисник обманом змушує користувачів або операторів транспортного засобу розкрити конфіденційну інформацію або вчинити зловмисні дії. Наприклад, зловмисник може надіслати фішинговий електронний лист оператору транспортного засобу, видаючи себе за надійне джерело, наприклад, виробника або постачальника послуг, і попросити надати приватні дані або доступ до систем автомобіля. Водій може ненавмисно надати зловмиснику доступ до систем автомобіля або конфіденційної інформації, якщо піддасться на фішингову аферу. Системи автомобіля також можуть бути заражені шкідливим програмним забезпеченням або іншими шкідливими програмами за допомогою фішингової тактики. Дуже важливо інформувати користувачів і операторів про небезпеку атак соціальної інженерії та впроваджувати надійні заходи автентифікації та контролю доступу, щоб обмежити доступ до конфіденційних даних і систем для запобігання фішинговим атакам. Регулярні тренінги з підвищення обізнаності про безпеку та симуляції фішингових атак також можуть допомогти навчити користувачів та операторів виявляти фішингові спроби та реагувати на них.

Програми-вимагачі - це різновид кібератак, які можуть бути спрямовані на антивірусні програми. У цій атаці зловмисник використовує шкідливе програмне забезпечення, щоб заблокувати або зашифрувати системи транспортного засобу, не даючи їм функціонувати, поки не буде сплачено викуп. Атаки з вимогою викупу можуть відбуватися різними способами, зокрема через фішингові електронні листи, вади в програмному забезпеченні або шкідливі завантаження. Зловмисник часто вимагає гроші після того, як системи автомобіля були зашифровані або заблоковані, в обмін на ключ для розшифрування або для відновлення доступу до систем автомобіля. Оскільки безпека функціонування АТЗ дуже залежить від програмного забезпечення та мереж зв'язку. Для усунення будь-яких відомих вразливостей і

гарантування можливості відновлення даних під час атаки слід впровадити надійні процедури безпеки, такі як регулярне оновлення програмного забезпечення та резервне копіювання. Також має бути розроблений ретельний план реагування на інциденти для своєчасного виявлення та реагування на можливі атаки з використанням програм-вимагачів [5].

Атака «людина посередині» (Man-in-the-middle, MITM) - це різновид кібератаки, яка може бути використана проти антивірусів. Зловмисник перехоплює і змінює зв'язок між системами автомобіля та іншими гаджетами або системами, наприклад, пультом дистанційного керування або стільниковою мережею. Потім зловмисник може змінити інформацію, що передається між двома системами, що може призвести до несподіваної поведінки автомобіля або розкриття приватної інформації. Наприклад, зловмисник може перехопити і змінити сигнал дистанційного керування, що призведе до відхилення автомобіля від курсу або раптового прискорення. Внаслідок цього пасажири або інші водії можуть наразитися на небезпеку травмування. Для захисту зв'язку між системами транспортного засобу та іншими пристроями або системами необхідно використовувати надійні процедури шифрування та автентифікації, щоб запобігти MITM-атакам. Впровадження систем виявлення вторгнень та реагування на них також може допомогти у виявленні та пом'якшенні потенційних загроз НВМ в режимі реального часу [6].

Соціальна інженерія - це різновид кібератаки, яка може бути використана для нападу на ППО. У цій атаці зловмисник обманом змушує користувачів або операторів розкрити конфіденційну інформацію або вдатися до деструктивної поведінки, використовуючи психологічні маніпуляції. Атаки соціальної інженерії можуть набувати різних форм, таких як фішинг, вигадка або приманка. Щоб обдурити оператора і змусити його надати доступ до систем транспортного засобу або критично важливої інформації, зловмисник, наприклад, може представитися авторизованим постачальником послуг або виробником транспортного засобу. Крім того, хакер може використовувати соціальну інженерію, щоб отримати фізичний доступ до систем автомобіля, наприклад, прикинувшись механіком або

співробітником з технічного обслуговування. Через залежність безпілотних автомобілів від надійності бортового обладнання та довіри операторів, атаки з використанням соціальної інженерії можуть викликати особливе занепокоєння. Дуже важливо інформувати користувачів і операторів про небезпеку соціальної інженерії та впроваджувати надійні процедури контролю доступу та автентифікації, щоб запобігти атакам соціальної інженерії. Регулярні тренінги з підвищення обізнаності щодо безпеки також можуть допомогти навчити користувачів та операторів виявляти потенційні загрози соціальної інженерії та реагувати на них .

Кібератака на бездротову мережу - це різновид кібератаки, яка може бути застосована проти автономних автомобілів. У цій атаці зловмисник використовує недоліки бездротових мереж Wi-Fi або Bluetooth автомобіля, щоб отримати несанкціонований доступ до його систем або даних. Потім зловмисник може використати цей доступ, щоб змусити автомобіль діяти ненавмисно або здійснити витік приватних даних. Наприклад, хакер може використати мережу Wi-Fi для доступу до інформаційно-розважальної системи автомобіля, а потім встановити шкідливе програмне забезпечення, яке надасть йому віддалений доступ до керування автомобілем. Крім того, зловмисник може використати з'єднання Bluetooth для доступу до діагностичних систем автомобіля і змінити його характеристики або функції безпеки. Для захисту бездротового зв'язку між системами автомобіля та іншими пристроями або системами необхідно використовувати надійні процедури шифрування та автентифікації, щоб запобігти атакам на бездротові мережі. Також дуже важливо встановити системи виявлення вторгнень та реагування на них для швидкого виявлення та припинення будь-яких атак, а також регулярно оновлювати програмне та апаратне забезпечення для усунення будь-яких відомих вразливостей [7].

Кібератака грубої сили - це різновид кібератаки, яка може бути застосована проти автономних автомобілів. У цій атаці зловмисник намагається отримати доступ до систем або даних автомобіля, вгадуючи паролі або інші облікові дані для автентифікації. У більшості випадків зловмисник використовує автоматизовані системи, які можуть швидко перевірити тисячі потенційних паролів. Припустимо,

що зловмиснику вдалося вгадати правильний пароль. У такому випадку він може отримати доступ до систем і даних автомобіля, що дасть йому змогу змусити автомобіль робити неочікувані речі або розголошувати приватні дані. Зловмисник може, наприклад, провести атаку грубою силою, щоб отримати доступ до систем керування автомобілем і змінити швидкість або напрямок руху. Використання методів багатофакторної автентифікації, які вимагають додаткової перевірки, окрім базового пароля, а також використання надійних, складних паролів є важливими кроками для запобігання атакам грубої сили. Крім того, атак грубої сили можна уникнути, регулярно змінюючи паролі та мінімізуючи кількість невдалих спроб входу .

Кібератака на ланцюг постачання - це різновид кібератаки, яка може бути використана для нападу на АВ. Об'єктом такої атаки є ланцюг постачання транспортного засобу, який складається з усіх частин і систем, необхідних для його будівництва та експлуатації. Зловмисник може отримати несанкціонований доступ до систем або даних автомобіля, скомпрометувавши один або кілька компонентів ланцюга постачання, що дасть йому можливість змусити автомобіль діяти несподівано або розголошувати приватні дані [8]. Наприклад, хакер може отримати доступ до мереж виробника компонентів, що дозволить йому вставити шкідливе програмне забезпечення у прошивку життєво важливої автомобільної деталі, наприклад, гальмівної системи. Це може дозволити зловмиснику контролювати функціональність або системи безпеки автомобіля на відстані. Щоб запобігти атакам на ланцюги поставок, дуже важливо ретельно перевіряти всі деталі та постачальників на наявність недоліків у системі безпеки, а також запроваджувати надійні засоби контролю безпеки по всьому ланцюгу поставок. Використання надійних систем шифрування та автентифікації, а також регулярний аудит і тестування безпеки можуть бути використані для захисту комунікацій і даних уздовж усього ланцюга постачання [9].

Кібератака з перепрограмуванням електронного блоку керування (ECU) - це категорія кібератак, яка передбачає втручання в програмне забезпечення або мікропрограму, що регулює роботу систем і частин транспортного засобу. Під час

такої атаки зловмисник отримує незаконний доступ до електронного блоку керування автомобілем, який відповідає за управління життєво важливими системами, такими як двигун, коробка передач і гальма, і змінює програмне забезпечення, щоб змусити автомобіль діяти в непередбачуваний або небезпечний спосіб. Наприклад, хакер може модифікувати електронний блок керування, щоб відключити життєво важливі заходи безпеки, такі як гальма або подушки безпеки, що може призвести до серйозної аварії. Для запобігання несанкціонованому доступу до систем автомобіля та спробам перепрограмування ЕБУ необхідно запровадити суворі обмеження доступу та процедури автентифікації. Додатковим запобіжником перехоплення або підробки даних і комунікацій з автомобіля є впровадження надійних систем шифрування та автентифікації. Регулярне тестування та аудит безпеки також може допомогти у виявленні та усуненні потенційних недоліків, які можуть бути використані в кібератаці з перепрограмування ЕБУ [10].

Кібератака побічного каналу - це різновид кібератаки, яка може бути застосована проти автономних автомобілів. У цій атаці зловмисник використовує недоліки в апаратному або програмному забезпеченні автомобіля-мішені для отримання несанкціонованого доступу до його систем або даних. Щоб отримати конфіденційну інформацію, таку як паролі або криптографічні ключі, зловмисник часто використовує складні алгоритми для аналізу сигналів і енергоспоживання компонентів автомобіля [11]. Наприклад, ключ, який використовується для шифрування бездротового зв'язку автомобіля, може бути вилучений зловмисником через атаку на побічний канал, що дозволить йому перехоплювати і контролювати ці розмови. Використання надійних методів шифрування та автентифікації, стійких до атак на побічні канали, має вирішальне значення для запобігання атакам на побічні канали. Використання заходів фізичної безпеки, таких як захищене від несанкціонованого доступу обладнання та безпечні процедури завантаження, також може допомогти запобігти фізичному доступу зловмисників до систем або компонентів транспортного засобу [12]. Регулярний аудит і тестування безпеки

також може допомогти знайти і виправити будь-які вразливості до того, як вони будуть використані проти вас .

1.5 Протоколи передачі та шифрування даних в АТЗ

Забезпечення інформаційної безпеки автономних транспортних засобів (АТЗ) є критично важливим для їхньої безпечної та надійної експлуатації. Захист від кіберзагроз значною мірою залежить від використання надійних протоколів шифрування та передачі даних. Цей розділ присвячено опису основних стандартів, що застосовуються в АТЗ для гарантування конфіденційності, цілісності та автентичності інформації.

Одним із ключових аспектів є захист комунікацій за допомогою криптографічних протоколів. Протокол TLS (Transport Layer Security), що еволюціонував з SSL (Secure Sockets Layer), є загальновизнаним стандартом для захисту зв'язку в мережі Інтернет. Він забезпечує шифрування даних, автентифікацію сервера, а за необхідності й клієнта, та гарантує цілісність повідомлень. Застосування TLS є доцільним для захисту зовнішніх комунікацій АТЗ, таких як зв'язок з хмарними сервісами та V2X-взаємодія (Vehicle-to-Everything), а також для внутрішніх комунікацій між електронними блоками керування. Важливо наголосити на необхідності використання актуальних версій TLS (1.2 або 1.3) з метою уникнення відомих вразливостей, притаманних попереднім версіям.

Для забезпечення безпеки на мережевому рівні використовується протокол IPsec (Internet Protocol Security). Він забезпечує захист IP-пакетів та може бути використаний для створення віртуальних приватних мереж (VPN) між АТЗ та іншими мережами, або для захисту внутрішньої комунікації між компонентами автомобіля. IPsec функціонує у двох основних режимах: транспортному, що захищає корисне навантаження IP-пакета, та тунельному, що забезпечує захист всього IP-пакета.

У випадках, коли важлива мінімізація затримок, наприклад, при передачі потокового відео або аудіо, застосовується протокол DTLS (Datagram Transport Layer Security), оптимізований для роботи з протоколом UDP. DTLS надає аналогічні TLS функції, але з меншими затримками, що є критичним для додатків, чутливих до часу, таких як V2X-комунікації [13].

Захист на рівні каналу передачі даних (Layer 2) забезпечується протоколом MACsec (Media Access Control Security). Він запобігає атакам типу "людина посередині" в локальних мережах та може бути використаний для захисту внутрішніх комунікацій АТЗ, особливо в мережах Ethernet.

Щодо алгоритмів шифрування даних, AES (Advanced Encryption Standard) є симетричним алгоритмом блочного шифрування, широко використовуваним для захисту конфіденційної інформації. Він характеризується високою надійністю та ефективністю. AES може працювати в різних режимах, таких як ECB, CBC, CTR та GCM. Режим GCM, зокрема, забезпечує не тільки шифрування, але й автентифікацію та перевірку цілісності даних.

Для обміну ключами та створення цифрових підписів часто використовується асиметричний алгоритм RSA (Rivest–Shamir–Adleman). Хоча RSA менш ефективний для шифрування великих обсягів даних порівняно з AES, він відіграє важливу роль у встановленні безпечного з'єднання. Альтернативою RSA є алгоритм цифрового підпису на основі еліптичних кривих ECDSA (Elliptic Curve Digital Signature Algorithm), який забезпечує високий рівень безпеки при меншій довжині ключа, що є важливим для систем з обмеженими ресурсами.

