МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітньо-професійна програма: «Комп'ютерна інженерія»

Група: 2БКС-29

КВАЛІФІКАЦІЙНА РОБОТА

здобувача освіти денної форми навчання

БКС.29.21.000.КРБ

ХАБІБУЛІНА ІЛЛІ РУСЛАНОВИЧА

м. Одеса
2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітньо-професійна програма: **«Комп'ютерна інженерія»**

Група: **2БКС-29**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему: **«Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій»**

Проектний матеріал складається з пояснювальної записки на 61 сторінках та графічного (презентаційного) матеріалу на 12 аркушах (слайдах)

Виконавець _____ (Хабібулін І.Р.)

Керівник проекту _____ (Кільдішев В.Й.)

Консультанти:

з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Завідувач кафедри _____ (Іванова Л.В.)

Завідувач відділенням _____ (Краснокутська К.Г.)

Захист «25» 06 2025 р. Протокол ЕК № 1

Оцінка ЕК 4 (добре) / 85

Секретар ЕК _____

АНОТАЦІЯ

Метою даної роботи є розробка методів захисту інформації в інформаційно-комунікаційних системах шляхом інтеграції шифрування, таймерного кодування та методів спектрального розширення сигналу для забезпечення підвищеного рівня прихованості та завадостійкості в умовах деструктивного впливу радіоелектронних засобів протидії.

Вивчено закономірності впливу параметрів таймерного кодування, структури спектрального розширення та властивостей стохастичного шифрування на рівень прихованості сигнальних конструкцій. Проведено аналіз взаємозв'язку між параметрами таймерних сигналів, спектральною шириною та здатністю протидіяти перехопленню та розпізнаванню інформації.

Отримані кількісні оцінки ефективності методів у вигляді залежностей рівня структурної та енергетичної прихованості від параметрів кодових і шифрувальних перетворень. Показано покращення завадозахищеності каналів передавання за рахунок використання розширення спектра та нелінійних сигнальних структур.

Створено багаторівневу модель захисту інформації, що поєднує криптографічні, кодові та спектральні методи для побудови шумоподібних сигнальних конструкцій. Запропоновано алгоритми формування таких сигналів та обґрунтовано критерії вибору їхніх параметрів залежно від умов функціонування системи зв'язку.

Розглянуто питання з охорони праці та техніки безпеки, зокрема вимоги до електромагнітної безпеки в умовах експлуатації телекомунікаційного обладнання, а також заходи щодо запобігання небезпечному впливу високочастотних випромінювань на персонал.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *Комп'ютерних систем* Кафедра *Комп'ютерної інженерії*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР *Беркань І.В.*

"28" 05 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

здобувачеві освіти *Хабібуліна Іллі Руслановича*

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій*

затверджена наказом по коледжу від "24" 11 2024 р. № 246

2. Термін здачі студентом кваліфікаційної роботи

3. Вихідні дані до роботи *1. Порівняння традиційних і сучасних методів прихованості інформації; 2. Аналіз ефективності методів прихованості сигнальних конструкцій; 3. Розробка алгоритму прихованого передавання інформації; 4. Реалізація програмного модуля для тестування*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

Аналіз загроз і вразливостей інформаційних систем; Методи приховування інформації та сигнальних конструкцій; Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій; Розробка алгоритму прихованого передавання інформації

5. Перелік графічного матеріалу (слайдів мультимедійної презентації) *Класифікація загроз інформаційній безпеці підприємства; Класифікація атак на інформаційні системи; Забезпечення прихованості сигнальних конструкцій; Забезпечення прихованості сигнальних конструкцій шляхом розширення спектра; Модель каналу з використанням стеганографії; Часова діаграма перетворення послідовності 10110010 за допомогою АМ; Часова діаграма перетворення послідовності 10110010 за допомогою ЧМ; Часові діаграми амплітудної модуляції інформаційного сигналу на основі логістичного відображення; Часові діаграми фазової модуляції інформаційного сигналу на основі логістичного відображення*

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів, що їх стосуються

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний розділ	*Кільдішев В.Й.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання _____

Керівник роботи *Кільдішев В.Й.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Вступ. Аналіз технічного завдання	21.05.2025	виконав
2.	Аналіз загроз і вразливостей інформаційних систем	22.05.2025	виконав
3.	Методи атаки на інформаційні системи	24.05.2025	виконав
4.	Концепція забезпечення прихованості сигнальних конструкцій у захисті інформації	26.05.2025	виконав
5.	Методи приховування інформації та сигнальних конструкцій	28.05.2025	виконав
6.	Методи спектрального розширення сигналу для підвищення захищеності	30.05.2025	виконав
7.	Порівняння традиційних і сучасних методів прихованості інформації	02.06.2025	виконав
8.	Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій	05.06.2025	виконав
9.	Алгоритми шифрування та їх інтеграція з методами прихованості	07.06.2025	виконав
10.	Аналіз ефективності методів прихованості сигнальних конструкцій	09.06.2025	виконав
11.	Розробка алгоритму прихованого передавання інформації	10.06.2025	виконав
12.	Розробка питань з охорони праці та техніки безпеки	12.06.2025	виконав
13.	Підготовка матеріалів мультимедійної презентації	14.06.2025	виконав

Здобувач освіти _____
(підпис)

Керівник роботи _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 29. 21 000. 00 КРБ	Випускна робота		
А4			БКС 29. 21 000. 00 КРБ ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	БКС 29. 21 000. 00 КРБ			
Розробив		Хабібулін І.Р.		16.06	Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій	Літ.	Аркуш	Аркушів
Перевірив		Кільдішев В.Й.		16.06		Н Д П	4	С1
Н. Контр.		Петрашова В.І.		16.06.25		ВСП "ОТФК ОНТУ" гр.2БКС-29		
Затверд.		Іванова Л.В.		20.06				

ЗМІСТ

ВСТУП

Сучасний розвиток інформаційних технологій та зростаючий обсяг цифрової комунікації призводять до підвищення ризиків витоку, перехоплення та модифікації конфіденційних даних. Традиційні криптографічні методи, хоча і забезпечують високий рівень безпеки, можуть привертати увагу зловмисників, що стимулює розвиток альтернативних підходів до захисту інформації. Одним із перспективних напрямків є використання методів прихованості сигнальних конструкцій, які дозволяють передавати дані таким чином, щоб сам факт їхнього існування залишався непомітним для сторонніх спостерігачів.

Прихованість сигнальних конструкцій може ґрунтуватися на застосуванні стеганографії, хаотичних коливань, методів спектрального розширення сигналу та інших технологій, що маскують передану інформацію серед природних шумів або фонового сигналу. Такий підхід є особливо актуальним в умовах посилення загроз у кіберпросторі та підвищеної уваги до методів несанкціонованого доступу до інформації.

Метою дослідження є розробка та аналіз методів захисту інформації на основі прихованості сигнальних конструкцій.

До завдання дослідження відноситься:

- аналіз сучасних загроз інформаційній безпеці та методи їхнього подолання;
- дослідження основних підходів по забезпеченню прихованості сигнальних конструкцій та оцінка їх ефективності;
- з’ясування особливостей застосування хаотичних коливань, спектрального розширення та стеганографії для забезпечення прихованого передавання інформації;
- розробити методику оцінювання ефективності методів прихованості сигнальних конструкцій;
- запропонувати та протестувати експериментальний метод захисту інформації на основі прихованості сигнальних конструкцій.

1 ОСНОВНИЙ РОЗДІЛ

1.1 Аналіз загроз і вразливостей інформаційних систем

1.1.1 Сучасні загрози інформаційній безпеці

Сучасний розвиток цифрових технологій супроводжується зростанням кількості загроз інформаційній безпеці, що становлять значну небезпеку для державних, комерційних та приватних інформаційних систем. Загрози можуть мати різну природу, походження та рівень складності, але їхньою спільною метою є несанкціонований доступ, зміна або знищення інформації.

Класифікацію загроз інформаційній безпеці можна зробити з урахуванням наступних груп: кіберзлочинність та хакерські атаки; зловмисне програмне забезпечення; загрози внутрішнього характеру; уразливості апаратного та програмного забезпечення; соціальна інженерія та маніпуляція користувачами; загрози національній та корпоративній безпеці.

На рис. 1.1 надана класифікація загроз інформаційній безпеці підприємства.

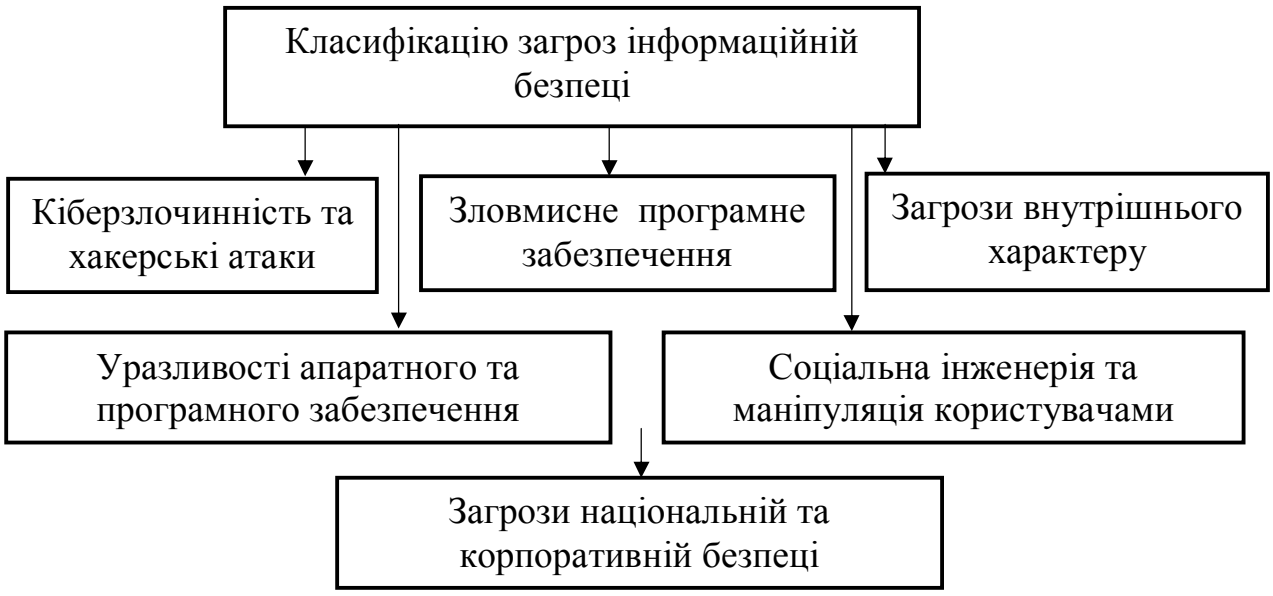


Рисунок 1.1. Класифікація загроз інформаційній безпеці підприємства

До кіберзлочинності та хакерських атак слід віднести: фішингові атаки; DDoS-атаки; атаки «людина посередині».

Фішингові атаки належать до методів соціальної інженерії, що спрямовані на виманювання конфіденційної інформації шляхом маніпуляції користувачами. Зловмисники використовують різні засоби, такі як електронні листи, фальшиві веб-сайти, повідомлення у месенджерах або телефонні дзвінки, щоб змусити жертву розкрити облікові дані, фінансову інформацію або інші чутливі відомості. Фішинг може мати різні форми, зокрема спірфішинг (цілеспрямовані атаки на конкретних осіб або організації), вішинг (голосовий фішинг через телефонні дзвінки) та смшинг (фішингові атаки через SMS-повідомлення). Основна небезпека фішингу полягає в тому, що він може призвести до фінансових втрат, компрометації облікових записів та витоку критично важливої інформації, що особливо небезпечно для компаній та державних установ.

DDoS-атаки (Distributed Denial of Service) спрямовані на перевантаження сервера або мережі великою кількістю запитів, що унеможливлює нормальну роботу сервісів. Для здійснення таких атак зловмисники використовують ботнети – мережі скомпрометованих пристроїв (комп'ютерів, серверів, IoT-пристроїв), які одночасно надсилають масові запити до цільової системи.

Існує кілька основних типів DDoS-атак: атаки на рівні мережі; атаки на транспортний рівень; атаки на рівні застосунків. Атаки на рівні мережі (Volume-Based Attacks) генерують величезний трафік, що перевантажує канал зв'язку (наприклад, UDP-флуд, ICMP-флуд). Атаки на транспортний рівень (Protocol Attacks) експлуатують вразливості мережевих протоколів, наприклад, SYN-флуд, що виснажує ресурси сервера. Атаки на рівні застосунків (Application Layer Attacks) імітують запити легальних користувачів, що ускладнює їх виявлення (наприклад, HTTP-флуд).

DDoS-атаки можуть призвести до значних фінансових втрат, порушення роботи критичних сервісів, зниження репутації компаній і навіть викликати серйозні проблеми у функціонуванні державних або військових інформаційних систем. Для захисту від таких атак застосовуються механізми фільтрації трафіку,

балансування навантаження, використання проксі-серверів і спеціалізованих систем виявлення та пом’якшення DDoS-атак.

Атаки «людина посередині» (MITM, Man-in-the-Middle) є одними з найнебезпечніших форм кіберзагроз і полягають у перехопленні, модифікації або підміні переданих даних між двома комунікуючими сторонами, не даючи їм знати про втручання. Зловмисник, що здійснює таку атаку, виступає посередником між відправником і отримувачем даних, здатний спостерігати, змінювати або навіть пересилати дані в обидва боки, залишаючи обох учасників у невіданні про маніпуляції. Існує кілька варіантів реалізації атак MITM, включаючи: перехоплення трафіку через незахищені мережі; SSL Stripping; DNS Spoofing; DNS Spoofing; Session Hijacking.

Перехоплення трафіку через незахищені мережі це найчастіше атаки MITM відбуваються у публічних бездротових мережах Wi-Fi, де зловмисник може вставати між користувачем і точкою доступу, перенаправляючи трафік через свій пристрій. SSL Stripping реалізується, коли зловмисник змінює зашифроване з’єднання HTTPS на незашифроване HTTP, що дозволяє йому зчитувати і змінювати передані дані. DNS Spoofing реалізується шляхом зміни записів DNS-серверу, щоб перенаправити користувачів на фальшиві веб-сайти, що виглядають як оригінальні, і тим самим отримати чутливу інформацію, таку як паролі та номери кредитних карток. Session Hijacking – зловмисник може перехопити активну сесію користувача, отримавши доступ до його акаунтів без необхідності введення паролів.

Завдяки цим методам зловмисники можуть викрадати конфіденційну інформацію, такі як паролі, фінансові дані або корпоративні дані, а також змінювати або вставляти шкідливий код в комунікації. Захист від атак MITM включає використання протоколів шифрування (наприклад, HTTPS, SSL/TLS), автентифікації серверів, перевірки сертифікатів та використання VPN для захищених з’єднань.

