# 1. ОСНОВНІ ПРИНЦИПИ КІБЕРБЕЗПЕКИ. СОЦІАЛЬНА ІНЖЕНЕРІЯ

1.1. Поняття інформаційна безпека та кібербезпека, кібергігієна.

1.2. Загальні правила кібербезпеки.

1.3. Методи соціальної інженерії.

1.4. Протидія соціальній інженерії.

1.5. Спам.

1.6. Конфіденційність і безпека в соціальних мережах.

## 1.1. Поняття інформаційна безпека та кібербезпека, кібергігієна.

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

- неповноту, невчасність та невірогідність інформації, що використовується;
- негативний інформаційний вплив;
- негативні наслідки застосування інформаційних технологій;
- несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Інформаційна безпека– стан захищеності інформаційного середовища суспільства, що забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави.

В залежності від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати наступним чином:

- як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;
- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
- інформаційних прав і свобод людини і громадянина.

Основні параметри, які є базовими для забезпечення захисту інформації:

- конфіденційність – гарантія того, що конкретна інформація доступна тільки тому колу осіб, для кого вона призначена; порушення цієї категорії називається розкраданням або розкриттям інформації;
- цілісність – гарантія того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;
- автентичність – гарантія того, що джерелом інформації є саме та особа, яку заявлено як її автора; порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення;
- апелюємість – гарантія того, що при необхідності можна буде довести, що автором повідомлення є саме заявлена людина, і не може бути ніхто інший; відмінність цієї категорії від попередньої в тому, що при підміні автора, інша людина намагається привласнити собі авторство повідомлення, а при порушенні апеллюємості – сам автор намагається «відхреститися» від своїх слів.

Кібербезпека – це заснована на обчисленнях дисципліна, що включає технології, фахівців, інформацію і процеси, покликані забезпечити роботу в умовах дій зловмисників. Вона спирається на основоположні області інформаційної безпеки і забезпечення цілісності і захисту інформації, при цьому фокусуючись на області комп'ютерної безпеки.

Кібербезпека – це безпека IT систем (обладнання та програм). Кібербезпека є частиною інформаційної безпеки будь-якої організації.

Наскільки захищений ваш домашній комп'ютер чи ваш вебсайт від зламу хакерами – це питання кібербезпеки. Але чи кріпите ви стікер із записаним паролем від комп'ютера чи профайлу у соцмережі на екран свого монітору – це вже питання вашої інформаційної безпеки.

Згідно із загальноприйнятим визначенням, безпечна комп'ютерна інформаційна система – це ідеальна система, яка коректно і у повному обсязі

реалізує ті і лише ті цілі, що відповідають намірам її власника. На практиці побудувати складну систему, що задовольняє цьому принципові, неможливо, і не лише з огляду на ймовірність виникнення несправностей і помилок, але й через складність визначення і формулювання суперечливих очікувань проектувальника системи, програміста, законного власника системи, власника даних, що обробляються, та кінцевого користувача. Навіть після їхнього визначення у багатьох випадках важко або й неможливо з'ясувати, чи функціонує програма у відповідності із сформульованими вимогами. У зв'язку з цим забезпечення безпеки зводиться найчастіше до управління ризиком: визначення потенційних загроз, оцінка ймовірності їхнього настання та оцінка потенційної шкоди, із наступним ужиттям запобіжних заходів в обсязі, що враховує технічні можливості й економічні обставини.


Кібергігієна є набором дій, що виконуються користувачами комп'ютерів та інших пристроїв для підвищення мережевої безпеки та забезпечення працездатності системи. Кібергігієна – це спосіб мислення та звички з фокусом на безпеку, які допомагають користувачам та організаціям знизити кількість порушень в Інтернеті.

Кібергігієну іноді порівнюють з особистою гігієною: в обох випадках це регулярні запобіжні заходи для забезпечення здоров'я та благополуччя.

Дотримання кібергігієни допоможе не допустити порушення безпеки та крадіжки особистих даних кіберзлочинцями, а також бути в курсі оновлень програмного забезпечення та операційних систем.

Кібергігієна дозволяє виключити випадки:

- порушень безпеки, у тому числі загрози з боку зловмисників, шкідливих програм та вірусів;
- втрати даних – якщо для жорстких дисків та хмарних сховищ не створено резервні копії, вони можуть зазнати злому, бути пошкоджені, або з ними можуть виникнути інші проблеми, що ведуть до втрати даних;
- використання застарілого програмного забезпечення, зокрема, антивірусного, використання якого може підвищити вразливість пристроїв для атак.

Дотримання кібергігієни забезпечується завдяки виконання регулярних дій та вироблення навичок, а також використання належних інструментів.

Кібергігієна – це не разовий захід, її потрібно дотримуватися постійно. Можна створювати звички, встановлювати автоматичні нагадування та додавати до календаря дати виконання різних завдань. Такі завдання можуть включати виконання антивірусної перевірки за допомогою відповідного програмного забезпечення, зміну паролів, підтримку в актуальному стані програм, програмного забезпечення та операційних систем, а також очищення жорсткого диска.

До інструментів, що забезпечують кібергігієну відносяться:

- мережевий екран (фаервол) – запобігає несанкціонованому доступу до вебсайтів, поштових серверів та інших джерел інформації, до яких можна отримати доступ з Інтернету;
- програмне забезпечення для видалення даних та непотрібних програм;
- менеджер паролів – використання надійних складних паролів, які необхідно регулярно змінювати, – це важливий аспект безпеки в Інтернеті;

- високоякісне антивірусне програмне забезпечення, що виконує регулярну автоматичну перевірку пристрою за розкладом, виявляє та видаляє шкідливі програми, а також захищає від мережевих загроз та порушень безпеки.

