МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«____» _____ 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

ДОСЛІДЖЕННЯ ЗАХИСТУ СИСТЕМИ ІНФОРМАЦІЙНОГО ОБМІНУ ПІДВОДНОГО АПАРАТА З РАДІОБУЄМ

Ступінь вищої освіти: магістр
Галузь знань: 14 Електрична інженерія
Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконав: студент 6 курсу групи 6366м
Юхименко Олексій Сергійович _____

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Керівник:
к.т.н., доцент кафедри комп'ютерних технологій та інформаційної безпеки

Сірівчук Андрій Сергійович _____

Миколаїв – 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми, д.т.н., професор,
професор кафедри КТІБ
_____ Передерій В.І.
«14» 10 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студент: Юхименко Олексій Сергійович

Курс:6

Група: 6366м

Ступінь вищої освіти: магістр

Галузь знань: 14 Електрична інженерія

Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

1. Тема роботи: Дослідження захисту системи інформаційного обміну підводного апарата з радіобуєм

затверджена наказом НУК від «14» 10 2025 р. № 1217-ц

2. Вихідні дані до роботи: об'єкт дослідження – автономний підводний апарат з радіобуєм; наявніть радіоканалу зв'язку; сиктема керування побудована на базі одноплатних комп'ютерів

3. Перелік питань, які необхідно розробити: визначити структуру та дані інформаційних потоків в системі; визначення основних вразливостей для системи АНПА РБ; провести моделювання загроз методами STRIDE та DREAD; визначи засоби зменшення ризиків; провести моделювання системи при застосуванні засобів захисту.

4. Терміни виконання завдання:
термін видачі завдання: «01- 05» вересня 2025 р.
термін подання роботи: «18» грудня 2025 р.

6. План-графік виконання кваліфікаційної роботи

п/п	Заходи	Дата		Готовність
		Навч. тиждень	Контрольна дата	
1.	Наукове стажування	1 - 8	27.10.2025	Звіт з наукового стажування
2.	Організаційні збори	9	29.10.2025	Попередній варіант змісту КР
3.	Рубіжний контроль	10	05.11.2025	Попередній варіант оглядових розділів, звіт з практика
4.	Рубіжний контроль	13	27-28.11.2025	Доповідь на 13-ій Всеукраїнській науково-технічній конференції з міжнародною участю «СПІБТ–2025»
5.	Рубіжний контроль	14	3.12.2025	1. Попередній варіант повної КР 2. Попередній варіант презентації
6.	КЕ на рівень «магістра»	15	8,9.12.2025	Складання державного екзамену зі спеціальності на ступінь магістра
7.	Перевірка на плагіат	15	10.12.2025	Електронний варіант кваліфікаційної роботи, попередній захист (робота передається студентом на кафедру для внутрішньої рецензії).
8.	Оформлення КР та супутньої документації	16	15-17.12.2025	1. Оформлена КР (в форматі pdf) У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).
9.	Подання документів на захист	16	18.12.2025	1. Подання щодо захисту КР: тема, успішність, висновок керівника та висновок кафедри про КР. 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Електронний варіант презентації. 4. Електронний варіант КР на диску
10.	Захист ДР	17	22,23,24 12.2025	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.

Керівник
к.т.н., доцент кафедри комп'ютерних технологій
та інформаційної безпеки, _____ А.С. Сірівчук

Студент _____ О.С. Юхименко

АНОТАЦІЯ

Юхименко О. С. Дослідження захисту системи інформаційного обміну підводного апарата з радіобуєм. – Кваліфікаційна робота на правах рукопису.

Кваліфікаційна робота на здобуття ступеня вищої освіти «магістр» за спеціальністю 141 «Електроенергетика, електротехніка та електромеханіка» галузі знань 14 «Електрична інженерія» освітньо-професійної програми «Системи технічного за-хисту інформації, автоматизація її обробки». – Національний університет кораблебудування імені адмірала Макарова, Миколаїв, 2025.

Пояснювальна записка: 72 с., 39 джерел.

Кваліфікаційна робота присвячена актуальній темі забезпечення захисту системи інформаційного обміну підводного апарата з радіобуєм та наземною інфраструктурою в умовах використання відкритих каналів зв’язку.

Метою даної роботи є дослідження вразливостей системи інформаційного обміну, оцінка ризиків інформаційної безпеки та розроблення заходів щодо їх зменшення до прийнятного рівня.

У роботі представлено аналіз архітектури системи обміну даними між підводним апаратом, радіобуєм, постом керування, сервером зберігання та постом обробки інформації, а також проведено оцінку ризиків із застосуванням методів STRIDE та DREAD.

Також було розроблено рекомендації щодо підвищення рівня конфіденційності, цілісності та доступності інформації, а також виконано кількісне моделювання ефективності запропонованих заходів захисту.

Ключові слова: автономний ненаселений підводний апарат, радіобуй, STRIDE, DREAD, система інформаційного обміну.

ABSTRACT

Yukhimenko O. S. Research on the protection of the information exchange system of an underwater vehicle with a radio buoy. – Qualification work in the form of a manuscript.

Qualification work for the degree of higher education "Master" in the specialty 141 "Electrical power engineering, electrical engineering and electromechanics" field of knowledge 14 "Electrical engineering" of the educational and professional program "Systems of technical protection of information, automation of its processing". – Admiral Makarov National University of Shipbuilding, Mykolaiv, 2025.

Explanatory note: 72 p., , 39 sources.

The qualification work is devoted to the topical topic of ensuring the protection of the information exchange system of an underwater vehicle with a radio buoy and ground infrastructure in the conditions of using open communication channels.

The purpose of this work is to study the vulnerabilities of the information exchange system, assess information security risks and develop measures to reduce them to an acceptable level.

The work presents an analysis of the architecture of the data exchange system between the underwater vehicle, radio beacon, control post, storage server and information processing post, and also conducts a risk assessment using the STRIDE and DREAD methods.

Recommendations were also developed to increase the level of confidentiality, integrity and availability of information, and quantitative modeling of the effectiveness of the proposed protection measures was performed.

Keywords: autonomous unmanned underwater vehicle, radio beacon, STRIDE, DREAD, information exchange system.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АНПА – автономний ненаселений підводний апарат

РБ – радіобуй

ПК – пост керування

ТПА – телекерований підводний апарат

ПА – підводний апарат

ГНСС – глобальна навігаційна система

ВСТУП

На даний час моніторинг підводної обстановки є важливою задачею забезпечення безпеки водних транспортних шляхів. Одним з перспективних засобів моніторингу внутрішніх водних шляхів України є автономні підводні апарати з радіобуєм (АНПА РБ) [1].

При використанні автономних систем є необхідність забезпечення надійного захисту від кіберінцидентів, що в значній мірі впливає на якість виконання місій підводного апарата.

Наявність постійного зв'язку з постом керування через радіоканал збільшує можливість виконання інцидентів при роботі системи АНПА РБ. Розуміння природи кожного типу загроз створює основу для формування комплексної системи безпеки, де фізичні, програмні та організаційні заходи доповнюють одне одного, забезпечуючи надійність усієї інфраструктури.

Об'єктом дослідження є система інформаційного обміну між АНПА РБ та постом керування, що включає інформаційний канал зв'язку, пост керування та сервер постобробки інформації, і функціонує в умовах дії кіберзагроз.

Предметом дослідження є методи та засоби забезпечення безпеки каналом інформаційного обміну між автономним морським рухомим об'єктом та постом керування, зокрема процеси моделювання загроз, оцінювання ризиків, вибору та впровадження технічних і організаційних заходів захисту.

Метою кваліфікаційної роботи є проведення аналізу вразливостей системи інформаційного обміну підводного апарата з радіобуєм та визначення вимог для збільшення стійкості системи.

Для вирішення поставленої мети необхідно вирішити наступні завдання:

– визначити структуру та дані інформаційних потоків в системі;

– визначення основних вразливостей для системи АНПА РБ;

– провести моделювання загроз методами *STRIDE* та *DREAD*;

– визначи засоби зменшення ризиків;

– провести оцінку системи при застосуванні засобів захисту.

Практичне значення роботи полягає у можливості використання запропонованого підходу до оцінки ризиків інформаційної безпеки при проєктуванні та модернізації систем інформаційного обміну автономних підводних апаратів. Отримані результати можуть бути використані інженерами та розробниками для обґрунтування вибору засобів захисту та підвищення надійності системи.

Результати роботи частково опубліковані в наступному джерелі:

Желтов В.С., Юхименко О.С., Аналіз потоків інформації що циркулює в системі автономний підводний апарат-радіобуй-пост керування/ Наук. керівник А.С. Сірівчук // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали XIII всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2025, 12-15 сс.

Кваліфікаційна робота відповідає компетентностям:

– КФ-1 – Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки;

– КФ-3 – Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури;

– КФ-5 – Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх

впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

– КФ7 – Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

1 ПРИЗНАЧЕННЯ ТА ОБЛАТЬ ЗАСТОСУВАННЯ

1.1 Область застосування автономних підводних апаратів

Автономні ненаселені підводні апарати (АНПА) – це складні роботизовані платформи, призначені для самостійної роботи під поверхнею води. На відміну від телекерованих підводних апаратів (ТПА), які потребують постійного людського контролю за допомогою тросів, АНПА навігують, збирають дані та виконують місії автономно, використовуючи бортові датчики, попередньо запрограмовані інструкції та штучний інтелект. Їхня здатність досліджувати середовища, які в іншому випадку є занадто глибокими, небезпечними або дорогими для пілотованих місій, робить їх незамінними в широкому спектрі галузей промисловості та наукових сфер.

Використання автономних ненаселені підводних апаратів з радіобуєм (АНПА РБ) працюють аналогічно стандартним АНПА але мають можливість передавати великі об’єми інформації в режимі реального часу[2].

Область використання АНПА РБ обмежена, зазвичай, довжиною кабель буксиру та складністю навігаційної обстановки. До задач які можуть виконувати такі апарати є:

– картографування морського дна та гідрографічні дослідження. АНПА РБ здатні створювати високодетальні карти морського дна за допомогою передових гідролокаційних технологій, таких як багатопроменеві ехолоти, гідролокатори бокового огляду та піддонні профілографи. Ці прилади можуть виявляти та візуалізувати підводний рельєф, геологічні формації та штучні споруди з надзвичайною точністю. АНПА РБ можна використовувати для картографування прибережних зон, підводних ліній розломів та континентального шельфу, що має вирішальне значення для безпеки морського судноплавства, геологічних досліджень та готовності до стихійних лих. Крім

того, дані, зібрані АНПА, підтримують створення морських карт та цифрових моделей місцевості, що використовуються судноплавною галуззю та військово-морськими операціями. Точність та ефективність картографування АНПА РБ знижують ризик для людини та значно знижують вартість довгострокових геодезичних проектів;

– нафтогазова промисловість. АНПА можуть використовуються для сканування морського дна на наявність ознак родовищ вуглеводнів, оцінки геотехнічних умов та інспекції підводної інфраструктури, такої як трубопроводи, гирла свердловин та бурові платформи. Використовуючи інструменти візуалізації високої роздільної здатності та лазерні сканери, АНПА РБ можуть виявляти структурні пошкодження, корозію або потенційні небезпеки вздовж трубопроводів, що дозволяє своєчасно проводити ремонт і зменшувати ризик дорогих аварій або розливів в навколишнє середовище. Крім того, АНПА РБ скорочують час простою та підвищують безпеку, усуваючи необхідність використання надводних суден або втручання людини в рутинний моніторинг. Їхня здатність автономно виконувати складні місії на великих відстанях робить їх важливим активом для забезпечення ефективності та безпеки підводних операцій в енергетичному секторі;

– моніторинг навколишнього середовища – це ще одна критична сфера, де АНПА РБ можуть мати значний вплив. Ці апарати допомагають дослідникам та регуляторним органам відстежувати стан морських екосистем, виявляти забруднення та оцінювати вплив діяльності людини на водне середовище. Оснащені хімічними та біологічними датчиками, АНПА можуть виявляти витоки нафти, забруднення важкими металами, зміни *pH* та наявність шкідливого цвітіння водоростей. Вони також використовуються для моніторингу стану коралових рифів, заростей морських трав та інших чутливих середовищ існування, вразливих до зміни клімату та розвитку прибережних зон. Оскільки АНПА РБ можуть працювати протягом тривалого часу та отримувати доступ до віддалених або важкодоступних районів, вони надають високоякісні дані, які було б важко або неможливо отримати в іншому випадку.

Ця інформація є життєво важливою для формування політики охорони природи, проведення оцінки впливу на навколишнє середовище та забезпечення дотримання міжнародних правил охорони морського середовища;

– підводне гуманітарне розмінування. Підводні апарати стали невід'ємною складовою сучасного гуманітарного розмінування у водному середовищі. Їх застосування забезпечує якісно новий рівень безпеки, точності та ефективності під час роботи з вибухонебезпечними предметами. Завдяки використанню дистанційно керованих та автономних систем, фахівці можуть проводити детальну розвідку, створювати карти небезпечних ділянок і виконувати підготовчі операції без безпосереднього ризику для водолазів і саперів. Крім того, багато підводних апаратів можуть не лише виявляти небезпечні предмети, а й активно брати участь у процесі їх знешкодження: встановлювати підривні заряди, розчищати ґрунт, переміщувати невеликі об'єкти або забезпечувати безпечний доступ для вибухотехніків. Це значно скорочує час проведення операцій та мінімізує ризик людських втрат;

– підводна археологія. У галузі підводної археології, АНПА відкривають доступ до стародавніх корабельних аварій, затонулих міст та інших затоплених об'єктів культурної спадщини. Археологи використовують АНПА для проведення неінвазивних досліджень морського дна в прибережних акваторіях, створюючи детальні 3D-моделі історичних артефактів та ландшафтів за допомогою камер високої роздільної здатності, сонару та фотограмметрії. Ці апарати можуть працювати контрольовано та дбайливо, мінімізуючи ризик пошкодження крихких артефактів або порушення шарів осадових порід. Їхня здатність ефективно охоплювати великі площі також збільшує шанси на виявлення раніше невідомих пам'яток. Окрім досліджень, АНПА РБ можуть відігравати вирішальну роль у збереженні та документуванні підводної культурної спадщини, пропонуючи цінну інформацію про нашу спільну історію людства та сприяючи цифровим зусиллям зі збереження для майбутніх поколінь.

Підводні апарати трансформують наші можливості досліджувати та керувати підводними об’єктами. Від наукових відкриттів до промислового інспекційного контролю та захисту навколишнього середовища. АНПА РБ пропонують універсальне, економічно ефективне та безпечне рішення для роботи під хвилями. З розвитком технологій їхня роль лише розширюватиметься, відкриваючи нові горизонти підводних інновацій.

