

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ МОРСЬКИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут інформаційних технологій та інноваційного
підприємництва

Кафедра кібербезпеки та захисту інформації

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни

«КІБЕРФІЗИЧНІ СИСТЕМИ, ЇХ АРХІТЕКТУРА І ЗАХИСТ»

для здобувачів
другого (магістерського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Методичні вказівки до виконання лабораторних робіт з дисципліни «Кіберфізичні системи, їх архітектура та захист» для здобувачів другого (магістерського) рівня вищої освіти спеціальності F5 Кібербезпека та захист інформації / Укл.: А.А.Кобозєва. – Одеса: ОНМУ, 2026. - 25 с.

Укладач: д.т.н., проф. Кобозєва А.А.

Методичні вказівки схвалено на засіданні кафедри «Кібербезпека та захист інформації»

(Протокол від «29» квітня 2026 р. № 7)

Методичні вказівки схвалено на засіданні НМК ННІ ІТІП

(Протокол від «29» квітня 2026 р. № 7)

ЗМІСТ

ВСТУП	4
ЛАБОРАТОРНА РОБОТА 1. Дослідження хронометричної стійкості та часового бюджету стеганографічної системи в імітованому контурі кіберфізичної системи (на прикладі сценарію MASS)	5
ЛАБОРАТОРНА РОБОТА 2. Дослідження стійкості до контекстного аналізу та оцінка антагонізму між хронометричною стійкістю і стійкістю до контекстного аналізу стеганосистеми в імітованому контурі кіберфізичної системи (на прикладі сценарію MASS)	12
ЛІТЕРАТУРА	25

ВСТУП

Дисципліна «Кіберфізичні системи, їх архітектура та захист» відповідає освітньо-професійній програмі «Кібербезпека та захист інформації», навчальному плану підготовки здобувачів другого (магістерського) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації, і є складовою циклу дисциплін професійної підготовки обов'язкової частини навчального плану.

Навчальна дисципліна «Кіберфізичні системи, їх архітектура і захист» орієнтований на формування у здобувачів системного розуміння принципів побудови, архітектурних особливостей та забезпечення безпеки сучасних кіберфізичних систем (КФС) в умовах жорстких ресурсних, зокрема часових, обмежень. В межах дисципліни розглядаються КФС двох категорій: мобільні та стаціонарні, особливості в забезпеченні їх безпеки. Окрему увагу приділено адаптації сучасних систем захисту, методам стеганографії в каналах управління, вимогам хронометричної стійкості, стійкості до контекстного аналізу та специфіці безпеки для автономних систем (на прикладі сценаріїв морських автономних об'єктів). Курс має практичну спрямованість: студенти виконують комп'ютерне моделювання в імітованому контурі КФС, досліджують часові бюджети, вплив мережевого джиттера та компроміси між показниками захисту.

Метою дисципліни є розвиток у здобувачів здатності: розуміти архітектуру, принципи побудови та функціонування сучасних КФС; аналізувати вразливості та вектори кібератак на критичну інфраструктуру й автономні системи (на прикладі сценаріїв MASS); застосовувати методи захисту й стеганографії в контурах управління КФС з урахуванням жорстких часових обмежень реального часу.

Мета лабораторних занять полягає у практичному формуванні та розвитку відповідних професійних компетентностей майбутніх фахівців, які слугуватимуть підґрунтям для їхньої практичної роботи, що пов'язана із забезпеченням захисту інформації та організацією інформаційної та кібербезпеки.

Лабораторна робота 1

Дослідження хронометричної стійкості та часового бюджету стеганографічної системи в імітованому контурі кіберфізичної системи (на прикладі сценарію MASS)

Сучасні кіберфізичні системи (КФС) критичної інфраструктури, зокрема морські автономні надводні системи (MASS - *Maritime Autonomous Surface Ships*), характеризуються високим ступенем інтеграції цифрових обчислювальних модулів та фізичних виконавчих механізмів. Надійність функціонування таких систем безпосередньо залежить від детермінованості, своєчасності й захищеності інформаційних потоків у реальному часі.

Впровадження додаткових механізмів інформаційної безпеки, зокрема стеганографічних систем для прихованого передавання службових даних, управляючих команд усередині легальних телеметричних чи медійних потоків, неминуче впливає на часові характеристики мережі. Будь-які додаткові накладні витрати на модифікацію контейнерів або обробку пакетів можуть порушити суворий часовий бюджет контуру керування.

У реальних умовах експлуатації каналом зв'язку КФС притаманні випадкові коливання затримки та джиттер, викликані мережевими перевантаженнями або зовнішніми перешкодами. Тому оцінка хронометричної стійкості - здатності стеганографічної системи зберігати працездатність і не створювати критичних затримок під час вбудовування додаткової інформації різного обсягу - є ключовим завданням для проєктування безпечних і надійних автономних КФС.

1. Мета роботи

Експериментально дослідити шляхом імітаційного моделювання (у віртуалізованому середовищі КФС) вплив обчислювальної складності стеганографічних перетворень та обсягу вбудовуваної додаткової інформації на дотримання вимог реального часу при передаванні керуючих або сенсорних потоків даних в умовах коливання затримок у каналах зв'язку.

Робота забезпечує досягнення наступних результатів навчання:

РНЗ. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

2. Теоретичні відомості

2.1. Архітектура та базові принципи кіберфізичних систем

Кіберфізичні системи - це інтегровані комплекси, у яких обчислювальні компоненти тісно взаємодіють із фізичними процесами - сенсорами, виконавчими механізмами, приводами.

Типова архітектура КФС включає три рівні:

- *Фізичний рівень:* датчики (сенсори), які вимірюють параметри навколишнього середовища чи стану обладнання (температура, тиск, швидкість, положення), та виконавчі механізми (актуатори), які виконують керуючі команди;
- *Мережевий рівень:* середовище передавання даних (промислові мережі, бездротові сенсорні мережі, шини даних), через яке сенсори передають інформацію до контролерів, а контролери - команди до виконавчих пристроїв;
- *Обчислення:* програмовані логічні контролери (ПЛК), мікрокомп'ютери або сервери, що обробляють вхідні потоки даних, приймають рішення за алгоритмами керування та формують керуючі впливи.

