ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Приховування комунікаційних каналів в інтерактивних застосунках»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Денис РОЗГОН
(підпис)

Виконав: здобувач вищої освіти групи БСДМ-61
РОЗГОН Денис
(прізвище, ім'я)

Керівник д.т.н., професор КОЖУХІВСЬКИЙ Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасному цифровому світі швидке зростання обсягу даних і розвиток інтерактивних застосунків відкриває нові горизонти для комунікації, але також створює нові загрози для інформаційної безпеки. Зокрема, зростання популярності прихованих комунікаційних каналів ускладнює забезпечення прозорості та захищеності даних. Ці канали можуть використовуватися як для законних цілей, так і для здійснення злочинних дій, що визначає їхню складну природу та важливість дослідження.

Об'єкт дослідження – приховані комунікаційні канали в інтерактивних застосунках.

Предмет дослідження – методи створення, виявлення та нейтралізації прихованих комунікаційних каналів.

Мета роботи – розробка рекомендацій щодо виявлення та протидії прихованим комунікаційним каналам в інтерактивних застосунках.

Наукові завдання:

Проаналізувати сутність прихованих комунікаційних каналів та їх класифікацію.

Дослідити методи створення прихованих каналів у інтерактивних застосунках.

Розробити підходи до їх виявлення за допомогою сучасних технологій.

Проаналізувати правові та етичні аспекти використання прихованих каналів.

Розробити рекомендації щодо нейтралізації цих каналів.

Методи дослідження – аналіз літератури, експериментальне моделювання, програмна реалізація та тестування.

Практичне значення роботи полягає у створенні підходів до ефективного виявлення та протидії прихованим каналам у інтерактивних застосунках, що сприятиме підвищенню рівня інформаційної безпеки.

Результати кваліфікаційної роботи апробовані на VII Міжнародній студентській науковій конференції «Модернізація та сучасні українські і світові наукові дослідження», яка відбулася 6 грудня 2024 року в м. Чернігів, Україна.

1. ТЕОРЕТИЧНІ ОСНОВИ ПРИХОВАННЯ КОМУНІКАЦІЙНИХ КАНАЛІВ В ІНТЕРАКТИВНИХ ЗАСТОСУНКАХ

1.1. Сутність та особливості прихованих комунікаційних каналів

Приховані комунікаційні канали в інтерактивних застосунках є специфічними шляхами передачі інформації [1], які не виявляються звичайними методами перевірки безпеки. Вони можуть використовуватися для передачі конфіденційної інформації, скриптів або навіть шкідливого коду. Особливості прихованих комунікаційних каналів полягають у тому, що вони можуть бути розміщені в різноманітних елементах програмного забезпечення, таких як зображення, аудіо або навіть в пересиланні даних між користувачами [2]. Важливо зазначити, що їх виявлення вимагає спеціалізованих методів та технік аналізу, які можуть бути трудомісткими та складними для виконання.

У таких ситуаціях, особливо важливо звернути увагу на можливість використання стеганографії [7] - методу, який дозволяє заховати інформацію в незначних змінах сигналу. Стеганографія це метод приховування інформації, який використовується для вбудовування її в інше повідомлення або об'єкт з метою зробити присутність самої інформації максимально непомітною для спостерігачів та збільшити ступінь конфіденційності. Цей унікальний підхід дає змогу передавати секретні дані за допомогою різних предметів або мовою комунікації, що є загальноприйнятим і невидимим для багатьох. Використання стеганографії може бути дуже корисним для важливих переговорів, розвідувальних операцій та захисту конфіденційної інформації. Завдяки своїм технічним можливостям, стеганографія зміцнює безпеку та забезпечує надійний обмін даними між сторонами.

Захист інформації є ключовим аспектом у багатьох сферах діяльності, і стеганографія грає важливу роль в забезпеченні безпеки й конфіденційності цих

даних. При розвитку технологій стеганографія постійно вдосконалюється, щоб відповідати сучасним вимогам у сфері безпеки і конфіденційності. Використання стеганографії сприяє ефективному обміну інформацією та забезпечує захист від несанкціонованого доступу до важливих даних. Впровадження стеганографії в різні галузі дозволяє зберегти цінні дані без ризику їх пошкодження або втрати [3].

Стеганографія має тривалу історію (рисунок 1.1), що починається ще в 480 році до н.е., коли в Давній Греції використовували воскові дощечки для того, щоб заховати текст під шаром воску. У 494 році до н.е. перський цар Демаратес застосував метод тату на голові свого раба, для того щоб приховати повідомлення, яке могло бути розкрите лише після зростання волосся. У період Відродження, близько в 1558 році, секретні записи ховалися всередині варених яєць, що забезпечувало додатковий рівень безпеки. У 1680 році композитори закладали приховані коди у музичні ноти, дозволяючи передавати інформацію лише тим, хто знав ключ до дешифрування. Протягом 19 століття, зокрема в 1800 році, використовували газетні коди, які приховували повідомлення серед звичайного тексту газети, роблячи їх непомітними для сторонніх читачів. У 1915 році під час Першої світової війни активно застосовували невидимі чорнила для передачі секретних повідомлень, що ставали видимими під впливом тепла або спеціальних реагентів. У 1940 році, під час Другої світової війни, була розроблена технологія мікроточок, що дозволяла зберігати велику кількість інформації у мініатюрних точках на фотографіях або документах, які можна було прочитати за допомогою спеціального оптичного обладнання. Сучасна стеганографія продовжує еволюціонувати, поєднуючи традиційні методи з цифровими технологіями для забезпечення безпеки та приховування інформації.

Рис. 1.1. Ключові етапи становлення стенографії

Розвиток стеганографії в останні двадцять років відновився через широке поширення мультимедійних технологій. Разом з появою нових типів каналів передачі інформації це стало подальшим стимулом для розвитку і вдосконалення стеганографії, що спричинило виникнення нових стеганографічних методів.

Особливості представлення інформації в комп'ютерних файлах та обчислювальних мережах відіграли важливу роль у цьому процесі, що свідчить про розвиток комп'ютерної стеганографії.

Сучасний рівень стеганографії значно зріс завдяки прогресу цифрових технологій. Комп'ютерна стеганографія надає можливість приховувати інформацію

в різних цифрових носіях, таких як зображення, відео, аудіофайли та текстові документи. Одним з найпоширеніших методів є зміна менш важливих бітів (LSB) пікселів зображень або аудіоданих, що дозволяє вставляти секретні повідомлення без помітних змін у зовнішньому вигляді файлу. Інші сучасні методи включають використання алгоритмів перетворення, таких як дискретне косинусне перетворення (DCT) та перетворення Фур'є, для впровадження інформації в частотні компоненти медіафайлів. Крім цього, сучасні інструменти стеганографії часто поєднують криптографічні алгоритми для додаткового захисту, забезпечуючи двофакторну безпеку: шифрування інформації перед її приховуванням [4]. Це робить стеганографію ефективним засобом для захисту даних від несанкціонованого доступу та розкриття. Комп'ютерна стеганографія має широке застосування у різних галузях, включаючи кібербезпеку, захист авторських прав, цифровий маркетинг та передачу конфіденційних даних. У сфері кібербезпеки стеганографія використовується для приховування команд та контролюючих сигналів у комунікаціях, що ускладнює їх виявлення та аналіз зловмисниками. Окрім легітимних застосувань, стеганографія також може бути використана злочинцями для приховування шкідливого програмного забезпечення або конфіденційних даних, що створює додаткові виклики для правоохоронних органів. Сучасні дослідження в області стеганографії зосереджені на підвищенні стійкості методів до аналізу та розкриття, а також на розробці нових технік детекції прихованої інформації. Зі стрімким розвитком технологій стеганографія продовжує залишатися важливим інструментом як для захисту, так і для потенційного зловживання інформацією, підкреслюючи її значення в сучасному цифровому світі.

Одним з сучасних напрямків стеганографії є застосування методів, що дозволяють приховувати інформацію у сигналах, які передаються за різноманітними протоколами зв'язку. Цей підхід базується на використанні різних аспектів комунікаційних протоколів, таких як заголовки пакетів, поля управління або навіть самі дані, для вбудовування секретної інформації без впливу на основні функції передачі даних. Наприклад, можна маніпулювати непомітними бітами у

заголовках протоколів TCP/IP, ICMP або HTTP, щоб вставити приховані повідомлення, які не впливають на нормальну роботу мережі і залишаються непомітними для стандартних засобів моніторингу. Інші техніки включають використання таймінгових каналів, де зміни у часових інтервалах між пакетами кодують інформацію, або приховування даних у параметрах маршрутизації та аутентифікації. Застосування цих методів дозволяє забезпечити додатковий рівень безпеки та конфіденційності, оскільки передані дані можуть залишатися захищеними від несанкціонованого доступу та аналізу. Проте, такі підходи також створюють виклики для кібербезпеки, оскільки зловмисники можуть використовувати їх для приховування шкідливих дій або передачі конфіденційної інформації, що вимагає розробки ефективних методів виявлення та протидії таким прихованим каналам передачі даних.

Приховані комунікаційні канали є одними з найсучасніших і найскладніших способів передачі інформації, які використовують різні технічні засоби для приховування секретних повідомлень у звичайних даних. Ці канали можуть бути реалізовані через різні медіа, такі як цифрові зображення, аудіофайли, відео, мережеві протоколи та навіть фізичні носії даних [5]. Наприклад, у цифрових зображеннях можна використовувати техніку зміни найменш значущих бітів пікселів (LSB) для вбудовування інформації, яка залишається непомітною для людського ока. У мережевих протоколах приховані дані можуть передаватися через нестандартні поля заголовків пакетів або через таймінгові варіації між передачею пакетів, що ускладнює їх виявлення за допомогою звичайних засобів моніторингу. Негативні приклади використання прихованих комунікаційних каналів включають їх застосування у кіберзлочинності та тероризмі. Зловмисники можуть використовувати стеганографію для приховування шкідливого програмного забезпечення у легітимних файлах, таких як зображення чи документи, що дозволяє обходити антивірусні програми та засоби виявлення загроз. Також приховані канали використовуються для нелегальної передачі конфіденційних даних, таких як фінансова інформація, державні таємниці або особисті дані, що може

призводити до серйозних наслідків для безпеки національних та корпоративних систем. Крім того, терористичні організації можуть використовувати приховані канали для координації своїх дій без ризику бути виявленими правоохоронними органами. Ці негативні аспекти створюють значні виклики для кібербезпеки, оскільки вимагають розробки нових методів детекції та протидії прихованим комунікаційним каналам, щоб захистити інформаційні системи від зловмисного використання.

Одним з сучасних прикладів використання прихованих комунікаційних каналів є діяльність кіберзлочинних груп, що використовують стеганографію для того, щоб приховувати команди та керуючі сигнали в зображеннях, що публікуються в соціальних мережах або на публічних веб-сайтах. Наприклад, у 2022 році було виявлено, що деякі шкідливі програми використовують стеганографію для вбудовування команд у PNG-файли, які потім завантажуються на платформи типу Twitter або GitHub. Ці зображення виглядають звичайними для користувачів і не викликають підозр, однак спеціалізовані інструменти можуть витягувати приховану інформацію для отримання інструкцій від командного центру (C2). Ще одним прикладом є використання стеганографії в сучасних атаках типу "ransomware". Кіберзлочинці можуть приховувати інформацію про захоплені системи або викрадені дані у вигляді зображень або відео, які розповсюджуються через інтернет. Це дозволяє їм уникати виявлення традиційними засобами безпеки, такими як антивірусні програми чи системи виявлення вторгнень. Наприклад, група Maze, яка спеціалізувалася на атаках "ransomware", використовувала стеганографію для приховування інформації про жертви у файлах, що розповсюджувалися серед потенційних цілей. Такий підхід ускладнює завдання аналітикам кібербезпеки щодо виявлення та нейтралізації загроз, підсилюючи ефективність злочинних дій. Ці сучасні приклади показують, як приховані комунікаційні канали стають все більш складними та витонченими, що вимагає від фахівців з кібербезпеки постійного вдосконалення методів виявлення та протидії таким загрозам. Використання стеганографії в кіберзлочинності підкреслює

необхідність інтеграції передових технологій аналізу даних та штучного інтелекту для забезпечення ефективного захисту інформаційних систем.

Це може бути великим викликом для професіоналів з області кібербезпеки, оскільки виявлення та розкриття прихованого комунікаційного каналу вимагає знань, вмінь та спеціального обладнання. Застосування різноманітних методів стеганалізу може допомогти знайти та знищити приховані канали комунікації, забезпечуючи таким чином безпеку та захищеність інтерактивних застосунків. Крім того, розробники програмного забезпечення повинні приділяти належну увагу захисту від прихованих комунікаційних каналів, враховуючи можливі порушення безпеки та наслідки, що вони можуть мати.

Виявлення прихованих каналів зв'язку є критично важливим для забезпечення безпеки інформаційних систем та протидії кіберзлочинності. Методи представлені нижче (рисунок 1.2).