Соціальна інженерія та маніпуляція користувачами є техніками, що використовуються зловмисниками для отримання конфіденційної інформації або

доступу до захищених систем через маніпулювання людьми, а не через технічні вразливості. Ці методи базуються на знаннях людської психології та емоцій, що дозволяють обдурити користувачів, змусивши їх виконати небезпечні або несанкціоновані дії, які можуть призвести до витоку даних, фінансових втрат чи компрометації системи. Основні типи соціальної інженерії включають: фішинг; спірфішинг; вішинг; смшинг; приманки та підроблені ресурси; псевдоавторитети та психологічний тиск.

Фішинг це один з найпоширеніших методів, де зловмисники надсилають фальшиві електронні листи, повідомлення в месенджерах або створюють підроблені веб-сайти, що імітують справжні, щоб змусити користувача ввести свої персональні дані (паролі, фінансову інформацію тощо). Вони часто маскуються під відомі компанії, банківські установи чи навіть колег, що робить їх більш переконливими.

Спірфішинг (Spear Phishing) э цілеспрямованим фішингом, при якому атаки орієнтовані на конкретних осіб чи організації. Зловмисники збирають інформацію про свою жертву через соціальні мережі або інші джерела для створення дуже правдоподібних повідомлень, що вводять в оману.

Вішинг (Vishing) використовує атаку через телефонні дзвінки, де зловмисники представляються, наприклад, співробітниками банку чи державних органів, і просять користувача надати особисті дані, фінансову інформацію або здійснити певні дії, що дозволяють отримати доступ до облікових записів.

Смшинг (Smishing) реалізується за допомогою атаки через SMS-повідомлення, в яких зловмисники пропонують перейти за посиланням або зателефонувати за номером, щоб, наприклад, «підтвердити рахунок» або «отримати вигоду». Ці повідомлення можуть містити шкідливі програми, які активуються після натискання на посилання.

Приманки та підроблені ресурси реалізуються зловмисниками за допомогою створення фальшивих веб-сайтів або файлів, що видаються за законні, щоб змусити користувачів відвідати їх, завантажити шкідливе

програмне забезпечення чи ввести свої облікові дані. Цей метод може також включати підроблені документи, програми чи інструменти.

Псевдоавторитети та психологічний тиск орієнтується на маніпулювання жертвами через створення ілюзії авторитету або виявлення надмірної терміновості. Це може бути ситуація, коли зловмисник, видаючи себе за керівника або важливу особу, змушує користувача виконати дію швидко, не роздумуючи.

Соціальна інженерія використовує наступні психологічні принципи: довіра; терміновість; групова належність. Принцип довіри основується на тому, що люди природно довіряють тим, хто здається знайомим або авторитетним, що часто використовується для того, щоб змусити їх поділитися конфіденційною інформацією. Принцип терміновості спрямований на створення відчуття, що дія повинна бути виконана негайно, щоб уникнути негативних наслідків. Це сприяє ухваленню поспішних рішень без належного обмірковування. Принцип групової належності використовує маніпулювання через створення відчуття, що дія відповідає нормам групи або суспільства, наприклад, пропозиція досягнути «спільної мети».

Існують наступні підходи до захист від соціальної інженерії: освітлення користувачів; аутентифікація двома факторами; регулярні перевірки безпеки; захист від шкідливих програм. Освітлення користувачів використовує навчання співробітників чи користувачів, як розпізнавати ознаки фішингових повідомлень, вішингу та інших форм маніпуляцій. Аутентифікація двома факторами (2FA) використовує додатковий рівень безпеки, що ускладнює зловмисникам доступ до облікових записів навіть при отриманні пароля. Регулярні перевірки безпеки побудовані на перевірки використання безпечних паролів, моніторинг підозрілих дій та активностей в мережах та системах. Захист від шкідливих програм потребує використання антивірусних програм та засобів безпеки, що можуть блокувати шкідливі файли та посилання.

Отже, соціальна інженерія є одним з найпоширеніших і найнебезпечніших методів атак, оскільки вона не залежить від технічних вразливостей, а

використовує слабкі місця в людській природі. Тому важливо постійно працювати над підвищенням обізнаності та обережності користувачів.

1.1.2 Методи атаки на інформаційні системи

Атаки на інформаційні системи є ключовою загрозою кібербезпеці та можуть мати різні цілі: несанкціонований доступ до даних, модифікація інформації, знищення ресурсів або порушення нормального функціонування системи. Методи атак постійно удосконалюються, що ускладнює їхнє виявлення та нейтралізацію. Можна визначити наступну класифікацію методів атак на інформаційні системи з урахуванням механізму їх реалізації: атаки на рівні мережі; атаки на рівні програмного забезпечення; атаки соціальної інженерії.

На рис. 1.2 надана класифікація атак на інформаційні системи.

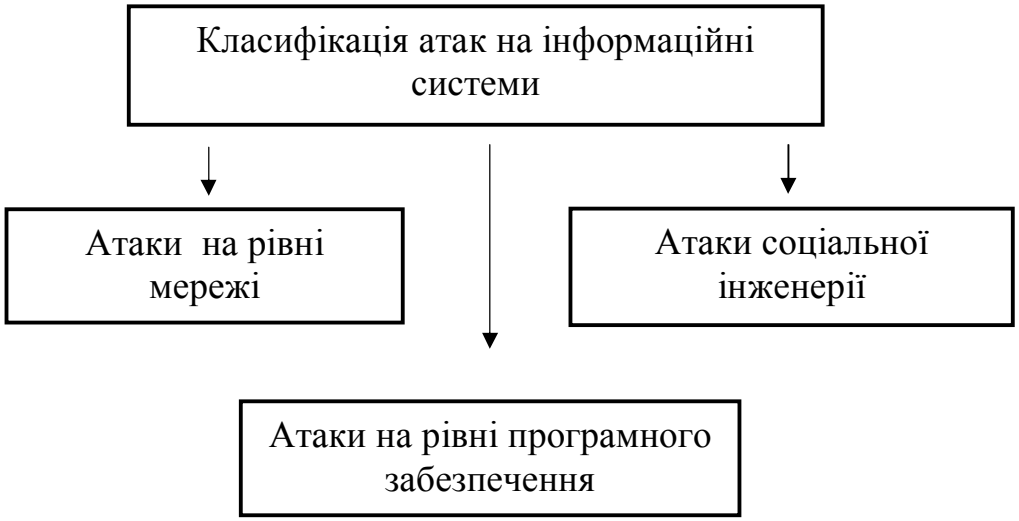


Рисунок 1.2. Класифікація атак на інформаційні системи

Атаки на рівні мережі спрямовані на порушення функціонування мережевої інфраструктури або перехоплення переданих даних. Можна зазначити, що при цьому використовується: атака «Людина посередині»; перехоплення трафіку DNS-спуфінг; атаки на бездротові мережі. Атака «Людина посередині» (MITM, Man-In-The-Middle) реалізується зловмисником шляхом перехоплення та зміни трафіку між двома комунікуючими сторонами. При перехопленні трафіку (Packet Sniffing) відбувається використання аналізаторів трафіку для відстеження переданих даних, зокрема незашифрованих паролів або

конфіденційної інформації. DNS-спуфінг (DNS Spoofing) використовує підміну записів DNS, що змушує користувачів заходити на підроблені сайти замість легітимних. При використані атаки на бездротові мережі (Wi-Fi Attacks) відбувається злам шифрування WPA2/WPA3, створення підроблених точок доступу (Evil Twin), атаки деаутентифікації.

Атаки на рівні програмного забезпечення спрямовані на використання вразливостей у коді або логіки роботи програм. При цьому використовуються: SQL-ін'єкції; XSS; буферне переповнення; атаки на криптографічні алгоритми.

SQL-ін'єкції (SQL Injection) реалізуються шляхом впровадження шкідливих SQL-запитів у веб-додатки для отримання доступу до бази даних. Атаки XSS (Cross-Site Scripting) реалізуються шляхом впровадження шкідливих скриптів у веб-сторінки для викрадення даних користувачів. Атака типу буферне переповнення (Buffer Overflow) використовує експлуатацію помилок у керуванні пам'яттю для виконання довільного коду. Атаки на криптографічні алгоритми використовують підбір ключів, аналіз побічних каналів, атаки за відкритим текстом.

При реалізації атаки соціальної інженерії зловмисники використовують психологічні методи для маніпулювання користувачами та отримання конфіденційної інформації. Це може бути фішінг, вішинг, приманювання. Атака фішинг (Phishing) використовує розсилання підроблених електронних листів або створення підроблених сайтів для виманювання даних. Атака вішинг (Vishing) використовує телефонні дзвінки, спрямовані на отримання конфіденційної інформації шляхом соціальної маніпуляції. Атака приманювання (Baiting) реалізується шляхом поширення шкідливого програмного забезпечення під виглядом корисних файлів або програм.

Атаки на рівні системних ресурсів спрямовані на виведення з ладу інформаційної системи шляхом перевантаження або знищення ресурсів. Ці види атак реалізуються за допомогою: DDoS-атаки; атаки на файлову систему; атаки на завантажувальний сектор. DDoS-атаки (Distributed Denial of Service) реалізуються за допомогою масового надсилання запитів до сервера, що

викликає його перевантаження та відмову в обслуговуванні. Атака на файлову систему спрямована знищення або модифікація критично важливих файлів, видалення логів. Атака на завантажувальний сектор (Bootkit) спрямована на модифікацію завантажувальних записів диска для отримання повного контролю над системою.

Атаки із використанням шкідливого програмного забезпечення (Malware Attacks) спрямовані на отримання контролю над системою або викрадення інформації. При цьому використовується наступні шкідливі програми: віруси та черв'яки; трояни; програми-здирники; програми-шпигуни. Віруси та черв'яки (Viruses & Worms) це програми, що поширюються у файловій системі або мережі та виконують шкідливі дії. Трояни (Trojans) це шкідливі програми, які маскуються під легітимне ПЗ для викрадення даних або відкриття бекдорів. Програми-здирники (Ransomware) використовують шифрування файлів користувача та вимагають викуп за їх розшифрування. Програми-шпигуни (Spyware) це приховане ПЗ, що передає зловмисникам інформацію про користувача.

Атаки на ланцюг постачання (Supply Chain Attacks) використовуються зловмисниками, які атакують постачальників ПЗ чи обладнання, щоб впровадити шкідливий код на ранніх етапах розробки. Такий вид атаки реалізуються на основі наступних дій: компрометація оновлень; заміна апаратного забезпечення.

Компрометація оновлень (Update Hijacking) відбувається шляхом впровадження шкідливого коду в офіційні оновлення ПЗ. Заміна апаратного забезпечення (Hardware Trojans) забезпечується шляхом модифікація компонентів пристроїв перед їх постачанням кінцевому користувачеві.

Атаки на фізичному рівні передбачають безпосередній фізичний доступ до обладнання. Для цього використовується: перехоплення електромагнітного випромінювання; підключення до портів введення/виведення; крадіжка або фізичне пошкодження обладнання. Перехоплення електромагнітного випромінювання (TEMPEST Attacks) реалізується на основі зчитування даних через аналіз електромагнітних хвиль, що випромінюються пристроями.

Підключення до портів введення/виведення спрямовано на отримання доступу до системи через відкриті USB, HDMI, Ethernet-порти. Крадіжка або фізичне пошкодження обладнання спрямовано на викрадення жорстких дисків, серверів або інших носіїв інформації.

Методи захисту від атак на інформаційні системи спрямовані на зменшення ризику успішного здійснення атак необхідно застосовувати комплексні заходи захисту. Такі методи можуть бути наступними: використання сучасних алгоритмів шифрування даних; регулярне оновлення програмного забезпечення та виправлення вразливостей; впровадження багатофакторної автентифікації (MFA); використання систем виявлення та запобігання вторгненням (IDS/IPS); розробка політик безпеки та навчання користувачів основам кібергігієни.

Отже, можна відзначити, що сучасні методи атак стають дедалі витонченішими, тому дослідження нових підходів до захисту інформації, зокрема на основі прихованості сигнальних конструкцій, є актуальним напрямком у сфері кібербезпеки.

1.1.3 Концепція забезпечення прихованості сигнальних конструкцій у захисті інформації

Сучасні загрози інформаційній безпеці, зокрема атаки на інформаційні системи, вимагають нових підходів до захисту даних. Одним із перспективних методів є використання прихованості сигнальних конструкцій, що передбачає маскування інформаційних потоків і ускладнення їхнього перехоплення та аналізу. Основні принципи прихованості сигнальних конструкцій базуються на декількох ключових принципах: маскування інформації; стеганографія; спектральне розширення сигналу; адаптивна зміна параметрів сигналу; шифрування. Маскування інформації може бути реалізовано шляхом використання хаотичних або спеціально сформованих сигналів для приховування корисного навантаження.

На рис. 1.3 надано варіанти прихованості забезпечення сигнальних конструкцій.

Рисунок 1.3. Забезпечення прихованості сигнальних конструкцій

Стеганографія – це спосіб приховування інформації в такому вигляді, що вона не привертає уваги зловмисників або сторонніх осіб. Вона передбачає впровадження секретних даних у звичайні файли або сигнали, які не викликають підозри у процесі передачі по каналу зв'язку. Основна мета стеганографії полягає в тому, щоб зробити передану інформацію невидимою або невиразною для тих, хто може спробувати її перехопити або проаналізувати.

Існує кілька методів впровадження інформації в контейнер-файл, серед яких можна виділити: впровадження в зображення; впровадження в аудіофайли; впровадження в текст; впровадження в відео; техніки впровадження в мережевий трафік. Впровадження інформації в зображення (Image Steganography) це один з найпоширеніших способів. Дані можуть бути сховані в пікселях зображення шляхом зміни значень кольорів, що є непомітним для людського ока. Наприклад, зміни на рівні найменш значущих біт (LSB, Least Significant Bit) пікселів можуть не змінити видимого зображення, але дозволяють зберігати приховану інформацію. Впровадження інформації в аудіофайли (Audio Steganography) це аналогічно до зображень, дані можуть бути заховані в аудіофайлах шляхом маніпуляцій із звуковими хвилями. Вони можуть бути внесені в частину сигналу, яка для людини не сприймається, але може бути відновлена при обробці за допомогою спеціальних інструментів. Впровадження в текст (Text

Steganography) – тут приховану інформацію можна зашифрувати у вигляді прихованих символів або за допомогою синтаксичних та граматичних маніпуляцій, які не змінюють смислового навантаження тексту. Це може включати додавання або зміну пробілів, літерних варіантів або навіть розподілу виведених символів. Впровадження в відео (Video Steganography) – відеофайли надають більше можливостей для приховування даних через вбудовування їх у окремі кадри або навіть в звук. Оскільки відеофайли мають значно більший обсяг, можна використовувати різні техніки для впровадження даних у різних частинах файлу (наприклад, в аудіотрек, в рухи об'єктів на кадрах або в кольорові фільтри). Техніки впровадження в мережевий трафік (Network Steganography) – стеганографія може використовуватися і для приховування даних у мережевому трафіку. Це може включати в себе передачу прихованих повідомлень в пакетах даних, таких як нестандартні порти, або навіть маніпуляції з часу передавання пакетів.