Ключова особливість КФС полягає в тому, що кібернетичні рішення безпосередньо впливають на фізичний світ, тому будь-які збої або затримки тут мають не просто «інформаційний», а часто катастрофічний фізичний характер.

2.2. Вимоги реального часу в КФС та параметри каналів зв'язку

Управління фізичними процесами вимагає суворого дотримання часових обмежень .

- *Жорсткий реальний час:* пропуск дедлайну (часового ліміту на доставку та обробку команди) призводить до аварії, виходу обладнання з ладу або техногенної катастрофи (наприклад, системи аварійного гальмування, стабілізації суден або БПЛА).
- *М'який реальний час:* пропуск дедлайну знижує якість керування чи ефективність системи, але не призводить до критичних наслідків одразу.

На надійність і своєчасність доставки даних у мережах КФС впливають такі параметри:

- *Затримка:* час, необхідний для передавання пакета даних від джерела до отримувача;
- *Джиттер (Jitter):* коливання (нестабільність) часу затримки прибуття пакетів. У реальних мережах зв'язок ніколи не буває ідеальним: навантаження на мережу, перешкоди чи черги пакетів викликають випадковий розкид затримок.

2.3. Стеганографічні перетворення та приховані канали в КФС

У контексті КФС стеганографічні підходи можуть розглядатися з двох протилежних точок зору:

1. *Як загроза*, коли зловмисник може використовувати приховані канали в телеметричному трафіку або потоках сенсорних даних для несанкціонованої крадіжки інформації або передавання команд керування в обхід систем виявлення вторгнень;
2. *Як метод захисту*: використання мікро-вбудовування маркерів, цифрових водяних знаків або службових метаданих у потоки даних для перевірки цілісності та автентичності керуючих пакетів.

Незалежно від мети, процес стеганографії передбачає модифікацію оригінального цифрового контенту (наприклад, молодших бітів сенсорних вимірювань, значень коефіцієнтів у частотній області тощо) заради розміщення додаткового корисного навантаження.

2.4. Вплив обчислювальної складності на часові обмеження КФС

Головна проблема, яка досліджується в цій роботі, полягає у *конфлікті між безпекою/прихованістю та часовими обмеженнями*:

- *Обчислювальні витрати*: будь-який алгоритм стеганографічного перетворення (вбудовування та вибудовування додаткової інформації) вимагає додаткових циклів процесора. Чим складніший алгоритм, тим більше часу контролер витрачає на його виконання;
- Додавання інформації, що приховується, може збільшити розмір пакетів даних, що передаються мережею, але головним тут є вимога додаткового часу;
- *Накопичувальний ефект у реальному часі*: якщо сумарний час (час обчислень на вбудовування додаткової інформації, час передавання мережею з урахуванням джиттеру) перевищує допустимий інтервал циклу опитування датчиків чи формування керуючого впливу, виникає порушення часового регламенту.

У межах лабораторної роботи №1 необхідно дослідити за допомогою імітаційного моделювання, де саме проходить межа критичного навантаження: при якому обсязі прихованих даних та якій складності алгоритмів система ще дотримується вимог реального часу, а коли починаються небезпечні затримки.

3. Математична та структурна модель імітаційного експерименту

Для проведення дослідження у віртуалізованому середовищі пропонується розглянути спрощену дискретну модель каналу передавання даних та обробки інформації в КФС.

Нехай кожен пакет даних (сенсорне вимірювання або керуюча команда), що генерується джерелом, характеризується такими параметрами:

- S_0 - базовий розмір пакета (у байтах);
- L - обсяг додаткової (приховуваної) інформації, що вбудовується в пакет за допомогою стеганографічного алгоритму;

- T_{gen} - період генерації пакетів (час між сусідніми вимірюваннями датчика, наприклад, 10-50 мс).

Загальний час циклу обробки та доставки пакета T_{total} складається з чотирьох послідовних етапів:

$$T_{total} = T_{emb} + T_{net} + T_{ext} + T_{proc},$$

де T_{emb} - час виконання стегоперетворення (вбудовування додаткової інформації), який залежить від обсягу корисного навантаження L та обчислювальної складності стеганоалгоритма C_{alg} :

$$T_{emb} = f_1(L, C_{alg});$$

T_{net} - час передавання пакета через мережу зв'язку, який визначається розміром пакета $S_0 + L$, пропускною здатністю каналу B та випадковою затримкою (джиттером) Δt , яка імітує нестабільність реального середовища:

$$T_{net} = \frac{S_0 + L}{B} + \Delta t$$

(Зауваження: джиттер Δt зазвичай моделюється за нормальним законом розподілу або за законом Пуассона для імітації випадкових затримок у мережі);

T_{ext} - час витягування прихованої інформації на приймальній стороні:

$$T_{ext} = f_2(L, C_{alg});$$

T_{proc} - час обробки пакету.

Критерій порушення реального часу:

Система вважається такою, що втратила працездатність у режимі реального часу (стану аварійного зриву дедлайну), якщо виконується умова:

$$T_{total} > T_{deadline},$$

де $T_{deadline}$ - максимально допустимий час реакції системи.

4. Порядок виконання роботи

Загальне завдання лабораторної роботи №1: У ході лабораторної роботи студенти варіюють параметри L та C_{alg} , спостерігаючи за статистикою

перевищень $T_{deadline}$ та формуючи графіки залежності ймовірності втрати пакетів/дедлайнів від рівня стеганографічного навантаження (L).

4.1. *Підготовка середовища:* налаштувати потрібного програмного середовища (наприклад, Python), підключити необхідні бібліотеки.