Щодо протоколів передачі даних, CAN (Controller Area Network) залишається поширеним протоколом для внутрішніх комунікацій в автомобілях. Однак, зважаючи на відсутність вбудованих механізмів безпеки в оригінальному CAN протоколі, для захисту CAN-комунікацій застосовуються додаткові методи, такі як CANsec. Ethernet, з його більшою пропускною здатністю, стає все більш популярним в автомобільних мережах, особливо для передачі великих обсягів даних. Для захисту Ethernet-комунікацій використовуються протоколи MACsec та TLS. V2X-комунікації, що охоплюють взаємодію між транспортними засобами та

іншими об'єктами, використовують різні протоколи, такі як DSRC та C-V2X, безпека яких забезпечується за допомогою TLS/DTLS та цифрових підписів.

Важливими нормативними документами в галузі кібербезпеки автомобілів є стандарт ISO/SAE 21434, що визначає вимоги до кібербезпеки дорожніх транспортних засобів протягом усього їхнього життєвого циклу, та рекомендації SAE J3061, що надають настанови з кібербезпеки для автомобільних систем.

При виборі та реалізації протоколів шифрування та передачі даних необхідно враховувати такі фактори, як продуктивність системи, особливо в умовах обмежених обчислювальних ресурсів, безпечне керування криптографічними ключами та можливість оновлення протоколів та алгоритмів для протидії новим загрозам. Застосування описаних стандартів та протоколів є необхідним для забезпечення належного рівня інформаційної безпеки АТЗ.

Для подальшого дослідження ми розглянемо саме криптографічні алгоритми, що використовуються в АТЗ.

РОЗДІЛ 2 КРИПТОГРАФІЧНІ АЛГОРИТМИ В АТЗ

2.1 Криптографічні алгоритми протоколу Bluetooth

Використання Bluetooth в автотранспортних засобах (АТЗ) стало невід'ємною частиною сучасних автомобілів, пропонуючи бездротове з'єднання для різноманітних функцій, від гучного зв'язку та аудіосистеми до навігації, діагностики та систем безпеки. Bluetooth дозволяє водіям здійснювати дзвінки hands-free, відтворювати аудіо з мобільних пристроїв, отримувати навігаційні вказівки, підключати діагностичні сканери та моніторити параметри автомобіля в реальному часі. Крім того, ця технологія використовується в системах безключового доступу, сповіщеннях про аварійні ситуації, оновленні програмного забезпечення та персоналізації налаштувань автомобіля. Завдяки своїй зручності, низькій вартості та широкій сумісності Bluetooth значно покращує комфорт та функціональність сучасних АТЗ.

Однак, використання Bluetooth в АТЗ також створює певні виклики для інформаційного захисту. Бездротовий характер з'єднання робить його потенційно вразливим до перехоплення даних, атак "людина посередині", несанкціонованого доступу (bluejacking та bluesnarfing) та інших кіберзагроз. Зважаючи на те, що Bluetooth обмінюється важливою інформацією, включаючи дані про місцезнаходження, особисті контакти, діагностичні дані автомобіля та навіть потенційно керуючі команди (в системах безключового доступу), забезпечення безпеки Bluetooth-з'єднань є критично важливим. Для мінімізації ризиків необхідно використовувати сучасні версії Bluetooth з надійними механізмами шифрування (наприклад, AES-CCM), дотримуватися правил безпеки (вимикати Bluetooth, коли він не використовується, не приймати з'єднання від невідомих пристроїв), регулярно оновлювати програмне забезпечення пристроїв та впроваджувати додаткові заходи захисту, такі як використання брандмауерів та систем виявлення вторгнень. Таким чином, хоча Bluetooth і надає значні переваги для АТЗ,

забезпечення його інформаційної безпеки є ключовим аспектом для захисту даних та функціональності автомобіля.

Загальні відомості про безпеку Bluetooth: Bluetooth розроблено з урахуванням вимог безпеки, але, як і будь-яка технологія, він не є абсолютно захищеним. Безпека Bluetooth базується на кількох механізмах, включаючи аутентифікацію, яка є перевіркою ідентичності пристроїв, що встановлюють з'єднання; авторизацію, що визначає права доступу одного пристрою до ресурсів іншого; та шифрування, що захищає конфіденційність даних, які передаються між пристроями.

Методи шифрування в Bluetooth: Bluetooth використовує різні методи шифрування залежно від версії протоколу та профілю з'єднання. Основні методи включають E0, потоковий шифр, що використовувався в ранніх версіях Bluetooth (до 2.0+EDR) та вважається криптографічно слабким і не рекомендується до використання; SAFER+, блоковий шифр, що використовувався в Bluetooth 2.0+EDR та забезпечував кращий рівень безпеки порівняно з E0; AES-CCM, блоковий шифр AES (Advanced Encryption Standard) у режимі лічильника з кодом автентифікації повідомлень (Counter with CBC-MAC, CCM), що використовується в Bluetooth 2.1+EDR та пізніших версіях та забезпечує високий рівень безпеки та автентифікацію даних; та шифрування LE (Low Energy), де Bluetooth Low Energy (BLE) використовує AES-CCM з довжиною ключа 128 біт.

Технічні характеристики та алгоритми: E0 є потоковим шифром з довжиною ключа 64 біт. Його принцип роботи полягає у генерації ключового потоку на основі секретного ключа та початкового вектора (IV), який потім XOR-иться з відкритим текстом для отримання шифротексту. Слабкі сторони E0 полягають у вразливості до різних атак, таких як атака з відомим відкритим текстом. SAFER+ є блоковим шифром з довжиною ключа 128 біт. Його принцип роботи полягає у використанні кількох раундів перетворень над блоками даних. Він був замінений на AES-CCM через кращу криптографічну стійкість останнього. AES-CCM є блоковим шифром (AES) з довжиною ключа 128 біт у режимі лічильника з кодом автентифікації повідомлень (CCM). Його принцип роботи полягає в тому, що AES шифрує лічильник, що інкрементується, та XOR-иться з відкритим текстом. CCM додає

автентифікацію повідомлень, забезпечуючи цілісність даних. Алгоритм CCM включає обчислення MAC (Message Authentication Code) на основі повідомлення та додаткових даних (наприклад, адреси пристроїв), шифрування лічильника за допомогою AES, XOR шифрованого лічильника з відкритим текстом для отримання шифротексту та додавання MAC до шифротексту. Шифрування LE (Low Energy) використовує AES-CCM з довжиною ключа 128 біт, аналогічно до Bluetooth 2.1+EDR та пізніших версій.

Процес встановлення захищеного з'єднання (Simplified Secure Simple Pairing – SSP): Сучасні версії Bluetooth використовують спрощений процес безпечного сполучення (SSP), який включає обмін інформацією про можливості, де пристрої обмінюються інформацією про підтримувані методи аутентифікації та шифрування; генерацію спільного секретного ключа, де використовуються різні методи, такі як Numeric Comparison, Passkey Entry, Just Works, Out of Band (OOB); аутентифікацію, де відбувається перевірка ідентичності пристроїв на основі спільного секретного ключа; та шифрування з'єднання, де встановлюється шифрований канал зв'язку за допомогою AES-CCM.

Вразливості та рекомендації: Незважаючи на використання сильних криптографічних алгоритмів, Bluetooth залишається вразливим до деяких атак, таких як атаки "людина посередині" (Man-in-the-Middle), де зловмисник перехоплює та змінює дані, що передаються між пристроями, та Bluejacking та Bluesnarfing, де відбувається несанкціонований доступ до даних на пристрої Bluetooth. Для підвищення безпеки Bluetooth рекомендується використовувати останні версії Bluetooth з підтримкою SSP та AES-CCM, вимикати Bluetooth, коли він не використовується, не приймати з'єднання від невідомих пристроїв та регулярно оновлювати програмне забезпечення пристроїв.

2.2 RSA та ECDSA

RSA (Rivest–Shamir–Adleman) є одним з найпоширеніших асиметричних криптографічних алгоритмів, що широко використовуються в різних сферах,

включаючи захист інформації в автотранспортних засобах (АТЗ). Асиметрична криптографія, на відміну від симетричної, використовує пару ключів: відкритий ключ, який може бути загальнодоступним, та закритий (секретний) ключ, який відомий лише власнику. RSA базується на математичній складності факторизації великих чисел на прості множники. Процес генерації ключів RSA починається з вибору двох великих простих чисел p та q. Потім обчислюється їх добуток n = p * q, який є модулем для обох ключів. Далі обчислюється функція Ейлера φ(n) = (p-1) * (q-1). Після цього обирається ціле число e (1 < e < φ(n)), яке є взаємно простим з φ(n), тобто їх найбільший спільний дільник дорівнює 1. Число e є відкритим ключем. Закритий ключ d обчислюється як мультиплікативна обернене до e за модулем φ(n), тобто d * e ≡ 1 (mod φ(n)). Отже, відкритий ключ складається з пари (n, e), а закритий ключ – з пари (n, d). Шифрування повідомлення M (0 < M < n) відбувається за формулою C = M^e (mod n), де C – шифротекст. Розшифрування шифротексту C відбувається за формулою M = C^d (mod n). Безпека RSA ґрунтується на тому, що знаючи n та e, обчислювально складно знайти d без знання p та q. В контексті АТЗ, RSA може застосовуватися для різних цілей. Одним з важливих застосувань є цифрові підписи. За допомогою закритого ключа можна створити цифровий підпис повідомлення, який потім можна перевірити за допомогою відповідного відкритого ключа. Це дозволяє гарантувати автентичність та цілісність даних, що передаються між різними компонентами автомобіля, або між автомобілем та зовнішніми серверами. Наприклад, виробник автомобіля може підписувати оновлення програмного забезпечення своїм закритим ключем, а автомобіль, отримавши оновлення, перевіряє підпис за допомогою відкритого ключа виробника, гарантуючи, що оновлення є справжнім і не було змінено зловмисниками. RSA також може використовуватись для шифрування ключів сеансу, які потім використовуються для швидшого симетричного шифрування даних, наприклад, за допомогою AES [14]. Це дозволяє забезпечити конфіденційність даних, що передаються між автомобілем та зовнішніми пристроями або серверами. Наприклад, під час обміну діагностичною інформацією з сервісним центром, ключ сеансу може бути зашифрований за допомогою RSA, що

гарантує, що лише авторизований сервісний центр зможе отримати доступ до цієї інформації. Важливо зазначити, що безпека RSA залежить від довжини ключа. Чим довші ключі використовуються, тим складніше їх зламати. В сучасних системах рекомендується використовувати ключі довжиною не менше 2048 біт, а в особливо важливих застосуваннях – 3072 біт або більше. Правильна генерація та зберігання ключів також є критично важливими для забезпечення безпеки RSA. Неправильне поводження з ключами може призвести до компрометації системи.

ECDSA (Elliptic Curve Digital Signature Algorithm) – це алгоритм цифрового підпису, що базується на криптографії еліптичних кривих, і є важливим інструментом для забезпечення безпеки в автотранспортних засобах (АТЗ). На відміну від RSA, який базується на складності факторизації великих чисел, ECDSA використовує властивості еліптичних кривих над скінченними полями. Еліптична крива визначається рівнянням виду $y^2 = x^3 + ax + b$, де a та b – константи. Точки на кривій разом з операцією додавання утворюють абелеву групу. Безпека ECDSA ґрунтується на складності задачі дискретного логарифмування на еліптичних кривих, тобто знаходження такого числа k, що $Q = kP$, де P та Q – точки на кривій. Генерація ключів в ECDSA починається з вибору еліптичної кривої E та базової точки G на цій кривій, що має великий простий порядок n. Закритий ключ d – це випадкове ціле число в діапазоні від 1 до n-1. Відкритий ключ Q обчислюється як $Q = dG$, тобто результат скалярного множення базової точки G на закритий ключ d. Для створення цифрового підпису повідомлення m, спочатку обчислюється його хеш $h = H(m)$, де H – криптографічна хеш-функція, наприклад SHA-256. Потім генерується випадкове число k в діапазоні від 1 до n-1. Обчислюється точка $R = kG$ на еліптичній кривій, і значення $r = x \pmod n$, де x – координата x точки R. Якщо $r = 0$, генерується нове випадкове число k. Далі обчислюється $s = k^{-1}(h + rd) \pmod n$. Якщо $s = 0$, також генерується нове випадкове число k. Підписом повідомлення m є пара чисел (r, s). Для перевірки підпису (r, s) повідомлення m, обчислюється хеш $h = H(m)$. Потім обчислюються два значення: $u1 = h * w \pmod n$ та $u2 = r * w \pmod n$, де $w = s^{-1} \pmod n$. Після цього обчислюється точка $V = u1G + u2Q$ на еліптичній кривій. Якщо x-координата точки V дорівнює r (mod n), то підпис вважається

дійсним. В контексті АТЗ, ECDSA знаходить широке застосування завдяки своїй ефективності та високому рівню безпеки при відносно коротких ключах. Це особливо важливо для вбудованих систем з обмеженими обчислювальними ресурсами. ECDSA використовується для автентифікації повідомлень між різними електронними блоками управління (ECU) в автомобілі, запобігаючи підміні даних та несанкціонованому втручанню в роботу систем автомобіля. Наприклад, повідомлення від датчика ABS до блоку управління гальмами може бути підписано за допомогою ECDSA, гарантуючи його цілісність та автентичність [15]. ECDSA також використовується для захисту оновлень програмного забезпечення "по повітрю" (OTA). Виробник автомобіля підписує оновлення своїм закритим ключем ECDSA, а автомобіль перевіряє підпис за допомогою відповідного відкритого ключа, гарантуючи, що оновлення є автентичним та не було модифіковано зловмисниками. Це запобігає встановленню шкідливого програмного забезпечення на автомобіль. Крім того, ECDSA може використовуватись в системах V2X (Vehicle-to-Everything) для автентифікації повідомлень, що передаються між автомобілями, дорожньою інфраструктурою та іншими пристроями. Завдяки своїй ефективності та безпеці, ECDSA є важливим криптографічним інструментом для захисту сучасних АТЗ від кіберзагроз.

