КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1113
УДК 004.49

Черниш Юлія Олександрівна
старша наукова співробітниця
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0002-6626-5656
yuliia.chernysch@viti.edu.ua

Терещенко Тетяна Павлівна
старша наукова співробітниця
Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна
ORCID: 0000-0002-9659-7897
tetiana.tereshchenko@viti.edu.ua

Терещенко Катерина Володимирівна
студентка
Державний університет "Київський авіаційний інститут" , Київ, Україна
ORCID: 0009-0008-8469-9854
katerina60411@gmail.com

КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ – ДОСЛІДЖЕННЯ ТА МОДЕЛЮВАННЯ

Анотація. Автоматизовані системи накопичують величезні обсяги даних, у тому числі конфіденційного характеру, що робить питання їх безпеки особливо актуальним. Глобалізація водночас зумовила появу нових викликів, пов'язаних із захистом інформації. Характерними рисами сучасного використання обчислювальної техніки є зростання ролі автоматизованих процесів, підвищення відповідальності рішень, прийнятих на їх основі, інтеграція інформаційних ресурсів у масштабні бази даних, забезпечення віддаленого доступу для великої кількості користувачів та ускладнення режимів функціонування технічних засобів. Виявлення, аналіз та моделювання каналів витоку інформації, а також оцінка потенційних ризиків для інформаційної безпеки користувачів є важливим завданням. Тому предметом дослідження є канали витоку інформації, що виникають у процесі функціонування інформаційно-комунікаційних систем і засобів обчислювальної техніки, зокрема комп'ютерних мереж, веббраузерів та мультимедійних файлів.
Будь-які порушення конфіденційності, цілісності чи доступності інформації можуть спричинити серйозні наслідки – від фінансових збитків і зниження ефективності діяльності підприємств до підриву репутації або навіть створення загроз національній безпеці. Саме тому питання класифікації інформаційних ресурсів, а також виявлення і аналізу можливих каналів витоку даних набувають особливої актуальності.
Метою роботи є аналіз методів та механізмів реалізації каналів витоку інформації, зокрема мережевих протоколів (HTTP, DNS, TCP/UDP), автоматичну передачу даних браузерами (cookies, referer, user-agent, сесійні токени), електромагнітні та акустичні канали побічних випромінювань, а також стеганографічні способи прихованої передачі повідомлень у графічних файлах.
Дослідження дозволило всебічно дослідити деякі канали витоку інформації, ознайомитися з методами їх виявлення та оцінити ризики для безпеки користувача.

Ключові слова: канали витоку інформації, аналіз трафіку, мережні підключення, перехоплення пакетів.

ВСТУП

У сучасних умовах науково-технічний прогрес, що охопив сферу інформатизації суспільства, досяг безпрецедентних масштабів. Використання обчислювальної техніки, новітніх засобів зв'язку та методів автоматизованої обробки даних стало невід'ємною складовою всіх сфер діяльності людини. Інформація один із найцінніших ресурсів та

ключових факторів економічного й технологічного розвитку. Доступ до своєчасних і достовірних відомостей забезпечує конкурентні переваги та визначає успіх у будь-якій сфері. Саме тому інформаційний ресурс розглядається вже, як стратегічний актив, що формує основу сучасного управління, науки та виробництва.

Глобалізація водночас зумовила появу нових викликів, пов'язаних із захистом інформації. Автоматизовані системи накопичують величезні обсяги даних, у тому числі конфіденційного характеру, що робить питання їх безпеки особливо актуальним. Характерними рисами сучасного використання обчислювальної техніки є зростання ролі автоматизованих процесів, підвищення відповідальності рішень, прийнятих на їх основі, інтеграція інформаційних ресурсів у масштабні бази даних, забезпечення віддаленого доступу для великої кількості користувачів та ускладнення режимів функціонування технічних засобів.

Разом із підвищенням ефективності обробки інформації зростає й небезпека її витоку або несанкціонованої модифікації. Саме тому питання інформаційної безпеки виходить на перший план, метою якої є забезпечення збереження конфіденційності, цілісності й доступності інформаційних ресурсів, що циркулюють в автоматизованих системах. Таким чином, у сучасних умовах проблема захисту інформації має комплексний характер і вимагає поєднання організаційних, технічних та програмних методів. Вона є ключовим аспектом функціонування будь-якої інформаційної системи, адже лише за умови надійного захисту даних можливе ефективне використання інформаційних ресурсів[1].

Постановка проблеми. Виявлення, аналіз та моделювання каналів витоку інформації, а також оцінка потенційних ризиків для інформаційної безпеки користувачів є важливим завданням. Тому предметом дослідження є канали витоку інформації, що виникають у процесі функціонування інформаційно-комунікаційних систем і засобів обчислювальної техніки, зокрема комп'ютерних мереж, веббраузерів та мультимедійних файлів.

Аналіз останніх досліджень і публікацій. Актуальність нашого дослідження зумовлена тим, що в сучасному світі інформація посідає місце стратегічного ресурсу, який відіграє ключову роль у розвитку економіки, науки, техніки та суспільства загалом. Володіння необхідними відомостями у потрібний час і в потрібному місці стає запорукою успіху, а конфіденційні дані дедалі частіше прирівнюються до цінностей, від збереження яких залежить конкурентоспроможність та безпека підприємств, організацій і навіть держав.

Зростання масштабів інформатизації та широке використання автоматизованих систем призводять до накопичення значних обсягів даних, що циркулюють у комп'ютерних мережах, передаються каналами зв'язку та зберігаються на технічних носіях. Водночас ускладнення архітектури сучасних інформаційних систем, поява великої кількості користувачів, віддалений доступ і інтеграція різнорідних інформаційних масивів суттєво збільшують кількість потенційних загроз безпеці[1].

Будь-які порушення конфіденційності, цілісності чи доступності інформації можуть спричинити серйозні наслідки – від фінансових збитків і зниження ефективності діяльності підприємств до підриву репутації або навіть створення загроз національній безпеці. Саме тому питання класифікації інформаційних ресурсів, а також виявлення і аналізу можливих каналів витоку даних набувають особливої актуальності.

Забезпечити надійний захист інформації сьогодні можна лише на основі системного підходу, що передбачає поєднання організаційних, програмних і технічних заходів. Це потребує чіткого розуміння значущості різних інформаційних ресурсів,

визначення рівня їхньої критичності та прогнозування можливих каналів несанкціонованого доступу [2]. Таким чином, вивчення основ класифікації інформаційних ресурсів і проведення аналізу потенційних каналів витоку інформації є важливим завданням, яке дозволяє сформувати необхідні знання та практичні навички у сфері інформаційної безпеки.

Мета статті. Метою роботи є аналіз методів та механізмів реалізації каналів витоку інформації, зокрема мережевих протоколів (HTTP, DNS, TCP/UDP), автоматичну передачу даних браузерами (cookies, referer, user-agent, сесійні токени), електромагнітні та акустичні канали побічних випромінювань, а також стеганографічні способи прихованої передачі повідомлень у графічних файлах.

РЕЗУЛЬТАТ ДОСЛІДЖЕННЯ

Дослідження відкритих мережевих підключень. У межах цього дослідження було виконано команду netstat-anb у середовищі Windows (для Linux або macOS – ss -tulpen або netstat-tulpen) (Рис.1).