Основними перевагами стеганографії є її здатність приховувати існування передачі даних і зменшити ймовірність виявлення, порівняно з традиційними методами шифрування, де сам факт передачі інформації може викликати підозри. Однак, стеганографія також має свої обмеження, такі як можливість виявлення при застосуванні спеціалізованих інструментів для аналізу файлів або трафіку, а також ризик втрати даних при порушенні цілісності контейнера. Тому для підвищення надійності часто поєднують стеганографію з шифруванням, що додає додатковий рівень захисту та робить інформацію ще більш недосяжною для зловмисників.

Спектральне розширення сигналу побудовано на застосуванні технологій, що зменшують імовірність виявлення сигналу в каналі засобами радіоелектронної розвідки противника за рахунок розширення його спектру.

Адаптивна зміна параметрів сигналу основана використанні динамічних характеристик для ускладнення аналізу та виявлення передачі даних.

Методи забезпечення прихованості сигнальних конструкцій можуть бути реалізовані за допомогою різних методів, що відрізняються залежно від рівня

реалізації та способу маскування інформації. Це можуть біти такі методи: хаотичні коливання в системах зв'язку; методи спектрального розширення; стеганографічні методи; маскування передачі інформації у фонових потоках

Хаотичні коливання в системах зв'язку реалізуються на основі використання нелінійних динамічних систем для генерації сигналів, що нагадують природні шуми. Для них характерним є генерування псевдовипадкових послідовностей, які важко розпізнати серед фонових перешкод, а також висока завадостійкість і складність для аналізу традиційними методами спектрального аналізу.

Методи спектрального розширення сигналу використовуються наступні методи: пряме розширення спектра; псевдовипадковий перескок робочої частоти; ортогональні методи мультиплексування; стеганографічні методи; маскування передачі інформації у фонових потоках.

На рис. 1.4 надано методи забезпечення прихованості шляхом розширення спектра сигнальних конструкцій.

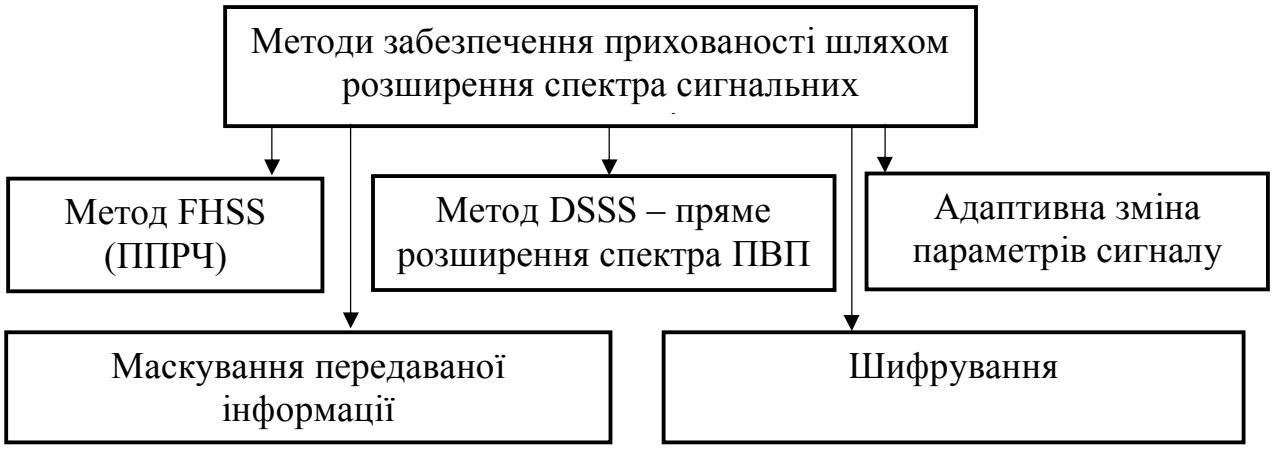


Рисунок 1.4. Забезпечення прихованості сигнальних конструкцій шляхом розширення спектра

Пряме розширення спектра (Direct Sequence Spread Spectrum, DSSS) – множення корисного сигналу на швидку псевдовипадкову послідовність для розширення спектра, тобто метод прямого розширення спектра за допомогою псевдовипадкових послідовностей (ПРС-ПВП). Псевдовипадковий перескок

робочої частоти (Frequency Hopping Spread Spectrum, FHSS) – зміна частоти передавання за псевдовипадковим законом, тобто псевдовипадковий перескок робочої частоти (ППРЧ). Ортогональні методи мультиплексування (OFDM, CDMA) – застосування множинного доступу з використанням ортогональних сигналів. Принцип розширення спектра вузькосмугового сигналу пояснюється на рис. 1.5. З рис. 1.5 бачимо, що спектр смуга частот $\Delta F_н$ збільшується у порівнянні із спектром отриманого широкосмугового сигналу $\Delta F_в$.

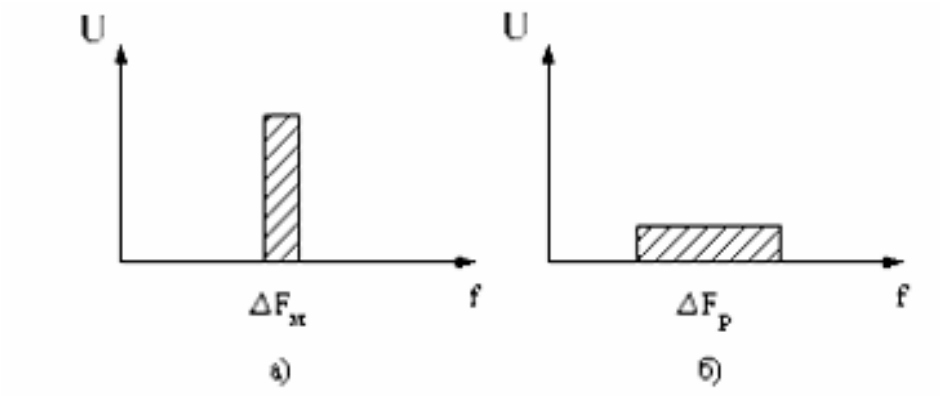


Рисунок 1.5. Розширення спектра вузькосмугового сигналу:
а – вузькосмуговий сигнал; б – широкосмуговий сигнал

Стеганографічні методи використовують приховання інформації в незначних змінах сигналів, що використовуються для передавання легітимних даних. При цьому відбувається вбудовування повідомлень у цифрові носії, такі як аудіо- та відеопотоки. Також використовується надлишкові компоненти цифрових сигналів для передавання секретних даних.

Маскування передачі інформації у фонових потоках реалізується шляхом імітації природних шумів для приховування факту передавання інформації. Доцільним також є використання адаптивних алгоритмів для зміни характеристик сигналу відповідно до умов навколишнього середовища. Перспективним для завдання маскування є застосування динамічного кодування для маскування структури переданих даних.

Можна визначити наступні переваги використання прихованих сигнальних конструкцій у захисті інформації: стійкість до перехоплення; стійкість до аналізу

трафіку; висока завадостійкість; гнучкість реалізації. Стійкість до перехоплення забезпечується за рахунок того, що зловмиснику не може легко виявити або ідентифікувати корисний сигнал. Стійкість до аналізу трафіку пояснюється складністю розпізнавання структури інформаційного потоку навіть у разі його перехоплення. Висока завадостійкість обґрунтовується шляхом використання хаотичних або псевдовипадкових сигналів забезпечує природну захищеність від перешкод. Гнучкість реалізації пояснюється тим, ця концепція може бути застосована до різних каналів зв'язку, включаючи радіочастотні, оптичні та цифрові системи передавання даних.

Визначимо наступні виклики та обмеження використання технології прихованості передавання інформації. Попри наданих переваг, концепція прихованості сигнальних конструкцій має низку технічних і практичних обмежень:

1) складність синхронізації, тобто виникають певні технічні проблеми узгодження передавача та приймача в умовах динамічної зміни параметрів сигналу;

2) складність реалізації процесів розширення спектра сигналів;

3) збільшене енергоспоживання, тобто розширення спектра сигналу або використання хаотичних генераторів потребує додаткових ресурсів;

4) обмеження пропускної здатності – приховане передавання інформації може знижувати ефективність використання каналів зв'язку.

Розглянемо складність реалізації процесів розширення спектра сигналів. Розширення спектра сигналів (Spread Spectrum) – це технологія, яка полягає у збільшенні смуги частот переданого сигналу за рахунок застосування спеціальних методів модуляції або кодування. Такий підхід використовується для забезпечення стійкості до перешкод, перехоплення та спотворення. До найвідоміших методів розширення спектра належать пряма послідовна модуляція (DSSS) і частотна модуляція з перестрибуванням (FHSS), а також методи на основі хаотичних сигналів.

Однак попри очевидні переваги, реалізація таких систем має ряд складностей, зокрема:

1) складність генерації псевдовипадкових або хаотичних послідовностей;

2) підвищені вимоги до синхронізації;

3) складність у цифровій реалізації;

4) проблеми з передачею в обмежених середовищах;

5) зростання складності приймально-передавальної апаратури;

6) забезпечення захищеного обміну службовою інформацією.

Складність генерації псевдовипадкових або хаотичних послідовностей пояснюється наступним необхіднвстю забезпечити високу ентропію, непередбачуваність та відтворюваність у приймачі. Для хаотичних методів важливо синхронізувати передавач і приймач по початкових умовах, що потребує додаткового захисту цих параметрів.

Також при цьому потрібно вирішувати задачу підвищення вимоги до синхронізації. У методах розширення спектра приймач повинен точно знати часові параметри (фази, частоти) псевдовипадкової послідовності. Найменший зсув у часі може призвести до повної втрати сигналу.

Складність у цифровій реалізації пояснюється в наступному:

1) потрібні потужні обчислювальні ресурси для генерації та обробки широкосмугових сигналів;

2) в умовах реального часу реалізація алгоритмів DSSS чи хаотичних модуляцій вимагає високопродуктивного ПЗ або спеціалізованих апаратних рішень (DSP, FPGA).

Також існує проблеми з передачею в обмежених середовищах:

1) розширений спектр сигналу може займати широку смугу частот, що обмежено у деяких діапазонах радіозв’язку;

2) в умовах щільного спектрального середовища можуть виникати конфлікти з іншими службами.

Зростання складності приймально-передавальної апаратури полягає в наступному:

1) реалізація приймачів з можливістю розширення спектра потребує більш складної схеми детектування, декодування та фільтрації;

2) особливо складними є адаптивні системи, які повинні працювати за змінних умов завад.

Забезпечення захищеного обміну службовою інформацією потрібно для нормальної роботи системи потрібно обмінюватись службовими даними: ключами, параметрами генерації послідовностей, синхросигналами. Ці дані також повинні бути захищені від перехоплення.

Таким чином, хоча методи розширення спектра сигналу є надзвичайно ефективними для забезпечення конфіденційності, захищеності та стійкості до перешкод, їх реалізація вимагає значних технічних та алгоритмічних зусиль. Найбільш перспективними залишаються гібридні підходи, які поєднують традиційні та хаотичні методи з використанням сучасних цифрових технологій і алгоритмів синхронізації.

Одним із суттєвих недоліків методів розширення спектра сигналів та використання хаотичних коливань є збільшене енергоспоживання. Це пояснюється кількома факторами:

1) складність обчислень;

2) широкосмуговість сигналу;

3) складність синхронізації;

4) використання складних алгоритмів обробки сигналівє

Методи прямої псевдовипадкової модуляції (DSSS), частотної перестрибуючої модуляції (FHSS), а також модуляції на основі хаотичних сигналів потребують обробки великих обсягів даних у реальному часі. Це вимагає більш потужних процесорів, що безпосередньо впливає на споживання електроенергії.

Передавання розширеного у спектрі сигналу означає, що передавач повинен генерувати й передавати сигнал із більшою смугою частот, що збільшує потужність радіопередачі. Для стабільного прийому таких сигналів також потрібен підсилений приймач.

Системи, що використовують розширення спектра або хаотичні генератори, потребують точної синхронізації між передавачем і приймачем. Це призводить до збільшення числа службових операцій (пошук, виявлення, корекція), що також підвищує загальне енергоспоживання системи.

Хоча хаотичні генератори можуть бути реалізовані в цифровій або аналоговій формі, обидва варіанти вимагають додаткових елементів, які збільшують споживання енергії в порівнянні з традиційною передачею гармонічного сигналу.

У випадку прихованої передачі, додатково застосовуються алгоритми шифрування, маскування та фільтрації, які теж навантажують систему та підвищують загальні витрати енергії.

Незважаючи на високу ефективність з погляду завадостійкості та захищеності, методи розширення спектра та модуляції на основі хаотичних коливань значно збільшують енергоспоживання системи. Це накладає обмеження на їх використання в енергонезалежних або мобільних пристроях і вимагає ретельного балансу між рівнем захисту та енергоефективністю.

Отже, прихованість сигнальних конструкцій є ефективним підходом до забезпечення захисту інформації, особливо в умовах високої загрози кібератак і радіоелектронної розвідки. Впровадження таких методів дозволяє ускладнити виявлення, перехоплення та аналіз інформаційних потоків, що робить їх перспективним напрямом у сфері інформаційної безпеки.

1.2 Методи забезпечення прихованості сигнальних конструкцій

1.2.1 Основні принципи стеганографії та її застосування

Стеганографія є важливим методом забезпечення конфіденційності інформації, що полягає в приховуванні повідомлення у носіях даних так, щоб факт його існування залишався непомітним. На відміну від криптографії, яка приховує зміст інформації, стеганографія маскує сам факт передавання даних, що значно ускладнює її виявлення та аналіз зловмисниками.

Основні методи стеганографії базуються на кількох ключових принципах: непомітність; ємність; стійкість; безпека. Непомітність (Stealthiness) базується на тому, що приховане повідомлення не повинно викликати підозр у сторонніх спостерігачів. Ємність (Capacity) контейнера полягає на тому, що носій інформації повинен мати достатній обсяг даних для приховування повідомлення. Стійкість (Robustness) до перетворення, яке полягає в тому, що приховане повідомлення має зберігати цілісність навіть після можливої обробки носія (наприклад, стиснення, фільтрації або зміни формату). Безпека (Security) забезпечується лише авторизованим користувачам, які повинні мати можливість витягти приховану інформацію. На рис. 1.6 представлена модель каналу з використанням стеганографії. За типом стеганографії вона може бути з секретним або відкритим ключем.

Як правило, класифікація стеганографічних методів відбувається за видом носія та способом приховування інформації: цифрова стеганографія; мережева стеганографія; фізична стеганографія.

Цифрова стеганографія може бути реалізована в зображеннях, аудіофайлах, відео, тексті. Стеганографія в зображеннях припускає використання незначних змін у кольорових або яскравісних складових пікселів для вбудовування даних (наприклад, метод найменш значущих біт – LSB). Стеганографія в аудіофайлах припускає приховування інформації в непомітних для слуху частотних діапазонах або зміна фазових характеристик сигналу. Стеганографія у відео припускає модифікацію окремих кадрів відеопотоку без значного погіршення якості. Стеганографія в тексті засновано на використанні варіацій форматування, невидимих символів або зміни інтервалів між словами.