ECDSA (Elliptic Curve Digital Signature Algorithm) має значні переваги над RSA (Rivest–Shamir–Adleman) щодо ресурсозатратності та швидкодії, особливо важливі для пристроїв з обмеженими ресурсами, як в АТЗ. ECDSA досягає еквівалентного рівня безпеки з набагато коротшими ключами, наприклад, 256-бітний ключ ECDSA відповідає 3072-бітному ключу RSA. Це суттєво зменшує обчислювальні витрати, оскільки операції з еліптичними кривими, на яких базується ECDSA, потребують менше ресурсів, ніж операції з великими числами в RSA. Зокрема, множення та піднесення до степеня в RSA є більш витратними, ніж додавання та скалярне множення точок на кривій в ECDSA. Коротші ключі також означають менші вимоги до пам'яті для зберігання ключів та проміжних результатів, що важливо для вбудованих систем з обмеженим обсягом пам'яті та для передачі даних в мережах з низькою пропускною здатністю. Завдяки меншим обчислювальним витратам,

ECDSA забезпечує швидше генерування та перевірку підписів, що критично для застосувань в реальному часі, таких як автентифікація між ECU або захист V2X-комунікацій. Менші обчислення також означають менше споживання енергії, що важливо для електромобілів та гібридів. Таким чином, ECDSA є ефективнішим вибором для багатьох автомобільних застосувань, де важливі обмежені ресурси, висока швидкість та низьке енергоспоживання, наприклад, для автентифікації ECU, захисту OTA-оновлень, безпеки V2X та захисту діагностичних даних.

2.3 Advanced Encryption Protocol

AES (Advanced Encryption Standard) – це симетричний блоковий шифр, прийнятий урядом США як стандарт шифрування в 2001 році. Він замінив застарілий DES (Data Encryption Standard) та став одним з найпоширеніших алгоритмів шифрування у світі. AES є симетричним шифром, тобто для шифрування та розшифрування даних використовується один і той самий секретний ключ. Він є блоковим шифром, тобто дані обробляються блоками фіксованої довжини. AES оперує блоками даних розміром 128 біт (16 байт). AES підтримує ключі довжиною 128, 192 та 256 біт. Більша довжина ключа забезпечує вищу криптографічну стійкість. AES базується на алгоритмі Rijndael, розробленому бельгійськими криптографами Жоаном Даеменом та Вінсентом Райменом. Rijndael підтримував різні розміри блоків та ключів, але AES стандартизував розмір блоку до 128 біт.

AES працює з блоком даних (128 біт), який представляється у вигляді матриці 4x4 байти, що називається станом (state). Алгоритм виконує кілька раундів перетворень над цим станом. Кількість раундів залежить від довжини ключа: 10 раундів для ключа 128 біт, 12 раундів для ключа 192 біт та 14 раундів для ключа 256 біт. Кожен раунд складається з чотирьох основних операцій: SubBytes (Заміна байтів) – нелінійна заміна кожного байта стану за допомогою таблиці підстановки (S-box). Ця операція забезпечує заплутування (confusion); ShiftRows (Зсув рядків) – циклічний зсув рядків стану. Перший рядок не зсувається, другий зсувається на 1

байт вліво, третій – на 2 байти, четвертий – на 3 байти. Ця операція забезпечує дифузію (diffusion); MixColumns (Змішування стовпців) – лінійне перетворення стовпців стану за допомогою матричного множення. Ця операція також забезпечує дифузію; AddRoundKey (Додавання ключа раунду) – XOR стану з ключем раунду, отриманим з основного ключа за допомогою процедури розширення ключа (Key Expansion).

Процедура розширення ключа генерує ключі для кожного раунду з основного ключа. Вона забезпечує, щоб кожен раунд використовував різний ключ, що підвищує криптографічну стійкість алгоритму.

AES знаходить широке застосування в різних системах автомобіля, де потрібний захист даних: безпека зв'язку між електронними блоками управління (ECU). AES може використовуватись для шифрування даних, що передаються між різними ECU в автомобілі, запобігаючи несанкціонованому доступу та підміні даних. Це особливо важливо для систем керування двигуном, гальмами та подушками безпеки; захист даних діагностики [16]. AES може використовуватись для шифрування даних, що зберігаються в бортовому комп'ютері автомобіля, таких як коди помилок та дані про роботу систем. Це захищає конфіденційну інформацію від несанкціонованого доступу під час діагностики або технічного обслуговування; безпека безключового доступу та запуску двигуна. AES може використовуватись для шифрування повідомлень між ключем та автомобілем, запобігаючи перехопленню сигналу та викраденню автомобіля; захист даних телематики. AES може використовуватись для шифрування даних, що передаються між автомобілем та сервером телематики, таких як дані про місцезнаходження, стиль водіння та технічний стан автомобіля. Це захищає приватність водія та запобігає несанкціонованому доступу до даних автомобіля; захист оновлень програмного забезпечення "по повітрю" (OTA). AES може використовуватись для шифрування оновлень програмного забезпечення, що передаються на автомобіль "по повітрю", гарантуючи їхню цілісність та автентичність. Це запобігає встановленню шкідливого програмного забезпечення на автомобіль.

Використання AES в АТЗ є важливим елементом забезпечення інформаційної безпеки та захисту від кіберзагроз. Його висока криптографічна стійкість, швидкість та гнучкість роблять його оптимальним вибором для захисту даних в сучасних автомобілях. AES має високу криптографічну стійкість та вважається одним з найбільш безпечних алгоритмів шифрування, стійкий до більшості відомих атак. AES є відносно швидким алгоритмом, що дозволяє використовувати його в реальному часі в системах автомобіля. AES може бути ефективно реалізований як програмно, так і апаратно, що забезпечує гнучкість у його застосуванні. AES є міжнародним стандартом, що забезпечує сумісність між різними системами та пристроями [17].

2.4 Режими роботи AES

AES, будучи блочним шифром, для обробки даних різної довжини використовує режими роботи, які визначають, як саме шифруються послідовні блоки. Розглянемо режими ECB, CBC, CFB, OFB та CTR з їхніми особливостями.

Електронна кодова книга (ECB). У ECB кожен блок відкритого тексту шифрується незалежно. Це найпростіший режим, де однаковий відкритий текст завжди дає однаковий шифротекст при використанні того ж ключа. Це є серйозною вразливістю, оскільки дозволяє криптоаналітику ідентифікувати повторювані блоки та отримувати інформацію про структуру даних, навіть не знаючи ключа. Перевагою ECB є простота реалізації та можливість паралельного шифрування/розшифрування блоків. Через низьку безпеку, ECB не рекомендується для більшості застосувань, хіба що для шифрування коротких випадкових даних, наприклад, ключів [18].

Зчеплення блоків шифротексту (CBC). У CBC кожен блок відкритого тексту перед шифруванням XOR-иться з попереднім блоком шифротексту. Для першого блоку використовується вектор ініціалізації (IV). Це забезпечує дифузію: зміна одного біта відкритого тексту впливає на всі наступні блоки шифротексту. CBC є значно безпечнішим за ECB, оскільки однакові блоки відкритого тексту

шифруються по-різному залежно від їх позиції. Недоліком CBC є послідовне шифрування, що унеможливлює паралелізацію шифрування, хоча розшифрування можна паралелізувати. Важливою умовою безпеки є унікальність та випадковість IV [19].

Зворотній зв'язок за шифротекстом (CFB). У CFB шифрується не сам відкритий текст, а попередній блок шифротексту, результат XOR-иться з поточним блоком відкритого тексту. Це перетворює блочний шифр на потоковий. Розмір зворотного зв'язку (кількість біт з попереднього шифротексту, що використовуються) може бути меншим за розмір блоку. CFB забезпечує самосинхронізацію: якщо в шифротексті трапиться помилка, то після кількох блоків розшифрування відновиться. Проте, CFB чутливий до змін в IV, і його безпека менша, ніж у CBC при однаковій довжині ключа. CFB також не підтримує повну паралелізацію.

Зворотній зв'язок за виходом (OFB). OFB генерує ключовий потік, шифруючи попередній вихід шифру, і XOR-ить цей потік з відкритим текстом. Подібно до CFB, OFB перетворює блочний шифр на потоковий. Головна відмінність від CFB полягає в тому, що помилки в шифротексті не поширюються на наступні блоки при розшифруванні. OFB також дозволяє попередню генерацію ключового потоку, що може бути корисним у деяких застосуваннях. Проте, OFB має слабку стійкість до атак з відомим відкритим текстом, тому його використання не рекомендується для нових систем [20].

Лічильник (CTR). У CTR шифрується лічильник, значення якого збільшується для кожного блоку, а результат XOR-иться з відкритим текстом. Для першого блоку використовується nonce (одноразове число). CTR, як і OFB та CFB, перетворює блочний шифр на потоковий. CTR має важливі переваги: можливість паралельного шифрування та розшифрування, стійкість до помилок передачі (помилка в одному блоці не впливає на інші), можливість випадкового доступу до блоків. Важливою умовою безпеки є унікальність комбінації ключа та nonce для кожного повідомлення. CTR широко використовується завдяки своїй ефективності та гнучкості.

Отже, вибір режиму роботи AES залежить від конкретних вимог до безпеки, продуктивності та функціональності. ECB слід уникати, CBC є хорошим загальним вибором, CFB та OFB мають обмежене застосування, а CTR є кращим вибором для багатьох сучасних застосувань завдяки своїй ефективності та можливості паралелізації.

РОЗДІЛ 3 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

3.1 Обгрунтування вибору інструментів експериментального дослідження

Вибір мови програмування для експериментального дослідження затратності обчислювальних ресурсів при використанні різних криптографічних шифрів, що застосовуються в автономних транспортних засобах (АТЗ), є важливим етапом, який безпосередньо впливає на ефективність та достовірність отриманих результатів. У даному дослідженні обґрунтовується вибір мови програмування Python, виходячи з її особливостей та переваг для вирішення поставлених задач.

Однією з ключових переваг Python є наявність потужних та добре документованих криптографічних бібліотек, що значно спрощують реалізацію та тестування різних алгоритмів шифрування. Серед найбільш популярних варто виділити PyCryptodome, що є форком PyCrypto та пропонує великий набір криптографічних алгоритмів, включаючи симетричні (AES, DES, Blowfish), асиметричні (RSA, DSA, ECC), функції хешування (SHA-256, SHA-3) та інші криптографічні примітиви. Важливо, що PyCryptodome активно підтримується та оновлюється, що забезпечує актуальність та безпеку використання. Іншою важливою бібліотекою є Cryptography, розроблена проектом Python Cryptographic Authority, яка надає високоякісні криптографічні примітиви, написані на чистому Python та з використанням C-розширень для підвищення продуктивності. Вона підтримує широкий спектр алгоритмів та стандартів, включаючи TLS/SSL, X.509, PKCS та інші. Також варто згадати стандартну бібліотеку Python cryptography (з малою літерою "c"), що надає доступ до деяких базових криптографічних функцій. Наявність цих бібліотек дозволяє дослідникам зосередитися на дослідженні затратності обчислювальних ресурсів, а не на складній реалізації самих алгоритмів шифрування "з нуля".

Python відомий своєю простотою та читабельністю синтаксису, що значно полегшує розробку, налагодження та аналіз коду. Це особливо важливо при проведенні експериментальних досліджень, де необхідно швидко прототипувати та

змінювати експериментальні установки. Читабельний код також сприяє кращому розумінню та перевірці результатів іншими дослідниками.

Крім того, Python є кросплатформною мовою програмування, що дозволяє запускати експерименти на різних операційних системах (Windows, macOS, Linux) без необхідності значних змін у коді. Це забезпечує гнучкість при виборі апаратного забезпечення для проведення досліджень.

Важливим фактором є також велика та активна спільнота розробників Python, що забезпечує доступ до великої кількості документації, навчальних матеріалів, прикладів коду та готових рішень. Це значно спрощує вирішення проблем, що можуть виникнути під час дослідження.

