



НАВЧАЛЬНИЙ ПОСІБНИК З ПИТАНЬ КІБЕРГІГІЄНИ

для закладів вищої освіти зі спеціальними
умовами навчання МВС України

Київ 2024



Організація з безпеки та
співробітництва в Європі



МІНІСТЕРСТВО
ВНУТРІШНІХ
СПРАВ
УКРАЇНИ

УДК 004.77.056(075.8)

M22

ISBN

Навчальний посібник з кібергігієни для закладів вищої освіти зі спеціальними умовами навчання МВС України. Київ, 2024. 230 с.

Колектив авторів:

Манжай Олександр Володимирович, завідувач кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, кандидат юридичних наук, професор, національний експерт з питань кібербезпеки Програми підтримки ОБСЄ для України – лекція «Понятійний апарат у сфері кібергігієни»; лекції та модулі: «Безпека мобільних пристроїв», «Безпечне користування мережею Інтернет», «Захист персональних даних», «Соціальна інженерія», «Убезпечення від неправдивих повідомлень»; частина III (у співавторстві з В.В. Носовим)

Носов Віталій Вікторович, професор кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ, кандидат технічних наук, доцент, національний експерт з питань кібербезпеки Програми підтримки ОБСЄ для України – лекції та модулі: «Безпечне користування електронною поштою», «Безпека користування соціальними мережами», «Реагування на інциденти безпеки інформації», «Фізична безпека», «Шкідливе програмне забезпечення»; частина III (у співавторстві з О.В. Манжаєм)

У посібнику розкриваються основні поняття та правила кібергігієни, досліджуються види персональних даних та відповідні заходи захисту, визначаються головні загрози та загальний алгоритм налаштування безпеки мобільних пристроїв. Надається класифікація видів шкідливого програмного забезпечення та наводяться популярні рішення для протидії цьому негативному явищу. Окрема увага приділяється інструментам та методам убезпечення від неправдивих повідомлень, та головним аспектам фізичної безпеки та правил безпечної поведінки в мережі Інтернет. Підручник розрахований на здобувачів вищої освіти і фахівців з безпеки. Він може бути корисним викладачам та аспірантам закладів вищої освіти, які займаються дослідженнями у сфері безпеки інформації.



Організація з безпеки та співробітництва в Європі

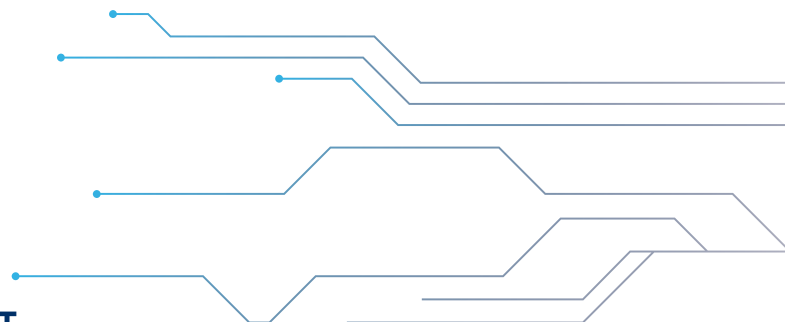


Опубліковано за сприяння Програми підтримки ОБСЄ для України в рамках проєкту «Посилення спроможностей національних партнерів для зміцнення кіберстійкості» за фінансової підтримки донорів – держав-учасниць ОБСЄ та партнерів.

Загальне керівництво проєктом: Тетяна Медун, національна менеджерка проєктів Програми підтримки ОБСЄ для України

Усі права захищені. Зміст цієї публікації може безкоштовно копіюватися та використовуватися для освітніх та інших некомерційних цілей за умови посилання на джерело інформації.

У цій публікації висловлено виключно погляди авторів. Вони не обов'язково збігаються з офіційною позицією ОБСЄ.



ЗМІСТ

ЧАСТИНА I. ТЕОРЕТИЧНІ ВІДОМОСТІ

6

Тема 1. Загальні правила безпечної роботи з пристроями та програмами	6
Понятійний апарат у сфері кібергігієни.....	6
Захист персональних даних.....	18
Безпека мобільних пристроїв.....	31
Шкідливе програмне забезпечення.....	47
Фізична безпека.....	62
Убезпечення від неправдивих повідомлень.....	70
Тема 2. Базові правила убезпечення роботи в комп'ютерній мережі	90
Соціальна інженерія.....	90
Безпечне користування мережею Інтернет.....	104
Безпечне користування електронною поштою.....	114
Безпека користування соціальними мережами.....	126
Реагування на інциденти безпеки інформації.....	133

ЧАСТИНА II. ПРАКТИКУМ

146

<i>Модуль: Захист персональних даних</i>	147
Практична вправа «Перевірка факту компрометації персональних даних».....	147
Альтернативна практична вправа «Розв'язання задач».....	148
<i>Модуль: Безпека мобільних пристроїв</i>	149
Практична вправа «Налаштування захисних механізмів у мобільному пристрої».....	156
<i>Модуль: Шкідливе програмне забезпечення</i>	156
Практична вправа «Вбудована в ОС Windows 10 система захисту від вірусів і загроз».....	156
Альтернативна практична вправа «Антивірусні програми «Zillya!» та «ZoneAlarm».....	160
<i>Модуль: Фізична безпека</i>	163
Практична вправа «Створення захищеного флеш-накопичувача».....	163
Альтернативна практична вправа «Блокування доступу до операційної системи за відсутності активності».....	169
<i>Модуль: Убезпечення від неправдивих повідомлень</i>	172
Практична вправа «Інструменти виявлення неправдивих повідомлень».....	172

Альтернативна практична вправа «Агрегація каналів новин та аналіз відомостей з окремих каналів системи Telegram».....	175
<i>Модуль: Соціальна інженерія</i>	178
Практична вправа «Аналіз поштового повідомлення».....	178
Альтернативна практична вправа «Захист від фішингових атак».....	183
<i>Модуль: Безпечне користування мережею Інтернет</i>	185
Практична вправа «Безпечний перегляд веб-сторінок та способи організації безпечного з'єднання в мережі».....	185
Альтернативна практична вправа «Накладання електронного підпису».....	189
<i>Модуль: Безпечне користування електронною поштою</i>	191
Практична вправа «Двофакторна автентифікація поштового облікового запису. Менеджер паролів».....	191
Альтернативна практична вправа «Електронний підпис та шифрування повідомлень».....	200
<i>Модуль: Безпека користування соціальними мережами</i>	209
Практична вправа «Двофакторна автентифікація облікового запису Facebook. Метадані фотозображень».....	209
<i>Модуль: Реагування на інциденти безпеки інформації</i>	214
Практична вправа «Виявлення провісників та індикаторів інциденту інформаційної безпеки».....	214

ЧАСТИНА III. САМОСТІЙНА РОБОТА

222

Зміст веб-квесту.....	223
-----------------------	-----



ЧАСТИНА I

ТЕОРЕТИЧНІ ВІДОМОСТІ

ЧАСТИНА І. ТЕОРЕТИЧНІ ВІДОМОСТІ

Тема 1. Загальні правила безпечної роботи з пристроями та програмами

Понятійний апарат у сфері кібергігієни

План лекції

Вступ

1. Що таке кібергігієна?
2. Що таке кібербезпека?
3. Що таке інформаційна безпека?

Висновки

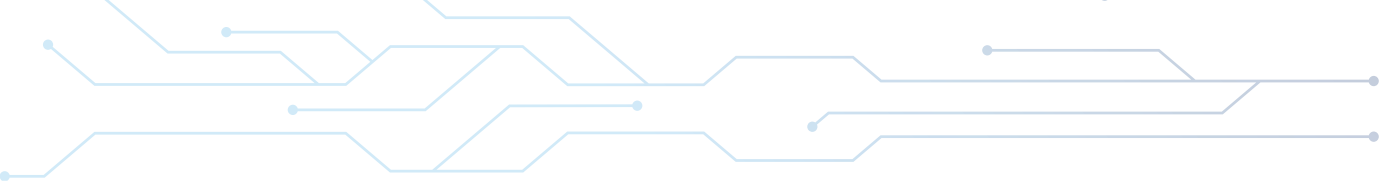
Рекомендована література

Основна

1. Даник Ю.Г., Гришук Р.В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 262 с.

Допоміжна

5. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 65–67.
6. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 72–73.
7. Про критичну інфраструктуру: Закон України від 16.11.2021. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
8. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
9. Простворення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11.03.2021, введено в дію Указом Президента України від 19.03.2021 № 106/2021. URL: <https://zakon.rada.gov.ua/laws/show/106/2021#Text>.

- 
10. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>.
 11. Стратегія кібербезпеки України, затверджена Указом Президента України від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>.
 12. Maennel K., Mäses S., Maennel O. Cyber Hygiene: The Big Picture. In: Gruschka N. (eds) Secure IT Systems. NordSec 2018. *Lecture Notes in Computer Science*. 2020. Vol. 11252. Springer, Cham. (DOI: 10.1007/978-3-030-03638-6_18).
 13. Pfleeger S. L., Sasse M. A., Furnham A. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*. 2014. Vol. 11. Iss. 4. pp. 489–510. (DOI: 10.1515/jhsem-2014-0035).
 14. Review of cyber hygiene practices (December 2016). European Union Agency For Network and Information Security (ENISA). https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport, p. 4.
 15. Vishwanath A., Neo L. S., Goh P., Lee S., Khader M., Ong G., Chin J. Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*. 2020. Vol. 128 (DOI: 10.1016/j.dss.2019.113160).

Інформаційні ресурси в Інтернеті

16. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

Текст лекції

Вступ

Сьогодні безпека роботи з інформацією є актуальною як ніколи. Зростаючі кібератаки на державні та приватні підприємства, установи й організації тільки посилюють цей тренд. Окрема категорія загроз стосується громадян, які все частіше стають об'єктом прискіпливої уваги правопорушників. Враховуючи це, поступово набуває поширення відносно нова концепція необхідності самостійного дотримання користувачами елементарних правил безпеки. Такий підхід дає змогу значно посилити систему колективної безпеки суспільства та держави в цілому. Агентство Європейського Союзу з мережевої та інформаційної безпеки (European Union Agency for Network and Information Security) відзначає, що кібергігієна повинна розглядатися так само, як і особиста гігієна, й після належної інтеграції в організацію стати простою повсякденною процедурою, яка забезпечить стан кіберздоров'я організації на оптимальному рівні.

Порушення правил кібергігієни може призвести для згубних наслідків не лише для окремої людини. Досить часто від дій зловмисників страждає і роботодавець жертви. Навіть великі держави можуть зазнати величезної шкоди від необачного ставлення до вимог безпеки однієї людини. Часто порушники використовують окрему особу як лаз для проникнення на об'єкти критичної інфраструктури, викрадення чутливих державних даних, створення умов для скоординованих повномасштабних атак.

Таким чином, недотримання вимог кібергігієни здатне нанести значну матеріальну та моральну шкоду. А, крім того, ще й істотно вплинути на вашу особисту репутацію!

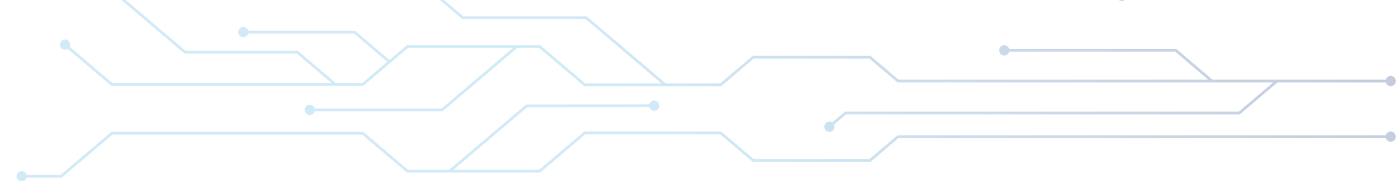
1. Що таке кібергігієна?

У світі існує достатньо велика кількість тлумачень слова «кібергігієна». Вони, як правило, відображають найбільш значущі аспекти цього терміна, важливі для конкретної галузі знань. Серед останніх оприлюднених визначень можна навести такі:

- ▶ правила кібербезпеки, яких мають дотримуватися онлайн-користувачі з метою забезпечення цілісності та убезпечення своїх персональних даних на мережевих пристроях від компрометації у випадку кібератаки;
- ▶ сукупність практик, спрямованих на захист від негативного впливу на певні об'єкти ризиків, пов'язаних з кібербезпекою;
- ▶ способи заохочення користувачів комп'ютерних технологій до безпечної поведінки в Інтернеті.

Більш спрощена інтерпретація цього терміна дозволяє представити кібергігієну як дотримання правил безпечної поведінки у кіберсфері.

Така поведінка обумовлена наявністю загроз, які виникають під час роботи користувачів з інформацією в електронному вигляді. Спроби реалізації загроз називаються атаками.



Як і на рибалці або полюванні, зловмисники можуть заздалегідь обирати цілі, які вважають цікавими для себе, а можуть навпаки – розставити пастки й чекати, доки жертва потрапить в одну з них. Те саме стосується ситуацій, коли порушники випадковим чином обирають жертву, стосовно якої намагаються реалізувати свої наміри.

Виділяють кілька типів *інформаційних атак*: соціальна інженерія, одержання віддаленого доступу за допомогою вірусів, вплив на інфраструктуру стільникового зв'язку, маніпуляція через ЗМІ, атаки відмови в обслуговуванні, атаки на енергетичні системи та комунікації, політичний спамінг, атаки на системи управління та провайдерів тощо.

Перед тим, як напасти, зловмисниками можуть здійснюватися підготовчі дії. Це дістає вияв у підшукуванні працездатних схем нападу, збиранні інформації про жертву різними способами, створенні умов для реалізації атаки.

Для того, щоб мінімізувати ризик успішної реалізації таких атак, саме і потрібна кібергігієна. По суті, це – рутинний процес. І з тим, щоб його полегшити, потрібно використовувати допоміжний інструментарій. Якщо у класичній гігієні такими інструментами є мило, шампунь, зубна щітка тощо, то для забезпечення її кібернетичного аналогу використовуються спеціальні програми: антивіруси, фаєрволи, захищені браузері та багато інших застосунків і сервісів.

Важливим моментом в роботі з інструментами кібергігієни є правильне їх застосування. Це приблизно те саме, що і правильне підрізання нігтів ножицями або зачісування волосся гребінцем. З одного боку, все просто, а з іншого – потрібно чітко визначити для себе елементарний порядок дій з певними програмами, щоб не вскочити у халепу. Просте озброєння купою застосунків для захисту інформації, як правило, не приносить користі. Без знання правил роботи з такими програмами вони стають просто набором коду, який навряд чи зможе вас захистити.

Так само потрібно мати на увазі, що чим меншою буде кількість інформації, яку ви хочете вберегти, тим менше вам потрібно буде вживати дій для її убезпечення. Тому під час продукування фотознімків, написання повідомлень у мережі, спілкування телефоном з незнайомими – та й навіть зі знайомими людьми подумайте, чи дійсно це є необхідним, і наскільки шкідливим може бути використання відповідної інформації проти вас.

Саме тому бажано користуватися перевагами Інтернету в частині забезпечення анонімності та використання вигаданих даних. Особливо це стосується мережевих ресурсів, у безпеці яких не можна бути впевненим. У випадку атаки на вас зловмисники зможуть отримати доступ лише до вигаданих даних. Це може стати ще одним додатковим ешелonom, що убезпечить вас від протиправних посягань.



Немаловажним принципом забезпечення кібергігієни є періодичне резервування даних. Можна використовувати мережеве резервування або дублювання даних на фізичних запам'ятовувальних пристроях. Усе залежить від чутливості даних, які потрібно зберегти, та відповідних знань предметного характеру. Так, наприклад, другорядні дані цілком можуть бути перенесені у хмару. Це дозволить зменшити кількість інформації, що потребує захисту на локальних пристроях, і, таким чином, тримати їх у чистоті.

Найкращий варіант – якщо ви зробите кібергігієну своєю повсякденною звичкою. При цьому вона не потребує суттєвих витрат коштів і часу. Згодом ви звикнете до виконання відповідних процедур і відчуєте їх корисність як в особистих, так і в службових справах.

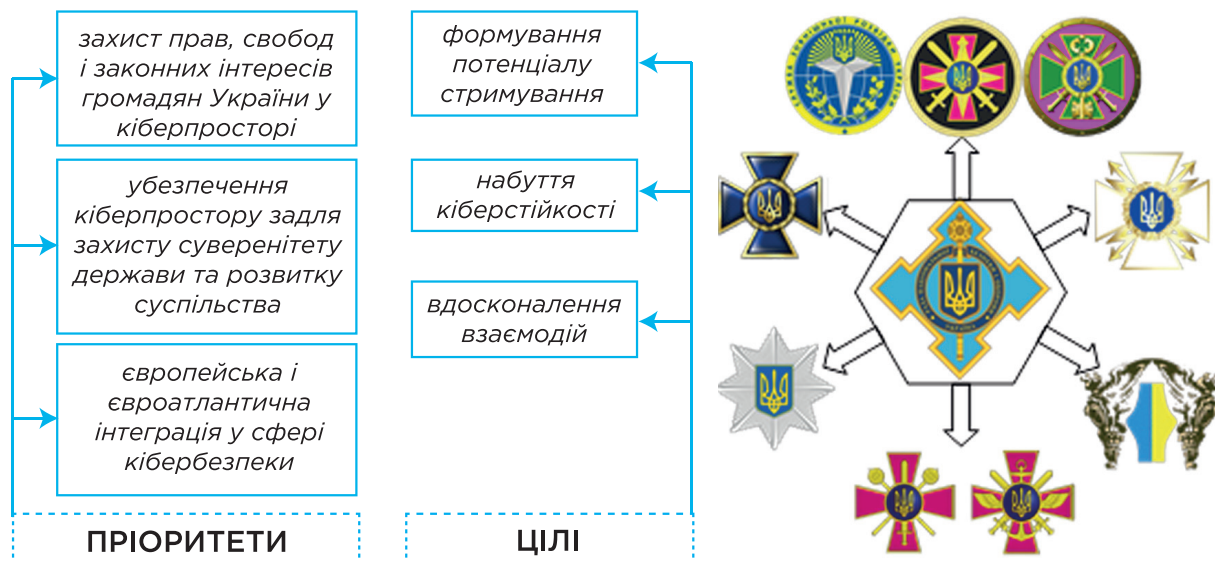
Тісно пов'язаними з кібергігієною є поняття «кібербезпека» та «інформаційна безпека».

2. Що таке кібербезпека?

У Законі України від 05.10.2017 «Про основні засади забезпечення кібербезпеки України» **кібербезпека** визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Актуальні загрози кібербезпеці та шляхи їх блокування викладено у підзаконних актах. Наприклад, **Стратегія кібербезпеки України** – це документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Докладніше структуру вказаного документа зображено на рис. 1.

МЕТА - створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави



ЗАГРОЗИ КІБЕРБЕЗПЕЦІ

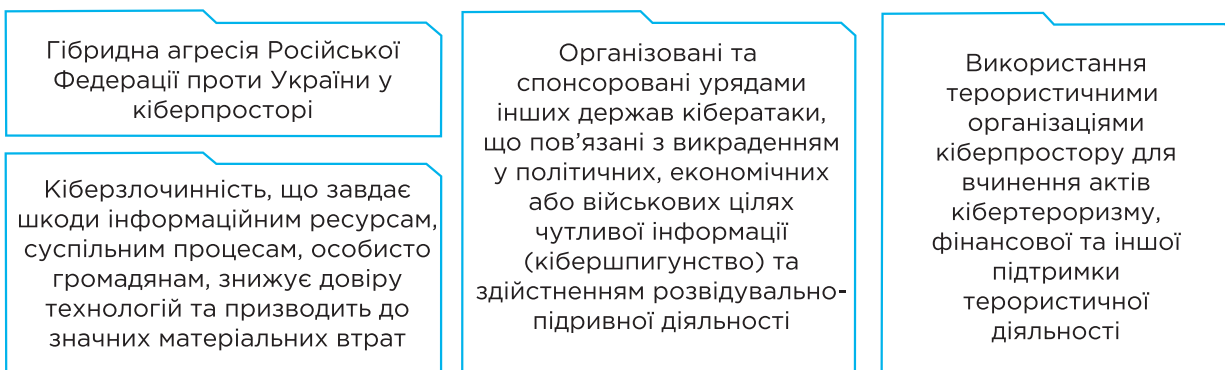


Рис. 1. Основні елементи стратегії кібербезпеки України

Об'єктами кібербезпеки є:

- 1) конституційні права і свободи людини і громадянина;
- 2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
- 3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
- 4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
- 5) об'єкти критичної інфраструктури.

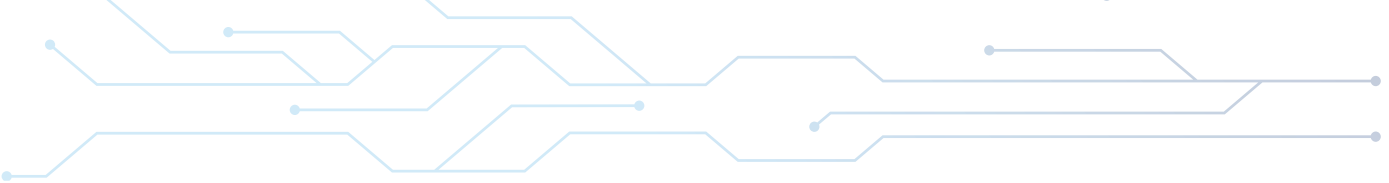
Цікавим нововведенням Стратегії кібербезпеки стало запровадження відповідних маркованих літерно-числовими ідентифікаторами стратегічних цілей (табл. 1).

Таблиця 1. Потенціал та стратегічні цілі кібербезпеки

ПОТЕНЦІАЛ ЦІЛІ	СТРИМУВАННЯ (С)	КІБЕРСТІЙКІСТЬ (К)	УДОСКОНАЛЕННЯ ВЗАЄМОДІЇ (В)
1	Дієва кібероборона	Національна кіберготовність та надійний кіберзахист	Зміцнення системи координації
2	Ефективна протидія розвідувально-підбивній діяльності у кіберпросторі та кібертероризму	Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки	Формування нової моделі відносин у сфері кібербезпеки
3	Ефективна протидія кіберзлочинності	Безпечні цифрові послуги	Прагматичне міжнародне співробітництво
4	Розвиток асиметричних інструментів стримування		

Для досягнення виділених цілей передбачено виконання цілої низки завдань. Так, наприклад, для досягнення цілі К.1 Україна у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю забезпечить посилення національної кіберготовності та кіберзахисту шляхом:

- ▶ розроблення Національного плану реагування на надзвичайні (кризові) ситуації в кіберпросторі, який визначить механізми реагування на кібератаки загальнонаціонального масштабу щодо об'єктів критичної інформаційної інфраструктури та заходи з подальшого відновлення;
- ▶ створення національної системи управління інцидентами, розроблення та впровадження стандартних операційних процедур для реагування на різні види подій у кіберпросторі з визначенням критеріїв для оцінки критичності подій та пріоритетності реагування залежно від визначеного рівня критичності;
- ▶ забезпечення постійного моніторингу національних електронних комунікаційних мереж та інформаційних ресурсів, аналізу вторгнень щодо цих мереж і ресурсів, а також виявлення в режимі реального часу аномалій їх функціонування;
- ▶ запровадження планування видатків на кібербезпеку за окремими бюджетними програмами;

- 
- ▶ розроблення базових (визначатимуть мінімальний обов'язковий рівень) вимог та рекомендацій з питань забезпечення кібербезпеки для державного і приватного секторів з урахуванням кращих світових практик;
 - ▶ налагодження на основі взаємної довіри системного обміну інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз між усіма суб'єктами забезпечення кібербезпеки, насамперед на базі технологічної платформи Національного координаційного центру кібербезпеки, уніфікації форматів обміну інформацією;
 - ▶ впровадження ризик-орієнтованого підходу стосовно заходів забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів, зокрема, розроблення методики ідентифікації та оцінки кіберризиків на національному рівні та для секторів критичної інфраструктури держави, врегулювання на законодавчому рівні обов'язковості здійснення періодичного оцінювання ризиків на підставі розроблених методик;
 - ▶ впровадження системи сертифікації продукції, яка використовується для функціонування та кіберзахисту інформаційно-комунікаційних систем, насамперед об'єктів критичної інформаційної інфраструктури;
 - ▶ забезпечення розвитку організаційно-технічної моделі кіберзахисту;
 - ▶ завершення процесів визначення об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, створення і забезпечення функціонування державного реєстру об'єктів критичної інформаційної інфраструктури, постійного перегляду та оновлення вимог щодо їх кіберзахисту з урахуванням сучасних міжнародних стандартів з питань кібербезпеки;
 - ▶ запровадження на постійній основі оцінювання стану захищеності об'єктів критичної інформаційної інфраструктури та державних інформаційних ресурсів на вразливість, встановлення обов'язковості та періодичності проведення такого оцінювання з урахуванням категорій критичності об'єктів, стимулювання участі у цих заходах фахівців з кібербезпеки приватного сектору;
 - ▶ впровадження системи аудиту інформаційної безпеки, насамперед на об'єктах критичної інфраструктури, визначення механізмів та базових методик проведення аудитів, встановлення вимог до аудиторів інформаційної безпеки, їх сертифікації, атестації (переатестації), навчання та підвищення кваліфікації, а також щодо обов'язковості та періодичності проведення аудитів, надання узагальненої інформації про результати аудитів до Національного координаційного центру кібербезпеки;
 - ▶ забезпечення розвитку систем технічного і криптографічного захисту інформації, пріоритетності використання засобів технічного і криптографічного захисту інформації вітчизняного виробництва для кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;
 - ▶ впровадження вітчизняних рішень із захисту інформації;

- 
- ▶ проведення командно-штабних кібернавчань стратегічного рівня, а також тематичних кібернавчань та тренінгів за участю представників державного та приватного секторів;
 - ▶ забезпечення розвитку мережі центрів реагування на кібератаки та кіберінциденти;
 - ▶ завершення розгортання Національної телекомунікаційної мережі, збільшення її пропускної здатності, передбачення під час її функціонування використання винятково вітчизняних засобів криптографічного захисту інформації;
 - ▶ забезпечення функціонування та розвитку Національного центру резервування державних інформаційних ресурсів, проведення модернізації системи захищеного доступу державних органів до мережі Інтернет;
 - ▶ створення національного сервісу доменних імен (DNS).

Крім розглянутих документів, існує ціла низка відповідних методичних рекомендацій, які, хоч і не є обов'язковими до виконання, проте можуть бути використані під час побудови системи кіберзахисту. Так, Адміністрація Держспецзв'язку наказом від 06.10.2021 № 601 затвердила Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. Рекомендації розроблені з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity), виданої у 2014 році та оновленої у 2018 році Національним інститутом стандартів і технології Сполучених Штатів Америки (National Institute of Standards and Technology).

3. Що таке інформаційна безпека?

15 жовтня 2021 року Рада національної безпеки та оборони України розглянула та схвалила Стратегію інформаційної безпеки, проект якої був внесений Кабінетом Міністрів України.

Результатами реалізації Стратегії мають стати:

- ▶ захищений інформаційний простір;
- ▶ ефективне функціонування системи стратегічних комунікацій;
- ▶ ефективна протидія поширенню незаконного контенту;
- ▶ інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України;
- ▶ підвищення рівня медіакультури та медіаграмотності населення;
- ▶ забезпечення захисту прав журналістів;
- ▶ формування загальнонаціональної ідентичності.

Згідно з положеннями Стратегії інформаційної безпеки *інформаційна безпека України* – це складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності,

демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії завданню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом.

Серед іншого, в документі наводиться аналіз головних викликів та загроз (рис. 2).



Рис. 2. Загрози та виклики інформаційній безпеці

Основними напрямками забезпечення інформаційної безпеки України є стійкість та взаємодія, для досягнення яких необхідним є виконання семи стратегічних цілей (рис. 3) та низки завдань.

Так, наприклад, для досягнення цілі підвищення рівня медіакультури та медіаграмотності суспільства потрібно виконати такі завдання:

- ▶ підготовка та проведення просвітницької кампанії з медіаграмотності, що включатиме такі компоненти, як розвиток критичного мислення, навички перевірки фактів і визначення маніпуляційних технік, ознайомлення з найпоширенішими порушеннями прав людини із застосуванням інтернет-технологій тощо;
- ▶ створення сприятливих умов для здійснення діяльності засобів масової інформації;
- ▶ створення сприятливих умов для підвищення рівня професійної підготовки медіафахівців;
- ▶ удосконалення законодавства у сфері реклами, зокрема щодо лібералізації норм у цій сфері та посилення відповідальності за трансляцію прихованої реклами;
- ▶ стимулювання розвитку соціально відповідального бізнесу серед засобів масової інформації.



Рис. 3. Стратегічні цілі забезпечення інформаційної безпеки

Механізми реалізації окресленої мети та завдань визначаються через уповноваження відповідних суб'єктів (рис. 4) на здійснення заходів щодо забезпечення інформаційної безпеки.



Рис. 4. Суб'єкти забезпечення інформаційної безпеки

Виходячи з наведеного, нескладно побачити, що інформаційна безпека, на відміну від кібербезпеки, більшою мірою стосується убезпечення інформаційного простору від різних загроз, у тому числі під час здійснення інформаційної війни.

Висновки

Підсумовуючи, окреслимо деякі головні правила кібергігієни:

1. Завжди критично ставтеся до відомостей, одержаних з мережі Інтернет.
2. Регулярно здійснюйте резервування важливих даних, не зберігайте все в одному місці.
3. Намагайтеся користуватися останніми версіями програмного забезпечення та регулярно виконуйте оновлення.
4. Залишайте якомога менше персональних даних у мережі Інтернет.
5. Дотримуйтесь вимог парольного захисту та використовуйте за можливості багатофакторну автентифікацію.
6. Користуйтеся антивірусним програмним забезпеченням та іншими засобами убезпечення.
7. У випадку компрометації чутливих даних повідомте про це уповноважену особу та вживайте заходів убезпечення решти відомостей.
8. Максимально обмежте доступ сторонніх осіб до терміналів, за якими ви працюєте.
9. Використовуйте тільки перевірені носії інформації.
10. Регулярно оновлюйте знання у сфері кібергігієни.

Захист персональних даних

План лекції

Вступ

1. Зарубіжний досвід захисту персональних даних
2. Вимоги законодавства України щодо захисту персональних даних
3. Окремі аспекти роботи з персональними даними в МВС України та Національній поліції

Висновки

Рекомендована література

Основна

1. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти: наук.-практ. посіб. К. : К.І.С., 2021. 160 с. URL: <https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69>.
2. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 106 с.
3. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.
4. Щодо захисту персональних даних в умовах воєнного стану. URL: <https://ombudsman.gov.ua/storage/app/media/Воєнний%20стан/Захист%20персональних%20даних/Захист%20персональних%20даних%20в%20умовах%20воєнного%20стану.pdf>.

Допоміжна

5. Про захист персональних даних: Закон України від 01.06.2010. Офіційний вісник України. 2010. № 49 (09.07.2010). ст. 1604.
6. Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: постанов Кабінету Міністрів України від 29.03.06 № 373. Офіційний вісник України. 2006. № 13 (12.04.2006). ст. 878.
7. Про доступ до публічної інформації: Закон України від 13.01.2011. Офіційний вісник України. 2011. № 10 (18.02.2011). ст. 446.
8. Про затвердження документів у сфері захисту персональних даних: наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1/02-14. Баланс. 2014. № 19. С. 5. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n11.
9. Про інформацію: Закон України від 02.10.1992. Відомості Верховної Ради України. 1992. № 48 (01.12.1992). ст. 650.
10. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27.04.2016 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу. 04.05.2016. L 119. С. 1. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

Інформаційні ресурси в Інтернеті

11. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

Текст лекції

Вступ

Персональні дані є однією з ключових складових приватного життя людини. Відповідно до ст. 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення *конфіденційної інформації про особу* без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

1. Зарубіжний досвід захисту персональних даних

Захист персональних даних, які містять інформацію про особу, є одним із найважливіших аспектів побудови громадянського суспільства. Як і в Україні (2010 р.), спеціальні закони про захист персональної інформації були прийняті в більшості європейських країн: Австрії (1978 р.), ФРН (1977 р.), Великобританії (1984 р.), Франції (1987 р.), Норвегії (1988 р.), Португалії (1991 р.), Бельгії (1992 р.), Іспанії (1993 р.) та ін.

Радою Європи ухвалено Конвенцію про захист особи у зв'язку з автоматизованою обробкою персональних даних (1981 р.), 15 директив і рекомендацій у галузі захисту даних, у тому числі про захист: персональних даних у приватному (1973 р.) та державному (1974 р.) секторах; даних, що використовуються у медичних цілях (1981 р.), наукових дослідженнях та статистиці (1983 р.), прямому маркетингу (1985 р.), соціальному забезпеченні (1986 р.), правоохоронній сфері (1987 р.); даних у галузях зайнятості (1981 р.), платежів (1990 р.) тощо. Нормативні акти та рекомендації у вказаній сфері прийняті також Європейським Союзом (95/46/CE), Організацією економічного співробітництва та розвитку.

У 2016 році в Європейському Союзі було прийнято Загальний регламент про захист даних у ЄС (General Data Protection Regulation /GDPR/). У 2018 році цей регламент набув чинності. Як і в Конвенції про захист особи у зв'язку з автоматизованою обробкою персональних даних (ст. 2), згідно з п. 1 ст. 4 GDPR персональними даними визнається інформація про фізичну особу, яка ідентифікована або може бути ідентифікована. Фізичну особу можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами, як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор, або за одним чи кількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.



У п.30 GDPR наголошується, що фізичні особи можуть бути пов'язані з онлайн-ідентифікаторами за допомогою їхніх пристроїв, додатків, інструментів чи протоколів, зокрема IP-адрес, ідентифікаторів «cookie» (реп'яшків) або інших ідентифікаторів, таких як мітки радіочастотної ідентифікації. Це може залишити підказки, які, особливо в поєднанні з унікальними ідентифікаторами та іншою інформацією, отриманою з серверів, можна використати для створення профілів фізичних осіб та їхньої ідентифікації.

Одним з головних завдань, що його мало вирішити впровадження GDPR, було підвищення спроможності громадян контролювати опрацювання своїх персональних даних. Для того, щоб опрацювання було законним, персональні дані необхідно опрацьовувати на підставі згоди відповідного суб'єкта даних або на іншій законній підставі.

Суб'єкт даних повинен дати згоду на опрацювання своїх персональних даних, а також мати право доступу до персональних даних, які збирають щодо нього, і реалізовувати таке право вільно та через розумні проміжки часу для того, щоб бути обізнаним про законність опрацювання та перевірити її (п. 63 GDPR). Зважаючи на це великі компанії, які працюють з персональними даними в Інтернеті, мають форму зворотного зв'язку для запиту відповідних персональних даних:

- ▶ Google (<https://takeout.google.com>);
- ▶ Apple (<https://support.apple.com/en-us/HT208502>);
- ▶ Viber (<https://help.viber.com/hc/en-us/articles/9062953104029-Request-Review-and-Delete-Your-Data-on-Viber#request-your-data-file>);
- ▶ Facebook (<https://www.facebook.com/help/212802592074644>);
- ▶ Instagram (<https://help.instagram.com/181231772500920>);
- ▶ TikTok (<https://support.tiktok.com/en/account-and-privacy/personalized-ads-and-data/requesting-your-data>);
- ▶ Telegram (<https://t.me/EURegulation>);
- ▶ Microsoft (<https://support.microsoft.com/en-us/windows/accessing-your-data-17e3d0dc-1351-3b03-9127-cc126a4e9568>);
- ▶ WhatsApp (https://faq.whatsapp.com/526463418847093/?cms_platform=iphone);
- ▶ ClubHouse (<https://support.clubhouse.com/hc/en-us/articles/4407302577939-How-do-I-request-a-copy-of-my-personal-data->);
- ▶ Signal (<https://support.signal.org/hc/en-us/articles/360007059412-Signal-and-the-General-Data-Protection-Regulation-GDPR->).

Важливими нормами GDPR є встановлене право особи на виправлення (ст. 16) та стирання (ст. 17) своїх персональних даних. Інструменти для реалізації цих норм також передбачені у великих компаніях, які здійснюють свою діяльність у кіберсфері. Наприклад, Google реалізував та запропонував користувачам кілька способів та інструментів видалення даних (<https://blog.google/products/search/new-privacy-tools/>).

Принципами опрацювання персональних даних згідно зі ст. 5 GDPR є:

- ▶ законність, правомірність і прозорість;
- ▶ цільове обмеження;
- ▶ мінімізація даних;
- ▶ точність;
- ▶ обмеження зберігання;
- ▶ цілісність і конфіденційність;
- ▶ підзвітність.

2. Вимоги законодавства України щодо захисту персональних даних

Національне законодавство у сфері захисту персональних даних значною мірою наслідує європейську практику з цього питання. Наразі в Україні є чинним Закон України від 01.06.2010 «Про захист персональних даних». Відповідно до ч. 2 ст. 5 цього Закону **персональні дані** можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. При цьому персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ст. 11 Закону України від 02.10.1992 «Про інформацію»). Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження.

Первинними джерелами відомостей про фізичну особу є: *видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.* Інформацію про особу можна поділити на:

- ▶ **загальну**, яка є відкритою і може використовуватися іншими особами. Це, наприклад, ім'я фізичної особи, право на використання якого відповідно до ч. 3 ст. 296 Цивільного кодексу України допускається без її згоди, з метою висвітлення діяльності особи або діяльності організації, в якій вона працює чи навчається, що ґрунтується на відповідних документах (звітах, стенограмах, протоколах, аудіо-, відеозаписах, архівних матеріалах тощо).

Також згідно з ч. 2 ст. 5 Закону України «Про захист персональних даних» не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень. У даному випадку варто підкреслити, що саме інформація стосовно виконання посадовцем публічних обов'язків є відкритою. Це наприклад, можуть бути такі дані, як копії наказів про заохочення, надання відпустки, відомості про відповідні витрати бюджетних коштів тощо.



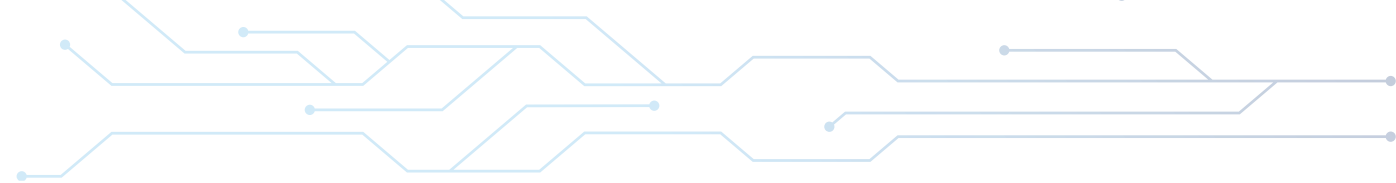
Публічною за законом є і інформація з декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування. Така інформація розміщується на сайті Національного агентства з питань запобігання корупції.

При цьому згідно з ч. 1 ст. 47 Закону України від 14.10.2014 «Про запобігання корупції» у відкритому доступі **не відображається** така інформація з декларації (має обмежений доступ):

- 1) відомості щодо реєстраційного номера облікової картки платника податків або серії та номера паспорта громадянина України;
- 2) унікальний номер запису в Єдиному державному демографічному реєстрі;
- 3) місця проживання, дати народження фізичних осіб, щодо яких зазначається інформація в декларації;
- 4) місцезнаходження об'єктів, які наводяться в декларації (крім області, району, населеного пункту, де знаходиться об'єкт);
- 5) номер рахунку в банківській чи іншій фінансовій установі.

➤ **вразливі персональні дані (конфіденційна інформація про особу)**, що є інформацією з обмеженим доступом. Саме про такі дані йдеться у ст. 32 Конституції України та у ст. 302 Цивільного кодексу України: «Збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». До таких даних належать, зокрема, персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, засудження до кримінального покарання. Також згідно з Рішенням Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г. Устименка) від 30.10.1997 до *конфіденційної інформації про особу*, зокрема, належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані).

У 2012 році Конституційний Суд України додатково розтлумачив, що інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка обіймає посаду, пов'язану зі здійсненням функцій держави або органів місцевого



самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини¹.

Відповідно до ч. 2 ст. 21 Закону України «Про інформацію» **конфіденційною** є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформація, визнана такою на підставі закону.

Оскільки персональні дані є інформацією, вимога щодо захисту якої встановлена Законом «Про захист персональних даних», відповідно до п. 4 Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373, вона підлягає захисту в системі.

Враховуючи викладене, відповідно до Закону України «Про захист персональних даних», Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та інших нормативних актів у сфері захисту інформації **загальна інформація про особу**, що зберігається в інформаційних системах держави, повинна бути захищена як відкрита інформація, а **вразливі персональні дані** – як службова інформація відповідно до вимог чинного законодавства у державних органах, або як окремий вид інформації – згідно з вимогами Закону України «Про захист персональних даних».

Дія цього Закону *поширюється* на діяльність з обробки персональних даних, яка здійснюється повністю або частково *із застосуванням автоматизованих засобів*, а також на обробку персональних даних, що містяться в *картотеці* (будь-які структуровані персональні дані, доступні за визначеними критеріями, незалежно від того, чи такі дані централізовані, децентралізовані або розділені за функціональними чи географічними принципами) чи призначені до внесення до картотеки, із застосуванням *неавтоматизованих засобів*.

Відповідно до ст. 2 Закону України «Про захист персональних даних» **база персональних даних** – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних.

Суб'єктами відносин, пов'язаних із персональними даними, є:

- ▶ суб'єкт персональних даних;
- ▶ володілець бази персональних даних;
- ▶ розпорядник бази персональних даних;
- ▶ третя особа;
- ▶ Уповноважений Верховної Ради України з прав людини.

¹ Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. Офіційний вісник України. 2012. № 9 (10.02.2012). ст. 332.

Володільцем чи розпорядником бази персональних даних можуть бути підприємства, установи й організації **всіх форм власності**, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, які обробляють персональні дані відповідно до законодавства.

Розпорядником бази персональних даних, володільцем якої є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності. Прикладами бази персональних даних можуть бути бази даних комп'ютерних соціальних мереж, реєстраційних даних інтернет-магазинів, медичні картки пацієнтів в реєстратурі закладу охорони здоров'я, шкільний журнал тощо.

Персональні дані, крім знеособлених персональних даних, за порядком доступу **є інформацією з обмеженим доступом** (рис. 1).



Рис. 1. Класифікація інформації за порядком доступу

Склад і зміст персональних даних мають бути **відповідними, адекватними та ненадмірними** стосовно визначеної мети їх обробки.

Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, **без її згоди**, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Для обробки персональних даних суб'єктом персональних даних має бути надана згода на обробку його даних. Згідно із законом така згода повинна бути задокументованою, зокрема у письмовій формі або в окремих випадках – в електронному вигляді. Згідно з нормами Цивільного та Сімейного кодексів України згоду на обробку персональних даних **дітей** дають **законні представники**.

Повну цивільну дієздатність має фізична особа, яка досягла вісімнадцяти років (повноліття) (ч. 1 ст. 34 ЦК). Фізична особа, яка не досягла чотирнадцяти років (малолітня особа), має часткову цивільну дієздатність і має право: 1) самостійно вчиняти дрібні побутові правочини; 2) здійснювати особисті немайнові права на результати інтелектуальної, творчої діяльності, що охороняються законом (ч. 1 ст. 31 ЦК). Частиною 1 ст. 242 ЦК визначено, що батьки (усиновлювачі) є законними представниками своїх малолітніх та неповнолітніх дітей.

Розголошення чи публікація будь-якої інформації про дитину, що може заподіяти їй шкоди, без згоди законного представника дитини забороняється (ст. 10 Закону України «Про охорону дитинства»).

У 2018 році в м. Одеса розглядалась справа, у якій мати оскаржила публікацію фотографій своєї маленької доньки. Вони були опубліковані у Facebook без згоди мами. Відповідачі, зі свого боку, вважали, що публікація даних на приватних сторінках соцмереж з обмеженим доступом «рідним та друзям» не є поширенням на широкий загал. До того ж, це було зроблено з відома та за згоди батька дитини, який має рівні права на її виховання. Проте суд став на бік матері, аргументуючи це тим, що розміщення та поширення зображення у соцмережах може бути здійснено за згодою обох батьків (<https://www.radiosvoboda.org/a/zahyst-personalnyh-danyh-dytyny/31603271.html>, <https://reyestr.court.gov.ua/Review/75031032>, <https://reyestr.court.gov.ua/Review/82910394>).



Забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях і професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних.

Суб'єкта персональних даних наділено низкою прав, зокрема на доступ до своїх персональних даних, що містяться у відповідній базі персональних даних. Причому відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості. Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб'єкта персональних даних, наданої володільцю бази персональних даних на обробку цих даних, або відповідно до вимог закону. Для отримання доступу складається запит.

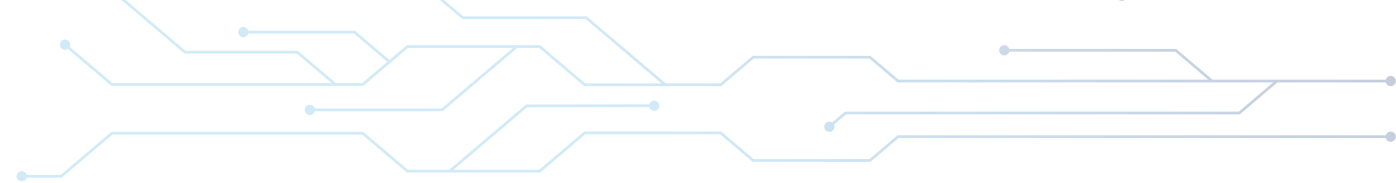
Суб'єкти відносин, пов'язаних із персональними даними, зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, в тому числі незаконного знищення чи доступу до персональних даних.

В органах державної влади та органах місцевого самоврядування, організаціях, установах і на підприємствах усіх форм власності створюється *структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних під час їх обробки відповідно до закону.*

Цей самий підрозділ нерідко відповідає за надання за запитами осіб публічної інформації, пов'язаної з персональними даними. Під час прийняття рішення про надання такої інформації керуються так званим «трискладовим тестом», суть якого полягає у визначенні можливості надання інформації шляхом відповіді на три ключових запитання (ч. 2 ст. 6 Закону України від 13.01.2011 «Про доступ до публічної інформації»):

1. Чи слугує засекречення цієї інформації інтересам:
 - ▶ національної безпеки;
 - ▶ територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням;
 - ▶ охорони здоров'я населення;
 - ▶ захисту репутації або прав інших людей;
 - ▶ запобігання розголошенню інформації, одержаної конфіденційно;
 - ▶ підтримання авторитету і неупередженості правосуддя?
2. Чи може завдавати розголошення цієї інформації істотної шкоди таким інтересам?
3. Чи шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні?

За порушення роботи з персональними даними передбачена дисциплінарна, цивільно-правова, адміністративна та кримінальна відповідальність. У випадку адміністративного правопорушення треба звертатися до Уповноваженого



Верховної Ради України з прав людини. Власне види правопорушень та відповідальність за їх учинення викладені у ст. 188-39 Кодексу України про адміністративні правопорушення. У відповідній статті виділено три основні види правопорушень:

1. неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи недостовірних відомостей;
2. невиконання законних вимог (приписів) Уповноваженого Верховної Ради України з прав людини або визначених ним посадових осіб секретаріату Уповноваженого Верховної Ради України з прав людини щодо запобігання або усунення порушень законодавства про захист персональних даних;
3. недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних.

Передбачена також більш сувора відповідальність за повторне вчинення таких правопорушень.

За незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації передбачено кримінальну відповідальність згідно зі ст. 182 Кримінального кодексу України.

3. Окремі аспекти роботи з персональними даними в МВС України та Національній поліції

У системі МВС України захист персональних даних урегульовано наказом МВС від 25.09.2020 № 685 «Про організацію роботи, пов'язаної із захистом персональних даних при їх обробці». Наказом передбачено організацію моніторингу та контроль за розглядом звернень з питань обробки та захисту персональних даних, що надходять до структурних підрозділів апарату МВС, територіальних органів надання сервісних послуг МВС, закладів, установ та підприємств, що належать до сфери управління МВС, Національної гвардії України, центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України. Відповідний моніторинг здійснюється за результатами звітування (2 рази на рік) окремими підрозділами перед МВС про стан розгляду звернень з питань обробки та захисту персональних даних. Крім того, Управління моніторингу дотримання прав людини МВС України також узагальнює стан організації щодо обробки та захисту персональних даних, для чого підрозділи МВС надсилають відповідні організаційно-розпорядчі документи.

Певні особливості щодо роботи з персональними даними існують і в Національній поліції. В цілому, вони є типовими для всієї правоохоронної системи. Так, наприклад, збирання інформації про осіб, доступної через відкриті джерела, може кваліфікуватися як посягання на недоторканність приватного життя. Зокрема, Європейський суд з прав людини своїм рішенням у справі «Швеція проти Сегерстед Віберг» кваліфікував дії правоохоронних органів зі збирання інформації, яка є відкрито доступною для користувачів мережі Інтернет, як порушення права на недоторканність приватного життя, гарантованого ст. 8 Конвенції Ради Європи про захист прав людини і основоположних свобод від 04.11.1950. Систематичне збирання інформації розцінюється як втручання у приватне життя у зв'язку з тим, що особа, яка розміщує інформацію, розраховує на зберігання відомостей та відсутність моніторингу за її профілем. Збирання відомостей є допустимим тільки відповідно до закону та в цілях боротьби зі злочинністю (ст. 8 (2) Конвенції).

У 2023 році за процесуального керівництва Тернопільської обласної прокуратури до суду направлено обвинувальний акт щодо працівника правоохоронного органу з Тернопільщини, який незаконно збирав персональні дані громадян. Встановлено, що фігурант систематизував та зберігав імена жителів Тернопільщини, дати їх народження, місця реєстрації та проживання, наявність у власності рухомого та нерухомого майна, вогнепальної зброї та спецзасобів. Ці дані він пересилав іншому працівнику правоохоронного органу незахищеними каналами зв'язку, під час чого могло статись несанкціоноване поширення цієї інформації.

Правоохоронця обвинувачують в незаконному збиранні, зберіганні, поширенні конфіденційної інформації (частини 1, 2 ст. 182 КК України). Досудове розслідування здійснювалось слідчими ТУ ДБР, розташованого у місті Львові. Санкція інкримінованої статті КК України передбачає покарання у вигляді позбавлення волі на строк до п'яти років (https://www.facebook.com/permalink.php?story_fbid=pfbid0FAso5vWz3P4tsYFXtcDk4u6n7XfbALWkYjmUaVRY9MspTeC3jf6WkkvQosMNyygSl&id=100064561967246).

Враховуючи викладене, правоохоронні органи мають право збирати будь-яку інформацію, якщо це передбачено законом, а також накопичувати безособову відкриту інформацію. Відомості щодо окремих осіб вони мають право збирати лише в межах визначених адміністративних процедур, у межах заведеної оперативно-розшукової справи або відкритого кримінального провадження. У ч. 2 ст. 264 Кримінального процесуального кодексу України наголошується, що здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або

утримувачем чи не пов'язаний з подоланням системи логічного захисту, не потребує дозволу слідчого судді.

Регуляторні процедури щодо персональних даних з кожним роком стають все жорсткішими, особливо в частині захисту конфіденційної інформації про особу. У багатьох країнах передбачена серйозна відповідальність для юридичних осіб за втрату персональних даних або порушення під час роботи з ними (<https://www.enforcementtracker.com>). Більш того, вже стає звичною практикою накладання великих штрафів регуляторами по всьому світу за незаконне збирання та використання інформації про осіб, навіть із відкритих джерел.

У травні 2023 року британський орган з нагляду за даними (Information Commissioner's Office) оштрафував компанію Clearview AI на £7,552,800 за використання зображень осіб з Об'єднаного Королівства без їх згоди. Регулятор також зобов'язав Clearview перестати надавати та використовувати дані підданих Об'єднаного Королівства, а також наказав видалити такі дані з бази даних компанії. (<https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/>). Власне база зображень збирається компанією з відкритих джерел, у тому числі з соціальних мереж, з метою надання послуг з розпізнавання облич. Компанія Clearview часто надає послуги з розпізнавання облич правоохоронним органам та спеціальним службам по всьому світу. Ця технологія є дуже корисною для вирішення завдань у сфері безпеки.

Враховуючи викладене, під час роботи з персональними даними слід не лише дуже уважно вивчати національне законодавство, а й досліджувати відповідну зарубіжну практику правозастосування, адже персональні дані часто поширюються в електронному вигляді, а відтак – можуть бути доступними і за кордоном.

Висновки

Для забезпечення безпеки персональних даних слід здійснити низку кроків організаційного та технічного характеру. Серед них можна виділити такі:

1. Неухильно дотримуватись вимог чинного законодавства в частині збирання, обробки, зберігання та захисту персональних даних.
2. Призначити відповідальну особу за організацію захисту персональних даних та затвердити внутрішні інструкції щодо захисту персональних даних.

- 
3. Постійно вивчати та застосовувати кращі вітчизняні та зарубіжні практики щодо захисту персональних даних.
 4. Мінімізувати кількість накопичених персональних даних та своєчасно видаляти вже непотрібні дані.
 5. Не зберігати всі персональні дані в одному місці. Найкраще розділити їх таким чином, щоб без наявності однієї з частин неможливо було ідентифікувати конкретну особу.
 6. Забезпечити заходи фізичного та технічного захисту місць і технічних засобів, які використовуються для збирання, обробки, збереження та забезпечення доступу до персональних даних.
 7. Заборонити доступ до баз персональних даних з неавторизованих пристроїв та локацій.
 8. Здійснювати регулярний контроль за станом збирання, обробки, зберігання та захисту персональних даних.
 9. Відбирати зобов'язання у відповідних осіб про нерозголошення персональних даних, які стали їм відомі під час виконання функціональних обов'язків.
 10. У випадку інцидентів безпеки, пов'язаних з персональними даними, своєчасно інформувати особу, відповідальну за безпеку в організації.
 11. Організувати регулярне підвищення кваліфікації персоналу в частині захисту персональних даних.

Безпека мобільних пристроїв

План лекції

Вступ

1. Блокування доступу до пристрою
2. Безпечна робота в мультимедійних засобах спілкування
3. Передавання вживаних мобільних пристроїв іншим особам
4. Передавання контактної інформації іншим особам
5. Захоплення номеру телефона
6. Шкідливе програмне забезпечення

Висновки

Рекомендована література

Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.

Допоміжна

5. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.
6. Про електронні комунікації: Закон України від 16.12.2020. *Офіційний вісник України*. 2021. № 6 (21.01.2021). ст. 306.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

Текст лекції

Вступ

Сучасний комунікатор має не тільки функціонал телефону!
У ньому органічно поєднуються можливості:

- ▶ комп'ютера;
- ▶ кредитної картки;
- ▶ пристрою управління;
- ▶ мультимедіа;
- ▶ засобу зв'язку.

Така універсальність, з одного боку, робить зручнішим виконання повсякденних завдань, а з іншого – створює загрозу одномоментної втрати великої кількості персональних даних. В окремих випадках така втрата може стати критичною.

Кілька років тому бізнесмен ледь не втратив мережевий бізнес, який розбудовував кілька років. Спочатку зломисники захопили управління його мобільним номером. У подальшому з використанням номеру телефону бізнесмена було одержано доступ до його електронної поштової скриньки, через яку було захоплено адміністративну панель домена, який було перереєстровано на інший обліковий запис. Для зміни паролю для доступу у даному випадку було встановлено двофакторну автентифікацію. А оскільки зломисники захопили номер телефону бізнесмена, то, відповідно, стало можливим управління доменом. У нашому випадку бізнесмен вчасно звернувся до поліції, відповідних провайдерів та реєстраторів, завдяки чому через деякий час йому повернули облікові записи. Але такий результат буває далеко не завжди.

Під час користування смартфоном ви повинні постійно враховувати загрози, які особливо часто реалізуються за недбалого ставлення до вимог безпеки. Наслідки реалізації таких загроз можуть не тільки вплинути на вашу персональну безпеку, а й скомпрометувати підрозділ, в якому ви працюєте, а інколи й державу в цілому.

Давайте розглянемо кілька типових ситуацій, які можуть призвести до небажаних наслідків.

1. Блокування доступу до пристрою

Якщо ви залишаєте телефон без особистого нагляду, не забудьте його заблокувати надійним паролем або біометричним замком. В останньому випадку йдеться про використання як засобу автентифікації відбитку пальця або обличчя. У разі недотримання цих простих вимог зловмисники можуть не тільки захопити управління вашим телефоном, а й швидко авторизуватися у месенджерах з вашими обліковими даними, поштових сервісах, системі онлайн-банкінгу тощо. В останньому випадку ви можете не тільки втратити персональні дані, а й постраждати фінансово.

В одній з областей України зловмисник заволодів телефоном працівниці державної установи. У подальшому за допомогою системи онлайн-банкінгу він привласнив з її банківського рахунку 40 тис. грн. Поліція встановила особу зловмисника, яким виявився неодноразово засуджений за майнові злочини молодик. Йому повідомили про підозру одразу за двома статтями Кримінального кодексу України: ч. 1 ст. 187 «Розбій» та ч. 2 ст. 185 «Крадіжка».

Може трапитися, що ви навіть не помітите, як стали жертвою зловмисника. А в цей час ваші облікові записи будуть успішно використовуватись з протиправною метою (рис. 1).

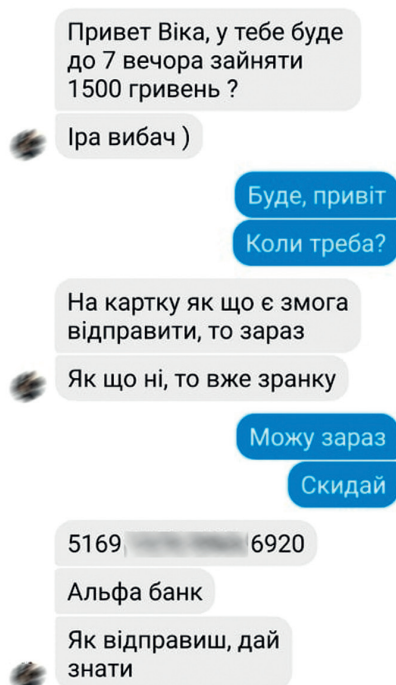


Рис. 1. Використання шахраями захоплених облікових записів

Здійснюючи атаку, шахраї можуть вивчати жертву для того, щоб бути більш переконливими. Найбільш простий приклад цього, коли зловмисник листується з потенційною жертвою тією самою мовою, якою жертва вела листування із захопленим обліковим записом (рис. 2).

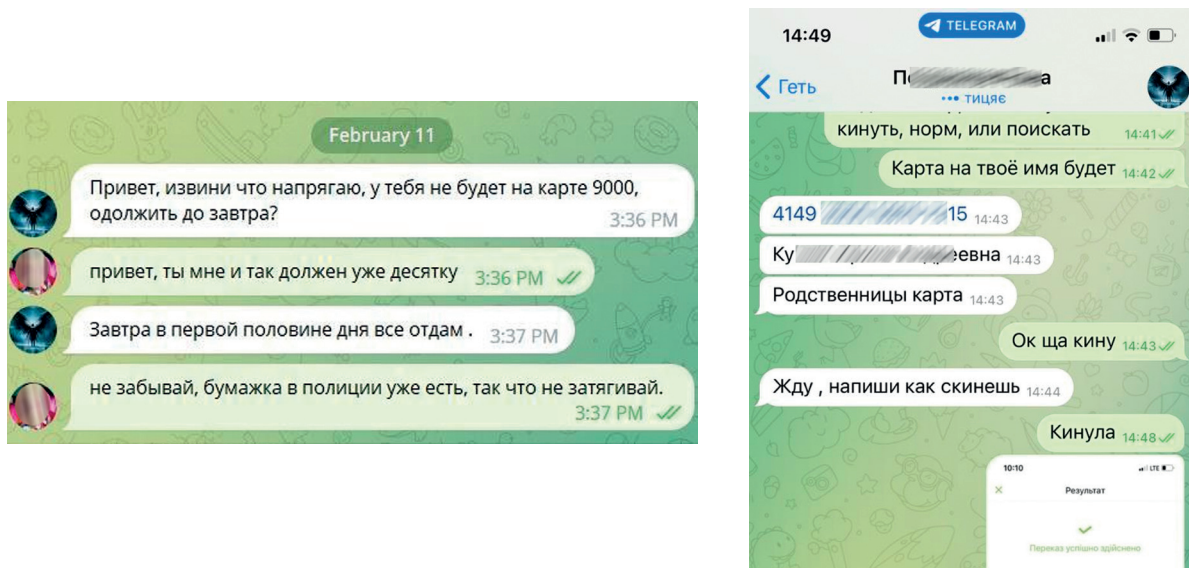


Рис. 2. Приклад спілкування зловмисника від імені захопленого облікового запису в Telegram

Для того, щоб частково зменшити ризики потрапляння в подібні ситуації, намагайтеся використовувати там, де це можливо, двофакторну автентифікацію, тобто коли для входу до якогось мережевого ресурсу потрібно ввести кілька паролів. Це може бути, наприклад, особистий пароль та додаткове підтвердження через СМС.

У будь-якому випадку, не ігноруйте повідомлення системи підтримки сервісів, у яких ви зареєстровані, оскільки в таких повідомленнях може міститися інформація про сторонній вхід до вашого облікового запису або про спроби такого входу.

Ранком на мобільний номер Сергія В. – одного з працівників обласної державної адміністрації – почали телефонувати його колеги і друзі та цікавитися, що у нього трапилося й для чого йому потрібні кошти. Не розуміючи, що відбувається, Сергій почав розпитувати колег про причину таких дивних дзвінків. Виявилося, що з його облікових записів у Skype, Viber та Telegram вночі почали надходити повідомлення про те, що йому терміново потрібні гроші, а також вказано номер банківської платіжної картки, куди слід їх переказати. Як потім виявилося, попереднього дня Сергій забув телефон на роботі, й хтось, скориставшись його незапароленим пристроєм, спробував вчинити неправомірні дії.

У випадку потрапляння у згадані ситуації терміново:

- ▶ заблокуйте найбільш чутливі облікові записи (банківські, службові електронні кабінети);
- ▶ зверніться до особи, яка відповідає за безпеку у вашій установі (підприємстві, організації), та повідомте її про компрометацію облікових записів;
- ▶ якщо дозволяють налаштування, завершіть усі активні сеанси у ваших облікових записах та змініть паролі.

Для того, щоб пересвідчитись, що ваші облікові дані не скомпрометовано, скористайтеся одним або кількома з наведених сервісів:

<https://breachalarm.com/>
<https://ghostproject.fr/>
<https://haveibeenpwned.com/>
<https://leakcheck.appspot.com/>
<https://monitor.firefox.com/>
<https://sitecheck.sucuri.net/>
<https://www.dehashed.com/>

Крім наведеного, зловмисники здатні, скориставшись вашим незаблокованим пристроєм, одержати доступ до його історії, а також до історії вже існуючих облікових записів. Це може дозволити порушникам встановити місця вашого частого перебування, ваші коло інтересів, фінансовий стан тощо.

Спробуйте скористатися ресурсом takeout.google.com, який призначений для завантаження історії облікового запису Google. Як запитуваний обліковий запис використайте активний запис для телефону під управлінням операційної системи Android.

2. Безпечна робота в мультимедійних засобах спілкування

Залишення незаблокованим телефонного пристрою не є єдиною загрозою. Сьогодні телефон часто використовується не тільки для класичного мобільного зв'язку, а й також як комп'ютер, на якому встановлено різні мультимедійні засоби спілкування. Найбільш поширеними месенджерами, як правило, є Telegram, Viber, WhatsApp.

Деякі з наведених засобів дозволяють паралельне підключення з кількох пристроїв: комп'ютера, телефона, планшета. З одного боку, це досить зручно для користувача, а з іншого – створює додаткові ризики з точки зору безпеки. Якщо, наприклад, ви авторизуєтесь зі стороннього пристрою у своєму

обліковому записі та випадково забудете вийти з нього при завершенні роботи, то існує ризик подальшого використання злоумисниками облікового запису з неправомірною метою.

Найбільш часто не виходять із своїх облікових записів вдома, на робочому місці, у місцях проведення інструктивних занять, у комп'ютерних класах навчальних закладів, у комп'ютерах колег або знайомих, які використовувалися з метою вирішення якихось короткострокових завдань. Ще однією, вельми поширеною помилкою є перехід за неперевіреними посиланнями, які вам надсилають у засобах спілкування. Крім вірусів, такі посилання можуть містити перехід на фішингові сервіси, призначені для введення в оману користувачів. На сьогодні існують дуже велика кількість подібних рішень не тільки для веб-сайтів, а й для заволодіння управлінням месенджером, що є вкрай небезпечним.

Наприклад, якщо у месенджері Telegram вам надійде повідомлення такого вигляду:

[https://drive.google.com@fdsgdxsfdgdgvcg.tw,](https://drive.google.com@fdsgdxsfdgdgvcg.tw)

то з першого погляду воно може здатися безпечним, адже є посилання на захищене з'єднання https зі справжнім сайтом Google. Однак, насправді, при натисканні на таке посилання у браузері відбудеться переадресація на сайт злоумисника fdsgdxsfdgdgvcg.tw.

Фішингове посилання може виглядати і не так незрозуміло, як уже наведене (рис. 3).

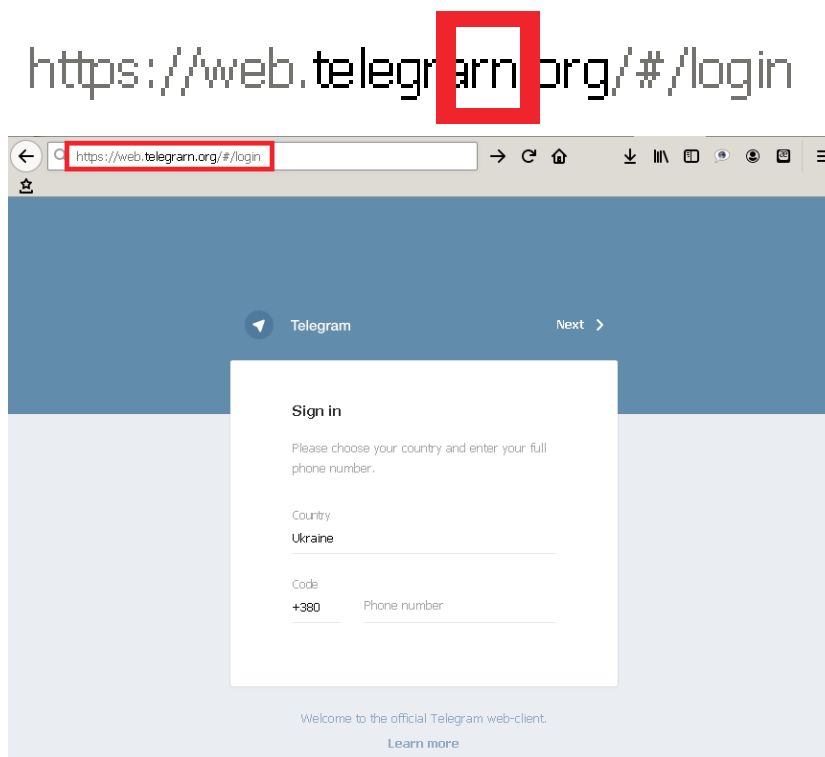


Рис. 3. Приклад фішингового сервісу Telegram

Враховуючи викладене, при переході за посиланнями, де вас просять ввести якісь дані, уважно передивіться текст посилання на предмет його справжності.

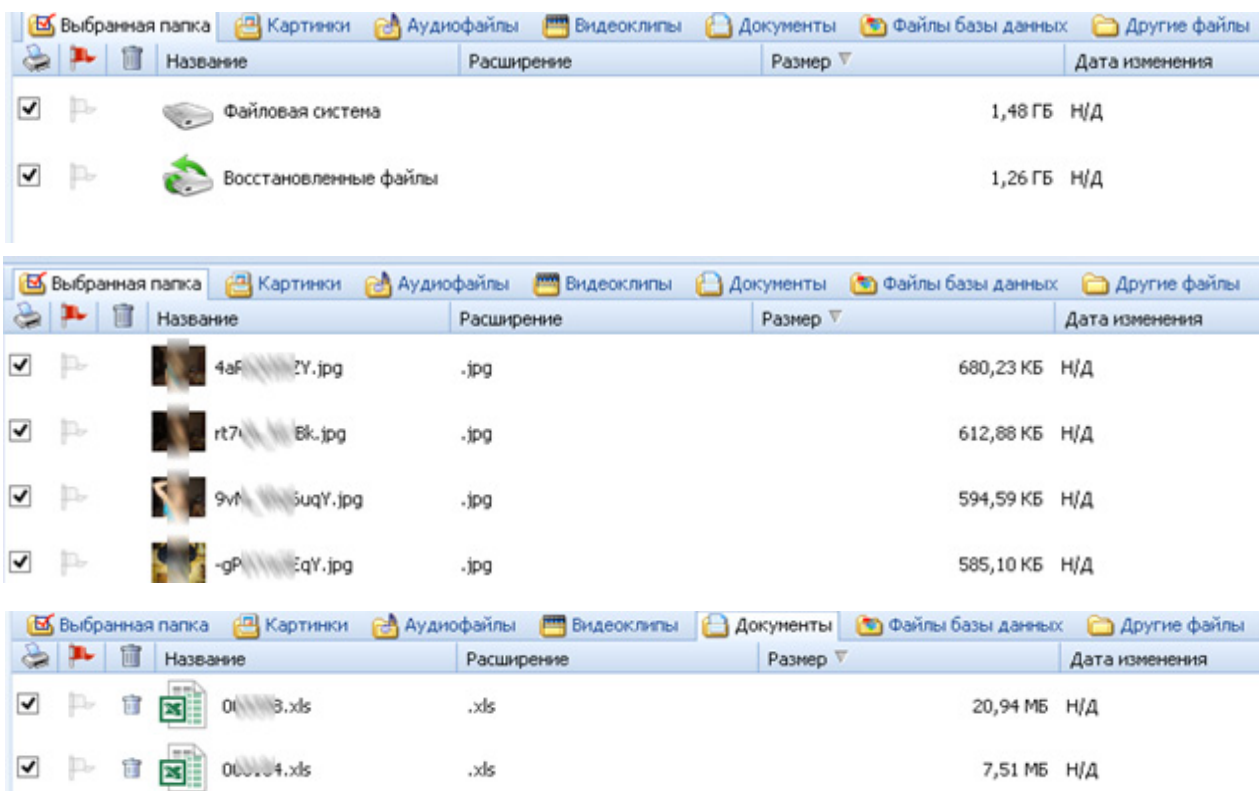
3. Передавання вживаних мобільних пристроїв іншим особам

Досить необачно вважати, що описані загрози є вичерпними. Уявіть ситуацію: ви хочете придбати новий телефон, при цьому вважаєте за доцільне одержати якісь кошти від продажу старого. Тому ви виставляєте його на продаж через систему OLX або просто продаєте на ринку.

Така ситуація трапляється досить часто, проте мало хто замислюється про те, що разом зі старим телефоном новий покупець може одержати доступ до ваших персональних даних.

Продемонструємо це на практиці.

Через систему OLX придбано вживаний смартфон марки LG, у якому попереднім власником було видалено усі персональні дані. За допомогою спеціалізованого програмного забезпечення для криміналістичного дослідження мобільних пристроїв було знято образ даних смартфона. За результатами пошуку інформації в образі вдалося виявити паролі доступу до точки доступу Wi-Fi та електронної пошти, частину листування в соціальних мережах, окремі фотографії, які зберігалися у смартфоні, повністю відновлено телефонну книгу до її видалення тощо (рис. 4).



Список	Дата	Контакт	GEO timeline
Тип	Время (Врем...	От	Кому
Сообщения ...	26.11.21	Ал	ин
Vkontakte m...	25.11.21	Ал	ин
Vkontakte m...	25.11.21	Вл	Ал
Vkontakte m...	25.11.21	Ал	ин
Vkontakte m...	25.11.21	Вл	Ал
Vkontakte m...	25.11.21	Вл	Ал
Vkontakte m...	25.11.21	Ал	ин
Vkontakte m...	23.11.21	Ал	Ал
Vkontakte m...	23.11.21	Ал	Ал
Vkontakte m...	22.11.21	Вл	Ал
Vkontakte m...	22.11.21	Ал	ин
Vkontakte m...	22.11.21	Ал	ин
Vkontakte m...	22.11.21	Вл	Ал
Vkontakte m...	22.11.21	Ал	ин
Vkontakte m...	22.11.21	Вл	Ал
Vkontakte m...	22.11.21	Ал	ин

Приложения (5)	Интернет (1)
Учетная запись	Пароль
с...	н...
sl...	н...
x...	н...
X...	н...
X...	н...
Сервис	Исходный файл
Web Browser (https://touch.mail.ru)	/data/data/com.android.browser/databases/webview.db
Web Browser (https://mail.ru)	/data/data/com.android.browser/databases/webview.db
Web Browser (https://touch.mail.ru)	/data/data/com.android.browser/databases/webview.db
Web Browser (http://mail.ru)	/data/data/com.android.browser/databases/webview.db
Web Browser (http://mail.ru)	/data/data/com.android.browser/databases/webview.db

Табличный вид	Перписка
Тип	От
Сообщ...	А
Сообщ...	800...
Сообщ...	+38...
Сообщ...	+38...
Сообщ...	3117...
Кому	Время (Время устройства)
А	02.09.20
А	01.09.20
А	01.09.20
А	01.09.20
А	01.09.20
Текст	О дт
Шт	0 дт
Я с	3 мн
Я :	.15
Я :	.15
Я :	днм

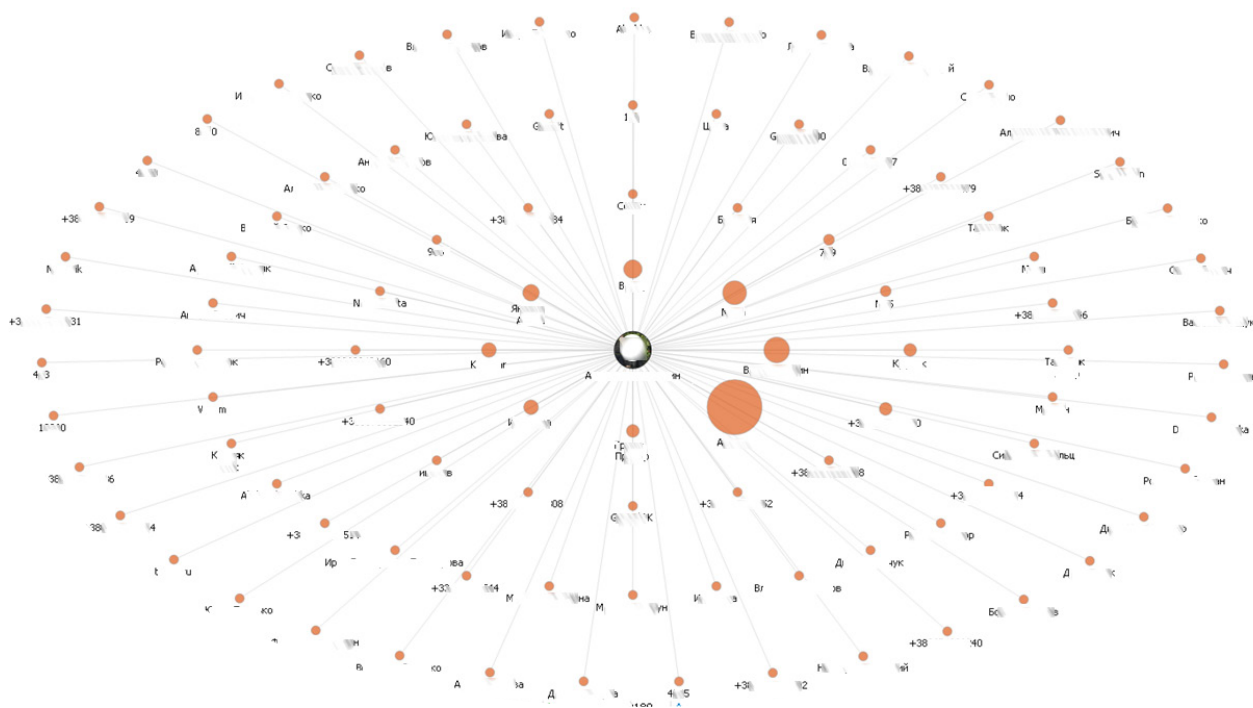


Рис. 4. Результаты відновлення даних з мобільного пристрою

Для того, щоб унеможливити подібні ситуації, потрібно або взагалі не передавати іншим особам свої старі мобільні пристрої, або використовувати спеціалізоване програмне забезпечення для видалення персональних даних. Крім наведеного, під час продажу власне мобільного пристрою ви можете стикнутися з іншими загрозами, які реалізуються знов таки через мобільні пристрої.

Мешканка Львова Тетяна Л. вирішила продати свій мобільний телефон Samsung S8 через систему OLX за 5000 грн. За деякий час до неї надійшла пропозиція придбати телефон від дівчини Аліни за 4800 грн. Телефон домовилися відправити поштою післяплатою до м. Одеса. Наступного дня до Тетяни зателефонував чоловік, який представився працівником служби технічної підтримки поштової компанії, та повідомив про помилку у введенні даних отримувача і про те, що зараз вони їх виправлять, а Тетяні потрібно продиктувати СМС із підтвердженням цієї операції.