Мережева стеганографія використовує приховування повідомлень у заголовках мережевих пакетів або часових затримках при їхньому передаванні, а також використання надлишкових сигналів у протоколах зв’язку, таких як TCP, UDP або ICMP.

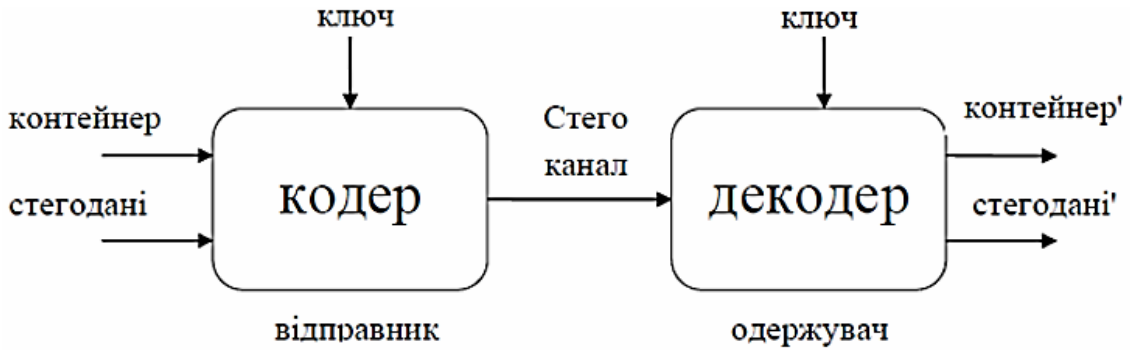


Рисунок 1.6. Модель каналу з використанням стеганографії

Фізична стеганографія заснована на використанні мікротексту, водяних знаків та інших фізичних засобів для приховування інформації в друкованих матеріалах.

Стеганографічні методи знаходять застосування в різних сферах, включаючи: захист конфіденційної інформації; водяні знаки та авторські права; захищений зв'язок; аналітика та криміналістика. Захист конфіденційної інформації забезпечує приховування секретних повідомлень у файлах для безпечного передавання. Водяні знаки та авторські права – це захист інтелектуальної власності за допомогою цифрових водяних знаків у мультимедійних даних. Захищений зв'язок є доцільним для застосування в військових та урядових системах зв'язку для приховування переданих даних. Аналітика та криміналістика це виявлення прихованої інформації в цифрових носіях під час розслідувань.

Отже, стеганографія є потужним інструментом для захисту інформації, що дозволяє приховувати її у видимих носіях без явних слідів змін. Використання стеганографічних методів у поєднанні з криптографічними засобами забезпечує високий рівень безпеки передавання даних, роблячи їх стійкими до виявлення та несанкціонованого доступу.

1.2.2 Використання хаотичних коливань для маскування сигналів

Хаотичні коливання є ефективним інструментом для маскування сигналів у системах захисту інформації. Використання хаотичних динамічних систем дозволяє створювати сигнали, що виглядають як природний шум, що ускладнює їхнє виявлення та аналіз. Такий підхід має широке застосування в криптографії, радіозв'язку та стеганографії, забезпечуючи високий рівень захищеності інформації. На рис. 1.7 представлена доцільність використання динамічного хаосу для забезпечення прихованості передавання інформації.

Рисунок 1.7. Доцільність використання динамічного хаосу в системах зв'язку для забезпечення прихованості передавання інформації

Визначимо основні властивості хаотичних коливань, які мають кілька ключових характеристик, що роблять їх досить ефективними для маскування: невизначуваність; псевдовипадковість; широкий спектр; висока чутливість до параметрів. Невизначуваність пояснюється той особливістю хаотичних коливань, що навіть невеликі зміни в початкових умовах можуть суттєво змінити форму сигналу. Псевдовипадковість пояснюється тим, що хаотичні сигнали

нагадують природні випадкові процеси, що ускладнює їхнє розпізнавання. Широкий спектр є характерним для хаотичних сигналів, тому що вони займають широкий спектральний діапазон, що забезпечує їхню стійкість до перехоплення. Висока чутливість до параметрів пояснюється тим, що навіть незначне коригування параметрів генератора хаотичних сигналів може кардинально змінити їхню структуру.

Розглянемо характерні методи генерації хаотичних сигналів. Для створення хаотичних сигналів використовуються нелінійні динамічні системи, серед яких. Прикладом дискретного генератора хаосу є логістичне відображення, яке є одним з найпростіших рівнянь, що описує хаотичні процеси:

$$x_{n+1} = a x_n (1 - x_n), \tag{1.1}$$

де $x_0 = 0{,}9$ – початковий параметр хаотичного коливання, який може змінюватися від 0 до 1; $a = 3{,}9$ – параметр генератору хаосу. Приклад реалізації центрованого хаотичного коливання надано на рис. 1.8, що потребувало використання наступної формули:

$$x_{n+1} = a x_n (1 - x_n) - m_x, \tag{1.2}$$

де m_x – математичне очікування хаотичної реалізації.

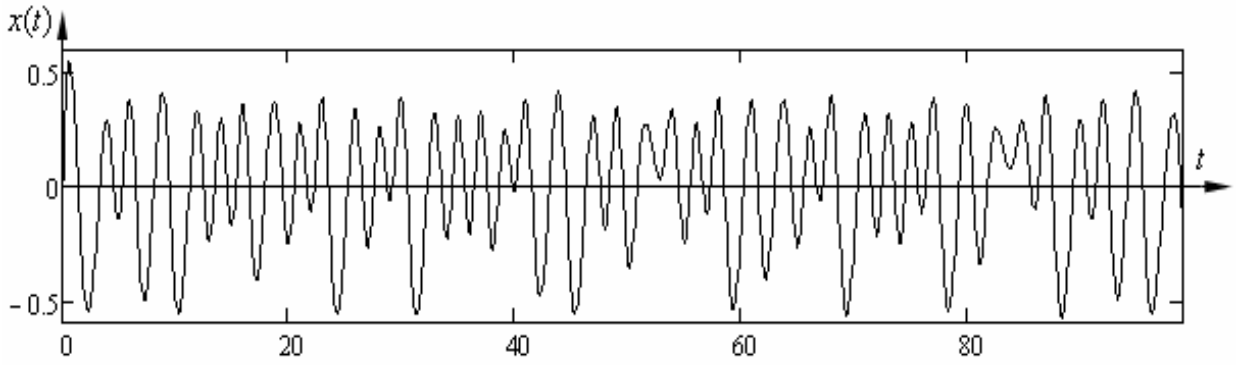


Рисунок 1.8. Реалізація хаотичного сигналу з реалізацією чисел

від -0,5 до 0,5

Іншим прикладом є кубічне відображення дискретного генератору хаосу:

$$x_{n+1} = (1-4a)x_n + 4ax_n^3, \qquad (1.3)$$

де $x_0 = 0{,}5$ – початковий параметр хаотичного коливання, який може змінюватися від 0 до 1; $a = 0{,}92$ – параметр генератору хаосу.

Також існує систем Лоренца, яка є нелінійною системою диференціальних рівнянь. Дана система використовується для моделювання динамічних хаотичних процесів у реальних фізичних системах. Також відомі генератори Чуа, Ресслера, Хенона, які є більш складними хаотичними системами, які застосовуються для створення нелінійних коливань.

Методи маскування сигналів на основі хаосу використовуватися для маскування інформаційних сигналів у кількох основних варіантах:

– модуляція інформації в хаотичному сигналі;

– синхронізація хаотичних систем;

– спектральне розширення хаотичними сигналами;

– стеганографічне приховування даних у хаотичних коливаннях.

Модуляція інформації в хаотичному сигналі це коли корисний сигнал вбудовується в хаотичний процес, що ускладнює його відокремлення без знання початкових параметрів. При цьому можливе використання амплітудної або фазової модуляції.

При синхронізація хаотичних систем відправник і приймач використовують ідентичні хаотичні генератори, які синхронізуються для декодування інформації. Прикладом є використання синхронізованих генераторів Лоренца для прихованого передавання сигналів.

Спектральне розширення хаотичними сигналами це коли корисний сигнал маскується хаотичним сигналом, що має широкий спектр, роблячи його

невідчутним для стандартних методів виявлення. Метод широко використовується в безпровідних мережах і військових системах зв’язку.

Стеганографічне приховування даних у хаотичних коливаннях це коли використовуються хаотичні процеси для передачі цифрових даних у вигляді малопомітних варіацій амплітуди або частоти. Метод особливо ефективний у мультимедійних та мережевих застосуваннях.

Можна визначити наступні переваги використання хаотичних коливань для маскування сигналів:

– складність виявлення;

– висока завадостійкість;

– можливість адаптації;

– ефективність у реальних системах.

Складність виявлення пояснюється тим, що традиційні методи спектрального аналізу погано пристосовані для розпізнавання хаотичних сигналів. Висока завадостійкість пояснюється тим, що хаотичні сигнали стійкі до перешкод та спроб фільтрації. Можливість адаптації пояснюється тим, що параметри хаотичних генераторів можна налаштовувати для забезпечення оптимального рівня захисту. Ефективність у реальних системах пояснюється тим, що хаотичні методи можуть застосовуватися в бездротових мережах, супутниковому зв’язку, захищених каналах передавання даних.

Попри значні переваги, використання хаотичних коливань у захисті інформації має деякі обмеження: необхідність точної синхронізації; обмеженість практичних реалізацій; високі обчислювальні витрати.

Необхідність точної синхронізації пояснюється тим, що навіть незначні розбіжності у параметрах генераторів можуть призвести до втрати інформації. Обмеженість практичних реалізацій хаотичних генераторів у цифрових пристроях також потребує високої точності обчислень. Також, для генерація хаотичних сигналів у деяких випадках потрібні значні обчислювальні ресурси.

Таким чином, використання хаотичних коливань є перспективним підходом до маскування сигналів у системах інформаційного захисту. Завдяки

своїм унікальним властивостям хаотичні сигнали забезпечують високий рівень стійкості до перехоплення, аналізу та несанкціонованого доступу. Впровадження хаотичних методів у стеганографічні та криптографічні системи дозволяє створювати ефективні механізми захисту інформації, що можуть використовуватися в умовах кіберзагроз і радіоелектронної боротьби.

1.2.3 Методи спектрального розширення сигналу для підвищення захищеності

Методи спектрального розширення сигналу (Spread Spectrum, SS) є ефективним способом підвищення захищеності інформаційного передавання, особливо в умовах радіоелектронної боротьби (РЕБ) та інформаційних загроз. Такі методи забезпечують захист від перехоплення, спотворення та глушіння сигналу шляхом збільшення його спектральної ширини. Вони широко використовуються у військовому зв’язку, супутникових системах, стільникових мережах та бездротових технологіях.

Розглянемо основні принципи спектрального розширення. Методи спектрального розширення базуються на двох основних принципах при якому відбувається збільшення ширини спектра сигналу, тобто корисний сигнал поширюється на більшу смугу частот, ніж необхідно для його передавання в традиційний спосіб. При цьому застосовуються псевдовипадкові послідовності для модуляції сигналу або хаотичні коливання, що ускладнює перехоплення сигнальних конструкцій та їх аналіз.

До основних переваг таких методів можна віднести наступне:

– захист від перехоплення;

– стійкість до завад;

– можливість багатокористувацького доступу.

Захист від перехоплення обґрунтовується тим, що передаваний сигнал складно виділити без знання використовуваної кодової послідовності. Стійкість до завад пояснюється тим, що широкий спектр робить сигнал менш чутливим до вузькосмугових завад. Можливість багатокористувацького доступу пояснюється

тим, що різні користувачі можуть використовувати свої кодові послідовності без взаємного впливу.

При прямому розширенні спектра (Direct Sequence Spread Spectrum, DSSS) інформаційна цифрова послідовність множить на високочастотну ПВП (PN). Прикладом таких ПВП є коди Баркера або Голда. Формула для DSSS-модуляції наступна:

$$S(t)=d(t)\cdot c(t), \tag{1.4}$$

де $d(t)$ – передаваний цифровий сигнал, $c(t)$ – кодова послідовність.

Ця технологія використовується в стандарті Wi-Fi (802.11b), системах GPS та військових каналах зв’язку.

При ППРЧ частота сигналу змінюється за псевдовипадковим законом відповідно до кодової послідовності. Цей метод передачі сигналів дозволяє уникати перехоплення та зменшити вплив вузькосмугових завад. Формула для зміни частоти:

$$f\,i = f_0 + k_i \cdot \Delta f, \tag{1.5}$$

де f_0 – початкова частота; k_i – номер стрибка; Δf – ширина частотного кроку. Цей метод передавання використовується в Bluetooth, військових системах зв’язку та супутникових мережах.

Також можливе комбіновані методи розширення спектра, коли об'єднуються два методи DSSS та FHSS, що забезпечує досягнення максимальної завадостійкості та прихованості. Цей метод використовується у військових мережах зв’язку та захищених супутникових системах.

Методи спектрального розширення активно застосовуються у різних сферах: захищений військовий зв’язок; системи навігації (GPS, ГЛОНАСС); бездротові мережі (Wi-Fi, Bluetooth); радіоелектронна боротьба (РЕБ).

Захищений військовий зв’язок забезпечує прихованість передавання сигналів, завадостійкість та зменшення можливості перехоплення сигналу. Системи навігації (GPS, ГЛОНАСС) використовують розширення спектра для

зменшення впливу завад і покращення точності позиціонування. Бездротові мережі (Wi-Fi, Bluetooth) використовують розширення спектра для мінімізації взаємних перешкод між пристроями. Радіоелектронна боротьба (РЕБ) використовують розширення спектра для підвищення захищеності від перехоплювання сигналів засобами радіоелектронної розвідки противника.

Отже, методи спектрального розширення є потужним інструментом для підвищення захищеності інформаційних систем, забезпечуючи стійкість сигналу до глушіння, перехоплення та аналізу. Вони відіграють ключову роль у військових, навігаційних та цивільних системах зв'язку, підвищуючи рівень безпеки передавання інформації.

1.3 Розробка методів захисту інформації на основі прихованості сигнальних конструкцій

1.3.1 Аналіз методів передавання інформаційної послідовності на основі традиційних методів маніпуляції

Маніпуляція сигналу це процес зміни параметрів гармонійного (синусоїдального) сигналу-носія відповідно до цифрового повідомлення (бітової послідовності). Основна ідея полягає в тому, щоб кожному біту (0 або 1) відповідала певна зміна характеристик сигналу, що дозволяє передавати інформацію в аналоговому середовищі.

Гармонійний сигнал можна описати рівнянням:

$$s(t)=A\cdot\cos(2\pi ft+\varphi)s(t) \qquad (1.6)$$

де: A – амплітуда (висота сигналу); f – частота (кількість коливань за секунду); φ – фаза (початковий зсув сигналу); t – час.

На основі цього сигналу виділяють три основні види цифрової маніпуляції:

– амплітудна маніпуляція;

– фазова маніпуляція;

– частотна маніпуляція.