## 1.2. Загальні правила кібербезпеки.

Для дотримання кібергігієни доцільно використовувати наведені нижче правила.

1. Правильно використовуйте надійні паролі:

- не використовуйте той самий пароль для кількох облікових записів;
- регулярно змінюйте пароль;
- використовуйте паролі завдовжки не менше 12 символів (в ідеалі, довше);
- використовуйте паролі, до складу яких входять великі та малі літери, символи та цифри;
- не використовувати прості паролі. У паролі не повинні використовуватися комбінації послідовних цифр (1234) та особисту інформацію, яку може вгадати той, хто вас знає, наприклад, дата народження або ім’я домашньої тварини;
- змінюйте встановлені за замовчуванням паролі на Ваших пристроях;
- не записувати паролі та не повідомляти їх іншим людям;
- використовувати менеджер паролів, щоб створювати, зберігати та керувати всіма паролями за допомогою єдиного захищеного облікового запису.

2. використовуйте багатофакторну автентифікацію:

- налаштуйте захист за допомогою багатофакторної автентифікації для всіх основних облікових записів (електронна пошта, соціальні мережі, банківські програми);
- зберігайте резервні коди багатофакторної аутентифікації у диспетчері паролів.

3. виконуйте регулярне резервне копіювання даних:

- створюйте резервні копії важливих файлів в автономному режимі, на зовнішньому жорсткому диску, флешці або у хмарі.

4. Забезпечення конфіденційності:

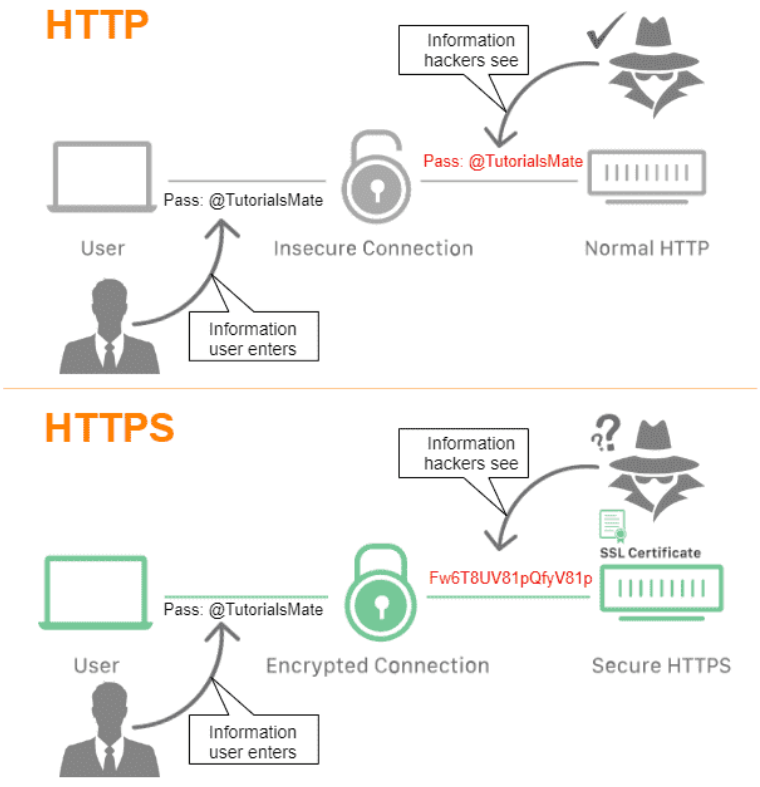
- не публікуйте в соціальних мережах особисту інформацію, таку як домашню адресу, особисті фотографії, номер телефону, номери кредитних карток;
- оцініть налаштування конфіденційності у соціальних мережах та переконайтеся, що вони встановлені на належному рівні;
- уникайте вікторин, ігор та опитувань у соціальних мережах, де запитується конфіденційна особиста інформація;
- обережно ставтеся до надання дозволів для програм й додатків, які ви встановлюєте;
- заблокуйте комп’ютер та телефон за допомогою пароля або PIN-коду;
- намагайтеся не розголошувати особисту інформацію під час використання загальнодоступних мереж Wi-Fi;
- скористайтеся віртуальною приватною мережею (VPN), особливо при використанні загальнодоступних мереж Wi-Fi, це допоможе забезпечити максимальну конфіденційність;
- здійснюйте всі онлайн-транзакції на безпечних вебсайтах, веб-адреси яких починаються з https://, а не http://, а ліворуч від адресного рядка є позначка замка.

4. Оновлення програм, програмного забезпечення та прошивок:

- регулярно оновлюйте програми, веб-браузери, операційні системи та прошивки, щоб використовувати останні версії, в яких усунуто або виправлено можливі вразливості безпеки;
- налаштуйте функції автоматичного оновлення програмного забезпечення;
- видаляйте програми, які Вам більше не потрібні;
- завантажуйте програми лише з надійних чи офіційних джерел.

5. Забезпечення безпеки роутерів:

- змініть стандартне ім’я для домашньої мережі Wi-Fi;
- змініть ім’я користувача та пароль роутера;
- підтримуйте актуальність прошивки;
- вимкніть віддалений доступ, універсальне налаштування мережевих пристроїв (Universal Plug and Play) та налаштування захищеного Wi-Fi;
- створіть окрему мережу;
- перевірте, чи підтримує роутер шифрування WPA2 або WPA3 для захисту конфіденційності інформації, що передається через мережу.



6. Захист від атак соціальної інженерії:

- не переходьте за підозрілими посиланнями, у яких ви не впевнені;
- не відкривайте листи, що підозріло виглядають;
- не завантажуйте підозрілі вкладення у повідомленнях електронної пошти та текстові повідомлення, на які ви не очікуєте;
- не переходьте за оголошеннями, які обіцяють безкоштовні гроші, призи та знижки.

