Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Метод захисту даних, отриманих за допомогою сенсорів 6G»

Виконав: студент 2 курсу, групи 1БС-22м
Спеціальність – 125 Кібербезпека
_____ Володимир КЛЮЧКІВСЬКИЙ

Керівник: к. т. н., доцент каф. ЗІ
_____ Віталій ЛУКІЧОВ
«13» грудня 2023 р.

Рецензент: к. т. н. доцент каф. ПЗ
_____ Володимир МАЙДАНЮК
«13» грудня 2023 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____Володимир ЛУЖЕЦЬКИЙ
«14» 12 2023 р.

Вінниця ВНТУ– 2023 р.

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти ІІ-й (магістерський)
Галузь знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ, д.т.н., проф.
_____ Володимир ЛУЖЕЦЬКИЙ
«19» 09 2023 року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Ключківському Володимиру Олександровичу

1. Тема роботи: «Метод захисту даних, отриманих за допомогою сенсорів 6G», керівник роботи: Лукічов Віталій Володимирович, к.т.н., доцент каф. ЗІ, затверджені наказом ректора ВНТУ від 18 вересня 2023 року, протокол №247.
2. Строк подання студентом роботи 13 грудня 2023 р.
3. Вихідні дані до роботи:
   - сенсори 6G;
   - принцип сортування незв'язності даних;
   - захист конфідеційної інормації;
   - захист інформації на етапі збору.
4. Зміст текстової частини: Вступ. 1. Аналіз стану питання та постановка задач дослідження. 2. Розробка методу захисту даних отриманих за допомогою сенсорів 6G. 3. Експериментальні дослідження. 4. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Принцип роботи сенсору AWR2944(плакат, А4). Структурна схема проведення спуфінг атаки (плакат, А4). Схема процесу обфускації та передачі даних за принципом незв'язності (плакат, А4). Загальна структурна схема обміну даними в автомобільній мережі 6G (плакат, А4). Вікно з програмного застосунку для моделювання (без обфускації) (плакат, А4). Вікно з програмного застосунку для моделювання (з обфускацією) (плакат, А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанти	Підпис, дата	
		завдання видав	виконання прийняв
1	Віталій ЛУКІЧОВ., к.т.н., доцент каф. ЗІ	01.09	22.09
2	Віталій ЛУКІЧОВ, к.т.н., доцент каф. ЗІ	01.09	17.10
3	Віталій ЛУКІЧОВ, к.т.н., доцент каф. ЗІ	01.09	07.12
4	Ольга РАТУШНЯК., к.т.н., доцент каф. ЕПВМ	01.09	16.11

7. Дата видачі завдання 1 вересня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	01.09.2023 – 10.09.2023	
2	Аналіз літературних джерел за напрямком магістерської кваліфікаційної роботи	10.09.2023 – 15.09.2023	
3	Науково-технічне обгрунтування	16.09.2023 – 22.09.2023	
4	Розробка технічного завдання	23.09.2023 – 29.09.2023	
5	Розробка рішень	30.09.2023 – 12.10.2023	
6	Практична реалізація, моделювання, експериментування, результати	14.10.2023 – 10.11.2023	
7	Розробка розділу економічного обгрунтування доцільності розробки	11.11.23 – 17.11.2023	
8	Аналіз виконання ТЗ, висновки	18.11.2023 – 24.11.2023	
9	Оформлення пояснювальної записки	25.11.2023 – 30.11.2023	
10	Попередній захист та доопрацювання МКР	28.11.2023 – 01.12.2023	
11	Перевірка магістерської роботи на наявність плагіату	02.12.2023 – 10.12.2023	
12	Представлення МКР до захисту	11.12.2023 – 14.12.2023	
13	Захист МКР	14.12.2023 – 21.12.2023	

Студент _____ Володимир КЛЮЧКІВСЬКИЙ

Керівник роботи _____ Віталій ЛУКІЧОВ

АНОТАЦІЯ

УДК 004.056

Ключківський В. Метод захисту даних, отриманих за допомогою сенсорів 6G. Магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2023. 60 с. Укр. мовою. Бібліогр.: 21 назв; рис.: 14; табл.: 18.

Магістерська кваліфікаційна робота присвячена розробці методу захисту даних отриманих за допомогою сенсорів 6G. Підготовлено науково-дослідне та техніко-економічне обґрунтування доцільності досліджень У роботі здійснено аналіз існуючих методів захисту даних отриманих за допомогою сенсорів 6G. Розроблено власний метод захисту даних на етапі збору сенсорами. Розроблено карту ризиків для інформації отриманої за допомогою сенсорів 6G.

Ілюстративна частина складається з 6 плакатів з демонстрацією результатів моделювання і проведених досліджень.

В економічному розділі оцінено витрати на розробку.

Ключові слова: сеснсори 6G, обфускація, принцип незв’язності, конфідеційна інформація.

ABSTRACT

Klyuchkivskyi, V. Data Protection Method for Information Obtained through 6G Sensors. Master's Thesis in the field of 125 – Cybersecurity, Educational Program – Information and Communication Systems Security. Vinnytsia: VNTU, 2023. 60 p. In Ukrainian. Bibliography: 21 titles; figures: 14; tables: 18.

The master's thesis is devoted to the development of a method of protecting data obtained with the help of 6G sensors. A scientific research and technical-economic justification of the feasibility of research was prepared. The work analyzed the existing methods of data protection obtained with the help of 6G sensors. A proprietary method of data protection at the stage of sensor collection has been developed. A risk map has been developed for information obtained using 6G sensors.

The illustrative part consists of 6 posters demonstrating the results of modeling and conducted research.

The economic section evaluates the costs associated with the development.

Keywords: 6G sensors, obfuscation, principle of independence, confidential information.

ЗМІСТ

ВСТУП

В епоху безпрецедентного розвитку технологій та бездротового зв'язку, майбутнє суспільство входить в еру, де висока швидкість передачі даних та безперервний обмін інформацією стають не просто вимогою, але й визначальним фактором для ефективного функціонування різних сфер життя. Після впровадження стандартів 5G, світ перебуває на порозі нової ери бездротових комунікацій, орієнтованої на мережі 6G.

Технологія 6G, яка є наступником 5G, має на меті забезпечити ще вищі швидкості передачі даних та низьку затримку, створюючи основу для інновацій у багатьох сферах, включаючи автомобільну промисловість. За допомогою вдосконаленого бездротового зв'язку, 6G може значно поліпшити системи безпеки та автономії автомобілів, забезпечуючи більш точний обмін даними між транспортними засобами та оточуючими елементами інфраструктури. Це дозволить реалізувати передові технології, такі як розумні мережі доріг, що відіграють ключову роль у створенні безпечних та ефективних систем автопілоту та допомагаючих водієві асистентів [1].

Однак, наряду з величезним потенціалом прогресу, виникає низка викликів і проблем, особливо щодо безпеки обміну даними в цих мережах. Збільшення обсягів інформації, які обробляються, а також різноманітність джерел її походження, роблять питання захисту конфіденційності та цілісності даних надзвичайно актуальними.

Особливу увагу в цьому контексті слід приділити інформації, здобутої від сенсорів, яка може включати в себе величезний спектр особистих та конфіденційних даних. Ця інформація може виявитися вразливою перед різноманітними загрозами, починаючи від несанкціонованого доступу та закінчуючи можливістю використання трекінгів, які на основі зібраних даних, можуть відстежувати рух користувача. Тим самим, виникає належне питання про необхідність впровадження ефективних заходів для забезпечення конфіденційності та захисту особистої інформації.

Об'єктом дослідження є процес збору, передачі та обробки інформації, отриманої за допомогою сенсорів в мережі 6G.

Предметом дослідження є методи та стратегії захисту даних, які збираються, передаються та оброблюються за допомогою сенсорів в контексті мереж 6G.

Метою магістерської кваліфікаційної роботи є підвищення захисту конфіденційних даних, зібраних за допомогою сенсорів 6G.

Для досягнення мети потрібно виконати наступні завдання:

– виконати аналіз існуючих методів збору, сортування інформації отриманої за допомогою сенсорів 6G;

– удосконалення методів та розробка власної методики захисту;

– виконати експериментальне дослідження підсистеми.

Новизна дослідження: набув подальшого розвитку метод захисту даних, отриманих за допомогою сенсорів 6G на етапі збору даних, що допоможе розв’язати актуальні проблеми конфіденційності даних.

Практичне значення розроблювальний метод, допоможе забезпечити безпеку та конфіденційність даних у високотехнологічному світі майбутнього.

Результати здійснених досліджень під час виконання магістерської кваліфікаційної роботи будуть доповідатись на Міжнародній науково-практичній конференції студентів, аспірантів та молодих науковців «Молодь в науці: дослідження, проблеми, перспективи».

1 АНАЛІЗ СТАНУ ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

1.1 Науково-технічне обґрунтування розробки методу захисту даних отриманих за допомогою сенсорів 6G

У сучасному світі інформація стала життєво важливим ресурсом, що приводить до появи нових викликів у сфері її захисту та безпеки. Із стрімким розвитком телекомунікаційних технологій та мереж наступного покоління, таких як мережі 6G, зростає обсяг та важливість даних, що збираються та передаються через різноманітні сенсори.

Шосте покоління бездротових мереж (6G) є природнім еволюційним кроком після 5G та визначається більш високою пропускною здатністю, зменшеною затримкою та розширеними можливостями використання частотного спектру. В порівнянні з 5G, мережі 6G мають використовувати більш високі частоти, що дозволить досягти значної пропускної здатності та знизити затримку до однієї мікросекунди в умовах високої мобільності [2].

Серед основних характеристик мережі 6G, можна виділити наступні:

– Висока пропускна здатність. Очікується, що 6G підтримуватиме швидкість передачі даних 1 терабайт в секунду (Тбіт/с), що є значним покращенням порівняно з 5G.

– Малі затримки. Однією з ключових цілей 6G є підтримка затримки в одну мікросекунду, що в 1000 разів швидше, ніж у 5G, що стає важливим для реального часу та високопродуктивних застосувань.

– Розширені можливості Інтернет речей (IoT). Інтернет речей (IoT) - це концепція, в якій фізичні об'єкти та пристрої обладнані сенсорами, здатні обмінюватися даними та взаємодіяти через мережу. У мережах 6G, Інтернет речей отримає нові можливості завдяки високій пропускній здатності, низькій затримці та покращеній підтримці для великої кількості підключених пристроїв. Мережі 6G дозволять ефективно збирати, обробляти та обмінювати даними в реальному часі,

роблячи Інтернет речей ще більш інтегрованим та потужним елементом сучасних технологічних екосистем.

– Обчислювальна інфраструктура. Робота 6G буде включати в себе силу штучного інтелекту та обчислювальну інфраструктуру для автономного прийняття рішень щодо обробки, зберігання та обміну даними.

– Використання високих частот. Застосування високих частот, включаючи міліметровий спектр, дозволить отримати вищі швидкості передачі даних та поліпшити дискретизацію сигналів.

– Розширені сфери застосування. 6G очікується принести значні вдосконалення у сферах візуалізації, технології присутності, інформування про місцезнаходження та інших інноваційних технологій.

– Інтеграція з MEC та HPC. Вбудовані мобільні обчислювальні технології (MEC) та високопродуктивні обчислення (HPC) будуть важливими компонентами для забезпечення ефективного використання ресурсів та підтримки різноманітних застосувань.

– Комерційне впровадження в 2030 році. Очікується, що мережі 6G будуть готові для комерційного впровадження приблизно в 2030 році.

Таким чином, за допомогою вдосконаленого бездротового зв'язку, 6G може значно поліпшити системи безпеки та автономії автомобілів, забезпечуючи більш точний обмін даними між транспортними засобами та оточуючими елементами інфраструктури. Це дозволить реалізувати передові технології, такі як розумні мережі доріг, що відіграють ключову роль у створенні безпечних та ефективних систем автопілоту та асистентів, які будуть допомагати водієві під час руху.

Отже, шосте покоління бездротових мереж (6G) визначається високою пропускною здатністю, мінімальними затримками та розширеними можливостями використання високих частот, порівняно з попереднім поколінням 5G. Ці характеристики роблять 6G ключовим фактором для розвитку ряду інноваційних технологій, таких як Інтернет речей (IoT), автономні транспортні системи та розумні мережі доріг. Очікується, що мережі 6G нададуть значний імпульс

розвитку технологій, що вимагають велику пропускну здатність, мінімальні затримки та високу ефективність обчислювальних процесів.

З урахуванням цих характеристик і тенденцій до комерційного впровадження 6G приблизно в 2030 році, розробка методу захисту даних, отриманих за допомогою сенсорів у мережах 6G, набуває важливого значення. Висока швидкість передачі даних та мінімальні затримки вимагають розробки ефективних засобів безпеки, спрямованих на забезпечення конфіденційності та цілісності інформації в умовах високої продуктивності та реального часу. Такий метод захисту має стати необхідною складовою для успішної і безпечної експлуатації перспективних технологій мереж 6G.

1.2 Збір та аналіз даних за допомогою сенсорів 6G

Сенсор для збору даних є ключовим технічним пристроєм, який спроектований для вимірювання фізичних величин або реєстрації подій та перетворення їх на електричні сигнали або цифрові дані. Ці дані використовуються для реалізації різноманітних завдань, включаючи аналіз, моніторинг, керування та інші цілі в різних областях техніки та науки.

Демонстрація використання сенсорів для відтворення руху людини наведено на рисунку 1.1.

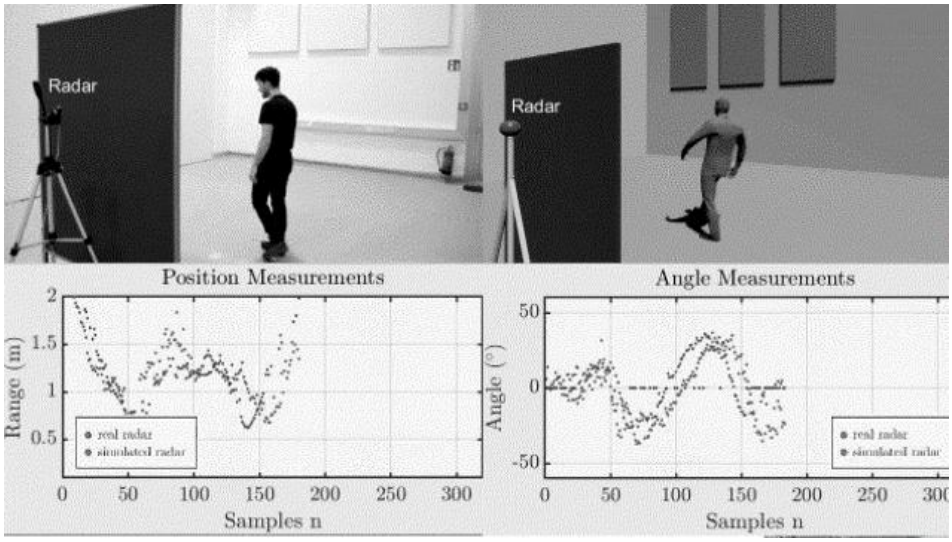


Рисунок 1.1 – Моделювання руху людини за допомогою сенсорів

Одним із передових сенсорів у цій сфері є AWR2944, який відзначається високочастотними характеристиками та високою роздільною здатністю. Здатний працювати в широкому частотному діапазоні (76-81 ГГц), також відомий як діапазон міліметрових хвиль або ж ММХ (Millimeter Wave Range) охоплює від 30 до 300 ГГц., особливість міліметрових хвиль полягає в тому, що вони мають високу частоту і коротку довжину хвиль. Це дозволяє їм бути ефективно використаними для високочастотних застосувань, таких як створення деталізованих образів об'єктів, взаємодія з якими вимагає високої роздільної здатності. Надалі він буде використовуватись для експериментальних дослідженнях згідно поставленого завдання, даний сенсор відкриває нові можливості для збору та обробки даних з винятковою ефективністю. Зовнішній вигляд високочастотного сенсору AWR2944, представлено на рисунку 1.2.