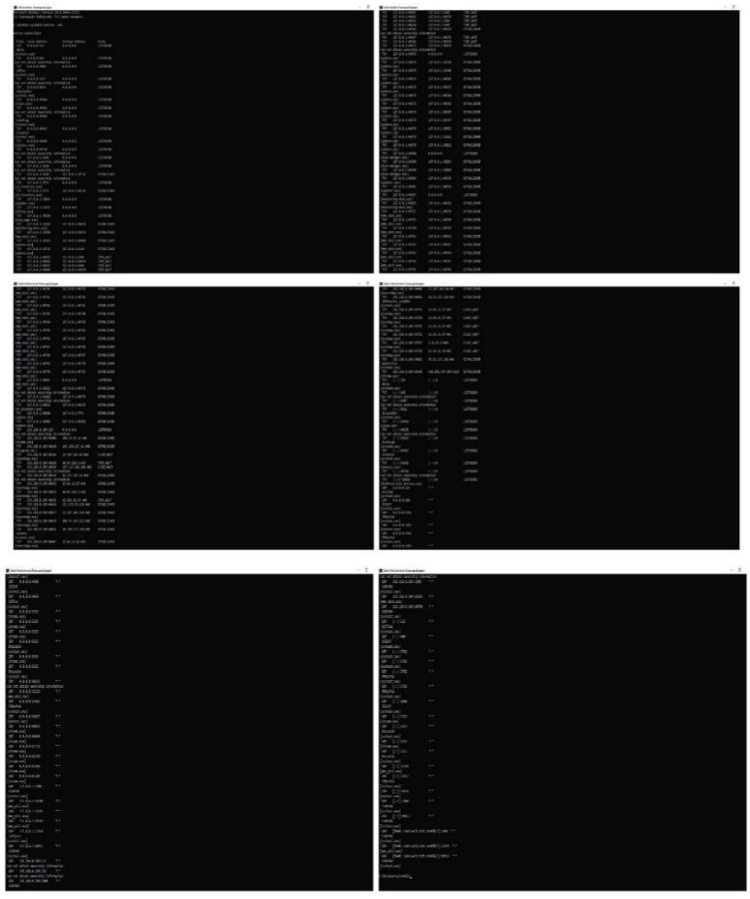

Рис. 1. Повний результат виводу команди netstat -anb у Windows

Під час аналізу наданих зображень, що містять результати роботи команди netstat -anb, виявлено низку процесів із відкритими портами та активними підключеннями. Значна частина з’єднань належить системним службам Windows. Окрім них, у виводі помітні кілька користувацьких програм і допоміжних процесів. Серед них – sh-inventory.exe, update.exe, SDTray.exe та bckp_amgr.exe, які встановлюють з’єднання з

адресою 127.0.0.1 у стані ESTABLISHED. Імовірно, це локальні утиліти для інвентаризації, оновлення чи резервного копіювання. Подібну картину демонструють і процеси task-manager.exe, monitoring-mini.exe та mms_mini.exe, що активно працюють через локальний інтерфейс та переважно перебувають у станах LISTENING або ESTABLISHED, що характерно для програм із внутрішньою архітектурою клієнт–сервер. Особливу увагу привертає процес caakoe.exe, який створює велику кількість підключень до адреси 127.0.0.1. Назва цього процесу не пов'язана з типовими службами Windows чи поширеними програмними застосунками, тому доцільно перевірити його походження та призначення.

Серед підключень до зовнішніх адрес зафіксовано активну роботу веббраузера chrome.exe, який підтримує декілька з'єднань через порт 443 до різних віддалених IP-адрес, що є типовим під час вебперегляду. Також активно працює месенджер Telegram.exe, який встановлює з'єднання з низкою зовнішніх серверів через порт 443, що відповідає стандартному механізму обміну даними цього застосунку. Декілька підключень належать процесу SearchApp.exe, який є складовою системного пошуку Windows та взаємодіє із серверами Microsoft. Окремо варто відзначити службу wildsvc, що функціонує через процес svchost.exe і має з'єднання з віддаленою адресою на порт 443; з огляду на її відносно рідкісне використання доцільно здійснити додаткову перевірку.

У підсумку більшість виявлених відкритих портів і підключень належать до штатних компонентів Windows або добре відомих користувацьких програм, таких як веббраузер і месенджер [3]. Водночас підозру викликають численні локальні з'єднання процесу caakoe.exe та окремі зовнішні підключення, пов'язані з wildsvc. Для підтвердження безпечності системи доцільно перевірити ці процеси за допомогою антивірусного програмного забезпечення та додатково простежити їхнє призначення.

Аналіз трафіку браузера. Для аналізу мережевого трафіку було відкрито сучасний веббраузер та інструменти розробника DevTools → Network із попереднім скиданням фільтрів (All) і відображенням колонок Time та Initiator (Рис.2).

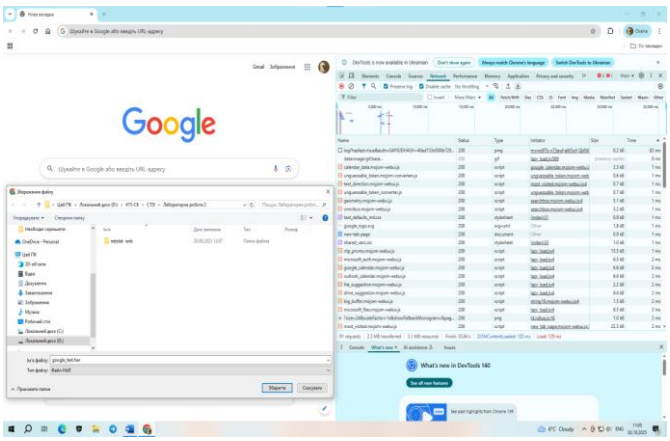

Рис. 2 Процес збору та експорту мережевого трафіку у форматі HAR за допомогою вкладки Network

Послідовно було відвідано кілька вебресурсів (поштовий сервіс, соціальну мережу та новинний ресурс) виконано типові дії та здійснено очікування завершення фонового завантаження ресурсів (Рис.3).

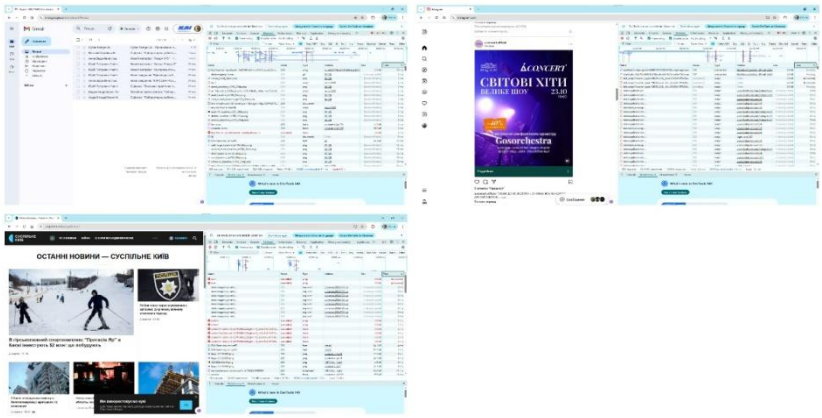

Рис. 3. Послідовний процес збору та експорту мережевого трафіку з кількох сайтів

Отримані записи було відсортовано за часом ініціації. Виділено запити, що виконуються без безпосередніх дій користувача (скрипти, web-push, фонова синхронізація), та зафіксовано для кожного з них метод (GET/POST), URL, розмір відповіді й час ініціації.