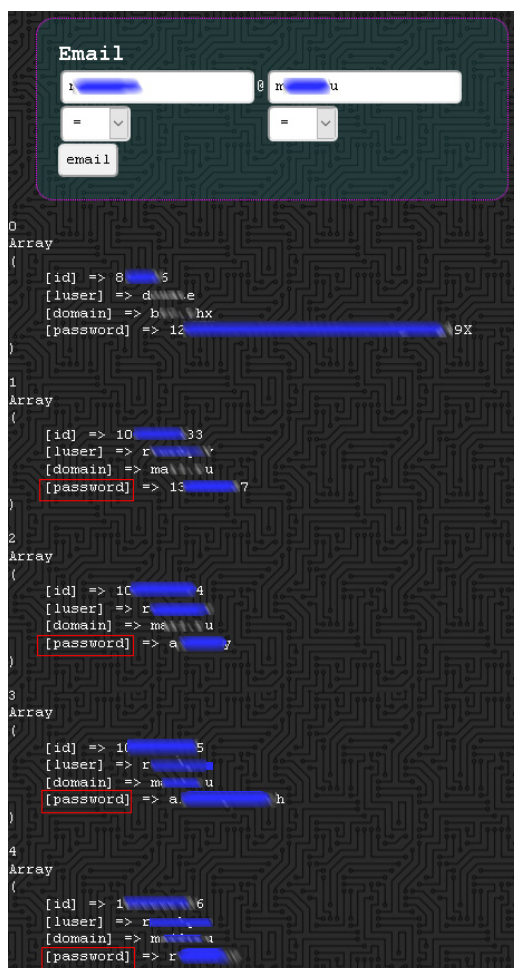
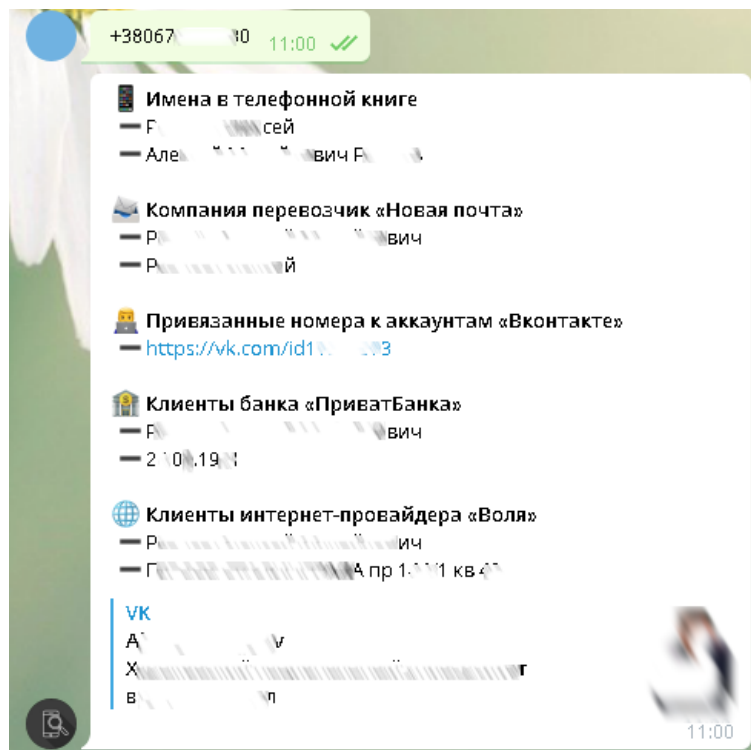
За допомогою цього коду шахраї увійшли в особистий кабінет Тетяни на сайті поштової компанії та скасували післяплату. Таким чином, ними було одержано телефон без оплати, а Тетяна втратила і телефон, і гроші.

Після подання скарги до поштової компанії її представник повідомив, що така ситуація трапилася в їх компанії вперше.

4. Передавання контактної інформації іншим особам

Взагалі слід якомога менше ділитися своїми персональними даними з іншими особами. Адже це теж підвищує ризик встановлення зловмисниками ваших повних персональних даних, які потім можуть бути використані з неправомірною метою.

На рис. 5 наведено приклад (особисті дані приховано), як, маючи суто телефонний номер особи, за допомогою спеціалізованих сервісів можна зібрати на неї повне досьє.



Report for phone: +38067****0

Facebook checker

email_part:

- r*****v@m***.ru
- r*****v@u**.net

phone_part:

- +3806****0

exists: true

Instagram exists: true

Skype possible accounts

skype_profile_uid: r*****

skype_profile_deep_link:

skype://r*****?chat

skype_contact_type:

Skype4Consumer

Telegram

firstname: O****j

lastname: R*****

telegram_profile_uid: 9*****8

lastseen: 202*-1*-1T14:05:45

Caller ID

fullname:

carrier: *****

country_code: **

Рис. 5. Результаты збирання даних про особу за номером телефону з використанням загальнодоступних мережевих сервісів

Одержана інформація може бути використана з різними цілями. Це – і шахрайство, і дискредитація, і шантаж, і створення умов для масштабної атаки на об'єкти, пов'язані з жертвою, тощо.

Зібравши інформацію про ваше коло спілкування, зловмисники можуть використати систему підміни параметру CallerID (Caller ID Spoofing). Відомими сервісами, які надають послуги із заміни CallerID, є spoofcard.com, spooftel.com. Далі порушники можуть зателефонувати вам з будь-якого знайомого номеру, наприклад, близької особи (рис. 6) або керівника. У випадку, якщо ви не виявите підміну номеру, це може призвести до незворотних наслідків.



Рис. 6. Підміна CallerID

5. Захоплення номеру телефона

При роботі з мобільними пристроями слід пам'ятати й про іншу небезпеку, яка виходить з недосконалості системи ідентифікації власника мобільного номеру. Йдеться про перереєстрацію зловмисником вашого номеру на своє ім'я через перевипуск SIM-картки. Очевидно, що заволодівши вашим мобільним номером, зловмисник здатен реалізувати наведені вище загрози, а також використовувати цей номер з неправомірною метою для вирішення поточних завдань.

Увечері державний службовець Галина П. одержала SMS від свого оператора про те, що відбувається заміна її SIM-картки. Вранці зв'язок припинився. Галина звернулася до сервісного центру мобільного оператора, де їй відновили телефонний номер протягом двох годин. Проте за цей час відбулося списання грошей з її банківського рахунку через систему онлайн-банкінгу.





У цьому прикладі зловмисник скористався системою відновлення мобільного номеру, алгоритм роботи якої базується на тому, що оператору потрібно вказати:

- ▶ номери, з яких найчастіше телефонували на відновлюваний номер;
- ▶ коли було здійснено останнє поповнення балансу;
- ▶ з якими номерами відбувалися останні з'єднання.

На теперішній час відповідно до ч. 2 ст. 107 Закону від 16.12.2020 «Про електронні комунікації» відновлення послуг у разі втрати електронних ідентифікаційних засобів знеособленим (анонімним) абонентом (у тому числі SIM-карти, e-SIM, налаштування інтернет-роутера тощо) здійснюється за умови ідентифікації цього абонента у постачальника електронних комунікаційних послуг та надання персональних даних. Разом з тим ніхто не заважає зловмисникам залучити для процедури відновлення особу-посередника з паспортом, яка за певну винагороду погодиться відновити SIM-карту на своє ім'я.

Якщо вам часто телефонують з невідомих номерів, раптово поповнюють баланс, це може свідчити про підготовку до зміни номеру.

Для того, щоб убезпечитись від вказаної ситуації, потрібно прив'язати свій телефонний номер до паспортних даних. Крім того, бажано для чутливих операцій використовувати телефонний номер, невідомий нікому, крім його володільця та оператора зв'язку, або про який обізнані тільки близькі особи. Якщо все ж таки ваш телефонний номер захопили, вам слід терміново спробувати заблокувати діючі банківські платіжні картки, а якщо це не виходить, спробувати зняти з них кошти у найближчому відділенні банку чи банкоматі.

Інколи користувачі мають упевненість, що вжили усіх заходів реагування. Проте, як показує практика, жодні додаткові заходи безпеки зайвими не будуть.

Зловмисники реалізували схему заволодіння коштами особи, які зберігалися в банку, який здійснює обслуговування без відділень. У власниці мобільного пристрою iPhone спочатку було вкрадено телефон. Власниця оперативно заблокувала його через Інтернет на сайті Apple та вирішила, що блокувати банківську платіжну картку не має сенсу, оскільки доступ до рахунку в банку можливий тільки зі знанням PIN-коду. Проте зловмисники перевели вкрадений пристрій в режим польоту, а згодом підключили його до мережі Інтернет через свій маршрутизатор, на якому було обмежено доступ до сервісів Apple. У той же час банківські застосунки продовжували працювати. Відтак, викрадачам вдалося вивести більше 70 тис. грн з рахунків жертви.



6. Шкідливе програмне забезпечення

Українським небезпечним, з погляду безпеки, є потрапляння на мобільний комунікатор шкідливого програмного забезпечення. Такі програми можуть виконувати різні функції. У будь-якому разі вони здатні скомпрометувати не тільки власну систему, в якій вони запущені, а й її власника.

Нерідко шкідливе програмне забезпечення здатне спричинити неприємні наслідки у вигляді зашифровки даних телефону, перехоплення автентифікаційних даних, надсилання повідомлень на платні номери, оформлення платних підписок на різні сумнівні сервіси, використання пристрою для скоординованої атаки на різні об'єкти тощо (рис. 7).



Рис. 7. Приклад роботи вірусу

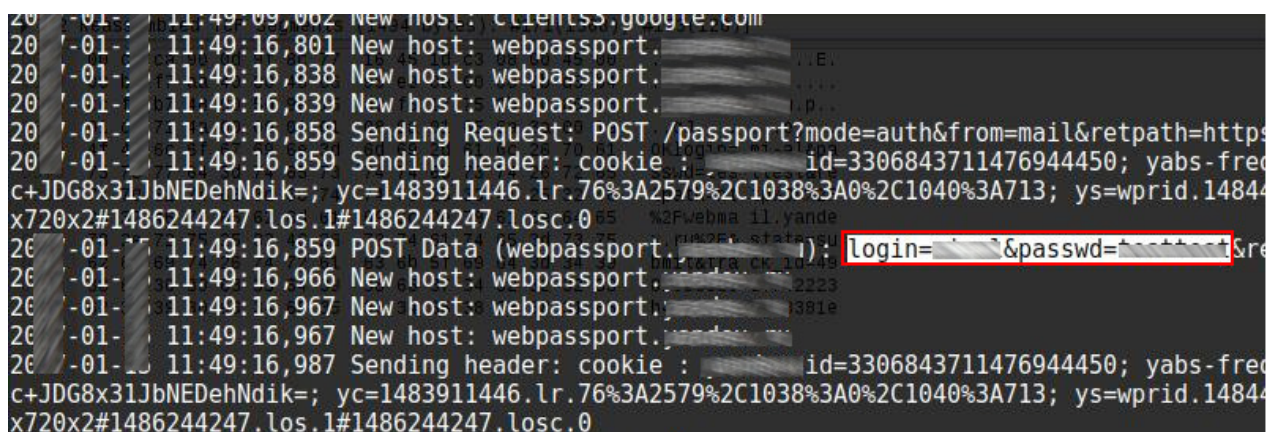
Кілька років тому було зламано телефон одного з найбагатших людей світу за допомогою спеціального відеофайлу в месенджері WhatsApp. За кілька годин після злому зі скомпрометованого телефону було викрадено кілька особистих файлів, а фотографії бізнесмена було передано одному з таблоїдів.

Враховуючи викладене, намагайтеся ніколи не встановлювати програмні рішення з неперевірених джерел. Інсталуйте антивірусне програмне забезпечення на свій пристрій. Не намагайтеся без крайньої необхідності отримати права суперкористувача root на своїх мобільних пристроях. З одного боку, рутінг дає можливість користувачеві зняти обмеження виробника чи оператора комунікацій, проте з іншого – полегшує зловмисникам доступ до вашого пристрою.

Додаткові функції мобільного пристрою

Крім наведеного, візьміть за звичку вимикати в телефоні функції, які ви не використовуєте.

Так, якщо у вас налаштовано автопідключення до відомих точок доступу Wi-Fi, ви так само автоматично можете бути під'єднаним до підробленої точки доступу. У подальшому весь трафік Інтернет може бути пропущений через обладнання зловмисника. Це дозволяє порушнику примусово перенаправляти запити з вашого пристрою на свої ресурси (рис. 8). При цьому ви можете навіть нічого не помітити.



```
20 -01- 11:49:09,002 New host: clients3.google.com
20 -01- 11:49:16,801 New host: webpassport.
20 -01- 11:49:16,838 New host: webpassport.
20 -01- 11:49:16,839 New host: webpassport.
20 -01- 11:49:16,858 Sending Request: POST /passport?mode=auth&from=mail&retpath=https
20 -01- 11:49:16,859 Sending header: cookie : id=3306843711476944450; yabs-fre
c+JDG8x31JbNEdehNdik=; yc=1483911446.l.r.76%3A2579%2C1038%3A0%2C1040%3A713; ys=wprid.1484
x720x2#1486244247.los.1#1486244247.losc.0
26 -01- 11:49:16,859 POST Data (webpassport.): login=*&passwd=*&re
26 -01- 11:49:16,966 New host: webpassport.
26 -01- 11:49:16,967 New host: webpassport.
26 -01- 11:49:16,967 New host: webpassport.
26 -01- 11:49:16,987 Sending header: cookie : id=3306843711476944450; yabs-fre
c+JDG8x31JbNEdehNdik=; yc=1483911446.l.r.76%3A2579%2C1038%3A0%2C1040%3A713; ys=wprid.1484
x720x2#1486244247.los.1#1486244247.losc.0
```

Рис. 8. Результат роботи програми mitmAP, призначеною для автоматизації створення безпроводної точки доступу та перехоплення трафіку

Необхідність вимикати невикористовувані функції стосується не тільки Wi-Fi, а й інших технологічних рішень. Увімкнений NFC-модуль, наприклад, може спричинити втрату грошових коштів або зараження вірусом.

У 2018 році працівники компанії Checkmarx продемонстрували, як зламати мобільний пристрій одним дотиком. Цей спосіб злому одержав назву NFCdrip і полягає в передачі зі спеціального пристрою або іншого смартфона через модуль NFC шкідливого програмного забезпечення на пристрій жертви.

Варто відзначити, що від цілеспрямованих атак на мобільні пристрої не можуть бути застраховані навіть особи, обізнані з правилами інформаційної та кібербезпеки. Тому слід дуже прискіпливо ставитися до усіх незрозумілих подій з вашим пристроєм і ретельно обмірковувати свої дії в таких випадках.

Кілька років тому близько двадцяти керівників криптовалютних бірж Ізраїлю стали жертвами кіберзлочинців, які зламали їх облікові записи в Telegram. Попередньо зловмисники одержали доступ до стільникової мережі за кордоном та надіслали звітти оператору в Ізраїлі службове повідомлення про зміну місцезнаходження абонента-жертви. Після цього вони фактично змогли контролювати вхідні повідомлення жертви і таким чином зламати її облікові записи. У даному випадку, очевидно, у жертв злочину не було встановлено двофакторної автентифікації, що дозволило зловмисникам захопити їх облікові записи.

Висновки

Усі наведені загрози не є вичерпними. Слід враховувати, що вони відображають тільки кілька ризиків. При цьому постійно з'являються нові вразливості та атаки, які можна відслідкувати тільки в процесі самоосвіти.

Тим не менш, для забезпечення прийнятного рівня безпеки слід дотримуватися базових правил:

1. Встановити PIN-код на SIM-картку для того, щоб у разі її втрати зловмисники не змогли її використати з неправомірною метою.
2. Де можливо, використовуйте двофакторну автентифікацію.
3. Активуйте у смартфоні функції «Знайти телефон». Якщо ви втратите телефон, то в подальшому це може допомогти оперативно встановити місцезнаходження втраченого пристрою.
4. Не прикріплюйте всі банківські платіжні картки до єдиного телефонного пристрою. У випадки втрати пристрою вам не доведеться блокувати всі платіжні картки.
5. Встановіть складний пароль на доступ до пристрою та увімкніть біометричну автентифікацію.
6. За можливості не вмикайте в телефоні функцію Smart Lock (розблокування за допомогою сторонніх пристроїв, наприклад, смарт-годинника). Зловмисники можуть скористатися цією функцією для злову вашого пристрою.
7. Слід вимкнути функцію виведення повідомлень на заблокований екран:

iOS: «Налаштування» > «Повідомлення» > «Показ мініатюр» > «Ніколи».

Android: «Налаштування» > «Повідомлення» > «Повідомлення (Екран блокування)» > «Приховати вміст».

- 
8. Не створюйте та не пересилайте за допомогою месенджерів і повідомлень телефону скан-копії важливих документів, інтимні фотографії.
 9. Якщо вам хтось надсилає повідомлення або телефонує з проханням термінового переказу коштів, візьміть паузу, все добре обдумайте. За можливості передзвоніть іншим особам, пов'язаним із запитувачем, а також йому самому та переконайтеся, що це саме та особа, про яку ви думаєте. У подібних ситуаціях намагайтеся не пересилати кошти на карти чи електронні гаманці: краще передати їх особисто.
 10. Якщо змінюється номер мобільного телефону, потрібно не забути перереєструвати усі наявні облікові записи на новий номер.
 11. Якщо телефон було втрачено, потрібно терміново звернутися до оператора телекомунікацій та заблокувати SIM-картку, заблокувати банківські платіжні картки. Надішліть повідомлення на сайти мікрофінансових установ про те, що ваш телефонний номер було втрачено. У разі необхідності зверніться до поліції. Повідомте про інцидент безпосереднього керівника та особу, яка відповідає за безпеку у вашому підрозділі. Поділіться із колегами досвідом розв'язання інциденту, пов'язаного з порушенням безпеки.

Шкідливе програмне забезпечення

План лекції

Вступ

1. Джерела шкідливого програмного забезпечення
2. Шляхи розповсюдження, вектори атак
3. Види шкідливого програмного забезпечення
4. Ознаки ураження ШПЗ

Висновки

Рекомендована література Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.

Допоміжна

5. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 72–73.
6. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 65–67.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

Текст лекції

Вступ

Шкідливе програмне забезпечення (ШПЗ) – це програмне забезпечення (ПЗ), яке використовується зловмисниками для проведення атак на комп'ютерні системи. Наслідками активності ШПЗ може бути знищення, блокування, модифікація, копіювання інформації або порушення роботи комп'ютерних систем і мереж.

1. Джерела шкідливого програмного забезпечення

ШПЗ може створюватись як окрема програма, а може базуватися на корисних програмах. Наприклад, програми легального віддаленого доступу та адміністрування можуть бути використані як шкідливі.

ШПЗ можна купити на спеціалізованих форумах та сайтах в мережі Інтернет, вартість коливається від кількох десятків доларів то кількох тисяч. Досить часто ШПЗ надається як сервіс (Malware-as-a-service), де клієнт платить місячну/денну/тижневу плату за користування ШПЗ. На рис. 1 наведений фрагмент реклами ШПЗ на хакерському форумі.

The image is a screenshot of a forum post on a Russian-language hacker forum. The post is titled "Avalon stealer - один из лучших стиллеров [билдер за 100\$]" (Avalon stealer - one of the best stealers [builder for 100\$]). The user "Morwenns" posted it on July 7. The post describes the capabilities of the "Avalon" malware, listing various data it can steal from a system, such as browser data, system information, and files. It also mentions that the malware is available for purchase for 100\$. The post is written in Russian and includes a list of features and a price.

Avalon stealer - один из лучших стиллеров [билдер за 100\$]

By Morwenns, July 7 in [Software] - malware, exploits, bundles, crypts

Представляем вам свежий проект, имеющий больше возможности, которые заинтересуют вас. В его функционал входит:

1. Сбор со всех браузеров на данные Chromium КРОМЕ нового Яндекс браузера. - формы автозаполнения, куки, данные истории и загрузок, пароли, кредитные карты.
2. Сбор со всех браузеров на данные Firefox (Firefox и так далее) - формы автозаполнения, пароли, куки, кредитные карты.
3. Сбор с браузера Edge - только пароли.
4. Сбор сессий Telegram, Discord, Authy, FileZilla, Total Commander, Psi+, Pidgin.
5. Сбор данных почты Outlook.
6. Продвинутый граббер файлов с возможностью выбора нужных расширений, минимального размера файла и путей поиска. Сортирует файлы по расширению и папки, откуда скопированы.
7. Рекурсивный сбор файлов RDP и кошелек wallet и wallet.dat с учетной записью пользователя.
8. Копирование файловых сертификатов (по выбору).
9. Сбор файлов кошельков кошельков Armory Wallet, Atomic Wallet, Bitcoin Core, Bytecoin, Dash Core, Electrum, Exodus, Jaxx, Litecoin Core, Monero Wallet, Zcash.
10. Детектор доменов (настроен по умолчанию - возможность своей настройкой).
11. Загрузка (по выбору) с возможностью запуска с задержкой.
12. Подмена бита файлового сертификата (по выбору).
13. Файлы данных буфера обмена, запущенных процессов, установленных программ, и, конечно же, скриншот.
14. Подробная информация о системе:
 - Операционная система.
 - Имя пользователя.
 - Ключ активации системы.
 - Расширение экрана.
 - Модель процессора.
 - Размер оперативной памяти.
 - Модель видеокарты.
 - Данные BIOS.
 - IP.
 - Номер HWID.
17. Защита: Предотвратить уклад компьютера в сон, запуск с задержкой, анти виртуальная машина (= файсовое сообщение), анти отладчик (= выход по выбору), самоуничтожение, шифрование строк, внутренний модуль обфускации, возможность отключения работы стиллера если на компьютере запущен VPN.
18. Весь стиллер работает в оперативной памяти, и не создает никаких файлов кроме временных архивов.
19. Информационный файл (Information.html) имеет вид красной html страницы и содержит в себе следующие данные. Если выбрана отправка по Telegram то данные идут как в сообщении, так и в файле:
 - Имя компьютера/имя пользователя.
 - IP адрес, страна, включен ли VPN.
 - Данные о собранных данных с браузеров.
 - Имеется ли на компьютере кошельки кошельки (если да, то какие).
 - Количество собранных файлов граббером.
 - Количество собранных кошельков wallet и wallet.dat рекурсивным методом.
 - Количество собранных файлов RDP рекурсивным методом.
 - Была ли собрана сессия Discord (если она установлена).
 - Была ли собрана сессия Telegram (если она установлена).
 - Количество собранных данных забот клиента (если она установлена).
 - Количество собранных данных FTP клиента (если она установлена).
 - Количество собранных данных VPN клиентов (если они установлены).
 - Данные номера железа (HWID).
 - Операционная система.
 - Домены, которые обдували детектор.
20. Отправка на Mega.nz, FTP, Telegram.
21. При каждом последующем билде меняется информация манифеста файла, и названия переменных кода.
22. Функционал кейлоггера.
1. Логг идут туда же куда и шли от стиллера.
2. Возможность выбрать интервал символов для отправки.
3. Кейлоггер записывает следующие данные: Текущее окно, в котором происходит ввод, обычные и системные клавиши, информирование о смене раскладки.

Важная информация:
Стиллер работает на всех системах Windows с установленным .NET Framework 4.

Мы гарантируем вам хороший отклик на любой вид отправки.

Стиллер НЕ работает в следующих странах: Армения, Азербайджан, Беларусь, Казахстан, Киргизстан, Молдова, Россия, Таджикистан, Узбекистан, Украина.

Цена: 100\$, а не входит: сам билдер, лицензионный ключ, и техническая поддержка на протяжении 30 дней с момента покупки.

Ваша поща на FTP и Mega.nz:

Рис. 1. Реклама ШПЗ

У вільному доступі існують різноманітні інструменти конструювання ШПЗ для отримання несанкціонованого віддаленого доступу до систем, зокрема це – Metasploit-Framework, Veil-Framework (рис. 2) та інші.

```
$ ./Veil.py
=====
Veil | [Version]: 3.1.6
=====
[Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
=====

Main Menu

2 tools loaded

Available Tools:

1) Evasion
2) Ordinance

Available Commands:

exit      Completely exit Veil
info      Information on a specific tool
list      List available tools
options    Show Veil configuration
update    Update Veil
use       Use a specific tool

Veil>
```

Рис. 2. Меню Veil-Framework

2. Шляхи розповсюдження, вектори атак

Спам. Існує кілька найпоширеніших шляхів розповсюдження ШПЗ, серед них безперечним лідером є масова розсилка повідомлень, зазвичай рекламного характеру, людям, які не дали згоди на їх отримання, – спаму.

Зловмисники можуть надсилати спам, атакуючи певні галузі, наприклад, страхові компанії, медичні установи, державні структури або певних користувачів. Бази адресів для спаму зазвичай купуються на хакерських форумах.

Таргетовані або цільові спам-кампанії спрямовані на конкретних осіб або організації. Це – більш складний тип атаки, оскільки таргетовані спам-кампанії передбачають попереднє вивчення майбутньої жертви, наприклад, її активності в соціальних мережах, родинних зв'язків, уподобань, хобі, життєвих проблем тощо. Ця інформація дозволяє зловмиснику створювати переконливе повідомлення, щоб змусити жертву запустити ШПЗ.

Зловмисники надсилають через вкладення до електронного листа спеціально створені файли, наприклад, MS Word/Excel, PDF, PNG, ZIP, EXE, які після активізації вже завантажують ШПЗ із віддаленого серверу та запускають на комп'ютері жертви (рис. 3).

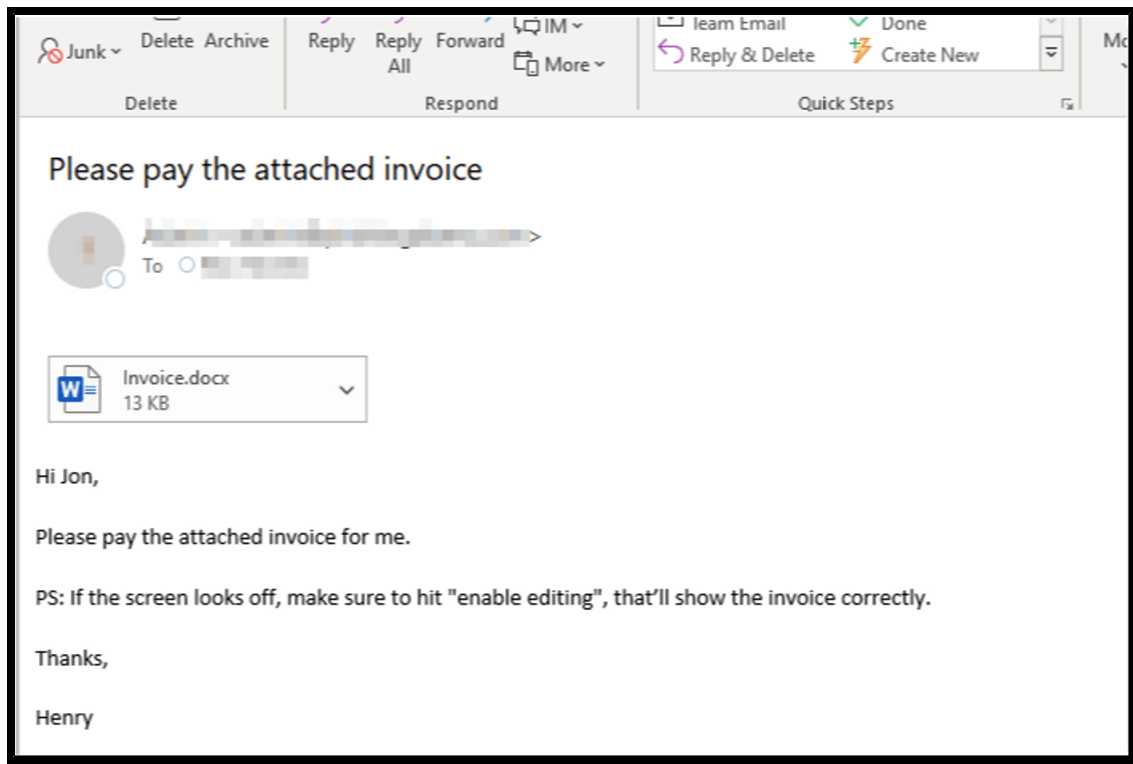


Рис. 3. Вкладення файлу MS Word, який містить макрос завантаження ШПЗ

Іншим способом є надсилання шкідливого файлу із «фейковим» або з так званим «подвійним розширенням». У такому випадку зловмисники змінюють розширення файлу, а також змінюють іконку файлу на відповідне розширення. Це створює враження, що файл є безпечним та може бути відкритий. Наприклад, файл `note.txt.exe` насправді є виконуваним файлом, а не текстовим, і якщо у користувача вимкнено функцію показувати розширення файлів, у нього складеться враження, що він відкриває текстовий файл, натомість запускаючи при цьому ШПЗ.

Щоб увімкнути функцію «Показувати розширення файлів»:

- Натисніть кнопку «Пуск» і виберіть пункт меню «Мій комп'ютер».
- Далі в меню оберіть пункт «Сервіс», потім пункт «Властивості папки».
- У вікні «Властивості папки», виберіть вкладку «Вигляд».
- Знайдіть пункт «Приховувати розширення для зареєстрованих типів файлів» і зніміть з нього галочку.

* може дещо відрізнятись залежно від версії операційної системи.

Для того, щоб змусити жертву відкрити вкладений шкідливий файл, зломисники застосовують засоби соціальної інженерії.

Як альтернатива, злочинці можуть вставляти посилання на завантаження ШПЗ безпосередньо в повідомленні та маскувати його під виглядом легітимної програми чи додатку. На рис. 4 показані приклади фішингових листів, які використовували тему світової пандемії коронавірусу 2020 р. для розповсюдження ШПЗ.

Фішинг – вид онлайн-шахрайства, який базується на методах соціальної інженерії та має на меті шляхом обману змусити користувача здійснити дії, які б він не здійснив у звичних умовах, наприклад, розкрити свої персональні дані, завантажити, встановити чи запустити шкідливе програмне забезпечення. Фішинг може бути здійснений у різних формах: електронні листи, надіслані нібито від імені легальних компаній, фейкові веб-сайти, дзвінки нібито співробітників банку тощо.

Coronavirus - Recommendations to prevent infection spread



Coronavirus Cases:	Deaths:	Recovered:
1,203,428	64,754	246,803

Dear

Common signs of infection include respiratory symptoms, fever, cough, shortness of breath and breathing difficulties. In more severe cases, infection can cause pneumonia, severe acute respiratory syndrome, kidney failure and even death.

Recommendations to prevent infection spread include regular hand washing, covering mouth and nose when coughing and sneezing, thoroughly cooking meat and eggs. Avoid close contact with anyone showing symptoms of respiratory illness such as coughing and sneezing.

If you want to know how many people are infected in your city, follow the [link](#) and download our application

Sincerely,
Department of Public Health
© 2020 WHO

This is an automatically generated message.



Coronavirus Cases:	Deaths:	Recovered:
279,344	11,587	92,913

Your health and well-being are our priority. Learn more about COVID-19, what Medicare covers, and how to assess your risk, protect yourself and get care.

With the support of the United States Department of Health and Human Services, we will provide you with a certificate for free medical care

[DOWNLOAD](#)

To avoid the coronavirus and other illnesses such as the flu, the CDC recommends:

- Avoiding close contact with people who are sick,
- Avoiding touching your eyes, nose, and mouth,
- Staying at home when you are sick,
- Covering your cough or sneeze with a tissue, then throwing the tissue in the trash,
- Washing your hands often with soap and water for at least 20 seconds, especially after going to the bathroom; before eating; and after blowing your nose, coughing, or sneezing.

The eHealth's Medicare Team



This article is for general information and should not be relied on as medical advice. Check with a medical professional for medical advice.

eHealth's Medicare is operated by eHealthInsurance Services, Inc., a licensed health insurance agency doing business as eHealth. The purpose of this site is the solicitation of insurance. Contact may be made by an insurance agent/producer or insurance company. We offer plans from a number of insurance companies.

Speak with a licensed insurance agent 1-888-672-0651 TTY User: 711 | Mon - Fri, 8am - 9pm

Рис. 4. Приклади фішингових листів

Програми нелегальної активації комерційного ПЗ. Іншим, не менш поширеним способом розповсюдження ШПЗ є поширення так званих «креків» для комерційного програмного забезпечення або власне примірників «зламаного» комерційного програмного забезпечення, яке «не потребує купівлі ліцензії».

«Крек» (від англ. «crack») – це програма, яка генерує код активації для комерційного програмного забезпечення чи змінює систему перевірки ліцензії комерційного програмного забезпечення і тим самим порушує авторські права виробника.

У такому випадку зловмисники додають шкідливий програмний код у модифіковане комерційне програмне забезпечення. Нічого не підозрюючи, користувач встановлює таку програму, а разом з нею – і ШПЗ, за допомогою якого зловмисники отримують доступ до системних файлів. На рис. 5 показаний приклад розповсюдження програми-вимагача (ransomware) під виглядом програми активації ОС Windows.

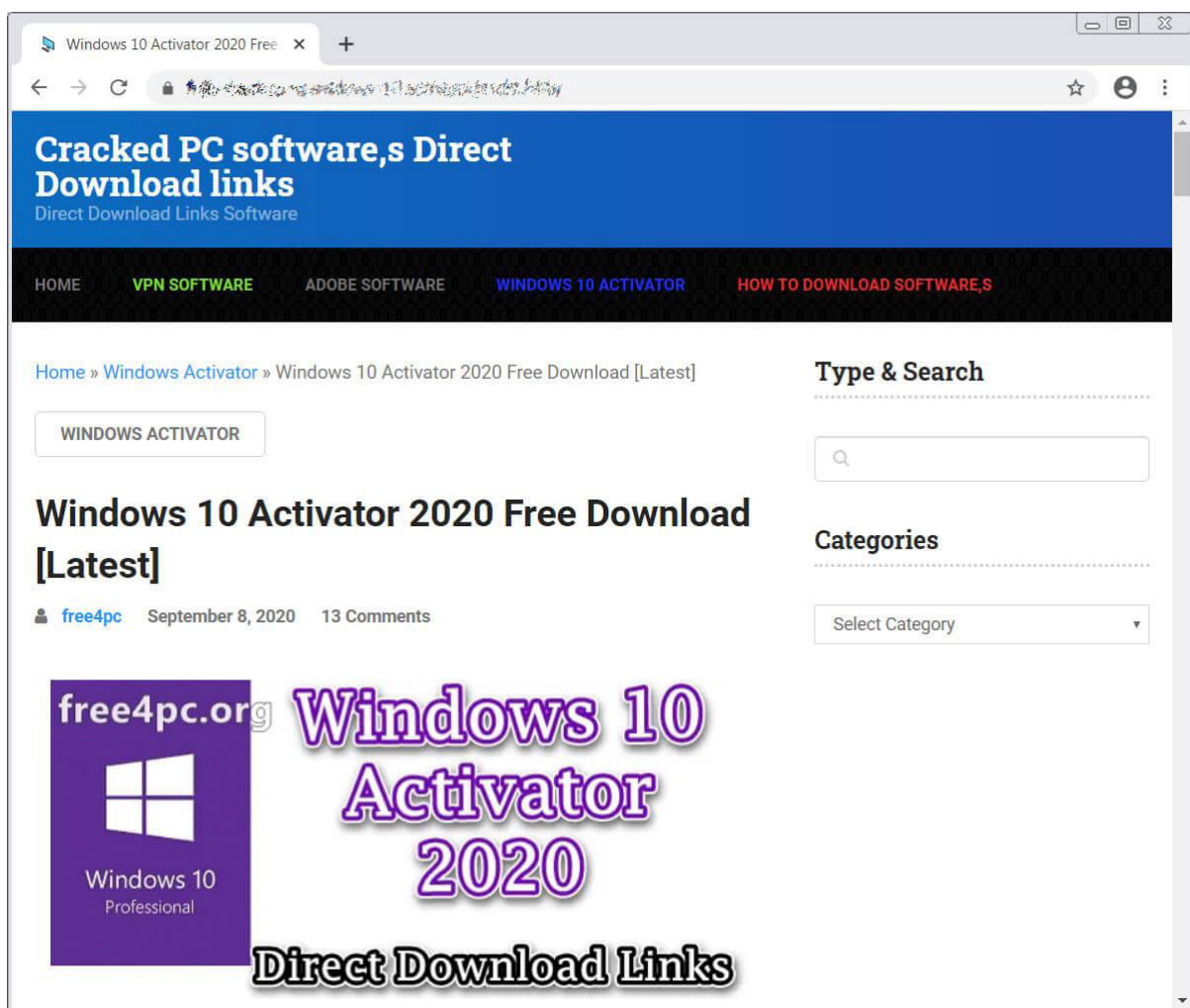


Рис. 5. Приклад розповсюдження програми-вимагача (ransomware) під виглядом програми активації ОС Windows

Безкоштовне ПЗ. Різновидом цього способу є поширення ШПЗ під виглядом «freeware»-програм. Це, як правило, так звані «корисні» програми, такі як ліхтарики для мобільних телефонів, калькулятори, конвертери валют тощо. Найбільш поширеними вони є для мобільних пристроїв. На рис. 6 зображено програми для фітнесу, які приховано встановлювали на мобільний пристрій ШПЗ для крадіжки банківської інформації.

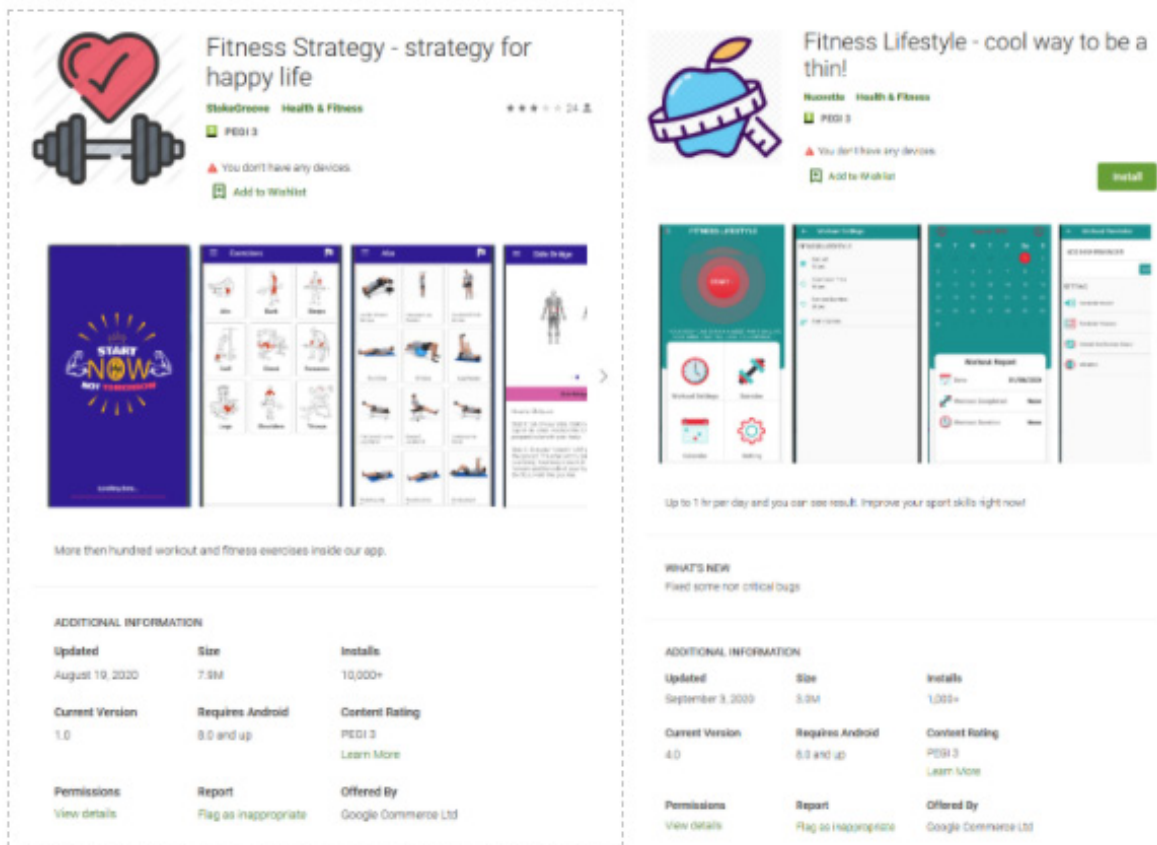


Рис. 6. ШПЗ під виглядом корисного ПЗ

Для зменшення ризику встановлення ШПЗ під виглядом корисної безкоштовної програми необхідно:

- ▶ уникати ПЗ з малим рейтингом та поганими відгуками користувачів у репозиторії (магазині) додатків;
- ▶ при встановленні ПЗ звертати увагу на дозволи доступу до ресурсів операційної системи, які запитує додаток. Очевидно, що програмі ліхтарика не потрібний доступ до текстових повідомлень, камери, мікрофону чи фото, щоб ефективно працювати;
- ▶ ознайомитись з інформацією про розробника ПЗ: наскільки він відомий на ринку ПЗ, чи існують інші додатки й який у них рейтинг, чи є власний сайт тощо.

Таргетовані атаки із використанням «нетрадиційних методів». Сюди можна віднести «випадково загублені флешки», фізичний доступ злоумисника до комп'ютера, складні прийоми соціальної інженерії: коли телефонують користувачеві та просять встановити ту чи іншу програму, наприклад, під виглядом співробітників банку. На окрему увагу заслуговує загроза від інсайдерів, які вербуються для встановлення ШПЗ, відключення антивірусів та міжмережевих екранів (рис. 7).

**Наша команда ищет ответственных сотрудников государственных структур, банков, сотовых операторов и т.д
РФ, БЕЛОРУССИЯ, КАЗАХСТАН, УКРАИНА!**

Кого мы ищем?

Сотрудников банков (РФ, БЕЛОРУССИЯ, КАЗАХСТАН, УКРАИНА!)

Спойлер: КАКИЕ БАНКИ ПОДОЙДУТ? ПРИМЕР

*По остальным странам интересуют все сотрудники банков.
ПО рф так же любой банк интересуется!

Сотрудники государственных учреждений: (РФ, БЕЛОРУССИЯ, КАЗАХСТАН, УКРАИНА!)

**Россия: ФНС, МВД, ПФР, ЗАГС, ФСБ, ГИБДД и т.д
БЕЛОРУССИЯ, КАЗАХСТАН, УКРАИНА: Любые гос. служащие.**

Сотрудники сотовых компаний: (РФ, БЕЛОРУССИЯ, КАЗАХСТАН, УКРАИНА!)

**Россия: Мегафон, Теле2, Тинькофф мобайл, СберМобайл, Йота, Билайн, Мтс
БЕЛОРУССИЯ, КАЗАХСТАН, УКРАИНА: Любые сот. операторы.**

Рис. 7. Оголошення про пошук інсайдерів

3. Види шкідливого програмного забезпечення

Складність класифікації ШПЗ полягає в широкому функціоналі таких програм. Наприклад, ШПЗ *Agent Tesla* виконує функції кейлогера (keylogger), викрадача інформації (stealer) та є вдосконалим трояном віддаленого доступу (RAT). З огляду на базові функції ШПЗ можна поділити на види, про які йдеться нижче.

Вірус. Основна функція – самореплікація (саморозмноження) в комп'ютерній системі, за рахунок якої він стає здатним впроваджувати свій код в інші програми, тим самим заражаючи їх. Заражене ПЗ стає здатним далі також самореплікувати код вірусу в інші ПЗ. Чистий вірус не має жодної іншої логіки, крім самореплікації.

Наразі найпоширенішими вірусами є макровіруси (інструкції, які приєднані до файлів офісних документів), що впроваджуються у файли типу .docx, .xlsx та інші.

Троян. Основна функція – обманювати жертв за рахунок застосування оболонки безпечного ПЗ. Порівняно із вірусом (а також з безліччю інших ШПЗ), троян не має як таких алгоритмів виконання, а є лише оболонкою для інших ШПЗ.

Хробак. Основна функція – самореплікація в комп'ютерній мережі, завдяки якій він стає здатним дублювати себе як у межах однієї системи, створюючи численні копії в каталогах, так і переміщаючись в інші системи комп'ютерної мережі, створюючи в кожній окремій свою копію.

На відміну від вірусу, що має точно такий самий механізм самореплікації, хробак не впроваджується в уже наявне ПЗ, а створює свою копію як окремий файл.

Шифрувальник (вимагач). Основна функція – шифрування файлів на системі жертви таким чином, щоб жертва не могла відновити все раніше зашифроване, що призводить до втрати всіх файлів. Часто шифрувальника також називають вимагачем, оскільки трапляються випадки, коли ШПЗ пропонує за викуп надати ключ розшифрування (рис. 8).

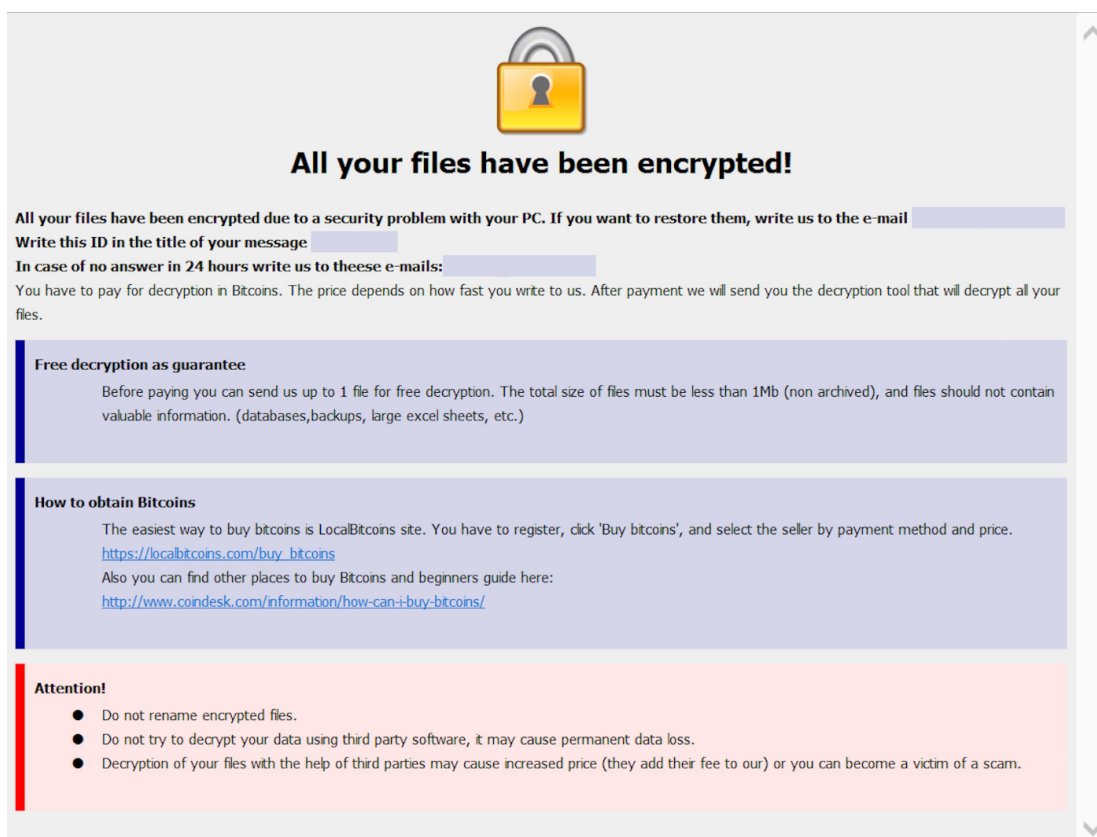


Рис. 8. Повідомлення шифрувальника (вимагача)



Локаер. Основна функція – блокування дій жертви під час роботи в системі. У такому разі жертва або не може посувати мишкою, або не може переглядати файли, або зовсім може не мати доступу до файлової системи. Локаера також іноді називають вимагачем, коли таке ШПЗ блокує екран жертви і виводить на екран поле введення пароля розблокування і реквізити з необхідністю «викупити» можливість далі користуватися системою.

На відміну від шифрувальника, що блокує доступ до файлів за допомогою їхнього шифрування, локаери використовують блокування інтерфейсу, не шкодячи самим файлам.

На відміну від вірусів, троянів і хробаків, які не мають у своєму виконанні деструктивної логіки, шифрувальники представляють логіку руйнування.

Програма віддаленого доступу. Програма віддаленого доступу сама по собі не є ШПЗ, проте може використовуватися як така. Програми віддаленого доступу забезпечують передачу даних від однієї системи до іншої. Супутні дії (у тому числі деструктивні) можуть розглядатися як комбінація застосувань кількох програм. Програми віддаленого доступу, що використовуються як ШПЗ, також називають RAT (Remote Access Trojan).

Стілер. Основна функція – автоматична крадіжка інформації з системи жертви. Стілери мають багато реалізацій, починаючи від програм-шпигунів (Spyware), що зчитують інформацію в потоковому режимі з клавіатури та веб-камери, закінчуючи стілерами, що розміщені для автоматичного запуску на флешці або у мікропроцесорі Arduino.

Руткіт. Основна функція – приховування дій, видалення слідів або забезпечення відмовостійкості заданих програм. Руткіт не має конкретної деструктивної логіки, на відміну від шифрувальників, локаерів та стілерів, але водночас забезпечує приховування їхніх дій або запобігання передчасному їхньому вимкненню, тобто забезпечують безперебійність виконання конкретно заданих зовнішніх функцій.

Буткіт. Основна функція – виклик програм до завантаження операційної системи, внаслідок чого буткіт стає здатний ефективно приховувати раніше запущені процеси, які не можна буде побачити стандартними засобами ОС.

Ботнет. Основна функція – це кооперування безлічі заражених жертв (ботів) з метою здійснення запланованої дії, що вимагає багато обчислювальних ресурсів. Прикладом таких ШПЗ можуть слугувати майнери криптовалют, які обчислюють необхідний ґеш у завданні типу Proof-of-Work. Також прикладом ботнетів може слугувати атака розподіленої відмови в обслуговуванні (DDoS).

Ботнет може бути як централізованим, так і децентралізованим. Остання форма також може бути поділена на два види – підконтрольний і

безконтрольний ботнет. У першому випадку існує контролюючий вузол, у той час як у другому випадку контролю дій не існує зовсім.

Спамер. Основна функція спамера – створення, видача або заміна рекламних банерів у браузерях, застосунках, сайтах, а також можливе надсилання повідомлень у месенджерах, соціальних мережах і поштою. Цей вид ШПЗ також називають рекламними програмами (Adware).

Установник (завантажувач, дропер/лоадер). Основна функція – автоматичне завантаження і запуск програм (рис. 9). Певною мірою установники схожі з програмами віддаленого доступу – вони створені для транспортування даних. Але на відміну від програми віддаленого доступу, дії якої здійснюються ручним способом і спрямовані від зловмисника до жертви, установники діють повністю автономно за конкретно заданим алгоритмом, а їхні дії протилежні віддаленому доступу і спрямовані від жертви до зловмисника.

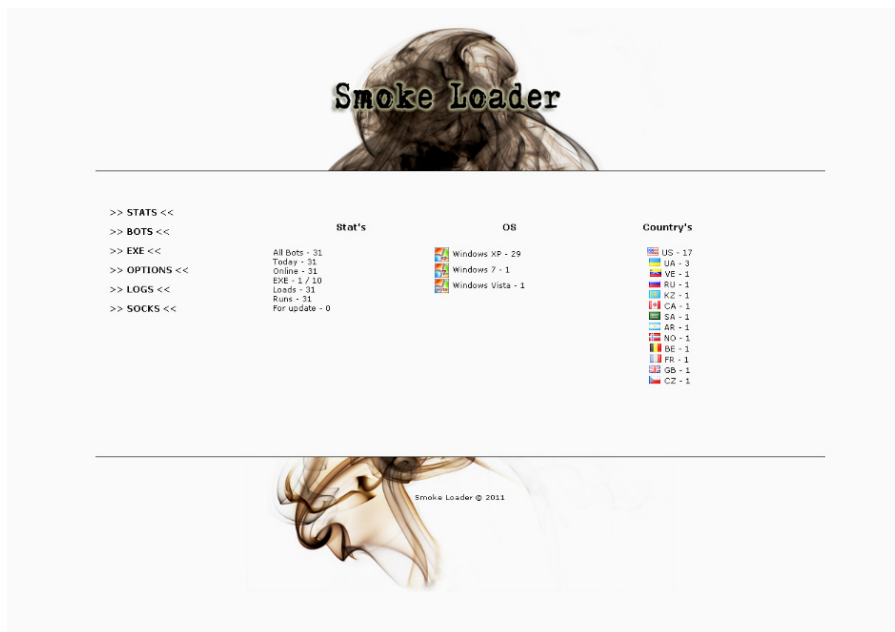


Рис. 9. Меню налаштування ШПЗ типу установника

Логічна бомба. Основна функція – зчитування умови, за якої відбуватиметься розпакування та/або запуск певного ПЗ. На відміну від безлічі інших ШПЗ, логічна бомба не самодостатня і потребує додаткової логіки виконання (шкідливого навантаження).

Очищувач. Основна функція – безповоротне видалення всіх можливих файлів на системі жертви.

Ініціалізатор. Основна функція – забезпечення автоматичного запуску ШПЗ операційною системою після свого старту. Є одним із найпоширеніших помічників за рахунок своєї відносної простоти і можливості відтворювати виконання програм навіть після перезавантаження системи.

За функціями ШПЗ можна також розділити на 3 категорії (табл. 1):

- ▶ **виконувачі** – безпосередньо виконують шкідливу дію щодо системи або користувача;
- ▶ **розповсюджувачі** – здійснюють доставку ШПЗ від однієї системи до іншої;
- ▶ **помічники** – забезпечують відмовостійкість, живучість та прихованість інших ШПЗ.

Таблиця 1. Категорії ШПЗ за функціями

ВИКОНУВАЧІ	РОЗПОВСЮДЖУВАЧІ	ПОМІЧНИКИ
Шифрувальник Локаер Стілер Спамер Ботнет Очишувач	Троян Хробак Програма віддаленого доступу (ПВД) Установник	Вірус Логічна бомба Руткіт Буткіт Ініціалізатор

Часто ШПЗ є композицією кількох видів і категорій програм, зокрема:

- ▶ Виконувач + Розповсюджувач:
 - Хробак + Шифрувальник
 - Троян + Стілер
 - Хробак + Ботнет
 - Троян + Спамер
 - ПВД + Стілер
- ▶ Виконувач + Помічник:
 - Буткіт + Локаер
 - Руткіт + Спамер
 - Вірус + Ботнет
- ▶ Виконувач + Виконавець:
 - Шифрувальник + Локаер
 - Спамер + Стілер
- ▶ Помічник + Розповсюджувач:
 - Руткіт + ПВД
 - Вірус + Установник
- ▶ Помічник + Помічник:
 - Руткіт + Вірус
 - Вірус + Руткіт
- ▶ Розповсюджувач + Розповсюджувач:
 - Троян + Хробак
 - Хробак + Троян
 - Троян + ПВД
 - ПВД + Троян
 - Хробак + ПВД

- ▶ Виконувач + Помічник + Розповсюджувач:
 - Ботнет + Буткіт + Хробак
 - Стілер + Логічна бомба + Троян
 - Спамер + Вірус + Установник
- ▶ інші композиції.

4. Ознаки ураження ШПЗ

Поміж загальних ознак, таких як повільна робота комп'ютера (мобільного пристрою), поява рекламних повідомлень, постійні безпричинні перезавантаження, відключений антивірус, значна мережева активність, брак системних ресурсів, поява на робочому столі чи екрані смартфона невідомих іконок або іконок програм, які ви не встановлювали, тощо, можна виділити кілька специфічних ознак.

Підозріла активність акаунтів у соціальних мережах, поштових акаунтів тощо.

- ▶ вам прийшло повідомлення, що хтось намагався увійти до ваших акаунтів Facebook, Twitter, Gmail тощо;
- ▶ ви помітили IP-адреси, з яких не здійснювали доступ до своїх акаунтів, чи підозрілі прилади, які здійснювали доступ;
- ▶ ви помітили імейли, дописи, пости, фото, які особисто не додавали або не надсилали.

Дії:

- ▶ негайно змінити усі паролі, встановити двофакторну автентифікацію (2FA);
- ▶ перевірити систему антивірусом чи іншою програмою із виявлення ШПЗ;
- ▶ звернутися по допомогу до спеціалістів з інформаційної безпеки (ІТ-департамент, приватні організації).

Вам надійшло повідомлення від вашого банку про списання або спробу списання коштів.

Дії:

- ▶ звернутися до служби підтримки банку та повідомити про підозрілу активність, заблокувати банківський рахунок та платіжні картки;
- ▶ змінити паролі до банківських рахунків, встановити 2FA;
- ▶ перевірити систему, в тому числі мобільний пристрій, антивірусом чи іншою програмою із виявлення ШПЗ;
- ▶ звернутися по допомогу до спеціалістів з інформаційної безпеки (ІТ-департамент, приватні організації).

Ви помітили підозрілу активність операційної системи:

- ▶ система завантажена та зависає;
- ▶ файли стали недоступними;
- ▶ ви помітили файли із підозрілим розширенням;
- ▶ на робочому столі та в папках з'явилися підозрілі файли, а вам надійшло повідомлення, що ваші файли зашифровано.

Дії:

- ▶ вимкнути комп'ютер та звернутися по допомогу до спеціаліста.

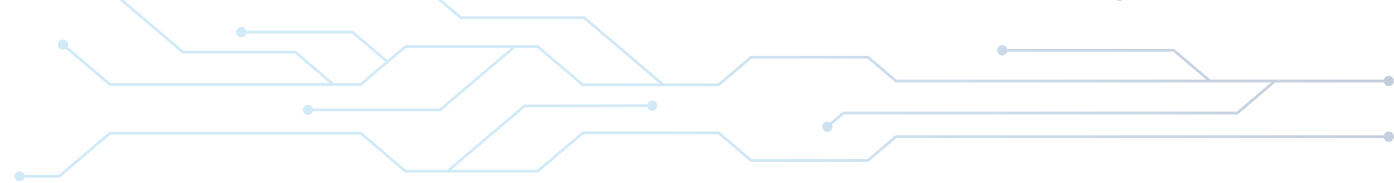
Якщо файли все ж були зашифровані, можна спробувати визначити тип вимагача та пошукати дешифратор, хоча ймовірність повернути файли за відсутності резервних копій мінімальна.

Як визначити, яким типом вимагача (ransomware) була уражена система:

- ▶ визначити розширення, яке додає файлам ransomware: це може бути «.KICK», «.crash», «.harma», «.PLUT», «.wal», «.txt», «.FREDD» та сотні інших;
- ▶ із відкритих джерел встановити, чи було випущено дешифратор для цього типу ransomware, АБО скористатися сайтом <https://id-ransomware.malwarehunterteam.com>.

Ознаки ураження ШПЗ мобільного пристрою:

- ▶ пристрій працює значно повільніше, ніж зазвичай, зависає, батарея розряджається значно швидше, ніж зазвичай;
- ▶ з'явилися іконки програм, яких не встановлювали; замість звичного веб-браузера запускається інший;
- ▶ невідомі програми просять надати їм root-права (root-права – це права суперкористувача на пристроях під управлінням операційної системи «Android». Основними цілями root-прав є зняття обмежень виробника чи оператора зв'язку, маніпулювання системними програмами й можливість запуску застосунків, що вимагають прав адміністратора);
- ▶ програми просять надати їм права чи доступ до ресурсів, які не властиві їх функціональному призначенню (наприклад, ви встановили програму «Ліхтарик» і помітили, що вона просить доступ до функції відправки або зчитування СМС, ваших фотографій тощо);
- ▶ ви помітили списання коштів із мобільного рахунку або/а також підписки на платні сервіси.



Висновки

Як мінімізувати ризики та що робити, якщо я став(ла) жертвою ШПЗ:

1. Використання лише ліцензійного програмного забезпечення та користування програмним забезпеченням останніх версій. Увімкніть автоматичні оновлення для операційних систем, програм. Встановлюйте та використовуйте лише те програмне забезпечення, якому довіряє ваша організація (як приклад, використання «AppLocker»).
2. Не відкривайте підозрілі додатки до імейлів; не встановлюйте підозрілі розширення для інтернет-браузерів чи інші програми із сумнівною репутацією. Вимкніть використання макросів (використовуються в багатьох офісних продуктах, наприклад, у Microsoft Office, CorelDRAW, Notepad++). Якщо ви завантажили документ з невідомого джерела або він прийшов від невідомого чи підозрілого адресата та просить активувати макрос – **не робіть цього**. Якщо це можливо, під час використання віддаленого доступу дозволити підключення лише визначеним користувачам за допомогою «білого списку» IP-адрес (IP-whitelisting). Не користуйтеся чужими чи знайденими зовнішніми носіями інформації (флешками, дисками тощо).

Фізична безпека

План лекції

Вступ

1. Загрози фізичній безпеці

2. Об'єкти загроз

Висновки

Рекомендована література

Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків : Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.

Допоміжна

5. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 72–73.
6. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 65–67.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

Текст лекції

Вступ

Фізична безпека є невід'ємною частиною захисту установи від втручання в роботу її комп'ютерних систем. Але чому? Справа в тому, що маючи фізичний доступ, порушник може безпосередньо взаємодіяти із системою та обійти існуючі механізми захисту. Тому розглянемо загрози, пов'язані з недотриманням правил фізичної безпеки, та рекомендації щодо захисту.

1. Загрози фізичній безпеці

У 2009 році заводи у місті Натанзе (Іран), які збагачували уран у рамках ядерної програми, зазнали безпрецедентної кібератаки. Було уражено близько 200 000 комп'ютерів та 1000 одиниць спеціального обладнання виведено з ладу.

Згідно зі звітом «Business Blackout» збитки становили близько 243 млрд дол. США та змусили Іран припинити свою ядерну програму.

Питання: вищезгадані об'єкти не були підключені до мережі Інтернет. Тож як злочинцям вдалось доставити шкідливий програмний код?

Відповідь: за допомогою флеш-носія, який співробітник заводу вставив у свій комп'ютер. І це – питання фізичної безпеки.

Загроза – проникнення на територію і до приміщень організації.

Зловмисники можуть спробувати потрапити на територію установи, до якої доступ мають тільки авторизовані особи. Відомі методи такого проникнення наступні.

«Вхід на плечах» (Tailgating). Зловмисник намагається приєднатись до групи авторизованих осіб, які заходять до будівлі, видаючи себе за людину, яка теж працює у цій установі (рис. 1).



Рис. 1. Неавторизований прохід «Вхід на плечах» (Tailgating)

«Зайняті руки». Зловмисник видає себе за авторизовану особу, демонструє зайняті руки (наприклад, якимось пакунком/речами/кавою) та нібито не має можливості відчинити двері або пред'явити перепустку. Він сподівається, що авторизовані особи допоможуть йому та пропустять, відкриваючи двері/турнікет своєю картою (рис. 2а, 2б).



а)



б)

Рис. 2. Неавторизований прохід «Зайняті руки»

«Доставка». Зловмисник маскується під кур'єра доставки або працівника якої-небудь служби забезпечення тощо (рис. 3).



Рис. 3. Неавторизований прохід «Доставка»

Потрібно пам'ятати

- Особа, що намагається потрапити до контрольованої території без атрибутів авторизації (перепустка/картка), є потенційним зловмисником.
- Будь-яке несвідоме сприяння порушенню правил фізичної безпеки не звільняє від відповідальності.
- Потрапляння на контрольовану територію будь-кого повинно регламентуватися визначеними процедурами.

Крадіжка комп'ютерних пристроїв, носіїв даних та ключів (карток) доступу. Зловмисник фізично здійснює крадіжку носіїв даних, які містять цінну інформацію.

Встановлення програми несанкціонованого віддаленого доступу. Отримавши фізичний доступ до комп'ютерного пристрою, зловмисник намагається встановити шкідливу програму, що забезпечує в подальшому несанкціонований віддалений мережевий доступ до системи.

Несанкціонована зміна системних налаштувань для перенаправлення мережевого трафіку на контрольований вузол («людина посередині», man-in-the-middle). Маючи фізичний доступ до комп'ютера, зловмисник змінює мережеві налаштування системи, що дозволяє в подальшому перехоплювати мережевий трафік з пристрою (рис. 4).

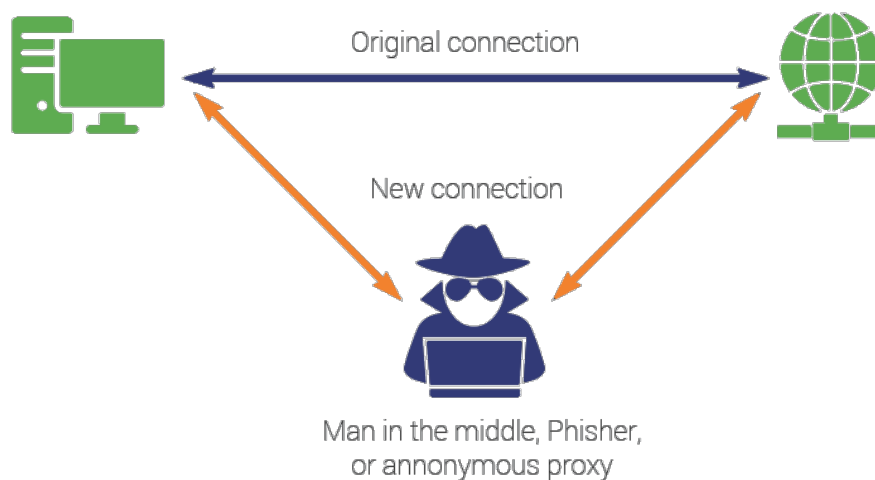


Рис. 4. Атака «людина посередині», man-in-the-middle

Підглядання (shoulder surfing). Зловмисник підглядає за користувачем, коли він вводить у систему чутливі дані: рін-коди, паролі, дані облікових записів, персональну інформацію тощо (рис. 5).



Рис. 5. Підглядання (shoulder surfing)

2. Об'єкти загроз

Об'єктами загроз при фізичному доступі зловмисника до комп'ютерних пристроїв є наступні дані.

Дані банківських карток (рис. 6).



Рис. 6. Дані банківських карток як об'єкт загроз

Паролі розблокування доступу комп'ютерних пристроїв (рис. 7).



Рис. 7. Паролі розблокування доступу комп'ютерних пристроїв як об'єкт загроз

Паролі підключення до Wi-Fi мережі (рис. 8).



Рис. 8. Паролі підключення до Wi-Fi мережі як об'єкт загроз

Флеш-накопичувачі. Флеш-накопичувачі є засобом розміщення ШПЗ, яке в подальшому вручну або автоматично активізується в системі при під'єднанні до комп'ютера.

Дослідження

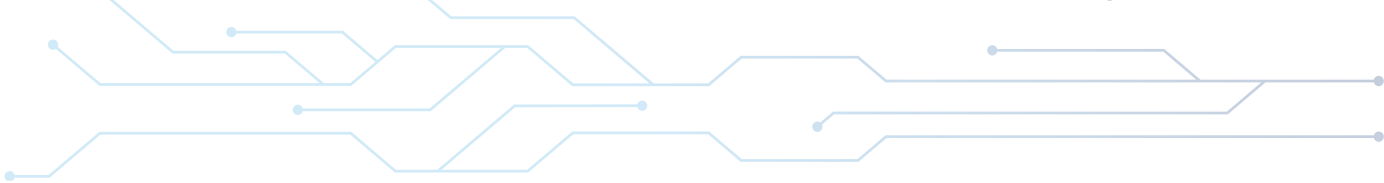
В 2015 році дослідники з компанії «Google», Університет штату Іллінойс та Університет штату Мічиган провели експеримент² щодо ефективності доставки ШПЗ в систему жертви через флеш-накопичувач. На території університетів з метою аналізу поведінки людей та визначення успішності такої атаки було розкидано 297 флешок (рис. 9). Важливо зазначити, що цільова аудиторія була технічно обізнана.



Рис. 9. Експериментальні флешки з ШПЗ (<https://zakird.com/papers/usb.pdf>)

Результат дослідження показав, що 98% людей забрали флеш-носії та 48% відкрили файли. Найкоротший проміжок часу від моменту підняття до відкриття файлу становив 6 хвилин, середній час – 6,9 годин. 68% опитаних

² Matthew Tischer, Zakir Durumeric, Sam Foster, Sunny Duan, Alec Mori, Elie Bursztein, Michael Bailey. Users Really Do Plug in USB Drives They Find / Conference: 2016 IEEE Symposium on Security and Privacy (SP). URL: DOI:10.1109/SP.2016.26.



сказали, що хотіли повернути пристрої власникам, а 18% сказали, що їм був цікавий зміст файлів. Деякі користувачі зазначили, що флеш-накопичувачі з ключами спонукали їх знайти власника. «Хтось не зможе потрапити до квартири/дому, тому я хотів повернути його якомога швидше».

Користуючись людською психологією і бажанням допомогти/суто почуттям цікавості, зловмисники можуть успішно отримати віддалений контроль над пристроєм та реалізовувати інші атаки.

Висновки

Загальні рекомендації із дотримання фізичної безпеки комп'ютерних систем.
Контроль фізичного периметра:

- ▶ перевірка особи, яка намагається потрапити до будівлі;
- ▶ заборона допомагати потрапити до будівлі без перевірки особи;
- ▶ перевірка кур'єрів і іншого технічного персоналу, які нібито отримали виклик;
- ▶ не залишати сторонніх осіб без супроводу всередині установи;
- ▶ зачиняти за собою двері.

Нагляд або блокування доступу до пристроїв:

- ▶ не залишати пристрої без нагляду;
- ▶ налаштувати автоматичне блокування пристроїв у разі тимчасової відсутності поряд із пристроєм.

Блокування доступу для ОС Windows:

- ▶ клавіші Windows+L;
- ▶ клавіші Ctrl-Alt-Del і обрати «Заблокувати»;
- ▶ через налаштування параметрів автоматичного блокування після 5 хвилин відсутності активності.

Блокування доступу для MacOS:

- ▶ клавіші Command+Control+Q;
- ▶ яблуко у верхньому лівому куті – «Заблокувати екран»;
- ▶ «Налаштування» -> «Безпека та приватність» -> «Вимагати пароль відразу».

При введенні чутливих даних (паролі від облікових записів, банківські дані, персональна інформація тощо) слід прикривати другою рукою клавіші, що натискаються.

Політика чистого столу – не залишати на столі носіїв з чутливими даними.

Не використовувати невідомі або чужі комп'ютерні пристрої або носії даних.

Убезпечення від неправдивих повідомлень

План лекції

Вступ

1. Види маніпуляцій

2. Пропаганда

3. Заходи протидії

Висновки

Рекомендована література

Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.

Допоміжна

5. Простворення Центру протидії дезінформації: Рішення Ради національної безпеки і оборони України від 11.03.2021, введено в дію Указом Президента України від 19.03.2021 № 106/2021. URL: <https://zakon.rada.gov.ua/laws/show/106/2021#Text>.
6. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

Текст лекції

Вступ

Ви, напевно, неодноразово чули фразу про те, що той, хто володіє інформацією, володіє світом. Сьогодні ця теза є актуальною як ніколи. Технології неправдивих повідомлень для впливу на маси почали активно використовувати у XX столітті (рис. 1).



Рис. 1. Видалення з фото учасника першого загону космонавтів Григорія Нелюбова

Але якщо раніше для цього залучалися професійні команди, то сьогодні, із появою різних комп'ютерних технологій та мережі Інтернет, буквально кожен більш-менш обізнаний користувач може створювати фейкові повідомлення та поширювати їх. Згадайте, наприклад, як за допомогою фоторедакторів ви або ваші знайомі редагували зроблені фотознімки. Із появою штучного інтелекту проблема лише поглибилась. Зараз за допомогою відповідних програм досить легко зробити не тільки неправдиве фото (рис. 2, 3), а й відео (рис. 4), яке буде виглядати як справжнє (github.com/iperov/DeepFaceLive, kaiber.ai) та навіть аудіо (fakeyou.com, [@clonevoicebot](https://clonevoicebot.com)). Серед іншого, почастишали випадки створення порнографічного контенту за допомогою штучного інтелекту з використанням фото певних осіб з метою їх подальшого шантажу або порнопомсти (bleepingcomputer.com/news/security/sextortionists-are-making-ai-nudes-from-your-social-media-images/). Так, наприклад, для оголення осіб на фото може бути застосований Telegram-бот [@BodyScannerBot](https://t.me/BodyScannerBot).

У згаданому контексті однією з небезпечних тенденцій є генерування контенту, який містить зображення насильства, зокрема над дітьми, з використанням

систем штучного інтелекту. Зокрема, окремі користувачі використовують для генерування подібних зображень продукт stablediffusionweb.com. Так, на теперішній час в мережі Даркнет можна знайти тисячі зображень, які містять сцени сексуального насильства над дітьми та оголених дітей, і це, насправді, є ще одним викликом для правоохоронної системи.

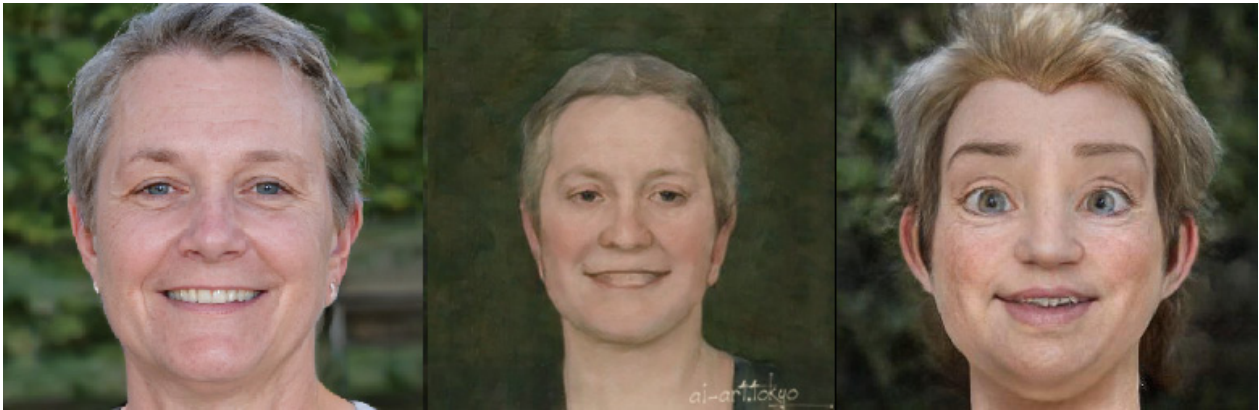


Рис. 2. Зображення, створені за допомогою штучного інтелекту, зліва направо: зображення неіснуючої людини, створене за допомогою сервісу thispersondoesnotexist.com; портрет, створений на основі першого фото за допомогою сервісу ai-art.tokyo; мультяшний персонаж на основі першого фото, створений за допомогою одного з ботів Telegram



Рис. 3. Зображення, створені за допомогою штучного інтелекту, зліва направо: зображення неіснуючої людини, створене за допомогою сервісу thispersondoesnotexist.com; зміна зачіски за ключовими словами «Trump's hair», на обличчі з першого фото за допомогою сервісу anything-ai.com

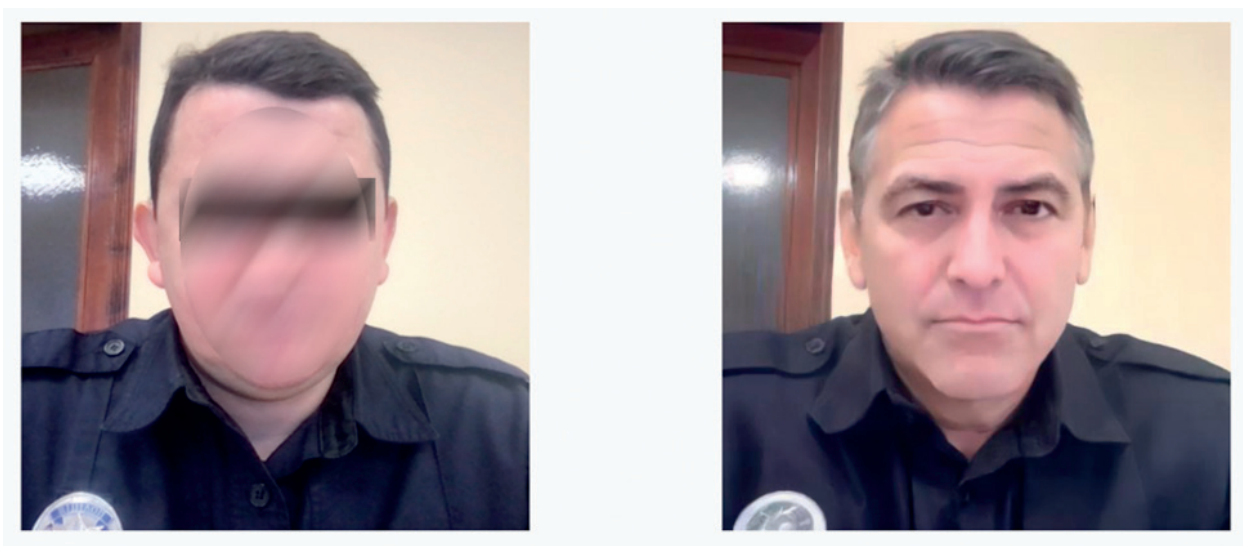


Рис. 4. Діпфейк відео, яке створюється в режимі реального часу за допомогою інструменту fal.ai/camera

Серед інших інструментів, за допомогою яких можна генерувати різноманітний контент, можна згадати Telegram @DeepPaintBot – для покращення якості фото, @qq_2d_ai_bot – для перетворення фото на аніме, @videotoanimebot – для анімації фото у різних стилях, сервіс www.deepswap.ai – для заміни обличчя тощо.

Як не заблукати в мережі, відрізнити правду від вимислу? Саме цим питанням присвячено цю тему.

1. Види маніпуляцій

Перенесення переважної кількості інформаційних потоків у мережу Інтернет, з одного боку, значно полегшило доступ користувачам до різних відомостей і знань, а з іншого – створило велику кількість можливостей для маніпуляції з боку правопорушників. Такі маніпуляції можуть бути спрямовані на окремих осіб, групи, створювати передумови для формування «потрібної» громадської думки.

Маніпуляції можуть бути *свідомими* або *несвідомими*, проте вони все одно здатні вплинути на прийняття рішень як звичайними користувачами, так і керівним складом державних органів.

Одним із найбільш поширених прикладів подібних відомостей є інформаційні сторінки, що містять інформацію з минулого, але позиціонуються як новина дня.

01 листопада 2020 року в мережі Інтернет було розміщено новину про те, що доларові депозити завдають їхнім власникам збитки, у той час як гривневі є більш прибутковими³. Проте, якщо уважно проаналізувати зміст повідомлення, стає зрозуміло, що це – новина 2013 року, і на день публікації вона може бути зовсім неактуальною.

Неправдиві ресурси часто називають фейками. Наприклад, ресурс fakeinfo.net (рис. 5) дозволяє створити фейки за різними напрямками. Так само для створення неіснуючих об'єктів може бути використано сервіс thisxdoesnotexist.com (рис. 6).