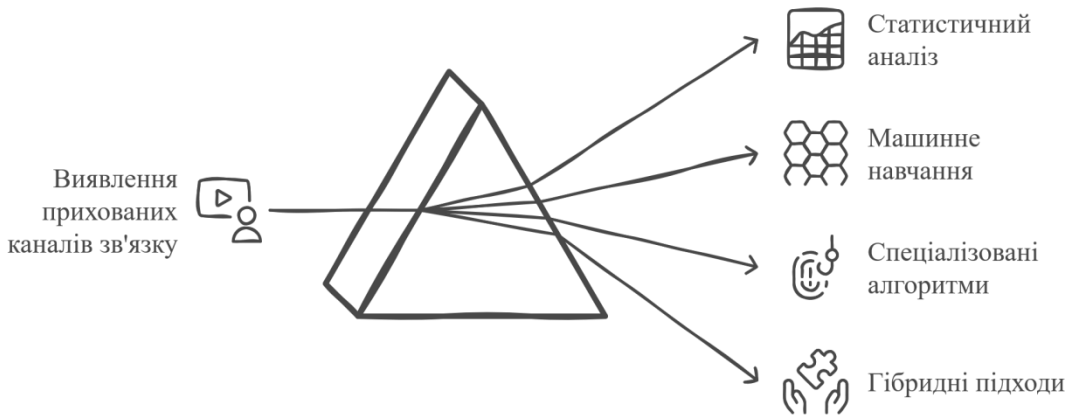

Рис. 1.2. Методи виявлення прихованих каналів зв’язку

Одним із основних підходів є статистичний аналіз даних, який полягає у виявленні аномалій або нетипових патернів у передаваних даних. Наприклад, зміни найменш значущих бітів (LSB) у зображеннях можуть бути виявлені шляхом аналізу розподілу бітів та пошуку відхилень від нормального статистичного фону. Інші статистичні методи включають аналіз ентропії та кореляції, які дозволяють

визначити невідповідності між очікуваними та фактичними характеристиками даних. Крім традиційних статистичних методів, сучасні підходи до виявлення прихованих каналів зв'язку активно використовують машинне навчання та штучний інтелект. Алгоритми машинного навчання можуть бути навчені на великих наборах даних для розпізнавання складних патернів, характерних для стеганографічних технік. Наприклад, нейронні мережі можуть аналізувати зображення або аудіофайли для виявлення невидимих змін, що вказують на приховану інформацію. Інші методи включають використання глибинного навчання та методів обробки природної мови для аналізу текстових документів та виявлення прихованих повідомлень. Додатково, спеціалізовані алгоритми стеганалітики розробляються для конкретних типів даних та стеганографічних технік. Ці алгоритми можуть включати методи аналізу частотних компонентів, такі як дискретне косинусне перетворення (DCT) або перетворення Фур'є, для виявлення аномалій у частотному домені медіафайлів. Інші методи зосереджуються на аналізі метаданих файлів, що дозволяє виявити підозрілі зміни або додаткові дані, що можуть містити приховану інформацію. Крім того, інтеграція декількох методів виявлення та використання гібридних підходів підвищує ефективність і точність розпізнавання прихованих каналів зв'язку. Таким чином, комбінація статистичних аналізів, машинного навчання та спеціалізованих алгоритмів забезпечує ефективні інструменти для виявлення прихованих комунікаційних каналів. Постійний розвиток технологій вимагає також удосконалення методів виявлення, щоб йти в ногу з новими стеганографічними техніками та забезпечувати високий рівень захисту інформаційних систем від несанкціонованого доступу та зловмисних дій.

Отже, для забезпечення безпеки важливо бути в курсі інтерактивних застосунків та спеціалізованої методології виявлення прихованих каналів комунікації.

1.2. Класифікація та види прихованих каналів

Класифікація прихованих комунікаційних каналів (рисунок 1.3) в інтерактивних застосунках проводиться згідно з різними критеріями, такими як природа каналу (активний чи пасивний), спосіб приховування (стеганографія, криптографія), тип носія (текст, зображення, звук), спосіб передачі (паралельний, послідовний), інші технічні та організаційні характеристики. Види прихованих каналів включають такі форми, як інформаційний шум, встраивання, пристосування та перетворення. Класифікація та розуміння типів прихованих каналів дозволяє забезпечити більш ефективне виявлення та захист від їх використання в інтерактивних застосунках.

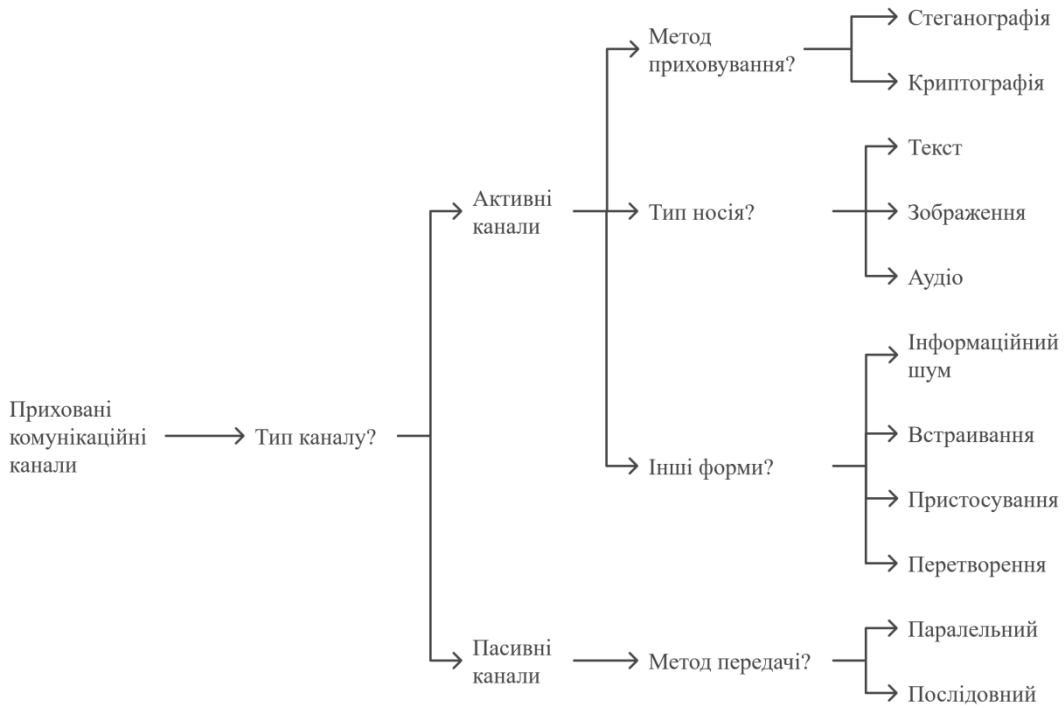

Рис. 1.3. Класифікація прихованих комунікаційних каналів

Активні канали включають активний вплив на процес передачі даних, наприклад, вставку повідомлень у структуру протоколів або маніпуляцію параметрами трафіку. Пасивні канали використовують уже існуючі властивості

системи без змін її функціоналу, наприклад, аналіз часових інтервалів між пакетами для прихованої передачі інформації.

Стеганографія ґрунтується на техніці приховування інформації всередині інших даних, таких як зображення, аудіо чи відео, з метою зробити сам факт існування повідомлення непомітним [10]. Криптографія, натомість, забезпечує захист тільки змісту інформації, а не її існування. У багатьох випадках криптографічні методи використовуються спільно зі стеганографічними для підвищення рівня безпеки.

Зміни, вносить у різні типи даних, можуть бути виконані за допомогою різних технік, таких як маніпуляція пробілами, синтаксисом або форматуванням. Також можна використовувати зображення шляхом використання технік LSB або маніпуляції кольоровими каналами, а також аудіо та відео за допомогою вбудовування інформації у частотні компоненти або часові проміжки. Крім того, можливо проводити маніпуляції полями заголовків чи міжпакетними інтервалами мережевих пакетів.

Паралельний канал одночасно передає конфіденційні дані разом з основним потоком інформації. Послідовний канал передбачає передачу конфіденційної інформації розрізаною на окремі частини, які передаються в різний час або серед різних потоків.

Інформаційний шум - це використання статистичних або фізичних властивостей даних, такі як додавання фонових сигналів, що містять сховану інформацію. Вбудовування - це інтеграція прихованої інформації у звичайний потік даних, наприклад, шляхом модифікації неважливих частин повідомлення. Адаптація - це зміна характеристик сигналу або даних, наприклад, маніпуляція частотами чи інтервалами передачі. Трансформація - це приховування інформації через кодування в альтернативних представленнях, наприклад, у вигляді шуму чи зображень.

Також присутні і інші параметри по яким ми можемо класифікувати приховані канали. Рівень доступу до системи (легітимний чи нелегітимний доступ).

Складність впровадження (вимоги до обладнання, програмного забезпечення чи рівня знань). Обсяг переданої інформації (низька чи висока пропускна здатність).

Розуміння класифікації і видів прихованих каналів допоможе виявити їх більш ефективно. Більше розуміння цього питання забезпечує можливість раннього виявлення прихованих каналів і прийняття ефективних заходів для їх ліквідації.

1.3. Правові та етичні аспекти прихованих каналів у інтерактивних застосунках з точки зору безпеки

Правові та етичні аспекти прихованих каналів у інтерактивних застосунках з точки зору безпеки є дуже важливими, оскільки використання таких каналів може порушити конфіденційність та приватність користувачів. Це може стати причиною злочинних дій, порушень законодавства про захист особистих даних та навіть терористичних актів. Тому важливо розробляти і впроваджувати етичні та законні стандарти щодо використання прихованих комунікаційних каналів в інтерактивних застосунках. Це включає в себе публічний обговорення, розробку рішень та правила для регулювання використання таких каналів, а також встановлення відповідальності за їхнє недодержання.

Використання таємних комунікаційних засобів у взаємодії програм створює важливі юридичні та етичні питання, які потребують уважного вивчення (рисунок 1.4). Юридично законодавство багатьох країн ще не повністю пристосоване до викликів, пов'язаних із стеганографією та таємними засобами зв'язку. З одного боку, ці технології можуть бути використані для законних цілей, таких як захист авторських прав, забезпечення конфіденційності даних або підвищення безпеки комунікацій. Наприклад, державні установи можуть використовувати стеганографію для захисту секретних повідомлень від несанкціонованого доступу. З іншого боку, злочинці можуть використовувати таємні канали для незаконних дій, включаючи кібершпигунство, поширення шкідливого програмного забезпечення

або організацію терористичних актів. Це створює дилему для законодавців, які повинні знайти баланс між захистом прав громадян на приватність та необхідністю боротьби з кіберзлочинністю.

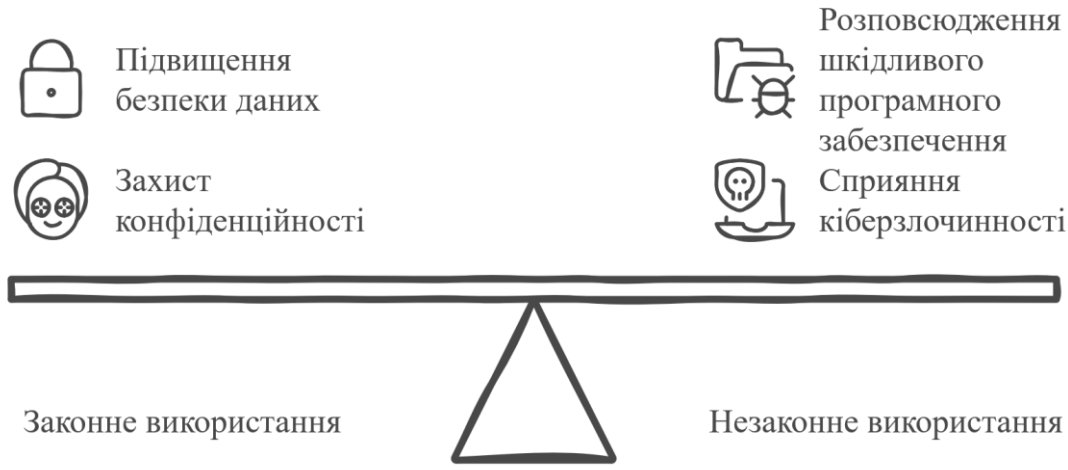

Рис. 1.4. Законне і незаконне використання комунікаційних каналів

Розглянемо правові аспекти використання прихованих каналів комунікації в Україні. Питання інформаційної безпеки регулюються кількома основними законами, серед яких: закон України "Про інформацію", закон України "Про захист інформації в інформаційно-телекомунікаційних системах", кримінальний кодекс України, закон України "Про захист персональних даних".

Перший закон встановлює основні принципи інформаційної діяльності, включаючи захист інформації від несанкціонованого доступу та розповсюдження. Використання стеганографії для приховування інформації може розглядатися в контексті захисту інформації, якщо воно здійснюється з метою забезпечення конфіденційності та приватності.

Закон "Про захист інформації в інформаційно-телекомунікаційних системах" регулює заходи щодо захисту інформації, включаючи технічні та організаційні засоби захисту. Використання прихованих каналів може бути частиною таких заходів у сфері інформаційної безпеки.