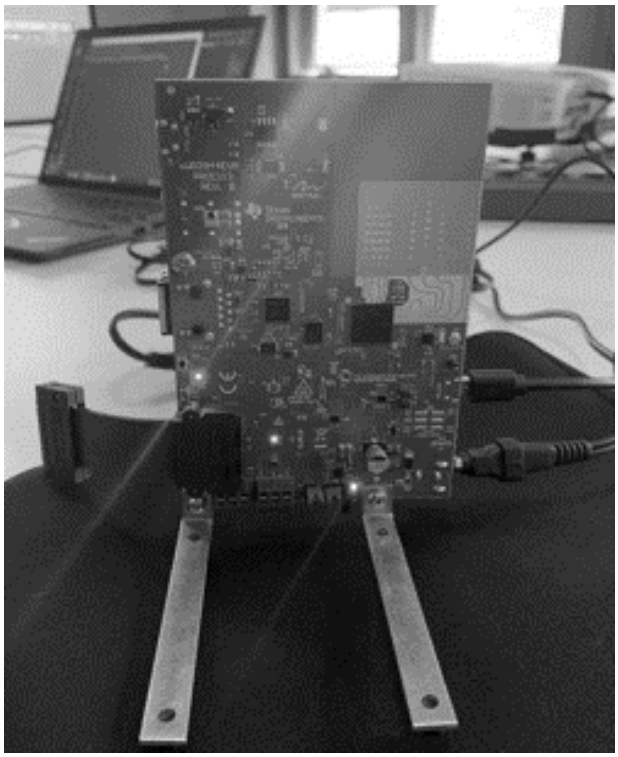


Рисунок 1.2 – Зовнішній вигляд високочастотного сенсору AWR2944

Зазначений сенсор знаходить широке застосування в автомобільних системах допомоги водієві (ADAS) та інших областях, де вимірювання та виявлення об'єктів в різних умовах має стратегічне значення. Його високі технічні характеристики роблять його оптимальним вибором для високопродуктивних додатків, де важлива

якість та ефективність збору даних. Способи розміщення сенсорів зображено на рисунку 1.3.

Рисунок 1.3 – Способи розміщення сенсорів AWR2944

Принцип збору даних базується на використанні мікрохвильових хвиль, що видаються сенсором та виконується у наступній послідовності [9]:

– Випромінювання сигналу. Сенсор висилає мікрохвильові хвилі у навколишнє середовище. Ці хвилі є необхідним інструментом для взаємодії з об'єктами та отримання від них інформації.

– Відбиття від об'єктів. Сигнал відбивається від об'єктів, які перебувають в зоні дії сенсора. Різниця у відбитому сигналі визначається різницею властивостей об'єктів та їх розташуванням.

– Реєстрація змін в частоті. Сенсор реєструє зміни в частоті відбитого сигналу, які виникають за рахунок ефекту доплера. Ці зміни пов'язані з рухом об'єктів, їх відстанню та іншими фізичними властивостями.

Ефект доплера - це явище зміни частоти (або довжини хвилі) хвилі відносно спостерігача при русі джерела хвилі або самого спостерігача. Це явище виникає внаслідок руху джерела хвилі, спостерігача або обох.

Зазвичай ефект доплера спостерігається у звуці або світлових хвилях. Якщо джерело (наприклад, звуковий динамік або світлодіод) рухається відносно спостерігача, хвилі, які вони випромінюють, будуть зменшувати свою довжину для

звукових хвиль або збільшувати частоту для світлових хвиль, якщо рух відбувається назустріч спостерігачеві, і, навпаки, збільшувати довжину або зменшувати частоту, якщо рух відбувається в протилежному напрямку.

– Аналіз та обробка даних. Отримані дані піддаються аналізу та обробці. Сучасні алгоритми і штучний інтелект допомагають витягти значущі відомості з об'ємних даних, отриманих від різних джерел.

– Формування тривимірної карти. На основі оброблених даних створюється тривимірна карта, яка відображає розташування об'єктів у просторі. Ця карта може використовуватися для різних цілей, включаючи визначення форми об'єктів, відстані до них та їх руху.

Даний метод збору даних не лише надає високу роздільну здатність та точність, але також дозволяє вивчати об'єкти в реальному часі, відкриваючи широкий спектр можливостей в області наукових досліджень, автомобільних технологій, медицини та інших галузей.

Структурна схема принципу роботи сенсору зображено на рисунку 1.4.

Рисунок 1.4 – Принцип роботи сенсору AWR2944

Отже, сенсор для збору даних виявляється необхідним технічним засобом у сучасному світі, спроектованим для вимірювання фізичних величин, реєстрації подій та перетворення їх на електричні сигнали чи цифрові дані. Ці дані стають основою для виконання різноманітних завдань, таких як аналіз, моніторинг, керування тощо, і знаходять своє використання в різних галузях техніки та науки.

Наочність використання сенсорів для відтворення руху людини видно на рисунку 1.1, де передовий сенсор, AWR2944, вирізняється високочастотними характеристиками та високою роздільною здатністю. Його застосування в експериментальних дослідженнях відкриває нові перспективи для ефективного збору та обробки даних. Зовнішній вигляд сенсору AWR2944 представлено на рисунку 1.2, що свідчить про його високі технічні характеристики.

Використання AWR2944 розповсюджене в автомобільних системах допомоги водієві та інших областях, де виявлення об'єктів має велике значення. Його технічні переваги роблять його важливим для високопродуктивних застосувань, де вимагається якість та ефективність збору даних.

Принцип збору даних заснований на використанні мікрохвиль і включає етапи випромінювання сигналу, відбиття від об'єктів, реєстрацію змін в частоті, аналіз та обробку даних, і формування тривимірної карти. Ефект Доплера використовується для визначення руху об'єктів, а алгоритми обробки даних допомагають витягти значущу інформацію [10].

1.3 Аналіз основних вразливостей для отриманих даних

З кожним роком кількість автомобілів на дорогах постійно збільшується, що призводить до загострення екологічних проблем, погіршення мобільності транспортних засобів і збільшення кількості дорожньо-транспортних пригод і трагічних випадків. Розробники вже давно шукають безпечні рішення, які покращать ситуацію на дорогах та збільшать пропускну здатність. Існують різноманітні пропозиції, включаючи літаючі транспортні засоби, підземні

автомагістралі і навіть системи надземних шляхопроводів. Однак кожне з цих рішень має свої труднощі у впровадженні.

Серед найперспективніших проектів, спрямованих на підвищення безпеки та ефективності автомагістралей, є технологія підключених та автономних транспортних засобів (CAV - Connected and Automated Vehicle). Ідея полягає в тому, щоб використовувати інфраструктуру з дорожніми блоками (RSU - Road Side Unit), яка збирає інформацію про транспортні засоби з бортовим блоком (OBU - On-Board Unit) у вигляді базових повідомлень безпеки (BSM - Basic Safety Messages) [11]. В такому випадку CAV отримують інформацію про ситуацію на дорозі не лише за допомогою сенсорів та радарів, як звичайні автомобілі, але і взаємодіючи один з одним та із навколишньою інфраструктурою. Це дозволяє CAV і іншим учасникам руху діяти автономно, стаючи більш ефективними.

Проте і в цьому проекті є проблема - наявність загальної мережі, до якої підключені всі автомобілі.

Існує ризик передачі даних незахищеною мережею, особливо при її очікуваному перевантаженні. Це може породжувати загрозу для конфіденційності особистої інформації та створювати можливості використання трекінгів, які на основі зібраних даних можуть відстежувати рух користувача.

Конфіденційна інформація - це інформація, доступ до якої обмежений або обов'язковий згідно з певними правилами чи політиками [12]. Це може включати комерційні та технічні відомості, бізнес-плани, винаходи, особисті дані та будь-яку іншу інформацію, яка підлягає обов'язковому збереженню в таємниці.

Особиста інформація - це дані, які стосуються конкретної особи, такі як ім'я, адреса, номер телефону, електронна пошта, дата народження, медична інформація та інші особисті характеристики.

Вишка RSU (Roadside Unit) є ключовим елементом інфраструктури в системах бездротового зв'язку, зокрема, у контексті транспортних мереж. Ця вишка розташована при дорозі та використовується для збору, обробки та передачі безпровідних сигналів між транспортними засобами та іншими елементами мережі [13].

На основі проведеного аналізу можна сказати, що "інформація з обмеженим доступом" може відповідати поняттю, яке є середнім між конфіденційною та особистою інформацією. Це означає, що ця інформація може містити як загальні характеристики, що стосуються широкого кола користувачів, так і конфіденційні аспекти, які вимагають особливого рівня захисту та обмеженого доступу. Такий підхід враховує необхідність утримання рівноваги між відкритістю і конфіденційністю, особливо в контексті обробки і збереження інформації, яка може включати елементи як загального, так і особистого характеру.

Одна з можливих стратегій зловмисників пов'язана як з автомобільними радарами, так і мережами 6G - це створення перешкод у каналі, а також спуфінг - маскування під легального користувача або підключеного до мережі пристрою.

Атака спуфінгу із підміною легітимної RSU (Roadside Unit) вишки має за мету введення в оману системи зв'язку, переконуючи інші пристрої, що фальшива RSU є легітимною точкою доступу. Основна ідея полягає в тому, щоб створити імітацію діючої RSU та перехоплювати або модифікувати комунікаційний трафік, що проходить через неї.

Структурна схема атаки шляхом підміни легітимної RSU зображено на рисунку 1.5.

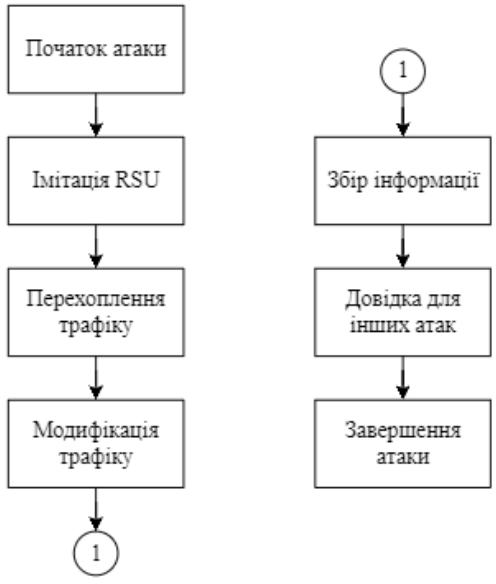


Рисунок 1.5 – Структурна схема проведення спуфінг атаки

Детальніше процес виглядає наступним чином:

– Імітація RSU. Атакуючий створює фальшиву RSU, яка може мати подібний ідентифікатор або параметри до легітимної RSU, щоб легітимні пристрої не могли відрізнити її від реальної RSU.

– Перехоплення трафіку. Фальшива RSU перехоплює трафік від інших пристроїв, які вважають її легітимною. Це може включати інформацію про маршрутизацію, обмін даними між транспортними засобами, або будь-яку іншу чутливу інформацію, що передається через RSU.

– Модифікація трафіку. Атакуючий може модифікувати переданий трафік, вставляти хибні дані чи навіть видаляти або блокувати певні типи інформації. Це може вплинути на надійність та безпеку систем комунікації між транспортними засобами та RSU.

– Збір інформації. Фальшива RSU може також використовуватися для збору інформації про підключені пристрої, їхні характеристики або розташування, що може мати наслідки для конфіденційності та безпеки користувачів.

– Довідка для інших атак. Інформація, зібрана фальшивою RSU, може використовуватися для планування і виконання інших атак, таких як напади на безпеку даних чи подальші спроби вторгнення в мережу.

Дана атака може мати серйозні наслідки для безпеки особистої конфідеційної інформації та функціональності систем зв'язку між транспортними засобами та RSU в інфраструктурі мереж 6G. Вона спрямована на створення заторів, які майже неможливо виявити за допомогою простих захисних підходів, таких як невідповідність розташування та швидкості транспортного засобу, телепортація або обгін із поверненням на ту саму смугу руху. На рисунку 1.6, представлено загальну схему сценарію атаки, що моделюється.

У цьому контексті визначимо обмеження для подальших розглядів, роблячи певні припущення. Припустимо, що зловмисник має здатність змінювати вміст BSM (Basic Safety Message), який передається між транспортними засобами і RSU (Roadside Unit).

BSM (Basic Safety Message) це коротке повідомлення, яке висилається або отримується транспортним засобом, щоб обмінювати базовою інформацією про безпеку на дорозі. Ці повідомлення використовуються в розумних транспортних системах (ITS) для підтримки функцій, таких як моніторинг сліпих зон, попередження про зіткнення, адаптивний круїз-контроль та інші системи безпеки на дорозі. BSM може включати інформацію, таку як швидкість транспортного засобу, його положення, напрямок руху та інші параметри, які дозволяють оточуючим транспортним засобам та інфраструктурі отримувати актуальну інформацію про дорожні умови та взаємодіяти для забезпечення безпеки на дорозі. Це часто використовується в контексті розумних автомобільних систем та технологій, спрямованих на покращення безпеки дорожнього руху.

Проте, відзначимо, що у нього немає можливості впливати на потужність радіосигналу в межах ефективної зони покриття зв'язку між RSU і зловмисником. Це припущення робиться за умови, що RSU знаходиться в зоні дії зловмисника.

Додатково, припускаємо, що зловмисник не може підробити підпис відправників, що означає, що ідентифікатор або маркер автентичності вказує на легітимність відправника даних. Це є важливим обмеженням для забезпечення безпеки інформаційного обміну між транспортними засобами та RSU.

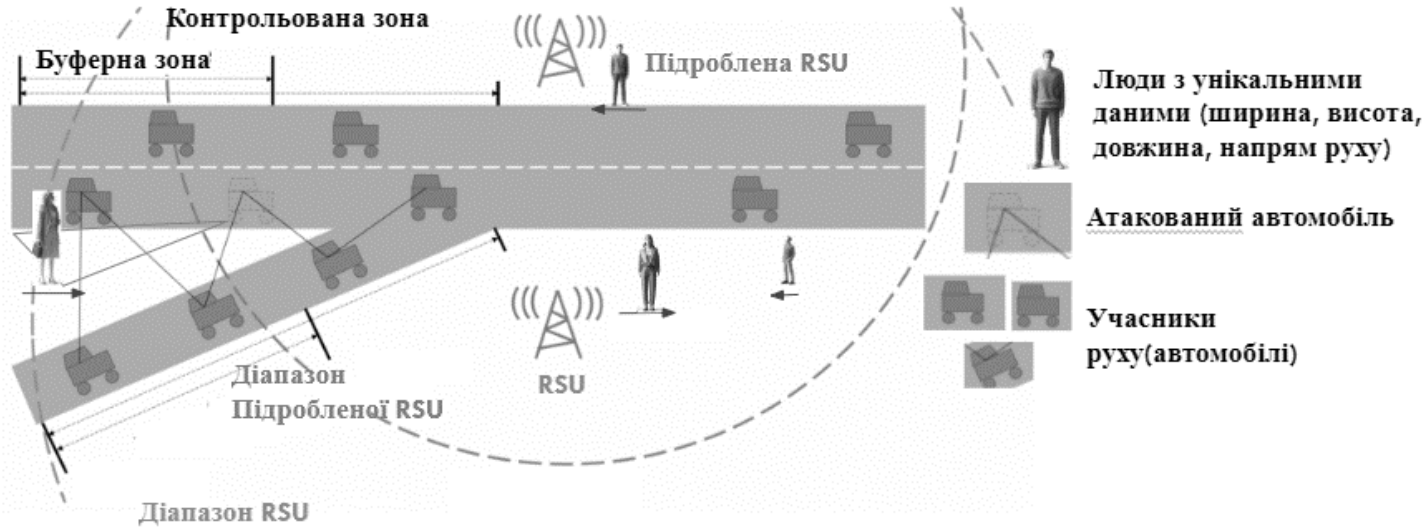


Рисунок 1.6 – Загальна схема сценарію атаки, що моделюється

Зловмисник знаходиться поряд з RSU і може перехоплювати BSM'и, які транслюються обладнаними транспортними засобами. Потім зловмисник розгортає атаки типу "людина посередині" (man-in-the-middle) для зміни BSM і повторно відправляє їх в RSU. Наприклад, червоний автомобіль є атакованим транспортним засобом, а значок пунктирної лінії представляє область атаки, де зловмисник намагається підробити RSU.