4.2. *Симуляція мережевого джиттера:* згенерувати масив із 100 випадкових значень мережевої затримки, що імітують роботу супутникового каналу зв'язку відповідно до вашого індивідуального варіанта.

4.3. *Моделювання стеганоперетворення:*

- Розробити програмний код деякого стеганографічного алгоритму, що вбудовує додаткову інформацію різного обсягу в контейнер заданого розміру;
- За допомогою функції вимірювання часу зафіксувати обчислювальну затримку алгоритму.

4.4. *Розрахунок та аналіз:*

- Обчислити сумарний час для кожного з 100 пакетів.
- Визначити відсоток «аварійних» спрацювань (коли сумарний час перевищує поріг у 50 мс).
- Побудувати графіки залежності сумарного часу від параметрів експерименту.

4.5. *Аналіз:* проаналізувати отримані графіки, зробити висновки.

5. Варіанти

Оберіть варіант завдання:

Варіант 1:

- Розмір контейнера: 512×512 пікселів;
- Обсяг додаткової інформації: 256 байт;
- Діапазон мережевого джиттера: 25-40 мс.
- Стеганографічний метод модифікації найменшого значущого біта (визначити попередньо обчислювальну складність).

Варіант 2:

- Розмір контейнера: 1024×1024 пікселя.
- Обсяг додаткової інформації: 512 байт.
- Діапазон мережевого джиттера: 30-45 мс.
- Стеганометод Коха і Жао (визначити попередньо обчислювальну складність).

Варіант 3:

- Розмір контейнера: потоковий кадр (роздільна здатність HD).
- Обсяг додаткової інформації: 128 байт.
- Діапазон мережевого джиттера: 20-35 мс.

- Обрати стеганометод самостійно (визначити попередньо обчислювальну складність).

Варіант 4:

- Розмір контейнера: 2048×2048 пікселів.
- Обсяг додаткової інформації: 1024 байти.
- Діапазон мережевого джиттера: 25-45 мс.
- Обрати стеганометод самостійно (визначити попередньо обчислювальну складність).

Варіант 5:

- Розмір контейнера: 640×480 пікселів.
- Обсяг додаткової інформації: 64 байти (компактні команди керування).
- Діапазон мережевого джиттера: 35-50 мс.
- Обрати стеганометод самостійно (визначити попередньо обчислювальну складність).

6. Зміст звіту

Звіт має містити:

1. Назву і мету роботи.
2. Фрагменти розробленого програмного коду моделювання.
3. Графіки залежності сумарного часу від розміру контейнера та обсягу вбудовуваної додаткової інформації.
4. **Аналітичні висновки:** чітко окреслені межі (поєднання розміру контейнера та обсягу даних), при яких алгоритм починає порушувати хронометричну стійкість, із поясненням впливу характеру переданої інформації на стабільність імітованого контуру КФС.

Контрольні запитання до лабораторної роботи № 1

1. Що таке хронометрична стійкість стеганографічної системи і чому аналіз часових характеристик виконання процедур є критичним елементом захисту в контурі MASS?
2. Яку загрозу становлять часові побічні канали для прихованого передавання даних? Як зловмисник може використати різницю в часі обробки чистих і стего-контейнерів?
3. Як зміна обсягу прихованої інформації впливає на час виконання процедур вбудовування та вилучення? Чому ця залежність може стати демаскувальною ознакою?
4. Якими програмними методами та засобами (наприклад, високоточними таймерами) забезпечується вимірювання часових інтервалів виконання окремих етапів стего-алгоритму без внесення системних похибок?

5. Що таке випадкові коливання часу виконання (джиттер) у середовищі функціонування MASS і як вони впливають на виділення стабільних часових ознак стеганографічної системи?
6. Які прийоми (наприклад, вирівнювання часу виконання до константи або додавання штучних псевдовипадкових затримок) використовуються для захисту від часового аналізу? Поясніть.
7. Як обмеження максимального часу циклу керування ускладнюють завдання маскуванню часового сліду стеганографічної системи на борту морського автономного судна?

Лабораторна робота 2

Дослідження стійкості до контекстного аналізу та оцінка антагонізму між хронометричною стійкістю і стійкістю до контекстного аналізу стеганосистеми в імітованому контурі кіберфізичної системи (на прикладі сценарію MASS)

У сучасних кіберфізичних системах, зокрема та морських автономних надводних суднах (MASS) для передавання прихованої інформації все частіше застосовуються новітні типи контейнерів, зокрема цифрові зображення та відеоматеріали, синтезовані за допомогою систем штучного інтелекту. Це відкриває нові можливості для стеганографії, проте породжує принципово новий клас загроз.

Сьогодні ключовим викликом стає забезпечення не лише значної/достатньої пропускної спроможності прихованого каналу зв'язку та незначних збурень контейнера в результаті стеганоперетворення, а й семантичного правдоподібності контейнера/стеганоповідомлення. ШІ-генератори здатні добре сховати секретні дані, наприклад, в цифровому зображенні (ЦЗ), але водночас допускати грубі порушення законів фізики та логіки навколишнього середовища при генерації контейнера, що задовольняє певним вимогам (наприклад, неприродний напрямок тіней від предметів, порушення законів освітлення чи перспективи). В умовах експлуатації MASS такий візуальний чи семантичний артефакт виявляється миттєво, навіть без використання складних стеганоаналітичних засобів, оскільки виникає закономірне питання про доцільність генерації подібних аномальних зображень на борту автономного судна. Наявність таких невідповідностей розглядається як непрямий індикатор (демаскувальна ознака) існування стеганоканалу. Це зумовлює необхідність введення спеціального критерію ефективності стегосистеми - *стійкості до контекстного аналізу*, що визначається як неможливість виявлення факту існування стеганоканалу через перевірку відповідності згенерованого контейнера штатному функціонуванню системи та законам природних фізичних явищ (для цифрових зображень і відео у складі MASS).