При амплітудної маніпуляції (AM, ASK — Amplitude Shift Keying) змінюється амплітуда гармонійного сигналу залежно від значення біта: біт «1» – висока амплітуда (наприклад, АА); біт «0» – низька або нульова амплітуда. Формула АМ наступна:

$$s(t)=\mathrm{Ab}\cdot\cos(2\pi ft), \tag{1.7}$$

де A_b – амплітуда, що залежить від біта.

Переваги АМ є достатня проста реалізація. До недоліку можна віднести низьку завадостійкість до шумів.

При фазової маніпуляції (ФМ, PSK – Phase Shift Keying) змінюється фаза гармонійного сигналу залежно від значення біта, тобто: біт «1» – фаза 00; біт «0» – фаза π (сигнал інвертується). Отримуємо в результаті наступну формулу:

$$\mathrm{s(t)=A}\cdot\cos(2\pi\mathrm{ft}+\varphi\mathrm{b}) \tag{1.8}$$

де: φb – фазовий зсув для кожного біта.

До переваги ФМ можна віднести високу завадостійкість. Про такий метод модуляції потребує точного синхронізатора фази.

При частотної маніпуляції (ЧМ, FSK – Frequency Shift Keying) змінюється частота гармонійного сигналу відповідно до біта. При цьому біт «1» передається частотою f_1, біт «0» – частотою f_0. Формула ЧМ наступна:

$$s(t)=\mathrm{A}\cdot\cos(2\pi f_b t) \tag{1.9}$$

де: $f_b \in \{f_0, f_1\}$ – частота, що залежить від значення біта.

До переваги ЧМ можна віднести достатньо високу завадостійкість, тобто таки сигнали можна передавати в умовах високого рівня завад. Проте, сигнали ЧМ потребують більшого спектрального ресурсу.

Порівняльна характеристика методів маніпуляції надана в табл. 1.1.

Таблиця 1.1. Порівняльна характеристика методів маніпуляції

Параметр	**ASK**	**PSK**	**FSK**
Маніпульований параметр	Амплітуда	Фаза	Частота
Завадостійкість	Низька	Середня/висока	Висока
Складність реалізації	Низька	Середня	Вища

Такі методи маніпуляції широко застосовуються у радіозв'язку, телекомунікаціях, проте наявність гармонійного коливання є ознаком демаскуючого показника. Це є причиною, що такі сигнали досить легко перехоплюються засобами радіоелектронної розвідки.

Нижче наведена програма АМ з використанням гармонічним сигналу, що розроблена на мові програмування Pyton:

```
import numpy as np
import matplotlib.pyplot as plt

# --- Вхідне повідомлення ---
message_bits = [1, 0, 1, 1, 0, 0, 1, 0]

# --- Параметри ---
samples_per_bit = 100
bit_duration = 1  # в умовних одиницях часу
f_carrier = 10    # частота гармонічного сигналу (Hz)
fs = samples_per_bit / bit_duration  # частота дискретизації

# --- Створення гармонічного носія ---
t = np.linspace(0, len(message_bits) * bit_duration, len(message_bits) * samples_per_bit, endpoint=False)
carrier = np.sin(2 * np.pi * f_carrier * t)
```

```
# --- Амплітудна модуляція (ASK) ---
modulated_signal = np.zeros_like(t)
bit_signal = np.zeros_like(t)

for i, bit in enumerate(message_bits):
    start = i * samples_per_bit
    end = (i + 1) * samples_per_bit
    if bit == 1:
        modulated_signal[start:end] = carrier[start:end]
    else:
        modulated_signal[start:end] = 0
    bit_signal[start:end] = bit

# --- Побудова графіка ---
plt.figure(figsize=(14, 6))
plt.plot(bit_signal, 'r--', label='Цифровий сигнал (біти)', linewidth=1)
plt.plot(modulated_signal, 'b', label='Амплітудно модульований сигнал (ASK)', linewidth=1)
for i in range(1, len(message_bits)):
    plt.axvline(i * samples_per_bit, color='gray', linestyle='--', linewidth=0.5)
plt.title("Амплітудна маніпуляція цифрового сигналу з гармонічним носієм")
plt.xlabel("Зразки")
plt.ylabel("Амплітуда")
plt.grid(True)
plt.legend(loc='upper right')
plt.tight_layout()
plt.show()
```

На рис. 1.9 наведена часова діаграма перетворення послідовності 10110010 за допомогою АМ з використанням гармонічним сигналу.

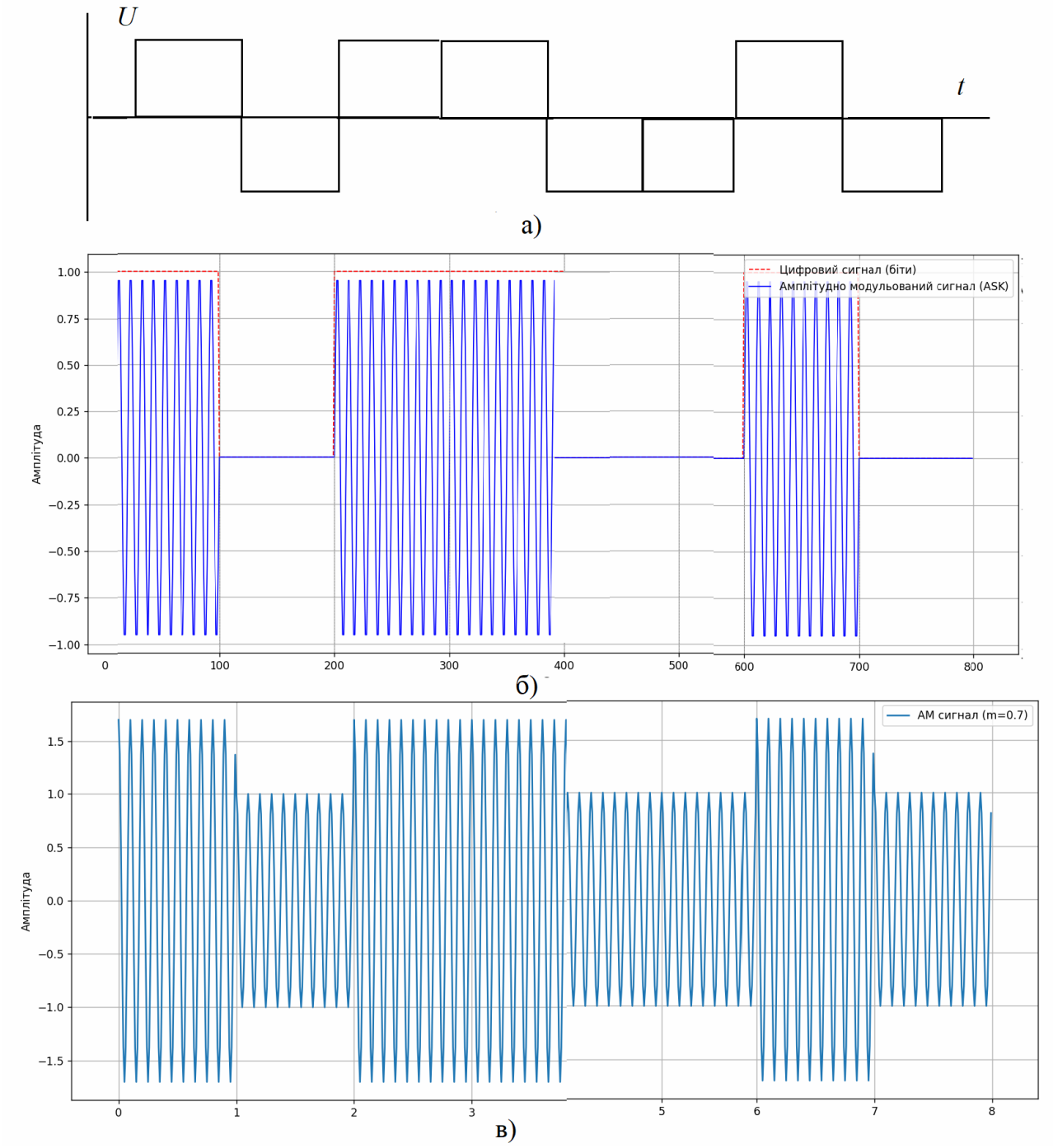


Рисунок 1.9. Часова діаграма перетворення послідовності 10110010 за допомогою АМ

Нижче наведена програма ФМ з використанням гармонічним сигналу, що розроблена на мові програмування Pyton:

```
import numpy as np
import matplotlib.pyplot as plt
```

```
# --- Вхідне повідомлення ---
message_bits = [1, 0, 1, 1, 0, 0, 1, 0]

# --- Параметри ---
samples_per_bit = 100
bit_duration = 1
f_carrier = 5  # Зменшено у 2 рази з 10 до 5 Гц

# --- Часова шкала ---
total_samples = len(message_bits) * samples_per_bit
t = np.linspace(0, len(message_bits) * bit_duration, total_samples, endpoint=False)

# --- Повторення бітів ---
message_signal = np.repeat(message_bits, samples_per_bit)

# --- Генерація PSK сигналу ---
# Якщо біт 1 -> фаза 0, якщо біт 0 -> фаза π (інверсія)
phase_shifts = np.pi * (1 - message_signal)  # 0 або π
psk = np.cos(2 * np.pi * f_carrier * t + phase_shifts)

# --- Візуалізація ---
plt.figure(figsize=(12, 4))
plt.plot(t, psk, label='Фазова маніпуляція (BPSK)', color='purple')
plt.title("Фазова маніпуляція (BPSK) із зменшеною частотою")
plt.xlabel("Час (с)")
plt.ylabel("Амплітуда")
plt.grid(True)
plt.legend()
plt.tight_layout()
```

plt.show()

На рис. 1.10 представлена часова діаграма перетворення послідовності 10110010 за допомогою ЧМ.

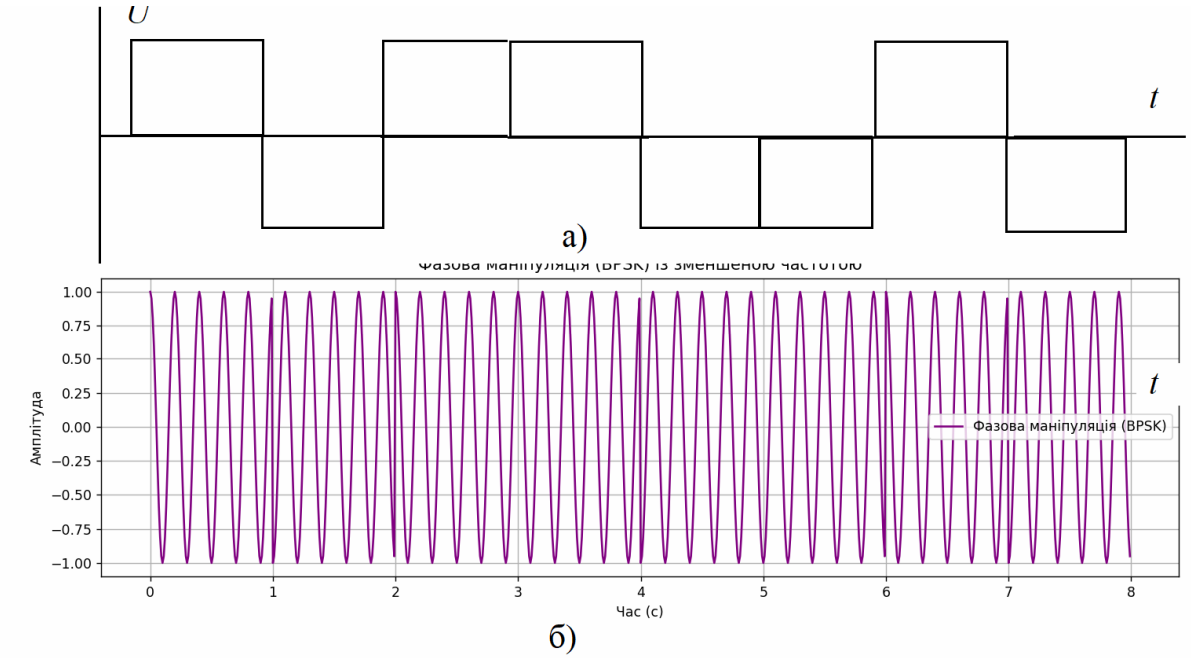


Рисунок 1.10. Часова діаграма перетворення послідовності 10110010 за допомогою ЧМ

1.3.2 Аналіз демаскуючих ознак сигнальних конструкцій

У класичних системах цифрової передачі інформації широко застосовуються методи маніпуляції сигналу на основі гармонійних коливань, такі як амплітудна (АМ – ASK), частотна (ЧМ – FSK) та фазова (ФМ – PSK) маніпуляції. Хоча ці методи є ефективними з точки зору реалізації, спектральної ефективності та стійкості до шумів, вони мають низку демаскувальних ознак, що значно знижують їхню придатність для використання в умовах радіоелектронної боротьби (РЕБ) або при потребі в прихованій передачі даних.

Розглянемо наступні демаскуючі ознаки гармонійних методів:

1) спектральна складова;

2) статична структура сигналу;

3) Низька ентропія;

4) синхронізація за гармонікою.

Для гармонійних сигналів характерна певна спектральна складова із вузькими піками на визначених частотах, які легко виявляються засобами радіотехнічної розвідки. Спектральний аналіз дозволяє точно локалізувати носій сигналу навіть за низького рівня потужності.

Незалежно від інформаційного навантаження, гармонійні сигнали з маніпуляцією зберігають передбачувану форму, тобто вони мають певну статичну структура сигналу. Це спрощує аналіз та подальше дешифрування або подавлення сигналу з боку противника.

Сигнали з гармонійною структурою мають низький рівень ентропії, тобто вони добре піддаються статистичному аналізу, що полегшує їх виявлення у фоновому шумі.

Синхронізація за гармонікою: часто виявлення можливо провести за допомогою фіксації початку періоду або фази сигналу. Гармонійність дозволяє точно визначити повторюваність сигналу, що є ще одним фактором демаскування.

До переваги хаотичних коливань для прихованої передачі можна віднести наступе. На відміну від гармонійних сигналів, хаотичні коливання мають ряд властивостей, що роблять їх ідеальними для прихованого передавання сигналів, особливо в умовах РЕБ та активної протидії противника.

До основних переваг використання хаотичних коливань можна визначити наступне:

1) широкий спектр;

2) висока ентропія;

3) чутливість до початкових умов;

4) синхронізація тільки з ідентичними хаотичними системами.

Хаотичні сигнали мають широкий, майже рівномірний спектр, подібний до шуму. Це ускладнює їх виявлення за допомогою класичних методів спектрального аналізу.

Завдяки неперіодичності та непередбачуваності, хаотичні сигнали мають високу ентропію, що забезпечує їхню імітозахищеність та складність відділення від природних завад.

Для правильного прийому та демодуляції хаотичного сигналу необхідне точне знання параметрів генератора (наприклад, логістичної функції чи системи Лоренца), що значно ускладнює несанкціонований доступ до інформації.

