МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний вищий навчальний заклад
«Донбаський державний педагогічний університет»

ОСНОВИ КІБЕРБЕЗПЕКИ

Рекомендовано вченою радою
Державного вищого навчального закладу
«Донбаський державний педагогічний університет»
як навчальний посібник

Дніпро – 2023

УДК 004.056.5 (075.8)

С 36

Сілін Є.С., Кадубовський О.А. Основи кібербезпеки : навчальний посібник [електронний ресурс]. Дніпро, 2023. – 200 с.

Адресовано здобувачам другого (магістерського) рівня вищої освіти, які вивчають навчальну дисципліну «Сучасні інформаційні технології». Буде корисним широкому колу користувачів, які використовують інформаційні технології. Основними завданнями навчального посібника є: надання студентам базових теоретичних знань у галузі кібернетичної безпеки та розуміння основних принципів забезпечення кібербезпеки; набуття студентами практичних навичок застосування сучасних технологій забезпечення кібербезпеки.

РЕКОМЕНДОВАНО
вченою радою Державного вищого навчального закладу
«Донбаський державний педагогічний університет»,
протокол №9 від 29.06.2023 р.

Рецензенти:

кандидат фізико-математичних наук **С.В. ВОЛКОВ**,
Донецький національний технічний університет,
доцент кафедри вищої математики і фізики;

кандидат фізико-математичних наук **Т.В. ТУРКА**,
ДВНЗ «Донбаський державний педагогічний університет»,
доцент кафедри методики навчання математики та методики навчання інформатики.

Відповідальний за випуск:

кандидат фізико-математичних наук, доцент кафедри математики та інформатики Є.С. Сілін

Зміст

ПЕРЕДМОВА

Кафедра математики та інформатики Державного вищого навчального закладу «Донбаський державний педагогічний університет» забезпечує викладання обов'язкової навчальної дисципліни «Сучасні інформаційні технології» для здобувачів другого (магістерського) рівня вищої освіти різних спеціальностей. Розвиток інформаційних технологій неминуче супроводжується збільшенням кількості різноманітних загроз. Тому, однією з обов'язкових тем зазначеного курсу є елементи кібербезпеки. Майбутній фахівець повинен знати, розуміти, виявляти, аналізувати та нейтралізувати, принаймні, основні види кіберзагроз. Навчальний посібник «Основи кібербезпеки» сприятиме розвитку наступних компетенцій:

знання та розуміння основних принципів кібергігієни й захисту від загроз соціальної інженерії; особливостей створення стійкого пароля; джерел і симптомів шкідливого та потенційно небезпечного програмного забезпечення;

забезпечення надійної роботи з даними (створення та зберігання резервних копій файлів, видалення або відновлення втрачених даних, захист інформації за допомогою шифрування й маскування);

побудова стратегії попередження методів соціальної інженерії; оцінка ефективності обраних підходів до безпечної та анонімної роботи в Мережі.

1. ОСНОВНІ ПРИНЦИПИ КІБЕРБЕЗПЕКИ. СОЦІАЛЬНА ІНЖЕНЕРІЯ

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:

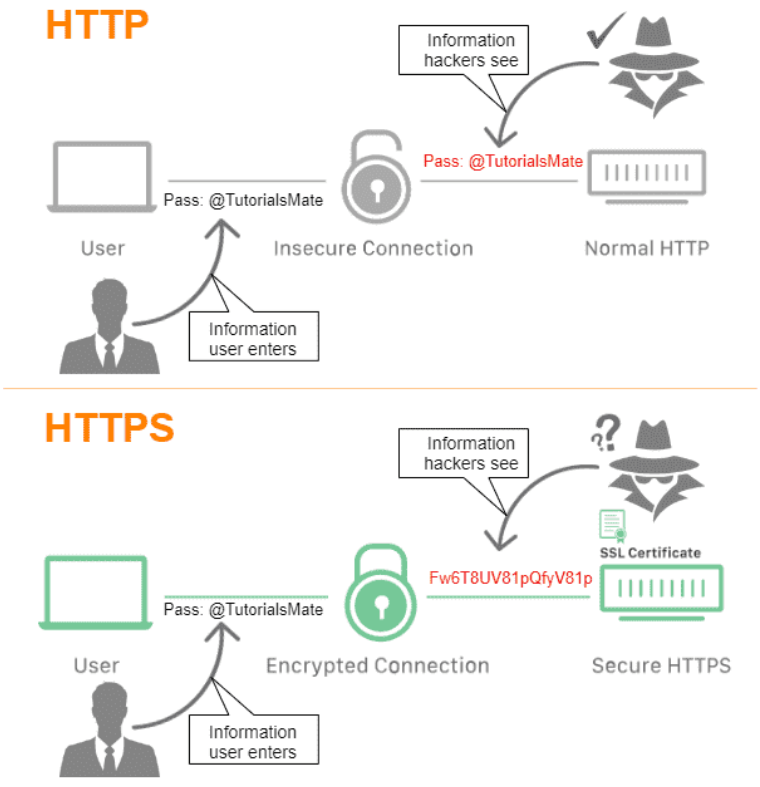
- не публікуйте в соціальних мережах особисту інформацію, таку як домашню адресу, особисті фотографії, номер телефону, номери кредитних карток;
- оцініть налаштування конфіденційності у соціальних мережах та переконайтеся, що вони встановлені на належному рівні;
- уникайте вікторин, ігор та опитувань 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.

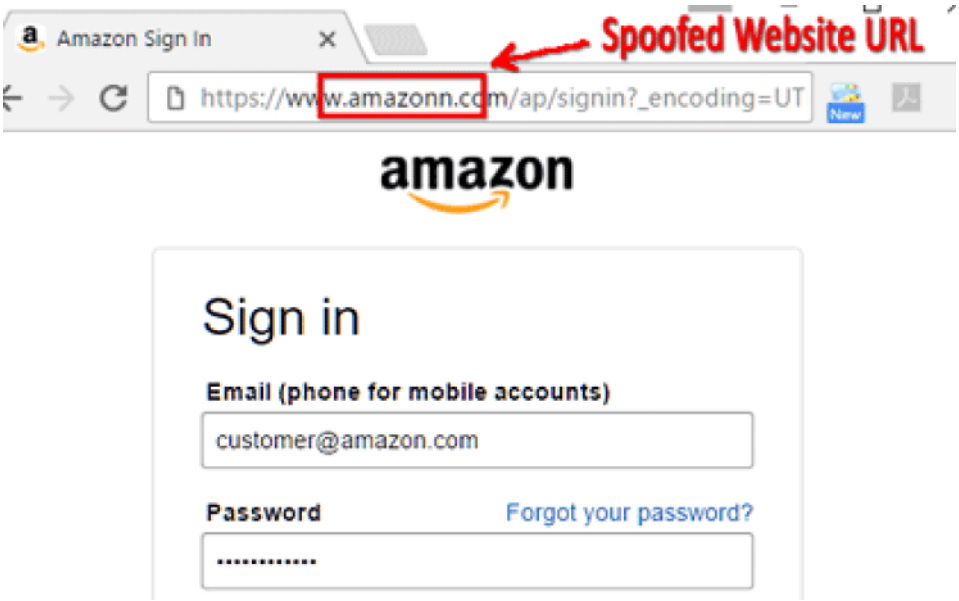
Китобійна атака складніша, ніж звичайна фішингова атака. Зловмисники проводять ретельне дослідження, щоб створити повідомлення, яке змусить конкретні цілі відповісти та виконати бажану дію. Китобійні листи часто

«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

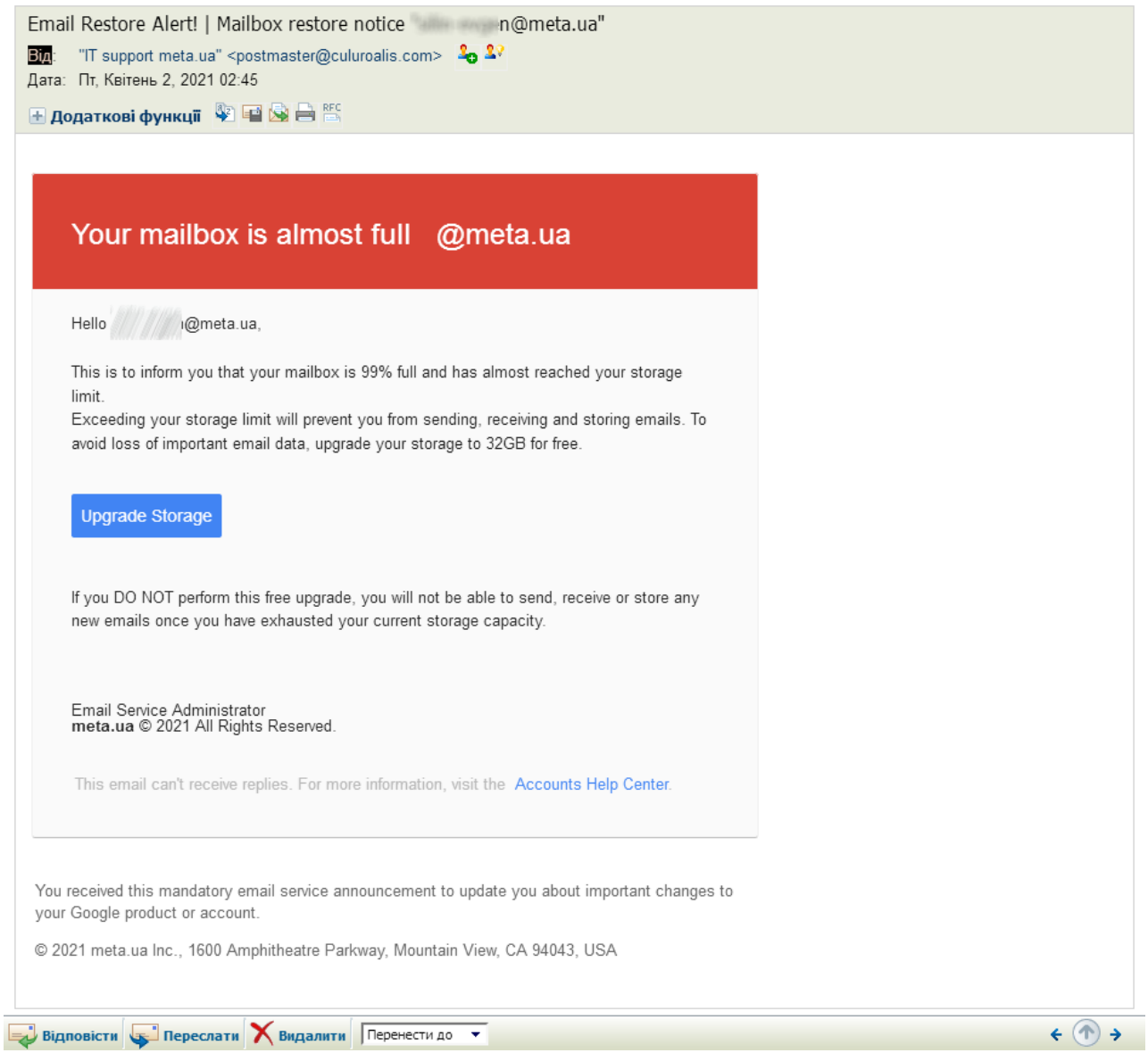
Thank you for choosing Zoom.
-The Zoom Team

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.

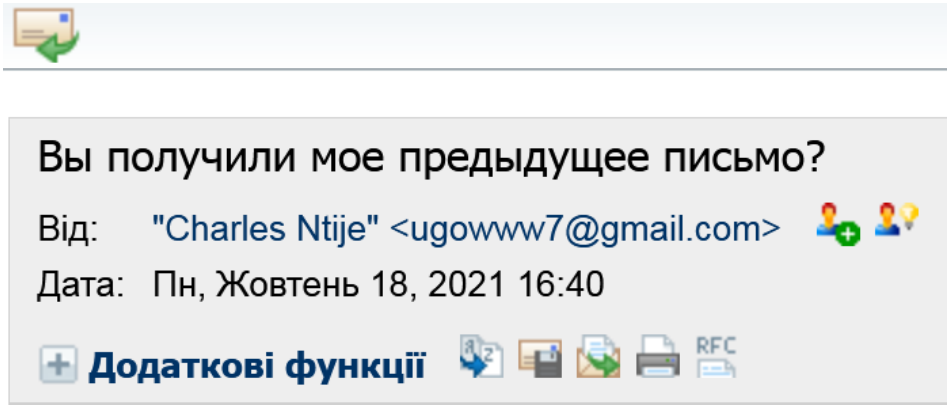
2. Якщо з якихось причин адресу електронної пошти доводиться публікувати, його можна написати, наприклад, таким чином: «u_s_e_r_(a)_d_o_m_a_i_n_._n_e_t». Спамери використовують спеціальні програми для сканування сайтів і збору поштових адрес, тому навіть таке маскування адреси може допомогти. Проте,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

ЛАБОРАТОРНА РОБОТА №1. РОЗПІЗНАВАННЯ ФІШІНГУ.

Мета вивчення: отримати теоретичні знання та практичні навички розпізнавання фішингу.

Обсяг навчального часу: 1 година.

Обладнання: комп'ютер (планшет, смартфон), наявність підключення до мережі Інтернет.

План заняття:

1. Отримати теоретичні знання аналізу повідомлень щодо фішингового вмісту.
2. Пройти тест від Jigsaw щодо вміння розпізнавати фішингові повідомлення.

Інформаційні джерела:

тест на вміння розпізнавати фішингові листи:

- https://phishingquiz.withgoogle.com/?hl=uk,

перевірка документів та URL на шкідливий вміст:

- https://virustotal.com/;
- https://iris-h.malwageddon.com/submit;
- https://cape.contextis.com/submit/;
- https://urlscan.io/.

ЗАВДАННЯ:

1. Ознайомитися з методикою розпізнавання фішингу, перевірити отриманні знання за допомогою тесту від Jigsaw – підрозділу Google (https://phishingquiz.withgoogle.com/?hl=uk). Зробити скріншот із результатами Вашого тестування та додати до звіту.

2. Перевірити за допомогою відповідних ресурсів принаймні один файл та одне посилання з вашої електронної пошти.

ВИМОГИ ДО ЗВІТУ:

1. Скрін екрану з результатами проходження тесту від Jigsaw.

ХІД РОБОТИ.

1. Фішингові листи – це різновид соціальної інженерії, спосіб прихованої маніпуляції діями обраної людини. Щоб примусити жертву відреагувати на фішинговий лист, а не видалити його одразу, зловмисники підбирають відповідного адресанта – лист може прийти начебто від державної фіскальної служби або від організації-підрядника, із яким співпрацює компанія жертви. Текст фішингового листа, як правило, пропонує ознайомитися з документами, частіше – пов'язаними з фінансовими операціями.

Під час створення листа зловмисники можуть використовувати інформацію, яку вони знаходять у відкритих джерелах (Google, Facebook тощо). Припустимо, жертва на своїй сторінці в соціальній мережі показує всім, що вона дуже захоплюється авіамоделюванням або є палким фанатом певного музичного гурту – в такому разі їй можуть надіслати листа із пропозицією переглянути свіжий каталог моделей чи придбати квитки на найближчий концерт із суттєвою знижкою, або завантажити рідкісний концертний запис. Ймовірність того, що, зацікавлена такою приманкою, жертва перейде за посиланням або відкриє документ, значно вища, ніж у випадку типових масових сповіщень, наприклад, від банків.

Правила захисту від фішингу в електронних листах.

1) Не довіряти нікому, або правило 30 секунд. Не поспішайте відкривати приєднані файли чи переходити за посиланням, зупиніться і дайте собі 30 секунд на коротку перевірку нового листа.

Зазвичай, безпосередньо під час розсилки і кілька годин потому більшість звичайних антивірусів не розрізняють загрозу, яку вам надіслали під виглядом документів. Але навіть цільовий, персональний фітинг, досить часто легко відрізнити за деталями, яких, на жаль, часто не помічають.

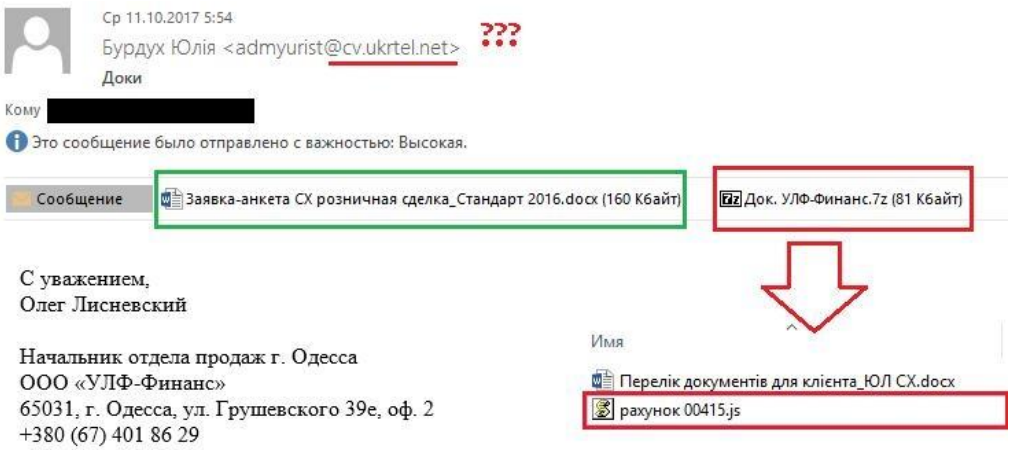
Надайте собі відповіді на такі запитання:

- Від кого надійшов лист? Яка його тема?
- Кому надіслано листа? Вам чи відділу, де ви працюєте?
- Чи є вкладення?

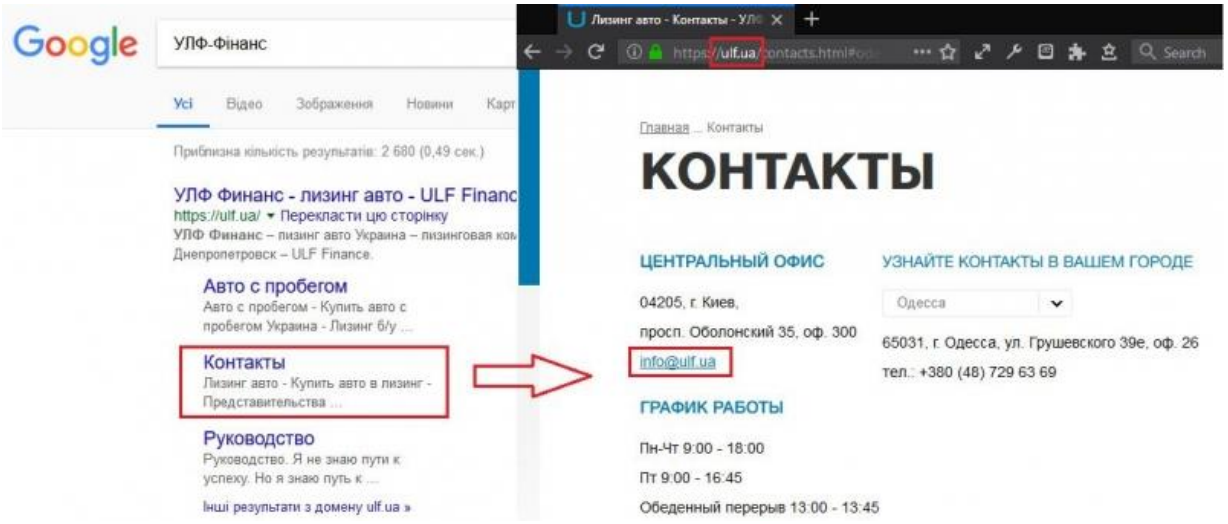
- Текст листа – чи збігається він із темою листа?
- Про що вас намагаються попросити? Чи маєте ви право це робити?
- Чи є в кінці листа підпис тієї особи, яка начебто писала його вам?
- Чи співпадає поштова скринька, з якої ви отримали цього листа, з доменним ім'ям тієї організації, що вказана в підписі?
- Чи співпадає зазначена в підписі листа організація з тою, що вказана в темі листа або ж у його тексті?
- Чи помічаєте ви грубі граматичні та/або орфографічні помилки в тексті листа?
- Чи містить текст листа будь-які посилання?

Мета цього поверхневого огляду – пересвідчитися, що лист адресовано дійсно вам, що він стосується саме вас. Правило просте: повідомлення, яке прямо вас не стосується та не пов'язане з вашою роботою, яким би спокусливим або ж, навпаки, яким би незрозумілим воно не здавалося, помітити як небажане та видалити.

Навіть якщо ви держслужбовець і ваша робота полягає в розгляді звернень громадян – так, ви, дійсно, маєте реагувати на кожного листа, але навіть тоді, ви не мусите відкривати приєднання чи посилання листа, який надійшов вам іншою мовою. Якщо щось не збігається – приміром, підпис із скринькою, від якої надійшов лист, або ім'я в заголовку листа не співпадає із тим, що вказане в підписі, чи текст листа містить грубі помилки і так далі – не відкривайте приєднання, не переходьте за посиланням



Відправник Юлія, скринька належить до cv.ukrtel.net. Тема «Доки» – викликає невелику підозру. Лист містить два приєднання – документ і архів. Можливо, так і має бути (насправді так роблять, аби обманути фільтри пошти, сам документ – порожній, там лише текст, а ось архів містить приманку, що завантажує вірус). Підпис – Олег замість Юлії, в офіційному діловому спілкуванні таке зустрічається дуже рідко. Назва компанії – «УЛФ-Фінанс» у місті Одеса дозволить пошукати контакти цієї компанії в Google:

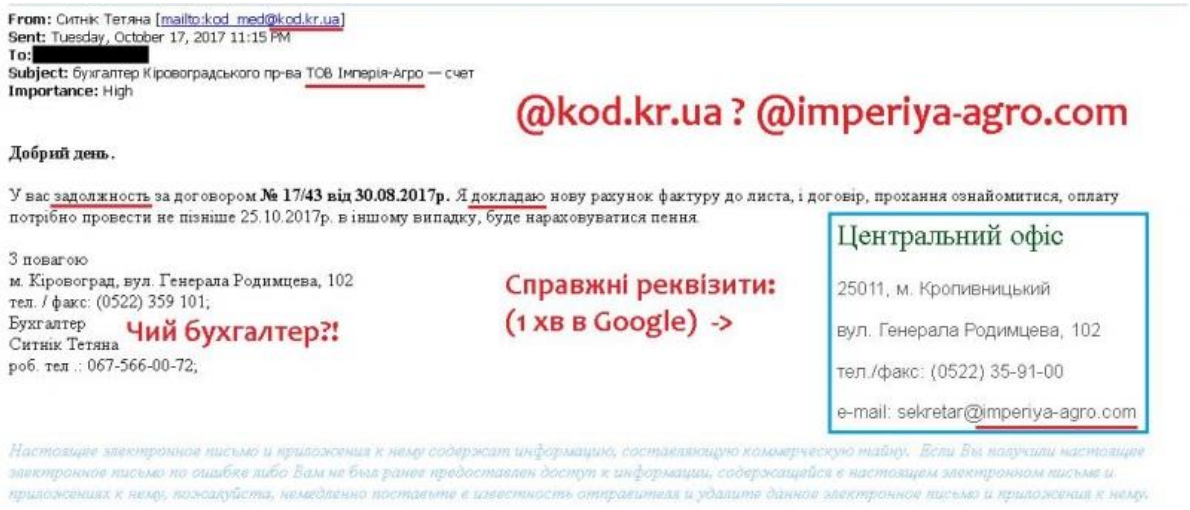


Адреса в підписі та на офіційному сайті співпадають, а домен – ні. Але ж у більшості сучасних компаній адреси їхніх електронних скриньок матимуть таку ж саму назву, як і офіційний сайт. Наприклад, офіційний сайт організації – ulf.ua, отже, листи від них можуть надходити лише з адрес на кшталт user@ulf.ua. А в цьому випадку ми маємо зразок фейкового (несправжнього) листа, це фішинг:

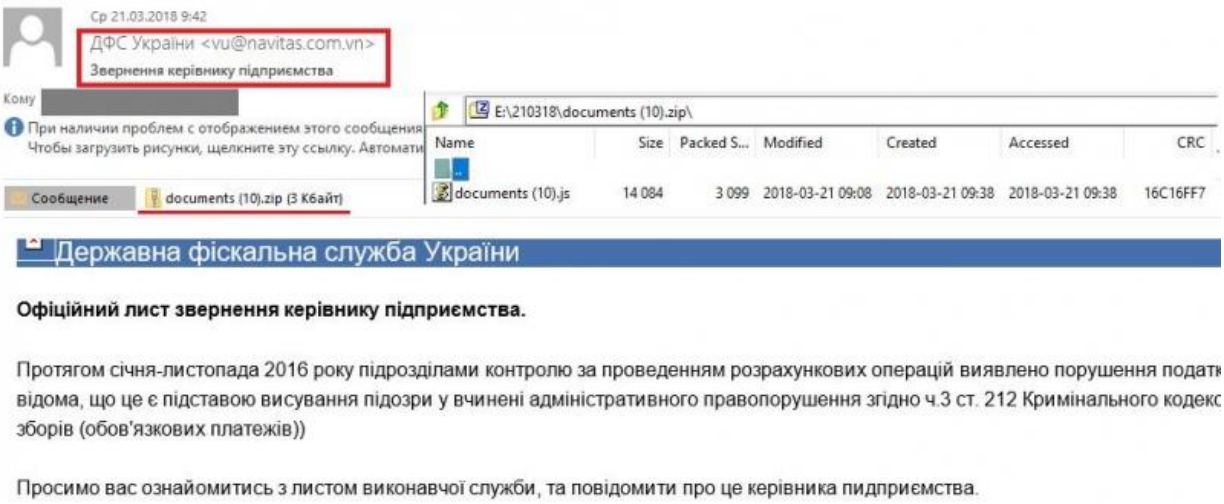
- адреса скриньки, від якої надійшов лист, не співпадає з офіційними контактами організації;
- неформальний текст у темі, жаргонізми;
- чужий підпис, його туди просто вставили.

ви можете пересвідчитися, що вам надсилали документи саме з тієї організації, яка вказана в підписі, але в жодному разі не користуйтеся контактами в підписі. Якщо лист писали зловмисники, їм ніхто не заважав указати там свої номери, а отже, щойно ви зателефонуєте до них, вони одразу вас запевнять, що цей підозрілий документ надіслано саме вам. Тому треба

звернутися за телефонами, які вказані на офіційному сайті, й перепитати, чому Олег зі скриньки Юлії надіслав якісь незрозумілі документи.

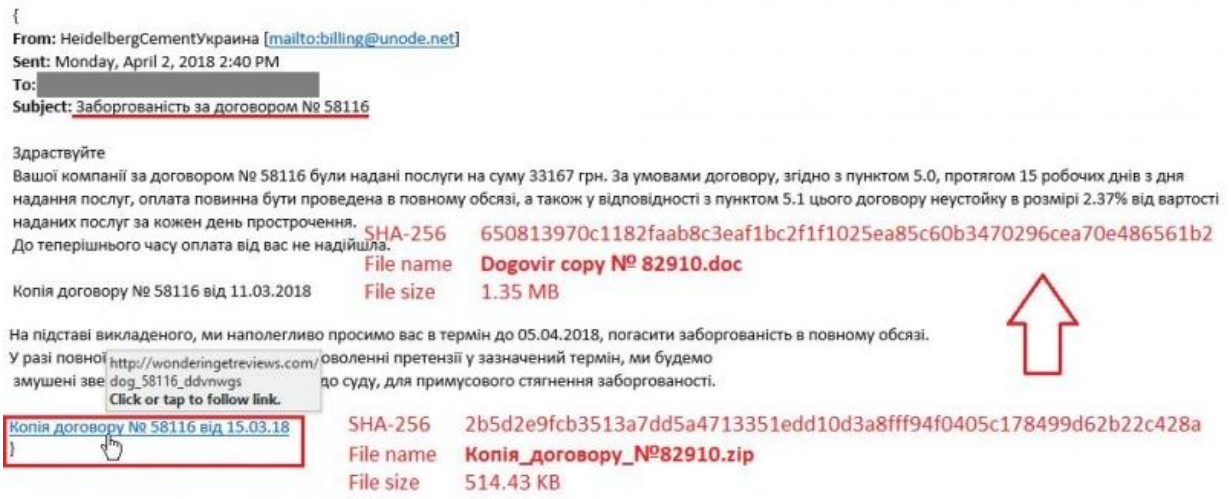


Перша і головна ознака фішингу – скринька, від якої надійшов лист, не має абсолютно нічого спільного з доменом, який зареєстрований на компанію, що фігурує в темі листа. Далі, в підписі відсутня інформація про компанію. Вказали лише посаду і телефон людини. Хто вона? До якої організації належить? Дуже велика кількість помилок.



Скринька не співпадає з офіційними контактами ДФС. Відсутній формалізований підпис. Це фейк. Зловмисники дуже полюбляють надсилати фішинг від імені всіляких державних установ або контрольних органів. Основна їхня мета – залякати жертву і примусити її відкрити приєднання.

Фішингові листи часто містять посилання на фейкові сторінки чи ресурси.



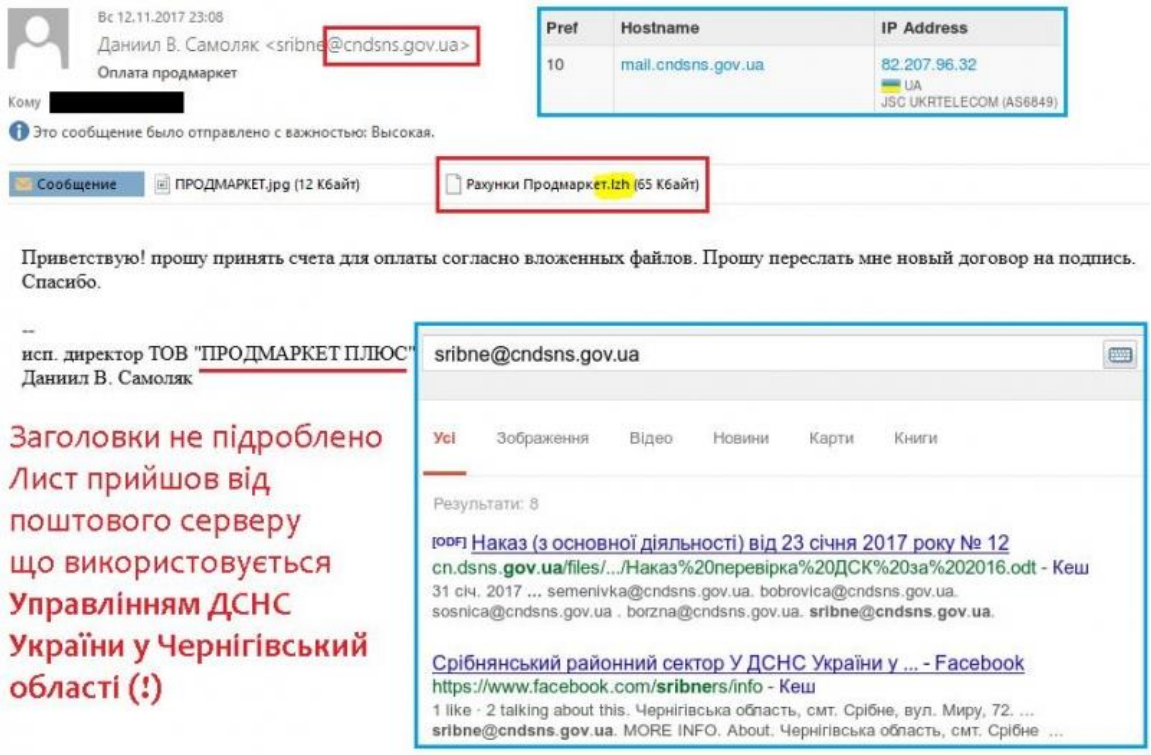
«Здраствуйте» на початку і ламана українська в тексті. Скринька не співпадає з офіційними контактами вказаної організації. Але зверніть увагу на посилання – це улюблений прийом.

Справа в тому, що в листі можна взяти будь-який текст і вставити в нього посилання на певне джерело в Інтернеті. Зловмисники беруть текст правильного джерела, припустимо rada.gov.ua, але ставлять на нього посилання на якийсь сервер, що розповсюджує віруси. Люди, як правило, не читають текст справжнього посилання, вони бачать лише те, що лежить на поверхні.

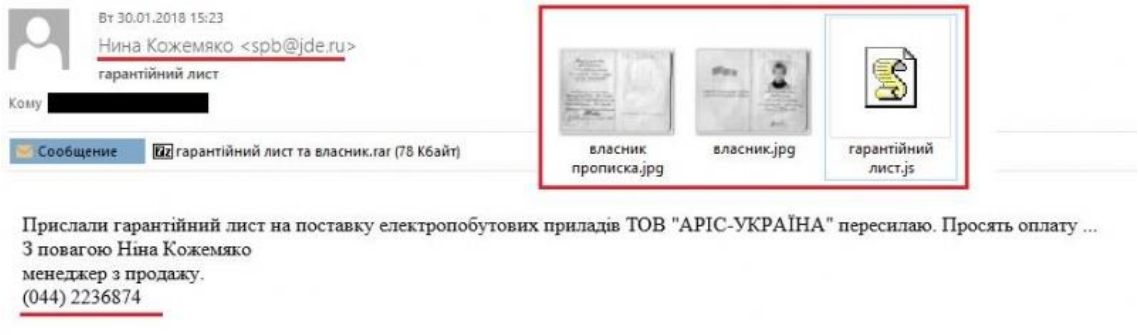
Щоб захиститися від таких трюків, варто просто не клікати одразу на посилання, а навести на нього курсор (як на знімку екрана вище). Або можна також через контексте меню скопіювати посилання та вставити його у блокнот, щоб порівняти зі справжнім сайтом організації, на який вас відправляють.

Також відомі випадки, коли офіційна скринька (або ж навіть цілий поштовий сервер) реальної організації були скомпрометовані, і вам може надійти лист, який пройде всі фільтри.

Лист дійсно надійшов від ДСНС. Нападники досить примітивно скористалися доступом до одного з регіональних серверів ДСНС– вони від скриньки служби розсилають фішинг із підписом «продмаркет плюс».



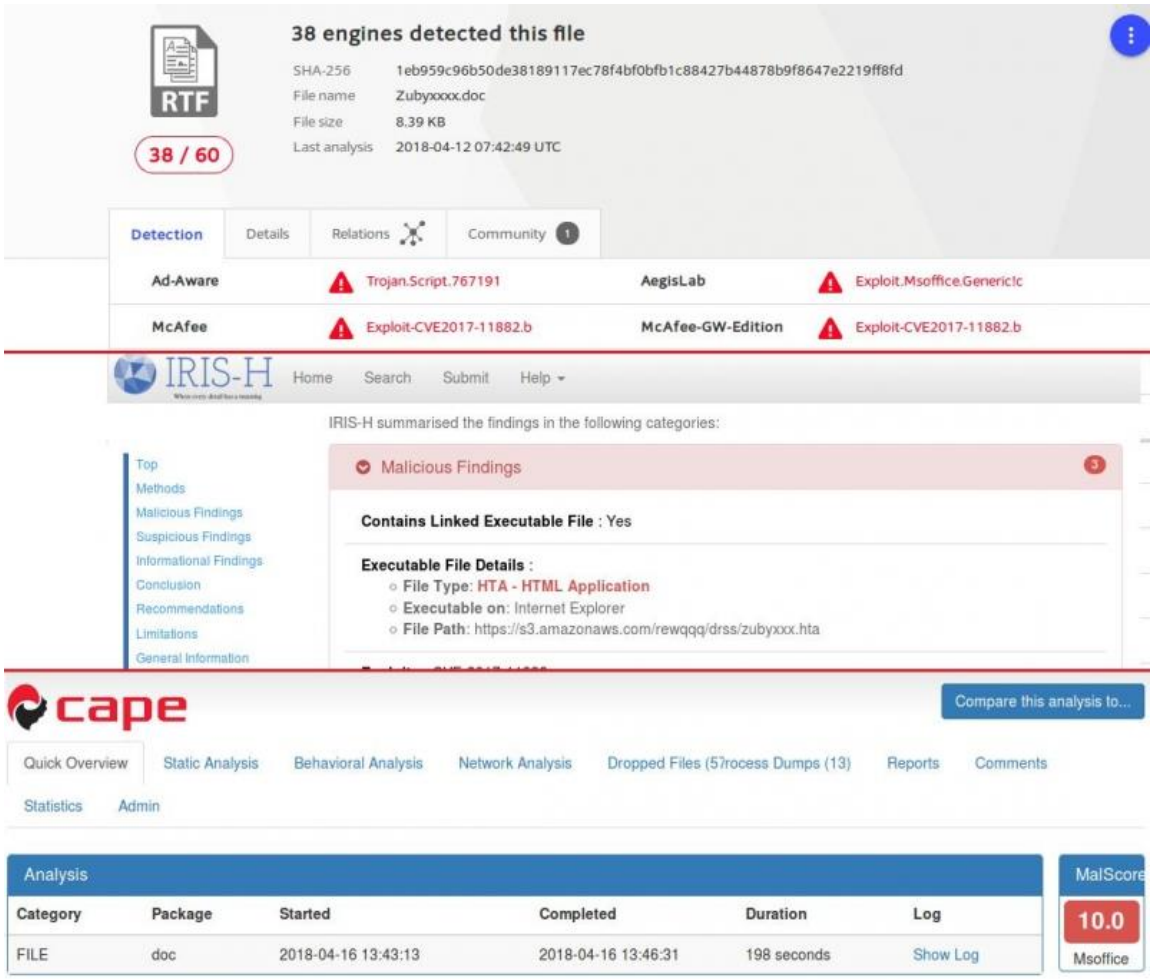
2) Перевіряти посилання та файли, перш ніж відкрити.



Червоним обведено зміст архіву. Третій файл — скрипт-приманка. Перш ніж відкривати документ або переходити за посиланням, ви можете безкоштовно та швидко перевірити їх на публічних сервісах:

- https://virustotal.com/ – перевірка файлів різних типів багатьма антивірусами (за контрольними сумами);
- https://iris-h.malwageddon.com/submit – перевірка документів MS Office;
- https://cape.contextis.com/submit/ – статичний та динамічний аналіз файлів;
- https://urlscan.io/ – перевірка URL на шкідливий вміст.

Зазначені ресурси є публічними та безкоштовними. Основна мета – переконатися, що зміст листа безпечний, до того, як запускати його на вашому комп'ютері.



Куди звернутися по допомогу:

Повідомити про кіберзлочини, кібершахрайство тощо: кіберполіція callcenter@cyberpolice.gov.ua;

Повідомити про кібератаки, кіберінциденти, у тому числі фішингові розсилання на органи влади, бізнес, громадян: урядова команда реагування на комп'ютерні надзвичайні події e-mail: incidents@cert.gov.ua, форма повідомлення на сайті: https://cert.gov.ua/contact-us, через сторінку у Facebook: https://www.facebook.com/UACERT;

Повідомити про кібератаки, кіберінциденти, у тому числі фішингові розсилання на державні органи влади: оперативний центр реагування на кіберінциденти e-mail: soc@scpc.gov.ua, тел.: (044) 281-87-37;

Оперативно-технічна служба Державного центру кіберзахисту: (044) 281-88-01.

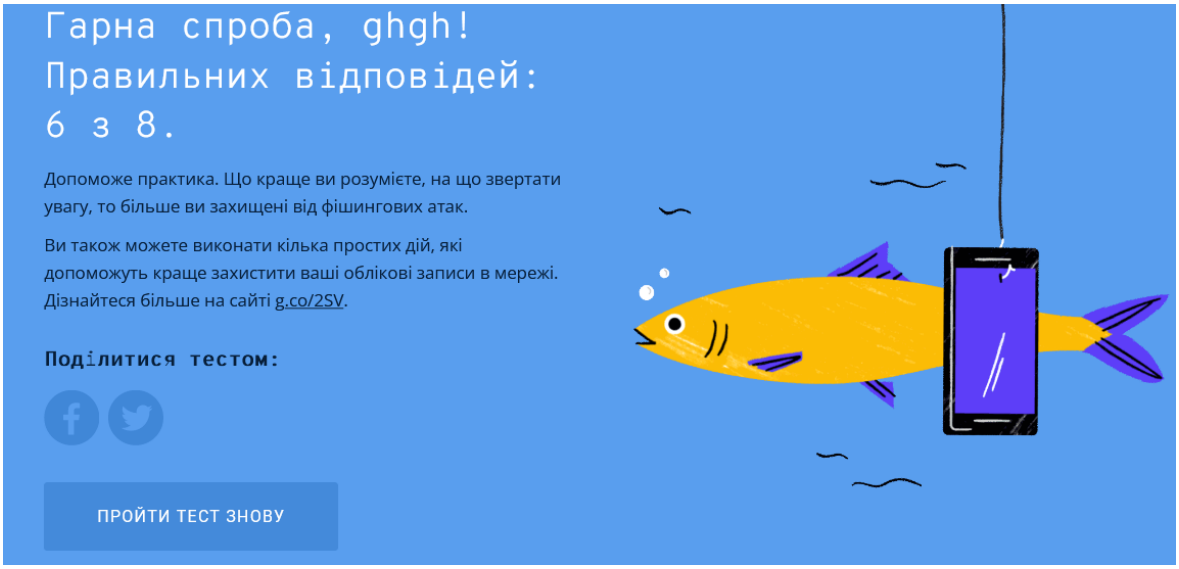
Повідомити про ресурси в інтернеті, які розповсюджують дезінформацію: департамент кіберполіції Національної поліції України: https://t.me/stopdrugsbot.

Повідомити про загрозу нацбезпеці України в інтернеті, зокрема спроби та факти кіберрозвідки інших держав, кібертероризму та кібершпигунства – ситуаційний центр забезпечення кібербезпеки СБУ:

incident@dis.gov.ua – про виявлені кіберінциденти на об'єктах критичної інфраструктури та в органах державної влади;

cvd@dis.gov.ua – про виявлені вразливості в інформаційно-телекомунікаційних системах на об'єктах критичної інфраструктури та в органах державної влади.

Результат тестування в Jigsaw:



2. КЕРУВАННЯ ПАРОЛЯМИ

2.1. Аутентифікація користувача.

2.2. Створюємо надійний пароль.

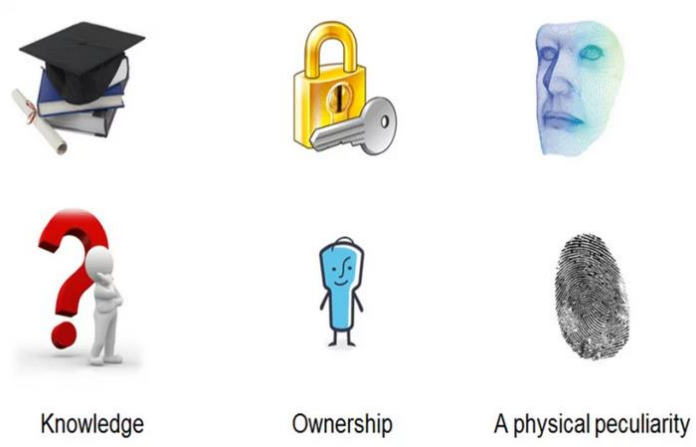
2.3. Менеджери паролів.