Кримінальний кодекс України містить статті, що стосуються кіберзлочинності, включаючи незаконне втручання в інформаційні системи, розповсюдження шкідливого програмного забезпечення та захист державної таємниці. Використання прихованих каналів для незаконної діяльності, такої як кібершпигунство або розповсюдження шкідливих програм, підпадає під дію цих норм. Таким чином стаття 361-4 Кримінального кодексу України про шкідливе програмне забезпечення передбачає кримінальну відповідальність за розробку, поширення або використання програм, що завдають шкоди комп'ютерним системам, мережам або інформації. Використання стеганографії для розповсюдження малваре також підпадає під цю статтю. Крім того, стаття 361-1 Кримінального кодексу України передбачає відповідальність за порушення правил захисту інформації.

Закон України "Про захист персональних даних" захищає права громадян на приватність та контроль над їхніми персональними даними. Використання стеганографії для приховування персональних даних може розглядатися як легітимний захід захисту приватності, але також може бути зловживаним для порушення цих прав. Національна безпека. В умовах конфлікту з Росією та загроз кібербезпеки, українське законодавство особливо акцентує увагу на захисті інформаційних ресурсів та запобіганні їх зловживанню. Використання прихованих каналів у військових або державних структурах регулюється спеціальними нормативними актами та інструкціями щодо інформаційної безпеки. Міжнародні зобов'язання. Україна, будучи учасником різних міжнародних угод та стандартів з інформаційної безпеки, зобов'язана дотримуватися міжнародних норм щодо захисту даних та боротьби з кіберзлочинністю. Це впливає на національне законодавство та політику у сфері використання прихованих комунікаційних каналів.

Етичні питання використання стеганографії є вельми складними і різноманітними (рисунок 1.5). З одного боку, ця технологія може сприяти збільшенню приватності і захисту даних. Це особливо важливо в сучасному

цифровому суспільстві, де журналісти та активісти можуть використовувати стеганографію для безпечного обміну інформацією в репресивних умовах. З іншого боку, існує ризик зловживання цією технологією для порушення приватності, маніпуляції інформацією або здійснення незаконних дій. Також виникають етичні питання щодо відповідальності розробників програмного забезпечення та користувачів: чи повинні вони вживати заходів для запобігання зловживанням стеганографією, чи такі обмеження порушують права на свободу вираження та приватність. Важливо, щоб етичні норми супроводжували правові регуляції, забезпечуючи прозорість, відповідальність та захист прав усіх сторін у використанні стеганографії.

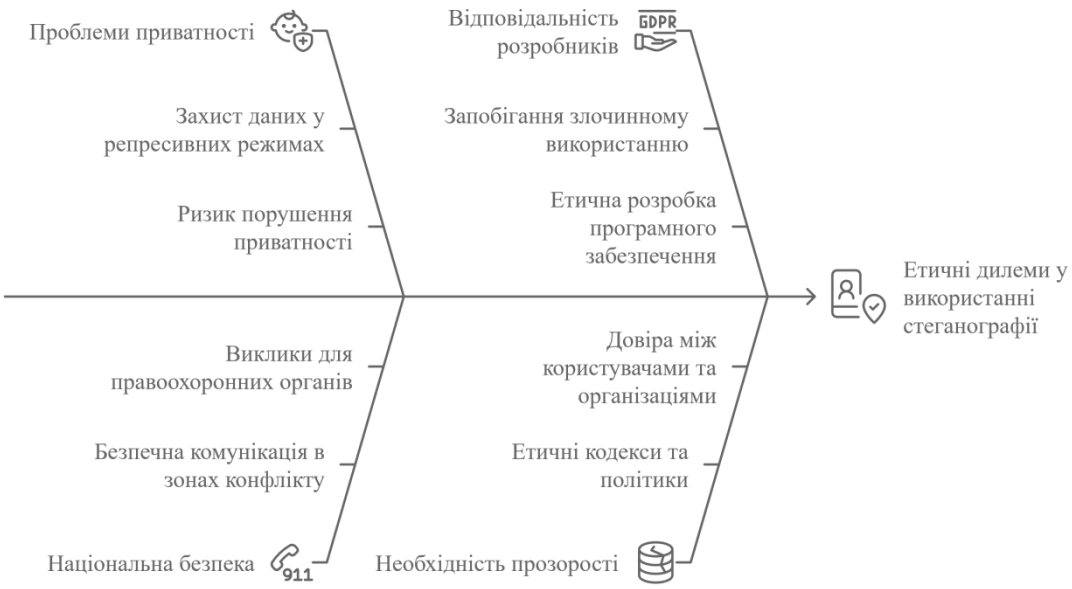

Рис. 1.5. Етичні питання використання стенографії

Розглянемо більш детально етичні аспекти використання прихованих каналів. Використання прихованих каналів, таких як стеганографія, виникає питання про баланс між правом на приватність та потребою забезпечення національної безпеки. З одного боку, технології прихованої комунікації можуть захищати приватні дані користувачів та забезпечувати безпечну комунікацію у складних умовах, таких як

репресивні режими чи зони конфлікту. З іншого боку, вони можуть бути використані для сховища злочинної діяльності, що ускладнює освідчення правоохоронних органів.

Розробники програмного забезпечення та користувачі мають етичну відповідальність щодо того, як використовуються приховані канали. Створення інструментів для стеганографії повинно супроводжуватися заходами, що запобігають їх використанню у злочинних цілях. Користувачі, в свою чергу, повинні усвідомлювати потенційні наслідки використання таких технологій та діяти відповідально.

Необхідно забезпечити прозорість у використанні схованих каналів, особливо в державних та корпоративних структурах. Цю мету можна досягти шляхом розробки етичних кодексів, внутрішніх політик та процедур контролю, які регулюють використання таких технологій. Прозорість сприяє уникненню зловживань та забезпечує довіру між користувачами та організаціями.

1.4. Виявлення та аналіз ключових аспектів проблеми

Ключовими аспектами проблеми приховування комунікаційних каналів є методи приховування, виявлення та їх знешкодження, застосування таких каналів, та загрози, які вони несуть (рисунок 1.6).

Виявлення схованих каналів може бути здійснене за допомогою статистичного аналізу мережового трафіку для виявлення аномалій, а також використання систем виявлення/запобігання вторгнень (IDS/IPS). Знешкодження включає нормалізацію трафіку, аудит, а також обмеження можливостей використання протоколів, які потенційно піддаються створенню схованих каналів. Що ж стосується самого процесу статистичного аналізу, то він включає в себе детальне дослідження пакетів даних, їх характеристик та поведінки. За допомогою різних алгоритмів та моделей аналітики даних, проводиться виявлення потенційно

підозрілих чи аномальних пакетів, які можуть свідчити про наявність схованих каналів. Після виявлення підозрілих пакетів, система IDS/IPS приймає відповідні заходи для блокування, заборони або реагування на ці потенційно небезпечні дії. Важливим етапом є також нормалізація трафіку, яка дозволяє виокремити аномалії вже на рівні потоку даних та виправити їх. Що стосується аудиту, то цей процес передбачає детальний аналіз журналів подій на серверах, щоб виявити порушення безпеки та несправності в мережевому трафіку. Тим самим, все це дозволяє забезпечити надійний та безпечний режим роботи мережі.

Рис. 1.6. Ключові аспекти проблеми

Приховані канали можуть використовуватися як зловмисниками для крадіжки даних і координації атак, так і системними адміністраторами для безпечної передачі інформації. Часто вони є частиною кіберзагроз, що ускладнює виявлення витоку інформації чи несанкціонованої активності. Поміж цим, приховані канали мають потенціал розширити можливості зловмисників і адміністраторів, для забезпечення ще більшої ефективності їхніх дій. Історично, розвиток кіберзлочинності надає можливість для появи нових методів та технологій у сфері прихованої комунікації. Кожен новий випадок виявлення

прихованих каналів приводить до розширення спектру захисних заходів та аналізу сучасних підходів у цій галузі. Застосування прихованих каналів стає все більш складною задачею, оскільки зловмисники впроваджують вдосконалені методи та алгоритми, щоб уникнути виявлення та ідентифікації. Тому, для забезпечення безпеки і протидії відповідним загрозам, необхідно постійно вдосконалювати методи і технології виявлення та захисту прихованих каналів.

1.5. Методологічні підходи до вивчення прихованих комунікаційних каналів

Вивчення та виявлення прихованих комунікаційних каналів потребує застосування різноманітних методологічних підходів для забезпечення глибокого та всебічного аналізу. Методологія дослідження визначає структуру, інструменти та методи, необхідні для досягнення поставлених цілей. У контексті цього дослідження важливо обрати такі підходи, які дозволяють ефективно виявляти, аналізувати та оцінювати характеристики та механізми функціонування прихованих каналів комунікації (рисунок 1.7).

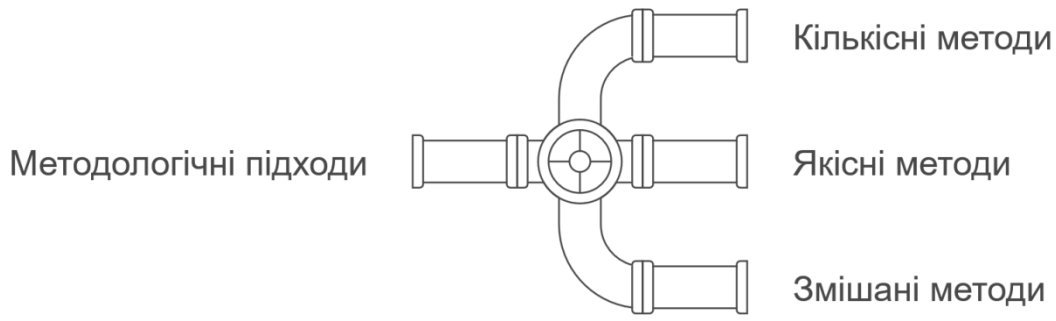

Рис. 1.7. Методичні підходи

Кількісні методи, такі як вимірювання трафіку, статистичне моделювання та експериментальні дослідження, зосереджуються на отриманні даних та їх статистичному аналізі. Вони надають можливість отримати об'єктивні та узагальнені висновки, виявити аномалії в передачі даних і передбачити потенційні шляхи на основі поведінкових характеристик мережі. З іншого боку, якісні методи, такі як кейс-стаді, контент-аналіз та інтерв'ю, зосереджуються на глибокому розумінні сутності та механізмів функціонування явищ шляхом детального аналізу контекстуальних даних та мотивацій учасників.

Змішані методи об'єднують якісний і кількісний підходи, що забезпечує комплексний аналіз вивченого явища. Наприклад, тривалі дослідження поєднують вимірювання з якісним аналізом для відстеження змін у використанні прихованих каналів з часом, а порівняльні аналізи використовують різні типи даних для оцінки ефективності методів виявлення в різних умовах. Крім традиційних соціальних методів, технічні методи, такі як аналіз мережевого трафіку, сигналізаційні системи та криптографічний аналіз, відіграють ключову роль у виявленні та нейтралізації прихованих каналів.

Вибір відповідної методології залежить від конкретних цілей та завдань дослідження, а також від доступних ресурсів та інструментів. Для ефективного вивчення прихованих комунікаційних каналів рекомендується використовувати комбінацію кількісних, якісних та технічних методів, що дозволяє забезпечити всебічний та глибокий аналіз досліджуваного явища. Такий підхід забезпечує більш повну картину механізмів функціонування прихованих каналів, їх впливу на комунікаційні системи та способів їх ефективного виявлення та нейтралізації.

Висновки до 1 розділу

У першому розділі було розглянуто теоретичні основи приховання комунікаційних каналів в інтерактивних застосунках. Приховані комунікаційні

канали є специфічними шляхами передачі інформації, які залишаються непомітними для звичайних методів безпеки. Вони можуть бути використані як для законних цілей захисту конфіденційної інформації, так і для злочинних дій, що підкреслює їхню двозначну природу. Було проаналізовано сутність та особливості цих каналів, зокрема використання стеганографії як методу приховування інформації. Історичний огляд показав, що методи приховання інформації мають глибокі корені та продовжують розвиватися з розвитком технологій. Сучасні приклади демонструють, як стеганографія та приховані канали можуть використовуватися як для забезпечення безпеки, так і для здійснення кіберзлочинів. Класифікація прихованих каналів за різними критеріями дозволяє глибше розуміти їхню природу та механізми дії. Розглянуто різні види та методи приховування, що допомагає в розробці ефективних стратегій їх виявлення та нейтралізації. Правові та етичні аспекти використання прихованих каналів були детально проаналізовані з точки зору українського законодавства. Питання балансу між правом на приватність та необхідністю забезпечення національної безпеки є особливо актуальним. Етичні міркування підкреслюють відповідальність розробників та користувачів у запобіганні зловживанням цими технологіями. Нарешті, визначено ключові аспекти проблеми та методологічні підходи до її вивчення. Використання комбінації кількісних, якісних та технічних методів дослідження є необхідним для всебічного аналізу прихованих комунікаційних каналів. Це сприяє розробці ефективних засобів їх виявлення та запобігання потенційним загрозам у сфері інформаційної безпеки.