На практиці це створює новий вимір антагонізму: з одного боку, досягнення високої семантичної та фізичної правдоподібності ШІ-контейнера вимагає складних багаторівневих ітерацій генерації, контролю фізичних законів (освітлення, кінематики, геометрії), тобто значних додаткових обчислювальних витрат; з іншого боку, обмеження часового бюджету та хронометричної стійкості контуру управління MASS вимагають мінімального часу на формування й обробку контенту, що змушує спрощувати процеси генерації та збільшує ризики появи семантичних аномалій.

1. Мета роботи

Метою лабораторної роботи №2 є дослідження впливу параметрів ШІ-генерації та вбудовування даних на семантичну правдоподібність контейнерів, а також оцінка компромісу між хронометричною стійкістю системи та її стійкістю до контекстного аналізу в умовах сценарію MASS.

Робота забезпечує досягнення наступних результатів навчання:

РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

2. Теоретичні основи

2.1. Семантична правдоподібність та особливості контекстного аналізу ШІ-контентів

У сучасних кіберфізичних системах, зокрема морських автономних надводних системах для маскування прихованих (стеганографічних) каналів зв'язку все частіше використовуються цифрові зображення та відео фрагменти. Для забезпечення потрібних властивостей отриманого стеганоповідомлення тут можуть використовуватися контейнери, згенеровані за допомогою систем штучного інтелекту. На відміну від класичної стеганографії попередніх років, де контейнери, як правило, були природними (зображення, відео, аудіо, отримані фізичними відеокамерами), використання синтезованого контенту породжує специфічний клас загроз для стеганосистеми.

Контекстний аналіз у таких умовах спрямований на перевірку семантичної та фізичної правдоподібності контенту. Нейромережеві генератори здатні забезпечити гарне вбудовування додаткової інформації з точки зору статистичних властивостей отриманого стеганоповідомлення, проте вони часто допускають грубі порушення законів фізики, оптики та логіки довкілля (наприклад, невідповідність напрямку тіней, аномалії перспективи або віддзеркалень). В умовах реальної експлуатації MASS наявність подібних візуальних артефактів миттєво привертає увагу систем контролю або оператора. Генерація немотивованих чи «аномальних» контентів (зображень) на борту автономного судна є «демаскувальною» ознакою, яка може вказувати на:

- наявність прихованого каналу зв'язку (стеганоканалу), оскільки у штатному режимі роботи MASS вирішує чітко визначені навігаційні та технологічні завдання. Якщо система створює або передає згенеровані штучним інтелектом зображення чи відео, які не вимагаються поточними місіями (наприклад, для розпізнавання перешкод чи відеофіксації), це прямо вказує на те, що цей контент створюється з єдиною метою - використати його як контейнер для прихованої передачі даних;
- стороннє або несанкціоноване втручання, оскільки поява такого контенту сигналізує про те, що бортові обчислювальні потужності чи канали зв'язку використовуються для процесів, не передбачених регламентом управління судном. Для систем виявлення вторгнень (IDS) або зовнішніх комплексів радіоелектронної розвідки це чіткий індикатор того, що на борту відбувається підозріла активність (наприклад, спроба передати за межі контуру зібрані розвідувальні дані чи службові пакети).

2.2. Сутність антагонізму між хронометричною стійкістю та стійкістю до контекстного аналізу

Під час проєктування та розгортання захищених каналів зв'язку в контурах реального часу КФС, зокрема MASS, розробники стикаються з фундаментальною суперечністю - антагонізмом. Ця суперечність полягає у взаємній виключності або суворому конфлікті між двома критичними вимогами безпеки та працездатності стеганосистеми в межах MASS:

- Для того щоб прихований канал зв'язку залишався непомітним для систем моніторингу та контекстного аналізу, згенерований за допомогою штучного інтелекту контейнер (цифрове зображення чи відео) повинен мати абсолютну фізичну та семантичну правдоподібність. Це вимагає від обчислювальної підсистеми ретельного моделювання законів довкілля: коректного розрахунку кутів падіння світла, напрямків і контурів тіней, віддзеркалень, законів перспективи та фізичної динаміки об'єктів. Досягнення такого рівня якості неможливе за один крок генерації. Воно вимагає багаторівневих ітерацій нейромережевого синтезу, додаткових процедур фізично-інформованого контролю та складних обчислювальних процедур вбудовування. Це неминуче призводить до різкого зростання обчислювального навантаження та збільшення часу T_{gen} формування контейнера;
- Контур управління MASS функціонує в умовах жорсткого реального часу. Будь-які управлінські рішення, обробка сенсорних даних і передача телеметрії підпорядковані суворому часовому бюджету. Перевищення допустимих порогів затримки або поява критичного джиттера у мережі та обчислювачах може спричинити втрату стійкості рухомого об'єкта, навігаційні помилки або спрацьовування аварійних протоколів безпеки. Система керування судном фізично не може чекати тривалої генерації ідеального контенту. Часовий ліміт вимагає спрощення або прискорення процесу формування даних.

Зіткнення цих двох вимог створює дилему при проектуванні стеганосистеми для MASS. Якщо заради дотримання часового бюджету (хронометричної стійкості) скоротити час генерації контейнера (зменшити кількість ітерацій ІІІ-моделі або відмовитися від перевірки фізичних законів), у кадрі можуть з'явитися семантичні аномалії і, як наслідок, стеганоповідомлення, побудоване на основі такого контейнера, миттєво виявляється засобами контекстного аналізу як демаскувальна ознака наявності прихованого каналу. Якщо ж налаштувати систему на максимальну семантичну правдоподібність і бездоганне маскування, час генерації значно зросте. Це призведе до порушення часового бюджету контуру КФС, виникнення критичних затримок у передачі даних і потенційної втрати управління над автономним судном.