2.1. Аутентифікація користувачів.

Аутентифікація користувача – процедура встановлення за допомогою спеціальних програмних засобів достовірності користувача. Аутентифікація користувача включає дві процедури – ідентифікацію та верифікацію.

Підсистема аутентифікації користувачів – найважливіший компонент системи інформаційної безпеки. Ця підсистема підтверджує особу користувача інформаційної системи і тому повинна бути надійною та адекватною, тобто, виключати всі помилки в наданні доступу.

Наявні методи аутентифікації різні за ступенем надійності, та, як правило, з посиленням захисту різко зростає ціна систем, що вимагає при виборі засобів аутентифікації аналізу ризиків та оцінки економічної доцільності застосування певних заходів захисту.



Засоби аутентифікації можна розділити на три групи у відповідності з існуючими принципами:

- принцип «що ви знаєте» («you know»), що лежить в основі методів аутентифікації за паролем;

- принцип «що ви маєте» («you have»), коли аутентифікація здійснюється за допомогою магнітних карт, токенів та інших пристроїв;
- принцип «хто ви є» («you are»), що використовує персональні властивості користувача (відбиток пальця, структуру сітківки ока тощо).

Системи строгої аутентифікації використовують два чи більше факторів при аутентифікації користувачів.

На цей час аутентифікації першої групи («you know») є найбільш економічними за вартістю, але одночасно й найменш надійними. Пароль користувача можна підглянути, перехопити в каналі зв'язку, чи просто підібрати. Якщо політика безпеки вимагає застосування складних паролів, користувачам важко їх запам'ятовувати, і нерідко на самому видному місці з'являються паперові листочки із записами паролів.

Наслідки особливо небезпечні в системах, де використовується принцип «єдиного входу», коли співробітник застосовує один пароль для аутентифікації та роботи з багатьма корпоративними додатками й джерелами інформації. Часто, не усвідомлюючи важливості аутентифікації, працівники практикують передачу особистого пароля колегам.

Системи строгої аутентифікації, побудовані на факторі «you know» і «you have», надають більше можливостей для посилення захисту. Наприклад, роботу токенів, які генерують одноразові паролі, дуже складно підробити, а сам пароль не може бути повторно використаний.

Прикладами можуть служити пристрої RSA SecureID і Vasco Digipass. Найбільш актуальне застосування цих пристроїв в таких областях, як електронна комерція, включаючи Інтернет-банкінг, або для організації захисту ключових з точки зору безпеки користувачів (адміністраторів інформаційної системи та керівників).

Наприклад, подвійна аутентифікація користувача пластикової банківської картки є ефективним засобом підвищення безпеки платежів, здійснюваних з використанням мобільних пристроїв. Для підвищення безпеки Інтернет–платежів компанією Visa застосовується технологія двофакторної

аутентифікації платежів із використанням пластикових карт 3D-Secure. Користувачам карток цієї платіжної системи надається послуга Verified by Visa. Крім логіна і пароля користувачеві пропонується запит на підтвердження володіння пластиковою карткою. Це може бути одноразовий код, який надсилається банком у SMS-повідомленні на мобільний пристрій користувача. У цьому випадку необхідна інтеграція банку з оператором мобільного зв'язку.

При всьому різноманітті існуючих механізмів аутентифікації, найбільш поширеним із них залишається парольний захист. Для цього є декілька причин:

- відносна простота реалізації – механізми парольного захисту зазвичай не вимагає залучення додаткових апаратних засобів;
- традиційність – механізми парольного захисту є звичними для більшості користувачів автоматизованих систем і не викликають психологічного несприйняття – на відмінну, наприклад, від сканерів малюнка сітківки ока.

Блокування мобільних пристроїв.

1) Свайп – абсолютно ненадійний. Це просто захист екрана від випадкового натискання, що оберігає від незапланованих дій. Цей спосіб може вважатися більш-менш прийнятним, лише коли пристрій дійсно не містить будь-якої особистої інформації та повинен бути завжди доступний відразу для декількох осіб.

2) Графічний ключ – слабкий чи середній рівень безпеки. Для недорогих пристроїв на базі Android графічний ключ став популярним методом блокування екрану. Проте слід пам'ятати, що графічний ключ досить легко підглянути через плече. А у разі не надто чистого екрану його іноді можна побачити за слідами пальця.

3) PIN-код – середній або високий рівень безпеки. Ступінь захисту безпосередньо залежить від довжини та складності коду. Наприклад, PIN-код у вигляді 0000 вгадати зовсім не складно. Безпека визначається тим, наскільки швидко та непомітно для сторонніх осіб користувач вводить код.

4) Пароль – високий рівень безпеки. Пароль вважається вже серйозною мірою захисту смарт-пристрою, і при достатній складності підібрати його по-справжньому важко. Як недоліки можна відзначити, що складний пароль незручно вводити, а оскільки більшість користувачів розблокує екрани своїх пристроїв часто, метод ускладнює роботу з гаджетами.

5) Відбиток пальця – високий рівень безпеки. Сканер відбитків пальців став дуже популярним і широко використовується. На останніх моделях він спрацьовує швидко та зручно. До мінусів цього способу відноситься неможливість скористатися сканером відбитків у деяких ситуаціях. Наприклад, якщо руки мокрі або спітнілі. Зчитувач не спрацює і тоді, коли палець забруднений чи травмований. Іноді досить того, що рука огрубіла від холоду.

6) Розпізнавання обличчя – безпека цього способу залишається спірною. виробники стверджують, що цей метод вкрай надійний, але користувачі відзначають, що іноді технологія дає збій і розблокує екран побачивши фотографії користувача або когось із його родичів. Ще один недолік – періодичні збої при розблокуванні в темряві.

7) Сканер райдужної оболонки ока – високий рівень безпеки. По суті, райдужка ока схожа на відбитки пальців – вона унікальна для кожної людини і тому не піддається імітації. І, на відміну від відбитка пальця, ця технологія не потребує фізичного контакту. Однак хотілося б відзначити, що хоч дана функція вже працює на сучасних пристроях, відбувається це поки що досить повільно і вимагає певних зусиль. Зокрема, для розблокування телефон потрібно досить близько піднести до очей, і навіть у цьому випадку можливі збої. Проблеми виникають і при поганому освітленні, носінні окулярів або лінз. Крім того, деякі користувачі цієї технології скаржаться, що від сканування у них болять очі.

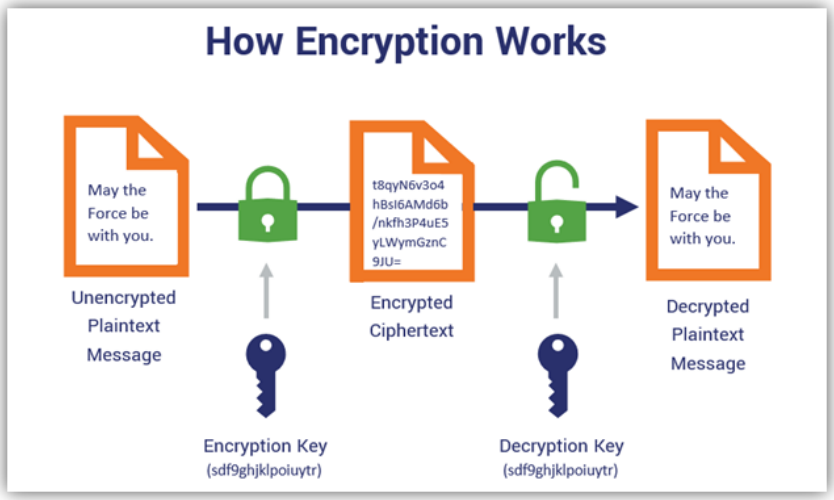
8) Smart Lock – середній рівень безпеки. Android у своїх пристроях пропонує, окрім традиційних способів розблокування екрану, ще й додаткові варіанти, що підвищують комфорт та швидкість користування телефоном. Це означає, що у певних ситуаціях автоматичне блокування екрана вимикається,

якщо телефон вирішує, що загрози безпеці немає. Наприклад, розпізнавання руху означає, що в ситуації, коли телефон розпізнає рух вашого тіла, він буде готовий до роботи після першого розблокування. Ця функція активна, поки телефон залишається в русі або, можливо, в руці власника. Крім того, для пристроїв на базі Android можна встановити безпечні місця, тобто місця зі спрощеним доступом до пристрою. Крім цього, у рамках функції Smart Lock можна призначити розпізнавання довірених додаткових пристроїв. Це означає, що телефон можна відкривати без зайвих паролів, поки поблизу нього знаходиться додатковий пристрій (наприклад, смарт-годинник).

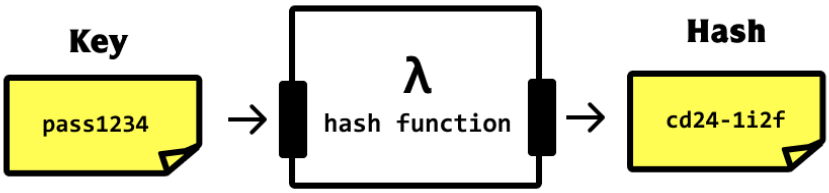
2.2. Створюємо надійний пароль.

Комп'ютерні системи, які використовують паролі для автентифікації, повинні певним чином визначати правильність введеного пароля. Найпростішим способом вирішення даної проблеми є зберігання списку всіх допустимих паролів для кожного користувача. Недоліком такого методу є те, що в разі несанкціонованого доступу до списку, зловмисник дізнається всі паролі. Більш поширений підхід полягає у зберіганні значень криптографічної хеш-функції від парольної фрази.

У межах кібербезпеки поняття «пароль» не треба плутати з поняттям «ключ». Із криптографічної точки зору це зовсім різні поняття. Пароль – це таємне слово або певна послідовність символів, призначена для підтвердження особи або її прав. Але комп'ютерні програми не використовують паролі безпосередньо для шифрування, вони з паролів отримують ключі. Ключі шифрування – це рядки бітів (0 або 1) різної довжини, найбільш часто використовуються 40, 64 і 128-бітові ключі.



Ключі з паролів отримують за допомогою спеціальної операції – хешування. Хешування – це досить складна криптографічна функція, яка отримує на вході рядок будь-якої довжини, і генерує на виході рядок бітів фіксованої довжини (хеш). Хешування володіє двома основними властивостями: навіть незначні зміни вхідного рядку призводять до повної зміни вихідного хеш-значення; по відомому хеш-значенню практично неможливо підібрати вихідний рядок.



Злочинець може отримати пароль із використанням методів соціальної інженерії чи за допомогою технічних (програмних) засобів. Для злому паролів в більшості випадків використовується перебір. Програмне забезпечення генерує різні варіанти паролів й повідомляє якщо був знайдений правильний. У деяких випадках персональний комп'ютер здатний видавати мільйони варіантів на секунду.

Час, необхідний для злому пароля є пропорційним довжині та складності цього пароля. Також швидкість перебору залежить від криптографічного функції, яка застосовується для генерації хешей пароля.

Для стійких криптоалгоритмів (коли атакуючий може лише генерувати і перевіряти паролі) існують 2 основних методи злому паролю: атака перебором і

за словником. Атака перебором використовується тоді, коли відсутня додаткова інформація щодо паролю й зловмисник пробує всі можливі паролі. Якщо зловмисник знає, що пароль – це певне реальне слово, він може використовувати атаку за словником. Тоді в якості можливих паролів перевіряються тільки слова із словника. В словнику міститься менше 100 000 слів, тому їх можна перевірити дуже швидко – в більшості випадків це займає лише декілька секунд.

Поєднання двох описаних вище атак називається «атака по складах». Вона використовується в тому випадку, якщо пароль спотворений або являє собою неіснуюче слово. Тоді зломщик може об'єднувати склади, щоб підібрати потрібне слово.

Найпотужніша – «атака на основі правил». Вона може бути використана у тих випадках, коли атакуючий володіє деякою інформацією про пароль, який він хоче зламати. Наприклад, йому відомо, що пароль складається зі слова і одно- або двозначного числа. Він пише правило, і програма генерує тільки відповідні паролі (user1, mind67, snapshot99 тощо). Або інший приклад: атакуючий знає, що перша буква у верхньому регістрі, друга – голосна і що пароль не довше 6 символів. Така інформація може зменшити кількість можливих паролів в 20–30 разів. Цей метод включає всі атаки — перебором, за словником і по складах.

Складність пароля зазвичай оцінюють в термінах інформаційної ентропії, яка вимірюється в бітах. Кількістю «бітів ентропії» в паролі називається логарифм за основою 2 від числа спроб, необхідних для того, щоб точно вгадати пароль. Наприклад, для визначення паролю із 40-бітною складністю

необхідно провести 2^{42} (4 398 046 511 104) спроб, перевіривши всі можливі варіанти. Кожен новий біт ентропії збільшує складність паролю вдвічі, отже, вдвічі ускладняється й завдання для зловмисника. В середньому зловмиснику доводиться випробувати половину можливих варіантів для успішного підбору пароля.

Паролі, які створені людьми, зазвичай недостатньо випадкові – у середньому 40 біт ентропії, це пов'язано із поганим сприйняттям ймовірності людьми (наприклад, число 20 здається менш ймовірним за число 17). Також, намагаючись обрати випадкові послідовності символів для створення паролю, люди не використовують усі символи абетки рівномірно (наприклад, літера «е» використовується набагато частіше за літеру «f).

На складність пароля впливають такі чинники:

- кількість символів у паролі. Чим більше знаків у послідовності, тим краще. У комбінації з 5 знаків є велика ймовірність швидкого злому. А на підбір послідовності з 20 знаків можуть піти роки;
- чергування великих і малих літер. Приклади: пароль dfS123UYt з використанням регістра заголовних букв на порядок складніше цієї ж комбінації, але лише з маленькими літерами – dfs123uyt;
- символьні набори – різноманітність типів символів підсилює стійкість;
- Якщо скласти пароль із маленьких й великих літер, цифр та спеціальних символів довжиною в 15-20 знаків, шанси його підібрати практично нульові. Дуже важливо рівномірно розподілити знаки у паролі. Але зазвичай користувачі цифри та спеціальні символи ставлять у кінець пароля, а великі літери на початок – Okn@333.Приклад рівномірного розподілу символів у паролі – kIs$t0cHk@.

Орієнтовний час підбору паролів різної складності:

- дата народження 12071996 – 0,003 секунди;
- ім'я з великої літери Maksim і малої maksim – максимум півсекунди;

- поєднання, що складається з букв і цифр 7s3a8f1m2a – близько доби;
- vSA-DFRLLz – 1 рік;
- поєднання iu2374NDHSA) DD – 204 млн років.

У наступній таблиці наведено приблизний час повного перебору паролів у залежності від їх довжини. Вважається, що в паролі можуть використовуватися 36 різних символів (латинські букви одного регістра та цифри), а швидкість перебору складає 100 000 паролів в секунду.

Кількість знаків	Кількість варіантів	Стійкість	Час перебору
1	36	5 біт	менше секунди
2	1296	10 біт	менше секунди
3	46656	15 біт	менше секунди
4	1679616	21 біт	17 секунд
5	60466176	26 біт	10 хвилин
6	2176782336	31 біт	6 годин
7	78364164096	36 біт	9 днів
8	$2,821\ 109\ 9x10^{12}$	41 біт	11 місяців
9	$1,015\ 599\ 5x10^{14}$	46 біт	32 роки
10	$3,656\ 158\ 4x10^{15}$	52 біта	1162 роки
11	$1,316\ 217\ 0x10^{17}$	58 біт	41823 роки
12	$4,738\ 381\ 3x10^{18}$	62 біта	1505615 років

Прикладами широко розповсюджених, але дуже примітивних та ненадійних паролів є такі:

- послідовності й повтори: 12345, 337799, 10011001, abcde, aaaabbbb;
- дати народження: 13051990, 19900513, 0513;
- номери телефону: 0508765432, 0661543210;
- відомі цифрові комбінації: «102», «911», «777»;
- поширені слова: password, administrator;
- Ваше ім’я, імена родичів або домашніх тварин: anton, alex, sveto4ka, barsik, kesha;
- географічні назви: Ukraine, Mississippi, pacificocean;
- системне ім’я користувача або його частини: guest, user, default;

- адреси електронної пошти: example@ukr.net, pochta@gmail.com;
- клавіатурні послідовності символів: qwerty, Asdfg.

Спортивні паролі — одні з найулюбленіших, особливо серед чоловіків. Найбільш очевидні приклади: football, baseball. Назви популярних у вашому регіоні спортивних команд та імена гравців, навіть у поєднанні з важливими для локальної спортивної історії датами: LevsKi1914, DinAmO1975 також є слабкими паролями.

Любов, довіра, ненависть та інші емоції — ще одна популярна тема для створення паролів. Їх можна розділити на дві категорії: прості комбінації: iloveyou, loveme, trustno1 чи почуття до певних людей. Злочинці можуть мати певну інформацію про вас. Тому не варто використовувати пароль IloveAnn чи (жартома, звичайно,) HategeorGe, особливо якщо це імена ваших жінки або чоловіка. Поширені паролі на тему природи на кшталт flower і sunshine залишаються одними з найпростіших для зламу. Серед найпопулярніших фантастичних є dragon, princess, ninja і superman. Паролі такого типу теж дуже легко зламати.

SplashData.com

позиція	2017	2018	2019	2020	2021
1.	123456	123456	123456	123456	123456
2.	password	password	23456789	123456789	123456789
3.	12345678	123456789	qwerty	qwerty	qwerty
4.	qwerty	12345678	password	parol	parol
5.	12345	12345	1234567	1234567	1234567
6.	123456789	111111	12345678	12345678	12345678
7.	letmein	1234567	12345	12345	12345
8.	1234567	sunshine	iloveyou	iloveyou	iloveyou
9.	football	qwerty	111111	111111	111111
10.	iloveyou	iloveyou	23123	123123	123123

NordPass.com, 2020

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213

Принципи створення стійкого пароля:

- логін і пароль не повинен бути ідентичним;
- пароль не повинен складатися з особистої інформації (дата народження, телефон тощо);
- пароль не повинен складатися виключно з літер;
- створювати новий пароль для кожного окремого сервісу;
- використовувати двофакторну автентифікацію (за наявності);
- не зберігати паролі у браузері;
- не вводити паролі на сайтах без протоколу HTTPS (за його допомогою шифруються всі дані між клієнтом і сервером, що створює повну конфіденційність інформації користувача, наприклад паролі або банківські реквізити);
- нікому не довіряти та не називати пароль;
- враховувати довжину паролю – бажано не менше 10 символів;
- міняти пароль щоразу, коли здається, що його могли вкрасти. В інших випадках змінювати пароль не рідше ніж раз на 6 місяців.

У той же час, новий пароль не повинен бути простою модифікацією діючого, наприклад, шляхом зміни однієї цифри: h0lst1, h0lst2, h0lst3.

Рекомендації щодо створення унікальних паролів для різних сервісів:

- для критично важливих ресурсів (поштова скринька, платіжні системи, месенджери та соцмережі) використовувати складні та довгі паролі з довільними комбінаціями верхнього та нижнього регістру, цифр та спеціальних символів. Наприклад: S9Scap$iDPRZ;
- для важливих ресурсів (навчальні сайти, альтернативна поштова скринька) – паролі, де довжина важливіша за складність. Наприклад: hrGbWzeCjZSqUl;
- для не дуже важливих ресурсів (форуми, розважальні портали) вигадати прості, але не примітивні паролі. наприклад: metHalPh.

Методи створення стійких паролів.

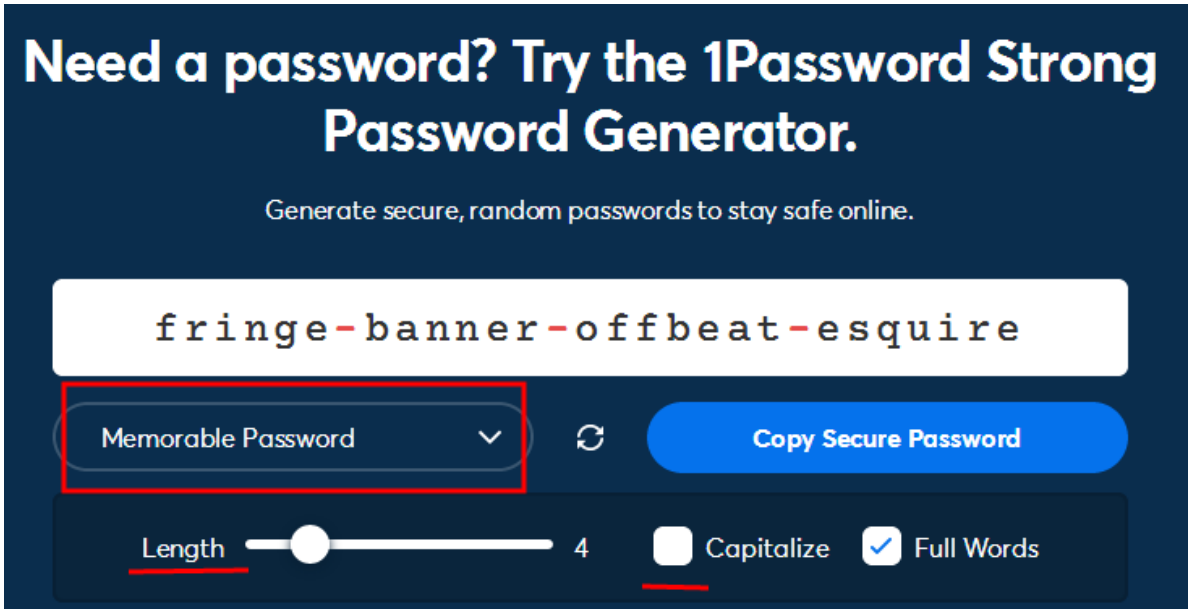
При створенні стійких паролів виникають дві проблеми – вигадати складний пароль та запам’ятати його.

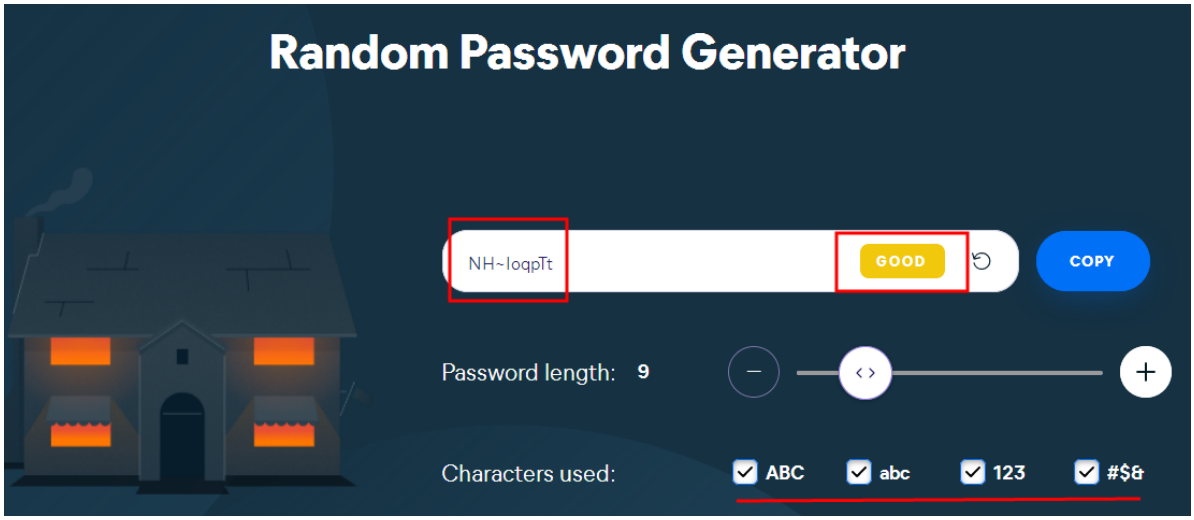
Якими б відповідальними не були люди, вони створюють паролі за шаблонами власного мислення, і це відомо зловмисникам. Дослідження та аналіз паролів показали, що 40% із них можна підібрати, використовуючи програмні методи. Часто людина, яка складає пароль, вказує в ньому те, що має безпосереднє відношення до неї та/або її оточення.

1. Найбільш стійкими є паролі, які створені за допомогою «генераторів паролей» – спеціалізованих сервісів, зокрема й хмарних. Наприклад, KeePass чи https://1password.com/password-generator/. При автоматичній генерації виключається взаємозв’язок між паролем та особистістю користувача. випадково обраний пароль створюється з величезного масиву даних і підібрати його дуже складно.

Але такі паролі є найбільш складними для запам’ятовування, наприклад, T2tgU#&y59kUOo чи 84aP@E&39uzxC1ka0. Якщо ви вирішили записати такий пароль (на папері чи у текстовий файл), то врахуйте, що не потрібно зберігати записаний пароль у доступному місці: приклеєному на робочий стіл або

захований під клавіатуру, оргтехніку; на робочому столі комп'ютера в текстових файлах (краще сховати в архів із нескладним парольним захистом); чи у браузері.



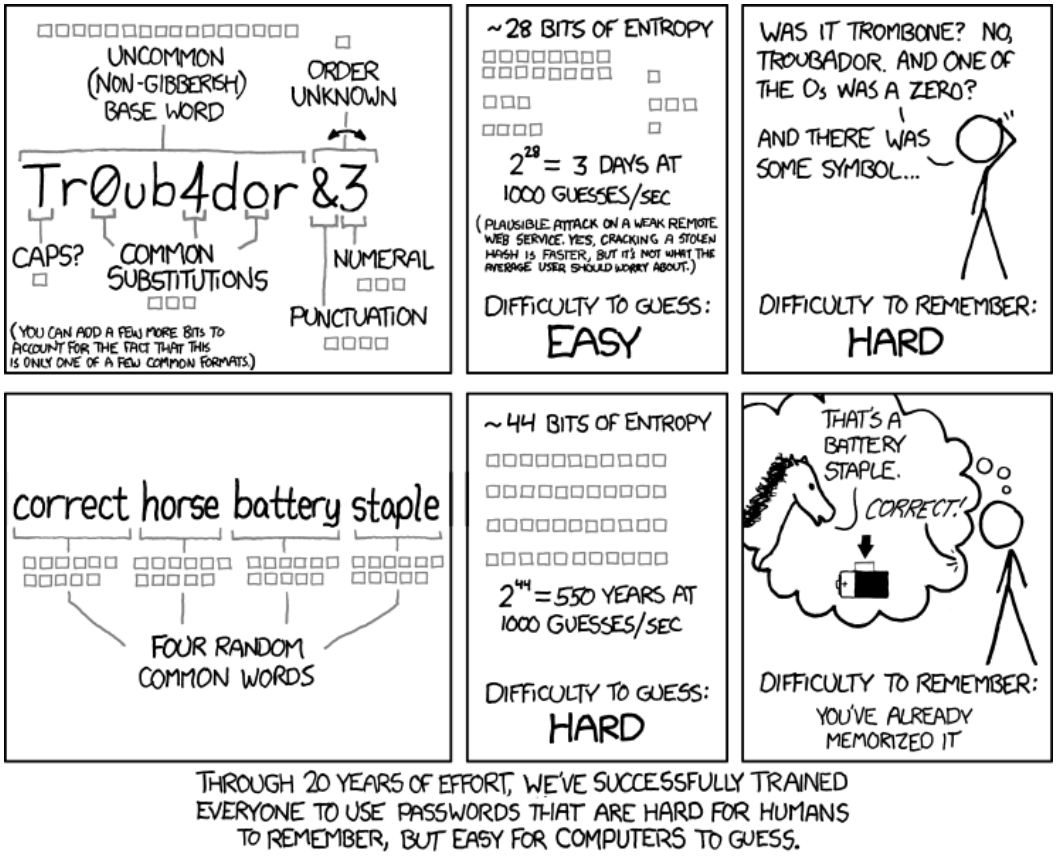


Краще завести спеціальний блокнот з паролями й тримати його у надійному місці. Американський криптограф Брюс Шнайєр рекомендує записувати паролі на маленьких шматочках паперу та зберігати у гаманці. Інший варіант – скористатися менеджером паролів.

2. При грамотному підході довжина пароля має пріоритет над його складністю, оскільки у рази збільшується кількість варіантів перебору. Марк Бернетт, дослідник у галузі безпеки, у своїй книзі Perfect passwords пише, що пароль завдовжки 12-15 знаків надійніший, ніж короткий, складений із

довільної послідовності символів, з використанням спеціальних символів та літер верхнього регістру. Таку ж думку має й Ден Уілер – IT-фахівець із Dropbox. Замість T@MQ36n^iL можна успішно використовувати correcthorsebatterystaple.

Проте, проста парольна фраза, така як iloverocknroll, передбачувана і тому зловмиснику її легше вгадати, у порівнянні з більш коротким паролем 9j%a#F,0.



3. вирішити проблему використання дуже складних варіантів допоможуть мнемонічні паролі, які добре запам’ятовуються. Спочатку треба скласти (вигадати) якусь фразу-нісенітницю (каламбур), що не має жодного практичного сенсу: ГЛОКАЯ КЕЗДРА МІНОРИТЬ БОКРЕНЯ. Далі беремо від однієї до трьох чи більше перших літер із кожного слова та записуємо відповідні їм літери латиною:

ГЛ	КУ	МІ	БО
UK	RE	VS	,J

Результат: «ukrevs,j».

Пароль можна покращити шляхом додавання між слогами певної дати (див. метод 5), краще у зворотному порядку, зміною регістру літер (наприклад, кожна друга літера – велика) та додаванням спецсимволів:

%uK2rE1vS0,J1.

4. Певною модифікацією методів 2 та 3 є такий прийом. В основі пароля лежить нетривіальне та довге слово української мови (чи іншої, за винятком англійської), можливо, вузький професіональний термін, чи застаріле, діалектичне слово: професорсько-викладацький, перехняблюватися, дихлордифенілтрихлорметилметан (*інсектицид проти шкідників, побутова назва ДДТ*), *екстрадихлордифенілтрихлорметилметан*.

Шляхом трансформації кириличних букв у англійські, отримаємо надійний пароль:

ghjatcjhcmrj-dbrkflfwmrbq,

gtht[yz,k/dfnbcz,

lb[kjhlbatyiknhb[kjhvtnbkvtnfy.

5. Цифровий метод. За основу паролю вибираємо Ваші пам’ятні дати. Але це не повинен бути Ваш день народження або день початку сімейного життя! Подія має бути виняткової важливості, але про неї повинні знати лише ви. Наприклад, день, коли ви вперше втекли з уроку або зламали підбор.

Оскільки основу пароля складають цифри, доцільно перемішати їх із літерами. Приклад: 22.10.1993 та 16.03.2021 Замініть точки, що розділяють день, місяць і рік, на будь-яку букву, наприклад маленьку англійську «l» (ель). Між двома датами поставимо «!». Нулі замінимо на літери «O»:

«22l1Ol1993!16lO3l2O21».

Цифровий метод можна вдосконалити, якщо проводити певні розрахунки з датами, що лежать в основі паролю. Наприклад, перемножити дві дати між собою: 22101993×2021=44668127853. За допомогою програми калькулятор можна перевести це число в шістнадцятирічну систему числення: досить натиснути кнопку Hex: A666D8A6D.

6. Метод мастер-пароля. Для того, щоб спростити створення унікальних паролів для різних сервісів можна скористатися наступним методом (але більш надійним буде використання абсолютно різних паролів для кожного сервісу!). Створюємо мастер-пароль, наприклад, A666D8A6D. Далі, за певним алгоритмом, додаємо до цієї основи ідентифікатор певного сервісу. Наприклад, ставимо символ «+» й додаємо 4 літери, які характеризують вебресурс:

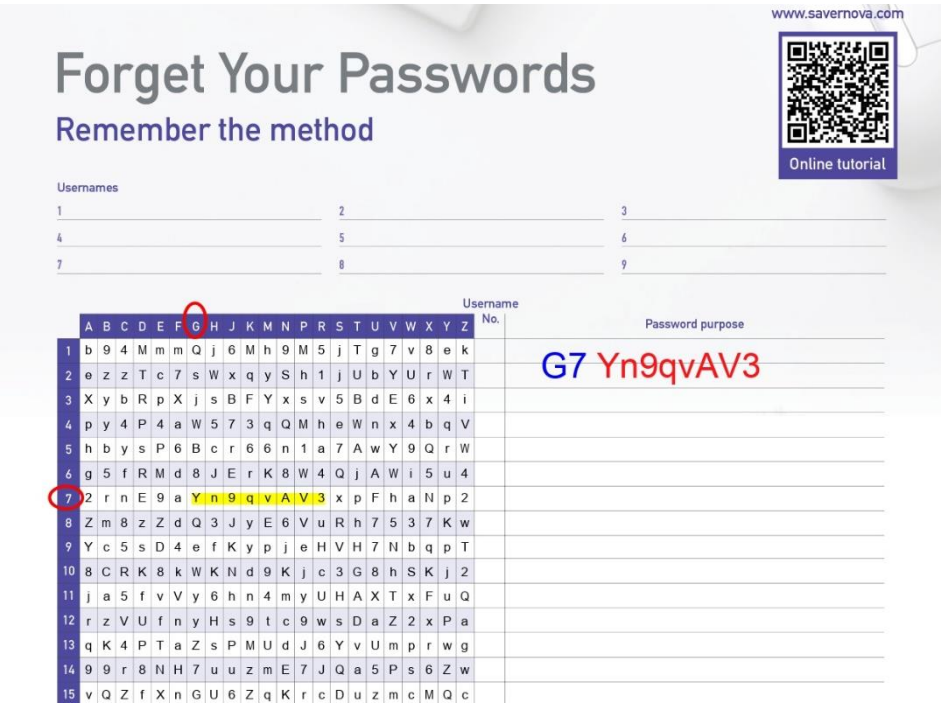
A666D8A6D+bank – для фінансових справ;

A666D8A6D+twit – соціальні мережі;

A666D8A6D+mail – електронна пошта.

7. Графічний метод. Створіть візуально контури геометричної фігури або будь-якого предмета на клавіатурі вашого комп’ютера. використовуйте символи, за якими проходять лінії. Важливо: фігура не повинна бути примітивною, наприклад квадратом.

8. Карта паролів (https://www.savernova.com/). визначте Ваш метод читання, який використовуватиметься кожного разу. Він складається з початкової точки та напряму руху. Такі паролі задовольняють сучасні критерії безпеки, їх важко зламати; якщо користувач втратить картку, це також не проблема: без особистого методу читання карта непотрібна. Кожна картка є унікальною.



Для перевірки стійкості створених паролів доцільно скористатися відповідними онлайн-сервісами, наприклад:

https://exploit.in/passcheck/,

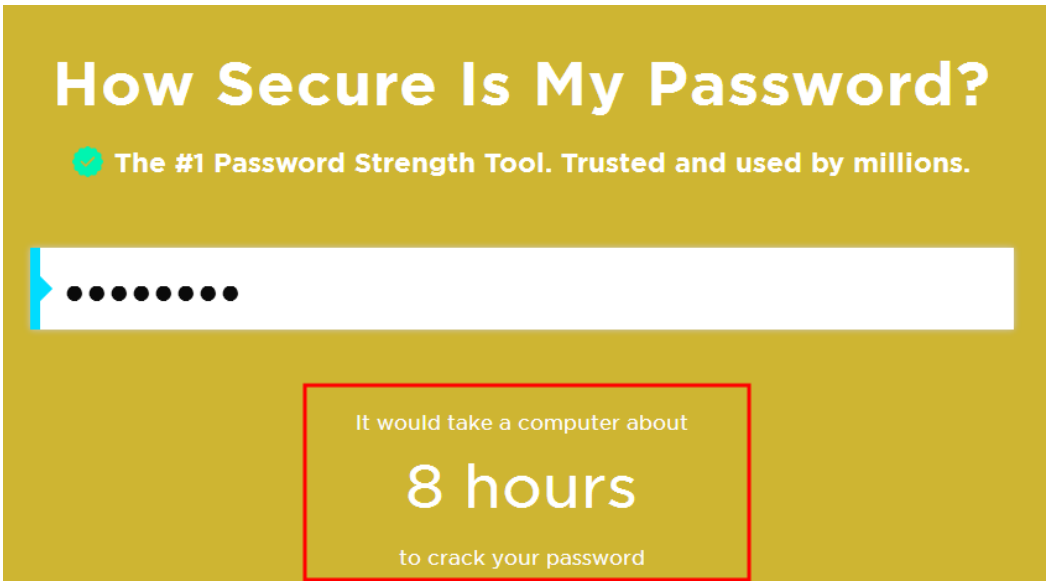
https://zillya.ua/check-password,

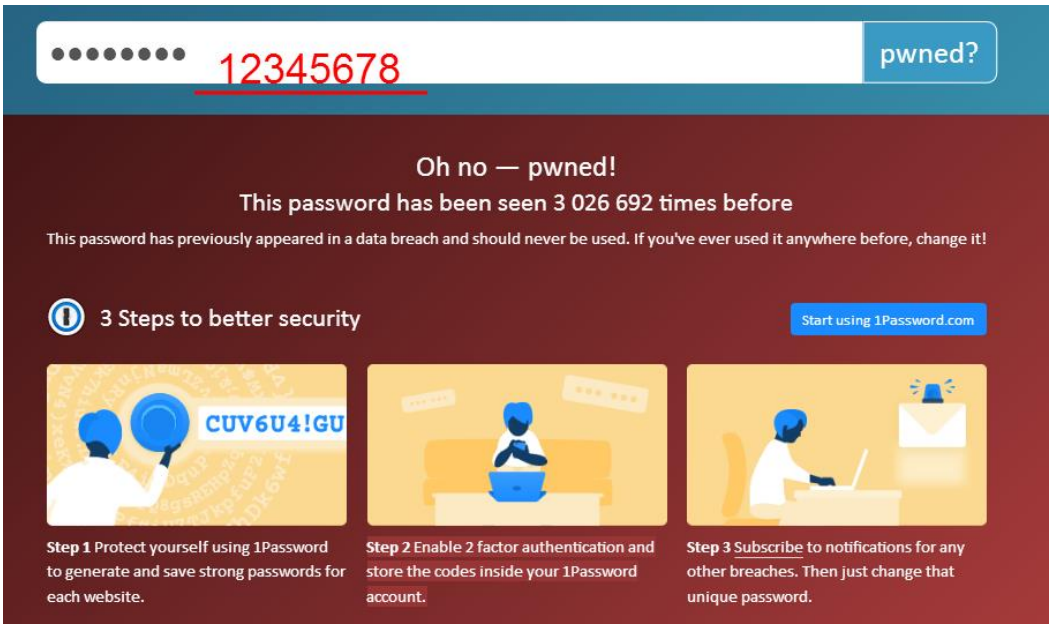
https://www.security.org/how-secure-is-my-password/.

Сервісі, що містять бази з реальними паролями, які раніше були розкриті в результаті порушення даних:

https://haveibeenpwned.com/Passwords, https://breachalarm.com/,

https://pwnedlist.com/query.





Інциденти:

- компанія «Нутелла» порадила передплатникам використовувати як надійний пароль слово Nutella;
- один із співробітників Білого дому загубив на автобусній зупинці папірець, на якому було записано незахищений пароль від електронної пошти;
- у Google стажувався студент з Індії, який зміг отримати доступ до супутника компанії через адміністративну панель, просто залишивши поля введення логіну та пароля порожніми;
- дані понад 14 мільйонів виборців штату Техас стали доступними в режимі онлайн оскільки сервер не захистили паролем;
- співробітники Організації Об'єднаних Націй зберігають документи у Trello та Google Docs, які не захищені паролем. За посиланнями вони стають доступними для всіх бажаючих.

2.3. Менеджери паролів.

Для надійного зберігання великої кількості сильних паролів, які важко запам'ятати, доцільно використовувати менеджери (диспетчери) паролів – спеціалізовані програмні продукти для роботи з паролями, PIN-кодами. Менеджери паролів мають наступні переваги:

- гарантована безпека важливих даних – сервіс дає можливість зберігати не лише ідентифікатори, а також PIN-коди від банківських карт, номери рахунків тощо;
- генерування унікальних послідовностей – більшість програм оснащені спеціальним інструментом, який генерує оригінальні випадкові комбінації символів за заданими параметрами. Вони захищені від підбору, адже не містять будь-якої особистої інформації користувача;
- спрощення авторизації – програма запам'ятовує послідовності для конкретних ресурсів і під час повторного входу автоматично заповнює необхідні поля. Функція автозаповнення не застосовується до програм і додатків, але в такому разі можна просто скопіювати потрібний пароль;

- відсутність потреби запам’ятовувати всі комбінації – вони містяться в одному сервісі, тож Вам потрібно запам’ятати лише майстер-пароль.

Менеджер паролів може бути реалізовано як онлайн-сервіс, бути вбудованим до браузеру чи інстальований в операційну систему Вашого пристрою. Менеджер використовує досить потужне шифрування AES, яке практично не піддається зламу з довжиною ключа у 256 біт. Таку базу можна розблокувати тільки за допомогою використання правильного майстер-паролю, отже, користувачу необхідно запам’ятати лише один надійний пароль.

Менеджер паролів Вашого браузера дозволяє без додаткового програмного забезпечення зберігати всі паролі та надійно синхронізувати їх між своїми пристроями. Обліковий запис, з яким синхронізовано Ваш браузер, може бути захищений двоступеневою автентифікацією.

Але вбудовані до браузеру менеджери мають й недоліки – менші потужність та обмежений функціонал, у порівнянні зі спеціальними програмними засобами; прив’язка до певного браузера та, інколи, й операційної системи.

Спеціалізовані менеджери паролів мають розширений функціонал, який полегшує доступ до паролів, ліцензійних ключів, Wi-Fi-кодів тощо. Такі менеджери паролів мають функції спільного використання паролів та системи попередження, які вказують слабкі та повторно використані паролі, повідомляють, коли пароль, який ви використовуєте, було виявлено в базах даних паролів, які зазнали витоку.

Перевагу треба надавати менеджерам паролів, які існують вже багато років та мають відкритий код.

Кампанія Avast надає такі поради щодо вибору менеджеру паролів:

- безпека – наявність функцій керування паролями для додатків і сайтів, попередження про витік даних із сайтів, на яких ви зареєстровані;
- багатофакторна автентифікація;
- генератор безпечних паролів;
- безпечна синхронізація паролів для різних пристроїв;
- автоматичне оновлення паролів для зламаних сайтів;
- зручність використання, наприклад, автозаповнення паролів;
- розширення для браузера;
- менеджер паролів для програм;
- функція «Електронний гаманець» – зберігає номери Ваших кредитних карток та інші платіжні реквізити у захищеному вигляді, автоматизуючи процес їхнього введення при покупці;
- екстрений доступ для інших користувачів – дозволяє членам сім'ї або колегам отримати доступ до важливих облікових записів у разі надзвичайної ситуації;
- багатоплатформні рішення.

ЛАБОРАТОРНА РОБОТА №2. КЕРУВАННЯ ПАРОЛЯМИ.

Мета вивчення: ознайомитися з різними методами та правилами створення надійних паролів. Отримати практичні навички утворення паролів та їх перевірки на стійкість. Налаштувати двохфакторну автентифікацію акаунту в Google.

Обсяг навчального часу: 1 година.

Обладнання: комп'ютер (планшет, смартфон), наявність підключення до мережі Інтернет.