2. МЕТОДИ ТА ЗАСОБИ СТВОРЕННЯ ПРИХОВАНИХ КОМУНІКАЦІЙ В ІНТЕРАКТИВНИХ ЗАСТОСУНКАХ

2.1. Методи та технології приховування інформації в інтерактивних застосунках

Методи та технології приховування інформації в інтерактивних застосунках включають в себе використання криптографії, стеганографії, а також різних методів обфускації даних [8] (рисунок 2.1). Криптографія дозволяє забезпечити конфіденційність та цілісність інформації шляхом застосування різних шифрувальних алгоритмів. Стеганографія полягає у приховуванні інформації у природних об'єктах, таких як зображення, звуки тощо. Одним із методів обфускації даних є змішування корисної інформації з непотрібною, або використання різних синтаксичних трансформацій для збентеження аналізаторів. Ці методи та технології допомагають створити невидимі та запобіжні комунікаційні канали в інтерактивних застосунках [9]. Криптографія забезпечує захист змісту даних, стеганографія приховує факт їх існування, а обфускація ускладнює аналіз та розуміння інформації.

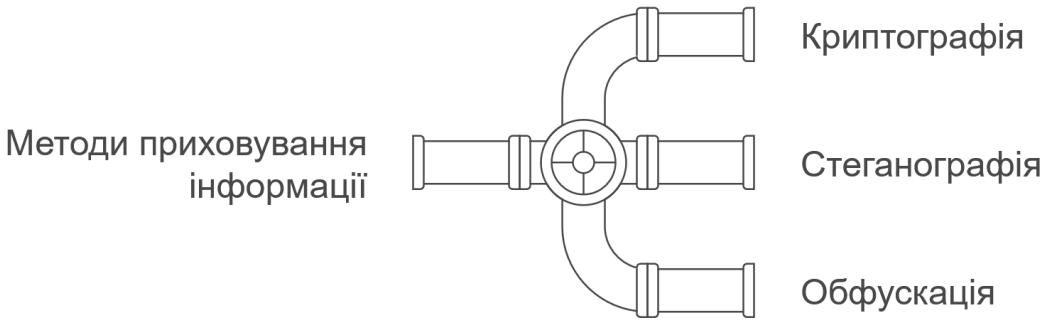

Рис. 2.1. Методи приховування інформації

Шифрування є важливим методом захисту інформації, що гарантує конфіденційність, цілісність та автентичність. Воно використовує алгоритми для перетворення відкритого тексту у зашифрований, що дозволяє забезпечити захист даних від несанкціонованого доступу. Існують симетричні алгоритми, які використовують один ключ для шифрування та дешифрування, такі як AES та DES, а також асиметричні алгоритми, що використовують пару ключів – публічний та приватний, наприклад, RSA та ECC (рисунок 2.2). Крім того, шифрування включає хеш-функції та цифрові підписи, які використовуються для перевірки цілісності даних та автентичності відправника.

Рис. 2.2. Методи шифрування

Симетричні методи шифрування є одними з найпоширеніших та найефективніших способів захисту повідомлень у сучасних інтерактивних застосунках. Однією з основних характеристик симетричних методів є використання одного й того ж ключа для шифрування та дешифрування даних. Це забезпечує високу швидкість обробки даних, що робить симетричні методи ідеальними для застосування в реальному часі, де важлива оперативність та ефективність обробки інформації. Один з найпопулярніших симетричних алгоритмів - це AES (Advanced Encryption Standard), що став стандартом США в 2001 р. AES підтримує різні розміри ключів (128, 192 і 256 біт), що дозволяє забезпечити різні рівні безпеки. Інший відомий алгоритм - DES (Data Encryption Standard), він вважається застарілим через менший розмір ключа (56 біт) та підвищену вразливість. Для подолання цих обмежень було розроблено більш

безпечні варіанти, такі як Triple DES (3DES), який використовує три окремі ключі для шифрування даних. Симетричні алгоритми шифрування забезпечують конфіденційність повідомлень, перетворюючи відкритий текст у зашифрований. Це особливо важливо в інтерактивних застосунках, де дані часто передаються через відкриті мережі, як Інтернет, де ризик перехоплення інформації є високим. Крім того, симетричні алгоритми можуть забезпечувати цілісність даних шляхом поєднання з криптографічними хеш-функціями або механізмами автентифікації.

Однією з ключових переваг симетричних алгоритмів є їхня висока ефективність у обробці значних обсягів даних. Завдяки простішій структурі та меншій кількості математичних операцій у порівнянні з асиметричними алгоритмами, симетричні методи можуть швидко шифрувати та дешифрувати дані, що є критично важливим для застосунків, які вимагають великої пропускної здатності та низької затримки. Однак, основним недоліком є проблема управління ключами: необхідно забезпечити безпечний обмін ключами між сторонами, що може бути складним завданням у великих або децентралізованих системах.

Асиметричні методи шифрування, відомі також як криптографія з відкритим ключем, є необхідною складовою сучасних систем інформаційної безпеки. У відміну від симетричних алгоритмів, які використовують один спільний ключ для шифрування та дешифрування даних, асиметричні методи базуються на парі ключів: публічному та приватному. Публічний ключ доступний для всіх та використовується для шифрування повідомлень, тоді як приватний ключ зберігається у власника в таємниці і використовується для їх розшифрування. Ця структура гарантує безпечний обмін інформацією, оскільки навіть якщо публічний ключ стає відомим, приватний ключ лишається захищеним від несанкціонованого доступу. Серед найпоширеніших асиметричних алгоритмів варто відзначити RSA (Rivest–Shamir–Adleman) та ECC (Elliptic Curve Cryptography). Алгоритм RSA базується на складності факторизації великих простих чисел, що робить його надзвичайно безпечним при використанні довгих ключів. ECC, натомість, використовує властивості еліптичних кривих для забезпечення високого рівня

безпеки при меншій довжині ключів у порівнянні з RSA, що робить його більш ефективним для застосування у мобільних пристроях та інших обмежених середовищах. Асиметричні методи шифрування широко використовуються в різних сферах інформаційної безпеки. Одним із ключових застосувань є забезпечення безпечної передачі даних через Інтернет, наприклад, у протоколах SSL/TLS, що забезпечують захищене з'єднання між веб-браузерами та серверами. Крім того, асиметрична криптографія використовується для створення цифрових підписів, які гарантують автентичність та цілісність повідомлень, а також для аутентифікації користувачів та серверів у різних системах.

Незважаючи на багато переваг, асиметричні методи мають свої обмеження. Основним недоліком є велика обчислювальна складність у порівнянні з симетричними алгоритмами, що може негативно вплинути на продуктивність систем, особливо при обробці великих обсягів даних. Крім того, управління ключами є критично важливим аспектом, оскільки пошкодження приватного ключа може призвести до повного порушення безпеки системи. Проте постійний розвиток технологій та оптимізація алгоритмів допомагають зменшити ці недоліки, роблячи асиметричні методи шифрування ще більш ефективними та надійними в сучасних умовах.

Стеганографія спрямована на те, щоб приховати існування інформації, зробивши сам факт передачі повідомлення непомітним для сторонніх спостерігачів. Основні методи стеганографії (рисунок 2.3) включають зміну найменш значущих бітів (LSB) в зображеннях або аудіофайлах, що дозволяє вбудовувати секретну інформацію без суттєвих змін у носії. Інші техніки, такі як частотні перетворення (DCT, перетворення Фур'є) та стеганографія в тексті, використовуються для більш стійкого приховування інформації, що ускладнює її виявлення навіть при аналізі частотних компонентів або синтаксичних структур.

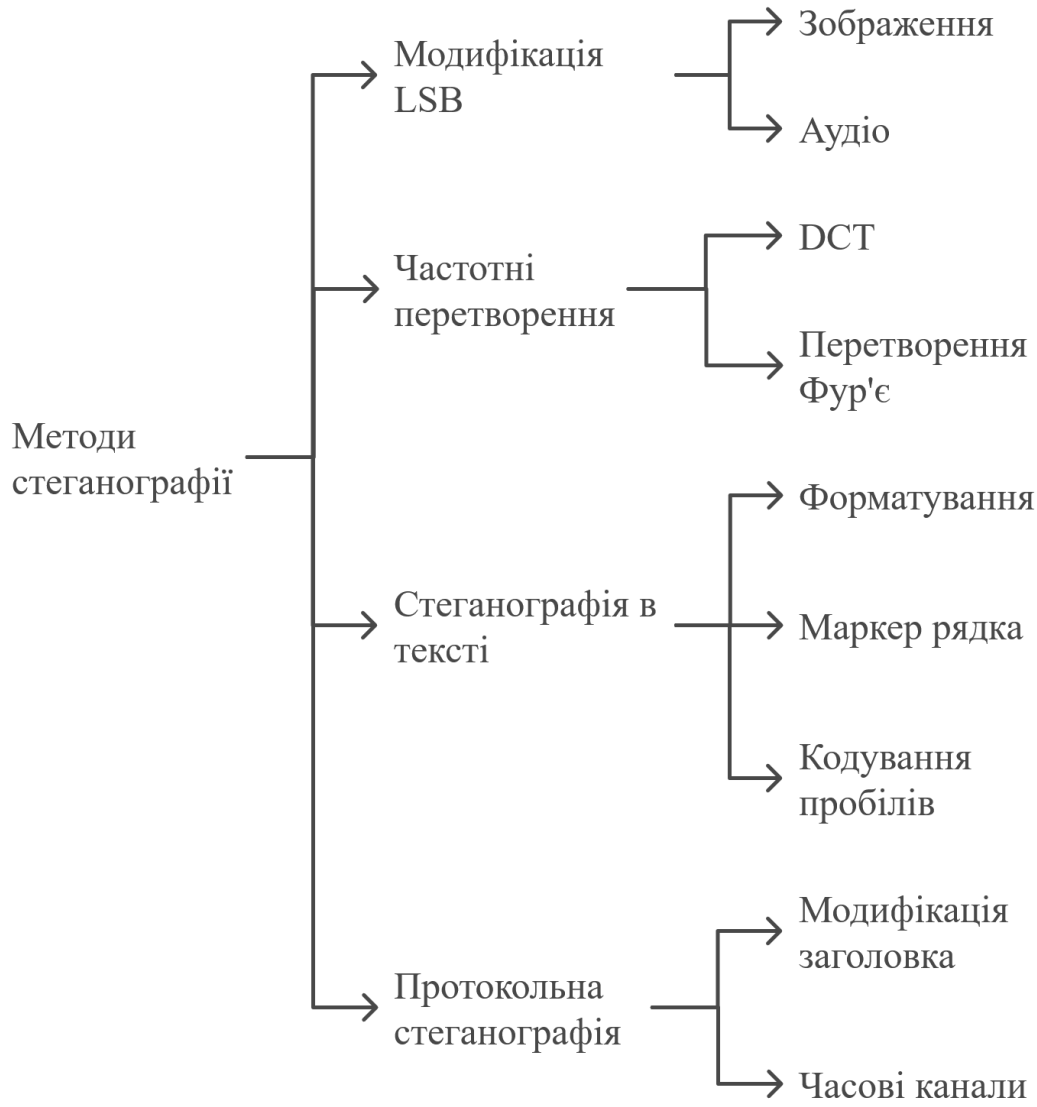

Рис. 2.3 Методи стеганографії

Метод зміни найменших значущих бітів (LSB) у зображеннях або аудіофайлах полягає у модифікації найменших значущих бітів пікселів зображень або бітів аудіоданих для вбудовування секретної інформації. Оскільки зміни відбуваються у бітовій структурі даних, вони є майже непомітними для людського ока та вуха. У зображеннях, наприклад, змінюючи останній біт кольорового компонента кожного пікселя, можна приховати великі обсяги даних без суттєвого впливу на якість зображення. Аналогічно, у аудіофайлах зміна LSB бітів дозволяє вбудовувати інформацію без помітних змін у звуковому потоці. Цей метод є

простим у реалізації та ефективним для приховування невеликих обсягів даних, проте його стійкість до компресії та інших перетворень може бути обмеженою.

Частотні перетворення, такі як DCT та перетворення Фур'є, є складнішими методами стеганографії, обирають зміни у частотному домені медіафайлів. Наприклад, DCT широко використовується у стисненні зображень та відео (наприклад, у форматі JPEG). У стеганографії DCT дозволяє вбудовувати інформацію у частотні компоненти, зроблює її більш стійкою до змін, таких як стиснення або фільтрація. Перетворення Фур'є також дозволяє розміщувати секретні дані у частотних компонентах аудіо та зображень, забезпечуючи високий рівень стійкості до змін носія. Ці методи забезпечують більшу невидимість та стійкість порівняно зі зміною LSB, але вимагають більше обчислювальної потужності та складності у реалізації.

У технічному контексті, текстова стеганографія - це варіант стеганографії, який використовує текстові елементи для схову даних. Це досягається шляхом внесення змін у розташування та кількість символів у тексті, що залишають його незмінним для людини та комп'ютера. Методи текстової стеганографії включають форматування тексту, зміну маркерів рядків, використання пробілів та зміну кодування пробілів. Ці підходи дозволяють приховати інформацію без значного впливу на зовнішній вигляд тексту, що ускладнює виявлення прихованих даних. На жаль, сучасні методи виявлення текстової стеганографії є практично не розвиненими, і дослідження, які проводяться, зосереджені на обмеженій кількості підходів. Більшість програм, які використовуються для текстової стеганографії, є вітчизняними розробками, зокрема ті, які використовують метод символів однакового зображення. Ці програми ефективно ховають інформацію, при цьому мінімізуючи вплив на читабельність тексту, та зручно використовуються в різних відомостях.