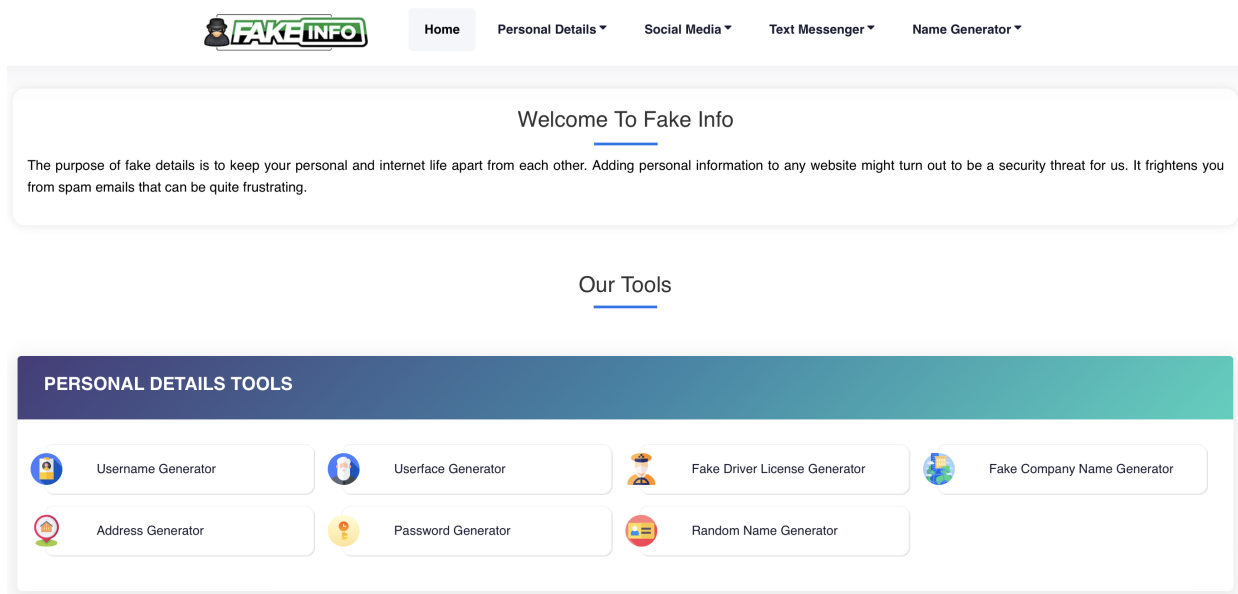


Рис. 5. Зовнішній вигляд ресурсу для генерування фейків

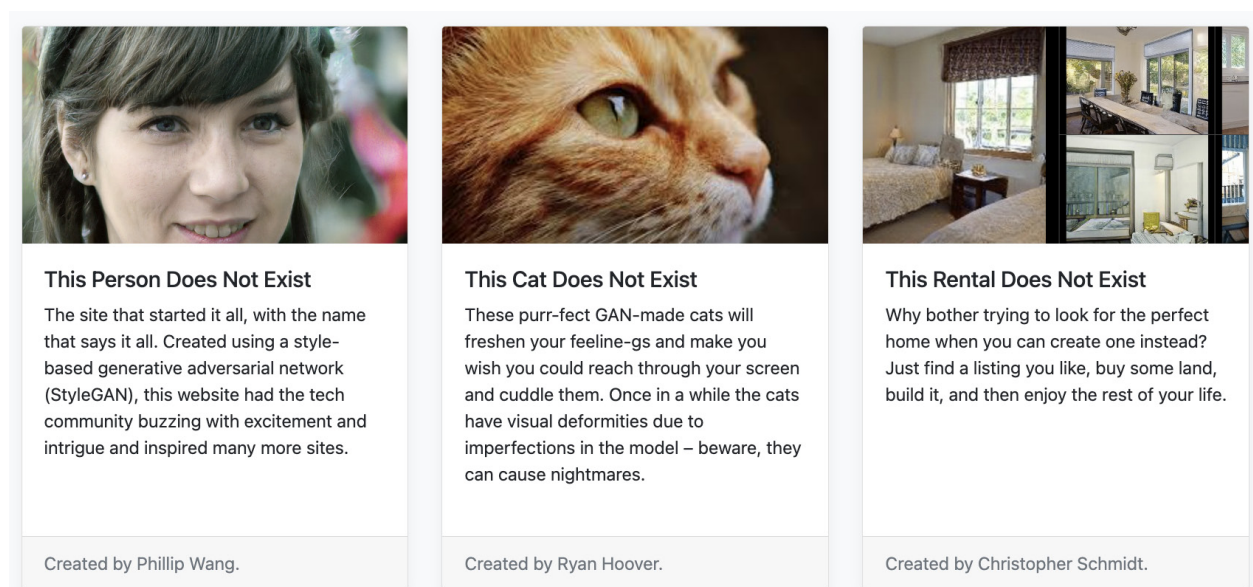


Рис. 6. Зовнішній вигляд ресурсу для генерування неіснуючих об'єктів

³ Долларовые депозиты приносят их держателям одни убытки, в то время как вклады в гривне дают более значительную доходность. URL: <https://web.archive.org/web/20201106213245/https://telegraf.com.ua/biznes/finansyi/amp-656615-depozityi-v-grivne-vyigodnee-chem-v-dollarah.html>.

Фейк може бути візуальним, для чого використовуються графічні та відеоредактори. У межах інформаційного впливу під час доведення до відома інформації використовується певний набір характеристик: видовищність, порушення звичної моделі світу, примушуюча пропаганда, «наклеювання ярликів», «тролінг» (активна участь у багатьох дискусіях під вигаданими іменами), копіпастинг. Типові ознаки троля: емоційні меседжі, чіткі тези із закликами, одноманітний профіль у мережі, незначна кількість віртуальних друзів, відсутність власних постів, створена нещодавно сторінка⁴.

У мережі Інтернет найбільш частими каналами для поширення фейків є веб-сайти новин, соціальні мережі, блоги, розсилки електронною поштою.

У жовтні 2020 року в мережі Інтернет низка ЗМІ поширила повідомлення про те, що президент Туреччини не визнає Крим російським, оскільки вважає, що півострів належить його країні. Ця інформація з'явилася на фоні просування Міністерством закордонних справ України ідеї створення «Кримської платформи», покликаної вирішити питання деокупації Криму.

У відповідних матеріалах ЗМІ посилалися на турецьке видання «Haberler», в одній з новин якого була стаття із розділом «Ердоган бажає, щоб Крим віддали Туреччині». У цьому розділі видання посилається на фрагмент статті з газети «Московський комсомолец», у якій її автор зробив припущення про позицію президента Туреччини. Таким чином, в результаті маніпуляції припущення, яке пройшло через низку «фільтрів», у підсумку було подано як факт. Згодом інформацію було спростовано⁵, але не всі звернули на це увагу.

Фейки можуть бути орієнтовані на конкретну національну аудиторію, а можуть бути й інтернаціональними.

У мережі Інтернет можна знайти фейк про те, що в німецькому виданні Fuldaer Zeitung було викладено інтерв'ю з ветераном Другої світової війни Людвігом Піллером (Ludwig Piller) з ФРН, у якому він нібито зауважив (рис. 5), що найкращими роками його сімейного життя був полон у росіян. Якщо спробувати знайти першоджерело цієї новини по ключових словах або на сайті fuldaerzeitung.de, то позитивного результату досягнути не вдасться, тому що це – спотворена інформація. Людвіг Піллер дійсно був у полоні, але не в СРСР, а у Франції (<https://www.faz.net/aktuell/gesellschaft/menschen/hochzeit-im-zweiten-weltkrieg-das-paar-heiratete-vor-80-jahren-16376299.html>), і не п'ять років, а рік

⁴ Іванцова А. Інтернет-тролі на службі в олігархів та політиків. URL: <https://www.radiosvoboda.org/a/27042051.html>.

⁵ «Надо вернуть Турции»: РосСМИ распространили фейк о позиции Эрдогана по Крыму. URL: <https://bykvu.com/ru/bukvy/treba-povernuti-turechchini-roszmi-rozpovsjudili-fejk-shhodo-pozicii-erdogana-po-krimu/>.

(<https://www.donaukurier.de/archiv/ludwig-der-flieger-2385405>).

Незважаючи на неправдивість цього повідомлення, вказана інформація з 2020 року продовжує жити своїм життям та нерідко з'являтися в німецькомовних облікових записах в соціальних мережах, наприклад (рис. 7), <https://web.archive.org/web/20230814120415/https://www.facebook.com/photo/?fbid=183523304070831>.



Рис. 7. Фейкове фото

Кілька років тому О. Юркова на підставі сучасного практичного досвіду представила низку способів створення недостовірних новин⁶. Серед них:

1. Маніпуляції з медіаданими:

- ▶ редагування;
- ▶ подання справжніх медіаданих в іншому контексті, зміна часу і місця їх створення;
- ▶ створення повністю недостовірного медіаконтенту.

2. Маніпулювання новинами:

- ▶ викривлення сенсу заголовків новин;
- ▶ подання окремої думки як факту;
- ▶ викривлення фактів;
- ▶ подання повністю недостовірної інформації як факту;
- ▶ ігнорування важливих деталей, які змінюють контекст.

⁶ Yurkova O. Six Fake News Techniques and Simple Tools to Vet Them. URL: <https://gijn.org/six-fake-news-techniques-and-simple-tools-to-vet-them/>.

3. Маніпулювання експертними оцінками:

- ▶ використання думок псевдоекспертів (несправжніх експертів, експертів в інших сферах тощо) та аналітичних центрів;
- ▶ перекручування заяв експертів або приписування видуманих заяв справжнім експертам;
- ▶ викривлення перекладу.

4. Маніпулювання повідомленнями:

- ▶ використання повідомлень маргінальних суб'єктів;
- ▶ перекручування реальних повідомлень з авторитетних джерел;
- ▶ посилення на неіснуючі повідомлення з авторитетних джерел.

5. Маніпуляції з результатами досліджень:

- ▶ використання слабкої або несправжньої методології;
- ▶ неправильна інтерпретація результатів;
- ▶ неправильні порівняння.

У цій самій праці було розкрито методи та інструменти викриття подібного виду підробок.

Однією з основних ознак інформаційної атаки є різкий дисбаланс позитивних і негативних повідомлень у доборі матеріалів, відсутність коректного обговорення різних точок зору, коли витісняється раціональна складова, а обговорення відбувається на рівні емоцій та особистих звинувачень⁷.

Емоційна складова є характерною рисою інформаційно-психологічного впливу. Коли людина лякається, в неї перестають працювати аналітичні центри. Психовіруси розраховані на те, щоб викликати в людини паніку та страх шляхом спекуляції на базових потребах. Наприклад, панічні новини про те, що все «жахливо подорожчає», вводять особу в стан паніки, вона перестає нормально аналізувати дійсність. Коли людину «зомбують», регулярно підкидаючи їй певні ідеї, вони приживаються як негласні аксіоми. Така людина буде вкрай важко сприймати будь-які нові ідеї, якщо вони входять у конфлікт з укоріненими старими⁸.

У серпні-вересні 2008 року один з українських банків зазнав прицільної інформаційної атаки⁹, у тому числі із застосуванням повідомлень у мережі Інтернет. Ця атака тривала кілька тижнів та була спрямована на те, щоб спровокувати паніку серед вкладників, які б масово почали виводити з банку свої кошти. Такі зловмисні дії досягли запланованої мети. За короткий період часу тисячі вкладників забрали з банку кілька мільярдів доларів. У результаті Національний банк України був вимушений здійснити

⁷ Пода Т.А. Інформаційна війна як стратегія формування політичної свідомості (соціально-філософський аналіз). *Вісник Національного авіаційного університету*. Сер.: Філософія. Культурологія. 2014. № 1. С. 69.

⁸ Ющенко А.Г. Україна обязана выиграть информационную войну. *Україна третє тисячоліття*. 2014. № 3. С. 22.

⁹ Жертва рейдерів. Хроніка атаки на «Промінвестбанк». URL: <https://minfin.com.ua/2008/10/17/pib/>.

рефінансування цього банку на суму 5 млрд. грн. Генеральною прокуратурою України було порушено кримінальну справу за доведення установи до банкрутства за ознаками злочину, передбаченого ч. 3 ст. 15, ст. 219 Кримінального кодексу України. Описана ситуація в подальшому сприяла посиленню фінансової кризи в усій державі.

2. Пропаганда

Одним з інструментів інформаційного впливу є пропаганда. Часто застосовуваними методами пропаганди є:

- ▶ *«гнилий оселедець»*. Використовується проти конкретної особи або групи осіб, стосовно яких висувуються неправдиві звинувачення, які мають бути якомога скандальнішими (розбещення дітей, убивство з корисливих мотивів тощо). Метою є виклик широкого обговорення несправедливості, неправдивості обвинувачення. Поступово згадування об'єкта у зв'язку зі скандалом наростає та немовби в'їдається в його одяг, залишаючи за ним шлейф «гнилого оселедця». Таким чином, під час згадування імені об'єкта він постійно асоціюється з брудним скандалом;
- ▶ *«перегорнута піраміда»* є прийомом створення текстів, коли пріоритетність інформації зменшується від початку тексту до його закінчення. Цим досягається приковування уваги до гучного початку матеріалу. Об'єкт впливу може не дочитувати матеріал до кінця, проте основний посил залишиться в його пам'яті;
- ▶ *«велика брехня»*. Полягає в тому, що аудиторії впевнено пропонується скомпонована та добре продумана велика брехня, здатна викликати емоційну травму. Це – така глобальна та страшна брехня, коли практично неможливо повірити, що можна брехати про таке (наприклад, інформація про розіп'ятого хлопчика);
- ▶ *«40 на 60»*. Полягає в донесенні інформації, в якій 60 % інформації дається на користь супротивника, а інші 40 % – на користь суб'єкта інформаційного впливу. Перша частина інформації спрямована на заслугування довіри супротивника, друга – на донесення дезінформації;
- ▶ *«абсолютна очевидність»* спрямована на створення у групи людей ефекту приєднання. Інформація, яку планується впровадити в маси, не доказується, а позиціонується як очевидний факт, що підтримується більшістю людей. Незважаючи на свою простоту, цей метод є дуже ефективним, оскільки людська психіка автоматично реагує на думку більшості, намагаючись долучитися до неї. Більшість має бути переважаючою, а її підтримка – абсолютною та безперечною, адже в іншому випадку ефект приєднання буде відсутнім.

Пропаганда може бути очевидною та неочевидною, орієнтованою на різні вікові категорії. Так, наприклад, пропаганда ксенофобії може бути спрямована навіть на дітей для того, щоб привчити їх до думки про те, що принижувати інші національності є нормою.

У російському мультфільмі «Овощи» із серії «Синій трактор» (https://www.youtube.com/watch?v=a_Zc4PFtxVg) овоч баклажан асоційовано з особою, одягненою в національний костюм мешканців Кавказу, яка має відповідний акцент (рис. 8).

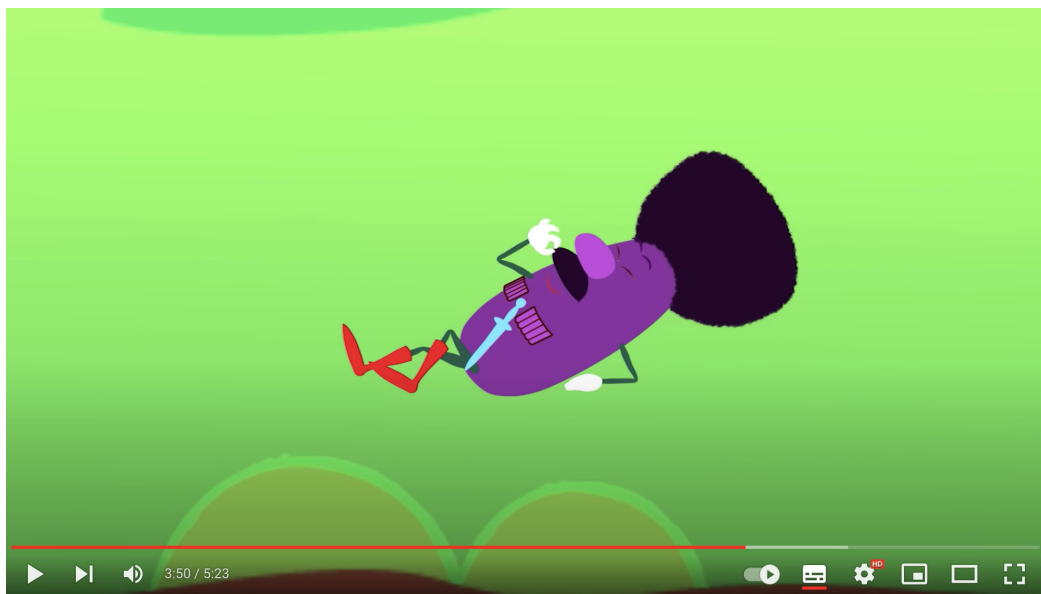


Рис. 8. Фрагмент мультфільму «Овощи»

У той же час, здійснивши пошук в мережі Інтернет за ключовими словами російською мовою «кого называють баклажаном», можна побачити, що на жаргоні відповідним терміном російськомовні можуть називати темношкірих осіб, що, до речі, продемонстровано в фільмі «Жмурки».

Інформаційні ресурси з доброю репутацією подекуди самі можуть ставати інструментом маніпуляції. Особливо це актуально для тих ресурсів, які не проводять ретельний аналіз наданих їм даних на достовірність. Так, через спеціально створений ресурс запускається недостовірна інформація, яку без перевірки публікують інші засоби масової інформації та інформаційні ресурси всередині країни. ЗМІ іншої держави, зацікавленої у проведенні інформаційної операції, викривають представлену інформацію як недостовірну, тим самим формуючи суспільну думку як у своїй державі, так і в країні, про яку йдеться у недостовірній інформації, – і саме це стає метою проведення інформаційної операції.

Як зазначив у своєму Телеграм-каналі журналіст Андрій Цаплієнко (<https://t.me/Tsaplienko/35018>), напередодні саміту НАТО у 2023 році російські пропагандисти створили відео-фейк щодо втоми США від Президента України Володимира Зеленського. Начебто, на перехресті 5-ої авеню та 57-ої вулиці Нью-Йорку вивісили плакат «Немає Зеленського, немає війни», на підтвердження чого додали відеофайл.. Насправді це відео було змонтовано з оригіналу, який можна знайти за адресою <https://m.youtube.com/watch?t=66&v=yhkbg8p2Gts&feature=youtu.be>

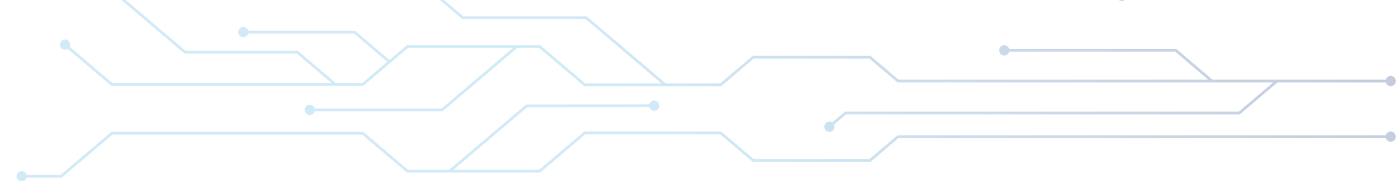
Фейковий варіант відео перепостили всі агенти російського впливу в Америці. Тож можна зробити висновок, що інформаційна спецоперація була розрахована на американців.

У іншому своєму дописі Андрій Цаплієнко викриває інший приклад пропаганди, орієнтованої на громадян США з метою зменшити підтримку України (<https://t.me/Tsaplienko/38326>).

Так, на опублікованому Fox News (<https://www.foxnews.com/politics/cartoons-slideshow#bf7f54c7-7bf7-5bb1-aa2a-ed0f82aff5b>) малюнку (рис. 9) зображено посил, який можна інтерпретувати таким чином, що ледачий, брудний хіппі незрозумілої орієнтації, який підтримує Україну, «хейтить» звичайного роботящого хлопця із зоряно-смугастим прапором на футболці: «Цей прапор мене ображає». Тобто, якщо вимагаєш підтримувати Україну, значить, ти брудний ледачий нероба із заплутаною орієнтацією. Є й більш маніпулятивна деталь. На синьо-жовтому прапорці написано «Підтримуй війну в Україні». Нібито це сама Україна її розпочала. І асоціальний тип, який сидить на плечах у добропорядного платника податків, насправді виступає за продовження війни, а не за її припинення.



Рис. 9. Малюнок з ознаками пропаганди



Розквіт пропаганди в країні нерідко межує з «епідемією» такого явища, як «стукацтво». У гіпертрофованому вигляді це можна було спостерігати за часів СРСР періоду правління Йосипа Сталіна. Сьогодні те саме починає простежуватися на російській території. Так, одним з ентузіастів у січні 2023 року було розроблено жартівливий застосунок «Мой Донос». До травня 2023 року через застосунок надійшло вже більше 5 тис. доносів, 20% з яких містили докладний опис «правопорушень» та особисті дані правопорушників¹⁰.

Під час війни пропаганда набуває особливого розквіту. Бельгійська дослідниця Анна Морелі узагальнила напрацювання Понсоби та вивела 10 основних принципів воєнної пропаганди:

1. «Ми не хочемо війни».
2. «У цій війні винні лише наші противники».
3. «Наш ворог – це втілення зла та самого диявола».
4. «Ми б'ємося за благородну мету, а не за власні інтереси».
5. «Ворог навмисно проявляє жорстокість, інциденти з нашого боку вимушені або випадкові».
6. «Ворог використовує заборонену зброю».
7. «У нас незначні втрати, в той час як втрати ворога – величезні».
8. «Визнані артисти та інтелектуали нас підтримують».
9. «Наша мета – священна».
10. «Кожен, хто ставить нашу пропаганду під сумнів, – зрадник».

У 2022 році А. Романюк у статті «10 принципів воєнної російської пропаганди на прикладі Херсона» (censor.net/ua/b3346432) достатньо докладно описала на прикладі українського міста, як працюють ці 10 принципів.

3. Заходи протидії

Існує низка способів протидії неправдивим повідомленням. Умовно їх можна розділити на логічні, технічні та комбіновані. Найбільш простими та дієвими логічними способами є такі:

- ▶ критичне осмислення будь-якої інформації;
- ▶ під час сприйняття інформації потрібно намагатися більше керуватися розумом, аніж емоціями;
- ▶ звертати увагу на репутацію інформаційних ресурсів;
- ▶ перевіряти інформацію з кількох джерел;
- ▶ намагатися переглядати першоджерело відповідного інформаційного повідомлення.

Для логічного опрацювання мультимедійних даних може стати в нагоді ресурс, який акумулює інформацію про різноманітні предмети та особливості країн, – geohints.com.

¹⁰ Андрусак А. «Такий молодий, а вже проти Путіна»: росіяни написали понад 5000 доносів на жартівливому сервісі. URL: <https://focus.ua/uk/world/584979-takij-molodij-vzhe-proti-putina-rosiyani-napisali-ponad-5000-donosiv-na-zhartivlivomu-servisi>.

Як приклад технічних інструментів викриття неправдивих фотоповідомлень можна навести плагіни «Who stole my pictures» (рис. 10) та «Fake news debunker by InVID & WeVerify», що їх легко знайти в мережі Інтернет та встановити у відповідному браузері.

Яркая иллюстрация, как в Украине защищают от коронавируса врачей и чиновников



Размещено: 16.04.2020



Наибольшее количество зарегистрированных случаев COVID-19 среди медиков в Черновицкой области - 126 медицинских работников. Сегодняшние данные Минздрава.

Что с обеспечением средствами индивидуальной защиты в Черновицкой области? Официальные данные Кабмина показывают обеспеченность на уровне 62,33%, то есть чуть больше половины от потребности.

Что сказать властям, которые переживают за больницы, могли закупить маски? Пожелания можно подкреплять стабильным обеспечением.

Защиты. Слева - врачи, справа - чиновники,

чиновников Украины.

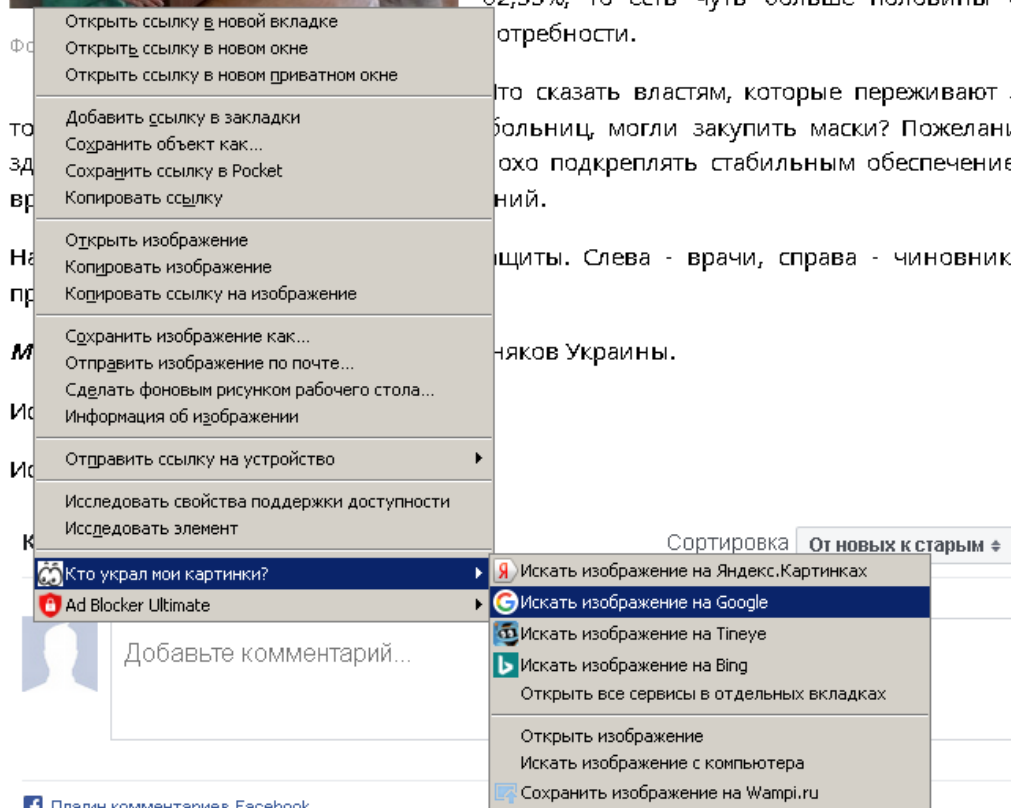


Рис. 10. Використання інструменту

Коментуючи новину на рис. 10, потрібно відзначити, що вона була спрямована на маніпулювання громадською думкою (<http://archive.is/tUogM>). У ній коментується фотографія, яка нібито зроблена в українській лікарні, у той час як насправді зображення запозичено із новини про відвідування лікарні губернатором Псковської області в Російській Федерації.

Для пошуку зображень в мережі Інтернет також згодиться і простий реверс-пошук за зображенням у пошуковій системі (рис. 11).

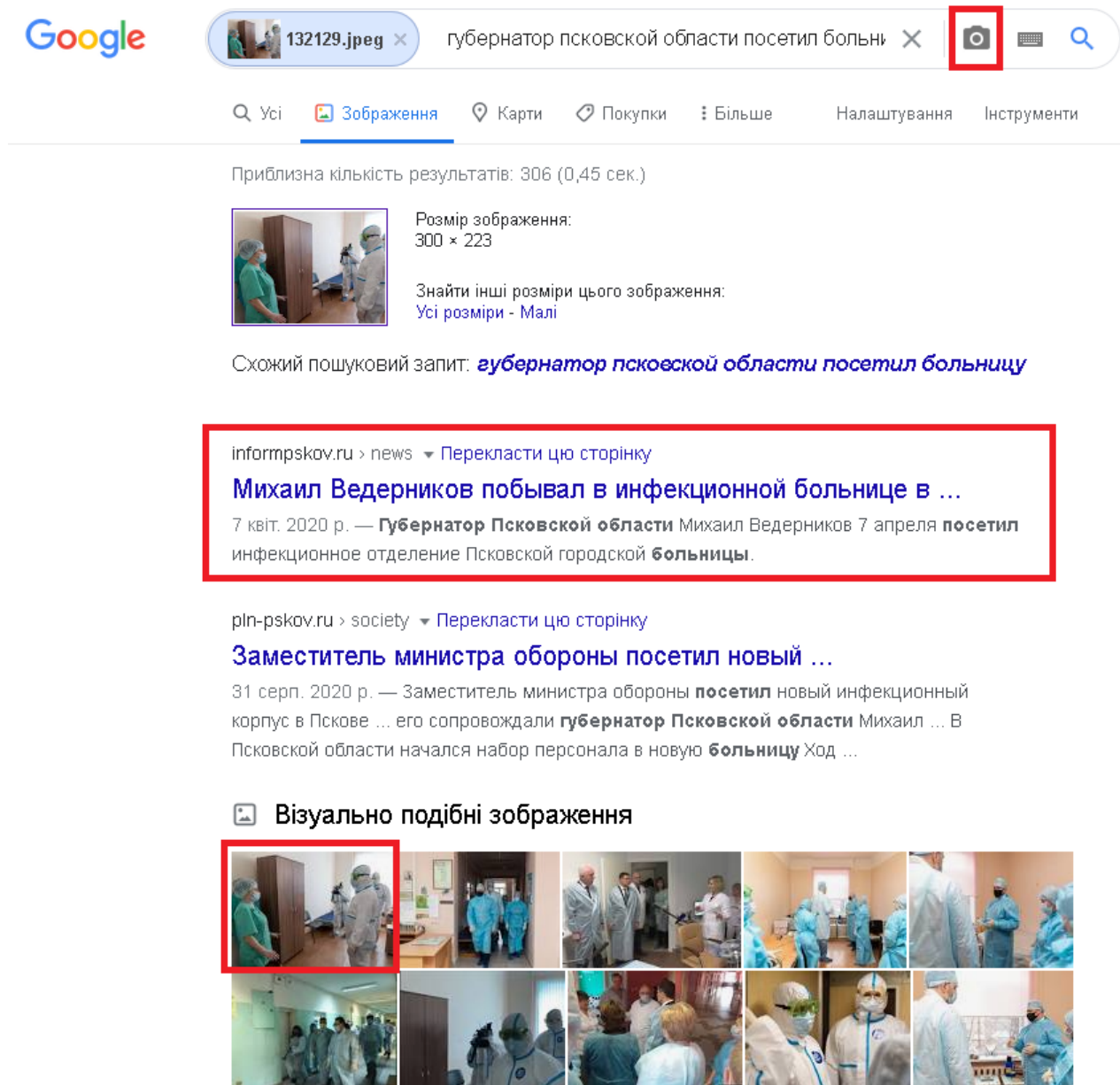


Рис. 11. Використання зворотного пошуку за зображенням у пошуковій системі Google здійснюється шляхом натискання на зображення фотокамери на сторінці пошукової системи пошуку зображень «Who stole my pictures»

Крім наведених інструментів, для виявлення редагування зображень та аналізу додаткових даних можна використовувати такі сервіси, як www.imageforensic.org, 29a.ch/photo-forensics та fotoforensics.com. Наприклад, вид аналізу Error Level Analysis, або ELA дозволяє виявити накладені зображення, оскільки вони різняться за рівнем шуму – яскравістю точок (рис. 12).

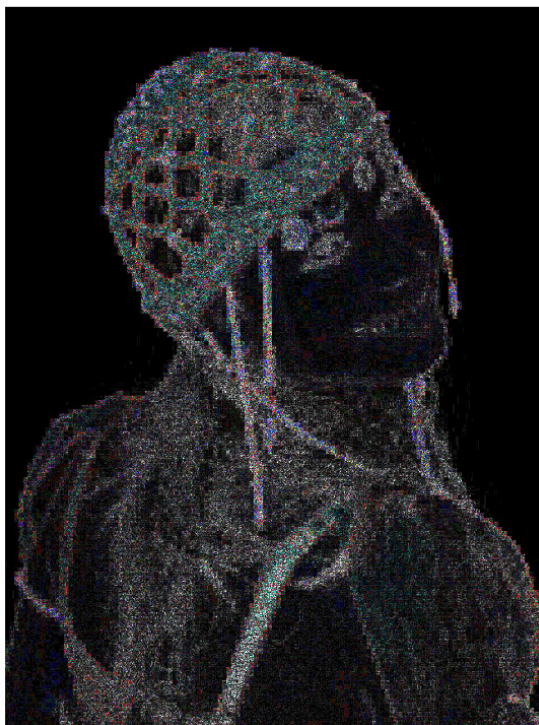


Рис. 12. На рисунку видно, що рівень шуму для білого фону різко відрізняється від загального, і це свідчить про те, що білий фон було створено окремо від основного фото (fotoforensics.com/tutorial-ela.php)

Для аналізу відеофайлів, розміщених на сервісі YouTube, може бути використаний сервіс citizenevidence.amnestyusa.org (рис. 13).



Youtube DataViewer

Теперь то уж точно! Украина СПАСЕНА!!!

Оригинал видеозаписи по адресу <http://www.youtube.com/watch?v=dvZD-2ww1ww> от 19.07.2014г. Читай подробнее досье на Порошенко и других украинских политиков на сайте <http://whoswho.com.ua/>

Video ID: sTzK4MgKfoU
Upload Date (YYYY/MM/DD): 2014-09-01
Upload Time (UTC): 12:03:18 ([convert to local time](#))

Thumbnails:



[reverse image search](#)

Рис. 13 <https://ebird.org/>. Аналіз фейкового відео, в якому опис не відповідає відеоряду

Як додаткові інструменти для аналізу метаданих відео у YouTube можна також запропонувати сервіси:

- ▶ youtube-lookup.vercel.app;
- ▶ mattw.io/youtube-metadata.

У листопаді 2020 року блогер А. Шарій випустив відеоролік, у якому продемонстрував фотографію Президента України з лікарями та вказав, що під час хвороби Президент, нехтуючи масковим режимом, фотографується з лікарями без маски (рис. 14).



Рис. 14. Фрагмент відеоблога А. Шарія

подальшого зворотного пошуку в пошуковій системі легко встановити, що знімок було зроблено у 2016 році в Ізраїлі, про що йдеться, наприклад, у знайденій новині (рис. 15) за адресою <http://www.bagnet.org/news/pressreliz/353826/pervyy-meditsinskiy-tsentr-tel-aviva-gorod-zdorovya-v-gorode-mechty>.

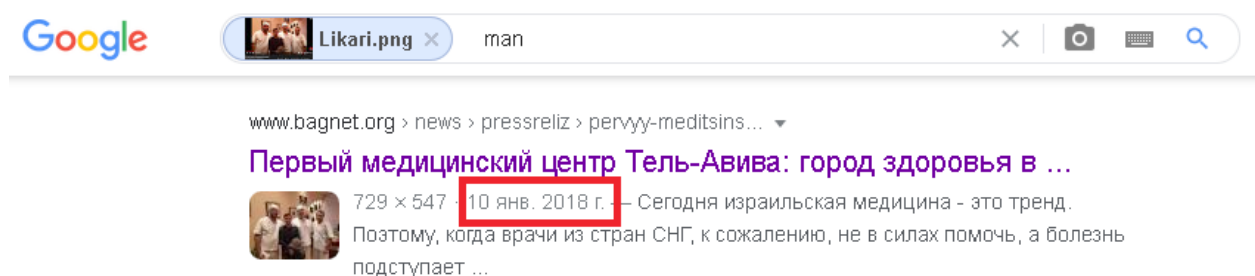


Рис. 15. Результати зворотного пошуку

Наразі після публічного викриття А. Шарій перемонтував своє відео та видалив частину з описаним фото. Натомість видалений фрагмент можна переглянути за посиланням: https://censor.net/ru/photo_news/3230988/propagandist_shariyi_vydal_feyik_o_tom_cho_bolnoyi_koronavirusom_zelenskiyi_fotografiruetsya_s_vrachami¹¹.

Нерідко для того, щоб зрозуміти політику наповнення того або іншого інформаційного ресурсу, потрібно проаналізувати сайт, через який доноситься інформація. З цією метою вельми корисним вбачається застосовувати ресурс github.com/jonkeegan/behind-this-website, який містить чекліст для визначення особи, яка стоїть за тим або іншим сайтом. Технічні особливості виявлення сайтів з дезінформацією можна знайти за адресами:

- ▶ A Look at Misinformation & Disinformation and How to Fight It: Part 1 (maltego.com/blog/infographic-misinformation-and-disinformation/);
- ▶ Investigating Misinformation & Disinformation: Part 2 (maltego.com/blog/investigating-misinformation-and-disinformation-campaigns/).

Коли йдеться про комбіновані способи виявлення фейків, тут поєднуються обидва раніше наведених підходи. І це, насправді, найбільш ефективний інструмент протидії інформаційним загрозам.

27 березня 2014 року в мережі Інтернет за адресою: <https://www.youtube.com/watch?v=LTBpSGnD09I> було розміщено аудіозапис із назвою «Телефонный разговор бойцов СОКОЛА. Следующая цель СБУ – ЯРОШ (18+) без цензури», в якому нібито два працівники спецпідрозділу міліції України обговорюють наказ свого керівництва про злочинну ліквідацію під час затримання одного відомого громадського і політичного діяча. Аналіз мови діалогу дозволяє зазначити, що один із співрозмовників має характерний російський говір, в який він зрідка вставляє українські слова, хоча для так званого українського суржику навпаки є притаманною вставка російських слів в українську мову. Аналіз сигналу запису в звуковому редакторі дозволив виявити факт того, що аудіосигнал нібито перехоплення телефонної розмови складається із двох незалежних сигналів для кожного співрозмовника. Тобто запис учасників діалогу здійснювався із двох відокремлених незалежних мікрофонів, а потім два моносигнали було об'єднано у стереосигнал діалогу, що суперечить факту запису мовного сигналу із монофонічного телефонного каналу зв'язку. На рис. 16 показано перші 3 секунди аудіозапису, де звучить дійсна стереофонічна музична заставка, й в кожному каналі існують корельовані сигнали, а на рис. 17 показаний наступний фрагмент некорельованих моносигналів, що об'єднанні у стереосигнал нібито перехоплення із монофонічного телефонного каналу зв'язку.

¹¹ Пропагандист Шарій выдал фейк о том, что больной коронавирусом Зеленский фотографируется с врачами, прикрепив фото 4-летней давности. ВИДЕО+ФОТО. URL: https://censor.net/ru/photo_news/3230988/propagandist_shariyi_vydal_feyik_o_tom_cho_bolnoyi_koronavirusom_zelenskiyi_fotografiruetsya_s_vrachami.

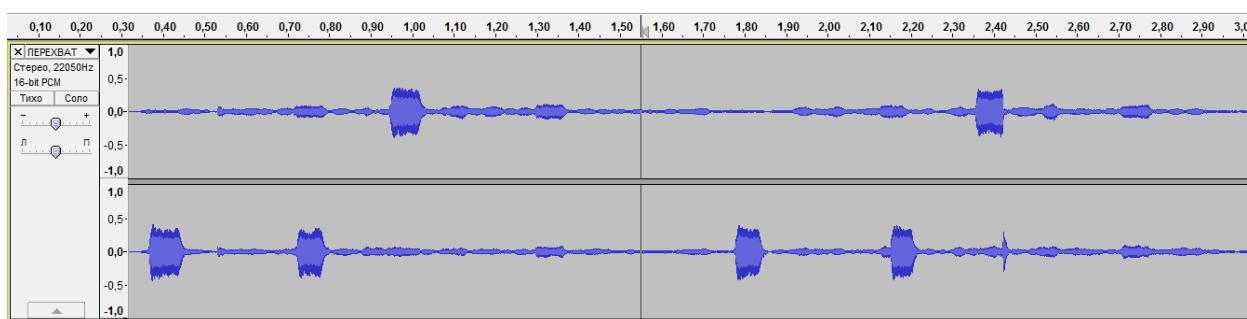


Рис. 16. Перші 3 секунди аудіозапису, де звучить дійсна стереофонічна музична заставка, і в кожному каналі існують корельовані сигнали

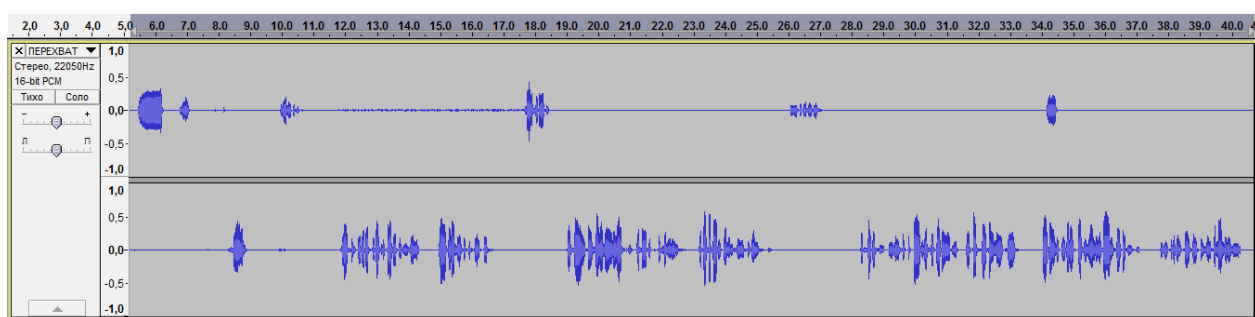


Рис. 17. Фрагмент аудіозапису некорельованих моносигналів, що об'єднані у стереосигнал нібито перехоплення із монофонічного телефонного каналу зв'язку¹²

Велику кількість інструментів розпізнавання фейків наведено на сайтах stopfake.org, snopes.com, factcheck.org, truthorfiction.com.

Для перевірки новинного контенту на предмет його висвітлення засобами масової інформації різної спрямованості досить корисним буде ресурс ground.news. За його допомогою можна оцінити подачу різного новинного матеріалу з точки зору лівих, центристських та правих засобів масової інформації (рис. 18).

У цього проекту також є розширення та функція Blindspot, яка допомагає вивчити новини, що не потрапили у тренди.

¹² Носов В.В., Манжай О.В. Окремі аспекти протидії інформаційній війні в Україні. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2015. № 1(29). С. 26–29.

Russia attacked civilian building in Zaporizhzhia -officials

Left

Center

Right



- A Russian missile struck a hotel in Zaporizhzhia, [Ukraine](#), killing one person and injuring 16 others. The Iskander missile hit the city at 7:20 p.m.
- The damaged hotel, Reikartz Hotel, was frequently used by United Nations personnel and NGOs, according to Denise Brown, the humanitarian coordinator for Ukraine.
- The Zaporizhzhia nuclear plant, which is controlled by the Russian military, lost connection to its main external power line and switched to a reserve line. The reserve line has less power capacity and poses a risk to the plant's equipment.

Insights by Ground AI ⓘ

GROUND
News

Published 3 days ago · [Ukraine](#)



News Articles

All

Left

Center

Right

More Filters



TVA Nouvelles

Lean Left

Mixed Factuality



A child killed by a Russian strike in western Ukraine

An eight-year-old child was killed by a Russian missile in the Ivano-Frankivsk region on Friday.

3 days ago

[Read Full Article](#)

Рис. 18. Результат роботи сервісу ground.news

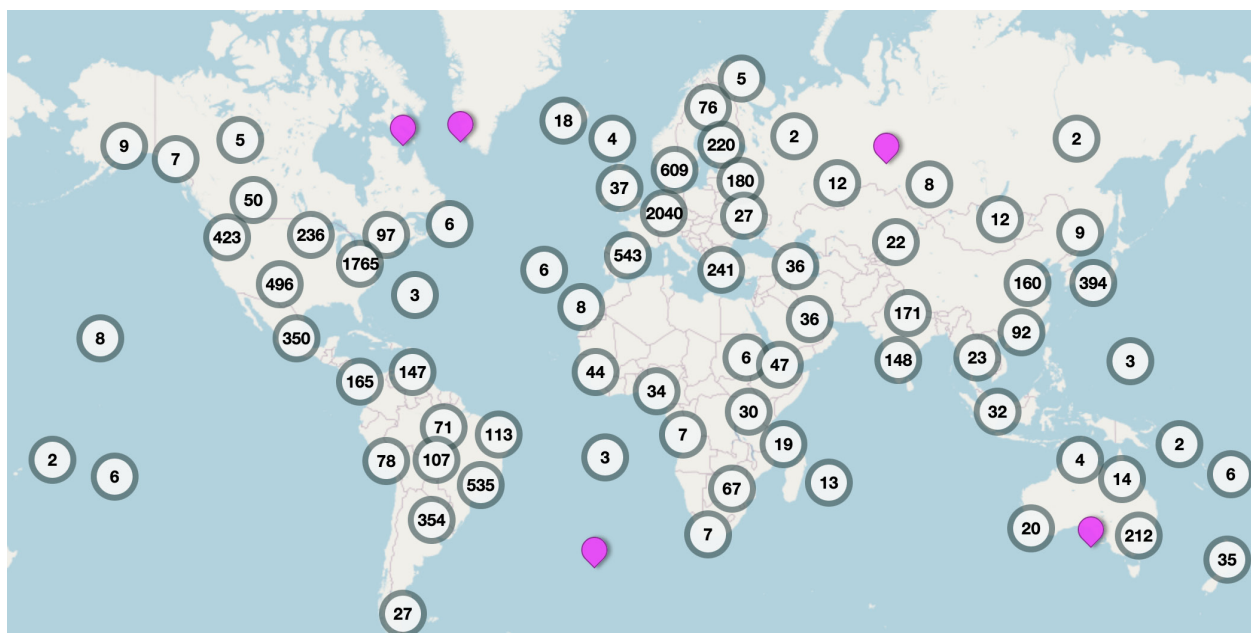


Рис. 19. Ресурс Newspaper Map ([newspapermap.com](#))

Також Google має у своєму арсеналі інструментарій Fact Check Tools (toolbox.google.com/factcheck), за допомогою якого можна перевіряти окремі відомості на достовірність (рис. 20).

Україна

More results in other languages

Language filter

Ukrainian

Claim by notes_veterans:

"Просто YouTube Music опублікував ТОП виконавців для прослуховування в Україні. Жодного виконавця українською"

Голос Америки rating: Неправда

Націоналістичні канали в Росії підтасовують дані YouTube, щоб стверджувати, що українці буцімто не слухають українських музикантів

6 days ago

Музикант

YouTube

Україна

Голос Америки

Fact Check Explorer

Україна

Language filter

Ukrainian

Claim by Пост у Фейсбучі:

На фото – український паспорт Олени Зеленської

Demagog rating: Фейк

Ізраїльський паспорт Олени Зеленської? Це фальшивка

Jun 27, 2023

Олена Зеленська

Паспорт

Україна

Demagog

Рис. 19. Fact Check Tools

Також Google має у своєму арсеналі інструментарій Fact Check Tools (toolbox.google.com/factcheck), за допомогою якого можна перевіряти окремі відомості на достовірність (рис. 20).

Висновки

Найбільш складним і часовитратним, проте достатньо ефективним методом протидії неправдивим повідомленням, на нашу думку, є підвищення аналітичних здібностей суспільства, навчання методам критичного аналізу повідомлень, убезпечення від інформаційних диверсій. Усе наведене дає підстави говорити про необхідність активізації в нашій країні зусиль з розбудови ефективної структури інформаційного протиборства.

Тема 2. Базові правила забезпечення роботи в комп'ютерній мережі

Соціальна інженерія

План лекції

Вступ

1. Зміст явища «соціальна інженерія»
2. Популярні вектори атак
3. Методи протидії

Висновки

Рекомендована література

Основна

1. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 106 с.
2. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 262 с.
3. Oles N. How to Catch a Phish: A Practical Guide to Detecting Phishing Emails. Apress Berkeley, CA, 2023. 147 p. DOI: <https://doi.org/10.1007/978-1-4842-9361-4>.

Допоміжна

5. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 65–67.
6. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 72–73.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.
8. Ви вмієте розпізнавати фішинг? URL: <https://phishingquiz.withgoogle.com/?hl=uk>.

Текст лекції

Вступ

Соціальна інженерія як явище зародилося ще на початку історії людства і було часто пов'язано з потребою вивчення людської поведінки для прийняття побутових, військових, політичних та інших рішень, вчинення правопорушень. У 1894 році термін «соціальна інженерія» було введено в обіг нідерландським підприємцем Якобом Корнелісом (Жаком) ван Маркенімом. З появою засобів комп'ютерної техніки та розвитком мережі Інтернет про комп'ютерну соціальну інженерію дізналися люди з усього світу, а її інструментарій став активно застосовуватися правопорушниками у межах різного виду протиправної поведінки у кіберсфері.

1. Зміст явища «соціальна інженерія»

Соціальну інженерію у широкому розумінні можна розглядати як науку, яка вивчає поведінку людей та фактори, що на неї впливають. У більш вузькому контексті соціальна інженерія – це інструмент психологічного маніпулювання, спрямований на досягнення бажаної поведінки суб'єкта або групи суб'єктів за певних умов.

Соціальна інженерія як інструмент застосовується у більшості видах кібератак та нерідко спрямована на заволодіння персональними даними.

Безпосередньо здійснюючи відповідні кібератаки, зловмисники можуть використовувати соціальну інженерію (рис. 1):

- ▶ взагалі не вступаючи в контакт з людьми (підбирання паролів, в якому міститься день народження жертви, номер мобільного телефону тощо, взаємодія із системами відновлення паролів у частині відповіді на секретне питання на кшталт «дівоче прізвище матері»);
- ▶ не вступаючи в контакт з цільовою особою (комунікація зі службами підтримки провайдерів цільової особи, її друзями, знайомими, родичами);
- ▶ під час комунікації з цільовою особою (назватися службою підтримки банку, начальником керівного підрозділу, поліцейським тощо).



Рис. 1. Напрями застосування інструментарію соціальної інженерії

Розглянемо популярні техніки соціальної інженерії.

Фішинг (англ. phishing, від fishing – риболовля) – вид маніпуляції, який передбачає створення підроблених об'єктів у кіберсфері, які викликають довіру в цільовій групі користувачів та спрямовані на отримання від таких користувачів чутливої інформації або вчинення певних дій, вигідних атакуючому. Цілями зловмисників можуть бути автентифікаційні дані облікових записів, отримання коштів від жертви тощо.

Телефонний вид фішингу називають **вішингом** (англ. vishing – voice fishing). Він передбачає використання голосового контакту телефоном атакуючого з жертвою з метою вплинути на поведінку цільової особи. Популярними схемами вішингу є повідомлення жертви про те, що її дитина потрапила в аварію, спричинила жертви і тепер терміново потрібні кошти, або це може бути банківське шахрайство тощо. У будь-якому разі сценарій вішингу продумується заздалегідь та передбачає вибір певного часу телефонного дзвінка, окремі підходи до спілкування з різними віковими групами тощо.

Жителька м. Чернігова заявила у кіберполіцію, що стала жертвою шахрайства. Так, зловмисники зателефонували їй та представившись оператором зв'язку, повідомили, що у зв'язку зі складнощами у роботі мережі можливі збої, а тому є можливість тимчасово безкоштовно перейти у режим роумінгу, аби залишатись на зв'язку.

Погодившись, жінка повідомила коди підтвердження з СМС, які насправді були від її систем авторизації. З банківської картки жінки вивели 48 тис. грн., а з її месенджерів почали надсилати інформацію контактам з проханням позичити кошти. Таким чином, злочинці додатково отримали ще 3 тис. грн.

Одним з ключових елементів фішингу є фейк – неправдива інформація словесного, мультимедійного та іншого характеру. Фейки можуть бути як простими, так і досить складними, які вкрай важко відрізнити від оригінальної інформації.

Серед засобів, за допомогою яких найчастіше здійснюють фішингові атаки, слід виділити такі:

- ▶ електронна пошта, в тому числі спам-розсилка;
- ▶ фейкові веб-сайти;
- ▶ рекламні повідомлення та їх різновид у вигляді спливаючих вікон;
- ▶ контрафактні програми або дані іншого виду;
- ▶ месенджери тощо.

Як правило, фішингові атаки передбачають використання кількох з наведених засобів. Так, якщо згадати класичну кваліфіковану схему фішингу, то цільовій особі спочатку може надходити електронний лист з підробленим заголовком, де вказується довірена електронна пошта відправника листа, а

в самому тілі листа дається закамфльоване посилання на фейковий ресурс банку, державної установи, певного підприємства, установи, організації, з якою взаємодіє або потенційно може взаємодіяти жертва атаки. Все може бути і набагато простішим (рис. 2).

ВАЖЛИВІ НОВИНИ

Umma Yusha'u <ummayushau1986@gmail.com>

20 лютого 2022, 20:47 ☆

Кому: undisclosed-recipients;

Привіт друже,
Як твої справи сьогодні? Я Лотаріо Манфредо Алексіс, співробітник UBI Banca, Італія. Я зв'язуюсь з вами щодо померлого клієнта, який загинув у автокатастрофі під час свого шляху до Мілана, Італія, у 2004 році, він був моїм відомим клієнтом.
Перед смертю мій клієнт вніс (420 346,00 євро) в скриньку моєї фінансової установи тут, у Римі, Італія, документація щодо цієї трансакції вказує на те, що претензії можуть пред'являти лише його найближчі родичі. На жаль, на момент смерті у нього не було заповіту.
Усі зроблені зусилля не виявили жодного зв'язку з кимось із членів його родини. Однак нове італійське право про спадкування/претензії/фонд вказує термін, протягом якого такі позови можуть бути допустимими. Фінансова установа доручила мені представити найближчих родичів, які вимагатимуть кошти, і якщо не відповісти на цей ультиматум, фінансова установа юридично дозволить звітувати про ці кошти до Banca d'Italia (Центральний банк Італії) як про незатребувані кошти.
Я і мій колега встановили всі необхідні вимоги щодо вивільнення цих коштів, і я маю намір представити цю можливість вам, як бенефіціару. Зверніть увагу, що юридично я маю всю необхідну інформацію/документацію щодо цього фонду. Будь ласка, зв'яжіться зі своєю думкою, надіславши відповідь на мою особисту електронну адресу:
manfredo.alexis14@gmail.com

З повагою
Манфредо Алексіс
ОФІЦЕР БАНКІВСЬКОГО РАХУНКУ

Рис. 2. Приклад шахрайського повідомлення

Якщо атака не цільова, то часто відповідні листи шахрайського змісту розсилаються масово і нерідко потрапляють до спаму (рис. 3).



Рис. 3. Посилання на приклад листів з маніпулятивним змістом
(<https://docs.google.com/document/d/11oTX14GzEcaZMgyKIKejVQKn6BjWCPzQVjh5p3vEfG0/edit>)

У листі може міститися пропозиція з переходом на сайт зломисників, який, як правило, є фейком справжнього відомого ресурсу (рис. 4, 5).



Рис. 4. Фейкова сторінка сайту i.ua
(i-ua.website станом на 06.07.2023)

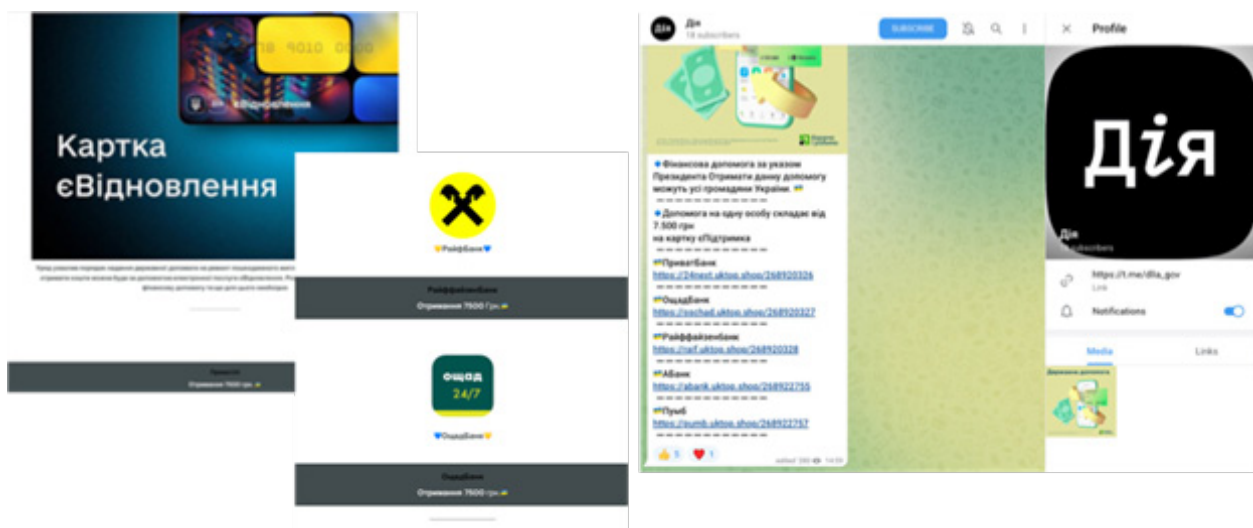


Рис. 5. Зміст фейкового сайту надання допомоги
(viplataua.art.blog станом на 24.07.2023)

У більш витончених атаках фішингу можуть використовуватися вразливості в роботі великих компаній та застосовуватися комерційна реклама. Так, у липні 2023 року компанія MalwareBytes виявила фішингову атаку, націлену на американських громадян, під маркою великої поштової компанії USPS (<https://www.malwarebytes.com/blog/threat-intelligence/2023/07/malicious-ad-for-usps-phishes-for-jpmorgan-chase-credentials>).

Зловмисники замовили в Google рекламу фейкового сайту поштової служби від імені громадянки України Анастасії Іващенко. В результаті користувачі після введення в пошуку USPS tracking бачили у пошуковій видачі на перших позиціях рекламне посилання на фейковий сайт зловмисників (рис. 6).

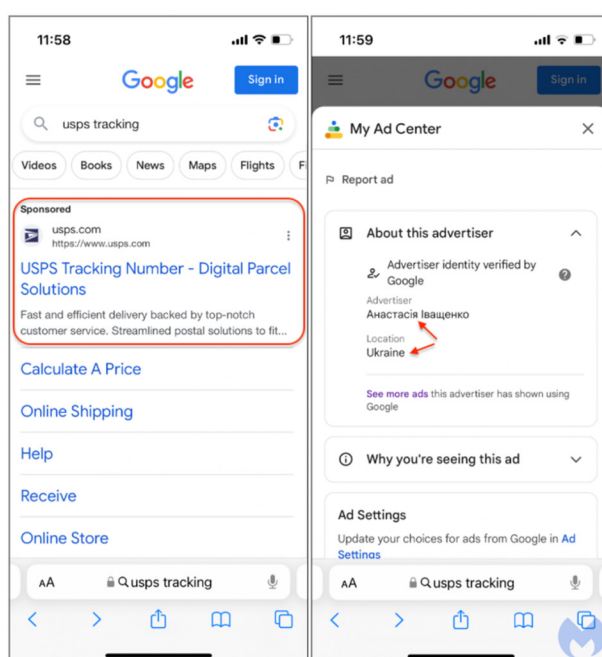


Рис. 6. Результати пошукової видачі

Зверніть увагу, що зломисники вказали українського замовника реклами, проте вже після викриття атаки, якщо перейти за посиланням фейкового сайту <https://super-trackings.com/>, можна побачити відомості, які опосередковано вказують на російський слід атакуючих (рис. 7).

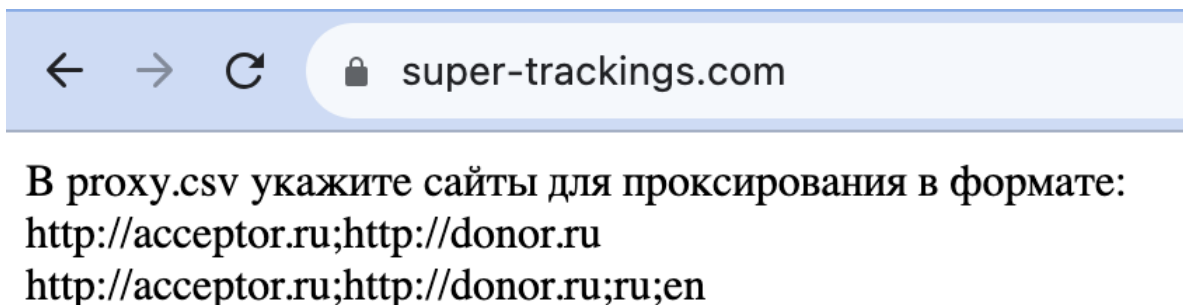


Рис. 7. Результати переходу на сайт зломисників
(станом на 27.07.2023)

Схожа атака через рекламу Google була здійснена зломисниками у 2015 році стосовно веб-банкінгу Ощад 24/7, у серпні 2023 року стосовно компанії Amazon (<https://www.bleepingcomputer.com/news/security/sneaky-amazon-google-ad-leads-to-microsoft-support-scam/>).

Ще одним інструментом здійснення фішингу є неліцензійне (контрафактне) програмне забезпечення. Користувачі, намагаючись «зекономити», нерідко стають жертвами зломисників, що в свою чергу може потягнути тяжкі наслідки. Наприклад, восени 2022 року з російського боку була ініційована багаторівнева атака через **проміжну ланку** (supply chain), спрямована проти урядових установ України (<https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government>). Так, на кількох російськомовних та україномовних торрент-трекерах зломисники поширили троянізований образ неліцензійної збірки Windows 10 (рис. 8).

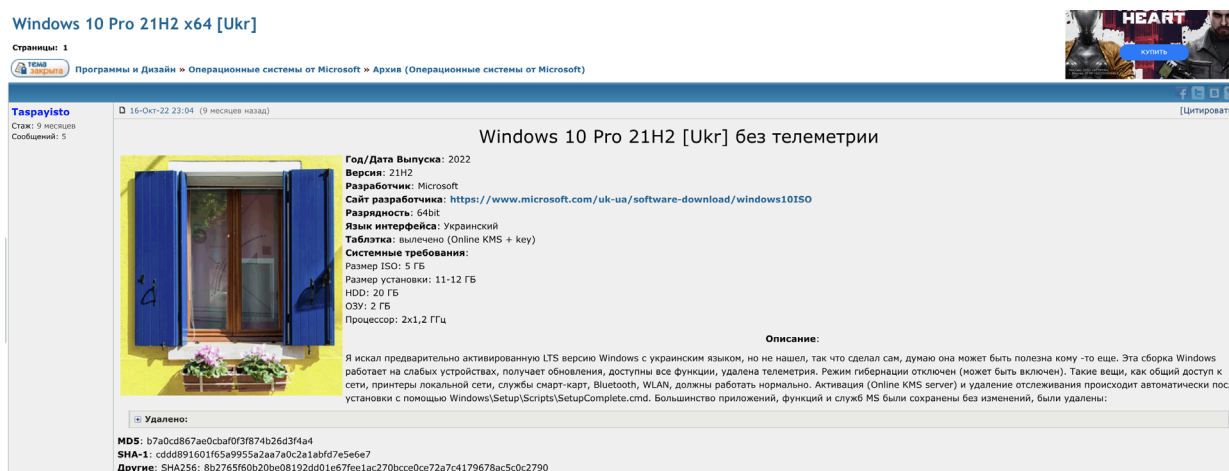


Рис. 8. Результати переходу на сторінку з описом небезпечного образу ОС Windows на одному з торрент-трекерів
(станом на 28.07.2023)

У наведеному образі були передбачені завдання, призначені для отримання команд через PowerShell. Це давало змогу збирати дані з відповідних комп'ютерів, встановлювати шкідливе програмне забезпечення та передавати вкрадені дані на контрольовані зловмисниками сервери. Після попередньої розвідки в систему встановлювалися бекдори, через які зловмисники управляли системою. У процесі атаки зловмисники проводили аналіз заражених пристроїв та атакували ті з них, які належали працівникам урядових структур.

Крім вже наведених інструментів здійснення фішингових атак, слід також згадати розсилання небезпечних повідомлень з використанням месенджерів. Як правило, сценарій таких атак та використання програмного забезпечення розробляється під конкретний вид месенджера. Так, восени 2022 року відбулася хвиля атак на громадян України через месенджери WhatsApp та Telegram.

У першому випадку йшла масова розсилка повідомлень від імені компанії Amazon з пропозицією працевлаштування (рис. 9).

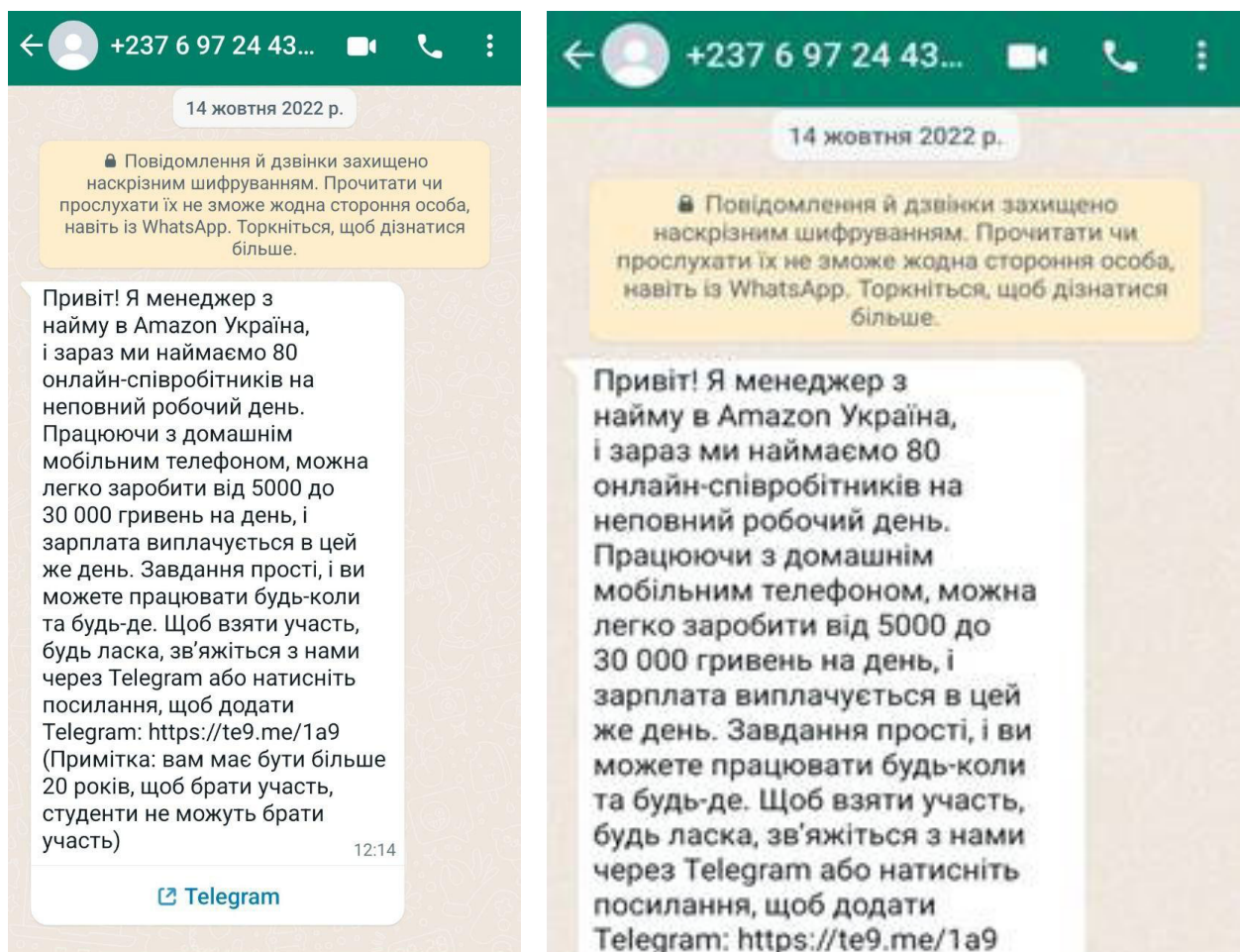


Рис. 9. Пропозиція з працевлаштування

Якщо переглянути реєстраційну інформацію про ресурс **te9.me**, вказаний в оголошенні, то можна побачити, що його створили нещодавно, при цьому усіляко намагаючись приховати відомості про реєстратора (рис. 10).

Address lookup

canonical name **te9.me.**

aliases

addresses **104.21.37.163**
172.67.210.147
2606:4700:3034::ac43:d293
2606:4700:3037::6815:25a3

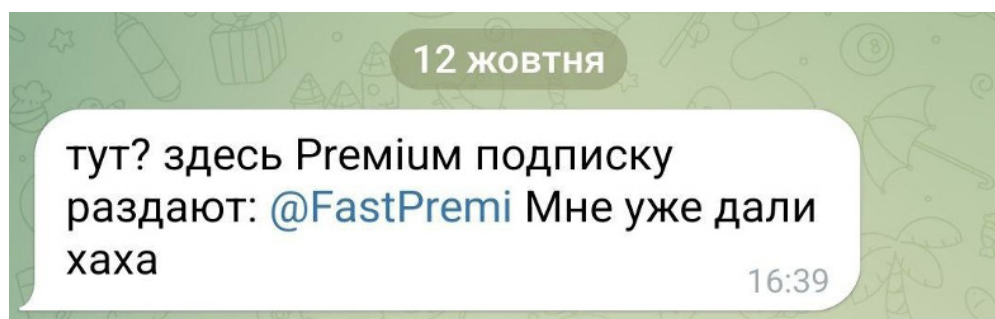
Domain Whois record

Queried **whois.nic.me** with "**te9.me**"...

Domain Name: TE9.ME
Registry Domain ID: D425500000339260668-AGRS
Registrar WHOIS Server: whois.rrpproxy.net
Registrar URL: http://www.key-systems.net
Updated Date: 2023-03-29T09:08:30Z
Creation Date: 2022-04-17T00:26:40Z
Registry Expiry Date: 2024-04-17T00:26:40Z
Registrar Registration Expiration Date:
Registrar: Key-Systems GmbH
Registrar IANA ID: 269
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Reseller:
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Registrant Organization: c/o whoisproxy.com
Registrant State/Province: VA
Registrant Country: US
Name Server: COBY.NS.CLOUDFLARE.COM
Name Server: PAIGE.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: <https://www.icann.org/wicf/>
>>> Last update of WHOIS database: 2023-07-28T11:58:52Z <<<

Рис. 10. Відомості про сайт te9.me

Докладніше про цю атаку можна прочитати за адресою <https://gwaramedia.com/fejk-amazon-rozsilaie-povidomlennya-z-propozicziieyu-roboti-dlya-ukraincziv/>.



Видалити цей чат

Рис. 11. Шахрайське повідомлення у Telegram

У випадку переходу за наведеним у повідомленні посиланням користувачеві пропонувалося знову авторизуватися в Telegram. У разі виконання цих дій захоплювалася сесія Telegram жертви. Надалі від імені користувача, чия сесія була захоплена, серед його контактів починалася розсилка аналогічного шахрайського повідомлення. Маючи захоплену сесію Telegram, зловмисники мали змогу не тільки дістатися синхронізованих контактів, а й завантажити відповідне листування тощо.

Крім фішингу, популярною технікою соціальної інженерії є збирання інформації з відкритих джерел.

Розвідка з відкритих джерел (OSINT) з'явилася вже досить давно, проте саме з появою глобальних мереж вона набула суттєвого значення для збирання інформації про певні об'єкти в усьому світі. Якщо раніше значна частина чутливої інформації зловмисниками добувалася з використанням різноманітних зламів, то сьогодні можна спостерігати збільшення ролі OSINT в цьому процесі. Немаловажним є той факт, що навіть якщо в мережі відсутня безпосередня інформація про розшукуваний об'єкт, її можна спробувати знайти через пов'язані з об'єктом зв'язки, що робить OSINT універсальним інструментом.

На ринку технічних пошукових сервісів зараз присутня велика кількість комплексних спеціалізованих рішень, які за окремим ідентифікатором дозволяють зібрати інформацію про особу чи інший об'єкт (рис. 12). Вказані обставини значно спрощують роботу атакуючих, в тому числі щодо збирання інформації про жертву.

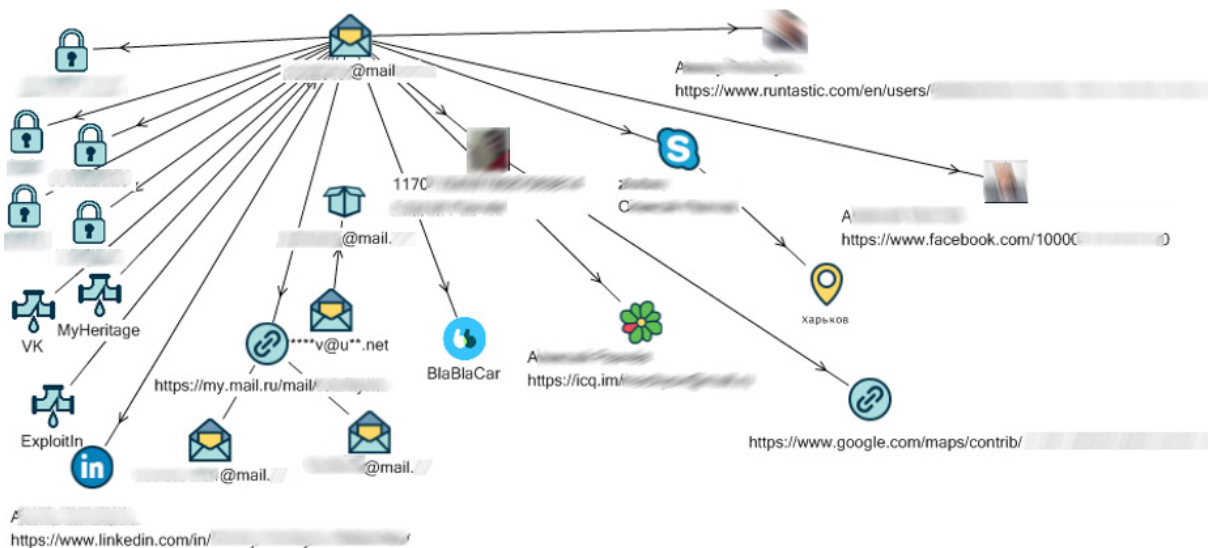


Рис. 12. Результати роботи комплексного рішення з пошуку інформації

У цьому випадку за електронною поштою вдалося знайти п'ять старих паролів до різних ресурсів із вказівкою джерела витоку, прив'язані до електронної пошти облікові записи Skype, LinkedIn, Facebook, ICQ, Google, BlaBlaCar, Runtastik, резервні та пов'язані облікові записи, місто знаходження. Обліковий запис на runtastic.com свідчить, що його володілець, імовірно за все, користується фітнес-браслетом, а відтак – існує ймовірність відслідкувати його переміщення.

Варто відзначити, що навіть без наявності спеціалізованих інструментів кваліфіковані зловмисники здатні зібрати суттєву інформацію про об'єкт атаки за незначний проміжок часу. Так, наприклад, знаючи електронну пошту на сервері Gmail або номер телефону, прив'язаний до такої пошти, можливо дізнатися GAIA ID (Google user ID), знання якого за певних обставин може допомогти зібрати інформацію про об'єкт атаки (рис. 13).

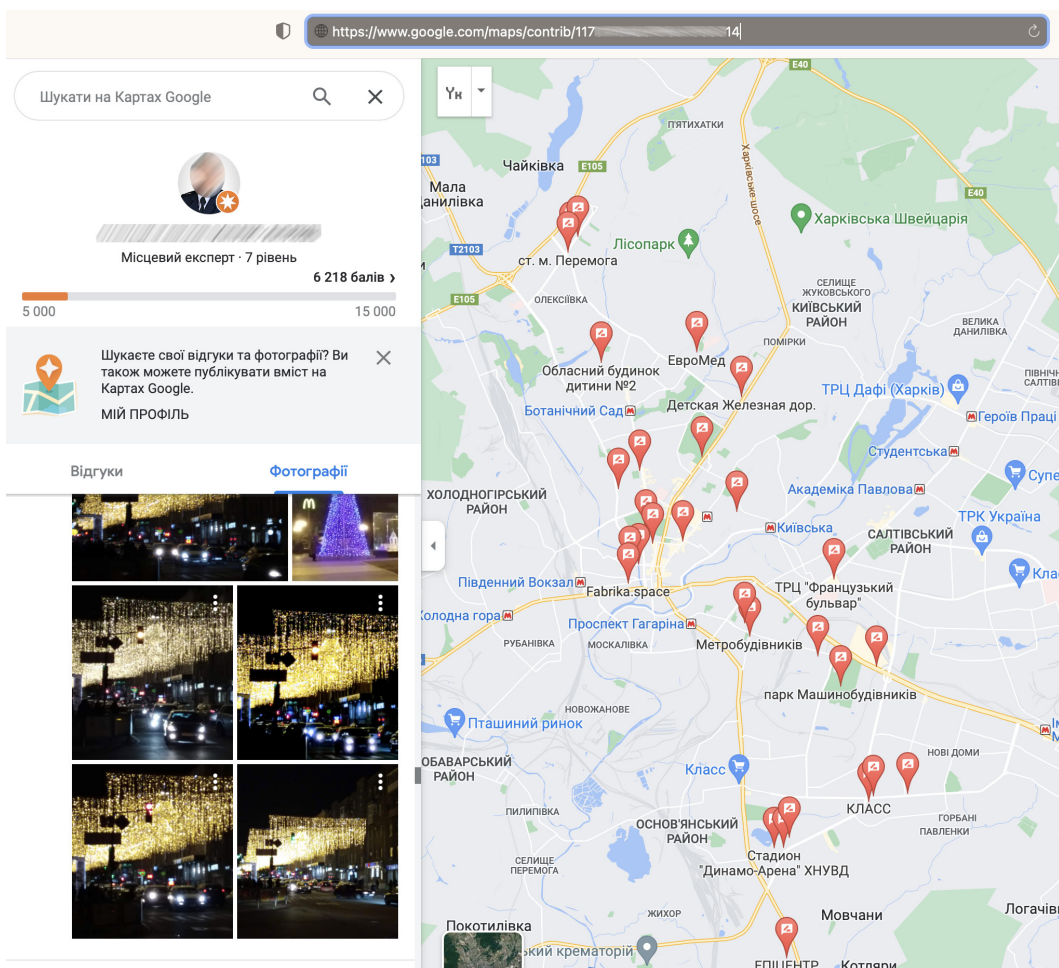


Рис. 13. Виведення карти з відмітками користувача за його GAIA ID

Потрібно наголосити, що OSINT не є самодостатнім інструментом. Тому під час здійснення атаки зловмисники застосовують пошук інформації з відкритих джерел разом із іншими техніками соціальної інженерії.

Ще однією технікою соціальної інженерії є **претекстинг**. Він передбачає як раз попереднє збирання інформації про жертву з відкритих джерел для того, щоб потім представитися жертві особою з певними повноваженнями та стимулювати її виконати дії, вигідні зловмисникам. Прикладом такого виду атаки може слугувати ситуація, коли особа намагається влаштуватися на роботу до правоохоронних органів. Зловмисник, довідавшись про це, вступає в контакт з кандидатом на посаду та представляється керівником певного рівня, від якого може залежати рішення про працевлаштування. Надалі атакуючий намагається, користуючись своїми «повноваженнями», маніпулювати жертвою. Під час здійснення претекстингу застосовується такий інструмент, як *імперсонація*, в межах якої зловмисник може використовувати фізичне маскування типу уніформи, гриму, документів прикриття, створення легенди тощо.

Для набуття даних іншої особи в сучасних умовах нерідко застосовуються засоби штучного інтелекту, які дозволяють створити реалістичні фейкові зображення (рис. 14), відео, підробити голос атакуючого тощо.