План заняття:

1. Створити паролі різними методами та різної довжини.
2. Перевірити створені паролі на стійкість та в базах, що містять скомпрометовані паролі.
3. З'ясувати, чи впливають довжина й складність паролю на його стійкість.
4. Налаштувати двохфакторну автентифікацію акаунту в Google.

Інформаційні джерела:

генератори паролів:

- https://www.avast.ua/random-password-generator,
- https://1password.com/password-generator/,
- https://axcrypt.net/information/password-generator;

створення карти паролів: https://www.savernova.com/;

перевірка надійності паролів:

- https://exploit.in/passcheck/,
- https://www.security.org/how-secure-is-my-password/,
- https://zillya.ua/check-password;

бази паролів, які були скомпрометовані:

- https://breachalarm.com/?,
- https://pwnedlist.com/query,
- https://haveibeenpwned.com/Passwords;

підтримка Google: https://support.google.com/mail/?hl=uk.

ЗАВДАННЯ:

1. Створити паролі наступними методами: цифровим методом, за допомогою парольної фрази (слова), генератором паролів (використайте не менше двох відповідних онлайн-сервісів), за допомогою карти паролів, надайте приклад майстер-пароля. Занести створені паролі у перший стовпчик вашого звіту.

2. Перевірити створені паролі на стійкість та наявність у базах паролів, що були скомпрометовані. Результати занести у звіт.

3. Додайте до таблиці-звіту принаймні два «легких» пароля, але різної довжини: 8-10 символів та 14-16. виконайте для цих паролів завдання 3. Зробіть висновки.

4. виконайте налаштування двохфакторної автентифікації на прикладі акаунту в Google.

ВИМОГИ ДО ЗВІТУ:

1. Таблиця зі створеними паролями та результати їх перевірки.

2. Висновок, щодо залежності стійкості паролю від його довжини та складності.

ХІД РОБОТИ.

1. Онлайн-генератор паролів AxCrypt завдяки використанню статистичного аналізу фактичного тексту створює надійні паролі, які не є безглуздим набором символів, отже їх легко запам’ятати. Вам буде запропоновано три паролі різного рівня складності.

Скористайтеся генератором паролів від Avast для перевірки залежності стійкості паролю від його довжини та знаків, що використовуються.

Приклад таблиці зі звітом:

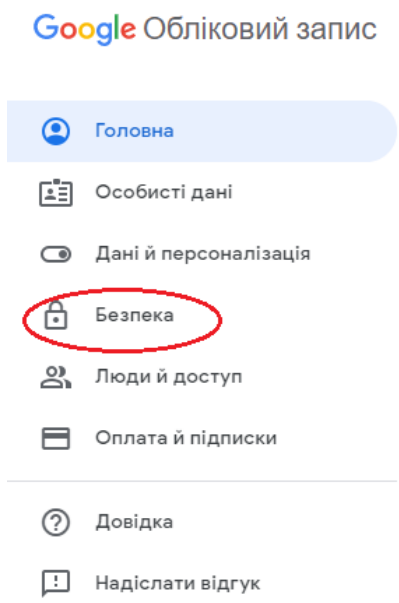
Пароль та метод утворення	Результати перевірки на стійкість		Чи був пароль скомпрометовано
	zillya.ua	**security.org**	**haveibeenpwned.com**
ghjatcjhcmrj-dbrkflfwmrbq метод парольної фрази	Ваш пароль має високий рівень надійності. Зламати такий пароль практично неможливо	16 sextillion years	—
12345678910 елементарний пароль	Якщо Ваш пароль настільки простий, то у вас проблеми! На злам такого паролю хакерам знадобиться зовсім мало часу.	2 seconds	+ This password has beenseen 170 284 times before

2. Двохфакторна автентифікація в Google. Акаунти найпопулярніших сервісів типу Google та Facebook використовуються для авторизації на інших онлайн-ресурсах. Отже, якщо зловмисники отримують доступ до одного акаунту, вони автоматично заволодівають інформацією з багатьох сервісів.

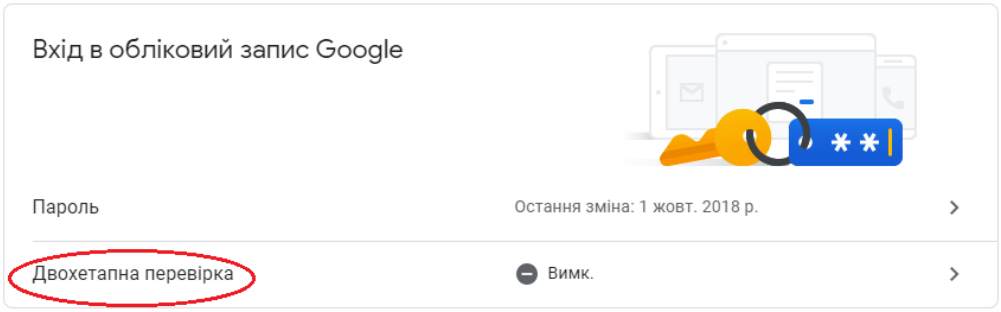
При налаштованій двофакторній авторизації система не надасть доступ до сервісу без додаткової ідентифікації, навіть якщо буде введений правильний пароль. Таким чином, якщо Ваш пароль буде викрадений, і хтось спробує ним скористатися, ви отримаєте про це сповіщення й зможете оперативно зреагувати (змінити пароль).

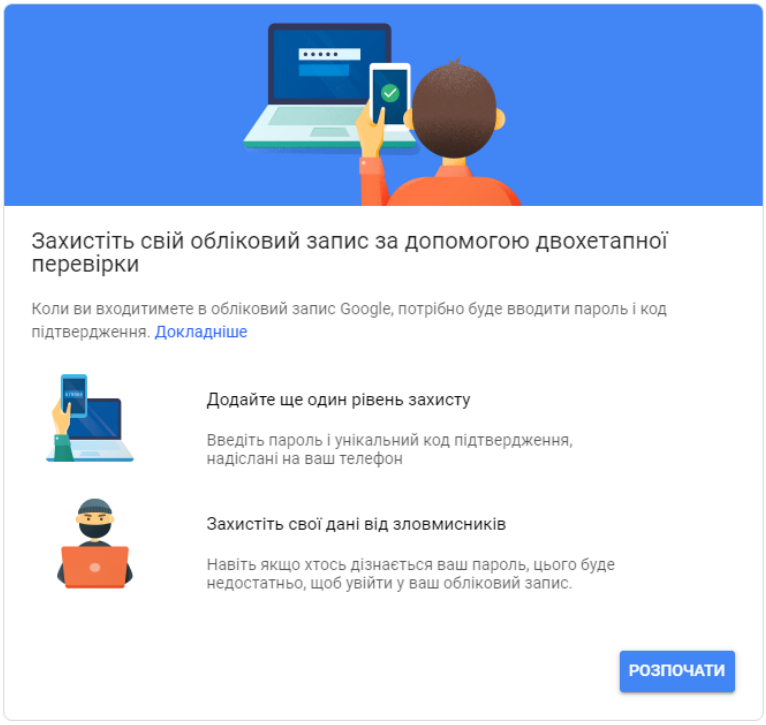
Єдиним мінусом є те, що користувач змушений надавати додаткову персональну інформацію, наприклад, реальний номер свого телефону. Але цей недолік є досить відносним. Створення та підтримка двофакторної авторизації потребує значних фінансових ресурсів, тому запроваджують її лише великі компанії (Google, соціальні мережі, банки, великі торгові платформи тощо), яким користувачі і так надають достатньо приватної інформації, оскільки це передбачено умовами їх використання.

Для налаштування двофакторної авторизації акаунту Google авторизуйтесь та перейдіть на вкладку «Безпека».

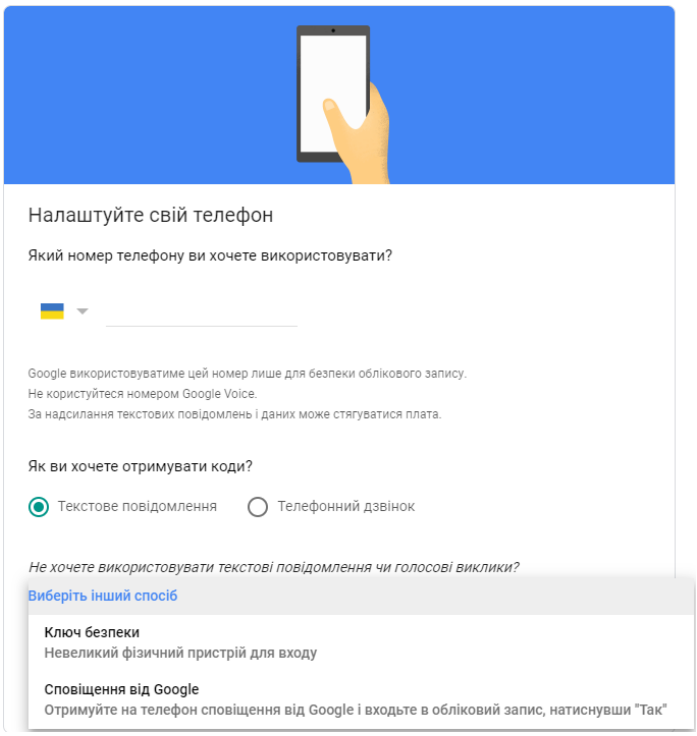


У параметрах входу в обліковий запис оберіть «Двохетапна перевірка», щоб розпочати налаштування.

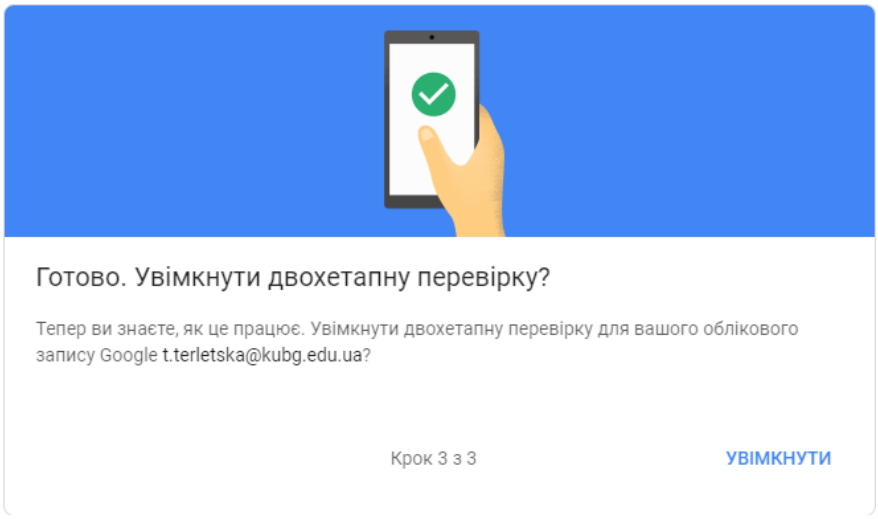




Додайте номер телефону та оберіть, в який спосіб ви бажаєте отримувати сповіщення.



Для використання варіанту «Сповіщення від Google» Вам буде необхідно додатково увійти в свій акаунт Google зі свого мобільного пристрою. Цей спосіб не вимагає надання номеру мобільного телефону. Його перевага в тому, що якщо сім-картка з якоїсь причини заблокована, доступ до Google-акаунту зберігається й залишається недоступним зловмисникам. Недоліком є те, що для входу в акаунт телефон повинен мати підключення до Інтернету. При виборі опції «Текстове повідомлення» або «Телефонний дзвінок» зверніть увагу, що код країни вказаний в форматі +380, тому номер телефону необхідно вводити в 9-значному форматі (без першого нуля).



3. ЗАХИСТ ДАНИХ

3.1. Створення резервних копій файлів. Зберігання копій.

3.2. видалення та відновлення даних.

3.3.Основні поняття криптографії. Шифрування та маскування даних.

3.1. Створення резервних копій файлів. Зберігання копій.

Для захисту інформації необхідно забезпечити її конфіденційність, цілісність та доступність. Одним із найвідоміших та простих методів запобігання втрати важливих даних є резервне копіювання файлів або бекап.

Даний процес забезпечує зберігання будь-якого важливого документа або інформації в окремому місці від оригіналу для уникнення втрати інформації. Якщо вихідний документ пошкоджений, можна відновити інформацію завдяки наявності копії, яка зберігалася в іншому безпечному місці.

Розрізняють такі типи резервних копій:

- резервна копія операційної системи;
- резервна копія логічного диску (розділу);
- резервна копія окремих файлів та папок — найпоширеніший спосіб резервного копіювання.

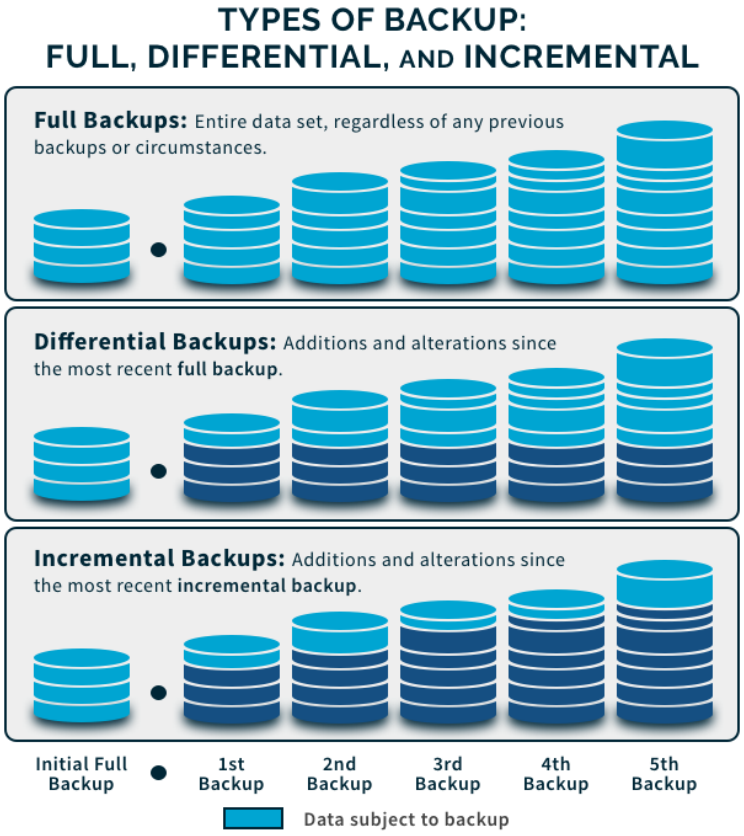
Можна навести й іншу класифікацію резервного копіювання.

Повне резервне копіювання (Full Backup або L0) – повна копія даних. Рівень, який забезпечує створення повної копії об’єкту резервного копіювання.

Цей рівень дозволяє забезпечити максимальну відповідність оригіналу даних його копії.

Диференційне резервне копіювання (Differential Backup або L1) – копіювання змін, що були зроблені після створення останньої повної копії. Створення такої копії потребує більше часу та займає більший об’єм, ніж додаткове копіювання, але дозволяє пришвидшити процес відновлення. Загалом є альтернативою між створенням повної або додаткової копії.

Додаткове резервне копіювання (Incremental Backup або L2) – копіювання змін, що відбулись із часу повного, диференційного або додаткового копіювання. Загалом на додаткове копіювання затрачається менше часу, бо копіюється менше файлів. Однак процес відновлення даних займає більше часу, оскільки повинні спочатку відновлюватися дані останньої повної копії і після цього — всі резервні копії, від яких залежить додаткова копія.



Компанія Eset надає такі поради. Після вибору типу бекапа, який найкраще підходить для Ваших потреб, важливо вирішити, яким чином слід зберігати. Протягом останніх 20 років типи носіїв, які найчастіше використовуються для зберігання даних, змінювалися та вдосконалювалися.

Найвідомішими серед них є перфокарти, дискети, оптичні носії, такі як CD, DVD та Blu-Ray, стрічки, зовнішні жорсткі диски, зберігання даних у хмарі. Під час вибору носія для зберігання власних резервних копій варто в першу чергу врахувати тривалість її зберігання відповідно до Ваших потреб. Наприклад, CD/CD-ROM, MD (Mini Disc) та DVD служать довше – 25-50 років. Після них йдуть HDD, SSD, USB флеш-накопичувачі та карти пам'яті з тривалістю зберігання 10 років. І найменший життєвий цикл до 10 років мають дискети та Blu-Ray диски.

Поширені помилки при резервному копіюванні файлів.

1. Невиконання процесу резервного копіювання важливих файлів. Такі дії – найпоширеніша помилка. Дуже часто резервне копіювання не було виконано через те, що інформація здавалася не важливою до моменту, поки вона не була втрачена.

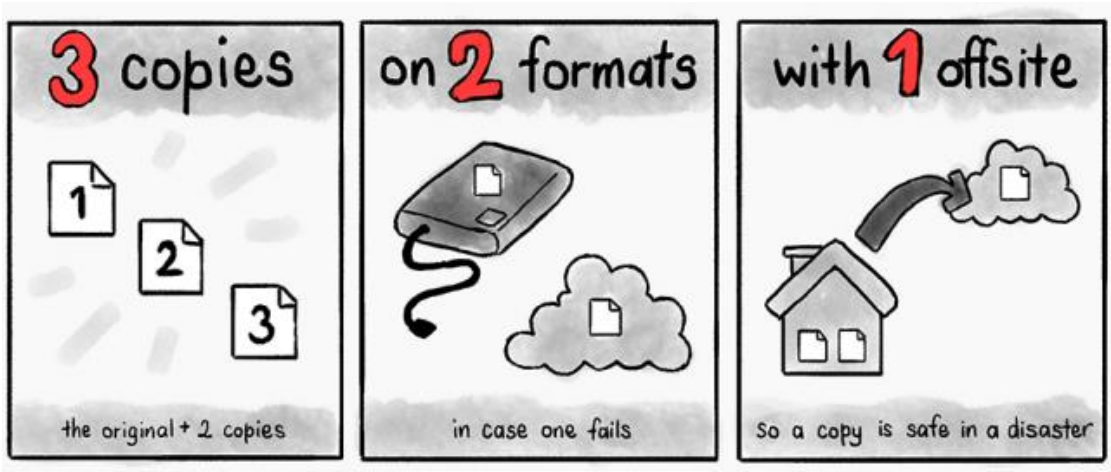
2. Збереження резервних копій на тому ж пристрої, що й оригінальні файли. Копія повинна зберігатися окремо від оригінальних документів. Якщо вони зберігаються на одному пристрої та обладнання пошкоджено, то резервні копії можуть бути втрачені разом із оригіналами.

3. Відсутність тестування. Створення резервної копії включає ряд процесів. Недостатньо просто створити копію – потрібно перевірити файли, щоб переконатися, що збережені дані фактично доступні в разі потреби. Оскільки під час зберігання вони можуть бути пошкоджені, то в цьому випадку потрібно зробити нове резервне копіювання.

4. Здійснення бекапа недостатньо часто. Важливо регулярно створювати резервні копії, особливо якщо інформація часто оновлюється.

5. Відсутність маркування файлів резервного копіювання. Під час бекапа важливо фіксувати, на якому обладнанні зберігаються певні дані. У разі необхідності відновлення даних записи допоможуть прискорити цей процес.

Фахівці радять для зберігання критично важливих даних керуватися законом «3-2-1»: три копії зберігати на двох різних носіях, один із яких – в офлайні.

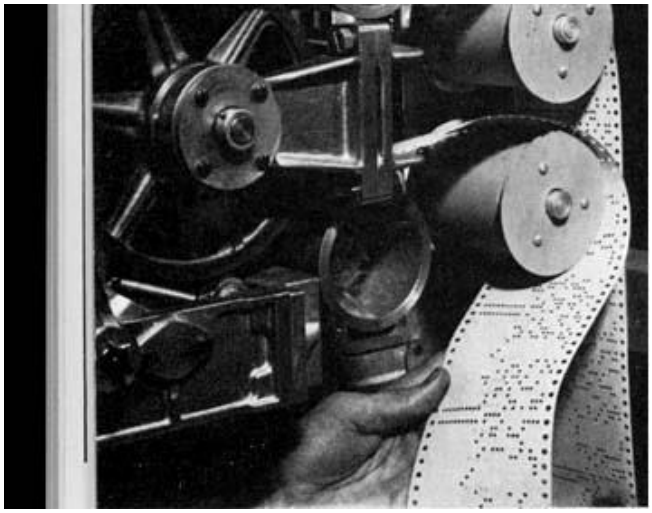


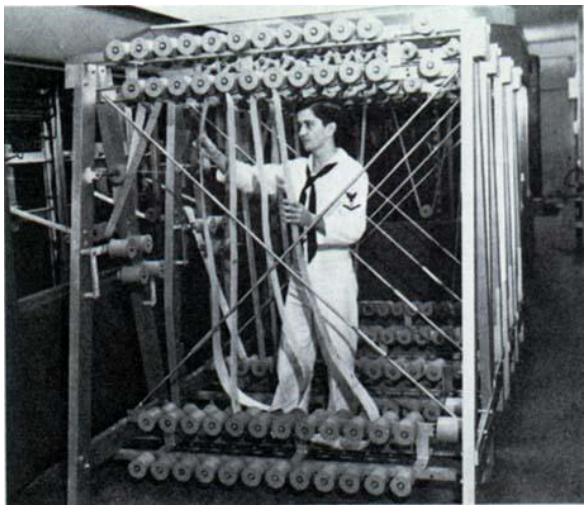
Слід уникати нестандартних способів зберігання (у всякому разі, як єдиного способу), рідких та пропрієтарних форматів, мов (наприклад, для документів краще використовувати ODF і TXT, а не DOCX чи DOC). Зберігати інформацію слід у стиснутих форматах і незашифрованому вигляді – інакше, навіть незначне пошкодження цілісності даних може зробити всю інформацію

недоступною. Наприклад, якщо потрібно надовго зберегти медіа файли, то для звуку краще буде WAV, для фотографій – RAW, TIFF та BMP.

З іншого боку, відсутність шифрування особливо важливих файлів може бути небезпечною!

Ще одна проблема – з часом пристрої зчитування інформації з носіїв стають застарілими.





1. Початковий рівень. Хмарні сховища. Наприклад, сервіс Mega. Безкоштовний акаунт дозволяє зберігати до 50 Гб інформації. Сервіс пропонує зручний десктоп-додаток. Він автоматично копіює в хмару всі зміни в папці. Інший, дуже популярний варіант – Googke-диск.

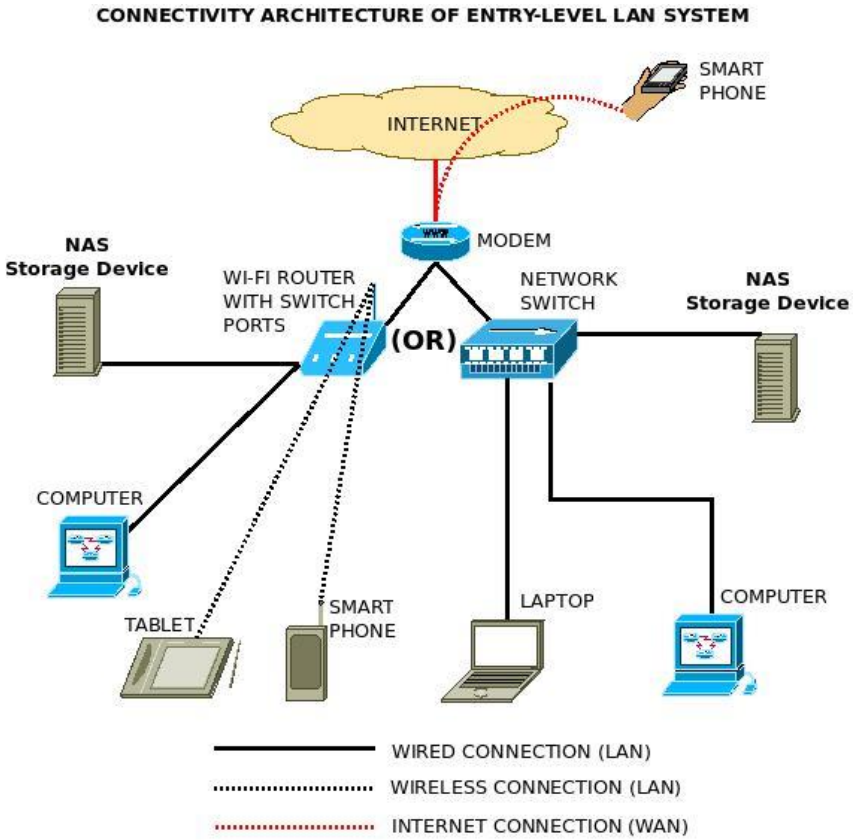
2. Напівпрофесійний рівень. Резервний жорсткий диск. Більшість фахівців із відновлення даних рекомендують для резервування критично важливих файлів використовувати додатковий жорсткий диск, причому саме HDD, а не SSD.

Фахівці не радять зберігати важливу інформацію на SSD-дисках, SD-картах т а USB-флешках, оскільки відновити інформацію з таких типів носіїв складно та вони мають менший термін працездатності в порівнянні з HDD.

3. Професійний рівень.

1) Для більш надійного зберігання доцільно скористатися сховищем даних типу NAS – Network Attached Storage. Жорсткі диски для NAS

відрізняються від інших великим ресурсом і спеціальними алгоритмами оптимізації читання та запису. Недоліком NAS є його висока ціна.



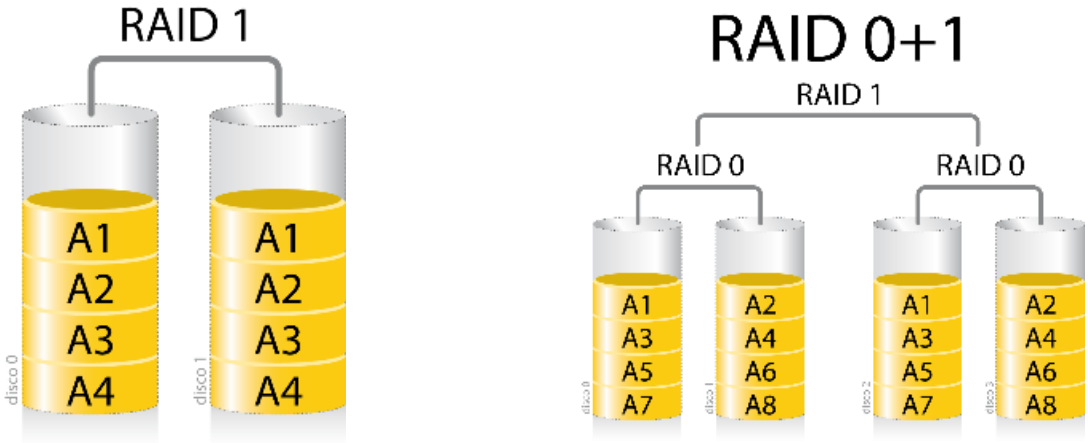
2) Технологія RAID (Redundant Array of Independent Disks) – це дисковий масив, об'єднання декількох жорстких дисків, для операційної системи вони будуть функціонувати як один, підвищуючи швидкість читання даних або надійність їх збереження. Всього існує 7 основних (типових) конфігурації (з номерами від 0 до 6) а також кілька комбінованих варіацій, наприклад, RAID 10 – комбінує розширюваність RAID 0 і надійність RAID 1.

Дискові масиви RAID 0 будуються мінімум із 2 дисків й використовують усі диски одночасно для зберігання на них файлів. Технологія за якою працює цей масив називається data striping, або розбивка даних. Суть полягає в тому що дані розбиваються на блоки фіксованого розміру і по черзі складаються на кожен диск. Тобто один файл може лежати шматочками на усіх дисках масиву. Таким чином досягається дуже висока швидкість читання, адже файл «збирається» вже не з одного (часто фрагментованого) диска, а одразу з декількох, хоча при запису швидкість, звичайно, менша ніж при роботі з одним

диском. При втраті одного диска з масиву дані безповоротно пошкоджуються, оскільки практично всі файли лежать одразу по всіх дисках.

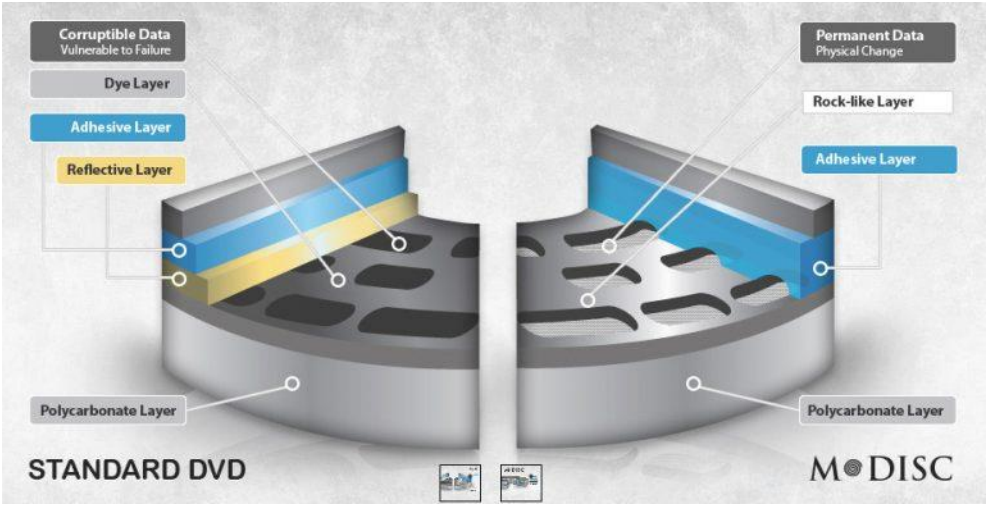
Масиви RAID 1 також будуються мінімум із 2 дисків. Технологія за якою працюють дискові масиви типу RAID 1 називається mirroring, або віддзеркалювання. Суть технології полягає в тому що всі дані лежать на одному диску, а інший працює як «двійник» тримаючи на собі повну копію основного диска. Таким чином, дана технологія забезпечує збереженість даних навіть при виході з ладу одного диска в масиві, що робить її ідеальною для зберігання на ній важливих даних, яким між тим не потрібен дуже швидкий доступ, оскільки в швидкості читання/запису вона програє навіть одиночним (які не стоять в RAID) дискам.

Доцільно, за можливості, поєднувати обидві технології.



4. Суто професіональний рівень.

1) M-Disc:



2) LTO-стрімер (стандарт Linear Tape-Open):

3.2. Видалення та відновлення даних.

З метою захисту файлів від видалення чи копіювання можна скористатися як засобами операційної системи так і допомогою спеціальних програм.

Для захисту комп’ютера від копіювання файлів на знімні носії необхідно внести певні зміни до реєстру операційної системи. Якщо необхідно заборонити видалення деяких файлів, то достатньо створити на локальному диску спеціальну папку, в якій будуть зберігатися файли, втрата яких є небажаною.

Окрім штатних засобів Windows, розроблена достатня кількість сторонніх програм, які можуть захистити файли від копіювання та видалення.

Відновлення видалених даних або, навпаки, видалення даних без можливості їх відновлення, суттєво залежить від типу накопичувача.

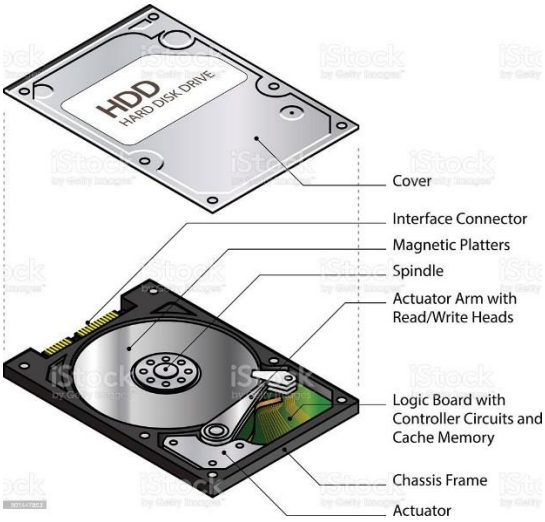
Дисковий накопичувач типу HDD (hard (magnetic) disk drive).

Процедура знищення певного файлу відбувається у кілька етапів:

1. ви видаляєте файл «X» (наприклад, через Кошик), і для користувача він зникає з папки.

2. Фізично «X» залишається на диску, але комірка, де він зберігається, отримує статус вільної.

3. При записі на диск нових файлів, комірка зі статусом «вільна» заповнюється, й відбувається затирання файлу «X» новим. Якщо ж комірка при збереженні нового файлу не використовувалася, то видалений раніше файл «X» продовжує фізично перебувати на жорсткому диску.



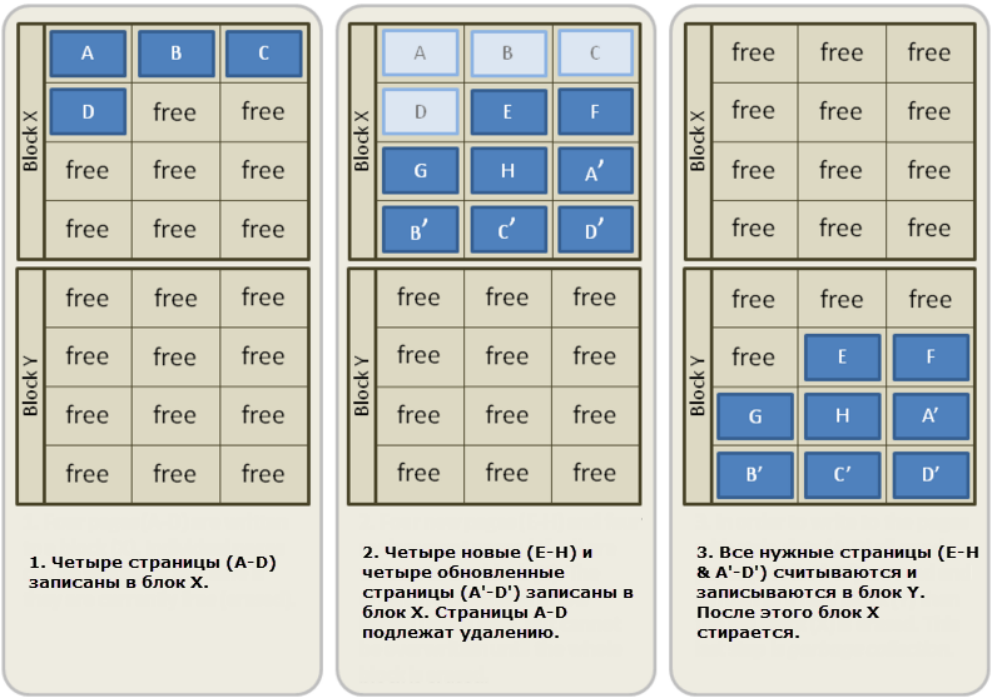
4. Після багаторазового перезапису даних у комірці (2-3 рази) видалений файл «X» буде остаточно знищенно. Якщо ж файл займає більше місця, ніж одна комірка, то, в такому випадку, буде знищено лише фрагмент файлу «X».

Отже, існує можливість досить легко відновити видалені файли за допомогою спеціальних програм. На успіх відновлення прямо впливає період часу від знищення до початку процедури відновлення, та інші чинники – кількість вільного місця на диску, чи записували ви великі файлі після знищення.

З іншого боку, для гарантованого видалення файлу, без подальшого відновлення, необхідно ініціювати його примусовий перезапис. Для цього існує чимало утиліт, проте найпростіше скористатися штатними засобами Вашої операційної системи.

Жорстки диски типу SSD (solid-state drive). Твердотілий накопичувач розбито на блоки (обсягом декілька мегабайт), блоки, у свою чергу, поділено на сторінки (обсягом декілька десятків кілобайт кожна). Сторінка може бути заповнена даними лише один раз, при цьому сторінки в межах блоку повинні програмуватися строго в порядку зростання їх номерів. Для повторного заповнення сторінки необхідно повністю стерти весь блок. Стерти лише частину блоку неможливо.

Логіка роботи накопичувача побудована таким чином, що сторінка, яка була видалена користувачем, фактично продовжує зберігати записану інформацію. Для запису нової інформації контролер ініціює процедуру, відому як Garbage Collection/TRIM, яка видаляє непотрібні дані й перерозподіляє існуючі. Для цього всі сторінки, за винятком непотрібної, копіюються на інший, вільний блок, тоді як перший блок повністю стирається. Далі актуальні сторінки переносяться назад до першого блоку, видаляються з другого, і лише після цього нові дані остаточно займають своє місце.



Для прискорення роботи SSD, при наявності вільного місця, нові файли відразу записуються на вільні сторінки, а оптимізація сміття відкладається до моменту простою накопичувача.

висновки:

1. Якщо інформація була дійсно фізично знищена в пам’яті накопичувача, вона не підлягає відновленню за жодних обставин.

2. Навіть якщо процедуру оптимізації сміття не було завершено, користувач не зможе отримати доступ до неочищених сторінок (за винятком наявності спеціального обладнання).

3. В абсолютній більшості випадків відновити файли, які були видалені з SSD-накопичувача, не вдасться.

4. Якщо накопичувач чи операційна система (наприклад, Windows XP) чи протокол (наприклад, при роботі з usb) не підтримує команду TRIM, або вона не включена, то відновлення видаленої інформації можливе.

5. Для видалення даних без можливості їх подальшого відновлення необхідно виконати форматування диску чи скористатися відповідною утілитою від виробника.

USB flash-накопичувач, карта пам’яті. Ці накопичувачі мають наступні правила: пам’ять розділена на блоки розміром декілька мегабайт; перед

записом у блок пам’яті його необхідно очистити від вже існуючих даних; блок складається зі сторінок, розміром у десятки кілобайт; запис даних у блок проводиться сторінками, одночасно може бути записана відразу вся сторінка даних; сторінки даних усередині одного блоку повинні записуватись строго у порядку зростання їх номерів; кожна сторінка після стирання блоку може бути записана лише один раз до наступного стирання.

Отже, при видаленні файлу фактично він не знищується. Натомість система позначає його як видалений, а відповідну частину дискового простору – як вільне місце для використання новими файлами. Доки ці кластери не будуть перезаписані іншими файлами, видалений файл можна відновити, особливо, якщо накопичувач має багато вільного місця, а процедура відновлення проводиться негайно після видалення.

Методи відновлення/знищення даних засновані на певних фізичних процесах, із використанням відповідного обладнання чи на застосуванні спеціалізованого програмного продукту (наприклад, Transcend RecoveRx, Recuva, Ashampoo Undeleter, MiniTool Power Data Recovery).

Принцип роботи програм відновлення даних наступний: необхідно визначити носій, на якому розташовано видалені файли. Це може бути весь жорсткий диск, USB-накопичувач або лише певні папки. Доцільно максимально звузити пошук. Введіть індивідуальні умови пошуку та встановіть різні фільтри, такі як тип інформації: музика, відео або контакти. Також можна вказати розмір файлу або дату, наприклад, певний період часу. Після цього почніть пошук. Далі з’явиться індикатор стану чи кількість результатів, вони будуть показані відповідно до різних критеріїв. Програми відновлення даних зазвичай вказують ймовірність повного відновлення та збереження файлу. виберіть потрібні файли та вкажіть папку, в яку вони мають бути відновлені, а далі дотримуйтесь інструкцій на екрані.

Важливо: не відновлювати інформацію на той самий носій, де вона зберігалася до видалення.

Для надійного видалення інформації використовується наступна процедура: на носій здійснюється запис випадковим чином згенерованої інформації, запис виконується декілька разів (залежно від обраного режиму), наприклад, алгоритм Міністерства оборони США DoD 5220.22-M: перезапис комбінаціями цифр, що передбачає до 7 циклів чи алгоритм за методом Гутмана, перезапис комбінаціями цифр у 35 циклів. Вважається, що однократного перезапису недостатньо для гарантованого знищення даних. Збалансованим з точки зору пари «час – надійність» є трикратний цикл перезапису. Метод Гутмана триває дуже довго, переважно більше доби, але це максимально безпечний алгоритм.

Приклади програм для видалення інформації: CCleaner, Eraser, File Shredder, Alternate File Shredder.

Програма Eraser, наприклад, надійно видаляє файли і папки, очищає вільний дисковий простір. Користувач може вибирати один із 14 алгоритмів видалення на власний розсуд. Програма вбудовується в контекстне меню операційної системи.

Важливо: єдиний надійний спосіб видалити всі дані з жорсткого диска без можливості відновлення – проведення повного форматування зі зміною типу файлової системи. Наприклад, якщо необхідно видалити без можливості відновлення зображення, але при цьому в ОС включено відображення ескізів, то просте видалення файлу не допоможе. Обізнана людина зможе відновити його, використовуючи файл Thumbs.db, що зберігає в собі ескізи фото. Аналогічна ситуація і з файлом підкачки та іншими системними документами, які містять у собі копії чи ескізи даних користувача.

3.3.Основні поняття криптографії. Шифрування та маскування даних.

Криптографія – наука про математичні методи забезпечення конфіденційності, цілісності та автентичності інформації. виникла з практичної потреби передавати важливі відомості найнадійнішим чином. Тривалий час під

криптографією розумілось лише шифрування – процес перетворення звичайної інформації в абстрактні конструкції.

Відкритий (вихідний) текст – дані (не обов'язково текстові), що передаються без використання криптографії.

Шифротекст, шифрований (закритий) текст – дані, отримані після застосування криптосистеми (зазвичай – з деяким ключем).

Ключ – параметр шифру, що визначає вибір конкретного перетворення даного тексту.

Шифр, криптосистема – сімейство оборотних перетворень відкритого тексту в шифрований.

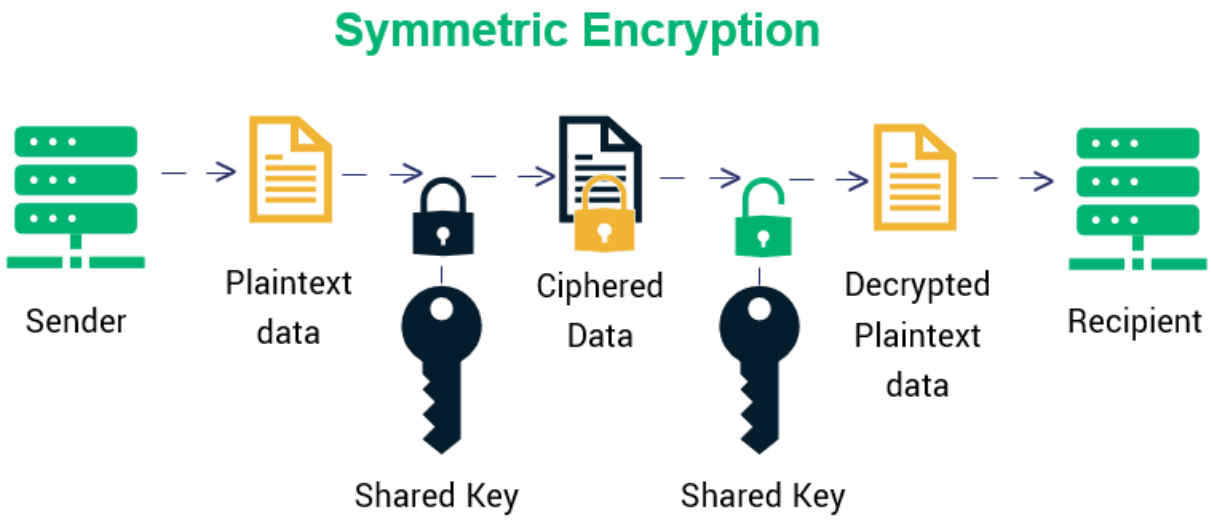
Шифрування – процес нормального застосування криптографічного перетворення відкритого тексту на основі алгоритму та ключа, в результаті якого виникає шифрований текст. Розшифрування – процес нормального застосування криптографічного перетворення шифрованого тексту у відкритий.