Розглянемо дві нетривіальні стратегії спуфінгу, а саме:

– Аварійна зупинка.

– Підміна накопичувального дрейфу позиції.

"Нетривіальні стратегії спуфінгу" це такі методи або підходи до атаки спуфінгу, які є складними, винахідливими та важкими для виявлення або протидії. У цьому контексті "спуфінг" означає створення фальшивого сигналу або інформації з метою введення в оману системи виявлення, аутентифікації або ідентифікації.

Аварійна зупинка . У випадку коли цільова CAV входить у зону дії атакуючого, може постійно отримувати BSM від цієї CAV [14]. Зловмисник застосовує атаки типу "людина посередині", які змушують інформацію про місцезнаходження CAV фіксуватися у відповідній точці входу, звідки зловмисник проводить атаку, і фальсифікують інформацію про нульову швидкість, а потім надсилають всю цю інформацію в RSU. У цьому випадку алгоритм управління надаватиме неправильну рекомендовану швидкість тим, хто слідує за CAV в межах тієї ж смуги атакованого транспортного засобу, щоб вони сповільнилися або навіть повністю зупинилися.

Підміна накопичувального дрейфу позиції. В даному типі атаки зловмисник продовжує отримувати повідомлення BSM від цільового CAV, як тільки атакований автомобіль потрапляє в зону дії зловмисника. Потім зловмисник також безперервно генерує фальсифіковану інформацію про швидкість, але вже протягом досить тривалого часу, показуючи учасникам руху, що автомобіль, який рухається вперед, поступово сповільнюється. Крім того, хибне місцезнаходження обчислюється на основі підробленої швидкості. Це невелике неузгодження між

місцем розташування та швидкістю можна розглядати як результат втрати сигналу або помилок GPS, які трапляються досить часто. Однак при накопиченні різниці між фактичною позицією та заявленою в системі виявляться більш серйозні впливи (наприклад, перевантаження) на вихідний трафік.

Також перехоплені дані (напрям руху, швидкість, унікальні фізичні характеристики людини тощо) можуть використовуватися для порушення конфіденційності та приватної інформації, зокрема для відстеження напряму руху людини за допомогою трекінгів.

Процес відстеження напряму руху людини за допомогою трекінгів виглядає наступним чином:

– Вхідні дані. Трекінг отримує вхідні дані від датчиків чи інших джерел, які вимірюють розташування та параметри навколишніх об'єктів.

– Обробка Даних. Система обробляє вхідні дані для визначення параметрів цілей, таких як координати, швидкість тощо.

– Відстеження. Трекінг використовує алгоритми відстеження для визначення, як об'єкти рухаються в просторі і як вони можуть змінювати своє розташування в майбутньому.

– Неоднозначність. В умовах неоднозначності, наприклад, коли датчики надають нечіткі чи суперечливі дані, трекінг може використовувати алгоритми або стратегії для управління цією неоднозначністю та надання найбільш ймовірних результатів.

– Вихідні дані. Система надає вихідні дані, які можуть бути використані для подальшого управління або прийняття рішень, наприклад, у ситуаціях навігації або управління рухом.

Даний процес підкреслює важливість захисту особистих даних та розробки ефективних методів для запобігання небажаному відстеженню та використанню персональної та конфідеційної інформації без належного дозволу.

RSSI (Received Signal Strength Indicator) — це параметр, що вказує на потужність сигналу, отриманого приймачем (наприклад, бездротовим пристроєм чи мобільним телефоном) від передавача (наприклад, точки доступу Wi-Fi чи

іншого пристрою). У бездротових технологіях, таких як Wi-Fi, Bluetooth, або мобільні мережі, вимірювання RSSI може використовуватися для визначення якості зв'язку, визначення відстані між пристроями, а також для розташування та навігації в системах позиціонування в приміщенні. Важливо враховувати, що RSSI сам по собі не завжди є точним індикатором якості зв'язку. Вплив на якість зв'язку можуть мати різні фактори, такі як перешкоди, електромагнітні перешкоди, інші пристрої, які працюють на тому ж частотному діапазоні, та інші аспекти навколишнього середовища.

Стратегія захисту від спуфінг атак, заснована на середньоквадратичній помилці (MSE - Mean Square Error), спрямована на виявлення та фільтрацію транспортних засобів (BSM) з підробленими даними на стороні RSU (Roadside Unit). Розглянемо дану стратегію більш детально[4]:

– Одержання Даних BSM. RSU отримує повідомлення BSM від реальних транспортних засобів (CAV) і можливо від потенційного зловмисника, який намагається підробити дані.

– Вимірювання Потужності Сигналу (RSSI). для кожного BSM RSU вимірює потужність сигналу (RSSI). Це індекс, що вказує на силу сигналу, отриманого RSU від кожного транспортного засобу.

– Визначення Статистики RSSI. збирається статистика RSSI для кожного транспортного засобу, яке включає середню, максимальну, мінімальну потужність сигналу та інші показники.

– Отримання Інформації про Місцезнаходження. крім того, RSU отримує інформацію про місцезнаходження (географічні координати) з отриманих BSM.

– Обчислення MSE: для кожного транспортного засобу RSU обчислює MSE відстаней, використовуючи інформацію про місцезнаходження з BSM та статистику RSSI. MSE визначає точність вимірювань в порівнянні із фактичною відстанню.

– Фільтрація Даних: RSU фільтрує BSM, відкидаючи ті, для яких MSE виявляє низьку точність вимірювань. Таким чином, фальшиві дані з меншою потужністю сигналу можуть бути виявлені та відкинуті.

– Ідентифікація Лінії Руху: RSU визначає лінії руху транспортних засобів, використовуючи отримані дані, інформацію про місцезнаходження та вимірювання RSSI.

Mean Square Error (MSE) - це метрика, яка використовується для вимірювання середньої квадратичної різниці між фактичними і прогнозованими значеннями в регресійних моделях. У контексті аналізу даних і машинного навчання, MSE є однією з найпоширеніших метрик для оцінки точності моделей прогнозування.

Основна ідея MSE полягає в тому, щоб взяти різницю між фактичними та прогнозованими значеннями для кожного спостереження, підняти цю різницю до квадрату, підсумувати всі квадрати і поділити на кількість спостережень. Чим менше значення MSE, тим краще модель вирішує завдання прогнозування.

Такий підхід дозволяє виявляти підроблені BSM, спираючись на аналіз потужності сигналу та порівняння із фактичною географічною відстанню. Фільтрація за допомогою MSE дозволяє виявити та відкинути дані з помилками, забезпечуючи більш високу достовірність ідентифікації та захист від атак на систему зв'язку між транспортними засобами та RSU.

У результаті проведеного аналізу атак на систему зв'язку між транспортними засобами та RSU в контексті 6G виявлено, можливі атаки, такі як спуфінг, перехоплення даних та порушення конфіденційності за допомогою трекінгів можуть становити серйозні загрози. Щодо захисту від цих атак, розглянуто стратегію з використанням середньоквадратичної помилки (MSE) для виявлення та фільтрації підроблених даних BSM на стороні RSU. Ця стратегія базується на вимірюванні потужності сигналу (RSSI) як інструменту для пошуку даних із більшою потужністю сигналу порівняно з іншими, з метою забезпечення надійності системи та запобігання атакам на зв'язок в інфраструктурі 6G.

1.4 Постановка завдання

З розвитком мереж 6G та високої мобільності користувачів виникає необхідність впровадження ефективних заходів безпеки для забезпечення

конфіденційності та цілісності даних, отриманих через сенсори. Особлива увага приділяється вирішенню викликів, пов'язаних із захистом даних отриманих за допомогою сенсорів 6G. Провівши аналіз основних вразливостей та існуючих способів захисту було визначено перелік завдань що потрібно виконати для розробки власного методу захисту даних отриманих за допомогою сенсорів 6G:

– Розробити метод захисту, який враховує особливості сучасних сенсорів, їх використання в мережах 6G та впровадити свій метод ще на етапі збору даних.

– Розробити метод оцінювання ризиків в кібербезпеці.

– Провести експериментальне дослідження розробленого методу на практиці та оцінити його ефективність в реальних умовах.

У результаті науково-технічного обґрунтування розробки методу захисту даних у контексті використання сенсорів 6G визначено велику важливість подальших наукових та технічних досліджень у даній області. Розробка ефективного методу виявляється ключовою для забезпечення конфіденційності та цілісності даних, які обмінюються в мережах 6G, з огляду на їхню високу мобільність та великі обсяги інформації.

Однак аналіз основних вразливостей для отриманої інформації виявив ряд серйозних викликів та потенційних загроз. Зокрема, висока мобільність користувачів та обробка великих обсягів даних створюють унікальні умови для можливих атак. Враховуючи ці вразливості, стає очевидною необхідність розробки надійного методу захисту ще на етапі збору даних.

2 РОЗРОБКА МЕТОДУ ЗАХИСТУ ДАНИХ ОТРИМАНИХ ЗА ДОПОМОГОЮ СЕНСОРІВ 6G

2.1 Основні положення стандарту управління ризиками в кібербезпеці

Для ефективного управління ризиками в галузі інформаційної безпеки було створено міжнародний стандарт ISO/IEC 27005, який був розроблений та опублікований Міжнародною організацією стандартизації ISO та міжнародною електротехнічною комісією IEC. Цей стандарт підтримує інформаційну безпеку за допомогою підходу до управління ризиками. У порівнянні з методами, такими як структура кібербезпеки NIST, цей стандарт проходить сертифікацію [6].

ISO 27005 ґрунтується на вказівках, що містяться у ISO/IEC 27001 та ISO/IEC 27002. Спочатку він був опублікований у червні 2008 року під назвою ISO/IEC 27005:2008, потім перевиданий у 2011 році та знову у 2018. Розділи ISO 27005 з шостого по дванадцятий розробляють стратегію управління ризиками для інформаційних систем. Розділ сьомий деталізує аналіз ризиків, що є основою ефективної стратегії кібербезпеки. Глава восьма присвячена оцінці ризиків, а розділи з дев'ятого по дванадцятий розглядають впровадження та контроль стратегії управління ризиками.

Міжнародна організація стандартизації рекомендує використовувати стандарт ISO 27005 не лише компаніям, але й для державних органів, таких як урядові установи різних рівнів, а також для некомерційних організацій (НКО). На практиці цей стандарт інформаційної безпеки використовується для забезпечення конфіденційності, доступності та цілісності даних основних інформаційних активів організації і призначений для всіх структур, схильних до кіберризиків та зростаючого обсягу даних в межах їхньої діяльності.

Стандарт ISO 27005 є фундаментальним для управління ризиками в інформаційній безпеці та має на меті підтримку надійної реалізації заходів із забезпечення безпеки інформації. Навчання персоналу є необхідним для розвитку навичок ефективного впровадження процесів управління ризиками інформаційної

безпеки. Особи, що пройшли навчання згідно з ISO 27005, володіють здатністю виявляти, аналізувати, вимірювати та усувати ризики.

Стандарт також призначений для допомоги компаніям у впровадженні та налаштуванні Систем Управління Інформаційною Безпекою (СУІБ). Це включає створення процесів та політик кібербезпеки, постійне поліпшення управління ризиками, а також врахування людських і технічних факторів. Згідно з логікою методології безперервного вдосконалення PDCA (плануй, роби, перевіряй, дій) [7]:

– плануй: ідентифікація та оцінка кіберризиків з подальшим стратегічним розглядом відповідних заходів щодо пом'якшення наслідків;

– роби: виконайте розглянуті заходи;

– перевіряй: запустити перевірку продуктивності;

– дій: відстежуйте та покращуйте свою стратегію управління ризиками.

Стандарт містить детальний опис різноманітних підходів до управління ризиками інформаційної безпеки на понад двадцяти сторінках. Його загальна концепція базується на чотирьох основних етапах:

1) Контекстуалізація управління ризиками. Контекстуалізація аналізу ризиків визначає початкову та кінцеву точки управління ризиками. Це також час для встановлення деяких критеріїв:

– критерії оцінки допомагають визначити активи, схильні до ризику кіберризику, і порогові значення, за якими необхідно усувати ризики;

– критерії впливу відповідають мінімальному рівню наслідків, за межами якого слід розглядати ризик;

– критерії прийнятності – це порогові значення нижче яких ризик можна допускати.

2) Оцінка ризиків.

На цьому кроці спочатку визначаємо фактори ризику: організацію, інформаційні системи, групи даних та служби.

На наступному етапі потрібно визначити вразливі місця та загрози, що пов’язані з цими елементами.

Згідно зі стандартом ISO 27005, наступним етапом є узгодження загроз та їх виникнення з потребами безпеки організації. Цей процес сприяє встановленню пріоритетів відповідно до критеріїв, визначених на першому етапі.

Стандарт ISO 27005 допомагає виявити вразливості в галузі кібербезпеки, проте не надає конкретної шкали для оцінки ризиків. Замість цього, команда, відповідальна за впровадження стандартів, повинна розробити власну систему рейтингування. Така система може базуватися на якісних чи кількісних методах оцінки, і останні, в свою чергу, можуть ґрунтуватися на вимірюваних показниках. Важливо відзначити, що аналіз ризиків часто є якісним, оскільки конкретні вказівки відсутні в стандарті ISO. На рисунку 2.1 зображено етапи управління ризиками згідно зі стандартом ISO 27005.

Рисунок 2.1 – Етапи управління ризиками за стандартом ISO 27005

3) Стратегія реагування на ризики

На цьому етапі структура повинна встановити цілі кібербезпеки з урахуванням результатів, що були отримані на другому етапі. Як тільки ці цілі встановлені, можна скласти власні специфікації, що допоможе розробити заходи для боротьби з ризиком.

У ISO 27005 концептуалізація таких заходів означає зважування ризиків та витрат на їхнє виправлення. Після чого є чотири можливі стратегії:

– заперечувати або уникати: заява про те, що ваша організація надто серйозно ставиться до кіберзагроз і її слід уникати за будь-яку ціну. Потім ви можете ухвалити рішення про припинення діяльності, яка може бути причиною цього;

– зередача: об'єкт поділяє ризик із третьою стороною (страховою або субпідрядником з кібербезпеки), яка може принаймні фінансово захистити від ризику;

– пом'якшення: розробка заходів для зниження впливу або ймовірності ризику, щоб зробити його більш прийнятним;

– утримання: ризик вважається прийнятним та недостатньо небезпечним для організації, щоб не брати його до уваги. Кожен варіант має залишковий ризик, який слід систематично оцінювати.

4) Прийняття ризику.