1.2 Структура системи інформаційного обміну

Система інформаційного обміну АНПА РБ – це складний комплекс апаратних, програмних та комунікаційних засобів, призначених для забезпечення надійного, захищеного та безперервного передавання даних у середовищі з підвищеними ризиками. Її структура формується з урахуванням особливостей фізичного середовища (морська вода, тиск, глибина, температура), обмежених енергетичних ресурсів апаратів, а також вимог до безпеки інформації. Система має багаторівневу архітектуру, де кожен рівень виконує специфічні функції і має власні вразливості, що потребують відповідних заходів захисту.

Типова система складається з трьох головних компонентів: АНПА РБ, береговий (судновий) пост керування та віддалений центр даних (необов’язково) (рис. 1.1).

Підводний апарат (ПА) — автономний чи дистанційно керований об’єкт, який здійснює моніторинг підводного середовища, збір гідрологічних, хімічних чи технічних даних. Основні модулі:

– сенсорний комплекс – набір датчиків (температури, тиску, солоності, швидкості течії, камер тощо), що забезпечують збір інформації про середовище;

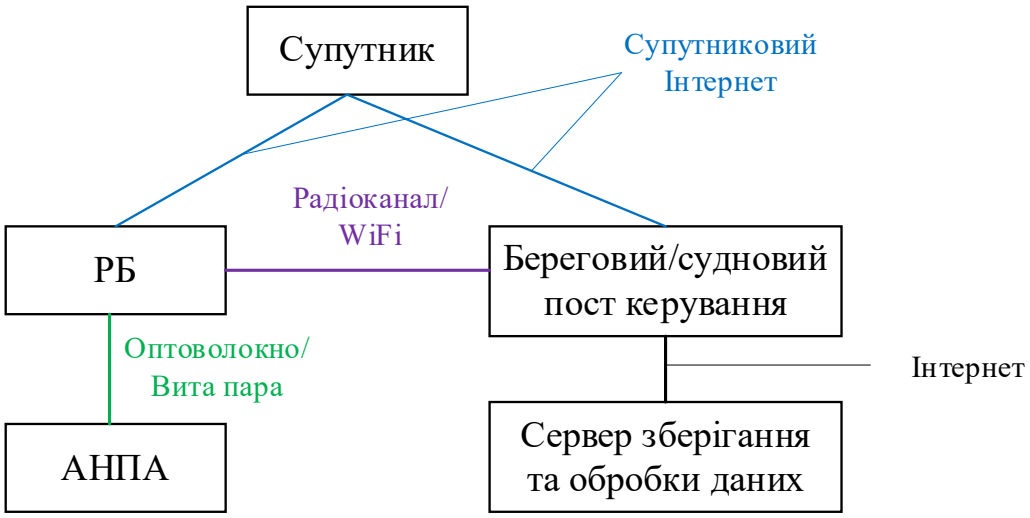

Рисунок 1.1 – Узагальнена структура системи інформаційного обміну

– бортова обчислювальна система – контролер або мікропроцесор, який обробляє дані, здійснює кодування та формує пакети для передавання;

– комунікаційний модуль – включає в себе пристрої перетворення інтерфейсів для взаємодії між окремими модулями та коммутатор для взаємодії з радіобуєм (РБ);

– енергетичний блок — система живлення на основі літій-іонних батарей або паливних елементів, що забезпечує автономність;

Радіобуй (РБ) — поверхневий вузол зв’язку, який приймає дані з підводного апарата та ретранслює їх через радіомережу або супутниковий канал до берегового/суднового поста керування. Типова конструкція буя включає:

– радіомодуль/супутниковий модем (*VHF/UHF, LTE, Iridium, Starlink* тощо) для передачі даних на великі відстані, до якого входить модуль управління й шифрування, що забезпечує автентифікацію сигналів і перевірку їх походження;

– акумуляторний блок для автономного живлення;

– бортовий контролер зв’язку, який виступає посередником між підводним апаратом і надводною інфраструктурою.

Береговий/судновий пост керування – ланка взаємодії з оператором місії та здійснення керування АНПА РБ. Пост керування є центральним елементом системи управління автономним морським рухомим об’єктом та виконує сукупність функціональних, інформаційних і безпекових задач, спрямованих на забезпечення ефективного та безпечного виконання місії. Він забезпечує взаємодію між оператором та автономним об’єктом, здійснює обробку інформації, формування керуючих впливів і контроль стану системи в цілому.

Однією з основних задач поста керування є планування та управління місією автономного морського об’єкта. У межах цієї задачі здійснюється формування маршрутів руху, визначення цілей та етапів місії, задання обмежень щодо швидкості, глибини або зон заборони. Пост керування дозволяє оператору коригувати параметри місії в реальному часі з урахуванням отриманої телеметричної та сенсорної інформації.

Важливою задачею поста керування є формування та передавання команд управління. Пост забезпечує генерацію керуючих команд відповідно до обраного режиму роботи автономного об’єкта – повністю автономного, напівавтономного або дистанційно керованого. Перед передаванням команди проходять логічний та безпековий контроль, що дозволяє запобігти помилковим або небезпечним діям автономного об’єкта.

Не менш важливою є задача приймання, обробки та візуалізації телеметричної інформації. Пост керування збирає дані про навігаційні параметри, технічний стан бортових систем, результати роботи сенсорів і стан каналу зв’язку. Отримана інформація обробляється та відображається оператору у зручному вигляді, що забезпечує ситуаційну обізнаність та підтримку прийняття рішень.

Окрему групу складають задачі контролю справності та діагностики автономного морського об’єкта. Пост керування аналізує телеметрію з метою виявлення відхилень від нормального режиму роботи, прогнозує можливі відмови та формує попередження для оператора. У разі виявлення критичних

несправностей пост керування може ініціювати аварійні сценарії або перевести об’єкт у безпечний режим.

Значну роль відіграють задачі забезпечення інформаційної та кібербезпеки. Пост керування реалізує механізми автентифікації операторів, криптографічного захисту команд і телеметрії, контролю цілісності даних та ведення журналів подій. Крім того, він забезпечує моніторинг стану інформаційного каналу та виявлення спроб несанкціонованого доступу або кібератак.

До задач поста керування також належить управління конфігурацією та програмним забезпеченням автономного об’єкта. Це включає передавання оновлень програмного забезпечення, зміну параметрів роботи бортових систем, а також контроль версій та цілісності програмних компонентів. Такі дії виконуються з урахуванням вимог безпеки та зазвичай у регламентованих режимах.

Важливою функцією поста керування є забезпечення взаємодії з іншими інформаційними системами. Пост може інтегруватися з навігаційними, метеорологічними, логістичними або командно-штабними системами, що дозволяє враховувати зовнішню інформацію при управлінні автономним морським об’єктом та підвищує ефективність виконання місії.

Окремо слід виділити задачу реагування на аварійні та позаштатні ситуації. У разі втрати зв’язку, відмови бортових систем або загроз безпеці пост керування забезпечує ініціювання аварійних процедур, координацію дій оператора та, за необхідності, відновлення управління після усунення інциденту.

Таким чином, пост керування виконує комплекс взаємопов’язаних задач, що охоплюють планування, управління, моніторинг, забезпечення безпеки та підтримку прийняття рішень. Ефективне виконання цих задач є необхідною умовою надійної та безпечної експлуатації системи інформаційного обміну з автономним морським рухомим об’єктом.

Сервер зберігання та обробки даних (сервер постобробки) – включає серверну частину, бази даних, аналітичні програми та сервіси доступу до архівних даних.

Однією з основних функцій сервера постобробки інформації є накопичення та довготривале зберігання даних, отриманих від автономного морського об’єкта та поста керування. Сервер забезпечує збереження телеметрії, навігаційних параметрів, журналів подій, логів інформаційного каналу та результатів роботи бортових сенсорів. Архівування інформації здійснюється з урахуванням вимог до цілісності, доступності та відновлюваності даних.

Важливим призначенням сервера є постобробка та аналітична обробка інформації. На сервері виконуються обчислювально трудомісткі алгоритми аналізу даних, зокрема фільтрація, агрегація, кореляційний аналіз та формування зведених показників. Це дозволяє виявляти приховані закономірності, аномалії в роботі автономного об’єкта та відхилення від заданих параметрів руху або режимів функціонування.

Сервер зберігання та обробки (постобробки) інформації також виконує задачу підтримки аналізу ефективності виконання місії. На основі накопичених даних здійснюється оцінювання точності навігації, стабільності каналу зв’язку, енергетичної ефективності та надійності бортових систем. Отримані результати використовуються для коригування алгоритмів управління, оптимізації маршрутів та вдосконалення технічних характеристик автономного морського об’єкта.

Окреме місце займає забезпечення ретроспективного аналізу та розслідування інцидентів. Сервер постобробки інформації зберігає журнали подій та телеметричні дані, що дозволяє відновити хронологію подій у разі виникнення аварійних ситуацій, збоїв або кіберінцидентів. Це є важливим елементом системи управління безпекою та відповідності нормативним вимогам.

Ще одним призначенням сервера є формування звітів та інформаційних продуктів. Сервер забезпечує автоматизоване створення звітів щодо результатів місій, технічного стану системи, статистики відмов та показників безпеки. Такі звіти можуть використовуватися як для внутрішнього аналізу, так і для надання регуляторним органам або керівництву.

Сервер постобробки інформації виконує також роль інтерфейсу інтеграції з зовнішніми інформаційними системами. Через захищені інтерфейси він може передавати узагальнену інформацію до аналітичних, логістичних або командно-штабних систем, забезпечуючи узгодженість даних і підтримку міжсистемної взаємодії.

З точки зору інформаційної безпеки сервер постобробки інформації призначений для централізованої реалізації політик захисту даних. Він забезпечує контроль доступу до архівів, захист даних від несанкціонованого доступу, резервне копіювання та відновлення інформації, а також ведення аудитних журналів відповідно до вимог нормативних документів.

Таким чином, сервер постобробки інформації є важливим елементом системи управління автономним морським рухомим об’єктом, що забезпечує перехід від оперативного управління до глибокого аналізу та оцінювання результатів функціонування системи, підвищуючи її надійність, ефективність та рівень інформаційної безпеки.

Висновки по розділу

Розглянуто структуру системи інформаційного обміну АНПА РБ та визначено ключові елементи: підводний апарат, радіобуй, пост керування та сервер постобробки. Встановлено їхні функціональні завдання та потенційні особливості взаємодії. Проведений аналіз дозволив визначити, що система інформаційного обміну працює у складних техногенних та природних умовах, що створює значну кількість вразливостей.

2 АНАЛІЗ ВРАЗЛИВОСТЕЙ СИСТЕМИ ІНФОРМАЦІЙНОГО ОБМІНУ ПІДВОДНОГО АПАРАТА

2.1 Аналіз потоків інформації під час роботи апарата

Інформаційний обмін між постом керування та підводним апаратом складається з кількох типів даних, що передаються в обох напрямках, і кожен із цих потоків виконує важливу функцію в успішній роботі апарата. У напрямку від поста керування до апарата передаються насамперед керуючі команди. Це можуть бути вказівки щодо курсу, швидкості, глибини та інших параметрів руху. У ручному режимі роботи АНПА РБ, такі команди надсилаються багаторазово протягом секунди, створюючи фактично безперервний цикл керування. Крім основних вказівок щодо руху, пост керування може передавати апарату інструкції щодо зміни режимів роботи: наприклад, перейти зі стандартного картографування на режим пошуку об’єктів, зменшити інтенсивність збору даних для економії енергії або активувати певні датчики, які зазвичай перебувають у сплячому режимі.

У деяких випадках апарат отримує також дані, які використовуються його внутрішніми алгоритмами: оновлені параметри контролера, нові точки маршруту, карти небажаних для входу зон, а іноді навіть оновлені моделі машинного навчання, якщо місія цього потребує. Крім того, пост керування може надсилати діагностичні команди, наприклад ініціювати перезавантаження системи, провести калібрування сенсорів або перевести апарат у тестовий режим для перевірки працездатності.

У зворотному напрямку – від підводного апарата до поста керування – надходять дані різного характеру, і першою категорією є навігаційна інформація. Апарат періодично передає показники глибини, курсу, швидкості, кута нахилу та крену, а також оцінки свого поточного положення, що

ґрунтуються на інерційній навігаційній системі, доплерівському лагу чи системах акустичного позиціонування. Окрім цього, надходять дані, які використовуються апаратом для побудови карт місцевості та виявлення перешкод, хоча зазвичай вони сильно стискаються або передаються лише у зведеному вигляді через низьку пропускну здатність підводного каналу зв’язку.

Друга важлива категорія – це інформація про технічний стан самої машини. Пост керування отримує дані про рівень заряду батареї, температуру акумуляторних секцій, стан двигунів і сервоприводів, працездатність баластної системи, нагрів електронних модулів, рівень вологості у відсіках та інші параметри, що дозволяють оцінити безпеку та надійність роботи. Такі телеметричні пакети є короткими, але критично важливими, оскільки дозволяють оперативно реагувати на ймовірні збої чи аварійні ситуації.

Окремий сегмент інформаційного обміну становлять дані, пов’язані з науковими або прикладними завданнями, які виконує апарат. Такі дані передаються у вигляді потокового відео з камер високої роздільності, зображень із сонарів та інших сенсорів у режимі реального часу, оскільки радіозв’язок через РБ забезпечує високу пропускну здатність.

Нарешті, найбільш пріоритетною інформацією є аварійні повідомлення, які апарат надсилає навіть у найскладніших умовах. Це можуть бути сигнали про втрату стійкості, виявлення води всередині корпусу, критичне падіння заряду, перегрів акумуляторів, відмову двигуна або втрату зв’язку з постом керування. Такі повідомлення мають найвищий пріоритет у каналі зв’язку: вони пакуються у максимально короткий формат, дублюються кілька разів і надсилаються до отримання підтвердження. Якщо підтвердження не надходить, апарат автоматично переходить до запрограмованої аварійної поведінки – наприклад, спливає на поверхню.

У підсумку інформаційний обмін між постом керування та підводним апаратом являє собою складну систему взаємопов’язаних потоків, у якій одночасно передаються команди, навігаційні дані, телеметрія, наукова інформація та аварійні сигнали. Кожен із цих потоків має власні вимоги до

швидкості, надійності та обсягу передавання, і саме правильна організація цього обміну визначає успішність і безпечність роботи апарата під водою.

2.2 Огляд загроз основних елементів системи

Вразливості системи інформаційного обміну АНПА РБ мають багатовимірний характер і охоплюють як технічні, так і організаційні аспекти. Вони можуть виникати на різних етапах функціонування: під час розробки, налаштування, експлуатації чи технічного обслуговування. Важливим завданням є їх систематизація, адже тільки через усвідомлення потенційних ризиків можна побудувати надійну систему захисту.

2.2.1 Категорії вразливостей

Умовно вразливості поділяються на п’ять головних груп: фізичні, комунікаційні, програмні, криптографічні та організаційні [3-5].

2.2.1.1Фізичні вразливості.

Ці ризики пов’язані з матеріальною природою обладнання. Підводні апарати і радіобуї працюють у складних умовах – під високим тиском, за змінної температури, впливу солоної води, корозії та біологічного обростання корпусу. Будь-яка механічна несправність може призвести не лише до втрати функціональності, але й до порушення безпеки передавання даних. Наприклад, вихід з ладу ізоляції кабелю може створити канал для електромагнітних перешкод або витоку сигналів.