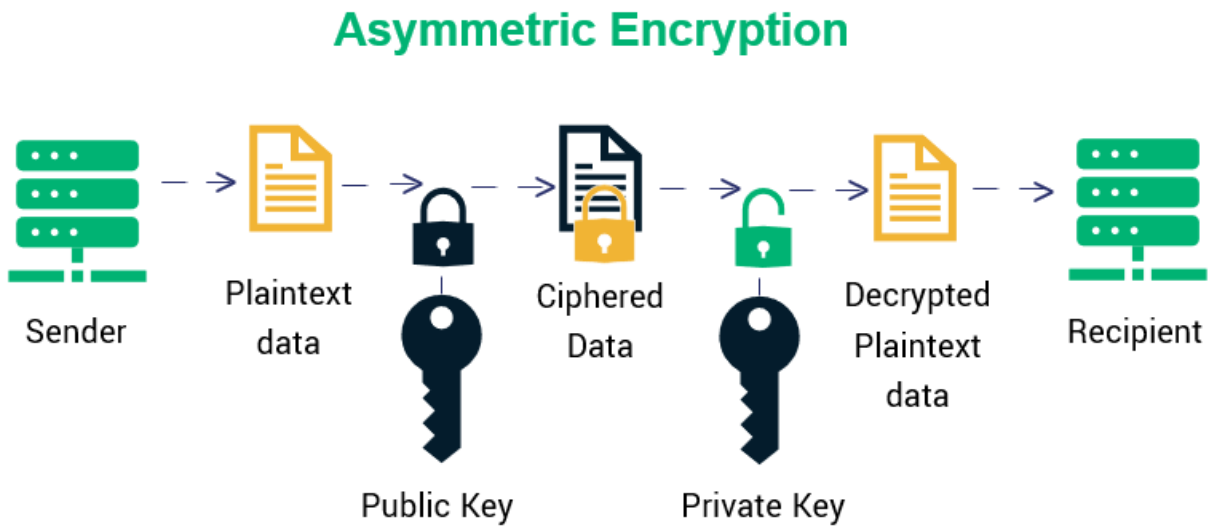
В симетричних криптосистемах для шифрування та розшифровуння інформації використовується один і той же загальний секретний ключ, яким взаємодіючі сторони заздалегідь обмінюються по деякому захищеному каналу.

Асиметричні криптосистеми характерні тим, що в них використовуються різні ключі для шифрування та розшифровуння інформації:

- закритий ключ (private key) – ключ, що відомий лише своєму власнику, одержувач, будучи монопольним власником закритого ключа (для розшифровування), буде єдиним, хто зможе розшифрувати призначені для нього повідомлення;

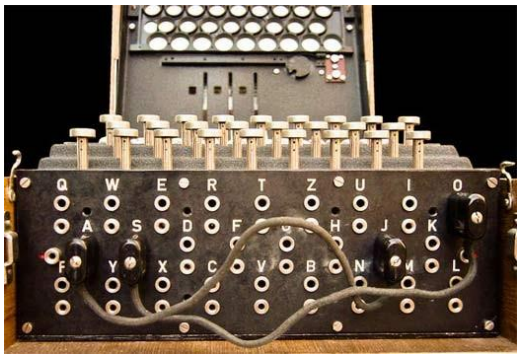
- відкритий ключ (public key) – ключ, який є загальнодоступним, будь-хто може зашифровувати повідомлення для певного одержувача.





Головна властивість ключової пари: по закритому ключу легко обчислюється відкритий ключ, але, маючи відкритий ключ практично неможливо вирахувати закритий ключ.

В алгоритмах, що використовуються для реалізації цифрового підпису ролі закритого та відкритого ключів змінюються на протилежні: візування електронного документа відбувається приватним ключем автора документа, а перевіряється загальнодоступним публічним ключем. Таким чином будь-хто може перевірити достовірність авторства певної особи. Таким чином, асиметричні алгоритми, можуть забезпечувати не тільки конфіденційності та цілісності інформації, але і її автентичність.



Зазвичай пакети офісних програм (зокрема, Microsoft Office, LibreOffice) мають засоби для захисту текстових документів, електронних таблиць, презентацій тощо шляхом шифрування. В залежності від цілей користувача, передбачено захист файлу від відкриття чи захист від редагування. В останньому випадку передбачаються такі ступені захисту:

- лише перегляд змісту;
- заборона змін, окрім коментарів;
- фіксування записи виправлень – внесення змін дозволено, але вони фіксуються і можуть бути скасовані автором;
- дозвіл введення даних тільки в поля форм (у вибіркові розділи документа).

Утілити-архіватори та програми перегляду файлів формату pdf також можуть встановлювати парольний захист на відкриття чи редагування документів.

Можна скористатися й онлайн-сервісами для встановлення парольного захисту документів.

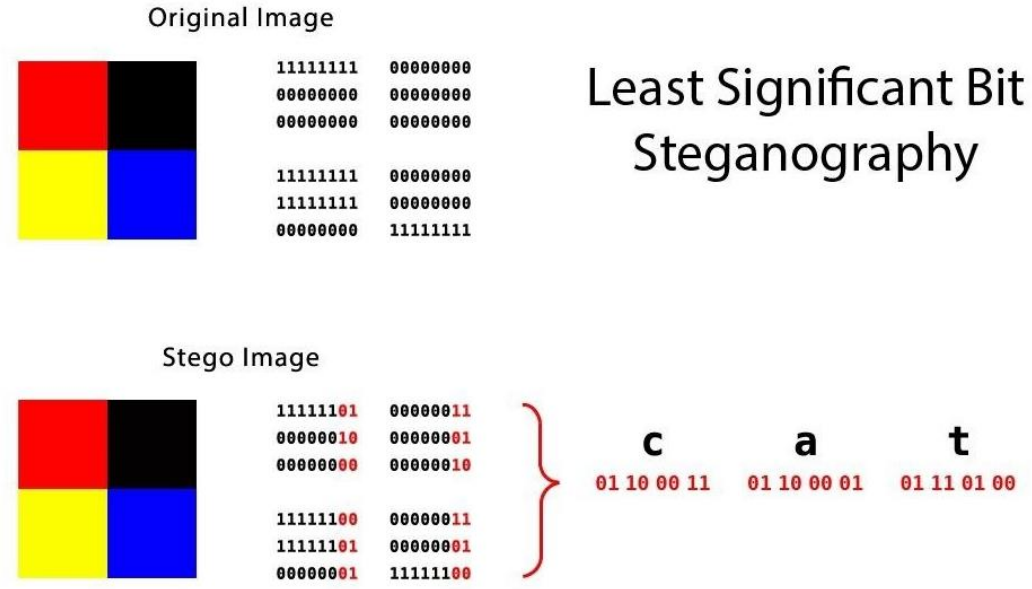
Важливо: такий захист є не дуже надійним й може бути скасований, в окремих випадках, навіть без застосування спеціальних інструментів.

При виборі програми для шифрування файлів та дисків доцільно обрати ту, яка існує вже багато років, поширюється у вигляді вихідних текстів, використовує стійкі алгоритми, коректно їх реалізує, причому ця реалізація була проаналізована кількома незалежними фахівцями з криптографії. Наприклад, Encrypto, VeraCrypt AxCrypt.

Стеганографія – це наука про приховану передачу інформації шляхом збереження в таємниці самого факту передачі. На відміну від криптографічного захисту, коли у зловмисника існує можливість знайти, перехопити та зробити спробу дешифрувати криптограму, стеганографічні методи дозволяють вмонтувати інформацію, що передається, в невинні на вигляд послання так, щоб не можна було навіть запідозрити існування підтексту.

Шанси знайти приховане повідомлення невеликі, але на той випадок, якщо повідомлення буде виявлено, його можна ще додатково зашифрувати. У цьому випадку стеганографія являє собою більш високий рівень захисту інформації в порівнянні з методами криптографії.

Науково-технічний прогрес дозволив стеганографії зайняти певну нішу у галузі захисту інформації, з'явився такий напрям в області захисту інформації, як комп'ютерна стеганографія. Комп'ютерна стеганографія, враховуючи природні неточності пристроїв дискретизації і надмірність аналогового відео або аудіо сигналу, дозволяє приховувати повідомлення в комп'ютерних файлах (контейнерах, наприклад, зображення чи звуковий файл – у файлі WAV, MP3 або у відео файлі).



Також треба зазначити, що без спеціальних засобів збережену інформацію не можливо отримати із файла-контейнера.

У сучасному інформаційному просторі стеганографічні системи активно використовуються для вирішення таких основних завдань:

1) захист конфіденційної інформації від несанкціонованого доступу;

2) подолання систем моніторингу та управління мережевими ресурсами;

3) камуфлювання програмного забезпечення;

4) захист авторського права на деякі види інтелектуальної власності.

Стеганографічні методи також спрямовані на протидію системам моніторингу та управління мережевими ресурсами промислового шпигунства, дозволяють протистояти спробам контролю над інформаційним простором при проходженні інформації через сервери керування локальних і глобальних обчислювальних мереж. Для корпорацій та державних відомств, що зберігають важливі масиви даних, це одна із неоціненних функції стеганографії.

Іншим важливим завданням стеганографії є камуфлювання програмного забезпечення. У тих випадках, коли використання ПЗ незареєстрованими користувачами є небажаним, воно може бути закамуфльовано під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховано в файлах мультимедіа (наприклад, у звуковому супроводі комп’ютерних ігор).

Прикладом використання стеганографії у захисті авторського права від піратства є нанесення спеціальної мітки на комп’ютерні графічні зображення. Мітка залишається невидимою для очей людини, але розпізнається спеціальним ПЗ, яке вже використовується в комп’ютерних версіях деяких журналів. Даний напрямок стеганографії призначений не тільки для обробки зображень, але і для файлів з аудіо- та відео-інформацією й забезпечує захист інтелектуальної власності.

Для приховування інформації у цифровому вигляді за допомогою стеганографії існують спеціальні алгоритми. Внесення нової інформації у вже наявні файли (наприклад, мультимедійні) призводить до спотворенн, які перебувають нижче порогу чутливості людини, тому це не викликає помітних змін у сприйнятті вхідних файлів.

На тепер найбільш поширеним, але найменш стійким є метод заміни найменших значущих бітів або LSB-метод (Least Significant Bit, найменший значущий біт). Він полягає у використанні похибки дискретизації, яка завжди існує в оцифрованих зображеннях, аудіо– або відеофайлах. Дана похибка дорівнює найменшому значущому розряду числа, що визначає величину колірної складової елемента зображення (пікселя). Тому модифікація молодших бітів в більшості випадків не викликає значної трансформації зображення і не виявляється візуально. Так, наприклад, одна секунда оцифрованого звуку з частотою дискретизації 44100Гц та 8-бітним рівнем відліку у стереорежимі дозволяє приховати за рахунок зміни найменш значимих молодших розрядів повідомлення у 10 Кбайт.

Іншим популярним методом вбудовування повідомлень є використання особливостей форматів даних із стисненням з втратою даних (наприклад JPEG). Цей метод (на відміну від LSB) більш стійкий до геометричних перетворень і виявленню при передачі, так як є можливість в широкому діапазоні варіювати якість стислого зображення, що робить неможливим визначення походження спотворення.

При побудові стегосистеми необхідно враховувати:

1) зловмисник має повне уявлення про стегосистему і деталі її реалізації, єдиною інформацією, яка залишається невідомою, є ключ, за допомогою якого тільки його власник може встановити факт наявності і зміст прихованого повідомлення;

2) якщо зловмисник якимось чином дізнається про факт існування прихованого повідомлення, це не повинно дозволити йому отримати подібні повідомлення в інших даних до тих пір, доки ключ зберігається у таємниці;

3) потенційний зловмисник повинен бути позбавлений будь-яких технічних та інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

У якості контейнера (повідомлення) може використовуватися будь-яка інформація призначена для приховування таємних повідомлень.

Повідомленням може бути як текст або зображення, так і, наприклад, аудіодані (файли мультимедіа) тощо. Порожній контейнер – контейнер без вбудованого повідомлення; заповнений контейнер (стег) – контейнер, що містить вбудовану інформацію. Вбудоване (приховане) повідомлення – повідомлення, яке вбудовується в контейнер. Стеганографічний канал або просто стегоканал – канал передачі стег. Стегоключ або просто ключ – секретний ключ, необхідний для приховування інформації. В залежності від кількості рівнів захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) в стегосистеми може бути один або декілька стегоключів.

За аналогією з криптографією, за типом стегоключа стегосистеми можна поділити на системи з секретним ключем та системи з відкритим ключем.

Отже, стегосистема має відповідати таким вимогам:

1) властивості контейнера повинні бути модифіковані таким чином, щоб зміни неможливо було виявити при візуальному контролі, що визначає якість приховування повідомлення (для безперешкодного проходження стегоповідомлення каналами зв’язку воно не повинно привернути увагу);

2) стегоповідомлення повинно бути стійким до спотворень, в тому числі і до зловмисних (у процесі передачі зображення, звука або використання інших контейнерів можуть відбуватися різні трансформації зі зменшення або збільшення, перетворення в інший формат, ущільнення, в тому числі і з використанням алгоритмів з втратою даних тощо);

3) для збереження цілісності вбудованого повідомлення необхідно використовувати коди з виправленням помилок;

4) для підвищення надійності вбудоване повідомлення має бути продубльовано.

ЛАБОРАТОРНА РОБОТА №3. ЗАХИСТ ДАНИХ.

Мета вивчення: формування вмінь і навиків захисту офісних документів від ненавмисних пошкоджень та несанкціонованого доступу. Отримання знань щодо методів й способів подолання парольного захисту та навиків використання відповідного програмного забезпечення. Формування вмінь і навиків відновлення втрачених даних та безпечного видалення інформації.

Обсяг навчального часу: 4 години.

Обладнання: комп'ютер (планшет, смартфон), зйомний диск, наявність підключення до мережі Інтернет.

План заняття:

1. Дослідження захищеного хмарного сховища Mega для резервного копіювання.
2. Захист паролем архівів, текстових документів та pdf, електронних таблиць.
3. Подолання парольного захисту.
4. Відновлення втрачених даних.
5. видалення даних без можливості відновлення.

Інформаційні джерела:

підтримка Mega: https://mega.io/help;

огляд сховища Mega:

- https://www.youtube.com/watch?v=v09UAmsXZeA,
- https://www.youtube.com/watch?v=wrer5w7GOFE;

посібник для самостійного вивчення LibreOffice:

http://lpk.ucoz.ua/Informatika/LibreOfficee_posibnik_ua.pdf;

документація та підтримка LibreOfficee:

- https://documentation.libreoffice.org/en/english-documentation/,
- https://help.libreoffice.org/6.3/uk/text/shared/05/new_help.html;

сервіси відновлення втрачених паролів:

- https://www.lostmypass.com,

- https://www.password-find.com/.

ЗАВДАННЯ:

1.1. Створить акаунт в хмарному сервісі Mega. Створить на Вашому диску Мега папку «Документи».

1.2. Завантажте зі жорсткого диску (змінного носія) текстовий документ, деяке зображення на диск Мега. Перемістить документ з кореневого каталогу диску до папки «Документи», копію рисунку також розташуйте в папці «Документи». видаліть будь-який файл з Вашого диску Мега.

1.3. Надайте доступ до будь-якого з файлів Вашого диску Мега іншому користувачу за допомогою ключа доступу.

2.1. Створіть захищений шифром AES архів.

2.2. Створіть захищений від відкриття документ LibreOffice.

2.3. Обмежте доступ до текстового документу LibreOffice: відкривати лише для читання та записувати зміни.

2.4. Експортуйте документ LibreOffice у формат pdf та встановіть захист отриманого файлу.

2.5. Встановіть захист від редагування декількох абзаців у текстовому документі. Встановіть захист від редагування певних комірок електронних таблиць.

3. Захистить слабким паролем деякий офісний документ чи архів та спробуйте відновити пароль за допомогою онлайн-сервісів.

4.1. На зйомному носії створіть папку, яка містить декілька офісних документів, файл із зображенням (фото, малюнок), архів із цими файлами та вкладену папку, яка також містить зазначені файли.

4.2. Знищить папку разом із усіма даними та спробуйте відновити. Перевірте якість відновлення.

5.1. Створить на зйомному диску папку та налаштуйте програму Ccleaner на видалення інформації з неї без можливості відновлення. видаліть вміст цієї папки.

5.2. Спробуйте відновити видалені файли.

5.3. виконайте стирання вільного простору на зйомному диску. Якщо час виконання перевищує 5 хвилин, відмініть операцію.

ВИМОГИ ДО ЗВІТУ:

1. Скрін екрану під час роботи зі сховищем Mega.

2. Завантажити зразки наступних файлів:

захищений шифром AES архів;

текстовий документ, який можна відкривати лише для читання;

електронну таблицю, в якій перший стовпчик містить Ваше прізвище та назву факультету й яку захищено від редагування.

3. Скрін екрану з результатами відновлення паролю за допомогою онлайн-сервісів.

4. Скрін екрану із результатами відновлення видалених файлів.

5. Скрін екрану з увімкненою програмою для знищення даних.

ХІД РОБОТИ.

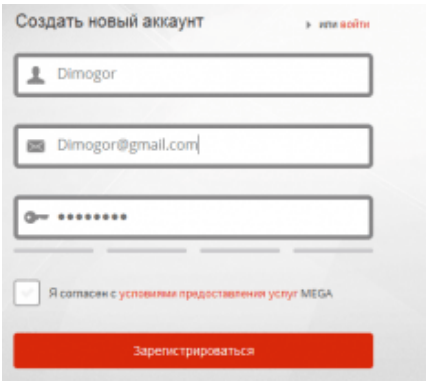
1. Хмарний сервіс Mega (mega.io) розшифровується як «MEGA Encrypted Global Access» (зашифрований глобальний доступ) – це безпечне хмарне сховища, яке вигідно відрізняється від більшості подібних сервісів використанням так званої «Політики нульового доступу». Згідно з цим принципом всі дані між клієнтським пристроєм і комп'ютером передаються по захищеному протоколу. Для отримання доступу до об'єктів в «хмарі» потрібно мати криптографічний ключ. Без нього відкрити файл не зможуть ні розробники сервісу, ні спецслужби – це виключено логікою роботи сховища. MEGA також надає вам можливість використовувати 2-факторну автентифікацію.

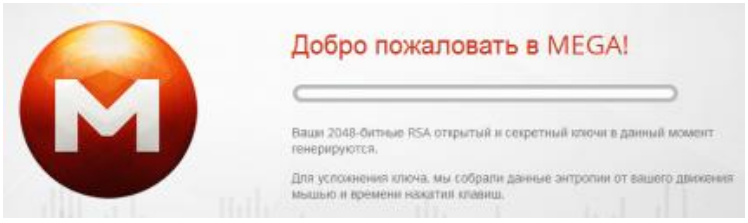
Ще одна перевага Мега – це досить великий обсяг простору, що виділяється безкоштовно – 20 гігабайт. Збільшити місце на диску можна за додаткову плату.

Серед інших особливостей – інтегрований чат, адресна книга, автоматична синхронізація об’єктів, стиснення файлів в архів перед скачуванням, інтеграція в провідник і можливість використання proxy-сервера. Найбільший інтерес представляє опція генерування посилань, саме тому Mega часто виступає в ролі файлообмінника з функцією «прямих» URL для скачування файлів.

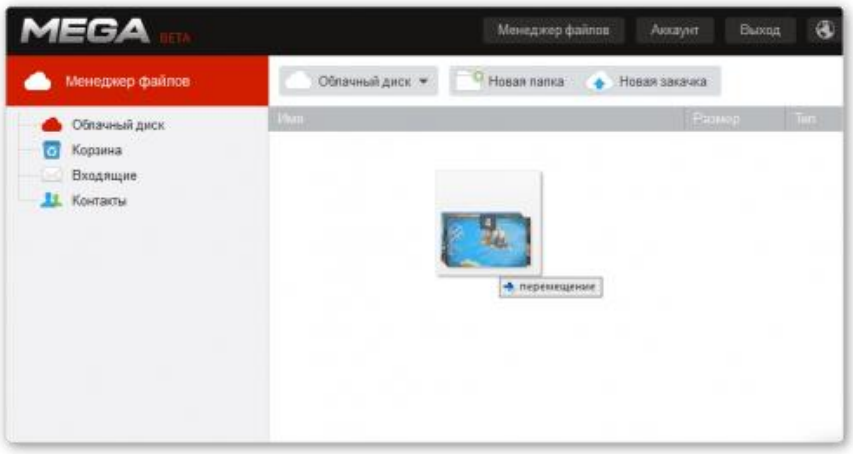
При завантаженні даних в сховищі всі файли шифруються в браузері за допомогою алгоритму AES і зберігаються на сервері в зашифрованому вигляді. Окрім того, Mega не зберігає паролі. Вони належать лише користувачеві й не можуть бути відновлені в компанії. Якщо ви забули пароль, єдиний спосіб відновити його – мати майстер ключ Mega.

Для початку роботи необхідно зареєструватися. Для цього потрібно вказати своє ім’я, поштову адресу та пароль.



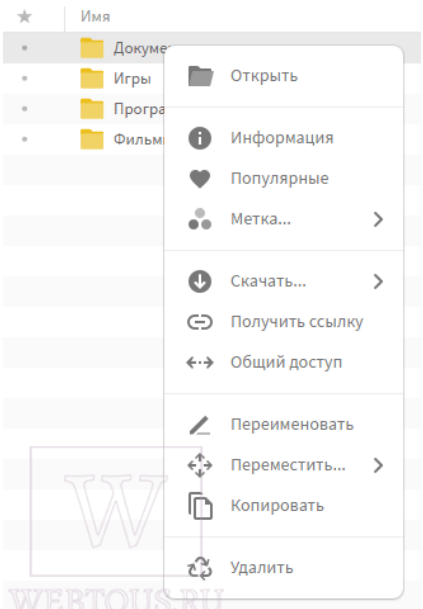


Після закінчення реєстрації вам надішлють посилання для входу на вказану вами адресу електронної пошти.



Далі потрапляємо в хмарне сховище – ліворуч дерево папок, по центру область відображення файлів, зверху панель інструментів. За допомогою інструментів у верхній частині вікна можна створювати нові папки та завантажувати з комп'ютера папки з файлами. Клік правою кнопкою миші на папці або файлі викликає контекстне меню з цілим набором можливостей.

З його допомогою можна: отримувати інформацію про елемент (розмір, дата створення тощо); призначати кольорові мітки та додавати до Обраного; перейменовувати; переміщувати в межах диска, копіювати, видаляти; завантажувати файли; відкривати спільний доступ до папок; створювати публічне посилання на скачування файлів. Файли можна організувати в папки. Переміщення файлів між папками проводиться перетягуванням або за допомогою контекстного меню. Рівень вкладеності каталогів не обмежений.

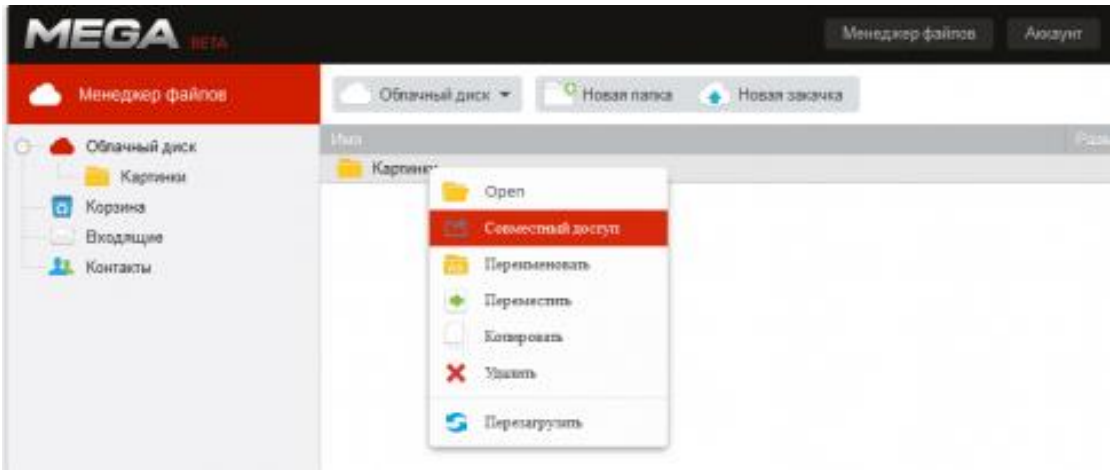


До будь-якої папки у своєму онлайн сховищі ви можете організувати спільний доступ (розшарити її). Для цього:

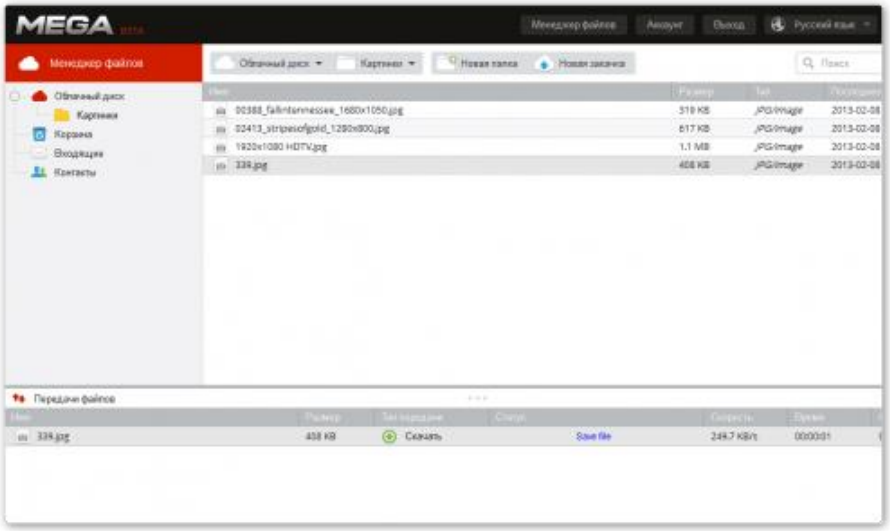
1. Клацніть на ній правою клавішею миші і в контекстному меню виберіть опцію «Загальний доступ».

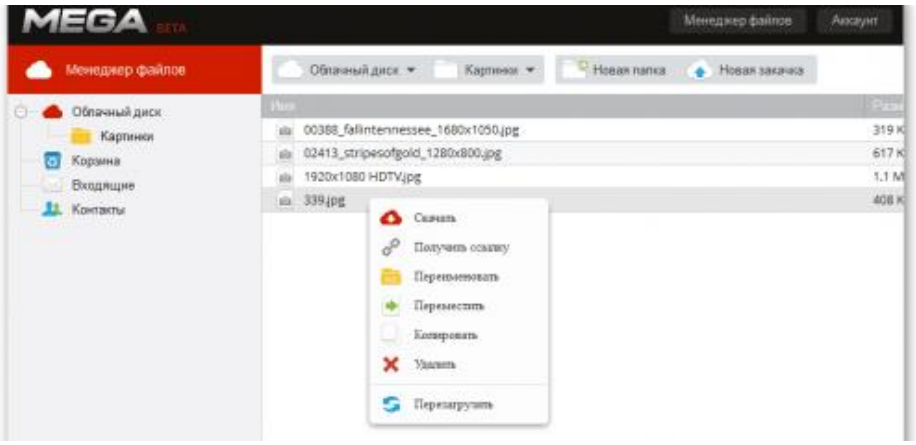
2. Вкажіть адресу електронної пошти користувача, якому потрібно надати доступ до папки (можна відразу вказати цілий список користувачів).

3. Оберіть спосіб доступу: лише для читання, читання та запис або повний доступ.

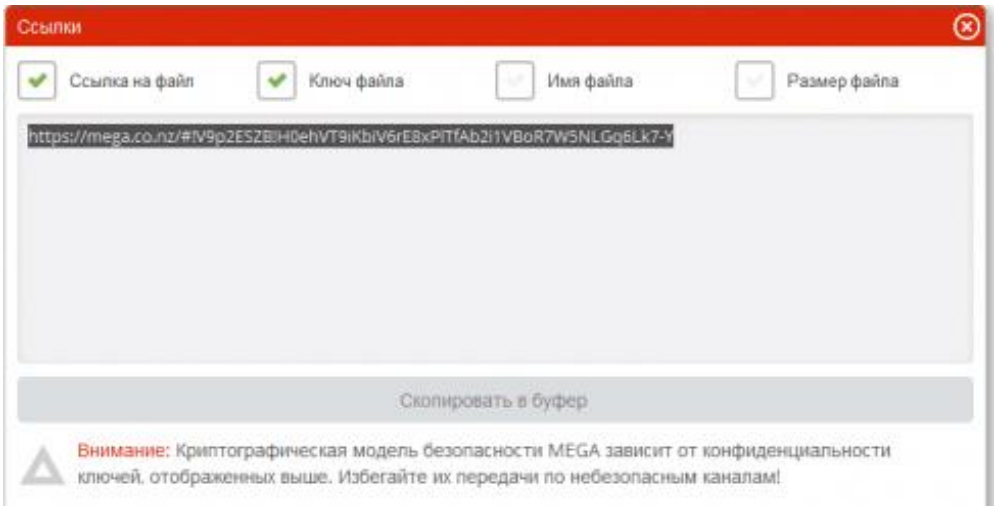


Після цього вказаному користувачеві на електронну пошту прийде лист із посиланням для доступу до розшарованої папки.

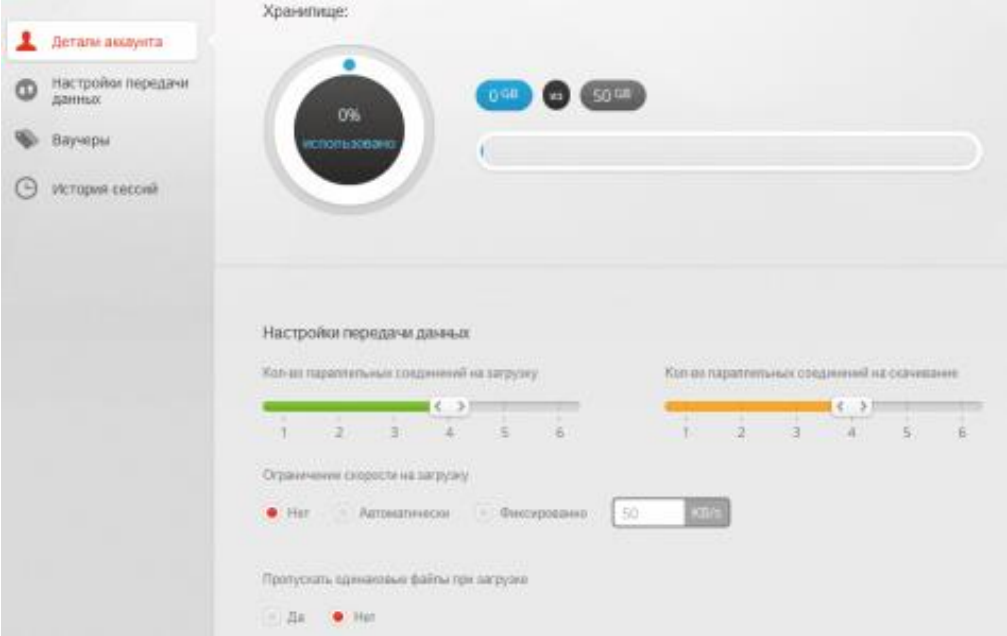




Існує можливість надати спільний доступ й до окремих файлів. У спливаючому вікні генерується посилання для скачування файлу. Зверніть увагу на опції у верхній частині цього вікна. Якщо включено тільки «Посилання на файл», то Ваш абонент не зможе завантажити файл без введення спеціального пароля, який ви можете вислати йому окремо. Таким чином, можна публікувати посилання на скачування в загальнодоступних місцях але дозволяти завантажувати лише певним особам. Якщо ж додатково відзначено «Ключ файлу», то за створеним посиланням файл зможе завантажити будь хто.

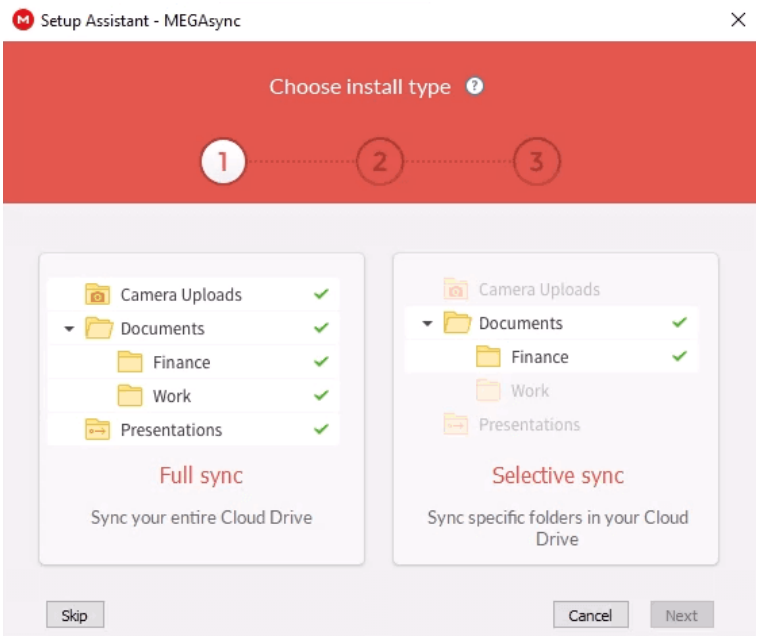


В розділі аккаунт можна переглянути кількість зайнятого міста у сховищі, купити додаткове місце, змінити налаштування передачі даних тощо.



Хмарне сховище Mega, крім роботи в браузері, надає декстопні версії програми для Windows, Mac і Linux, а також мобільні версії програми для Android та Iphone. Коли ви вносите зміни у файли локально на своєму комп'ютері, ці зміни синхронізуються з файлами у вашому хмарному сховищі MEGA.

ви можете синхронізувати або весь хмарний диск, або окремі папки. Надалі можна змінити ці папки або додати інші. У вкладці « Просунуті» можна змінити папки завантаження та завантаження за замовчуванням, а також виключити імена файлів та папок із синхронізації. Можна також виключити за розміром файлів.



Наприклад, можна виключити тимчасові файли або файли відео, які зазвичай займають багато дискового простору.

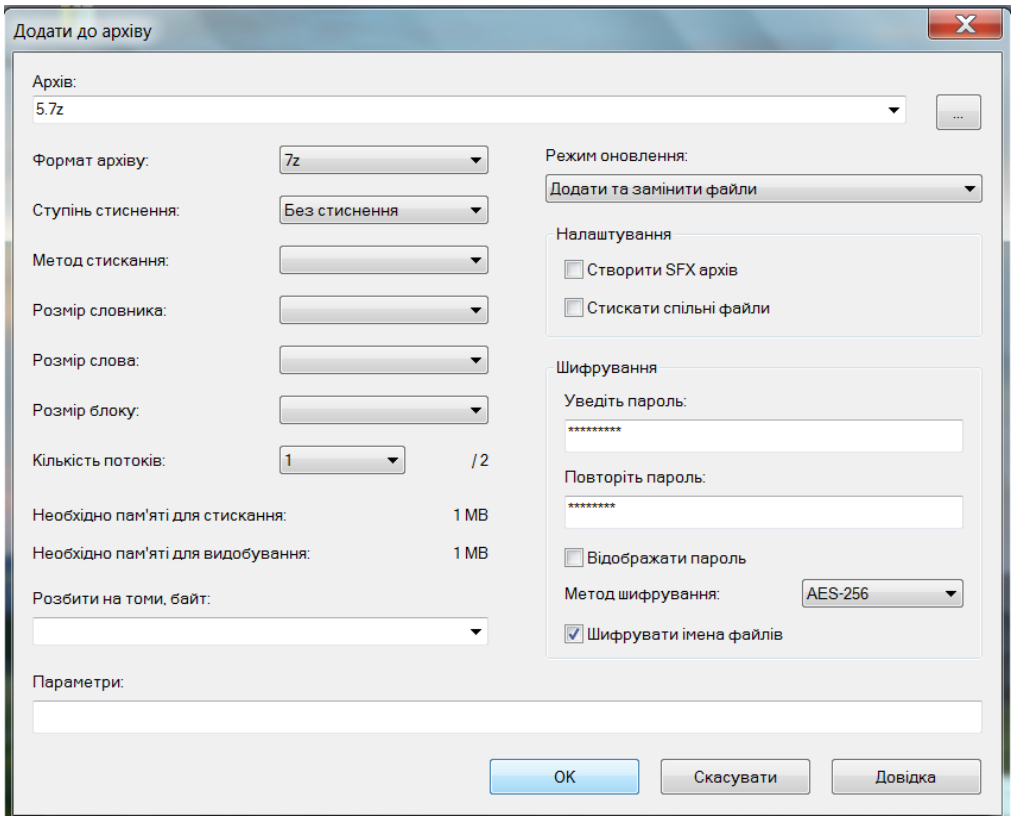
Окремий файл можна завантажити на Mega, просто натиснувши файл у провіднику Windows правою кнопкою миші і вибравши в контекстному меню «Завантажити на MEGA». І навпаки, завантажити файл із хмари MEGA можна, клацнувши по значку MEGAsync в треї правою кнопкою миші і вибравши в контекстному меню «завантажити».

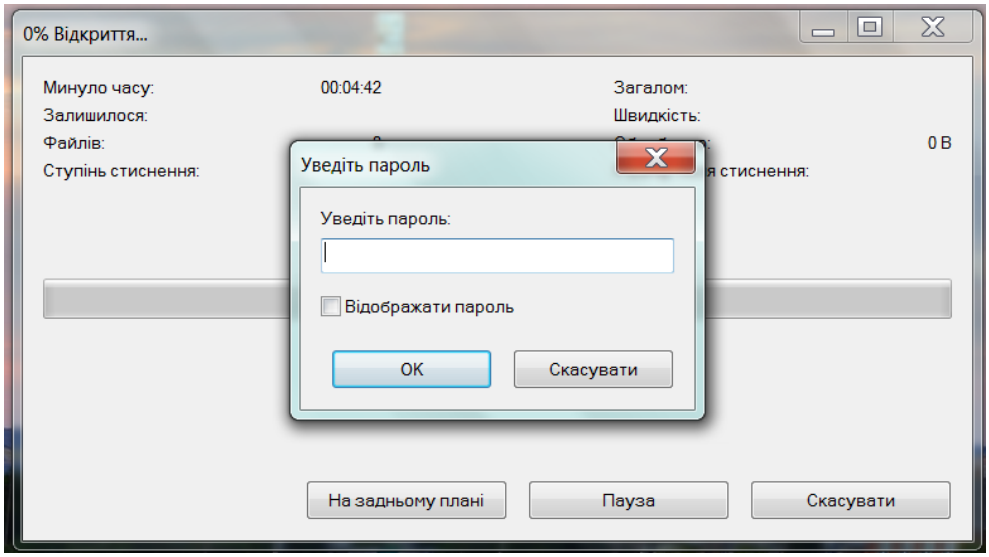
2. Захист паролем архівів, pdf / текстових документів / електронних таблиць.

Безкоштовний архіватор 7-Zip дозволяє створити захищений шифром AES архів. Процес є однаковим для файлу чи папки. Для створення зашифрованого архіву необхідно викликати контекстне меню та обрати пункти «7-Zip» – «створити архів».

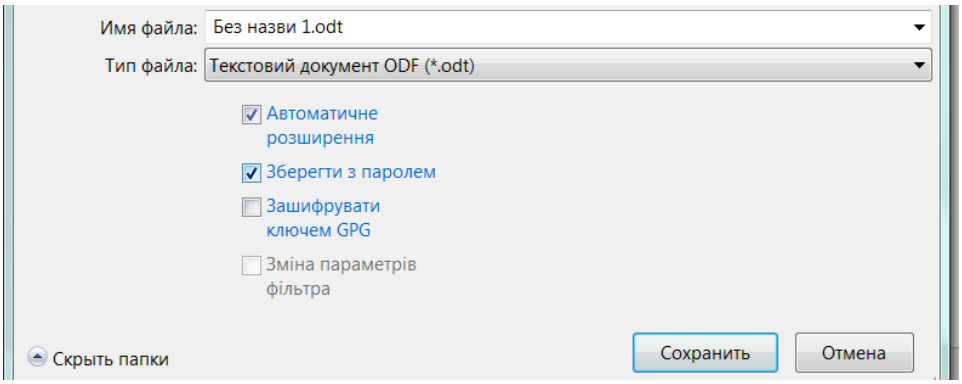
Далі ви вказуєте пароль, доцільно відмітити пункт «шифрувати імена файлів». Якщо ви маєте на меті лише захистити дані, оберіть пункт «без стиснення» – це прискорить процес створення архіву чи його розпакування, особливо для великих обсягів інформації.

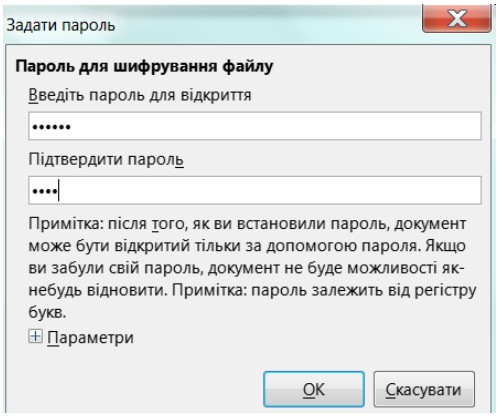
Варто подумати, чи не приверне ім’я архіву зайвої уваги. видаліть оригінальний файл чи папку, які ви захистили шифруванням, та подбайте про надійне видалення.



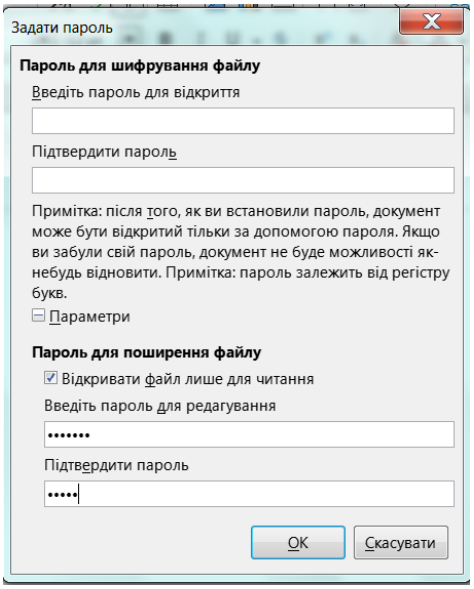


Розглянемо шифрування офісних документів на прикладі вільного пакету LibreOffice. Для захисту текстового документу, електронної таблиці, презентації тощо необхідно виконати команду «зберегти як», ввести ім’я та тип файлу, встановити прапорець «зберегти з паролем», ввести пароль та підтвердити його. При спробі відкрити захищений файл спливе вікно для вводу паролю.