Стеганографія у протоколах зв'язку - це спосіб сховати інформацію безпосередньо у параметрах та структурах мережевих протоколів. Цей підхід включає в себе зміну заголовків пакетів, контрольних полів або навіть самих даних

для вбудовування секретних повідомлень, який не порушує основний функціонал передачі даних. Наприклад, у протоколі TCP/IP можна змінювати непомітні бітові поля заголовків пакетів для вбудовування інформації, яка залишиться непомітною для стандартних засобів моніторингу мережі. Інші техніки включають використання таймінгових каналів, де інформація кодується у варіаціях часових інтервалів між передачею пакетів або приховування даних у параметрах маршрутизації та аутентифікації. Ці методи дозволяють створювати приховані канали передачі даних, які важко виявити за допомогою традиційних засобів аналізу мережевого трафіку, що робить їх привабливими як для легітимного використання, так і для зловмисних дій. Стеганографія у протоколах підвищує рівень конфіденційності та безпеки комунікацій, але водночас створює нові виклики для фахівців з кібербезпеки, що повинні розробляти ефективні методи виявлення та протидії таким прихованим каналам.

Окрім зазначених вище методів, сучасні підходи до стеганографії включають використання більш складних технік, таких як 3D-стеганографія, яка дозволяє приховувати інформацію у тривимірних моделях або відео, створюючи більш складні та непомітні приховані канали.

Обфускація даних полягає у тому, щоб змішати корисну інформацію з непотрібною або неправдивою, а також у застосуванні різних синтаксичних трансформацій для ускладнення аналізу і розуміння даних. Методи обфускації (рисунок 2.4) включають синтаксичні трансформації, застосування хеш-функцій та шифрування, а також складні алгоритмічні зміни. Цей метод широко застосовується для приховування інформації в інтерактивних застосунках, де необхідно забезпечити не лише конфіденційність, але й складність розкриття самого факту існування прихованих даних. Обфускація ускладнює завдання аналізаторів та зловмисників, які намагаються виявити та розшифрувати приховані комунікаційні канали, використовуючи автоматизовані інструменти або ручні методи аналізу.

Основні методи обфускації включають змішування даних, синтаксичні трансформації, використання хеш-функцій та шифрування, а також застосування складних алгоритмічних змін. Наприклад, змішування даних може включати поєднання корисної інформації з додатковими шумовими даними, що ускладнює виділення секретного повідомлення. Синтаксичні трансформації, як-от зміна структури коду або розбиття логічних блоків, роблять аналіз коду більш складним і вимагають більше ресурсів, що ускладнює процес зворотного інжинірингу. Використання хеш-функцій та шифрування перетворює дані у форму, яка є непередбачуваною та важкою для розуміння без відповідних ключів або методів дешифрування.

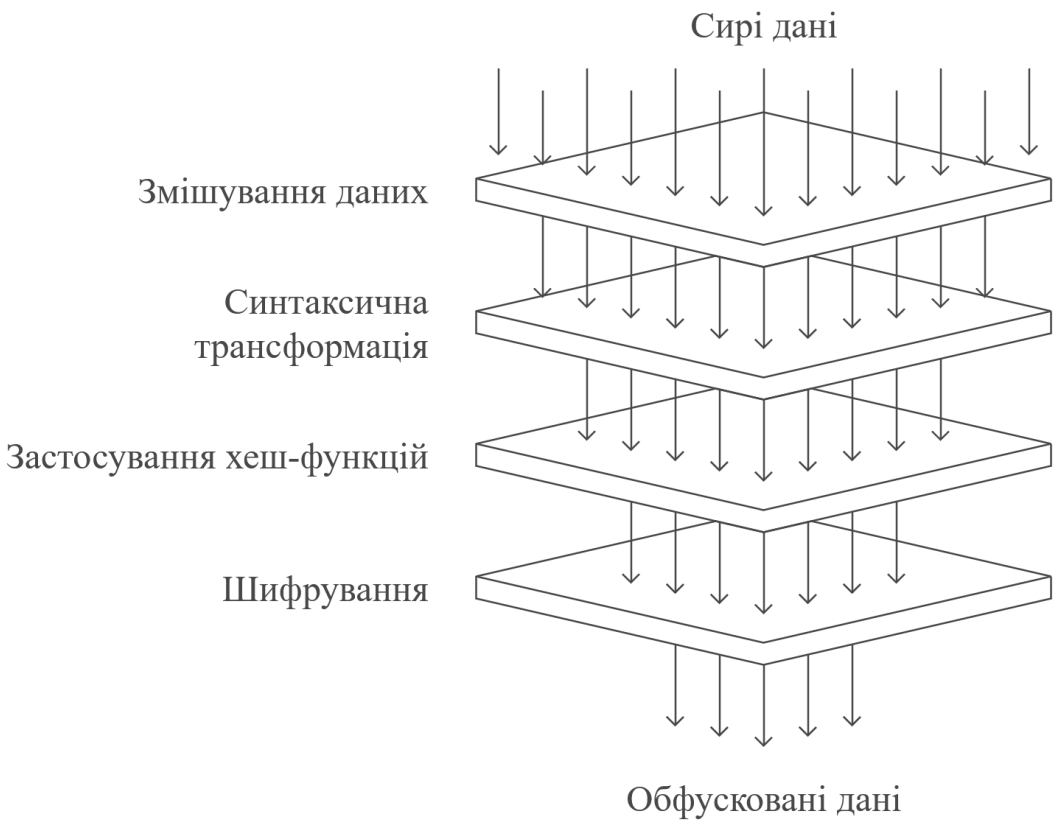

Рис. 2.4. Обфускація даних

Під час створення програмного забезпечення обфускація також використовується для захисту від зворотного інженірингу та аналізу коду. Це

особливо важливо для інтерактивних застосунків, де приховані канали можуть бути використані для передачі конфіденційної інформації або здійснення шкідливих дій. Обфусковані алгоритми та структури даних ускладнюють завдання аналітикам та розробникам систем безпеки, які намагаються виявити та нейтралізувати потенційні загрози. Таким чином, обфускація виступає як важливий інструмент у забезпеченні багаторівневого захисту інформації, доповнюючи стеганографічні методи та підвищуючи загальний рівень безпеки інтерактивних застосунків.

Кожен з методів замаскування інформації має свої переваги та обмеження. Криптографія забезпечує високий рівень захисту змісту даних, але не приховує факт їх існування. Стеганографія дозволяє сховати існування інформації, проте її ефективність залежить від вибору носія та методів стеганографії. Обфускація ускладнює аналіз даних, але не забезпечує прямого захисту конфіденційності. Комбінація цих методів дозволяє створювати більш ефективні засоби захисту інформації, забезпечуючи як конфіденційність, так і непомітність передачі даних. У майбутньому очікується подальший розвиток цих технологій, а також поява нових методів укриття інформації, що відповідатимуть зростаючим вимогам у сфері інформаційної безпеки.

2.2. Архітектура інтерактивного застосунку з прихованим комунікаційним каналом

Для демонстрації можливостей прихованого каналу було розроблено інтерактивний застосунок, який передбачав можливість шифрування та приховування інформації в процесі взаємодії користувачів з програмою. Для цього була використана спеціальна архітектура (рисунок 2.5), що дозволяла ефективно використовувати прихований канал в інтерактивному середовищі.

Для забезпечення безпеки та конфіденційності інформації, архітектура інтерактивного застосунку має включати ефективний механізм приховування комунікаційних каналів, що дозволить ефективно захищати дані від несанкціонованого доступу. Для цього можна використовувати алгоритми шифрування та стеганографії, які забезпечують надійний рівень захисту інформації. Також додатково потрібно захистити код програми від виявлення прихованих каналів комунікації за допомогою обфускації.

Рис 2.5. Основні компоненти архітектури додатку

Архітектура додатка повинна бути складена з двох основних частин: великого інтерактивного додатку і меншої частини з прихованим комунікаційним каналом. Основний інтерактивний додаток відповідає за потрібні функції та можливості, що використовуються користувачами. Він забезпечує зручний та інтуїтивно зрозумілий інтерфейс, де користувачі можуть взаємодіяти з додатком, виконувати різні завдання. Він необхідний для маскування активності комунікаційного каналу під звичайну активність інтерактивного додатка.

Частина з прихованим комунікаційним каналом є менш помітною та недоступною для звичайних користувачів. Вона призначена для забезпечення

конфіденційного обміну даними між користувачами. Цей комунікаційний канал повинен бути зашифрованим і прихованим від очей користувачів, які не повинні про нього знати, з метою забезпечення безпеки та недоступності для несанкціонованого доступу. Самі повідомлення, що будуть передаватись по цьому комунікаційному каналі також повинно бути зашифровано.

2.3. Реалізація інтерактивного застосунку з прихованим комунікаційним каналом

В якості інтерактивного застосунку було обрано гру, розроблену на Unity. Цей вибір має декілька переваг (рисунок 2.6):

1. Ігри часто передають великі обсяги даних у режимі реального часу, що дозволяє приховати значну кількість інформації без підозри на аномальну активність. Постійний обмін даними між клієнтом і сервером створює природний фон для маскування прихованих повідомлень.

2. Постійні зміни в ігровому середовищі створюють додатковий рівень шуму, який може маскувати закодовану інформацію, ускладнюючи її виявлення. Рухи гравців, зміни стану гри та взаємодія з об'єктами забезпечують безперервний потік даних, в якому можна вбудовувати приховані повідомлення.

3. У іграх використовуються різноманітні види даних та протоколів для обміну інформацією між клієнтом і сервером. Це дозволяє використовувати одночасно кілька каналів для захисту інформації від викриття. Наприклад, можна поєднувати приховування даних в графічних елементах з використанням таймінгових каналів у мережевих пакетах.

4. Інтерактивні аспекти гри, такі як чат, спільні місії або гра у кооперативному режимі, відкривають додаткові можливості для прихованого обміну повідомленнями серед гравців. Це дає змогу використовувати текстові або аудіо повідомлення для передачі конфіденційної інформації без ризику викриття.

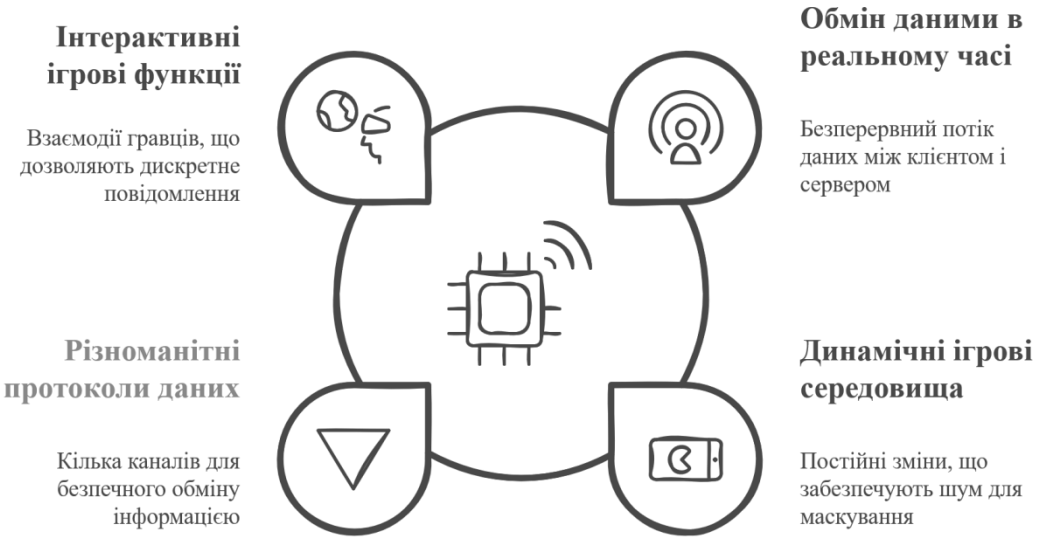

Рис. 2.6 Переваги використання ігор для приховування комунікаційних каналів

Ці переваги роблять ігри ідеальним середовищем для створення прихованих комунікаційних каналів, забезпечуючи високий рівень непомітності та ефективності передачі секретних даних. Використання різноманітних методів приховування в інтерактивних застосунках, таких як ігри, сприяє підвищенню рівня безпеки інформації та захисту від несанкціонованого доступу.