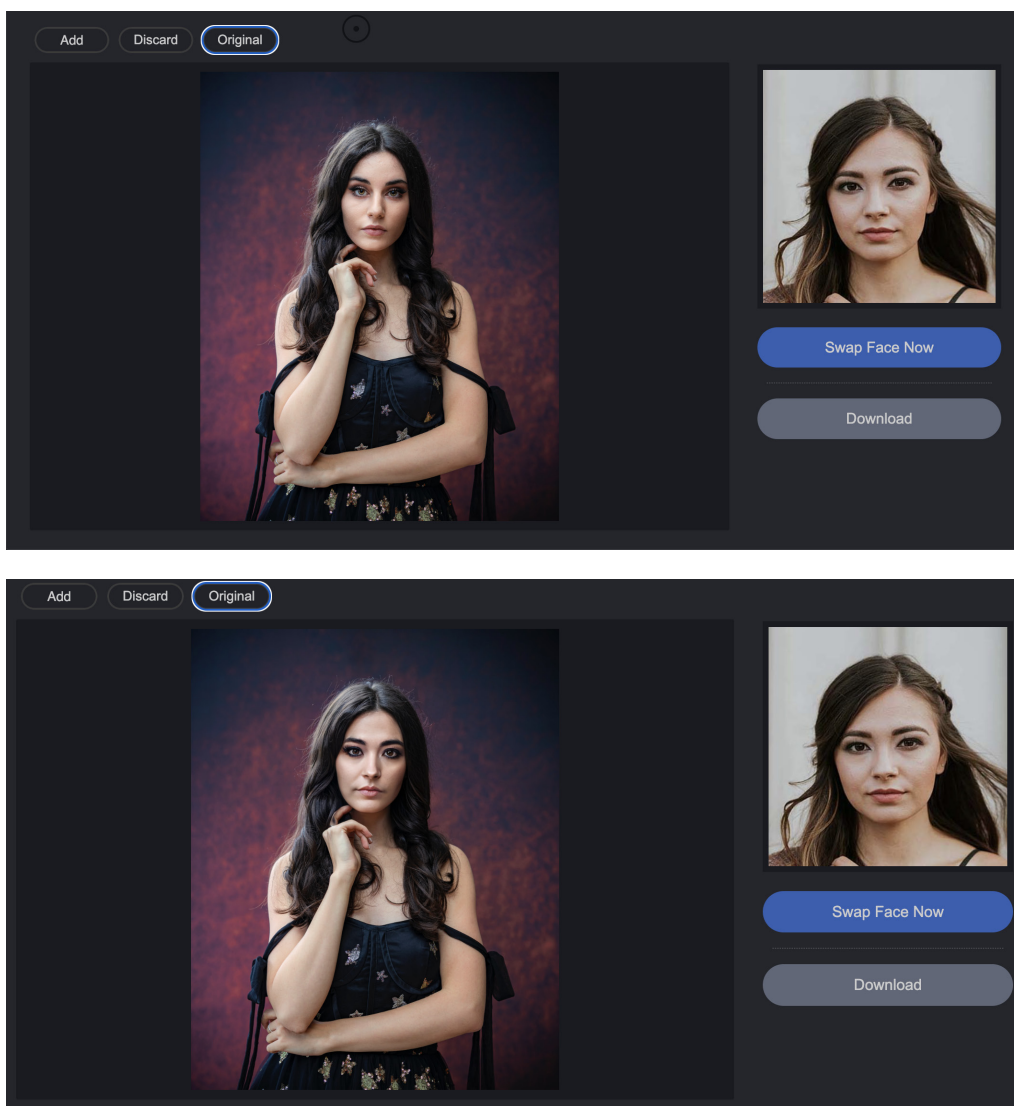


Рис. 14. Заміна обличчя особи (https://unsplash.com/photos/QK_NtQtML8M) за допомогою сервісу faceswapper.ai

Певний сценарій атаки з використанням соціальної інженерії може реалізовуватися без контакту з фізичними особами, як, зокрема, в техніці **«дорожнє яблуко»**. У межах цього методу здійснюється підкидання співробітнику фізичного носія інформації зі шкідливим програмним забезпеченням. Носій може мати певний логотип чи напис, що викличе інтерес, на кшталт «фото ню [ПРИЗВИЩЕ_ПРАЦІВНИКА]» тощо. Щойно співробітник вставить такий носій у комп'ютер, запуститься шкідливий код, який виконуватиме завдання, запрограмовані зловмисником.

Серед небезпечного виду носіїв, які можуть використовуватися в такого виду атаках, слід назвати флеш-накопичувач Rubber Ducky (рис. 15), який під час приєднання до комп'ютера визначається як клавіатура, а скрипт, записаний на такий флешці, виконується на комп'ютері жертви.



Рис. 15. USB Rubber Ducky в упаковці

Продовжуючи цикл популярних технік соціальної інженерії, слід згадати про зворотну соціальну інженерію. За сценарієм такої атаки, жертва повинна сама зв'язатися із зловмисником та надати йому потрібні дані. Прикладом подібної атаки може слугувати попереднє повідомлення поштою або телефоном користувача про зміну контактних даних провайдера електронних комунікацій. У подальшому щодо жертви може бути зімітовано «несправність Інтернету» для того, щоб користувач, згадавши, що йому нещодавно надходило повідомлення про зміну контактних даних, сам вийшов на зв'язок з атакуючим. У подальшому зловмисник інструктуватиме жертву, що потрібно зробити для «усунення несправності».

Зворотна соціальна інженерія може бути не тільки цільовою, а й розрахованою на масову аудиторію. Так, свого часу в Україні розсилали підроблені квитанції про комунальні платежі (<https://glavred.info/stolica/328199-kiev-navodnili-falshivye-kvitancii-zhkh-kommunalshchiki-rasskazali-kak-vernuty-dengi.html>). Оплативши відповідну квитанцію, споживачі, по суті, переказували кошти на рахунки шахраїв (рис. 16).

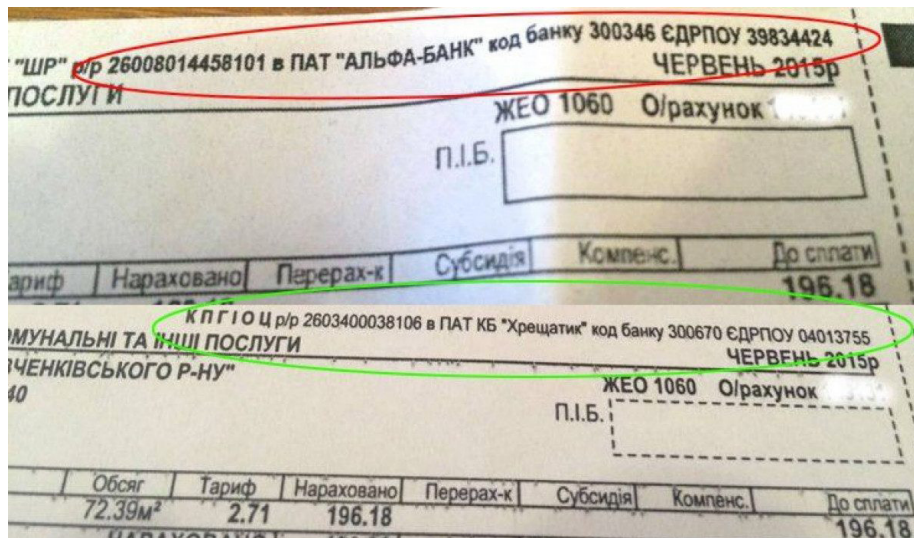
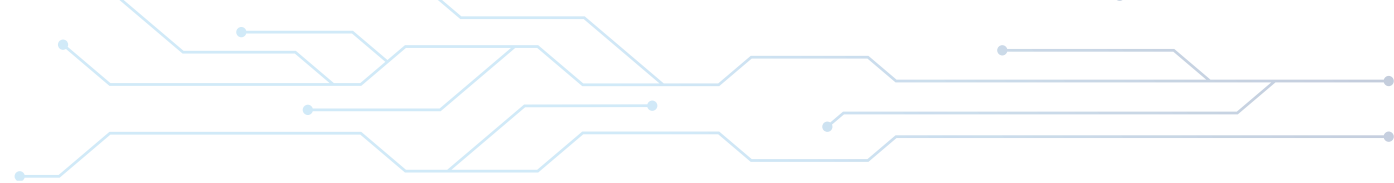


Рис. 16. Зверху – підроблена квитанція, знизу – справжня

Подібні схеми реалізуються шахраями і за кордоном. Так, у США у травні 2023 року була виявлена схема (<https://www.kget.com/news/state-news/san-francisco-parking-ticket-scammers-issue-fake-tickets-set-up-fake-payment-site/>), в межах якої зловмисники підкладали під двірники автомобілів квитанції для оплати паркування, які відрізнялися від справжніх реквізитами для оплати у QR-коді (рис. 17).



Рис. 17. Підроблена квитанція за паркування



Виявити шахрайство вдалося завдяки тому, що атакуючі вказували у квитанції дату, яка ще не настала.

Крім вже наведених технік, варто також згадати банальне підглядання та підслуховування, аналіз сміття тощо. Взагалі, такі схеми постійно удосконалюються зловмисниками, тому для свого убезпечення користувачам слід дотримуватися базових правил кібергігієни щодо безпечного поводження у кіберсфері. Частина таких правил наведена у висновках.

Висновки

Про застосування щодо користувача технік соціальної інженерії може свідчити:

- ▶ надходження нетипового листа з дивним вмістом;
- ▶ збурення емоцій відповідним повідомленням або серією повідомлень;
- ▶ короткий термін, протягом якого слід надати відповідь на повідомлення;
- ▶ зміст повідомлення виглядає надто привабливим, аби бути правдою;
- ▶ пропозиція допомоги, яку не просили;
- ▶ відправник не може підтвердити особу.

Методи протидії соціальній інженерії:

1. Не довіряйте «підозрілим» повідомленням та предметам.
2. Підтверджуйте особу.
3. Утилізуйте сміття належним чином.
4. Навчіться розрізняти працівників.
5. Не робіть компрометуючі фотознімки та відеозаписи.
6. Перевіряйте інформацію з різних джерел.

Як програмний інструментарій протидії соціальній інженерії в частині фішингу можуть бути запропоновані вітчизняна розробка Ukrainian Malicious URL Blocklist (<https://github.com/braveinnovators/url-blocklist>) та зарубіжна система, заснована на використанні штучного інтелекту для аналізу сайтів, – CheckPhish (<https://checkphish.ai/>).

Безпечне користування мережею Інтернет

План лекції

Вступ

1. Поняття, структура та класифікація комп'ютерних мереж
2. Інтернет-технології
3. Безпека браузерів
4. Електронний підпис

Висновки

Рекомендована література

Основна

1. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>.
2. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 106 с.
3. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 262 с.

Допоміжна

4. Про електронні комунікації: Закон України від 16.12.2020. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>.
5. Про електронні документи та електронний документообіг: Закон України від 22.05.2003. Офіційний вісник України. 2003. № 25 (04.07.2003). ст. 1174.
6. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017. Офіційний вісник України. 2017. № 91 (21.11.2017). ст. 2764.
7. Інтернет-технології. URL: <https://uk.wikipedia.org/wiki/Інтернет-технології>.
8. Веб-сайт. URL: <https://uk.wikipedia.org/wiki/Веб-сайт>.
9. Електронна дошка оголошень. URL: https://uk.wikipedia.org/wiki/Електронна_дошка_оголошень.
10. Social bookmarking. URL: http://en.wikipedia.org/wiki/Social_bookmarking.
11. Skype. URL: <https://uk.wikipedia.org/wiki/Skype>.
12. Viber. URL: <https://uk.wikipedia.org/wiki/Viber>.

Інформаційні ресурси в Інтернеті

13. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

Текст лекції

Вступ

У своїй повсякденній діяльності користувачам нерідко доводиться мати справу з різними мережевими технологіями – як для здійснення специфічної службової діяльності, так і для комунікацій у цілому. В основному, середовищем, де це відбувається, є Інтернет.

1. Поняття, структура та класифікація комп'ютерних мереж

Для поняття «комп'ютерна мережа» більш загальним терміном є дефініція «електронна комунікаційна мережа», яка згідно зі ст. 2 Закону України від 16.12.2020 «Про електронні комунікації» є комплексом технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг.

Як впливає із цього визначення, для організації роботи мережі потрібно використовувати певну сукупність апаратних та програмних засобів (кабелів, з'єднувачів, мережових адаптерів, трансіверів, репітерів, концентраторів, комутаторів, маршрутизаторів, мостів, шлюзів тощо).

За територіальною ознакою комп'ютерні мережі поділяються на *локальні* (Local Area Networks – LAN), *міські* (Metropolitan Area Networks – MAN), *глобальні* (Wide Area Networks – WAN). Інколи в цій класифікації виділяють мережі *кампусні* (Campus Area Network – CAN) та *широкомасштабні* (Wide Area Network – WAN).

Одним з ключових елементів організації сучасних комп'ютерних мереж є відповідна система адресації. Найбільш поширеною подібною системою є адресація з використанням стеку протоколів TCP/IP.

У стеку TCP/IP використовуються три типи адрес:

- ▶ апаратні (найпоширенішими є MAC-адреси, проте можуть використовуватися адреси IPX і X.25);
- ▶ IP-адреси;
- ▶ доменні імена.

MAC-адреса, яка складається з 6 байт, призначається мережевим адаптерам і мережевим інтерфейсам. Вона функціонує у межах локальної мережі.

Уся множина комп'ютерів ідентифікується за допомогою IP-адрес, яка для IPv4 складається з 32 біт (4 октети по 8 біт, розділених крапками), а для IPv6 – зі 128 біт. IP-адреса призначається окремим інтерфейсам, тому якщо один комп'ютер (хост) містить кілька інтерфейсів, він може мати і кілька IP-адрес. IP-адреса складається з двох частин: старшої (ліворуч) – мережевої, яка визначає номер мережі, і молодшої (праворуч) – хостової, яка визначає номер хоста в цій мережі.



Для організації роботи з IP-адресами використовуються дві основних моделі: класова (для IPv4 – класи А, В, С, D і Е) та безкласова. Для того, щоб відрізнити хостову та мережеву частину, в IP-адресі може використовуватися або маска мережі (стандарт IPv4), або префікс мережі (визначається слешем « / » в обох стандартах).

Для того, щоб спростити процес ідентифікації для людини, в мережі використовуються доменні імена. Інформацію про асоційовані з доменними іменами IP-адреси надають служби імен доменів (DNS). У мережі існує ієрархія доменів, так само як і ієрархія служб DNS.

2. Інтернет-технології

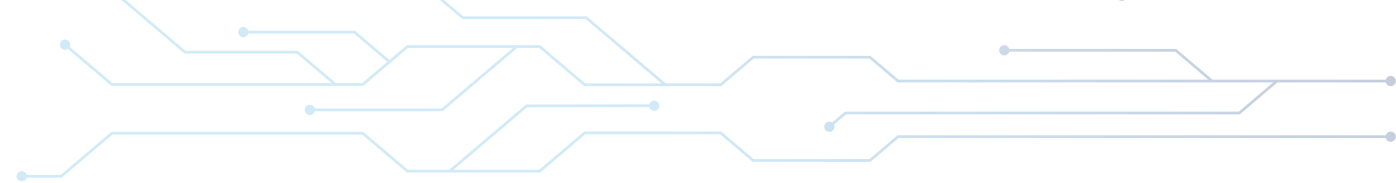
Інтернет-технології – це технології створення і підтримки різних інформаційних ресурсів у комп'ютерній мережі Інтернет. Найбільш поширеними *програмними технологіями*, які використовуються для вчинення протиправної діяльності у кіберсфері, є:

- ▶ спеціально створені веб-сайти;
- ▶ дошки оголошень (www.ss.ua, olx.ua, www.ria.com, www.sudver.com, inforico.ua, www.doshka.net, k4.at.ua, www.stop.kiev.ua, www.ukrboard.com.ua);
- ▶ комп'ютерні соціальні мережі (Facebook, Twitter, LinkedIn, Instagram, TikTok);
- ▶ електронна пошта (Evolution, KMail, Mozilla Thunderbird, Netscape Mail, Outlook Express, TheBat!);
- ▶ чати (<http://www.e-chat.co/>, <http://tinychat.com/>, <http://www.ukrainianwomendating.com/>, <http://www.wireclub.com/places/ukra>);
- ▶ мультимедійні засоби спілкування (MSN, Google Talk, Pidgin, AIM, Trillian, Windows Live Messenger, Yahoo Messenger, Skype, Viber, WhatsApp);
- ▶ засоби забезпечення анонімності (Proxy servers (HTTP, SOCKS, CGI), Dark-net, Tor, 2IP);
- ▶ засоби шифрування (PGP, Red Phone, Truecrypt);
- ▶ засоби стеганографії;
- ▶ мережеві сховища (хмари, Peer-to-peer, FTP, відеохостинги);
- ▶ електронні гроші (PayPal, Bitcoin, Paxum);
- ▶ площадки, які можуть бути використані для легалізації коштів (WesternUnion, Forex);
- ▶ шкідливе програмне забезпечення.

Розглянемо докладніше окремі технології, які можуть бути використані для вчинення протиправних дій.

Веб-сайт – це сукупність веб-сторінок, доступних у мережі Інтернет, які об'єднані як за змістом, так і за навігацією.

Веб-сайти нерідко застосовуються зі злочинною метою. Це може бути купівля / продаж за їх допомогою викраденої інформації або заборонених



до використання предметів і речовин, поширення протиправного контенту, подання оголошень щодо вчинення певних дій протиправного характеру тощо.

Електронна дошка оголошень – це веб-сайт, цілком аналогічний звичайним побутовим дошкам оголошень або рекламним газетам. Її вміст – це набір оголошень комерційного та/або некомерційного характеру, які розміщуються як на оплатній, так і на безоплатній основі, залежно від конкретного сайту. Багато рекламних компаній, що мають паперові видання і працюють у сфері теле- і радіореклами, також створюють і підтримують власні електронні дошки оголошень.

Електронна дошка оголошень зазвичай поділена на кілька тематичних розділів – відповідно до змісту оголошень. Як правило, це – продаж/купівля товарів, надання послуг, пошук/пропонування роботи тощо.

Для розміщення свого оголошення користувачеві потрібно лише ввести в спеціальній формі його тему, своє ім'я/псевдонім або назву організації, а також координати: адресу електронної пошти, поштову адресу, телефон, свій сайт тощо (набір даних залежить від конкретного ресурсу).

Після публікації оголошення воно відображається у відповідному розділі, і разом з ним, як правило, відображаються ім'я автора, його тема та зміст, а також контактні дані.

Електронні дошки оголошень бувають двох видів: ті, що модеруються (ті, у яких є так званий модератор – людина, яка контролює роботу цієї дошки), і ті, що не модеруються, – вони працюють автоматично.

В умовах стрімкого розвитку високих інформаційних технологій дошки оголошень стали потужним інструментом інтернет-реклами. Все більше людей купують/продають товари та послуги через Інтернет, використовуючи для цього дошки оголошень. Український сегмент мережі Інтернет не є винятком і налічує сотні різних дошок оголошень, і ось найпопулярніші з них: www.ss.ua, olx.ua, www.ria.com, www.sudver.com, inforico.ua, www.doshka.net, k4.at.ua, www.stop.kiev.ua, www.ukrboard.com.ua тощо.

Для вчинення протиправних дій у кіберсфері нерідко застосовуються **комп'ютерні соціальні мережі**. Термін «соціальні мережі» – відносно нове явище інформаційних технологій, що має різні визначення. Технології соціальних мереж набувають різноманітних форм і, по суті, засновані на мережевих інтернет-технологіях, включаючи електронні журнали та інтернет-форуми, веб-журнали, соціальні блоги, мікроблоги, вікі, соціальні медіа, підкасти, фотографії або зображення, відео, рейтинги та соціальні закладки. Найбільш популярними соціальними мережами в Україні є Facebook, Twitter, LinkedIn, Instagram, TikTok, ClubHouse.



З точки зору криміналу, сайти соціальних мереж створюють надзвичайно зручну платформу для глобальних форумів, на яких правопорушники можуть провадити свою протиправну діяльність, майже не ризикуючи бути впійманими.

Соціальні медіа пропонують злочинцям елемент анонімності й прикриття, тому вони можуть спілкуватися на ранньому етапі своєї діяльності, майже не ризикуючи, що їх виявлять правоохоронні органи.

Електронна пошта (email, e-mail) – це метод обміну цифровими повідомленнями між одним автором та одним або більше отримувачем. Сьогодні системи електронної пошти спираються на модель проміжного накопичення і передачі, а сервери електронної пошти приймають, передають, доставляють і зберігають повідомлення. Ані користувачі, ані їх комп'ютери не повинні перебувати в онлайн-режимі одночасно – їм потрібно лише ненадовго з'єднатися з поштовим сервером на час, потрібний для відправлення або прийому повідомлень.

Користуватися послугами електронної пошти можна як через інтернет-браузер (Gmail, Yahoo, Hotmail, I.ua, Ukr.net), так і за допомогою спеціальних поштових клієнтів. Найпопулярнішими з них є: Mozilla Thunderbird, Outlook Express, TheBat!.

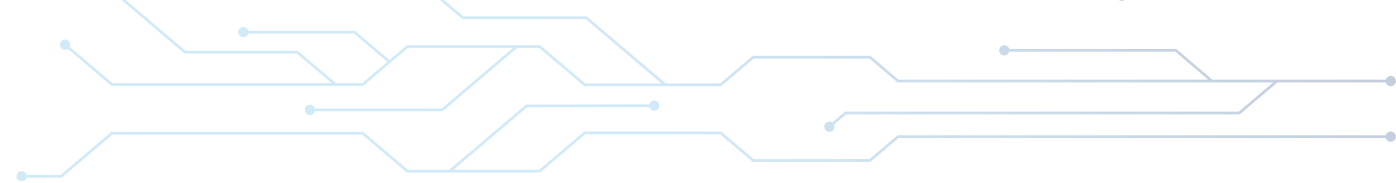
Повідомлення електронної пошти складається з двох частин:

- 1) *тіло повідомлення*, яке може містити текстову інформацію та інші дані, наприклад, графічні (фото/відео-, аудіо- (звукові) та бінарні (програми/додатки) файли. Також цілком можна включити гіперпосилання на інші джерела, такі як веб-сайти, групи новин та ftp-сайти;
- 2) *заголовок повідомлення*, який містить службову інформацію, у тому числі адресу електронної пошти відправника та одну або більше адрес одержувачів. Ці дані включають технічні деталі, наприклад те, хто надіслав повідомлення, за допомогою якої програми його було складено, а також через які поштові сервери пройшло повідомлення на шляху до одержувача.

Рівень сучасних технологій дозволяє швидко передавати значний обсяг медіа-контенту, тому серед правопорушників є досить популярними програмні **засоби медіа-спілкування**.

Одним із таких засобів є інтернет-пейджери (Instant Messengers) – це програми, які дозволяють обмінюватися текстовими повідомленнями між комп'ютерами у режимі реального часу.

Для спілкування також можуть використовуватись так звані «чати». Цей термін переважно застосовується для опису будь-якої форми синхронного конференц-зв'язку, а іноді – навіть асинхронного конференц-зв'язку. Отже,



цей термін може означати будь-яку технологію – від онлайн-чатів у реальному часі, онлайн-взаємодії з незнайомцями, обміну миттєвими повідомленнями та онлайн-форумів до повного занурення у графічне соціальне середовище. Основною метою чату є обмін текстовою інформацією з групою інших користувачів. Загалом здатність спілкуватися з багатьма людьми в рамках однієї бесіди відрізняє чати від програм обміну миттєвими повідомленнями, які переважно призначені для спілкування один-на-один. Користувачі певного чату зазвичай мають спільний інтерес або інший аналогічний зв'язок, а існуючі чати охоплюють широку низку тем. Нова технологія дозволяє передбачати в деяких програмах можливість обміну файлами та використання веб-камер.

Слід зазначити, що останнім часом правопорушники почали користуватися складнішими засобами спілкування, зокрема створеними на базі поширеного протоколу передачі даних VoIP. VoIP-протокол (протокол передачі голосу Інтернетом) та відеотелефонія є наступним кроком розвитку інтернет-технологій, а тому за своєю суттю переважно використовуються молоддю, особливо якщо цю технологію вбудовано у певні соціальні медіа, і вони присутні на планшетах чи смартфонах.

Найпопулярнішими застосунками такого штибу є Skype, Telegram, WhatsApp, Viber.

3. Безпека браузерів

Що таке інтернет-браузер? Це – програмне забезпечення, яке дозволяє користувачам отримувати інформацію з сайтів мережі Інтернет. Браузери транслюють код інтернет-сторінок у зрозумілий для людини вигляд. Для передачі використовується протокол HTTP або його безпечніша версія HTTPS. Протокол – це набір правил передачі файлів (тексту, зображень, відео тощо) через мережу Інтернет. Приклади браузерів: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari.

Але браузери наразі не тільки надають доступ до сторінок, а і слугують платформою для додаткових програм, що полегшують користування мережею Інтернет. Ці програми називаються плагінами. Плагіни розширюють функціональність браузера, додаючи додаткових функцій. Більшість плагінів можуть встановлювати додаткові панелі інструментів, маркетинг і помічників пошуку. Крім того, ви може помітити нові кнопки, посилання або функції, такі як блокування спливаючих вікон, доданих у браузер. Деякі плагіни невидимі для користувача, оскільки вони працюють у фоновому режимі й не мають графічного інтерфейсу. Деякі з плагінів можуть бути шкідливими. Щоб пам'ятати вас, браузери використовують таку річ, як cookies.



Cookies – це невеликі текстові файли у нас на комп'ютерах, у яких зберігається інформація про ваші попередні дії на сайтах. Крім входів до акаунтів, вони вміють запам'ятовувати:

- ▶ налаштування користувачів: наприклад, мова, валюта або розмір шрифту;
- ▶ товари, які ви переглядали або додали до кошика;
- ▶ текст, який ви вводили на сайті раніше;
- ▶ IP-адресу і місце розташування користувача;
- ▶ дату і час відвідування сайту;
- ▶ версію ОС і браузера;
- ▶ кліки та переходи.

Коли ми робимо на сайті якісь дії, наприклад, додаємо товар до кошика або вводимо дані входу до акаунту, сервер записує цю інформацію в cookies і відправляє браузеру разом зі сторінкою. Коли ми переходимо на іншу сторінку сайту або заходимо на нього через деякий час, браузер відправляє cookies назад.

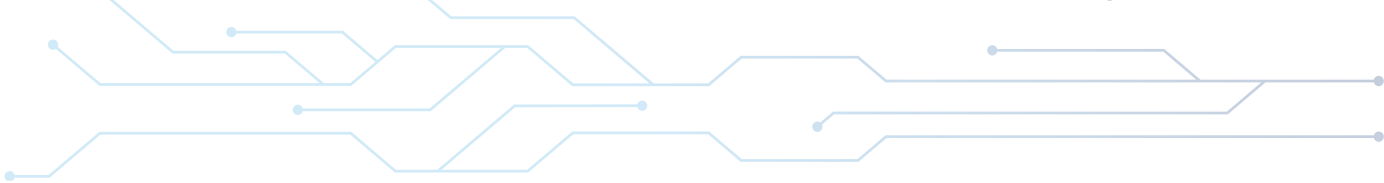
Cookies бувають тимчасовими і постійними. Постійні cookies залишаються на комп'ютері, коли ми закриваємо вкладку з сайтом, а тимчасові – видаляються. Які саме cookies використовувати на конкретному сайті – тимчасові або постійні – вирішує його розробник. Саме тому на одних сайтах ми не виходимо з акаунтів, навіть коли заходимо на них раз через кілька днів, а на інших вводимо пароль заново, хоча відійшли від комп'ютера на п'ять хвилин. Самі по собі cookies не є небезпечними – це звичайні текстові файли. Вони не можуть запускати процеси на комп'ютері та взагалі взаємодіяти з операційною системою. Але їх можуть спробувати перехопити або вкрати, щоб відстежувати ваші попередні дії в мережі або входити до ваших акаунтів без авторизації.

Зазвичай інформацію, яку записують у cookies, зашифровують перед відправкою, а власне cookies передають за HTTPS-протоколом. Це допомагає захистити призначені для користувача дані, але за впровадження шифрування і безпечну відправку відповідає розробник сайту. Відвідувачам залишається тільки сподіватися, що все налаштували грамотно. Зі свого боку, користувач може тільки заборонити браузеру використовувати cookies або час від часу чистити їх самостійно.

Зовсім відключати cookies – не завжди хороша ідея. Наприклад, усі інтернет-магазини працюють за допомогою cookies. Якщо заборонити браузеру їх використовувати, сервер не зможе запам'ятати, що саме ви додали до кошика. Чистити cookies вручну практичніше, але доведеться щоразу заново налаштовувати зовнішній вигляд сайту і входити до акаунтів.

Чому через браузер можуть реалізовуватись загрози?

Браузери застарівають та з'являються вразливості, які експлуатуються хакерами віддалено.



Хакери зламують легітимні сайти та розміщують на них шкідливий код та програми, а ви можете навіть не знати про те, що стали жертвою.

Зловмисники зламують публічні точки доступу до мережі Інтернет і намагаються перехопити інформацію користувачів.

Якщо ви звернете увагу на новини зі світу кібербезпеки, то побачите, що браузер майже щомісяця публікують оновлення та звітують про винайдені та закриті вразливості. Чому? Тому що дуже велика кількість вразливостей виявляється ледь не щоденно. І хакери одразу починають їх використовувати у своїх атаках.

Треба зрозуміти, що не існує абсолютно безпечного браузера. Іноді виникає ситуація, коли вразливості можуть залишатися незакритими протягом десятиліть. Тобто ви, щоб не стати жертвою, маєте ретельно піклуватись про безпеку вашого браузера. Але треба пам'ятати, що ваша необачність може нести ризики не тільки вам особисто, а й усій вашій установі.

З метою убезпечення браузера необхідно постійно його оновлювати, щоб не допустити появи відомих вразливостей у ньому. Також необхідно коректно налаштувати вимоги до приватності даних у браузері. Встановити додаткові плагіни безпеки, наприклад, HTTPS Everywhere (буде попереджати, якщо сайт не захищено HTTPS і є ризик перехоплення даних – логінів, паролів тощо) або Adblock (блокувальник реклами).

4. Електронний підпис

Одним із сучасних інструментів убезпечення в мережі Інтернет є електронний підпис. Згідно зі ст. 5 Закону України «Про електронні документи та електронний документообіг» **електронний документ** – це документ, інформація в якому зафіксована у вигляді електронних даних, враховуючи **обов'язкові реквізити документа**.

Реквізитом електронного документа є **електронний підпис** – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються та використовуються ним як підпис.

Електронний підпис накладається за допомогою *особистого ключа* та перевіряється за допомогою *відкритого ключа*.

При цьому **особистий ключ** – це параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів, а відкритий ключ – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів.

Згідно зі ст. 15 Закону України «Про електронну ідентифікацію та електронні довірчі послуги» залежно від ступеня довіри до засобів електронної ідентифікації вводяться три рівні електронного підпису:

- ▶ простий електронний підпис та печатка – низький рівень довіри;
- ▶ удосконалений електронний підпис та печатка – середній рівень довіри;
- ▶ кваліфікований електронний підпис та печатка – високий рівень довіри.

Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, а також презумпцію його відповідності власноручному підпису. Кваліфікована електронна печатка має презумпцію цілісності електронних даних і достовірності походження електронних даних, з якими вона пов'язана.

Перехід до використання на практиці електронного підпису є черговим важливим кроком на шляху втілення електронного урядування, адже електронний підпис є важливим компонентом електронного документообігу.

Упровадження електронного підпису, зокрема, робить можливим:

- ▶ подання різноманітної бухгалтерської, податкової, статистичної та іншої звітності до державних органів в електронному вигляді телекомунікаційними каналами, зокрема через Інтернет;
- ▶ організацію онлайн-закупівель державних суб'єктів господарювання через систему електронних торгів, що сприяє забезпеченню прозорості їх діяльності та зменшенню кількості випадків зловживань;
- ▶ юридично значущий електронний документообіг між органами державної влади, підприємствами й організаціями;
- ▶ отримання громадянами різноманітних офіційно засвідчених документів та участь у виборах через мережу Інтернет.

Загальна схема накладання електронного підпису наведена на рис. 1, а його перевірки – на рис. 2.

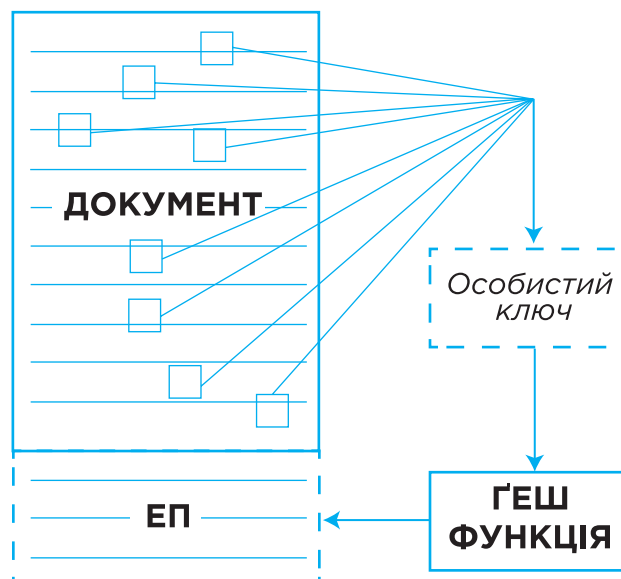


Рис. 1. Приблизна модель накладання електронного підпису



Рис. 2. Приблизна модель перевірки електронного підпису

Підсумовуючи викладене, необхідно зазначити, що накладання електронного підпису не забезпечує конфіденційності документа, тобто його зміст **не шифрується**, але при цьому можна впевнитись у **цілісності** документа й **ідентифікувати** його підписувача.

Висновки

Як головні правила убезпечення в мережі Інтернет можна запропонувати такі:

1. Налаштуйте браузер на безпечний перегляд сторінок.
2. Не завантажуйте підозрілі файли.
3. Використовуйте антивірус та фаєрвол.
4. Шифруйте повідомлення.
5. Використовуйте захищені з'єднання.
6. Встановлюйте оновлення.

Безпечне користування електронною поштою

План лекції

Вступ

1. Принцип роботи електронної пошти
2. Види атак
3. Загрози під час користування поштовою скринькою

Висновки

Рекомендована література

Основна

1. Даник Ю.Г., Гришук Р.В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.

Допоміжна

5. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 72–73.
6. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 65–67.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

Текст лекції

Вступ

Кожного дня ми використовуємо електронну пошту в робочих та особистих цілях. Вона стала одним з основних каналів комунікації з нами, а відтак – неабияким чином привабливою для кіберзлочинців. Розглянемо, які існують загрози під час використання електронної скриньки, а також як від них захиститись.

1. Принцип роботи електронної пошти

Електронна пошта – сервіс Інтернет для передавання текстових повідомлень та прикріплених до них файлів у вигляді листів та відкладеного їх зчитування (рис. 1).

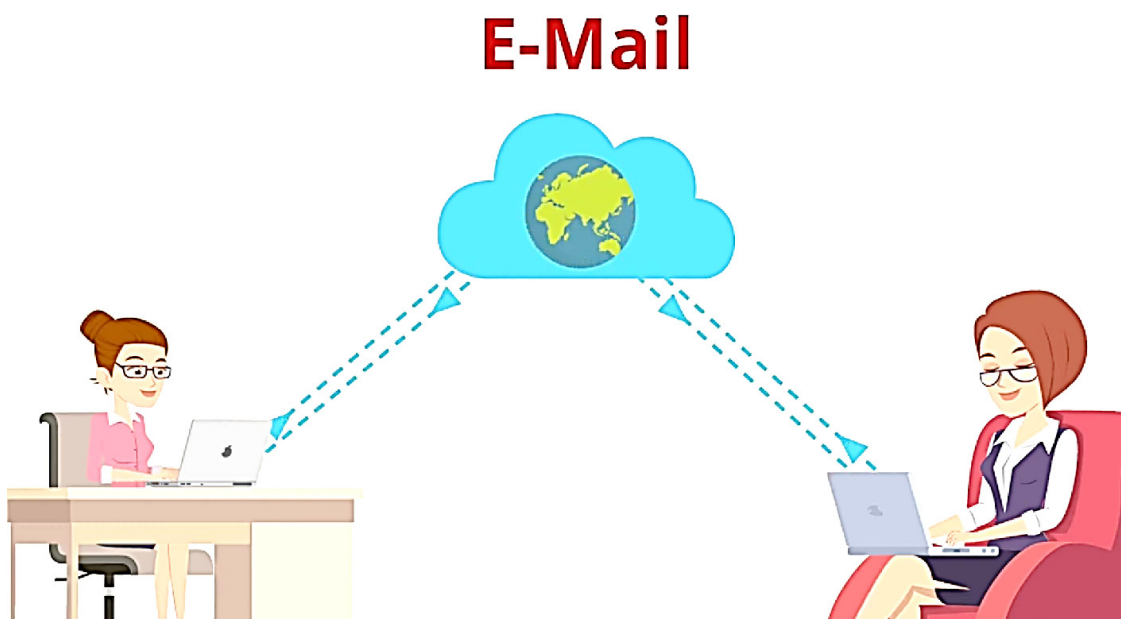


Рис. 1. Електронна пошта як сервіс передавання текстових повідомлень та прикріплених до них файлів з відкладеним зчитуванням (<https://www.youtube.com/watch?v=VEYC1VnnEaY>)

Розглянемо принцип роботи електронної пошти.

На рис. 2 показано типову послідовність подій, коли Аліса відправляє листа за допомогою поштової програми (клієнта) (Mail User Agent, MUA). Аліса вводить e-mail адресата та натискає кнопку «Відправити».

1. Поштовий клієнт форматує повідомлення в спеціальний формат та відправляє його за протоколом SMTP (Simple Mail Transfer Protocol) до агента з відправлення пошти (mail submission agent, MSA) на поштово-му сервері smtp.a.org, де зареєстрована її поштова скринька.

2. MSA визначає адресу призначення, що фігурує у протоколі SMTP (а не в заголовку повідомлення), – bob@b.org. Назва перед @ – це локальна частина адреси, часто це – ім'я користувача / одержувача, а текст після @ – доменне ім'я. MSA надсилає запит до сервера системи доменних імен (DNS), щоб визначити доменне ім'я поштового сервера Боба.
3. DNS-сервер для домена b.org (ns.b.org) надсилає у відповідь MX-записи, в яких перелічено поштові сервери цього домена, зокрема mx.b.org – це поштовий сервер домена b.org.
4. Сервер smtp.a.org за допомогою протоколу SMTP надсилає лист на mx.b.org до кінцевого агента доставки повідомлень (message delivery agent, MDA), який доставляє його до поштової скриньки Боба.
5. Боб натискає кнопку «Отримати повідомлення» в поштовому клієнті, який отримує листи з сервера за протоколом Post Office Protocol (POP3) або Internet Message Access Protocol (IMAP).
6. MUA користувача bob забирає повідомлення за допомогою поштового протоколу (POP3) або протоколу доступу до інтернет-повідомлень (IMAP).

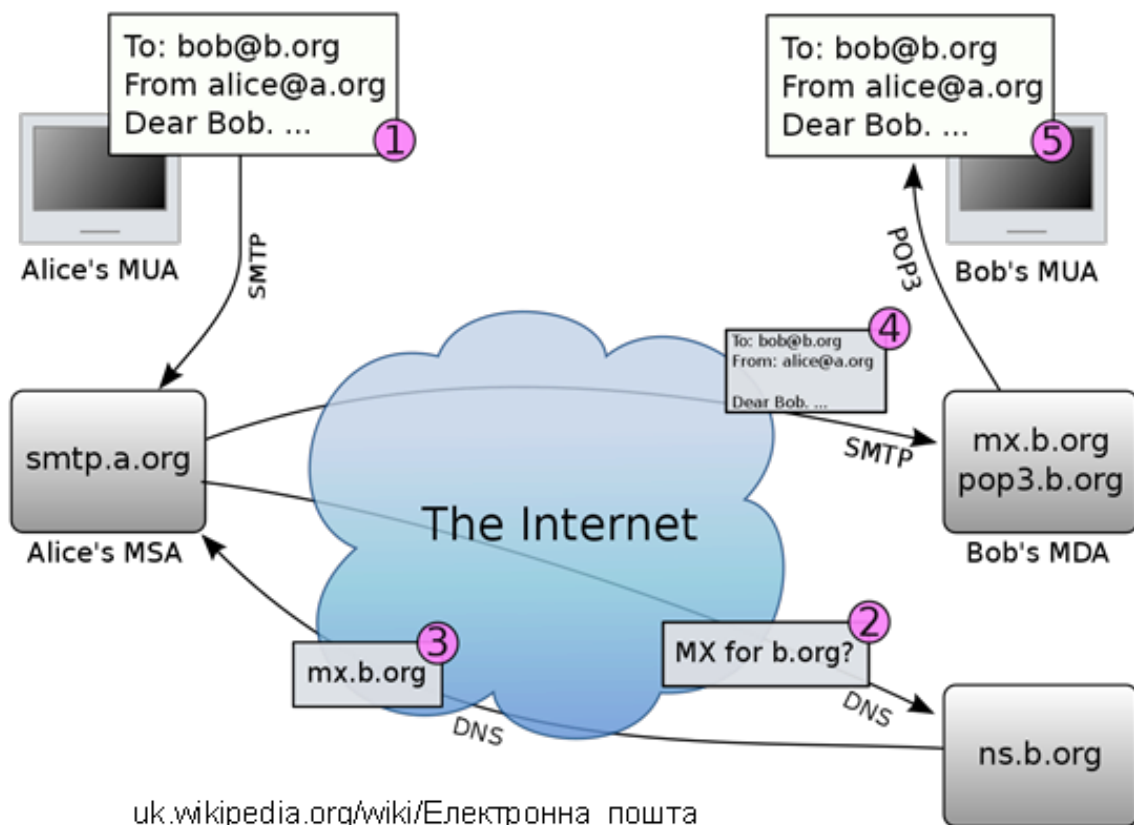


Рис. 2. Принцип роботи електронної пошти

Замість поштового клієнта користувачі часто використовують веб-браузер, який підключається до поштового сервера за протоколом https.

2. Види атак

Після того, як люди почали активно користуватись імейлом, історія бачила чимало успішних кібератак, які використовували пошту як інструмент доставки шкідливого програмного забезпечення (ШПЗ) та виманювання у людей конфіденційної інформації.

- Вірус **ILOVEYOU** (2001) завдав збитків на суму близько 10 млрд дол. США. Було уражено ~10% всіх комп'ютерних систем у світі. Злочинці надіслали листи із зізнанням у коханні та скористались людською цікавістю, щоб адресати відкрили файл у вкладенні.
- **Вірус MyDoom** (2009) завдав збитків на суму близько 38 млрд дол. США. Користувачі отримували листа нібито з помилкою доставки імейлу до якогось отримувача, і деталі помилки знаходились у вкладенні листа.

Основним каналом доставки зловмисних повідомлень є електронна пошта (рис. 3).

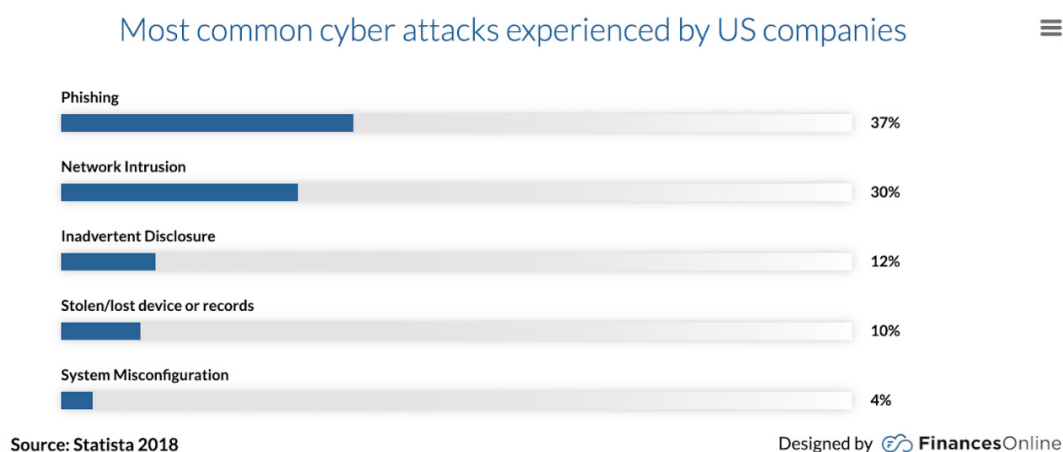


Рис. 3. Статистика атак за 2018 рік

Чому електронна пошта є настільки привабливою для кіберзлочинців?

- Базы даних поштових адрес відносно легко знайти в Інтернеті.
- Функція вкладень до листів дозволяє надсилати файли зі шкідливим програмним кодом.
- Користувачі не очікують отримати листи зі шкідливими вмістом.
- Користувачі часто несвідомо відкривають всі вхідні листи.

Особиста та робоча пошта

Одним з перших правил безпеки електронної скриньки (насправді – не тільки її) є чітке розмежування особистого та службового акаунту. Чому це так важливо?

Службова пошта:

- ▶ показує вашу належність до організації – (vasyl@me.gov.ua). Ми бачимо, що Василь має відношення до Міністерства розвитку економіки. Одне це вже зумовлює довіру до листів, які надходять з цієї адреси;
- ▶ дані зберігаються на серверах вашої установи і керуються відділом інформаційних технологій. Треті сторони не мають доступу до цих даних;
- ▶ містить конфіденційну інформацію, яка стосується вашої організації.

Особиста пошта:

- ▶ зберігається на серверах компанії, яка надає послуги поштового сервісу;
- ▶ містить вашу приватну інформацію;
- ▶ використовується для реєстрації у соціальних мережах та на інших ресурсах.

Отже, при використанні особистої та службової пошти не за призначенням:

- 1) ми знаємо, хто може мати доступ до приватних або службових даних. IT-відділ може бачити вашу особисту переписку, а провайдери поштових сервісів – службову комунікацію;
- 2) не контролюємо, до яких ресурсів буде мати доступ злочинець у разі компрометації вашої скриньки;
- 3) збільшуємо ймовірність зламу ваших облікових записів.

Наслідком може бути те, що саме ваші облікові записи можуть стати інструментом для атаки на вашу організацію.

Як слід обирати поштовий сервіс для власного користування.

Необхідно зазначити, що провайдери поштового сервісу – це комерційні компанії, і вони потребують отримання доходу від своєї діяльності, тому:
«Якщо ми не платимо за продукт, ми є продуктом (в даному випадку – наші дані та інформація, яка проходить через нас)».

Так, наприклад, компанія «Google» прописує в своїх політиках, що вони дійсно заробляють на інформації про нас. Ось витяг з цих політик*:
«Ми використовуємо ваші особисті дані, щоб зробити сервіси Google корисніше для вас, наприклад, пропонувати варіанти автозаповнення під час введення пошукових запитів, підбирати оптимальні маршрути на Картах або показувати вам рекламу на основі ваших інтересів».

Ми отримуємо кошти або за розміщення оголошення (наприклад, банера у верхній частині сторінки), або за результати показу, такі як клік по оголошенню».

Отже, коли ви обираєте поштовий сервіс, необхідно відповісти на питання: Чи готові ви платити за користування поштовим сервісом?

- якщо Так, тоді рекомендований сервіс: <https://protonmail.com/ua/signup> (є безкоштовна опція з лімітом на 500 Мб);
- якщо Ні, тоді ви будете платити вашими даними.

Якщо ви обрали все ж таки платити своїми даними, звертайте увагу на такі питання:

- з якої країни походить компанія?
- чи підвладна ця компанія державі?
- чи була помічена вона у витоках інформації про своїх користувачів?
- чи є політичний інтерес у цієї держави?

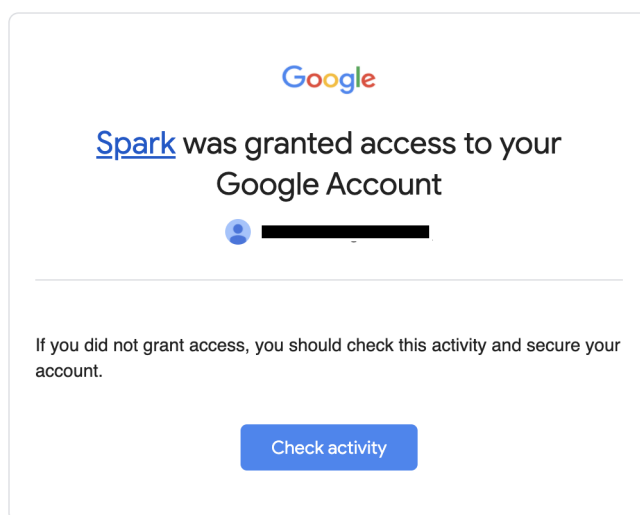
2. Загрози під час користування поштовою скринькою

Фішинг – це схема, за якої зловмисники змушують користувачів передавати конфіденційну інформацію, наприклад, паролі та номери соціального страхування. Вона, зазвичай, передбачає надсилання повідомлення спаму, яке нібито походить із довіреного джерела, наприклад, із банку (це – наживка). У повідомленні спаму міститься посилання на шахрайський веб-сайт, що видається за довірене джерело (це – пастка). Користувач, нічого не підозрюючи, вводить інформацію, яка цікавить зловмисників, вважаючи, що перебуває на сайті, який заслуговує на довіру.

Які мотиви зловмисника надсилати фішингові листи?

1. Отримати конфіденційні дані.

Злочинець надсилає лист з темою «Вас зламали! Швидше змініть пароль» і видає себе за авторитетне джерело – Google (рис. 4).



You received this email to let you know about important changes to your Google Account and services.
© 2019 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Рис. 4. Підроблений лист від Google

Мета листа – перехід за підробленим посиланням і підтвердження даних облікового запису через ввід паролю. Для цього створюється сайт, який буде майже не відрізнятись від справжнього (рис. 5).

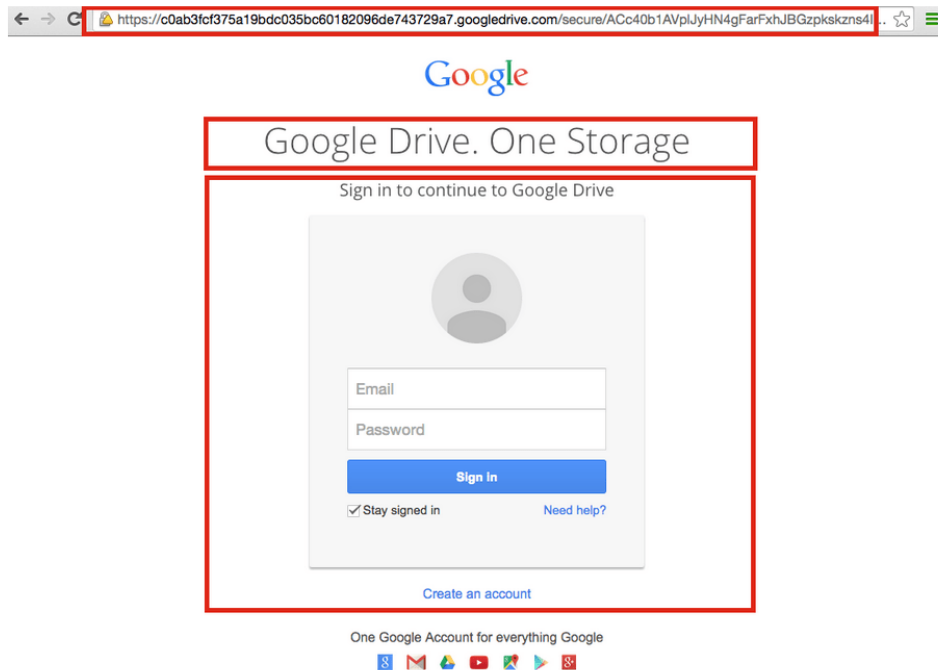


Рис. 5. Підроблений сайт автентифікації Google

Одержавши ваші конфіденційні дані, злочинець отримає доступ до облікового запису та зможе завантажити цікаву йому інформацію або скористатись ним для наступного етапу атаки (наприклад, на вашу установу).

Додатковим рівнем захисту у цьому випадку буде другий фактор автентифікації. Адже якщо злодій отримає ваші дані для входу, йому буде необхідно ще мати секретний код, який генерується на вашому телефоні. Інформація про фішингову атаку.

«14.02.2018 відбулась фішингова розсилка з електронної адреси otkachenko@me.gov.ua з темою повідомлення «Нарада» та прикріпленими шкідливими файлами – 28.02.docx.exe. При відкритті файлу запускався шкідливий код Schwarze-Sonne-Remote-Access-Trojan. Цей процес зв'язувався з центром, який віддалено отримував команди від сервера – gordon6.hopto.org»

2. Руйнування комп'ютерної системи/мережі організації.

Зловмисник надсилає листа і видає себе за авторитетне джерело. Його мета – щоб ви запустили файл у вкладенні.

Як тільки ви відкриєте файл, почнеться процес шифрування файлів системи з метою подальшого вимагання грошового викупу за ключі відновлення файлів.

Маючи доступ до вашого комп'ютера, зловмисники можуть спробувати також отримати доступ до інших комп'ютерних систем, які знаходяться в одній з вами мережі. Вони зацікавлені у заробітку: чим більше шифрують, тим більше вимагають (рис. 6).

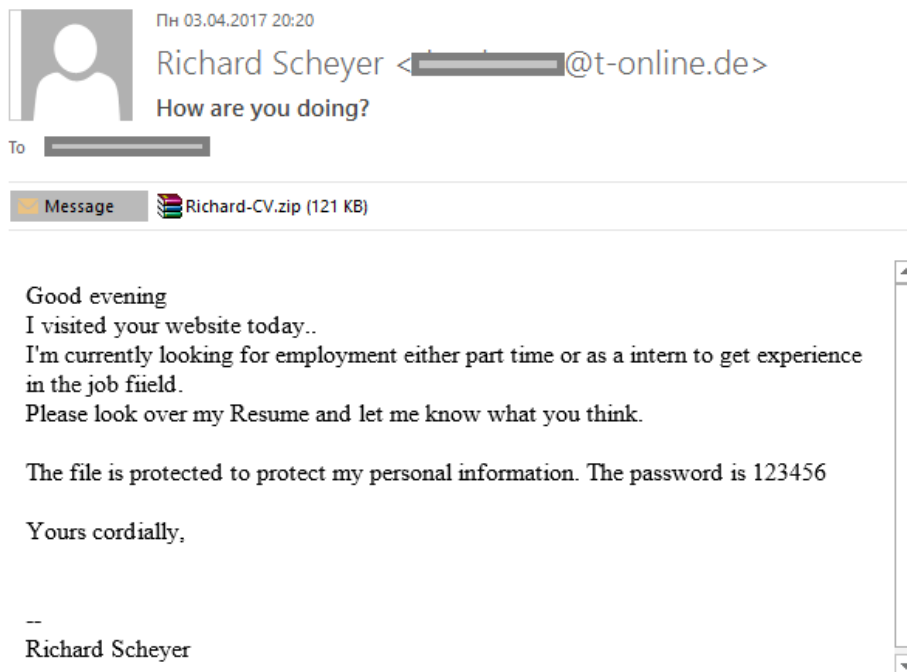


Рис. 6. Приклад листа із шкідливим вкладенням

3. Отримання віддаленого доступу до комп'ютера.

У 2015 році група хакерів надіслала електронного листа українським енергетичним компаніям з файлом Excel у додатку, видаючи себе за легітимне джерело. При відкритті того файлу відбувалось зараження комп'ютера, що надавало хакерам віддалений доступ для управління системою (рис. 7).

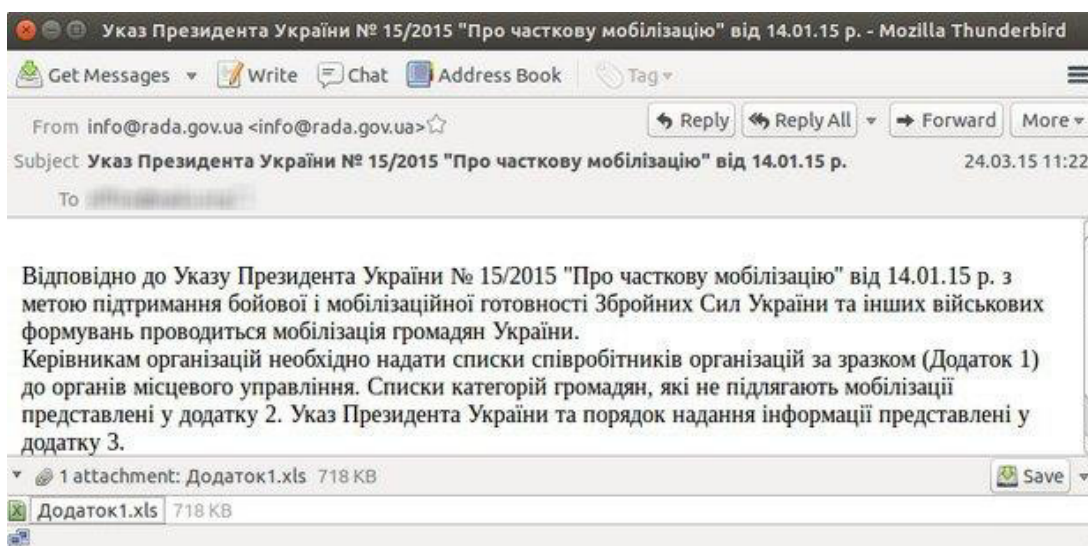


Рис. 7. Лист із ШПЗ

Злочинцям вдалось віддалено вплинути на роботу систем, а результатом цієї атаки стало:

- ▶ щодо «Прикарпаттяобленерго»: вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин;
- ▶ щодо «Київобленерго»: відключено 30 вузлових підстанцій, від яких живиться низка стратегічних об'єктів, понад 80 тисяч споживачів були без електрики протягом однієї-трьох годин.

Кіберзлочинці надсилають фішингові листи з метою:

- отримання доступу до облікового запису;
- шифрування файлів системи комп'ютера;
- отримання віддаленого доступу.

Як відрізнати легітимні листи від фішингових?

Переважна більшість фішингових листів є неочікуваними для отримувача. Перш ніж довіряти листу, необхідно здійснити аналіз заголовків (метаданих), змісту і вкладень листа.

Аналіз метаданих.

1. Звернути увагу на ім'я відправника, але воно може бути будь-яким, його легко підробити (рис. 8).

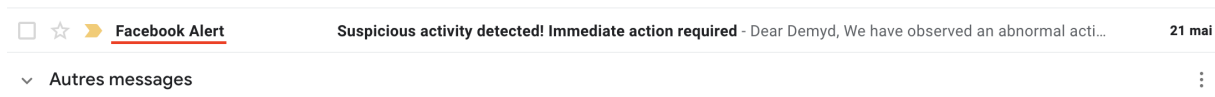


Рис. 8. Сумнівне ім'я відправника листа

2. Повідомлення, що закликає до швидких і термінових дій є індикатором фішингу, наприклад: «Вас зламали! Швидше поміняйте пароль за наданим посиланням».
3. Проаналізуйте правильність написання доменного імені відправника. Кіберзлочинці часто підмінюють літери/символи, щоб замаскуватись під авторитетне джерело. Так, accounts-google.com маскується під accounts.google.com

У період президентських виборів у США 2016 року для проведення фішинг-атаки на базі схожих доменів зловмисники використали сайт **«accounts-google.com»** як клону сайту **«accounts.google.com»**.

Іноді доменне ім'я відправника взагалі не маскується під легітимне (рис. 9).

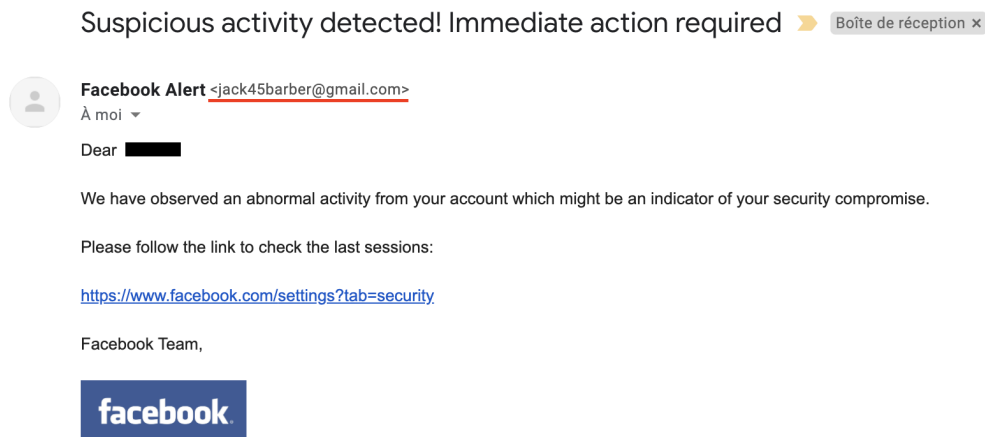


Рис. 9. Нерелевантне доменне ім'я відправника

Аналіз змісту повідомлення.

1. Звернути увагу на звернення: якщо використовуються загальні фрази «Шановні колеги», «Шановний клієнте» тощо, то у більшості випадків це – ознака фішингу (рис. 10). Злочинець може вказати ваше ім'я, тоді атаку можна вважати підготовленою спеціально під вас.

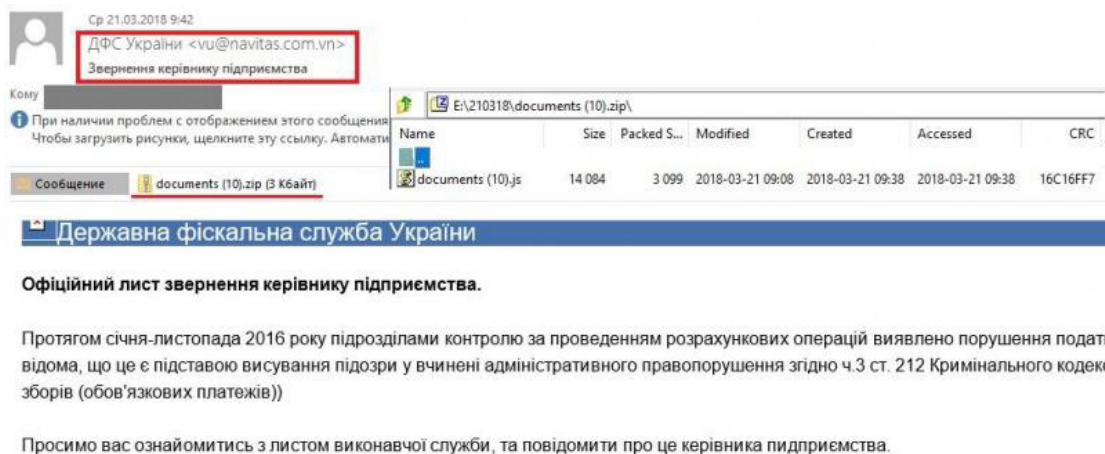


Рис. 10. Загальне звернення у листі

2. Невідповідна налаштуванням акаунту мова та наявність граматичних/орфографічних помилок є індикатором фішингового листа. Наприклад, Google надсилає листи, що стосуються облікового запису, мовою інтерфейсу цього запису. Тобто, якщо у вас інтерфейс українською мовою, а лист прийшов російською, це – серйозна причина задуматися.
3. Якщо файл у вкладенні зашифрований (архівований з паролем), а пароль зазначений у листі, то, скоріш за все, файл є шкідливим. Антивірусні системи поштових сервісів в цьому випадку не можуть виявити наявність ШПЗ у листі.

4. Необхідно здійснити аналіз активних посилань у листі. Обережно навести мишкою на посилання (не натискаючи) та потримати кілька секунд. У лівому куті буде відображено дійсне посилання (рис. 11).

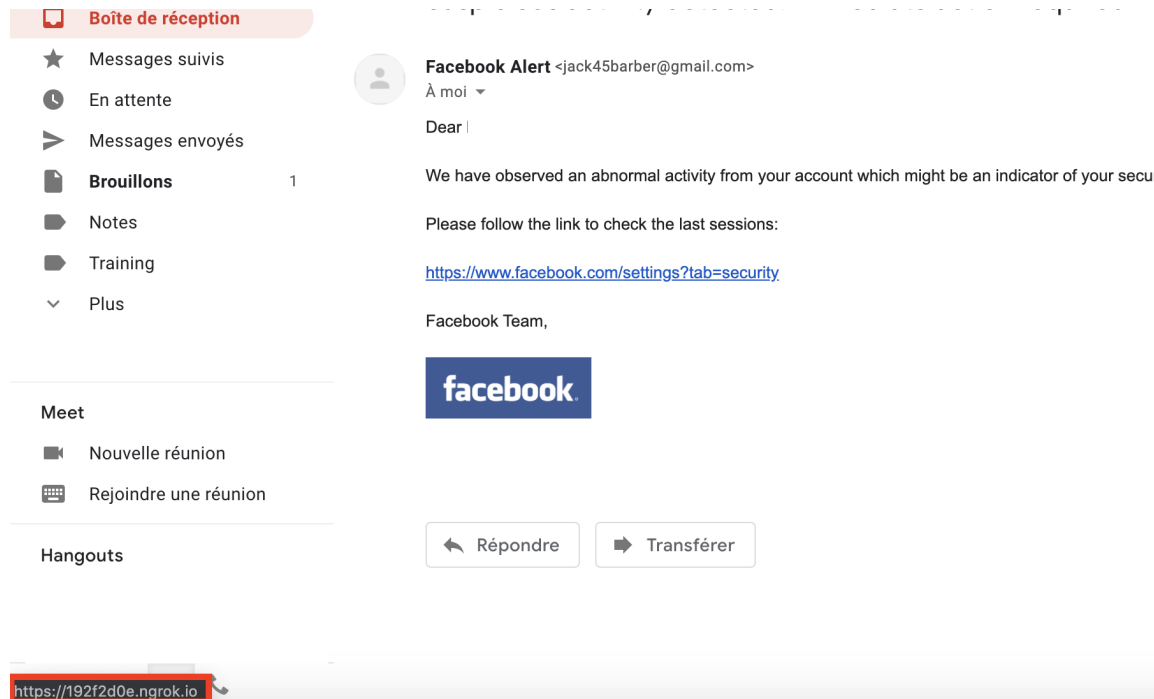


Рис. 11. Аналіз активного посилання у листі

Важливо!!!

Посилання такого вигляду `accounts.google.com.evilwebsite.pe/EditPasswd` також шахрайське, бо адреса має починатися з `accounts.google.com/` (тобто, після `.com` мусить бути `/`, а не крапка).

Аналіз вкладення.

Перелічені нижче файли можуть виконувати код в системі при їх відкритті і становити небезпеку:

- ▶ будь-які виконувані файли: EXE, COM, CMD, BAT, PS1, SWF, JAR, JS, VBS тощо;
- ▶ файли MS Office, особливо з макросами: DOC/DOCX/DOCM, XLS/XSLX/XLSM тощо;
- ▶ файли PDF;
- ▶ файли векторної графіки з вбудованим кодом: SVG;
- ▶ файли архівів, особливо з паролем: RAR, ZIP, 7Z тощо.

Висновки

Рекомендації із забезпечення поштового акаунту:

- ▶ використовувати складний пароль:
 - містить маленькі й великі літери, спеціальні символи та цифри, довжиною не менше 8-10 символів
 - перевірити складність паролю, який буде схожий на ваш: passwordmonster.com, www.security.org/how-secure-is-my-password;
 - не словникове слово, навіть модифіковане. Поганий пароль: rockandroll123. Складний пароль: T@8l3S0bk4hA7;
- ▶ зберігати складні паролі у пароліних менеджерах;
- ▶ встановлювати двофакторну автентифікацію або passkey¹³;
- ▶ не відкривати вкладені файли, не переконавшись у їхньому походженні:
 - для перевірки можна використовувати [virustotal.com](https://www.virustotal.com) (в цьому випадку ви надаєте доступ до файлу третім особам);
- ▶ використовувати додатковий канал комунікації з тим, аби перевірити, чи дійсно надсилали вам цей лист (наприклад, за допомогою телефону, месенджера тощо);
- ▶ не використовувати службову пошту в особистих цілях;
- ▶ виходити з сеансу облікового запису;
- ▶ якщо у листі є скорочені посилання (<https://bit.ly/xxxxxx>), перевірити їх можна через сервіси checkshorturl.com, expandurl.net.

Якщо все ж таки перейшли за посиланням у фішинговому листі, тоді:

- ▶ швидше змініть пароль;
- ▶ перегляньте відкриті сесії та закрийте ті, які вам не належать;
- ▶ зверніться до відділу IT-технологій.

Якщо відкрили вкладений файл і зрозуміли, що це був фішинг, тоді:

- 1) вимкніть комп'ютер;
- 2) зверніться до відділу IT-технологій.

¹³ [https://en.wikipedia.org/wiki/Passkey_\(authentication\)](https://en.wikipedia.org/wiki/Passkey_(authentication)).

Безпека користування соціальними мережами

План лекції

Вступ

1. Правила реєстрації
2. Правила парольної безпеки
3. Конфіденційність даних

Висновки

Рекомендована література

Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: <https://univd.edu.ua/science-issue/issue/4315>.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К. : ВАІТЕ, 2021. 262 с.

Допоміжна

5. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 72–73.
6. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 65–67.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: <https://osvita.diia.gov.ua/courses/cyber-hygiene>.

Текст лекції

Вступ

Соціальні мережі, такі як Facebook, LinkedIn, Instagram, TikTok або Snapchat, дозволяють вам ділитися особистою інформацією, спілкуючись з друзями, партнерами і колегами по всьому світу. Хоча мережі дозволяють вам залишатися на зв'язку, ви наражаєтеся на ризик того, що зловмисники можуть дізнатися, де ви, що ви робите, чим ви володієте, а також іншу інформацію.

Безпека і соціальні мережі – речі, на перший погляд, якщо не протилежні, то точно ледь сумісні. Реєструючись у соціальній мережі, користувачі, за рідкісними винятками, не дотримуються анонімності. Ми ділимося фотографіями, уподобаннями в музиці, підписками на сторінки – все це є елементами «профайлу», за якими нас знайдуть друзі й знайомі ... і маркетологи. А отже, всю цю інформацію можна продати.

Проблема в тому, що багато власників сервісів за гроші нададуть не лише інформацію про товари, які ви шукали онлайн, а і більшість особистих даних. Так що інформацію, яку ви не готові афішувати на весь світ, не можна завантажувати в соціальні мережі зовсім: ані в закриті альбоми, ані в особисті повідомлення – нікуди.

У березні 2018 року стало відомо, що британська аналітична компанія «Cambridge Analytica» збирала дані користувачів через свій додаток у Facebook і використовувала для розміщення політичної реклами, зокрема під час президентської кампанії в США і референдуму про вихід Великобританії з Євросоюзу в 2016 році. Втручання в цілому могло торкнутися 87 млн користувачів соцмережі. «Cambridge Analytica» заперечувала свою провину, стверджуючи, що це був звичайний і законний збір даних для онлайн-реклами. Потім компанія втратила всіх клієнтів і оголосила про банкрутство. Засновник соцмережі Марк Цукерберг визнав помилку, зазначивши, що у Facebook зробили недостатньо для запобігання використанню її функціоналу на шкоду. Facebook було оштрафовано більш ніж на 5 млрд дол. США.

Тож далі розглянемо, як варто поводитися онлайн у соціальних мережах, щоб не стати або жертвою зловмисників, або «елементом статистики».

1. Правила реєстрації

Ви хочете використовувати своє справжнє ім'я? Деякі мережі раніше дотримувалися «політики справжніх імен», але з часом послабили вимоги. Якщо вам не хочеться використовувати своє справжнє ім'я в соціальних мережах, можете цього не робити.



Під час реєстрації не надавайте більше інформації, ніж потрібно. Якщо ви хочете зберегти свої контактні дані, використовуйте окрему, спеціально створену адресу електронної пошти і не вказуйте свій номер телефону. Основна адреса пошти і номер телефону можуть розкрити вашу особистість і зв'язати вас з іншими обліковими записами.

Будьте обережні, вибираючи фото профілю або інші зображення, які ви завантажуєте. Мало того, що в метаданих файлу може бути вказане місце і час зйомки, власне зображення може також розкрити будь-яку інформацію про вас. Поставте собі питання перед завантаженням зображення: фото було знято поза межами дому або роботи? Чи видно покажчики з назвою вулиць або інші знаки і вивіски? Чи не видно робочих документів або змісту екрану комп'ютера?

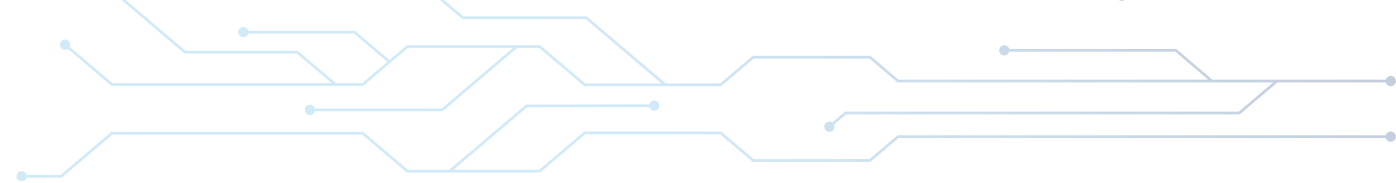
Не слід правильно відповідати на питання для відновлення доступу до облікового запису («В якому місті ви народилися?» або «Яке ім'я вашої домашньої тварини?»), оскільки відповіді на такі питання можуть бути знайдені за допомогою загальнодоступних даних ваших акаунтів у соціальних мережах. Ви можете вказати довільні відповіді на ці питання. Запам'ятати ці відповіді буде важкувато, тому їх можна записати в окремому місці або зберігати за допомогою менеджера паролів.

2. Правила парольної безпеки

Захистіть ваш обліковий запис надійним паролем. Надійні паролі довгі, складні та унікальні. Це означає, що вони повинні бути довше 10–16 символів, містити різні типи символів (великі й маленькі літери, цифри, спеціальні символи) та бути різними для кожного облікового запису та системи. Паролі не повинні бути засновані на простих словах, які можна знайти в словниках. Паролі не повинні бути когнітивними – це означає, що вони не повинні бути засновані на даних про вас, що їх можна знайти у вашому ж обліковому записі! Дату народження, ім'я близької людини, кличку собаки та іншу доступну інформацію не варто використовувати як складові паролю. Краще використовуйте парольні фрази, щоб уникнути проблем зі слабкими паролями.

Оберіть фразу, яку ви не зможете легко забути в наступні 2–3 дні: рядок з вірша або пісні, прислів'я, гасло тощо. Потім трансформуйте цю фразу у єдине «слово», видаливши пробіли та замінивши деякі літери схожими на них цифрами або спецсимволами: А->4, В->8, С->3, Е->3, І->1, L->7, S->5, T->7 тощо. Додавання цифр та спецсимволів, а також переведення деяких букв у верхній регістр зроблять парольну фразу ще сильнішою.

Ніхто, крім вас, не повинен знати ваші паролі та парольні фрази. Не розказуйте їх нікому, навіть дружині, батькам, дітям. Ніколи не записуйте ваші паролі



та паролні фрази на папері або в незашифрованому файлі. Захищений паролем файл Excel – це не шифрування. Архів, захищений паролем, не є належним шифруванням. Використовуйте надійні паролні менеджери.

Прикладами надійних паролних менеджерів є:

- ▶ 1Password: <https://1password.com> (платний);
- ▶ Bitwarden: <https://bitwarden.com> (безкоштовний);
- ▶ Dashlane: <https://www.dashlane.com/> (безкоштовний з обмеженнями);
- ▶ KeePassXC: <https://keepassxc.org/> (безкоштовний).

Змінюйте паролі та паролні фрази на регулярній основі та принаймні один раз на рік. Паролі та паролні фрази, які ви використовуєте найчастіше (наприклад, кілька разів на день), повинні змінюватися принаймні щомісячно або раз на два місяці.

3. Конфіденційність даних

Інформація, що зберігається третьою стороною, захищена її власною політикою конфіденційності й може бути використана в комерційних цілях та навіть передана іншим компаніям (наприклад, маркетинговим). Оскільки читання всієї політики конфіденційності – майже непосильне завдання для будь-якої людини, спробуйте ознайомитися лише з розділом, у якому йдеться про те, як використовуються ваші дані, в яких випадках дані можуть бути передані кому-небудь ще, а також як компанія реагує на запити правоохоронних органів.

Сайти соціальних мереж – це, в основному, бізнес, зосереджений на отриманні прибутку. Вони часто збирають конфіденційну інформацію, крім наданої вами: де ви перебуваєте, які ваші інтереси і переваги, на яку рекламу ви реагуєте, які сайти ви відвідуєте (за допомогою кнопок «Like»). Ви можете використати розширення (плагін) браузера з блокуванням стеження для запобігання пасивної передачі зайвої інформації стороннім сайтам.

Головна порада: змініть налаштування за замовчуванням. Наприклад, чи хочете ви ділитися своїми публікаціями з усіма або тільки з будь-якою конкретною групою людей? Чи можна дозволити людям шукати вас за номером телефону або адресою електронної пошти? Чи хочете ви публікувати своє місце розташування в автоматичному режимі?

Незважаючи на те, що на кожній платформі соціальних мереж є свої унікальні налаштування, ви можете помітити деяку схожість.

Налаштування конфіденційності надають відповідь на питання: «Хто може це бачити?» Тут ви зможете вибрати аудиторію («Всі», «Друзі друзів», «Тільки



друзі» тощо) для своїх публікацій, розташування, фотографій, контактної інформації, міток і тих, хто може знайти ваш профіль через пошук.

Налаштування безпеки будуть пов'язані з можливістю блокування інших облікових записів і способів оповіщення про спроби неавторизованого доступу до вашого профілю. Іноді в цьому розділі будуть присутні налаштування входу до акаунту: наприклад, включення двофакторної автентифікації та резервна адреса електронної пошти/номер телефону.

Скористайтеся «перевірками» налаштувань безпеки і конфіденційності. Facebook, Twitter і багато інших веб-сайтів пропонують провести «перевірку налаштувань безпеки» облікового запису. Ці перевірки є чудовими покроковими настановами, описаними простою мовою. Вони дуже добре допомагають вам відповідним чином налаштувати безпеку і конфіденційність свого облікового запису.

Пам'ятайте, що налаштування конфіденційності можуть змінитися. Іноді вони можуть ставати більш надійними і докладними, а іноді – навпаки. Звертайте увагу на ці зміни: раптом інформація, раніше конфіденційна, стала вже відкритою для всіх, або нові додаткові налаштування дозволять краще контролювати рівень вашої конфіденційності?