Таблиця 1

Мережеві запити сторінки пошти користувача з відповідними характеристиками

Метод	URL / Ресурс	Тип	Статус	Розмір відповіді	Час ініціалізації	Ініціатор
GET	log7?hasfst=true&hash...	png	200	0.2 kB	59 ms	fetch
GET	create_black_24dp.png	png	200	1.3 kB	52 ms	ServiceWorker
GET	chat_bubble_baseline...	png	200	2.6 kB	61 ms	ServiceWorker
GET	mail_baseline_nv700...	png	200	4.6 kB	60 ms	ServiceWorker
GET	archive_baseline_nv700...	png	200	2.4 kB	60 ms	ServiceWorker
GET	DM-Sans-regular.woff2	font	200	14.1 kB	75 ms	other
POST	log?format=json&hashfast=true...	fetch	200 (canceled)	52.8 kB	85 ms	fetch

У випадку використання поштового сервісу Gmail більшість мережевих запитів виконуються автоматично завдяки роботі ServiceWorker. Користувач безпосередньо не ініціює ці операції – вони здійснюються у фоновому режимі з метою забезпечення коректної роботи інтерфейсу та синхронізації даних.

Таблиця 2

Мережеві запити сторінки соцмережі користувача з відповідними характеристиками

Метод	URL / Ресурс	Тип	Статус	Розмір відповіді	Час ініціалізації	Ініціатор
GET	realtime/?hc...	websocket	101	0.0 kB	Pending	Instagram скрипт
GET	chat?sd=...	websocket	101	0.0 kB	Pending	Instagram скрипт
GET	init_script/Worker_type...	script	(unknown)	--	--	Instagram
GET	www.instagram.com/... (кілька рядків)	script	200	(memory cache)	0–7 ms	ServiceWorker
GET	cdninstagram.com/...	data/application	200	--	0–6 ms	ServiceWorker
GET	static.xx.fbcdn.net/...	script	200	--	0–6 ms	facebook.com/instagram

Під час завантаження сторінки Instagram встановлюються WebSocket-з'єднання необхідні для забезпечення роботи push-повідомлень, оновлення стрічки в реальному часі та функціонування чатів. Крім того, браузер виконує автоматичні запити до серверів Instagram і Facebook (зокрема cdninstagram.com, fbcdn.net) для завантаження мультимедійного контенту та скриптів. Частина ресурсів отримується з кешу, що сприяє підвищенню швидкодії сторінки. Усі зазначені процеси виконуються без участі користувача та забезпечують інтерактивність сервісу.

Таблиця 3

Мережеві запити новинної сторінки з відповідними характеристиками

Метод	URL / Ресурс	Тип	Статус	Розмір відповіді	Час ініціалізації	Ініціатор
GET	rum	ping	(canceled)	0.0 kB	(unknown)	--
GET	datamaps/svg-xml...	svg+xml	200	(memory cache)	0–5 ms	common.202e770.css
GET	collect?v=... (кілька рядків)	fetch	(canceled)	0.0 kB	2–6 ms	Google Analytics
GET	DM-Sans-regular.woff2	font	200	141.1 kB	3 ms	latest/
GET	logo-036685d.png	png	200	1.2 kB	8 ms	content-all.js
GET	34f9d6c98d65.png	png	200	12.8 kB	9 ms	content-all.js
GET	main-styles.css	stylesheet	200	329 kB	11 ms	latest/

На новинному порталі "Суспільне Київ" значна частина автоматичних запитів пов'язана з аналітикою та збором метрик відвідуваності. Зокрема, це запити rum та collect, які передають статистичні дані на сервери для оцінювання ефективності ресурсу. Окрім цього, браузер автоматично підвантажує шрифти, іконки та таблиці стилів, необхідні для коректної візуалізації контенту. Усі ці запити виконуються у фоновому режимі.

У процесі аналізу мережевих звернень вебдодатків Gmail, Instagram та сайту "Суспільне Київ" було ідентифіковано сторонні домени й трекери, які використовуються для завантаження додаткових ресурсів, реалізації аналітики та механізмів відстеження активності користувачів.

Для сервісу Gmail виявлено звернення до доменів fonts.gstatic.com і clients6.google.com, що використовуються для завантаження шрифтів, роботи допоміжних API сервісів Google, а також можуть виконувати функції телеметрії та збору статистичних даних.

У випадку Instagram зафіксовано використання сторонніх ресурсів, зокрема cdninstagram.com для доставки мультимедійного контенту, static.xx.fbcdn.net для підвантаження скриптів і стилів, а також можливі звернення до facebook.com/tr/, що свідчить про інтеграцію механізму Facebook Pixel для відстеження дій користувачів.

Для сайту "Суспільне Київ" виявлено запити до сервісу Google Analytics (www.google-analytics.com/collect), який здійснює збір статистики відвідуваності, а також до сервісу RUM (Real User Monitoring), що дозволяє оцінювати швидкодію сайту та взаємодію користувачів із ресурсом. Додатково фіксується використання домену fonts.gstatic.com для завантаження шрифтів із зовнішнього CDN.

Таблиця 4

Аналіз сторонніх сервісів та мережевих компонентів веб-сторінок

Сайт	Домен (FQDN)	IP / Інфо	Роль
Gmail	https://fonts.gstatic.com	(IP прихований у скріні)	CDN (шрифти)
	https://clients6.google.com	--	API / аналітика
Instagram	https://cdninstagram.com	--	CDN (зображення)
	https://static.xx.fbcdn.net	--	CDN (JS, CSS)
	https://facebook.com/tr/	--	Трекер (Facebook Pixel)
Suspilne	https://www.google-analytics.com/collect	--	Аналітика
	rum	--	Моніторинг
	https://fonts.gstatic.com	--	CDN (шрифти)

Під час детального аналізу вибраних мережевих запитів було переглянуто заголовки Request/Response, зафіксовано наявність cookies, полів Referer, Authorization, User-Agent та інших метаданих, а також перевірено URL-параметри на наявність чутливих даних.

Таблиця 5

Заголовки (Cookies, Referer, User-Agent, Authorization), зафіксовані під час аналізу трафіку

Сайт / Запит	Заголовок	Вміст (приклад)	Коментар
Gmail (mail.google.com)	Cookies	SID=...; HSID=...;SSID=...	Сесійні cookies, використовуються для автентифікації користувача.
	Referer	https://mail.google.com/mail/u/0/	Вказує на сторінку поштового сервісу, з якої здійснено перехід.
	User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64)...	Інформація про браузер, ОС та пристрій користувача.
	Authorization	(відсутній у більшості запитів)	Gmail використовує cookies і токени у фонових запитах.
Instagram (www.instagram.com)	Cookies	sessionid=...; csrftoken=...; ds_user_id=...	Використовуються для збереження сесії користувача та CSRF-захисту.
	Referer	https://www.instagram.com/	Вказує на головну сторінку Instagram.
	User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64)...	Дозволяє серверу визначати тип пристрою та браузера.
	Authorization	Іноді токен у фон. API-запитах	Використовується для підтвердження автентифікації користувача.
Новини (suspilne.media)	Cookies	user_consent=accepted; _ga=...; _gid=...	Використовуються для аналітики (Google Analytics) та згоди користувача.
	Referer	https://www.google.com/ або внутрішні сторінки	Дозволяє визначити, з якої сторінки користувач перейшов.
	User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64)...	Дозволяє сервісу адаптувати контент під пристрій.
	Authorization	Відсутній	Для публічних ресурсів авторизація не використовується.