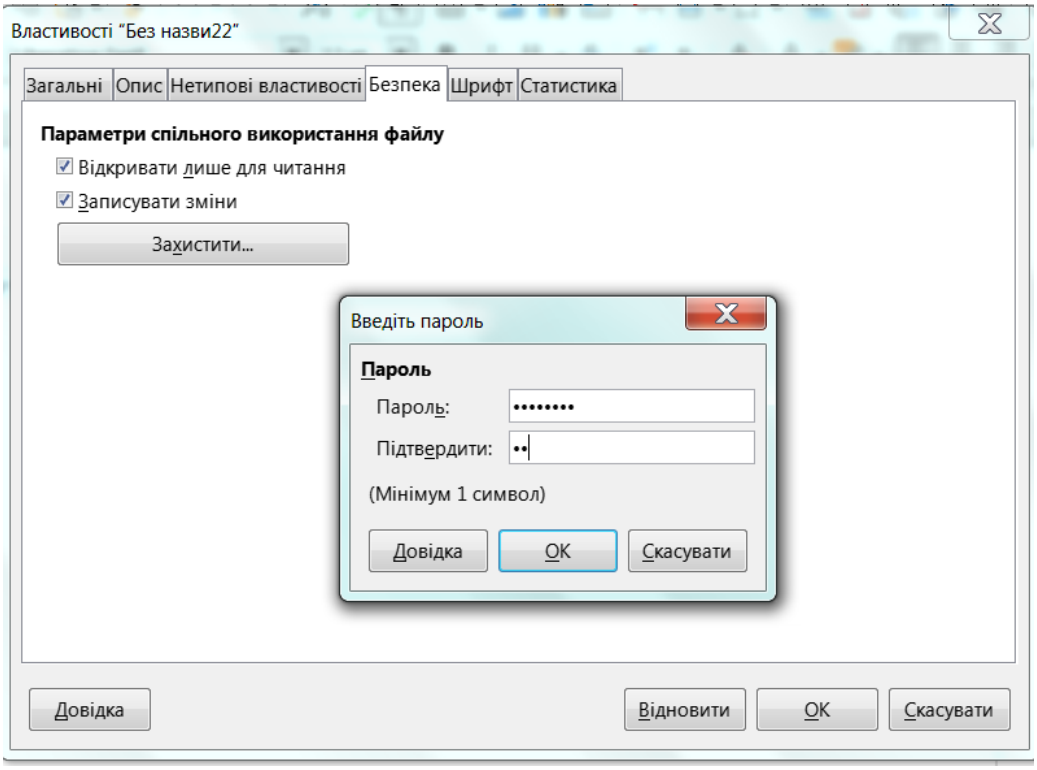


За необхідності, ви можете обмежити редагування документа, встановивши відповідні налаштування.

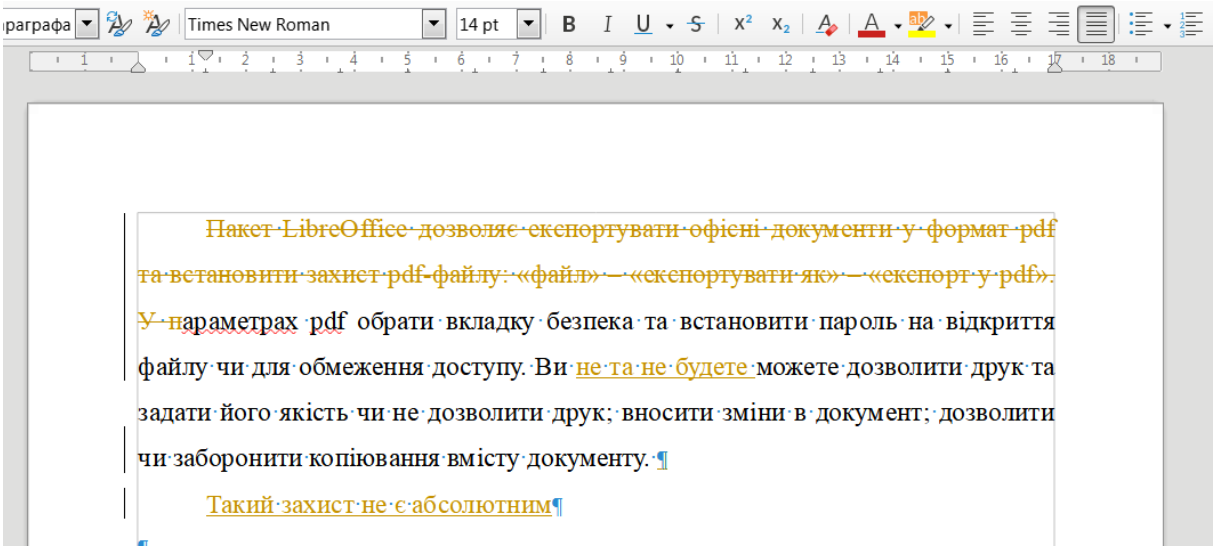


Інший варіант обмеження доступу до документів LibreOffice – встановити режими «відкривати лише для читання» та «записувати зміни». Для цього скористаємося пунктом меню «властивості» та опцією безпека, де встановимо необхідні властивості.

Увага! Режим «лише для читання» легко зняти – досить лише зберегти захищений файл за допомогою пункту меню «зберегти як». Нова версія документу буде доступна для повноцінного редагування.

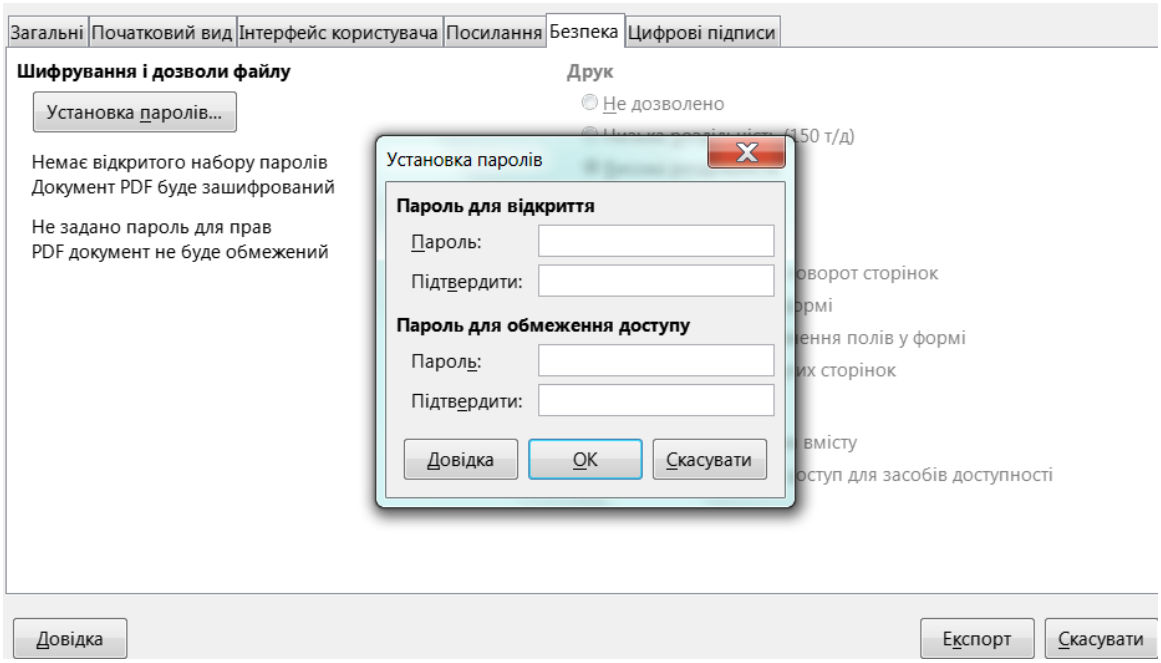


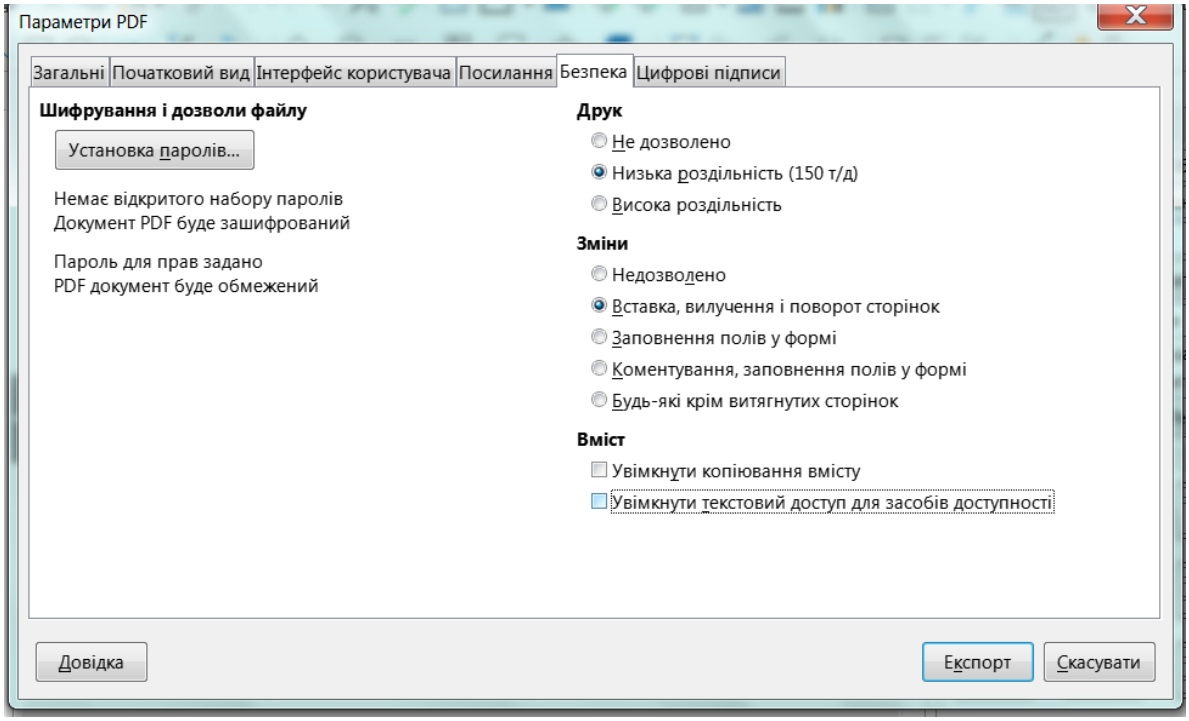
У той же час, якщо опція запису змін увімкнена, то, навіть подолав захист від редагування всі внесені правки будуть відображатися в документі.



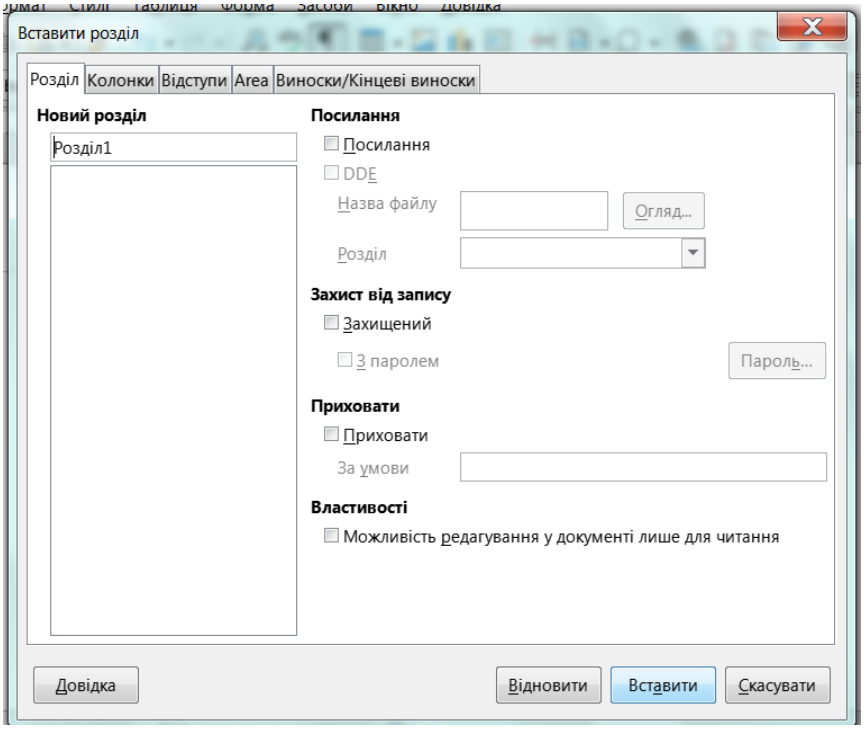
Пакет LibreOffice дозволяє експортувати офісні документи у формат pdf та встановити захист pdf-файлу: «файл» – «експортувати як» – «експорт у pdf». У параметрах pdf обрати вкладку безпека та встановити пароль на відкриття файлу чи для обмеження доступу. ви можете дозволити друк та задати його

якість чи взагалі не дозволити друк; вносити зміни в документ; дозволити чи заборонити копіювання вмісту документу.

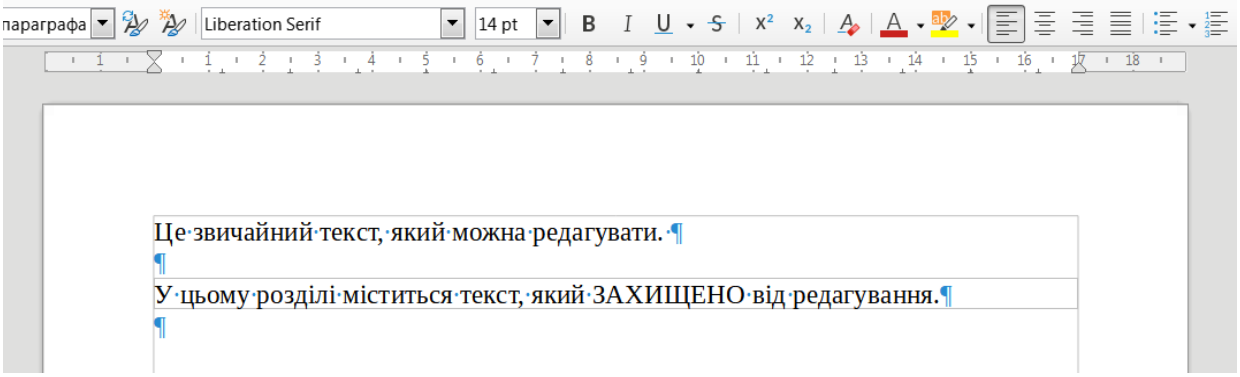




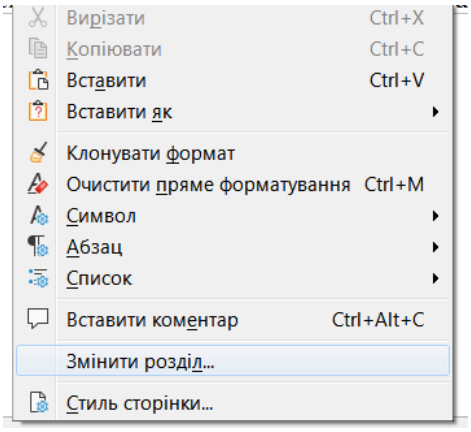
Також можна заборонити редагування певних розділів документа і навіть встановити пароль для захисту. Цей захист лише від випадкових змін файлу, він не є абсолютно надійним захистом. У LibreOffice Writer для заборони редагування файлу на рівні розділів попередньо у меню виберіть «вставка» – «розділ» та додайте новий розділ у документ.



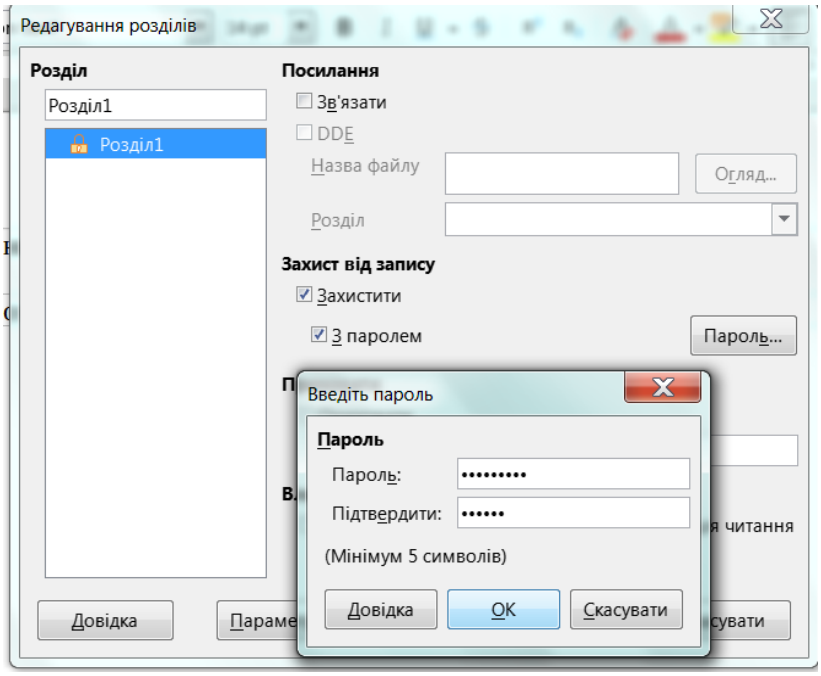
Розділ у документі буде виділений рамкою. Далі ви вводите текст, який потрібно захистити від редагування.



Після завершення роботи з захищеним тестом викликаємо контекстне меню розділу та обираємо пункт «змінити розділ».

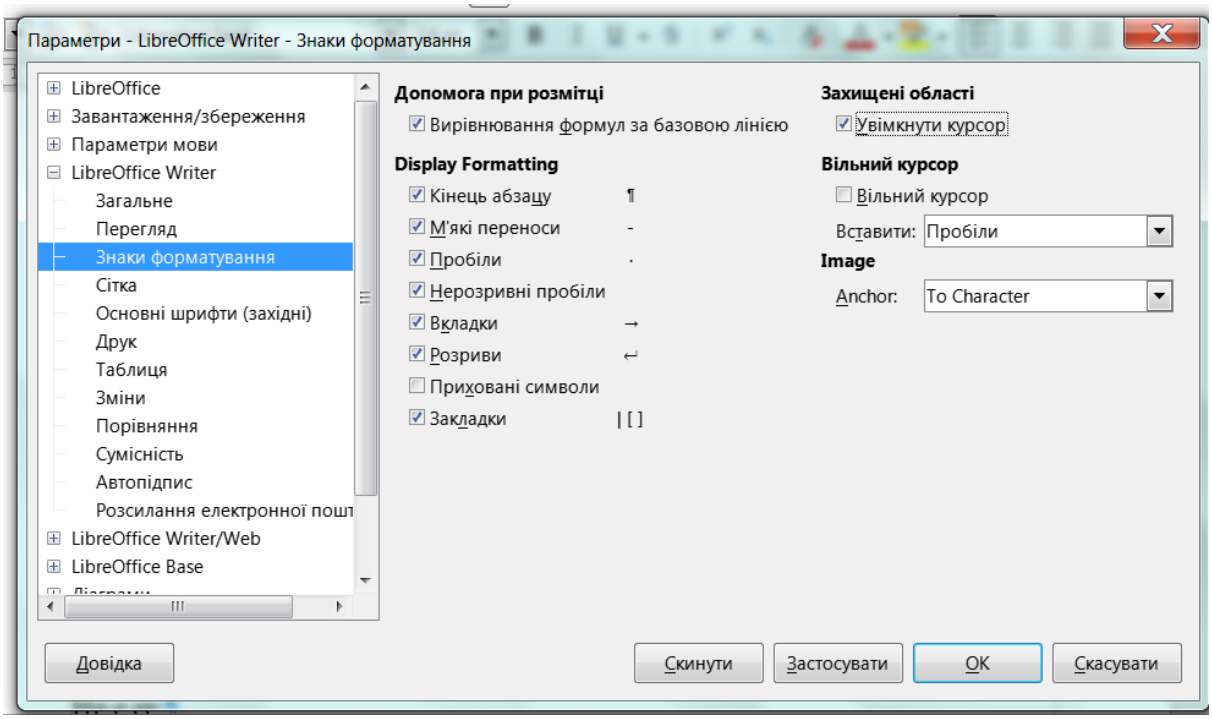


Ставимо позначку «захистити» та, за необхідності, «з паролем», вводимо пароль й зберігаємо налаштування.



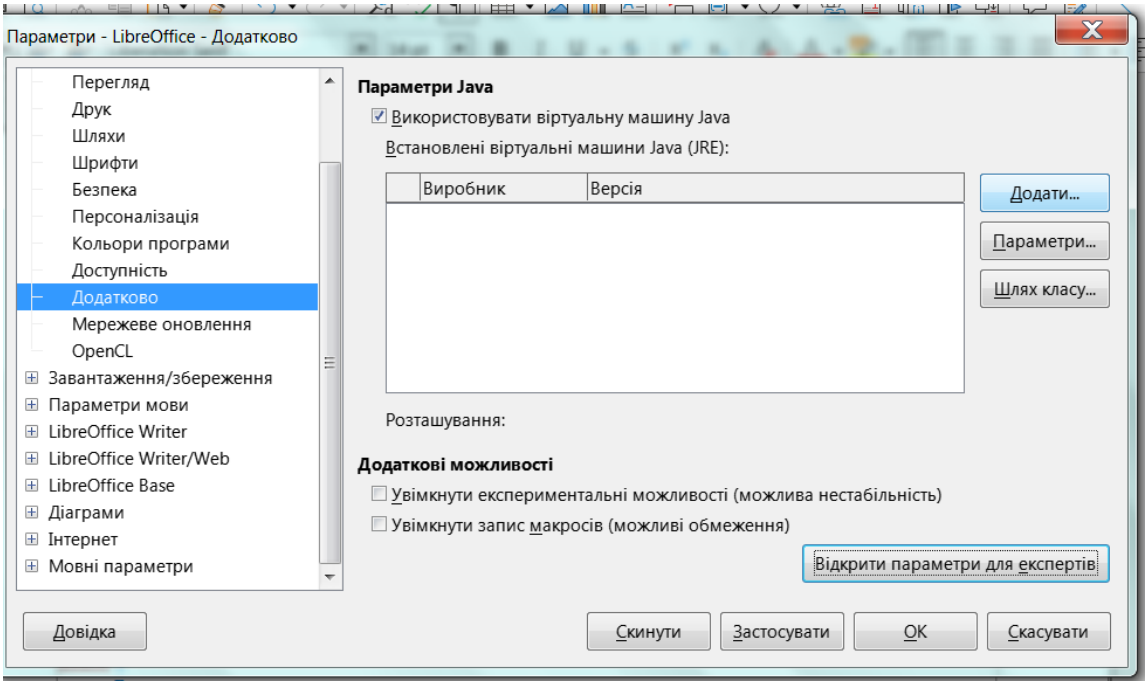
При спробі форматувати захищений розділ з'являється вікно зі сповіщенням про неможливість змінити захищений від змін вміст.

Для скасування захисту необхідно повторити налаштування й прибрати позначку «захист від запису», якщо встановлено пароль, то буде необхідно ввести його.

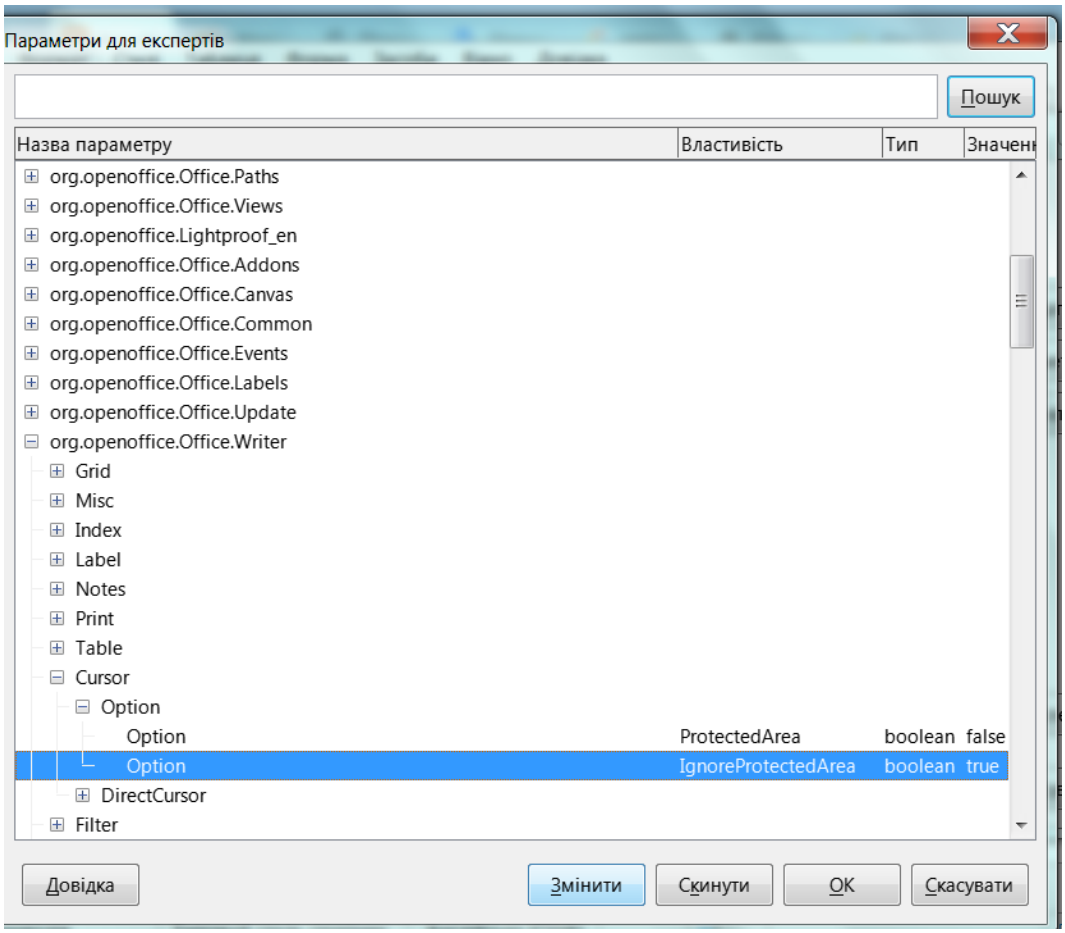


Але існує можливість змінити глобальні налаштування Writer таким чином, що захист розділів, включно з застосуванням паролю буде ігноруватися. Для цього необхідно в налаштуваннях перейти до «засоби» – «параметри» –

«додатково» – «відкрити параметри для експертів» та перейти до пункту меню «org.openoffice.Office.Writer», обрати «Cursor–Options–Ignored Protected Aria».



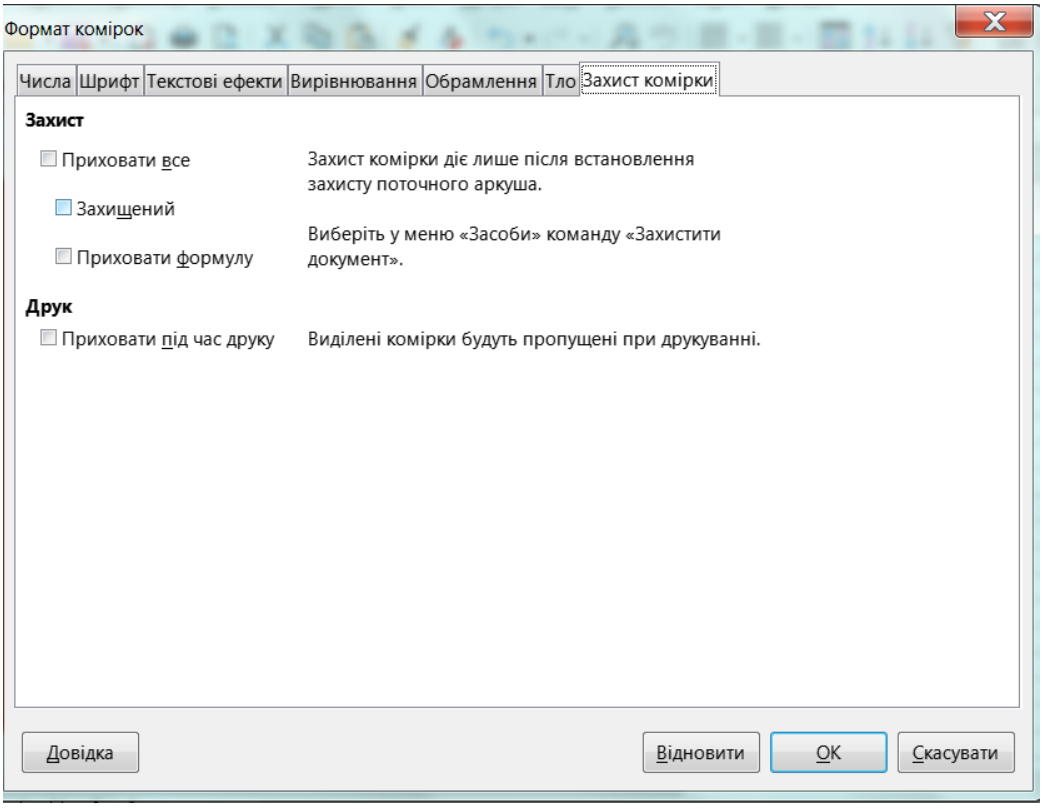
Якщо змінити значення останньої опції з false на true, то всі області, які захищенні від редагування будуть доступними для змін для всіх документів.



У процесорі електронних таблиць LibreOffice Calc можна захистити окремі аркуші чи весь документ. Налаштування надають можливість обрати захист комірок від випадкових змін, надавати чи ні дозвіл на перегляд формул, чи будуть комірки видимі, чи можуть комірки бути надруковані.

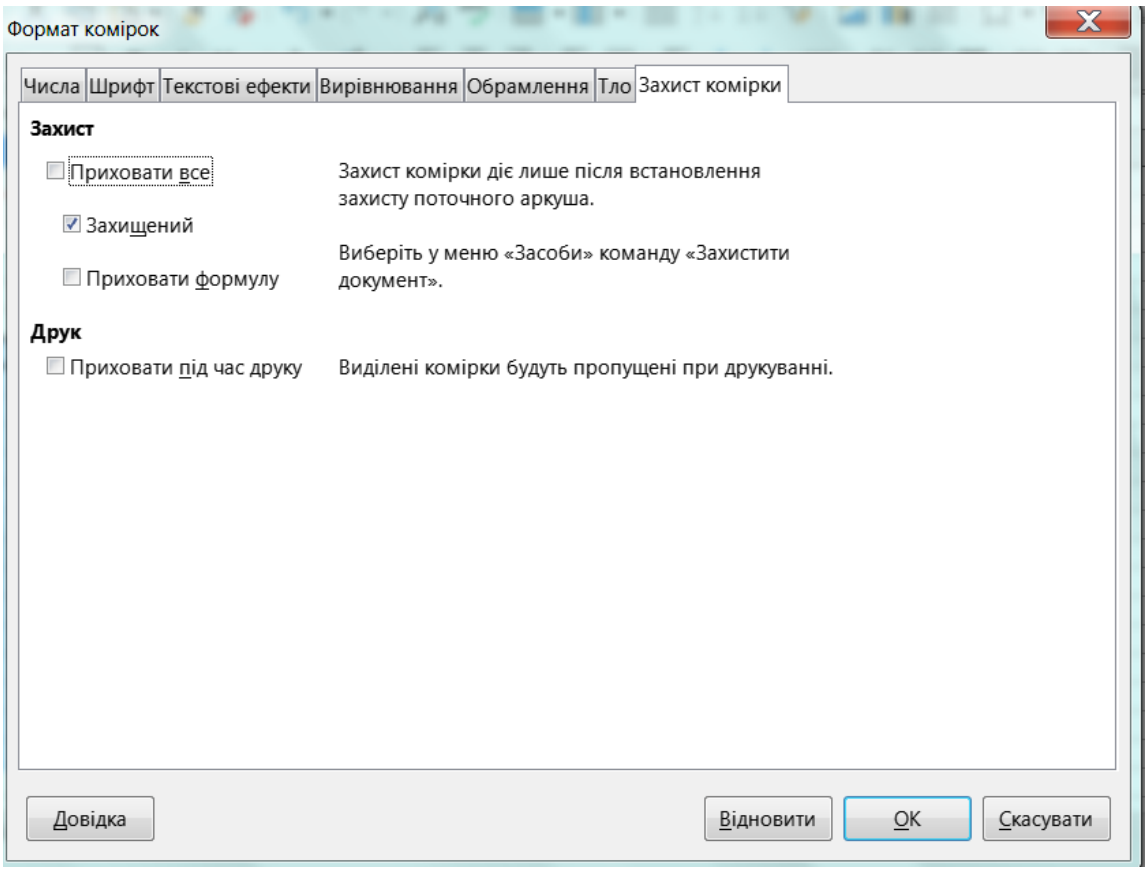
Для захисту аркушу від редагування необхідно обрати пункт меню «засоби» – «захистити аркуш». Захист може бути забезпечений паролем, але він не є обов'язковим. Для захисту від змін структури документа, наприклад, змін кількості, імен чи порядку аркушів, необхідно вибрати команду «засоби» – «захистити структуру таблиці».

Захистити окремі комірки від змін можна наступним чином. Оберіть комірки, в які можна вносити зміни та зніміть із них захист (за замовчуванням, усі комірки мають захист) «формат комірок» – «захист комірки» (через контекстне меню чи пункт меню «формат» – «комірки») – «захищений».



Для комірок, які необхідно захистити перемикач «Захищено» залиште встановленим та, за необхідності, задайте додаткові параметри захисту: приховати комірки підчас редагування; приховати формули, за якими

здійснюються розрахунки (результати роботи формул залишаються видимими); не виводити на друк зміст комірок.

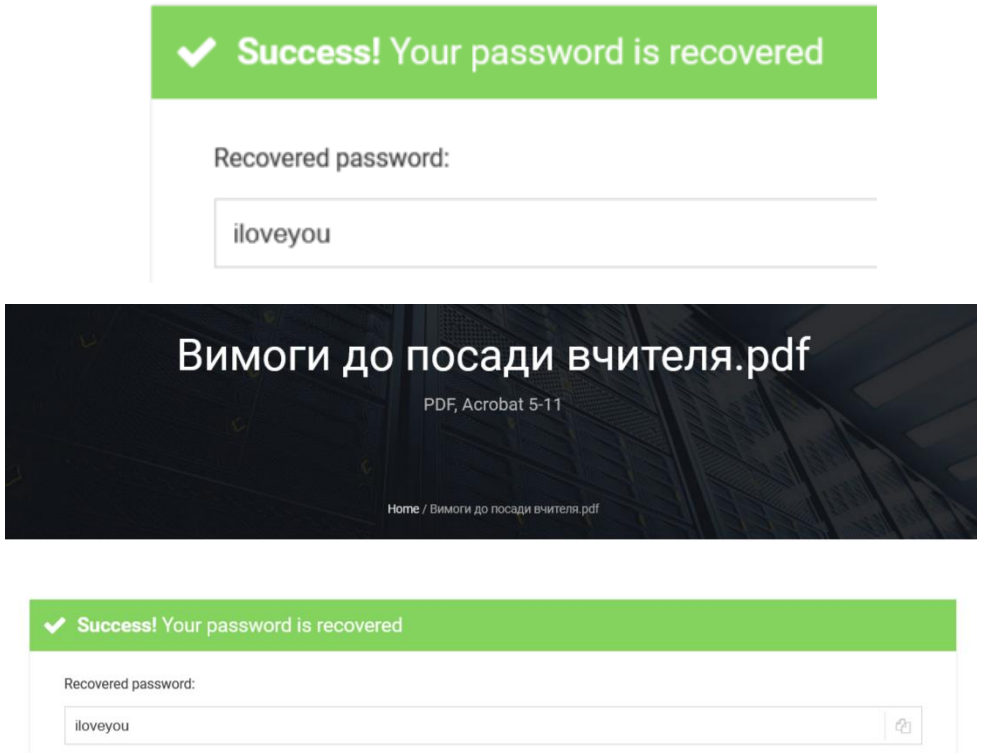


3. Подолання парольного захисту.

Якщо ви втратили пароль, який захищає офісний документ від відкриття, то за допомогою десктопних чи онлайн-сервісів можна спробувати відновити його. Наприклад, частково безкоштовний онлайн-сервіс https://www.password-find.com/ підтримує файли Word, Excel та PowerPoint.

Онлайн-сервіс https://www.lostmypass.com окрім вказаних вище типів файлів, працює також із документами pdf та популярними архівами: Zip, RAR, 7z. Пошук слабких паролів є безкоштовним – словник містить 3 мільйони слабких паролів; імовірність успіху ≈ 22%; час виконання — декілька хвилин.

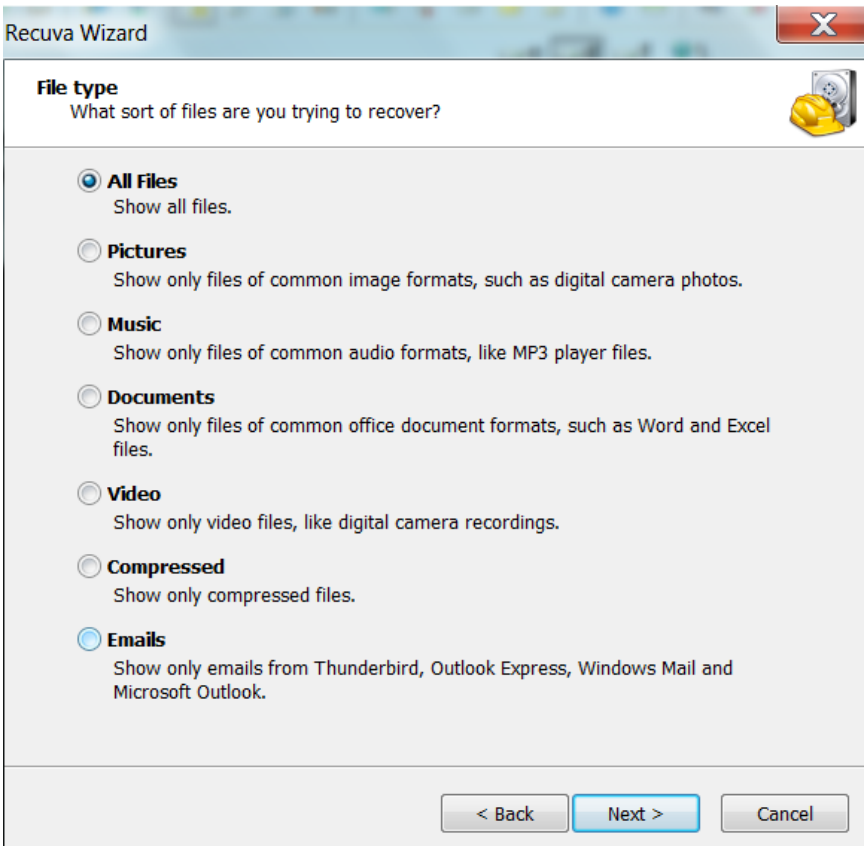
Наприклад, документ формату pdf було захищено паролем iloveyou, сервіс успішно підібрав його.



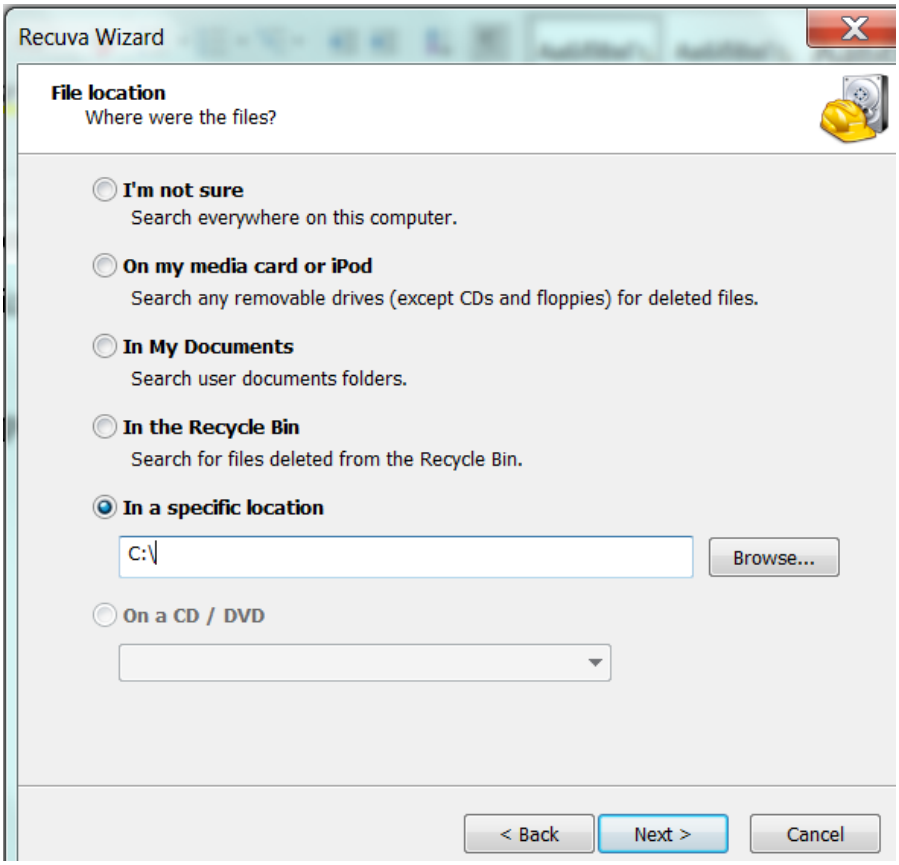
4. Відновлення втрачених даних.

Суттєво збільшити шанси на відновлення втрачених даних дозволяє мінімізація діяльності: не встановлюйте нових програм та не зберігайте нічого на диск, із якого зникла інформація. Якщо перезаписати інформацію поверх втраченої, відновлення стане неможливим. Із тієї ж причини не можна відновлювати файли на той самий носій, з якого вони були видалені. Для відновлення втрачених даних існує багато спеціалізованих програм, у тому числі й безкоштовних. Наприклад, Pandora Recovery, Recuva, R-STUDIO.

Після встановлення та запуску програми виберіть тип відновлюваних даних. Якщо ви, наприклад, хочете відновити музику, видалену з флешки, обирайте третій пункт. Якщо бажаєте побачити всі знайдені до відновлення дані, залишайте прапорець на першому пункті «всі файли», і натискайте «далі».