Плани реагування на ризики та залишкові ризики повинні пройти етап "прийняття", що означає отримання затвердження вищого керівництва. На цьому етапі керівники різних відділів можуть висловити сумніви щодо витрат, які їм здаються занадто високими, або взяти на себе певні ризики, при цьому всі винятки мають бути обґрунтовані.

Хоча теоретично методологія ISO 27005 завершується на цьому етапі, важливо відзначити, що виконана організацією робота з впровадження може слугувати частиною її процедур моніторингу та перевірки. Це включає в себе історію виявлених ризиків, сценаріїв, проведений аналіз ризиків та прийняті стратегії виправлення. Зрозуміло, що цю методологію слід регулярно оновлювати на випадок змін у загрозах та вразливостях. Крім того, ця робота сприяє ефективному взаємодії з зацікавленими сторонами.Стандарт керування кіберизиками має декілька переваг. Одним із найбільш примітних є його адаптованість до різних типів організацій та структур Однак йому не вистачає директивного виміру критеріїв аналізу ризиків.

До переваг методології ISO 27005 можна віднести такі характеристики:

– цей метод можна використати самостійно;

– команда розвиває навички, необхідні для структурованого управління кіберризиками;

– він виявляє організаційні слабкості та різні загрози;

– цей метод адаптується до всіх структур, включаючи організації, що адаптуються до умов, які постійно змінюються;

– підвищення довіри зацікавлених сторін.

До недоліків ISO 27005 можна віднести відсутність нормативних аспектів. Коли доводиться визначати галузь управління ризиками, компанія має робити все незалежно від того, чи це критерії ризику чи застосування СУІБ. Тому такий підхід підходить лише для організацій, що готові вкладати значні ресурси в створення власної методології [8].

2.2 Розробка методу оцінювання ризиків в кібербезпеці

Оскільки стандарт ISO 27005 в першу чергу призначений для фахівців у сфері кіберзахисту і, до певної міри, є нестандартним з точки зору конкретних рішень щодо реагування та вимірювання ризиків, його можна характеризувати як якісний. Стандарт ґрунтується на суб'єктивному підході окремих експертів, які вирішують, наскільки серйозним є конкретний кіберризик у даному контексті.

Даний стандарт базується на "досвіді експертів з ІТ" та використовує шкали класифікації ризиків за кольоровою картою, яка варіюється від червоного до зеленого (див. рис. 2.2). Зазвичай, червоний колір вказує на великий ризик чи важливість, а зелений — на низький ризик чи меншу важливість. Це може використовуватися для візуалізації та зрозуміння різних аспектів ризиків в галузі інформаційної безпеки.

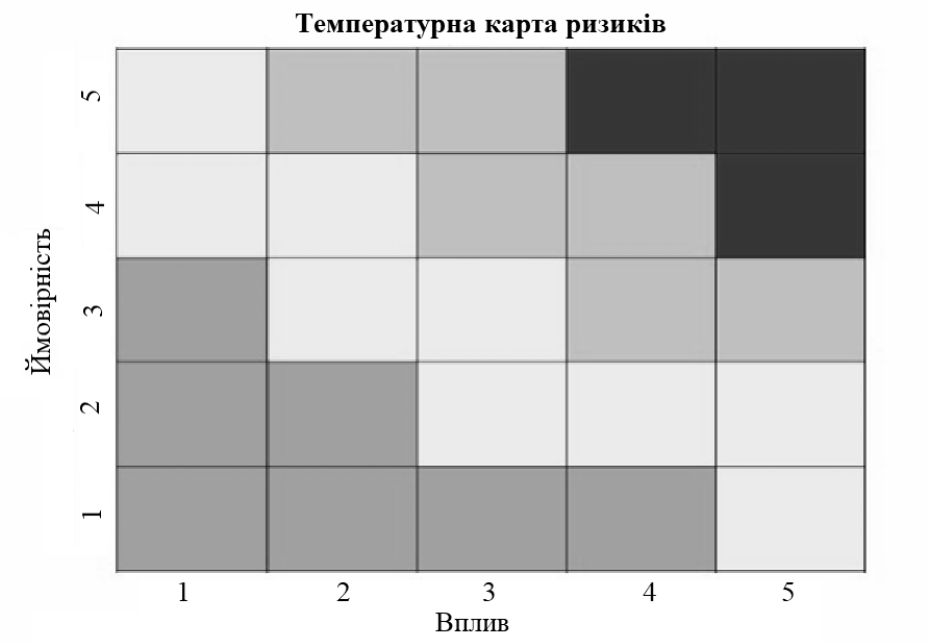


Рисунок 2.2 – Кольорова карта критичності ризику

Звісно, такий підхід сприяє розвитку необхідних навичок кібергігієни та встановленню ефективної практики в галузі кібербезпеки. Однак, оскільки він ґрунтується на суб’єктивному аналізі ризиків, він не забезпечує загальної структури для всіх бізнес-функцій.

Для того, щоб експерт з кібербезпеки, який залучений до оцінювання ризиків, міг швидко та точно розрахувати стан інформаційно-безпечної системи, враховуючи методологію ISO 27005 та надавати зрозумілі показники оцінювання ризиків для всіх бізнес-функцій, необхідно розробити метод оцінювання ризиків. У цьому методі можна використовувати елементи суміжних методологій, де використовуються елементи кількісного виміру для математичної оцінки ризику. Це надасть можливість відповідати критеріям ступеня ризику та забезпечить більш об’єктивний підхід до оцінювання.

Крок 1. На першому етапі введення визначено набори термінів для опису основних станів інформаційної безпеки та їх підмножин. Загальний набір станів інформаційної безпеки, позначений як підмножина "A", поділяється на п'ять підмножин станів:

A_1 – вкрай поганий стан ІБ;

A_2 – поганий стан ІБ;

A_3 – середній стан ІБ;

A_4 – відносно безпечний стан ІБ;

A_5 – максимальний безпечний стан ІБ.

Відповідно до набору А повної множини ризиків інформаційної безпеки, визначеної як підмножина "А", множина загрози В також розподіляється на п'ять підмножин:

B_1 – граничний ризик загрози;

B_2 – високий ризик загрози;

B_3 – середній ризик загрози;

B_4 – низький ризик загрози;

B_5– незначний ризик загрози.

Нехай В прийматиме значення від одиниці до нуля. Для будь-якого окремого показника оцінки інформаційної безпеки позначатиметься F_i де, повний набір його значень позначатиметься як M_i та поділяється на такі підмножини:

M_{i1} – дуже низький рівень M_i;

M_{i2} – низький рівень M_i;

M_i3 – середній рівень M_i;

M_{i4} – високий рівень M_i;

M_{i5} – дуже високого рівня M_i.

Також є умова відповідності множин А, В та М такого вигляду: коли усі показники аналізу мають, згідно класифікації, рівень підмножини M_{ij}, то стан інформаційної безпеки кваліфікується як A_j, і ступінь ризику загрози кваліфікується як B_j.

Виконання такої умови має вплив на вірну кількісну класифікацію всіх рівнів показників.

Крок 2. Побудувати набір показників $F = \{F_i\}$ в кількості $N = 4$, що на думку експерта-аналітика впливає на оцінювання загрози кіберризику (табл. 2.1).

Таблиця 2.1 – Набір показників F

Назва показника	Значення показника
F_1	1.2
F_2	0.7
F_3	0.025
F_4	0.004

Крок 3. Визначимо відповідність для кожного показника рівень його значення для аналізу P_i. Для оцінки такого рівня, необхідно розташувати значення в спадному порядку величин, аби дотримуватися правила:

$$P_i = 1/N \tag{2.1}$$

Необхідно враховувати що, якщо систему показників розмістити в порядку спадання їх значень – значення і-того індексу має визначатися за правилом Фішберна.

$$P_i = \frac{1}{N} = \frac{1}{4} = 0.25 \tag{2.2}$$

Правило Фішберна [19] показує те, що нам нічого не відомо про рівень значення показників (2.1). В той час як оцінка (2.2) яка показує максимум ентропії існуючої невизначеності інформації, що стосується нашого об'єкту дослідження.

Крок 4.Створення класифікації значень b фактора ризику B як критерію поділу даного набору на підмножини (табл. 2.2).

Таблиця 2.2 – Значення показника b.

Інтервал B	Набір назв відповідних підмножинам
$0.8 < b \leq 1$	B_1 –граничний ризик загрози
$0.6 < b \leq 0.8$	B_2 –високий ризик загрози

Продовження таблиці 2.2 – Значення показника b.

$0.4 < b \leq 0.6$	B_3 – середнього ризику загрози
$0.2 < b \leq 0.4$	B_4 – низький ризик загрози
$0 < b \leq 0.2$	B_5– незначна загроза ризику

Крок 5. Створити класифікацію значення f для показників F як критерію поділу повного набору їх значень у підмножині типу M (табл. 2.3).

Таблиця 2.3 – Розподіл відносно підмножини значень

Назва показника	Критерії поділу підмножини				
	M_{i1}	M_{i2}	M_{i3}	M_{i4}	M_{i5}
F_1	$f_1 \leq 0.02$	$0.02 < f_1 \leq 0.16$	$0.16 < f_1 \leq 0.84$	$0.84 < f_1 \leq 1$	$1 < f_1$
F_2	$f_2 \leq 0.02$	$0.02 < f_2 \leq 0.16$	$0.16 < f_2 \leq 0.84$	$0.84 < f_2 \leq 1$	$1 < f_2$
F_3	$f_3 \leq 0.02$	$0.02 < f_3 \leq 0.16$	$0.16 < f_3 \leq 0.84$	$0.84 < f_3 \leq 1$	$1 < f_3$
F_4	$f_4 \leq 0.02$	$0.02 < f_4 \leq 0.16$	$0.16 < f_4 \leq 0.84$	$0.84 < f_4 \leq 1$	$1 < f_4$

Крок 6. Потрібно зробити оцінку поточного рівня показників та обмежити результати (табл. 2.4).

Таблиця 2.4 – Оцінка рівнів показників F.

Назва показника	Діапазон показника F
Дуже високий	$F_1 > 1$
Високий	$0.1 < F_2 \leq 1$
Середній	$0.01 < F_3 \leq 0.1$
Низький	$0.001 < F_4 \leq 0.01$
Дуже низький	< 0.001

Крок 7. На даному кроці ми класифікуємо поточні значення f у відповідності до критеріїв що наведені в таблиці 3. У результаті класифікації маємо таблицю 5:

де $\lambda_{ij} = 1$ при $m_{i(j-1)} < F_i < m_{ij}$ і $\lambda_{ij} = 0$, коли значення не потрапляє у обраний діапазон класифікації (табл. 2.5).

Таблиця 2.5 – Результат класифікації

Назва показника	Значення	Результат класифікації відносно підмножин				
		M_{i1}	M_{i2}	M_{i3}	M_{i4}	M_{i5}
F_1	0.25	0	0	0	0	1
F_2	0.25	0	0	1	0	0
F_3	0.25	0	1	0	0	0
F_4	0.25	1	0	0	0	0

Крок 8. Потрібно виконати арифметичні обчислення для оцінювання ступеня ризику В за допомогою наступної функції:

$$B = \sum_{i=1}^{N} P_i \lambda_{ij} \ \ \sum_{j=1}^{5} b_i, \qquad (2.3)$$

де

$$b_i = 0.8 - 0.2 * (j - 1). \qquad (2.4)$$

Обчислюємо наступним чином:

$$B = 0.2 * 0.25 + 0.4 * 0.25 + 0.6 * 0.25 + 0.8 \ * \ 0.25 = 0.5.$$

Після обчислення значення В бачимо, що його значення відповідає підмножині середнього ризику загрози інформаційної безпеки. А отже отриманий результат ступеня ризику ІБ відповідає результатам дослідження.

2.3 Принцип незв’язності

Принцип незв’язності, представляє собою концепцію, спрямовану на забезпечення максимального рівня анонімності та незалежності даних. У віртуальному та фізичному середовищі цей принцип дозволяє опрацьовувати

інформацію, не розкриваючи ідентичність або внутрішні зв'язки окремих елементів даних.

Даний принцип взаємодіє з даними таким чином, щоб ускладнити або навіть унеможливити встановлення конкретних зв'язків між ними. Основною метою є збереження анонімності та конфіденційності даних, забезпечуючи при цьому можливість їхнього безпечного оброблення та використання.

Вплив принципу незв’язності на конфіденційність та приватність полягає в тому, що він створює ефективний бар'єр для захисту від можливих загроз та забезпечує високий рівень безпеки особистих даних. Обфускація та анонімізація інформації допомагає уникнути витоку чутливих даних та забезпечити надійний захист ідентичності та приватності користувачів.

Головні аспекти та важливість принципу незв'язності:

– Обфускація даних: Використання технік обфускації, таких як шифрування та хешування, допомагає приховати конкретний зміст даних, зробивши їхню інтерпретацію складною чи неможливою без відповідного ключа.

– Захист від атак: Принцип незв'язності створює бар'єр для зловмисників, які можуть намагатися здобути чутливу інформацію, та ускладнює їхні спроби здійснення аналізу та витоку даних.

– Застосування в інтернеті речей (IoT): У сфері IoT, де велика кількість пристроїв обмінюється даними, принцип незв'язності може застосовуватися для забезпечення анонімності та відокремлення ідентифікаційних даних.

– Контроль над доступом: Використання адекватних механізмів контролю доступу до даних разом із засобами незв'язності гарантує, що лише авторизовані користувачі мають доступ до конкретних чутливих даних.

Застосування в різних галузях, таких як транспорт, охорона здоров'я, Інтернет речей та фінансові технології. У кожній сфері він вирішує конкретні завдання забезпечення анонімності та захисту особистих даних, та вирізняється своєю універсальністю та ефективністю в контексті різноманітних викликів, пов'язаних з обробкою та обміном даними в сучасному цифровому світі.

Отже, принцип незв’язності створює ефективний захисний бар'єр для анонімізації та захисту особистих даних, ускладнюючи встановлення зв'язків між ними. Його вплив на конфіденційність та приватність полягає у запобіганні можливим загрозам та наданні високого рівня безпеки. Застосування принципу в різних галузях підкреслює його ефективність та універсальність у вирішенні викликів цифрового обміну даними.

2.4 Метод захисту даних отриманих за допомогою сенсорів 6G

Запропонований метод базується на створенні захисту даних ще на етапі їх збору за принципом незв’язності. Головна мета полягає в тому, щоб зробити інформацію максимально незалежною, ускладнити або навіть унеможливити ідентифікацію взаємозв'язків між різними частинами даних чи об'єктами. Це в свою чергу спрощує або навіть унеможливлює використання трекінгів для порушення приватності та конфіденційності інформації. За цей метод може надати ефективний захист від можливих загроз та забезпечити високий рівень безпеки особистих даних.

Для забезпечення конфіденційності та приватності висувається ідея розділення інформації на конкретні типи об’єктів відповідно до їхніх характеристик, таких як висота, ширина, довжина тощо, що сприятиме захисту конфіденційних даних ще на етапі їх збору. Розроблений клас групи об’єктів дозволяє систематизувати та класифікувати отриману інформацію за різними критеріями, спрощуючи процес її подальшого зберігання та обробки. Поділ інформації на типи об’єктів становить ефективний захисний бар’єр, що сприяє уникненню можливих загроз конфіденційності та збереженню особистої приватності.

В таблиці 2.6 представлено клас групи об’єктів, за допомогою якого сортується отримана інформація на типи об’єктів.

Таблиця 2.6 – клас групи об’єктів для сортування на типи об’єктів

Групи Об’єктів	Розмір висота (м)	Розмір ширина (м)	Розмір Довжина (м)	Тип Об’єкта
Об’єкт 1	1.6	1.9	4.2	Легковий автомобіль
Об’єкт 2	3.6	2.4	10.0	Вантажівка
Об’єкт 3	1.9	0.5	1.9	Велосипед
Об’єкт 4	1.8	0.5	0.3	Пішохідний

Наведено приклад типу “Пішохідний”. На рисунку 2.3 представлено приклад типу “Пішохідний”.