7. використовуйте мережевий екран:

- використовуйте мережевий екран для запобігання доступу до Вашого комп'ютера або мережі з боку шкідливих програм через Інтернет;
- перевірте правильність налаштувань мережевого екрана.

8. Шифрування пристроїв: використовуйте шифрування Ваших пристроїв та носіїв, які містять конфіденційні дані, включаючи ноутбуки, планшети, смартфони, зйомні диски та хмарне сховище.

9. Очищення жорстких дисків перед утилізацією або продажом комп'ютера, планшета чи смартфона, необхідно очистити жорсткі диски, з метою унеможливити доступ третіх осіб до Ваших персональних даних.

10. Забезпечення надійного антивірусного захисту:

- використовувати надійне антивірусне програмне забезпечення, яке запобігає вірусам та іншим шкідливим програмам з подальшим їх видаленням.
- постійно оновлюйте антивірусне програмне забезпечення.

## 1.3. Методи соціальної інженерії.

Захист від проникнення – це комплексна робота, яка передбачає і автоматичні, і ручні методи перевірки. Але, як і раніше, найуразливішою ланкою залишається людина: вона має доступ до інформації і на неї можна впливати методами соціальної інженерії.

Соціальна інженерія – низка методів, якими користуються шахраї, щоб «зламати» людей з метою незаконно отримати від них необхідну інформацію чи засоби доступу до неї. При цьому шахраї використовують психологічні

маніпуляції та знання соціології, й не застосовують технічні засоби. Соціальна інженерія – нетехнічна загроза інформаційній безпеці

Професор психології Роберт Чалдіні («Психологія впливу», 1984 р.) описав шість принципів впливу , які застосовують соціальні інженери:

- взаємність – віддячити добром за добро;
- послідовність – дотримуємось власних переконань;
- соціальний доказ – погоджуємося з тим, що робить більшість людей;
- влада та авторитет – готові слідувати за людьми, яким довіряємо та яких поважаємо;
- симпатія – із задоволенням виконуємо прохання людей, які нам подобаються;
- дефіцит – бажаємо, те, що нам недоступно.

Соціальні інженери користуються тим, що психологічні маніпуляції не вимагають великих витрат та специфічних знань (крім кількох психологічних прийомів), їх можна застосовувати протягом тривалого часу до того ж їх складно виявити. Джон Макафі (творець антивірусу McAfee) стверджує , що три чверті інструментів середнього хакера – це методи соціальної інженерії і в особливо успішних хакерів їх частка досягає 90%. У 2020 році було створено 6,95 міліона нових фішингових та шахрайських сторінок. Найпоширеніші типи атак на малий бізнес у 2021 році (embroker.com):

- фішинг/соціальна інженерія: 57%
- зламані/викрадені пристрої: 33%
- крадіжка облікових даних: 30%

Інструменти (методи) соціальної інженерії.

Фішинг (fishing ) – дозволяє обманним шляхом отримувати різну цінну інформацію, маскуючи комунікації так, ніби вони надійшли з надійного джерела. Надалі інформація може бути використана для доступу до пристроїв або мереж. При фішинговій атаці зловмисник використовує повідомлення, надіслане електронною поштою, в соціальних мережах, клієнта для обміну миттєвими повідомленнями або SMS, щоб отримати конфіденційну інформацію

від жертви або обманним шляхом змусити її клацнути посилання на шкідливий вебсайт.

Фішингові повідомлення привертають увагу жертви та закликають до дії, викликаючи цікавість, просячи допомоги чи викликаючи інші емоційні спускові механізми. Вони часто використовують логотипи, зображення чи стилі тексту, щоб підробити особистість, створюючи враження, що повідомлення походить від колеги по роботі, банку жертви чи іншого офіційного каналу.

У більшості фішингових повідомлень використовується фактор терміновості, який змушує жертву вважати, що будуть негативні наслідки, якщо вони не передадуть конфіденційну інформацію швидко.

Частинними випадками фішінгу є «водопій» (watering hole) та «атака китобою» (whaling attack).

Атака «водопою» включає запуск або завантаження шкідливого коду з легітимного вебсайту, який зазвичай відвідують цілі атаки. Наприклад, зловмисники можуть скомпрометувати сайт новин фінансової індустрії, знаючи, що люди, які працюють у сфері фінансів і, таким чином, представляють привабливу мету, можуть відвідати цей сайт. Зламаний сайт, як правило, встановлює троян-бекдор, який дозволяє зловмиснику зламати та дистанційно керувати пристроєм жертви.

Атаки водопою зазвичай виконуються досвідченими зловмисниками, які виявили експлойт нульового дня (програму або код, що використовує недоліки в системі безпеки конкретного додатку для інфікування пристрою).

Атака китобою є типом атаки фішингу, спрямованої на конкретних користувачів з привілейованим доступом до систем або доступом до дуже цінної конфіденційної інформації. Наприклад, китобійна атака може бути здійснена проти старших керівників, заможних людей або мережевих адміністраторів.