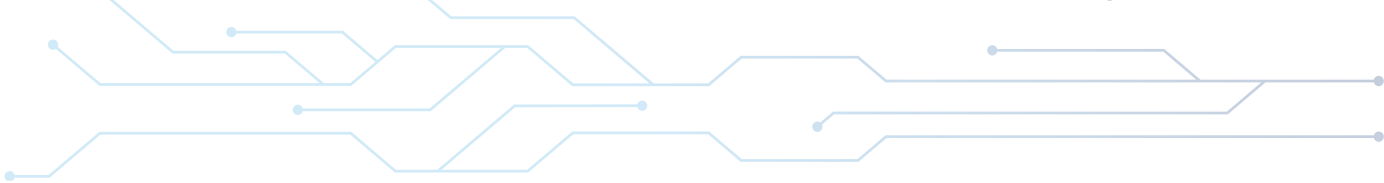
Ось посилання на налаштування безпеки для найпопулярніших соціальних мереж:

- ▶ Facebook: <https://www.facebook.com/settings?tab=security§ion=ap-provals>;
- ▶ Twitter: <https://twitter.com/settings/security>.

Пам'ятайте, що більшість сучасних онлайн-сервісів підтримують двофакторну автентифікацію. Увімкніть її за допомогою програмного коду (доступний у Facebook, Twitter тощо) або за допомогою одноразового паролю з SMS. Надавайте перевагу використанню Google Authenticator, фізичного токена, або перевірці за допомогою мобільного додатку. Використання одноразових кодів через SMS менш безпечно.

Більше інформації про двофакторну автентифікацію тут:
<https://twofactorauth.org/>.

Не використовуйте сторінку в соціальній мережі для реєстрації на сайтах, які запитують доступ до вашої особистої інформації та інформації про ваших друзів. Багато сайтів зараз пропонують авторизуватися через соцмережі, щоб проголосувати в опитуванні, залишити коментар або дізнатися результати якого-небудь тесту. Побережіть дані, обійдіться без інформації про те, яким є ваш психологічний вік або хто ви з героїв «Гаррі Поттера».



Крім того, не анонсуйте на сторінці свої плани. Інформацією про те, що ви найближчими вихідними збираєтеся в іншу країну, можуть скористатися квартирні крадії.

Пам'ятайте: все, що ви публікуєте, може бути використано проти вас!

Чим більше інформації ви публікуєте про своє особисте життя, тим легше зловмиснику підготувати атаку проти вас. Наприклад, якщо ви публікуєте багато інформації про свою родину, захоплення або про майбутню відпустку чи робочу поїздку, зловмисник може зібрати всі ці конкретні дані й створити фішингового електронного листа або зробити телефонний дзвінок, спеціально призначений для вас.

Якщо ви напишете, що серед ваших уподобань є випікання, зловмисник може створити фішинговий лист зі спеціальною рекламою нового набору мисок. До цього електронного листа він може додати вкладення з купоном на 50% знижки на купівлю продукції вашого улюбленого бренду для випікання. **Якщо пропозиція здається занадто гарною, щоб бути правдою, це, ймовірно, шахрайство.**

Крім того, щоб забезпечити безпеку вашого роботодавця, ніколи, з жодної причини не розміщуйте конфіденційну інформацію про вашу роботу в Інтернеті. Завжди звертайте увагу на те, що ви публікуєте і чим ділитесь на своїй сторінці. Слідкуйте за коментарями. Йдеться не тільки про коментарі, які ви залишаєте на інших ресурсах, а й про коментарі, що їх інші залишають на вашій сторінці. Іноді найгіршого удару по онлайн-репутації посадової особи завдають не злами і «зливи» даних, а необдумані жарти, в яких хтось може побачити грубість або необережні висловлювання ваших же друзів.

Як і фішингові атаки електронною поштою, кіберзловмисники можуть спробувати обдурити вас у соціальних мережах. Поширений метод атаки: злочинець отримує доступ до облікового запису в соціальній мережі, наприклад, вашого колеги. Потім він може відправити вам терміновий запит, що його пограбували або він застряг під час відпустки й потрібні гроші, які він просить відправити йому прямо зараз.

Якщо ви отримуєте будь-які дивні або підозрілі повідомлення від колеги, друга або знайомого, дійте обачно і будьте обережні з відповіддю. Не відповідайте безпосередньо через обліковий запис у соціальних мережах. Замість цього зателефонуйте своєму другові по телефону, щоб підтвердити, чи дійсно він опублікував повідомлення і потребує вашої допомоги.

Закінчення користування

Чи зможете ви згадати, скільки і в яких соціальних мережах ви створювали облікових записів? А яка частина з них залишаються покинутими через



забутий пароль? Зі зростанням популярності соцмереж кожен такий акаунт може становити інтерес для зловмисників.

Отримавши доступ до покинутого акаунту, можна використовувати його для дискредитації вас, опублікувати рекламну – і не тільки – інформацію.

Щоб уникнути цього, не забувайте про свої старі облікові записи – видаляйте, за можливості, або хоча б блокуйте їх. А якщо не маєте доступу, спробуйте звернутись до служб технічної підтримки по допомогу. Іноді це може спрацювати!

Висновки

І, наостанок, згадайте, що ви – офіційна особа, і навіть якщо обліковий запис ваш особистий, все одно у користувачів буде до нього інше ставлення.

Реагування на інциденти безпеки інформації

План лекції

Вступ

1. Система управління інформаційною безпекою
2. Управління інцидентами інформаційної безпеки
3. Реагування на інциденти інформаційної безпеки

Висновки

Рекомендована література

Основна

1. Манжай О.В., Мелешко Д.Г., Носов В.В., Самойлов С.В. Навчальний посібник для учасників тренінгу «Розробка та впровадження системи управління безпекою інформації». К.: ВАІТЕ, 2021. 138 с.

Допоміжна

2. ДСТУ ISO/IEC 27035-1:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами (ISO/IEC 27035-1:2016, IDT).
3. ДСТУ ISO/IEC 27035-2:2018 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2016, IDT).
4. NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling. Guide Recommendations of the National Institute of Standards and Technology. 79 p. (Aug. 2012).

Інформаційні ресурси в Інтернеті

5. <http://dx.doi.org/10.6028/NIST.SP.800-61r2>.
6. <https://www.enisa.europa.eu/topics/incident-response>.
7. <https://learn.microsoft.com/en-us/security/operations/incident-response-overview>.
8. <https://www.techtarget.com/searchsecurity/tip/Incident-response-best-practices-for-your-organization>.
9. <https://www.incidentresponse.org/playbooks/>.

Текст лекції

Вступ

Реалізація загроз (ризиків) інформаційної безпеки через наявні вразливості інформаційних систем призводить до впливу на інформаційні активи, що забезпечують діяльність організації, і при цьому система захисту інформації або система управління інформаційною безпекою має фіксувати події, які можуть бути кваліфіковані як інциденти інформаційної безпеки, що впливають на інформаційну діяльність організації (рис. 1).

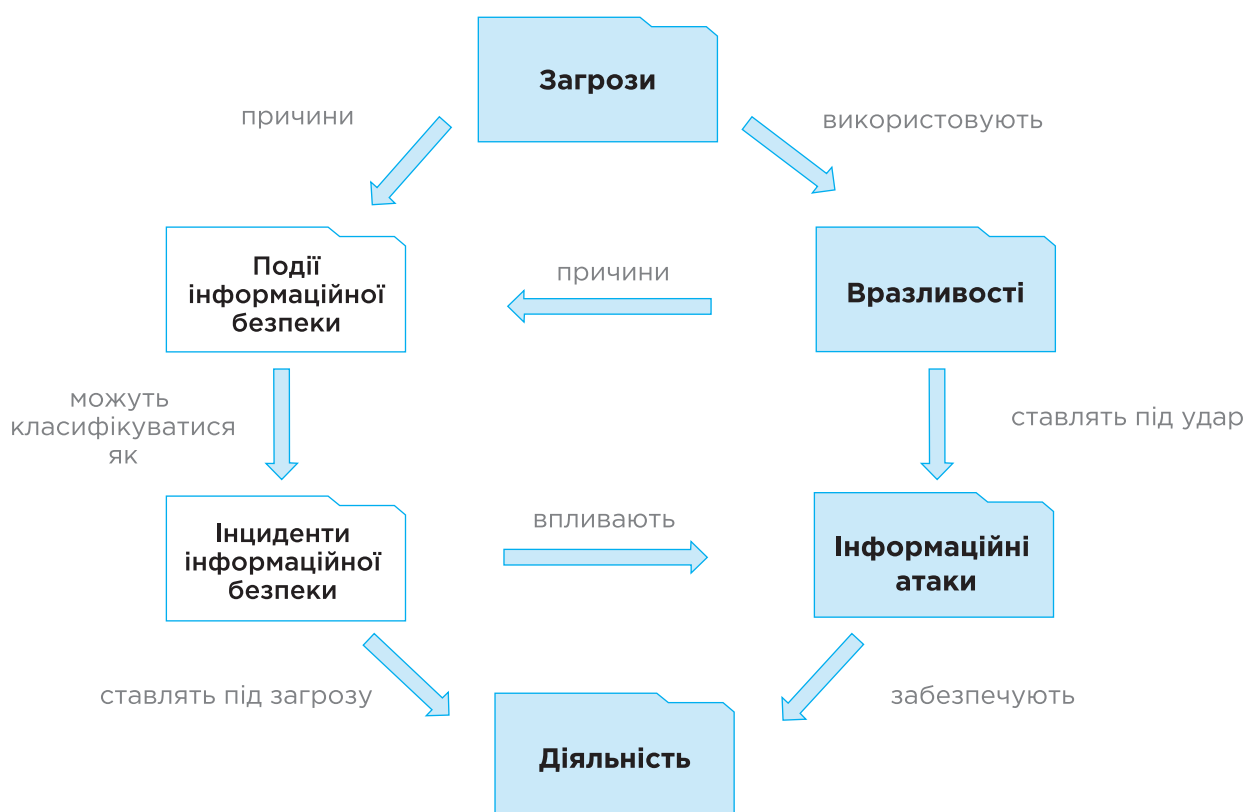
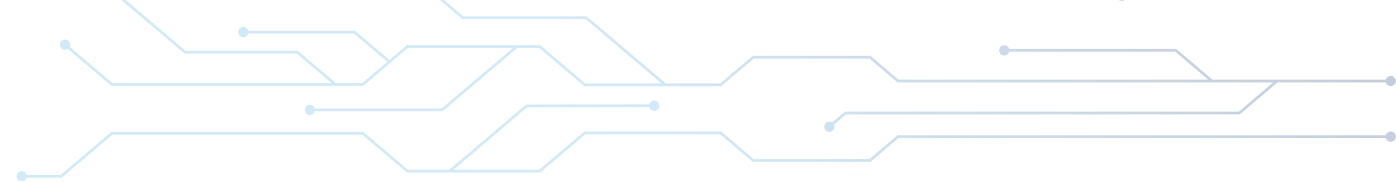


Рис. 1. Взаємозв'язок понять при виникненні інцидентів інформаційної безпеки за ДСТУ ISO/IEC 27035-1:2018

Реагування на інциденти інформаційної безпеки як системний процес є складовою системи управління інформаційною безпекою.

1. Система управління інформаційною безпекою

Закон України «Про захист інформації в інформаційно-комунікаційних системах» в ч. 2 ст. 8 визначає як умову обробки державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, застосування *комплексної системи захисту інформації* з підтвердженою відповідністю.



Відповідно до ч. 4 ст. 8 цього Закону державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі **без** застосування комплексної системи захисту інформації у разі виконання **всіх** таких умов:

- ▶ підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності;
- ▶ використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації;
- ▶ жоден з елементів системи не може бути розташований на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та на територіях держав, які входять до митних союзів з такими державами;
- ▶ виконання особливих вимог, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, що обробляються.

Серія стандартів ДСТУ ISO/IEC 27xxx регламентує побудову та підтримання функціонування систем управління інформаційної безпеки (СУІБ).

Етапи побудови СУІБ у загальному вигляді можна представити так:

- ▶ визначення сфери дії СУІБ;
- ▶ попередня перевірка відповідності системи безпеки організації вимогам стандарту ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги». На цьому етапі можуть бути застосовані й інші стандарти, у тому числі ДСТУ ISO/IEC 27004:2018 «Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання»;

- 
- ▶ оцінка ризиків інформаційної безпеки, де основою для вибору відповідної методики є стандарт ДСТУ ISO/IEC 27005:2019 «Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки»;
 - ▶ опис процедур та їх документування. На цьому етапі описуються процеси у сфері управління та забезпечення безпеки, які потрібно виконати, а також формується відповідна документація;
 - ▶ впровадження процедур та відповідної документації;
 - ▶ дослідна експлуатація СУІБ;
 - ▶ сертифікація, яка проводиться у формі аудиту, за результатами якого організація має отримати сертифікат про відповідність СУІБ вимогам ДСТУ ISO/IEC 27001:2015.

Для управління інформаційною безпекою у випадках реалізації ризиків, які призвели до виникнення інцидентів, з метою ефективного відновлення інформаційної безпеки, поширення інформації про події безпеки та слабкі місця (вразливості) згідно з ДСТУ ISO/IEC 27002:2015 необхідно впровадження підсистеми **управління інцидентами інформаційної безпеки та вдосконалення СУІБ**.

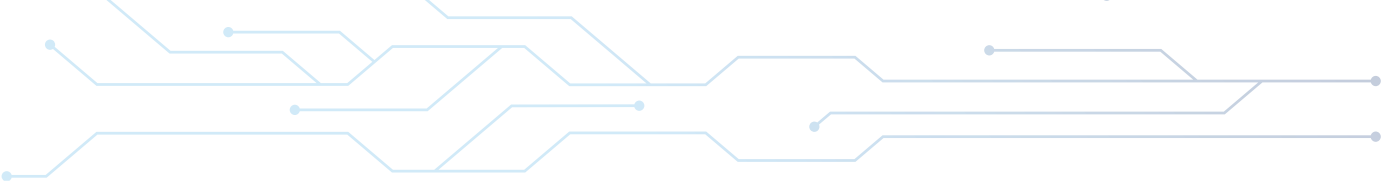
2. Управління інцидентами інформаційної безпеки

Реагування на інциденти інформаційної безпеки здійснюється в рамках управління інцидентами інформаційної безпеки та вдосконалення СУІБ, що передбачає наступні заходи безпеки:

- а) визначення відповідальності керівництва організації та процедур реагування на інциденти інформаційної безпеки;
- б) звітування про події інформаційної безпеки;
- в) звітування щодо виявлених недоліків та вразливостей системи інформаційної безпеки;
- г) оцінка подій інформаційної безпеки та прийняття рішень стосовно віднесення їх до інцидентів інформаційної безпеки;
- д) реагування на інциденти інформаційної безпеки відповідно до встановлених процедур;
- е) аналіз і зіставлення інцидентів інформаційної безпеки для визначення потреб у вдосконаленні або впровадженні додаткових заходів безпеки СУІБ;
- ж) ідентифікація, збирання, отримання і зберігання доказів для притягнення винних до різних видів юридичної відповідальності.

Визначення відповідальності керівництва щодо управління інцидентами інформаційної безпеки потрібно для забезпечення **розроблення та поширення** належним чином всередині організації **процедур**:

- 1) планування та підготовки реагування на інцидент;
- 2) моніторингу, виявлення, аналізу та звітування про події та інциденти інформаційної безпеки;

- 
- 3) реєстрації діяльності щодо управління інцидентами;
 - 4) збирання про інциденти інформації, яка може бути визнана в судовому процесі як доказ;
 - 5) оцінювання й прийняття рішення щодо подій інформаційної безпеки та оцінювання слабких місць інформаційної безпеки;
 - 6) реагування на інцидент, відновлення після інциденту, інформування зацікавлених сторін.

Визначені **процедури реагування на інциденти інформаційної безпеки** мають забезпечувати, що:

- 1) компетентний персонал всередині організації може реагувати на інциденти інформаційної безпеки;
- 2) запроваджена точка контакту (інформаційний канал) для звітування про виявлені інциденти інформаційної безпеки;
- 3) підтримуються відповідні комунікації з регуляторними органами та зовнішніми групами (центрами) з аналізу інцидентів інформаційної безпеки.

Процедури звітування мають включати:

- 1) шаблони звітів про події інформаційної безпеки;
- 2) процедури негайного реагування в разі події інформаційної безпеки, наприклад:
 - а) реєстрація типу події: порушення чи відмова;
 - б) реєстрація повідомлення на екрані;
 - в) негайна реєстрація в точці контакту і тому подібне;
- 3) посилання на порядок дисциплінарного провадження стосовно працівників, які вчинили порушення безпеки;
- 4) порядок доведення до працівників, які повідомили про подію інформаційної безпеки, результатів реагування та аналізу події.

Звітування про події інформаційної безпеки повинно здійснюватися через визначені належні канали управління. Всі працівники організації та підрядники повинні бути поінформовані про їх відповідальність щодо як-найшвидшого звітування про будь-які події інформаційної безпеки через точку контакту за визначеними процедурами.

Подіями інформаційної безпеки, що потребують звітування, є:

- а) неефективність заходів безпеки;
- б) порушення цілісності, конфіденційності або очікуваної доступності;
- в) людські помилки;
- г) невідповідності політиці чи настановам;
- д) порушення заходів фізичної безпеки;
- е) несанкціоновані зміни системи;
- ж) збій програмного забезпечення чи апаратних засобів;
- з) порушення доступу.



Звітуванню також підлягають будь-які виявлені або очікувані слабкі (вразливі) місця у системах чи послугах, що, відповідно, є **слабкими місцями інформаційної безпеки**. Процес звітування має бути якомога простішим, доступнішим і досяжним.

Необхідно попередити працівників та підрядників про заборону тестування слабких місць і розцінювання таких дій як потенційне зловживання системою, що тягне юридичну відповідальність.

Події інформаційної безпеки, інформація про які надходить через відповідну точку (місце) контакту до окремої команди реагування на інциденти інформаційної безпеки (ISIRT), мають бути **оцінені** за допомогою попередньо узгодженої кваліфікації **та прийнято рішення** стосовно **віднесення їх до інцидентів інформаційної безпеки**. Кваліфікація та пріоритизація подій і інцидентів допоможе оцінити їх вплив на стан безпеки організації. Результати оцінювання та прийняття рішення мають бути докладно записані для подальшої їх перевірки й посилання на них.

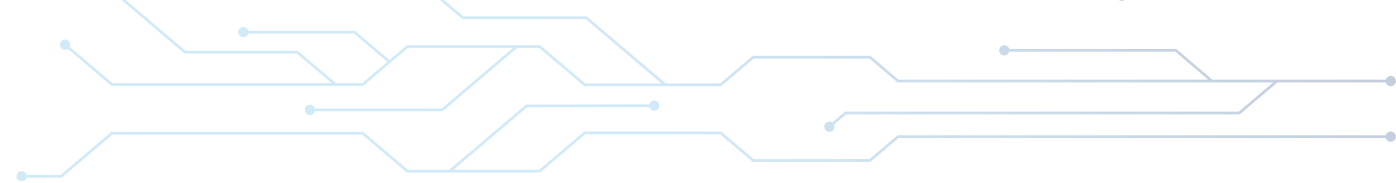
Реагування на інциденти інформаційної безпеки має здійснюватися відповідно до визначених процедур і включати:

- a) якнайшвидше збирання доказової інформації (цифрових слідів) для встановлення фактичних обставин та наслідків події;
- b) за потреби – проведення криміналістичного дослідження зібраних доказових даних;
- c) за потреби (якщо інцидент продовжує розвиватися) – ескалацію зусиль щодо зупинки небезпечних подій і відновлення безпеки;
- d) забезпечення документування (реєстрації) всієї діяльності реагування на інцидент інформаційної безпеки;
- e) інформування у визначених межах про існування інциденту всіх зацікавлених сторін, які мають знати про це;
- f) ідентифікацію слабких місць (вразливостей) інформаційної безпеки, які були причиною або сприяли появі інциденту;
- g) формальне закриття та звітування про інцидент по завершенні реагування.

Основною метою реагування на інцидент є повернення до вихідного рівня стану інформаційної безпеки.

Докладні настанови стосовно управління інцидентами інформаційної безпеки викладено в ДСТУ ISO/IEC 27035.

Після формального закінчення реагування на інцидент має бути проведений **аналіз** і зіставлення з іншими інцидентами інформаційної безпеки **для визначення потреб у вдосконаленні** або впровадженні додаткових заходів безпеки СУІБ. Для цього повинні бути механізми, які дозволяють кількісно оцінити й відслідкувати типи, обсяги й вартість інцидентів інформаційної безпеки.



За результатами аналізу інцидентів можна розробити типові сюжети подій інформаційної безпеки організації й використовувати їх у навчанні користувачів з питань безпеки.

Організація повинна **визначити** і при реагуванні на інциденти інформаційної безпеки використовувати **процедури для ідентифікації, збирання, отримання і зберігання інформації, яку можна використовувати як докази** для притягнення до юридичної відповідальності осіб, які вчинили правопорушення у сфері інформаційної безпеки.

Процедури ідентифікації, збирання, отримання і зберігання доказів мають передбачати різні типи інформаційного середовища, обладнання, стану обладнання (наприклад, увімкнено чи вимкнено) і включати питання:

- a) засторог на місці інциденту;
- b) убезпечення потенційних цифрових доказів;
- c) убезпечення персоналу;
- d) ролей та відповідальності персоналу, якого стосуються пов'язані із доказами процеси;
- e) компетентності персоналу, якого стосуються пов'язані із доказами процеси;
- f) хронологічного документування виконуваних дій стосовно потенційних цифрових доказів;
- g) інструктажу персоналу, якого стосуються пов'язані із доказами процеси.

Для посилення значущості й довіри до збережених потенційних цифрових доказів доречно розглянути можливі засоби підтвердження кваліфікації персоналу, наприклад, у вигляді сертифікації.

Потенційні цифрові докази інциденту можуть знаходитися за межами комп'ютерних систем організації та/або в інших юрисдикціях, тому необхідно враховувати вимоги як вітчизняного законодавства, так і інших юрисдикцій щодо повноважень зі збирання та отримання цифрових доказів за межами організації.

При неочевидності правової кваліфікації виявленої події інформаційної безпеки для збереження допустимості й належності в можливому судовому процесі потенційних доказів доцільно одразу залучати до розслідування представника юридичного відділу організації та правоохоронні органи.

Докладно процедури ідентифікації, збирання, отримання та зберігання цифрових доказів описано в настановах ДСТУ ISO/IEC 27037.

Прийняті державні стандарти України, які або безпосередньо регламентують управління інцидентами інформаційної безпеки, або впливають на цю діяльність, зазначені в ДСТУ ISO/IEC 27035-1:2018 через класифікацію фаз процесу розслідування інцидентів (рис. 2).

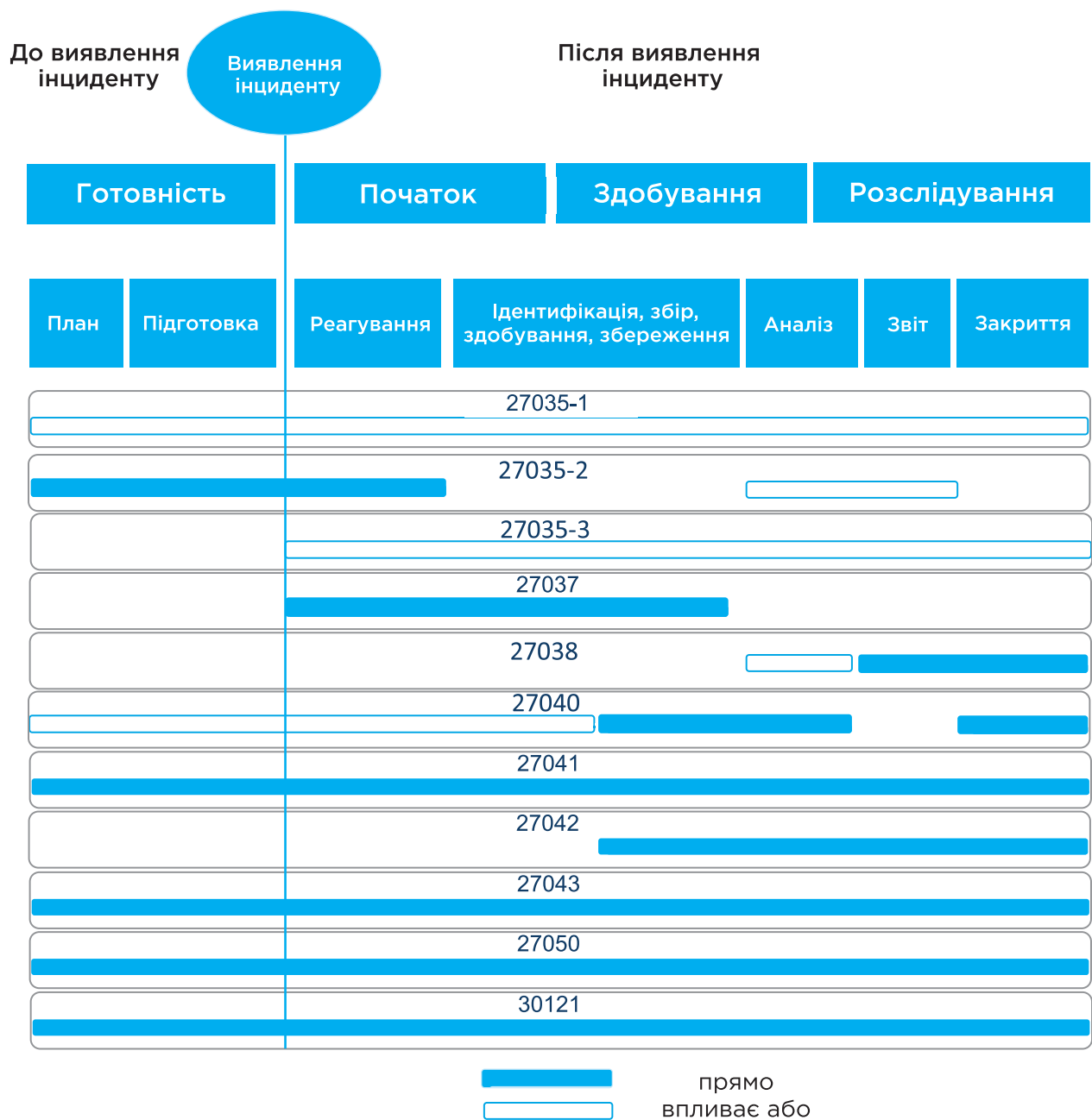


Рис. 2. ДСТУ ISO/IEC, які або безпосередньо регламентують управління інцидентами інформаційної безпеки, або впливають на цю діяльність

3. Реагування на інциденти інформаційної безпеки

Процес реагування на інциденти в кожній організації може відрізнятися залежно від організаційної структури, можливостей і накопиченого досвіду. Під час інциденту важливо наступне.

- **Зберігати спокій.** Інциденти можуть викликати надзвичайні емоції, які можуть завадити діяти відповідним чином. Потрібно зосередитись на слідуванні визначеним процедурам реагування.
- **Не завдавати шкоди.** Необхідно переконатись, що встановлені процедури реагування та їх виконання дозволяє уникнути втрати даних, критично важливих функцій інформаційної системи та доказів. Потрібно уникати дій, які можуть зашкодити відтворенню хронології подій, встановленню причин, а в подальшому – вдосконаленню системи захисту.
- **Залучати юридичний відділ (юриста).** Потрібна юридична кваліфікація інциденту як можливого правопорушення, яке потребує залучення правоохоронних органів і відповідного планування розслідування та процедур відновлення.
- **Обережно оприлюднювати інформацію про інцидент.** Поширення інформації про інцидент можливе тільки після узгодження з юридичним відділом (юристом).
- **За потреби отримувати допомогу.** При складних атаках потрібне залучення фахівців з глибокими знаннями та досвідом.

Слід зосередитися на тому, щоб була готовність до реагування на інциденти, які використовують поширені вектори атак, наприклад:

- **зовнішні/знімні носії.** Атака, що виконується зі знімного носія (наприклад, флешки, компакт-диска) або периферійного пристрою;
- **виснаження.** Атака, яка використовує методи «грубої сили» для компрометації, деградації або знищення систем, мереж або служб;
- **веб.** Атака, що виконується з веб-сайту або веб-додатку;
- **електронна пошта.** Атака, що виконується за допомогою електронного повідомлення або вкладення;
- **неналежне використання.** Будь-який інцидент, спричинений порушенням політики прийнятого використання організації авторизованим користувачем, за винятком вищезазначених категорій;
- **втрата або крадіжка обладнання.** Втрата або крадіжка комп'ютерного пристрою або носія інформації, що використовується організацією, наприклад, ноутбука або смартфона;
- **інше.** Атака, яка не підпадає під жодну з інших категорій.

Процедури реагування розробляються на визначені типи інцидентів інформаційної безпеки для ISIRT і користувачів із задокументованими процесами та пов'язаними з ними обов'язками та розподілом ролей між призначеними особами для виконання різних видів діяльності (окремій особі може бути призначено більше однієї ролі, залежно від розміру, структури та характеру діяльності організації), наприклад, включаючи наступне:

- відключення ураженої системи, служби та/або мережі за певних обставин, що узгоджується за попередньою домовленістю з відповідним керівництвом IT та/або організації;

- 
- ▶ залишення ураженої системи, служби та/або мережі підключеною та працюючою;
 - ▶ моніторинг даних, що надходять від, до та всередині ураженої системи, служби та/або мережі;
 - ▶ активація звичайних процедур резервного копіювання та управління кризами відповідно до політики безпеки системи, служби та/або мережі;
 - ▶ здійснення моніторингу та забезпечення збереження електронних доказів, які потрібні для притягнення винних до дисциплінарної або іншої відповідальності;
 - ▶ повідомлення деталей інциденту інформаційної безпеки визначеним внутрішнім і зовнішнім зацікавленим сторонам, наприклад, іншим групам реагування на інциденти та організаціям, інтернет-провайдерам, постачальникам програмного забезпечення, правоохоронним органам, клієнтам, ЗМІ та ін. Усі контакти та комунікації із зовнішніми сторонами мають бути задокументовані.

Найскладнішою частиною процесу реагування на інциденти є точне виявлення та оцінка можливих інцидентів – визначення того, чи стався інцидент, і якщо так, то який тип, ступінь і масштаб проблеми. Це завдання ускладнюється поєднанням трьох факторів:

- ▶ інциденти можуть бути виявлені за допомогою багатьох різних засобів, з різним рівнем деталізації та точності. Автоматизовані засоби виявлення включають мережеві та хостові системи виявлення вторгнень, антивірусне програмне забезпечення та аналізатори журналів. Про інциденти можуть повідомити користувачі. Деякі інциденти мають явні ознаки, які можна легко виявити, тоді як інші виявити майже неможливо;
- ▶ кількість потенційних ознак інцидентів, як правило, досить велика, наприклад, нерідко від сенсорів виявлення вторгнень надходить тисячі або навіть мільйони сповіщень на день;
- ▶ для ефективного аналізу даних, пов'язаних з інцидентами, необхідні глибокі спеціалізовані технічні знання та досвід.

Ознаки інциденту поділяються на дві категорії: *провісники (precursors)* та *індикатори (indicators)*. **Провісник** – це ознака того, що інцидент може статися в майбутньому. **Індикатор** – це ознака того, що інцидент міг статися або може відбуватися зараз.

Більшість атак не мають жодних провісників, які можна було б ідентифікувати або виявити відносно цілі. Якщо провісники виявлені, організація може запобігти інциденту, змінивши політику безпеки. Прикладами провісників є:

- ▶ записи журналу веб-сервера, які свідчать про використання сканера вразливостей;
- ▶ анонс на спеціалізованих ресурсах нового експлойту, який експлуатує вразливість поштового сервера організації;
- ▶ погрози здійснити атаку на організацію.

У той час, як провісники зустрічаються відносно рідко, індикатори є дуже поширеним явищем. Існує безліч різних індикаторів, серед яких можна зазначити такі:

- ▶ сенсор системи виявлення мережових вторгнень сповіщає про спробу переповнення буфера на сервері бази даних;
- ▶ антивірусне програмне забезпечення сповіщає про виявлення шкідливої програми;
- ▶ системний адміністратор бачить ім'я файлу з незвичними символами;
- ▶ у журналі аудиту з'являється запис зміни конфігурації хосту;
- ▶ у журналі аудиту застосунку зареєстровано кілька невдалих спроб входу з незнайомої віддаленої системи;
- ▶ адміністратор електронної пошти бачить велику кількість заблокованих листів з підозрілим вмістом;
- ▶ мережовий адміністратор помічає незвичне відхилення потоків мережевого трафіку від типових значень.

Основними джерелами провісників і індикаторів є:

- ▶ сповіщення спеціалізованих застосунків (IDPS, SIEM, антивіруси та ін.);
- ▶ записи журналів аудиту застосунків і сервісів операційних систем;
- ▶ мережовий трафік;
- ▶ публічна інформація про знайдені вразливості та розроблені експлойти;
- ▶ звіти внутрішніх користувачів організації та користувачів інших організацій.

Приклад шаблону звіту про події інформаційної безпеки наведений в табл. 1.

Таблиця 1. Шаблон звіту про події інформаційної безпеки

ЗВІТ ПРО ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		
1. Дата події	3. Ідентифікаційні номери відповідної події та/або інциденту (якщо застосовне)	
2. Номер події (надається фахівцем ISIRT)		
4. РЕКВІЗИТИ ОСОБИ, ЯКА ЗВІТУЄ		
4.1. Ім'я та прізвище	4.2. Адреса	
4.3. Організація	4.4. Відділ	
4.5. Телефон	4.6. E-mail	
5. ОПИС ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ		
5.1. Опис події:		
• Що сталося • Яким чином сталося • Чому так сталося • Які компоненти/активи піддалися впливу • Оцінка впливу на діяльність організації • Будь-які виявлені вразливості		

6. ДЕТАЛІ ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

6.1. Дата та час події	
6.2. Дата та час виявлення події	
6.3. Дата та час повідомлення про подію	
6.4. Чи відповідь на цю подію усунула небезпеку?	ТАК ☐ НІ ☐ (позначте відповідне)
6.5. Якщо так, вкажіть, скільки часу тривала подія (у днях/годинах/хвилинах)	

Контрольний список реагування на інцидент (Incident Handling Checklist) у табл. 2 містить основні кроки реагування, які можуть відрізнятися залежно від інциденту. Наприклад, якщо відомо про те, що сталося, на основі аналізу індикаторів (1.1), може і не виникнути необхідності виконувати (1.2) або (1.3)

Таблиця 2. Контрольний список реагування на інцидент

ДІЯ		ВИКОНАНО
ВИЯВЛЕННЯ ТА АНАЛІЗ		
1.	Визначення факту інциденту	
1.1.	Аналіз провісників та індикаторів	
1.2.	Пошук відповідної інформації	
1.3.	Проведення досліджень (наприклад, пошукові системи, база знань)	
1.4.	Якщо має місце інцидент, то розпочати документування, розслідування та збирання доказів	
2.	Визначення пріоритетності реагування на основі відповідних факторів (функціональний і інформаційний вплив, зусилля з відновлення тощо)	
3.	Доведення інформації про інцидент до відповідного внутрішнього персоналу та зовнішніх організацій	
ЛОКАЛІЗАЦІЯ, ЛІКВІДАЦІЯ ТА ВІДНОВЛЕННЯ		
4.	Здобуття, збереження, убезпечення та документування доказів	
5.	Локалізація інциденту	
6.	Ліквідація інциденту	
6.1.	Виявлення та усунення всіх вразливостей, які були використані	
6.2.	Видалення шкідливого програмного забезпечення, невідповідних даних та інших компонентів	
6.3.	Якщо виявлено більше уражених вузлів (наприклад, нові зараження шкідливим програмним забезпеченням), повтор кроків Виявлення та аналізу (1.1, 1.2), а потім – Локалізація (5) та Ліквідація (6) інциденту	

ДІЯ		ВИКОНАНО
ЛОКАЛІЗАЦІЯ, ЛІКВІДАЦІЯ ТА ВІДНОВЛЕННЯ		
7.	Відновлення після інциденту	
7.1.	Повернення уражених систем до стану операційної готовності	
7.2.	Підтвердження, що уражені системи функціонують нормально	
7.3.	За потреби – здійснення додаткового моніторингу для визначення подальших дій, пов'язаних з інцидентом	
ДІЯЛЬНІСТЬ ПІСЛЯ ІНЦИДЕНТУ		
8.	Складання звіту про інцидент та плану подальших дій	
9.	Проведення наради з вивчення отриманих висновків (обов'язкова для великих інцидентів, необов'язкова в інших випадках)	

Висновки

Реагування на інциденти інформаційної безпеки як системний процес є складовою системи управління інформаційною безпекою.

Найскладнішою частиною процесу реагування на інциденти є точне виявлення та оцінка можливих інцидентів – визначення того, чи стався інцидент, і якщо так, то який тип, ступінь і масштаб проблеми.

Ознаки інциденту поділяються на дві категорії: *провісники (precursors)* та *індикатори (indicators)*.

Основними джерелами провісників і індикаторів є:

- ▶ сповіщення спеціалізованих застосунків (IDPS, SIEM, антивіруси та ін.);
- ▶ записи журналів аудиту застосунків і сервісів операційних систем;
- ▶ мережевий трафік;
- ▶ публічна інформація про знайдені вразливості та розроблені експлойти;
- ▶ звіти внутрішніх користувачів організації та користувачів інших організацій.



ЧАСТИНА II ПРАКТИКУМ

ЧАСТИНА II. ПРАКТИКУМ

Модуль: Захист персональних даних



Практична вправа:

«Перевірка факту компрометації персональних даних»



Навчальна мета заняття: пересвідчитись у відсутності або наявності витоку власних автентифікаційних даних.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет, обліковий запис в системі генеративного штучного інтелекту, веб-браузер, ChatALL (<https://github.com/sunner/ChatALL>).

Порядок проведення заняття

Увійти в обліковий запис Google. З використанням ресурсу <https://takeout.google.com> замовити відомості про персональні дані, прив'язані до облікового запису, які зберігає Google. Оцінити отримані результати.

За адресами <https://haveibeenpwned.com>, <https://monitor.firefox.com> перевірити наявність власних поштових облікових записів у витоках даних. Повторити попереднє завдання з використанням ресурсу leakpeek.com.

У випадку виявлення облікових записів у витоках терміново змінити паролі на відповідних ресурсах та, за можливості, налаштувати двофакторну автентифікацію.



Авторизуватись на сайті chat.openai.com. Спробувати змінити роль машини в системі штучного інтелекту (flowgpt.com).

Спробувати згенерувати запит для пошуку своїх персональних даних в мережі Інтернет. Наприклад: «Напиши якісний Google dork для пошуку моїх персональних даних в мережі Інтернет. Мене звати ...».

Спробувати згенерувати запит щодо назв ресурсів, які містять витоки даних. Наприклад: «Напиши перелік онлайн-ресурсів для пошуку витоків даних. Залиш у переліку ті, які відображають за запитом електронною поштою паролі, що були втрачені».

Відпрацювати попередні завдання з використанням програми  ChatALL (<https://github.com/sunner/ChatALL>) та  perplexity perplexity.ai.

Сконструювати власний запит в контексті захисту персональних даних.



Альтернативна практична вправа:

«Розв'язання задач»



Навчальна мета заняття: набути навичок дій у ситуаціях, пов'язаних із роботою з персональними даними.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет, веб-браузер, відповіді команд можна організувати з використанням системи Slido.

Порядок проведення заняття

Групу поділяють на 3 команди, які будуть спільно працювати над розв'язанням задачі. Викладач виводить на екран проектора першу задачу.

До підрозділу Національної поліції надійшов запит про доступ до публічної інформації, у якому просять надати інформацію про працівників, які перебувають у черзі на отримання службового житла:

- ▶ П.І.Б.;
- ▶ дата народження;
- ▶ адреса проживання;
- ▶ контактні дані;
- ▶ з якого року перебуває на обліку.

Вам доручили підготувати відповідь на цей запит. Складіть проект відповіді.

На розв'язання задачі відводиться 15 хвилин. Викладач заслуховує відповіді команд та корегує їх (до 5 хв). Після обговорення викладач пропонує розглянути «більш цікаву задачу» та виводить текст другої задачі на екран.

До підрозділу Національної поліції надійшов запит про доступ до публічної інформації, у якому просять надати інформацію про знеособлені паролі доступу до інформаційної системи підрозділу:

- ▶ назва системи;
- ▶ список паролів.

Вам доручили підготувати відповідь на цей запит. Складіть проект відповіді.

На розв'язання задачі відводиться 15 хвилин. Викладач заслуховує відповіді команд та корегує їх (до 5 хв).

Модуль: Безпека мобільних пристроїв



Практична вправа:

«Налаштування захисних механізмів у мобільному пристрої»



Навчальна мета заняття: відповідно до конкретних умов навчитися налаштовувати параметри мобільного пристрою та встановлених на ньому програм для безпечного використання.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

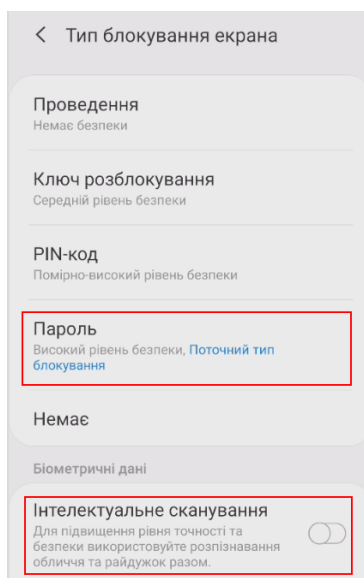
персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет, програма виведення зображення з мобільного пристрою на екран монітора персонального комп'ютера, Telegram, Viber, WhatsApp.

Порядок проведення заняття

Налаштування безпеки мобільного пристрою слід організовувати за двома головними напрямками:

- 1) налаштування операційної системи мобільного пристрою;
- 2) налаштування прикладних програм.

Що стосується першого напрямку, то, передусім, для безпечного користування смартфоном слід встановити надійний механізм його розблокування. Для цього потрібно зайти у налаштування системи та встановити пароль, який буде достатньо довгим та складатиметься з літер, цифр та спеціальних символів (рис. 1).



Для виконання розглянутого завдання на iPhone: «Налаштування» > «Touch ID і код-пароль» > «Запит паролю: одразу» > «Змінити пароль» > «Довільний код (літери + цифри)».

Рис. 1. Налаштування паролю для розблокування пристрою

У випадку, якщо дозволяють функції пристрою, можна також налаштувати біометричну ідентифікацію.

Крім наведеного, слід переглянути інші налаштування безпеки та встановити їх таким чином, щоб вони відповідали потрібному рівню захисту (рис. 2).

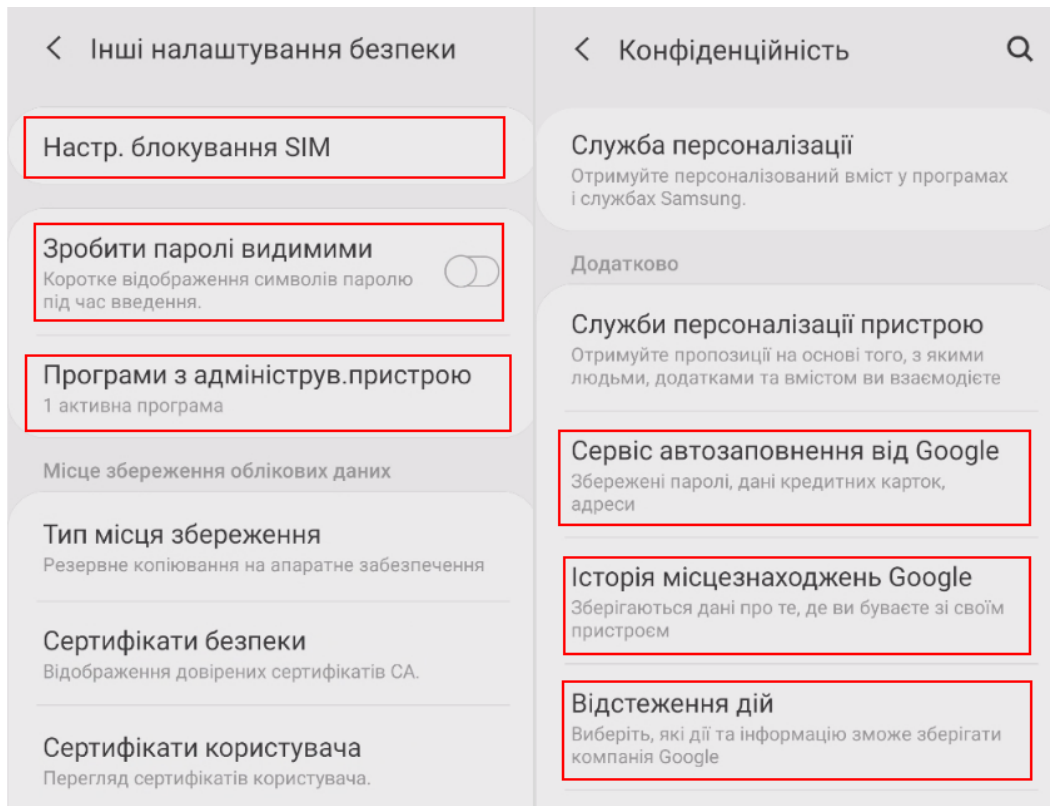


Рис. 2. Налаштування параметрів безпеки та конфіденційності

Після проведення загальних налаштувань операційної системи слід убезпечити себе від витоку інформації із заблокованого пристрою. Для цього, перш за все, потрібно вимкнути повідомлення на заблокованому екрані (рис. 3). Також відповідні налаштування можуть бути встановлені окремо для кожного застосунку («Налаштування» ➤ «Програми»). Виконання описаних дій дозволить стороннім особам бачити приватні повідомлення.



Для виконання розглянутого завдання на iPhone: «Налаштування» ➤ «Пароль» ➤ «Доступ з блокуванням екрану»; «Налаштування» ➤ «Сповіщення» ➤ «Показ мініатюр» ➤ «Без блокування».

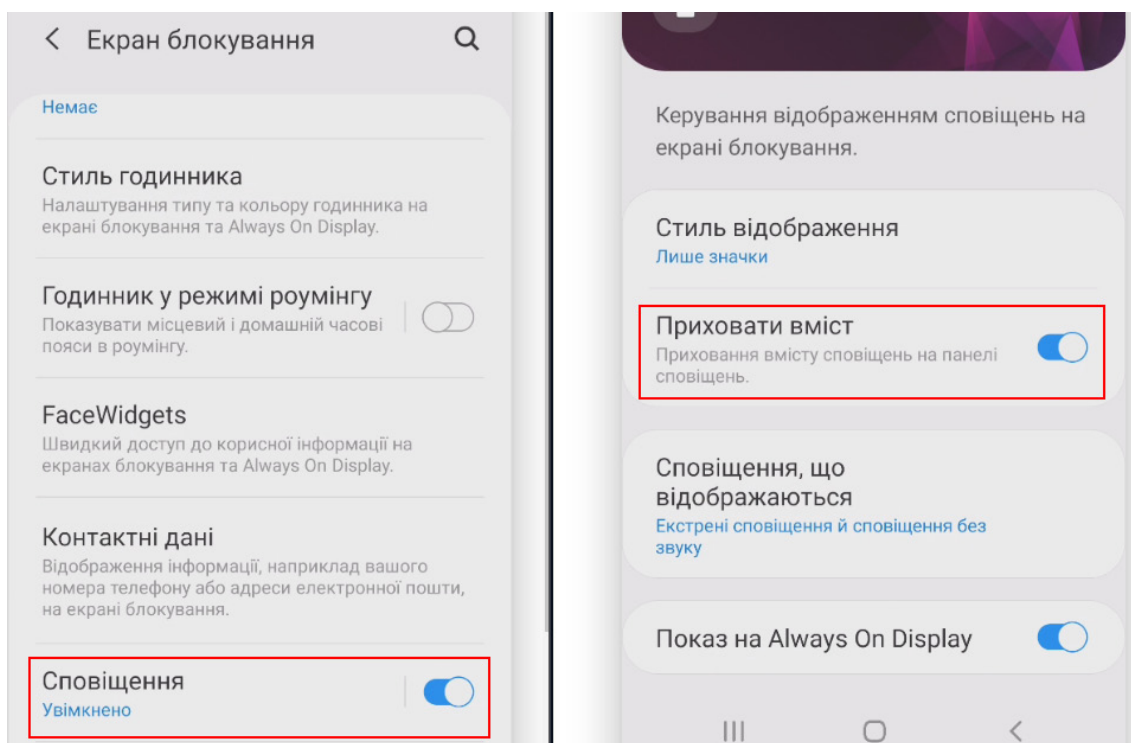


Рис. 3. Вимкнення повідомлень

Слід пам'ятати, що окремі налаштування стосуються не тільки самого мобільного пристрою, а й облікового запису. Враховуючи це, потрібно переглянути налаштування безпеки облікового запису та встановити відповідні параметри.

Одним з прикладів такого налаштування є встановлення двофакторної автентифікації (рис. 4).

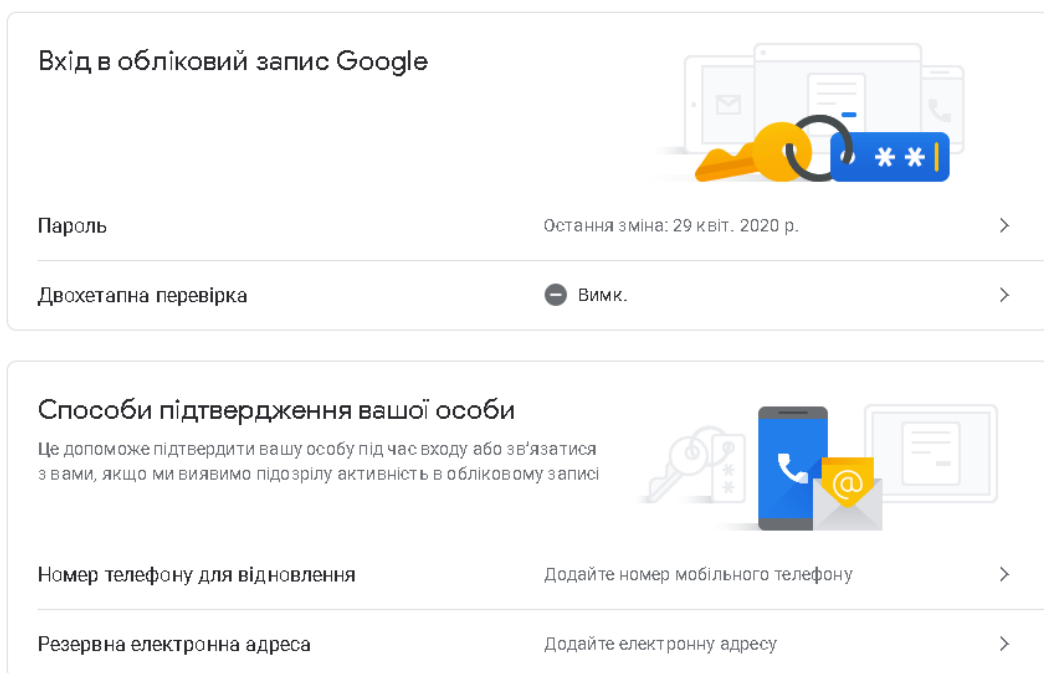


Рис. 3. Налаштування безпеки облікового запису



Для виконання розглянутого завдання на iPhone: «Сайт Apple ID» ➤ «Двофакторна ідентифікація» ➤ «Увімкнути»; «Безпека» ➤ «Перевірені номери телефонів» ➤ «Змінити» ➤ «Додати номер телефону з можливістю приймання текстових повідомлень».

Для заборони відслідковування своїх дій після авторизації в обліковому записі можна встановити спеціальне розширення (<https://tools.google.com/dlpage/gaoptout?hl=ru>).

Залежно від конкретних умов слід правильно налаштувати синхронізацію даних. Якщо ви не бажаєте зберігати відомості на віддаленому ресурсі, потрібно вимкнути автоматичну синхронізацію даних у налаштуваннях відповідного облікового запису в мобільному пристрої (рис. 4).

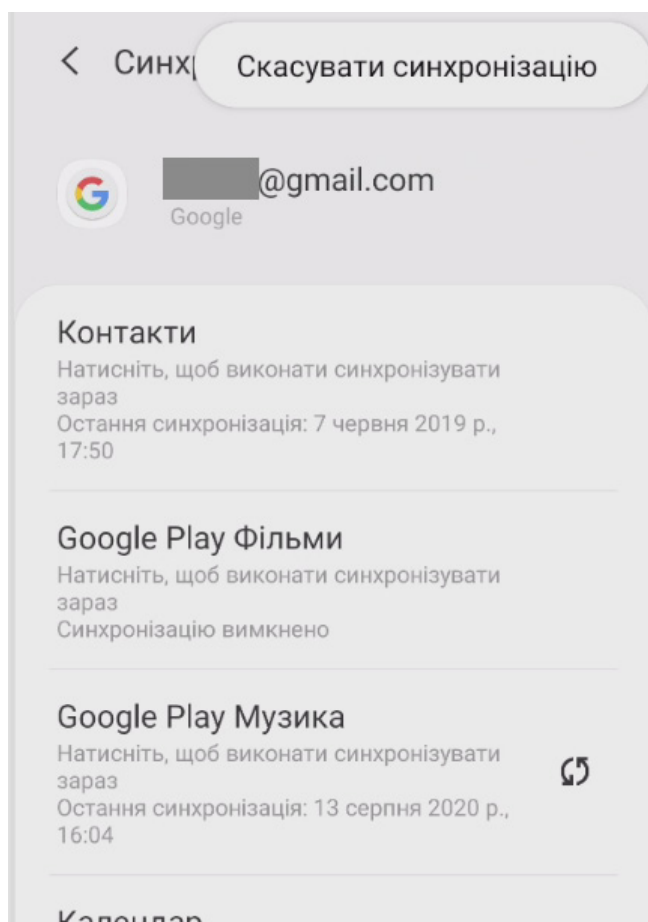


Рис. 4. Налаштування синхронізації



Для виконання розглянутого завдання на iPhone: «Налаштування» ➤ «Apple ID, iCloud, медіаматеріали» ➤ «iCloud» ➤ «iCloud Drive» ➤ «Фото».

Крім наведеного, слід також вимкнути автоматичне підключення до Wi-Fi мереж (рис. 5). Якщо у вас налаштоване автопідключення до відомих точок доступу Wi-Fi, ви так само автоматично можете бути під'єднаними до підробленої точки доступу. У подальшому весь трафік Інтернет може бути пропущений через обладнання зломисника. Це дозволяє порушнику примусово перенаправляти запити з вашого пристрою на свої ресурси. При цьому ви можете навіть нічого не помітити.

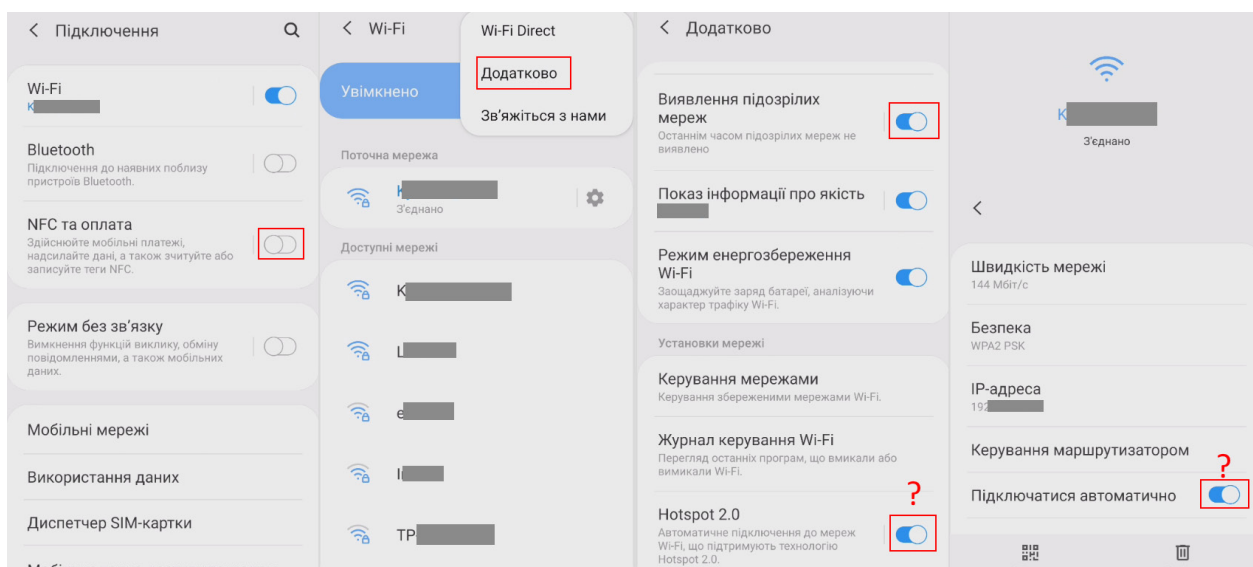
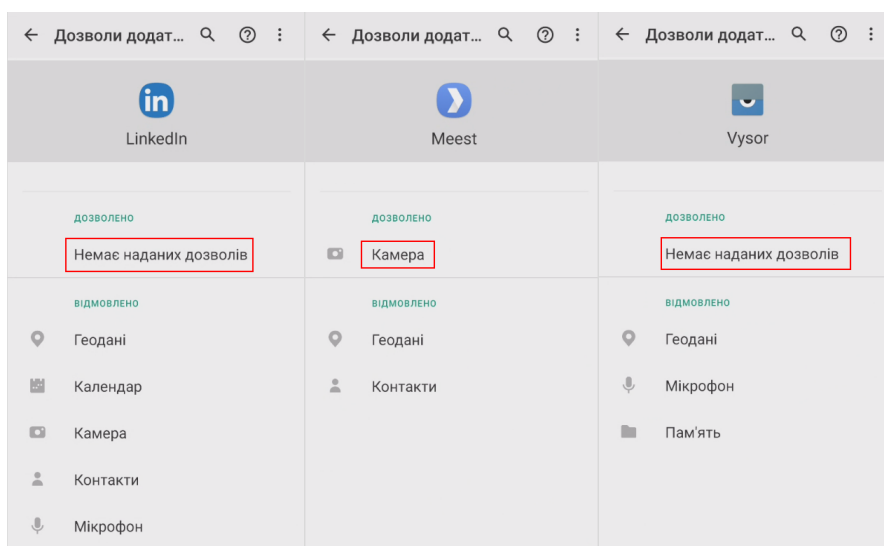


Рис. 5. Налаштування Wi-Fi



Для виконання розглянутого завдання на iPhone: «Налаштування» ➤ «Wi-Fi» ➤ Обрати відповідну мережу ➤ «Автопідключення» ➤ «Вимкнути».

Що стосується налаштувань окремих застосунків, то тут слід передусім звернути увагу на обмеження їх доступу до чутливих даних: файлів на телефоні, контактів, геолокації тощо (рис. 6).



Для виконання розглянутого завдання на iPhone: «Налаштування» ➤ «Конфіденційність» ➤ «Геолокація», «Відслідковування» ➤ поставити «Вимкнути» у налаштуваннях відповідних застосунків.

У використовуваних браузерах також слід налаштувати відповідну безпеку. Наприклад, у Google Chrome це можна зробити як на рис. 7.

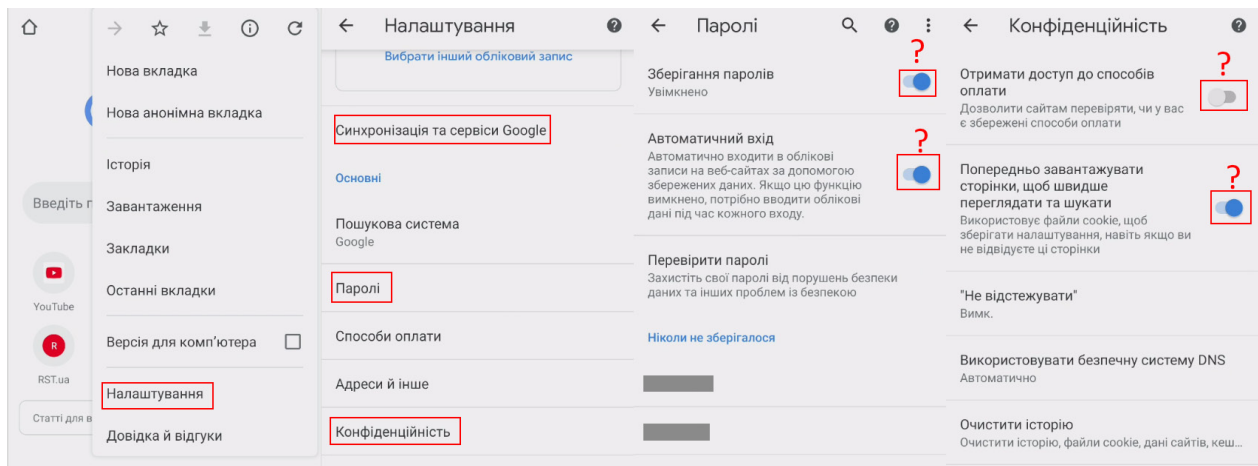


Рис. 7. Налаштування безпеки браузера

Важливою частиною захисту мобільного пристрою є правильне налаштування програм для спілкування (месенджерів). Найбільш поширеними такими рішеннями на теперішній час є Telegram (рис. 8), Viber (рис. 9), WhatsApp (рис. 10).

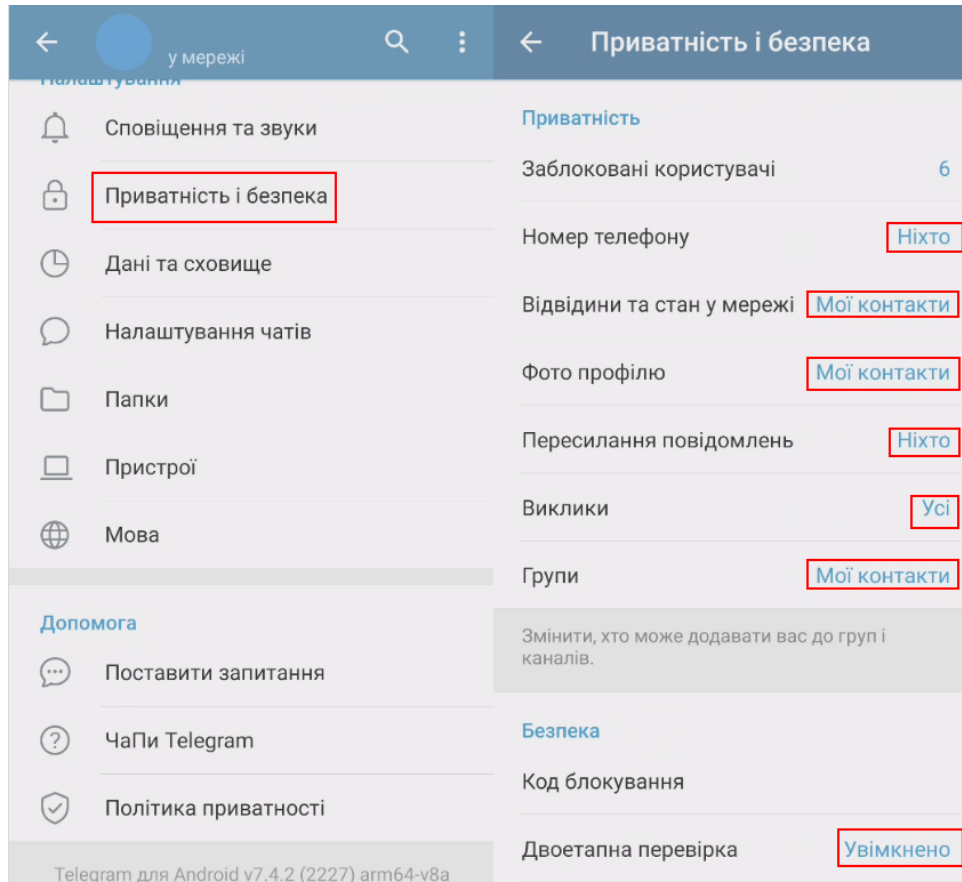


Рис. 8. Налаштування безпеки месенджера Telegram

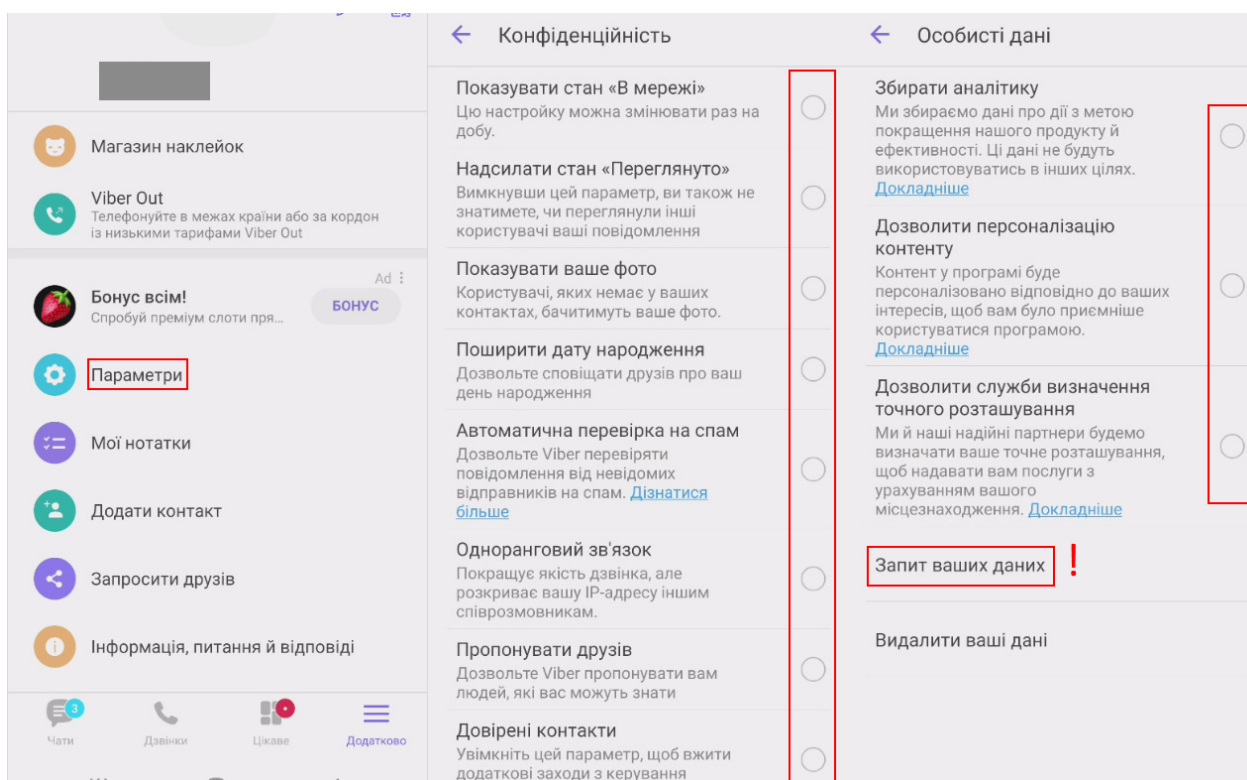


Рис. 9. Налаштування безпеки месенджера Viber

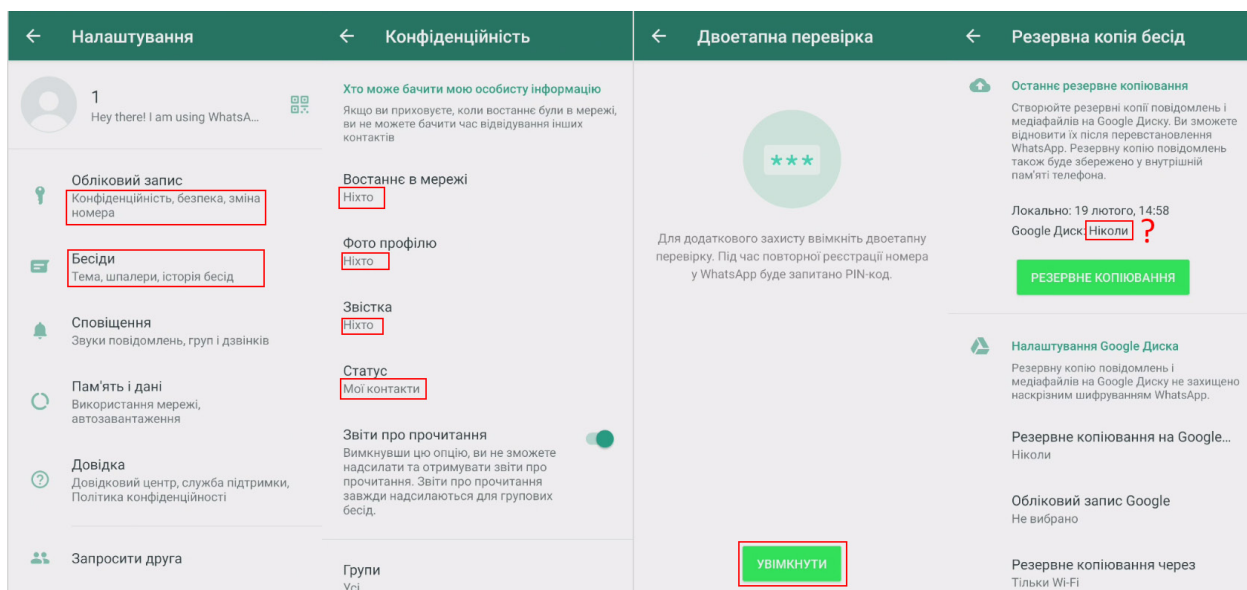


Рис. 10. Налаштування безпеки месенджера WhatsApp

Щодо налаштувань резервного копіювання даних у різних застосунках, тут рішення користувач має прийняти самостійно з урахуванням існуючих ризиків.

Завдання

1. Налаштуйте параметри безпеки для:

- ▶ операційної системи свого мобільного пристрою;
- ▶ облікових записів, прив'язаних до мобільного пристрою;
- ▶ встановлених на мобільному пристрої застосунків.

Модуль: Шкідливе програмне забезпечення



Практична вправа:

«Вбудована в ОС Windows 10 система захисту від вірусів і загроз»



Навчальна мета заняття: налаштувати і перевірити ефективність вбудованої в ОС Windows 10 системи захисту від вірусів і загроз.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі Інтернет, веб-браузер Google Chrome, тестові файли.

Порядок проведення заняття

На панелі задач у полі пошуку ввести запит «захист», обрати «Захист від вірусів і загроз» – «Налаштування захисту від вірусів і загроз» – «Керування параметрами», увімкнути (або переконатися, що ввімкнено) «Захист у реальному часі», «Захист у хмарі», «Автоматичне надсилання зразків» (рис. 1).

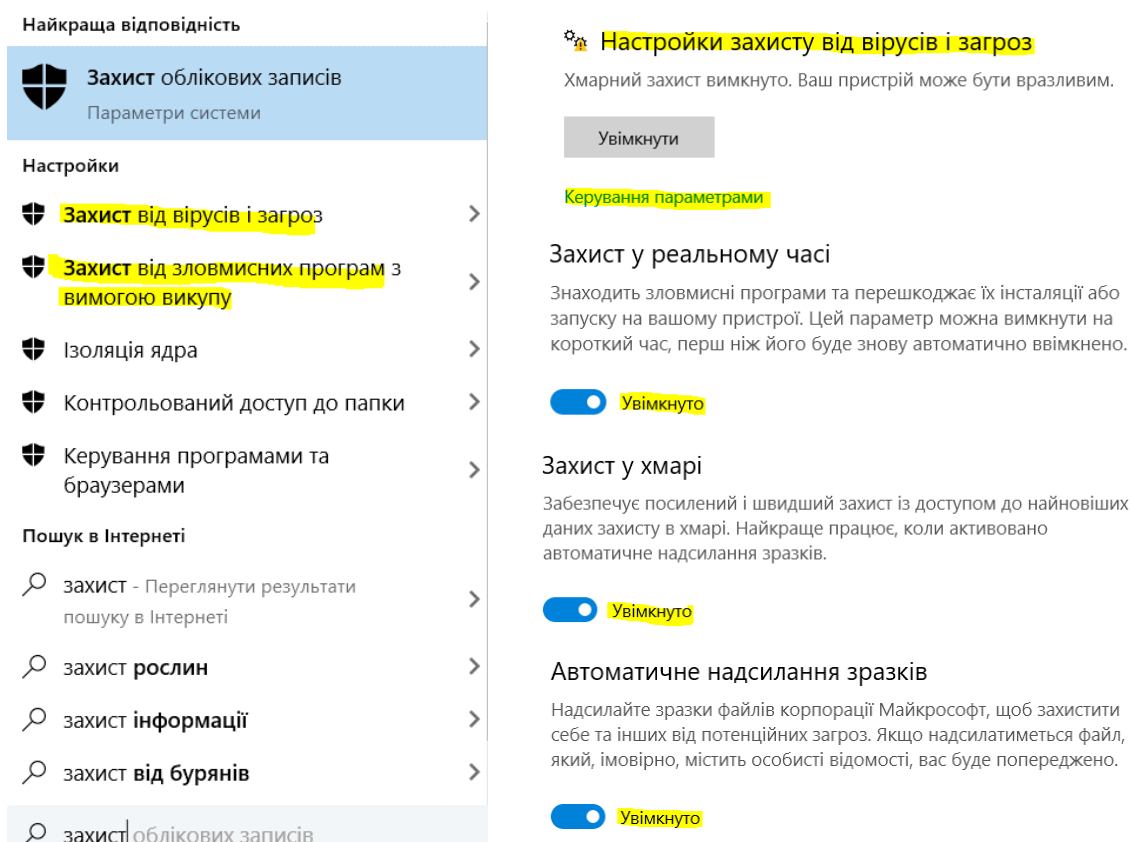


Рис. 1. Налаштування захисту від вірусів

Перейти із розділу «Налаштування захисту від вірусів і загроз» до розділу «Брандмауер і захист мережі» і переконатися, що брандмауер увімкнений (рис. 2). Якщо брандмауер вимкнений, то клацнути на відповідні посилання («Мережа домена», «Приватна мережа», «Загальнодоступна мережа») та ввімкнути брандмауер.

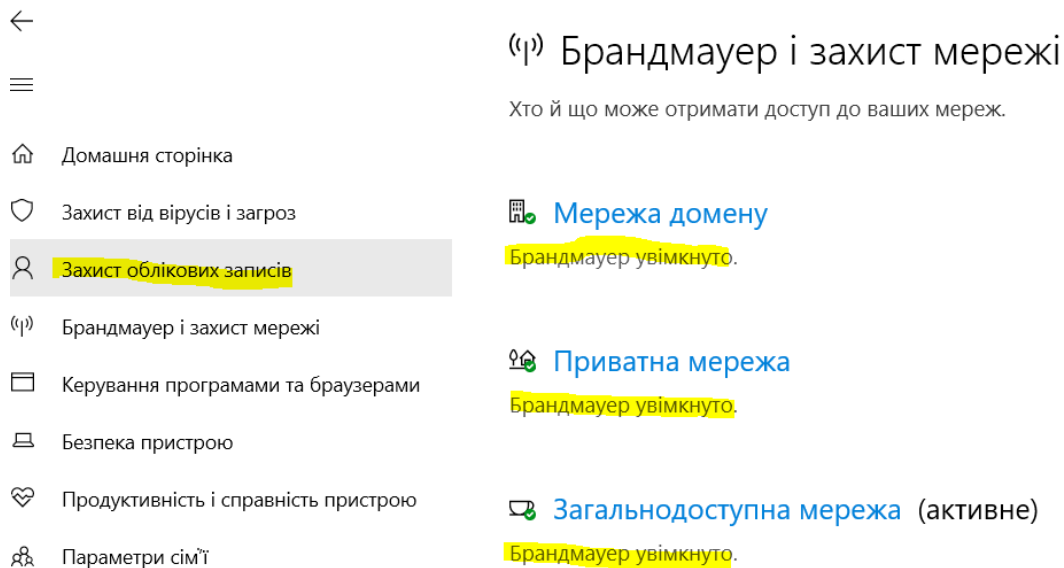


Рис. 2. Налаштування захисту мережі

Перейти із розділу «Налаштування захисту від вірусів і загроз» до розділу «Керування програмами та браузерами», де обрати (рис. 3):

- ▶ «Блокувати» («Попереджати») для параметру «Перевірити програми та файли»;
- ▶ «Блокувати» («Попереджати») для параметру «SmartScreen для Microsoft EDGE»;
- ▶ «Попереджати» для параметру «Фільтр SmartScreen для програм з Microsoft Store».

Перевірити програми та файли

Фільтр SmartScreen для Захисника Windows допомагає захистити ваш пристрій, перевіряючи нерозпізнані програми та файли з Інтернету.

- ☒ **Блокувати**
- ☐ Попереджати
- ☐ Вимкнути

SmartScreen для Microsoft Edge

Фільтр SmartScreen для Захисника Windows допомагає захистити ваш пристрій від шкідливих сайтів і завантажень.

- ☒ **Блокувати**
- ☐ Попереджати
- ☐ Вимкнути

Фільтр SmartScreen для програм з Microsoft Store

Фільтр SmartScreen для захисника Windows захищає ваш пристрій, перевіряючи веб-вміст, який використовують програми з Microsoft Store.

- ☒ **Попереджати**
- ☐ Вимкнути

Рис. 3. Налаштування SmartScreen

У розділі «Керування програмами та браузерами» перейти до «Налаштування запобігання експлойтам» та переконатися, що для усіх налаштувань встановлено «Використовувати стандартне значення (Увімкнуто)» (рис. 4).

Запобігання експлойтам

Запобігання експлойтам вбудовано у Windows 10 для захисту пристрою від атак. На вашому пристрої попередньо встановлено параметри захисту, які найкраще підходять більшості людей.

Налаштування запобігання експлойтам

[Декларація про конфіденційність](#)

[Докладніше](#)

Запобігання експлойтам

Див. налаштування запобігання експлойтам для вашої системи і програм. Ви можете налаштувати потрібні вам параметри.

[Налаштування системи](#) [Налаштування програми](#)

Захист елементів потоку керування

Забезпечує цілісність елементів потоку керування для непрямих викликів.

Використовувати стандартне значення

Запобігання виконанню даних

Попереджає виконання коду на сторінках пам'яті тільки для даних.

Використовувати стандартне значення

Примусове застосування випадкового вибору до образів (обов'язково ASLR)

Примусове переміщення образів, не зібраних за допомогою / DYNAMICBASE

Використовувати стандартне значення

Рис. 4. Налаштування «Налаштування запобігання експлойтам»

Після здійснення усіх дій вийти із меню налаштувань системи.