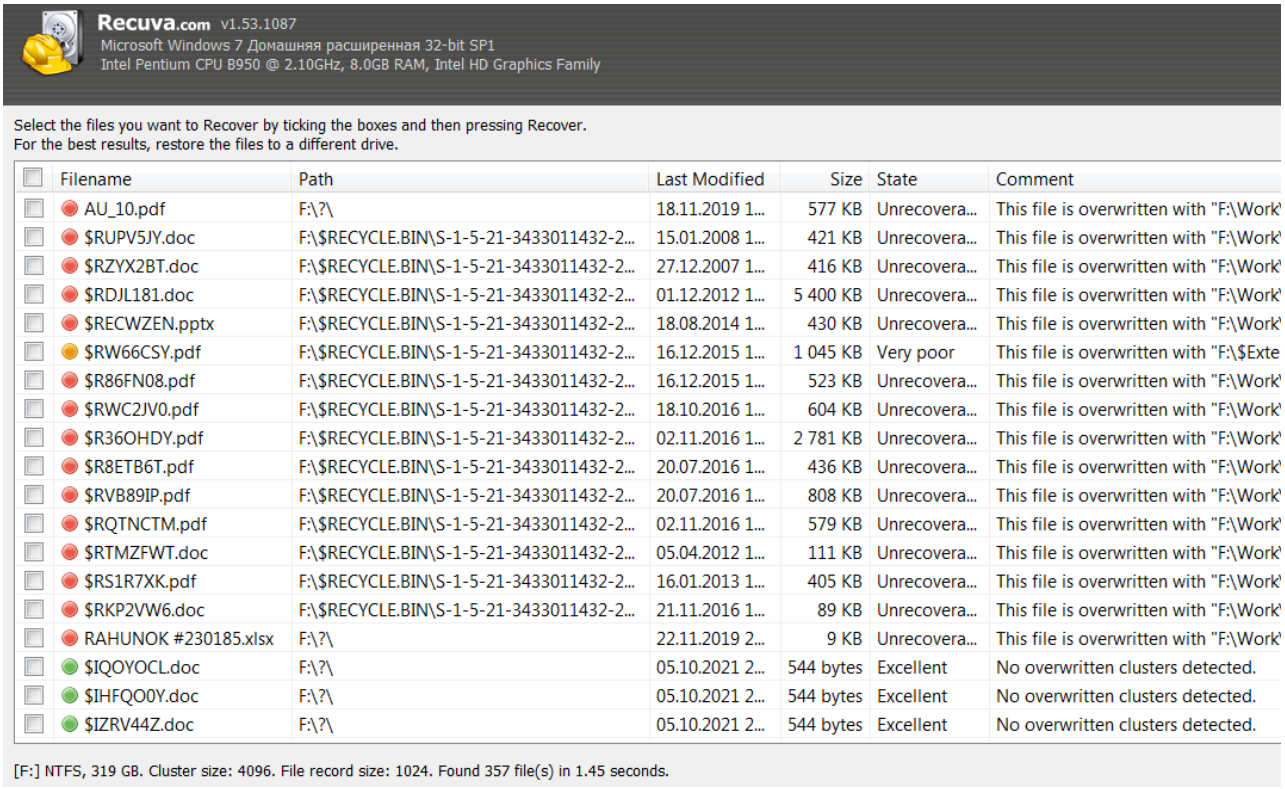


У випадку, коли точно відоме місце розташування видалених файлів, обирайте п’ятий пункт «У вказаному місці», відзначайте подвійним кліком у списку потрібний диск/папку та натискайте «Далі».



Після того, як ви вибрали потрібний диск/папку, перед вами з'явиться вікно завершення роботи майстра Recuva, де він запропонує включити поглиблений аналіз. При первинному проході це робити не рекомендується, оскільки ця опція сильно збільшує час сканування, при цьому результати можуть не відрізнятися. Після закінчення сканування з'явиться вікно із знайденими файлами, що було видалено раніше. Існує три типи колірної індикації знайдених файлів – червоні (відновлення не можливе), жовті (можливе часткове відновлення) та зелені (можуть бути відновлені повністю).

Позначте файли, які необхідно відновити, натисніть «Відновити…» та оберіть папку, куди необхідно розмістити відновлені файли. За необхідності, у тому ж вікні вибору файлів позначте ті, які хочете видалити назавжди, викличте правою кнопкою миші контекстне меню і вибирайте пункт «Надійно видалити зазначені». Через деякий час Recuva знищить ці файли без відновлення.



Filename	Path	Last Modified	Size	State	Comment
AU_10.pdf	F:\?\	18.11.2019 1...	577 KB	Unrecovera...	This file is overwritten with "F:\Work
$RUPV5JY.doc	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	15.01.2008 1...	421 KB	Unrecovera...	This file is overwritten with "F:\Work
$RZYX2BT.doc	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	27.12.2007 1...	416 KB	Unrecovera...	This file is overwritten with "F:\Work
$RDJL181.doc	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	01.12.2012 1...	5 400 KB	Unrecovera...	This file is overwritten with "F:\Work
$RECWZEN.pptx	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	18.08.2014 1...	430 KB	Unrecovera...	This file is overwritten with "F:\Work
$RW66CSY.pdf	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	16.12.2015 1...	1 045 KB	Very poor	This file is overwritten with "F:\$Exte
$R86FN08.pdf	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	16.12.2015 1...	523 KB	Unrecovera...	This file is overwritten with "F:\Work
$RWC2JV0.pdf	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	18.10.2016 1...	604 KB	Unrecovera...	This file is overwritten with "F:\Work
$R36OHDY.pdf	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	02.11.2016 1...	2 781 KB	Unrecovera...	This file is overwritten with "F:\Work
$R8ETB6T.pdf	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	20.07.2016 1...	436 KB	Unrecovera...	This file is overwritten with "F:\Work
$RVB89IP.pdf	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	20.07.2016 1...	808 KB	Unrecovera...	This file is overwritten with "F:\Work
$RQTNCTM.pdf	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	02.11.2016 1...	579 KB	Unrecovera...	This file is overwritten with "F:\Work
$RTMZFWT.doc	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	05.04.2012 1...	111 KB	Unrecovera...	This file is overwritten with "F:\Work
$RS1R7XK.pdf	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	16.01.2013 1...	405 KB	Unrecovera...	This file is overwritten with "F:\Work
$RKP2VW6.doc	F:\$RECYCLE.BIN\S-1-5-21-3433011432-2...	21.11.2016 1...	89 KB	Unrecovera...	This file is overwritten with "F:\Work
RAHUNOK #230185.xlsx	F:\?\	22.11.2019 2...	9 KB	Unrecovera...	This file is overwritten with "F:\Work
$IQOYOCL.doc	F:\?\	05.10.2021 2...	544 bytes	Excellent	No overwritten clusters detected.
$IHFQO0Y.doc	F:\?\	05.10.2021 2...	544 bytes	Excellent	No overwritten clusters detected.
$IZRV44Z.doc	F:\?\	05.10.2021 2...	544 bytes	Excellent	No overwritten clusters detected.

5. Видалення даних без можливості відновлення.

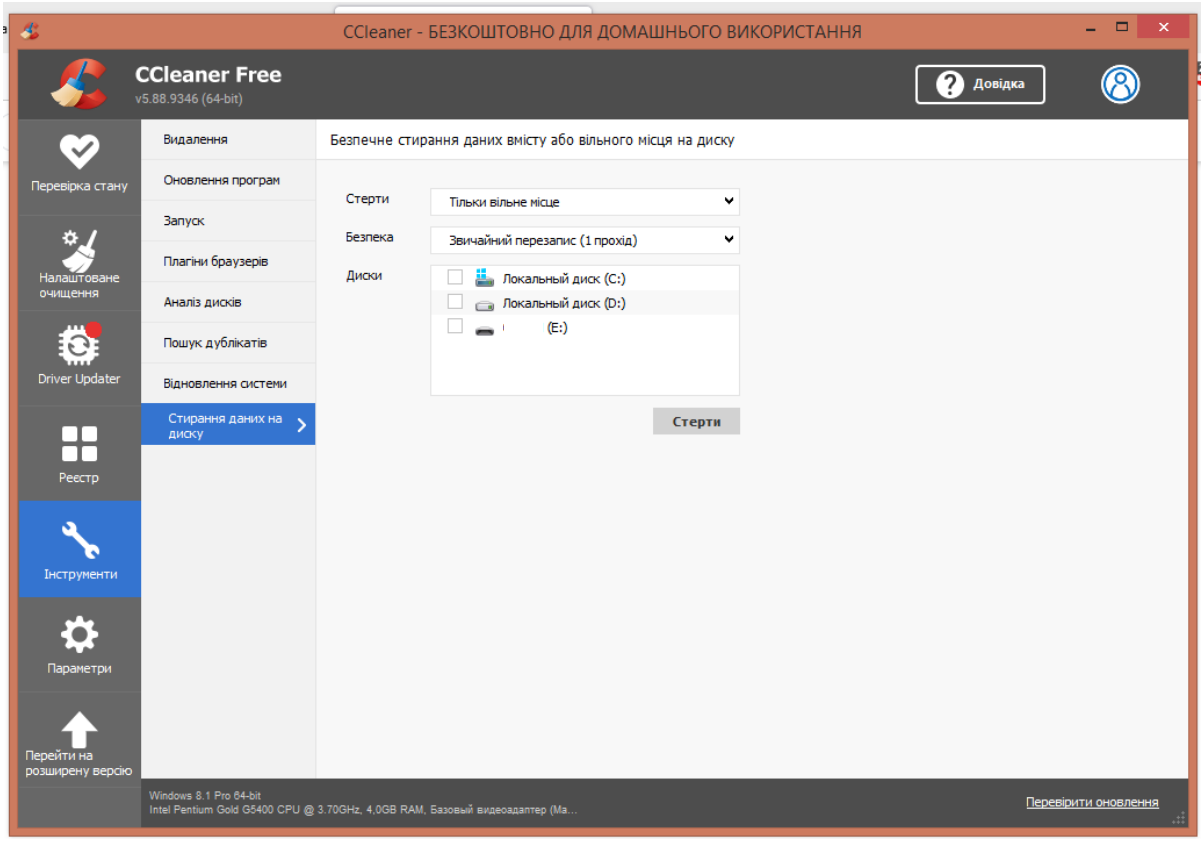
CCleaner – популярна сервісна програма від Piriform, потужний функціонал якої спрямований на очищення, захист приватних даних Й прискорення роботи персонального комп'ютера. Завдяки широкому спектру

інструментів ТА налаштувань ця утиліта чудово аналізує роботу операційної системи Windows і сторонніх додатків.

Можна визначити три основні напрями роботи CCleaner – це сканування та виправлення помилок, очищення, захист конфіденційності користувача. Сканування та аналіз відбувається шляхом перевірки системи й додатків, пошуку програмних помилок та їхніх причин. Під час очищення програма видаляє невживані й тимчасові файли що забезпечує більш швидку роботу операційної системи і звільняє місце на жорстких дисках. Також внаслідок цього знищуються сліди онлайн-активності користувача, наприклад історія його навігації в Інтернеті.

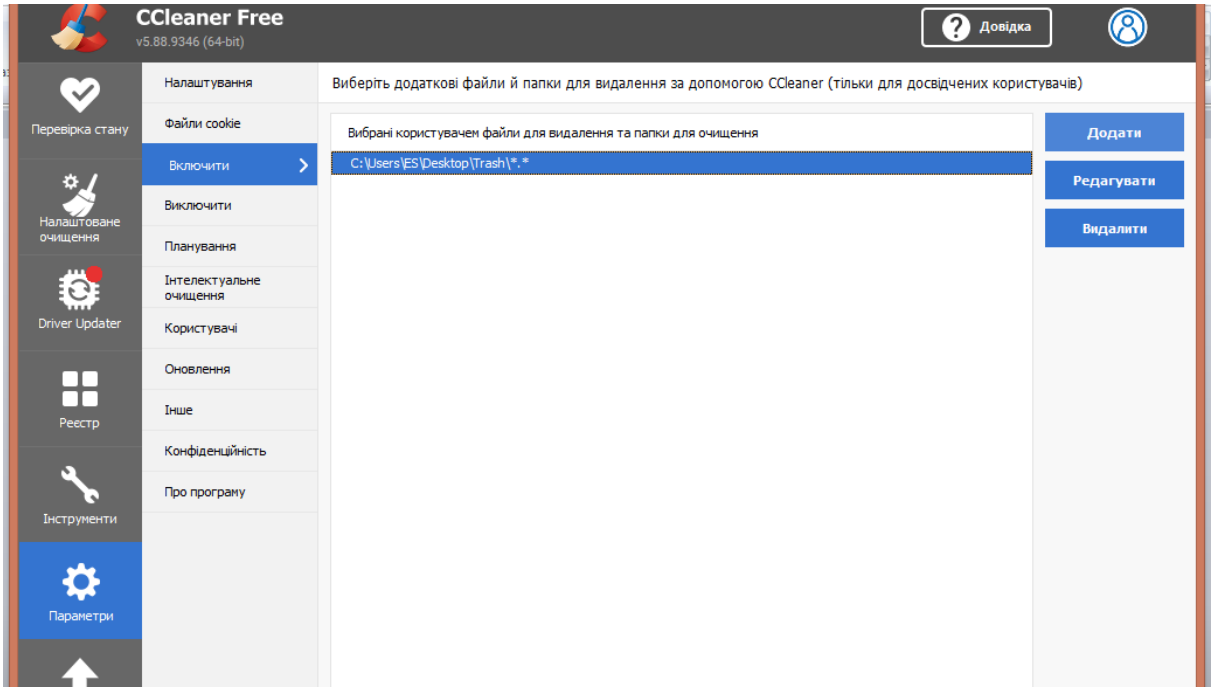
Програма формує список файлів, що потребують видалення, і пропонує його користувачу. У список можуть входити файли з помилками, кукі, тимчасові об’єкти чи додатки, які не використовує ні користувач, ні система. Їх наявність навантажує систему пристрою і впливає на швидкість проведення операцій, адже багато таких програм не припиняють свою активність навіть тоді, коли здається, що вони вимкнені.

Для безпечного видалення даних необхідно обрати пункт меню «Інструменти – Стирання даних на диску». В налаштуваннях обрати «тільки вільне місце», «звичайний перезапис (1 прохід)» та зйомний диск.

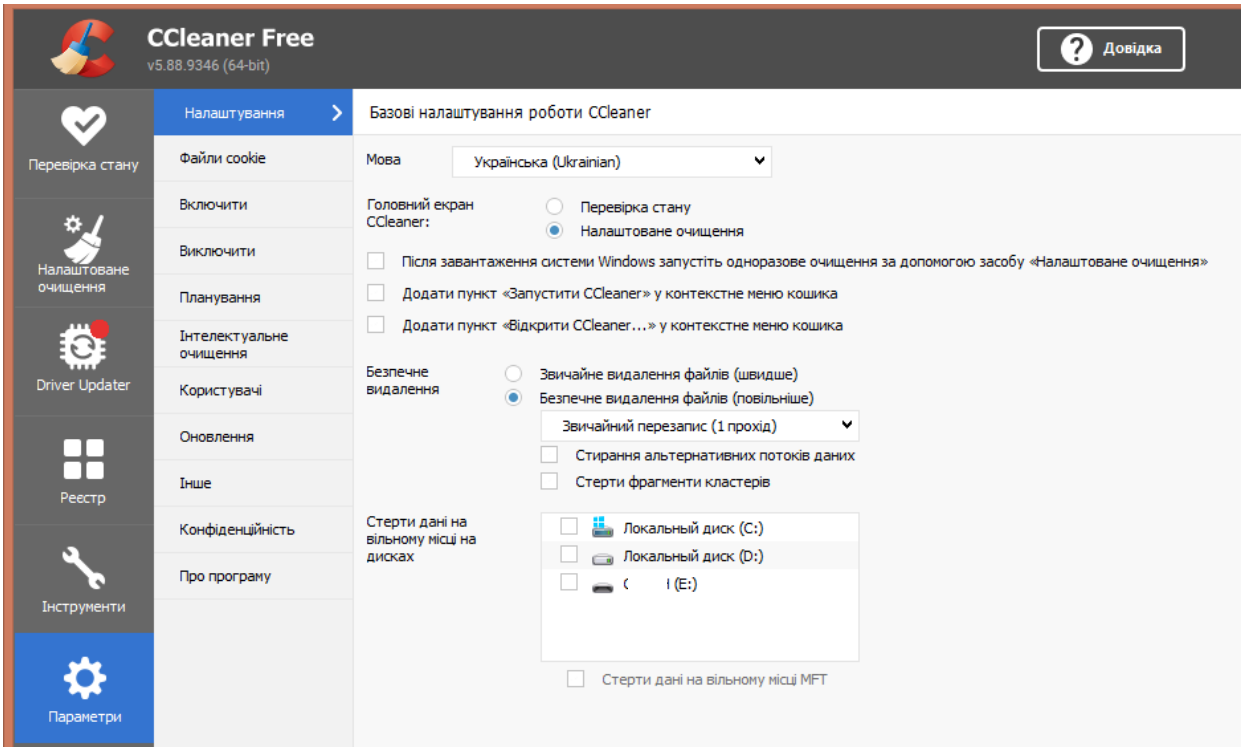


Для видалення дуже важливих даних доцільно обрати розширений перезапис – 3 проходи.

За необхідності, Ccleaner можна налаштувати для надійного видалення файлів із певної папки (як опція, включно з підпапками та самою папкою): «Параметри – Включити». При здійсненні операції очищення інформація з обраної папки буде видалена.



У пункті меню «Параметри – Налаштування» визначаються параметри видалення даних: звичайне видалення чи безпечне, з вибором кількості потрібних проходів.



4. ЗАХИСТ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

4.1. Найпоширеніші види шкідливого програмного забезпечення.

4.2. Основні технології захисту.

4.3. Віртуальні машини (пісочниця).

4.1. Найпоширеніші види шкідливого програмного забезпечення.