Для декодування сигналу потрібен аналогічний хаотичний генератор, синхронізований за фазою та параметрами. Це практично унеможливлює перехоплення без відповідної структури приймача.

Хаотичні сигнали добре підходять для прихованого вбудовування інформації (наприклад, у фоновий шум або інші сигнали), що підвищує рівень скритності комунікацій.

Таким чином, методи цифрової маніпуляції на основі гармонійних сигналів є ефективними, проте легко виявляються за спектральними та статистичними ознаками. У противагу їм, використання хаотичних коливань для амплітудної, фазової чи частотної модуляції дозволяє забезпечити високу прихованість, стійкість до виявлення, та додатковий рівень безпеки, що є особливо критичним у військових та захищених каналах зв'язку.

1.3.3 Прихований метод передавання на основі амплітудної маніпуляції інформаційного сигналу хаотичними коливаннями

Розглянемо процес розробки програми на мові програмування Python, яка демонструє амплітудну модуляцію інформаційного сигналу на основі логістичного відображення (logistic map), тобто генератора хаосу. У цьому випадку:

1) логістичне відображення використовується для формування хаотичної несучої;

2) бінарне повідомлення (0 або 1) амплітудно модулює цей сигнал (наприклад, 0 → низька амплітуда, 1 → висока амплітуда).

Нижче наведена програма реалізації амплітудної модуляції з логістичним відображенням на мові програмування Python:

```
import numpy as np
import matplotlib.pyplot as plt

# --- Параметри логістичного відображення ---
r = 3.99  # параметр хаотичності (3.57–4 — хаос)
x0 = 0.5  # початкове значення

# --- Вхідне повідомлення (бінарна послідовність) ---
message_bits = [1, 0, 1, 1, 0, 0, 1, 0]

# --- Кількість зразків на біт ---
samples_per_bit = 100

# --- Функція генерації логістичної послідовності ---
def generate_logistic_sequence(length, r, x0):
    x = x0
    seq = []
    for _ in range(length):
        x = r * x * (1 - x)
        seq.append(x)
    return np.array(seq)

# --- Генерація хаотичної несучої ---
total_samples = len(message_bits) * samples_per_bit
chaotic_carrier = generate_logistic_sequence(total_samples, r, x0)

# --- Амплітудна модуляція повідомлення ---
modulated_signal = np.zeros(total_samples)
```

```
for i, bit in enumerate(message_bits):
    amplitude = 1.0 if bit == 1 else 0.3  # модуляція: 1 -> висока амплітуда, 0 -> низька
    modulated_signal[i * samples_per_bit:(i + 1) * samples_per_bit] = amplitude * chaotic_carrier[i * samples_per_bit:(i + 1) * samples_per_bit]

# --- Візуалізація ---
plt.figure(figsize=(12, 6))
plt.plot(modulated_signal, label='Модульований сигнал')
plt.title("Модуляція інформації в хаотичному сигналі (логістичне відображення)")
plt.xlabel("Зразки")
plt.ylabel("Амплітуда")
plt.grid(True)
plt.legend()
plt.tight_layout()
plt.show()
```

В цій програмі логістичне відображення $x[n+1] = r * x[n] * (1 - x[n])$ генерує хаотичну послідовність. Кожен біт повідомлення визначає амплітуду хаотичного сигналу на відповідному фрагменті часу. Такий підхід ускладнює розпізнавання повідомлення сторонніми особами без знання:

1) параметра r;

2) початкового стану x_0;

3) схеми модуляції.

Часові діаграми амплітудної модуляції інформаційного сигналу 1, 0, 1, 1, 0, 0, 1, 0 на основі логістичного відображення надано на рис. 1.11.

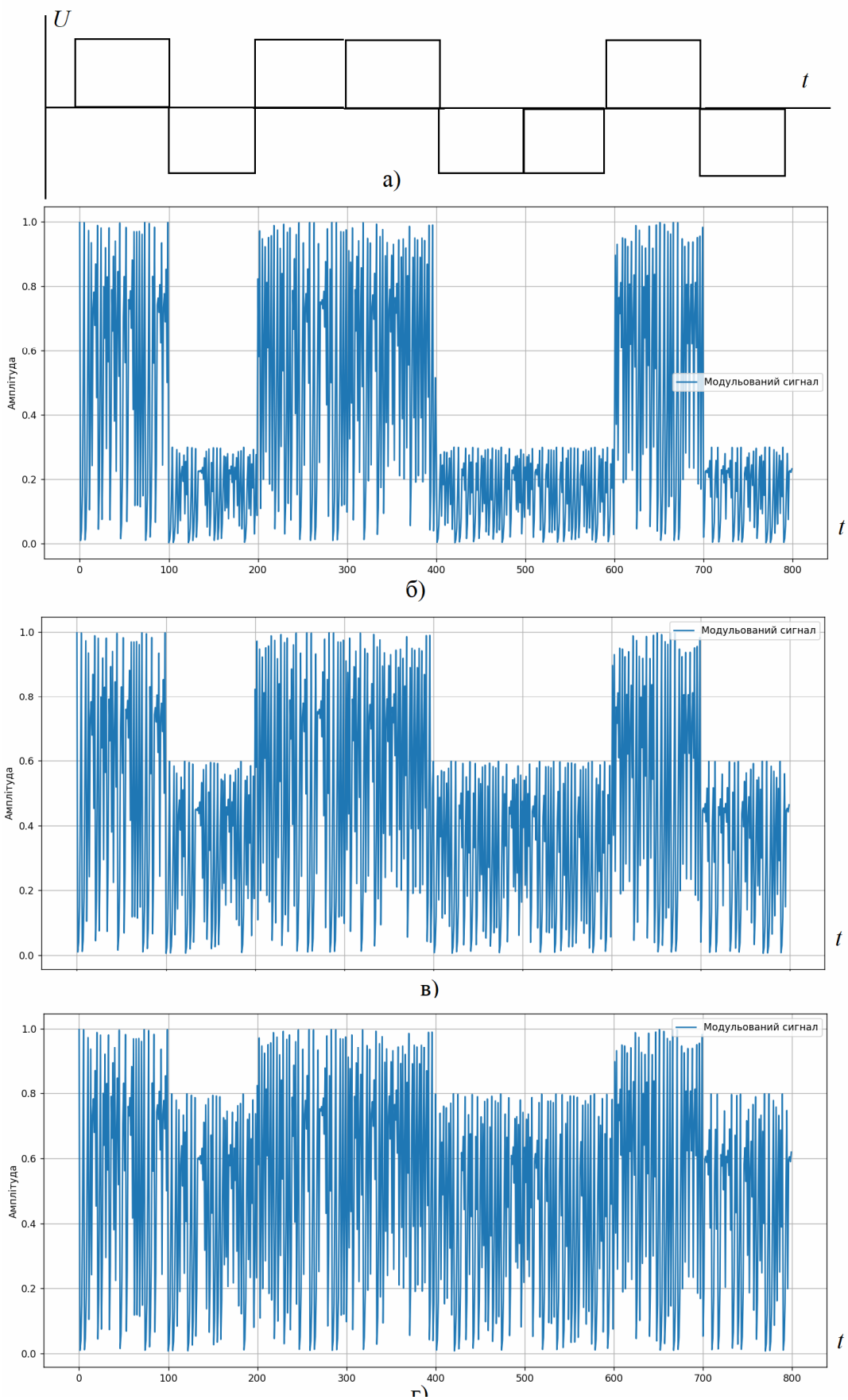


Рисунок 1.11. Часові діаграми амплітудної модуляції інформаційного сигналу на основі логістичного відображення

1.3.4 Прихований метод передавання на основі фахової маніпуляції інформаційного сигналу хаотичним коливанням

Розглянемо процес фазової модуляції інформаційного сигналу в хаотичному сигналі, з використанням логістичного відображення. У цій реалізації. При цьому відбувається наступне:

1) використовується логістична послідовність як базовий (хаотичний) сигнал;

2) для біта 1 – сигнал передається як є;

3) для біта 0 – сигнал інвертується (фаза зсувається на π, тобто 180°).

Python-програма фазової модуляція з хаотичним сигналом представлена нижче:

```
import numpy as np
import matplotlib.pyplot as plt

# --- Параметри логістичного відображення ---
r = 3.9      # коефіцієнт хаосу
x0 = 0.4     # початкове значення

# --- Вхідне повідомлення (бітова послідовність) ---
message_bits = [1, 0, 1, 1, 0, 0, 1, 0]

# --- Кількість зразків на біт ---
samples_per_bit = 100
total_samples = len(message_bits) * samples_per_bit

# --- Несуча частота ---
carrier_freq = 10  # Гц
t = np.linspace(0, len(message_bits), total_samples)  # нормалізований час
```

```
# --- Функція для генерації логістичної послідовності ---
def generate_logistic_sequence(length, r, x0):
    x = x0
    seq = []
    for _ in range(length):
        x = r * x * (1 - x)
        seq.append(x)
    return np.array(seq)

# --- Генерація хаотичної послідовності (огинаюча) ---
chaotic_carrier = generate_logistic_sequence(total_samples, r, x0)

# --- Фазова модуляція ---
modulated_signal = np.zeros(total_samples)
for i, bit in enumerate(message_bits):
    start = i * samples_per_bit
    end = (i + 1) * samples_per_bit
    segment_time = t[start:end]
        # Фазовий зсув: 0 для '1', π для '0'
    phase_shift = 0 if bit == 1 else np.pi
        # Синусоїда з хаотичною огинаючою
    segment = chaotic_carrier[start:end] * np.sin(2 * np.pi * carrier_freq *
segment_time + phase_shift)
        # Залишаємо в одній півплощині (всі значення позитивні)
    modulated_signal[start:end] = np.abs(segment)
# --- Візуалізація ---
plt.figure(figsize=(12, 6))
plt.plot(modulated_signal, label='Фазово модульований сигнал (в одній
площині)')
```

```
plt.title("Фазова модуляція в хаотичному сигналі (логістичне відображення, одна півплощина)")
plt.xlabel("Зразки")
plt.ylabel("Амплітуда")
plt.grid(True)
plt.legend()
plt.tight_layout()
plt.show()
```

В цій програмі segment = -segment виконує фазовий зсув на 180° (інверсія).

Таким чином, вбудована інформація маскується в хаотичному сигналі, і без знання параметрів логістичного генератора та схеми модуляції її дуже складно виділити.

Часові діаграми фазової модуляції інформаційного сигналу 1, 0, 1, 1, 0, 0, 1, 0 на основі логістичного відображення надано на рис. 1.12.

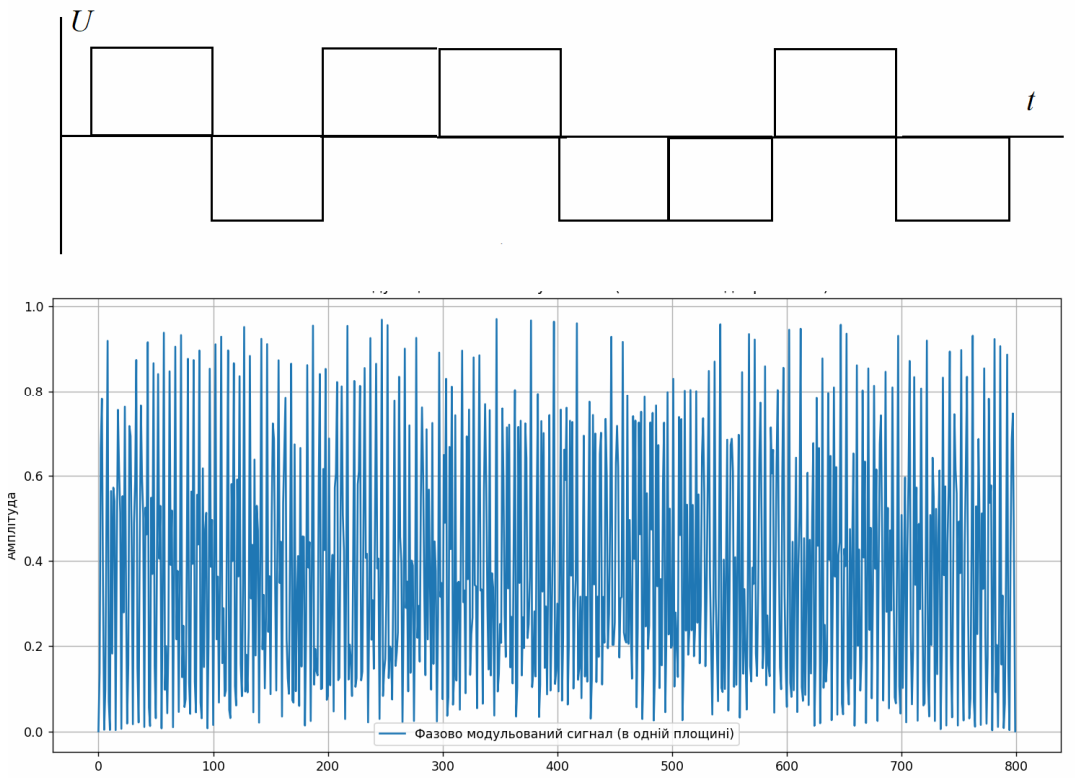


Рисунок 1.12. Часові діаграми фазової модуляції інформаційного сигналу на основі логістичного відображення

2 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Науково-технічний прогрес суттєво вплинув на умови праці програмістів, зробивши їхню діяльність більш інтенсивною та напруженою, що вимагає значних витрат розумових, емоційних і фізичних ресурсів. Це зумовило необхідність комплексного підходу до питань ергономіки, гігієни, організації робочого процесу, а також впровадження чітких регламентів щодо режимів праці та відпочинку.

Сьогодні комп'ютерні технології активно використовуються у всіх сферах людської діяльності. Однак робота програміста передбачає вплив низки потенційно небезпечних факторів, таких як електромагнітне поле, інфрачервоне та іонізуюче випромінювання, шум, вібрація, статична електрика.

Практична значущість роботи полягає в отриманні результатів, які можуть бути використані для розробки нових засобів захисту інформації, що забезпечують збереження її конфіденційності та підвищують стійкість до виявлення з боку зловмисників. Запропоновані методи можуть знайти застосування у військовій сфері, державних органах, а також у комерційних компаніях, що працюють з критичною інформацією.

2.1 Аналіз небезпечних і шкідливих чинників, що впливають на програміста

На багатьох офісних підприємствах програмісти та інші фахівці, що працюють із комп'ютерними системами, стикаються з несприятливими умовами праці. Шкідливі та небезпечні виробничі фактори тісно взаємопов’язані та можуть значно впливати на самопочуття і продуктивність працівників.

Усі шкідливі фактори умовно поділяються на такі групи:

Фізичні – охоплюють різноманітні зовнішні умови, що впливають на організм.

Психофізіологічні—напружений робочий ритм, високі навантаження та стрес.

Деякі фактори є неминучими у робочому середовищі. Серед найбільш

значущих:

Температурний режим, підвищена вологість та різні види випромінювання.

Електромагнітні поля.

Шумове навантаження.