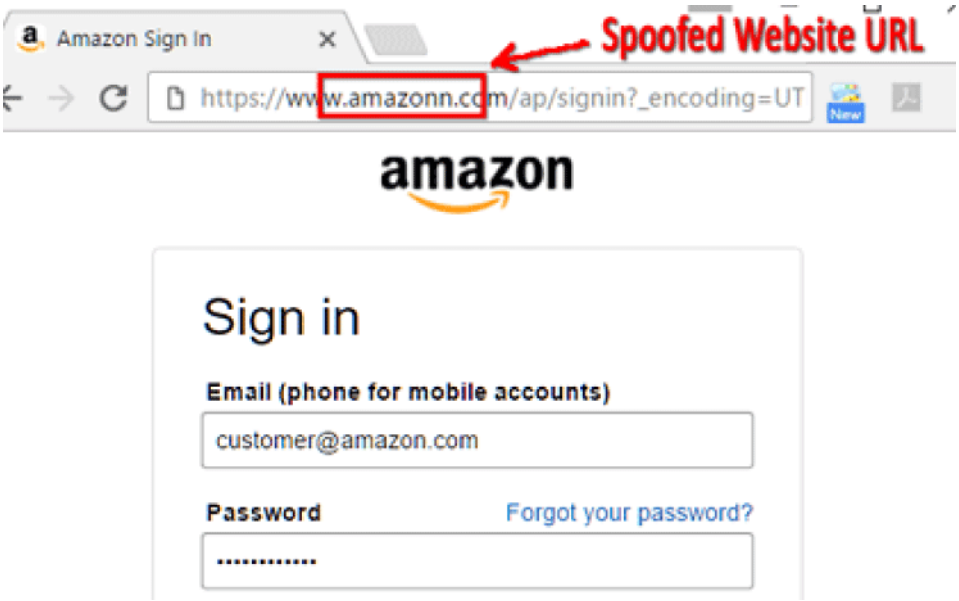
Китобійна атака складніша, ніж звичайна фішингова атака. Зловмисники проводять ретельне дослідження, щоб створити повідомлення, яке змусить конкретні цілі відповісти та виконати бажану дію. Китобійні листи часто

«прикидаються» критично важливими діловими листами, відправленими колегою, співробітником або провідним менеджером, які потребують термінового втручання з боку жертви.

Зазвичай зловмисники використовують наступні методи фішингу у своїх атаках.

Обманні веб-посилання. Найбільш часто використовувана стратегія полягає в тому, що шахраї маскують зловмисне веб-посилання як вказівку на легітимне або довірене джерело. Ці типи фішингових атак можуть приймати будь-яку кількість форм, наприклад, застосування шахрайських URL-адрес, створення піддомену для зловмисного вебсайту або експлуатація дуже схожих доменів.

Наприклад, латинська літера I дуже близька до L на стандартних клавіатурах QWERTY, що робить googie дуже схожим на google. У випадку субдоменів зловмисник, який, наприклад, контролює доменне ім’я example.com, може створити субдомени для нього: paypal.example.com. В період президентських виборів у США 2016 року для проведення фішинг-атаки на базі схожих доменів зловмисники використали сайт accounts-google.com як клон сайту accounts.google.com.




Інтернаціональні доменні імена (IDN) також можуть використовуватися для створення хибних, але схожих зі справжніми доменних імен, дозволяючи

використовувати не-ASCII символи. Візуальні подібності між символами, застосовують для створення доменних імен, які візуально неможливо диференціювати. Це спонукає користувачів приймати один домен за інший.

Клонування вебсайтів, підробка та перенаправлення. Вебсайти, вразливі до атак типу межсайтовий скриптинг (XSS), використовуються зловмисниками для запису власного контенту на інший вебсайт. XSS-атака може застосуватися для перехоплення даних, введених на скомпрометованому сайті (включно з ім'ям користувача та паролем), які зловмисники використають пізніше.

Деякі фішингові атаки використовують XSS для створення спливаючих вікон, які походять з вразливого вебсайту, але завантажують сторінку, яка контролюється зловмисниками. Часто такий тип прихованого перенаправлення відкриває форму для входу з метою збору реєстраційних даних.


From: **ZOOM** <noreply@[redacted]
Date: Tue, Apr 6, 2021 at 8:21 AM
Subject: Your meeting attendees are waiting!
To: [redacted]

zoom

Hi [redacted]

There are 7 attendees in your waiting room.

Please click this URL to start your Zoom meeting:
[redacted] Zoom Meeting Room, [redacted] zoom.us/j/99838789?pwd=Y0dyci9TWGJXSnluVllBOE1EUT09