До фізичних загроз належать: пошкодження корпусу буя, зняття або підміна сенсорних модулів, фізичний доступ до портів зв’язку. Для мінімізації таких ризиків застосовують герметизацію, захист від розкриття (тампериг), сигнальні індикатори та моніторинг фізичного стану пристроїв.

2.2.1.2 Комунікаційні вразливості.

Вони виникають у процесі обміну інформацією між компонентами системи. Уразливості цього типу найчастіше пов’язані з недоліками протоколів або реалізації зв’язку. Прикладами можуть бути: відсутність автентифікації між

вузлами, використання незашифрованих пакетів, передача ключів у відкритому вигляді, відсутність перевірки цілісності даних.

Комунікаційні вразливості роблять систему вразливою до пасивних і активних атак: перехоплення, підміни повідомлень, ін'єкцій команд, глушіння сигналу чи створення помилкових буїв. Для протидії необхідне застосування сучасних криптографічних протоколів, таких як *TLS* або *DTLS*, а також впровадження механізмів контролю доступу.

2.2.1.3 Програмні вразливості.

Помилки у програмному забезпеченні є однією з найпоширеніших причин компрометації систем. Сюди належать буферні переповнення, некоректна обробка введених даних, відсутність перевірки прав доступу, а також уразливості в бібліотеках, драйверах і прошивках. Підводні апарати часто використовують вбудовані операційні системи (*Embedded Linux, RTOS*), які, за недбалого оновлення, можуть містити відомі експлойти.

Шкідливий код може потрапити у систему під час оновлення прошивки або через маніпуляцію з каналом обміну між РБ і береговим центром. Для запобігання цьому застосовують цифрові підписи, перевірку цілісності образів і регулярний аудит програмного коду.

2.2.1.4 Криптографічні вразливості.

Цей тип пов'язаний з помилками у реалізації алгоритмів шифрування або управлінні ключами. Навіть найсильніший алгоритм, як-от *AES* чи *RSA*, не гарантує безпеки, якщо ключі зберігаються у незахищеній пам'яті або не оновлюються [6].

Типові загрози: використання застарілих протоколів (*MD*5, *SHA*-1), низька ентропія при генерації ключів, відсутність апаратного генератора випадкових чисел, спроби дешифрування за допомогою *brute-force* або *side-channel* атак.

Для протидії необхідне використання сучасних схем – *AES*-256, *ECC*, *ChaCha*20-*Poly*1305, а також централізоване управління ключами, апаратні модулі безпеки (*HSM*) і протоколи обміну ключами (*Diffie–Hellman, ECDH*).

2.2.1.5 Організаційні вразливості.

Жодна система не може бути безпечною без правильної організації процесів. Людський фактор залишається найслабшою ланкою. Неправильне налаштування мережі, використання стандартних паролів, недбале поводження з ключами, несвоєчасне оновлення програмного забезпечення — усе це створює передумови для компрометації системи.

Вразливості можуть виникати через відсутність політики безпеки, несанкціонований доступ технічного персоналу, відсутність контролю за підключеними пристроями. Тому необхідно впроваджувати регулярне навчання персоналу, багаторівневу аутентифікацію, принцип мінімізації доступу (*least privilege*) і централізоване логування подій [7].

2.2.2 Ідентифікація активів і об’єктів захисту

Першим кроком є визначення активів, які потребують захисту. До них належать:

– інформаційні активи – передані дані з сенсорів, навігаційна інформація, команди управління, телеметрія, криптографічні ключі;

– технічні активи – підводний апарат, радіобуй, сервери берегового центру, мережеве обладнання;

– програмні активи – прошивки, операційні системи, модулі шифрування, протоколи зв’язку;

– організаційні активи: користувачі, облікові записи, політики безпеки, канали оновлення.

Кожен актив має свою цінність і рівень критичності, що визначає пріоритетність його захисту. Наприклад, втрата конфіденційності навігаційних даних може дозволити ворогу відстежити місце перебування апарата, а зміна команд управління – призвести до повної втрати пристрою.

Інформаційні активи автономних підводних апаратів охоплюють увесь спектр даних, програмних ресурсів і знань, що створюються та використовуються під час їхньої роботи. Серцем інформаційної системи такого апарата є сенсорні дані, які він збирає в режимі реального часу. До них

належать гідролокаційні зображення, результати роботи ехолотів, акустичні сигнали, а також оптичні фото й відео, отримані під водою. Важливу роль відіграють навігаційні показники – дані інерціальної навігаційної системи, доплерівського логу, магнітометрів та інших приладів, які дозволяють апарату орієнтуватися без доступу до супутникових сигналів. Не менш значущими є океанографічні параметри: температура, солоність, тиск, швидкість течій і хімічний склад води, що забезпечують виконання дослідницьких або інспекційних завдань.

На основі цих сенсорних вимірювань формуються більш складні інформаційні активи: батиметричні карти, тривимірні моделі дна, геопросторові бази даних і каталоги підводних об'єктів. Усе це створює інформаційне середовище, яке допомагає апарату планувати маршрути, виконувати місії та аналізувати знайдену інформацію. Ці дані тісно пов’язані з програмними активами – алгоритмами автономного керування, системами уникнення перешкод, плануванням руху, а також моделями штучного інтелекту, які класифікують об’єкти, інтерпретують сонарні зображення або виявляють аномалії у зібраних даних.

До інформаційних активів належать і технічні журнали: телеметрія, записи про стан енергосистем, діагностичні звіти та логи, що фіксують всі події, помилки та характеристики роботи апарата. Важливим компонентом є дані комунікацій – обмін повідомленнями через акустичний канал, інформація, передана материнському судну, і пакети, відправлені на поверхні через супутниковий зв’язок.

Окрему групу становлять дані місій: маршрути, опис зон, яких слід уникати, параметри пошукових схем та інформація про корисне навантаження. Разом із ними існують адміністративні та безпекові активи, такі як ключі шифрування, параметри автентифікації, налаштування доступу й журнали аудиту, що забезпечують безпечну роботу системи.

Після завершення роботи сервер обробки даних генерує аналітичні та післямісійні дані: уточнені карти, класифікації об’єктів, підсумкові звіти та

набори даних, які можуть бути використані для навчання нових моделей або покращення алгоритмів.

2.2.3 Класифікація типів загроз

Усі потенційні загрози можна класифікувати за джерелами та характером впливу [8,9]:

– пасивні загрози – прослуховування каналів зв’язку, збір метаданих, аналіз трафіку, спроби відновлення криптографічних ключів. Такі дії не змінюють інформаційний потік, але призводять до втрати конфіденційності;

– активні загрози – модифікація повідомлень, вставлення хибних пакетів, повторне передавання перехоплених даних (*replay*-атаки), імітація вузлів системи (*spoofing*). Вони безпосередньо порушують цілісність та автентичність інформації;

– фізичні загрози – крадіжка або пошкодження буя, несанкціонований доступ до мікроконтролерів, підміна сенсорів;

– техногенні загрози – електромагнітні перешкоди, глушіння сигналів, втрата живлення, відмова елементів через тиск і корозію;

– організаційні загрози – порушення правил експлуатації, витік ключів через людський фактор, неправильне налаштування протоколів.

Для адекватного оцінювання загроз важливо окреслити типи можливих зловмисників:

– пасивний спостерігач: має обладнання для перехоплення сигналів, але не змінює їх;

– активний атакувальник – здатен генерувати або підмінювати повідомлення, створювати перешкоди.

– інсайдер – працівник чи підрядник, який має частковий доступ до системи й може навмисно або несвідомо її компрометувати;

– висококваліфікований державний супротивник – володіє значними ресурсами, здатний проводити багаторівневі кібератаки, використовувати супутникові засоби спостереження, складні криптоаналітичні методи.

Ймовірні методи атаки на безпілотні транспортні засоби.

Потенційно, проти безпілотних транспортних засобів може бути реалізовано шість типів методів кібератак: підміна даних Глобальної навігаційної супутникової системи (ГНСС), *DoS*, глушіння, атаки зі злому паролів, впровадження шкідливого програмного забезпечення та модифікація прошивки [3,8,10-12].

Проблема спуфінгу, тобто навмисної підміни підводного апарата або радіобуя зловмисником, є однією з найкритичніших для системи інформаційного обміну. У цьому випадку противник може видати себе за легітимний елемент системи, перехоплювати дані, втручатися в обмін повідомленнями або надсилати хибні команди, що безпосередньо впливають на роботу ПА. У морському середовищі загроза особливо значуща, адже контролювати фізичний доступ до радіобуя значно складніше, ніж у звичайних наземних системах. Тому створення надійного механізму підтвердження автентичності є ключовим компонентом захисту всієї архітектури обміну даними.

Фальсифікація даних, тобто навмисне спотворення або модифікація переданої інформації, є однією з найбільш небезпечних загроз для системи інформаційного обміну підводного апарата. На відміну від пасивного перехоплення, фальсифікація передбачає активне втручання у зміст пакетів, що передаються з АНПА РБ до поста керування та серверів збереження. Якщо зловмиснику вдається змінити телеметрію, він може приховати реальний стан апарата, створити хибні аварійні сигнали або навпаки – приховати критичні несправності. У випадку зміни команд управління наслідки можуть бути ще серйознішими, адже АНПА може виконати несанкціоновані дії, небезпечні як для себе, так і для оточення.

Під час атаки з використанням підміни ГНСС імітуються фактичні сигнали ГНСС, а для створення хибного знання про місцезнаходження передаються фальшиві сигнали. Виробники програмують приймачі ГНСС на використання найсильнішого сигналу, щоб приймач міг отримати точніше

місцезнаходження. Отже, для успішної атаки сигнали підміни повинні бути сильнішими за реальні сигнали, що спонукає приймач ГНСС приймати підроблені сигнали ГНСС замість реальних сигналів ГНСС. В результаті приймач не може визначити своє поточне (і точне) місцезнаходження.

Глушіння є однією з найважливіших проблем протоколів бездротового зв'язку. Цей тип атаки призводить до порушення роботи послуг шляхом блокування радіочастот. Глушіння може здійснюватися легально або незаконно. Пристрій глушіння, який називається глушителем, передає сигнал на тій самій частоті, що й цільова система або пристрій. Достатня потужність дозволяє сигналу глушіння перекривати справжній сигнал. В результаті цієї атаки приймач не може отримувати дані від справжнього передавача.

Здійснення атаки з глушінням ГНСС на безпілотний транспортний засіб простіше, ніж підміна ГНСС. Більше того, глушіння ГНСС менш небезпечне, ніж підміна ГНСС, оскільки цільовий приймач може виявити аномальну ситуацію та попередити оператора безпілотного транспортного засобу. Тим не менш, транспортний засіб або оператор не зможуть визначити поточне місцезнаходження за допомогою ГНСС, тим самим втрачаючи свої навігаційні можливості.

Проблема перехоплення інформації є однією з найбільш поширених та водночас небезпечних загроз для будь-якої системи зв’язку, особливо тієї, що працює у відкритих середовищах. Зловмисник, маючи можливість непомітно отримувати дані телеметрії, координати апарата, інформацію про сенсори та наземні команди, здатен значно посилити свої розвідувальні можливості. Більше того, отримання інформації про технічні характеристики сигналу або структурні особливості протоколів може стати підґрунтям для подальших атак, включаючи спуфінг, фальсифікацію та *DoS*.

Загалом, для доступу до інтерфейсів обслуговування системи потрібен пароль. Правильний пароль можна розкрити за допомогою кількох методів злому паролів, таких як атака за словником, атака райдужної таблиці та атака методом перебору. Після злому пароля зловмисники можуть змінювати робочі

параметри, що негативно впливає на ефективність та надійність ураженої системи.

Атака за словником використовує список слів, що використовуються окремо або в комбінації, для злому пароля жертви. Для порівняння, атака методом перебору схожа на атаку за словником, за винятком того, що вона може використовувати слова, що не входять до словника, з буквено-цифровими комбінаціями. Хоча використання цього методу для злому пароля може зайняти багато часу, пароль зрештою можна ідентифікувати, якщо жертва не вжила необхідних запобіжних заходів. Атака за райдужною таблицею також схожа на атаку на основі словника. Цей метод атаки використовує список попередньо обчислених хешів, створених з потенційних паролів, включаючи заданий алгоритм.

DoS – це ефективний метод кібератаки на мережі. У цьому випадку зловмисник передає до мережі великий обсяг пакетів нульових даних. Непотрібні пакети даних споживають мережеві ресурси. Мережа жертви не в змозі відповідати на надмірну кількість отриманих запитів і зрештою виходить з ладу.

Розподілена відмова в обслуговуванні (*DDoS*), різновид *DoS*-атаки, важче виявити з точки зору шкідливого трафіку, ніж *DoS*-атаку, оскільки зловмисник використовує «зомбі-комп'ютери» під час такої атаки. Термін «зомбі-комп'ютер» стосується комп'ютера, який був заражений шкідливим програмним забезпеченням перед атакою. Зловмисник запускає зомбі-комп'ютери непідготовлених користувачів, щоб вони надсилали шкідливі пакети даних до мережі жертви.

Внаслідок можливої *DoS*- або *DDoS*-атаки на примітивні датчики, зокрема, безпілотний транспортний засіб теоретично може бути змушений рухатися з занадто низькою швидкістю.

Впровадження шкідливого програмного забезпечення. Шкідливе програмне забезпечення – це шкідливе програмне забезпечення, розроблене для роботи в певній операційній системі, такій як *Mac OS, Windows* або *UNIX*. Різні

типи шкідливого програмного забезпечення, що використовуються для різних цілей, доступні під різними назвами, включаючи віруси, черв'яки, шпигунські програми, рекламні програми, трояни, боти, руткіти, кейлогери та програми-вимагачі. Шкідлива програма може пошкодити файли на комп'ютері, відстежувати діяльність жертви або створювати бекдор для подальших атак. Крім того, шкідливе програмне забезпечення може використовуватися для кібервійни.

Шкідливе програмне забезпечення може інфікувати системи керування, які можуть бути інфіковані через бортовий діагностичний порт, вбудовані веббраузери, медіаплеєри та знімні порти.

Виробники часто випускають нові версії прошивки, що використовується для систем безпілотних транспортних засобів, щоб виправити різні проблеми або підвищити продуктивність. Така нова прошивка може повністю змінити поведінку безпілотного транспортного засобу. Якщо зловмисник зможе внести будь-які зміни до прошивки або встановити модифіковану прошивку, що належить будь-яким системам безпілотного транспортного засобу, це може призвести до аварій.

Висновки до розділу

Проведено класифікацію основних вразливостей системи за п’ятьма групами: фізичні, комунікаційні, програмні, криптографічні та організаційні. Встановлено, що найбільш небезпечними є загрози, які пов’язані з відкритістю каналу зв’язку (перехоплення та фальсифікація даних), можливістю підміни вузла (спуфінг) та атакою на сервер постобробки.