Таким чином, *завдання розробника стеганосистеми для MASS зводиться не до досягнення ідеальних показників за кожним критерієм окремо, а до пошуку такого робочого діапазону параметрів, який забезпечує достатній рівень стійкості до контекстного аналізу за умови збереження часових характеристик у межах допустимих допусків безпеки КФС.*

У межах лабораторної роботи №2 необхідно дослідити за допомогою імітаційного моделювання, де саме проходить межа інженерного антагонізму: при яких параметрах генерації та обсягах вбудовування ІІІ-контейнер зберігає достатню семантичну й фізичну правдоподібність для протидії контекстному аналізу, не порушуючи водночас критичних обмежень часового бюджету контуру управління та хронометричної стійкості морської автономної надводної системи (MASS).

3. Математична та структурна модель імітаційного експерименту

Цей розділ формалізує процес формування синтетичного контейнера, оцінки його контекстної стійкості та часових витрат.

3.1. Математична модель

3.1.1. Модель генерації контейнера.

Нехай процес синтезу цифрового контейнера (зображення чи відео) C задається оператором генерації Gen :

$$C = Gen(K, M, q),$$

де K - стеганоключ, M - приховане повідомлення (додаткова інформація), а q - вектор параметрів складності та якості ІІІ-генерації, який впливає на деталізацію фізичних законів, наприклад, розрахунок тіней та освітлення.

Зауваження. Оскільки робота базується на імітаційному моделюванні у середовищі *Python*, під оператором генерації $C = Gen(K, M, q)$ розуміється програмна імітаційна модель (функція), яка відтворює часові витрати та ймовірнісні характеристики появи семантичних аномалій залежно від обраного рівня складності q , без необхідності розгортання повномасштабних генеративних нейромережових архітектур.

Тобто студенту не потрібно генерувати реальні картинки за допомогою ІІІ. У скрипті цей процес може бути змодельований, зокрема на одному з двох рівнів:

Варіант А.

У програмі створюється функція-імітатор, яка приймає параметри якості q (наприклад, ступінь деталізації розрахунку тіней від 1 до 10) і обсяг повідомлення M :

- основна умова для моделювання часу генерації T_{gen} : чим вища якість q і більший обсяг додаткової інформації M , тим більшу затримку (у секундах чи мілісекундах) видає функція (наприклад, через штучну затримку або розрахунок циклом);
- показник правдоподібності $S(C)$ моделюється за допомогою деякої розрахункової формули, для якої виконується наступна вимога: якщо якість генерації низька (q має мале значення), то вона видає показник того, що з високою ймовірністю контекстний аналіз виявив аномалію (наприклад, «тінь не на місці»). Якщо q високе - правдоподібність 1.0.

Варіант Б.

Контейнером C слугує звичайний невеликий матричний масив (або готовий базовий файл зображення).

- оператор генерації та вбудовування реалізується як додавання в цей масив даних повідомлення M (наприклад, *LSB*-методом) та процедура внесення «штучного артефакту» (наприклад, зміна контрасту чи зсув кольорового каналу для імітації помилки ІІІ-генерації тіні);
- «контекстний аналізатор» у скрипті - перевірка градієнту або дисперсії в цій зоні зображення.

3.1.2. Метрика контекстної правдоподібності (стійкості до контекстного аналізу)

Будь-який контейнер (будь то потік сенсорної телеметрії кіберфізичної системи, кадр з бортової камери безпілотного апарату чи морського судна) функціонує у певному природному або промисловому середовищі. Контекстний аналіз спрямований на виявлення аномалій, викликаних неякісною генерацією (наприклад, штучним синтезом за допомогою ІІІ) або грубим втручанням, які

будуть специфічними для кожного природного/промислового середовища.

Метрика контекстної правдоподібності $S(C)$ оцінює, наскільки досліджуваний контейнер відповідає статистичним, структурним та фізичним інваріантам реального середовища функціонування до початку будь-якого приховування даних.

Щоб уникнути суб'єктивності, оцінка не будується на «абстрактних» правилах для всіх зображень чи сигналів світу. Еталонні характеристики визначаються двома шляхами:

- *за профілем середовища* (конфігурацією симуляції): кожне середовище у моделюванні (наприклад, «відкрита водна поверхня для MASS») має заздалегідь визначений цифровий паспорт із допустимими діапазонами фонові дисперсії та спектру;
- *шляхом калібрування*: перед аналізом студент виконує попередню процедуру на наданому еталонному наборі чистих фонових даних, обчислюючи базові статистичні показники нормального середовища.

Математична формалізація. Рівень контекстної правдоподібності контейнера-зображення обчислюється через відносно-статистичне відхилення його фонових характеристик від еталонної моделі середовища.

За основну міру стабільності фону приймається локальна дисперсія (σ^2). Для цифрового зображення (або окремого каналу яскравості растрового кадру) локальна дисперсія обчислюється в межах обраної фонові зони (або через ковзне вікно) як міра розсіювання яскравості пікселів навколо їхнього середнього значення. Оскільки в однорідному фоні (наприклад, спокійна водна поверхня для MASS) яскравість сусідніх пікселів змінюється плавно, локальна дисперсія має стабільне, прогнозоване значення. Штучні артефакти або погана генерація різко змінюють цей показник.

Для розрахунку локальної дисперсії для зображення:

- на зображенні виділяється прямокутна ділянка фону розміром $n \times m$ пікселів, де немає різних об'єктів, контурів або деталей;
- знаходиться середнє значення яскравості пікселів у межах цієї зони:

$$\mu = \frac{1}{nm} \sum_{i=1}^n \sum_{j=1}^m I(i, j)$$

де $I(i, j)$ - яскравість пікселя (i, j) .