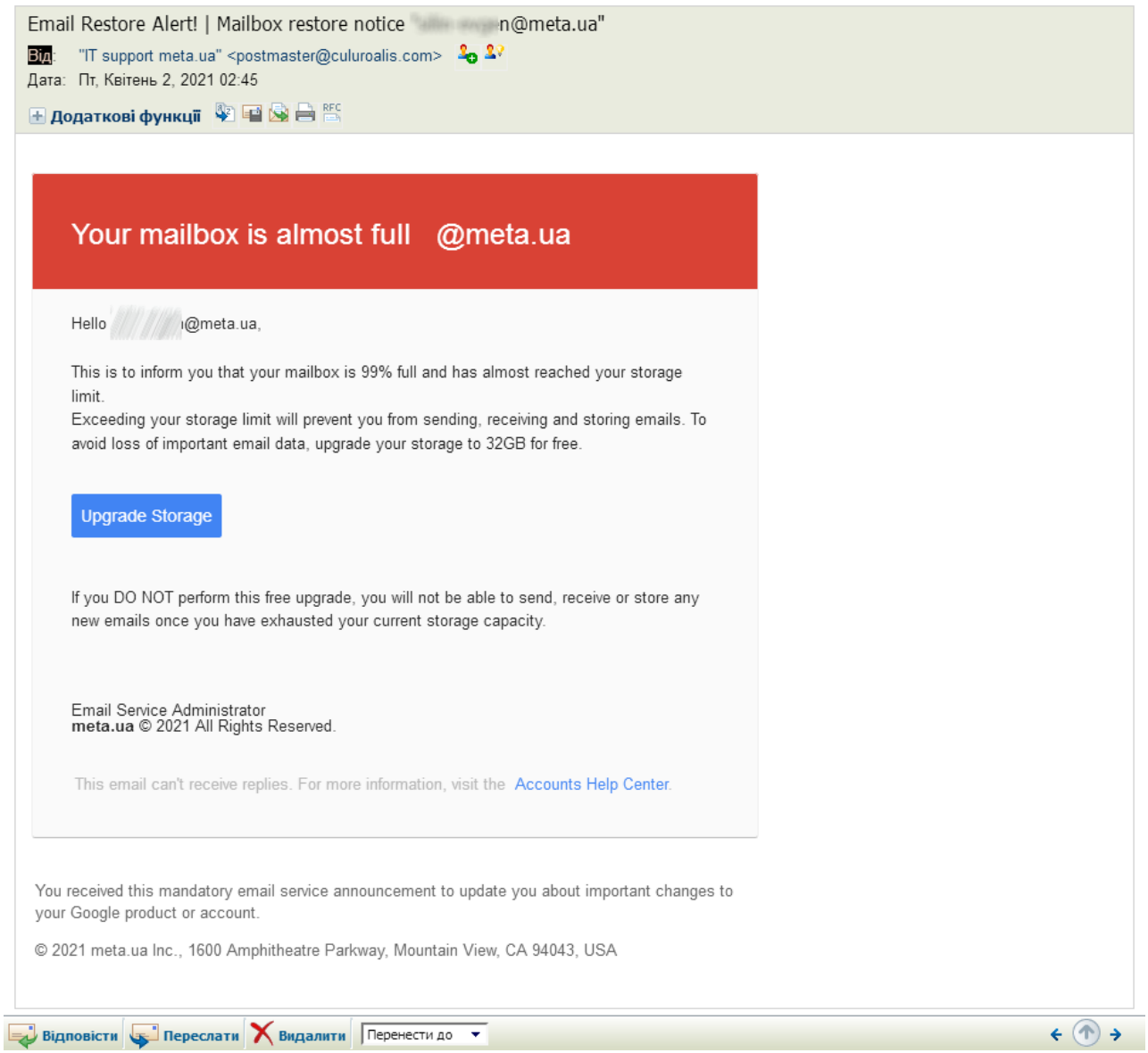
Thank you for choosing Zoom.
-The Zoom Team

Copyright ©2020 Zoom Video Communications, Inc. All rights reserved.

Вішинг (vishing) – голосовий фішинг аналогічний до фішингу, але виконується шляхом дзвінка жертвам по телефону.

Претекстинг (pretexting) – атака, в якій зловмисник представляється іншою людиною та за заздалегідь підготовленим сценарієм дізнається про конфіденційну інформацію. Для цього виду атак важливо мати заготовлений

сценарій розмови (обман має на увазі голосове спілкування), знати кілька фактів про жертву та діяти максимально швидко, не залишаючи часу на роздуми. Зазвичай реалізується через телефон чи електронну пошту. Наприклад, зловмисники можуть видати себе за зовнішнього постачальника IT-послуг та запросити дані облікового запису користувача та паролі, щоб допомогти їм у вирішенні проблеми. Або вони можуть прикинутися фінансовою установою жертви, запитуючи підтвердження номера їхнього банківського рахунку або облікових даних вебсайту банку.





Пошук інформації у відкритих джерелах (OSINT: Open source intelligence) – розвідка на основі відкритих джерел: ЗМІ, публікації в Інтернеті, загальнодоступні дані аерозйомок та радіомоніторингу, публічні звіти державних та комерційних організацій, професійні звіти, конференції, доповіді.

Плечовий серфінг (shoulder surfing ) – техніка, при якій потрібну інформацію підглядають з-за плеча. Найпростіше це зробити у місцях великого скупчення людей: у кафе, громадському транспорті, у залі очікування аеропорту чи вокзалу.

Обернена соціальна інженерія (reverse engineering) – жертва сама ділиться конфіденційною інформацією із шахраєм. Так, достатньо представитися співробітником техпідтримки банку, мобільного оператора чи будь-якої іншої організації, в якій людина залишила персональні дані. Усередині компанії працює інша схема: зловмисник пропонує послугу, від якої жертва не може або не хоче відмовитись, передаючи йому свої дані для авторизації чи іншу цінну інформацію. Наприклад, зловмисник, який працює разом із жертвою, змінює на її комп'ютері ім'я файлу або переміщає його в інший каталог. Коли жертва

помічає зникнення файлу, зловмисник заявляє, що може все виправити. Бажаючи якнайшвидше завершити роботу або уникнути покарання за втрату інформації, жертва погоджується на цю пропозицію. Зловмисник заявляє, що вирішити проблему можна лише увійшовши до системи з обліковими даними жертви. Тепер уже жертва просить зловмисника увійти до системи під її ім'ям, щоб спробувати відновити файл. Зловмисник неохоче погоджується та відновлює файл, та краде ідентифікатор й пароль жертви.

Атаки приманка (baiting) або троянський кінь – зловмисники надають дещо, що жертви вважають за корисне. Це може бути передбачуване оновлення програмного забезпечення, яке насправді є шкідливим файлом, чи використання фізичних носіїв інформації, які підкидають потенційній жертві. Флешка або диск «випадково» з'являються там, де їх легко знайти, а щоб підвищити їхні шанси бути знайденими, шахраї наносять на них логотип компанії або роблять напис, що інтригує, наприклад, «премія бухгалтерам».


Послуга за послугу (quid pro quo) – схожа на приманку, але замість того, щоб надати щось корисне, зловмисники обіцяють виконати дію, яка принесе жертві користь, але вимагає від неї дії в обмін. Наприклад, зловмисник може викликати випадкові додаткові номери в компанії, вдаючи, що телефонує за запитом служби технічної підтримки. Коли він потрапляє на людину, яка дійсно має проблему, він вдає, що надає допомогу, але інструктує жертву виконувати дії, які ставлять під загрозу її машину.