Проаналізовано методи потенційного впливу зловмисника: глушіння, підміна ГНСС-сигналу, ін’єкція команд, DoS/DDoS, компрометація паролів та впровадження шкідливого ПЗ.

3 СПОСОБИ ЗАБЕЗПЕЧЕННЯ ЗАХИСУ

3.1 Аналіз заходів зменшення вразливостей системам інформаційного обміну

3.1.1 Захист від спуфінгу та підміни підводного апарата

Одним із традиційних рішень, що використовується у телекомунікаційних системах, є застосування статичних криптографічних ключів [13,14]. У цьому випадку АНПА РБ і пост керування мають заздалегідь узгоджений секрет, який використовується для підтвердження справжності пакетів даних (наприклад, через *HMAC*). Перевага такого підходу полягає в простоті реалізації й невеликій обчислювальній вартості. Проте його основною слабкістю є вразливість до компрометації ключа. Якщо зловмисник отримує доступ до статичного секрету, він з легкістю може імітувати поведінку одного з пристроїв. Крім того, статичні ключі погано підходять для систем із тривалим циклом експлуатації, оскільки їх потрібно регулярно оновлювати, що в умовах підводних операцій робити складно.

Альтернативним варіантом є застосування криптографічних протоколів з обміном сеансовими ключами. Протоколи на зразок *ECDH* дозволяють генерувати унікальні, одноразові ключі для кожної сесії зв'язку. Це значно ускладнює спуфінг, оскільки сторонній пристрій не може передбачити або відтворити сеансовий ключ без участі обох легітимних сторін. Проте впровадження таких алгоритмів вимагає збільшених обчислювальних ресурсів, що є викликом для підводних апаратів, які мають обмежені енергетичні запаси.

Ще один метод захисту – використання цифрових підписів або сертифікатів (наприклад, *ECDSA*). У цьому випадку кожен пакет даних або команда має криптографічний підпис, який можна перевірити навіть на нестабільному каналі. Цей метод дає найвищу стійкість проти підміни, адже навіть у разі перехоплення сигналу атакувальник не здатен створити пакет,

який буде розпізнано як автентичний. Водночас підхід з цифровими підписами має певні обмеження – він потребує значних обчислювальних потужностей, а також наявності цілісної системи управління ключами. Для підводних апаратів, що мають обмежену енергетику й працюють у складних умовах, постійна генерація та перевірка підписів може стати суттєвим навантаженням.

Додатковим рішенням є застосування маркерів фізичного рівня. Це такі параметри, як унікальна спектральна структура сигналу, індивідуальний акустичний «відбиток» передавача або характерні частотні переходи. Подібні методи не ґрунтуються на криптографії, але дозволяють визначити, чи є джерело сигналу справжнім, аналізуючи його фізичні характеристики. Перевага такого методу полягає в тому, що він практично «безкоштовний» з точки зору обчислень і працює швидко. Його недолік – нижча точність та можливість обходу досвідченим супротивником, який здатний відтворити спектральні характеристики сигналу.

3.1.2 Захист від фальсифікації даних (*Tampering*)

Одним із найвідоміших базових засобів захисту є використання контролю цілісності на основі *CRC* або контрольних сум. Цей метод широко застосовується у багатьох промислових протоколах через свою простоту, швидкість і мінімальне навантаження на обчислювальні ресурси. Проте *CRC* абсолютно не придатний як засіб захисту від навмисної модифікації, оскільки зловмисник може легко перерахувати контрольну суму після зміни пакета. Отже, CRC підходить для базової перевірки, але не може забезпечити справжню безпеку перед навмисним втручанням [15,16].

Набагато ефективнішим механізмом є використання криптографічних кодів автентифікації повідомлень (*MAC*), зокрема *HMAC*. У цьому випадку кожен пакет даних отримує спеціальний тег, обчислений на основі секретного ключа, відомого лише двом сторонам. Будь-яке втручання в пакет, навіть заміна одного біта, призводить до повної зміни тегу, що робить модифікацію непомітною фізично неможливою для супротивника без знання ключа. Перевага *HMAC* полягає в тому, що він забезпечує високу стійкість, але при

цьому має невеликі обчислювальні вимоги, що є важливою умовою у проєктах, де необхідно зберігати енергію підводного апарата. Однак недолік цього методу – необхідність зберігати секретний ключ у безпечному вигляді та забезпечувати його періодичну ротацію.

Ще одним підходом до захисту є використання цифрових підписів і криптографічних сертифікатів. Ця технологія на рівень вища за *MAC*, адже дозволяє перевіряти не лише цілісність, а й походження повідомлення. Підписані дані забезпечують захист на основі відкритого ключа, що дозволяє виявляти навіть складні атаки, включаючи ситуації, коли супротивник отримав доступ до одного з проміжних вузлів. Усі зміни в підписаному пакеті негайно роблять його недійсним. Основний недолік цифрових підписів – велика обчислювальна вартість.

Окремо слід згадати про так звані протоколи «цілісність + автентифікація», які поєднують шифрування та захист від фальсифікації в одному алгоритмі. Найвідомішим із них є *AES* у режимі *GCM*, який забезпечує не лише конфіденційність, але й справжній захист від спотворення даних.

3.1.3 Захист від перехоплення інформації (*Confidentiality*)

Первинним і найпоширенішим методом захисту від перехоплення є застосування симетричного шифрування [18]. Алгоритми на основі *AES* давно зарекомендували себе як надійний та ефективний інструмент шифрування даних. Їхньою перевагою є висока продуктивність, хороша стійкість до криптоаналізу та відносно невелика кількість обчислень. Для системи АНПА РБ симетричне шифрування є привабливим через свою енергоефективність, але потребує безпечного обміну ключами. У випадку компрометації секретного ключа вся система стає відкритою для стороннього прослуховування. Цей недолік ускладнює застосування чистого симетричного шифрування без додаткових механізмів ротації ключів та їх оновлення.

Іншим підходом є використання асиметричного шифрування, яке дозволяє уникнути проблеми спільних секретів. Однак підводні апарати через обмежену енергетику та обчислювальні ресурси не можуть постійно

використовувати алгоритми на кшталт *RSA* або навіть більш сучасних еліптичних кривих у режимі шифрування великих обсягів даних. Проте асиметрична криптографія може використовуватися в системі управління ключами для періодичної генерації симетричних ключів, що значно підвищує стійкість системи без постійного додаткового навантаження на модем РБ.

Більш складним, але надзвичайно ефективним методом захисту є застосування шумоподібних сигналів або розширеного спектру. Технології *DSSS* чи *FHSS* широко використовуються в радіозв'язку. У такому випадку сигнал маскується під природний шум, має фрагментовану структуру або використовує стрибкоподібну зміну частоти. Це робить його майже непомітним на фоні гідроакустичних шумів. Основна перевага такого підходу – зміна форми сигналу на фізичному рівні, що ускладнює його детекцію навіть при застосуванні широкосмугових приймачів. Проте реалізація таких методів потребує складної апаратної підтримки і точного синхронізму між передавачем і приймачем.

Ще один напрям – захист конфіденційності через сегментацію інформації. Суть методу полягає у тому, що телеметрія і команди передаються у вигляді фрагментів, які не несуть самостійної інформаційної цінності. Навіть у випадку перехоплення кількох частин зловмисник не здобуває цілісної картини. Цей підхід ефективний для захисту від некваліфікованих противників, але не забезпечує надійного захисту проти спеціалізованих систем перехоплення.

3.1.4 Захист від атак типу *DoS* та глушіння сигналу (*Denial-of-Service*)

На відміну від більш прихованих видів атак, *DoS* не обов'язково потребує високої технічної підготовки. Часто достатньо створити сильні радіоперешкоди, щоб канал зв'язку став недоступним.

Одним із найпоширеніших методів протидії глушінню є використання розширеного спектру та стрибкоподібної зміни частоти (*FHSS*) [19,20]. У цьому підході передавач і приймач узгоджують послідовність частот, які постійно змінюються під час роботи каналу. Глушити один або кілька діапазонів стає марно, адже сигнал швидко перемикається між частотами. Противнику

доводиться створювати широкосмугову перешкоду, що потребує значно більшої енергетичної потужності. Цей метод давно застосовується у військових радіостанціях і добре зарекомендував себе у складних середовищах.

Іншим підходом є застосування технології *DSSS*, при якій сигнал розширюється у ширший діапазон частот за допомогою коду прямого розширення спектра. На фоні акустичних шумів такий сигнал стає менш помітним і менш чутливим до глушіння. Його перевага полягає в тому, що навіть при частковому перекритті спектра сигнал може бути реконструйований. Але *DSSS* потребує складної апаратної підтримки та високої обчислювальної потужності, що в умовах обмежених ресурсів АНПА є значним викликом.

Третім напрямом захисту є адаптивне регулювання потужності передавання. У разі виявлення перешкод система збільшує потужність сигналу або змінює його параметри, щоб подолати шум. Такий підхід добре працює у радіоканалах, але в акустичному середовищі підвищення потужності може призвести до небажаних ефектів: збільшення турбулентності, втрат енергії чи навіть викриття координат АНПА РБ. Крім того, цей метод має обмеження через енергоефективність батарейного живлення.

Надзвичайно ефективним практичним методом захисту від *DoS* є використання резервних каналів зв’язку. При відмові або блокуванні основного каналу система має змогу автоматично переключитися на резервний. Такий підхід забезпечує високу стійкість до глушіння, але вимагає складнішої архітектури обміну та наявності резервної апаратури, що збільшує масу, складність і вартість системи.

Існує й інший концептуально відмінний метод захисту – виявлення та класифікація перешкод. Замість того щоб протидіяти їм безпосередньо, система аналізує характеристики шуму і, за необхідності, переходить у аварійний режим. Наприклад, РБ може зробити паузу у передаванні, змінити позицію або зменшити інтенсивність обміну, щоб уникнути «забивання» каналу. Такий підхід підвищує живучість системи, але його ефективність залежить від точності алгоритмів виявлення перешкод.

3.1.5 Захист прошивки, обладнання та ланцюжка постачання

Одним із базових методів захисту є реалізація механізму захищеного завантаження (*Secure Boot*). У цій моделі кожен елемент прошивки, починаючи від первинного завантажувача до високорівневого програмного коду, перевіряється за допомогою криптографічного підпису. Пристрій дозволяє запуск лише тих компонентів, які пройшли верифікацію. У разі спроби замінити прошивку або модифікувати окремі блоки, система блокує запуск, що робить можливість інжекції шкідливого коду практично нереальною. Основною перевагою цього методу є високий рівень безпеки, але недоліком є необхідність точного управління ключами підпису [21, 22].

Іншим способом є використання апаратних захисних модулів, таких як *TPM* або *TEE*. Вбудовані модулі апаратної довіри забезпечують захист ключів, ізоляцію чутливих даних і функцій, а також механізми контролю цілісності. Такі модулі дозволяють гарантувати, що критично важливі обчислення (наприклад, верифікація команд або ключів) виконуються у середовищі, яке не може бути змінене навіть у разі зламу операційної системи. Проте, впровадження таких модулів у підводні апарати може бути проблематичним через вимоги до енергоспоживання, обмежений простір на платах і фізичні навантаження у морській воді.

Окрему увагу слід приділити контролю цілісності прошивки протягом експлуатації. Навіть якщо *Secure Boot* гарантує чистоту завантаження, необхідно забезпечити захист від модифікації програмного забезпечення вже після запуску. Для цього застосовуються технології періодичного хешування, ревізії контрольних сум або віддаленої валідації firmware. В умовах підводних операцій прямий віддалений аудит у реальному часі є недоступним, проте можна застосовувати модель з періодичним підняттям АНПА на поверхню або передаванням контрольних структур через акустичний канал. Такі підходи створюють компроміс між безпекою та практичними можливостями системи.

Важливим аспектом захисту є безпека ланцюжка постачання. Якщо зловмисник отримує доступ до апаратури на етапах виробництва,

транспортування або зберігання, він може встановити апаратні закладки, змінити компоненти, інтегрувати додаткові модулі прослуховування або відкрити приховані канали управління. Ці загрози часто є недооціненими, оскільки трапляються рідше, ніж атаки на канали зв’язку, але їхній вплив значно сильніший: підміна компонентів, зміна радіочастотних модулів або маніпуляції із сенсорами можуть бути майже непомітними під час експлуатації. Тому у системі необхідно передбачити процедури контролю якості, аудит апаратних партій, пломбування та маркування, а також застосування криптографічних сертифікатів автентичності обладнання.

Ще один важливий напрям – сегрегація прав доступу. Підводний апарат і радіобуй повинні мати мінімально необхідні привілеї, а всі команди зберігатися у захищених областях пам’яті. Адміністративний доступ має бути обмежений окремими обліковими даними, які не можуть передаватися через канал зв’язку. Така сегрегація дозволяє обмежити навіть внутрішні загрози, зокрема ризики помилок персоналу або підміни конфігурацій після технічного обслуговування.

3.1.6 Багаторівневий захист системи та протидія атакам на ланцюжок взаємодії

Захист системи інформаційного обміну підводного апарата не може бути забезпечений використанням лише одного методу чи ізольованої технології. З огляду на складність архітектури, різнорідність середовищ передачі (радіо, IP-мережі), обмеження апаратних ресурсів та можливість появи складних багатовекторних атак, система повинна мати багаторівневу архітектуру захисту. Її мета полягає не лише у запобіганні окремим загрозам, а у створенні ситуації, коли навіть комплексна атака на кілька рівнів одночасно не призведе до компрометації системи. Такий підхід відомий як «*defense in depth*» – оборона в глибину.

Першим рівнем багаторівневого захисту є фізичний контроль та апаратна безпека. Він включає перевірку цілісності обладнання, пломбування корпусів, захист портів, ізоляцію внутрішніх шин і встановлення модулів апаратної довіри. Саме на цьому рівні запобігають заміні компонентів, встановленню

шкідливих модулів та втручанню у ланцюжок постачання. Якщо цей рівень порушено, будь-які криптографічні або мережеві механізми втрачають сенс, адже атакувальник вже має прямий доступ до внутрішньої логіки пристроїв.

Другий рівень безпеки забезпечують криптографічні протоколи автентифікації та цілісності. Як було показано в попередніх підпунктах, використання *HMAC* у гідроакустичному каналі, *AES-GCM* у радіосегменті та цифрових підписів у наземній частині системи забезпечує потужний бар'єр для атак спуфінгу та *tampering*. Завдяки цьому навіть якщо зловмисник має можливість перехоплювати пакети, модифікувати їх чи намагатися підробити команди, він не може пройти криптографічний контроль і бути сприйнятим як легітимний вузол системи.