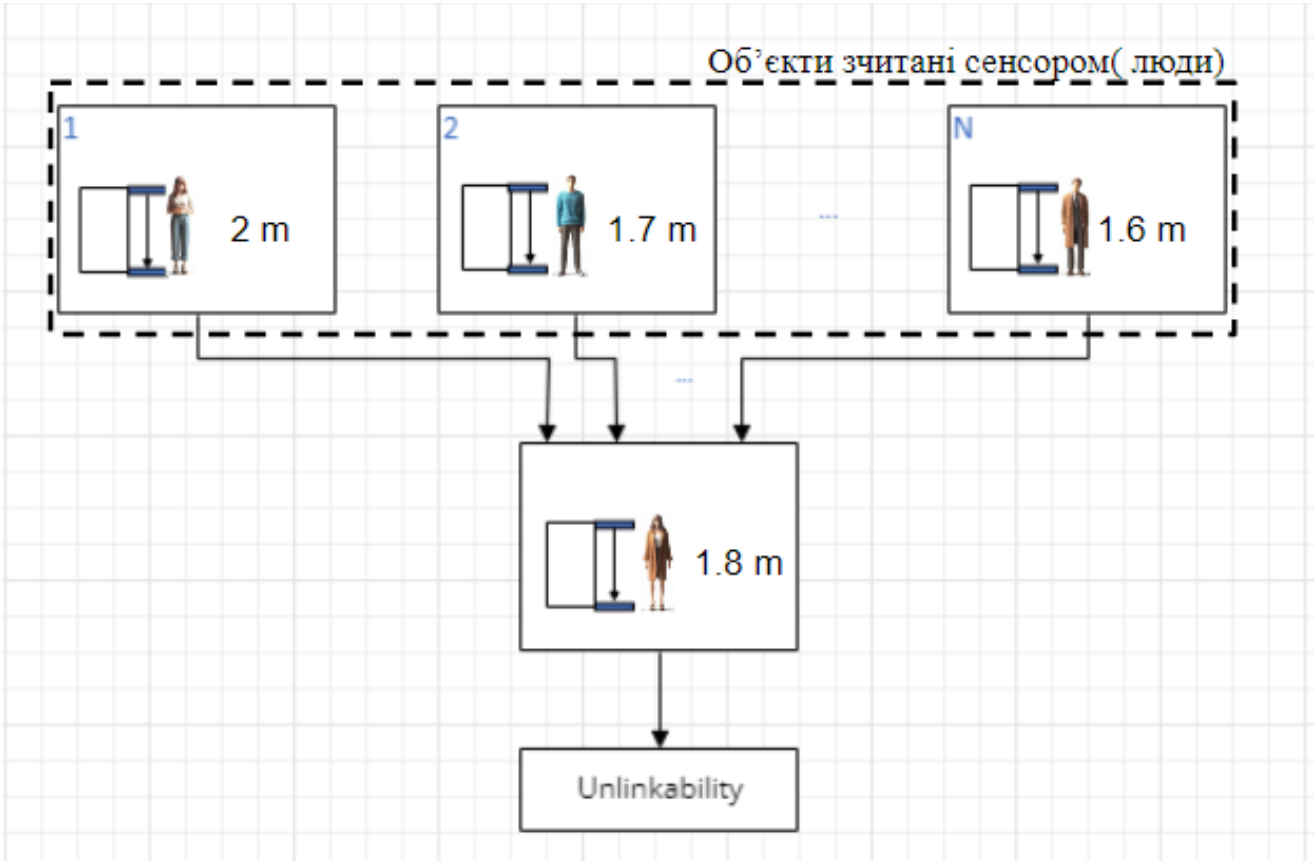


Рисунок 2.3 – Тип об’єкта “Пішохідний”

Сенсор, який реалізує принцип незв’язності, працює шляхом збору унікальних фізичних характеристик людей та їх подальшої обфускації. Під час цього процесу різноманітні та індивідуальні риси, які визначають фізичні особливості кожної людини, агрегуються в єдиний, стандартизований тип – уніфікований розмір 1.80.

Ця стратегія спрямована на збереження анонімності та приватності осіб, ускладнюючи або навіть унеможливлюючи можливість ідентифікації осіб за їхніми фізичними параметрами. Отриманий результат служить ефективним засобом захисту особистих даних та утримує велику різноманітність індивідуальних характеристик у рамках універсального стандарту. Це сприяє створенню абстрактної та агрегованої статистичної інформації, унеможливлюючи встановлення конкретних зв'язків між окремими особами на основі їхніх фізичних даних.

Після успішного процесу обфускації, який ґрунтується на принципі незв’язності, зашифровані дані надсилаються на центральний комп'ютер автомобіля(Onboard). Далі ці дані передаються на вишку RSU (Roadside Unit) та центральний комп'ютер(Onboard) інших учасників дорожнього руху у випадку, якщо вони знаходяться поруч.

Структурна схема процесу передачі обфускованих даних за принципом незв’язності в автомобільній мереж представлена на рисунку 2.4.

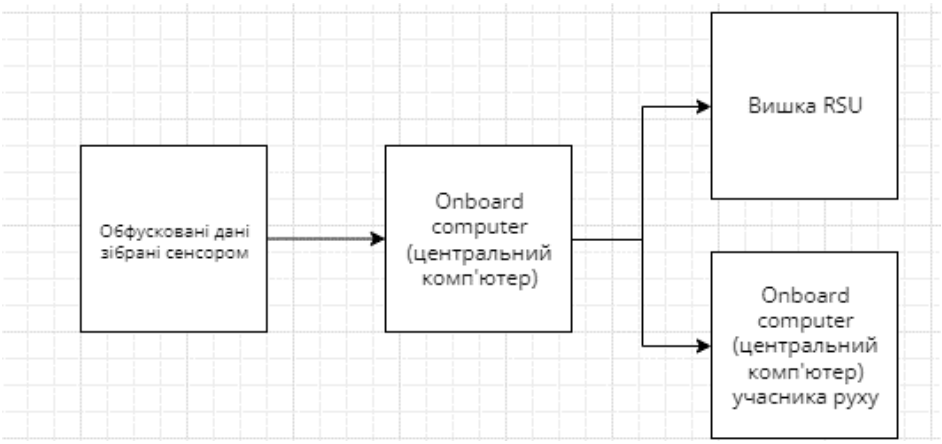


Рисунок 2.4 – Структурна схема процесу обфускації та передачі даних в автомобільній мережі

Цей механізм обміну інформацією сприяє взаємодії та спільному використанню безпечних та анонімізованих даних між автомобілями та іншими елементами інфраструктури. За допомогою принципу незв’язності, який забезпечує абстракцію та високий рівень захисту конфіденційності, система може взаємодіяти з іншими учасниками руху, не ризикуючи витоком особистої інформації.

Даний підхід до обміну даними сприяє створенню безпечного та ефективного середовища для взаємодії транспортних засобів та інфраструктури, забезпечуючи одночасно захист приватності учасників дорожнього руху.

Загальна сруктурна схема обміну даними в автомобільній мережі 6G зображено на рисунку 2.5.

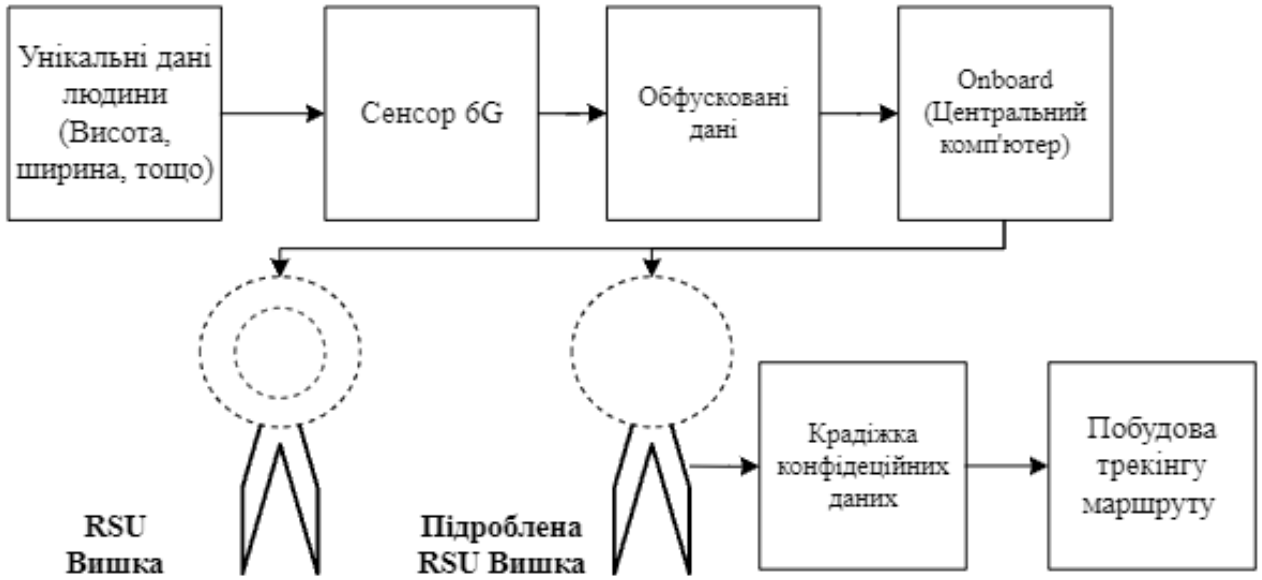


Рисунок 2.5 – Загальна сруктурна схема обміну даними в автомобільній мережі 6G

На основі проведеного аналізу можна впевнено стверджувати, що запропонований метод забезпечує високий рівень захисту інформації ще на етапі її збору. Навіть у випадку успішного перехоплення даних зловмисником шляхом підміни легітимної вишки RSU (рисунок 2.5), система використовує принцип незв’язності, що ускладнює або навіть унеможливлює побудову трекінгу маршруту особи.

Такий підхід не лише робить інформацію стійкою до перехоплення, а й гарантує, що навіть у випадку втрати легітимності вишки RSU, зловмисник не матиме змоги визначити маршрут конкретної людини. Такий високий рівень безпеки та приватності важливий для забезпечення довіри та успішного впровадження технологій обміну даними в мережах 6G.

Отже, запропонований метод, базуючись на принципі незв’язності, демонструє високий рівень ефективності в забезпеченні безпеки особистих даних ще на етапі їх збору. Основна мета цього підходу полягає в тому, щоб робити інформацію максимально незалежною та ускладнювати або навіть унеможливлювати ідентифікацію взаємозв'язків між різними частинами даних чи об'єктами.

Введення розділення інформації на конкретні типи об’єктів відповідно до їхніх характеристик є раціональним інструментом для захисту конфіденційних даних ще на етапі їх збору. Використання класу групи об’єктів спрощує систематизацію та класифікацію інформації, що в свою чергу полегшує подальший її облік та обробку. Поділ інформації на типи об’єктів встановлює ефективний захисний бар’єр, сприяючи уникненню можливих загроз конфіденційності та збереженню особистої приватності.

Враховуючи принцип незв’язності, сенсор, який здійснює збір фізичних характеристик, створює абстрактну, уніфіковану інформацію, ускладнюючи можливість ідентифікації осіб за їхніми фізичними параметрами. Це служить важливим заходом для збереження анонімності та захисту особистих даних.

Процес обфускації та подальша передача даних на центральний комп'ютер та іншим учасникам руху, враховуючи принцип незв’язності, сприяє створенню безпечного та ефективного середовища для обміну інформацією між транспортними засобами та інфраструктурою.

3 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ

Трекінг - це процес визначення та фіксації місцезнаходження об'єкта в просторі протягом часу. Цей термін широко використовується в різних контекстах, включаючи технології, спорт, дослідження та інші області [16].

"Track Closely Spaced Targets Under Ambiguity in Simulink" вказує на відстеження близько розташованих цілей в умовах невизначеності за допомогою Simulink.

Simulink - це інструмент для моделювання, аналізу та симуляції динамічних систем в середовищі MATLAB.

MATLAB - це інтерактивне середовище для виконання обчислень, аналізу даних, візуалізації та моделювання. Це програмне забезпечення, яке широко використовується в наукових, інженерних та математичних областях.

JPDA (Joint Probabilistic Data Association) є методом трекінгу, який використовується для відстеження об'єктів в умовах близькості та невизначеності відомостей, особливо коли об'єкти знаходяться дуже близько один до одного і можуть бути важко ідентифікувати [17].

Розглянемо сновні риси JPDA:

– Ймовірнісна асоціація даних. Використовує ймовірність асоціації для оцінювання ймовірностей того, що конкретний детектор відноситься до конкретного об'єкта. Це важливо в умовах невизначеності та можливості багатоасоціативних ситуацій.

– Сумісна оцінка. JPDA здатний робити сумісні оцінки для кількох гіпотез асоціацій, що дозволяє враховувати невизначеність та неоднозначність відомостей.

– Врахування близькості. Цей метод спеціально адаптований для вирішення задач трекінгу, де об'єкти розташовані дуже близько один до одного, що може призводити до невизначеності в рішеннях.

– Рекурсивна оцінка. JPDA використовує рекурсивні методи для постійного оновлення ймовірностей асоціацій та корекції треків об'єктів в часі.

Ймовірнісна асоціація даних дозволяє JPDA краще управляти ситуаціями, коли ідентифікація конкретного об'єкта ускладнена або може бути помилковою. Це дозволяє системі трекінгу працювати ефективно в умовах більшої невизначеності та близькості об'єктів, що робить JPDA важливим методом для застосувань, де можлива така ситуація, наприклад, в моніторингу транспортних потоків або системах слідкування.

Принцип роботи JPDA (Joint Probabilistic Data Association) в системі трекінгу "Track Closely Spaced Targets Under Ambiguity in Simulink" базується на ймовірнісній оцінці та асоціації даних для ефективного відстеження об'єктів, які знаходяться дуже близько один до одного і можуть викликати амбігвітність в ідентифікації [17].

Ймовірнісна оцінка — це метод визначення ймовірності того чи іншого явища або події. Цей підхід використовує ймовірність, яка є числовим значенням від 0 до 1, що вказує на ймовірність того, що певна подія відбудеться або не відбудеться.

Ймовірнісна оцінка може враховувати різні чинники та джерела даних для визначення ймовірностей. Вона є основою для багатьох математичних методів та моделей, особливо в статистиці та теорії ймовірностей.

Термін "амбігвітність" вказує на стан чи властивість чого-небудь, що має багатозначність або може розумітися різними способами. Це може включати в себе ситуації, коли інформація або обставини можуть тлумачитися або розумітися різними способами, що призводить до невизначеності чи конфузії.

У випадку розгляду трекінгу об'єктів під амбігвітністю може розумітися те, що існують умови, де ідентифікація чи відстеження об'єктів може бути ускладненою через їхню близькість один до одного, недостатню інформацію чи інші фактори, які можуть призвести до неоднозначності у визначенні їхньої ідентифікації чи руху.

Принцип роботи JPDA включає:

– Отримання даних: Система отримує вхідні дані від сенсорів, що можуть включати в себе інформацію про положення та характеристики об'єктів, які підлягають трекінгу.

– Детекція об'єктів: Для кожного об'єкта проводиться процес детекції, визначення ймовірності його присутності та характеристик.

– Оцінка ймовірностей асоціації: JPDA використовує ймовірнісні моделі для оцінки ймовірностей того, що конкретний детектор асоціюється з конкретним об'єктом.