Для розробки інтерактивного застосунку використовується Unity через те, що ця платформа пропонує потужні інструменти для розробки як 2D, так і 3D ігор, забезпечуючи високу якість графіки та реалістичну фізику. Unity підтримує кросплатформену розробку, що дозволяє запускати застосунок на різних пристроях та операційних системах, таких як Windows, macOS, Android, iOS та інших, розширюючи тим самим потенційну аудиторію користувачів. Крім того, Unity має велику та активну спільноту розробників, що надає доступ до численних ресурсів, плагінів та бібліотек, які спрощують інтеграцію складних методів приховування інформації, таких як стеганографія та криптографія. Система зручного візуального редактора та підтримка скриптування на мові C# дозволяють швидко прототипувати та впроваджувати нові функції, що є критично важливим для створення ефективних прихованих комунікаційних каналів. Додатково, Unity

забезпечує можливості для детального аналізу та оптимізації продуктивності застосунку, що сприяє забезпеченню стабільної роботи та високої безпеки інформаційних систем. Таким чином, вибір Unity як платформи для розробки інтерактивного застосунку дозволяє ефективно реалізувати складні механізми приховування інформації, забезпечуючи водночас високу якість користувацького досвіду та гнучкість у розробці (рисунок 2.7).

Рис. 2.7. Unity для інтерактивних застосунків

Unity була розроблена компанією Unity Technologies і вперше випущена у 2005 році як інструмент для створення тривимірних ігор на платформі Mac OS X. Завдяки своєму інтуїтивно зрозумілому інтерфейсу та можливості кросплатформенної розробки, Unity швидко здобула популярність серед розробників як інді-ігор, так і великих студій. З часом платформа розширила підтримку численних операційних систем і пристроїв, включаючи Windows, мобільні платформи (iOS та Android), консолі, а також віртуальну та доповнену реальність. Випуски Unity 3D та Unity 5 принесли значні покращення в графіці, фізиці та інструментах розробки, що ще більше закріпило її позиції на ринку.

Сьогодні Unity є однією з найпоширеніших платформ для розробки інтерактивних застосунків, ігор, симуляцій та віртуальних середовищ, забезпечуючи розробникам потужні можливості для створення високоякісного контенту.

Реалізація програмного прихованого комунікаційного каналу також буде розроблена на мові програмування C# і вбудована в інтерактивний додаток. Надійність та ефективність реалізації на мові програмування C# гарантує стабільну роботу додатка та його високу продуктивність.

Для забезпечення приховування каналу у інтерактивному застосунку саме повідомлення буде шифруватись симетричним алгоритмом Triple DES для спрощення реалізації, а доступ до каналу буде надаватись тільки користувачам, які виконають певні дії у інтерактивному застосунку. До таких дій може належати натискання специфічного поєднання клавіш, певна послідовність дій, перебування або виконання дій у певній області (зоні на карті), або інші специфічні дії і події, які не можуть бути випадково виконані користувачем, який не знає про існування прихованого комунікаційного каналу.

Сама гра (рисунок 2.8) представляє собою 2D платформер, що дозволяє реалізувати відкриття прихованого комунікаційного каналу при виконанні специфічних дій у певній області. Також плюсом є те, що в грі є кооператив, що як писалось вище, відкриває можливості для додаткових прихованих каналів комунікації. Для спрощення прихований комунікаційний канал буде відкриватись тільки у кооперативному режимі спеціальною комбінацією клавіш, але варіантів умов відкриття доступу до прихованого комунікаційного каналу є безлічь. Вікно, що відкривається від цієї дії передає повідомлення через прихований комунікаційний канал від одного користувача до іншого.

Рис. 2.8. Інтерактивний застосунок

Висновки до 2 розділу

У цьому розділі були описані методи створення схованих комунікаційних каналів у інтерактивному застосунку. Використання криптографії, стеганографії та обфускації забезпечує багаторівневий захист інформації. Криптографія гарантує конфіденційність і цілісність даних, стеганографія приховує факт передачі інформації, а обфускація ускладнює виявлення схованих каналів. Симетричний алгоритм шифрування Triple DES, забезпечує швидкість та ефективність. Сучасні методи стеганографії (LSB, DCT, текстові або мережеві канали) дозволяють впроваджувати дані у мультимедійні файли чи протоколи, створюючи стійкі та непомітні комунікаційні канали.

Для демонстрації прихованого каналу був створений інтерактивний застосунок на ігровому рушії Unity. Гра у форматі 2D платформера забезпечує маскування прихованого каналу серед звичайних дій користувачів. Використання

конкретних умов для активації каналу (наприклад, спеціальна послідовність клавіш) дозволяє обмежити доступ лише для тих, хто має знання про його існування. Впровадження шифрування за допомогою Triple DES забезпечує безпеку передачі повідомлень, інтерактивне середовище гри з постійним обміном даними створює природний фон для прихованої комунікації. Таким чином, впровадження прихованих каналів у ігри виявляється ефективним рішенням для забезпечення безпеки даних та непомітного обміну інформацією.

3. ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ПРИХОВАНОГО КОМУНІКАЦІЙНОГО КАНАЛУ В ІНТЕРАКТИВНОМУ ЗАСТОСУНКУ

3.1. Тестування інтерактивного застосунку з прихованим комунікаційним каналом

Тестування інтерактивного застосунку з прихованим комунікаційним каналом – це процес перевірки функціональності та ефективності прихованого каналу у програмному забезпеченні. Під час тестування проводиться набір тестових сценаріїв для виявлення, чи успішно функціонує прихований комунікаційний канал, а також для оцінки можливостей виявлення цього каналу з боку користувача. Проведення тестування дозволяє оцінити рівень захищеності застосунку від небажаної комунікації та виявлення можливих вразливостей.

Розглянемо детальніше прихований канал. Цей канал забезпечує можливість комунікації через чат, що відбувається паралельно з активністю застосунка (рисунок 3.1). Приховані повідомлення шифруються та передаються разом зі звичайними пакетами, що синхронізуються з активністю користувачів. Така система дозволяє зберігати конфіденційність та безпеку комунікації, адже інформація залишається непомітною для сторонніх осіб. Прихований канал є надійним і унікальним способом обміну шифрованими повідомленнями, що забезпечує додатковий рівень захисту для користувачів.

Доступ до каналу можливий тільки при натисканні специфічної комбінації клавіш. Ця комбінація клавіш включає натискання двох спеціальних клавіш одночасно. Така специфічна комбінація клавіш забезпечує високий рівень безпеки та захисту даних. Використовуючи цей метод доступу, можна запобігти несанкціонованому доступу до каналу і зберегти конфіденційність інформації. Комбінація клавіш може бути змінена в будь-який час для додаткової безпеки. Розглянемо як можна виявити цей прихований канал (рисунок 3.2).

Рис 3.1. Інтерфейс інтерактивного додатку з прихованим комунікаційним каналом

Формальний аналіз способів передачі даних є важливим елементом виявлення схованих каналів. Цей підхід передбачає моделювання всіх можливих шляхів, через які інформація може передаватися між різними компонентами системи. З використанням таких моделей, як графи залежностей або потокові діаграми, можна визначити місця можливого виникнення каналів, які не були передбачені при проектуванні системи. Практичне втілення аналізу включає використання спеціалізованих інструментів та технік для моніторингу та моделювання потоків даних. Це може бути зроблено за допомогою застосування статичних аналізаторів коду, які вивчають взаємодії між різними модулями програми, або динамічних інструментів моніторингу, які відстежують реальний рух даних під час роботи системи. Для нашого випадку цей метод не підходить тому, що код інтерактивного затосунку і прихованого каналу комунікацій пройшов

обфускацію і його дослідження стало максимально важким і займе занадто багато часу.

Рис. 3.2. Методи виявлення прихованих каналів зв’язку

Вивчення мережевого трафіку є одним з найефективніших методів для виявлення прихованих каналів, особливо в великих мережевих середовищах. Цей підхід передбачає збір і ретельний аналіз усіх даних, що передаються через мережу, з метою виявлення нетипових патернів або аномалій, які можуть вказувати на наявність прихованої комунікації. Наприклад, нестандартні розміри пакетів, незвичайно висока частота передачі даних або незвичні протоколи можуть вказувати на використання прихованого каналу. Технічні аспекти аналізу трафіку включають використання інструментів для моніторингу мережі, таких як Wireshark, tcpdump або спеціалізовані системи виявлення злому (IDS). Крім того, використання методів машинного навчання може підвищити ефективність аналізу, дозволяючи автоматично ідентифікувати складні патерни, які важко виявити за допомогою традиційних методів. Цей метод може визначити факт передачі

інформації через прихований комунікаційний канал за допомогою порівняння розмірів пакетів звичайної активності з підозрілими. Але це може бути ускладнено через те, що ігри можуть відправляти різні пакети з різними інтервалами для оновлення наприклад стану ігрового оточення і через це буде важко відслідкувати факт передачі повідомлення через прихований комунікаційний канал.

Слідкування за використанням системних ресурсів полягає у постійному спостереженні за завантаженістю процесора, використанням пам'яті, дискового простору та інших ключових ресурсів системи. Цей метод допомагає виявляти незвичайні зміни або піки споживання ресурсів, які можуть бути ознакою активної роботи прихованого каналу. Наприклад, якщо певний процес несподівано споживає більше оперативної пам'яті або процесорного часу, це може вказувати на те, що він використовується для передачі даних через прихований канал. Інструменти для моніторингу включають системні монітори, такі як Nagios, Zabbix або системні утиліти (наприклад, Task Manager в Windows або top/htop в Unix-подібних системах). Вони дозволяють адміністратору в режимі реального часу відстежувати використання ресурсів та налаштовувати оповіщення на випадок досягнення певних порогів. Крім того, аналіз історичних даних про використання ресурсів може допомогти виявити довготривалі тенденції або періоди аномальної активності, що не були помічені під час оперативного моніторингу. Цей підхід не призведе до розкриття схованого комунікаційного каналу у взаємодії з інтерактивним додатком, якщо цей додаток має доступ до мережі (наприклад, у випадку кооперативної гри), оскільки це можна пояснити звичайною активністю в грі.

Таймінг-аналітика фокусується на виявленні змін у часі виконання операцій, які можуть бути використані для передачі інформації через приховані канали. Цей підхід ґрунтується на тому, що відхилення у затримках або тривалості виконання певних дій можуть бути інтерпретовані як спосіб кодування даних. Наприклад, зміни у часі відповіді серверів на запити можуть бути використані для передачі бітів інформації між сторонами, які мають доступ до системи. Практичне

застосування аналітики часових параметрів полягає використання високоточних часових вимірювань та статистичних методів для аналізу часу виконання операцій. Інструменти для цього можуть включати профайлери коду, таймери та спеціалізоване програмне забезпечення для вимірювання затримок. Аналіз може включати порівняння очікуваних часів виконання з фактичними, виявлення аномалій або використання методів кореляції для ідентифікації потенційних каналів передачі даних. Крім того, цей метод може поєднуватися з іншими техніками аналізу, такими як аналіз трафіку або розпізнавання патернів, для підвищення точності виявлення. Аналіз часу дозволяє виявити приховані комунікаційні канали. Динамічні середовища інтерактивних застосунків можуть розкрити нетипову поведінку. Його ефективність залежить від точності вимірювань та відокремлення нормальних коливань. Атаки можуть використовувати різні методи маскування, що ускладнює їх виявлення. Краще комбінувати з іншими методами безпеки для більш комплексного підходу до захисту.

3.2. Виявлені проблеми і обмеження

Під час тестування інтерактивного застосунку з прихованим комунікаційним каналом було виявлено декілька проблем і обмежень. Зокрема, виникла складність у виявленні деяких типів прихованих комунікаційних каналів через їх високу ступінь прихованості. Також, обмеження стосувалося швидкості виявлення та низької точності результатів тестування (рисунок 3.3). Ці проблеми можуть ускладнити виявлення прихованих каналів у реальних умовах використання.

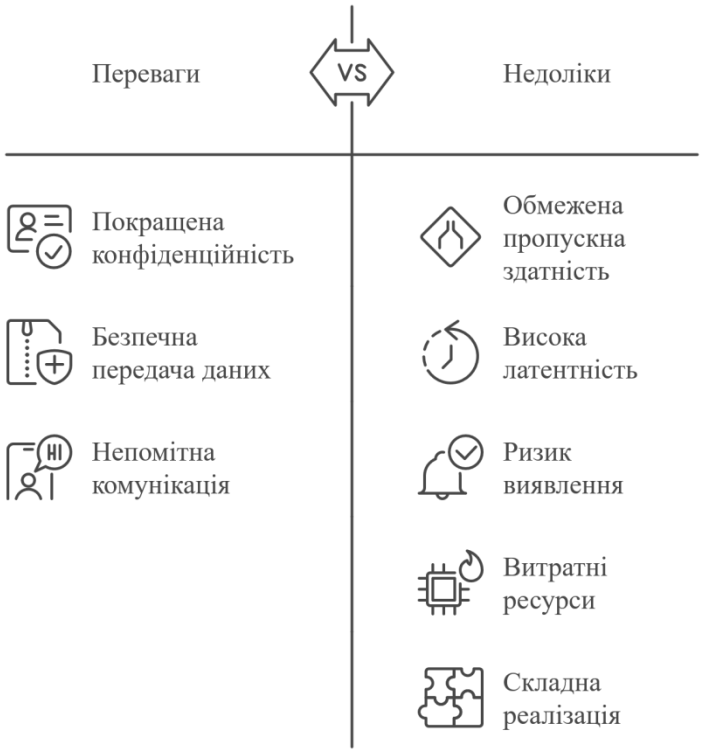

Рис. 3.3. Переваги і недоліки приховування комунікаційних каналів в інтерактивних застосунках

Виявлені проблеми і обмеження можна розділити на 2 групи: проблеми і обмеження для користувачів прихованого каналу і проблеми безпеки прихованих комунікаційних каналів. Розглянемо їх по черзі.