Освітлення – надмірна яскравість чи недостатня освітленість, що негативно впливає на зір.

Окремо ці фактори можуть не становити серйозної загрози, але їх поєднання та тривалий вплив можуть призводити до відчутних наслідків для здоров’я працівників.

2.2 Розробка заходів з охорони праці

Охорона праці на виробництві—важливий аспект, що впливає на ефективність і безпеку діяльності підприємства. Для забезпечення комфортних умов роботи необхідно розробити заходи, спрямовані на мінімізацію ризиків. Вони визначаються відповідно до загальних завдань компанії та специфіки робочого процесу.

Одним із ключових напрямків є ергономічне проектування робочих місць із відеотерміналами. Важливо, щоб робочий простір відповідав антропометричним, фізичним і психологічним вимогам працівників. Відповідність цим критеріям сприяє зниженню втоми, підвищенню продуктивності та зменшенню негативного впливу робочого середовища.

При організації робочого місця програміста слід враховувати такі основні вимоги:

Оптимальне розташування обладнання, що забезпечує зручність у роботі.

Достатній робочий простір, який дає можливість комфортно виконувати всі необхідні дії.

Врахування характеру роботи, зокрема необхідність тривалого перебування за комп’ютером.

Створення сприятливого робочого середовища сприяє покращенню здоров'я працівників та підвищенню їхньої продуктивності.

2.2.1 Виробниче освітлення

Робота з обчислювальною технікою створює певні виробничі фактори, що можуть впливати на комфорт та ефективність працівника. Серед них:

Ймовірність виникнення прямої блискості, що може спричиняти дискомфорт і підвищене навантаження на очі.

Погіршення контрастності між зображенням і фоном, що ускладнює сприйняття інформації.

Розмитість зображення на екрані, що впливає на якість роботи та візуальну зручність.

Через недостатню інтенсивність природного освітлення необхідне використання штучного світла. У дипломному проєкті запропоновано встановити два світильники типу ЛДР (2×40 Вт), загальний світловий потік яких становить 5700 лм. Таке розташування освітлення покликане забезпечити оптимальні умови роботи та зменшити вплив шкідливих факторів рис.2.1.

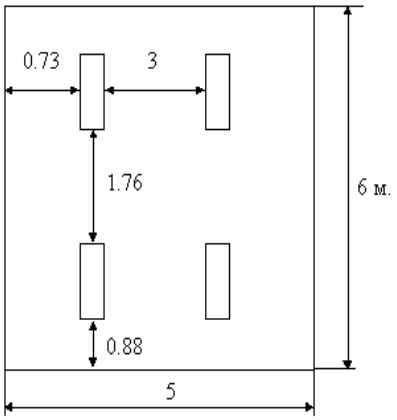


Рисунок 2.1 Схема розташування світильників

2.2.2 Шум, вібрація

На підприємствах, де в офісах стоять комп'ютери та інше обладнання, без шуму, як правило, не обходиться. Постійно працює техніка видає гучні звуки, які можуть змінювати свою інтенсивність від стану навантаження системи. Якщо людина змушена регулярно зазнавати такого впливу, то це негативно позначиться на його здоров'ї. Від сильного шуму починає боліти голова,

підвищується тиск, знижується гострота слуху. Зменшення негативного впливу шуму на працівника для цього рекомендують використовувати:

- виробляти звукоізоляцію галасливих місць з допомогою використання захисних кожухів, обладнання кабінок;
- оздоблення приміщень звукопоглинаючими матеріалами;
- облицювання стелі та стін звукопоглинальним матеріалом (знижує шум на 6-8 дб);
- екранування робочого місця (постановкою перегородок, діафрагм);
- установка в комп'ютерних приміщеннях обладнання, що виробляє мінімальний шум.

2.2.3 Організація робочого місця програміста

При організації робочого місця програміста повинно бути дотримані наступні основні умови: оптимальне розміщення устаткування, що до складу робочого місця і достатній робочий простір, що дозволяє здійснювати всі необхідні рухи і переміщення (рис. 2.2).

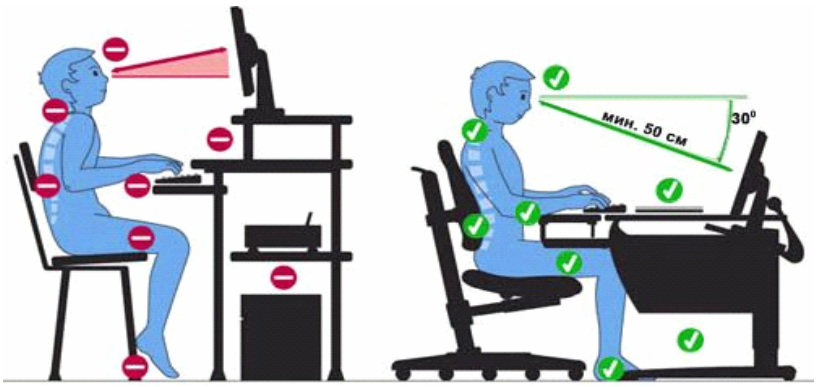


Рисунок 2.2. Організація робочого місця програміста

Робота програміста передбачає тривале перебування в сидячому положенні, що може негативно впливати на опорно-руховий апарат через недостатню рухливість. Особливу роль у цьому процесі відіграє плечовий пояс, адже будь-яке переміщення рук впливає не тільки на м’язи спини, а й на положення хребта, тазу та навіть ніг. Щоб уникнути негативних наслідків, важливо дотримуватися режиму праці та відпочинку, регулярно змінювати

положення тіла та виконувати фізичні вправи, які активізують незадіяні групи м’язів.

Щодо робочого місця, для комфортної роботи програміста необхідно, щоб його площа становила не менше 6 м², висота приміщення 4 м, а обсяг—20 м³ на одну людину. Однак аналіз реальних робочих місць показав, що ці параметри часто не відповідають стандартам, що може негативно позначатися на продуктивності та здоров’ї працівника.

Для покращення умов роботи програміста пропонується:

Робочий стіл: висота поверхні 720 мм (бажано регульована в межах 680-780 мм).

Розміри столу: 1600 × 1000 мм.

Простір для ніг: глибина 650 мм.

Підставка для ніг: довжина 400 мм, ширина 350 мм, нахил 15°.

Розташування клавіатури: не більше 300 мм від краю столу для комфортної опори передпліч.

Відстань між очима та екраном: 40-80 см, що забезпечує оптимальну видимість без надмірного навантаження на очі.

Правильна організація робочого місця не лише сприяє збереженню здоров’я працівника, а й підвищує його продуктивність. Якщо потрібно, можу допомогти додатково оптимізувати опис або внести коригування (рис. 2.3).

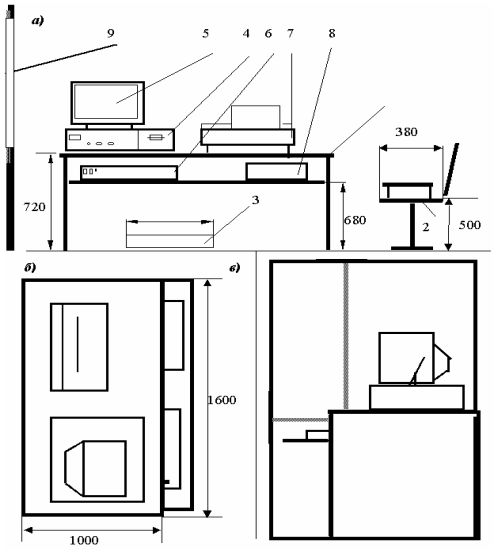


Рисунок 2.3. Розташування техніки на робочому місці програміста

ВИСНОВКИ

У кваліфікаційній роботі було проведено дослідження методів захисту інформації, що базуються на прихованості сигнальних конструкцій. На основі аналізу сучасних загроз інформаційній безпеці встановлено, що традиційні методи криптографічного захисту не завжди є достатніми в умовах складного інформаційного середовища та активного протиборства, особливо у військових та спеціалізованих телекомунікаційних системах.

Розглянуто основні методи атаки на інформаційні системи, зокрема соціальну інженерію, MITM-атаки, DDoS, фішинг та інші. Це дозволило обґрунтувати необхідність використання додаткових засобів захисту, таких як прихована передача даних.

Особливу увагу було приділено методам стеганографії, спектрального розширення та використанню хаотичних коливань для маскування сигнальних конструкцій. Практична частина роботи продемонструвала реалізацію амплітудної та фазової маніпуляції інформаційних сигналів на основі як гармонійних, так і хаотичних процесів, що дозволило порівняти їх ефективність.

Доведено, що методи на основі гармонійних сигналів мають характерні демаскувальні ознаки, які можуть бути виявлені при аналізі спектру або форми сигналу. Водночас використання хаотичних коливань забезпечує високий рівень прихованості передавання, оскільки такі сигнали наближені до шумових і мають широку смугу частот та високу ентропію.

Таким чином, результати дослідження підтверджують доцільність застосування методів прихованої передачі на основі хаотичних сигналів для підвищення стійкості інформаційних систем до перехоплення та аналізу. Запропонований підхід може бути використаний як у системах спеціального зв’язку, так і у цивільних захищених комунікаціях.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.

2. Остапов С. Е. Технології захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

3. Методи та засоби захисту інформації: Навчальний посібник для студентів вищих навчальних закладів./А.М. Олейніков. –Харків: НТМТ, 2014. –298с.

4. Фізичні основи захисту інформації в радіоелектронній апаратурі: навч. посіб./ Д.В. Євграфов. –К.:НТУУ"КПІ", 2014. –176с.

5. Тестування на проникнення: навч. посіб. Ч.1 / [Є.О. Живило]; за ред. Є.О. Живило. – П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2024. – 134 с.

6. Моніторинг інформаційних технологій [Електронний ресурс] – Режим доступу до ресурсу: https://pidru4niki.com/75828/ekonomika/monitoring_informatsiynih_tehnologiy.

7. Аудит інформаційних систем [Електронний ресурс] – Режим доступу до ресурсу: http://www.infocity.kharkov.ua/uk/static/audit-informatsiynih-sistem-49.html.

8. Ilyenko A. СУЧАСНІ МЕТОДИ АУДИТУ ТА МОНІТОРИНГУ В ЗАДАЧАХ ЗАХИСТУ ІНФОРМАЦІЇ [Електронний ресурс] / Anna Ilyenko // Researchgate. – 2018. – Режим доступу до ресурсу: https://www.researchgate.net/publication/328828497_SUCASNI_METODI_AUDITU_TA_MONITORINGU_V_ZADACAH_ZAHISTU_INFORMACII.

9. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ФОП Ямчинський О.В., 2020. – 445 с.

10. Ряба Л.С. Основи кібербезпеки: навчальний посібник. Рівне: Вище професійне училище №1, 2021, 170 с.

11. Основи інформаційної безпеки: навч. посібник/ В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020,128 с.

12. Основи управління інформаційною безпекою: навч. посібник /А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020,144 с.

ДОДАТОК А

Слайди мультимедійної презентації

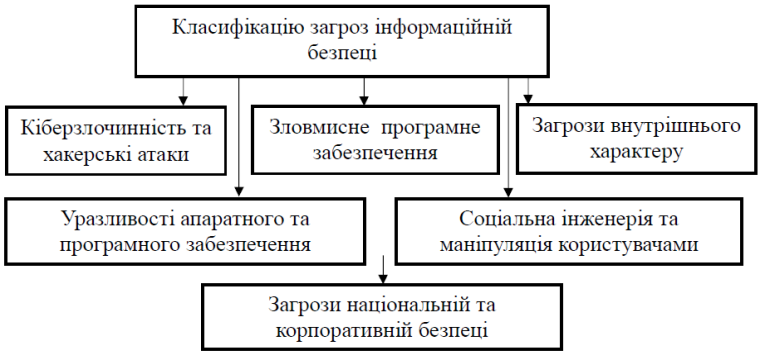
ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ПРИХОВАНОСТІ СИГНАЛЬНИХ КОНСТРУКЦІЙ

КВАЛІФІКАЦІЙНА РОБОТА

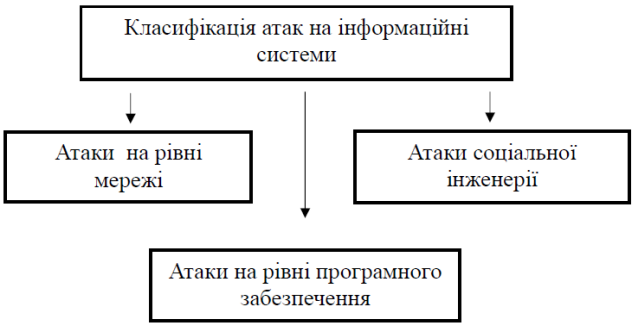
Дипломник: Хабібулін І.Р.
Керівник: Кільдішев В.Й.

2025

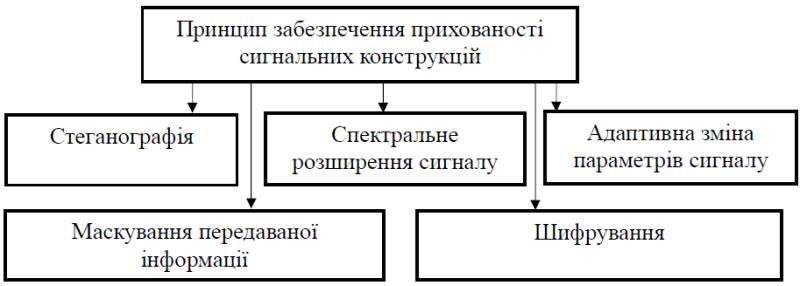
Класифікація загроз інформаційній безпеці підприємства



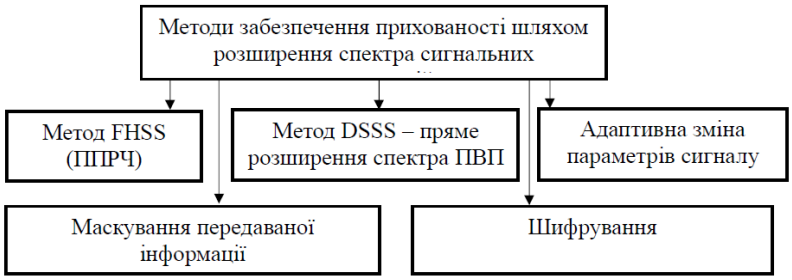
Класифікація атак на інформаційні системи



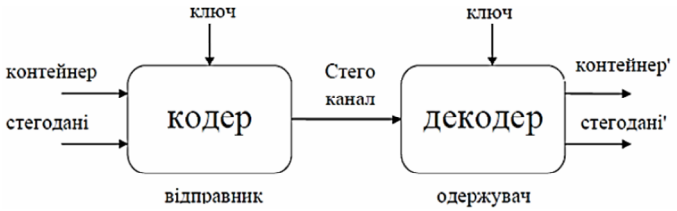
Забезпечення прихованості сигнальних конструкцій