На рисунках 4-6 наведено приклади HTTP-заголовків, отриманих під час аналізу мережевого трафіку (Рис.4-6).

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

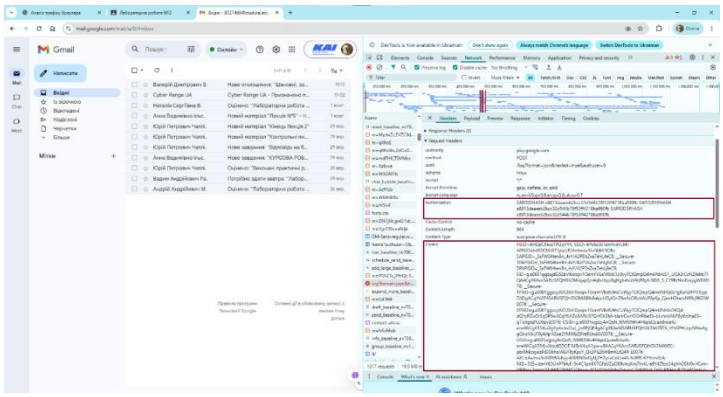

Рис. 4. Заголовки HTTP-запиту до сервісу Gmail (mail.google.com)

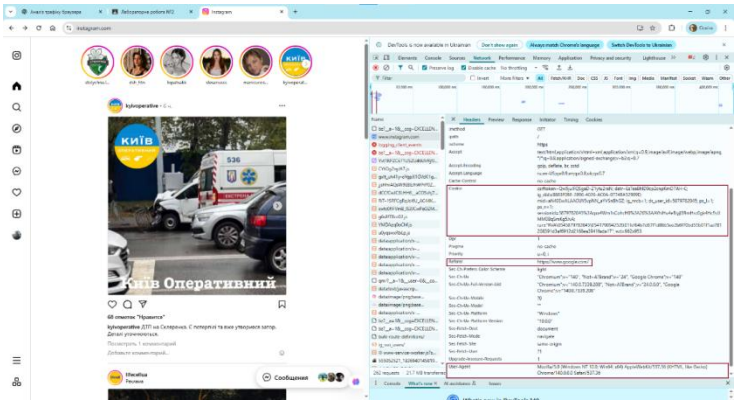

Рис.5. Заголовки HTTP-запиту до соціальної мережі Instagram

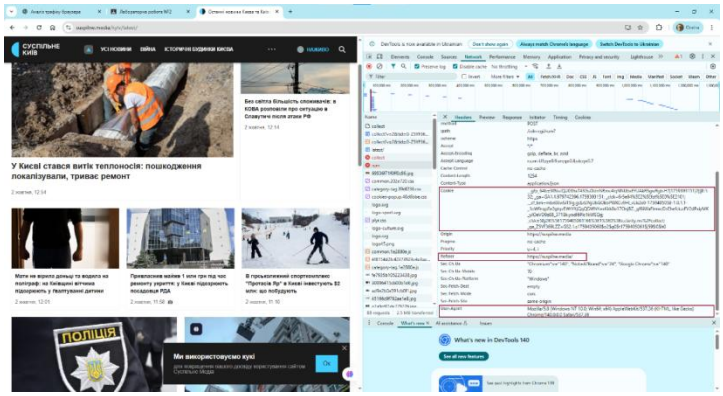

Рис. 6. Заголовки HTTP-запиту до новинного сайту Суспільне (suspilne.media)

У процесі роботи сучасних веббраузерів під час відвідування вебсайтів відбувається автоматична передача певних типів даних, які можуть розглядатися як потенційні джерела витоку інформації. До таких даних належать cookies, що містять унікальні ідентифікатори користувача, параметри сесій або токени авторизації. У разі їх неконтрольованої передачі стороннім сервісам існує ризик несанкціонованого доступу до облікових записів.

Поле Referer автоматично передає адресу сторінки, з якої було здійснено перехід, що може розкривати інформацію про історію відвідувань або внутрішню структуру сервісів. IP-адреса користувача, яка доступна серверу під час кожного запиту, дозволяє приблизно визначити геолокацію та становить додатковий ризик для конфіденційності. Також потенційну небезпеку несуть URL-параметри, які іноді передають логіни,

ідентифікатори або інші чутливі дані у відкритому вигляді. Окрему загрозу становлять токени сесій, перехоплення яких може призвести до компрометації облікових записів. Навіть поле User-Agent, попри його технічний характер, на практиці використовується для створення унікальних “відбитків браузера”.

Механізми витоку інформації є різноманітними. До них належать сторонні скрипти й віджети, що вбудовуються у вебсторінки з метою реклами, аналітики або інтеграції соціальних сервісів. Такі компоненти здатні збирати дані та передавати їх на зовнішні домени без прямої участі користувача. Іншим поширеним механізмом є HTTP-редиректи, які автоматично передають поле Referer і супровідні метадані. Окрему загрозу становлять WebSocket-з’єднання, що підтримують постійний обмін даними між клієнтом і сервером та можуть використовуватися для передачі чутливої інформації. Усі зазначені механізми впливають на рівень приватності користувача та можуть слугувати каналами витоку інформації [4].

Оцінюючи рівень ризику, можна зазначити, що використання cookies і сесійних токенів характеризується високим рівнем небезпеки, оскільки їх компрометація надає повний доступ до облікових записів. Передача чутливих параметрів у URL також має високий рівень ризику. Поля Referer і User-Agent становлять середній рівень ризику, оскільки сприяють профілюванню користувачів. Найнижчий, проте постійний ризик пов’язаний з IP-адресою, яка використовується переважно для геолокації та статистичних цілей. Для зниження рівня ризику доцільно застосовувати практичні заходи захисту. Використання блокувальників реклами й трекерів зменшує передачу даних стороннім сервісам. Регулярне очищення cookies і кешу знижує можливість ідентифікації користувача. Режим приватного перегляду обмежує збереження історії та тимчасових даних. Активація режиму HTTPS-only забезпечує шифрування трафіку й унеможливлює його просте перехоплення. Сукупне застосування цих заходів дозволяє істотно зменшити ризики витоку інформації та підвищити рівень захищеності користувача під час роботи в мережі Інтернет.

Перехоплення мережевих пакетів за допомогою Wireshark. Інсталюємо Wireshark і забезпечуємо права на захоплення пакетів: на Windows погоджуємо встановлення Npcap, на Linux додаємо свій обліковий запис у групу wireshark або запускаємо програму з правами адміністратора, на macOS надаємо дозволи для захоплення інтерфейсів. Запускаємо Wireshark і переглядаємо список доступних мережевих інтерфейсів, щоб визначити, через який інтерфейс виходимо в інтернет (Wi-Fi або Ethernet) (Рис.7).