Жахлива програма (scareware) – відображає на пристрої користувача повідомлення, про зараження шкідливим програмним забезпеченням і необхідність встановлення програмного забезпечення (шкідливого програмного забезпечення зловмисника) для очищення своєї системи.



Медова пастка (honeypot) – зловмисник вдає себе дуже привабливою людиною і фальсифікує онлайн-відносини, щоб отримати конфіденційну інформацію від своєї жертви.

Задні двері (backdoor) – зловмисник входить у об'єкт, що захищається, слідуючи за людиною, яка має санкціонований доступ, і просить його «просто притримати двері» щоб він також зміг увійти.

Фази соціальної інженерії.

1. Збір інформації. Застосовуються активні та пасивні методи методології OSINT.

2. вибір жертви – людини, слабкості якої будуть корисні шахраям. Найкращими претендентами на цю роль стануть ті, кого легко обдурити, ввести в оману, люди з почуттям образи чи вираженою емпатією.

3. Технічна підготовка до фішингу. Найбільш трудомістка та витратна частина у соціальній інженерії, яка включає реєстрацію домену, хостингу, їх налаштування та обкатку

4. Контакт. Увійти до кола довіри жертви

5. На фінальному етапі злочинці використовують отриману інформацію для досягнення мети: наприклад, дізнатися пароль до системи або схему розташування камер відеоспостереження.

Найпоширеніші методи дій соціального інженера:

- представлення себе як друга-колегу чи як нового працівника з проханням про допомогу;
- представлення себе працівником фірми-постачальника, партнерської компанії, представником закону;
- представлення себе як представника керівництва;
- представлення себе постачальником або виробником IT-продукції, який пропонує оновлення або патч для встановлення;
- пропозиція допомоги у разі виникнення проблеми та подальше провокування виникнення проблеми, що змушує жертву попросити про допомогу;
- використання внутрішнього сленгу та термінології для виникнення довіри;
- відправлення вірусу або троянського коня у вкладенні до листа;
- використання фальшивого спливаючого вікна, з проханням автентифікуватись ще раз, або ввести пароль;
- пропозиція призу за реєстрацію на сайті з ім’ям користувача та паролем;

- записування клавіш, які жертва вводить на своєму комп’ютері або програмі (кейлоггінг);
- підкидання різних носіїв даних (флеш-карт, дисків тощо) з шкідливим ПЗ на стіл жертви;
- підкидання документа або папки до поштового відділу компанії для внутрішньої доставки;
- видозміна написи на факсі, щоб здавалося, що він прийшов із компанії;
- прохання секретаря прийняти, а потім надіслати факс.

### 1.4. Протидія соціальній інженерії.

1. визначити інформацію, яка є вразливою до атаки. Співробітники повинні вміти класифікувати інформацію щодо ступеня захищеності та розуміти, розкриття яких даних може завдати шкоди компанії. Наприклад, облікові дані користувача завжди належать організації, їх не можна передавати третім особам або залишати у відкритому доступі. Отже, доведеться розпрощатися зі стікерами, де написані логіни/паролі, не авторизуватись на корпоративних ресурсах через відкриті Wi-Fi-мережі. Також допомагає звичка блокувати ПК або ноутбук у свою відсутність.

2. Підвищити компетентність у питаннях інформаційної безпеки. Техніки соціальної інженерії постійно вдосконалюються, а кібершахраї знаходять нові способи зіграти на людських емоціях. Тому співробітникам компанії необхідно знати, жертвами яких потенційних атак вони можуть стати і як поводитись у подібних ситуаціях. Наприклад, куди слід написати/зателефонувати, якщо треті особи запросили конфіденційну інформацію або дані для авторизації.

3. Обмежити права доступу до інформаційних систем. Доступ на копіювання, завантаження, зміну інформації повинні мати лише ті працівники, яким це необхідно для виконання посадових обов’язків. У деяких компаніях доцільно заборонити використання знімних носіїв.

4. Підготувати інструкції щодо обміну інформацією. Всі працівники повинні мати чіткі інструкції про те, за яких умов вони можуть розкрити важливу для компанії інформацію. В інструкції доцільно зазначити, які відомості можна передавати службам техпідтримки, представникам контролюючих органів тощо.

5. Оновити антивірусне програмне забезпечення до актуальної версії. Це допоможе зробити комп'ютери співробітників менш уразливими до масових атак фішингу. Сучасне антивірусне програмне забезпечення включає інструменти для захисту від шпигунських та шкідливих програм, і попереджає при переході за підозрілими посиланнями.

6. Будьте обережні з публікаціями у соціальних мережах. Розміщення надмірної інформації у соціальних мережах може полегшити кіберзлочинцям збір інформації про вас. Щоб забезпечити максимальну конфіденційність у мережі, рекомендується:

- уникати публікацій про свої переміщення та плани майбутніх поїздок, оскільки це інформація про те, що ви будете поза домом;
- уникати розкриття надто великої кількості інформації, наприклад, дати народження та місця роботи, у розділі «Про мене» або біографії у профілі соціальних мереж. Не публікуйте домашню адресу або номер телефону на публічних форумах;
- перевірити, чи додає соціальна мережа дані про місцезнаходження до Ваших публікацій. Якщо так, вимкніть цю функцію. У більшості випадків немає необхідності демонструвати своє місцезнаходження;
- уникати кумедних вікторин, які іноді проходять у соціальних мережах. Часто в них запитують, наприклад, про Вашу хатню тварину чи про те, де ви ходили до школи. Такі питання часто використовуються як перевірочні, тому публікація відповідей на них може полегшити зловмисникам зламування ваших облікових записів в мережі.