- знаходження дисперсії:

$$\sigma^2 = \frac{1}{nm} \sum_{i=1}^n \sum_{j=1}^m (I(i, j) - \mu)^2. \quad (1)$$

Якщо значення σ^2 занадто низьке (прямує до нуля), це означає неприродну «замальованість» або надмірне розмиття фону, що характерно для поганих алгоритмів заповнення або грубих помилок генерації. Якщо значення σ^2 занадто високе, це свідчить про наявність нехарактерного високочастотного шуму, артефактів стиснення або чужорідних вкраплень. Якщо σ^2 потрапляє в діапазон еталонної моделі середовища, фон вважається природним, і контейнер успішно проходить перевірку контекстної правдоподібності.

Локальна дисперсія характеризує рівень природного шуму або текстури. Інтегральна метрика визначається як:

$$S(C) = 1 - \frac{|\sigma_{cont}^2 - \sigma_{env}^2|}{\max(\sigma_{env}^2, \varepsilon)}, \quad (2)$$

де σ_{cont}^2 - дисперсія у виділеній фоновій зоні досліджуваного контейнера; σ_{env}^2 - еталонне значення дисперсії для обраного типу середовища; $\varepsilon > 0$ - мала захисна константа, що виключає невизначеність у випадку ділення на нуль.

Значення метрики $S(C)$ завжди лежить у діапазоні $[0, 1]$.

Порядок виконання розрахунку. Під час розрахунку $S(C)$ проходяться такі етапи:

- *Виділення робочої зони:* обирається однорідна фоновіа ділянка контейнера (наприклад, відкрита вода або стабільна поверхня без об'єктів), де відсутні активні рухомі елементи;
- *Розрахунок локальної статистики:* обчислюється фактична дисперсія (1) обраної фоновіа зони контейнера;
- *Обчислення інтегрального показника:* за формулою (2) розраховується $S(C)$.
- *Зіставлення з моделлю:* отримане значення порівнюється з еталонним профілем середовища, закладеним у системі моделювання:
 - якщо $S(C) \geq S_{thresh}$ (наприклад, порогове значення встановлено на рівні 0.85): контейнер вважається контекстно правдоподібним. Його внутрішня структура не порушує фізичних законів і закономірностей середовища, тому він допускається до подальшого етапу вбудовування даних;
 - якщо $S(C) < S_{thresh}$: фіксується наявність аномалій (аномальні градієнти, неприродний шум або артефакти генерації). Контейнер відхиляється як непридатний для безпечного функціонування в контурі КФС.

У межах лабораторної роботи 2 значення S_{thresh} задається одним із двох способів:

- *За рівнями критичності середовища (модель загроз):* різні контури кіберфізичних систем мають різну чутливість до аномалій:

- *високий рівень захищеності (критична інфраструктура, військові застосування):* вимагає жорсткого порогу, наприклад, $S_{thresh} \in [0.90, 0.95]$. Будь-яке незначне відхилення від природного фону вважається демаскувальною ознакою або спробою несанкціонованого втручання;
- *стандартний рівень (моніторингові системи загального призначення):* допускає більш м'який поріг, наприклад, $S_{thresh} \in [0.75, 0.80]$, оскільки середовище саме по собі має вищу природну мінливість.

- *Експериментальний підбір за критерієм мінімізації помилок:* у ході виконання лабораторної роботи 2 студенту пропонується дослідити, як зміна порогового значення впливає на якість роботи системи:

- якщо зробити поріг занадто високим ($S_{thresh} \rightarrow 1$), система почне відхиляти навіть абсолютно нормальні, легітимні контейнери через мінімальні природні коливання (хибнопозитивні спрацьовування);
- якщо зробити поріг занадто низьким ($S_{thresh} \rightarrow 0.5$), система пропускати грубі артефакти ШІ-генерації чи неякісне вбудовування (пропуск загрози).

У ході виконання лабораторної роботи 2 студент самостійно встановлює порогове значення S_{thresh} (наприклад, 0.85 для стандартного профілю MASS) та обґрунтовує свій вибір, демонструючи баланс між хибними спрацьовуваннями системи контекстного аналізу та пропуском демаскувальних ознак.

3.2. Модель часового бюджету та затримок

Формула часового бюджету виглядає так:

$$T_{total}(q, M) = T_{gen}(q) + T_{emb}(M) + T_{net} + T_{ext}(M) + T_{proc} \quad (3)$$

де:

- $T_{total}(q, M)$ - загальний час циклу. Це повний час, який витрачається від моменту прийняття рішення про передачу даних до доставки сформованого стегоповідомлення одержувачу в контурі КФС. Він залежить від двох ключових аргументів: якості/складності генерації q та обсягу прихованих даних M ;
- q - параметр, що визначає складність або якість генерації контейнера (наприклад, ступінь деталізації моделі середовища або кількість ітерацій ШІ-генератора);

- M - обсяг прихованої інформації (у бітах або байтах), який необхідно вбудувати в контейнер;
- $T_{gen}(q)$ - час генерації або підготовки контейнера. Якщо контейнер синтезується процедурно або за допомогою моделі, то зі збільшенням складності/якості q цей час зростає;
- $T_{emb}(M)$ - час вбудовування. Це обчислювальні витрати алгоритму на приховування корисного навантаження обсягом M у структуру контейнера (наприклад, модифікація коефіцієнтів або вибіркового пікселів);
- T_{net} - час мережевої передачі. Час, необхідний для транспортування готового файлу або потоку даних через мережу зв'язку КФС;
- $T_{ext}(M)$ - час вилучення прихованого повідомлення обсягом M на приймальному боці ;
- T_{proc} - стандартний час загальної системної та мережевої обробки пакета.

Практичне визначення складових (3).