– Асоціація даних: На основі отриманих ймовірностей система вирішує, які детектори асоціюються з якими об'єктами. Оскільки деякі детектори можуть бути спільно асоційовані з різними об'єктами, JPDA враховує цю неоднозначність у своїй моделі.

– Сумісна оцінка: За допомогою ймовірнісних моделей JPDA створює сумісні оцінки для кількох гіпотез асоціацій, що враховує невизначеність та амбігвітність відомостей.

– Корекція треків: На основі отриманих асоціацій система коригує і поновлює треки об'єктів в часі.

Структурна схема алгоритму роботи трекінгу JPDA зображено на рисунку 3.1.

Рисунок 3.1 – Структурна схема алгоритму роботи трекінгу JPDA

Даний процес дозволяє системі трекінгу ефективно враховувати невизначеність в умовах близькості об'єктів та амбігвітності в ідентифікації, що є важливим для точного та надійного відстеження в умовах обмеженого простору або інших викликів, пов'язаних із суміщенням об'єктів.

3.1 Моделювання руху людини по отриманих даних із сенсорів 6G, без обфускації

У даному розділі проведено моделювання руху людини по отриманих даних із сенсорів 6G, без обфускації. Наведемо вікно із застосунку для моделювання на рисунку 3.2. Дані для моделювання беремо із Github інституту Barkhausen (Towards Deep Radar Perception for Autonomous Driving: Datasets) [18].

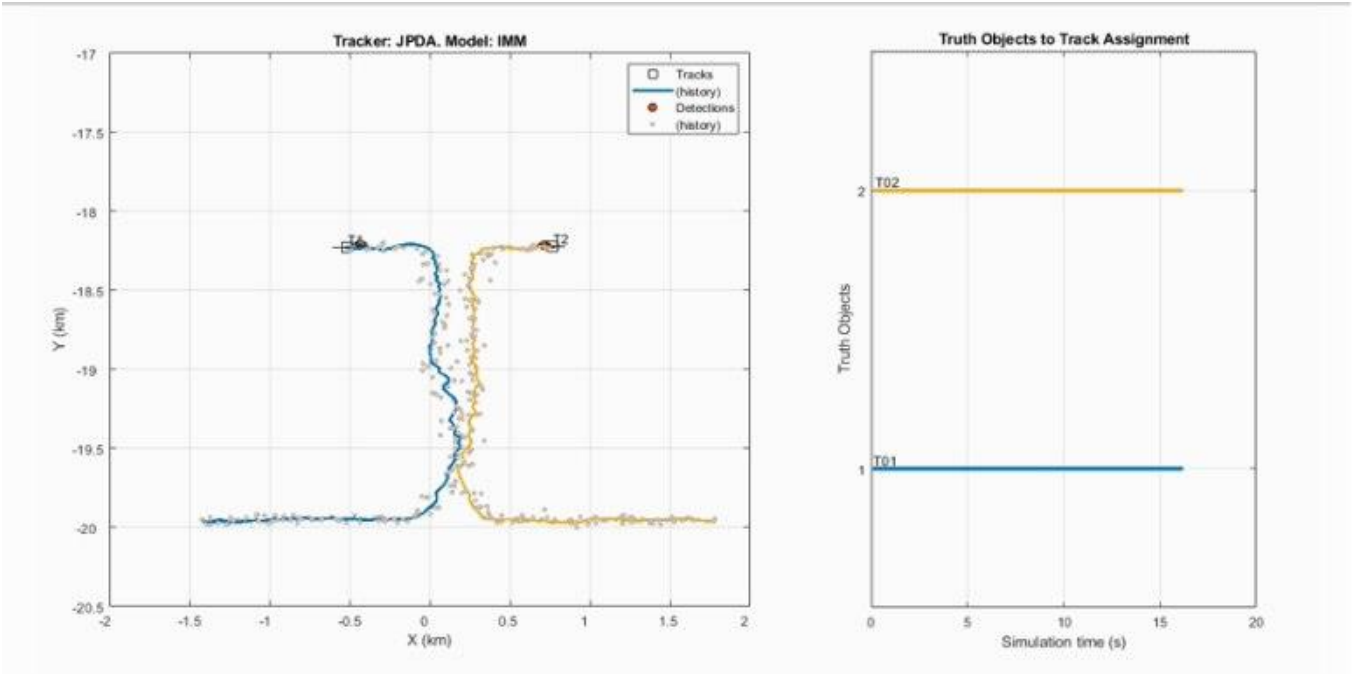


Рисунок 3.2 – Вікно з програмного застосунку для моделювання(без обфускації)

Провівши аналіз можна сказати, що передача даних без обфускації створює потенційні загрози для конфіденційності та приватності користувачів. Зловмисники, які перехоплюють ці дані, можуть легко проаналізувати їх та використовувати для створення трекінгу руху осіб.

Такий сценарій викликає серйозні обліки щодо захисту особистої інформації, оскільки вони можуть бути використані без дозволу та відстежувати рухи людей. Це може порушити особисту приватність та викликати побоювання щодо можливого зловживання цієї інформації.

Обфускація даних за принципом незв'язності в цьому контексті виявляється важливою стратегією для захисту приватності. Вона спрямована на ускладнення або навіть унеможливлення ідентифікації осіб на основі їхніх фізичних даних. Застосування цього принципу дозволяє зберігати анонімність та унікальність фізичних характеристик, роблячи трекінг значно складнішим для потенційних зловмисників.

3.2 Моделювання руху людини по отриманих даних із сенсорів 6G, з обфускацією

У даному розділі проведено моделювання руху людини по отриманих даних із сенсорів 6G, без обфускації. Наведемо вікно із застосунку для моделювання на рисунку 3.3.

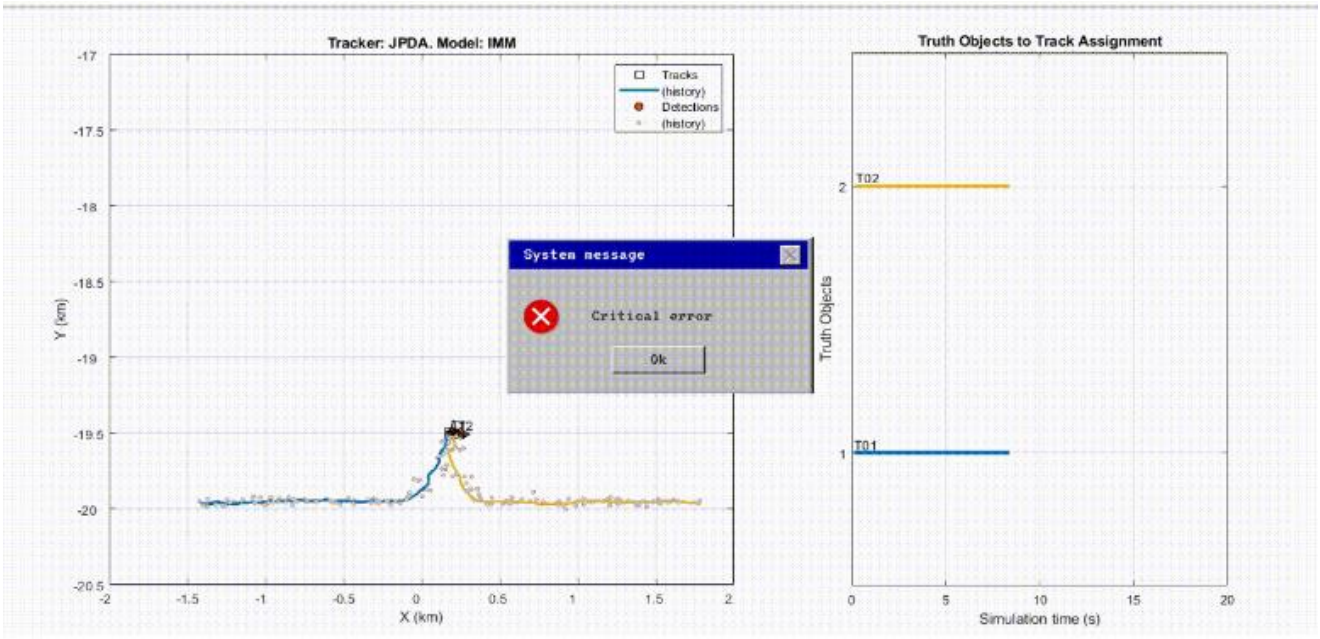


Рисунок 3.3 – Вікно з програмного застосунку для моделювання(без обфускації)

Програмний застосунок для моделювання завершився із помилкою з неможливістю згенерувати шлях руху об’єкту, що свідчить про ефективність даного методу.

Розроблений метод захисту буде представлено на науково-практичні інтернет-конференції "Молодь в науці: дослідження, проблеми, перспективи (МН- 2024) [20].

Отже, розділ присвячений вивченню трекінгу, використовуючи "Track Closely Spaced Targets Under Ambiguity in Simulink" та систему JPDA. Метод JPDA, який використовує ймовірнісну оцінку та асоціацію даних, ефективно вирішує завдання в умовах невизначеності та близькості об'єктів, що забезпечує точні результати визначення місцезнаходження об'єкта.

Результати моделювання руху людини без застосування обфускації на основі даних із сенсорів 6G підкреслили серйозні загрози для конфіденційності та приватності користувачів. Невідповідна захищеність може легко дозволити зловмисникам створювати трекінг руху осіб і порушувати їхню конфіденційність та приватність.

У той же час, спроба моделювання з обфускацією завершилася невдачею, що підкреслює актуальність та ефективність дослідження.

4 ЕКОНОМІЧНА ЧАСТИНА

Виконання науково-дослідної роботи завжди передбачає отримання певних результатів і вимагає відповідних витрат. Результати виконаної роботи завжди дають нам нові знання, які в подальшому можуть бути використані для удосконалення та/або розробки (побудови) нових, більш продуктивних зразків техніки, процесів та програмного забезпечення.

Дослідження на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G» може бути віднесено до фундаментальних і пошукових наукових досліджень і спрямоване на вирішення наукових проблем, пов’язаних з практичним застосуванням. Основою таких досліджень є науковий ефект, який виражається в отриманні наукових результатів, які збільшують обсяг знань про природу, техніку та суспільство, які розвивають теоретичну базу в тому чи іншому науковому напрямку, що дозволяє виявити нові закономірності, які можуть використовуватися на практиці.

Для цього випадку виконаємо такі етапи робіт:

1) здійснимо проведення наукового аудиту досліджень, тобто встановлення їх наукового рівня та значимості;

2) проведемо планування витрат на проведення наукових досліджень;

4.1 Оцінювання наукового ефекту

Основними ознаками наукового ефекту науково-дослідної роботи є новизна роботи, рівень її теоретичного опрацювання, перспективність, рівень розповсюдження результатів, можливість реалізації. Науковий ефект НДР на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G» можна охарактеризувати двома показниками: ступенем наукової новизни та рівнем теоретичного опрацювання.

Значення показників ступеня новизни і рівня теоретичного опрацювання науково-дослідної роботи в балах наведені в табл. 4.1 та 4.2, які було отримано із методички до роботи [21].

Таблиця 4.1 – Показники ступеня новизни науково-дослідної роботи виставлені експертами

Ступінь новизни	Характеристика ступеня новизни	Значення ступеня новизни, бали		
		Експерти (ПІБ, посада)		
		1	2	3
Принципово нова	Робота якісно нова за постановкою задачі і ґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отримані принципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод	-	-	-
Нова	Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів	56	60	58
Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв’язок (або знайдено новий зв’язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об’єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональна модифікація (з ознаками новизни)	-	-	-
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим	-	-	-
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам	-	-	-
Середнє значення балів експертів		58,0		

Згідно отриманого середнього значення балів експертів ступінь новизни характеризується як нова, тобто отримана нова інформація, яка суттєво зменшує невизначеність наявних знань (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту) та проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів.

Таблиця 4.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи виставлені експертами

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Експерт (ПІБ, посада)		
	1	2	3
Відкриття закону, розробка теорії	-	-	-
Глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	68	70	66
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	-	-	-
Елементарний аналіз зв'язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо	-	-	-
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	-	-	-
Середнє значення балів експертів	68,0		

Згідно отриманого середнього значення балів експертів рівень теоретичного опрацювання науково-дослідної роботи характеризується як глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу.

Показник, який характеризує рівень наукового ефекту, визначаємо за формулою.

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор}, \qquad (4.1)$$

де $k_{нов}, k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{нов} = 58{,}0, k_{теор} = 68{,}0$ балів;

0,6 та 0,4 – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{нау} = 0{,}6 \cdot k_{нов} + 0{,}4 \cdot k_{теор} = 0{,}6 \cdot 58{,}0 + 0{,}4 \cdot 68{,}00 = 62{,}00 \text{ балів.}$$

Визначення характеристики показника $E_{нау}$ проводиться на основі висновків експертів виходячи з граничних значень, які наведені в табл. 4.3.

Таблиця 4.3 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Відповідно до визначеного рівня наукового ефекту проведеної науково-дослідної роботи на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G», даний рівень становить 62,00 балів і відповідає статусу – середній рівень. Тобто у даному випадку можна вести мову про потенційну фактичну ефективність науково-дослідної роботи.

4.2 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G», під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.2.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам, технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та

іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою:

$$З_о = \sum_{i=1}^{k} \frac{М_{ni} \cdot t_i}{Т_р}, \quad (4.2)$$

де k – кількість посад дослідників залучених до процесу досліджень;

$М_{ni}$ – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

$Т_р$ – середнє число робочих днів в місяці, $Т_р$=24 дні.

$$З_о = 19400{,}00 \cdot 24 / 24 = 19400{,}00 \; грн.$$

Проведені розрахунки зведемо до таблиці.

Таблиця 4.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	19400,00	808,33	24	19400,00
Науковий співробітник	19150,00	797,91	14	11170,74
Інженер-програміст 1-ї категорії	19050,00	793,75	24	19050,00
Лаборант	8750,00	364,58	15	5468,70
Всього				55089,44

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G» розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} С_i \cdot t_i, \quad (4.3)$$

де $С_i$ – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}}, \quad (4.4)$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо $Мм$=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. 4.5).

Таблиця 4.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Встановлення допоміжного обладнання	8,50	2	1,10	63,34	538,36
Інсталяція програмного забезпечення	6,25	3	1,35	77,73	485,82
Калібрування сенсорів	5,20	5	1,70	97,88	508,99
Налаштування програмних застосунків	5,50	4	1,50	86,37	475,02
Підготовка дослідження	8,00	4	1,50	86,37	690,94
Формування бази даних результатів дослідження	14,00	2	1,10	63,34	886,70
Всього					3585,82

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 24 дн;

$t_{зм}$ – тривалість зміни, год.

C_1 = 6700,00 · 1,10 · 1,65 / (24 · 8) = 63,34 *грн.*

$З_{р1}$ = 63,34 · 8,50 = 538,36 *грн.*

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.5)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 11%.

$З_{дод}$ = (55089,44 + 3585,82) · 11 / 100% = 6454,27 грн.

4.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad (4.6)$$

де $Н_{зп}$ – норма нарахування на заробітну плату. Приймаємо 22%.

Зн = (55089,44 + 3585,82 + 6454,27) · 22 / 100% = 14328,49 грн.

4.2.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою «Метод захисту даних, отриманих за допомогою сенсорів 6G».

Витрати на матеріали на даному етапі проведення досліджень в основному пов’язані з використанням моделей елементів та моделювання роботи і досліджень за допомогою комп’ютерної техніки та створення експериментальних математичних моделей або програмного забезпечення, тому дані витрати формуються на основі витратних матеріалів характерних для офісних робіт.