Python надає зручні інструменти для профілювання коду та вимірювання продуктивності, що дозволяє точно визначити затрати обчислювальних ресурсів на виконання різних криптографічних операцій. Модулі `timeit` та `cProfile` дозволяють вимірювати час виконання коду, а також аналізувати використання процесора та пам'яті.

Python також легко інтегрується з іншими інструментами та бібліотеками, що можуть бути корисними для аналізу та візуалізації результатів дослідження. Наприклад, бібліотеки NumPy та SciPy надають потужні засоби для числових обчислень та статистичного аналізу, а Matplotlib та Seaborn дозволяють створювати графіки та візуалізації даних.

Нарешті, Python дозволяє швидко розробляти прототипи та експериментальні установки, що є важливим фактором при проведенні наукових досліджень, дозволяючи швидко перевіряти гіпотези та вносити зміни в експериментальний дизайн.

Враховуючи всі ці переваги, Python є оптимальним вибором для проведення експериментального дослідження затратності обчислювальних ресурсів при використанні різних криптографічних шифрів, що застосовуються в АТЗ. Наявність потужних криптографічних бібліотек, простота та читабельність коду, кросплатформність, велика спільнота, можливості профілювання та інтеграції з

іншими інструментами забезпечують ефективність та достовірність отриманих результатів.

Бібліотека filesplit буде використовуватися для поділу інформації на чанки визначених розмірів. Розбиття даних на чанки дозволяє паралелізувати процес шифруванняв непрямому розумінні. Кожен чанк може бути зашифрований незалежно від інших, що значно скорочує загальний час шифрування, особливо на багатоядерних процесорах, навіть якщо сам лгоритм шифрування не підтримує паралелізацію. Бібліотека filesplit забезпечує простий спосіб поділу файлу, що спрощує подальшу паралельну обробку. Бібліотека filesplit надає простий та зручний інтерфейс для поділу файлів на чанки заданого розміру. Вона підтримує різні режими поділу, включаючи поділ за розміром файлу та за кількістю чанків. Це дозволяє легко інтегрувати її в існуючі проекти та швидко реалізувати необхідну функціональність [21].

Обґрунтування використання бібліотеки PyCryptodome для експериментального дослідження затратності обчислювальних ресурсів при використанні різних криптографічних шифрів в АТЗ базується на декількох ключових аспектах [22].

PyCryptodome пропонує комплексну колекцію криптографічних алгоритмів, включаючи як симетричні (AES, DES, Blowfish, ChaCha20), так і асиметричні (RSA, DSA, ECC), функції хешування (SHA-256, SHA-3, BLAKE2), коди автентифікації повідомлень (HMAC), функції генерації ключів (HKDF, scrypt) та багато інших. Це дозволяє проводити експерименти з різними алгоритмами шифрування, що використовуються або потенційно можуть бути використані в АТЗ, та порівнювати їх продуктивність.

Більшість алгоритмів в PyCryptodome реалізовано на чистому Python, що полегшує розуміння їхньої роботи та дозволяє проводити дослідження на рівні коду. Для критичних до продуктивності операцій, таких як блокові шифри, використовуються C-розширення, що забезпечує прийнятну швидкість виконання та є важливим для отримання реалістичних результатів експериментів.

PyCryptodome є форком PyCrypto, який тривалий час не підтримувався. PyCryptodome активно розвивається та оновлюється, що гарантує виправлення помилок, додавання нових функцій та підтримку сучасних криптографічних стандартів. Це забезпечує актуальність та безпеку використання бібліотеки в дослідженнях.

Бібліотека має добре документований та інтуїтивно зрозумілий інтерфейс програмування (API), що спрощує розробку експериментального коду та зменшує час на його налагодження. Це особливо важливо при проведенні складних експериментів з великою кількістю параметрів.

PyCryptodome підтримує різні операційні системи (Windows, macOS, Linux), що дозволяє проводити експерименти на різному обладнанні та порівнювати результати.

Бібліотека надає доступ до низькорівневих криптографічних операцій, таких як операції з бітами та байтами, що може бути корисним для дослідження оптимізацій та атак на криптографічні алгоритми.

PyCryptodome розробляється з урахуванням вимог безпеки та проходить регулярні перевірки. Хоча жодна криптографічна бібліотека не може гарантувати абсолютної безпеки, використання PyCryptodome зменшує ризик використання вразливих алгоритмів або реалізацій.

PyCryptodome є проектом з відкритим вихідним кодом, що дозволяє перевіряти його роботу, вносити зміни та адаптувати під свої потреби.

Бібліотека має велику спільноту користувачів та розробників, що забезпечує доступ до великої кількості інформації, прикладів коду та допомоги у вирішенні проблем.

В контексті експерименту з затратністю обчислювальних ресурсів, PyCryptodome дозволяє реалізувати різні алгоритми шифрування з мінімальними зусиллями, точно вимірювати час виконання різних криптографічних операцій, порівнювати продуктивність різних алгоритмів на одному й тому ж обладнанні та досліджувати вплив різних параметрів (розмір ключа, режим шифрування, розмір блоку) на продуктивність.

Для запуску написаних на Python скриптів, які проводитимуть шифрування, будуть використовуватися Docker-контейнери.

Docker-контейнери створюють ізольоване середовище виконання для кожної експериментальної установки. Це означає, що експерименти проводяться в контрольованих умовах, незалежно від операційної системи хоста та встановленого на ній програмного забезпечення. Ізоляція гарантує відсутність конфліктів між різними залежностями програмного забезпечення та забезпечує відтворюваність результатів експериментів на різних машинах. Це критично важливо для наукових досліджень, де повторюваність є ключовим критерієм достовірності.

Docker дозволяє чітко визначати та обмежувати обсяг обчислювальних ресурсів, доступних для кожного контейнера. Можливо задавати ліміти для використання центрального процесора (CPU), оперативної пам'яті (RAM), дискового вводу-виводу (I/O) та мережевої пропускної здатності (див. рис. 3.1). Ця функціональність є надзвичайно важливою для експериментів з вимірювання затрат ресурсів, оскільки дозволяє створювати стандартизовані умови, забезпечуючи однакові обмеження ресурсів для всіх експериментів, що дає змогу коректно порівнювати результати, отримані на різних машинах або в різний час.

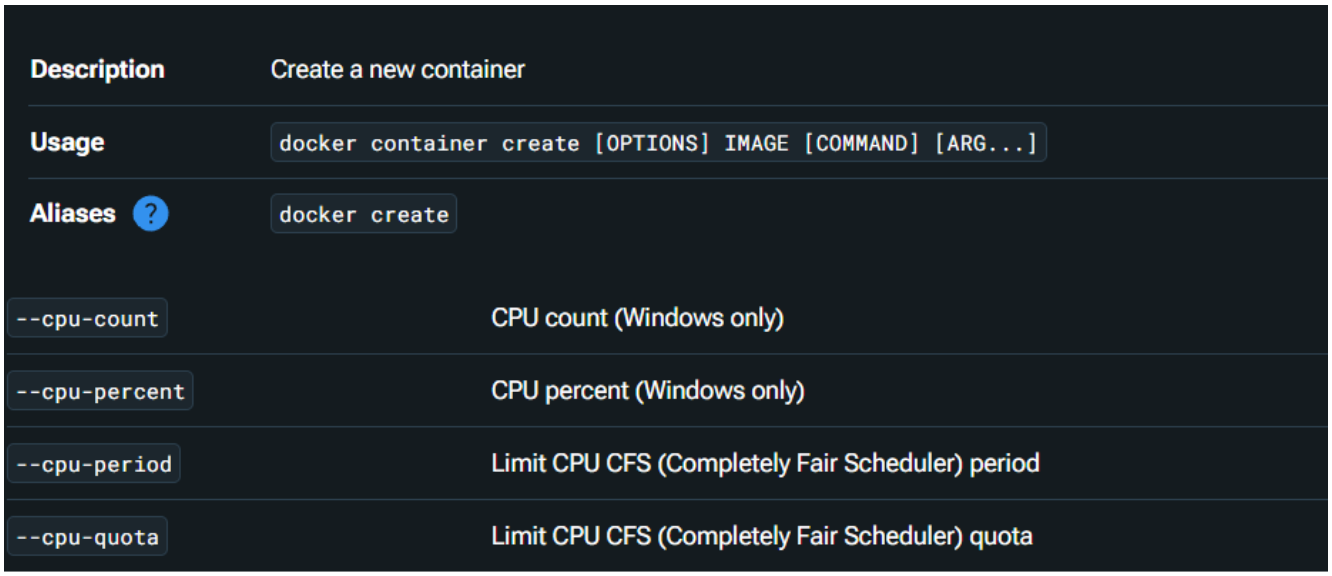

Рисунок 3.1 – Документація команди створення контейнерів

Також це дозволяє імітувати роботу на пристроях з обмеженими ресурсами, що є актуальним для АТЗ, де обчислювальні потужності можуть бути обмеженими, та запобігати виснаженню ресурсів хоста, оскільки обмеження ресурсів для контейнерів запобігає ситуації, коли один експеримент монополізує всі ресурси хост-машини, впливаючи на інші процеси або експерименти.

Docker-контейнери дозволяють легко пакувати Python-скрипти разом з усіма необхідними залежностями (бібліотеками, пакетами тощо) в єдиний образ. Цей образ можна легко переносити між різними машинами та запускати на них без додаткової конфігурації. Для запуску Python-скриптів всередині контейнера достатньо використовувати стандартний інтерпретатор Python, встановлений в образі. Це значно спрощує процес розробки, тестування та розгортання експериментального програмного забезпечення.

Docker дозволяє версіонувати образи контейнерів, що дає можливість відстежувати зміни в експериментальному середовищі та повертатися до попередніх версій у разі потреби. Крім того, використання Dockerfile для створення образів дозволяє чітко описувати всі залежності проекту, що спрощує відтворення експериментального середовища та запобігає проблемам з несумісністю версій бібліотек.

Використання Docker дозволяє легко масштабувати експерименти, запускаючи кілька контейнерів одночасно на одній або кількох машинах. Це дає можливість значно скоротити час проведення експериментів, особливо при дослідженні великої кількості параметрів або алгоритмів.

Docker-контейнери є портативними та можуть запускатися на різних операційних системах (Linux, Windows, macOS), за умови встановлення Docker Engine. Це забезпечує гнучкість у виборі апаратного забезпечення для проведення експериментів.

Таким чином, використання Docker-контейнерів є оптимальним рішенням для проведення експерименту з дослідження затратності обчислювальних ресурсів криптографічних шифрів, оскільки вони забезпечують ізоляцію, контроль ресурсів, простоту розгортання Python-скриптів, версіонування, масштабованість та

портативність [23]. Особливо важливим є можливість відведення конкретної кількості обчислювальних ресурсів під кожен контейнер, що дозволяє проводити коректні та відтворювані вимірювання в контексті експерименту.

3.2 Методика експерименту

Дослідження цієї роботи спрямоване на порівняльний аналіз продуктивності різних режимів роботи алгоритму симетричного блочного шифрування AES в умовах обмежених обчислювальних ресурсів, тому головним етапом дослідження є проведення дослідницького експерименту.

Для забезпечення ізоляції та контролю ресурсів використовується технологія контейнеризації Docker. Створюється Docker-контейнер з жорстко заданими обмеженнями: одне віртуальне ядро CPU з 1.2 Ггц частоти та 1024 МБ оперативної пам'яті. Важливо зафіксувати точну версію Docker Engine та операційної системи хост-машини, на якій запускається контейнер, для забезпечення відтворюваності результатів на інших системах.

В середині Docker-контейнера встановлюється операційна система (рекомендується мінімальний дистрибутив Linux, наприклад, Alpine Linux або Debian slim) та необхідне програмне забезпечення. Встановлюється інтерпретатор Python (версія 3.7 або вище) та криптографічна бібліотека `pycryptodome` (або `cryptography`), з фіксацією точних версій встановлених пакетів за допомогою `pip freeze > requirements.txt`. Це дозволить відтворити програмне оточення.

Розробляється Python-скрипт, який реалізує повний цикл експерименту, використовуючи згадані раніше бібліотеки.

Для забезпечення репрезентативності результатів створюється набір випадкових бінарних файлів випадкових різних розмірів. Це дозволить дослідити вплив розміру файлу на продуктивність шифрування. Для генерації випадкових даних можна використовувати функцію `os.urandom()` в Python. Файли зберігаються у окремій директорії, шлях до якої передається як параметр скрипту.

Досліджуються наступні режими роботи AES: ECB (Electronic Codebook), CBC (Cipher Block Chaining), CFB (Cipher Feedback), OFB (Output Feedback) та CTR (Counter). Важливо зазначити особливості кожного режиму та їхні потенційні вразливості.

Для кожного згенерованого файлу, для кожного режиму шифрування та для кожного розміру чанку виконується задана кількість незалежних шифрувань (N). В межах експерименту кількість заданих шифрувань дорівнюватиме 10.