Забезпечення прихованості сигнальних конструкцій шляхом розширення спектра



Модель каналу з використанням стеганографії

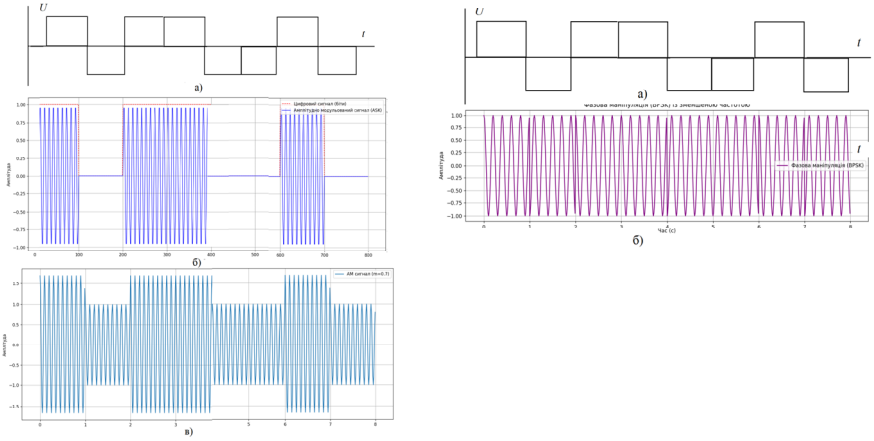


Доцільність використання динамічного хаосу в системах зв’язку для забезпечення прихованості передавання інформації

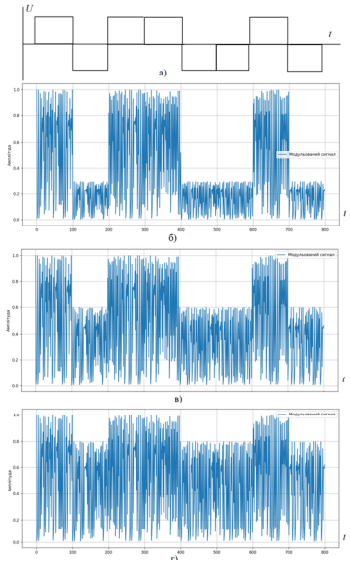
Порівняльна характеристика методів маніпуляції

Параметр	ASK	PSK	FSK
Маніпульований параметр	Амплітуда	Фаза	Частота
Завадостійкість	Низька	Середня/висока	Висока
Складність реалізації	Низька	Середня	Вища

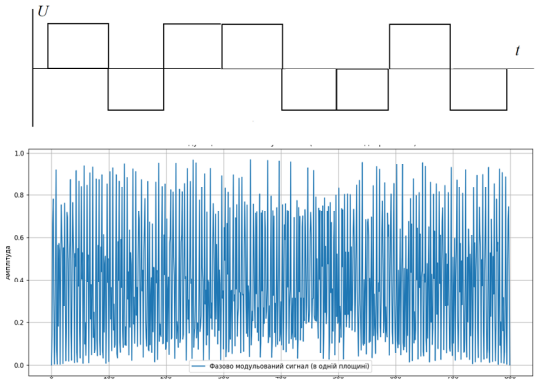
Часовф діаграми перетворення послідовності 10110010 за допомогою АМ та ЧМ



Часові діаграми амплітудної модуляції інформаційного сигналу на основі логістичного відображення



Часові діаграми фазової модуляції інформаційного сигналу на основі логістичного відображення



ДЯКУЮ ЗА УВАГУ!

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу бакалавра
відділення комп'ютерних систем

Хабібуліна Іллі Руслановича

(прізвище, ім`я та по батькові)

Спеціальність *123 «Комп'ютерна інженерія»*

Керівник дипломного проекту (роботи) *Кільдішев Віталій Йосипович*

(прізвище, ім`я та по батькові)

Тема кваліфікаційної роботи бакалавра: *Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій*

Обсяг розрахунково-пояснювальної записки *61* сторінок

Обсяг графічної частини проекту *12* аркушів

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЄКТУ (РОБОТИ)

а) Висновок про ступінь відповідальності виконаного кваліфікаційної роботи бакалавра завданню

Робота відповідає технічному завданню до дипломного проекту. Виконана у відповідності з вимогами.

б) Характеристика виконання кожного розділу проекту ступеню використання дипломником останніх досягнень науки та техніки, передових методів на виробництві

При виконанні дипломної роботи студент продемонстрував уміння використовувати останні досягнення науки та техніки, уміння працювати з літературою. Так, студент грамотно дослідив та проаналізував алгоритми та технології реалізації методів прихованого передавання інформації в інформаційних системах.

в) Оцінка якості виконання графічної частини проєкту (роботи) і пояснювальної записки

Графічна частина відповідає вимогам, виконана якісно та відображає основні елементи проектування системи. Розглянуто основні методи атаки на інформаційні системи, зокрема соціальну інженерію, MITM-атаки, DDoS, фішинг та інші.

г) Перелік позитивних якостей кваліфікаційної роботи бакалавра

Тема дипломної роботи є актуальною, виконана у достатньому обсязі, якісно, відповідно до поставленого завдання.

д) Основні недоліки кваліфікаційної роботи бакалавра

У пояснювальній записці присутні недоліки оформлення. Для підвищення ефективності захисту конфіденційної інформації було б доцільним застосувати методи спектрального розширення. Було б доцільним більш детально розглянути питання безпеки за допомогою методів стеганографії.

Оцінка розрахункової частини *Відмінно*

Оцінка графічної частини *Добре*

Загальна оцінка *Відмінно*

Прізвище, ім`я по батькові *к.т.н. Шибаєва Наталя Олегівна*

23.06.25

Місце роботи і посада рецензента *Національний університет «Одеська політехніка», доцент кафедри інформаційних технологій*

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на кваліфікаційну роботу бакалавра

відділення комп'ютерних систем

Хабібуліна Іллі Руслановича

(прізвище, ім`я та по батькові)

Спеціальність *123 «Комп'ютерна інженерія»*

Тема кваліфікаційної роботи бакалавра

Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЄКТУ (РОБОТИ)

а) Обсяг і якість виконання роботи (графічного матеріалу і розрахунково-пояснювальної записки)

Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми дипломного проекту, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дипломному проекті

Графічний матеріал виконано якісно, у достатньому обсязі. Графічний матеріал наочно демонструє результати роботи.

б) Самостійність роботи над проєктом (роботою)

Студент самостійно обрав напрям та тематику дипломного проекту. Провів аналіз існуючих рішень і зробив необхідні висновки для реалізації проекту. Виявив навички самостійно опрацьовувати новий матеріал та виконувати пошук необхідної літератури та інших джерел інформації.

в) Теоретична підготовка дипломника _____
відповідає вимогам, що надаються до бакалавра зі спеціальності _____
«Комп'ютерна Інженерія» _____
_____
_____
_____

г) Вміння розв`язувати виробничі і конструкторські питання на базі останніх досліджень науки і техніки, передових методів виробництва _____
У кваліфікаційній роботі досліджуються інтелектуальної системи захисту конфіденційних даних. Предметом дослідження є методи захисту інформації, що базуються на принципах прихованості сигнальних конструкцій. Отриманні результати можуть бути використані для розробки нових засобів захисту інформації, що забезпечують збереження її конфіденційності та підвищують стійкість до виявлення з боку зловмисників. _____
_____
_____

Оцінка розрахункової частини 4 (чотири)
Оцінка графічної частини 4 (чотири)
Загальна оцінка 4 (чотири)

Прізвище, ім`я, по батькові Кільдішев Віталій Йосипович
_____
_____

Місто роботи і посада керівника роботи к.т.н., доцент кафедри кібербезпеки та технічного захисту інформації ДУІТЗ
_____
_____

Підпис _____
«16» 06 2025р.

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Хабібулін Ілля Русланович,

здобувач освіти гр. 2БКС-29, та

Кільдішев Віталій Йосипович,
керівник випускної кваліфікаційної роботи,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи бакалавра на тему:

«Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій» (автор роботи – Хабібулін І.Р., керівник роботи – Кільдішев В.Й.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2025 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець _____ / Хабібулін І.Р. /

Керівник _____ / Кільдішев В.Й. /

«18» червня 2025 р.

ДОВІДКА

кафедри комп'ютерної інженерії
про допуск до захисту кваліфікаційної роботи
здобувача (здобувачки) освіти II курсу
відділення комп'ютерних систем групи 2БКС-29

Хабібуліна Іллі Руслановича

на тему *Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій*

Висновок відповідальної особи за проведення нормоконтролю:
пояснювальна записка до кваліфікаційної роботи виконана з некритичними порушеннями ДСТУ та оформлена відповідно до вимог Положення про дипломне проєктування

(підпис) *20.06.2025* (дата) *Петрашова В.І.* (П.І.Б.)

Висновок відповідальної особи за перевірку роботи на наявність академічного плагіату *згідно звіту про перевірку від 17.06.2025 р. значення коефіцієнту подібності в роботі становить 14,44%, коефіцієнт цитування – 1,03%.*

(підпис) *20.06.2025* (дата) *Краснокутська К.Г.* (П.І.Б.)

Попередня експертиза (малий захист) кваліфікаційної роботи

здобувача (здобувачки) освіти *Хабібуліна І.Р.* (П.І.Б.)

проведена « *20* » *червня* 2025 р.

Висновки *Пояснювальна записка до кваліфікаційної роботи виконана у повному обсязі. Випускна кваліфікаційна робота відповідає вимогам Положення про дипломне проєктування та рекомендована до захисту.*

Зав. кафедри КІ (підпис) *Іванова Л.В.* (П.І.Б.)

StrikePlagiarism.com

Дата звіту 6/17/2025
Дата редагування 6/17/2025

Документ прийнятий

Звіт подібності

метадані

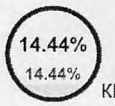
Назва організації
Odesa Technical Professional College of Odesa National University of Technology
Заголовок
Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій

Автор
Хабібулін Ілля Русланович
Науковий керівник / Експерт
Кільдішев Віталій Йосипович

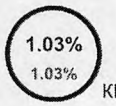
підрозділ
Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету"

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



КП 1



КЦ

25	10515	88837
Довжина фрази для коефіцієнта подібності 2	Кількість слів	Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	8
Інтервали	A→	0
Мікропробіли	·	0
Білі знаки	ß	0
Парафрази (SmartMarks)	a	63

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації [redacted] 6/15/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	272 2.59 %
2	https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download	51 0.49 %
3	https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download	46 0.44 %

4	https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download	32 0.30 %
5	Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації [redacted] 6/15/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	30 0.29 %
6	Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації [redacted] 6/15/2025 Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")	29 0.28 %
7	Розробка підсистеми “Обслуговування пасажирів” ІС аеропорту [redacted] 10/27/2024 National University of Shipbuilding named after Admiral Makarov (National University of Shipbuilding named after Admiral Makarov)	28 0.27 %
8	http://8ref.com/2/referat_28518.html	27 0.26 %
9	https://poradi.ru/suspilstvo/33817-shkidlivi-virobnichi-faktori-klasifikacija.html	24 0.23 %
10	https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download	24 0.23 %

з домашньої бази даних (10.22 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Аналіз сучасних криптографічних алгоритмів та їх ефективності у захисті конфіденційної інформації [redacted] 6/15/2025 **Odesa Technical Professional College of Odesa National University of Technology (Відокремлений структурний підрозділ "Одеський технічний фаховий коледж Одеського національного технологічного університету")**	**1075 (66) 10.22 %**

з програми обміну базами даних (0.38 %)

ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Розробка підсистеми “Обслуговування пасажирів” ІС аеропорту [redacted] 10/27/2024 **National University of Shipbuilding named after Admiral Makarov (National University of Shipbuilding named after Admiral Makarov)**	**28 (1) 0.27 %**
2	122_Барбак_Владислав_Дмитрович_2024 [redacted] 12/2/2024 Donetsk National University named after V. Stus (Donetsk National University named after V. Stus)	12 (1) 0.11 %

з Інтернету (3.83 %)

ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	**https://card-file.ontu.edu.ua/bitstreams/361286d7-8a03-4221-ad05-db5133ab5f79/download**	**193 (9) 1.84 %**
2	**http://8ref.com/2/referat_28518.html**	**42 (3) 0.40 %**
3	https://card-file.ontu.edu.ua/bitstreams/0e6c3361-ffbf-4469-86a1-fe84a1fe21cd/download	39 (3) 0.37 %
4	https://card-file.ontu.edu.ua/bitstreams/58aff421-793c-4741-a753-a286fa4b5496/download	27 (2) 0.26 %
5	https://poradi.ru/suspilstvo/33817-shkidlivi-virobnichi-faktori-klasifikacija.html	24 (1) 0.23 %

6	http://uadoc.zavantag.com/text/16872/index-1.html	20 (2) 0.19 %
7	https://card-file.ontu.edu.ua/bitstreams/549ee9fe-7574-4ae5-b500-9fe2711f33e6/download	19 (1) 0.18 %
8	http://www.tsatu.edu.ua/ophv/wp-content/uploads/sites/13/do-rozdilu-4-ohorona-praci.pdf	18 (2) 0.17 %
9	https://card-file.ontu.edu.ua/bitstreams/bbaf3f38-16a8-4070-bead-5562769b7c71/download	13 (1) 0.12 %
10	https://lektsii.org/3-116117.html	8 (1) 0.08 %

Список прийнятих фрагментів (немає прийнятих фрагментів)

ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: «Комп'ютерна інженерія»
Група: 2БКС- 29

КВАЛІФІКАЦІЙНА РОБОТА

здобувача **освіти денної форми навчання БКС.** 29.21.000.КРБ

ХАБІБУЛІНА ІЛЛІ
РУСЛАНОВИЧА

м. Одеса
2025 р. МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»
Освітньо-професійна програма: «Комп'ютерна інженерія»
Група: 2 БКС-29

ПОЯСНЮВАЛЬНА **ЗАПИСКА До кваліфікаційної роботи бакалавра на тему:**_____
_____
_____ **Проектний матеріал складається з пояснювальної записки на** _____ **сторінках та графічного (презентаційного) матеріалу на** _____ **аркушах (слайдах)** Виконавець_____(Хабібулін І.Р.)
Керівник проекту_____(Кільдішев В. Й.)

Консультанти: з розділу охорони праці та техніки безпеки _____ (Чорновол Н.І.) з нормоконтролю _____(Петрашова В.І.) старший консультант _____(Кривченко Ю. В.) До захисту допущений
Завідувач кафедри _____ (Іванова Л.В.) Завідувач відділенням _____ (Краснокутська К.Г.)

Захист «____»_____ 202____ р. Протокол ЕК No_____
Оцінка ЕК _____

Секретар ЕК _____

«Дослідження методів захисту інформації на основі прихованості сигнальних конструкцій»

АНОТАЦІЯ

Метою даної роботи є розробка методів захисту інформації в інформаційно-комунікаційних системах шляхом інтеграції шифрування, таймерного кодування та методів спектрального розширення сигналу для забезпечення підвищеного рівня прихованості та завадостійкості в умовах деструктивного впливу радіоелектронних засобів протидії.
Вивчено закономірності впливу параметрів таймерного кодування,