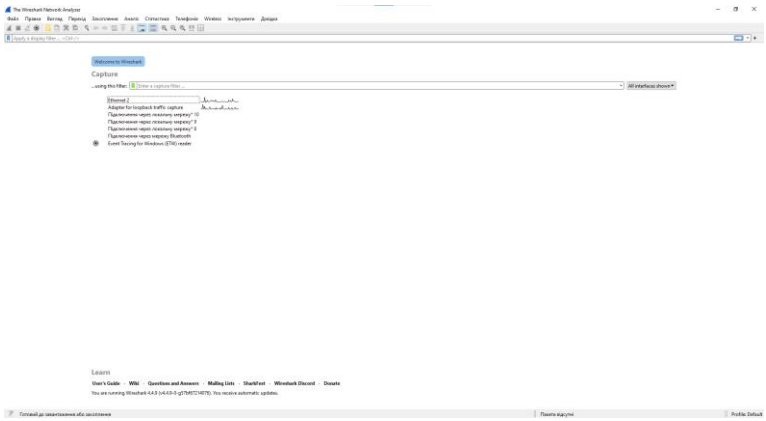

Рис. 7. Головне вікно Wireshark

Відкриваємо Capture Options для тонкого налаштування захоплення: вмикаємо Promiscuous mode за потреби і, за наявності апаратної підтримки та законних підстав, увімкнюємо monitor mode для 802.11 інтерфейсів. У полі Capture filter вводимо вираз udp port 53 or tcp port 80 для фокусування на DNS і незашифрованих HTTP-пакетах; якщо потрібно захоплювати весь трафік, залишаємо поле порожнім, розуміючи, що файл захоплення може значно збільшитися. Натискаємо Start і одразу переходимо у браузер для генерації трафіку. таким чином ловимо DNS-запити та незашифровані HTTP (порт 80) (Рис.8).

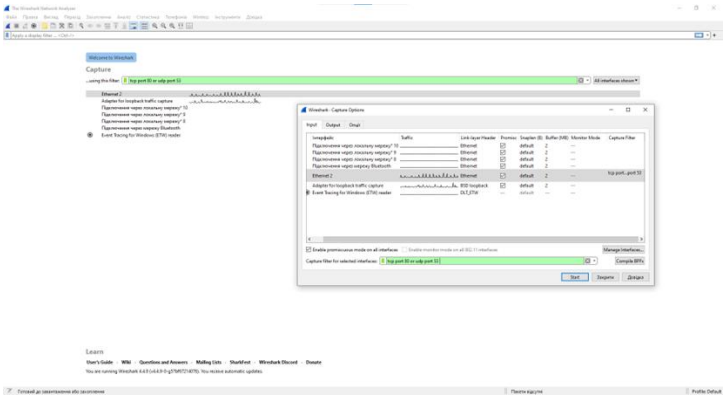

Рис. 8. Налаштування поля Capture filter для фокусування на DNS і незашифрованих HTTP-пакетах

Відвідуємо тестовий сайт: для гарантованого виявлення незашифрованих HTTP-запитів відкриваємо http://neverssl.com або локальний сервер http://localhost:8000 (наприклад, через команду python -m http.server 8000), для загального аналізу сучасних сайтів відкриваємо публічні сторінки без входу в акаунти, усвідомлюючи, що вміст передається через HTTPS і залишатиметься зашифрованим. Оновлюємо сторінки (F5), переходимо між розділами, натискаємо посилання, завантажуємо файли і, за потреби, відправляємо тестові форми з тестовими обліковими даними.

Спостерігаємо за вікном Wireshark і перевіряємо активність пакетів у середній панелі Packet List: переконуємося, що з’являються записи з часом, джерелом, призначенням, протоколом і коротким описом. Якщо пакетів не видно, зупиняємо захоплення, коригуємо Capture filter і повторно запускаємо збір (Рис.9).

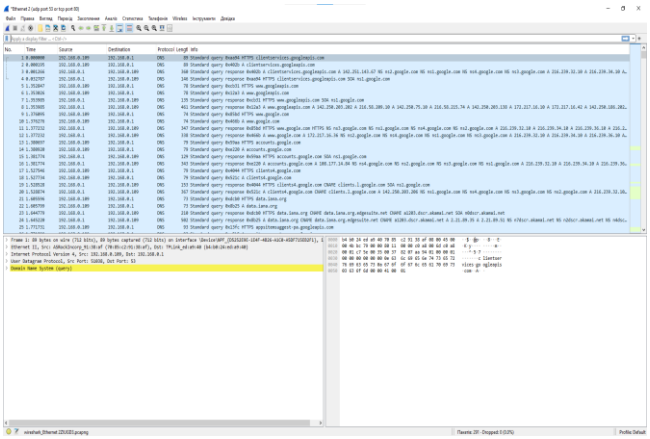

Рис. 9. Вікно Wireshark під час захоплення з активністю пакетів

ISSN 2663 – 4023

Зупиняємо захоплення кнопкою Stop і зберігаємо сесію через File → Save As під інформативною назвою, наприклад site_capture_YYYYMMDD_HHMM.pcapng (Рис.10).

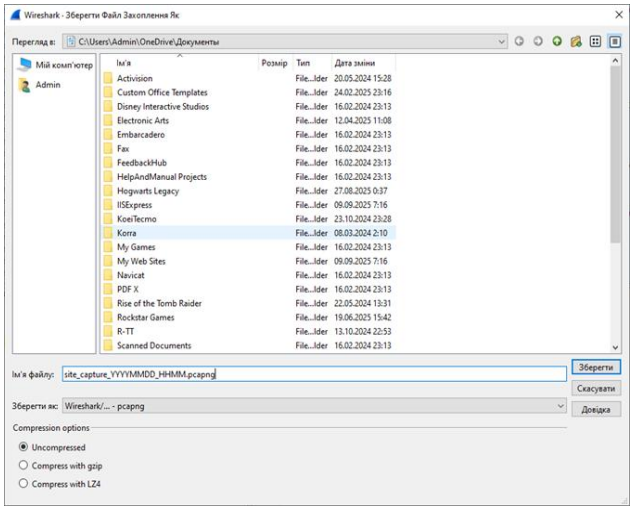

Рис. 10. Збереження виводу

Переходимо до аналізу: у верхньому полі Display filter вводимо потрібні вирази, натискаємо Enter і переглядаємо відфільтрований перелік пакетів. Для незашифрованих HTTP-запитів застосовуємо http.request або tcp.port == 80, для DNS – dns або udp.port == 53, для метаданих HTTPS – tls або tcp.port == 443 (Рис.11-13).