Під час кожного шифрування збираються наступні метрики з високою точністю:

– час виконання шифрування: вимірюється час, витрачений на операцію шифрування, з точністю до мілісекунд, використовуючи функцію `time.perf_counter()` в Python, яка забезпечує високу точність вимірювання часу. Вимірюється час від початку операції шифрування до її повного завершення.

– максимальне споживання оперативної пам'яті: вимірюється максимальний обсяг оперативної пам'яті, який був використаний процесом шифрування протягом виконання. Для цього використовуються вбудовані інтерфейсні інструменти Docker.

– середнє завантаження процесора: вимірюється середній відсоток завантаження процесора протягом операції шифрування. Для цього також застосовуються вбудовані інтерфейсні інстурменти Docker.

Усі зібрані дані зберігаються у структурованому форматі, наприклад, у Excel-таблицю.

Для кожного набору параметрів (режим шифрування, розмір чанку, розмір файлу) обчислюються середні значення для кожної з виміряних метрик.

Результати візуалізуються за допомогою графіків, наприклад, графіки залежності часу шифрування від розміру чанку для різних режимів, графіки споживання пам'яті та завантаження CPU.

Проводиться аналіз даних, щоб зробити обґрунтовані висновки про вплив досліджуваних факторів. Визначаються можливі напрямки подальших досліджень,

наприклад, дослідження впливу інших параметрів, таких як довжина ключа, або дослідження інших криптографічних алгоритмів.

3.3 Аналіз результатів

Для наочного представлення результатів експериментальних досліджень, що відображають вплив різних режимів шифрування AES та розмірів чанків на продуктивність в умовах обмежених обчислювальних ресурсів, отримані дані було зведено у три окремі таблиці. Ці таблиці містять усереднені значення ключових метрик продуктивності, отримані в результаті серії експериментів.

Перша таблиця (див. табл. 3.1) демонструє залежність часу, витраченого на шифрування, від комбінації режиму роботи AES (ECB, CBC, CFB, OFB, CTR) та розміру чанку даних. Дані в цій таблиці відображають середній час шифрування для кожного поєднання параметрів, отриманий після 10 повторних запусків експерименту, що дозволяє оцінити швидкодію різних режимів при обробці даних, розділених на чанки різного розміру. Аналіз цієї таблиці дозволяє виявити найбільш швидкі та повільні режими шифрування для різних розмірів чанків.

Таблиця 3.1 – Середні значення затраченого на шифрування часу, мс

File Size (KB)	ECB	CBC	CFB	OFB	CTR
500	95.21185	102.0275	109.7886	93.86719	103.1466
1500	98.4888	92.93154	128.3425	128.5103	105.0564
2200	198.6461	196.9985	230.7818	223.3263	218.0577
8000	678.015	682.962	647.7431	768.4193	789.0139
15000	1222.491	1511.968	1683.561	1421.722	1388.774
32000	2262.262	2698.022	2810.984	2978.244	2755.277

Друга таблиця (див. табл. 3.2) відображає середній обсяг оперативної пам'яті, використаний процесом шифрування для кожного поєднання режиму AES та розміру чанку. Ця таблиця надає інформацію про ефективність використання пам'яті різними режимами та дозволяє оцінити їх вимогливість до ресурсів системи.

Порівняння даних з таблиці 3.1 та таблиці 3.2 дозволяє зробити висновки про компроміс між швидкістю шифрування та споживанням пам'яті для різних режимів.

Таблиця 3.2 – Середні значення максимальних затрат RAM, Kb

File Size (KB)	ECB	CBC	CFB	OFB	CTR
500	0.012374	0.012708	0.012967	0.011879	0.013088
1500	0.011605	0.012948	0.01595	0.015655	0.012454
2200	0.025336	0.023632	0.027404	0.031288	0.028617
8000	0.083245	0.0935	0.085224	0.090168	0.094973
15000	0.160077	0.188281	0.230692	0.164645	0.181721
32000	0.318595	0.346757	0.343375	0.405583	0.360861

Третя таблиця (див. табл. 3.3) містить інформацію про середнє завантаження центрального процесора під час виконання операції шифрування для кожного поєднання режиму AES та розміру чанку. Ця таблиця дозволяє оцінити навантаження на процесор при використанні різних режимів та розмірів чанків, що є важливим фактором для ресурс-обмежених систем. Аналізуючи дані з усіх трьох таблиць разом, можна отримати повну картину впливу різних режимів шифрування AES та розмірів чанків на продуктивність системи в умовах обмежених ресурсів.

Таблиця 3.3 – Середні значення нагрузки CPU, %

File Size (KB)	ECB	CBC	CFB	OFB	CTR
500	1.007533	1.373175	1.37459	1.045358	0.925105
1500	1.244368	0.831611	1.376853	1.109099	1.122984
2200	2.398532	2.44987	2.906077	2.857182	2.302735
8000	9.003752	8.522686	8.216254	8.902325	10.53138
15000	15.79902	20.95592	21.73288	18.76428	16.73752
32000	30.65792	35.27031	37.2083	36.04184	36.8882

Для візуалізації отриманих результатів та полегшення їхнього аналізу було створено набір стовпчикових діаграм, по одній для кожної з трьох розглянутих метрик продуктивності: часу шифрування, споживання оперативної пам'яті та завантаження процесора. Ці діаграми дозволяють наочно порівняти вплив різних режимів шифрування AES та розмірів чанків даних на кожну з цих метрик.

На рисунку 3.2 представлено залежність часу шифрування від режиму роботи AES (ECB, CBC, CFB, OFB, CTR) для різних розмірів чанків. Кожен стовпчик на діаграмі відповідає певному поєднанню режиму та розміру чанку, а його висота відображає середній час, витрачений на шифрування. Цей рисунок дозволяє швидко ідентифікувати режими, які демонструють найвищу та найнижчу швидкість шифрування для різних розмірів чанків, а також оцінити вплив розміру чанку на продуктивність кожного режиму. Зокрема, можна візуально порівняти, як зміна розміру чанку впливає на час шифрування для кожного з режимів, та виявити оптимальні розміри чанків для досягнення найкращої швидкодії.

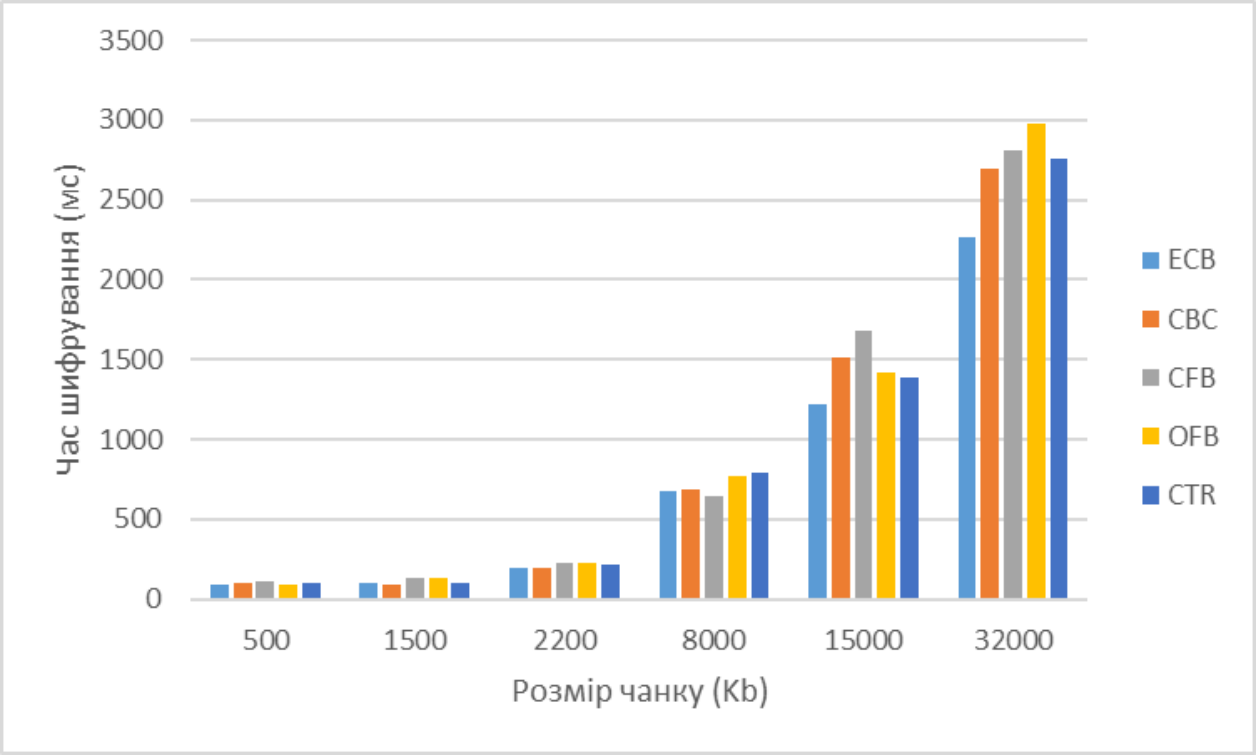

Рисунок 3.2 – Час шифрування для різних режимів роботи AES

На рисунку 3.3 відображено середній обсяг оперативної пам'яті, спожитий процесом шифрування для різних комбінацій режиму AES та розміру чанку. Аналогічно до попереднього рисунка, кожен стовпчик відповідає певному поєднанню параметрів, а його висота показує середнє споживання пам'яті. Цей рисунок дозволяє оцінити вимоги різних режимів до пам'яті та виявити режими, які є найбільш та найменш ресурсозатратними. Порівнюючи рисунок 3. та рисунок 3. ,

можна проаналізувати компроміс між швидкістю шифрування та споживанням пам'яті для різних режимів та розмірів чанків.

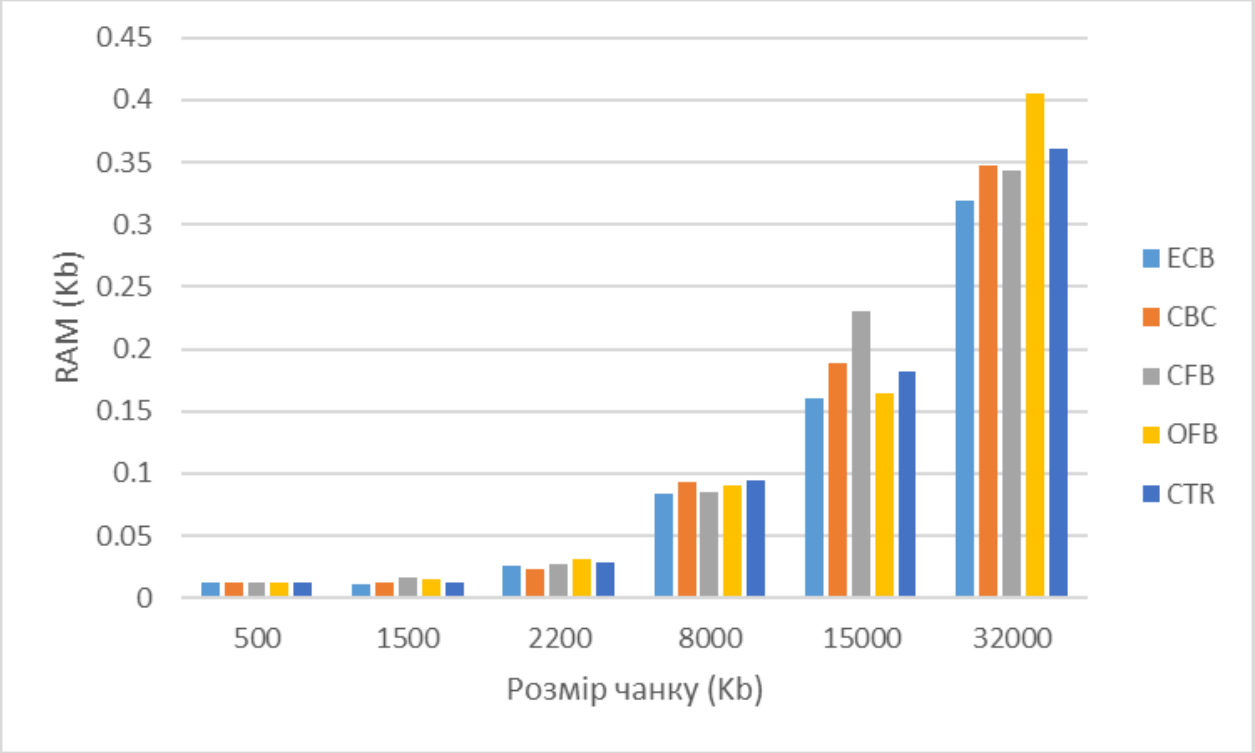

Рисунок 3.3 – Максимальні затрати RAM для різних режимів роботи AES

На рисунку 3.4 показано середнє завантаження центрального процесора під час виконання операції шифрування для різних режимів AES та розмірів чанків. Цей рисунок дає уявлення про навантаження на процесор при використанні різних параметрів шифрування. Аналізуючи цей рисунок разом з рис. 3. та рис. 3. , можна отримати повну картину впливу різних режимів та розмірів чанків на продуктивність системи в цілому, враховуючи як швидкість, так і споживання ресурсів.