До проблем і обмежень для користувачів прихованого каналу відносяться обмежена пропускна здатність, висока латентність, ризик виявлення і обмеження ресурсів системи (рисунок 3.4).

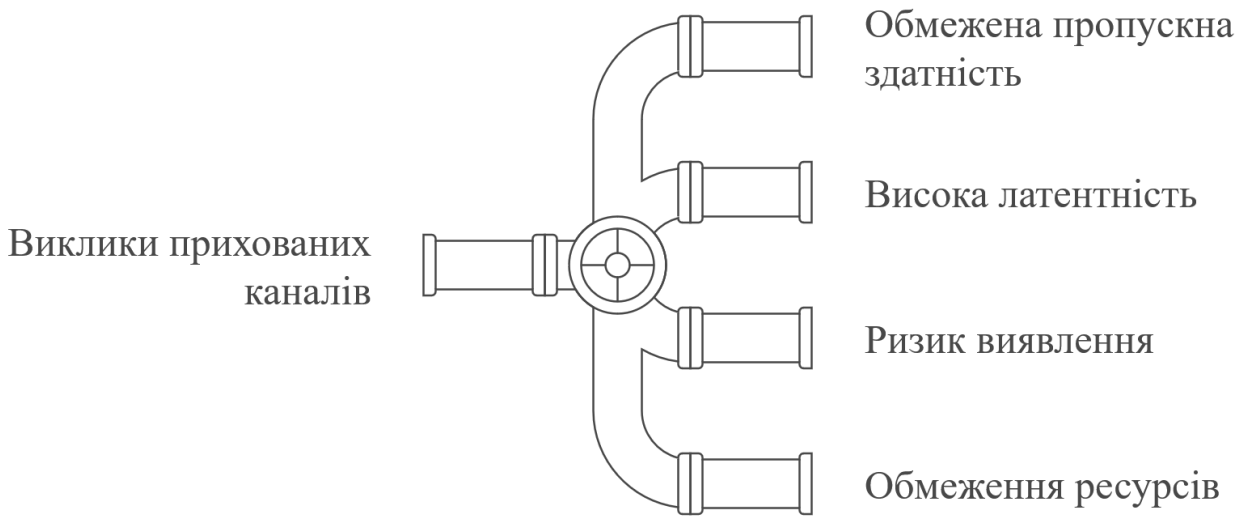

Рис. 3.4. Виклики прихованих каналів для користувачів

Обмежена швидкість передачі даних - це одна з ключових проблем, яка виникає при використанні прихованих каналів. Зазвичай такі канали надають набагато меншу швидкість передачі даних у порівнянні з традиційними комунікаційними засобами. Це обумовлено необхідністю маскування переданої інформації таким чином, щоб вона залишалася непомітною для систем безпеки. Наприклад, використання невеликих змін у трафіку або ресурсах системи для передачі бітів інформації суттєво обмежує кількість даних, які можна передати за певний проміжок часу. Ця обмеженість робить приховані канали непридатними для передачі великих обсягів інформації або для застосувань, що потребують високої швидкості обміну даними. Наприклад, передача мультимедійних файлів, потокового відео або великих баз даних через прихований канал може бути дуже повільною і нездійсненною через низьку пропускну здатність. Таким чином, користувачі повинні ретельно оцінювати необхідність використання таких каналів, враховуючи їх обмеження та специфічні вимоги до швидкості передачі даних.

Висока латентність є ще одним серйозним обмеженням для користувачів прихованих каналів. Латентність відноситься до затримок у передачі даних, які можуть бути спричинені різними факторами, включаючи обробку інформації для

маскування та декодування. У випадку інтерактивних застосунків, де важлива швидкість реакції системи, висока латентність може значно погіршити користувацький досвід. Наприклад, у онлайн-іграх або системах реального часу навіть незначні затримки можуть призвести до невідповідної поведінки застосунків або збоїв у комунікації між користувачами. Крім того, висока латентність може ускладнити синхронізацію даних між сторонами, що використовують прихований канал. Це особливо актуально для застосувань, де потрібна точна координація дій, наприклад, у фінансових транзакціях або управлінні критичними системами. Внаслідок цього, користувачі можуть бути змушені балансувати між необхідністю маскування каналу та вимогами до швидкості та ефективності комунікації, що ускладнює використання прихованих каналів у багатьох сценаріях.

Загроза виявлення є однією з найбільших загроз для користувачів прихованих каналів. Сучасні системи безпеки використовують різноманітні методи для моніторингу та аналізу діяльності в системі, що дозволяє виявляти аномалії та підозрілу активність. Використання прихованих каналів може привернути увагу адміністраторів системи або антивірусного програмного забезпечення, що може призвести до блокування доступу або інших санкцій. Наприклад, несподіване збільшення використання мережевих ресурсів або системних ресурсів може бути інтерпретовано як ознака шкідливої діяльності. Крім того, виявлення прихованих каналів може мати серйозні наслідки для користувачів, включаючи втрату доступу до системи, юридичні санкції або навіть кримінальну відповідальність, якщо використання такого каналу порушує законодавство або політики безпеки організації. Таким чином, ризик виявлення змушує користувачів бути обережними та ретельно оцінювати потенційні наслідки перед використанням прихованих каналів, а також сприяє розвитку більш складних методів маскування, що ускладнює їхнє виявлення.

Обмеження ресурсів системи можуть значно вплинути на ефективність використання прихованих каналів. Для маскування та передачі інформації через приховані канали часто потрібні додаткові ресурси, такі як процесорний час,

оперативна пам'ять або дисковий простір. Це може призвести до збільшеного навантаження на систему, що в свою чергу може негативно вплинути на її загальну продуктивність та стабільність. Наприклад, додаткові процеси, які використовуються для маскування даних, можуть збільшити використання CPU, що може бути критичним у системах з обмеженими ресурсами, таких як мобільні пристрої або вбудовані системи. Крім того, використання ресурсів системи для підтримки прихованого каналу може призвести до конкуренції між легітимними процесами та тим самим каналом, що може викликати затримки або навіть збої в роботі інших застосунків. Це особливо актуально в середовищах з високою концентрацією користувачів або обмеженими ресурсами, де кожне додаткове навантаження може мати суттєвий вплив на загальну продуктивність системи. Таким чином, користувачі повинні враховувати можливий вплив на ресурси системи та забезпечувати баланс між використанням прихованих каналів та підтримкою нормальної роботи системи.

Далі розглянемо проблеми безпеки прихованих комунікаційних каналів з точки зору їх виявлення (рисунок 3.5). Виходячи з вищенаписаного, можна виділити кілька ключових аспектів, що ускладнюють ефективне виявлення таких каналів та створюють значні виклики для забезпечення безпеки інформаційних систем, а саме обфускація, маскування під звичайну активність мережі, нормалізація використання системних ресурсів і використання методів маскування у таймінг-аналітиці.

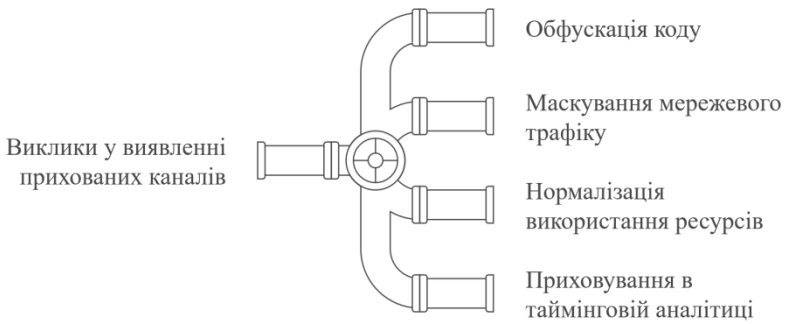

Рис. 3.5. Виклики у виявленні прихованих каналів

Однією з головних проблем є затемнення коду інтерактивного застосунку та прихованого каналу комунікацій. Затемнення ускладнює процес формального аналізу шляхів передачі даних, оскільки робить код важкодоступним для розуміння та дослідження. Це призводить до того, що традиційні методи статичного аналізу стають неефективними або потребують значно більше часу та ресурсів для виявлення потенційних каналів. В результаті, приховані канали можуть залишатися непоміченими навіть при ретельному аналізі системи, що підвищує ризик їх використання для несанкціонованої комунікації.

Інтерактивні застосунки часто виробляють велику кількість мережевого трафіку, який показує звичайну активність користувачів, таку як оновлення стану ігрового середовища або обмін даними між клієнтом та сервером. Приховані канали, які використовують схожі зразки передачі даних (наприклад, змінні розміри пакетів або різні інтервали відправки), можуть добре маскуватися під цю звичайну активність. Це значно ускладнює процес аналізу трафіку, оскільки необхідно розрізняти легітимний трафік від підозрілих зразків, які використовуються для передачі схованих повідомлень. Внаслідок цього ризик пропуску прихованого каналу зростає, особливо у великих та динамічних мережевих середовищах.

Приховані канали можуть бути розроблені з метою збереження нормального рівня використання ресурсів системи, таких як процесорний час, оперативна пам'ять або дисковий простір. Це означає, що під час моніторингу системних ресурсів може не бути помітних відхилень, які вказували б на активність прихованого каналу. Наприклад, якщо процес, який використовується для передачі прихованих даних, не перевищує нормальне споживання ресурсів, адміністратори системи можуть не виявити його діяльність через стандартний моніторинг ресурсів. Це створює додаткові ускладнення для ефективного виявлення прихованих каналів за допомогою методів моніторингу ресурсів.

Аналітика, спрямована на виявлення змін у часі виконання операцій, може бути корисною для виявлення схованих каналів. Проте, атаки можуть

використовувати різні методи замаскування часу, як-от додавання випадкових затримок або розподіл передачі даних у вигляді нерегулярних інтервалів. Це ускладнює розрізнення між звичайними коливаннями часу виконання операцій та тими, які використовуються для передачі схованих повідомлень. Висока точність вимірювань та складність аналізу часових параметрів можуть призвести до низької ефективності такої аналітики, особливо в умовах високої динаміки та різноманітності виконання операцій.

Для ефективного виявлення прихованих каналів часто необхідно використовувати комбінацію різних методів аналізу, таких як аналіз трафіку, моніторинг ресурсів та таймінг-аналітика. Однак, навіть при такому підході, складність та різноманітність методів маскування, що використовуються атакуючими, можуть значно ускладнити процес виявлення. Наприклад, якщо прихований канал інтегрується з декількома методами маскування, такими як обфускація трафіку та нормалізація використання ресурсів, це може зробити його практично непомітним для традиційних засобів захисту та моніторингу. Це вказує на необхідність постійного вдосконалення методів виявлення та розробки нових алгоритмів, здатних ефективно впоратися зі зростаючими загрозами маскування.

3.3. Розробка рекомендацій щодо виявлення комунікаційних каналів в інтерактивних застосунках

Виявлення та аналіз прихованих комунікаційних каналів у інтерактивних застосунках зустрічається зі значними труднощами з точки зору безпеки (рисунок 3.6), що виникають внаслідок складності аналізу коду, приховування під звичайну активність, нормалізації використання ресурсів та використання методів маскування в таймінг-аналітиці. Ці аспекти представляють серйозні виклики для професіоналів у галузі безпеки, оскільки традиційні методи виявлення можуть бути неефективними або вимагати великих ресурсів для аналізу. Для подолання цих

проблем необхідно розробляти більш продумані та поєднані підходи до моніторингу та аналізу систем, а також постійно удосконалювати засоби захисту для адаптації до нових методів прихованої комунікації.

Рис. 3.6. Виклики у виявленні прихованих комунікаційних каналів

Використання інструментів для аналізу мережевого трафіку є важливою частиною процесу виявлення прихованих каналів. Програми, такі як Wireshark, tcpdump та системи виявлення вторгнень (IDS), дозволяють реєструвати та детально досліджувати пакети даних, які проходять через мережу. Налаштування моніторингу мережевого трафіку для збору всіх пакетів та застосування фільтрів для виділення підозрілих пакетів за різними параметрами є важливими етапами. Використання методів машинного навчання для автоматичного виявлення нетипових патернів трафіку може значно підвищити ефективність цього процесу. Таймінг-аналіз дозволяє виявити зміни у часі виконання операцій, які можуть використовувати для передачі інформації через приховані канали. Використання високоточних таймерів та профайлерів для вимірювання часу виконання ключових операцій сприяє порівнянню фактичних затримок з очікуваними значеннями та

виявленню аномалій. Використання статистичних методів та кореляційного аналізу допомагає ідентифікувати потенційні сигнали прихованих каналів, особливо коли ці зміни відрізняються від звичайних коливань у виконанні операцій.