У своїй книзі Hacking Linux Exposed Б. Хатч та Дж. Лі запропонували такі рекомендації:

- «Навчайте користувачів» – соціальна інженерія завжди запускається проти людини, а тому найкращий спосіб її запобігти – це зробити так, щоб усі Ваші співробітники були обізнані про те, що необхідно робити, якщо вони зазнають впливу тактик соціальної інженерії.
- «Будьте параноїком» – автори рекомендують «культивувати здорову параною», оскільки хакери остерігатимуться тих, хто їм не довіряє. «Вони шукають найдовірливіший об'єкт».
- «Запитуйте їх про все» – рекомендується завжди запитувати людину, з якою ви спілкуєтеся, навіщо вона запитує таку інформацію. «Більшість атак з використанням методів соціальної інженерії зазнають невдачі, якщо передбачувана жертва починає ставити хакеру питання».
- «Завжди перевіряйте, звідки вони» – якщо ми отримал електронною поштою підозрілий запит, то необхідно перевірити його, передзвонивши по телефону. Якщо ми особисто спілкуємося з людиною, яку ми не знаємо, необхідно вимагати посвідчення особи.
- «Вчіться говорити ні» – коли хакер застосовує методи соціальної інженерії, то відхиляється від норми ділового етикету, або намагається змусити щось зробити. Залишайтеся в рамках встановлених правил – це гарна форма оборони у таких випадках.

## 1.5. Спам.

Спам — це небажані повідомлення у будь-якій формі, які надсилаються у великій кількості. Найчастіше спам надсилається у вигляді комерційних електронних листів, надісланих на велику кількість адрес, а також через миттєві та текстові повідомлення (SMS), соціальні медіа.


Закон України «Про електронні комунікації» дає таке означення: **спам** – електронні, текстові та/або мультимедійні повідомлення, що без попередньої згоди (замовлення) користувачів неодноразово (більше п’яти повідомлень одному абоненту) надсилаються на їхні адреси електронної пошти або кінцеве (термінальне) обладнання, крім повідомлень постачальника електронних комунікаційних послуг щодо надання ним електронних комунікаційних послуг або повідомлень від органів державної влади чи органів місцевого самоврядування з питань, що належать до їх повноважень.

Весь шкідливий трафік, який щодня передається каналами електронної пошти, можна умовно розділити на три основні категорії:

- звичайний спам (SPAM) – нав’язлива реклама послуг, товарів чи певних сайтів; серйозної загрози не становить, просто відволікає та забирає ваш час;
- фішинг задля крадіжки облікових даних – це такі листи, які надходять вам нібито від банків, операторів послуг або інших компаній. Ці повідомлення містять посилання на сайти, що дуже схожі на справжні, але їхня основна мета – видурити у вас ваш логін і пароль від того ресурсу, під який маскується фішингова сторінка. Зазвичай у таких листах мова йде про отримання доступу до певного документа чи певної важливої для жертви інформації. Жертву наполегливо підштовхують ввести свій логін та пароль у форму на сайті. Форми на фішингових сайтах можуть імітувати сторінки входу в такі популярні сервіси, як Gmail, OWA, Outlook, iCloud тощо;
- фішинг задля інфікування вашої системи вірусом – ті ж самі несправжні, підроблені листи від імені державних органів, фінансових установ

тощо але вже із приєднаним файлом (частіше) або посиланням, під час активації якого відбувається інфікування вірусом. Шкідливий код може бути різним (залежить від мети нападника). Останнім часом розсилають в основному дві категорії: ransomware та troyan. Віруси першого типу після запуску непомітно для користувача шифрують його файли та документи, щоб потім вимагати кругленьку суму за розшифровку. Віруси другого типу призначені для прихованого стеження за діями жертви. Як правило, зразки другого типу після інфікування закріплюються в системі жертви на період від кількох годин до кількох тижнів. За цей час зловмисники отримують повну інформацію про характеристики інфікованого комп'ютера, включаючи перелік установлених програм, перехоплені чи збережені паролі та знімки екрана або ж ті документи, над якими працює жертва.


Превентивні заходи захисту від спаму.

Самий дієвий спосіб боротьби із спамом – не дозволити спамерам заволодіти Вашою електронною адресою. З цією метою доцільно скористатися наступним.

1. Не публікувати свою адресу на загальнодоступних сайтах.

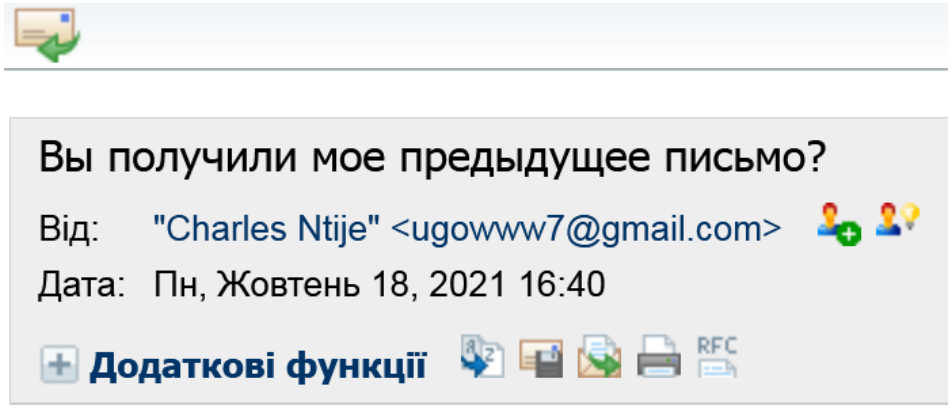
2. Якщо з якихось причин адресу електронної пошти доводиться публікувати, його можна написати, наприклад, таким чином: «u_s_e_r_(a)_d_o_m_a_i_n_._n_e_t». Спамери використовують спеціальні програми для сканування сайтів і збору поштових адрес, тому навіть таке маскування адреси може допомогти. Проте, слід пам'ятати, що в найпростіших

випадках «закодовану» адресу зможе розпізнати й програма. До того ж це створює незручності не лише для спамерів, але і для звичайних користувачів.