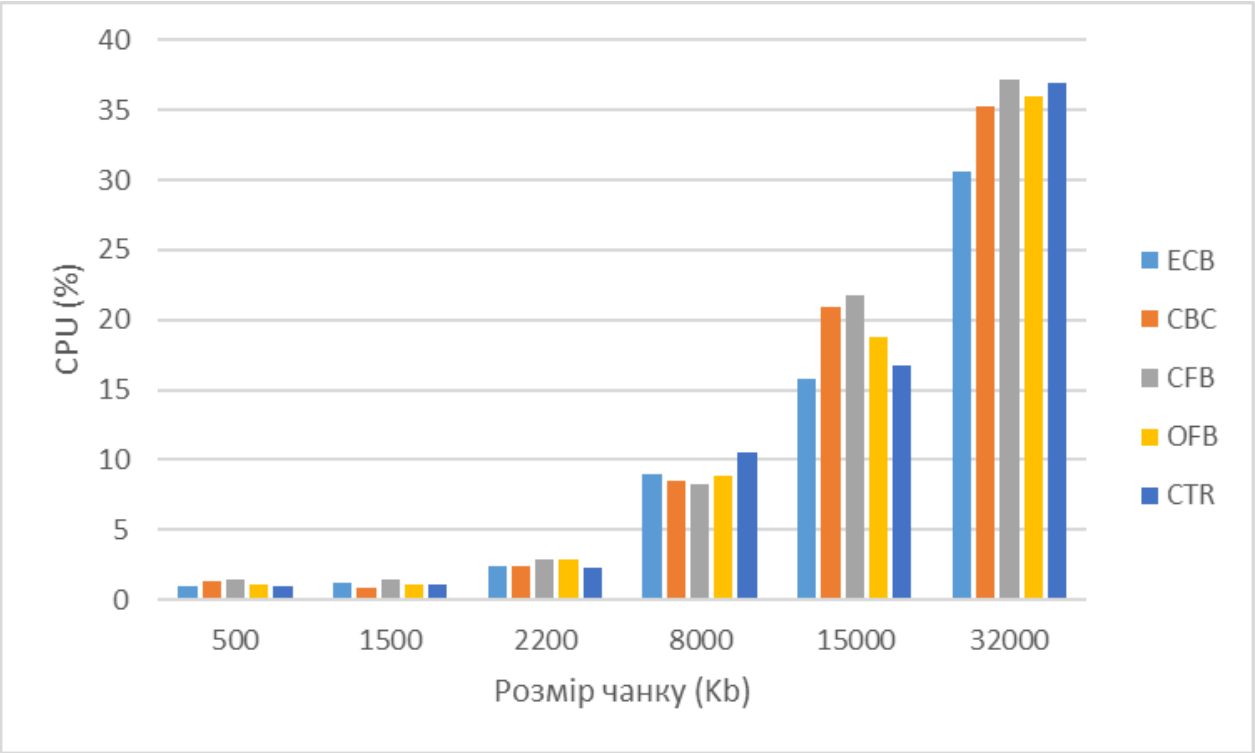

Рисунок 3.4 – Середні нагрузки CPU для різних режимів роботи AES

Для спрощення порівняльного аналізу та наочного визначення найбільш ефективного режиму шифрування AES, середні значення виміряних метрик (час шифрування, споживання оперативної пам'яті та завантаження процесора) було нормалізовано та представлено у вигляді відносних відсоткових значень. Цей підхід дозволив звести дані до єдиної шкали та усунути вплив абсолютних значень, що значно полегшило порівняння різних режимів між собою. Для кожної метрики було побудовано окрему стовпчикову діаграму, де кожен стовпчик відповідає одному з режимів роботи AES (ECB, CBC, CFB, OFB, CTR), а його висота відображає нормалізоване відсоткове значення.

На рисунку 3.5 представлено відносний час, витрачений на шифрування, для кожного режиму. Нормалізація даних дозволила порівняти швидкість шифрування різних режимів без урахування абсолютних значень часу. Аналізуючи цей рисунок, можна чітко визначити режим, який демонструє найменший відносний час шифрування, що свідчить про його найвищу швидкодію. Режими з більшими відносними значеннями часу шифрування, відповідно, є менш ефективними з точки зору швидкості.

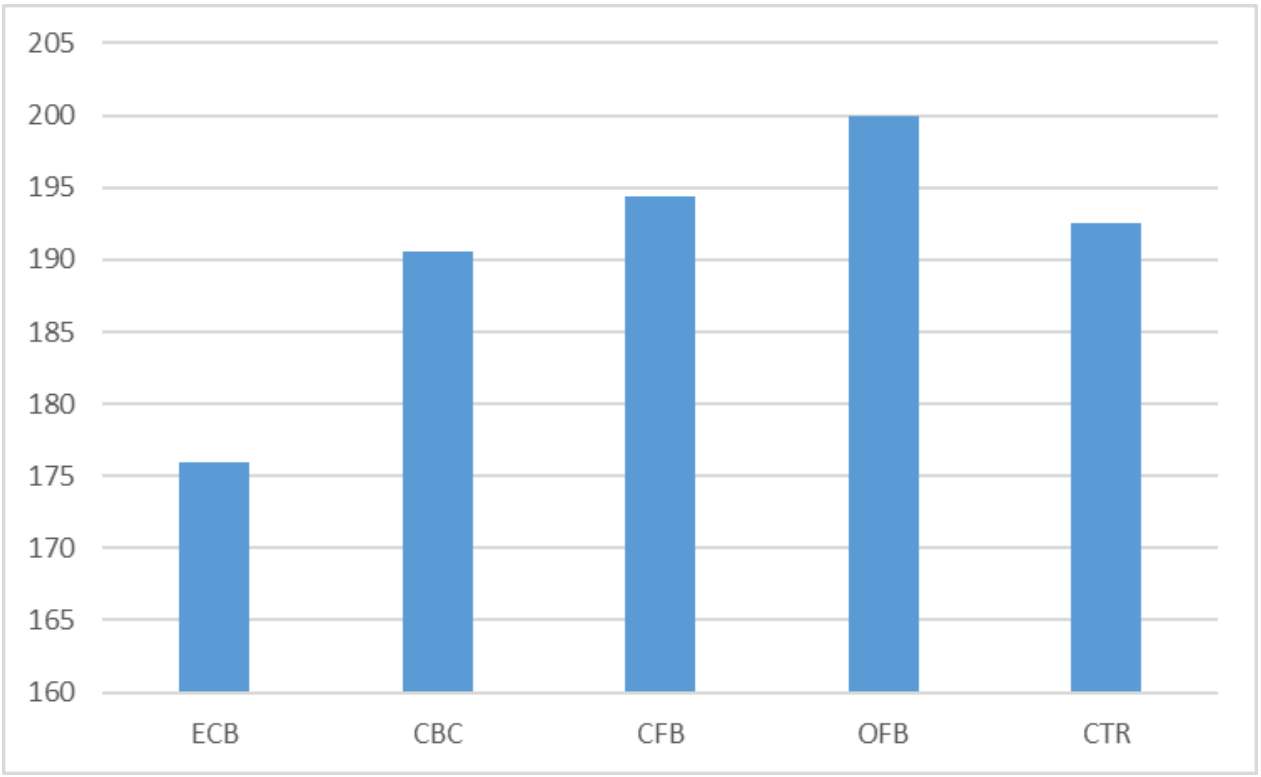

Рисунок 3.5 – Нормалізовані відносні значення часу шифрування

Рисунок 3.6 відображає відносне споживання пам'яті для кожного режиму. Нормалізація даних дозволила порівняти вимоги різних режимів до оперативної пам'яті. На цьому рисунку можна ідентифікувати режим, який потребує найменше пам'яті, що є критично важливим для ресурс-обмежених систем. Режими з більшими відносними значеннями споживання пам'яті є менш ефективними з точки зору використання пам'яті.

На рисунку 3.7 показано відносне завантаження центрального процесора під час шифрування для кожного режиму. Нормалізація даних дозволила порівняти навантаження на процесор, яке створюють різні режими. Аналіз цього рисунка дозволяє визначити режим, який створює найменше навантаження на процесор, що є важливим для забезпечення енергоефективності та запобігання перегріву системи.