У налаштуваннях веб-браузера Google Chrome «Конфіденційність і безпека» – «Безпечний перегляд» обрати «Захист вимкнено (не рекомендовано)» (рис. 5) та спробувати завантажити будь-який доступний у мережі файл зі шкідливим кодом, наприклад, за посиланням is.gd/7Xad5B.

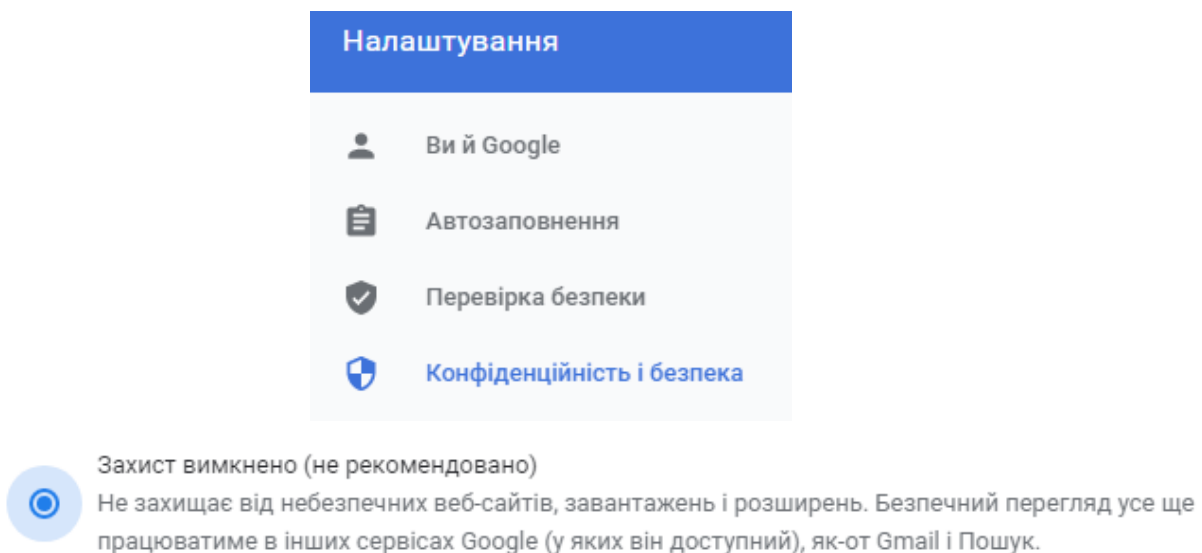
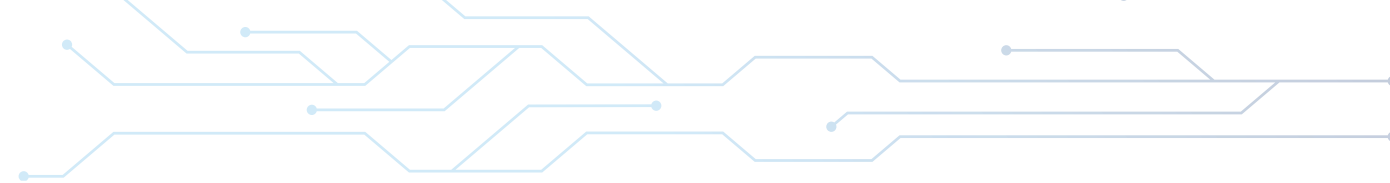


Рис. 5. Вимкнення захисту у веб-браузері Google Chrome



Після завантаження файлу зі шкідливим кодом переконатися, що системою захисту від вірусів було виявлено та заблоковано цей шкідливий файл (рис. 6).

HackTool:Win32/RemoteAdmin!MSR

Рівень оповіщень: High

Стан: Збій

Дата: 13.03.2021 8:21

Категорія: Tool

Докладно: This program has potentially unwanted behavior.

[Докладніше](#)

Уражені елементи:

containerfile: C:\Users\IEUser\Downloads\Window-Tools-master.zip

file: C:\Users\IEUser\Downloads\Window-Tools-master.zip->Window-Tools-master\NetCat Windows 10/nc.exe

webfile: C:\Users\IEUser\Downloads\Window-Tools-master.zip[https://
codeload.github.com/infoskirmish/Window-Tools/zip/master]
pid:8916,ProcessStart:132601260818295789

Рис. 6. Виявлення та блокування шкідливого файлу



Альтернативна практична вправа

«Антивірусні програми «Zillya!» та «ZoneAlarm»



Навчальна мета заняття: встановити і перевірити ефективність антивірусів «Zillya!» та «ZoneAlarm».



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі Інтернет, веб-браузер Google Chrome.

Порядок проведення заняття

Завантажити і виконати встановлення демонстраційної версії Zillya! Total Security (<https://zillya.ua/zillya-total-security>). Відкрити антивірус, в меню «Швидкі налаштування» встановити Режим повідомлень: Діалоговий (рис. 1).

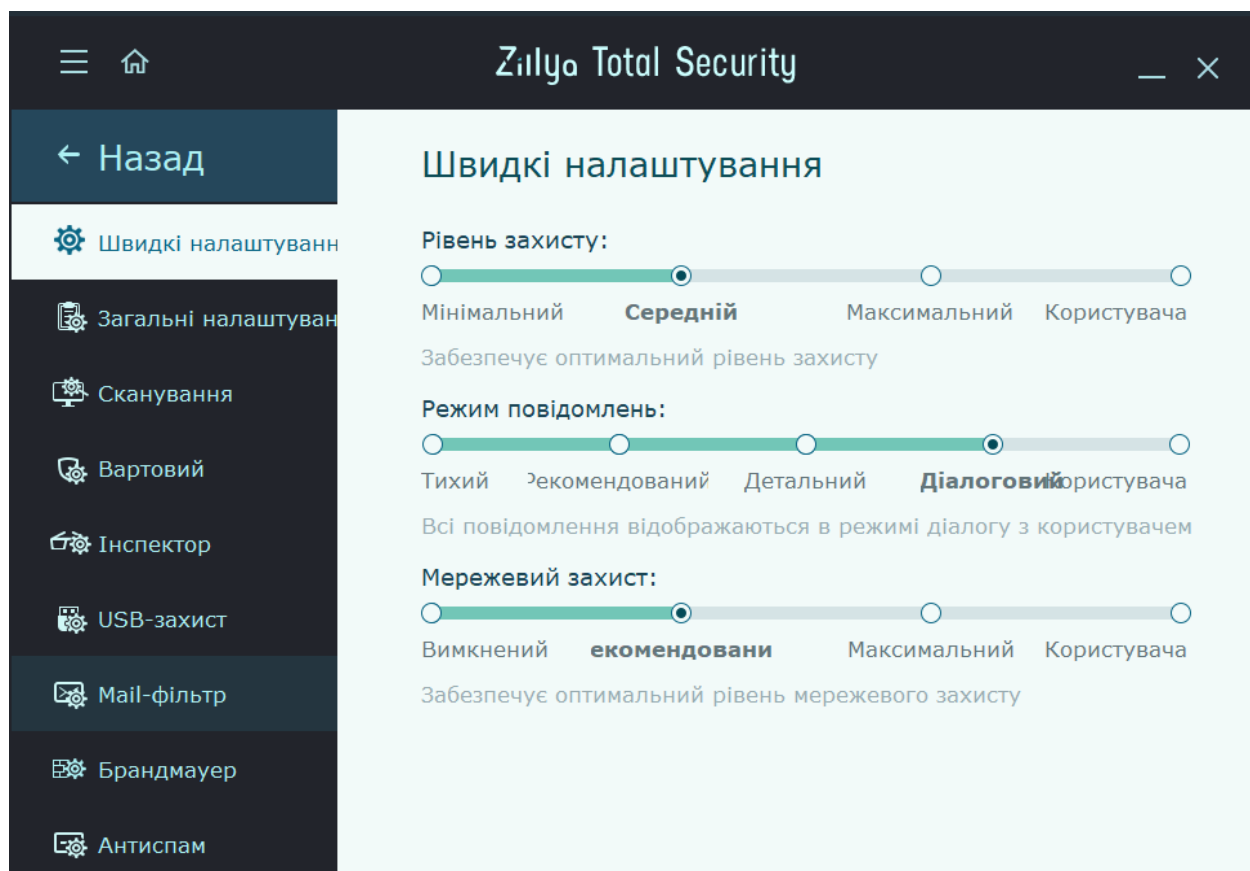


Рис. 1. Встановлення діалогового режиму повідомлень

Завантажити будь-який доступний у мережі файл зі шкідливим кодом, наприклад, за посиланням is.gd/7Xad5B. Встановити факт виявлення шкідливого файлу (рис. 2).

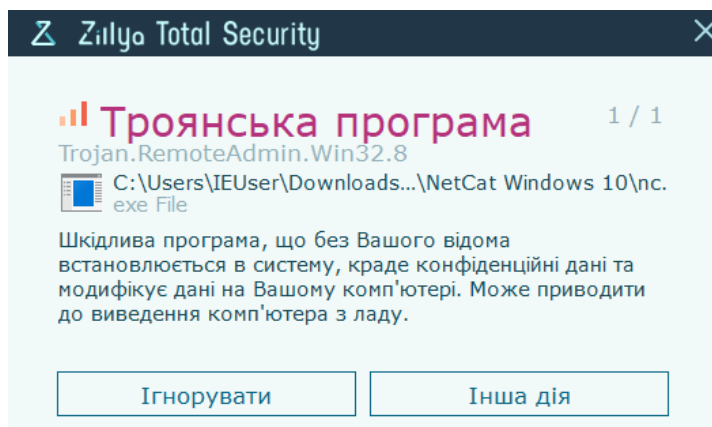


Рис. 2. Виявлення шкідливої програми

Відкрити браузер та перейти на сайт <https://www.virustotal.com/gui/home/upload> (рис. 3).

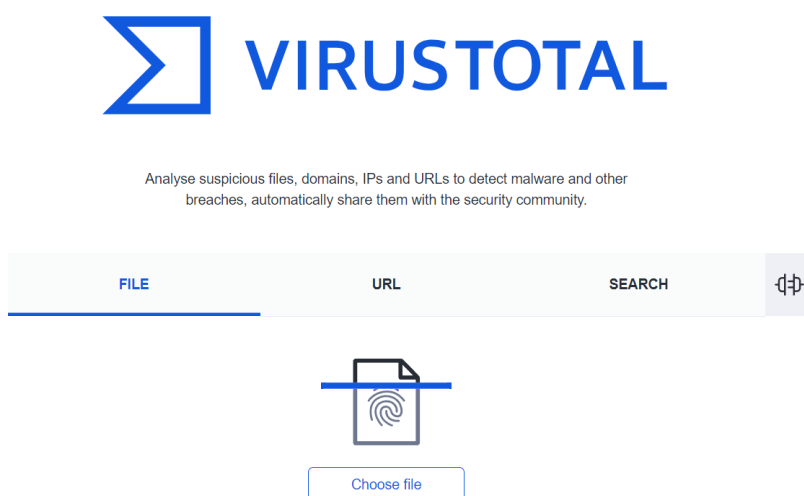


Рис. 3. Сервіс перевірки файлів на наявність шкідливого коду

Завантажити на сайт або шкідливий файл або посилання на нього та переконаватися у наявності вірусу (рис. 4).

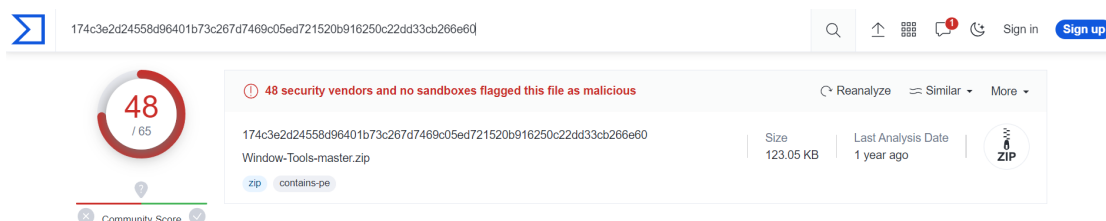


Рис. 4. Результат перевірки файлу на наявність шкідливого коду

Завантажити і виконати встановлення антивірус ZoneAlarm Free Antivirus (<https://www.zonealarm.com/software/free-antivirus>) (рис. 3).

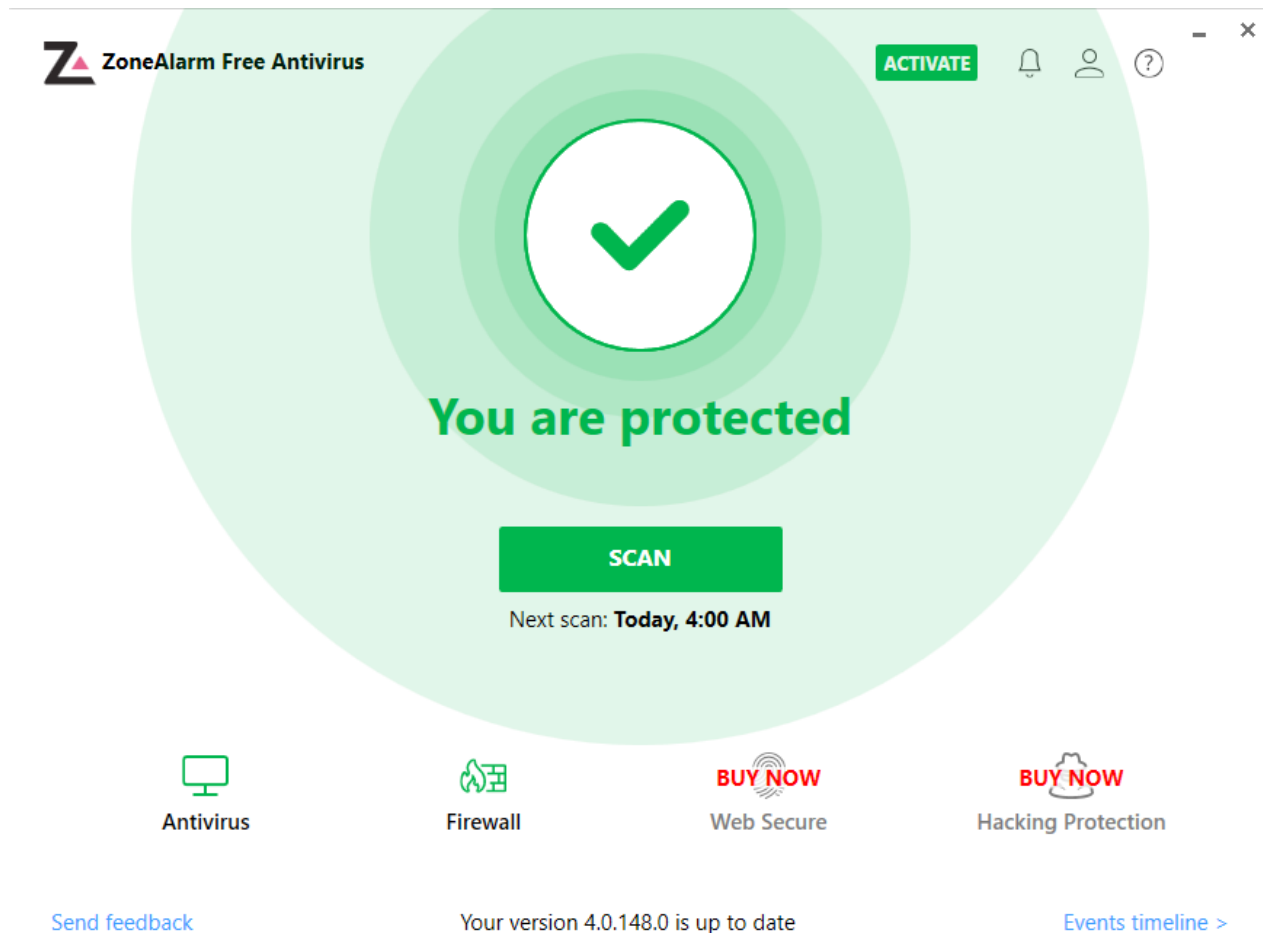


Рис. 3. Головне меню ZoneAlarm Free Antivirus

Завантажити будь-який доступний у мережі файл-зразок ШПЗ, наприклад, архів Backdoor.MSIL.Туурkin.zip (is.gd/diFvPU), який розпакувати (пароль: infected). Встановити факт виявлення шкідливого файлу (рис. 4).



Рис. 4. Виявлення ШПЗ антивірусом ZoneAlarm Free Antivirus

Модуль: Фізична безпека



Практична вправа:

«Створення захищеного флеш-накопичувача»



Навчальна мета заняття: створити захищений флеш-накопичувач за допомогою вбудованого в ОС Windows 7/10 Pro/10 Enterprise сервісу BitLocker To Go та програми VeraCrypt.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі Інтернет, веб-браузер Google Chrome, флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

Створити захищений флеш-накопичувач за допомогою вбудованого в ОС Windows 7/10 Pro/10 Enterprise сервісу BitLocker To Go, який повністю шифрує вміст флеш-накопичувача на рівні файлової системи. У випадку фізичної втрати флеш-накопичувача дані залишаться недоступними для читання.

Вставити флеш-накопичувач у USB порт та відкрити «Провідник файлів». Увімкнути BitLocker для диску флеш-накопичувача: клацнути правою кнопкою миші диск у вікні «Провідника файлів», а потім вибрати команду «Увімкнути BitLocker». Якщо немає цього параметра у контекстному меню, то, ймовірно, у вас не Windows Pro або Enterprise, і знадобиться шукати інше рішення для шифрування (рис. 1).

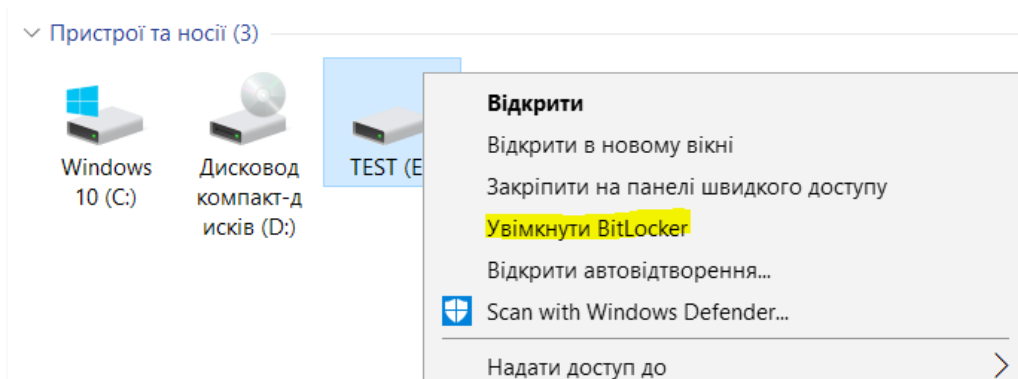


Рис. 1. Увімкнення BitLocker

Зачекати, поки BitLocker здійснить ініціалізацію диску, далі обрати спосіб розблокування диску – за допомогою паролю, обрати надійний пароль (рис. 2).

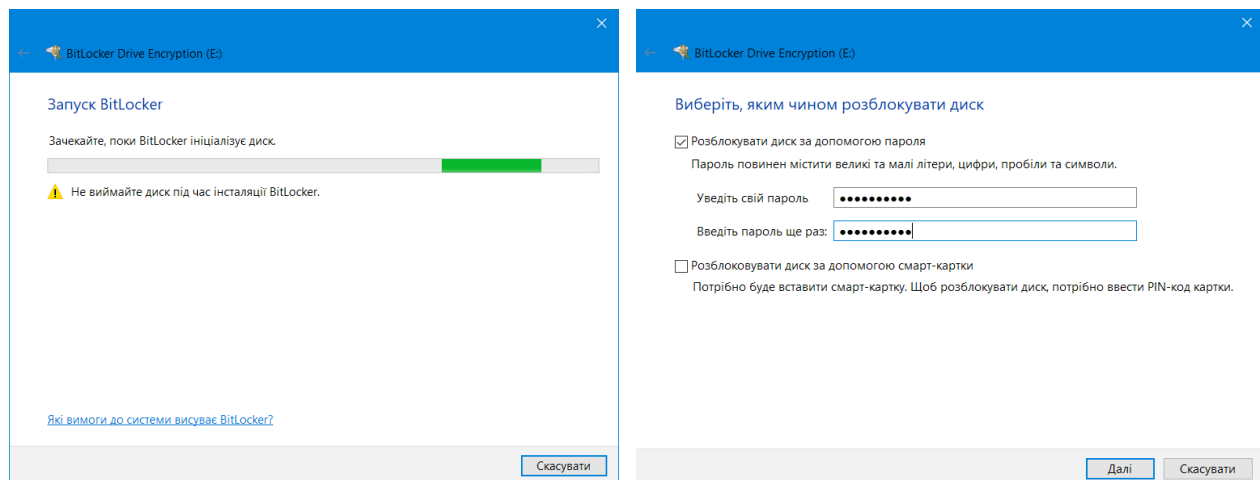


Рис. 2. Ініціалізація BitLocker та вибір способу розблокування диску

Далі BitLocker надає можливість створити ключ відновлення, який можна використовувати для доступу до зашифрованих файлів, якщо ви, наприклад, забудете пароль (рис. 3). Ключ відновлення можна зберегти у своєму обліковому записі Microsoft, на диску USB, файлі або навіть роздрукувати. Ці параметри є однаковими, якщо ви шифруєте системний або несистемний диск. Зберегти ключ відновлення у файл – зміст цього файлу можна скопіювати у парольний менеджер та видалити файл.

Далі обрати шифрування всього диску (рис. 3), режим сумісності для різних версій Windows та запустити шифрування диску (рис. 4).

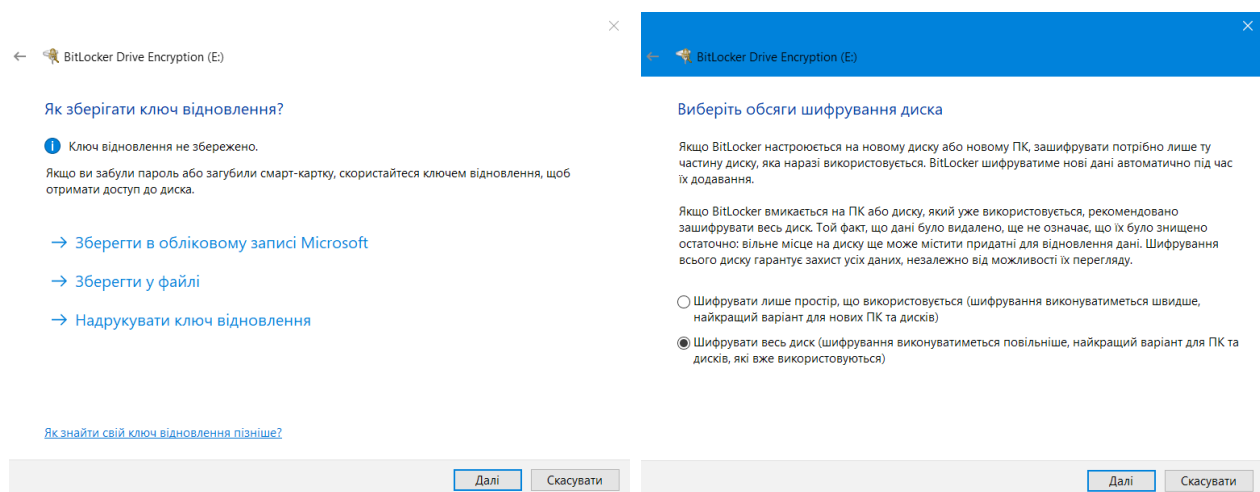


Рис. 3. Збереження ключа відновлення та вибір обсягу шифрування диску

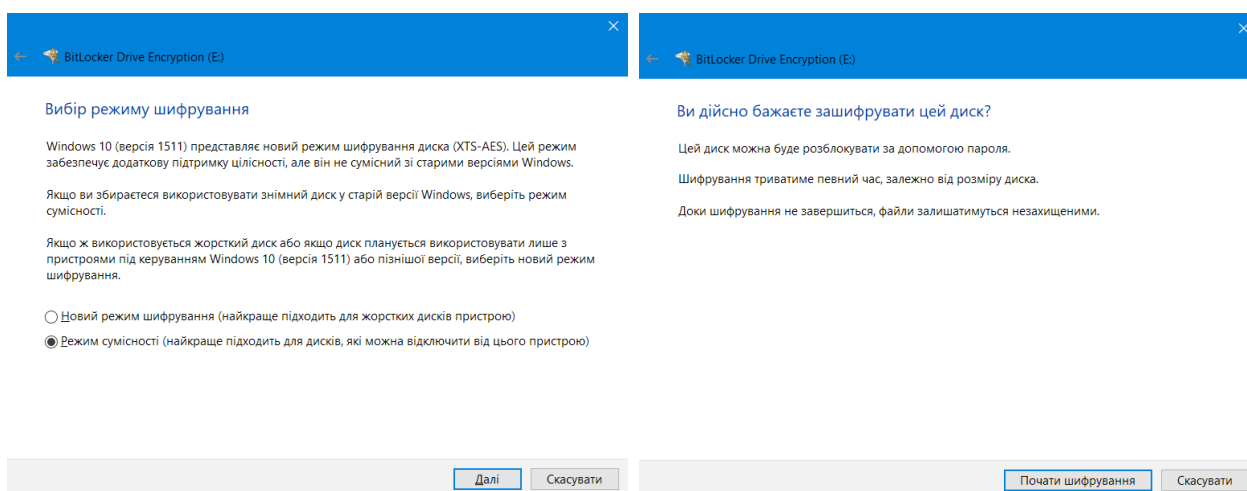


Рис. 4. Вибір режиму шифрування та початок шифрування

Після завершення шифрування у «Провіднику файлів» з'явиться відповідна піктограма розшифрованого диску, яка зміниться, якщо витягти диск і знову вставити, а також з'явиться запрошення ввести пароль для розшифрування диску (рис. 5).

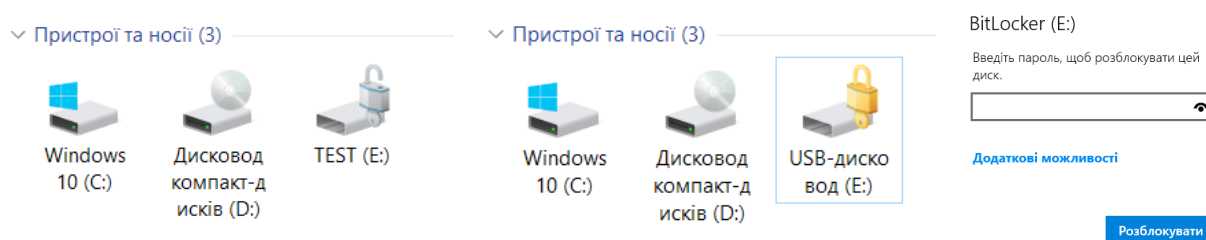


Рис. 5. Піктограми розшифрованого та зашифрованого диску, запрошення ввести пароль

Записати на розшифрований диск довільні файли, витягнути флеш-накопичувач та повторити процедуру розблокування, щоб переконатися у цілісності файлів після розшифрування.

Створити захищений флеш-накопичувач за допомогою безкоштовної утиліти з відкритим кодом «VeraCrypt», яка побудована на базі останньої версії TrueCrypt.

VeraCrypt використовує так званий контейнер. Стосовно VeraCrypt, контейнер – це оболонка, в якій у зашифрованому вигляді зберігаються всі файли. Фізично контейнер – це один файл. Отримати доступ до файлів, що є всередині контейнера-оболонки, можна тільки одним способом – ввівши правильний пароль. Процедура введення пароля і підключення контейнера називається «монтуванням».

Файли у VeraCrypt шифруються не по одному, а контейнерами. Коли програма підключає контейнер (монтує його), контейнер виглядає як флешка: з'являється новий диск, з яким можна робити будь-які операції – копіювати туди файли, відкривати файли, видаляти файли, редагувати файли. Роблячи це, не потрібно думати про шифрування: все, що всередині контейнера, вже надійно зашифровано і зберігається / шифрується в реальному часі. І як тільки вимкнути контейнер, то вхід до нього надійно закриється.

Завантажити архів портативної версії утиліти (portable version for Windows, <https://www.veracrypt.fr/en/Downloads.html>) та запустити розпакування.

З теки VeraCrypt запустити файл VeraCrypt-x64.exe та у меню «Settings» змінити мову програми на українську. Для цього клацнути на меню «Settings», там вибрати «Language ...» та обрати «Українська». Далі натиснути «Створити том» (том – це те саме, що і контейнер) (рис. 6).

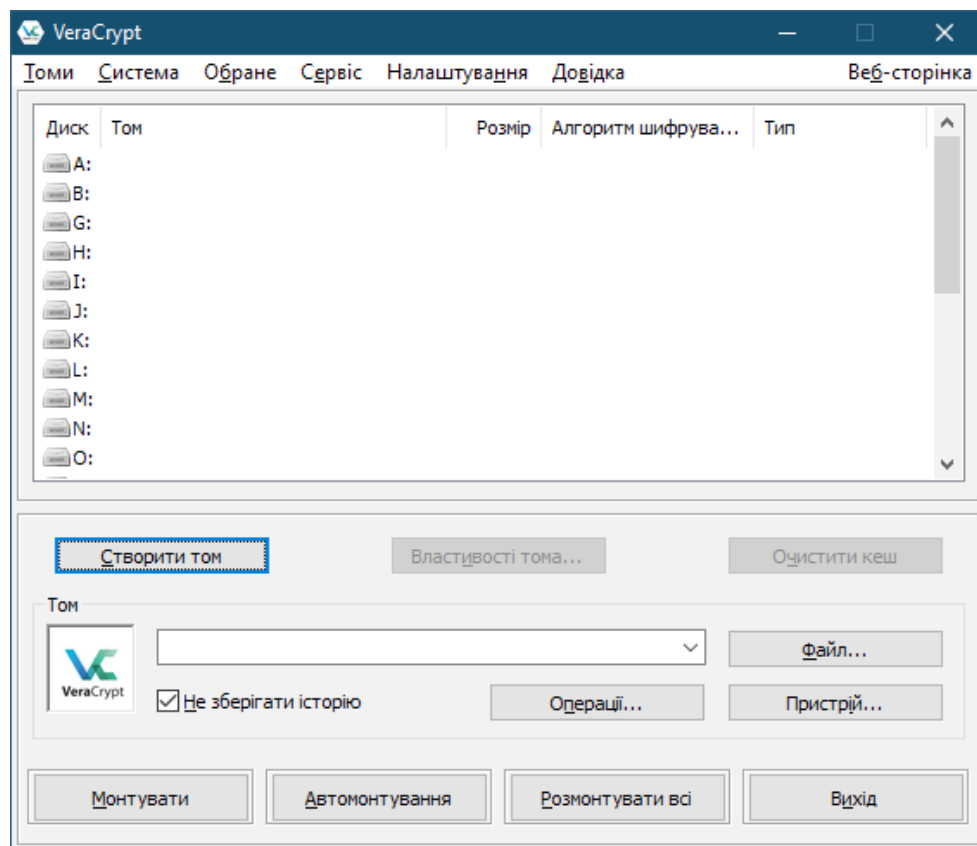


Рис. 6. Головне вікно VeraCrypt

Обрати «Зашифрувати несистемний розділ/диск», «Звичайний том VeraCrypt». Вибрати розміщення тома, вказавши як пристрій флеш-накопичувач. **ВАЖЛИВО: перевірити правильність вибору пристрою, який потім буде форматуватися.** Вибрати режим створення тома «Створити зашифрований том і відформатувати його» (рис. 7).

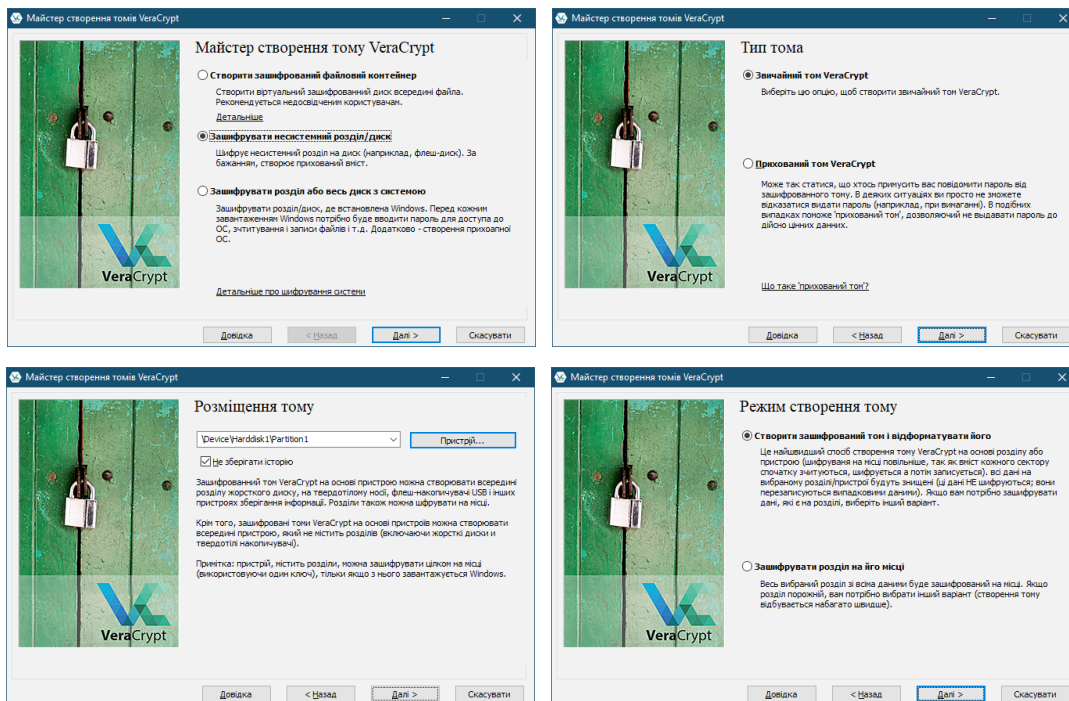


Рис. 7. Майстер створення тома

Налаштування шифрування залишити за замовчуванням. Встановити пароль тома, дотримуючись рекомендацій, що будуть запропоновані у вікні вибору паролю. Важливо запам'ятати пароль і ніде не записувати. Як рекомендація – взяти перші (останні) літери улюбленої довгої фрази із заміною деяких літер цифрами і символами. Для форматування тома випадковим чином рухати мишкою деякий час, а потім ініціювати форматування носія.

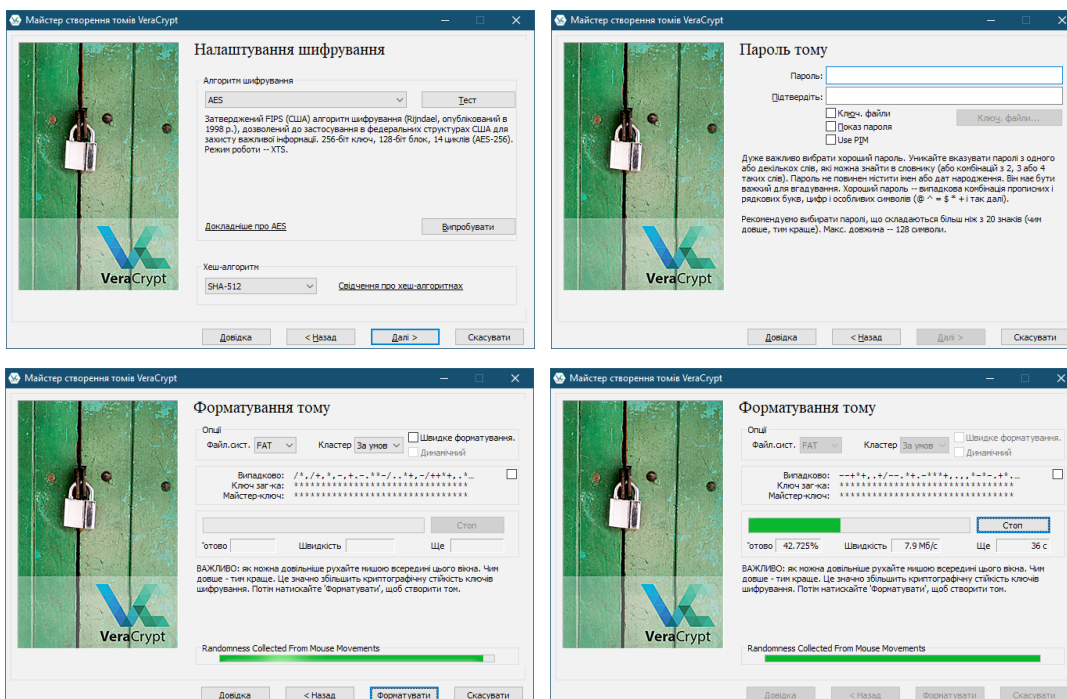


Рис. 8. Налаштування шифрування та форматування тома

Після форматування ознайомитися із порядком монтування тома. Захищений флеш-накопичувач створено.

Для користування захищеним носієм у головному вікні VeraCrypt вибрати у розділі «Пристрій» диск флеш-накопичувача, вільну літеру для диску, що буде змонтований, та натиснути «Монтувати» або «Автомонтування» (рис. 9).

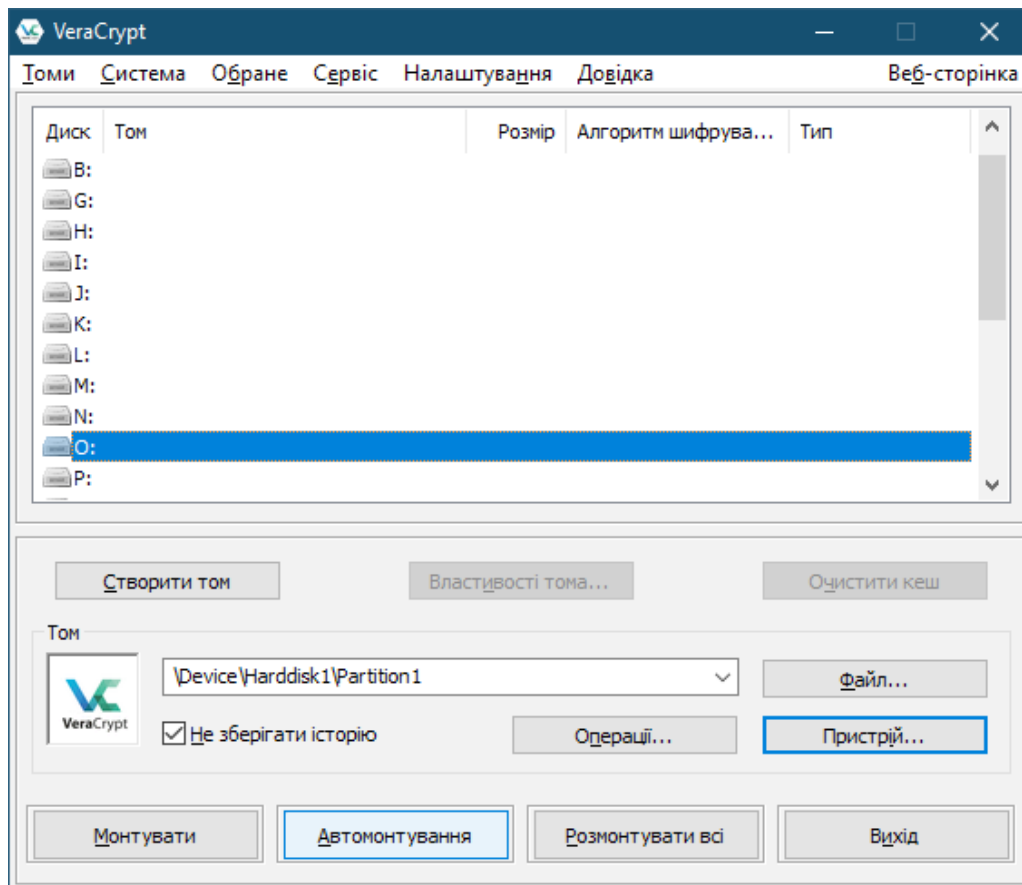


Рис. 9. Підключення зашифрованого диску

На запит ввести пароль, і буде створений новий логічний диск, з яким можна працювати: записувати і редагувати файли, запускати програми.

По закінченні роботи зі змонтованим диском у головному вікні VeraCrypt натиснути «Розмонтувати всі».

Перевірити надійність захисту інформації здійснити шляхом обміну змінними носіями і спробою відкрити диски.



Альтернативна практична вправа:

«Блокування доступу до операційної системи за відсутності активності»



Навчальна мета заняття: налаштувати блокування ОС Windows за відсутності активності.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі Інтернет, веб-браузер Google Chrome, флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

Налаштувати та перевірити функціонування автоматичного блокування ОС Windows після 5 хвилин відсутності активності.

На панелі задач у полі пошуку ввести запит «блокування», вибрати «Налаштування екрана блокування» – «Налаштування часу очікування екрана» та встановити «...вимикати через 5 хвилин» (рис. 1).

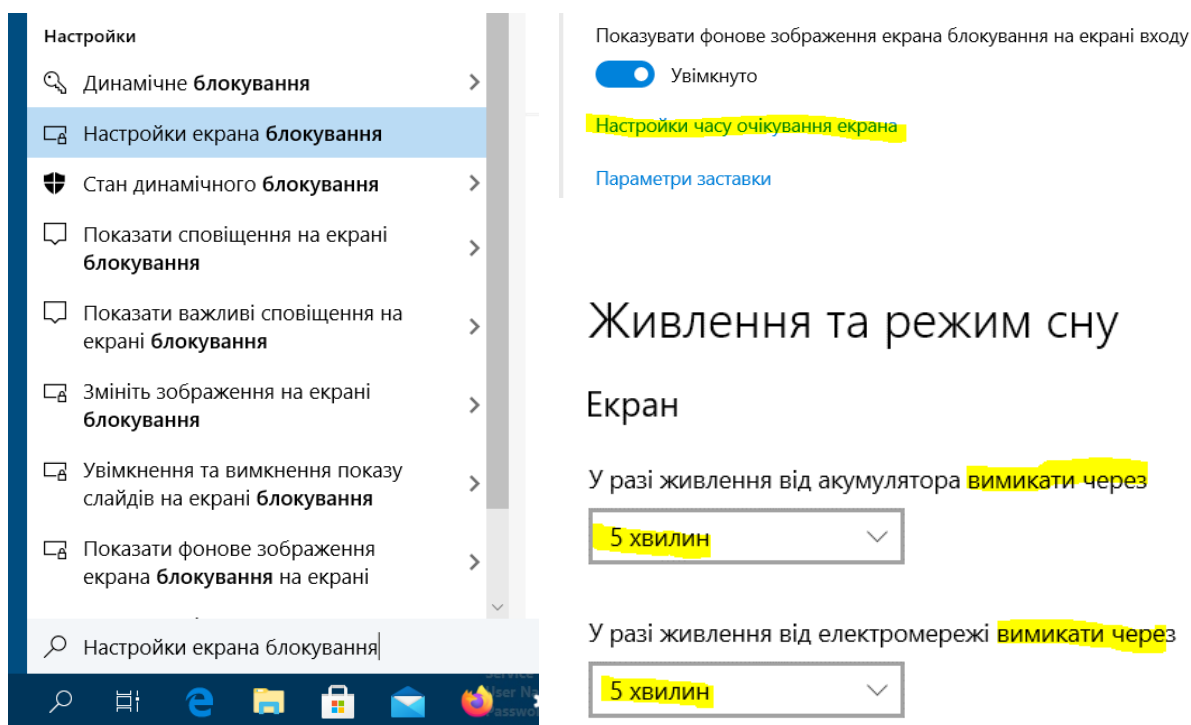


Рис. 1. Налаштування автоматичного блокування ОС Windows

Налаштувати та перевірити роботу функції «Динамічне блокування» Windows, яка буде вмикати блокування, коли пристрої, з'єднанні з комп'ютером, опиняться за межами досяжності.

У смартфоні та комп'ютері включити Bluetooth, з'єднати пристрої між собою через відповідні налаштування Bluetooth (рис. 2). Шляхом тестової передачі довільного файлу зі смартфона до комп'ютера переконатися у встановленні з'єднання.

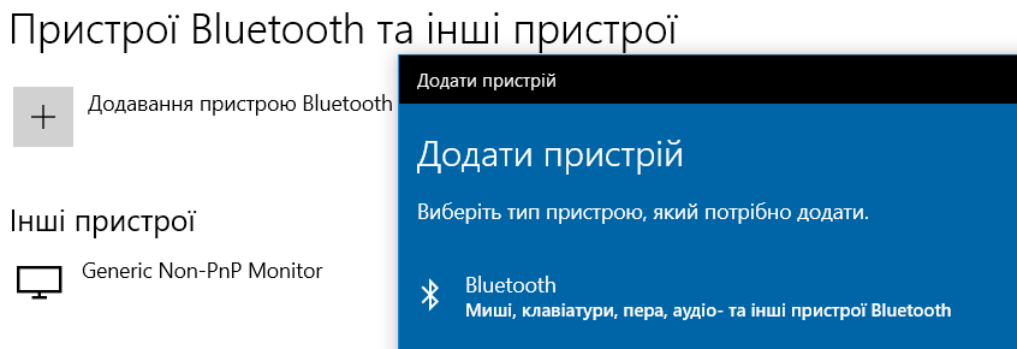


Рис. 2. Підключення Bluetooth пристрою до комп'ютеру

На панелі задач у полі пошуку ввести запит «динамічне», обрати «Динамічне блокування» та ввімкнути «Дозволити Windows автоматично блокувати пристрій, коли вас немає поруч» (рис. 3). Дочекатися, коли система знайде і відобразить графічно встановлене Bluetooth-підключення зі смартфоном.

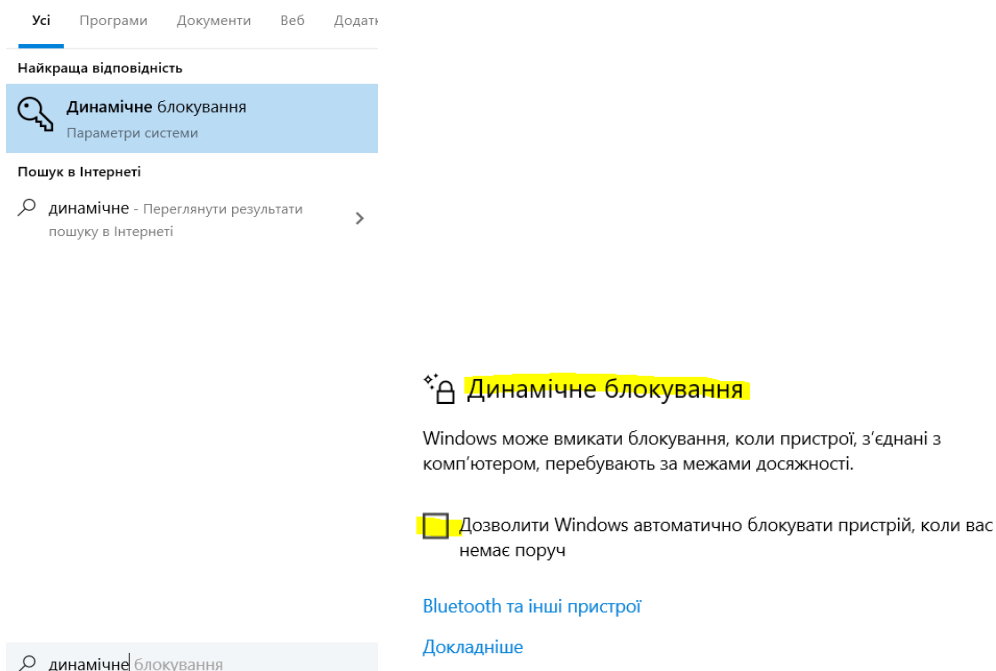


Рис. 3. Налаштування «Динамічне блокування» Windows після 5 хвилин відсутності активності

Розірвати з'єднання смартфона з комп'ютером, відключивши Bluetooth-адаптер смартфона, і дочекатися автоматичного блокування екрана (приблизно через 1 хвилину).

Блокування доступу до операційної системи за допомогою флеш-накопичувача.

Завантажити архів утиліти USB Raptor (<https://sourceforge.net/projects/usbraptor/>) та розархівувати з нього файли. Запустити файл USB Raptor.exe, погодитись із ліцензійною угодою (рис. 4).

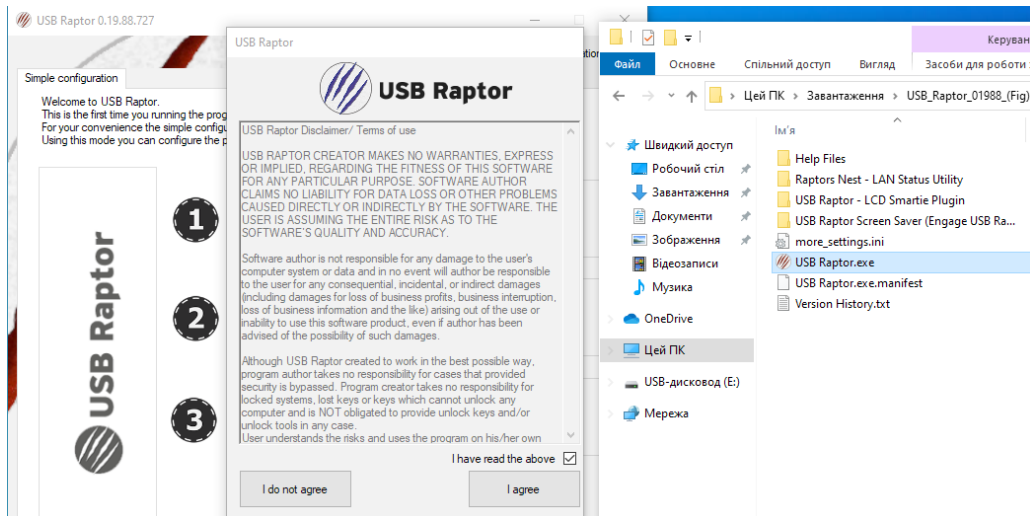


Рис. 4. Запуск утиліти USB Raptor

Вставити у комп'ютер флеш-накопичувач і через головне меню програми встановити пароль резервного розблокування системи при виході із ладу флеш-накопичувача, створити файл розблокування unlock.k3y та увімкнути USB Raptor (рис. 5).

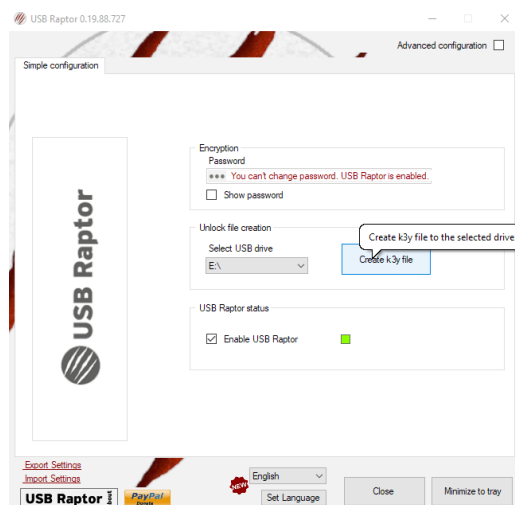


Рис. 5. Налаштування і увімкнення USB Raptor

Перевірити функціонування автоматичного блокування/розблокування ОС Windows після видалення/підключення флеш-накопичувача.

Здійснити спробу розблокування без флеш-накопичувача через введення паролю.

Модуль: Убезпечення від неправдивих повідомлень



Практична вправа:

«Інструменти виявлення неправдивих повідомлень»



Навчальна мета заняття: навчитися перевіряти окремі відомості в мережі Інтернет на достовірність.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет.

Порядок проведення заняття

Для перевірки повідомлень та інших матеріалів на предмет їх актуальності та достовірності можуть бути використані різні аналітичні методи. Для полегшення цього процесу також варто застосовувати низку технічних рішень.

Розширення **Fake Profile Detector (Deepfake, GAN)** – інструмент, який працює в браузері на базі Chrome або Chromium і дає змогу ідентифікувати зображення, створені з використанням штучного інтелекту (рис. 1). Саме тому, якщо обличчя реальної людини додано до іншого зображення, воно теж визначатиметься як справжнє. Розширення доступне за посиланням <https://chrome.google.com/webstore/detail/fake-profile-detector-dee/jbpcgcnhnmjmajjkgdaogpgfebnokpcc/related?hl=en-US>.

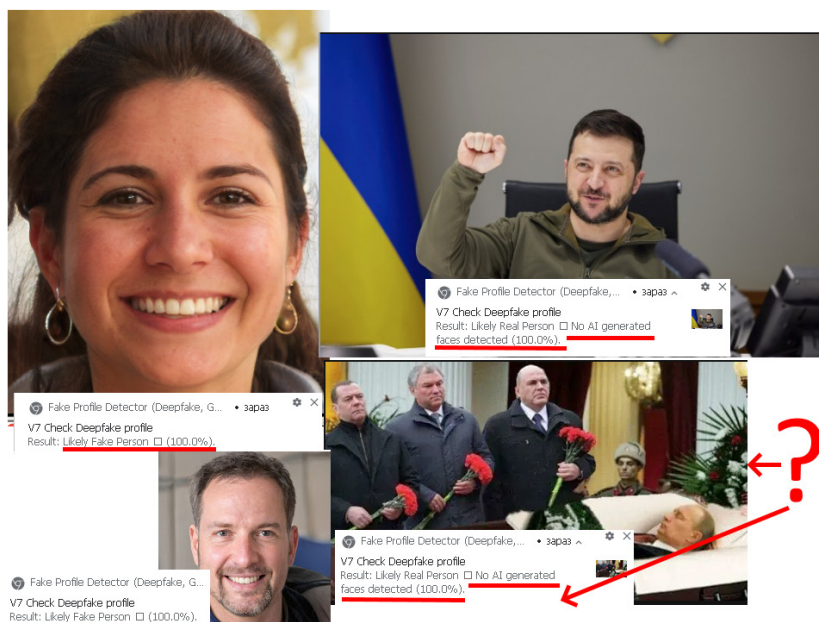


Рис. 1. Результат роботи розширення з виявлення дипфейків

Сервіси Sensity (platform.sensity.ai/login?redirect=%2Fdeepfake-detection), **Advanced AI Image Detector** (contentatscale.ai/ai-image-detector/), **Advanced AI Image Detector** (contentatscale.ai/ai-image-detector/), **Maybe's AI Art Detector** (huggingface.co/spaces/umm-maybe/AI-image-detector), **Is your image GAN generated?** (gan-detector-mayachitra.azurewebsites.net/), **AI or Not** (aiornot.optic.xyz/#home) та Illuminarty (app.illuminarty.ai/#/) виконують подібну функцію (рис. 2).

Сервіс **Forensically** (29a.ch/photo-forensics) дозволяє з використанням нескладних методів аналізу спробувати зрозуміти, чи вносилися до зображення якісь зміни.

Розширення **Deepfake Detection** (<https://github.com/deep2universe/DeepFakeChrome>) призначено для виявлення DeepFake-відео в сервісі YouTube. Також для ідентифікації фейкового відео призначено сервіс **Scan & Detect Deepfake Videos** (<https://scanner.deepware.ai>).

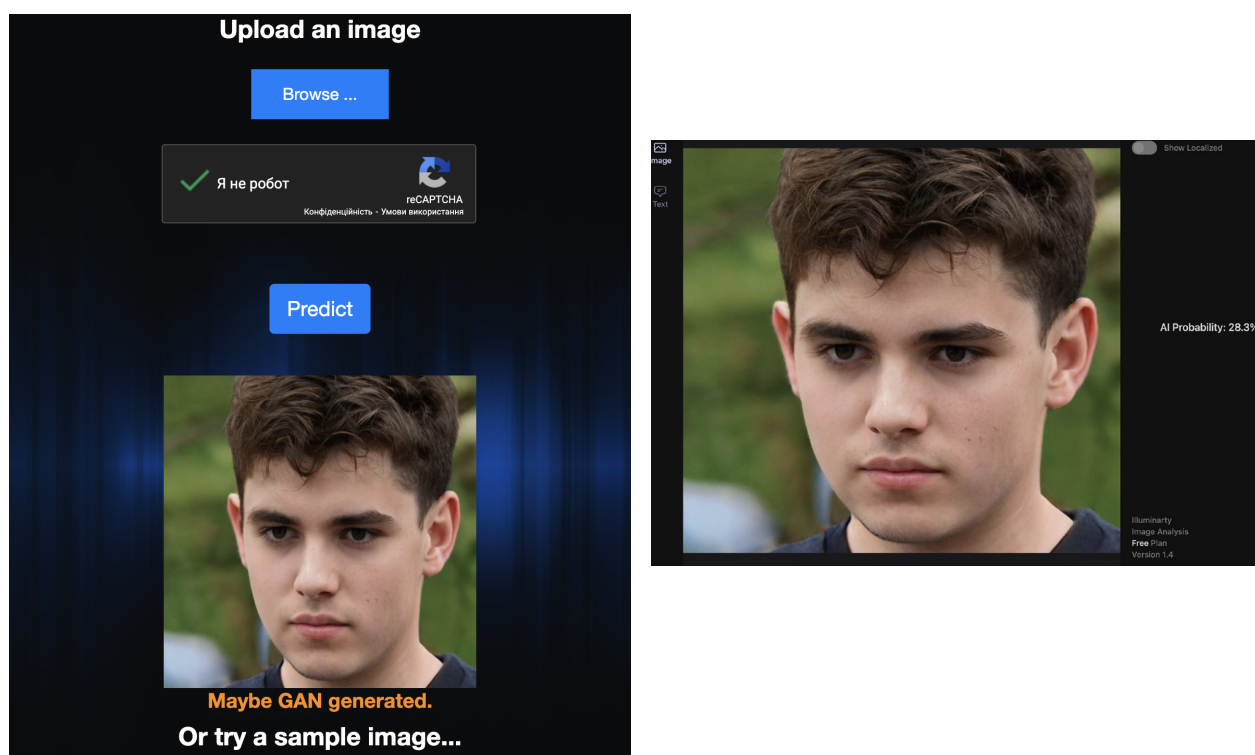


Рис. 2. Результат роботи сервісів з виявлення зображень, згенерованих за допомогою системи штучного інтелекту

Зображення можуть не мати ознак маніпуляцій, проте використовуватися у неправдивих повідомленнях у різних контекстах. Для того, щоб знайти першоджерело відповідних малюнків, можна використовувати розширення Who stole my pictures (рис. 3).

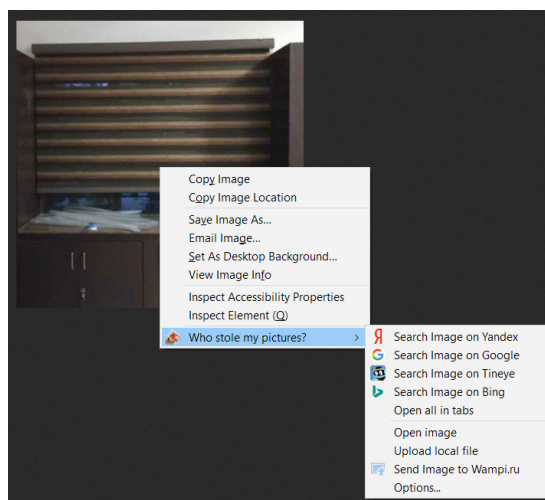


Рис. 3. Використання розширення для пошуку зображень

Завантажити описане розширення можна за адресами:

- ▶ для браузера Chrome (<https://chrome.google.com/webstore/detail/who-stole-my-pictures/mcdbnfhkikiofkkioppioekloflmaibd>);
- ▶ для браузера Firefox (<https://addons.mozilla.org/ru/firefox/addon/who-stole-my-pictures/>).

Подібними до описаного розширення є «**Fake news debunker by InVID & WeVerify**» (<https://www.invid-project.eu/tools-and-services/invid-verification-plugin/>), RevEye reverse image search (<https://chrome.google.com/webstore/detail/reveye-reverse-image-sear/keaaccljhehbbapnphnmpiklalfhelgf>), **Dessant Search by Image** (<https://github.com/dessant/search-by-image>).

Для аналізу тексту на предмет його створення за допомогою штучного інтелекту можна використати ресурс **GPTZero** (github.com/BurhanUITayyab/GPTZero, gptzero.me), **AI Detector** (contentatscale.ai/ai-content-detector/), **AI Content Detector** (copyleaks.com/ai-content-detector).

Створіть кілька зображень за допомогою ресурсу thispersondoesnotexist.com або generated.photos/faces та розмістіть їх у своєму профілі в соціальній мережі.

За допомогою описаних програмних продуктів спробуйте перевірити завантажені вами зображення на справжність. Спробуйте здійснити перевірку із зображеннями, опрацьованими Телеграм-ботом **@Pix2MixV2Bot**. Для різних фотознімків самостійно опрацюйте сервіс **Am I Real?** (<https://seintpl.github.io/AmIReal/>).

Перейдіть за посиланням olx.com та знайдіть кілька оголошень з продажу ігрових приставок. За допомогою розширення «Who stole my pictures» або «Fake news debunker by InVID & WeVerify» перевірте, чи немає серед фотографій у знайдених оголошеннях зображень, завантажених з інших сайтів.

Згенеруйте текст за допомогою однієї з систем генеративного штучного інтелекту, перевірте його за допомогою gptzero.me.



Альтернативна практична вправа:

«Агрегація каналів новин та аналіз відомостей з окремих каналів системи Telegram»



Навчальна мета заняття: навчитися швидко переглядати інформацію з кількох каналів новин одночасно та з використанням спеціальних сервісів аналізувати відомості з Telegram-каналів.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет, Telegram-Desktop.

Порядок проведення заняття

Одне з досить цікавих джерел інформації, в якому події подаються із прив'язкою до мапи, є ресурс Live Universal Awareness Map («Liveuamap» <https://liveuamap.com/>), який позиціонує себе як незалежний глобальний новинний та інформаційний сайт, присвячений висвітленню різноманітних важливих тем, включаючи конфлікти, питання прав людини, протести, тероризм, розгортання озброєнь, питання охорони здоров'я, стихійні лиха та погодні умови, з широкого спектру джерел. Одним з головних напрямів роботи цього сайту є висвітлення подій на лінії зіткнення з російським агресором (рис. 1).

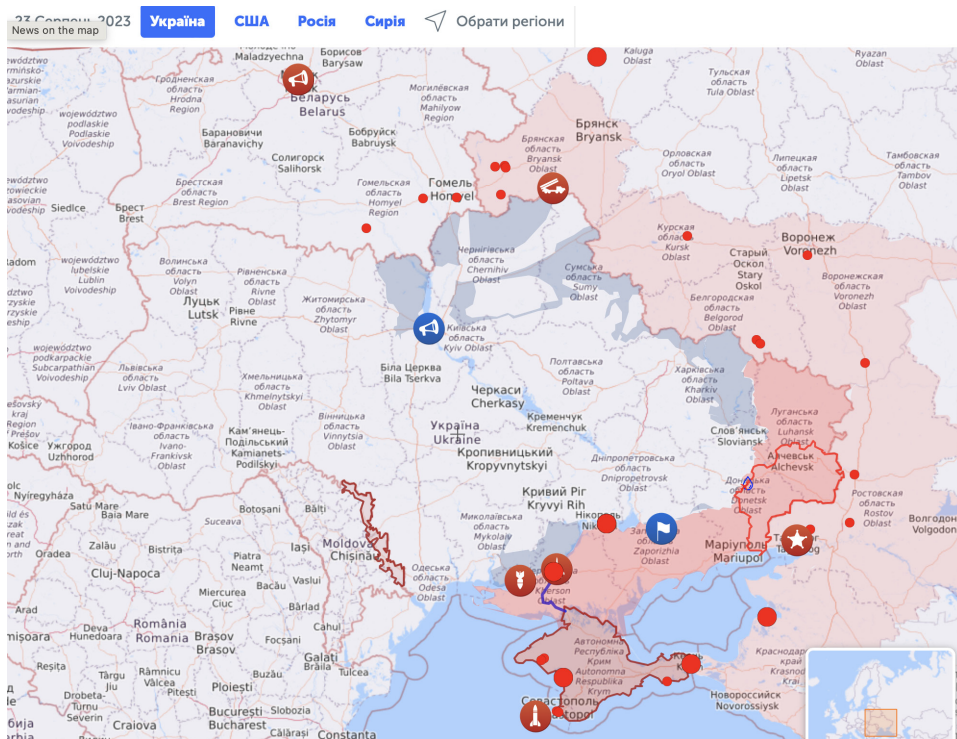


Рис. 1. Зовнішній вигляд однієї зі сторінок liveuamap.com

Якщо уважно вивчити цей ресурс, то можна побачити значну кількість джерел Telegram, з яких наводиться підтвердження тієї або іншої події. І дійсно: сьогодні у мережі Telegram є багато офіційних осіб, новинних агентств, блогерів, які регулярно представляють контент для користувачів. Враховуючи викладене, вбачається за доцільне запропонувати простий механізм одночасного перегляду інформації з кількох каналів у Telegram та деякі інструменти аналізу відомостей з Telegram-каналів, у тому числі з метою оцінки ступеню довіри до того або іншого джерела.

Для того, щоб прискорити та спростити процес перегляду повідомлень у тому або іншому Telegram-каналі, можна представити наведені в ньому повідомлення у вигляді RSS-стрічки. З цією метою можна скористатися сервісом RSSHub (<https://rsshub.app/>). Додати у RSSHub можна будь-який Telegram-канал, який має функцію «веб-перегляду», тобто з URL-адресою, яка починається з <https://t.me/s/>.

Для перетворення у RSS-стрічку даних з каналу потрібно сконструювати такий URL:

https://rsshub.app/telegram/channel/НАЗВА_КАНАЛУ

Після цього варто об'єднати отримані RSS-стрічки у єдиному веб-документі, який можна переглядати, автоматично перекладати, аналізувати тощо. Для вирішення завдання такого об'єднання можна скористатися сервісом FEED. INFORMER (<http://feed.informer.com/>).

Після реєстрації у сервісі з'явиться можливість створення дайджестів, які міститимуть набори RSS-стрічок за обраним напрямом (рис. 2).

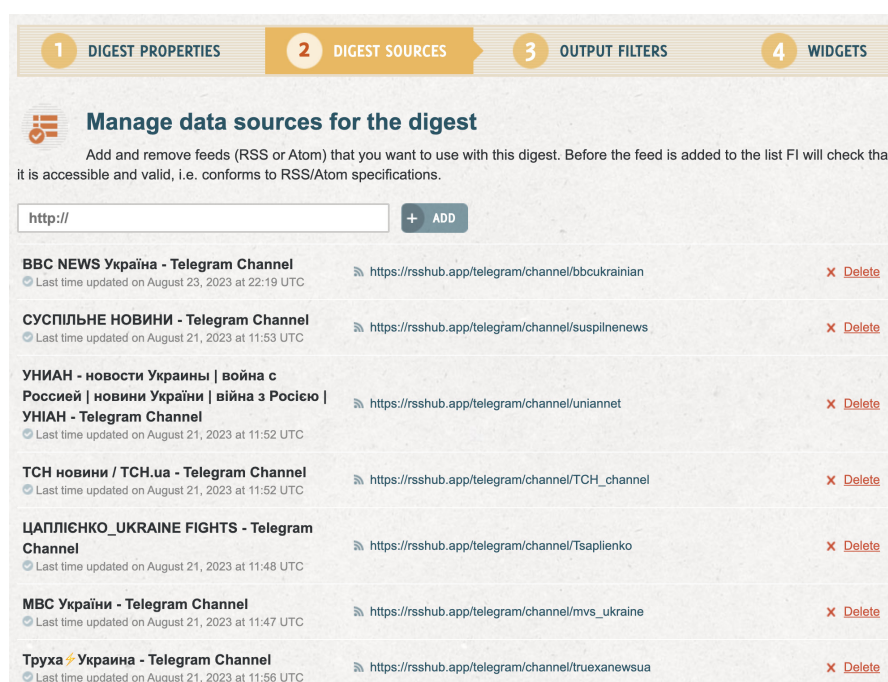


Рис. 2. Формування дайджесту

Результат можна переглядати через відповідний віджет (рис. 3) або у машинному вигляді для подальшої передачі до відповідних програм.

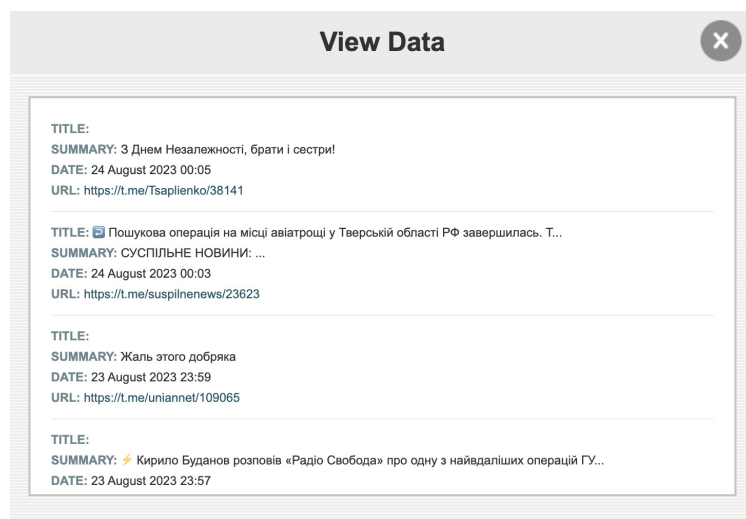


Рис. 3. Перегляд дайджесту у зручному для людини вигляді

За необхідності автоматизований аналіз відповідних каналів можна здійснити з використанням сервісу Chatanalytics (<https://github.com/mlomb/chat-analytics>). Приклад такого аналізу наведено на рис. 4.

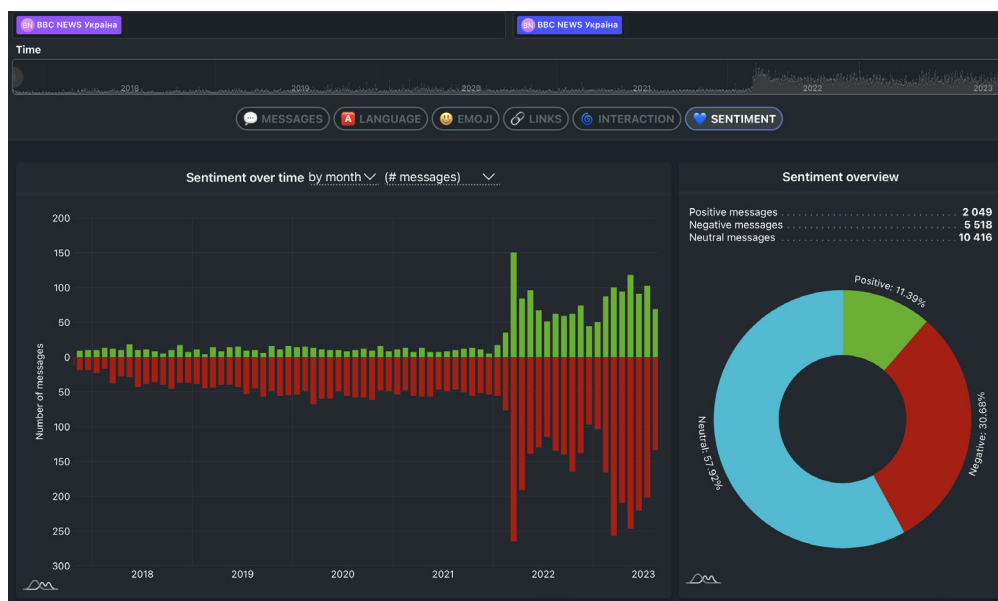


Рис. 4. Аналіз одного з Telegram-каналів

За допомогою сервісу Chatanalytics можна проводити аналіз чатів не тільки для системи Telegram, а й Discord Messenger, WhatsApp.

Враховуючи одержані відомості, створіть дайджест з кількох тематичних англomовних або арабomовних Telegram-каналів. З використанням електронного перекладача автоматизуйте переклад наведених у них відомостей українською мовою.

Проведіть аналіз Telegram-каналу.

Модуль: Соціальна інженерія



Практична вправа:

«Аналіз поштового повідомлення»



Навчальна мета заняття: отримати практичні навички аналізу поштового повідомлення.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**.

Фішингові повідомлення часто надходять користувачам за допомогою електронної пошти.

Змоделюємо ситуацію, яким чином це може відбуватися та як можна запобігти цьому негативному явищу.

Спершу слід зареєструвати тестову поштову скриньку, на яку будемо одержувати відповідні повідомлення. Після реєстрації електронної поштової скриньки слід надіслати на неї неправдиве повідомлення з підміною заголовка. Для цього можуть бути використані сервіси <https://emkei.cz/>, <https://anonymousemail.me/> тощо. Приклад відповідним чином сформованого листа наведено на рис. 1.

From Name:	Департамент персоналу
From E-mail:	hh@ministry.gov.ua
To:	???@proton.me
Subject:	Пропозиція роботи
Attachment:	Вибрати файл Файл не вибрано
	Attach another file
	Advanced Settings
Content-Type:	☐ text/plain ☒ text/html ☐ Editor
Text:	<pre><p>Канцелярія Міністра</p> <p>Добрий день, хочу запропонувати Вам посаду в Міністерстві. </p> <p>Заповніть, будь-ласка, форму за посиланням example.gov.ua </p></pre>

Рис. 1. Відправлення неправдивого повідомлення

У результаті на поштову скриньку надійде лист як на рис. 2.

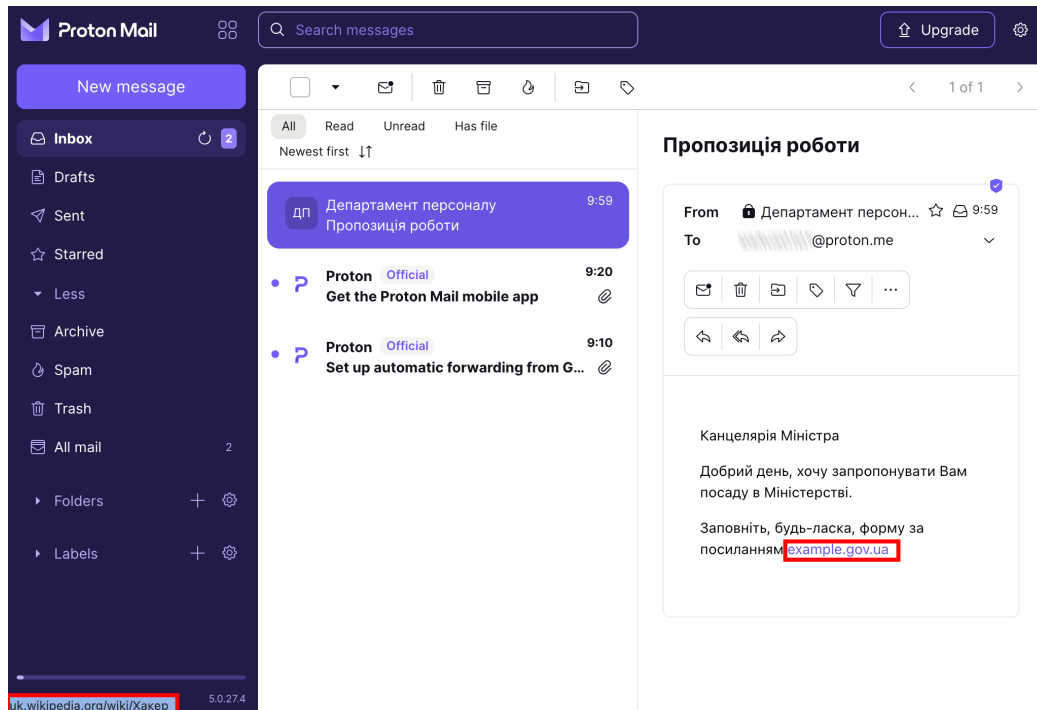


Рис. 2. Повідомлення, що надійшло

Для того, щоб виявити підробку в листі, потрібно дослідити його поштовий заголовок. Для цього слід після відкриття листа натиснути «Переглянути заголовок».

```
Return-Path: <hh@ministry.gov.ua>
X-Original-To: ???@proton.me
Delivered-To: ???@proton.me
Received: from emkei.cz (emkei.cz [89.187.129.22]) (using TLSv1.3 with cipher
TLS_AES_256_GCM_SHA384 [256/256 bits]
key-exchange X25519 server-signature RSA-PSS [4096 bits] server-digest SHA256)
(No
client certificate requested) by mailin005.protonmail.ch (Postfix) with ESMTPS id
4RYPgY4Bbzz9vNPV for <???@proton.me>; Sun, 27 Aug 2023 06:59:21 +0000 (UTC)
Received: by emkei.cz (Postfix, from userid 33) id 2E8B35849E1; Sun, 27 Aug 2023
08:59:15
+0200 (CEST)
Authentication-Results: mailin005.protonmail.ch; dmarc=none (p=none dis=none)
header.from=ministry.gov.ua
Authentication-Results: mailin005.protonmail.ch; spf=none smtp.mailfrom=ministry.
gov.ua
Authentication-Results: mailin005.protonmail.ch; arc=none smtp.remote-
ip=89.187.129.22
Authentication-Results: mailin005.protonmail.ch; dkim=none
To: ???@proton.me
Subject: =?utf-8?B?0J/RgNC+0L/QvtC30LjRhtGW0Y8g0YDQvtCx0L7RgtC4?=
```


From: =?utf-8?B?ltCU0LXQv9Cw0YDRgtCw0LzQtdC90Ylg0L/QtdGA0YHQvtC90LDQu9GDIiA8?=
=?utf-8?B?aGhAbWluaXN0cnkuZ292LnVhPg==?=

X-Priority: 3 (Normal)

Importance: Normal

Errors-To: hh@ministry.gov.ua

Reply-To: hh@ministry.gov.ua

Content-Type: text/html

Message-Id: <20230827065915.2E8B35849E1@emkei.cz>

Date: Sun, 27 Aug 2023 08:59:15 +0200

X-Rspamd-Server: cp3-mailin-005.plabs.ch

X-Rspamd-Queue-Id: 4RYPgY4Bbzz9vNPV

X-Rspamd-Action: add header

X-Spamd-Result: default: False [8.80 / 25.00]; MISSING_MIME_VERSION(2.00)[
MIME_HEADER_CTYPE_ONLY(2.00)[
PHISHING(2.00)[example.gov.ua->wikipedia.org];
HFILTER_FROMHOST_NORES_A_OR_MX(1.50)[ministry.gov.ua]; AUTH_NA(1.00)[
MIME_HTML_ONLY(0.20)[
ONCE_RECEIVED(0.10)[
FROM_EQ_ENVFROM(0.00)[
MIME_TRACE(0.00)[0:~]; RCVD_TLS_LAST(0.00)[
RCVD_COUNT_ONE(0.00)[1;
NEURAL_SPAM(0.00)[0.986]; ASN(0.00)[asn:35592, ipnet:89.187.129.0/24, country:CZ];
R_DKIM_NA(0.00)[
DMARC_NA(0.00)[ministry.gov.ua]; RCPT_COUNT_ONE(0.00)[1;
FROM_HAS_DN(0.00)[
ARC_NA(0.00)[
HAS_X_PRIO_THREE(0.00)[3]; R_SPF_NA(0.00)[no SPF
record]; REPLYTO_ADDR_EQ_FROM(0.00)[
TO_MATCH_ENVRCPT_ALL(0.00)[
TO_DN_NONE(0.00)[
HAS_REPLYTO(0.00)[hh@ministry.gov.ua]

X-Spam: Yes

X-Pm-Spam: 0yezJl6cihyJeYR3pi42biOpJJvbmsClel1msjN3X3blJp7ljBINlloj2sUjLIITJ
o4ljsjgLIBISiQ0Ti0x0wiOSPFIUR9FQEVkUUSUN9OSUwjoILJCfiVGZWdfd5maW6ylbeJ
yQE9kU jl7pBflnh3BcbIS6x4CMzM2cU00T3zEMMkDy1kDOSNiw1haWf2VZbFmt6ISZm
lzhFjdGv19aYNnl lZncFZy8IzMDxDgMMICs1Jnlbu91IYWijolYxWslZWLXY1RVzcmiiwlbF
Wpj9FbXYIR9yZ2uV9e Y1WlioJlVVEBRFQVsyIU1mhfxWa2Y0FdvZWfnlccJHv6liYCM44Y5
MT9jIMf0XshNmIGdnVJ5b3 ijoIVBVEFRVQyUsINylniWQaOli2hVGNjZ0QFhYjITdMNMm
3mJjMDN1QYiYTiSwfcE2iisnOXafN Bhc36SlbMwSivN2cmciUYsOjjnNlbJ3l6lCZiN14Jy
LCvXBZcQniisnOkTf95TREP0ZXU9IGN9kU jlbP4wNCiSwXQFkZfNVRTNiAsxOlSjALINnj
IJ3biOwAQ5LjiTkOXwSiGB1U0XFh9fTETEFUUIy6 w0yWjLdBJELCN0ISXF0EfB1UITeH1
BT0iU4SOslwdljLCLTJZfUEOk9TRIS6uAzWFM50hUIkfUxT TVUTHF0USR6lAuWzsF0M
l1kJfVUTFSNR9PTFZkxTlpjbx4CMSXiwRNSFNf9TS1UFP50X0XUhxftU HEFVlPjb04C
MSXiWINTUIV9RRFUEfJVR1QZRVfUEM05TWIS6uAzWVMs0RWIITF9RUFEDS9VRVQJR
9NT1GU5SUIC6uAzWFM91fx0=

X-Pm-Origin: external

X-Pm-Transfer-Encoding: TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256
bits)

X-Pm-Content-Encoding: on-delivery

X-Pm-Spamscore: 6

X-Pm-Spam-Action: inbox

Mime-Version: 1.0

Базовий формат поштових повідомлень (листів, messages) і статей USENET (article) визначається RFC 822 і його «спадкоємцем» RFC 2822. Кожне повідомлення (лист, message, стаття, article) складається з конверта і вмісту. Конверт зберігає адресну інформацію, необхідну для відправлення і передачі повідомлення одержувачеві. Формат конверта визначається середовищем розповсюдження. Для його автоматичного створення може використовуватися інформація зі вмісту повідомлення. Стандарт визначає тільки формат вмісту повідомлення і лише у момент передачі, тобто повідомлення можуть зберігатися абсолютно в іншому форматі. Повідомлення ділиться на рядки і складається з секції заголовків і тіла повідомлення (можливо, порожнього).