Третім рівнем є захист конфіденційності - шифрування даних на всіх сегментах каналу. Цей рівень особливо важливий з огляду на відкритість морського та радіоефірного середовищ. Шифрування забезпечує, що перехоплені дані не можуть бути прочитані, що критично у випадку передачі координат, телеметрії, стану апарата та об'єктів дослідження. Завдяки використанню симетричних алгоритмів помірної складності в акустичному сегменті та більш потужних протоколів у наземних частинах системи, забезпечується оптимальний баланс продуктивності й стійкості.

Четвертим рівнем стає захист доступності, тобто протидія атакам типу *DoS* та глушіння. Акустичний та радіоканали є природно вразливими до перешкод, тому застосування *FHSS*, зміни швидкості передачі, резервних частотних діапазонів та аналізу спектральних аномалій є ключовими механізмами підтримання працездатності системи. Крім того, резервні канали дозволяють зберегти хоча б мінімальний контроль над ПА навіть у разі повного глушіння основного каналу, що істотно підвищує надійність.

П'ятий рівень – це контроль поведінки та аналіз аномалій. Він передбачає постійний моніторинг параметрів трафіку, виявлення нестандартних шаблонів, незвичних стрибків потужності сигналу, частотних збоїв або непослідовності пакетів. Такі алгоритми можуть бути реалізовані як у РБ, так і на рівні поста

керування. Це дозволяє швидко виявити початок атаки, навіть якщо вона ще не призвела до повної втрати зв’язку чи компрометації.

Шостим рівнем виступає організаційний захист, що включає процедури оновлення ключів, ревізію прошивки, аудит логів, перевірку технічного стану та контроль доступу персоналу. Хоча він не впливає безпосередньо на технічні властивості каналів, саме цей рівень запобігає внутрішнім загрозам, помилкам операторів та порушенням процедури безпеки.

Загальна ефективність системи забезпечується саме взаємодією всіх рівнів. Наприклад, навіть якщо зловмисник використовує високопотужне обладнання для глушіння радіоканалу, *FHSS* уповільнить атаку, резервний канал дозволить передати аварійні повідомлення, а контроль аномалій зафіксує факт втручання. Якщо ж атакувальник спробує підмінити ПА чи РБ, криптографічна автентифікація заблокує його дії, а апаратна перевірка цілісності унеможливить встановлення шкідливої прошивки.

Таким чином, багаторівнева архітектура захисту перетворює навіть складну та різнорідну систему інформаційного обміну на стійку платформу, здатну протидіяти як простим, так і комплексним атакам. Це забезпечує не лише збереження даних та контрольованість ПА, але й довготривалу експлуатаційну надійність системи.

3.2 Аналіз моделей загроз

Моделювання загроз – це структурований процес виявлення, аналізу та зменшення потенційних загроз для системи, програми чи організації. Він проактивно виявляє вразливості до їх використання, що дозволяє краще зменшити ризики та підвищити безпеку. Воно допомагає виявляти, повідомляти та розуміти загрози та способи їх зменшення, одночасно захищаючи цінні активи. Моделювання загроз використовує гіпотетичні сценарії, системні схеми та тестування для захисту систем і даних.

Мета моделювання загроз полягає в тому, щоб якомога раніше виявити, повідомити та зрозуміти загрози та заходи щодо їх пом'якшення для зацікавлених сторін організації. Документація цього процесу надає системним аналітикам та захисникам детальний аналіз ймовірних профілів зловмисників, ймовірних векторів атак та активів, які найбільше шукають зловмисники.

Ключові компоненти моделі загроз:

– опис об'єкта моделювання;

– припущення, які можна підтвердити або оскаржити з часом;

– потенційні загрози, що стосуються системи або середовища;

– заходи з пом'якшення наслідків для кожної виявленої загрози;

– кроки перевірки для забезпечення ефективності пом'якшувальних заходів.

Процес моделювання загроз гарантує, що безпека інтегрована на етапі проектування та підтримується протягом усього життєвого циклу застосунку.

1. Визначте обсяг та цілі. Точно визначте, що ви моделюєте (наприклад, лише /*login* кінцеву точку фінансової програми), чому це важливо (наприклад, захист паролів користувачів і токенів сеансу) та хто відповідає за прийняття рішень.

2. Створіть схему системи. Накресліть основні компоненти, потоки даних, точки взаємодії з користувачем та межі довіри. Використовуйте простий *DFD* або ескіз у вигляді рамок та стрілок.

3. Виявлення загроз. Цей крок зосереджений на виявленні потенційних загроз та розумінні того, що може піти не так у процесі. Загрози можна виявити, аналізуючи системні схеми, потоки даних та взаємодію з користувачами. Такий інструмент, як *STRIDE*, допомагає охопити ключові категорії: підробка, втручання, розкриття інформації, *DoS* тощо.

4. Аналізуйте та визначайте пріоритети ризиків. Оцініть ймовірність та вплив (наприклад, крадіжка облікових даних має високий вплив, але робота зсередини трапляється рідко). Використовуйте просту таблицю оцінок або шкалу.

5. Пом'якшення наслідків. Для основних загроз оберіть стратегію пом’якшення: виправте її, зменшіть її ймовірність чи вплив або прийміть її. Задокументуйте власника, вартість та план перевірки.

6. Перегляд та повторення. Тестуйте впроваджені елементи керування (наприклад, спробуйте обійти зчитування відбитків пальців), оновлюйте діаграму, якщо додаток змінюється, і періодично повторюйте.

Команда розробників зможе впроваджувати безпеку додатків як частину процесу проектування та розробки, використовуючи моделювання загроз для виявлення загроз, ризиків та заходів щодо їх пом'якшення на етапі проектування. Існують різні методології моделювання загроз.

3.2.1 *STRIDE*

Метод моделювання загроз *STRIDE* [23] – один із найпоширеніших інструментів у сфері безпеки програмного забезпечення, який дозволяє системно аналізувати потенційні атаки та недоліки в архітектурі системи ще на етапі проєктування. Його застосування допомагає будувати системи з урахуванням принципів *Secure by Design*, мінімізуючи ризики ще до появи коду або у процесі його розробки.

Основна ідея *STRIDE* полягає в тому, щоб розглядати систему через призму шести можливих класів загроз. Кожна буква акроніму відповідає окремій категорії, що описує конкретний тип небезпек. Завдяки цьому модель дозволяє не просто виявити окремі вразливості, а створити повну картину поверхні атаки та зосередити увагу на покращенні специфічних елементів архітектури.

Категорії загроз у *STRIDE*:

1. *Spoofing* (Підміна особи). Це загроза, пов’язана з порушенням автентифікації — коли зловмисник може видавати себе за іншу особу або сервіс. Приклади включають підробку облікових даних, використання вкрадених токенів, маніпулювання ідентифікаторами сесій. Ціль атак – порушення ідентифікації.

2. *Tampering* (Підробка даних). Стосується загроз, пов’язаних із порушенням цілісності інформації. Це може бути зміна файлів на диску, перехоплення та модифікація повідомлень у мережі, або зміна конфігураційних параметрів. Ціль атак – порушення цілісності.

3. *Repudiation* (Відмова від авторства дій). Цей тип загроз виникає у випадках, коли відсутнє належне журналювання або цифрове підписування дій. Користувач може заперечити факт виконання транзакції, і довести його вину стає неможливо. Ціль атак – порушення спостережності.

4. *Information Disclosure* (Розкриття інформації). Загрози, пов’язані з порушенням конфіденційності. Сюди належать витоки персональних даних, доступ до внутрішніх документів, або можливість читати трафік, який не був належним чином зашифрований. Ціль атак: порушення конфіденційності.

5. *Denial of Service* (Відмова в обслуговуванні). Атаки, які роблять систему недоступною для звичайних користувачів. Це може бути перевантаження ресурсів, блокування каналів зв’язку, або навмисне пошкодження компонентів системи. Ціль атак – порушення доступності.

6. *Elevation of Privilege* (Підвищення привілеїв). Це загрози, коли зловмисник отримує рівень доступу, вищий за той, який йому дозволено. Часто можливе завдяки вразливостям у коді або неправильній конфігурації. Ціль атак: порушення моделі доступу.

STRIDE – це універсальний і широко застосовуваний метод моделювання загроз, який допомагає командам розробників і фахівцям з безпеки системно виявляти потенційні слабкі місця в архітектурі та процесах. Він забезпечує чітку структуру аналізу та дозволяє впроваджувати ефективні заходи захисту задовго до того, як проблеми стануть критичними.

3.2.2 *DREAD*

Метод моделювання загроз *DREAD* — це система оцінки ризиків у комп’ютерних системах, яка допомагає визначати пріоритетність загроз на основі кількісної шкали [24]. *DREAD* був розроблений компанією *Microsoft* і часто використовується разом із іншими методами моделювання загроз,

наприклад *STRIDE*, для більш повної оцінки безпеки системи. На відміну від *STRIDE*, який класифікує типи загроз, *DREAD* дозволяє оцінювати серйозність кожної загрози та визначати, на які саме слід звернути пріоритетну увагу.

DREAD – це акронім із п’яти факторів, за якими оцінюють загрозу:

– *D – Damage Potential* (Потенційна шкода). Наскільки серйозні наслідки, якщо загроза буде реалізована. Приклад: злам адміністративного облікового запису може призвести до повного контролю над системою, що має високий рівень шкоди;

– *R – Reproducibility* (Відтворюваність). Наскільки легко повторити атаку. Приклад: якщо атакувати систему можна лише один раз у складних умовах – низька відтворюваність, якщо будь-хто може легко відтворити атаку – висока;

– *E – Exploitability* (Експлуатованість). Наскільки легко зловмиснику реалізувати атаку. Приклад: доступність інструментів, складність коду, необхідність спеціальних знань;

– *A – Affected Users* (Кількість постраждалих користувачів). Скільки користувачів або систем постраждають від реалізації загрози. Приклад: загроза, яка впливає на всю базу користувачів, має вищий бал, ніж та, що впливає на одного користувача;

– *D – Discoverability* (Виявленість). Наскільки легко потенційному зловмиснику знайти вразливість. Приклад: якщо слабке місце очевидне або легко знайти у публічній документації – висока виявленість.

DREAD має так і етапи роботи:

– ідентифікація загроз – спочатку формують список потенційних загроз, наприклад, за допомогою *STRIDE* або іншого методу моделювання;

– оцінка кожної загрози за п’ятьма факторами – кожен фактор оцінюється за числовою шкалою, наприклад від 1 до 10.

– обчислення загального балу ризику – для кожної загрози сумують оцінки факторів або беруть середнє значення. Це дозволяє ранжувати загрози від найнебезпечніших до менш критичних.

– пріоритизація заходів безпеки – загрози з високим *DREAD*-балом розглядаються першочергово для розробки контрзаходів. Це допомагає ефективно розподіляти ресурси на захист системи.

DREAD – ефективний інструмент для кількісної оцінки та пріоритизації загроз у програмних системах. У поєднанні з STRIDE або іншими методами він дозволяє не тільки ідентифікувати потенційні загрози, а й визначати, які з них мають найвищий пріоритет для усунення або мінімізації ризиків.

3.2.3 *CIA*

Метод моделювання загроз *CIA* — це класичний підхід у сфері інформаційної безпеки, який базується на трьох ключових принципах: конфіденційність (*Confidentiality*), цілісність (*Integrity*) і доступність (*Availability*). Ця модель слугує фундаментальною рамкою для оцінки будь-якої системи з точки зору її безпеки [25].

Конфіденційність (*Confidentiality*) забезпечує захист інформації від несанкціонованого доступу. Це гарантує, що дані можуть читати лише ті користувачі або системи, які мають на це право. Прикладами заходів є шифрування, автентифікація користувачів і контроль доступу. Загрози конфіденційності включають витік персональних даних, крадіжку паролів або несанкціоноване читання файлів.

Цілісність (*Integrity*) гарантує, що дані або ресурси системи не змінюються без дозволу. Це забезпечує достовірність та коректність інформації. Заходи для забезпечення цілісності включають цифрові підписи, контроль версій та хешування даних. Прикладами загроз є підміна файлів, зміна бази даних або несанкціоноване редагування коду.

Доступність (*Availability*) забезпечує безперебійний доступ до інформації та систем для легітимних користувачів. Це означає, що користувачі можуть отримати необхідні ресурси у потрібний час. Для підтримки доступності застосовують резервування серверів, системи відновлення після збоїв, захист від DoS-атак. Загрози доступності включають відмови в обслуговуванні, збої обладнання або видалення даних.

Застосування методу *CIA* починається з ідентифікації активів системи та аналізу потенційних загроз для кожного активу через призму конфіденційності, цілісності та доступності. Після цього визначають пріоритетність ризиків і розробляють відповідні заходи захисту, такі як політики безпеки, технічні рішення та процедури контролю доступу.

Переваги методу *CIA* полягають у простоті та зрозумілості, а також у можливості охопити більшість загроз безпеці інформації. До обмежень належить те, що він не класифікує конкретні типи загроз і не дозволяє кількісно оцінювати ризики, тому для детального аналізу безпеки часто поєднується з іншими методами, наприклад *STRIDE* або *DREAD*.

Отже, метод *CIA* є фундаментальною моделлю для оцінки безпеки систем, що допомагає структурувати підхід до захисту активів через три основні аспекти: конфіденційність, цілісність і доступність.

3.2.4 *Trike*

Trike – це методологія, орієнтована на ризик, з кроками, подібними до кроків інших підходів [26].

1. На етапі ідентифікації система, що аналізується, розбивається на її компоненти, і виявляються потенційні загрози для кожного елемента, включаючи несанкціонований доступ, витоки даних, відмову в обслуговуванні та інші вразливості безпеки.

2. Виявлені загрози потім аналізуються для визначення їхньої ймовірності та потенційного впливу, оцінюючи поверхню атаки системи, цінність захищених активів та ймовірні наслідки успішної атаки.

3. На основі аналізу методологія рекомендує відповідні засоби контролю безпеки та контрзаходи для пом'якшення виявлених загроз, включаючи технічні рішення, засоби контролю доступу та шифрування, а також політики та процедури організації.

4. Заключний етап включає перевірку ефективності впроваджених засобів контролю безпеки та повторення процесу за необхідності для забезпечення постійної безпеки системи.

Організації, які обирають *Trike*, мають такі переваги:

– чітко визначена структура для систематичного виявлення, аналізу та пом'якшення загроз безпеці, яка може допомогти організаціям підтримувати послідовний та комплексний підхід до моделювання загроз.

– *Trike* дозволяє організаціям визначати пріоритети своїх зусиль щодо безпеки та приймати обґрунтовані рішення щодо розподілу ресурсів шляхом кількісної оцінки ймовірності та впливу загроз.

– методологія заохочує співпрацю між різними зацікавленими сторонами, такими як розробники, експерти з безпеки та бізнес-лідери, що призводить до більш цілісного розуміння вимог безпеки системи.

Як завжди, існують проблеми, зокрема:

– Впровадження методології *Trike* може бути трудомістким і вимагати значних ресурсів, особливо для великих або складних систем.

– Деякі аспекти процесу аналізу загроз та оцінки ризиків можуть бути суб'єктивними, що може призвести до невідповідностей або розбіжностей між членами команди.