Витрати на матеріали ($М$), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$M = \sum_{j=1}^{n} H_j \cdot Ц_j \cdot K_j - \sum_{j=1}^{n} B_j \cdot Ц_{вj}, \quad (4.7)$$

де H_j – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

K_j – коефіцієнт транспортних витрат, ($K_j = 1,1 \ldots 1,15$);

B_j – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів j-го найменування, грн/кг.

$M_1 = 2,0 \cdot 225,00 \cdot 1,11 – 0 \cdot 0 = 499,50$ *грн.*

Витрати на комплектуючі *($K_в$)*, які використовують при проведенні НДР на тему «Метод захисту даних отриманих за допомогою сенсорів 6G», розраховуємо, згідно з їхньою номенклатурою.

Проведені розрахунки зведемо до таблиці 4.6.

Таблиця 4.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір канцелярський офісний (А4)	225,00	2,0	-	-	499,50
Папір для заміток (А5)	116,00	4,0	-	-	515,04
Начиння канцелярське	195,00	3,0	-	-	649,35
Органайзер офісний	183,00	3,0	-	-	609,39
Картридж для принтера	950,00	1,0	-	-	1054,50
USB флеш накопичувач Transcend 16Gb JetFlash 700 (TS64GJF700)	200,00	1,0	-	-	222,00
Всього					3549,78

4.2.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G», розраховуємо, згідно з їхньою номенклатурою, за формулою:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \quad (4.8)$$

де $Н_j$ – кількість комплектуючих *j*-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих *j*-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ *= 1,1 ... 1,15*).

$К_в = 1 \cdot 3079{,}00 \cdot 1{,}11 = 3417{,}69$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.7 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Зовнішній жорсткий диск 2.5" 2TB Seagate (STGD2000200)	1	3079,00	3417,69
Концентратор Defender SEPTIMA SLIM (83505)	1	599,00	664,89
Кабель для передачі даних USB to COM 1.0m Patron (CAB-PN-USB-COM)	1	354,00	392,94
Всього			4867,52

4.2.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення.

Балансову вартість спецустаткування розраховуємо за формулою:

$$В_{спец} = \sum_{i=1}^{k} Ц_i \cdot С_{пр.i} \cdot К_i \ , \quad (4.9)$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, грн;

$C_{пр.і}$ –кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

$К_і$ – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, ($К_і = 1,10…1,12$);

k – кількість найменувань устаткування.

$В_{спец} = 3400,00 \cdot 1 \cdot 1,11 = 3774,00$ грн.

Отримані результати зведемо до таблиці:

Таблиця 4.8 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Маршрутизатор Mikrotik hAP ax2 (C52iG-5HaxD2HaxD-TC)	1	3400,00	3774,00
Радар AWR2944EVM	1	20000,00	22200,00
R&S AREG800A (спектральний аналізатор)	1	8100,00	8991,00
Всього			34965,00

4.2.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$В_{прг} = \sum_{i=1}^{k} Ц_{іпрг} \cdot С_{прг.і} \cdot К_і \ , \qquad (4.10)$$

де $Ц_{іпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$С_{прг.і}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

$К_і$ – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($К_і = 1,10…1,12$);

k – кількість найменувань програмних засобів.

Отримані результати зведемо до таблиці:

Таблиця 4.9 – Витрати на придбання програмних засобів по кожному виду

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Прикладне програмне забезпечення до радару AWR2944EVM	1	free	free
Прикладне програмне забезпечення для тестування методу захисту	1	free(Trial Software)	free(Trial Software)
Всього			0

4.2.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (53000{,}00 \cdot 1) / (2 \cdot 12) = 2208{,}33$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Ноутбук Lenovo Thinkpad T14 Gen 2, оперативна пам'ять 16GB, процесор Intel core i7-1185G7.	53000,00	2	1	2208,33
Робоче місце інженера	8752,00	5	1	145,87
Пристрої передачі даних	6810,00	2	1	283,75
Пристрій виводу інформації	6791,00	5	1	113,18
Оргтехніка	8300,00	4	1	172,92
Приміщення лабораторії	500000,00	20	1	2083,33
ОС Windows 10	8360,00	2	1	348,33
Прикладний пакет Microsoft Office 2023	7900,00	2	1	329,17
Всього				5684,88

4.2.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.12)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

Таблиця 4.11 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Ноутбук Lenovo Thinkpad T14 Gen 2, оперативна пам'ять 16GB, процесор Intel core i7-1185G7, пам'ять на жорсткому диску 256 GB	0,04	180,0	50,77
Робоче місце інженера	0,10	180,0	126,92
Пристрої передачі даних	0,01	180,0	12,69

Продовження таблиці 4.11 – Витрати на електроенергію

Пристрій виводу інформації	0,50	10,0	35,25
Оргтехніка	0,62	2,0	8,74
Маршрутизатор Mikrotik hAP ax2 (C52iG-5HaxD2HaxD-TC)	0,01	180,0	12,69
Всього			247,06

$Ц_е$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_е$ = 7,20 грн;

$К_{вп і}$ – коефіцієнт, що враховує використання потужності, $К_{вп і} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$В_е = 0,04 \cdot 180,0 \cdot 7,20 \cdot 0,95 / 0,97 = 50,77$ *грн.*

Проведені розрахунки зведемо до таблиці.

4.2.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Метод захисту даних отриманих за допомогою сенсорів 6G» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов’язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з’їзди, конференції, наради, пов’язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \quad (4.13)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 20%.

$В_{св} = (55089,44 + 3585,82) \cdot 20 / 100\% = 11735,05$ *грн.*

4.2.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» розраховуємо як 30…45% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{сп} = (З_о + З_р) \cdot \frac{Н_{сп}}{100\%}, \quad (4.14)$$

де $Н_{сп}$ – норма нарахування за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації», приймемо $Н_{сп}$= 30%.

$B_{сп}$ = (55089,44 + *3585,82) · 30 / 100% = 17602,57 грн.*

4.2.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$І_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.15)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 60%.

$І_в$ = (55089,44+ *3585,82) · 60 / 100% = 35205,15 грн.*

4.2.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати».. До них належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.16)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 130%.

$B_{нзв}$ = (55089,44 + 3585,82) · 130 / 100% = 76277,83 грн.

Витрати на проведення науково-дослідної роботи на тему «Методи захисту даних, отриманих за допомогою сенсорів 6G» розраховуємо як суму всіх попередніх статей витрат за формулою:

$$B_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + B_{спец} + B_{прг} + A_{обл} + B_е + B_{св} + B_{сп} + I_в + B_{нзв}. \quad (4.17)$$

$B_{заг}$= 55089,44 +3585,82 +6454,27 +14328,49 +3549,78+4867,52+34965,00 +0 + 5684,88+247,06+11735,05 +17602,57 +35205,15 +76277,83 = 269592,86 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.18)$$

де η – коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η =0,95.

ЗВ = 269592,86 / 0,95 = 283781,95 грн.

4.3 Оцінювання важливості та наукової значимості науково-дослідної роботи

Оцінювання та доведення ефективності виконання науково-дослідної роботи фундаментального чи пошукового характеру є достатньо складним процесом і часто базується на експертних оцінках, тому має вірогідний характер.

Для обґрунтування доцільності виконання науково-дослідної роботи на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G» використовується спеціальний комплексний показник, що враховує важливість, результативність роботи, можливість впровадження її результатів у виробництво, величину витрат на роботу.

Комплексний показник K_P рівня науково-дослідної роботи — це зважена комбінація різноманітних метрик та показників, яка використовується для оцінки та порівняння рівня науково-дослідної активності чи продуктивності науково-дослідницьких груп, організацій, країн або інших суб'єктів. Такий комплексний показник може враховувати різні аспекти дослідницької діяльності та намагається відобразити їх узагальненим числовим значенням, та може бути розрахований за формулою [21]:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \tag{4.19}$$

де I – коефіцієнт важливості роботи. Приймемо $I = 4$;

n – коефіцієнт використання результатів роботи; $n = 0$, коли результати роботи не будуть використовуватись; $n = 1$, коли результати роботи будуть використовуватись частково; $n = 2$, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках; $n = 3$, коли результати можуть використовуватись навіть без проведення дослідно-конструкторських розробок. Приймемо n=2;

T_C – коефіцієнт складності роботи. Приймемо $T_C = 3$;

R – коефіцієнт результативності роботи; якщо результати роботи плануються вище відомих, то $R = 4$; якщо результати роботи відповідають відомому рівню, то $R = 3$; якщо нижче відомих результатів, то $R = 1$. Приймемо $R = 4$;

B – вартість науково-дослідної роботи, тис. грн. Приймемо B =*283781,95* грн;

t – час проведення дослідження. Приймемо t = 0,08 років, (1 міс.).

Визначення показників *I, n, T_C, R, B, t* здійснюється експертним шляхом або на основі нормативів.

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t} = 4^2 \cdot 3 \cdot 4 \,/\, 283{,}7 \cdot 0{,}08 = 8{,}45.$$

Якщо $K_P > 1$, то науково-дослідну роботу на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G» можна вважати ефективною з високим науковим, технічним і економічним рівнем.

Таким чином, у даному розділ було проведено економічне тестування та витрати на проведення науково-дослідної роботи на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G» складають *283781,95* грн. Відповідно до проведеного аналізу та розрахунків рівень наукового ефекту проведеної науково-дослідної роботи на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G» є середній, а дослідження актуальними, рівень доцільності виконання науково-дослідної роботи $K_P > 1$, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

ВИСНОВКИ

У результаті проведеного дослідження методів та стратегій захисту даних, зібраних сенсорами в мережі 6G. Основним об'єктом уваги став процес збору, передачі та обробки інформації, а предметом – методи та стратегії її захисту. Мета магістерської роботи полягала в удосконаленні існуючих методів захисту даних у контексті сенсорів 6G.

Для досягнення цієї мети було проведено аналіз існуючих методів збору та сортування інформації від сенсорів 6G, удосконалено методи та розроблено власну методику захисту даних на етапі їхнього збору. Проведене експериментальне дослідження підсистеми дозволило визначити ефективність запропонованих методів захисту.

Новизною дослідження є розроблений метод захисту даних на етапі збору, спрямований на вирішення актуальних проблем конфіденційності даних у мережі 6G. Розроблений метод має важливе практичне значення, забезпечуючи високий рівень безпеки та конфіденційності даних у високотехнологічному світі майбутнього.

Відповідно до проведеного аналізу та розрахунків, рівень наукового ефекту проведеної науково-дослідної роботи на тему «Метод захисту даних, отриманих за допомогою сенсорів 6G» становить 8,45(середній рівень), а витрати 283781,95 грн, що свідчить про потенційну ефективність роботи з високим науковим, технічним і економічним рівнем.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Грінвуд, Д. Безпека високошвидкісних бездротових мереж 6G. Журнал мережевих технологій, 2022, № 3, с. 45-56.
2. Хендерсон, М. Кіберзахист в умовах високої мобільності в мережах 6G: виклики та перспективи. Міжнародна конференція з безпеки мереж і систем, 2021, с. 112-125.
3. Стівенсон, Р. Аналіз вразливостей та розробка стратегій захисту конфіденційності в мережах 6G. Журнал кібербезпеки, 2021, № 4, с. 33-46.
4. Ім, Л. та Ю, Ч. Захист від розподілених атак на збої обслуговування в мережах 6G. Технічні науки та інженерія, 2019, № 1, с. 56-67.
5. Дод, Д. Сучасні методи захисту в умовах високої мобільності в мережах 6G. Міжнародна конференція з кіберзахисту, 2022, с. 210-223.
6. Everything you need to know about ISO 27005. URL: https://www.c-risk.com/en/blog/iso-27005/ (дата звернення: 02.11.2023).
7. The FAIR™ Methodology for Cyber Risks. URL: https://www.c-risk.com/en/blog/fair-analysis/ (дата звернення: 05.11.2023).
8. Оновлений стандарт ISO/IEC 27005. URL: http://csm.kiev.ua/ index.php (дата звернення: 07.11.2023)
9. Технічні характеристики та принципи роботи сенсора AWR2944 [Електронний ресурс]. URL: https://www.ti.com/tool/AWR2944EVM (дата звернення: 10.11.2023).
10. The Doppler Effect AWR2944 [Електронний ресурс]. URL: https://phys.libretexts.org/Bookshelves/University_Physics/Book%3A_University_Physics_(OpenStax)/Book%3A_University_Physics_I_-_Mechanics_Sound_Oscillations_and_Waves_(OpenStax)/17%3A_Sound/17.08%3A_The_Doppler_Effect (дата звернення: 14.11.2023).
11. ACM Conference on Computer and Communications Security [Електронний ресурс]. URL: https://dl.acm.org/doi/10.1145/3629140 (дата звернення: 10.11.2023).

12. Закону України “Про інформацію” [Електронний ресурс]. URL: https://minjust.gov.ua/m/str_35738 (дата звернення: 17.11.2023).
13. What is RSU (Road-Side Unit) [Електронний ресурс]. URL: https://www.igi-global.com/dictionary/rsu-road-side-unit/34931 (дата звернення: 20.11.2023).
14. Connected and Autonomous Vehicles (CAVS) URL: https://www.arup.com/markets/highways/connected-and-autonomous-vehicles (дата звернення: 10.11.2023).
15. What is RSSI and what is it used for? URL: https://www.virginmedia.com/blog/wifi/what-is-rssi (дата звернення: 24.11.2023).
16. Tracking Performance of MIMO Radar for Accelerating Targets [Електронний ресурс].URL:https://www.researchgate.net/publication/260637387_Tracking_Performance_of_MIMO_Radar_for_Accelerating_Targets (дата звернення 03.12.2023).
17. Track Closely Spaced Targets Under Ambiguity in Simulink [Електронний ресурс]. URL: https://www.mathworks.com/help/fusion/ug/tracking-closely-spaced-targets-under-ambiguity-in-simulink.html 05.12.2023).
18. Towards Deep Radar Perception for Autonomous Driving: Datasets, Methods, and Challenges [Електронний ресурс]. URL: https://github.com/ZHOUYI1023/awesome-radar-perception (дата звернення: 10.12.2023).
19. Система вагових коефіцієнтів Фішберна. URL: https://cutt.ly/F0zLFy8 (дата звернення: 11.12.2023).
20. Ключківський В. О., Лукічов В.В. Метод захисту даних, отриманих за допомогою сенсорів 6G. Всеукраїнської науково-практичної інтернет-конференції Молодь в науці: дослідження, проблеми, перспективи (МН-2024). Вінниця, 11-20 травня 2024 р. [Електронний ресурс] URL: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/view/19752.
21. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт / Уклад. : В. О. Козловський, О. Й. Лесько, В. В. Кавецький. – Вінниця : ВНТУ, 2021. – 42 с.