Заголовок електронного поштового листа можна дослідити або вручну, або за допомогою програм чи сервісів (рис. 3).

IP Address	93.99.104.210
Country	Czech Republic 
Region	-
City	-
ISP	Liberty Global
Organization	Liberty Global
Latitude	50.0848
Longitude	14.4112

Рис. 3. Результат аналізу заголовка поштового листа

Виходячи з даних, наведених в теоретичних відомостях:

1. Зареєструвати поштову скриньку та надіслати тестове повідомлення.
2. Проаналізувати заголовок та тіло листа зі своєї електронної поштової скриньки. Визначити адресу відправника та маршрут руху листа за допомогою сервісів:

<https://www.iplocation.net/trace-email>, <https://mha.azurewebsites.net/>,
<https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=73671c03-950e-4f79-88ee-f78a785b2eef>, <https://www.ip2location.com/free/email-tracer>, <https://www.whatismyip.com/email-header-analyzer/>.

Приклад. «Розшифровка типового заголовка листа»

Return-path: ****@ukr.net – зворотна адреса, вказана відправником;

Received: from [212.9.224.21] (port=25 helo=mail-out.iptelecom.net.ua) – лист отримано від хосту

mail-out.iptelecom.net.ua з IP-адресою 212.9.224.21;

by mx5.mail.ru – ім'я комп'ютера, який приймав повідомлення;

with esmtp id 1COINS-000FOL-00 – комп'ютер, що прийняв повідомлення, надав йому ідентифікаційний номер 1COINS-000FOL-00;

Tue, 18 Nov 2008 02:14:18 +0300 – передавання листа здійснювалося у вівторок, 18 листопада 2008 року, о 02:14:18 за часом третього часового поясу, який випереджає Гринвічський часовий пояс на 3 години, звідси «+0300»;

Received-SPF: none (mx5.mail.ru: 212.9.224.21 is neither permitted nor denied by domain of ukr.net) client-ip=212.9.224.21 – отримана відповідь на SPF-запит. Технологія SPF (Sender Policy Framework) є одним зі способів ідентифікації відправника електронного листа та надає додаткову можливість фільтрування потоку пошти на наявність у ньому повідомлень зі спамом. За допомогою SPF пошта поділяється на «дозволену» й «заборонену» відносно домена одержувача чи відправника. В цьому випадку поштовий сервер-одержувач mx5.mail.ru здійснив SPF-запит до домена ukr.net, де було отримано відповідь про фактичну відсутність SPF-захисту (дослівно: mx5.mail.ru здійснив SPF-запит до домена ukr.net про наявність у списках IP-адреси 212.9.224.21, на що було отримано відповідь про те, що цю адресу не внесено ані в дозволені, ані в заборонені списки SPF домена ukr.net);

envelope-from=**@ukr.net** – заголовок, який додається до листа деякими поштовими програмами під час доставки кінцевому одержувачу;

helo=mail-out.iptelecom.net.ua;

Received: from h136.246.159.dialup.iptcom.net ([213.159.246.136]:64011 «HELO copm1» ident: «NO-IDENT-SERVICE[2]» whoson: «s-m-i-t»);

by pechkin.iptelecom.net.ua with SMTP id S358789AbUKAXOS (ORCPT <rfc822;igoset@mail.ru> + 3 others);

Tue, 18 Nov 2008 01:14:18 +0200 – час, коли одержано лист;

Message-ID: <021501c4c068\$4d89ba20\$0200a8c0@copm1> – процес одержання листа первинним провайдером для подальшого пересилання з ПК, підключеного за допомогою модемного з'єднання (h136.246.159.dialup.iptcom.net). Розшифрування є аналогічним вищевикладеному;

From: ****@ukr.net – напис на «конверті», від кого лист;

To: <***@mail.ru>, <***@ukrpost.net>, <***@mail.ru>, <***@ukr.net>, <***@yahoo.co.uk>, <***@ok.ru>, <***@yandex.ru>, <****@mail.ru>, <*****@mail.ru>, <***@bk.ru>, *@ukr.net – адреси доставки листа;

Subject: =?koi8-r?B?8NLFxMzP1sXOycU=?= – тема листа (у разі заміни кодування тема матиме вигляд напису «Предложение»);

Date: Tue, 18 Nov 2008 00:52:14 +0200 – дата та час створення листа (вівторок 2 листопада 2008 р., о 00:52:14 на комп'ютері зі встановленим другим часовим поясом);

MIME-Version: 1.0 – версія стандарту, відповідно до якого створено цей лист;

Content-Type: multipart/alternative – формат змісту листа. Визначається тип інформації в листі та спосіб її відображення. Зокрема, встановлюється кодування листа, якщо використовується який-небудь національний набір символів;

boundary=»-----= _NextPart_ 000_0015_01C4C076.3170DA90» – стандартизація розбивання великих листів на кілька частин. У полі «Content-Type» після значення «multipart/<subtype>» зазначається рядок – унікальний обмежувач фрагментів «boundary=<boundary string>». Потім перед кожним фрагментом пишеться цей рядок з двома мінусами попереду, а в кінці фрагментації – ще один рядок, який завершується такими самими двома мінусами.

X-Priority: 3 – пріоритет листа, позначений цифрами.

X-MSMail-Priority – нестандартне поле Microsoft – пріоритет листа. Буває «звичайним», «невідкладним» та «не невідкладним». Зазвичай використовуються слова: «Normal», «Urgent», «Non-urgent». Може впливати на швидкість обробки та передачі листа різними проміжними поштовими системами;

X-Mailer: Microsoft Outlook Express 5.50.4927.1200 – інформація про поштову програму, яка використовувалася для створення листа;

X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4927.1200 – інформація про фірму – виробника програмного забезпечення;

X-Spam: Not detected – лист не визначено як спам.



Альтернативна практична вправа:

«Захист від фішингових атак»



Навчальна мета заняття: ознайомлення з принципами фішингових атак та протидії ним.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, **підкреслено**.

Фішинг (англ. *fishing* – рибна ловля) – одержання доступу до конфіденційних даних користувачів, що досягається шляхом проведення масових розсилок електронних листів від імені популярних брендів, наприклад, від імені соціальних мереж (Facebook, Twitter, Instagram), банків (Приватбанк, Ощадбанк), інших сервісів (Google.com). У листі часто міститься пряме посилання на сайт, який зовні складно відрізнити від справжнього. Опинившись на такому сайті, користувач може повідомити інформацію, що дозволяє одержати доступ до облікових записів, тощо.

Фейк (Fake) – точна копія головної сторінки (або будь-якої іншої сторінки) оригінального сайту, яка використовується для фішингу з метою отримання конфіденційних даних користувачів.

Для демонстрації техніки фішингу можуть бути використані кілька способів. Скористаємося одним з них.

1. Створити фейкову сторінку.

Для створення фейку сайту можна скористатися такою технікою:

- ▶ завантажити оригінальну сторінку сайту з формою авторизації;
- ▶ відкрити вихідний код оригінальної сторінки (наприклад, з використанням правої кнопки миші);
- ▶ скопіювати вихідний код сторінки в текстовий файл та назвати його index.html.

2. Для розміщення сторінки в мережі слід завантажити утиліту ngrok. Для роботи з утилітою ngrok слід зареєструватися та отримати токен відповідно до інструкції (<https://dashboard.ngrok.com/get-started/setup>).

Запустити її з командного рядка:

ngrok http 80

Завантажити набір Uniform Server для створення та управління сайтами та привести його у готовність.

Створити в папці UniServerZ\www каталог з назвою сайту скопійованої сторінки.

Розмістити в папці www/назва_сайту скрипти сайту.

Запустити UniController (рис. 1).

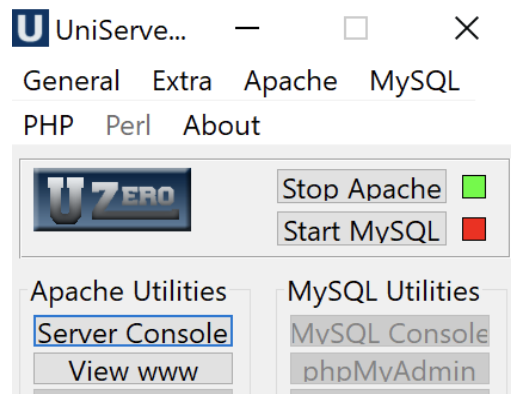


Рис. 1. Запуск Uniform Server

Перевірити роботу сайту.

Одним з додаткових інструментів фішингу може бути телефонування жертви з підміненого номера (Caller ID Spoofing), приклад налаштування та результат якого зображено на рис. 2.

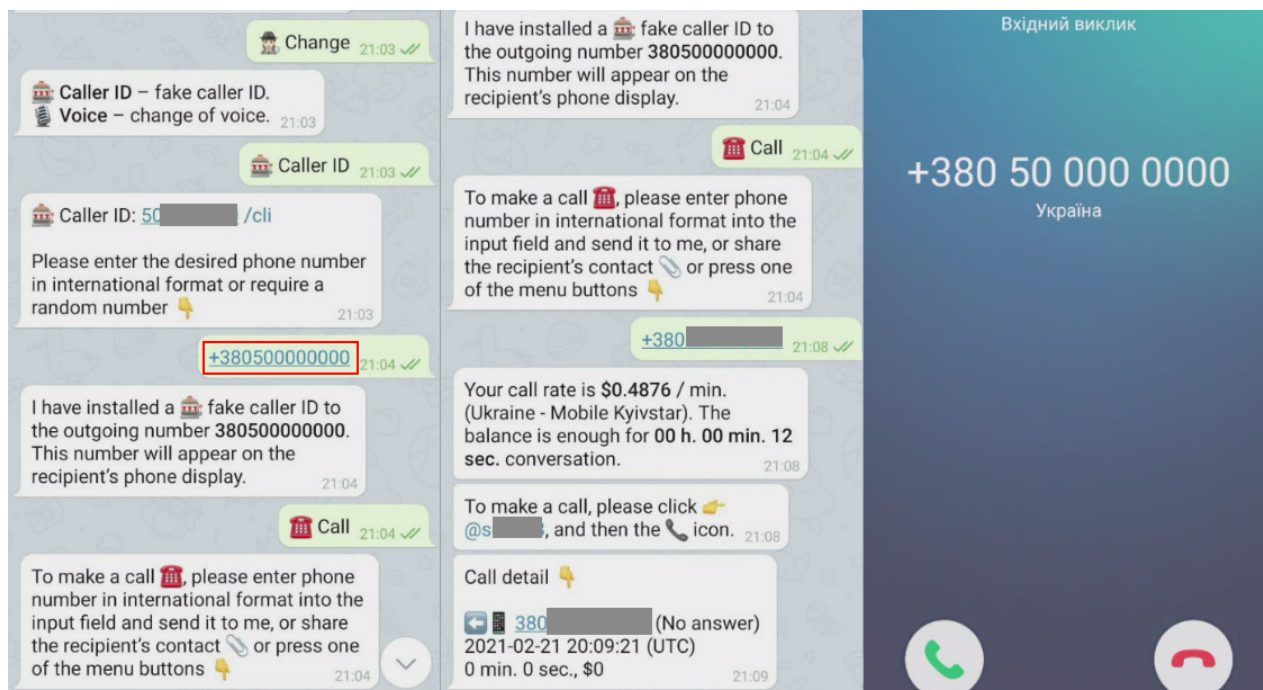


Рис. 2. Caller ID Spoofing

Для того, щоб захиститись від атак подібного виду, потрібно уважно перевіряти повідомлення, які надходять, та користуватись антифішинговими інструментами. Відповідні інструменти нерідко вбудовано у браузер.

Модуль: Безпечне користування мережею Інтернет



Практична вправа:

«Безпечний перегляд веб-сторінок та способи організації безпечного з'єднання в мережі»



Навчальна мета заняття: здійснити налаштування браузера та встановлення додаткових плагінів для безпечного серфінгу в мережі; відпрацювати різні технології забезпечення з'єднання в мережі.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет.

Перелік VPN-сервісів та проксі-серверів:

- ▶ free-proxy.cz
- ▶ vpnbook.com
- ▶ protonvpn.com

Перегляд веб-сторінок, як правило, здійснюється за допомогою програм-браузерів, найпоширенішими серед яких є Chrome та Firefox. В усіх сучасних браузерах присутнє меню налаштувань, за допомогою якого можна здійснити налаштування безпеки та конфіденційності (рис. 1).

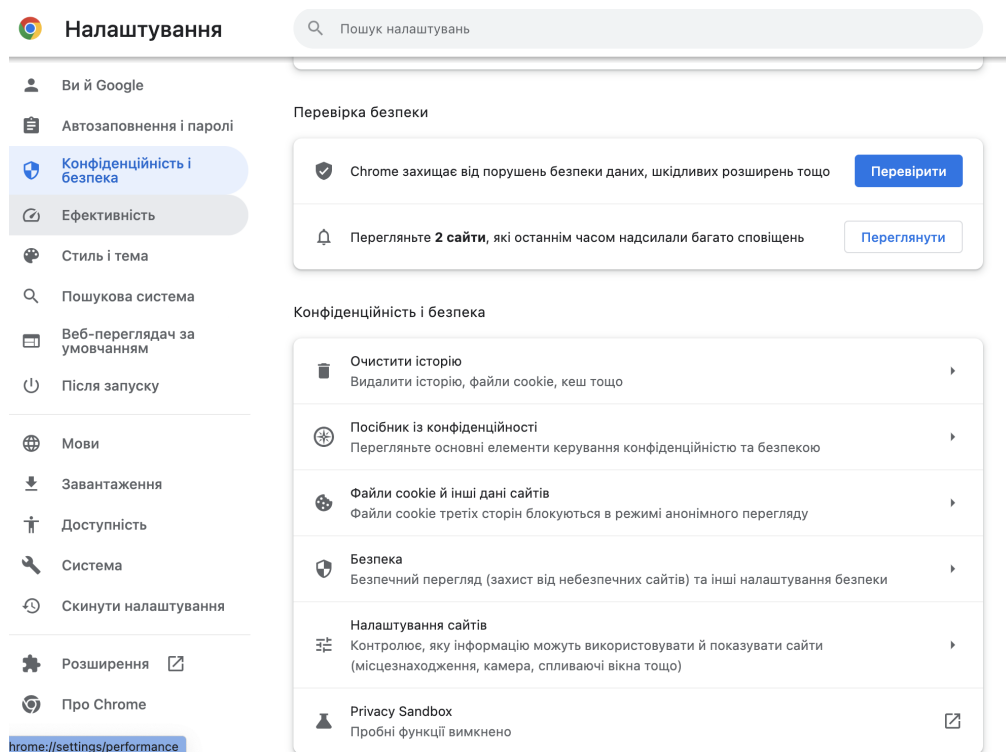


Рис. 1. Налаштування безпеки у браузері Chrome

Якщо налаштування безпеки не повною мірою влаштовують користувача, можна встановити додаткові плагіни. Як плагіни за напрямом безпеки можна навести:

- ▶ Adblock для блокування спливаючих вікон (<https://adblockplus.org/ru/download>);
- ▶ RequestPolicy для блокування міжсайтових запитів (<https://www.requestpolicy.com/>);
- ▶ Click&Clean для видалення тимчасових файлів у браузері (<https://www.hotcleaner.com/>).

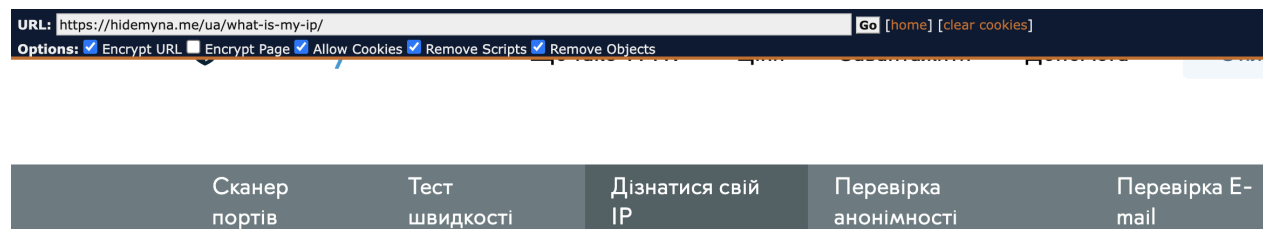
1. Налаштуйте параметри безпеки та конфіденційності браузера. Поясніть свій вибір налаштувань.

2. Встановіть додаткові плагіни, описані в матеріалах до заняття. Опишіть порядок їх використання.

Для налагодження безпечного з'єднання з віддаленими ресурсами може бути застосовано проміжні убезпечуючі механізми, зокрема проміжні проксі- або VPN-сервери. Для демонстрації роботи таких серверів можна здійснити таке.

Проксі-сервери

Відкрити сторінку <http://free-proxy.cz/en/web-proxylist/>, після чого обрати будь-який проксі-веб-сервер. Ввести у відповідному вікні адресу hidemyna.me/ua/what-is-my-ip або 2ip.ua. Оцінити одержані результати (рис. 2).



Дізнатися свою IP-адресу

Знаючи вашу IP-адресу, зловмисники можуть отримати дуже багато інформації. Нижче лише її мала частина.

Ваш IP-адреса	Хост	149-210-148-6.colono.transip.net
149.210.148.6	Система	macOS
Змінити IP-адресу	Ваш браузер	Chrome 115.0
	Звідки ви	Netherlands

Рис. 2. Результат використання проксі-сервера

VPN-сервери

На відміну від проксі-серверів, які працюють за окремими портами, VPN-сервери надають можливість організації повноцінного захищеного з'єднання між користувачем та відповідними ресурсами. Для користування VPN-сервером потрібно знати його налаштування та відповідні автентифікаційні дані.

Як правило, налаштувати відповідне підключення можна без необхідності встановлення додаткового програмного забезпечення. Для цього, наприклад, у системі Windows 10 слід відкрити «Центр управління мережами та спільним доступом» та створити нове з'єднання.

Далі слід вказати адресу VPN-сервера та перейти у розділ «Зміна параметрів адаптера» та двічі натиснути на новоутвореному з'єднанні. Після цього слід ввести відповідне ім'я користувача і пароль та дочекатися з'єднання.

Більш універсальний спосіб налаштування VPN-з'єднання полягає у використанні спеціальних програм для організації такої діяльності. З цією метою може бути використано, наприклад, безкоштовний застосунок OpenVPN, який можна завантажити за адресою: <https://openvpn.net/community-downloads/>.

Після встановлення програми відповідні файли налаштування з'єднання записуються у папку Config програми OpenVPN. Запустивши програму слід обрати відповідну конфігурацію та під'єднатися до VPN-сервера.

Альтернативним способом налаштування VPN є застосування окремих програмних клієнтів від надавачів послуг VPN. Як приклад наведемо порядок підключення Proton VPN (protonvpn.com). З метою використання відповідного застосунку слід завести обліковий запис на сайті protonvpn.com та завантажити застосунок для відповідної операційної системи ([account.protonvpn.com/downloads](https://protonvpn.com/downloads)).

У подальшому потрібно авторизуватися у завантаженому застосунку та просто обрати потрібний спосіб підключення (рис. 3).

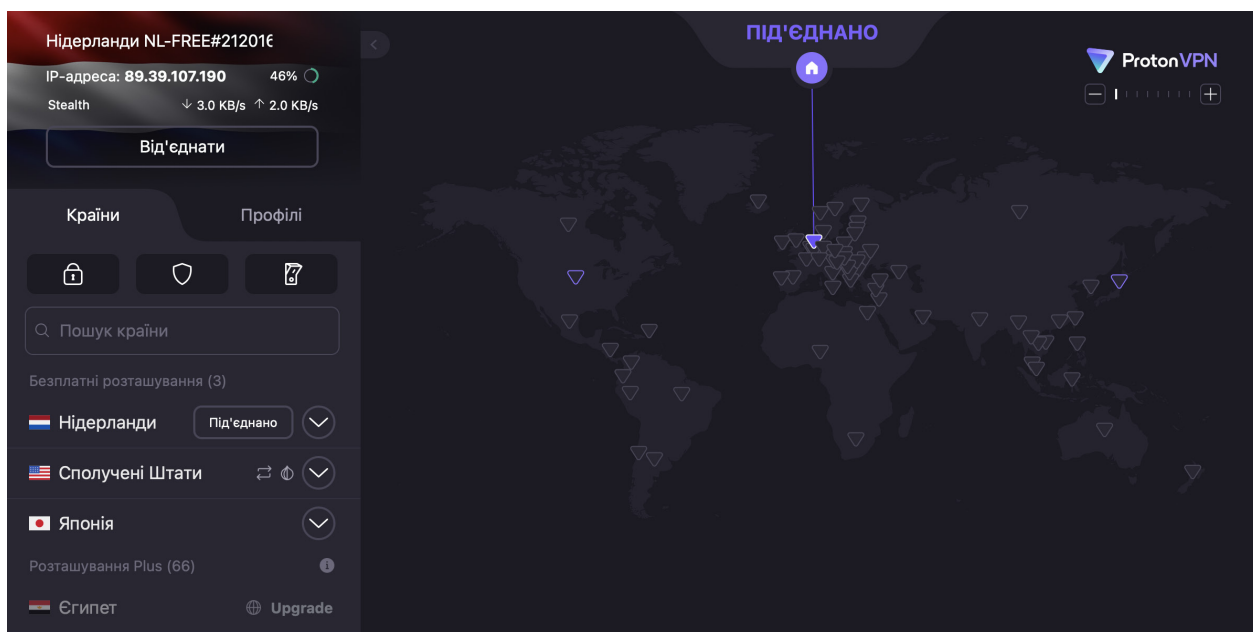


Рис. 3. Зовнішній вигляд клієнта Proton VPN

1. Відпрацювати підключення через одиничний та ланцюжок проксі-серверів.
2. Відпрацювати принаймні два способи налаштування VPN-з'єднання: 1) через налаштування параметрів мережевого підключення операційної системи та 2) за допомогою VPN Client).
3. Переконавшись у зміні параметрів виходу в мережу (наприклад, скориставшись сайтом 2ip.ua).
4. Встановити Firewall та антивірус ZoneAlarm.



Альтернативна практична вправа:
«Накладання електронного підпису»



Навчальна мета заняття: відпрацювати різні технології забезпечення з'єднання в мережі.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет.

Завдання, які потрібно виконати, підкреслено.

Реквізитом електронного документа є **електронний підпис** – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються та використовуються ним як підпис. Електронний підпис накладається за допомогою *особистого ключа* та перевіряється за допомогою *відкритого ключа*.

Отже, **особистий ключ** – це параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів, а **відкритий ключ** – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів.

Загальна схема накладання електронного підпису наведена на рис. 1, а його перевірки – на рис. 2.

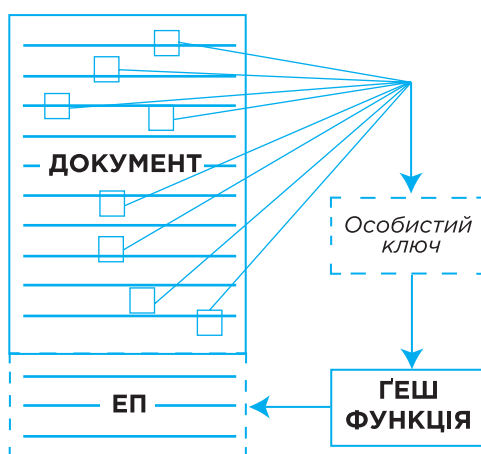


Рис. 1. Приблизна модель накладання електронного підпису



Рис. 2. Приблизна модель перевірки електронного підпису

Накладання електронного підпису не забезпечує конфіденційності документа, тобто його зміст **не шифрується**, але при цьому можна впевнитись у цілісності документа й *ідентифікувати його підписувача*.

Порядок проведення заняття

1. Одержати ключі електронного підпису через електронний кабінет у банку.
2. З використанням ресурсу sign.diia.gov.ua накласти електронний підпис на довільний файл. За допомогою сервісу sign.diia.gov.ua/verify перевірити цілісність документу. Змінити підписаний файл. Провести повторну перевірку.
3. З використанням електронного підпису авторизуватись за адресою <https://diia.gov.ua/services/informaciya-z-derzhavnogo-reyestru-rechovih-prav-na-neruhome-majno>. Одержати інформацію з державного реєстру речових прав.
4. З використанням електронного підпису авторизуватись на порталі електронних послуг Пенсійного фонду (portal.pfu.gov.ua). Перевірити відомості про свої відрахування.
5. З використанням електронного підпису авторизуватись в електронному кабінеті на порталі Державної податкової служби України (<https://cabinet.tax.gov.ua/>). Перевірити відомості про свої доходи.
6. Відпрацювати роботу програми «ІТ Користувач ЦСК-1» за адресою: acskidd.gov.ua/korustyvach_csk.

Модуль: Безпечне користування електронною поштою



Практична вправа:

«Двофакторна автентифікація поштового облікового запису. Менеджер паролів»



Навчальна мета заняття: відпрацювати навички налаштування двофакторної автентифікації для різних облікових записів та використання менеджера паролів.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет, веб-браузер Google Chrome, смартфони або телефони у слухачів.

Порядок проведення заняття

Створити безкоштовні особисті поштові облікові записи в доменах gmail.com та protonmail.com.

Налаштувати двофакторну автентифікацію через Google Authenticator для облікових записів gmail.com та protonmail.com.

Встановити і налаштувати менеджер паролів KeePass.

Для облікового запису gmail.com

Перейти у розділ «Ваш обліковий запис» – «Безпека» – «Як ви входите в обліковий запис Google». Обрати «Двохетапна перевірка» – «Розпочати» (рис. 1).

Як ви входите в обліковий запис Google

Своєчасно оновлюйте цю інформацію, щоб завжди мати доступ до облікового запису Google



Двохетапна перевірка

Двохетапну перевірку вимкнено



Ключі доступу

Почати використовувати ключі доступу



Рис. 1. Розділ налаштувань двохетапної перевірки

Обрати автентифікацію через коротке текстове повідомлення і зареєструвати особистий телефон через отримання коду в sms і вводу його у відповідному полі налаштувань.

Знову увійти в «Безпека» – «Вхід в обліковий запис Google» – «Двохетапна перевірка» – «Розпочати» та додати інші варіанти другого етапу перевірки, щоб підтверджувати свою особу, а саме «Додаток Google Authenticator». Завантажити за наданим посиланням у смартфон додаток «Генератор кодів Google» (рис. 2) та дотримуватися інструкцій щодо його налаштування.

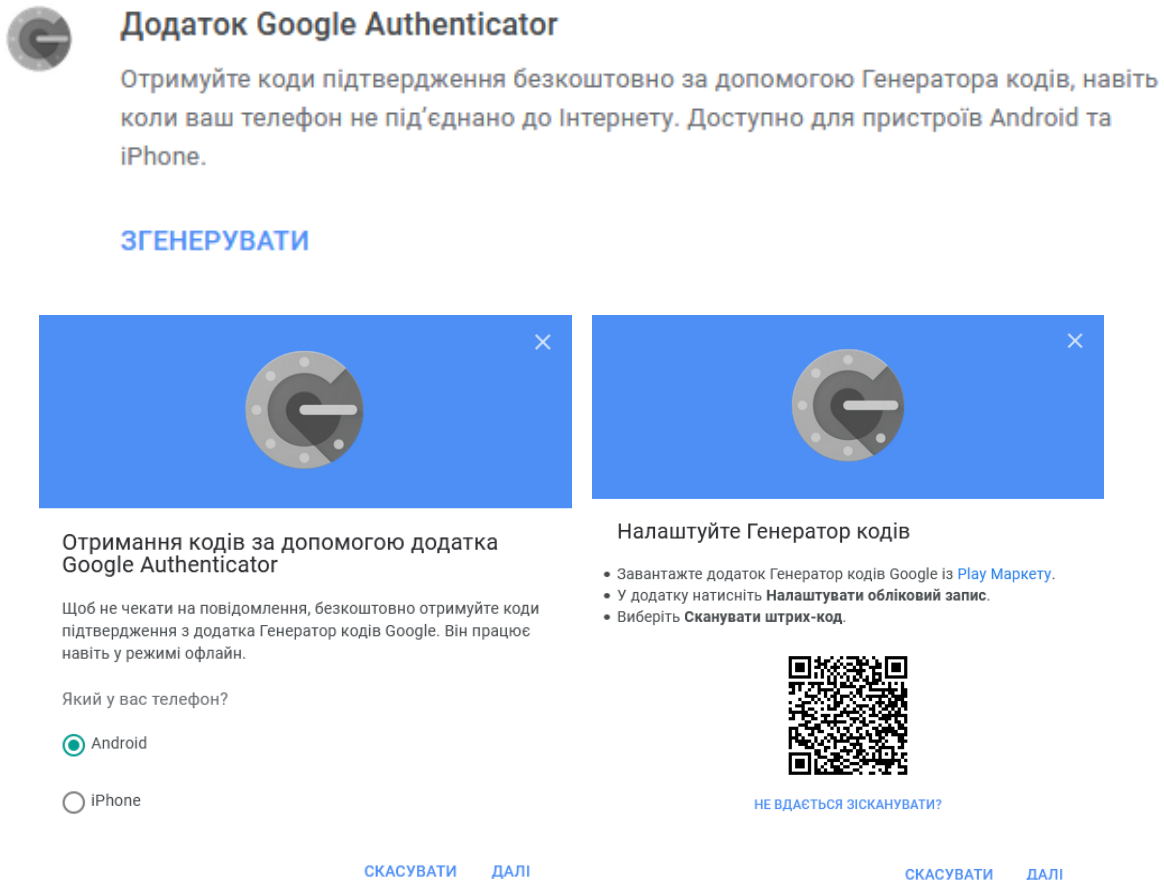


Рис. 2. Інструкції майстра налаштувань Google Authenticator

По закінченні налаштувань вийти із облікового запису та пройти вже двохетапну автентифікацію.

Для облікового запису protonmail.com

У поштовому обліковому записі protonmail перейти у розділ «Налаштування» – «Обліковий запис і пароль» – «Увімкнути двохетапну перевірку» (рис. 3).

Двоетапна перевірка

Розширте рівень захисту свого облікового запису. Необхідно проходити двоетапну перевірку щоразу під час входу в систему.

Програма автентифікації ⓘ



Ключ безпеки ⓘ



Налаштувати двоетапну перевірку

Скануйте цей код своїм пристроєм двоетапної перевірки, щоб налаштувати обліковий запис. [Ввести ключ вручну](#).



Скасувати

Далі

Налаштувати двофакторну автентифікацію

Скануйте цей QR-код своїм пристроєм двоетапної перевірки, щоб налаштувати обліковий запис.

[Ввести ключ вручну](#)



СКАСУВАТИ

ДАЛІ

Рис. 3. Інструкції майстра налаштувань двофакторної автентифікації

Скористатися вже встановленим у смартфоні застосунком Google Authenticator (встановлюється з Google Play або App Store) і налаштувати двоетапну автентифікацію. Вийти із облікового запису та пройти вже двоетапну автентифікацію.

Для облікового запису gmail.com

Перейти у розділ «Ваш обліковий запис» – «Безпека» – «Як ви входите в обліковий запис Google». Вибрати «Ключі доступу» – «Почати використовувати ключі доступу» – «Створити ключі доступу» (рис. 4), де буде зазначений мобільний пристрій Android, на якому вже автоматично створені ключі й активний відповідний обліковий запис Google.

← Ключі доступу

Ключі доступу дають змогу безпечно входити в обліковий запис Google за допомогою відбитка пальця, фейс-контролю, іншого способу розблокування екрана або апаратного ключа безпеки. Налаштовуйте ключі доступу лише на власних пристроях. [Докладніше](#)

**Почніть використовувати ключі доступу**
Додавши ключ доступу, ви зможете підтверджувати свою особу за допомогою відбитка пальця, фейс-контролю або розблокування екрана

Використовувати ключі доступу

Автоматично створені ключі доступу

Пристрої Android автоматично створюють ключі доступу, коли ви входите в обліковий запис Google. [Керувати пристроями](#)



Xiaomi Mi 5s

Останнє використання:
область, Україна

Chrome в ОС Windows

[+ Створити ключ доступу](#)

Рис. 4. Початкове вікно налаштування використання ключів доступу

Клікнути на опцію «Використовувати ключі доступу» для використання зазначеного пристрою (рис. 5) як засобу автентифікації через його розблокування і без введення паролю.

Тепер можна входити за допомогою ключів доступу



Коли ви наступного разу входите в обліковий запис Google на цьому пристрої, то зможете підтвердити свою особу за допомогою відбитка пальця, фейс-контролю або іншого способу розблокування екрана. [Докладніше](#)

Готово

Рис. 5. Активація налаштування «Ключі доступу»

Якщо обрати опцію «Створити ключі доступу» (рис. 4), то можна створити ключі на іншому пристрої, обравши «Скористатись іншим пристроєм» – «Вибрати інший телефон або планшет» (рис. 6).

Створити ключ доступу для облікового запису Google



Ключі доступу легко налаштувати. Вони дають змогу безпечно входити в обліковий запис Google за допомогою відбитка пальця, фейс-контролю, іншого способу розблокування екрана або апаратного ключа безпеки. Ви можете створити ключ доступу на цьому пристрої або скористатись іншим.

Скасувати

Скористатись іншим пристроєм

Продовжити

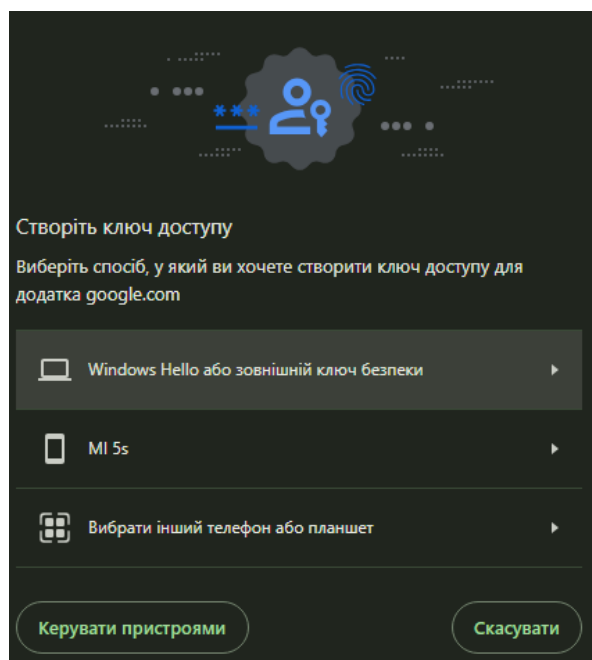


Рис. 6. Налаштування іншого пристрою для доступу в обліковий запис Google

Далі Chrome запропонує QR-код для зв'язування пристрою з комп'ютером, сканування якого ініціює створення на ньому відповідних ключів (рис. 7).

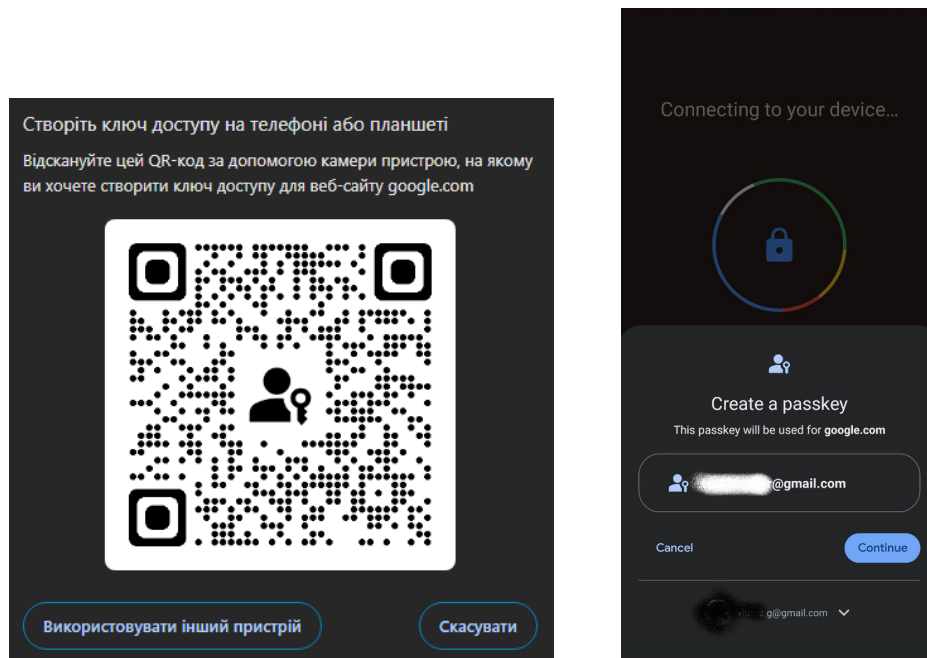


Рис. 7. Створення ключів доступу на мобільному пристрої через QR-код

Для перевірки автентифікації за ключами доступу вийти з облікового запису Google та спробувати знову увійти, обравши «Спробувати інший спосіб» – «Використати ключ доступу» (рис. 8).

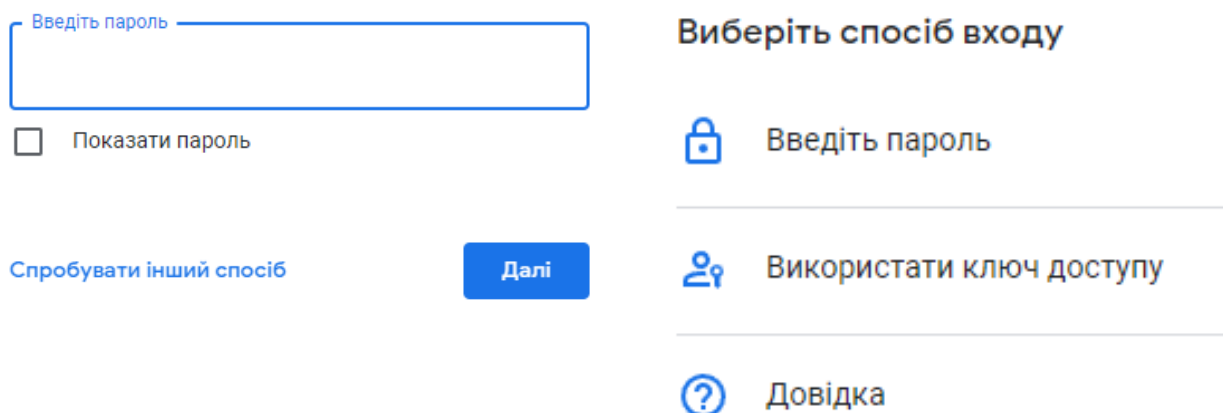


Рис. 8. Вибір автентифікації через ключ доступу

Завершити автентифікацію з використанням свого смартфона, в якому з'явиться запит відсканувати відбиток пальця, пройти фейс-контроль або розблокувати екран (рис. 9).

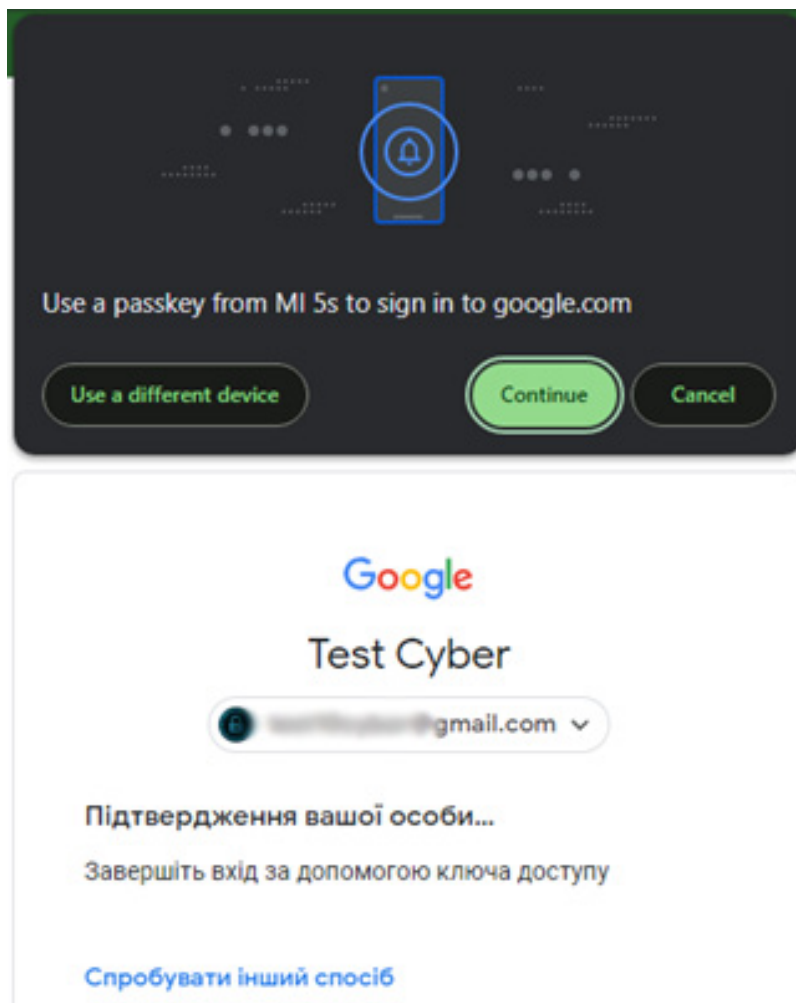


Рис. 9. Запит на продовження автентифікації через ключі доступу на смартфоні

Важливо!!!

Коли створюється ключ доступу, то обирається можливість входу без пароля за допомогою ключа доступу, тому це можна робити лише на особистих пристроях. Навіть якщо вийти зі свого облікового запису Google, створивши ключ доступу на пристрої, то кожен, хто може розблокувати пристрій, зможе знову увійти у ваш обліковий запис Google за допомогою ключа доступу.

Парольний менеджер KeePass

Завантажити (<https://keepass.info/index.html>), встановити та запустити парольний менеджер KeePass Password Safe (рис. 10).

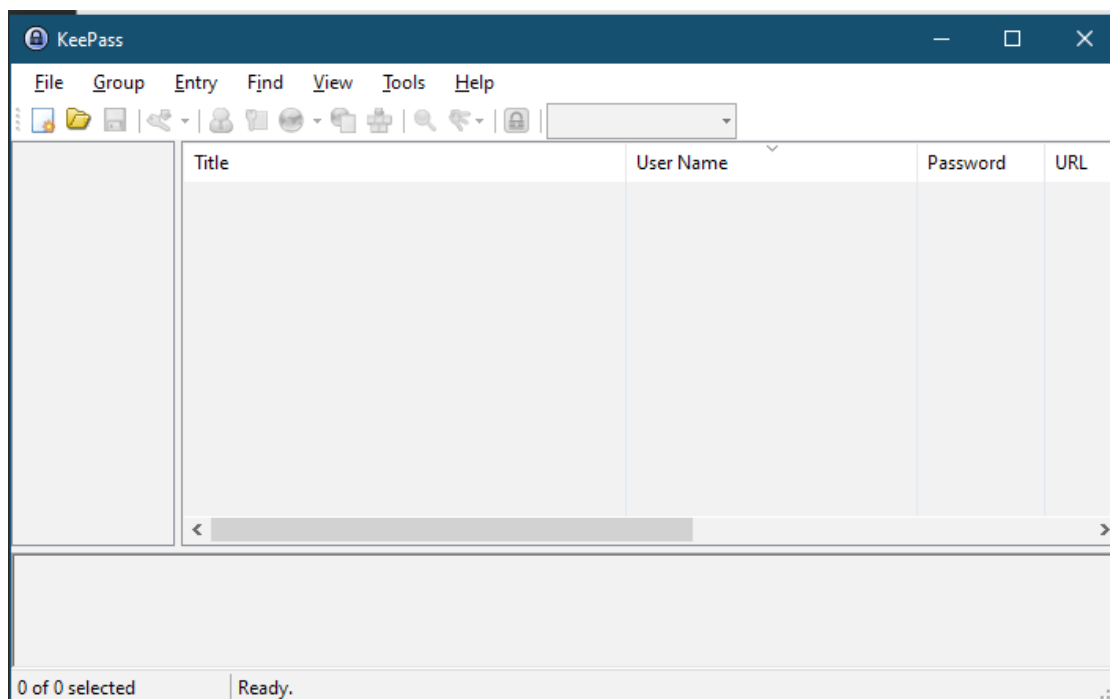


Рис. 10. Головне вікно KeePass

Комбінацією клавіш (Ctrl+N) створити та вказати місце зберігання файлу нової бази паролів (рис. 11).

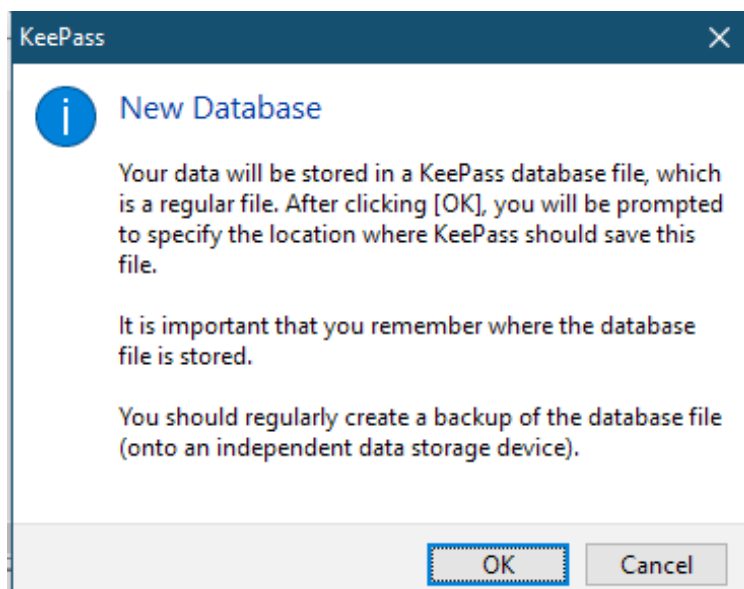


Рис. 11. Повідомлення щодо створення нової бази паролів

Придумати та запам'ятати майстер-пароль (парольну фразу) довжиною не менше 10-ти символів із використанням маленьких та великих літер, цифр та спеціальних символів. Ввести майстер-пароль (парольну фразу) та вибрати ім'я для бази паролів (рис. 12). Додатково можна роздрукувати основні дані щодо місця зберігання основної бази паролів, її резервної копії та підказки щодо майстер-пароля (рис. 13).

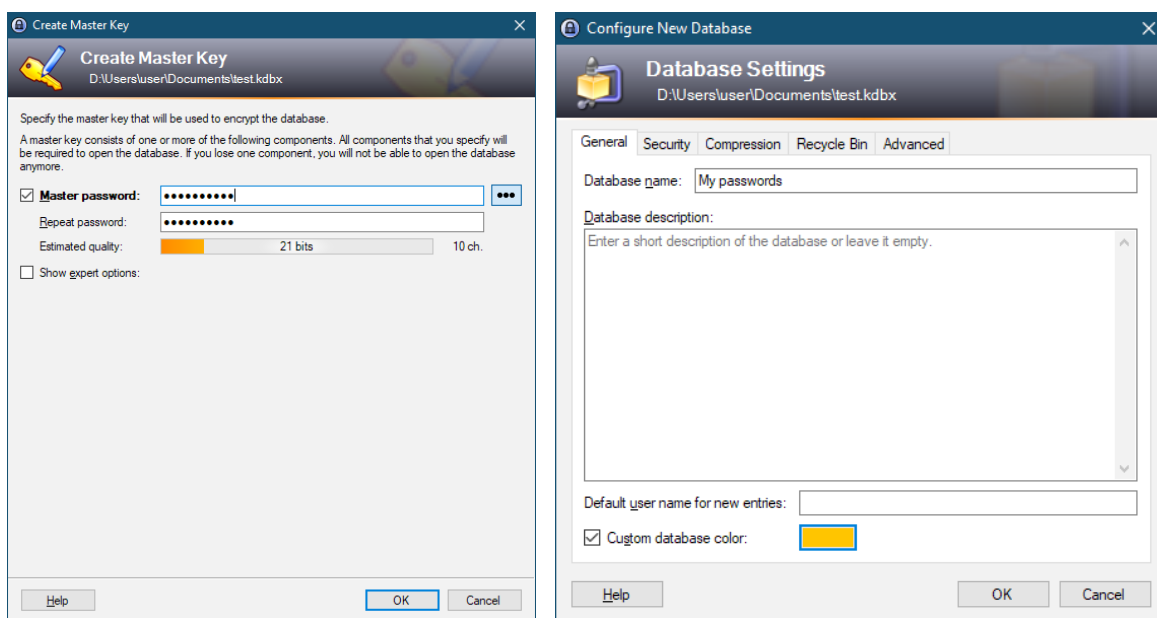


Рис. 12. Створення майстер-паролю та налаштування бази

KeePass

Emergency Sheet

05.02.2021

Database file:

D:\Users\user\Documents\test.kdbx

You should regularly create a backup of the database file (onto an independent data storage device). Backups are stored here:

Master Key

The master key for this database file consists of the following components:

- **Master password:**

Рис. 13. Пам'ятка щодо місця зберігання основної бази паролів, її резервної копії та підказки щодо майстер-пароля

В основному вікні KeePass зліва обрати теку «eMail», створити новий запис (комбінація клавіш Ctrl+I), заповнити поля для свого поштового облікового запису, перейти у налаштування Генератора паролів і обрати довжину пароля та абетку символів, з яких буде генеруватися пароль (рис. 14). Завершити редагування, зберегти зміни (комбінація клавіш Ctrl+S) і переглянути створений запис (рис. 15).

Зверніть увагу, що деякі веб-сервіси забороняють наявність в паролі спеціальних символів. У такому випадку або після генерації паролю вручну видалити спеціальні символи або виключити їх із абетки налаштувань Генератора паролів.

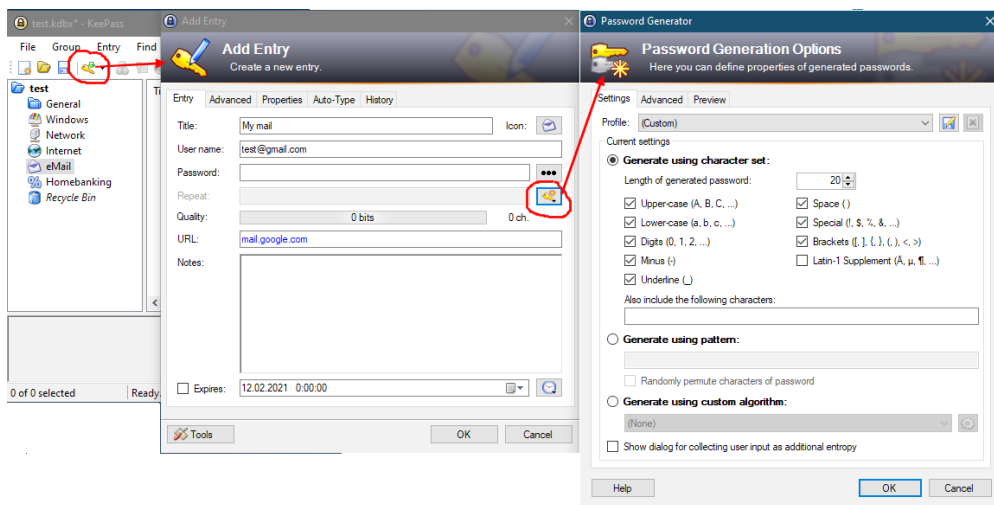


Рис. 14. Створення і налаштування параметрів нового запису у базі паролів

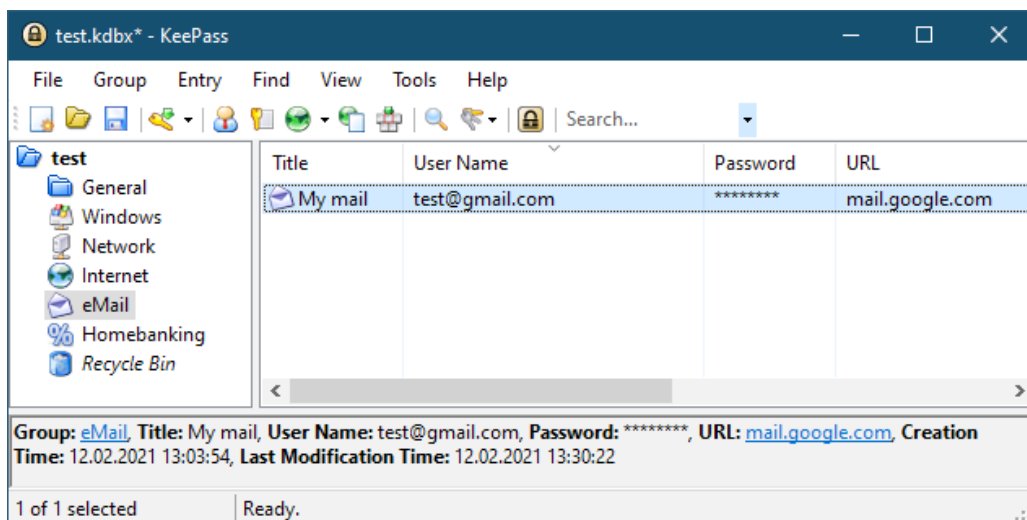


Рис. 15. Створений запис у базі паролів

Пройти автентифікацію в поштовому сервісі, використовуючи менеджер паролів. Для цього в KeePass обирається відповідний запис та по чергову копіюється у буфер логін (комбінація клавіш Ctrl+B) та пароль (комбінація клавіш Ctrl+C), які по чергову вставляються у відповідні поля форми автентифікації поштового сервісу.



Альтернативна практична вправа:

«Електронний підпис та шифрування повідомлень»



Навчальна мета заняття: отримати навички підписувати та зашифровувати повідомлення.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет, веб-браузер Google Chrome.

Порядок проведення заняття

Виконати такі дії:

- ▶ встановити на свій флеш-накопичувач утиліту gpg4usb;
- ▶ згенерувати пару своїх ключів;
- ▶ експортувати свій публічний ключ в окремий файл *_pub.asc;
- ▶ обмінятися своїм публічним ключем з іншими;
- ▶ імпортувати у програму публічні ключі інших;
- ▶ створити повідомлення для співрозмовника, підписати повідомлення та зашифрувати його з використанням публічного ключа адресата;
- ▶ отримати підписане та зашифроване повідомлення, розшифрувати повідомлення та перевірити електронний підпис.

За посиланням <https://www.gpg4usb.org/download.html> вибрати та завантажити на особистий флеш-накопичувач архів утиліти gpg4usb. Розпакувати архів, запустити утиліту start_windows.exe та обрати зручну мову інтерфейсу (рис. 1).

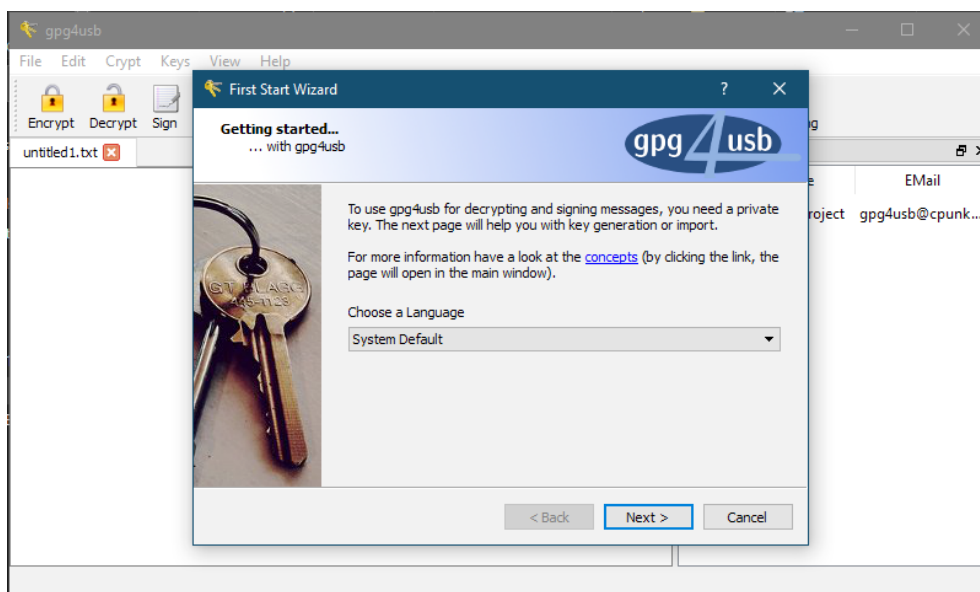


Рис. 1. Налаштування мови інтерфейсу gpg4usb

Далі клікнути на посилання «Створити нову ключову пару», обрати «Створити новий Ключ» та заповнити відповідні поля персональними даними (пароль згенерувати та зберегти у менеджері паролів). Завершити налаштування у майстрі першого запуску (рис. 2).

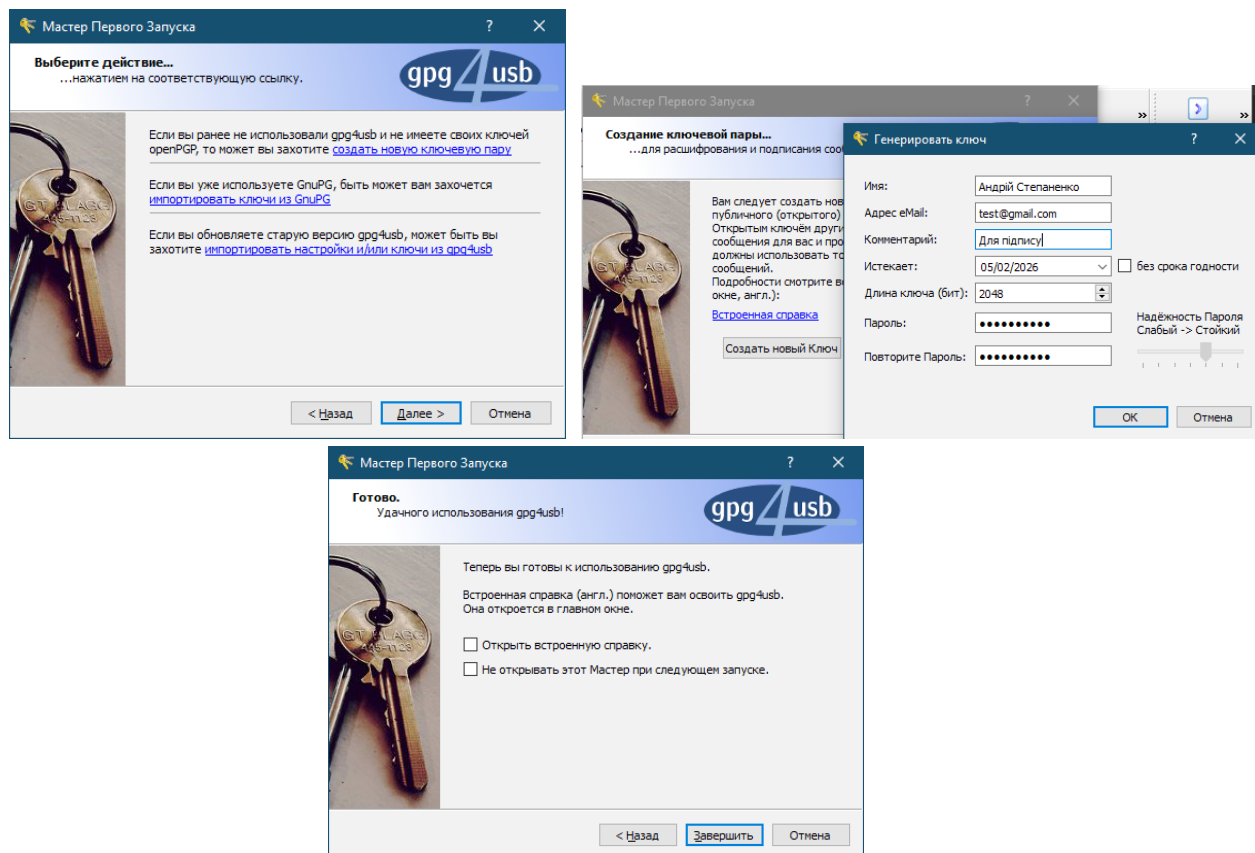


Рис. 2. Генерування ключів у майстрі першого запуску

Запустити «Менеджер ключів», обрати обліковий запис своїх ключів, вибрати «Експорт обраних ключів у файл» та зберегти свій публічний ключ (наприклад, Андрій Степаненко test@gmail.com(202AA4030C558985)_pub.asc) на флеш-накопичувач (рис. 3).

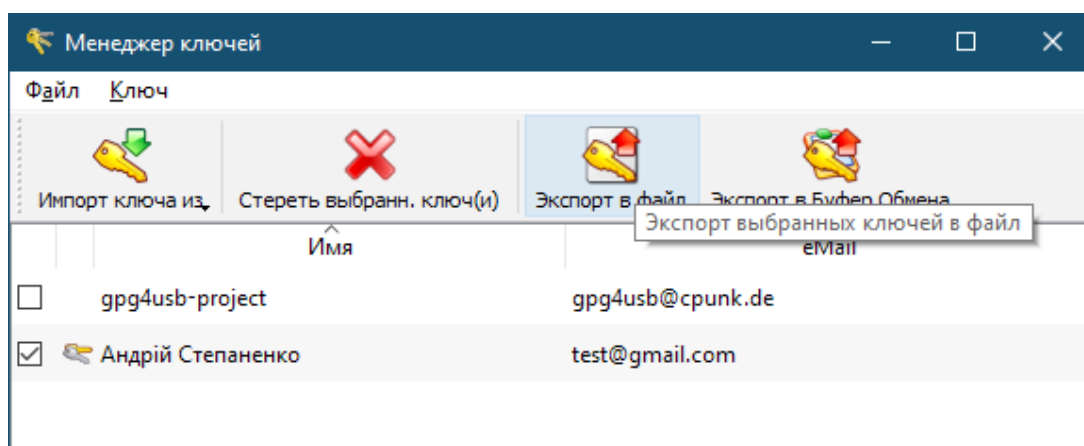


Рис. 3. Експорт публічного ключа

Слухачам обмінятися між собою своїми публічними ключами (Андрій Степаненко test@gmail.com(202AA4030C558985)_pub.asc) – це можна зробити пересиланням поштою або локальним копіюванням на свої носії.

У менеджері ключів здійснити імпорт у програму файлів публічних ключів, отриманих від інших слухачів (рис. 4).

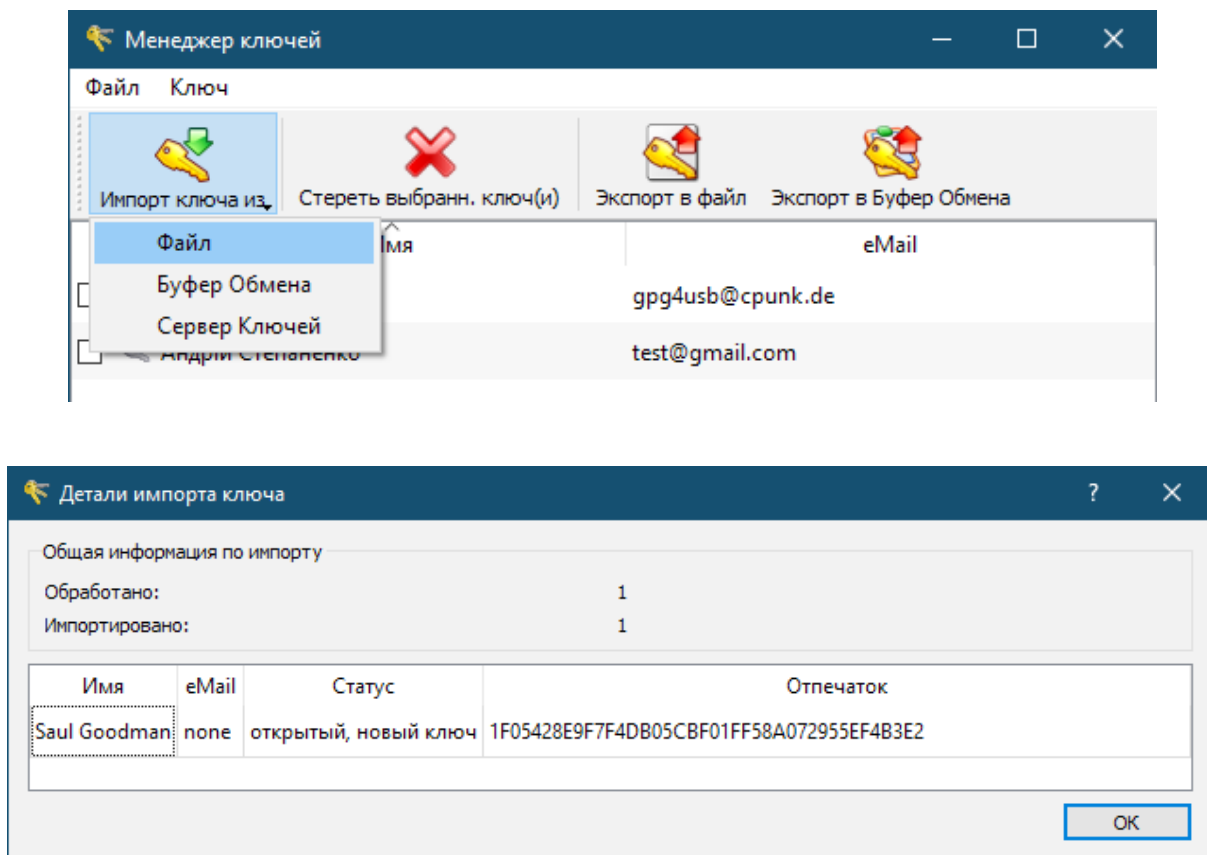
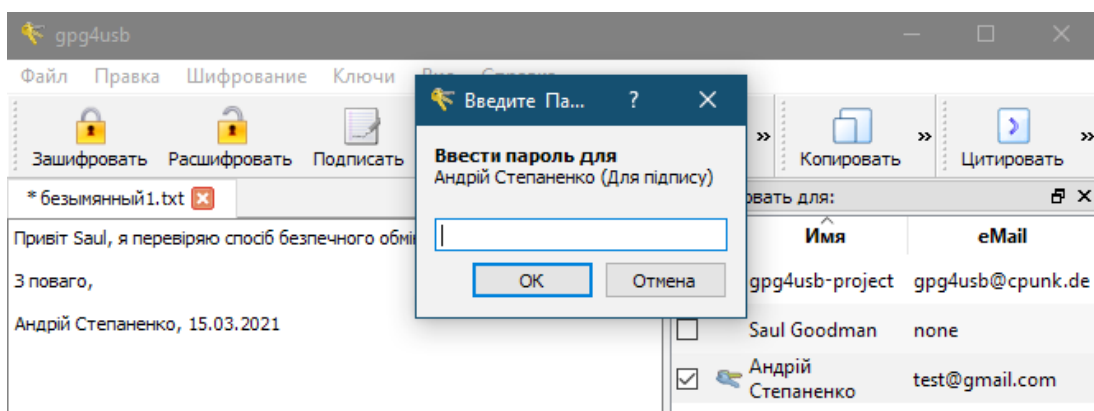


Рис. 4. Импорт публичных ключей собеседников

Создать произвольное сообщение для собеседника, указать дату, час та назначить свой ключ у правому окне программы. Обрати «Подписать» сообщение, ввести пароль для своего частного ключа та получить подпись (рис. 5).



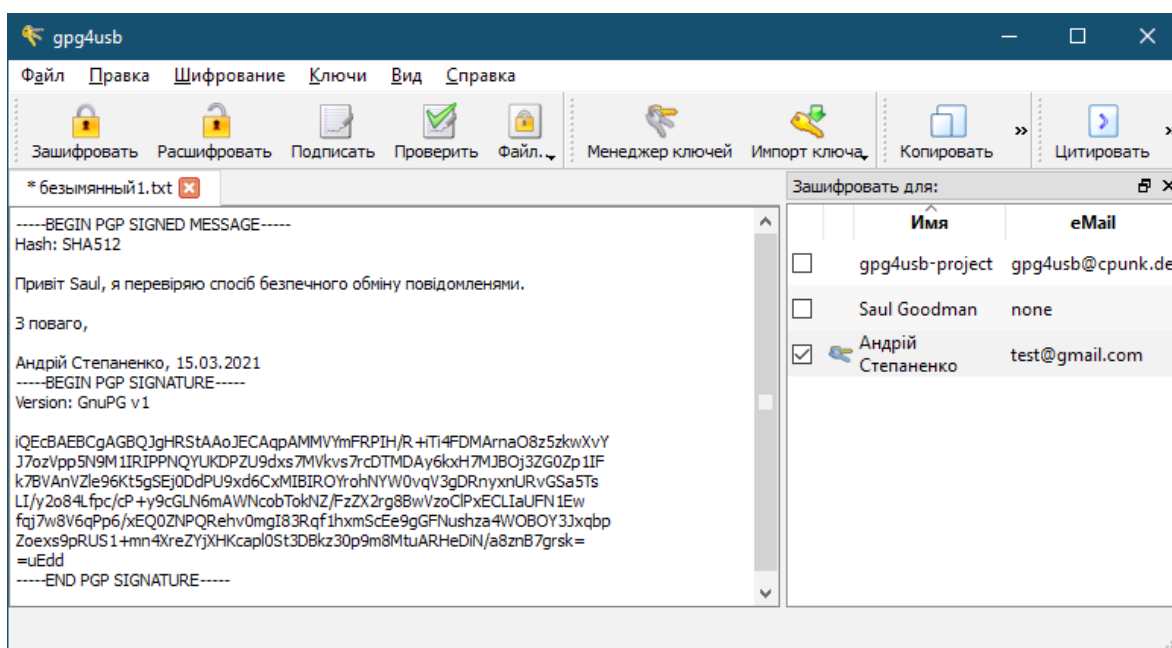


Рис. 5. Підпис повідомлення

Зняти позначку зі свого ключа та поставити на ключі співрозмовника у правому віконці програми, обрати «Зашифрувати» (рис. 6). Отримане зашифроване повідомлення відіслати своєму співрозмовнику.

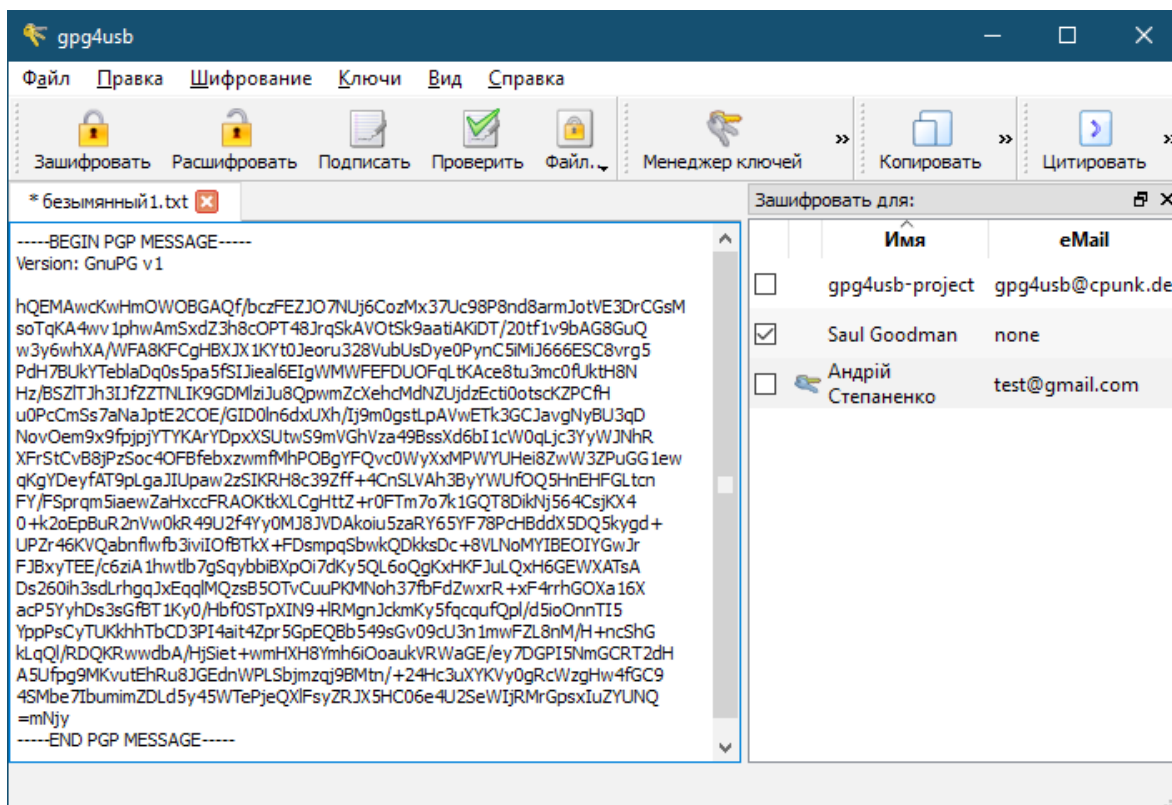


Рис. 6. Шифрування повідомлення

Співрозмовник, отримавши зашифроване повідомлення, або копіює його зміст у буфер пам'яті та вставляє у порожнє поле текстового файлу grg4usb, або відкриває його як текстовий файл в grg4usb. Після чого у правому полі програми позначає рядок із зазначенням своїх ключів, обирає «Розшифрувати», вводить пароль до свого приватного ключа та отримує розшифроване повідомлення (рис. 7).

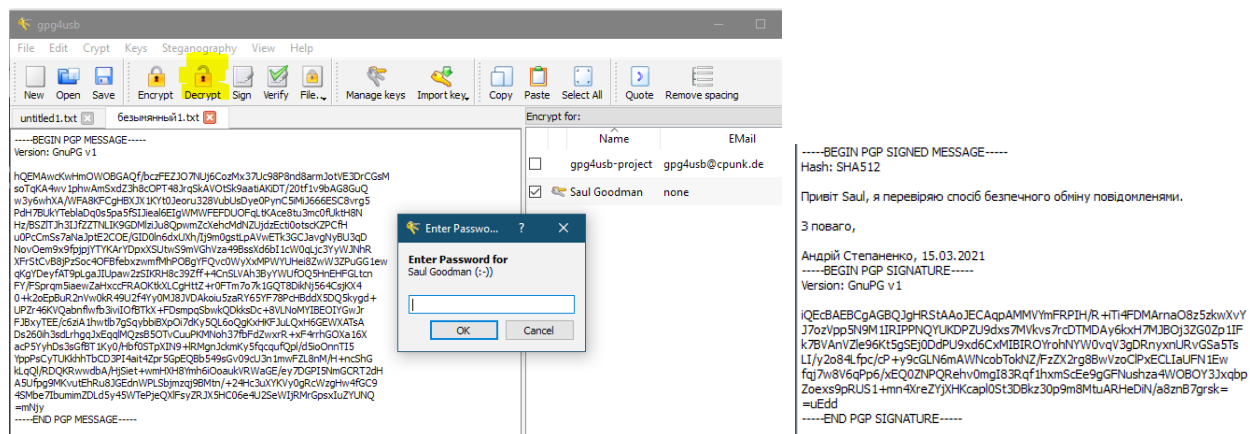


Рис. 7. Розшифрування повідомлення

У правому полі програми співрозмовник позначає рядок із зазначенням ключа відправника, обирає «Перевірити» та «Деталі» підпису (рис. 8). Виправити або додати у повідомленні одну літеру та повторити перевірку підпису у зміненому повідомленні (рис. 9).