– *TRIKE* може мати менш широке поширення та підтримку у спільноті безпеки порівняно з іншими методологіями моделювання загроз, такими як *STRIDE* або *PASTA*.

Методологія *Trike* найкраще підходить для організацій, яким потрібен комплексний та структурований підхід до моделювання загроз, особливо для складних або критично важливих систем.

3.2.5 *VAST*

Методологія *VAST* наголошує на використанні візуальних діаграм та моделей для представлення системи або програми, що оцінюється, допомагаючи зацікавленим сторонам краще зрозуміти архітектуру системи, потоки даних та потенційні поверхні атаки.

Основна увага *VAST* приділяється виявленню та аналізу потенційних загроз для системи, враховуючи різних суб'єктів загроз, їхню мотивацію та методи, які вони можуть використовувати для експлуатації вразливостей, а

також заохоченню комплексного аналізу загроз, щоб переконатися, що всі відповідні загрози враховані.

VAST розроблена для інтеграції в гнучкі процеси розробки або операцій організації, виконуючи пов'язані завдання ітеративно, з постійними оновленнями та вдосконаленнями в міру розвитку системи, допомагаючи забезпечити врахування питань безпеки протягом усього життєвого циклу розробки або розгортання.

Методологія *VAST* відома своєю простотою та зручністю використання. Вона не вимагає значної підготовки або спеціалізованих знань у сфері безпеки, що робить її доступною для багатьох зацікавлених сторін, включаючи розробників, керівників проектів та бізнес-аналітиків.

Переваги:

– *VAST* допомагає підвищити обізнаність зацікавлених сторін щодо безпеки, оскільки передбачає активну участь у виявленні та усуненні потенційних загроз.

– візуальний та орієнтований на загрози підхід *VAST* сприяє виявленню ширшого спектру загроз порівняно з більш традиційними методами моделювання загроз.

– інтеграція *VAST* у гнучкі процеси добре узгоджується із сучасними практиками розробки та розгортання програмного забезпечення.

– простота *VAST* полегшує його впровадження та застосування в організації, зменшуючи бар'єр для входу в практики безпеки.

Недоліки:

– хоча *VAST* чудово виявляє широкий спектр загроз, він може не забезпечувати такого ж рівня глибини та аналізу, як більш комплексні методології моделювання загроз.

– ефективність *VAST* залежить від знань та участі зацікавлених сторін, які можуть змінюватися залежно від їхньої експертизи та розуміння безпеки.

– простота *VAST* може призвести до зосередження на більш простих загрозах, потенційно ігноруючи більш складні або складні вектори атак.

Методологія моделювання загроз *VAST* найкраще підходить для організацій, які шукають легкий, простий у впровадженні підхід до моделювання загроз або прагнуть інтегрувати моделювання загроз у свої гнучкі процеси. Вона також корисна, коли організації мають обмежені ресурси або експертизу в галузі безпеки та потребують більш доступного рішення для моделювання загроз.

3.3 Аналіз нормативної бази захисту інформаційного каналу

Захист інформаційного каналу в системах дистанційного та автономного управління є одним із ключових аспектів забезпечення інформаційної та кібербезпеки. Для системи інформаційного обміну АНПА РБ та постом керування нормативна база визначає обов’язкові вимоги до забезпечення конфіденційності, цілісності, доступності та автентичності інформації, що передається каналами зв’язку.

Метою даного розділу є аналіз чинної нормативно-правової та нормативно-технічної бази України і Європейського Союзу щодо захисту інформаційного каналу, а також визначення її застосовності до досліджуваної системи.

3.3.1 Нормативно-правове забезпечення захисту інформації в Україні.

Основи захисту інформації в Україні визначаються законами та підзаконними актами, що регламентують діяльність у сфері інформаційної та кібербезпеки.

Базовим законодавчим актом є Закон України «Про захист інформації в інформаційно-комунікаційних системах» [27], який встановлює вимоги до обов’язкового захисту інформації, що обробляється та передається в ІКС. Відповідно до цього закону, передавання інформації каналами зв’язку повинно здійснюватися з використанням технічних та криптографічних засобів захисту, що забезпечують запобігання несанкціонованому доступу, модифікації та знищенню інформації.

Доповненням є Закон України «Про основні засади забезпечення кібербезпеки України» [28], який вводить поняття критичної інформаційної інфраструктури та визначає обов'язки суб'єктів щодо управління кіберризиками, моніторингу та реагування на кіберінциденти. Для систем автономного морського управління цей закон є особливо актуальним з огляду на потенційні фізичні та екологічні наслідки кібератак.

3.3.2 Нормативні документи системи технічного захисту інформації України (НД ТЗІ)

Практична реалізація вимог законодавства у сфері захисту інформації забезпечується нормативними документами Державної служби спеціального зв'язку та захисту інформації України, об'єднаними в систему нормативних документів технічного захисту інформації (НД ТЗІ). Особливу роль для захисту інформаційного каналу відіграють документи серій НД ТЗІ 1.х–3.х.

Документи серії НД ТЗІ 1.х регламентують загальні положення та методологічні основи технічного захисту інформації. До цієї серії належать документи, що визначають[29]:

– терміни та визначення у сфері ТЗІ;

– загальні принципи побудови систем захисту;

– підходи до класифікації інформації та об'єктів захисту.

Для інформаційного каналу між автономним морським об'єктом та постом керування ці документи задають концептуальні вимоги щодо необхідності комплексного підходу до захисту, зокрема поєднання криптографічних, технічних та організаційних заходів.

Серія НД ТЗІ 2.х присвячена питанням моделювання загроз, порушника та оцінювання ризиків. У цих документах визначено[30-32]:

– типові моделі загроз для інформаційних систем;

– класи порушників та їх можливості;

– підходи до аналізу вразливостей і визначення рівня захищеності.

У контексті інформаційного каналу дана серія документів є основою для обґрунтування необхідності захисту від перехоплення, підміни та модифікації

даних, а також від атак на доступність каналу зв’язку. Результати *STRIDE*- та *DREAD*-аналізу, виконані у межах цієї роботи, відповідають підходам, закладеним у документах НД ТЗІ 2.х.

Документи серії НД ТЗІ 3.х встановлюють вимоги до створення та впровадження комплексної системи захисту інформації (КСЗІ) в інформаційно-комунікаційних системах. Вони регламентують [33,34]:

– структуру та склад КСЗІ;

– вимоги до технічних і програмних засобів захисту;

– порядок впровадження, випробування та експлуатації системи захисту.

Для інформаційного каналу ці документи визначають необхідність використання сертифікованих засобів криптографічного захисту, організації контролю доступу, журналювання подій та забезпечення стійкості до порушень цілісності і доступності інформації. Впровадження КСЗІ є обов’язковою умовою для систем, що обробляють інформацію з обмеженим доступом.

3.3.3 Національні стандарти України у сфері інформаційної безпеки.

В Україні застосовуються гармонізовані міжнародні стандарти ДСТУ *ISO/IEC* 27001 та ДСТУ *ISO/IEC* 27005 [35,36], які визначають вимоги до системи управління інформаційною безпекою та процесу управління ризиками.

У межах цих стандартів захист інформаційного каналу розглядається як складова комунікаційної безпеки, криптографічного захисту та забезпечення безперервності діяльності. Застосування зазначених стандартів дозволяє інтегрувати вимоги НД ТЗІ у сучасну ризик-орієнтовану модель управління безпекою.

3.3.4 Нормативна база Європейського Союзу у сфері захисту інформаційних каналів

На рівні Європейського Союзу ключовими нормативними актами є Регламент (*EU*) 2016/679 (*GDPR*)[37] та Директива (*EU*) 2022/2555 (*NIS*2). *GDPR* встановлює вимоги до захисту персональних даних, зокрема під час їх передавання каналами зв’язку, а *NIS*2 визначає обов’язкові заходи з управління кіберризиками та забезпечення стійкості мережевих і інформаційних систем.

Технічною основою реалізації вимог ЄС є стандарти *ISO/IEC* 27001, *ISO/IEC* 27002 та *ISO/IEC* 27005, а також рекомендації агентства *ENISA*, які орієнтовані на захист критичних і бездротових комунікацій, у тому числі для автономних та кіберфізичних систем.

Порівняльний аналіз показує, що нормативні вимоги України та Європейського Союзу мають спільну концептуальну основу та базуються на ризик-орієнтованому підході. Водночас українська система НД ТЗІ характеризується більш жорсткою формалізацією процесів та вимог до сертифікації засобів захисту, тоді як у ЄС більший акцент робиться на досягненні визначеного рівня безпеки та відповідальності оператора системи.

Висновки до розділу

Розглянуто криптографічні методи захисту, у тому числі статичні ключі, сеансові ключі, цифрові підписи та використання маркерів фізичного рівня. Показано, що застосування базових механізмів (CRC, прості контрольні суми) є недостатнім для протидії навмисним атакам, а надійний захист може бути забезпечений лише шляхом впровадження криптографічних кодів автентифікації (HMAC) та цифрових підписів.

Також було визначено технічні та організаційні заходи, які підвищують захищеність системи: контроль доступу, журналювання, захист конфігурацій, безпечне оновлення прошивки та моніторинг інтеграції вузлів.

4 ОЦІНКА ЗАХИЩЕНОСТІ СИСТЕМИ

4.1 Оцінка загроз інформаційного обміну для системи автономний підводний апарат з радіобуєм

Система інформаційного обміну між автономним морським рухомим об’єктом та постом керування є критично важливою складовою забезпечення безпечного та ефективного виконання місії. Вона включає бортові обчислювальні засоби автономного об’єкта, сенсорні та навігаційні системи, модуль зв’язку, а також інфраструктуру поста керування з операторським інтерфейсом і серверами управління. Взаємодія між цими компонентами відбувається через потенційно небезпечні канали зв’язку, що обумовлює необхідність детального аналізу загроз інформаційній безпеці.

Згідно з методологією *STRIDE*, першою групою загроз є підміна суб’єктів взаємодії (*Spoofing*). У даній системі можливе маскування зловмисного пристрою під легітимний пост керування або під автономний морський об’єкт. Така атака може призвести до отримання несанкціонованого контролю над об’єктом або до передачі фальшивих телеметричних даних оператору. Наслідком цього є прийняття помилкових рішень або виконання небезпечних команд. Для протидії таким загрозам необхідно застосовувати взаємну криптографічну автентифікацію сторін, використання сертифікатів, а також надійні механізми ідентифікації операторів.

Другою категорією загроз є модифікація даних (*Tampering*). В умовах відкритого або слабко захищеного каналу зв’язку зловмисник може змінювати команди управління, телеметрію або оновлення програмного забезпечення, що передаються між автономним об’єктом і постом керування. Це може спричинити втрату керованості, порушення алгоритмів навігації або навіть фізичне пошкодження об’єкта. Запобігання таким загрозам досягається шляхом застосування механізмів контролю цілісності даних, цифрових підписів,

захищених протоколів зв’язку та перевірки автентичності програмного забезпечення під час завантаження.

Третя група загроз пов’язана із запереченням виконаних дій (*Repudiation*). У разі інцидентів оператор або інші суб’єкти можуть заперечувати факт передачі певних команд чи змін конфігурації, що ускладнює розслідування та аналіз причин подій. Відсутність надійних журналів подій знижує рівень відповідальності та створює юридичні ризики. Для мінімізації цих загроз необхідно впроваджувати невідмовні журнали з цифровими підписами та часовими мітками, що дозволяють однозначно ідентифікувати джерело кожної дії.

Четверта категорія *STRIDE* охоплює загрози розкриття інформації (*Information Disclosure*). Перехоплення даних телеметрії, відеоінформації або координат автономного морського об’єкта може призвести до компрометації місії, особливо у військових або спеціальних застосуваннях. Такі загрози є актуальними через використання бездротових або супутникових каналів зв’язку. Основними заходами захисту в цьому випадку є шифрування інформації на всіх етапах передавання та зберігання, а також обмеження доступу до даних відповідно до ролей користувачів.

П’ята група загроз пов’язана з відмовою в обслуговуванні (*Denial of Service*). Для системи автономного морського об’єкта особливо небезпечними є атаки, що спрямовані на глушіння каналу зв’язку, перевантаження поста керування або виснаження обчислювальних ресурсів бортових систем. Унаслідок таких атак може бути втрачений зв’язок з об’єктом або порушене виконання місії. Зменшення впливу цих загроз досягається шляхом резервування каналів зв’язку, впровадження механізмів виявлення атак та реалізації автономних сценаріїв безпечної поведінки об’єкта у разі втрати зв’язку.

Останньою категорією є підвищення привілеїв (*Elevation of Privilege*). Вразливості програмного забезпечення або помилки конфігурації можуть дозволити зловмиснику отримати розширені права доступу до систем

автономного об’єкта або поста керування. Це створює умови для повного захоплення контролю над системою та виконання шкідливих дій. Для протидії таким загрозам необхідно дотримуватися принципу найменших привілеїв, ізолювати компоненти системи, а також регулярно проводити аудит і оновлення програмного забезпечення.

Таким чином, застосування методу *STRIDE* дозволяє комплексно оцінити загрози інформаційній безпеці системи інформаційного обміну між автономним морським рухомим об’єктом та постом керування. Отримані результати свідчать про необхідність поєднання криптографічного захисту, організаційних заходів та автономних механізмів безпеки для забезпечення надійної та стійкої роботи системи в умовах дії потенційних загроз.

Нижче наведено адаптовану таблицю моделювання загроз (табл. 4.1), узгоджену з підходами ДСТУ (зокрема ДСТУ *ISO/IEC* 27005), *ISO/IEC* 27001 та *NIST* (SP 800-30 / 800-53)[38,39]. Метод *DREAD* використовується для кількісно-якісної оцінки ризиків інформаційної безпеки та доповнює ідентифікацію загроз, виконану, зокрема, за *STRIDE*. Аналіз за *DREAD* дозволяє оцінити кожну загрозу з точки зору потенційної шкоди, складності реалізації та масштабу впливу, що є важливим при визначенні пріоритетів захисту системи.

Згідно з методологією *DREAD*, кожна загроза оцінюється за п’ятьма критеріями: рівень потенційної шкоди (*Damage*), можливість відтворення атаки (*Reproducibility*), складність експлуатації вразливості (*Exploitability*), кількість уражених компонентів або користувачів (*Affected Users*) та можливість виявлення атаки (*Discoverability*) (табл. 4.2). Таблиці оцінки представлено в додатку А.

Найбільш критичною загрозою для досліджуваної системи є несанкціоноване управління автономним морським об’єктом шляхом підміни або компрометації поста керування.