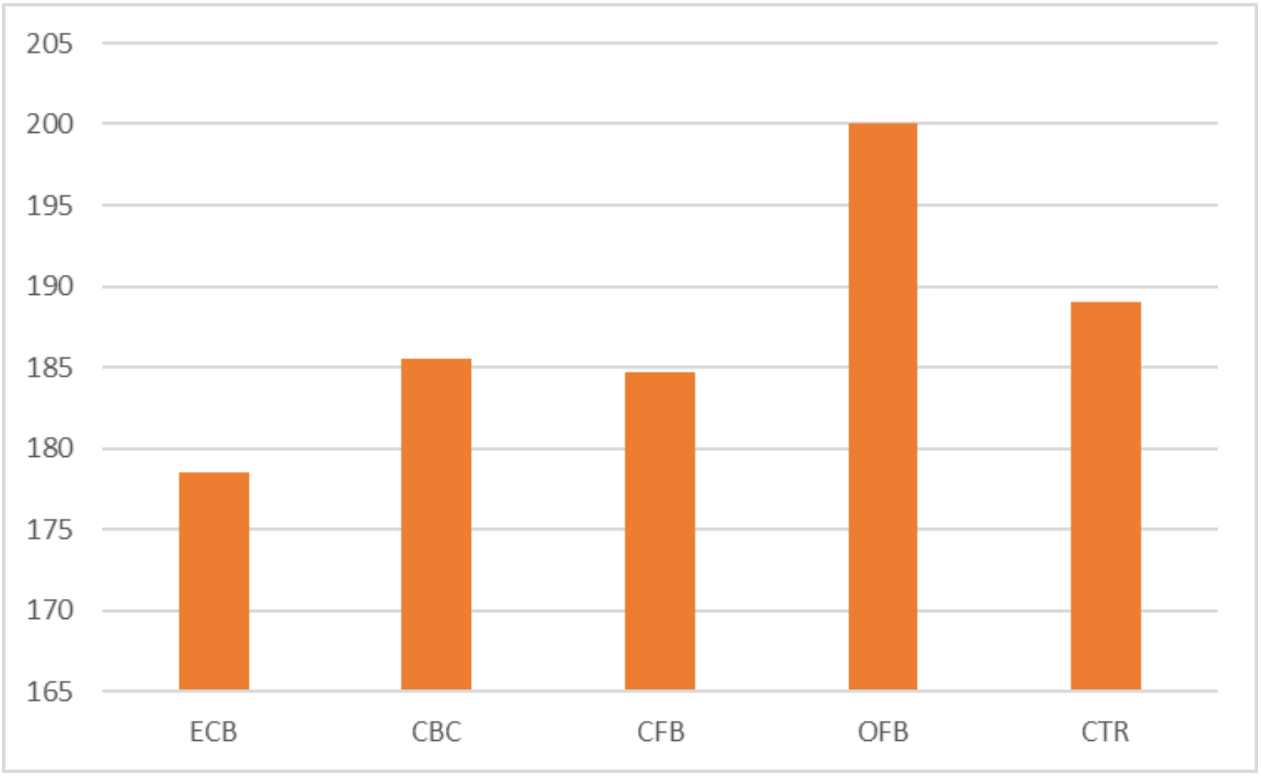

Рисунок 3.6 – Нормалізовані відносні значення затраченої RAM

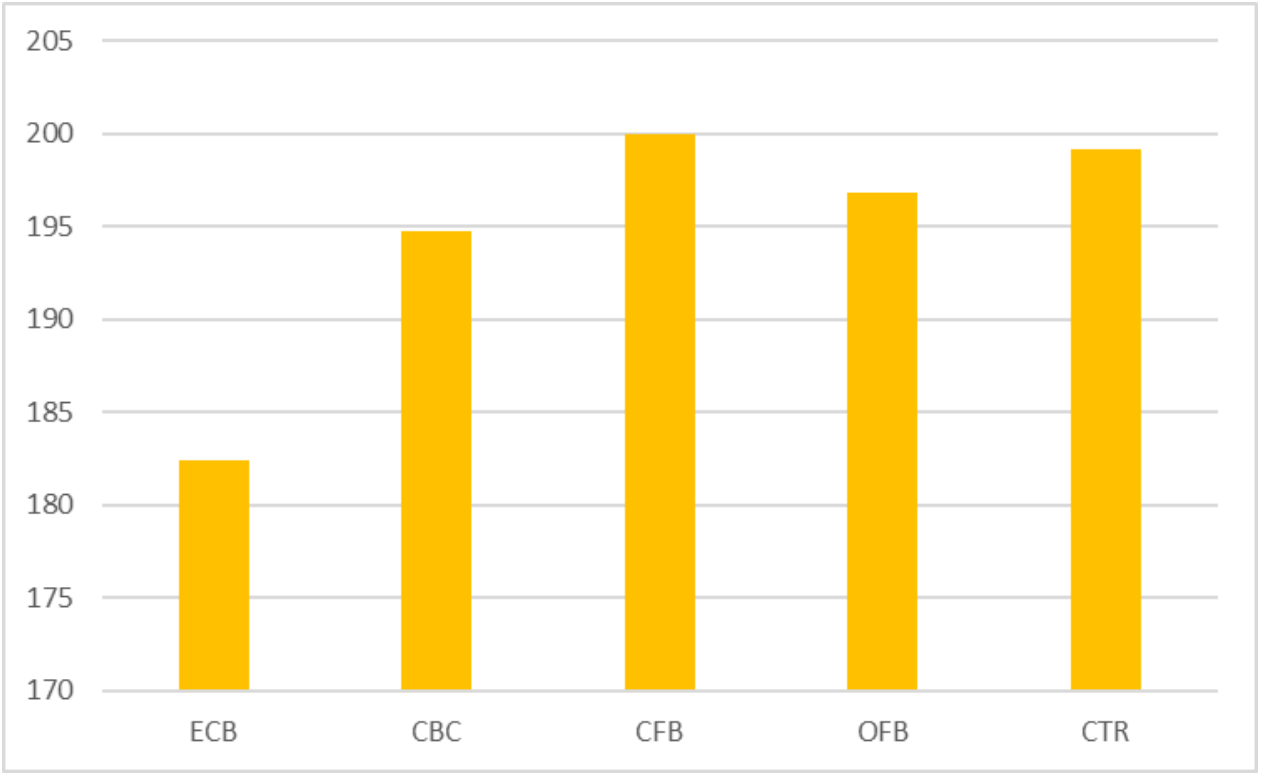

Рисунок 3.7 – Нормалізовані відносні значення нагрузки CPU

Порівнюючи рисунки 3.5 , 3.6 та 3.7 разом, можна отримати комплексну оцінку ефективності кожного режиму AES. Режим з найменшими відносними значеннями для всіх трьох метрик (час шифрування, споживання пам'яті та завантаження процесора) є найбільш ефективним з точки зору загальної продуктивності та використання ресурсів. Цей підхід дозволяє зробити обґрунтований вибір оптимального режиму шифрування для конкретних умов та вимог.

На основі візуалізації діаграм, можна дійсти висновку, що режим ECB демонструє найкращі результати по усіх показниках, проте він не рекомендується для використання через те, що однакові блоки відкритого тексту шифруються в однакові блоки шифрованого тексту при використанні одного ключа, що робить його вразливим до криптоаналізу та розкриття структури даних. Незважаючи на те, що він є частиною стандарту, його використання вводить суттєві вразливості. Тому відкидаючи режим ECB, наступним найбільш ефективним режимом є CBC.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою даної роботи є дослідження ефективності використання обмежених обчислювальних ресурсів автономного транспортного засобу при різних режимах роботи криптографічного шифру. Оскільки, проведення даного дослідження передбачає використання комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників з даного дослідження необхідно організувати безпечні умови праці. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Згідно Вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог:

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути

оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, ДБН В.2.5-56:2010, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп'ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п'ять комп'ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп'ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні має бути зворотним. Не допускається підключати комп'ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп'ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

Важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18. Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги». Відстань від екрана до ока фахівців, які працюють за комп'ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп'ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

Отже, у результаті аналізу вимог щодо охорони праці користувачів комп'ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної

роботи інженерів з розробки та впровадження системи резервування та керування трафіком.

4.2 Безпека в надзвичайних ситуаціях

Державна система моніторингу довкілля, як складова частина національної інформаційної інфраструктури, сумісної з аналогічними системами інших країн.

Законодавство України, а саме Статті 20 та 22 Закону України «Про охорону навколишнього природного середовища» [24], передбачають створення державної системи моніторингу довкілля та проведення спостережень за станом навколишнього природного середовища і рівнем його забруднення. Основні принципи функціонування державної системи моніторингу довкілля визначені у постанові Кабінету Міністрів України від 30.03.1998 №391 «Про затвердження Положення про державну систему моніторингу довкілля» [25]. Згідно з цим положенням, «Державна система моніторингу довкілля (ДСМД) – це система спостережень, збирання, оброблення, передавання, збереження та аналізу інформації про стан довкілля, прогнозування його змін і розроблення науково-обґрунтованих рекомендацій для прийняття рішень про запобігання негативним змінам стану довкілля та дотримання вимог екологічної безпеки».

Також визначається, що система моніторингу є відкритою інформаційною системою, складовою частиною національної інфраструктури, сумісної з аналогічними системами інших країн.

Пріоритетами такої системи є збереження екосистем, відвернення кризових змін в екологічному стані довкілля та запобігання відповідним надзвичайним ситуаціям. На даний час, у ДСМД функції і задачі спостережень та інформаційного забезпечення виконують такі суб`єкти системи моніторингу [25]:

- Міністерство захисту довкілля та природних ресурсів України;
- Міністерство аграрної політики та продовольства України;
- Міністерство розвитку громад і територій України;
- Державна служба з надзвичайних ситуацій;

- Державна служба геології та надр України;
- Державне агентство України з управління зоною відчуження;
- Державне агентство лісових ресурсів України;
- Державне агентство водних ресурсів України;
- Державна служба України з питань геодезії, картографії та кадастру;
- Державне космічне агентство України.

Окрім цього, виконання таких функцій покладено на інші центральні органи виконавчої влади, які є суб'єктами державної системи моніторингу довкілля, а також на підприємства, установи та організації, діяльність яких призводить або може призвести до погіршення стану довкілля. В загальному, система моніторингу спрямована на декілька основних цілей, серед яких підвищення рівня вивчення і знань про екологічний стан довкілля, зростання якості інформаційного обслуговування користувачів на всіх рівнях, покращення якості обґрунтування природоохоронних заходів та ефективності їх здійснення, а також сприяння розвитку міжнародного співробітництва у галузі охорони довкілля, раціонального використання природних ресурсів та екологічної безпеки [25].

Для досягнення поставлених цілей, положення про ДСМД визначає такі завдання: систематичні спостереження за станом довкілля, аналіз стану навколишнього середовища, прогнозування змін довкілля, інформаційна підтримка прийняття рішень, забезпечення органів державної та місцевої влади, населення та партнерів інформацією про актуальний стан довкілля [25]. Також згідно з положенням складовими частинами державного моніторингу навколишнього середовища України є моніторинг атмосферного повітря, води, земель, біологічного різноманіття, лісів, відходів, геологічного середовища, фізичних факторів впливу.

Нормативними актами, що регламентують моніторинг таких об’єктів є відповідні постанови Кабінету Міністрів України щодо порядків здійснення моніторингу повітря, вод, земель та ґрунтів. Система моніторингу ґрунтується на використанні існуючих організаційних структур суб'єктів моніторингу і функціонує на основі єдиного нормативного, організаційного, методологічного і метрологічного забезпечення, об'єднання складових частин та уніфікованих

компонентів цієї системи [26]. Зазначимо, що функціонування ДСМД здійснюється на трьох рівнях, які розподіляються за територіальним принципом, а саме: загальнодержавний, регіональний та локальний рівні.

Відповідальні суб'єкти здійснюють моніторинг різного роду об'єктів, серед яких [25]:

- ґрунти на природоохоронних територіях, а також ґрунти сільськогосподарського та лісового фондів;

- види рослинного і тваринного світу, що перебувають під загрозою зникнення чи під особливою охороною;

- вміст радіонуклідів в атмосферному повітрі, водах та ґрунтах;

- наявність та серйозність повеней, паводків, снігових лавин, селів;

- об'єкти зберігання та захоронення радіоактивних відходів;

- сільськогосподарські рослини, тварини і продуктів з них, мисливська фауна та лісова рослинність;

- якість вод водогосподарських систем міжгалузевого та сільськогосподарського водопостачання;

- зрошувані та осушувані землі у сенсі глибини залягання та мінералізації ґрунтових вод, ступені засоленості та солонцюватості ґрунтів;

- ґрунти і ландшафти щодо проявів ерозійних та інших екзогенних процесів та просторового забруднення земель об'єктами промислового і сільськогосподарського виробництва;

- берегові лінії річок, морів, озер, водосховищ, лиманів, заток, гідротехнічних споруд;

- стічні води міської каналізаційної мережі та очисні споруди, джерела скидання таких вод;

- зелені насадження у містах і селищах міського типу.

Якщо розглянути моніторинг повітря, то Державною гідрометеорологічною службою здійснюється спостереження за забрудненням атмосферного повітря у містах України. Державна екологічна інспекція здійснює відбір проб на джерелах викидів, а санітарно-епідеміологічна служба координує моніторинг якості

атмосферного повітря у житлових зонах. Контроль якості повітря також включає аналіз опадів та снігового покрову. Програма обов`язкового моніторингу якості атмосферного повітря охоплює сім забруднюючих речовин: пил, двоокис азоту, двоокис сірки, оксид вуглецю, формальдегід, свинець та бензапірен. Спостереження за водами суші на 151 об’єкті проводить Державна гідрометеорологічна служба, що включає в себе оцінку хімічного складу вод, біогенних параметрів, наявність зважених часток та органічних речовин, основних забруднюючих речовин, важких металів та пестицидів. Контроль за водами суші також здійснюють Державна екологічна інспекція, Державний комітет по водному господарству, Санітарно-епідеміологічна служба та Державна геологічна служба. Дослідження включають моніторинг річок, водосховищ, каналів тощо, контроль хімічних, радіаційних та фізичних показників, а також придатності води до споживання. За схожими параметрами відбувається й моніторинг прибережних вод. До моніторингу ґрунтів входить вимірювання забруднення ґрунтів пестицидами, агровідходами, токсинами та важкими металами на сільськогосподарських землях та промислових майданчиках. Також досліджується забруднення ґрунту у місцях захоронення відходів. Контроль здійснюється державною гідрометеорологічною службою, Міністерством захисту довкілля та Міністерством аграрної політики. Моніторинг радіаційного випромінювання включає в себе спостереження за радіоактивним забрудненням атмосфери, поверхневих вод та ґрунтів поблизу атомних електростанцій та у зоні відчуження [25].

Згідно з положенням [24] суб’єкти системи моніторингу інформаційно підтримують рішення в галузі охорони довкілля, безкоштовно обмінюються результатами спостережень на об’єктах та колективно використовують інформаційні ресурси, надаючи всім зацікавленим сторонам відповідні дані.

ВИСНОВКИ

Кібербезпека є критично важливим аспектом для безпечної експлуатації АТЗ. Зі зростанням рівня автономності та їх інтеграції в мережу, АТЗ стають все більш вразливими до кібератак, що можуть призвести до порушення приватності користувачів, втрати контролю над транспортним засобом та навіть до створення аварійних ситуацій.

Захист даних та комунікацій є ключовим елементом забезпечення кібербезпеки АТЗ. Застосування надійних протоколів шифрування та передачі даних, таких як TLS, IPsec, DTLS та MACsec, а також криптографічних алгоритмів, зокрема AES, RSA та ECDSA, є необхідним для гарантування конфіденційності, цілісності та автентичності інформації, що циркулює між компонентами АТЗ та зовнішніми системами.

Для забезпечення інформаційної безпеки АТЗ необхідний комплексний підхід, що охоплює захист на різних рівнях: від окремих компонентів та комунікаційних каналів до програмного забезпечення та системи в цілому. Важливим є впровадження не лише технічних рішень, але й організаційних та процедурних заходів, таких як керування ключами шифрування, своєчасне оновлення програмного забезпечення та навчання персоналу.

Стандартизація та нормативне регулювання відіграють значну роль у забезпеченні кібербезпеки АТЗ. Міжнародні стандарти, наприклад ISO/SAE 21434, та рекомендації, такі як SAE J3061, встановлюють вимоги та настанови, що сприяють уніфікації підходів та підвищенню рівня захисту.

Інтеграція АТЗ в екосистему Інтернету речей (IoT) створює нові виклики для кібербезпеки, оскільки розширює потенційну поверхню атаки. Захист має охоплювати не лише сам АТЗ, але й всю екосистему його функціонування, враховуючи специфічні загрози, пов'язані з IoT.

При виборі методів захисту необхідно враховувати обмежені обчислювальні ресурси, характерні для вбудованих систем АТЗ, та вплив криптографічних методів

на продуктивність. Важливо знайти баланс між вимогами до безпеки та продуктивності, ретельно підбираючи алгоритми та протоколи.

Ефективна протидія кіберзагрозам потребує постійного моніторингу та оновлення системи безпеки. З огляду на постійну еволюцію кіберзагроз, необхідно забезпечити оперативне виявлення та реагування на нові атаки, а також своєчасне оновлення програмного забезпечення та криптографічних протоколів.