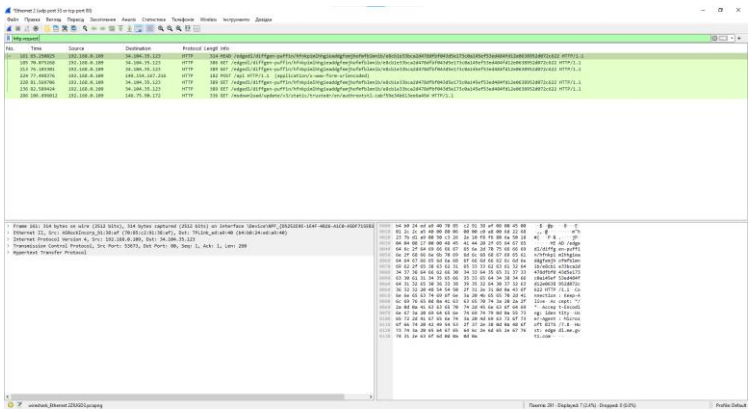

Рис. 11. Список пакетів з Display filter http.request (якщо є) або tcp.port == 80

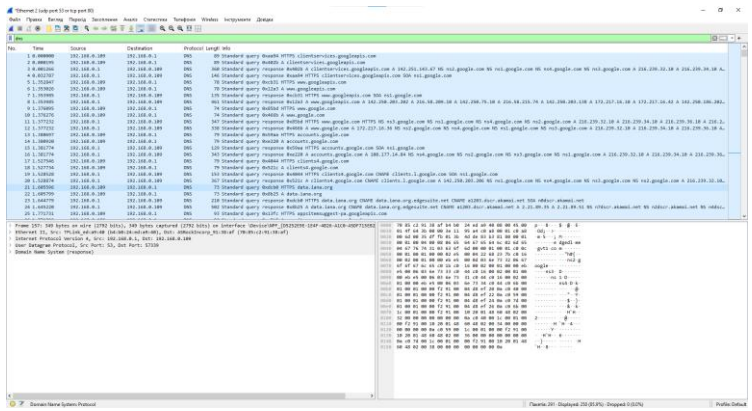

Рис. 12. Відфільтровані пакети за параметром "dns" або "udp.port == 53"

ISSN 2663 – 4023

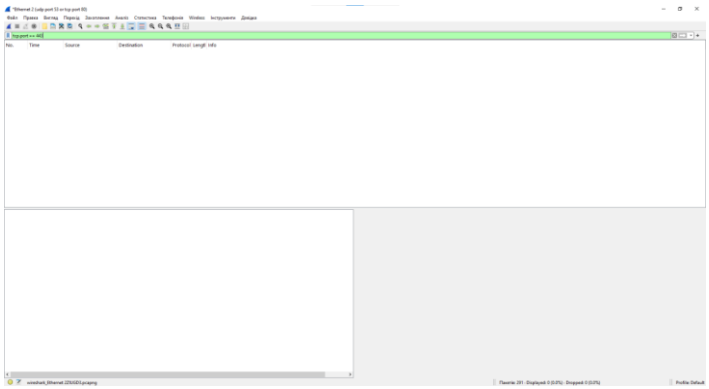

Рис. 13 Відфільтровані пакети за параметром "tls" або "tcp.port == 443"

Під час аналізу трафіку було використано сайт YouTube. У процесі тестування виконувалося відкриття головної сторінки, перегляд кількох відео, перехід до історії та запуск нових записів. Це дало змогу зафіксувати мережеву активність у Wireshark.

У результатах спостерігаються DNS-запити, які відповідають за розв'язання доменних імен у IP-адреси, а також HTTP-звернення до ресурсів. Водночас TLS-з'єднання у списках відсутні. Це пояснюється тим, що YouTube, окрім HTTPS, широко застосовує протокол QUIC, який працює поверх UDP та забезпечує шифрування даних без класичних TLS-пакетів у TCP. Також причиною може бути вибір певного фільтра чи інтерфейсу в Wireshark [5].

Акустичні та спектральні експерименти. Записавши короткий фрагмент мови тривалістю 20 секунд, завантажили отриманий аудіофайл у Audacity, перейдемо до перегляду спектрограми(Рис.14).

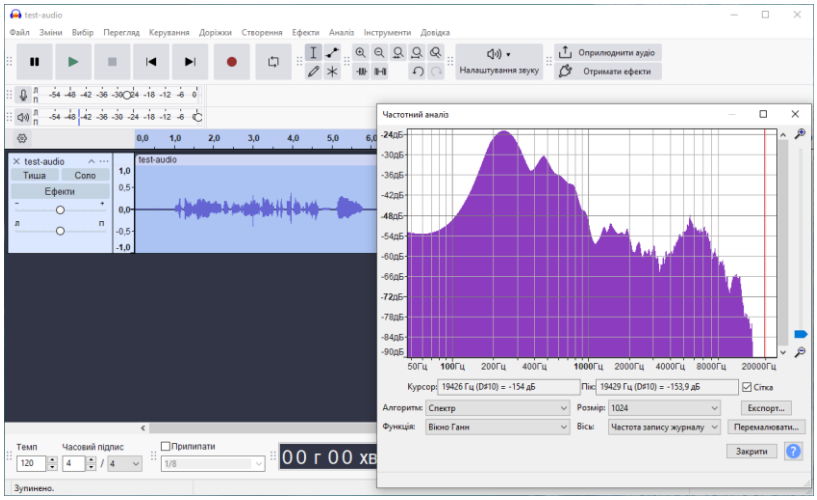

Рис. 14. Спектральний аналіз мовного сигналу у програмі Audacity

У результаті спектрального аналізу було виявлено, що сигнал містить основні енергетичні складові у діапазоні до 200-300 Гц, які відповідають фундаментальній частоті та першим гармонікам. Ці компоненти формують основу звучання голосу та забезпечують його насиченість і глибину.

Найбільш виражена активність спостерігається у межах 300-3400 Гц, які належать до мовного діапазону. У зоні приблизно 500-1200 Гц знаходяться перші форманти, що визначають забарвлення голосу, тоді як у діапазоні 1-3 кГц розташовані інформативні

гармоніки, які відіграють ключову роль у забезпеченні чіткості та розбірливості мовлення.

У високочастотній області, приблизно від 4 до 8 кГц, наявні додаткові гармоніки, які відповідають за формування тембру та передачу приголосних звуків, зокрема шиплячих та фрикативних. Саме вони надають голосу яскравості та природності. Після 8-10 кГц рівень сигналу поступово знижується, зберігаючи лише залишкові високочастотні складові.

Отже, проведений аналіз підтвердив, що досліджений сигнал містить як основні мовні частоти, так і додаткові гармоніки, які забезпечують природність, виразність і темброву різноманітність голосу.

Програмне моделювання ВЧ-нав'язування Було згенеровано високочастотну синусоїду (наприклад, 8 kHz) за допомогою онлайн-генератора тонів. Одночасно відтворено синусоїду та записану мовну доріжку, забезпечуючи їх накладання (Рис.15).

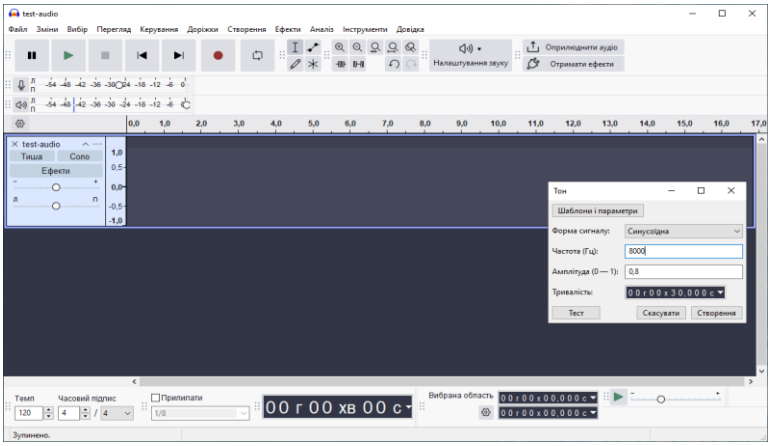

Рис. 15. Генерація високочастотної синусоїди за допомогою Audacity

Проведено спектральний аналіз запису, визначити наявність бічних смуг як ознаку амплітудної модуляції (Рис.16).