- $T_{gen}(q)$ - час, необхідний для створення або синтезу базового контейнера із заданим рівнем якості або складності q може бути визначений:
 - *експериментально (шляхом вимірювання)*: запускається функція генерації контейнера, а системний таймер фіксує інтервал від старту до завершення процесу;
 - *аналітично*: залежить від параметру q (наприклад, чим вища деталізація чи складність процедурної генерації, тим більший час витрачається за формулою залежності, заданою в умовах лаби).;
- $T_{emb}(M)$ - обчислювальні витрати алгоритму на приховування корисного навантаження обсягом M (у бітах або байтах) усередину вже згенерованого контейнера може бути визначений безпосередньо в процесі виконання процедури вбудовування. Студент змінює обсяг даних M (наприклад, віддає на вбудовування 100 байт, потім 500 байт, потім 1 КБ) і фіксує, як зростає цей час за допомогою вбудованого таймера. Зазвичай ця залежність є лінійною;
- T_{net} - час мережевої передачі розраховується за класичною інженерною формулою зв'язку: ділиться загальний розмір сформованого файлу (контейнера з даними) на пропускну здатність каналу зв'язку, до чого додається фіксована затримка поширення сигналу в середовищі. Наприклад, профіль «MASS (гідроакустичний канал зв'язку)» має наступні показники:
 - пропускну здатність низька (наприклад, 9600 біт/с);
 - швидкість поширення сигналу (W): швидкість звуку у воді (~ 1500 м/с).
 - фіксована затримка поширення: якщо судно знаходиться на відстані $d=3$ км від пункту управління, затримка поширення стає критичною ($3000 / 1500 = 2$ секунди);

- $T_{ext}(M)$ - час вилучення прихованого повідомлення обсягом M на приймальному боці. Вимірюється експериментально на стороні приймача. Цей показник критично важливий, оскільки він часто залежить від обсягу M та складності перевірки цілісності повідомлення;
- T_{proc} - стандартний час загальної системної та мережевої обробки пакета, визначається як константа із технічного паспорта обладнання (контролера КФС), що моделюється, або визначається як стабільна системна затримка за результатами базового калібрування мережі (для MASS часто 2 мс).

3.3. Цільова функція інженерного антагонізму

Необхідно знайти такий баланс параметрів q , M , за якого максимізується стійкість до контекстного аналізу за умови дотримання жорсткого часового ліміту контуру керування:

$$\max_{q,M} S(C) \text{ за умови } T_{total}(q,M) \leq T_{max}, \quad (4)$$

де T_{max} - гранично допустимий час такту керування системою, для навігаційного контуру MASS T_{max} може становити 1...2 с.

Якщо з урахуванням усіх складових (3) порушується умова $T_{total}(q,M) \leq T_{max}$, то конфігурація (q, M) бракується, навіть якщо вона забезпечує ідеальну маскування $S(C) = 0.99$.

У ході виконання лабораторної роботи 2 проводиться пошук робочої точки: змінюючи параметри генерації q (від простих до складних) та обсяг даних M (від малих до великих), для кожної пари (q, M) обчислюється $T_{total}(q,M)$ і порівнюється з T_{max} . Усі варіанти, де $T_{total}(q,M) > T_{max}$, відсіваються (потрапляють у зону аварійного зриву реального часу). Серед усіх прийнятних варіантів обирається той, який забезпечує найвищий показник контекстної правдоподібності $S(C)$.

3.4. Структурна модель (архітектура імітаційного експерименту)

Структура імітаційного комплексу складається з таких взаємодіючих модулів:

- **Блок генерації контенту:** генерує цифрові зображення/відео з урахуванням заданих параметрів якості та прихованого повідомлення;
- **Модуль семантичного та контекстного контролю:** симулює роботу алгоритмів перевірки фізичної правдоподібності (аналіз напрямку тіней, освітленості та геометрії тощо);
- **Хронометричний монітор:** вимірює час виконання.
- **Блок оцінки антагонізму:** зіставляє отримані показники затримок зі ступенем семантичних спотворень та формує результуючі графіки компромісу.

4. Порядок виконання лабораторної роботи

Етап 1. Ініціалізація

1. Ознайомтеся з індивідуальним варіантом завдання.
2. Зафіксуйте:
 - еталонне значення фонові дисперсії середовища σ_{env}^2 ;
 - допустимий поріг контекстної правдоподібності S_{thresh} ;
 - параметри каналу зв'язку (пропускну здатність та дистанцію);
 - апаратний профіль контролера (системну затримку T_{proc} та критичний такт реального часу T_{max}).

Етап 2. Оцінка контекстної правдоподібності контейнера

- Завантажте базовий файл контейнера (кадр телеметрії або фрагмент фонового зображення) для обраного середовища;
- Виділіть однорідну фонову зону без активних рухомих об'єктів та інженерних деталей;
- Розрахуйте локальну дисперсію σ_{cont}^2 обраної фонові зони;
- Обчисліть інтегральний показник контекстної правдоподібності $S(C)$.
- Проведіть зіставлення з моделлю. .

Етап 3. Моделювання та розрахунок часового бюджету контуру

Для ухваленого контейнера виконайте почерговий розрахунок усіх складових повного циклу передачі даних за формулою (3):

1. Зафіксуйте час підготовки контейнера $T_{gen}(q)$ залежно від обраного рівня складності/якості q ;
2. Виміряйте витрати часу $T_{emb}(M)$ на приховування корисного навантаження обсягом M ;
3. Обчисліть T_{net} за формулою зв'язку на основі розміру сформованого файлу, пропускну здатності каналу та дистанції поширення сигналу;
4. Визначте час $T_{ext}(M)$, необхідний приймальному контролеру на сканування, детектування та декодування прихованого повідомлення;
5. Візьміть фіксоване значення T_{proc} протокольної обробки для MASS.

Етап 4. Дослідження інженерного антагонізму

Виконайте пошук раціональної робочої точки системи за критерієм максимізації правдоподібності за умови дотримання часових обмежень (4):

1. Змініть параметри генерації q та обсяг вбудованих даних M у заданих межах;
2. Для кожної комбінації (q, M) розрахуйте повний час $T_{total}(q, M)$ та перевірте виконання умови: $T_{total}(q, M) \leq T_{max}$;
3. Відсійте всі конфігурації, що призводять до порушення $T_{total}(q, M) \leq T_{max}$ (потрапляють у зону аварійного запізнення);
4. Серед решти допустимих варіантів оберіть точку, яка забезпечує максимальний рівень $S(C)$.