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Метод захисту даних, отриманих за допомогою сенсорів 6G

Автор роботи: Ключківський Володимир Олександрович

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 83,3 %. Схожість – 16,7 %.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ (підпис) Валентина КАПЛУН

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ (підпис) Володимир КЛЮЧКІВСЬКИЙ

Керівник роботи _____ (підпис) Віталій ЛУКІЧОВ

Додаток Б

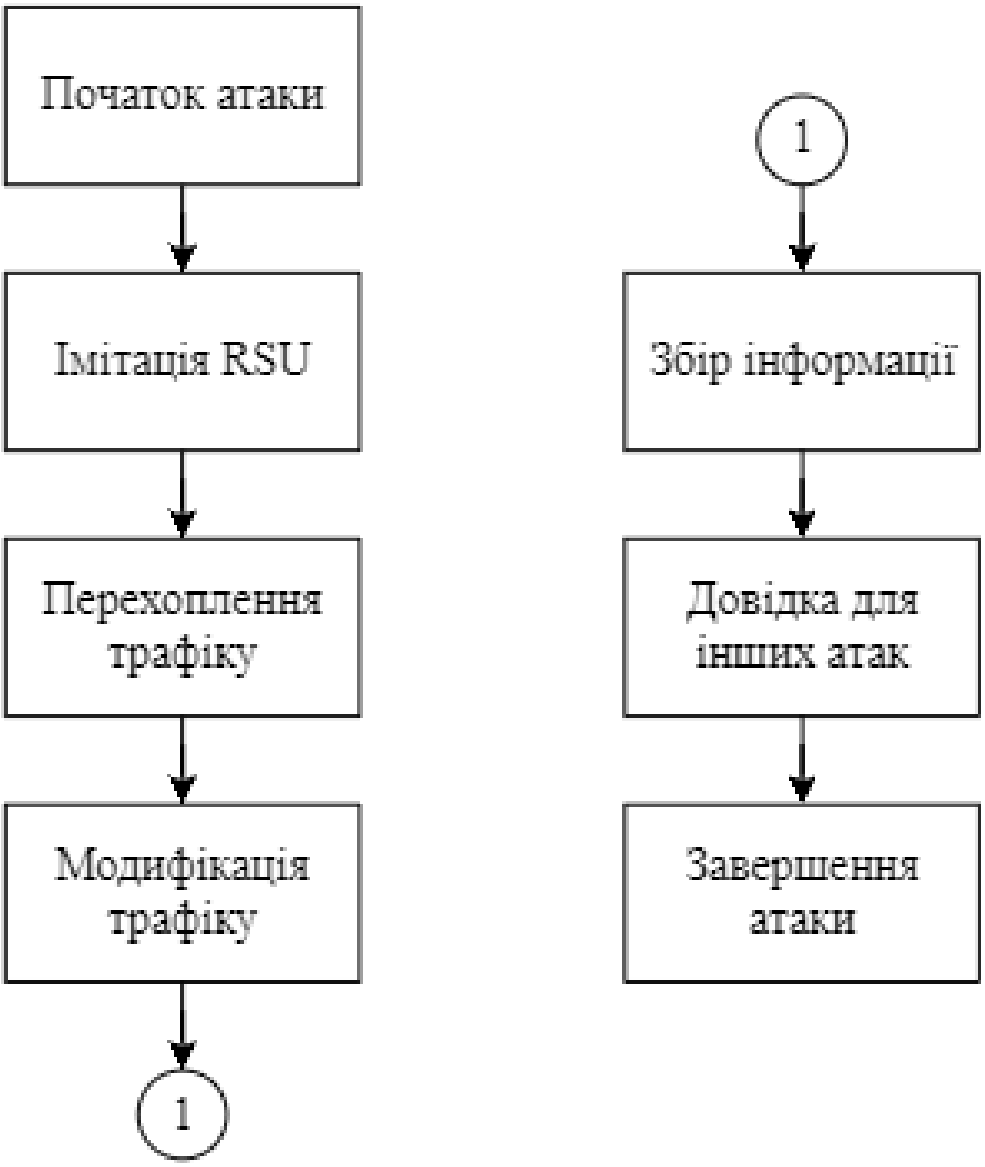
ІЛЮСТРАТИВНА ЧАСТИНА

Метод захисту даних, отриманих за допомогою сенсорів 6G

(Назва магістерської кваліфікаційної роботи)

Принцип роботи сенсору AWR2944

Структурна схема проведення спуфінг атаки



Принцип типу “Пішохідний”

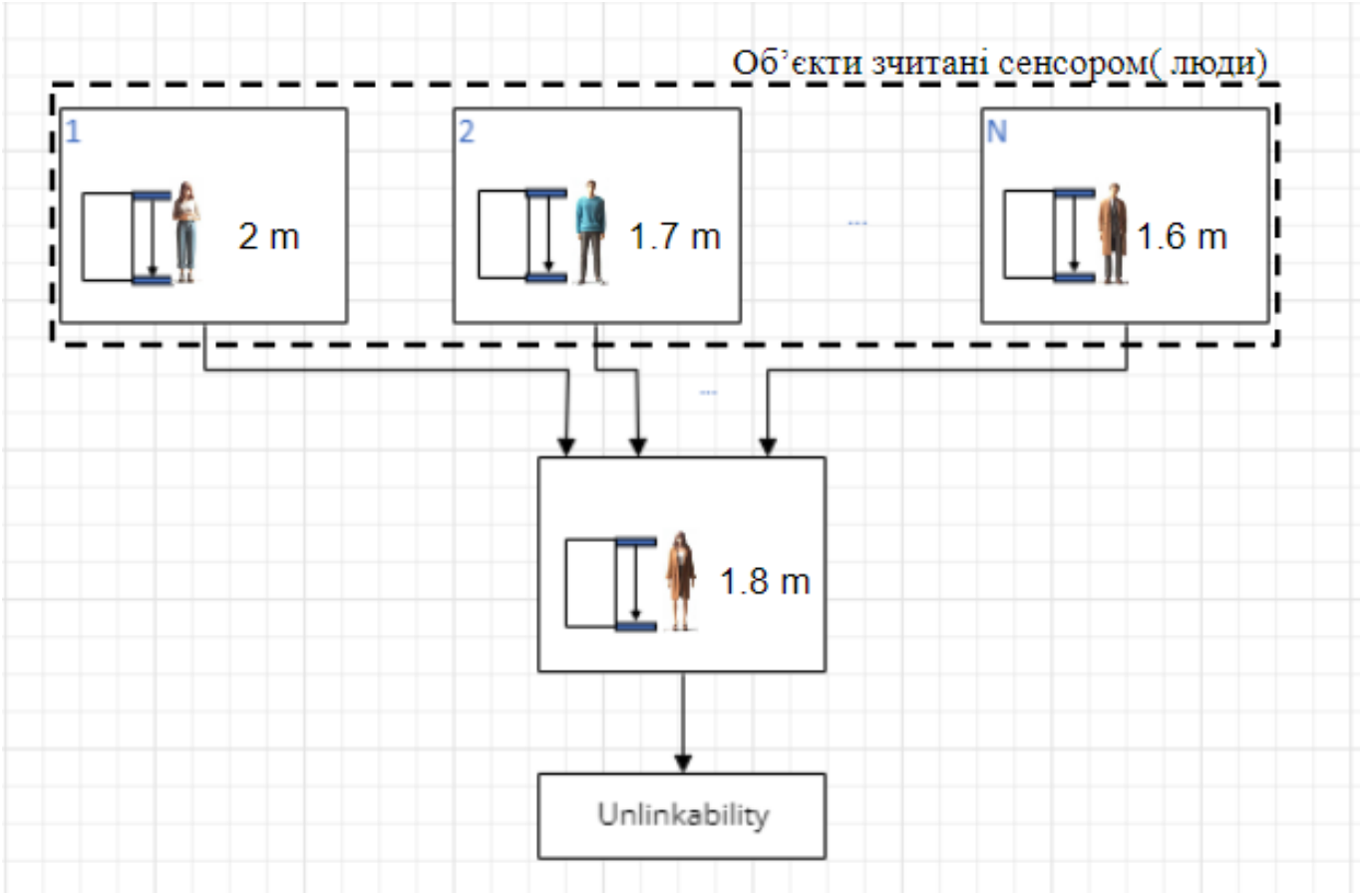
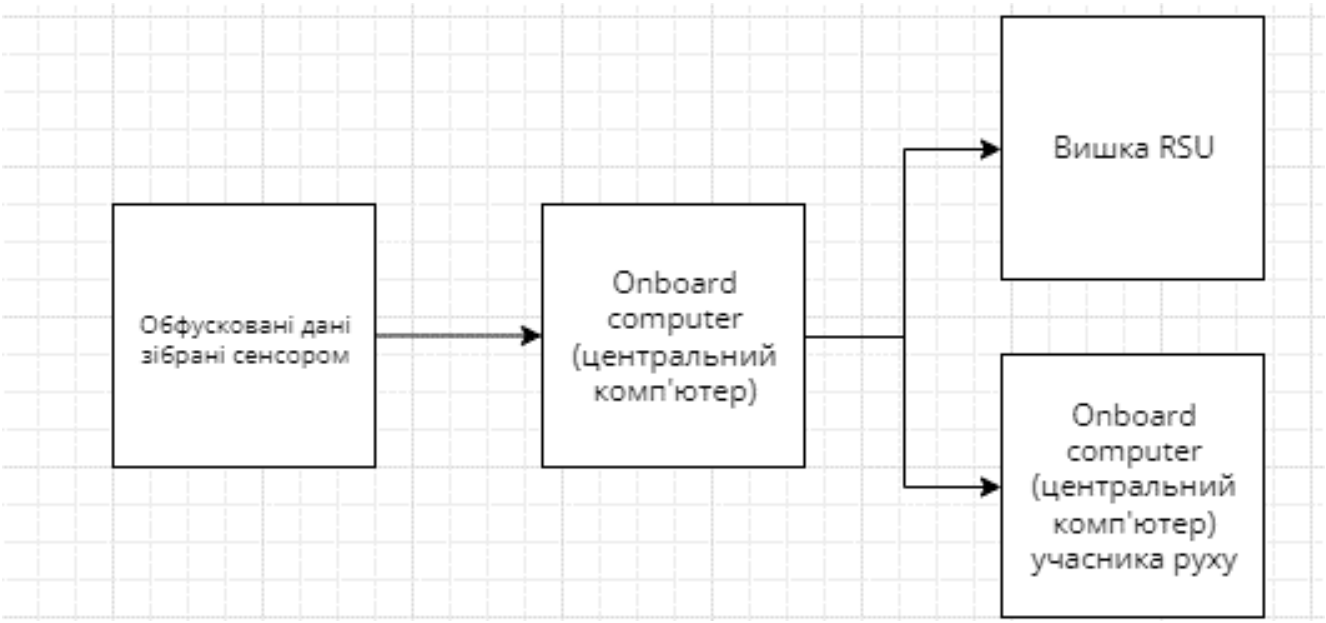
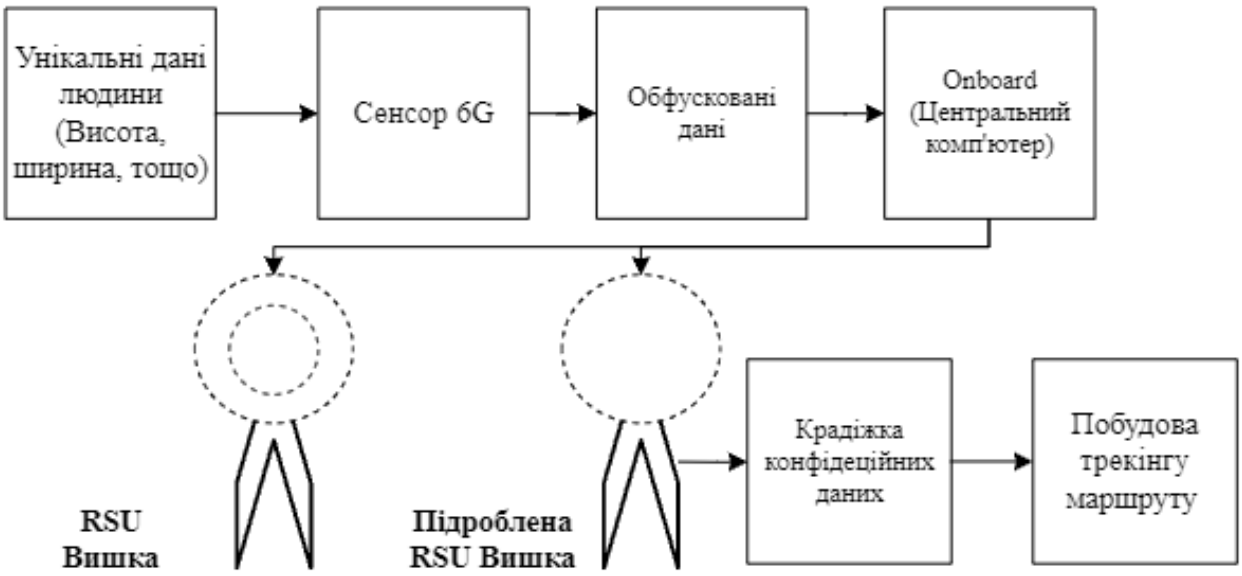


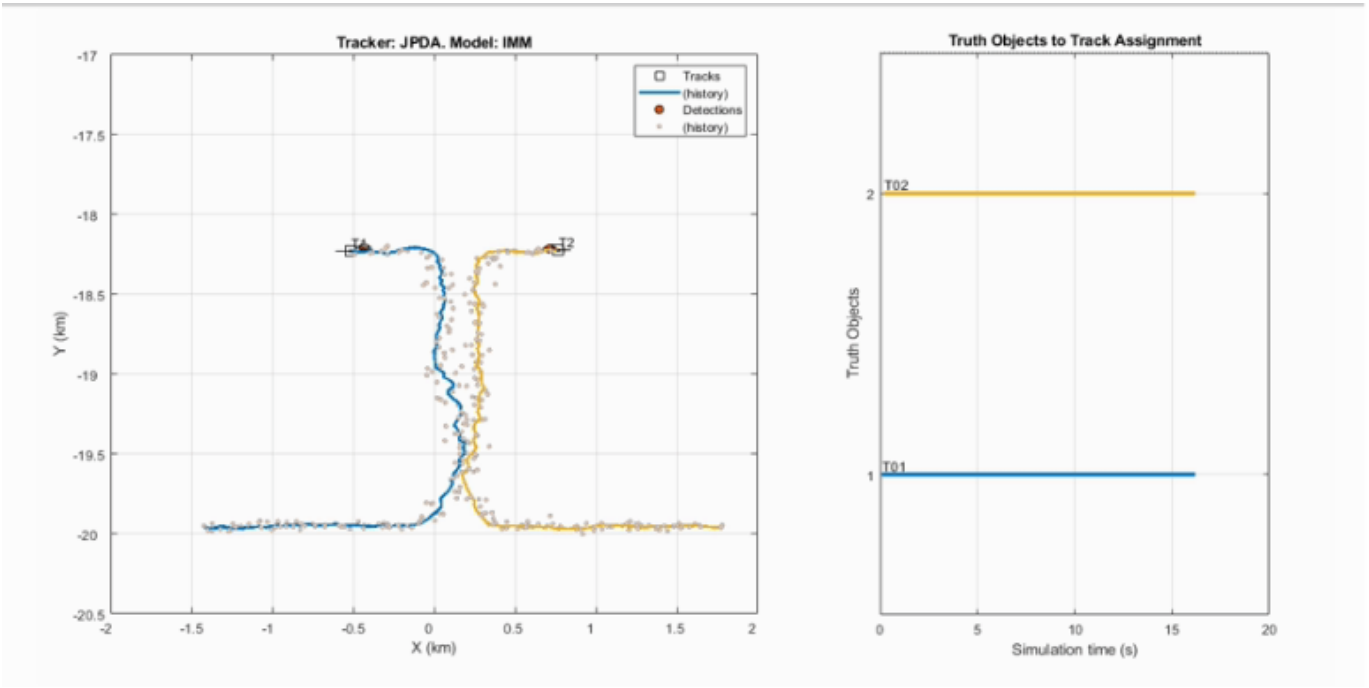
Схема процесу обфускації та передачі даних за принципом незв’язності



Загальна структурна схема обміну даними в автомобільній мережі 6G



Вікно з програмного застосунку для моделювання (без обфускації)



Вікно з програмного застосунку для моделювання (з обфускацією)