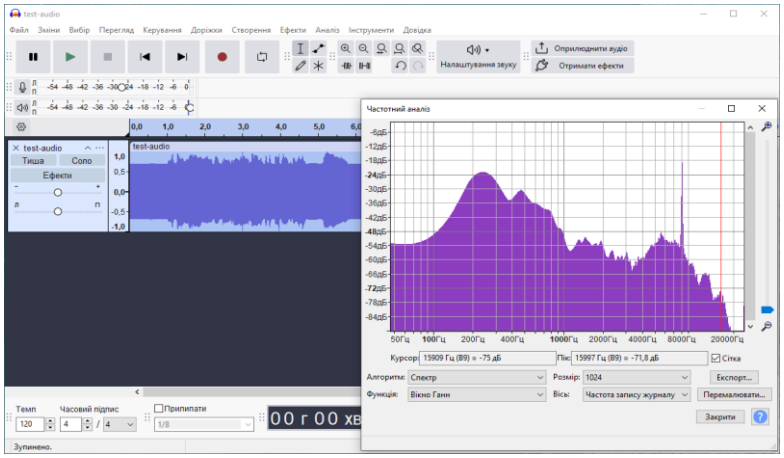

Рис. 16. Спектральний аналіз комбінованого сигналу у програмі Audacity

На спектрограмі, окрім несучої частоти (8 кГц), з'являються додаткові компоненти – бічні смуги. Вони виникають у результаті амплітудної модуляції:

верхня бічна смуга → частоти (8 кГц + частоти мовлення);

нижня бічна смуга → частоти (8 кГц – частоти мовлення).

Це підтверджує, що мовний сигнал модулює амплітуду синусоїди, створюючи спектрально рознесені смуги. У ході експерименту вдалося показати, що при додаванні мовного сигналу до синусоїди високої частоти (8 кГц) відбувається амплітудна модуляція. Це проявляється появою бічних смуг у спектрі запису, які є типовою ознакою АМ-сигналів.

Стеганографія та приховані канали. Вибрали невелике зображення у форматі BMP (конвертоване з JPG/PNG у Paint) для використання як контейнер. Це початковий файл, який зовні виглядає як звичайна картинка, але у подальшому в нього буде приховано секретне повідомлення (Рис.17).

Рис. 17. Початкове зображення-контейнер для стеганографії

За допомогою програми Xiao Steganography вбудували у файл контейнера текстове повідомлення “Тестова секретка”. Для цього обирається контейнер-зображення та текстовий файл із повідомленням (secret.txt), після чого утворюється новий стеганографічний файл. За потреби встановлюється пароль або обирається алгоритм шифрування (DES, Triple DES, RC4) (Рис.18).

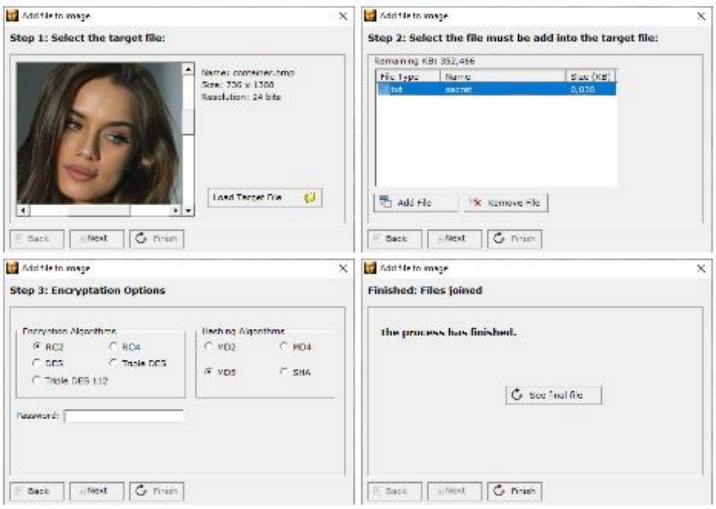

Рис. 18. Процес вбудовування текстового повідомлення у зображення в програмі Xiao

Під час вилучення повідомлення у Xiao Steganography обирається функція витягування даних, вказується пароль (якщо він був встановлений), і програма відновлює прихований текст. Це підтверджує працездатність методу стеганографії та наочно демонструє, що зовнішній вигляд зображення не змінюється (Рис.19).

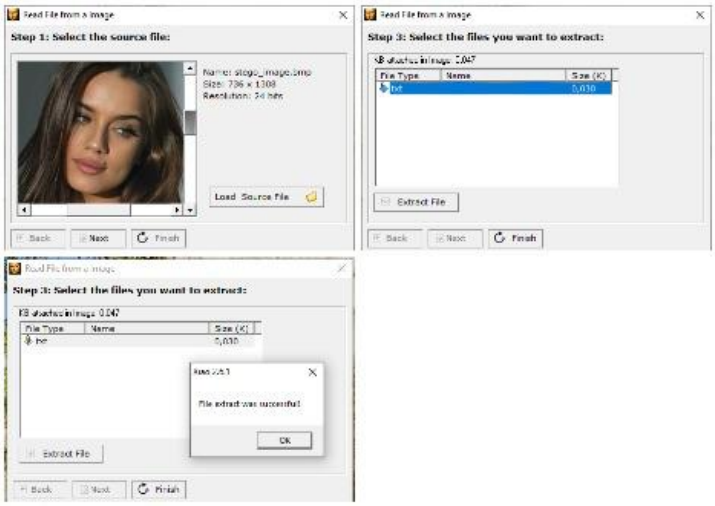

Рис. 19. Витягування прихованого повідомлення з зображення у програмі Xiao

Для виявлення підозрілих файлів, які можуть містити приховану інформацію, звертають увагу на кілька ознак. По-перше, розмір файлу може відрізнятися від очікуваного для зображення даного формату та розміру; порівняння з аналогічними файлами допомагає помітити аномалії. По-друге, перевірка метаданих (EXIF, інші поля) може виявити незвичайні або додаткові відомості, а також програми редагування, що вказують на можливу стеганографію. По-третє, статистичні аномалії у вигляді неприродних патернів пікселів або змін у гістограмах кольорів можуть свідчити про наявність прихованого тексту. Нарешті, звертають увагу на поведінку файлу: він може не відкриватися стандартними переглядачами або функціонувати нестандартно, а приховані дані можуть бути виявлені за допомогою спеціалізованих програм, таких як StegExpose або StegDetect.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті дослідження ми сформували важливі навички та уміння, методи й принципи практичної роботи з виявлення, аналізу та моделювання каналів витоку інформації. Дослідження надало можливість не лише ознайомитися з різними типами каналів витоку, але й на практиці оцінити потенційні ризики для інформаційної безпеки користувача та застосувати відповідні засоби захисту.