Таблиця 4.1 – Оцінка загроз системі інформаційного обміну методом STRIDE

STRIDE	Актив	Опис загрози	Вразливість	Можливі наслідки (вплив)	Заходи контролю (*ISO* 27001 / *NIST*)
S Spoofing	Канал зв'язку, ПК, АНПА	Підміна поста керування або автономного об'єкта	Відсутність взаємної автентифікації	Несанкціоноване управління, втрата контролю	*IA*-3, *IA*-7 (*NIST*); A.5.17, A.8.5 (*ISO* 27001); криптографічна автентифікація
T Tampering	Команди управління, телеметрія	Модифікація даних під час передавання	Незахищений або слабко захищений канал	Аварійні ситуації, порушення місії	*SC*-12, *SC*-16 (*NIST*); A.8.24, A.8.25; контроль цілісності
R Repudiation	Журнали подій, команди	Заперечення факту відправки команд	Відсутність невідмовних журналів	Неможливість розслідування інцидентів	*AU*-10, *AU*-12 (*NIST*); A.8.15; журнали з підписами і часовими мітками
I Information Disclosure	Телеметрія, координати	Перехоплення конфіденційної інформації	Відсутність шифрування	Компрометація місії, витік даних	*SC*-13, *SC*-28 (*NIST*); A.8.23; *end-to-end* шифрування
D Denial of Service	Канал зв'язку, сервер ПК	Глушіння або перевантаження каналу	Відсутність резервування	Втрата зв'язку, зрив місії	*CP*-10, *SC*-5 (*NIST*); A.5.30; резервні канали, автономні режими
E Elevation of Privilege	ОС АНПА, ПК	Отримання розширених прав доступу	Вразливості ПЗ, надмірні привілеї	Повна компрометація системи	*AC*-6, *CM*-7 (*NIST*); A.8.2, A.8.9; принцип найменших привілеїв

Таблиця 4.2 – Оцінка методом *DREAD*

№	Загроза	*D Damage*	*R (Reproducibility)*	*E (Exploitability)*	*A (Affected Users)*	*D (Discoverability)*	Середній ризик	Рівень ризику
1.	Несанкціоноване управління АНПА (підміна ПК)	10	8	7	9	7	8,2	Високий
2.	Модифікація команд управління	9	8	7	8	6	7,6	Високий
3.	Перехоплення конфіденційної інформації	8	7	6	8	6	7,0	Високий
4.	Відмова в обслуговуванні каналу зв’язку	8	9	8	8	5	7,6	Високий
5.	Підвищення привілеїв	10	6	5	9	6	7,2	Високий
6.	Компрометація журналів подій	6	7	6	6	5	6,0	Середній

Потенційна шкода від такої атаки оцінюється як дуже висока, оскільки зловмисник може повністю змінити поведінку об’єкта, спричинити аварійну ситуацію, втрату апарата або нанесення шкоди навколишньому середовищу. Відтворюваність атаки за наявності доступу до каналу зв’язку або викрадених облікових даних також є високою, а складність експлуатації — середньою або низькою за умови недостатнього рівня автентифікації. Уражається вся система в цілому, а виявлення атаки може бути ускладнене, якщо команди виглядають

легітимними. Сукупна оцінка за *DREAD* для цієї загрози є високою, що визначає її як пріоритетну.

Другою суттєвою загрозою є модифікація команд управління або телеметричних даних у каналі зв'язку. Потенційна шкода від такої атаки також є значною, оскільки викривлення даних може призвести до помилкових рішень оператора або до неправильних дій автономного об'єкта. Атака може бути відносно легко відтворена в умовах відсутності криптографічного захисту цілісності, а її виявлення є складним, оскільки змінені дані можуть не викликати негайних підозр. Кількість уражених компонентів включає як автономний об'єкт, так і пост керування, що зумовлює високий загальний ризик за *DREAD*.

Загроза розкриття конфіденційної інформації, зокрема координат, маршрутів руху або сенсорних даних, має дещо нижчий рівень безпосередньої шкоди порівняно з атаками на управління, однак у контексті спеціальних або військових застосувань вона може мати стратегічні наслідки. Перехоплення інформації є відносно легко здійсненним у бездротових каналах, а виявлення такої атаки зазвичай є складним, оскільки вона не впливає на працездатність системи. Ураженими є всі користувачі та компоненти, що отримують або обробляють дані. Сукупна оцінка за *DREAD* для цієї загрози визначається як середньо-висока.

Атаки типу відмови в обслуговуванні спрямовані на порушення доступності каналу зв'язку або обчислювальних ресурсів поста керування. Потенційна шкода в цьому випадку залежить від тривалості атаки та рівня автономності АНПА. За відсутності резервних каналів або автономних сценаріїв поведінки шкода може бути значною, включаючи зрив місії або втрату об'єкта. Такі атаки часто легко відтворюються та не потребують високої кваліфікації, однак їх виявлення, як правило, не є складним. Загальна оцінка ризику за *DREAD* для цієї категорії загроз є середньою або високою залежно від архітектури системи.

Менш очевидною, але небезпечною загрозою є підвищення привілеїв у програмному забезпеченні автономного об’єкта або поста керування. У разі успішної експлуатації вразливості зловмисник може отримати повний контроль над системою. Потенційна шкода від такої атаки є максимальною, однак її відтворюваність і складність реалізації зазвичай нижчі, ніж у атак на канал зв’язку, оскільки вони потребують глибокого знання системи або наявності внутрішнього доступу. Виявлення таких атак є складним, що підвищує загальний ризик.

Таким чином, аналіз за методом *DREAD* показує, що найвищі ризики для системи інформаційного обміну між автономним морським рухомим об’єктом та постом керування пов’язані з атаками на автентичність і цілісність управління, а також з можливістю несанкціонованого доступу до критичних функцій системи. Отримані результати дозволяють обґрунтовано визначити пріоритети впровадження заходів захисту, зосередивши увагу на криптографічному захисті каналів зв’язку, надійній автентифікації, контролі доступу та забезпеченні автономної безпечної поведінки об’єкта у разі виникнення інцидентів інформаційної безпеки.

4.2 Засоби зниження загрози

Захист інформаційного каналу між автономним морським рухомим об’єктом та постом керування є ключовим елементом забезпечення інформаційної безпеки всієї системи управління. З огляду на використання бездротових, супутникових або акустичних каналів зв’язку, такий канал є вразливим до широкого спектра загроз, включаючи перехоплення, модифікацію даних, підміну вузлів зв’язку та атаки на доступність. Тому система захисту інформаційного каналу повинна бути комплексною та поєднувати криптографічні, організаційні та технічні засоби (табл. 4.3).

Таблиця 4.3 – Засоби захисту інформаційного каналу

№	Засіб захисту інформаційного каналу	Призначення та опис	Відповідність ДСТУ / *ISO/IEC*	Відповідність *NIST SP* 800-53
1	Криптографічне шифрування каналу зв’язку	Забезпечення конфіденційності та цілісності команд управління і телеметрії при передаванні відкритими каналами	ДСТУ *ISO/IEC* 27001: А.8.23, А.8.24 ДСТУ *ISO/IEC* 27005: обробка ризиків конфіденційності	*SC*-12, *SC*-13, *SC*-16, *SC*-28
2	Взаємна автентифікація АНПА та ПК	Запобігання підміні поста керування або автономного об’єкта	ДСТУ *ISO/IEC* 27001: А.5.17, А.8.5	*IA*-3, *IA*-7, *IA*-8
3	Управління криптографічними ключами	Захищене створення, зберігання та ротація ключів шифрування	ДСТУ *ISO/IEC* 27001: А.8.28, А.8.29	*KM*-1, *KM*-2, *KM*-4
4	Контроль цілісності повідомлень (*HMAC*, цифрові підписи)	Захист від модифікації команд управління і телеметрії	ДСТУ *ISO/IEC* 27001: А.8.25, А.8.26	*SI*-7, *SC*-16

Продовження таблиці 4.3

5	Захищене завантаження та оновлення ПЗ (*Secure Boot, Signed Updates*)	Запобігання впровадженню шкідливого ПЗ через канал зв’язку	ДСТУ *ISO/IEC* 27001: А.8.9, А.8.32	*CM*-5, *CM*-7, *SI*-7
6	Резервування та диверсифікація каналів зв’язку	Підвищення доступності у разі глушіння або *DoS*-атак	ДСТУ *ISO/IEC* 27001: А.5.30, А.8.14	*CP*-8, *CP*-10, *SC*-5
7	Автономні безпечні режими роботи АНПА	Забезпечення безпечної поведінки при втраті зв’язку	ДСТУ *ISO/IEC* 27005: зниження впливу ризиків доступності	*CP*-2, *IR*-4
8	Моніторинг та виявлення атак у каналі	Виявлення аномалій, глушіння, спроб вторгнення	ДСТУ *ISO/IEC* 27001: А.8.16, А.8.15	*SI*-4, *AU*-6
9	Журналювання подій обміну даними	Забезпечення невідмовності та можливості розслідування інцидентів	ДСТУ *ISO/IEC* 27001: А.8.15, А.8.17	*AU*-2, *AU*-10, *AU*-12
10	Мінімізація та сегментація переданих даних	Зменшення обсягу шкоди при компрометації каналу	ДСТУ *ISO/IEC* 27001: А.8.2, А.5.15	*AC*-6, *SC*-7

Основним засобом забезпечення конфіденційності та цілісності переданої інформації є використання криптографічного захисту даних. Передавання команд управління, телеметрії та сенсорної інформації має здійснюватися через захищені канали зв’язку з використанням сучасних криптографічних алгоритмів симетричного та асиметричного шифрування. Криптографічні протоколи повинні забезпечувати не лише шифрування даних, але й перевірку їх цілісності та автентичності сторін, що взаємодіють. Це дозволяє запобігти атакам типу підміни поста керування або автономного об’єкта, а також модифікації переданих команд.

Важливою складовою захисту інформаційного каналу є взаємна автентифікація автономного морського об’єкта та поста керування. Для цього доцільно використовувати інфраструктуру відкритих ключів або апаратні криптомодулі, що зберігають криптографічні ключі в захищеному середовищі. Такий підхід дозволяє гарантувати, що передавання інформації здійснюється виключно між довіреними суб’єктами, а спроби підключення сторонніх пристроїв будуть виявлені та заблоковані.

З метою забезпечення цілісності команд управління та телеметричних даних необхідно застосовувати механізми цифрового підпису або коди автентифікації повідомлень. Це дозволяє автономному об’єкту перевіряти справжність отриманих команд та відхиляти будь-які змінені або підроблені повідомлення. Аналогічні механізми мають застосовуватися і на посту керування для перевірки достовірності телеметрії, що надходить від АНПА.

Для підвищення стійкості інформаційного каналу до атак типу відмови в обслуговуванні доцільно передбачити резервування каналів зв’язку та використання адаптивних механізмів перемикання між ними. У разі втрати або деградації основного каналу система повинна автоматично переходити на альтернативний спосіб зв’язку або активувати автономний режим роботи АМРО з безпечними сценаріями поведінки. Це дозволяє зменшити залежність від постійного зв’язку з постом керування та підвищити загальну живучість системи.

Окрему увагу слід приділити моніторингу та виявленню інцидентів інформаційної безпеки в інформаційному каналі. Засоби моніторингу повинні забезпечувати виявлення аномальної активності, спроб несанкціонованого доступу, різкого збільшення трафіку або характерних ознак глушіння сигналу. Реєстрація подій безпеки та ведення захищених журналів дозволяють своєчасно реагувати на атаки та здійснювати подальший аналіз інцидентів.

Додатковим засобом захисту інформаційного каналу є сегментація та мінімізація переданих даних. Передавання лише необхідної для виконання місії інформації, а також розмежування доступу до різних типів даних знижує потенційний обсяг шкоди у разі компрометації каналу. Це відповідає принципам мінімальних привілеїв та необхідної достатності, рекомендованим міжнародними стандартами інформаційної безпеки.

Таким чином, захист інформаційного каналу між автономним морським рухомим об’єктом та постом керування має базуватися на комплексному підході, що включає криптографічний захист, автентифікацію, контроль цілісності, резервування каналів зв’язку та постійний моніторинг. Реалізація зазначених засобів дозволяє суттєво знизити рівень ризиків, виявлених у ході *STRIDE*- та *DREAD*-аналізу, і забезпечити стійке та безпечне функціонування системи в умовах дії сучасних загроз.

4.3 Оцінювання надлишкової загрози

Проведене повторне моделювання загроз методом *DREAD* після впровадження технічних і криптографічних засобів захисту дозволило оцінити залишковий рівень ризиків інформаційної безпеки системи інформаційного обміну між автономним морським рухомим об’єктом та постом керування. Метою повторного аналізу було визначення ефективності обраних заходів захисту та встановлення того, наскільки знижено ймовірність успішної реалізації ідентифікованих раніше загроз (табл. 4.3).

Результати аналізу показали, що впровадження захищених каналів зв’язку, взаємної автентифікації, механізмів контролю цілісності повідомлень, резервування каналів та постійного моніторингу призвело до суттєвого зменшення показників відтворюваності та експлуатованості атак. Зокрема, для більшості загроз значення параметрів *Reproducibility* та *Exploitability* знизилися з високих до низьких або помірних, що свідчить про значне ускладнення реалізації атак навіть за наявності мотивації та технічних ресурсів у потенційного порушника.

Таблиця 4.3 – Повторне оцінювання загроз

№	Загроза	*D Damage*	*R (Reproducibility)*	*E (Exploitability)*	*A (Affected Users)*	*D (Discoverability)*	Середній ризик	Рівень ризику
1.	Несанкціоноване управління АНПА (підміна ПК)	10	3	3	8	3	5,4	Середній
2.	Модифікація команд управління	9	3	3	7	3	5,0	Середній
3.	Викривлення телеметрії та сенсорних даних	8	3	3	7	3	4,8	Середній
4.	Перехоплення конфіденційної інформації	7	3	3	6	4	4,6	Середній
5.	Відмова в обслуговуванні каналу зв’язку	8	6	6	7	4	6,2	Середній
6.	Підвищення привілеїв у ПЗ АНПА або ПК	10	4	4	8	3	5,8	Середній
7.	Компрометація журналів подій	6	3	3	5	3	4,0	Низький

Загроза несанкціонованого управління автономним морським об’єктом, яка в первинному аналізі мала критичний рівень ризику, після впровадження взаємної автентифікації та криптографічного захисту каналу була знижена до середнього рівня. Хоча потенційна шкода від такої атаки залишається максимальною через фізичну природу об’єкта, ймовірність її успішної реалізації суттєво зменшилась, а виявлення спроб втручання стало значно простішим завдяки журналюванню та моніторингу.

Аналогічна тенденція спостерігається для загроз модифікації команд управління та викривлення телеметричних даних. Використання цифрових підписів і механізмів контролю цілісності призвело до зменшення ризику успішної підміни або зміни інформації, що передається. У результаті ці загрози перейшли з категорії високих у категорію середніх залишкових ризиків, які можуть бути прийняті або контрольовані в межах системи управління інформаційною безпекою.

Загрози, пов’язані з розкриттям конфіденційної інформації, зокрема координат та сенсорних даних, також зазнали суттєвого зниження ризику. Повне шифрування переданих даних унеможливлює їх використання у разі перехоплення, що зменшує практичну цінність такої атаки для зловмисника. Водночас прихований характер перехоплення зумовлює збереження помірного рівня ризику, оскільки виявлення таких атак залишається технічно складним.