Етап 5. Оформлення звіту

Сформуйте звіт, який повинен містити:

1. Мету та теоретичні відомості роботи.
2. Результати розрахунку контекстної правдоподібності $S(C)$ для досліджуваного контейнера.
3. Зведену таблицю часового бюджету за всіма складовими $T_{total}(q, M)$ для різних сценаріїв.
4. Графіки залежності загальної затримки від обсягу даних M та рівня складності q із нанесеною лінією критичного обмеження T_{max} .
5. Обґрунтування знайденої оптимальної робочої точки та висновки щодо забезпечення безпеки і стійкості КФС.

5. Варіанти індивідуальних завдань

Студент виконує розрахунки згідно зі своїм порядковим номером у списку групи. Усі сценарії моделюють роботу бортових інформаційних систем морських автономних суден (MASS).

№ Варіан та	Морський сценарій / умови середовища	Еталон на дисперс ія σ_{env}^2	Поріг правдоподібн ості S_{thresh}	Канал зв'язку MASS (BW) та дистанція (d)	Апаратний профіль / системна затримка (T_{proc})	Критичн ий такт реальног о часу (T_{max})
1	Відкрите море (Денний фоновий кадр спокійної водної поверхні)	24.5	0.85	Гідроакустич ний канал: 4.8 кбіт/с, $d = 3$ км	Бортовий морський ІРС (5.0 мс)	2000 мс
2	Прибережн а зона (Мілководдя , наявність природних відблисків)	42.0	0.80	Мобільний морський радіоканал: 2 Мбіт/с, $d = 5$ км	Бортовий промислови й ПК (3.5 мс)	500 мс
3	Нічна навігація (Інфрачерво ний кадр поверхні в умовах обмеженої видимості)	12.8	0.90	Супутникови й канал зв'язку: 512 кбіт/с, $d = 20$ км	Захищений судновий шлюз (8.0 мс)	1500 мс
4	Портова акваторія (Інтенсивни й рух, складний текстурний	55.6	0.75	Судновий Wi-Fi / VHF: 10 Мбіт/с, $d = 1$ км	Бортовий мікроконтро лер (2.0 мс)	200 мс

	фон)					
5	Штормові умови (Висока турбулентність та білі гребені хвиль)	78.2	0.70	Гідроакустичний канал: 2.4 кбіт/с, $d = 2$ км	Бортовий морський ІРС (6.0 мс)	3000 мс
6	Океанський перехід (Дальній зв'язок, стабільний горизонт)	18.3	0.88	Супутниковий канал: 256 кбіт/с, $d = 50$ км	Захищений судновий шлюз (10.0 мс)	5000 мс

Зауваження. Зверніть увагу на специфіку каналів зв'язку MASS: гідроакустичні канали мають низьку пропускну здатність (BW) і велику затримку через низьку швидкість поширення звуку у воді, тоді як радіо- та супутникові канали працюють на швидкостях хвиль, але мають інші ліміти $T_{\max}$.

Усі розрахунки часового бюджету та перевірки на антагонізм проводяться суворо для обраного суднового сценарію.

Контрольні питання

1. Що саме оцінює метрика контекстної правдоподібності $S(C)$ і чому перевірку контейнера обов'язково виконують до початку вбудовування в нього конфіденційних даних?
2. Як саме обчислюється локальна дисперсія у виділеній фоновій зоні? Про що свідчить занадто низьке або занадто високе значення цього показника відносно еталона?
3. Яким чином обирається порогове значення контекстної правдоподібності для конкретного сценарію? До яких системних наслідків призведе встановлення занадто жорсткого або занадто м'якого порогу?
4. Запишіть та розшифруйте повну формулу часового циклу передачі. Які саме процеси охоплює кожен із п'яти її компонентів?
5. Як параметризація якості та складності генерації контейнера впливає на час його підготовки та на рівень стійкості до контекстного аналізу? Поясніть.
6. Чим відрізняється методика розрахунку часу мережевої передачі при використанні гідроакустичного каналу зв'язку порівняно з супутниковим каналом? Які фізичні константи при цьому враховуються?
7. Чому час вилучення прихованої інформації на приймальному боці виділено в окрему складову і чим він концептуально відрізняється від загальної системної та протокольної обробки?
8. Поясніть поняття «антагонізму» в розробці захищених систем для MASS. Між якими суперечливими вимогами доводиться шукати компроміс?

9. Як формулюється цільова задача оптимізації в роботі? Що відбувається з отриманою конфігурацією системи, якщо розрахований час циклу перевищує критичний такт реального часу?

Література

1. Інтегрована методологія виявлення, аналізу та нейтралізації загроз у сфері національної безпеки і оборони: монографія / С.В.Мілевський, С.С.Погасій, О.А.Лаптев, В.А.Савченко, А.Г.Салій, А.А.Кобозєва, П.В.Жук, Є.О.Меленті. – Харків: НТУ «ХПІ»; Львів: «Новий Світ-2000», 2026. – 424 с.
2. Кіберфізичні системи: технології збору даних [Текст]: монографія - О.Ю. Бочкарьов, В.А. Голембо, Я.С. Парамуд, В.О. Яцук. За редакцією професора А. О. Мельника. Львів: “Магнолія 2006”, 2024. – 176 с.
https://magnolia.lviv.ua/wp-content/uploads/2024/04/Kiiberfizyka-knyha2_zmist.pdf
3. Технології сучасних кібер-фізичних систем: Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології», освітньо-професійна програма «Автоматизація та комп’ютерно-інтегровані технології кібер-енергетичних систем»; укладач: Ю.Є. Грудзинський. – Електронні текстові дані (1 файл: 14,8 МБ). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 327 с.