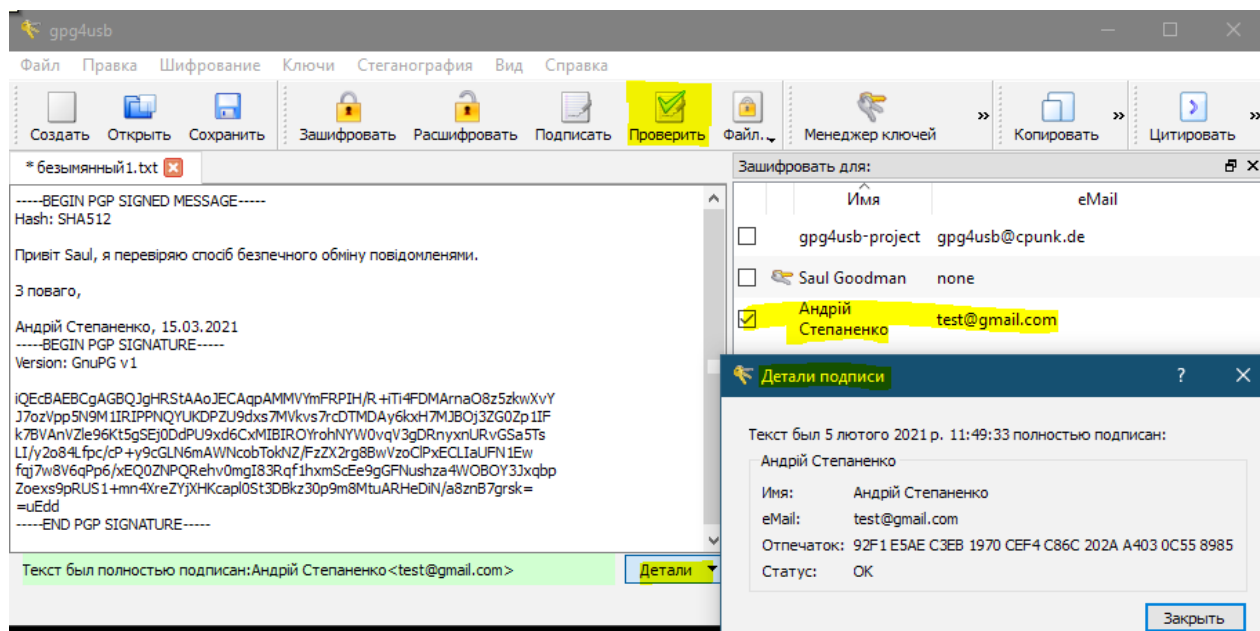


Рис. 8. Успішна перевірка підпису відправника повідомлення

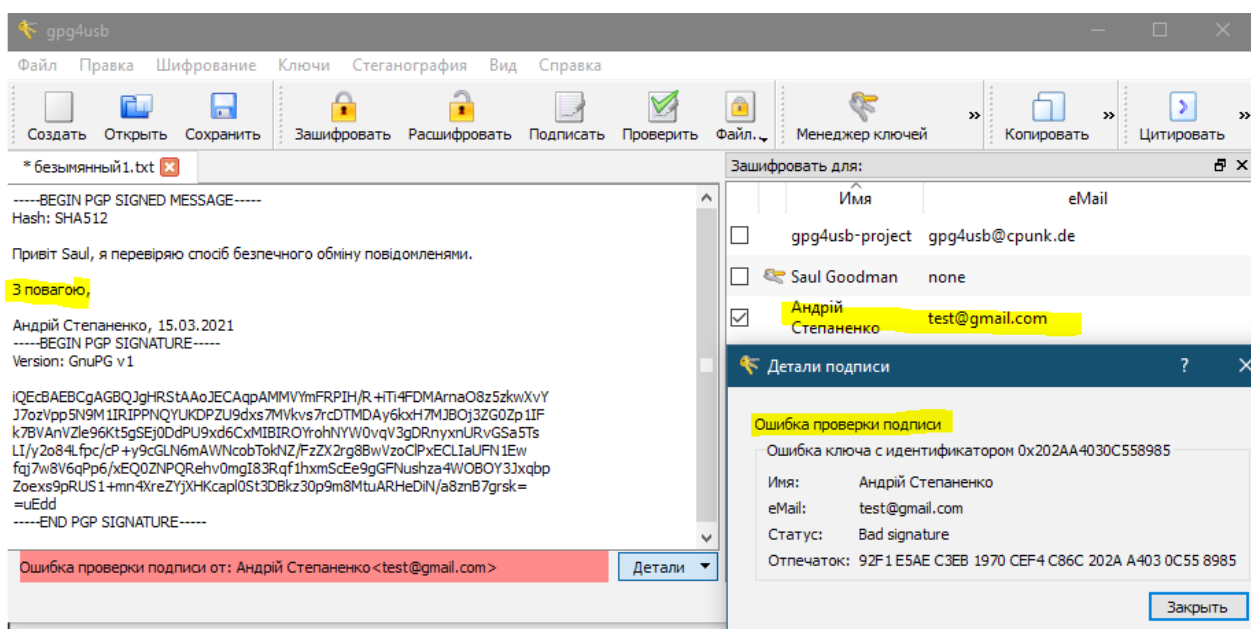
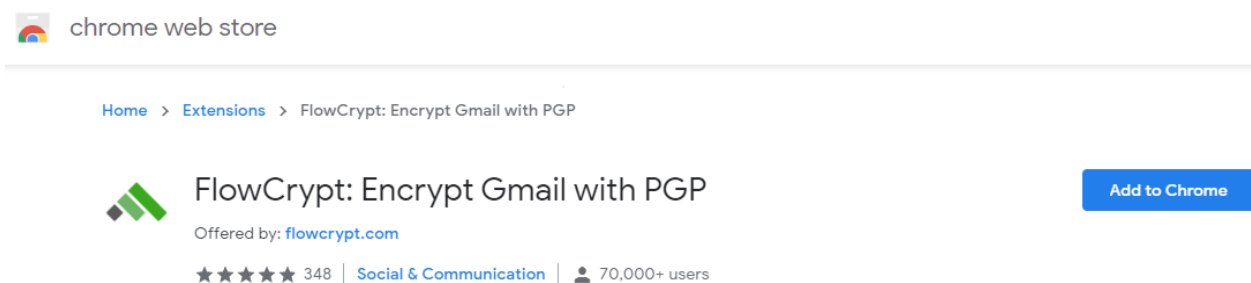


Рис. 9. Невдала перевірка підпису відправника повідомлення

Установити і налаштувати в обліковому записі Google розширення електронного підпису та шифрування. В обліковому записі ProtonMail здійснити налаштування інтегрованого сервісу електронного підпису та шифрування листів, які спрямовуються на зовнішні поштові домени. Після налаштувань переслати підписані та зашифровані листи між поштовими доменами protonmail.com та gmail.com. Переконавшись у забезпеченні конфіденційності та цілісності такого листування.

Додати в Google Chrome розширення FlowCrypt: Encrypt Gmail with PGP (<https://chrome.google.com/webstore/detail/flowcrypt-encrypt-gmail-w/bnjglocidkmhmoohhfkfbkbbkejdhdc?hl=ua>), клацнути на розширення та надати дозвіл FlowCrypt отримувати доступ до облікового запису Google (рис. 10).





FlowCrypt Browser Extension хоче
отримати доступ до вашого облікового
запису Google

...@gmail.com

FlowCrypt Browser Extension зможе:

Перегляд повідомлень і налаштувань електронної пошти

Керування чернетками й надсилання електронних листів

Переконайтеся, що додаток FlowCrypt Browser Extension
надійний

Можливо, ви надаєте цьому сайту або додатку конфіденційну
інформацію. Дізнайтеся, як додаток FlowCrypt Browser Extension
оброблятиме ваші дані, у його [політиці конфіденційності](#). В
[обліковому записі Google](#) завжди можна переглянути або скасувати
доступ.

[Докладніше про ризики](#)

[Скасувати](#)

[Дозволити](#)

Рис. 10. Встановлення та надання дозволу FlowCrypt

У FlowCrypt згенерувати і зберегти ключі: обрати New encryption key, Encryption key type – RSA 2048bit – Create and save (рис. 11).

Set Up FlowCrypt

Choose pass phrase to protect your encrypted emails. [choosing secure pass phrases](#)

.....

GOOD (time to crack: 40 years)

.....

☐ Remember Pass Phrase after closing browser

☒ Back up encrypted private key in inbox (recommended)

☒ Submit corresponding pubkey to FlowCrypt Attester (recommended)

Encryption key type: **RSA 2048bit**

[CREATE AND SAVE](#)

NEW ENCRYPTION KEY

IMPORT PRIVATE KEY

New to encryption?

Quick setup

Use your own PGP key

Manual setup

Рис. 11. Створення і збереження ключів
для облікового запису

Після налаштувань розширення в поштовому клієнті з'явиться кнопка Secure Compose (рис. 12).

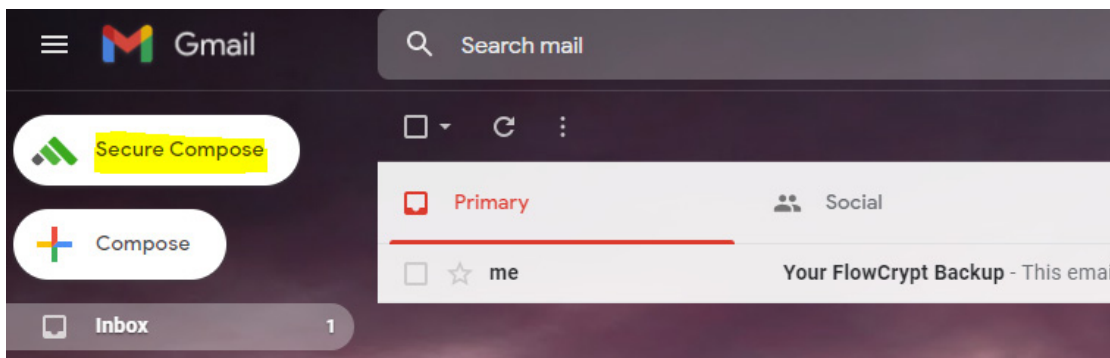


Рис. 12. Кнопка FlowCrypt Secure Compose

Авторизуватися у своєму обліковому записі ProtonMail. Перейти у «Налаштування» – «Безпека» і ввімкнути «External PGP Settings (optional)», Address Verification (optional) (рис. 22).

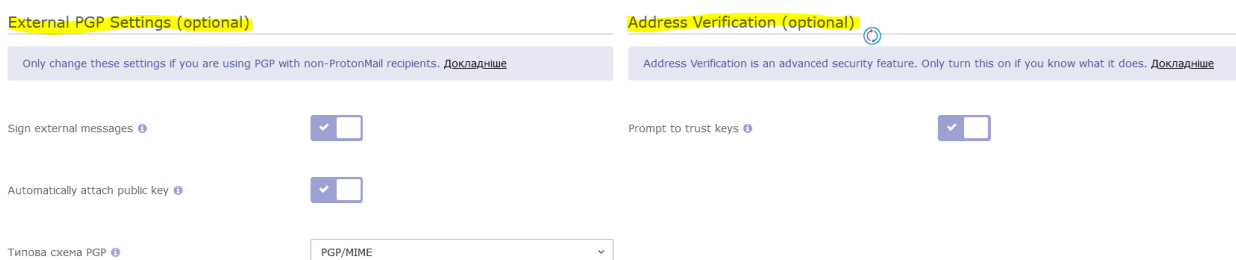


Рис. 13. Включення опцій підпису та шифрування

Відправити на адресу @gmail.com лист, до якого буде автоматично додано публічний ключ облікового запису @protonmail.com.

У @gmail.com після відкриття листа від @protonmail.com здійснити імпорт відкритого ключа @protonmail.com, та відповісти з підписом і шифруванням, натиснувши Secure Reply (рис. 23).

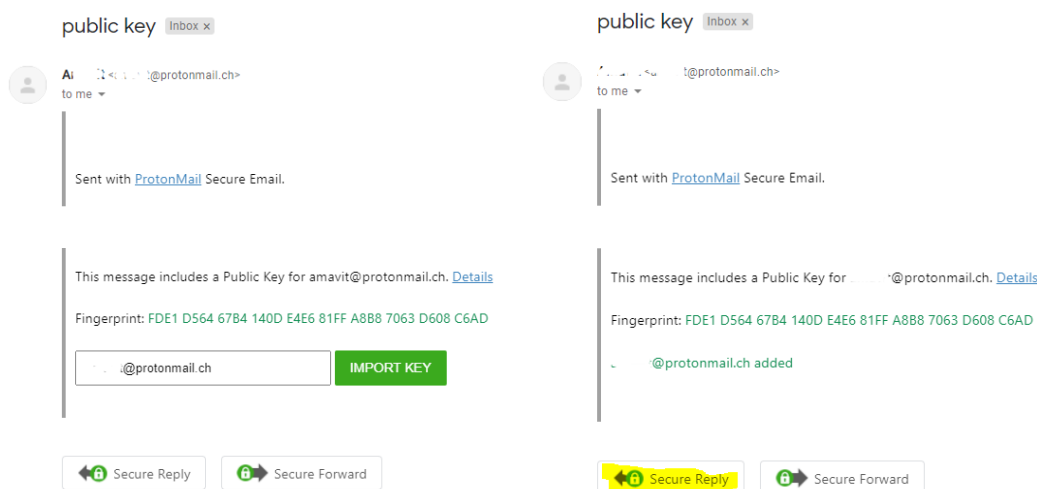


Рис. 14. Отримання публічного ключа та відповідь з підписом та шифруванням

У @protonmail.com буде автоматично розшифровано листа і перевірено підпис, але зазначено, що перевірка підпису була зроблена публічним ключом, який ще не є довіреним. Натиснути «ДОВІРЕНИЙ КЛЮЧ» (рис. 15).

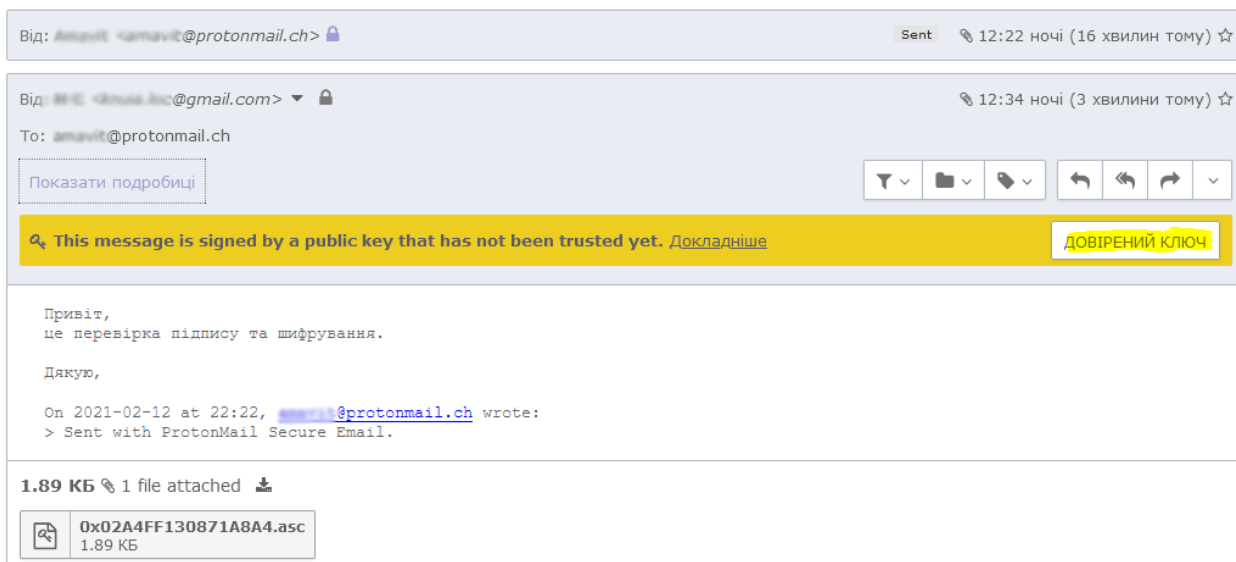


Рис. 15. Розшифрований і перевірений на правдивість підпису лист з пропозицією позначити публічний ключ як довірений

Далі всі листи між обліковими записами @gmail.com і @protonmail.com будуть автоматично підписуватися і шифруватися перед відправкою, а під час отримання – перевірятись та розшифровуватись.

Модуль: Безпека користування соціальними мережами



Практична вправа:

«Двофакторна автентифікація облікового запису Facebook. Метадані фотозображень»



Навчальна мета заняття: навчитись налаштовувати двофакторну автентифікацію облікового запису Facebook та контролювати метадані фотозображень.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі Інтернет, веб-браузер Google Chrome, особисті смартфони або телефони у слухачів, дата-кабелі підключення смартфона до комп'ютера, підготовлені файли фотозображень з метаданими.

Порядок проведення заняття

Двофакторна автентифікація облікового запису Facebook.

Створити, якщо немає, обліковий запис у соціальній мережі Facebook. Встановити для облікового запису Facebook двофакторну автентифікацію через Google Authenticator.

В обліковому записі перейти в «Налаштування та конфіденційність» – «Налаштування» – «Пароль і безпека» (рис. 1) – «Двохетапна перевірка» – «Використання двохетапної перевірки» – «Використовувати додаток для автентифікації» (рис. 2).

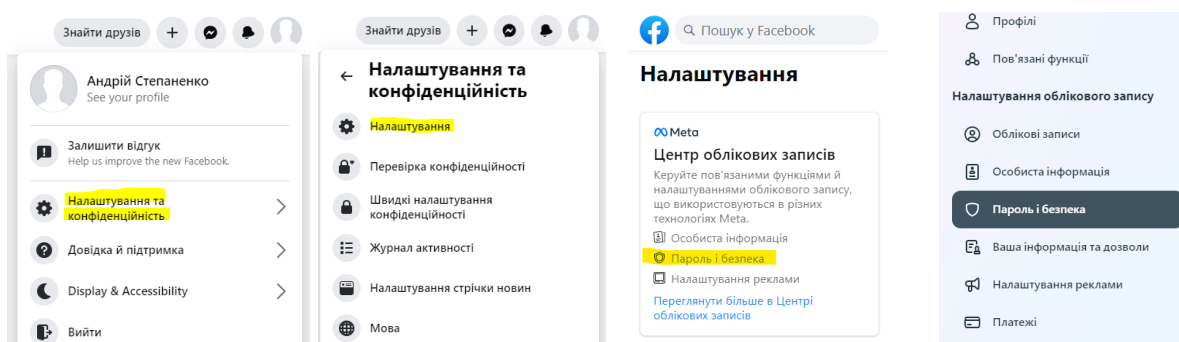


Рис. 1. Шлях до налаштувань «Пароль і безпека»

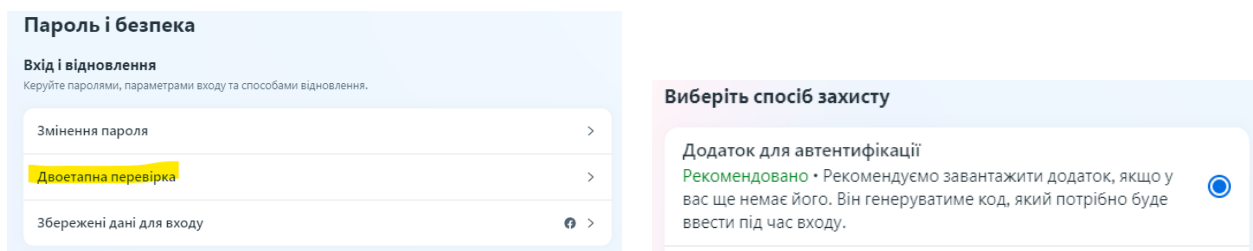


Рис. 2. Шлях до налаштування додатка автентифікації

Переконайтеся, що у власному смартфоні встановлений Google Authenticator (встановлюється з Google Play або App Store), увійти до «Використовувати додаток для автентифікації», зчитати додатком смартфона Google Authenticator QR-код та ввести код підтвердження (рис. 3).

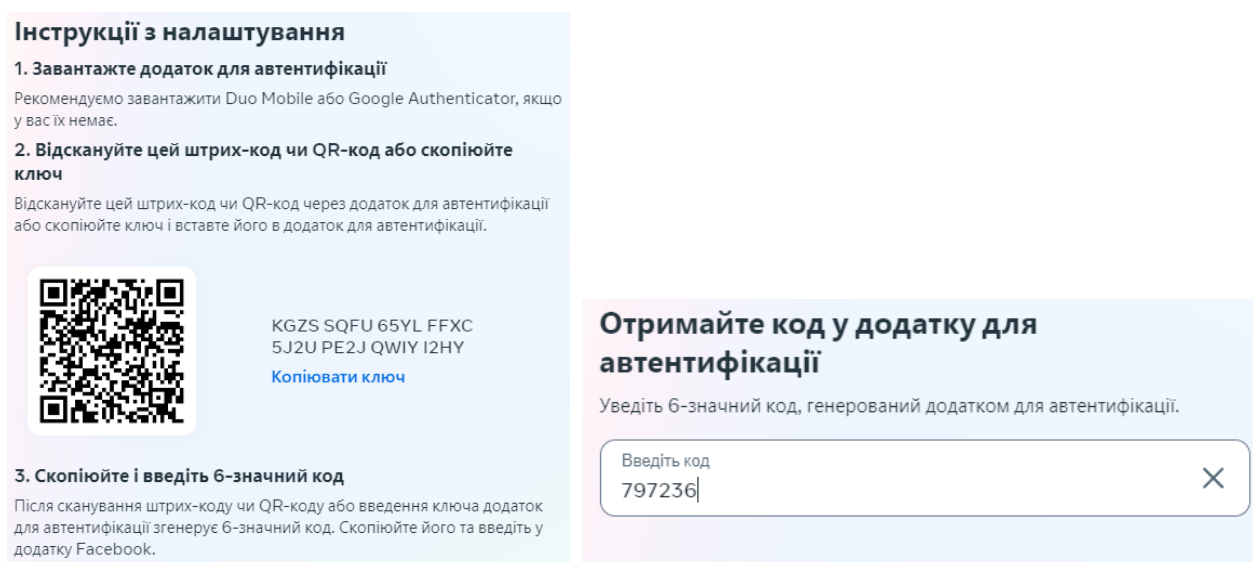
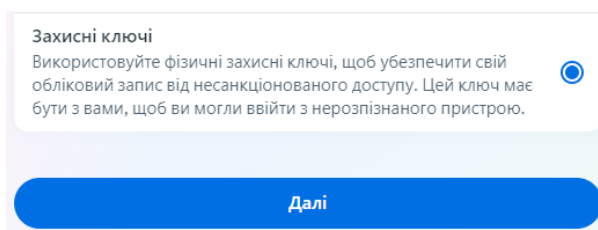


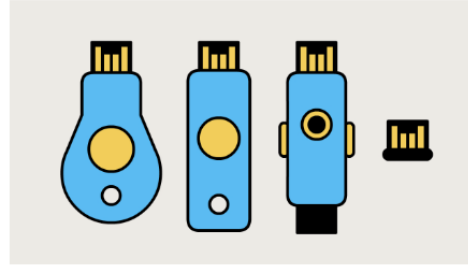
Рис. 3. Налаштування двохетапної перевірки

Після налаштування двохетапної перевірки повернутися у розділ «Використання двохетапної перевірки» – «Захисні ключі» – «Зареєструвати захисний ключ» (рис. 4) – Security key setup (Встановлення ключа безпеки) – Insert your security key into the USB port (Вставити ваш ключ безпеки в USB порт) – Скасувати (Cancel) (рис. 5). Далі обрати свій пристрій з ключами безпеки, який використовувався для автентифікації в акаунті Google і додатково ввести свій пароль (рис. 6).



Налаштуйте захисний ключ

Перш ніж використовувати захисний ключ для входу у Facebook, необхідно його зареєструвати. Переконайтеся, що захисний ключ під рукою.



Зареєструвати захисний ключ

Рис. 4. Налаштування автентифікації через захисні ключі

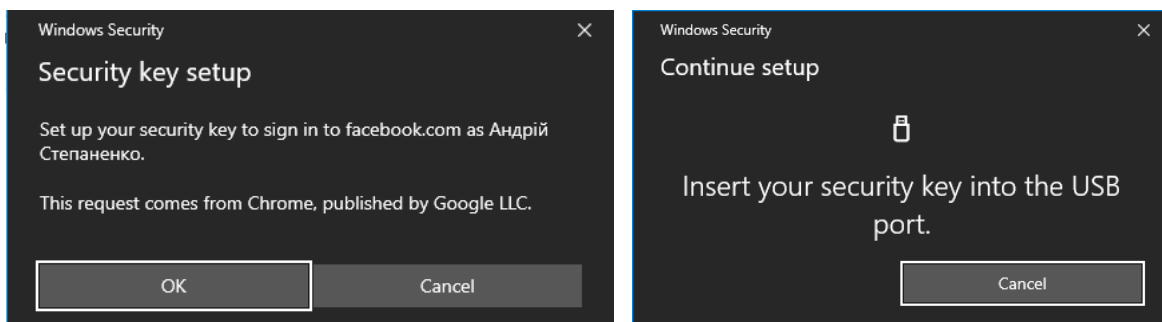


Рис. 5. Продовження налаштування автентифікації через захисні ключі

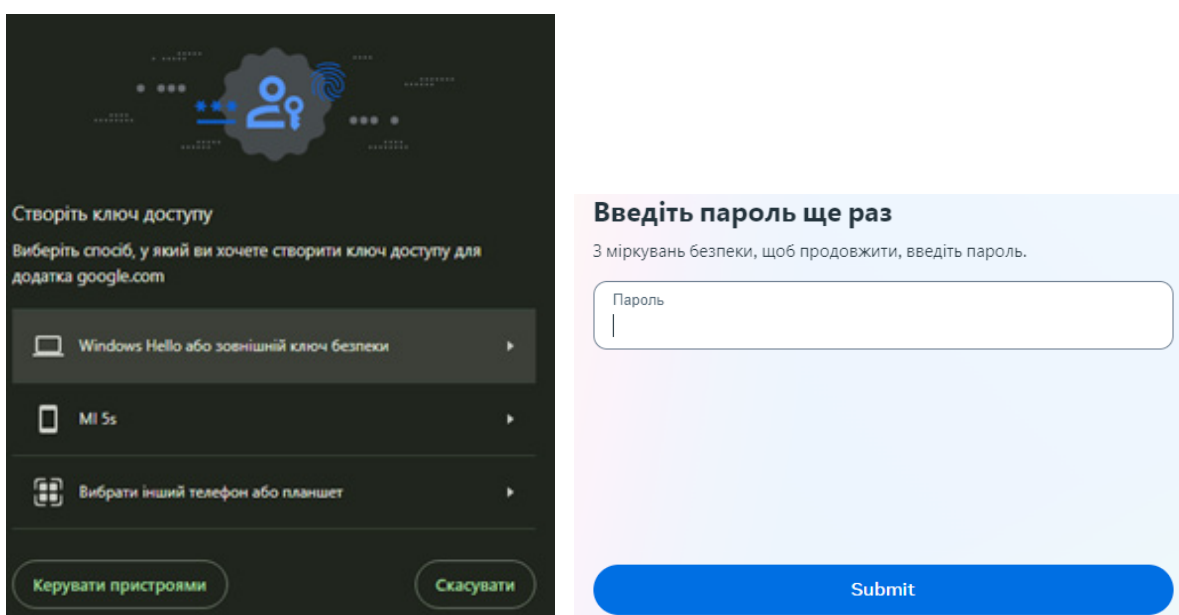


Рис. 6. Вибір свого пристрою з ключами безпеки

Повернутись у розділ «Пароль і безпека» і переглянути проблеми з безпекою, виконавши перевірку додатків, пристроїв і надісланих електронних листів (рис. 7).

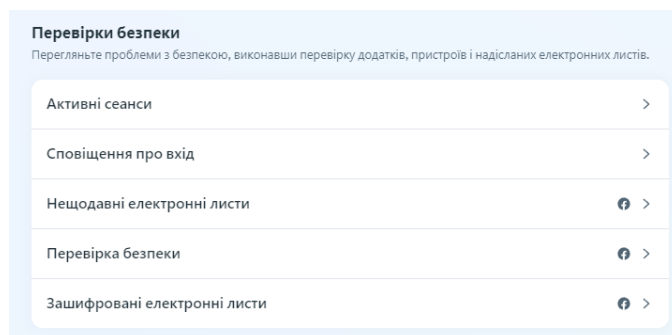


Рис. 7. Перевірка безпеки облікового запису

Після закінчення налаштувань вийти із облікового запису та увійти з використанням двохетапної автентифікації та пристрою з ключами.

Метадані фотозображень.

В особистому смартфоні включити GPS, підійти до вікна у приміщенні й дочекатися встановлення координат свого місцезнаходження, перевіривши цей факт запуском додатку «Карти», де відобразиться точне місцезнаходження смартфона.

Зробити кілька фотознімків фотокамерою смартфона, підключити смартфон до комп'ютера та завантажити фотозображення на комп'ютер. Або скопіювати на комп'ютер підготовлені файли фотозображень з метаданими. Перевірити наявність метаданих у файлах фотозображень та видалити їх.

Завантажити, встановити і запустити утиліту перегляду та редагування метаданих «AnalogExif» (<https://sourceforge.net/projects/analogexif>). Відкрити у AnalogExif фотозображення, переглянути метадані, двічі клацнути на поле Location та скопіювати у буфер координати (рис. 8).

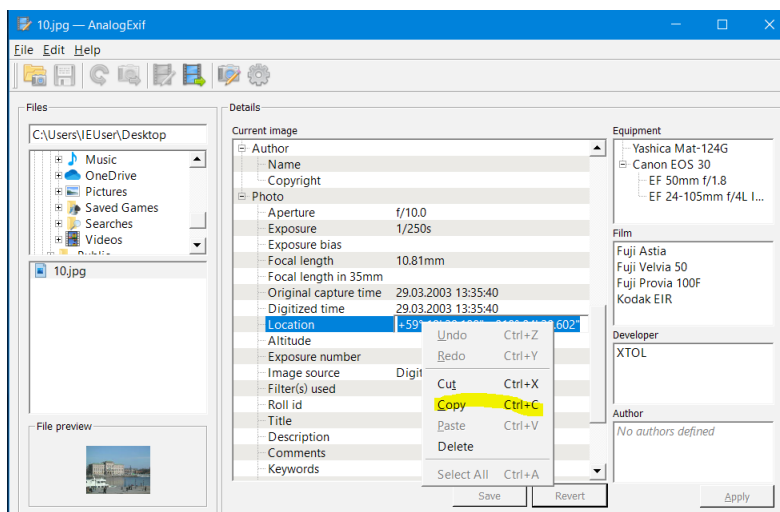


Рис. 8. Перегляд метаданих фотозображення

Відкрити веб-браузер Google Chrome, вставити координати в адресний рядок і здійснити пошук місця фотозйомки (рис. 9).

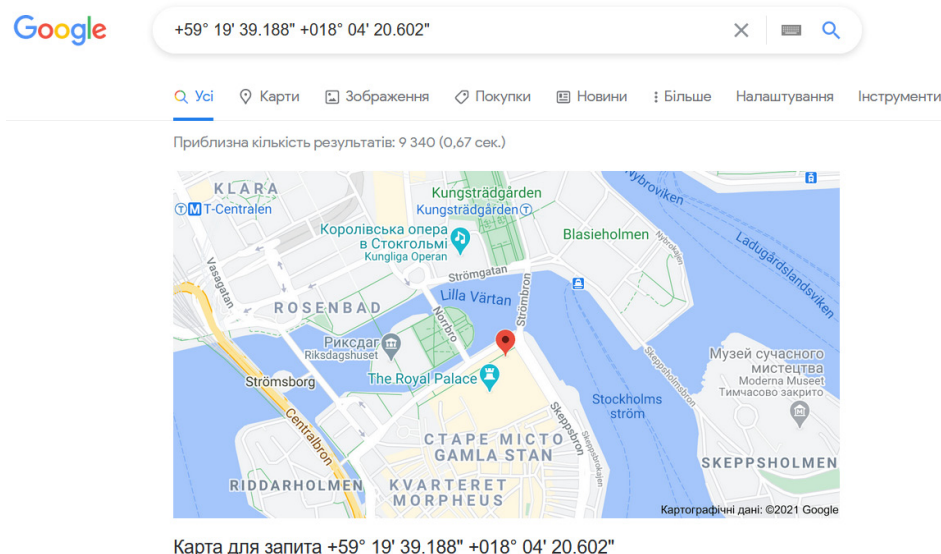


Рис. 9. Пошук місця фотозйомки за координатами з метаданих фотозображення

У Провіднику файлів через контекстне меню (клацнути правою кнопкою миші) подивитися «Властивості файлу фотозображення», перейти у вкладку «Докладно» та клацнути на «Видалити властивості та особисті відомості» – «Вибрати всі» – «ОК» (рис. 10).

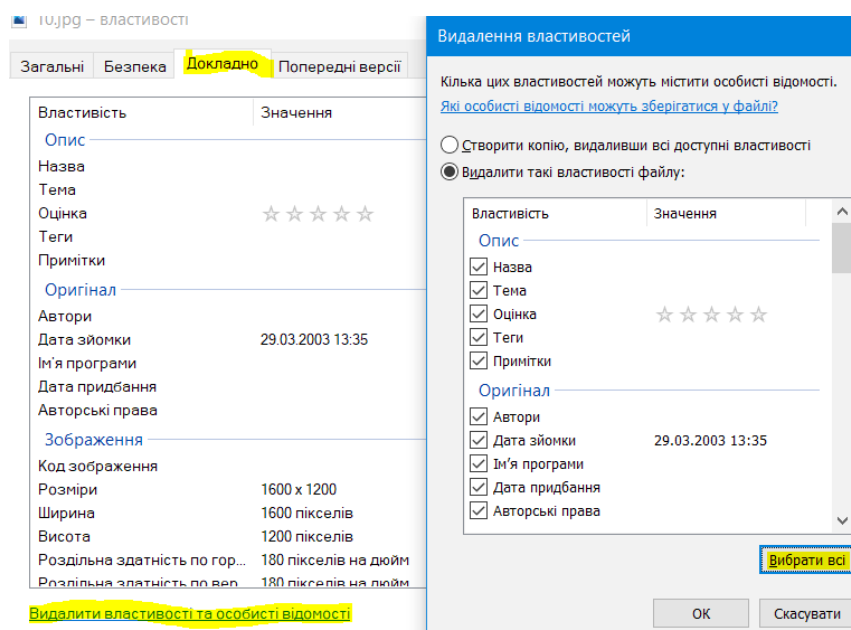


Рис. 10. Видалення метаданих фотозображень

Знову відкрити у AnalogExif фотозображення та переконатися, що метадані відсутні та можна їх безпечно завантажувати у соціальні мережі.

Модуль: Реагування на інциденти безпеки інформації



Практична вправа:

«Виявлення провісників та індикаторів інциденту інформаційної безпеки»



Навчальна мета заняття: навчитись виявляти провісники та індикатори інцидентів інформаційної безпеки.



Час проведення: 1 год.

Місце проведення: комп'ютерний клас.



Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі Інтернет, веб-браузер Google Chrome.

Порядок проведення заняття

Задача 1.

1. Налаштувати ведення та забезпечення доступу до журналу подій Windows Defender Firewall.
2. Встановити Nmap Security Scanner та здійснити сканування системи, яке розглядається як підготовка до атаки.
3. Виявити провісники атаки та заповнити звіт щодо події інформаційної безпеки.

Виконання.

Через рядок пошуку відкрити Windows Defender Firewall with Advanced Security (пошуковим виразом може бути «Засоби адміністрування») (рис. 1).

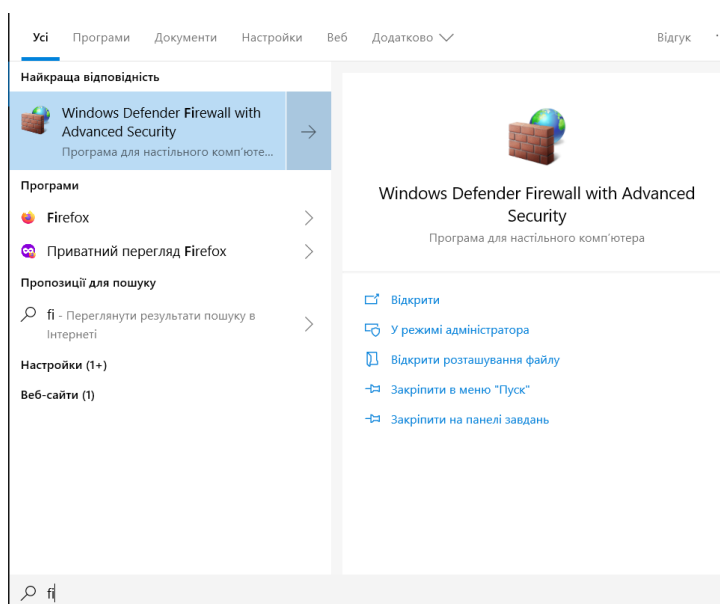


Рис. 1. Відкриття Windows Defender Firewall with Advanced Security

У Windows Defender Firewall with Advanced Security (рис. 2):

- ▶ відкрити налаштування Windows Defender Firewall Properties;
- ▶ пересвідчитись, що Firewall активований (Firewall state: on);
- ▶ для кожної вкладки Domain Profile, Private Profile, Public Profile через опцію Logging – Customize включити записування у журнал подій про блокування мережевих пакетів (Log dropped packets: Yes) та успішне встановлення мережевого з'єднання (Log successful connections: Yes).

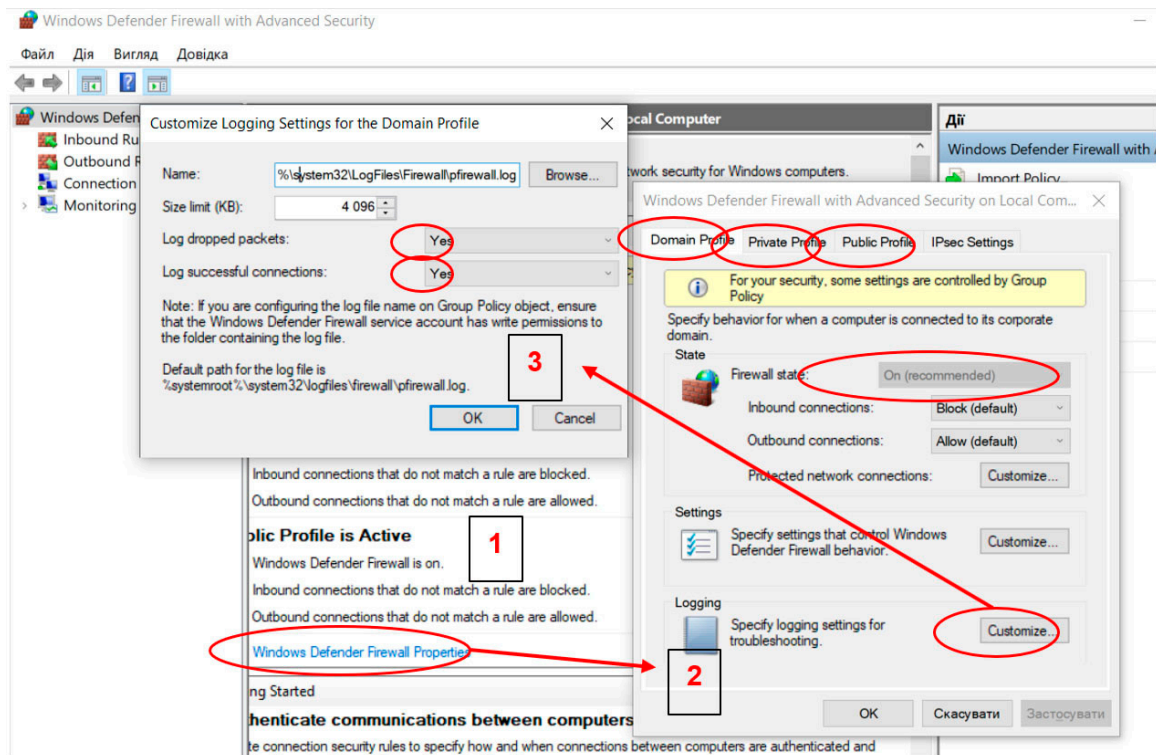


Рис. 2. Налаштування журналу подій Windows Defender Firewall

У каталозі C:\Windows\System32\LogFiles\Firewall знайти файл pfirewall.log (рис. 3).

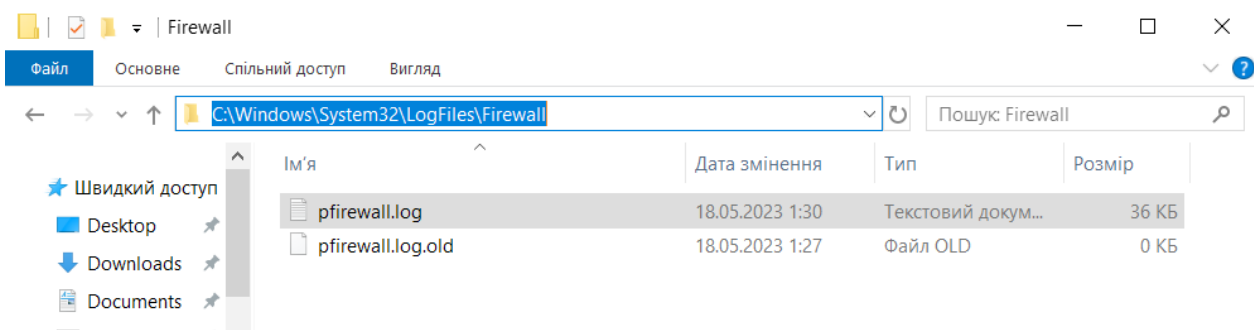


Рис. 3. Локація журналу подій pfirewall.log

Через властивості файлу `pfirewall.log` перейти по вкладкам Безпека – Додатково – Дозволи – Продовжити (рис. 4), а потім – Увімкнути успадкування (рис. 5).

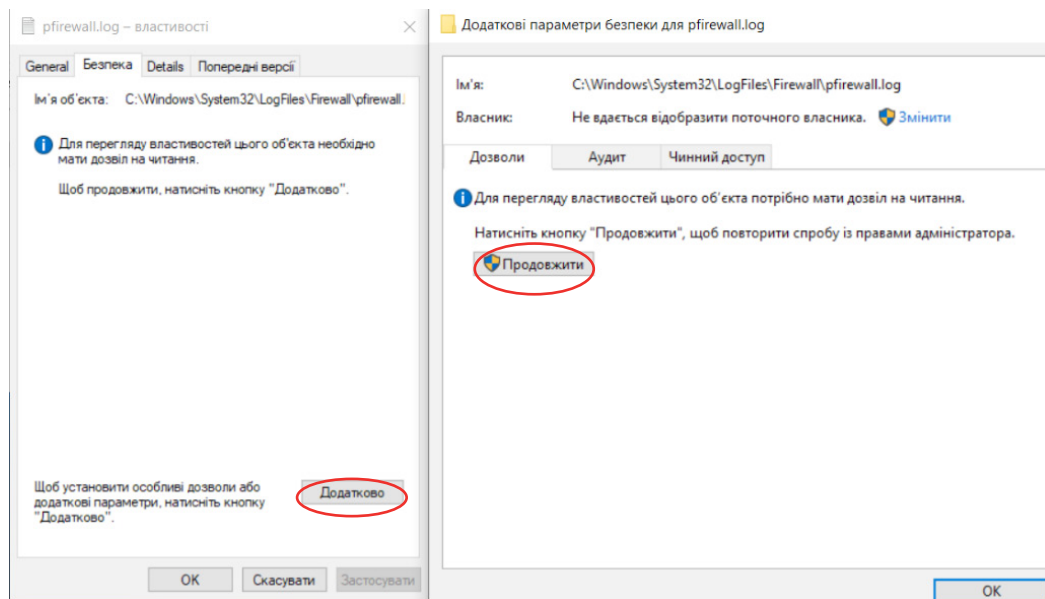


Рис. 4. Налаштування параметрів доступу до файлу `pfirewall.log`

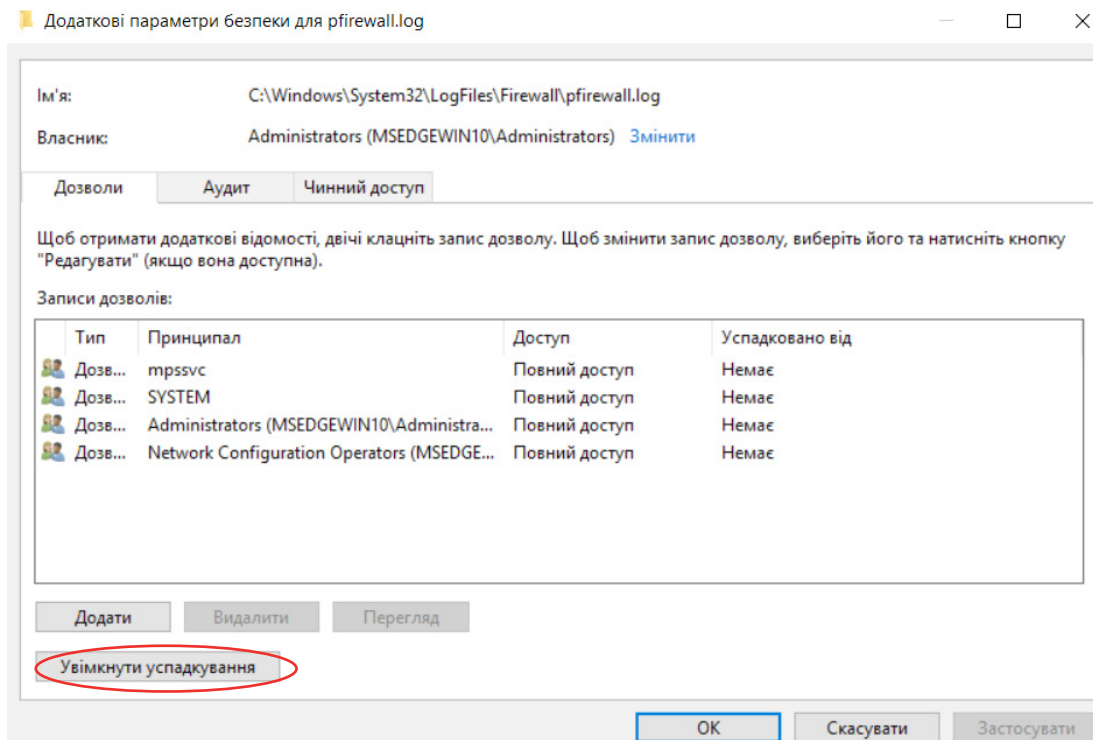
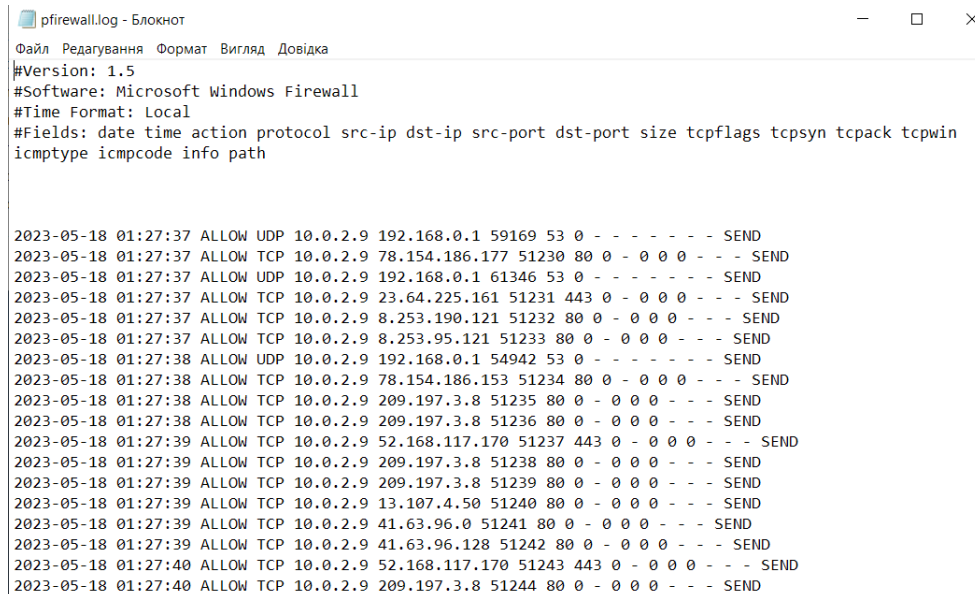


Рис. 5. Увімкнення успадкування прав доступу для файлу `pfirewall.log`

Переконайтеся, що файл журналу `pfirewall.log` доступний для читання, відкривши його текстовим редактором (рис. 6).

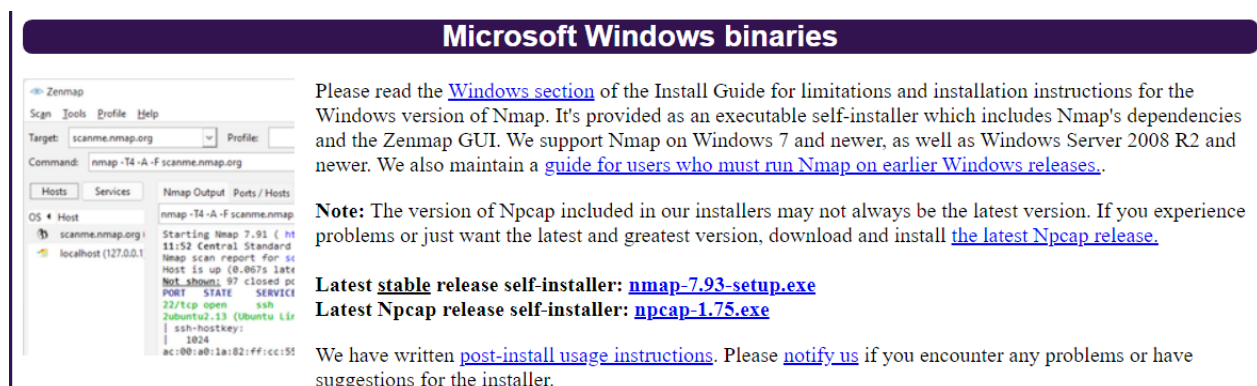


```
File Edit Format View Help
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin
icmp type icmpcode info path

2023-05-18 01:27:37 ALLOW UDP 10.0.2.9 192.168.0.1 59169 53 0 - - - - - SEND
2023-05-18 01:27:37 ALLOW TCP 10.0.2.9 78.154.186.177 51230 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:37 ALLOW UDP 10.0.2.9 192.168.0.1 61346 53 0 - - - - - SEND
2023-05-18 01:27:37 ALLOW TCP 10.0.2.9 23.64.225.161 51231 443 0 - 0 0 0 - - SEND
2023-05-18 01:27:37 ALLOW TCP 10.0.2.9 8.253.190.121 51232 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:37 ALLOW TCP 10.0.2.9 8.253.95.121 51233 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:38 ALLOW UDP 10.0.2.9 192.168.0.1 54942 53 0 - - - - - SEND
2023-05-18 01:27:38 ALLOW TCP 10.0.2.9 78.154.186.153 51234 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:38 ALLOW TCP 10.0.2.9 209.197.3.8 51235 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:38 ALLOW TCP 10.0.2.9 209.197.3.8 51236 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 52.168.117.170 51237 443 0 - 0 0 0 - - SEND
2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 209.197.3.8 51238 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 209.197.3.8 51239 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 13.107.4.50 51240 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 41.63.96.0 51241 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:39 ALLOW TCP 10.0.2.9 41.63.96.128 51242 80 0 - 0 0 0 - - SEND
2023-05-18 01:27:40 ALLOW TCP 10.0.2.9 52.168.117.170 51243 443 0 - 0 0 0 - - SEND
2023-05-18 01:27:40 ALLOW TCP 10.0.2.9 209.197.3.8 51244 80 0 - 0 0 0 - - SEND
```

Рис. 6. Зміст журналу аудиту Microsoft Windows Firewall

У журналі аудиту Microsoft Windows Firewall (рис. 6) зазначені: дата і час, дозвіл на встановлення з'єднання (ALLOW), протокол з'єднання (UDP, TCP), IP адреси з'єднання (src-ip, dst-ip), порти з'єднання (src-port, dst-port), інше. Завантажити та встановити Nmap Security Scanner в ОС Windows (<https://nmap.org/download#windows>) (рис. 7).



Microsoft Windows binaries

Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of Nmap. It's provided as an executable self-installer which includes Nmap's dependencies and the Zenmap GUI. We support Nmap on Windows 7 and newer, as well as Windows Server 2008 R2 and newer. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just want the latest and greatest version, download and install [the latest Npcap release](#).

Latest stable release self-installer: [nmap-7.93-setup.exe](#)
Latest Npcap release self-installer: [npcap-1.75.exe](#)

We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the installer.

Рис. 7. Сторінка завантаження Nmap Security Scanner для ОС Windows

Відкрити сканер через ярлик «Nmap – Zenmap GUI», у полі Target вписати loopback IP адрес своєї системи: 127.0.0.1 та у режимі Quick scan plus запустити сканування (рис. 8). Сканування є підготовчим етапом перед атакою на систему, при якому здійснюється послідовний перебір портів підключення до цільової системи.

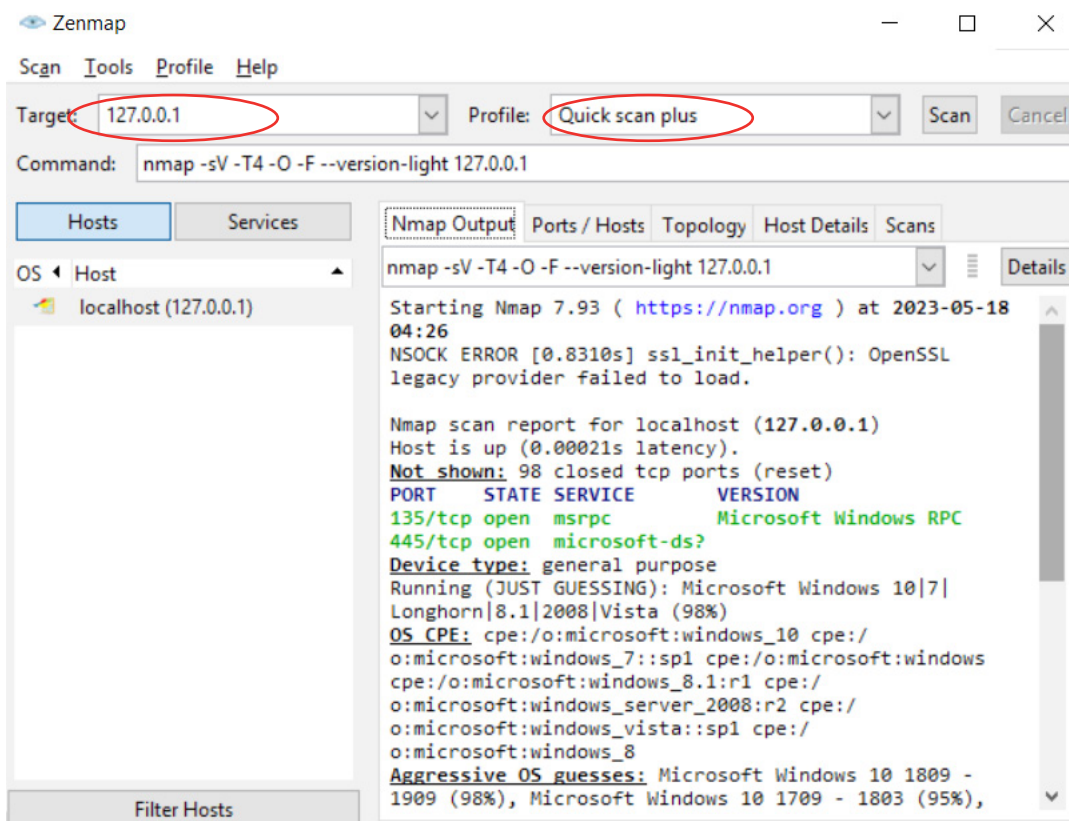


Рис. 8. Запуск сканування своєї системи

Відкрити файл журналу аудиту pfirewall.log та знайти записи, які свідчать про сканування портів системи і є провісниками майбутньої атаки на систему (рис. 9). Основною ознакою сканування є наявність великою кількості одночасних підключень з одного IP адреса до різних портів системи.

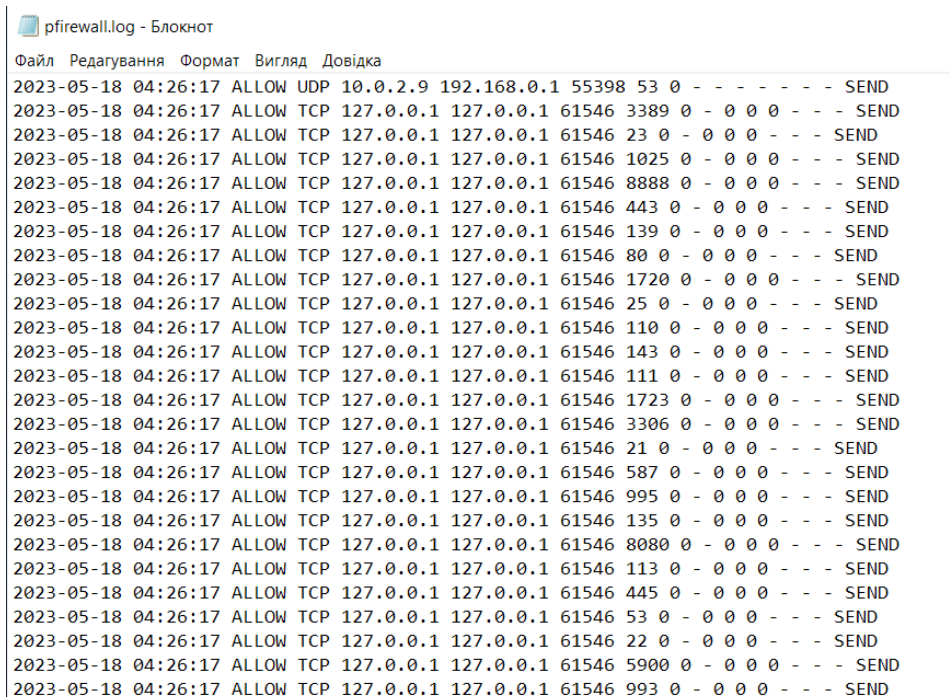


Рис. 9. Записи журналу аудиту pfirewall.log, які свідчать про сканування портів системи

Заповнити шаблон звіту про подію інформаційної безпеки (табл. 1).

Таблиця 1. Шаблон звіту про події інформаційної безпеки

ЗВІТ ПРО ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
1. Дата події	3. Ідентифікаційні номери відповідної події та/або інциденту (якщо застосовне)
2. Номер події (надається фахівцем ISIRT)	
4. РЕКВІЗИТИ ОСОБИ, ЯКА ЗВІТУЄ	
4.1. Ім'я та прізвище	4.2. Адреса
4.3. Організація	4.4. Відділ
4.5. Телефон	4.6. E-mail
5. ОПИС ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
5.1. Опис події: • Що сталося • Яким чином сталося • Чому так сталося • Які компоненти/активи піддались впливу • Оцінка впливу на діяльність організації • Будь-які виявлені вразливості	
6. ДЕТАЛІ ПОДІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	
6.1. Дата та час події	
6.2. Дата та час виявлення події	
6.3. Дата та час повідомлення про подію	
6.4. Чи відповідь на цю подію усунула небезпеку?	ТАК ☐ НІ ☐ (позначте відповідне)
6.5. Якщо так, вкажіть, скільки часу тривала подія (у днях/годинах/хвилинах)	

Задача 2.

1. Налаштувати аудит входу користувача в систему.
2. Ввести кілька разів неправильний пароль при вході до ОС Windows.
3. Виявити індикатори інциденту інформаційної безпеки та заповнити звіт щодо події інформаційної безпеки.

Виконання.

Через рядок пошуку відкрити Налаштування групової політики (Edit group policy) (рис. 10).

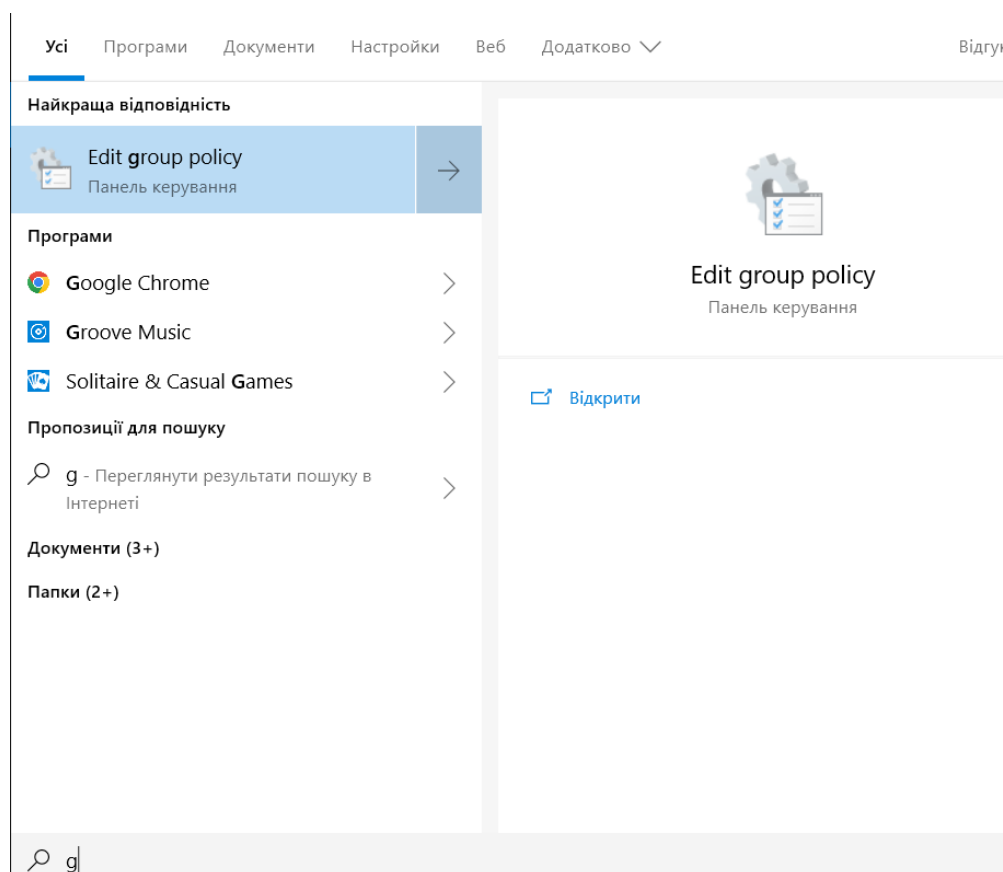


Рис. 10. Відкриття Налаштування групової політики (Edit group policy)

У розділі Конфігурація комп'ютера – Налаштування Windows – Security Settings – Advanced Audit Policy Configuration – «System Audit Policies – Local Group Policy Object» – Account Logon кликнути на параметр Audit Credential Validation та налаштувати аудит вдалих та невдалих перевірок автентифікаційних даних користувача при вході у систему (рис. 11).

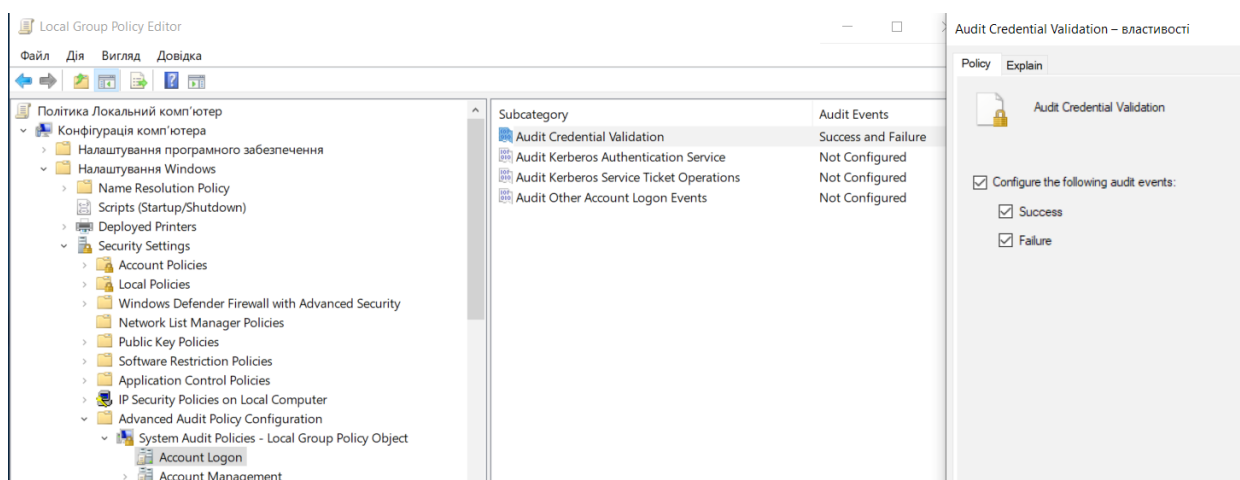


Рис. 11. Налаштування аудиту вдалих та невдалих перевірок автентифікаційних даних користувача при вході у систему

Після кількох спроб введення неправильного паролю (рис. 12) через рядок пошуку відкрити Переглядач подій (Event Viewer) – Windows Log – Security та знайти невдалі спроби вводу паролю (рис. 13).

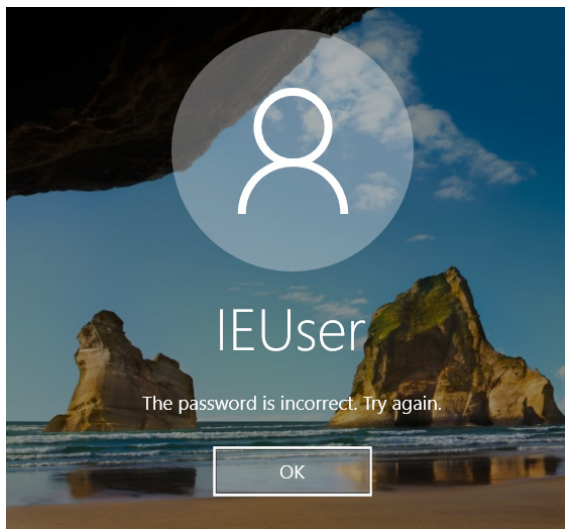


Рис. 12. Результат введення неправильного паролю

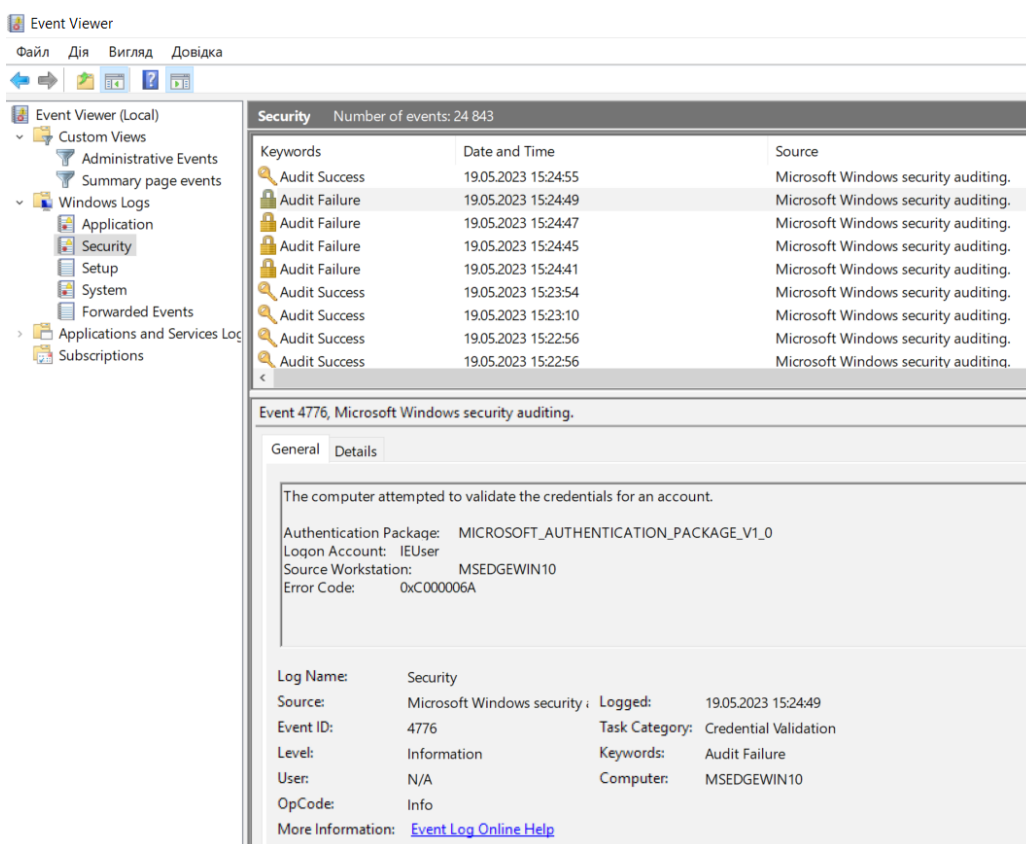


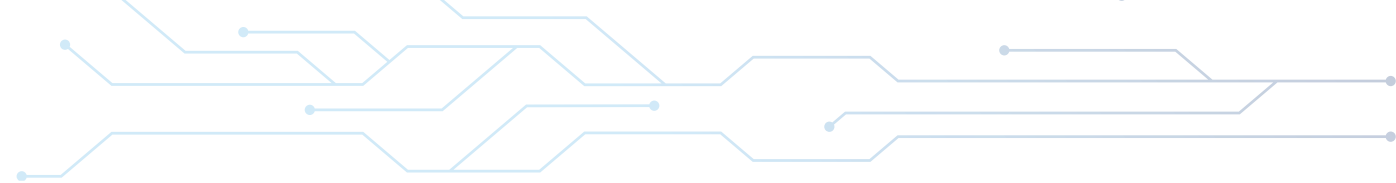
Рис. 13. Записи журналу подій про невдалі спроби входу у систему

Заповнити шаблон звіту про подію інформаційної безпеки (табл. 1).



ЧАСТИНА III

САМОСТІЙНА РОБОТА



У межах самостійної роботи здобувачам пропонується пройти веб-квест за адресою: <https://classroom.google.com/c/NjlwMTcxODg4NDQ1?cjc=dsjtt3r>.

Особливостями даного квесту є те, що під час проходження учасникам:

- ▶ дозволяється *користуватися будь-якими джерелами інформації*;
- ▶ потрібно надати відповідь на конкретні *питання, без яких неможливо пройти подальші завдання*;
- ▶ засвоюються *типові алгоритми дій* в різних ситуаціях.

Засвоїти базові поняття та важливі нюанси квесту допомагає використання ігрових навчальних платформ: AhaSlides, Kahoot, Menti, Quizizz, Slido. Для можливості залучення необмеженої кількості учасників до перевірки знань слід реєструватися як викладач.

Для створення веб-квестів можна використати GoogleClassroom.

GoogleClassroom об'єднує в собі:

- ▶ GoogleDrive для створення і обміну завданнями,
- ▶ Google Docs, Sheets and Slides для написання,
- ▶ Gmail для спілкування і
- ▶ Google Calendar для розкладу.

Учасники можуть бути запрошені до класу через приватний код чи автоматично імпортуватися з навчального сайту. Кожен клас створює окрему папку на Google-диску відповідного користувача GoogleDrive, куди учасник може подати роботу, яку оцінює викладач.

Поради, які будуть корисними при проведенні квестів:

- ▶ доступ до завдань потрібно відкривати послідовно та пояснювати помилки на кожному етапі;
- ▶ тестові питання мають бути радше маленькими завданнями, по завершенні виконання яких потрібно ввести результат як відповідь;
- ▶ усі документи, використовувані в завданнях, повинні відповідати реальним за формою;
- ▶ квест має охоплювати якомога більше елементів реального життя за відповідними категоріями;
- ▶ завдання повинні бути якомога цікавішими.

Зміст веб-квесту

Знайомтеся!

Олексій Сушко – молодий, амбітний випускник вишу, який влаштувався на роботу до державного органу.

Людина вельми комунікабельна, захоплюється дайвінгом та риболовлю.

Мріє побудувати блискучу кар'єру на державній службі.

Понятійний апарат у сфері кібергігієни

Коли Олексій Сушко влаштувався на роботу до державного органу, він почав активно вивчати нормативну базу у сфері інформаційної та кібербезпеки. Серед іншого, Олексій звернув увагу на Стратегію кібербезпеки України. Згідно з цим документом формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, що мають бути досягнуті протягом періоду реалізації цієї стратегії. Скільки стратегічних цілей визначено в описаному документі?

Захист персональних даних

Під час проведення розслідування підозрілого інциденту безпеки було встановлено, що працівник Олексій Сушко зареєструвався на хакерському форумі raidforums.com з використанням облікового запису seminaristik@gmail.com. З ресурсу raidforums.com у подальшому відбувся витік даних. Фахівцями з безпеки було прийнято рішення перевірити, чи не став цей витік передумовою захоплення облікового запису працівника підрозділу.

Знайдіть параметр salt паролю облікового запису seminaristik@gmail.com для ресурсу raidforums.com.

Безпечне користування мережею Інтернет

У межах розслідування витоку даних з серверів було вилучено логфайл (файл протоколу) доступу до облікового запису Олексія Сушка. У результаті аналізу в файлі було залишено тільки записи, які свідчать про вхід у систему, коли Олексій не міг цього робити. В результаті вивчення IP-адрес, з яких було здійснено авторизацію в системі, було встановлено, що більшість адрес асоційовані з закордонними VPN-сервісами, проте одна IP-адреса викликала інтерес у розслідувачів. Яка це адреса?

Безпека мобільних пристроїв

Під час дослідження службового мобільного пристрою особи, облікові дані якої було скомпрометовано, в месенджері Telegram було виявлено сторонній сеанс зв'язку з IP-адресою 46.201.227.191. Для з'ясування ситуації було вирішено зв'язатися із відповідним провайдером. Вкажіть назву провайдера, з яким необхідно встановити контакт.

Соціальна інженерія

Олексій Сушко взяв відпустку за власний рахунок та повідомив керівництво, що йому потрібно все обдумати й відпочити. Резервне джерело для спілкування – його електронна пошта.

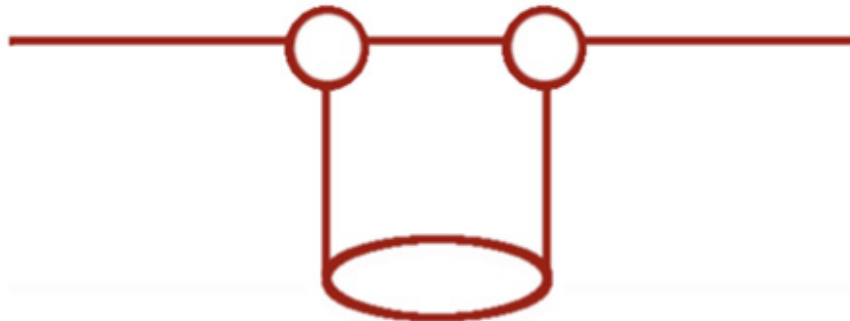
З'ясуйте яким чином могли бути скомпрометовані його облікові дані.

Введіть посилання на сторінку в Інтернет, яка могла бути використана для атаки.

Визначте Facebook-адресу потенційного зловмисника.

Убезпечення від неправдивих повідомлень

Під час вивчення облікового запису особи, яка становить інтерес (Аріеля), у розслідувачів виникла підозра, що наведені там відомості є фейковими. Для того, щоб пересвідчитись у цьому, були застосовані кілька спеціалізованих сервісів. За результатами проведеного аналізу було встановлено, що фото профілю ймовірно було згенеровано за допомогою ресурсу thispersondoesnotexist.com. Для перевірки цього факту застосовувався шаблон, як на рисунку.



Перевіряючи дописи на сторінці облікового запису Аріеля, було виявлено, що ймовірність їх створення системою штучного інтелекту становить 52%.

Вкажіть посилання в форматі https://назва_ресурсу/ на сервіс, звідки розслідувачі могли взяти шаблон для перевірки фото.

Вкажіть посилання в форматі https://назва_ресурсу.me/ на сервіс, за допомогою якого розслідувачі могли здійснювати перевірку тексту.

Під час проведення розслідування було встановлено, що для скорочення фішингового посилання зловмисник використав один із сервісів скорочення посилань, який він раніше побачив на каналі Освіта MBC (<https://t.me/osvitamvs>).

Проаналізуйте канал <https://t.me/osvitamvs>. Вкажіть, скільки сервісів скорочення посилань використано у цьому каналі?

Безпечне користування електронною поштою

Степан користується паролемним менеджером KeePass, але він забув майстер-пароль до файлу бази даних «Database.kdbx», де зберігався пароль до поштової скриньки відділу його організації scv89kl@corp.ua.



Олексій Сушко надіслав Степану у зашифрованому повідомленні пароль до файлу бази даних «Database.kdbx». У Степана є файл «Степан stepan@test.com(7503C2CC05A0D106)_pub_sec.asc» з його приватним і публічним ключами.

Яким є пароль до імейлу scv89kl@corp.ua?

Шкідливе програмне забезпечення

Під час огляду службового комп'ютеру у межах реагування на інцидент інформаційної безпеки був виявлений зашифрований архів arc.zip з трьома файлами. В подальшому був знайдений пароль для відкриття архіву: cd4hNs6ssFxGaf.

Визначити наявність в архіві шкідливого програмного забезпечення та його позначення антивірусною системою.

Безпечне користування соціальними мережами

Олексій Сушко попав у поле зору зломисників як працівник установи, на комп'ютерну мережу якої готується кібератака. Зломисники намагаються встановити поточне місце перебування Олексія, який опублікував у соціальній мережі фото зі свого смартфона.

Де зроблене фото?

Фізична безпека

На службовому комп'ютері встановлена ОС Windows 10 Home. З огляду на наявні ризики інформаційної безпеки є потреба у створенні захищених флеш-накопичувачів.

Який програмний засіб і як допоможе створити захищений флеш-накопичувач?

Реагування на інциденти безпеки

Олексій Сушко на службовому комп'ютері за встановленою процедурою з метою виявлення інцидентів інформаційної безпеки періодично переглядає файл журналу подій Microsoft Windows Firewall.

Чи містить наявний файл журналу подій (pfirewall.log) Microsoft Windows Firewall провісники або індикатори інциденту інформаційної безпеки?