Найбільш стійкою до зниження виявилася загроза відмови в обслуговуванні каналу зв’язку. Незважаючи на застосування резервних каналів і автономних сценаріїв поведінки автономного об’єкта, фізичні обмеження середовища передавання інформації, зокрема можливість глушіння сигналу, не дозволяють повністю усунути цю загрозу. У результаті вона зберігає рівень середнього або середньо-високого залишкового ризику і потребує постійного контролю та організаційних заходів реагування.

Загрози підвищення привілеїв у програмному забезпеченні автономного об’єкта або поста керування після впровадження принципу найменших привілеїв, ізоляції компонентів та захищеного завантаження також були

знижені до середнього рівня. Хоча потенційна шкода від таких атак залишається високою, складність їх реалізації та імовірність успіху істотно зменшилися.

У цілому повторне моделювання методом *DREAD* засвідчило, що впроваджені засоби захисту є ефективними та забезпечують досягнення прийнятного рівня залишкових ризиків відповідно до вимог ДСТУ *ISO/IEC* 27005 та рекомендацій *NIST*. Високих ризиків, які вимагали б негайного додаткового технічного втручання, не виявлено. Отримані результати підтверджують доцільність обраної архітектури захисту інформаційного каналу та можуть бути використані як обґрунтування ефективності системи інформаційної безпеки в цілому.

Висновку до розділу

У розділі було виконано кількісне моделювання загроз з використанням методик *STRIDE* та *DREAD*, що дозволило об’єктивно оцінити небезпеку основних типів атак на систему інформаційного обміну. Розраховано інтегральні рівні ризику для трьох критичних загроз – перехоплення даних, підміни вузла та несанкціонованого доступу до сервера. До впровадження заходів захисту їх середнє значення становило понад 8 балів, що відносить їх до категорії високого ризику.

Після реалізації запропонованих засобів (шифрування каналу, взаємної автентифікації, контролю доступу, забезпечення цілісності даних та моніторингу конфігурацій) інтегральний ризик зменшився до показників 5,4–5,6, що відповідає середньому рівню.

ВИСНОВКИ

Актуальність теми обумовлена зростанням ролі автономних ненаселених підводних апаратів з радіобуєм що використовує бездротові канали зв’язку, що підвищує рівень потенційних кіберзагроз.

У процесі виконання роботи було проаналізовано архітектуру системи інформаційного обміну, визначено основні інформаційні потоки та виявлено найбільш уразливі елементи системи. Проведений аналіз показав, що ключовими джерелами ризиків є відкритий радіоканал зв’язку, фізична доступність радіобуя та відсутність механізмів автентифікації та контролю цілісності переданих даних.

Для кількісної оцінки ризиків інформаційної безпеки застосовано методи *STRIDE* та *DREAD*. Метод *DREAD* дозволив визначити найбільш критичні загрози та пріоритизувати їх за рівнем ризику. Отримані результати підтвердили наявність підвищеного рівня ризику на етапі базової конфігурації системи.

У роботі запропоновано комплекс заходів захисту, що включає криптографічний захист каналу зв’язку, механізми взаємної автентифікації компонентів системи, контроль цілісності інформації та базові засоби підвищення доступності.

Таким чином, мету кваліфікаційної роботи досягнуто, а поставлені завдання виконано в повному обсязі. Отримані результати можуть бути використані на практиці під час проєктування та модернізації систем інформаційного обміну автономних ненаселених підводних апаратів з радіобуєм.

ПЕРЕЛІК ПОСИЛАНЬ

1. *Blintsov Volodymyr, Maidaniuk Pavlo, Sirivchuk Andrii Improvement of Technical Supply of Projects of Robotized Monitoring of Underwater Conditions in Shallow Water Areas. «EUREKA: Physics and Engineering»,* 2019. *Number* 3. P. 41-49. DOI: 10.21303 / 2461-4262.2019.00893

2. Блінцов В.С., Сірівчук А.С., Надточий А.В., Надточій В.А. Автоматизація керування автономним ненаселеним підводним апаратом з радіобуєм: монографія, Миколаїв: Іліон, 2022. 196 с.

3. Drones: Security, Vulnerability, Exploitation, Awareness, and Mitigation. URL: https://www.linkedin.com/pulse/drones-security-vulnerability-exploitation-awareness-dror-amrami

4. *Potential vulnerabilities of drone networks to cyberattacks and how they can be mitigated URL: https://www.linkedin.com/pulse/drones-security-vulnerability-exploitation-awareness-dror-amrami*

5. *P. Liu, A. Y. Chen, Y.-N. Huang, J.-Y. Han, J.-S. Lai, S.-C. Kang, T.-H. Wu, M.-C. Wen, M.-H. Tsai, et al. A review of rotorcraft unmanned aerial vehicle (uav) developments and applications in civil engineering. Smart Structures and Systems,* 13(6):1065–1094, 2014.

6. *Stallings W. Cryptography and Network Security: Principles and Practice. – 7th ed. – Pearson Education*, 2017.

7. Potential vulnerabilities of drone networks to cyberattacks and how they can be mitigated URL: https://www.linkedin.com/pulse/drones-security-vulnerability-exploitation-awareness-dror-amrami

8. *K. Hartmann and C. Steup. The vulnerability of UAVs to cyber attacks-an approach to the risk assessment. In Proc. of the 5th IEEE International Conference Cyber Conflict (CyCon'13), Tallinn, Estonia, pages 1–23. IEEE, June* 2013.

9. Shafique Arslan, Mehmood Abid, Elhadef Mourad, Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles. 2021 Access. PP. 1-1. 10.1109/ACCESS.2021.3066778.

10.R. N. Akram, K. Markantonakis, K. Mayes, O. Habachi, D. Sauveron, A. Steyven, and S. Chaumette. Security, privacy and safety evaluation of dynamic and static fleets of drones. In Proc. of the 36th IEEE Digital Avionics Systems Conference (DASC'17), St. Petersburg, FL, USA, pages 1–12. IEEE, September 2017.

11.A. Y. Javaid, W. Sun, V. K. Devabhaktuni, and M. Alam. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In Proc. of the IEEE Conference on Technologies for Homeland Security (HST'12),Waltham, MA, USA, November.

12.K. Mansfield, T. Eveleigh, T. H. Holzer, and S. Sarkani. Unmanned aerial vehicle smart device ground control station cyber security threat model. In Proc. of the IEEE Conference on Technologies for Homeland Security (HST'12),Waltham, MA, USA, November.

13.K. *Hartmann and C. Steup. The vulnerability of uavs to cyber attacks-an approach to the risk assessment.In Proc. of the 5th IEEE International Conference Cyber Conflict (CyCon'13), Tallinn, Estonia, pages 1–23. IEEE, June* 2013.

14.*S. M. Giray. Anatomy of unmanned aerial vehicle hijacking with signal spoofing. In Proc. of the 6th International Conference on Recent Advances in Space Technologies (RAST'13), Istanbul, Turkey, pages795–800. IEEE, June* 2013.

15.*M. S. Haque and M. U. Chowdhury. A new cyber security framework towards secure data communication for unmanned aerial vehicle. In Proc. of the International Conference on Security and Privacy in Communication Networks (SecureComm'17), ATCS and SePrIoT, Niagara Falls, Canada, pages* 113–122. *Springer, October* 2018.

16.*L. Kanellos. Safety, privacy and net neutrality aspects of civilian drones. In C. Springer, editor, Net Neutrality Compendium*

17.*Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – 2nd ed. John Wiley & Sons*, 2015.

18. *D. Rudinskas, Z. Goraj, and J. Stank¯unas. Security analysis of UAV radio communication system. Aviation*, 13(4):116–121, 2009.

19.*N. M. Rodday, R. d. O. Schmidt, and A. Pras. Exploring security vulnerabilities of unmanned aerial vehicles. In Proc. of the IEEE International Network Operations and Management Symposium (NOMS'16), 2016 IEEE/IFIP, pages* 993–994. IEEE, 2016.

20.*A. Orsino, A. Ometov, G. Fodor, D. Moltchanov, L. Militano, S. Andreev, O. N. Yilmaz, T. Tirronen,J. Torsner, G. Araniti, et al. Effects of heterogeneous mobility on d2d-and drone-assisted mission-critical mtc in 5g. IEEE Communications Magazine,* 55(2):79–87, 2017.

21.*K. E. Oleson, P. Hancock, D. R. Billings, and C. D. Schesser. Trust in unmanned aerial systems: A synthetic, distributed trust model.* 2011.

22.*T. Peng, C. Leckie, and K. Ramamohanarao. Survey of network-based defense mechanisms countering the dos and ddos problems. ACM Computing Surveys (CSUR),* 39(1):3, 2007.

23.STRIDE model / Threat model. Вікіпедія. URL: https://en.wikipedia.org/wiki/STRIDE_model (дата звернення: 10.12.2025).

24.DREAD (risk assessment model). Вікіпедія. URL: https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model) (дата звернення: 10.12.2025).

25.Kadhirvelan S. Threat Modelling and Risk Assessment. Chalmers University of Technology. URL: https://publications.lib.chalmers.se/records/fulltext/202917/202917.pdf (дата звернення: 10.12.2025).

26.Threat Modelling. FIRST.org. URL: https://www.first.org/global/sigs/cti/curriculum/ threat-modelling (дата звернення: 19.12.2025).

27.Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80 (дата звернення: 01.12.2025)

28.Закон України «Про основні засади забезпечення кібербезпеки України» від від 05.10.2017 № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text(дата звернення: 01.12.2025)

29.НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 (Зміна № 1 наказ Адміністрації Держспецзв’язку від 28.12.2012 № 806)

30.НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 28.12.2012 № 806)

31.НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблювальної інформації від несанкціонованого доступу, наказ ДСТСЗІ СБУ від 28.04.99 № 22 (Зміна № 1 наказ від 15.10.2008 № 172)

32.НД ТЗІ 2.6-004-21. Порядок авторизації безпеки інформаційних систем. Київ: Адміністрація Держспецзв’язку, 2021.

33.НД ТЗІ 3.6-008-21. Порядок моніторингу безпеки інформаційних систем. Київ: Адміністрація Держспецзв’язку, 2021.

34.НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу: наказ ДСТСЗІ СБ України від 20.12.2000 № 60; Зміна № 1: наказ Адміністрації Держспецзв’язку від 28.12.2012 № 806. Київ, 2000.

35.Інформаційні технології. Техніки безпеки. Системи управління інформаційною безпекою. Вимоги : ДСТУ ISO/IEC 27001:2023. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104398 (дата звернення: 10.11.2025).

36.Інформаційна безпека, кібербезпека та захист конфіденційності. ДСТУ ISO/IEC 27005:2023 URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104400(дата звернення: 10.11.2025).

37.*ENISA. Risk Management – Implementation principles and inventories for risk management/risk assessment methods and tools. — European Union Agency for Cybersecurity,* 2016.

38.*NIST Special Publication* 800-30. *Guide for Conducting Risk Assessments. — National Institute of Standards and Technology, Gaithersburg, MD, USA*, 2012.

39.*NIST Special Publication* 800-53. *Managing Information Security Risk: Organization, Mission, and Information System View*. *– NIST*, 2011.

ДОДАТОК А

Для використання методу *DREAD* використовуються категорії оцінювання по кожному з його параметрів. Параметр *Damage* вказує на скільки серйозні збитки може задати атака або вразливість (табл. А.1).

Таблиця А.1 – Категорії оцінювання параметра *Damage*

Бал	Опис рівня збитків	Характер впливу на систему
1-2	Незначні збитки	Мінімальний вплив на роботу системи, незначні тимчасові відхилення.
3-4	Низькі збитки	Порушення не впливають на основні функції; можливе локальне відновлення без втрат.
5-6	Середні збитки	Спостерігається часткове порушення роботи окремих компонентів, можливі втрати даних або затримки у виконанні місії.
7-8	Високі збитки	Значне порушення роботи системи, втрата частини функцій, імовірність зриву місії або пошкодження обладнання.
9-10	Критичні збитки	Повна втрата управління, знищення або захоплення АНПА, критичні порушення роботи поста керування або сервера, необоротні наслідки.

Reproducibility – характеризує, наскільки легко повторити атаку (табл. А.2).

Таблиця А.2 – Категорії оцінювання параметра *Reproducibility*

Бал	Опис рівня відтворюваності	Характер впливу
1–2	Атака майже не відтворюється	Потрібні унікальні умови, повторення практично неможливе.
3–4	Низька ймовірність повторення	Необхідні точні параметри середовища або глибокі знання системи.
5–6	Середня відтворюваність	Атака можлива, але вимагає підготовки або специфічного обладнання.
7–8	Висока відтворюваність	Може бути повторена при наявності доступу до каналу або обладнання.
9–10	Дуже легко відтворюється	Атака повторюється практично необмежену кількість разів, з мінімальними ресурсами.

Exploitability – характеризує, наскільки легко реалізувати атаку технічно (табл. А.3).

Таблиця А.3 – Категорії оцінювання параметра *Exploitability*

Бал	Опис складності	Характер впливу
1–2	Дуже складна експлуатація	Потрібні унікальні знання, закриті інструменти, складна підготовка.
3–4	Складна експлуатація	Потрібні значні ресурси, високий рівень технічної кваліфікації.
5–6	Середня складність	Можлива при використанні спеціалізованого обладнання або аналізу коду.
7–8	Порівняно проста	Виконується зі стандартними інструментами або відкритими вразливостями.
9–10	Дуже проста експлуатація	Реалізується без глибоких знань, доступна широкому колу нападників.

Affected Users – характеризує масштаби впливу загрози на систему і користувачів (табл. А.4).

Таблиця А.4 – Категорії оцінювання параметра *Affected Users*

Бал	Масштаб ураження	Характер впливу
1–2	Вражає один компонент	Проблема локальна, без поширення на інші елементи системи.
3–4	Вражає кілька другорядних компонентів	Порушення обмежені, не впливають на основну функціональність.
5–6	Вражає окремі функціональні підсистеми	Можливе часткове порушення роботи місії.
7–8	Вражає більшість користувачів / модулів	Загроза впливає на ключові частини системи управління.
9–10	Вражає всю систему	Повний вивід з ладу, критичні наслідки для всієї інфраструктури.

Discoverability – характеризує можливість виявлення вразливості або атаки (табл. А.5)

Таблиця А.5 – Категорії оцінювання параметра *Discoverability*

Бал	Опис виявлення	Характер впливу
1–2	Атака майже невиявна	Не залишає слідів, практично неможливо зафіксувати.
3–4	Важковиявна	Потребує глибокого аналізу журналів або спеціальних інструментів.
5–6	Середня ймовірність виявлення	Атака помітна після появи відхилень у роботі системи.

Продовження таблиці А.5

7–8	Виявляється відносно легко	Можна зафіксувати інструментами моніторингу або IDS.
9–10	Виявляється одразу	Спроба атаки відразу генерує події або очевидні зміни.