За результатами проведеного експериментального дослідження, спрямованого на порівняльний аналіз продуктивності режимів шифрування AES в умовах обмежених обчислювальних ресурсів, було встановлено, що режим CBC (Cipher Block Chaining) демонструє найкращу загальну ефективність. Аналіз нормалізованих даних щодо часу шифрування, споживання оперативної пам'яті та завантаження процесора показав, що саме CBC забезпечує оптимальний баланс між цими трьома ключовими показниками. Це свідчить про те, що CBC є найбільш ефективним вибором для систем, що мають обмеження в ресурсах. Важливо зазначити, що режим ECB (Electronic Codebook) не брався до уваги при формулюванні висновків щодо ефективності через свою відому ненадійність та вразливість до криптоаналізу, що робить його непридатним для практичного використання в будь-яких сценаріях, де потрібна криптографічна безпека. Таким чином, експериментально підтверджено, що в умовах обмежених ресурсів режим CBC є оптимальним рішенням, забезпечуючи належний рівень продуктивності.

Таким чином, забезпечення інформаційної безпеки АТЗ є складним, але досяжним завданням, що вимагає комплексного підходу, який поєднує використання надійних технологій, дотримання стандартів та постійний моніторинг. Це є необхідною умовою для безпечної та надійної експлуатації автономних транспортних засобів в сучасному інформаційному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Демчишин, М., Тимощук, В., Шиманська, В., & Тимощук, Д. (2024). Кіберзагрози сенсорним підсистемам автономних транспортних засобів. In Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя (pp. 135–136). Тернопільський національний технічний університет імені Івана Пулюя.

2. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми, Україна), 191-193.

3. Mecheva, T., & Kakanakov, N. (2020). Cybersecurity in intelligent transportation systems. Computers, 9(4), 83. https://doi.org/10.3390/computers9040083

4. Ahmad, M., Farid, M. A., Ahmed, S., Saeed, K., Asharf, M., & Akhtar, U. (2019). Impact and detection of GPS spoofing and countermeasures against spoofing. In 2019 2nd international conference on computing, mathematics and engineering technologies (icomet). IEEE. https://doi.org/10.1109/icomet.2019.8673518

5. Hamza, G., Taher, Y., Es-sadek, M. Z., & Tmiri, A. (2024). Cybersecurity in autonomous vehicles: A comprehensive review study of cyber-attacks and ai-based solutions. International Journal of Engineering Trends and Technology, 72(1), 101–116. https://doi.org/10.14445/22315381/ijett-v72i1p111

6. Giannaros, A., Karras, A., Theodorakopoulos, L., Karras, C., Kranias, P., Schizas, N., Kalogeratos, G., & Tsolis, D. (2023). Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. Journal of Cybersecurity and Privacy, 3(3), 493–543. https://doi.org/10.3390/jcp3030025

7. Durlik, I., Miller, T., Kostecka, E., Zwierzewicz, Z., & Łobodzińska, A. (2024). Cybersecurity in autonomous vehicles—are we ready for the challenge? Electronics, 13(13), 2654. https://doi.org/10.3390/electronics13132654

8. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., Lechachenko T., (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, pp. 1-11.

9. Luo, F., & Hou, S. (2019). Cyberattacks and countermeasures for intelligent and connected vehicles. SAE International Journal of Passenger Cars - Electronic and Electrical Systems, 12(1). https://doi.org/10.4271/07-12-01-0005

10. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., Tymoshchuk, V., (2024). Detection and classification of DDoS flooding attacks by machine learning methods. CEUR Workshop Proceedings, 3842, pp. 184 - 195.

11. Levinson, J., Askeland, J., Becker, J., Dolson, J., Held, D., Kammel, S., Kolter, J. Z., Langer, D., Pink, O., Pratt, V., Sokolsky, M., Stanek, G., Stavens, D., Teichman, A., Werling, M., & Thrun, S. (2011). Towards fully autonomous driving: Systems and algorithms. In 2011 IEEE intelligent vehicles symposium (IV). IEEE. https://doi.org/10.1109/ivs.2011.5940562

12. ТИМОЩУК, Д., ЯЦКІВ, В., ТИМОЩУК, В., & ЯЦКІВ, Н. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION ENVIRONMENTS. MEASURING AND COMPUTING DEVICES IN TECHNOLOGICAL PROCESSES, (4), 215-220.

13. Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. Transportation Research Part A: Policy and Practice, 124, 523–536. https://doi.org/10.1016/j.tra.2018.06.033

14. Chen, J., Zuo, Q., Jin, W., Wu, Y., Xu, Y., & Xu, Y. (2024). Study of network security based on key management system for in-vehicle ethernet. Electronics, 13(13), 2524. https://doi.org/10.3390/electronics13132524

15. Tu, B., Chen, Y., Cui, H., & Wang, X. (2023). Fast two-party signature for upgrading ECDSA to two-party scenario easily. Theoretical Computer Science, 114325. https://doi.org/10.1016/j.tcs.2023.114325

16. Farooq, U., & Aslam, M. F. (2017). Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an

FPGA. Journal of King Saud University - Computer and Information Sciences, 29(3), 295–302. https://doi.org/10.1016/j.jksuci.2016.01.004

17. Rachmat, N., & Samsuryadi. (2019). Performance analysis of 256-bit AES encryption algorithm on android smartphone. Journal of Physics: Conference Series, 1196, 012049. https://doi.org/10.1088/1742-6596/1196/1/012049

18. Aes modes of operation. (2019). International Journal of Innovative Technology and Exploring Engineering, 8(9), 2213–2217. https://doi.org/10.35940/ijitee.i8127.078919

19. Tymoshchuk, D., & Yatskiv, V. (2024). Slowloris ddos detection and prevention in real-time. Collection of scientific papers «ΛΌГОΣ», (August 16, 2024; Oxford, UK), 171-176.

20. Almuhammadi, S., & Al-Hejri, I. (2017). A comparative analysis of AES common modes of operation. In 2017 IEEE 30th canadian conference on electrical and computer engineering (CCECE). IEEE. https://doi.org/10.1109/ccece.2017.7946655

21. Murad, S., Khan, A., Shiaeles, S., & Masala, G. (2019). Data encryption and fragmentation in autonomous vehicles using raspberry pi 3. In 2019 IEEE world congress on services (SERVICES). IEEE. https://doi.org/10.1109/services.2019.00058

22. Загородна, Н. В., Лупенко, С. А., & Луцків, А. М. (2011). Обґрунтування вибору доступних програмно-апаратних засобів високопродуктивних обчислювальних систем для задач криптоаналізу. Електроніка та системи управління, 1, 42–50.

23. Skorenkyy, Y., Kozak, R., Zagorodna, N., Kramar, O., & Baran, I. (2021). Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. Journal of Physics: Conference Series, 1840(1), 012026. https://doi.org/10.1088/1742-6596/1840/1/012026

24. Про охорону навколишнього природного середовища. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/1264-12 (дата звернення: 18.12.2024).

25. Постанова Кабінету Міністрів України «Про затвердження Положення про державну систему моніторингу довкілля» №391-98-п. URL: https://zakon.rada.gov.ua/laws/show/391-98 (дата звернення: 18.12.2024)

26. Стручок, В. С. (Comp.). (2022). Безпека в надзвичайних ситуаціях. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання. ТНТУ. http://elartu.tntu.edu.ua/handle/lib/39196

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
імені ІВАНА ПУЛЮЯ
НАУКОВЕ ТОВАРИСТВО ім. ШЕВЧЕНКА

М А Т Е Р І А Л И

XII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

18-19 грудня 2024 року

ТЕРНОПІЛЬ
2024

УДК 001
М34

ПРОГРАМНИЙ КОМІТЕТ

Голова: Приймак Микола – професор кафедри комп'ютерних систем та мереж, д.т.н., професор.
Співголови: Марущак Павло – проректор з наукової роботи, докт. техн. наук, професор.
Баран Ігор – канд. техн. наук, доцент, декан факультету ФІС.
Науковий секретар: Надія Крива– старший викладач.

Члени: Василь Кривень - завідувач кафедри математичних методів в інженерії д.ф.-м.н., професор; Галина Осухівська – завідувач кафедри комп'ютерних систем та мереж, к.т.н., доцент; Микола Карпінський - професор кафедри кібербезпеки, д.т.н., професор; Жанна Баб'як - завідувач кафедри української та іноземних мов, к.пед. н., доцент; Ярослав Литвиненко – професор кафедри комп'ютерних наук, д.т.н., професор; Михайло Петрик - завідувач кафедри програмної іженерії, д.ф.-м.н., професор; Наталія Загородна – завідувач кафедри кібербезпеки, к.т.н., доцент.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: Скоренький Юрій Любомирович – канд. техн. наук, доцент кафедри фізики.
Члени: доцент кафедри комп'ютерних наук, к.т.н. В. Никитюк; доцент кафедри програмної інженерії, к.т.н. Д. Михалик; доцент кафедри кібербезпеки, к.т.н. М. Стадник; доцент кафедри комп'ютерних систем та мереж, к.т.н. Є. Тиш; ст. викладач Л. Джиджора.

М34 Матеріали XII науково-технічної конфції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя, (Тернопіль, 18–19 грудня 2024 р.). – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2024.

Адреса оргкомітету: ТНТУ ім. І. Пулюя, м. Тернопіль, вул. Руська, 56, 46001,
тел. (0352) 52-41-33, факс (0352) 25-49-83.
E-mail: conffis2024@gmail.com
Редагування, оформлення та верстка: Надія Крива

СЕКЦІЇ КОНФЕРЕНЦІЇ, ЯКІ ПРЕДСТВЛЕНІ В ЗБІРНИКУ

- Математичне моделювання
- Інформаційні системи та технології, кібербезпека
- Комп'ютерні системи та мережі
- Програмна інженерія та моделювання складних розподілених систем
- Новітні фізико-технічні та освітні технології

В збірнику надруковано тези доповідей XII науково-технічної конференції «Інформаційні моделі, системи та технології» (Тернопіль, 18–19 грудня 2024 р.) за такими науковими напрямками: математичне моделювання; інформаційні системи та технології, кібербезпека; комп'ютерні системи та мережі; програмна інженерія та моделювання складних розподілених систем; новітні фізико-технічні та освітні технології.

Розрахований на науковців, викладачів та студентів вузів.

За зміст тез та дотримання норм академічної доброчесності відповідальність несе автор.

© Тернопільський національний технічний університет імені Івана Пулюя, …… 2024

УДК 004.056:629.331
М. Демчишин, В. Тимощук, В. Шиманська, Д. Тимощук
(Тернопільський національний технічний університет імені Івана Пулюя)

КІБЕРЗАГРОЗИ СЕНСОРНИМ ПІДСИСТЕМАМ АВТОНОМНИХ ТРАНСПОРТНИХ ЗАСОБІВ

M. Demchyshyn, V. Tymoshchuk, V. Shymanska, D. Tymoshchuk
CYBER THREATS TO SENSOR SUBSYSTEMS OF AUTONOMOUS VEHICLES

Автономні транспортні засоби (АТЗ) є технологічним проривом, який обіцяє змінити сучасну транспортну інфраструктуру, забезпечивши підвищення ефективності, зниження кількості дорожньо-транспортних пригод та покращення якості перевезень. Завдяки використанню численних сенсорів, таких як LiDAR [1], камери, радари та ультразвукові датчики, АТЗ здатні аналізувати навколишнє середовище, ідентифікувати об'єкти, передбачати дії інших учасників руху та приймати рішення в реальному часі (рисунок 1).

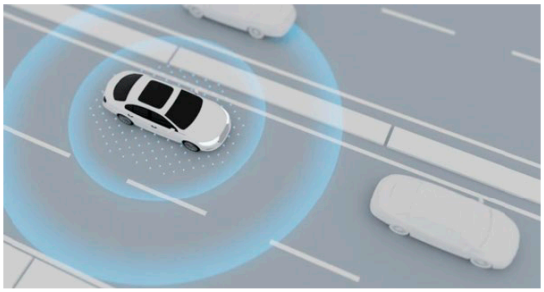

Рисунок 1 - Сенсори автономного транспортного засобу

Проте впровадження цієї технології супроводжується серйозними викликами в галузі кібербезпеки, особливо в контексті захисту критично важливих сенсорних підсистем. Ключовою складовою функціонування автономного транспорту є точне сприйняття навколишнього середовища. Залежність від сенсорних систем створює вразливості, які можуть бути використані зловмисниками для компрометації безпеки транспортного засобу. Такі атаки можуть включати викривлення даних, відтворення попередніх показників або повне відключення сенсорів. Найбільшу загрозу становлять атаки, спрямовані на сенсори, адже вони можуть створити небезпечні ситуації, що безпосередньо впливають на керування та прийняття рішень. Наприклад, маніпуляція даними LiDAR може привести до хибної ідентифікації об'єктів або створення «сліпих зон», що унеможливлює адекватне реагування транспортного засобу.

Зростаюча складність сучасних сенсорних систем вимагає розробки ефективних моделей захисту. Найбільш імовірними є атаки з частковою інформацією, коли зловмисник має обмежений доступ до системи та не може отримати повний огляд її роботи. У таких випадках атакуючий працює з мінімумом даних, наприклад, лише з вхідними показниками сенсора. Метою роботи був аналіз кіберзагроз сенсорним підсистемам АТЗ та розробка ефективних підходів до захисту.

Література

1. IBM. What is LiDAR? URL: https://www.ibm.com/topics/lidar (date of access: 07.12.2024).