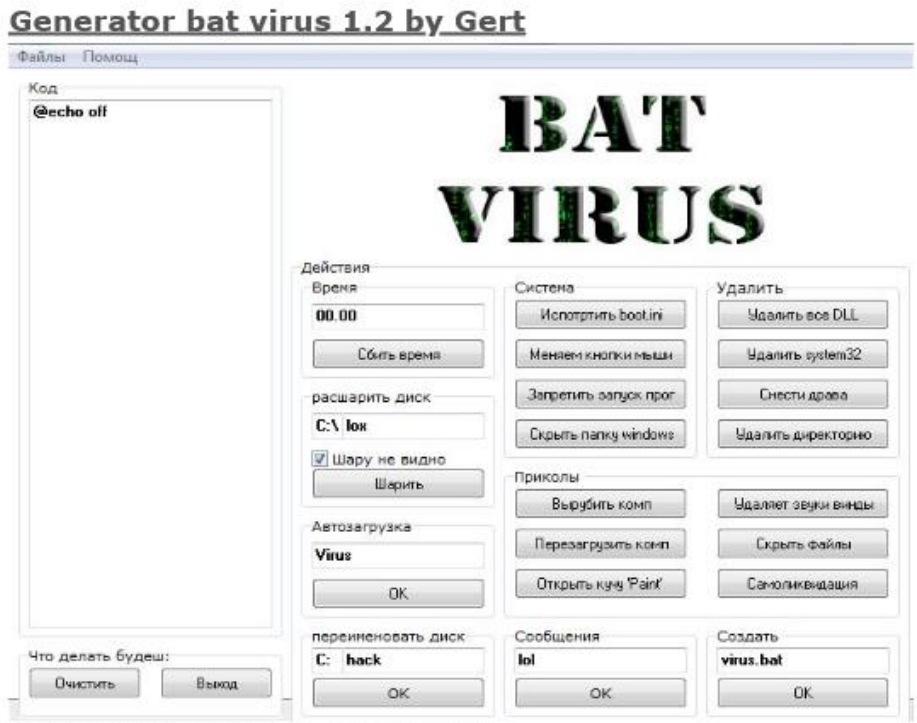
Ідея вірусу в комп'ютерах була вперше запропонована математиком Джоном фон Нейманом у 1949 році з його тезою про те, що програмне забезпечення може відтворювати себе. У наступні десятиліття з'явилися нові теоретичні підходи та були поставлені експерименти з кодом. Перший «практичний» вірус Creeper був розроблений в 1971 році і поширився через Arpanet. До 1980 у світі налічувалося понад 200 вірусів, а до 1990 – близько 3000.

```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19    3 JOBS
LOAD AV    3.87    2.95    2.14
JOB  TTY   USER        SUBSYS
1    DET   SYSTEM      NETSER
2    DET   SYSTEM      TIPSER
3    12    RT          EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

Комп'ютерний вірус – це невелика програма, яка здатна до саморозмноження й виконання різних деструктивних дій. На початку епохи комп'ютерних вірусів розробка вірусоподібних програм носила чисто дослідницький характер, поступово перетворюючись на відверто вороже протистояння користувачів та безвідповідальних, і навіть кримінальних «елементів». В ряді країн карне законодавство передбачає відповідальність за комп'ютерні злочини, в тому числі за створення та розповсюдження вірусів.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Віруси діють тільки програмним шляхом. Вони, як правило, приєднуються до файлу або проникають всередину файлу. У цьому випадку кажуть, що файл заражений вірусом. Вірус потрапляє в комп'ютер лише разом із зараженим файлом. Для активізації вірусу потрібно завантажити заражений файл, і тільки після цього вірус починає діяти самостійно. Деякі віруси під час запуску зараженого файлу стають резидентними (постійно знаходяться в оперативній пам'яті комп'ютера) і можуть заражати інші файли та програми, що завантажуються. Інші різновиди вірусів відразу після активізації можуть спричиняти серйозні пошкодження, наприклад, форматувати жорсткий диск.

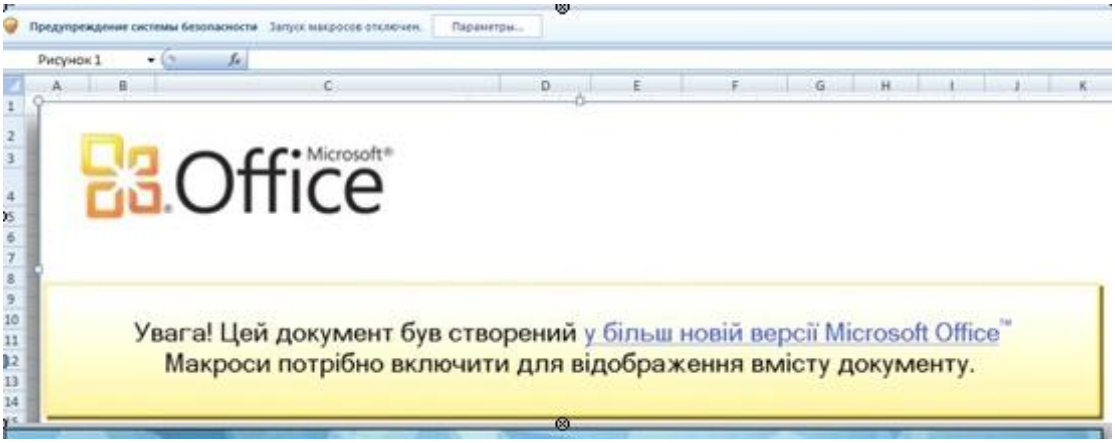


простенький генератор bat вирусов.

Дія вірусів може проявлятися по різному: від різних візуальних ефектів, що заважають працювати, до повної втрати інформації. Більшість вірусів заражують виконавчі програми, тобто файли з розширенням .exe та .com.

У даний час не існує єдиної системи класифікації та іменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO у 1991 році). Прийнято розділяти віруси:

- по уражаємих об’єктах (файлові віруси, завантажувальні віруси, скриптові віруси, макровіруси, віруси, що вражають вихідний код);
- по уражаємим операційним системам і платформам (DOS, Microsoft Windows, Unix, Linux);
- за технологіями, використовуваними вірусом (поліморфні віруси, стелс-віруси, руткіти);
- за мовою, на якій написано вірус (асемблер, високорівнева мова програмування, скриптова мова та ін.);
- по додатковій шкідливої функціональності (бекдори, кейлоггери, шпигуни, ботнети та ін.).

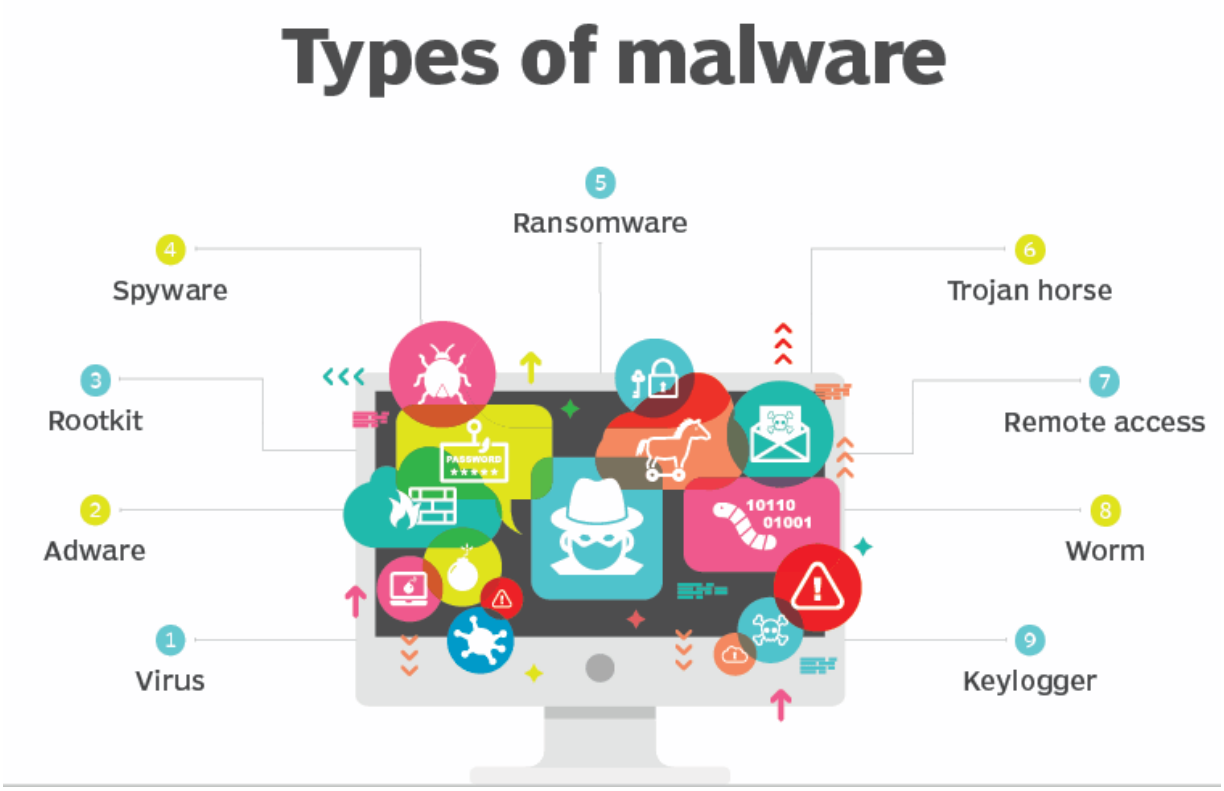


Термін «комп’ютерний вірус» часто неправильно використовується як загальний термін для позначення всіх підозрілих програм, плагінів або коду, які заражають програмне забезпечення, комп’ютери та файли. Насправді правильним загальним терміном для таких програм є шкідливе програмне забезпечення, категорія комп’ютерних вірусів є лише одним із типів. У світі поширений англійський термін – malware, malicioussoftware (шкідливе програмне забезпечення). Однак у вжитку укорінилась загальна назва «вірус», як синонім до шкідливих програм, це є поняттям слова вірус у широкому сенсі.

Інші основні типи шкідливих програм:

- бекдор програми – надають віддалений доступ до комп’ютера для зловмисників;
- хробаки – окремий вид шкідливих програм, головною задачею яких є розмноження серед комп’ютерів в мережі;

- адваре – рекламні модулі;
- дропери – по суті, це програми, які встановлюють троянські програми на комп'ютери користувачів;
- даунлоадери – маленькі троянські програми, у яких є усього одна функція – завантажити велику троянську програму.



Троянська програма – це програма, яка має приховані функції. Така назва виникла тому що перші програми цього типу потрапляли на комп'ютери під виглядом корисних програм, які користувачі завантажували й запускали власноруч. Зараз такий варіант розповсюдження також присутній, часто користувачі самі запускають подібні програми, намагаючись завантажити зламані неліцензійні версії програмного забезпечення чи програми для генерації зламаних серійних ключів.

Хробак – це програма, яка розмножується, від одного комп'ютера до іншого. Механізми можуть бути дуже різними: електронна пошта, локальна мережа чи USB-накопичувач. Так, хробак може скопіювати свої файли на флешку та створити відповідний файл автозавантаження і як тільки ви під'єднаєте флешку до комп'ютера, на ньому одразу ж активізується хробак.

При цьому слід зазначити, що хробаки які розповсюджуються через пошту чи через флешки, практично ні в чому не відрізняються, вони лише використовують різні шляхи поширення.

Бекдор – програма «чорний хід», зазвичай шкідливі програми цього типу дають зловмиснику віддалений доступ та можливість керування комп'ютером користувача. Методи їх дії бувають різними, наприклад така програма може відкрити мережевий порт, за допомогою якого зловмисник отримає повний доступ до ураженого комп'ютера: зможе надсилати різні команди, запускати інші програми.

Дропер – це по суті інсталятор троянської програми. Оскільки троянська програма це багатокомпонентний елемент, який потребує встановлення в системі певних драйверів та інших компонент, то цю задачу виконує дропер. Після того як дропер було активовано в системі, він встановлює всі частини троянської програми та активує її.

Завантажувальник – це по-суті троянська програма, мета якої – завантажити з мережі Інтернет іншу троянську програму. Характерна риса таких програм – вони дуже маленького розміру (кілька десятків кілобайт), а отже можуть завантажитись і активізуватись дуже швидко. І вже після вкорінення в системі, даунлоадер завантажує основну троянську програму. При цьому може бути завантажений, як дропер, так і окремі компоненти троянця, які будуть методично інсталюватись на комп'ютер. Отже, якщо у вас на комп'ютері був знайдений завантажувальник, то варто шукати й інші троянські програми.

Діалери – це програми-дзвонилки, вони були дуже популярні у часи активного використання модемів і телефонних ліній. Сучасні модифікації діалерів використовують дещо інші механізми, зокрема, це можуть бути дзвінки через Skype, відкриття певних спеціалізованих сайтів.

Руткіт – це спеціальний вид троянських програм, головна мета якого – максимально глибоко інсталюватись у систему, щоб його було якомога важче знайти і видалити. Як правило, руткіти містять драйвери операційних систем і працюють на досить низькому рівні. Руткіти використовуються для маскування всіх інших компонентів троянця від детектування. Тобто руткіт у системі призваний приховати роботу інших компонентів трояна. Головна проблема в тому, що руткіти дуже важко знайти і ще важче видалити з системи. Далеко не кожна антивірусна програма може з цим впоратись.

Умовно шкідливе ПО або потенційно небажані програми (PUA, Potentially Unwanted Application) – це широка категорія програмного забезпечення, яке не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни. Ці програми можуть інсталювати додаткове небажане ПЗ, змінювати поведінку або налаштування цифрового пристрою, а також виконувати неочікувані для користувача дії або не підтверджені ним.

Категорії програмного забезпечення, які можна розглядати як умовно шкідливе: ПЗ, що відображає рекламу або виконує завантаження інших програм, різноманітні браузерні панелі інструментів, ПЗ з оманливою поведінкою, пакетне ПЗ, ПЗ для відстеження користувацьких операцій, майнери криптовалют, програми для очищення реєстру (тільки в операційних системах Windows), будь-яке інше сумнівне ПЗ або програмне забезпечення із застосуванням противоправних або принаймні неетичних практик ведення бізнесу (незважаючи на те, що його використання може сприйматися як правомірне), яке кінцевий користувач може розцінити як небажане, коли він дізнається про особливості роботи цього ПЗ після інсталяції.

Потенційно небезпечна програма – це легітимне програмне забезпечення (можливо, комерційне), яке може несанкціоновано використовуватись зловмисниками для досягнення їх цілей. Рекламний модуль – адваре програми, мабуть найменш небезпечні з усіх шкідливих програм, але через дуже широку розповсюдженість і просто величезну зухвалість їх авторів в останній час вони стали досить неприємними. Задача рекламного модуля – показати вам рекламу. Це може відбуватись у різних проявах, наприклад у вас можуть самостійно відкриватись певні сторінки у браузері, які ви не відкривали – це будуть сайти з

дивною рекламою або просто сайти, які ви не збирались відвідувати. Тобто зловмисники таким чином підвищують відвідуваність певного сайту або провокують вас подивитись певну інформацію. Також рекламні модулі можуть показувати різні банери чи навіть вставляти банери на той сайт, де їх не було, або ж підмінювати рекламні повідомлення на сайтах. Наприклад якщо ви шукаєте певну інформацію у Гугл, то видача пошукового запиту містить 2 категорії – безкоштовні пошукові запити та рекламні повідомлення, рекламні модулі можуть підміняти одні рекламні повідомлення на інші й в результаті ви будете бачити не ту інформацію яку запитували, а те, що хоче вам показати власник рекламного модуля. Даний механізм підміни пошукових видач отримав назву «чорного SEO».

Основні джерела зараження ПК та мобільних пристроїв.

Найголовнішим джерелом вірусів буде той канал, який забезпечує максимальний обмін інформацією Вашого ПК з іншими. Тож, головним джерелом зараження є глобальна мережа Інтернет.

На жаль віруси існують практично для всіх каналів зв’язку і зловмисники охоче використовують ті, якими більш активно користуємось ми. Зараз найбільше користувачі використовують вебсайти та електронну пошту. Існують віруси, які розповсюджуються через Skype та інші месенджери. У свій час існували популярні віруси для RRS клієнтів, однак вони використовуються не

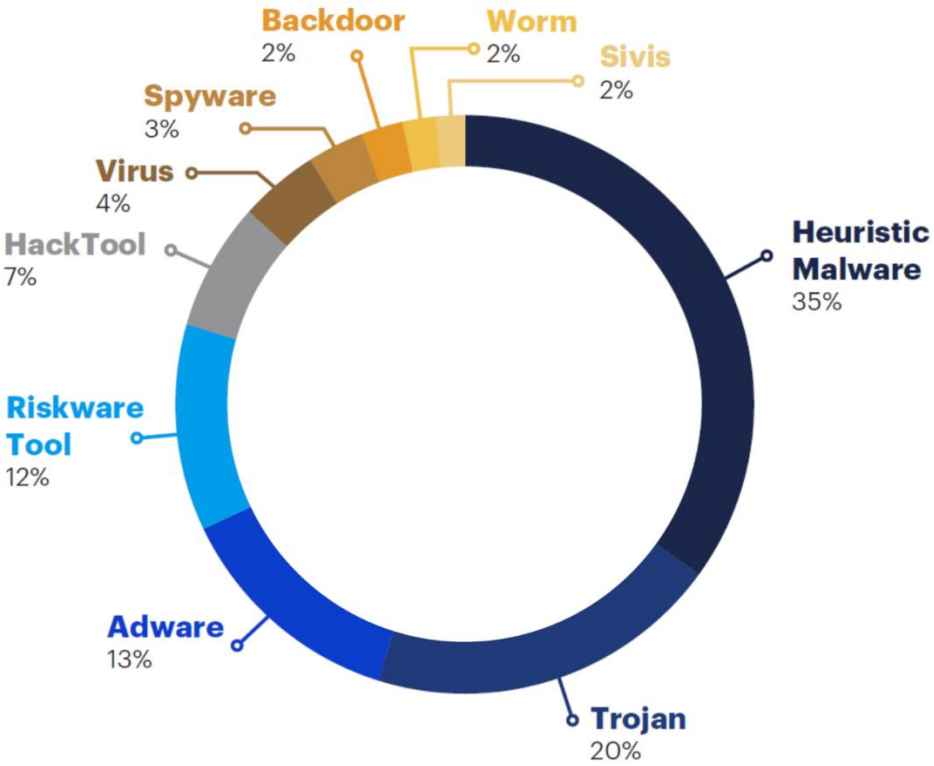
так широко. А от браузерами для відвідування сайтів користуються всі без виключення і як наслідок це джерело є найбільш популярним.

Другим по популярності джерелом зараження є електронна пошта. На початку 2000-их років практично всі загрози шли саме з електронної пошти. Зараз об'єм заражень через е-мейли не на стільки високий, однак все ж зустрічаються масові розсилки, в яких користувачі отримують листи, які маскуються під звичайну пошту від знайомих чи колег. І наприклад якщо вірус заразив комп'ютер Вашого знайомого і від нього пише вам листа, то вірогідність того що ви відкриєте цього листа дуже висока. Часто відбуваються масові СПАМ-розсилки, які маскують під повідомлення від банків, і взагалі під певну корисну інформацію: фото, архіви, які Вам пропонують подивитись. Звичайно ж після відкриття такого файлу нічого корисного для вас крім зараження Вашого ПК не відбудеться.

Третім за популярністю способом зараження ПК є змінні накопичувачі, перш за все це флеш диски та USB-накопичувачі. Перші комп'ютерні віруси взагалі почали свою історію саме зі змінних накопичувачів, тільки тоді це були дискети – гнучкі магнітні диски. Різниця лише у тому, що старі віруси не завжди могли запускатись автоматично і чекали коли користувачі самі запустять певну програму з диску, сучасні ж віруси можуть запускатись автоматично одразу після підключення флешки до комп'ютера.

За масовістю – найбільш розповсюдженими є рекламні модулі. На другому місці за популярністю є троянські програмі.

Із 2015 року небувалої активності набули програми-криптувальники, які шифрують дані та вимагають викуп для розблокування. На жаль, для шифрувальників використовують криптостійкі алгоритми і гарантувати розшифрування ніхто не може. Головна порада — не платити викуп. Відправивши гроші кіберзлочинцям, ви лише підтвердите, що вимагацьке ПЗ влучило в ціль; водночас ніхто не гарантує, що ви отримаєте потрібний ключ дешифрування.



Ознаки зараження комп'ютера вірусами:

- поява незвичайних системних повідомлень, наприклад, що програма з незнайомою назвою виконала неприпустиму операцію і буде закрита;
- повідомлення про брак системних ресурсів;
- поява рекламних банерів у той час, коли ви не працюєте в Інтернеті;
- поява вікон із попередженням про блокування та прохання надіслати SMS на вказаний номер;

- повідомлення від антивірусних програм, які ви не встановлювали на свій комп’ютер;
- різке зменшення вільного місця на жорсткому диску, хоча ви нічого великого не записували і не встановлювали громіздких програм;
- збільшення трафіку під час роботи в Інтернеті. Це особливо помітно тим, хто оплачує доступ до Інтернету залежно від обсягу інформації. Для тих, хто користується безлімітними тарифами, може бути помітним зменшення швидкості доступу до мережі;
- поява на флешці файлів, які ви туди не записували (особливо з розширенням .exe). Поява на знімному носії файлу autorun.inf та папки Recycler. При штатному безпечному видаленні флешки операційна система повідомляє про те, що пристрій не може бути зупинено прямо зараз, хоча файли на флешці не відкриті в жодній програмі;
- повідомлення від встановлених антивірусних програм про виявлення загрози.

4.2. Основні технології захисту.

Сигнатурний аналіз.

Із самого початку появи антивірусних програм, програмісти зрозуміли, що вірус потрібно детектувати за певною характеристикою, і, оскільки, спочатку віруси були досить незначними, і володіли достатньо унікальним кодом, використовували так звану сигнатуру. Сигнатура – це послідовність байт у певній програмі чи контрольна хеш сума деякого блоку програми, яка характеризує його. Тобто, антивірус знаходив у програмі деяку частину коду, яка була характерною лише для певного вірусу і якщо така частина була знайдена в певній програмі, то вважалось, що програма заражена вірусом, або вона є троянською програмою чи рекламним модулем. Сигнатура (signature – підпис) може розглядатися у більш широкому сенсі – унікальна послідовність, ланцюг, інформація, які характеризують певну загрозу. Це може бути і алгоритм, певна послідовність байт, може бути контрольна сума, сигнатура поведінки програми у системі.

У чому проблема сигнатурного пошуку? Для того щоб створити сигнатуру для певного вірусу, потрібно щоб він був у вірусної лабораторії. Не можна створити сигнатуру для вірусу якого ще не має, оскільки не має тієї унікальної послідовності яку можна додати у вірусну базу. Це основна проблема сигнатурного детектування вірусів. З іншого боку, у сигнатур є свої переваги. Якщо антивірус за допомогою сигнатур знайшов вірус, значить він знайшов у файлі чітку послідовність характерну для певного вірусу, він може назвати цей вірус, по цьому імені можна знайти опис того, що ця програма робить, а виходячи з такої інформації можна знати як даний вірус нейтралізувати, які операції потрібно зробити, які шкідливі функції він виконує, і як можна виправити наслідки їх дій. Тобто сигнатура характеризує якийсь конкретний вірус і дає переваги у подальшій його обробці антивірусом.

Із часом стало очевидно, що боротися з вірусами лише за допомогою сигнатурного аналізу не можливо, оскільки якщо ви сьогодні оновили вірусні бази, а завтра з’явився новий вірус, то Ваш антивірус не зможе його детектувати. Отже, антивірусна програма постійно перебуває позаду.

Евристичний аналізатор.

Наступною технологією, яка з'явилась досить давно є евристичний пошук, зараз ця технологія використовується в антивірусних програмах разом із сигнатурними методами.

У вірусів окрім унікальних характеристик є певні загальні властивості, певна модель поведінки яка їх характеризує, особливості, які притаманні для шкідливих програм і не характерні для звичайних програм. Евристичний аналізатор аналізує код програми, знаходить у ньому певні закономірності, притаманні для різних класів шкідливих програм і на основі цього приймає рішення щодо можливого визначення програми шкідливою. Часто антивірус повідомляє, що «Даний файл є підозрілим, можливо в ньому є такий-то вірус…». Сенс у тому, що евристичний аналізатор не знає точно який це вірус, не знає точно чи вірус це взагалі. В чому перевага евристичних аналізаторів? Вони дозволяють визначати загрози, які ще не були додані у сигнатурні бази, нові, ще невідомі загрози. Навіть якщо у вас не було можливості оновити вірусні бази, евристичний аналізатор зможе заблокувати ймовірні загрози.

Які недоліки евристичного аналізу? Перш за все це вірогідність хибного спрацювання. Евристичний аналізатор може знайти у програмі певну підозрілу діяльність, але її наявність ще не робить програму шкідливою. Можливо програмісти використовували при написанні програми схожі методи з тими, які використовували зловмисники. Тобто, евристичний аналізатор теоретично може помилитися, при чому, з досить великою долею вірогідності.

Автори вірусів активно протидіють евристичними аналізаторами. З'явились анти-евристичні прийомі, різні коди анти-аналізатори, щоб антивірусна програма не змогла перевірити цей код. використовувались й інші прийоми, щоб не дати можливості перевірити такі файли.

Поведінковий аналізатор.

Він схожий на роботу евристичного аналізатора, однак із тією різницею, що аналізується не код програми, а її поведінка в процесі роботи. Тобто, в системі запустилась програма і вона виконує певні дії. Наприклад, програма зберегла файл у системній папці і звернулась до Інтернет, щось завантажила, намагається цей закачаний файл запустити. Поведінковий аналізатор слідкує за діями програм і намагається зрозуміти чи є діяльність програм штатною, чи характерна для шкідливих програм. Якщо поведінковий аналізатор вважає що дана програма поводить себе як шкідлива, він може її заблокувати і навіть «відкотити» назад певні зміни у операційній системі, які зробила шкідлива програма. Поведінкові аналізатори можуть блокувати ще невідомі загрози.

Наприклад, якщо є певний алгоритм поведінки коли програма запускається, створює запис у реєстрі Windows і після цього одразу розсилає листи прикріпляючи копію себе – то це поштовий хробак. Логіка прозора – який би не був код поведінка хробака буде така сама, і тому не важливо як і на якій мові написана програма, чи є в ній шифрування чи ні, присутні анти-евристичні прийоми чи ні – діяти програма буде однаково. Тому її можна заблокувати.

Недоліки поведінкових аналізаторів. Нажаль, поведінковий аналізатор перевіряє програму тоді, коли вона вже працює. Тобто, якщо ви просто скопіюєте файли з флешки, то поведінковий аналізатор не зможе їх перевірити. У спокійному стані можна використовувати лише евристику та сигнатури. Якщо ж ви запустите програму, то спрацює поведінковий аналізатор, і добре, якщо вдасться шкідливу програму зупинити до того, як вона виконає певні шкідливі дії.

Отже, поведінковий аналізатор не забезпечує абсолютний захист. Цей модуль забезпечує дуже високий додатковий рівень захисту, але все ж таки є додатковим і саме так його варто розглядати.

Репутаційні технології.

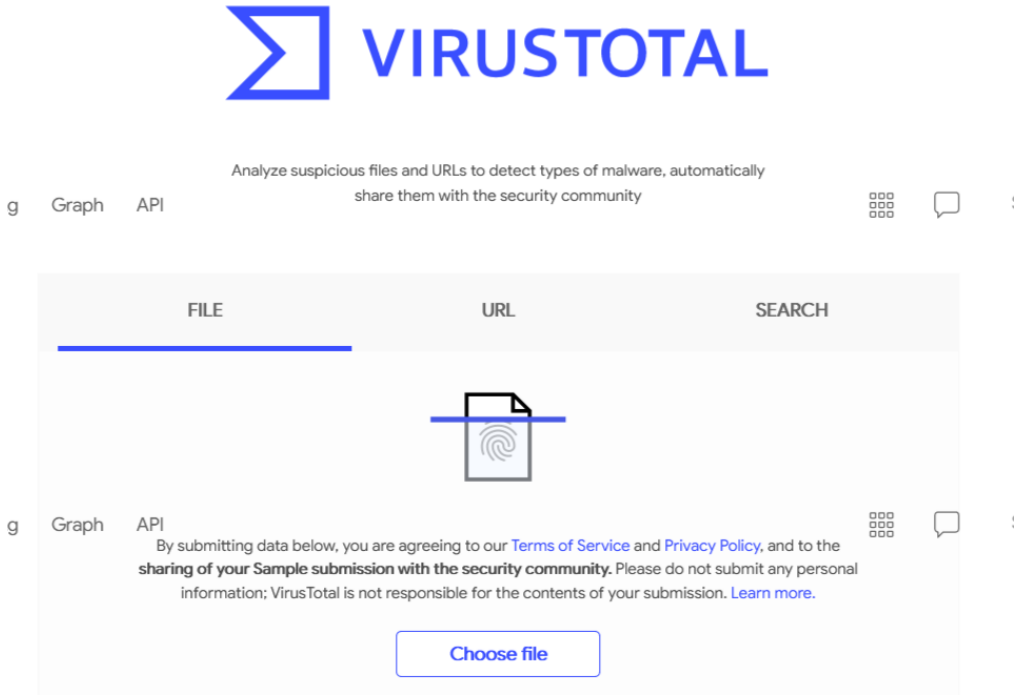
Дуже важливий момент – з розвитком Інтернет стало очевидно, що частина функцій антивірусного захисту може здійснюватися не на комп'ютері користувача, а на серверах антивірусної компанії. Антивірусні компанії запустили так звані хмарні антивірусні сервіси, а також репутаційні технології, які можна віднести до хмарних сервісів.

У чому суть репутаційних технологій? Коли на ваш комп'ютер вперше потрапляє новий файл, то для нього підраховується унікальна сигнатура, наприклад хеш-сума, певна послідовність байт, яка характеризує тільки цей файл. Вона передається на сервер і антивірус «консультується» з ним щодо наявної інформації про файл. Якщо сервер надає відповідь, що це новий файл і він до цього не зустрічався ні у кого з інших користувачів, то ви приймаєте рішення чи є ця програма шкідливою й можете залишити свій голос, сформувати репутацію цього файлу. Наприклад, користувач зазначає: «так, цей файл хороший, я його качав і хочу його запустити». Програма запускається, працює й аналізується поведінковим аналізатором. Якщо раптом виявиться що файл все таки шкідливий, на сервер передається інформація про те, що файл небезпечний і користувач помилився й для файлу сформується відповідний рейтинг. У подальшому користувач, який завантажує цей файл, навіть якщо його ще не додали в сигнатурні бази і не детектують евристичним чи поведінковим аналізатором, зможе побачити низький рейтинг довіри до файлу, і це дозволить бути більше обізнаним про можливу загрозу.

Що дають репутаційні технології? В роботі антивірусних компаній є певний виробничий процес: вірус має потрапити на комп'ютери користувачів заразити їх, після чого він потрапляє в антивірусну компанію, або антивірусна компанія сама його знайде, або користувач надішле зразок власноруч в антивірусну компанію. Часто антивірусні компанії проводять обмін зразками

вірусів. Далі буде потрібен певний час на аналіз такого файлу, який може зайняти години або дні. Після чого буде створена певний сигнатура, яка буде протестована всередині антивірусної компанії, що також займає певний час, далі створюється оновлення вірусних баз і користувачі мають ці оновлення скачати. Тобто з моменту створення загрози і першого зараження до моменту готовності антивірусу захищати користувача від даної загрози пройде певний час. Це можуть бути години, а можуть бути і дні, тобто сигнатурний метод немов запізнюється. Репутаційні аналізатори дозволяють боротись з загрозами практично в режимі реального часу, перший користувач, який стикається з файлом, вже отримає інформацію про нього, як мінімум, на рівні повідомлення, що це новий файл. За перші 5 хвилин існування у файлу вже буде певна репутація. Відповідно всі наступні користувачі вже будуть оповіщені про рівень загрози.

Хмарні технології.



Суть хмарних технологій полягає у тому, що сигнатурна перевірка файлів відбувається не у вас на комп'ютері, а на сервері антивірусної компанії. Всі відомі файли не потрібно передавати на аналіз, передаються лише нові, які визначаються на основі унікальної хеш-суми. І сервер відповідає, чи знає він про ці файли з відповідними хеш-сумам. Відповідно до рішення сервера

антивірус на вашому комп’ютері буде приймати рішення дозволити запускати ці файли чи ні. Якщо ж новий файл невідомий, то він буде переданий на сервер антивірусної компанії, де буде повністю досліджений усіма найпотужнішими антивірусними технологіями. Хмарні технології дозволяють перенести навантаження, потрібне для аналізу файлу, з вашого комп’ютера на сервер компанії, де він буде опрацьований більш якісно й не завантажуючи вашу систему.

Не існує найкращого універсального антивірусу. Він підбирається під ситуацію, під користувача, під комп’ютер на якому буде встановлений, під задачі, для яких буде використовуватись. Хороший антивірус той, який постійно працює. Якщо антивірус гальмує систему і ви його періодично вимикаєте, то це погано, адже чи не найголовнішою опцією антивірусної програми є те, що вона має постійно працювати. виключений антивірус інколи навіть гірше ніж відсутність антивірусу взагалі.

Варто наголосити, що вибір антивірусу є пошуком компромісу. Не складно зробити антивірус який буде максимально захищати від всіх загроз, можна вбудувати туди поведінковий аналізатор, зібрати сигнатури загроз із усього світу але є одна проблема – цей антивірус буде дуже сильно гальмувати роботу системи, буде займати дуже багато пам’яті, постійно видавати повідомлення, що певний файл є підозрілим. І тому його неможливо буде використовувати. Антивірусні компанії постійно йдуть на компроміс між якістю детектування і продуктивність, між автоматизацією і здатністю обробити певні загрози більше ефективно.

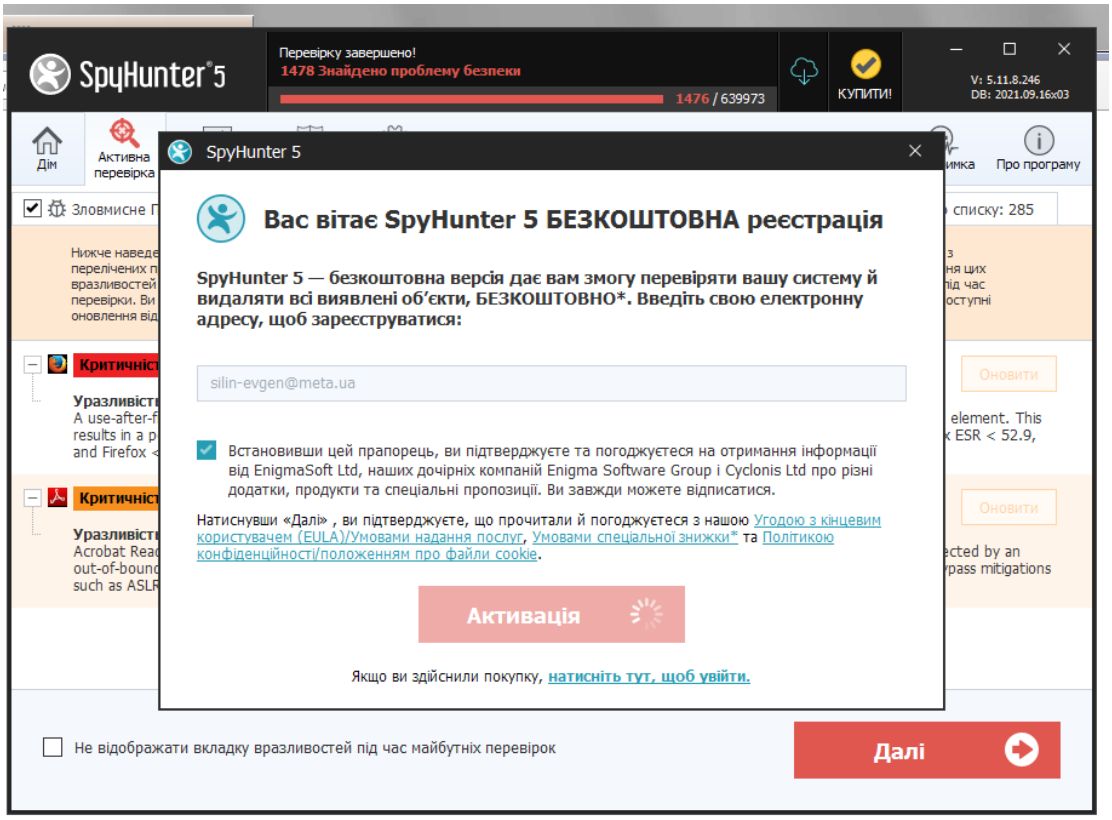
Отже, ви маєте обрати антивірус виходячи із того на скільки вам зручно ним користуватись, наскільки гарно він детектує загрози, які характерні саме для Вашого комп’ютера, виходячи із ресурсів якими ви користуєтесь, виходячи із регіону в якому перебуваєте.

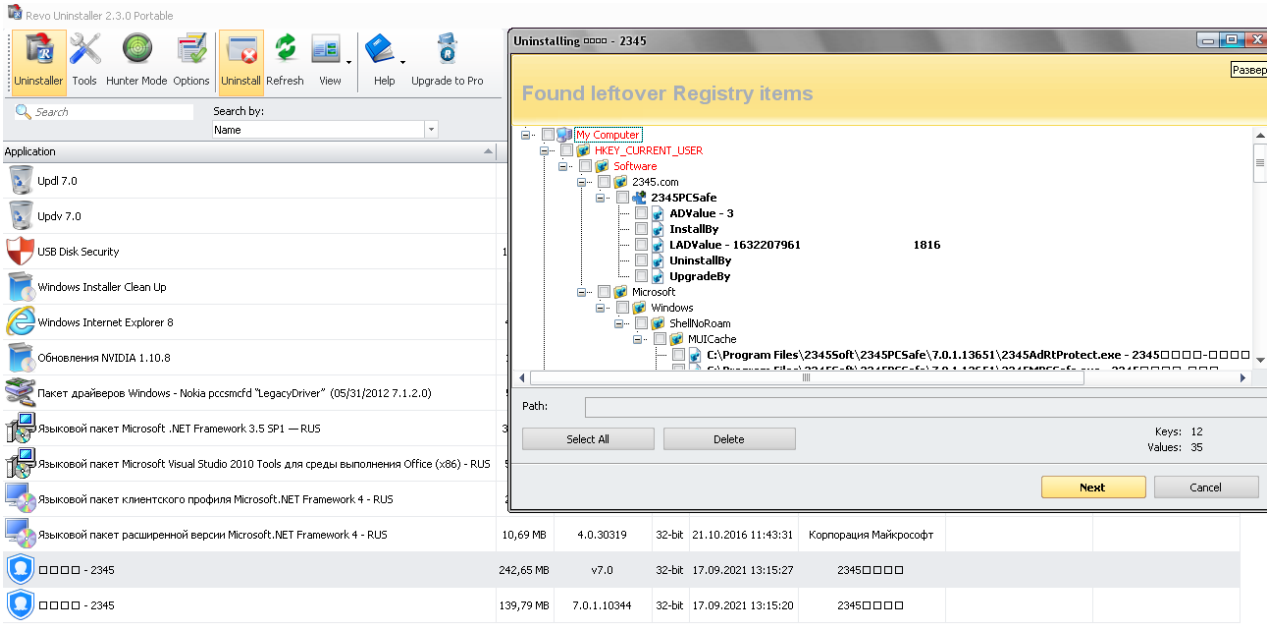
Тести антивірусного програмного забезпечення:

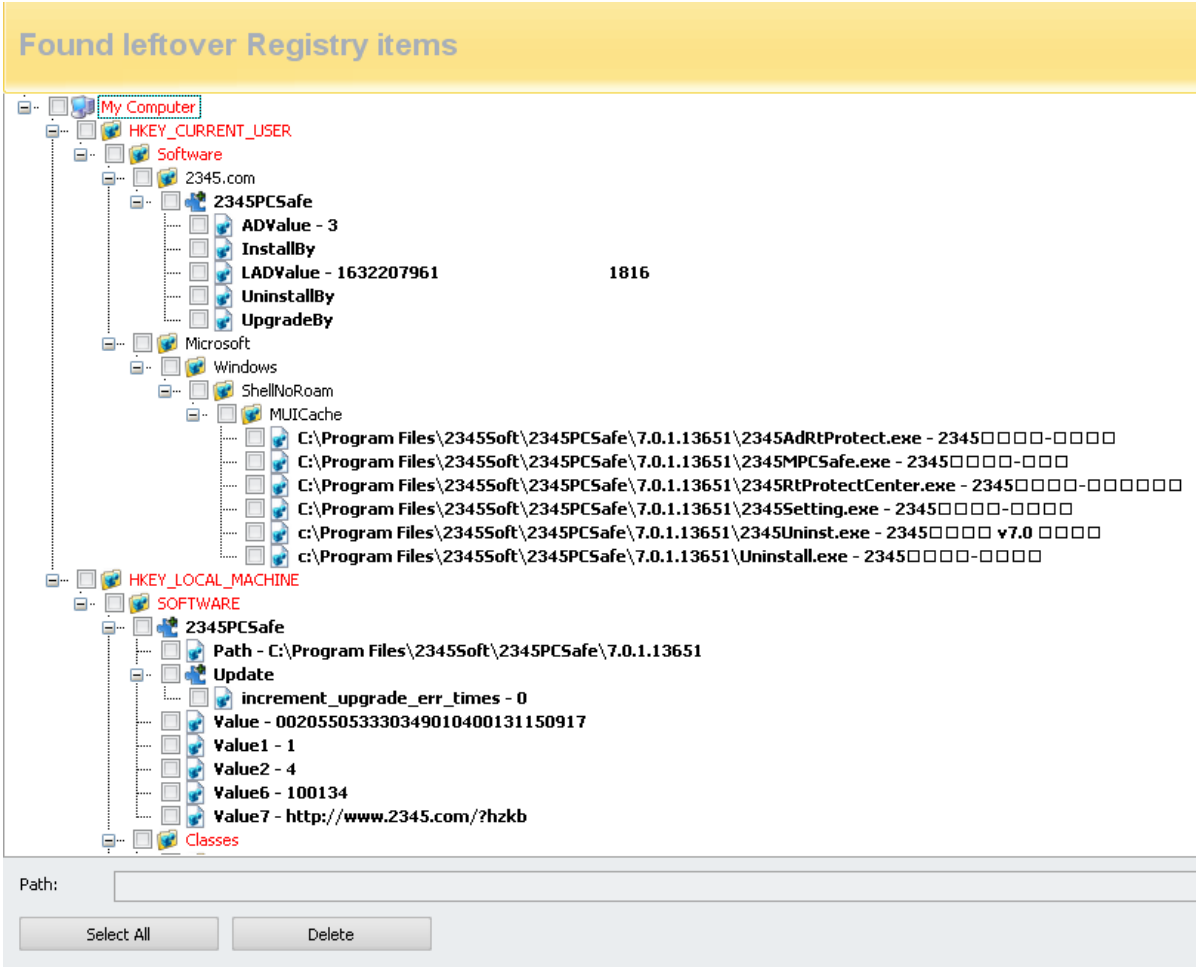
- https://www.av-test.org/en/antivirus/home-users/,
- https://www.av-comparatives.org/.

Producer		Certified	Protection	Performance	Usability
AhnLab	V3 Internet Security 9.0	TOP PRODUCT	6	6	6
Avast	Free AntiVirus 21.7 & 21.8	TOP PRODUCT	6	6	6
Avast	One Essentials 21.7 & 21.8	TOP PRODUCT	6	6	6
AVG	Internet Security 21.7 & 21.8	TOP PRODUCT	6	6	6
Avira	Internet Security for Windows 1.1	TOP PRODUCT	6	6	6
Bitdefender	Internet Security 25.0	TOP PRODUCT	6	6	6
BullGuard	Internet Security 21.0	TOP PRODUCT	6	6	6
eset	Internet Security 14.2	TOP PRODUCT	6	6	6
F-Secure	SAFE 18	TOP PRODUCT	6	6	6
G DATA	Total Security 25.5	TOP PRODUCT	6	6	6
K7 SECURITY	Total Security 16.0	TOP PRODUCT	5.5	6	6
kaspersky	Internet Security 21.3	TOP PRODUCT	6	6	6
Malwarebytes	Premium 4.4.5 & 4.4.7	TOP PRODUCT	5.5	6	6
McAfee	Total Protection 25.0	TOP PRODUCT	6	6	6
Microsoft	Defender 4.18	TOP PRODUCT	6	6	6
eScan Enterprise Security	eScan Internet Security Suite 14.0		5	6	5.5
NortonLifeLock	Norton 360 22.21	TOP PRODUCT	6	6	6
PC Matic	PC Matic 3.0		5.5	6	4.5
TOTAL AV	Total AV 5.15	TOP PRODUCT	6	6	6
TREND MICRO	Internet Security 17.0	TOP PRODUCT	6	6	6
VIPRE	VIPRE AdvancedSecurity 11.0	TOP PRODUCT	6	6	6

ESET AV Remover допоможе видалити практично будь-яке антивірусне програмне забезпечення, інстальоване в системі. Необхідно завантажити відповідний інструмент та запустити файл на виконання: https://www.eset.com/ua/support/av-remover/.







Для смартфонів характерні ті ж самі загрози, що і для персональних комп'ютерів, оскільки телефон, по суті, і є комп'ютером. Сьогодні існує величезна кількість загроз: віруси, троянські програми, мережеві хробаки, рекламні модулі орієнтовані на абсолютно різні платформи для мобільних пристроїв.

Краще встановлювати додатки лише з PlayMarket. Водночас, під час встановлення програми вам буде показуватись список привілеїв, які бажає отримати програма. Потрібно дуже уважно читати, що саме потребує програма. Тут має бути проста логіка. Наприклад, якщо ви встановлюєте гру, навіщо вона просить доступ до відправки sms. Звичайно, у цьому випадку це дуже підозріло і краще відмовитись від встановлення даної програми.

У налаштуваннях можна дозволити встановлення додатків не з офіційного магазину. Це пункт меню Налаштування / Безпека / Невідомі джерела. Навіть якщо ви досвідчений користувач та бажаєте встановити програму не з PlayMarket дуже важливо цей дозвіл давати саме на момент

встановлення вами програми. Під час звичайного користування смартфоном чи планшетом доцільно не вмикати цю опцію, оскільки у цьому випадку шкідливі програми не зможуть встановитись у той час, коли ви помилково перейдете за фішинговим посиланням.

Коли ви встановлюєте програмне забезпечення на смартфон, система запитує у вас дозвіл на цю операцію. На цей момент програма ще може бути не шкідливою. Але в подальшому вона може автоматично оновитися, отримати нові функцію, частина яких може бути шкідливими. Тому радимо не вмикати функцію автоматичного оновлення програм, та оновлювати необхідні вам програми вибірково, під вашим контролем, і тільки тоді, коли це дійсно необхідно. Тож ні в якому разі не вмикайте дозвіл на встановлення програм з невідомих джерел на тривалий термін.

Дії при ураженні шкідливим ПЗ.

1) Важливо розуміти, що, залежно від типу обгортки (приманки), процес інфікування може запуститися автоматично, а може очікувати остаточного підтвердження. Просто закрити документ або вкладку не завжди буде правильним рішенням. Деякі приманки розраховані на запуск саме під час закриття доданку.