Під час роботи були досліджені відкриті мережеві підключення. Виконання команд Windows netstat -anb та Linux/macOS ss -tulpen дозволило зафіксувати активні з’єднання, визначити процеси з відкритими портами та виявити підозрілі або нетипові з’єднання. Цей канал витоку інформації може надавати відомості про активні сервіси та мережеву активність користувача, тому для його контролю рекомендовано використовувати брандмауери, засоби моніторингу відкритих портів та регулярний аудит системних процесів.

Аналіз трафіку браузера показав, що значна кількість даних може автоматично передаватися на сторонні домени та сервіси (CDN, трекери, аналітика). Використання DevTools дозволило зафіксувати HTTP-запити, визначити методи, URL, розмір відповіді та проаналізувати заголовки (Cookies, Referer, User-Agent, Authorization). Було виявлено, що частина даних користувача витікає без його активної участі. Для зменшення ризиків можна застосовувати розширення для блокування трекерів, налаштування конфіденційності у браузері та шифрування переданих даних через HTTPS.

Перехоплення мережевих пакетів за допомогою Wireshark дозволило детально дослідити незашифровані HTTP- та DNS-запити, зафіксувати URL, заголовки та вміст пакетів. Це підтвердило, що неконтрольований доступ до мережевого трафіку може бути джерелом витоку конфіденційної інформації. Як засоби захисту доцільно використовувати VPN, шифрування каналів передачі даних та контроль доступу до локальної мережі.

Акустичні та спектральні дослідження продемонстрували можливість витоку інформації через звукові сигнали. Запис мовного сигналу та моделювання високочастотного нав’язування дозволили виявити амплітудні модульовані сигнали, що можуть передавати дані непомітно для користувача. Для захисту від таких каналів слід контролювати та обмежувати доступ до аудіопристроїв, застосовувати спеціальні фільтри та системи виявлення аномалій у звукових потоках[6].

Дослідження стеганографії показало, що приховані канали можуть бути реалізовані через файли-зображення. Вбудування текстового повідомлення в BMP-контейнер за допомогою Xiao Steganography та подальше витягування даних продемонстрували, як інформація може передаватися непомітно. Для захисту від цього виду витоків ефективними заходами є аналіз метаданих файлів, контроль за розмірами та статистичними характеристиками файлів, використання антивірусного та спеціалізованого програмного забезпечення для виявлення стеганографії.

Таким чином, дослідження дозволило всебічно дослідити деякі канали витоку інформації, ознайомитися з методами їх виявлення та оцінити ризики для безпеки користувача.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Horlichenko, S. (2023). Features of formation of technical information leakage channels from modern information and communication systems. *Ukrainian Scientific Journal of Information Security*, *29*(2), 80–87. https://doi.org/10.18372/2225-5036.29.17872
2. Maltseva, I., Chernish, Y., & Shtonda, R. (2022). Analysis of some cyber threats under wartime conditions. *Cybersecurity: Education, Science, Technique*, *4*(16), 37–44. https://doi.org/10.28925/2663-4023.2022.16.3744
3. HostZealot. (n.d.). *How to check port availability.* https://www.hostzealot.com.ua/blog/how-to/yak-pereviryty-dostupnist-portiv/
4. Datami. (n.d.). *19 cases of large-scale data breaches.* https://datami.ee/ua/blog/19-sluchaev-masshtabnoj-utechki-dannyh/
5. Nym Technologies. (n.d.). *What is packet sniffing? Tcpdump, Wireshark, and how your neighbor spies on you.* https://nym.com/uk/blog/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%BF%D0%B5%D1%80%D0%B5%D1%85%D0%BE%D0%BF%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F-%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D1%96%D0%B2/
6. National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”. (n.d.). *Methods and means of technical information protection: Practical guide.* https://ela.kpi.ua/items/8a9dd076-19c8-450a-93e1-c5bf18ed7820

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Yuliya Chernish
Senior Research Fellow
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID: 0000-0002-6626-5656
yuliia.chernysch@viti.edu.ua

Tetiana Tereshchenko
Senior Research Fellow
Kruty Heroes Military Institute of Telecommunications and Information Technology, Kyiv, Ukraine
ORCID: 0000-0002-9659-7897
tetiana.tereshchenko@viti.edu.ua

Katerina Tereshchenko
Student
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0009-0008-8469-9854
katerina60411@gmail.com

INFORMATION OUTPUT CHANNELS – RESEARCH AND MODELING

Abstract: Automated systems accumulate huge amounts of data, including confidential data, which makes the issue of their security particularly relevant. Globalization has also led to the emergence of new challenges related to information protection. The characteristic features of the modern use of computer technology are the growth of the role of automated processes, increased responsibility for decisions made on their basis, the integration of information resources into large-scale databases, ensuring remote access for a large number of users, and the complication of the modes of operation of technical means. Identification, analysis, and modeling of information leakage channels, as well as the assessment of potential risks to users' information security are an important task. Therefore, the subject of research is information leakage channels that arise in the process of functioning of information and communication systems and computer equipment, in particular computer networks, web browsers, and multimedia files.

Any violation of confidentiality, integrity or availability of information can cause serious consequences - from financial losses and reduced efficiency of enterprises to undermining reputation or even creating threats to national security. That is why the issues of classification of information resources, as well as the identification and analysis of possible data leakage channels are becoming particularly relevant.

The purpose of the work is to analyze the methods and mechanisms of implementing information leakage channels, in particular network protocols (HTTP, DNS, TCP/UDP), automatic data transmission by browsers (cookies, referer, user-agent, session tokens), electromagnetic and acoustic channels of side radiation, as well as steganographic methods of covert transmission of messages in graphic files.

The study allowed us to comprehensively investigate some information leakage channels, familiarize ourselves with the methods of their detection and assess the risks to user security.

Keywords: information leakage channels, traffic analysis, network connections, packet interception

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Horlichenko, S. (2023). Features of formation of technical information leakage channels from modern information and communication systems. *Ukrainian Scientific Journal of Information Security*, *29*(2), 80–87. https://doi.org/10.18372/2225-5036.29.17872
2. Maltseva, I., Chernish, Y., & Shtonda, R. (2022). Analysis of some cyber threats under wartime conditions. *Cybersecurity: Education, Science, Technique*, *4*(16), 37–44. https://doi.org/10.28925/2663-4023.2022.16.3744

3. HostZealot. (n.d.). *How to check port availability*. https://www.hostzealot.com.ua/blog/how-to/yak-pereviryty-dostupnist-portiv/
4. Datami. (n.d.). *19 cases of large-scale data breaches.* https://datami.ee/ua/blog/19-sluchaev-masshtabnoj-utechki-dannyh/
5. Nym Technologies. (n.d.). *What is packet sniffing? Tcpdump, Wireshark, and how your neighbor spies on you.* https://nym.com/uk/blog/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%BF%D0%B5%D1%80%D0%B5%D1%85%D0%BE%D0%BF%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F-%D0%BF%D0%B0%D0%BA%D0%B5%D1%82%D1%96%D0%B2/
6. National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". (n.d.). *Methods and means of technical information protection: Practical guide.* https://ela.kpi.ua/items/8a9dd076-19c8-450a-93e1-c5bf18ed7820

Отримано редакцією журналу / Received: 17.01.26
Прорецензовано / Revised: 02.02.26
Схвалено до друку / Accepted: 26.03.26