Спостереження за використанням системних ресурсів є важливою складовою виявлення прихованих каналів. Постійний контроль завантаженості процесора, використання пам'яті, дискового простору та інших ключових ресурсів системи дозволяє виявити незвичайні зміни або піки споживання ресурсів, які можуть свідчити про активність прихованого каналу. Використання системних моніторів, таких як Nagios, Zabbix або утиліти Task Manager в Windows та top/htop в Unix-подібних системах, дозволяє адміністратору відстежувати використання ресурсів в реальному часі та налаштовувати оповіщення на випадок досягнення певних порогів. Використання методу розпізнавання патернів допомагає ідентифікувати специфічні структури або послідовності даних, характерні для прихованих каналів. Алгоритми розпізнавання патернів, включаючи регулярні вирази, фільтри та машинне навчання, дозволяють виявляти відомі сигнатури методів прихованої передачі даних. Розробка або використання наявних баз сигнатур, а також застосування алгоритмів машинного навчання для виявлення нових або модифікованих патернів, є ключовими кроками для підвищення точності виявлення прихованих каналів.

Проведення статичного та динамічного аналізу коду дозволяє докладно вивчити застосунок на наявність потенційних каналів передачі даних. Статичний аналіз коду включає використання аналізаторів коду для виявлення неправильних взаємодій між модулями або невідповідних викликів функцій, тоді як динамічний аналіз полягає у моніторингу поведінки застосунку під час його виконання. Врахування обфускації коду та використання спеціалізованих технік для її декодування допомагає подолати труднощі, пов'язані з ускладненням аналізу коду, та ефективніше виявляти приховані канали. Регулярний аудит та оновлення політик безпеки є важливими заходами для забезпечення відповідності сучасним стандартам безпеки та швидкої реакції на нові загрози. Регулярний аудит

системних логів дозволяє виявляти підозрілу активність, а оновлення політик безпеки відповідно до нових загроз та виявлених вразливостей забезпечує постійну актуальність заходів захисту. Впровадження автоматизованих систем логування та моніторингу допомагає зменшити людські помилки та підвищити швидкість виявлення загроз, забезпечуючи більш ефективний контроль за безпекою інформаційних систем.

Використання штучного інтелекту та машинного навчання може істотно покращити процес виявлення прихованих каналів завдяки здатності аналізувати великі обсяги даних та виявляти складні патерни. Тренування моделей машинного навчання на великих наборах даних, що містять як нормальні, так і підозрілі патерни діяльності, дозволяє використовувати нейронні мережі або інші передові алгоритми для виявлення аномалій, що можуть свідчити про приховані канали. Постійне оновлення та вдосконалення моделей на основі нових даних та відгуків забезпечує підтримку високої точності виявлення, адаптуючись до нових методів маскування та атакуючих технік.

Однією з головних переваг використання ШІ в виявленні прихованих каналів є автоматизація та швидкість аналізу. ШІ-моделі можуть обробляти великі обсяги даних у режимі реального часу, що дозволяє швидко ідентифікувати потенційні загрози та реагувати на них. Це особливо важливо у середовищах з високою динамікою, таких як інтерактивні додатки та онлайн-ігри, де затримки у виявленні можуть призвести до серйозних наслідків. Крім того, ШІ здатен постійно вдосконалюватися через процес навчання, що дозволяє моделям адаптуватися до нових методів маскування та атакуючих технік, забезпечуючи більш ефективний захист від прихованих каналів. Ще одна суттєва перевага полягає в здатності ШІ до виявлення невідомих загроз. Традиційні методи, які базуються на сигнатурах або конкретних правилах, можуть бути обхідними для нових або модифікованих прихованих каналів. ШІ-моделі, навчені на різних даних, можуть розпізнавати аномалії, які не відповідають відомим сигнатурам, тим самим забезпечуючи більш гнучкий та всеохопний підхід до безпеки. Наприклад, аномалійне виявлення за

допомогою ШІ може ідентифікувати нетипові патерни використання ресурсів або трафіку, що можуть вказувати на присутність прихованого каналу, навіть якщо конкретний метод його маскування ще не відомий.

Незважаючи на ряд переваг, використання штучних інтелектуальних систем (ШІ) та машинного навчання для виявлення прихованих каналів супроводжується певними викликами та обмеженнями. Одним з основних обмежень є необхідність великої кількості даних. Для успішного навчання моделей ШІ потрібні великі обсяги якісних даних, які включають як нормальні, так і підозрілі патерни активності. Збір таких даних може бути складним та вимагати великих витрат ресурсів, особливо у специфічних середовищах, де приховані канали використовуються рідко або їх активність обмежена. Крім того, ризик помилкових спрацьовувань - ще одне суттєве обмеження. Моделі ШІ можуть помилково класифікувати легітимну активність як підозрілу, що може призвести до зайвих попереджень та потенційно знизити ефективність системи безпеки через перевантаження адміністраторів. Це особливо актуально у великих та динамічних системах, де великі обсяги даних можуть створювати багато шуму та ускладнювати процес точного виявлення загроз. Для зменшення кількості помилок необхідно ретельно налаштовувати та оптимізувати моделі, що потребує значних зусиль та експертних знань.

У майбутньому розвиток штучного інтелекту та машинного навчання відкриває нові можливості для більш ефективного виявлення прихованих комунікаційних каналів. Наприклад, підвищене навчання може бути використане для розробки адаптивних систем безпеки, які постійно вдосконалюються на основі досвіду та нових загроз. Також, федеративне навчання може дозволити створювати спільні моделі безпеки між різними організаціями, забезпечуючи обмін знаннями та поліпшенням моделей без необхідності ділитися конфіденційними даними. Інтерпретованість моделей штучного інтелекту також є важливим напрямком для покращення довіри та ефективності систем безпеки. Розробка моделей, які можуть пояснювати свої рішення та виявлені аномалії, допоможе фахівцям з безпеки краще

розуміти природу загроз та приймати обгрунтовані рішення щодо реагування на них. Це також сприятиме покращенню процесу навчання моделей та їхньої адаптації до нових методів маскування та атакуючих технік.

Висновки до 3 розділу

Виявлення прихованих комунікаційних каналів в інтерактивних застосунках потребує застосування комплексного та багаторівневого підходу, що включає використання різних методів аналізу, сучасних інструментів та технологій машинного навчання. Регулярний аудит, оновлення політик безпеки та підвищення обізнаності персоналу також грають ключову роль у забезпеченні ефективного захисту інформаційних систем від схованих каналів.

Штучний інтелект та машинне навчання відіграють критично важливу роль у сучасних методах виявлення схованих комунікаційних каналів, забезпечуючи високу точність та адаптивність систем безпеки. Незважаючи на існуючі виклики, такі як потреба в великих обсягах даних та ризик помилкового спрацьовування, переваги використання ШІ переважають, особливо при інтеграції з іншими методами захисту. Постійний розвиток та вдосконалення ШІ-моделей, а також їх інтеграція з традиційними методами аналізу, відкривають нові можливості для забезпечення безпеки інформаційних систем та ефективної протидії схованим каналам комунікації. Застосування цих новітніх технологій відчиняє двері перед новими можливостями і підвищує рівень безпеки у сфері інтерактивних застосунків, надаючи організаціям потужні інструменти для ідентифікації, виявлення та нейтралізації таких схованих каналів. Інноваційні методи та підходи породжують нову епоху в області безпеки, де захист інформаційних систем стає все більш надійним та ефективним. Завдяки постійному розвитку наукових досліджень та технологій ШІ, виявлення схованих комунікаційних каналів стає дедалі складнішим, проте за допомогою поєднання різних методів та інноваційних

розробок, нам вдається неухильно підвищувати надійність та ефективність систем захисту. У майбутньому можна очікувати подальшого розвитку та удосконалення технологій і методів виявлення схованих каналів комунікації інтерактивних застосунків, що дозволить зміцнювати безпеку та розвивати нові методи захисту інформації.

ВИСНОВКИ

У роботі було ретельно вивчено теоретичні та практичні аспекти приховування комунікаційних каналів в інтерактивних застосунках. Аналіз почався з розгляду сутності та особливостей замаскованих каналів зв'язку, де було підкреслено їхню двозначну природу: з одного боку, вони можуть бути використані для захисту конфіденційної інформації, а з іншого - для вчинення злочинних дій.

Особлива увага була приділена стеганографії як одному з основних методів замаскування інформації, її історії та сучасним технологіям, які забезпечують високий рівень непомітності та стійкості до аналізу.

Розглянуто різноманітні методи та технології створення прихованих комунікаційних каналів, включаючи криптографію, стеганографію та обфускацію даних. Були проаналізовані переваги та обмеження кожного методу, а також їхня взаємодія для забезпечення багаторівневого захисту інформації. На практиці був розроблений інтерактивний додаток на базі Unity, який демонструє можливості реалізації прихованого каналу комунікації у середовищі 2D платформера. Це підтвердило ефективність використання комбінованих методів для маскування передачі даних та забезпечення їхньої безпеки.

Також було розглянуто технологіям виявлення прихованих комунікаційних каналів в інтерактивних застосунках. Було розглянуто різні підходи до тестування, включаючи аналіз мережевого трафіку, моніторинг системних ресурсів та таймінгову аналітику. Виявлено ряд проблем та обмежень, таких як висока ступінь невидимості прихованих каналів, складність їхнього розпізнавання через обфускацію коду та маскування під звичайну активність системи. Розроблені рекомендації підкреслюють необхідність використання комбінації різних методів аналізу, а також впровадження сучасних технологій машинного навчання та штучного інтелекту для підвищення ефективності виявлення прихованих каналів.

Загалом, робота показує, що приховані комунікаційні канали виявилися дуже потужним інструментом у захисті та можливому зловживанні інформацією в інтерактивних застосунках. Тимчасом, ефективне виявлення таких каналів вимагає комплексного підходу, який поєднує традиційні методи аналізу з сучасними технологіями автоматизації та машинного навчання. Важливо також враховувати юридичні та етичні аспекти використання таємних каналів, забезпечуючи баланс між захистом приватності та необхідністю боротьби з кіберзлочинністю.

Подальші дослідження в цій сфері мають докладати зусиль для вдосконалення методів виявлення, розробки нових методів приховування і створення ефективних засобів протидії незаконним каналам комунікації. Крім того, важливо продовжувати інтегрувати етичні та правові норми у розробку та використання технологій стеганографії, забезпечуючи прозорість та відповідальність у їхньому застосуванні.

ПЕРЕЛІК ПОСИЛАНЬ

1. Gallagher, P. R. A Guide to Understanding Covert Channel Analysis of Trusted Systems. National Computer Security Center, USA, 1993.

2. Wolf, M. Covert channels in LAN protocols. In: Berson, T. A., Beth, T. (Eds.) Workshop on Local Area Network Security (LANSEC 89). Karlsruhe, FRG, 1989.

3. Cabuk, S. Network covert channels: Design, analysis, detection, and elimination. PhD Dissertation. Purdue University. URL: https://www.researchgate.net/publication/27234356 (дата звернення: 25.11.2024).

4. Anjan, K., Abraham, J. Behavioral Analysis of Transport Layer Based Hybrid Covert Channel. In: Third International Conference of Recent Trends in Network Security and Applications (CNSA 2010). India, 2010.

5. Multics Timing Channels. URL: https://www.multicians.org/timing-chn.html (дата звернення: 27.11.2024).

6. Petitcolas, F. A. P., Anderson, R. J., Kuhn, M. G. Information Hiding - A Survey. IEEE, 1999. URL: https://www.petitcolas.net/fabien/publications/ieee99-infohiding.pdf (дата звернення: 27.11.2024).

7. Стеганографія: принципи та застосування в кібербезпеці. URL: https://hackyourmom.com/osvita/shho-take-steganografiya-prynczypy-ta-zastosuvannya-v-kiberbezpeczi/ (дата звернення: 27.11.2024).

8. Kurtović, B. Obfuscating Hello World. URL: https://benkurtovic.com/2014/06/01/obfuscating-hello-world.html (дата звернення: 27.11.2024).

9. Niels Provos. Detecting Steganographic Content on the Internet. URL: http://niels.xtdnet.nl/papers/detecting.pdf (дата звернення: 27.11.2024).

10. Steganography and Image Downgrading. URL: https://www.petitcolas.net/steganography/image_downgrading/ (дата звернення: 27.11.2024).

11. Tromp, J. Maze Solving. URL: https://web.archive.org/web/20021016111325/http://www.cwi.nl/~tromp/maze.html (дата звернення: 27.11.2024).

12. Boaz Barak. On Obfuscation Informally. URL: https://web.archive.org/web/20051124025132/http://www.cs.princeton.edu/~boaz/Papers/obf_informal.html (дата звернення: 29.11.2024).

13. Kessler, G. C. An Overview of Steganography for the Computer Forensics Examiner. Forensic Science Communications, Vol. 6, No. 3, 2004. URL: https://www.garykessler.net/library/fsc_stego.html (дата звернення: 29.11.2024).

14. OWASP Foundation. OWASP Top 10 — The Ten Most Critical Web Application Security Risks. 2023. URL: https://owasp.org/www-project-top-ten/ (дата звернення: 29.11.2024).

15. McAfee Labs. Threats Report 2023. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-may-2023.pdf (дата звернення: 01.12.2024).

16. Google Research. TensorFlow Lite for Machine Learning on Edge Devices. URL: https://www.tensorflow.org/lite (дата звернення: 01.12.2024).

ДЕМОНСТРАНЦІЙНІ МАТЕРІАЛИ (Презентація)