3. Адресу можна представити у вигляді картинки. Існують онлайн-служби, що роблять це автоматично (проте, не слід забувати, що деякі з цих служб можуть самі збирати і продавати введені користувачами поштові адреси). Крім того це можна зробити у будь-якому графічному редакторові або просто написати електронну адресу від руки і сфотографувати.

4. Завести спеціальний ящик для реєстрації в службах, що не викликають особливої довіри, і не використовувати його для звичайної роботи. Існують навіть служби, які видають одноразові адреси електронної пошти спеціально для того, щоб вказувати їх в сумнівних випадках. Найвідоміша з них – mailinator.com.

5. Не відповідати на спам або переходити по посиланнях, що містяться в ньому. Така дія підтвердить що електронна адреса активно використовується і приведе до збільшення кількості спаму.




6. Факт завантаження зображень, які включені до листа, при прочитанні, може використовуватися для перевірки активності поштової адреси. Тому рекомендується при запиті поштового клієнта про дозвіл завантаження зображення забороняти дію, якщо ви не упевнені у відправнику.

7. вибираючи адресу електронної пошти, доцільно зупинитися на довгому та незручному для вгадування імені. Так, існує близько 12 мільйонів імен, що складаються з 5 чи меншої кількості латинських букв. Навіть якщо додати цифри і символ підкреслення, кількість імен не перевищить 70 мільйонів.

Спамер зможе відправити пошту на усі такі імена та відсіяти ті, з яких йому прийшла відповідь «адресата не існує». Отже, бажано, щоб ім'я було не коротше 6 символів, а якщо в ньому немає цифр – не коротше 7 символів. Бажано також щоб ім'я не було словом у будь-якій мові, включаючи поширені власні назви, а також записані латиницею українські слова. В цьому випадку адреса може бути вгадана шляхом перебору слів і комбінацій за словником.

8. Час від часу змінювати свою адресу (але це пов'язано з очевидними незручностями).

У методиках приховування адреси є принциповий недолік: вони створюють незручності не лише потенційним спамерам, але і реальним адресатам. До того ж, часто адресу опублікувати просто необхідно – наприклад, якщо це контактна адреса фірми.

Фільтрація.

Оскільки рекламні листи, як правило, сильно відрізняються від звичайної кореспонденції, поширеним методом боротьби з ними стало відсіювання їх із потоку пошти, що входить. На сьогодні цей метод – основний та загальноприйнятий.

Існує спеціалізоване програмне забезпечення для автоматичного визначення спаму (спам-фільтри). Воно може бути призначене для кінцевих користувачів або для використання на серверах. використовують два способи автоматичної фільтрації.

Перший полягає в тому, що аналізується зміст листа і робиться висновок, чи є він спамом. Лист, класифікований як спам, відділяється від іншої кореспонденції: він може бути помічений певним чином чи переміщеним в іншу теку, видаленим. Така програма може працювати як на сервері так і на комп'ютері клієнта.

Інший спосіб полягає в тому, щоб, застосовуючи різні методи, впізнати відправника як спамера, не проводячи аналіз тексту листа. Така програма може працювати лише на сервері, який безпосередньо приймає листи.

Недоліком автоматичної фільтрації є помилкове визначення листа як спам. Тому багато поштових сервісів і програми за бажанням користувача можуть не видаляти такі повідомлення, а розміщувати їх в окремій теці.

Інші методи боротьби зі спамом.

1. Загальне посилення вимог до листів та відправників, наприклад, відмова в прийомі листів з неправильною зворотною адресою (листи з неіснуючих доменів), перевірка доменного імені відправника по IP-адресу комп'ютера. За допомогою цих заходів відсівається лише найпримітивніший спам – незначна кількість повідомлень. Але не нульове.

2. Знайомтеся з політиками конфіденційності вебсайтів. Реєструючись в Інтернет-банку чи магазині або підписуючись на інформаційні бюлетені, уважно ознайомтеся з політикою конфіденційності сайту, перш ніж вказувати свою адресу електронної пошти чи інші особисті відомості. Знайдіть посилання або розділ під назвою «Декларація про конфіденційність», «Політика конфіденційності», «Умови та положення» або «Умови використання», який зазвичай розташовано в нижній частині головної сторінки вебсайту. Якщо на вебсайті не пояснюється, як використовуватимуться ваші особисті відомості, краще відмовитися від його послуг.

3. Звертайте увагу на прапорці, що встановлені за замовчуванням. На сторінках вебсайтів іноді вже встановлено прапорець, який означає Вашу згоду на продаж або передачу вашої адреси електронної пошти іншим компаніям (третім особам). Зніміть цей прапорець, щоб Вашу адресу електронної пошти не розголошували.

## 1.6. Конфіденційність і безпека в соціальних мережах.

Можна виділити наступні типи основних загроз інформації в соціальній мережі:

- загроза конфіденційності (витік конфіденційної інформації та заподіяння прямого або непрямого збитку користувачеві соціальної мережі);

- загроза цілісності (модифікація інформації усередині мережі інформації і втрата її адекватності);
- загроза доступності (порушення доступу до мережевої інформації і блокування доступу до ресурсу);
- загроза повноті (знищення інформації усередині мережі та заподіяння прямого або непрямого збитку як користувачеві соціальної мережі, так і її власнику);
- загроза актуальності (затримка отримання легальним користувачем мережі інформації);
- загроза важливості (несанкціоноване читання конфіденційної мережевої інформації, що призводить до втрати її ціннісних характеристик);
- загроза адресності (переадресація мережевої інформації, що може призводити до зниження її конфіденційності та доступності);
- загроза надмірності інформації (багаторазове дублювання мережевої інформації).