Можливо, процес інфікування вже розпочався, тому потрібно якнайшвидше розірвати канал передачі інформації – висмикнути кабель із мережевої карти або вимкнути Wi-Fi. Існує можливість, що ви обірвете завантаження основної частини вірусу.

2) Зробіть резервні копії (якщо вони відсутні) найважливіших файлів та документів. У подальшому проведіть додаткову антивірусну перевірку цих даних, перш ніж їх використовувати.

3) Після того як документи будуть скопійовані (або резервні копії у вас завжди наявні), не закриваючи документа-приманки, не натискаючи ні «Ок», ні «Скасувати», вимикайте систему довгим натисканням на кнопку або ж висмикуйте кабель живлення – не завершуючи роботу штатно (це необхідно, щоб обірвати запущені процеси вірусу, якщо він уже активний). Якщо ви

плануєте звернутися за допомогою до IT-фахівця, тоді ліпше систему перевести в режим так званого гібридного сну (hibernation). Такий підхід допоможе в розслідувані інциденту.

4) Завантажити систему з live CD/USB, підготовленого на іншій системі, та провести антивірусну перевірку.

У випадку зараження вірусом-шифрувальником:

1) Зробіть фотографію (знімок екрана) повідомлення з вимогою викупу на вашому екрані.

2) Якщо це можливо, використайте антивірусне програмне забезпечення або продукти захисту від шкідливих програм, щоб видалити вимагацьке програмне забезпечення з вашого пристрою. Можливо, доведеться перезавантажити систему у безпечному режимі.

3) видалення вимагацького ПЗ не призведе до дешифрування ваших файлів, але дозволить вам виконати наступні дії без зашифровування нових файлів.

4) Якщо у вас була резервна копія, відновіть інформацію.

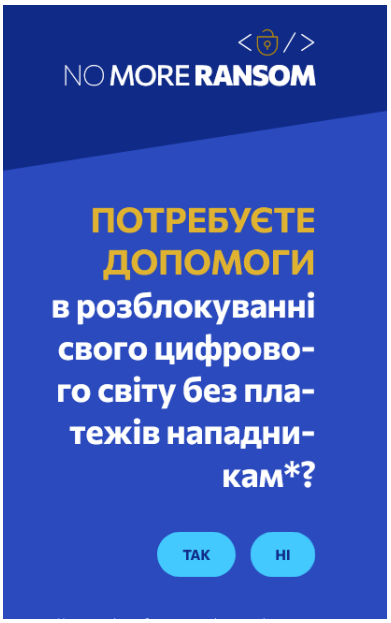
5) Не платіть викуп. Заплативши, ви фінансуватимете злочинність і заохочуватимете злочинців до нових незаконних дій. Немає жодних гарантій того, що ви отримаєте доступ до своїх даних або пристрою, і в майбутньому ви, найімовірніше, станете знову мішенню злочинців.

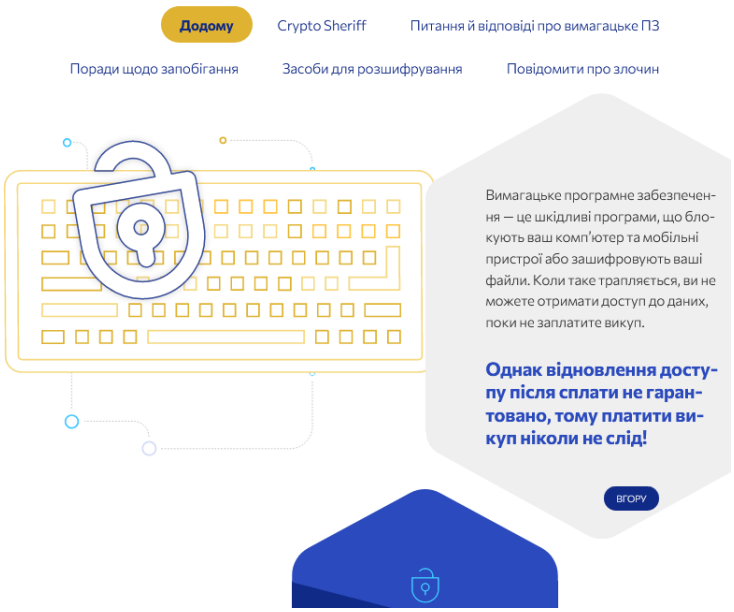
6) Якщо у вас немає резервної копії даних, відвідайте www.nomoreransom.org (https://www.nomoreransom.org/uk/index.html), щоб перевірити, чи не уражений ваш пристрій вимагацьким ПЗ, для якого сервіс пропонує безкоштовні засоби для розшифрування. Повідомлення з вимогою викупу стане в пригоді в цьому процесі.

Розшифрування можливо в таких випадках:

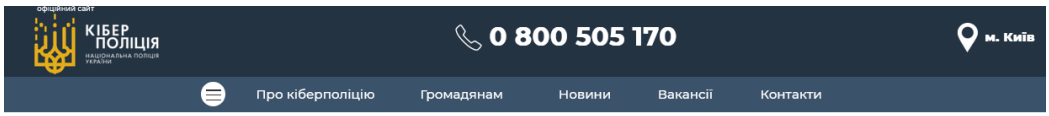
- автори шкідливого ПЗ помилилися в реалізації, вможлививши злом шифру. Таке мало місце з вимагацькими програмами Petya та CryptXXX;
- автори шкідливого ПЗ шкодують про свої дії й публікують ключі або головний ключ, як це було у випадку TeslaCrypt;

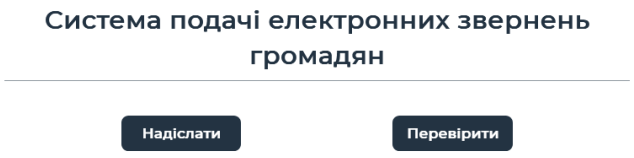
- правоохоронні органи захоплюють сервер з ключами й діляться ними. Одним з таких прикладів є CoinVault.





7) Повідомте про це Кіберполіцію України. Чим більше інформації ви надасте, тим вірогідніше, що правоохоронні органи зможуть зупинити злочинну діяльність.



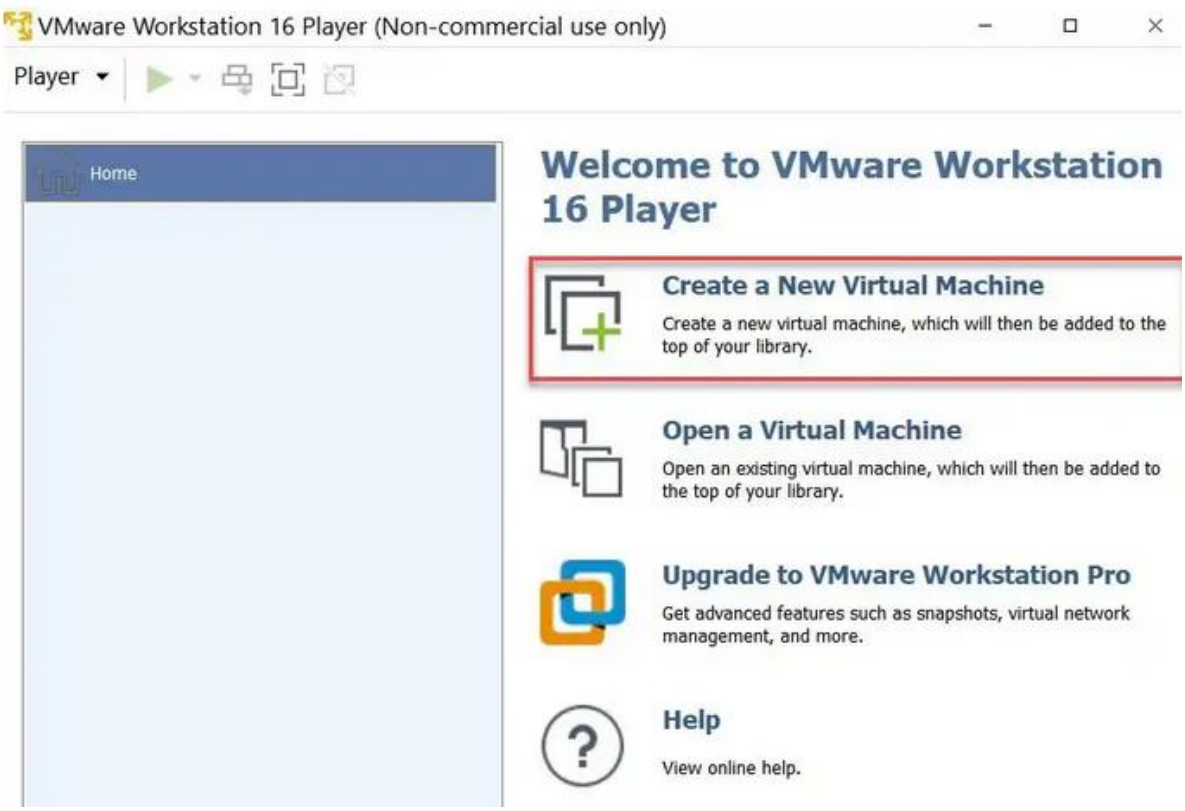


4.3. Віртуальні машини (пісочниця).

Віртуальна машина – це система для емуляції іншої платформи, вона допомагає користувачеві експлуатувати пристрій при встановленні декількох операційних систем, незалежних один від одного, завдяки чому один апарат може поєднати властивості двох і більше ПК. Створюються такі пристрої на реальних комп'ютерах в якості умовних. Це програма, що імітує копію існуючого апаратного забезпечення з усіма його компонентами (БІОС, жорсткий диск, периферійні пристрої). З допомогою спеціальних утиліт можна

запустити на одному комп’ютері кілька віртуальних машин з однаковими або різними операційними системами.

Операційна система, на якій встановлено віртуальну машину, називається основною або хост-ОС (від англ. host – головний, базовий, ведучий), а операційна система самої віртуальної машини називається гостьовою. Кожна гостьова ОС запускається в окремому вікні на основній ОС, аналогічно до звичайної програми. Все віртуальне обладнання, яке живить гостьову ОС, керується спеціальним механізмом, який називається гіпервізором. Гіпервізор відомий як менеджер віртуальної машини: він виділяє фізичні ресурси для кожної з систем і гарантує, що вони не перериватимуть роботу одна одної. Як правило, гіпервізори реалізуються на програмному рівні, але існують і такі, що вже вбудовані в прошивку системи.



Більшість віртуальних машин зберігають свої дані, включаючи операційну систему й додатки, в спеціальному файлі під назвою віртуальний диск, який містить файлову систему і представлений гостьовій ОС як звичайний фізичний жорсткий диск. Такий файл або набір файлів може

зберігатися на основному або віддаленому комп'ютері, бути частиною віртуальної машини або монтуватися в ОС фізичної машини.

Основними варіантами домашнього використання віртуальних машин є наступні.

Створення персонального віртуального середовища, ізольованого від хостової системи, що дозволяє використовувати на одному комп'ютері кілька копій робочих оточень, повністю ізольованих один від одного.

Створення переносних віртуальних машин, готових до використання на будь-який інший сумісній з архітектури платформі. Якщо Вам необхідно продемонструвати роботу певної програми, при цьому вона або оточення операційної системи повинні бути відповідним чином налаштовані – віртуальні машини кращий варіант в цьому випадку.

Отримання безпечних для користувача оточень для Інтернет. При роботі в мережі Інтернет віртуальна машина є більш виграшним варіантом, оскільки шкідлива програма після отримання контролю над операційною системою в віртуальній машині, може завдати шкоди тільки всередині неї, не зачіпаючи при цьому хостову ОС. Але останнім часом почали з'являтися віруси, які виявляють свою присутність в віртуальній машині й не видають себе в цьому випадку, однак поки таких шкідливих програм одиниці, і в будь-якому випадку шкоди важливим даним завдано не буде, поки заражені об'єкти не будуть перенесені в хостову ОС. Тому застосування віртуальних машин в цьому випадку аж ніяк не виключає використання антивірусного ПЗ.

Створення середовищ для експериментів із потенційно небезпечним програмним забезпеченням. На віртуальній машині можна без жодного ризику встановлювати прикладне ПЗ, яке може при певних умовах пошкодити систему або дані. В цьому випадку віртуальна машина виступає в ролі «пісочниці», в якій «граються» програми.

Можливість навчання роботі з операційними системами, відмінними від вашої хостової.

ЛАБОРАТОРНА РОБОТА №4. ХМАРНІ АНТИВІРУСНІ СЕРВІСИ

Мета вивчення: отримати практичні навички роботи з хмарними антивірусними сервісами.

Обсяг навчального часу: 2 години.

Обладнання: комп'ютер (планшет, смартфон), наявність підключення до мережі Інтернет.

План заняття:

1. Онлайн перевірка файлів та вебсайтів щодо наявності шкідливих програм.
2. Хмарна пісочниця.
3. Сканування комп'ютера за допомогою хмарних антивірусних засобів.

Інформаційні джерела:

статті щодо антивірусного програмного забезпечення: https://itech.co.ua/?s=%D0%B0%D0%BD%D1%82%D0%B8%D0%B2%D1%96%D1%80%D1%83%D1%81;

тести антивірусного програмного забезпечення:

- https://www.av-test.org/en/antivirus/home-users/,
- https://www.av-comparatives.org/;

хмарні антивірусні сервіси:

- https://www.virustotal.com/gui/home/upload,
- https://www.hybrid-analysis.com/,
- https://metadefender.opswat.com;

онлайн сканери:

- https://www.eset.com/ua-ru/home/online-scanner,
- https://zillya.ua/zillya-skaner,
- https://www.trendmicro.com/.

ЗАВДАННЯ:

1. виконати перевірку декількох файлів й сайтів за допомогою хмарних сервісів.

2. Встановить антивірусний додаток у браузер та виконайте перевірку файлу, який ви завантажуєте.

3. виконайте швидке сканування Вашого комп'ютера та папки Мої документи за допомогою онлайн сканера.

ВИМОГИ ДО ЗВІТУ:

1. Скрін екрану з результатами перевірки Вашого файлу за допомогою хмарних антивірусних сервісів.

2. Скрін екрану з результатами швидкого сканування певної папки чи диску Вашого комп'ютера за допомогою онлайн сканера.

ХІД РОБОТИ.

1. Онлайн перевірка файлу чи сайту на наявність шкідливих програм. Хмарна пісочниця.

використання хмарних антивірусних програм дозволяє виконати наступні дії:

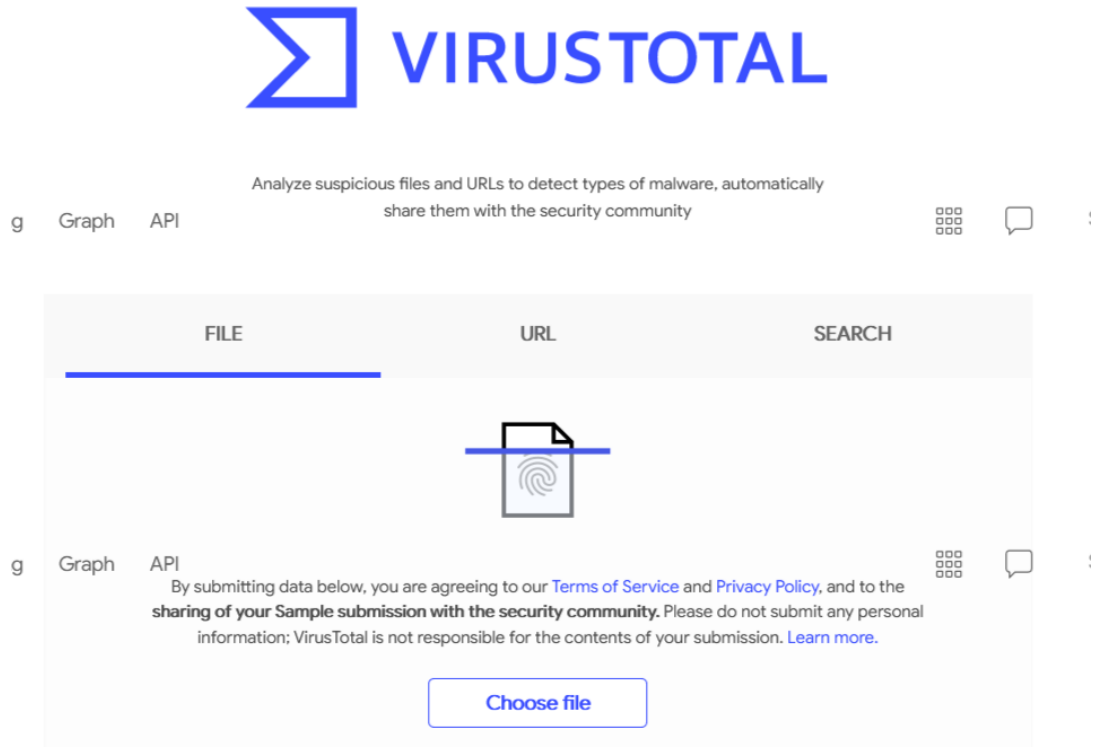
1) перевірити на віруси окремі програми та інші файли шляхом завантаження їх у спеціальні сервіси чи виконати цю перевірку за URL;

2) завантажити спеціальні антивірусні утиліти, які мають назву «онлайн сканер», але працюють саме на Вашому комп'ютері, але використовують антивірусну базу з Інтернету для перевірки (яка також може завантажуватись на комп'ютер). Зазвичай, такі утиліти не конфліктують із уже встановленими на комп'ютері антивірусами;

3) виконати перевірку комп'ютера на наявність активних вірусів та інших шкідливих програм.

Важно розуміти, що хмарні засоби доповнюють, але не замінюють інстальоване до операційної системи антивірусне програмне забезпечення, яке забезпечує профілактичний захист та постійно сканує та відстежує загрози.

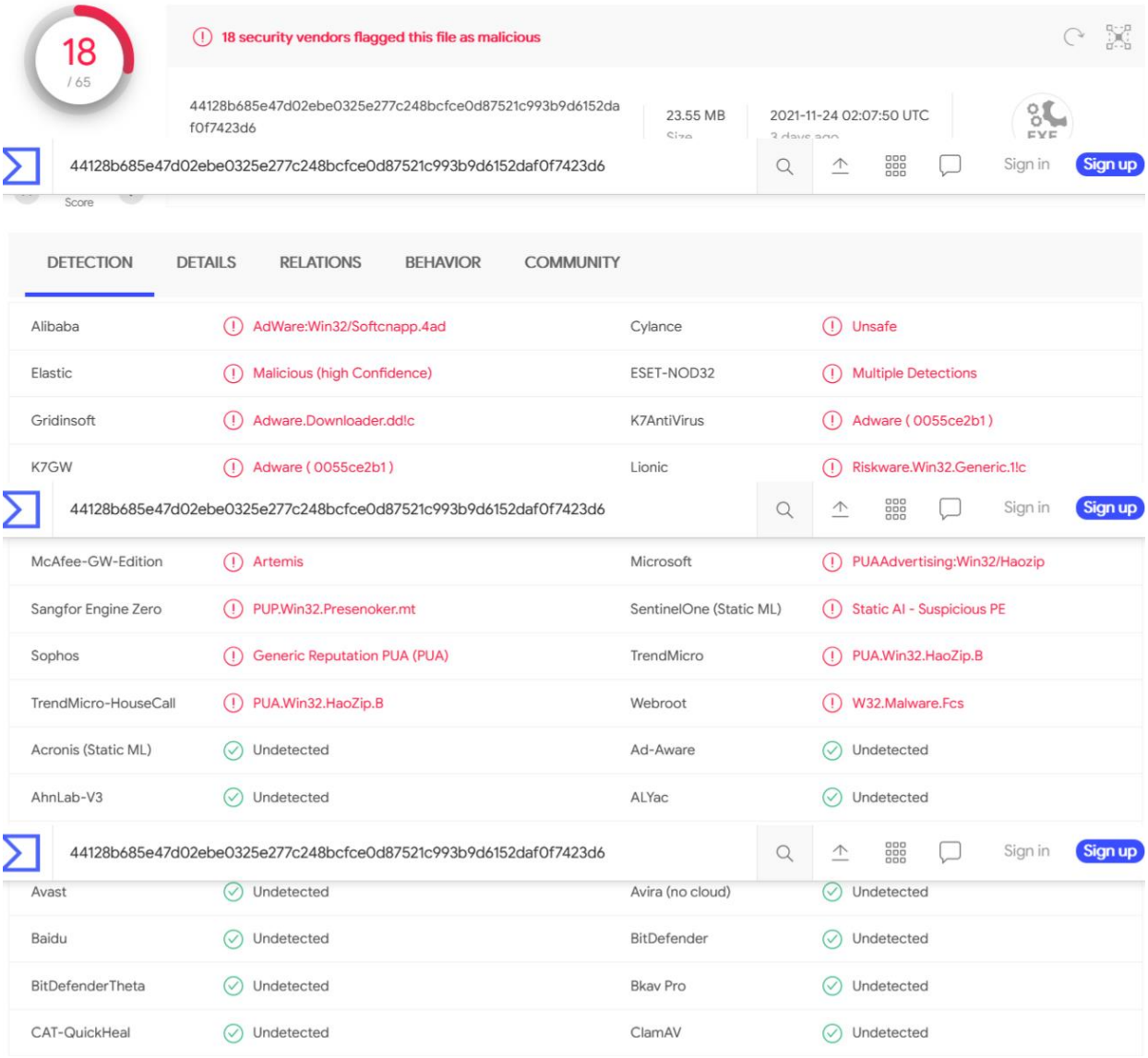
VirusTotal (https://www.virustotal.com) – це спеціальний онлайн-сервіс для перевірки на віруси та інші шкідливі програми файлів і сайтів. Належить Google, є безкоштовним та не містить рекламу. Існує обмеження на розмір файлу для перевірки – не більше 650 Мб. Система проводить перевірку 70 антивірусними сканерами та службами. Аналізує URL-адреси, евристичні механізми, підписи, метадані. Звіт про результати сканування поширюються разом із суспільством VirusTotlal. Будь-який користувач може коментувати та голосувати, чи дійсно файл є шкідливим.



Вам необхідно завантажити файл із комп'ютера чи вказати URL та зачекати на результати перевірки. При цьому повідомлення про те, що файл підозрілий (suspicious) в одному-двох антивірусах може говорити про те, що насправді файл не є особливо небезпечним і занесений до списку підозрілих лише з тієї причини, що виконує якісь не зовсім нормальні дії , наприклад, з його допомогою можна зламати ліцензію на програмне забезпечення. В такому випадку доцільно перейти до розділу «Деталі», оскільки, імовірно, цей файл

вже перевіряли, але під іншими іменами. Також перегляньте додаткову інформацію в розділі «Історія» та коментарі (за наявності).

Якщо ж, навпаки, звіт рясніє попередженнями, то краще видалити цей файл із комп'ютера та в жодному разі не запускати його. Покажчик у верхньому лівому куті інформує, яка кількість сканерів від усіх задіяних знайшла небезпеку.

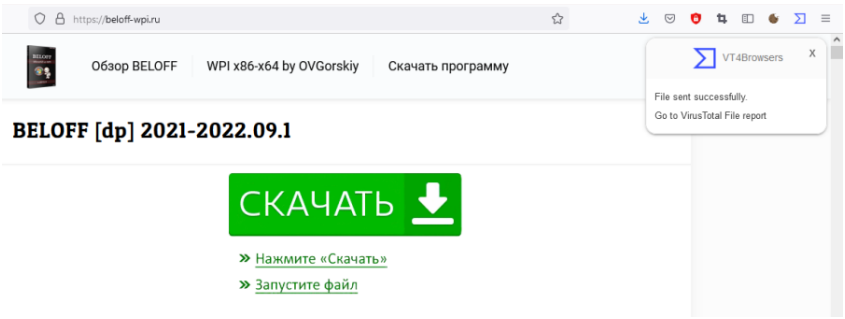


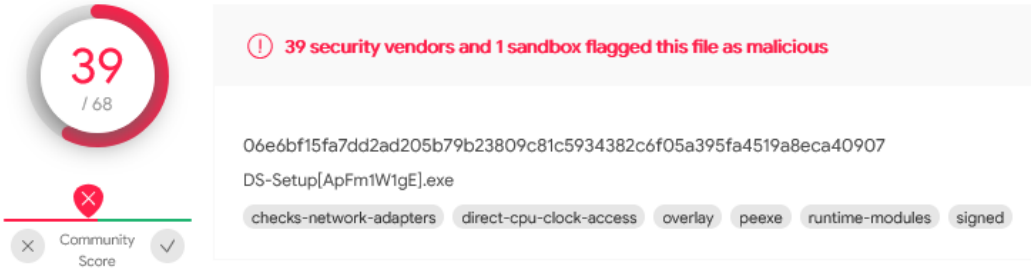
Аналогічно можна перевірити певний сайт, досить вказати його адресу у відповідному полі. Така перевірка є доцільною, якщо ви потрапили на сайт, який наполегливо пропонує оновити браузер, завантажити якусь програму або повідомляє про те, що на Вашому комп'ютері виявлено віруси.

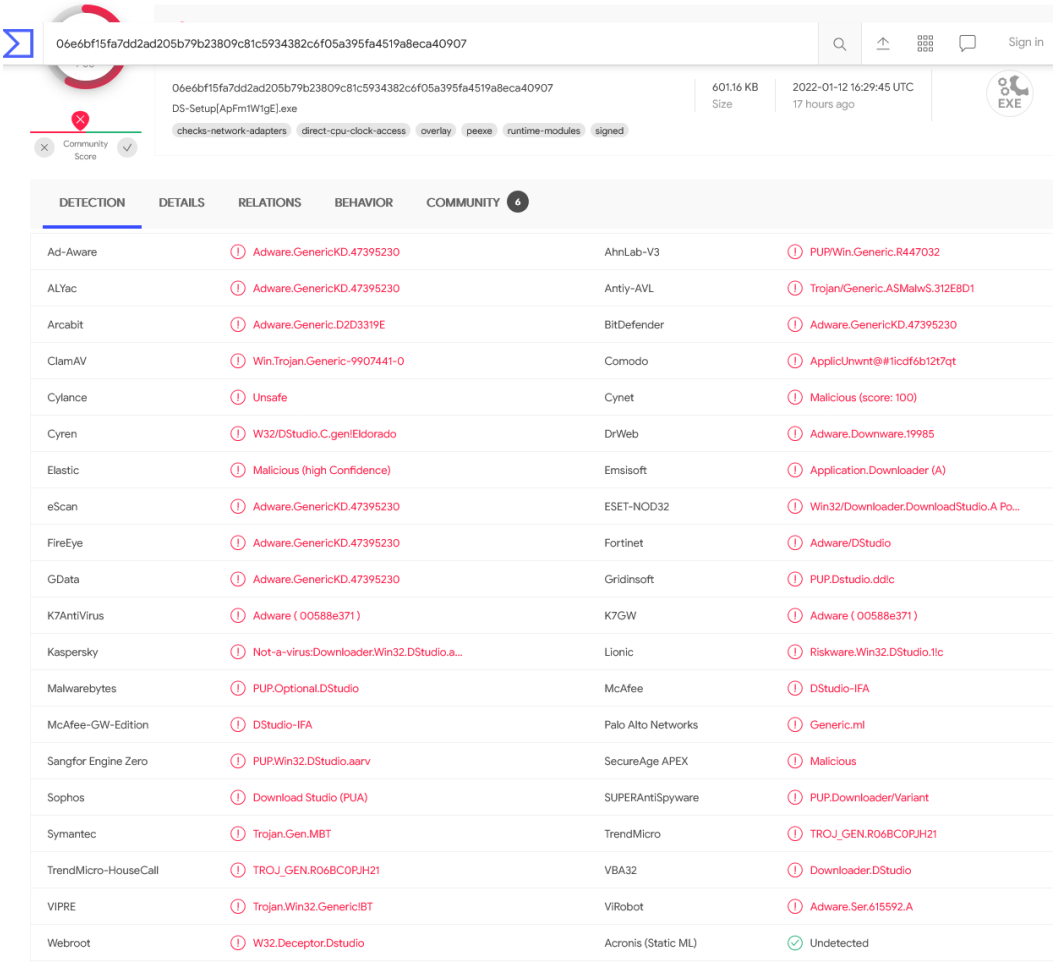
За бажанням, можна встановити VirusTotal як додаток у браузері чи безпосередньо на комп'ютер: VirusTotal Browser Extensiony

https://support.virustotal.com/hc/en-us/articles/115002700745-Browser-Extensions#google-chrome. При скачуванні файлів відбувається їх перевірка, корисним буде також додатково ознайомитися зі звітом VT4Browsers.

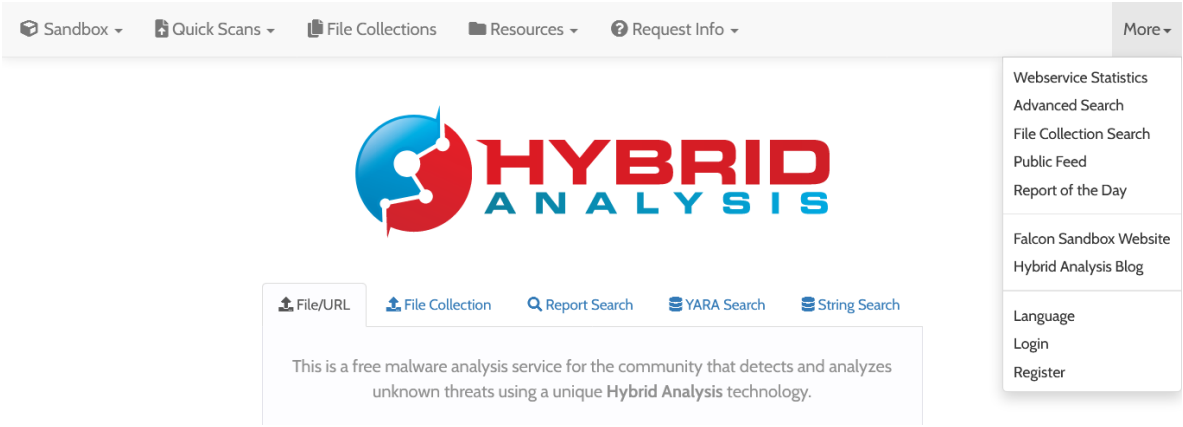
Результат перевірки збірки програм Beloff:



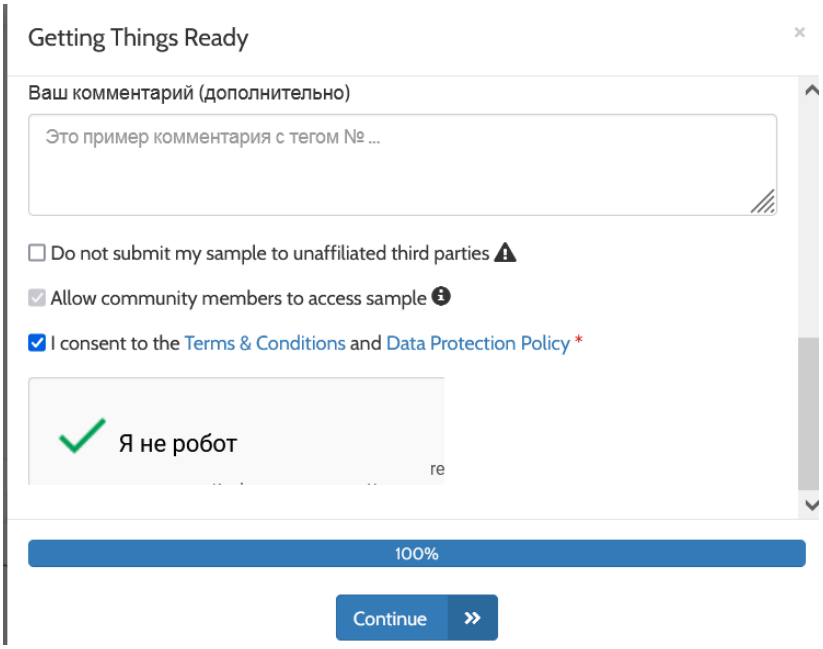




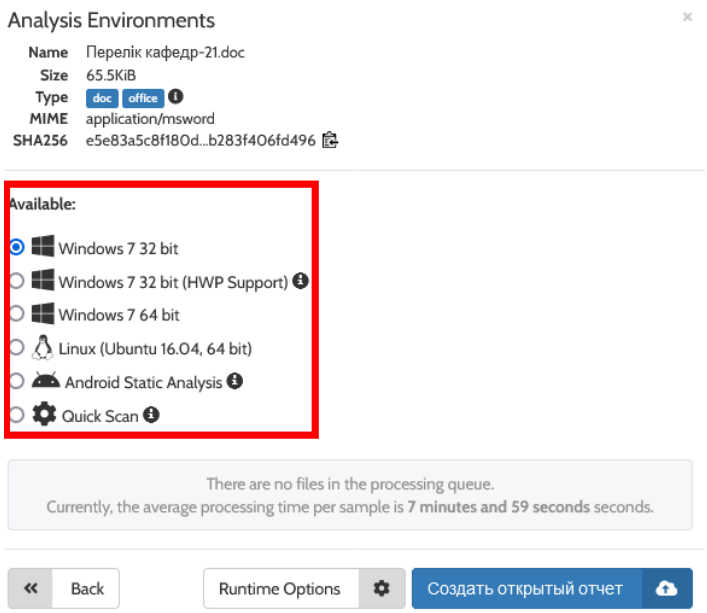
Hybrid Analysis (https://www.hybrid-analysis.com/) – дозволяє не лише виконати перевірку файлу на віруси, а й пропонує додаткові засоби аналізу шкідливих та потенційно небезпечних програм. На вкладці сайту «More» можна обрати зручну для вас мову.



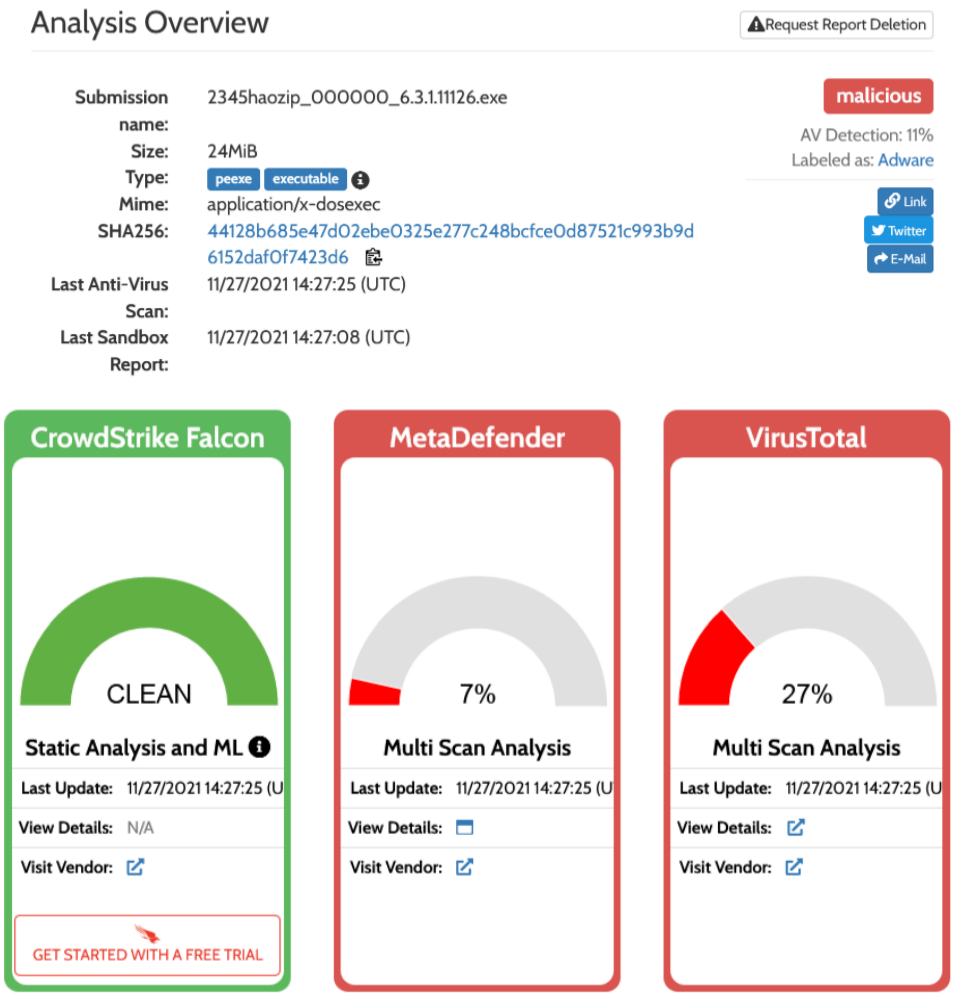
Далі завантажте файл чи вкажіть певну адресу, прийміть правила користування та підтвердить, що ви не робот, продовжте роботу.



Наступний крок – обрати, на якій віртуальній машині буде запущено Ваш файл для додаткової перевірки. Після вибору натисніть «Створити відкритий звіт».

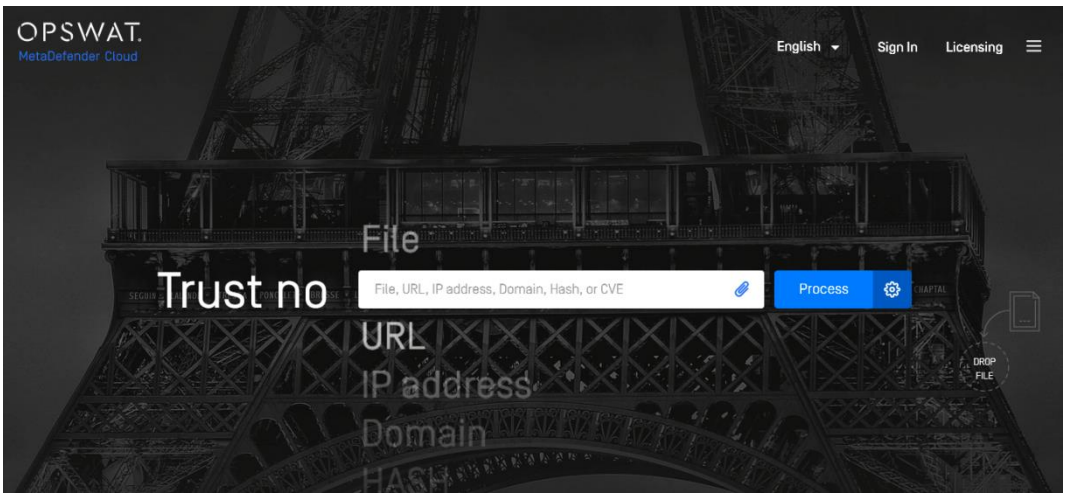


У результаті ви отримаєте наступні звіти: результат евристичного аналізу CrowdStrike Falcon, результат сканування в MetaDefender та результати VirusTotal, якщо раніше цей файл там перевірявся.



Через певний час (близько 10 хвилин) також з’явиться результат пробного запуску цього файлу у віртуальній машині. Якщо він запускався кимось раніше, результат з’явиться одразу. Залежно від результатів він може мати різний вигляд: у разі наявності підозрілих активностей ви побачите у заголовку Malicious. Можна переглянути детальні результати роботи віртуальної машини, зокрема скріншоти запуску програми чи відкриття документу.

MetadefenderCloud: офіційна сторінка https://metadefender.opswat.com. Без реєстрації доступно не більше 3 сканувань на добу.



Після завантаження файлу та його перевірки ви побачите зведення (Overview) з ім'ям загрози (за наявності), кількістю антивірусних движків, які виявили загрозу, а також результат голосування користувачів на тему безпеки файлу у правій колонці Community Insights. При відкритті розділу Static Analysis можна отримати докладну інформацію про результати, що були отримані під час сканування файлу в різних антивірусах і зробити попередні висновки щодо наявності загроз у перевіреному файлі. Додатково, у розділі Scan History можна ознайомитися з попередніми результатами сканування цього файлу (за наявності).

Натиснувши на кнопку шестерні отримаємо додаткові налаштування сканування:

Sandbox – запуск файлу, що перевіряється в пісочниці (віртуальній машині) з операційною системою Windows 10 чи Windows 7 й аналізом поведінки запущеного файлу. Існує вибір тривалості аналізу, а також браузера, що використовується в пісочниці (якщо передбачається, що загроза може впливати на роботу певного браузера);

розпакування архівів, що завантажуються (Unarchiving) – для перевірки файлів, які знаходяться в архіві, у тому числі й з паролем (у цьому випадку треба ввести пароль у полі «Archivepassword»).

Результат при перевірці файлу на наявність загроз із використанням запуску в пісочниці дозволяє отримати більш точне уявлення про те, які процеси створює програма, що запускається, отримати відомості про виконувані команди, звернення до записів у реєстрі та загальний висновок Metadefender про підозрілість процесу.

2. Онлайн-антивірус для перевірки комп'ютера.

Безкоштовна утиліта від Eset встановлюється на комп'ютер й дозволяє здійснити сканування щодо наявних загроз: https://www.eset.com/ua-ru/home/online-scanner. Не конфліктує зі встановленим на комп'ютері штатним антивірусом. Eset описує порядок роботи із сканером наступним чином.

1. Завантажте ESET OnlineScanner на вебсайті ESET. Для цього натисніть кнопку «Сканувати зараз». Для запуску програми двічі клацніть завантажений файл із розширенням .exe. виберіть мову продукту.

2. Клацніть «Початок роботи» й підтвердьте дію в діалоговому вікні Windows Керування обліковими записами користувачів. На екрані Умови використання клацніть Прийняти, якщо ви погоджуєтеся з умовами використання. Після прийняття умов використання на робочому столі створюється ярлик для ESET OnlineScanner.

3. Натисніть «Початок роботи» на екрані привітання. виберіть, чи потрібно брати участь у програмі підвищення якості програмного забезпечення та вмикати систему зворотного зв'язку. Клацніть «Продовжити».

4. Виберіть тип сканування. виберіть, чи потрібно вмикати виявлення потенційно небажаних програм, або налаштуйте параметри в розділі Додаткові параметри. Клацніть «Почати сканування».

5. Після завантаження оновлень модуля виявлення запускається сканування. Стан перебігу сканування відображається на індикаторі перебігу разом зі шляхом до сканованого файлу та його ім'ям. Сканування можна призупинити або скасувати в будь-який час.

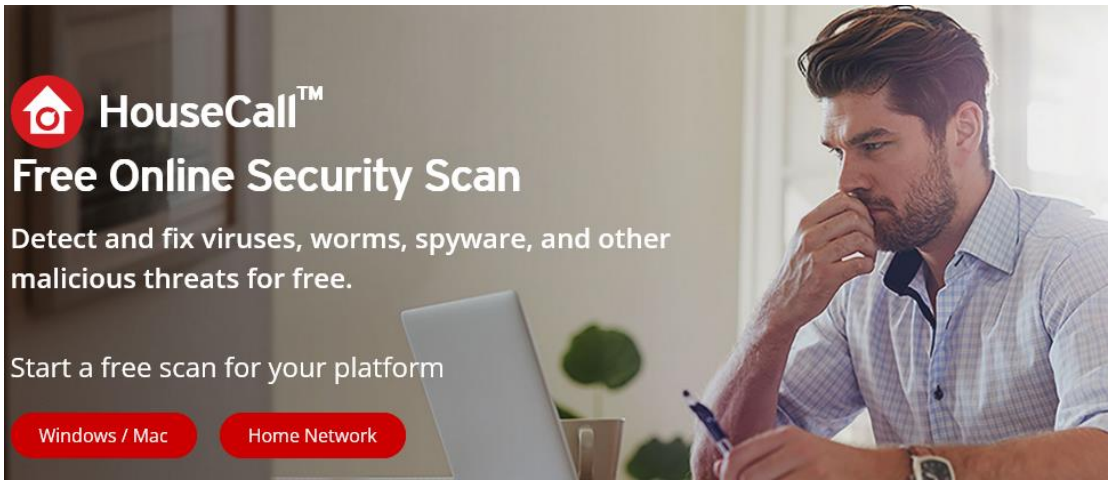
6. Після завершення сканування й виявлення загроз клацніть «Переглянути детальну інформацію». Для перегляду результатів сканування пізніше, оберіть «Зберегти журнал сканування» та «Продовжити».

Zillya! Сканер (https://zillya.ua/zillya-skaner) – вітчизняна програма, що сканує комп'ютер на наявність вірусів. Не вимагає установки на комп'ютер, достатньо лише завантажити та запустити, програму можна записати на змінний носій. Таким чином, ви завжди зможете виконати перевірку на віруси своїх файлів та папок, незалежно від того на якому комп'ютері вони знаходяться, а у разі потреби відразу виконати очищення заражених файлів. Запуск програми сканування можливий також і у безпечному режимі роботи Windows.

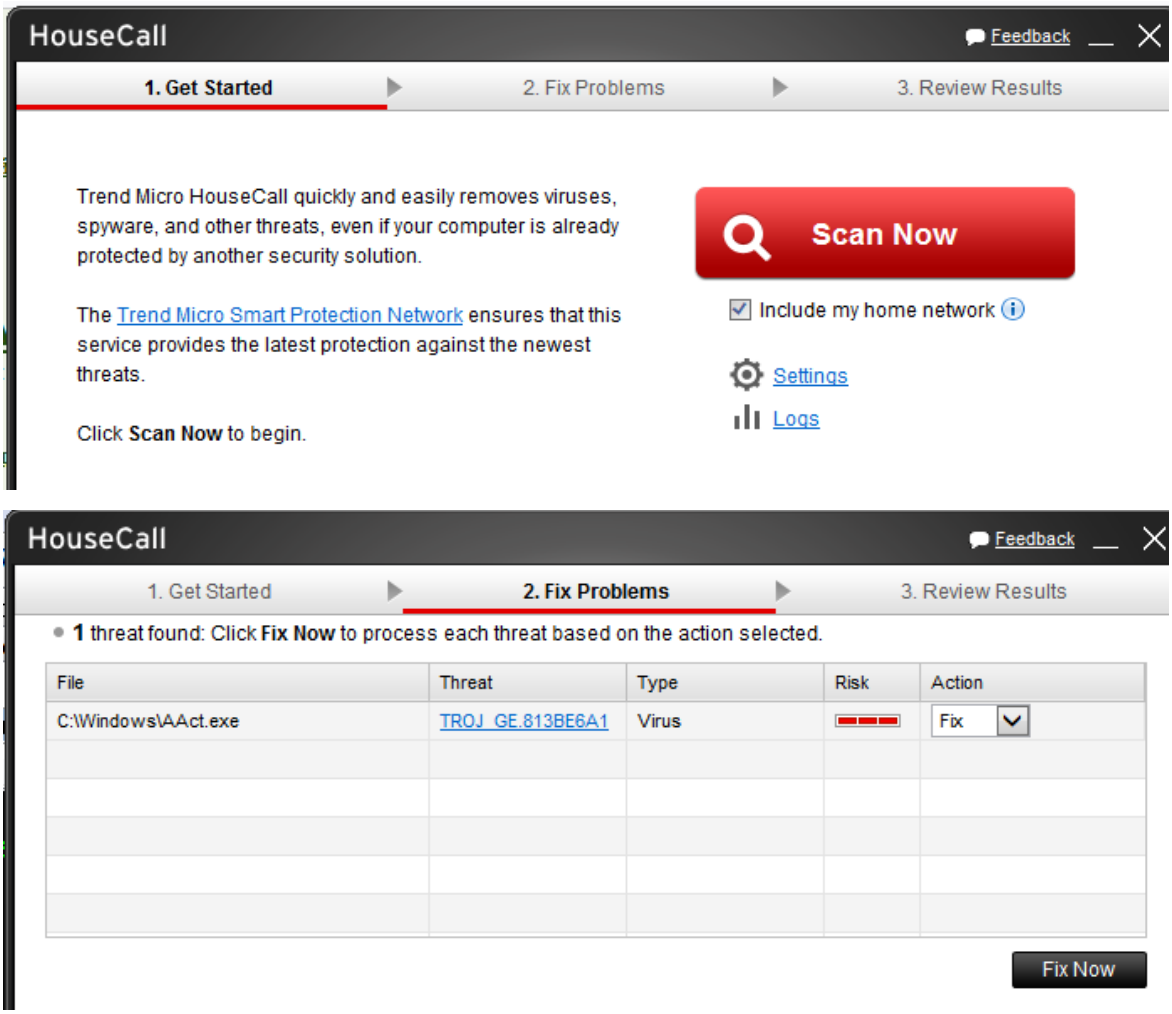
Онлайн-сканер від **TrendMicro** надає можливість обрати мову інтерфейсу, модуль запуску (лише 2,7 Мб) можна завантажити за наступною адресою: https://www.trendmicro.com/en_us/forHome/products/housecall.html.

Можна виконувати три типи антивірусних перевірок:

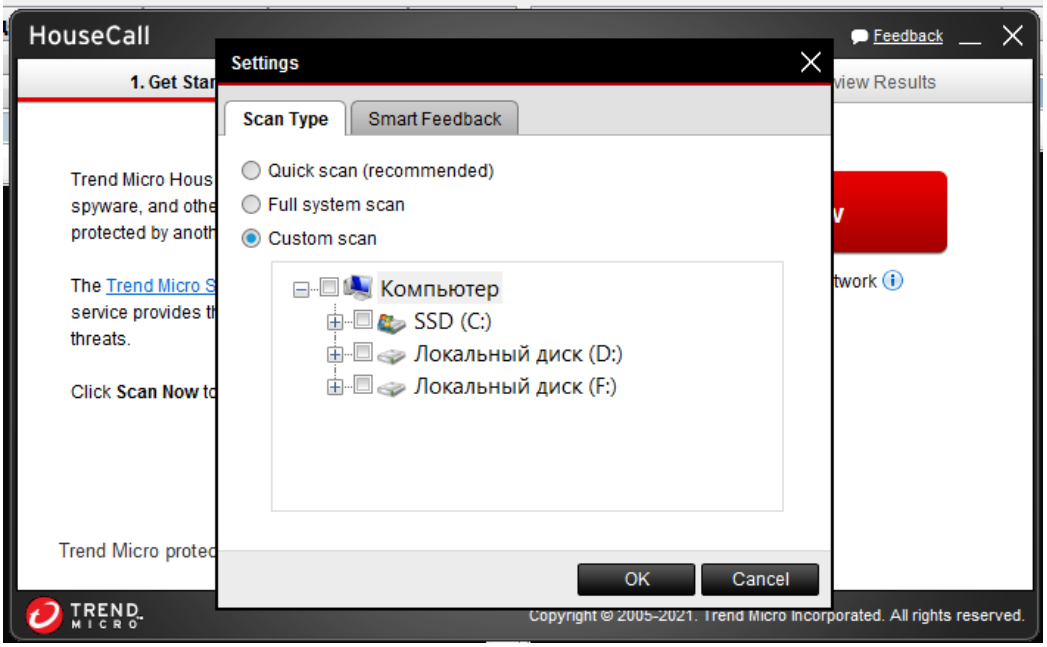
- швидке сканування – це сканування критичних областей системи для виявлення та видалення активних шкідливих програм, такі перевірки призначені для виявлення активних загроз та можуть бути виконані протягом декількох хвилин;
- повне сканування перевіряє всі системні області, у тому числі всі файли та папки, процес займає більше часу, але дає змогу перевірити весь комп'ютер на наявність загроз;
- вибіркове сканування перевіряє лише певні папки.

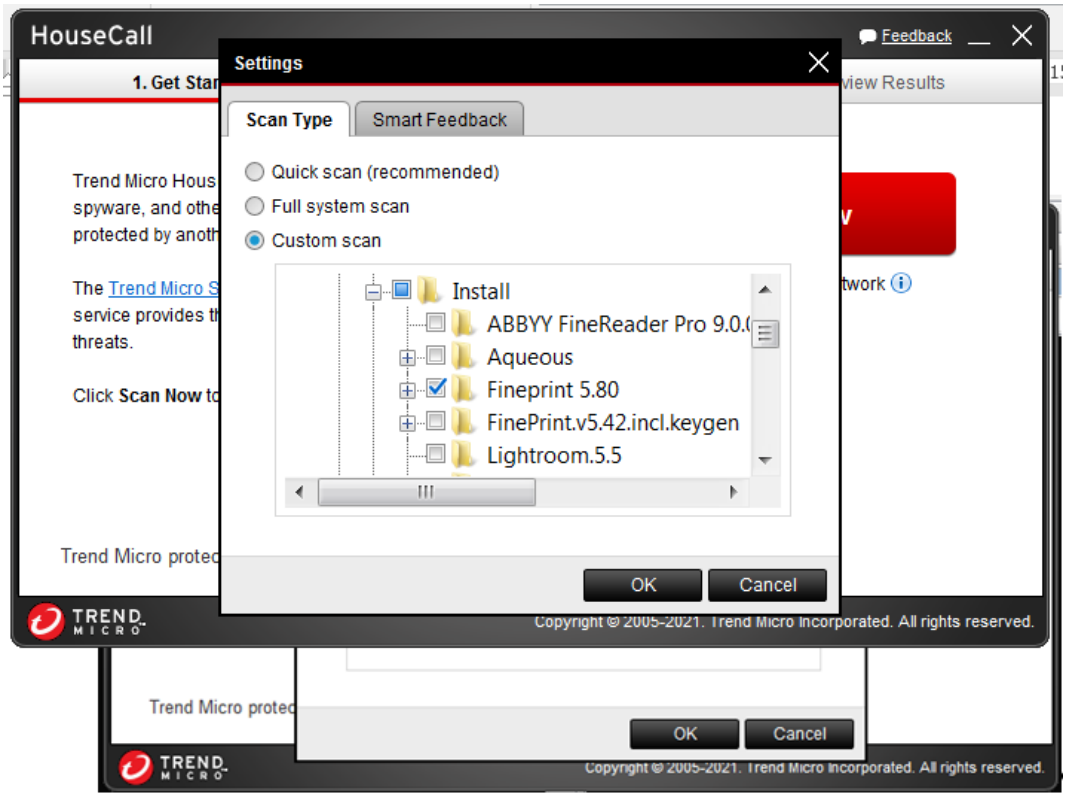


Швидке сканування виявило програму AAct, яка є інструментом незаконної активації Windows або інших продуктів Microsoft.



Для перевірки певних документів на комп’ютері, виберіть папку, яка містить підозрілі файли.


HouseCall
Feedback
Settings
Scan Type
Smart Feedback
Quick scan (recommended)
Full system scan
Custom scan
Компьютер
SSD (C:)
Локальный диск (D:)
Локальный диск (F:)
OK
Cancel
Trend Micro Hous
spyware, and othe
protected by anoth
The Trend Micro S
service provides th
threats.
Click Scan Now to
Trend Micro protec
TREND MICRO
Copyright © 2005-2021. Trend Micro Incorporated. All rights reserved.


HouseCall
Feedback
Settings
Scan Type
Smart Feedback
Quick scan (recommended)
Full system scan
Custom scan
Install
ABBYY FineReader Pro 9.0.(
Aqueous
Fineprint 5.80
FinePrint.v5.42.incl.keygen
Lightroom.5.5
OK
Cancel
Trend Micro Hous
spyware, and othe
protected by anoth
The Trend Micro S
service provides th
threats.
Click Scan Now to
Trend Micro protec
TREND MICRO
Copyright © 2005-2021. Trend Micro Incorporated. All rights reserved.

5. МЕРЕЖЕВА КІБЕРБЕЗПЕКА

5.1. Відстеження особистості та цифровий слід.

5.2. Безпека браузерів.

5.3. Технології Proxy, VPN, DNSFilter, Firewall, Wi-Fi.

5.1. Відстеження особистості та цифровий слід.

Цифровий слід (digital footprint) – це унікальний слід даних про діяльність, дії, повідомлення або транзакції користувача в цифрових носіях інформації. Цей слід можна залишити в Інтернеті, на комп'ютерах, мобільних пристроях чи інших носіях. Цифровий слід може використовуватися для відстеження діяльності та пристроїв користувача.

Цифрова тінь – це інформація, яку кожна сучасна людина створює про себе, сама того не підозрюючи, а цифровий слід – це гігабайти інформації, які користувачі щодня самостійно передають через Всесвітню павутину, відправляючи електронні листи з вкладенням, ділячись фільмом або публікуючи пости в соціальних мережах.

Обсяг цифрового сліду кожної людини щодня постійно збільшується. Відповідальність за зберігання та використання цієї цифрової інформації покладається на певні організації, Інтернет-сервіси, провайдерів та дата-центри, де інформація розміщується фізично.

Цифровий слід, який лишає людина має кілька складових.

1. Візуальна інформація. Фотографії, відеоролики, сигнал цифрового телебачення і камер зовнішнього спостереження.

Публікація фотографій та відео, де присутній користувач. Один раз з'явившись в Мережі, ці матеріали залишаються там назавжди, навіть якщо автор їх видалить. Це початок цифрового сліду того, хто опублікував фотографію і цифрової тіні всіх присутніх там людей.

Різні веб-архіви, копії баз даних, що постійно поновлюються не дадуть цим матеріалам зникнути безслідно. Багато фото-хостингів підкреслюють як

перевагу довічне зберігання фотографій, а більшість із них взагалі не видаляють завантажені клієнтами матеріали, лише за умови, що вони порушують закон.

2. Текстова інформація. використання текстової інформації, такої як електронні листи, онлайн спілкування, опубліковані статті, пости і тому подібне.

Це більше відноситься до цифрового сліду людини, але за наявності вмінь завжди можна витягнути приховану інформацію про інших осіб. Сучасні користувачі, зазвичай, мають акаунти в більшості сервісів обміну повідомленнями. Абсолютно все листування з друзями, колегами, сторонніми людьми залишається на сервері протягом тривалого часу, зберігається в резервних копіях і може бути використане третіми особами.

Це стосується багатьох сервісів електронної пошти та цифрових копій документів, які передаються і в яких є відомості про користувача. Наприклад, Gmail радить не видаляти кореспонденцію, а просто архівувати. І більшість людей так і роблять.

Часто користувачі для спілкування або реєстрації створюють логіни та нікнейми, які характеризують віртуальну індивідуальність особи. Такі відомості також стають частиною цифрового сліду.

3. Голосова інформація. Технологія VoIP, звичайні аналогові мережі, мобільний зв’язок.

Голосова складова цифрового світу найбільш проста для розуміння. Оператори зв’язку часто записують розмови своїх абонентів, хоча офіційно це не підтверджують, але вкладають гроші в обладнання для запису мільйонів своїх абонентів. Це зазвичай робиться для тестування алгоритмів щодо запобігання злочинної діяльності. Запис розмов є самим малопоширеним типом цифрового сліду та тіні.

VoIP-мережі займаються цим легальним шпигунством в меншій мірі, але існує ймовірність, що співрозмовник завжди має можливість записати розмову з метою використання отриманої цифрової тіні проти користувача.

4. Часова інформація. Записи кожної дії кожного користувача (логи) в Інтернет, які ведуться провайдерами і серверами вебсайтів. Така докладна інформація зважаючи на величезні обсяги (десятки гігабайт у день для відвідуваного сайту) недовговічна – лог-файли автоматично видаляються раз у декілька днів. Але витягнуті з логів важливі дані зберігаються довго.

Навіть в ситуації, коли людина не спілкується в Інтернеті і відімкнула телефон, вона постійно знаходиться під наглядом. У великих містах в місцях масового скупчення присутнє приховане і явне відео спостереження. Камери дорожнього спостереження реєструють пересування всіх транспортних засобів з їх номерами і швидкістю. Звичайні веб-камери і охоронні системи офісів та будинків що записують усі пересування людей, є прекрасними помічниками для тих, хто хоче обчислити маршрути й навіть розпорядок дня певної особи.

Цифрова тінь зазвичай формується без відома людини. Наприклад, випадкове потрапляння машини користувача в кадр чужої фотокамери, але цю фотографію публікують в Інтернеті. Дехто починає обговорювати цю машину, з'ясовується номер та інформація про господаря з'являється на форумі. Починається обговорення, і генерується багато ключових слів, за якими можна знайти цю машину на фотографії. І тепер ця фотографія сформувала цифрову тінь для власника машини.

На сьогодні головним засобом для збільшення цифрової тіні людини стали мобільні телефони з вбудованими камерами, що дозволяють буквально знімати кожен крок, блоги, електронні щоденники та соціальні мережі. Сучасні Інтернет-сервіси поєднують і засоби спілкування, і файловий сервер під зберігання фотографій, і навіть хостинг потокового відео.

Значна кількість людей під час реєстрації вказує справжні прізвище та ім'я, домашню адресу, телефони та іншу особисту інформацію. На сьогоднішній день мільйони людей по всьому світу з задоволенням прагнуть викласти побільше своїх фотографій, відео та контактних даних, щоб їх онлайн-друзі могли подивитися та залишити коментарі. При цьому ніхто не підозрює, що навіть закрита від відвідувачів сторінка завжди доступна для

адміністраторів і хакерів. І вже відомі факти масового злому і викрадення баз даних із подібних сервісів.

Цифрова тінь – явище доволі небезпечне. З поліпшенням якості фото- та відео- техніки, зростанням обсягу пам'яті та швидкості Інтернету, вона буде ставати все більш осяжною і небезпечною. Найголовніша небезпека цифровий тіні полягає в тому, що люди не в змозі її контролювати. З часом вона буде структурована, між тінню і цифровим слідом вже не залишиться різниці.

Файли cookie – інформація у вигляді текстових або бінарних даних, отриманих від вебсайту, яку збережено у клієнта для відправлення на той самий сайт при повторному відвідуванні. Вони також можуть зберігати облікові дані, щоб полегшити вам вхід на раніше відвіданий сайт.

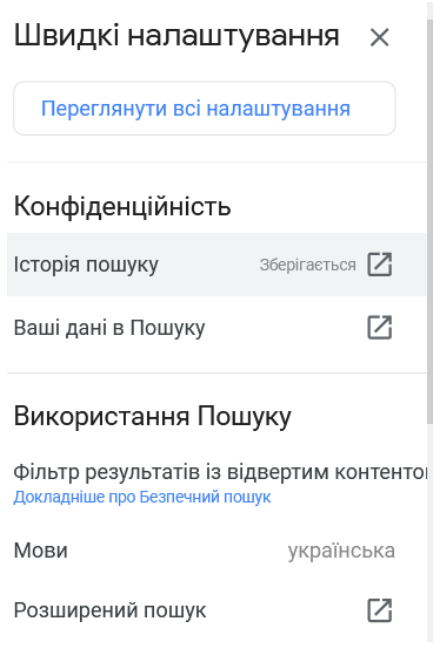
Сесійні файли cookie існують лише під час перебування на вебсайті. Після виходу з цього вебсайту cookie автоматично зникає.

Інші файли cookie називаються стійкими. Вони певний час залишаються на вашому жорсткому диску (іншому пристрої зберігання даних) й використовуються для автентифікації.

Також існує певний різновид стійкого файлу cookie – сторонні файли cookie. Вони генеруються на інших вебсайтах, ніж той, який ви відвідуєте. Зазвичай, сторонні файли cookie пов'язані з рекламою та використовуються рекламодавцями для відстеження активності користувача на всіх сайтах, що містять їх оголошення. Ці файли cookie збирають багато інформації: що саме ви шукаєте в Інтернет-магазині, місцезнаходження (через IP-адресу), конфігурацію пристрою, скільки часу ви провели на певному сайті, публікації у Facebook та багато іншого.

Вебсайти, які використовують файли cookie, законодавством змушені інформувати вас про цю ситуацію та пропонувати кнопку прийняти або відхилити їх.

Зібрати дані про користувачів сьогодні легко, здебільшого вони самі їх надають в обмін на використання різних сервісів. Величезна кількість корисних продуктів Google доступна для користувачів безкоштовно, але натомість потрібно погодитися на збір і обробку персональних даних. Google постійно збирає статистику про своїх користувачів: пам'ятає запити, відвідані сайти, гео-дані, кількість надісланих листів, фотографій, часто вживані слова. Google підлаштовується під користувача, а отже, знає і його звички.



Єдиний спосіб зламати та отримати ці дані – отримати доступ до облікового запису Google. Тому обліковий запис Google захищає двоетапна аутентифікація та якісна реалізація безпеки для мобільних пристроїв (наприклад, можна віддалено заблокувати смартфон або акаунт).

Користувач може дозволити чи заборонити стежити за певними активностями для покращення підбору інформації: особиста інформація користувача; дані в обліковому запис Google і його місце перебування; дії користувача; поточний пошуковий запит; історія пошуку; діяльність облікового запису Google; взаємодії з оголошеннями; сайти, які він відвідував; дії в мобільних додатках; дії на інших пристроях під власним акаунтом в Google; час доби; інформація, яку користувач надав рекламодавцю. Наприклад, адреса електронної пошти, вказана при підписці на розсилку.

Також Google зберігає інформацію про всі додатки та розширення, які є на вашому пристрої. Компанії відомо, як часто, де і з ким ви використовуєте їх. Ця функція зберігає дані з телефонів і планшетів: контакти, календарі, додатки, музика, інформація щодо пристрою (наприклад, рівень заряду батареї, версія Android, місцезнаходження).

Листи Gmail – дані про електронне листування, відстежується кількість отриманих і відправлених листів. Сам інтерфейс Gmail містить блоки з рекламними оголошеннями. Процес показу оголошень в Gmail повністю автоматизовано, і реклама підбирається з врахуванням дій користувача в обліковому записі Google.

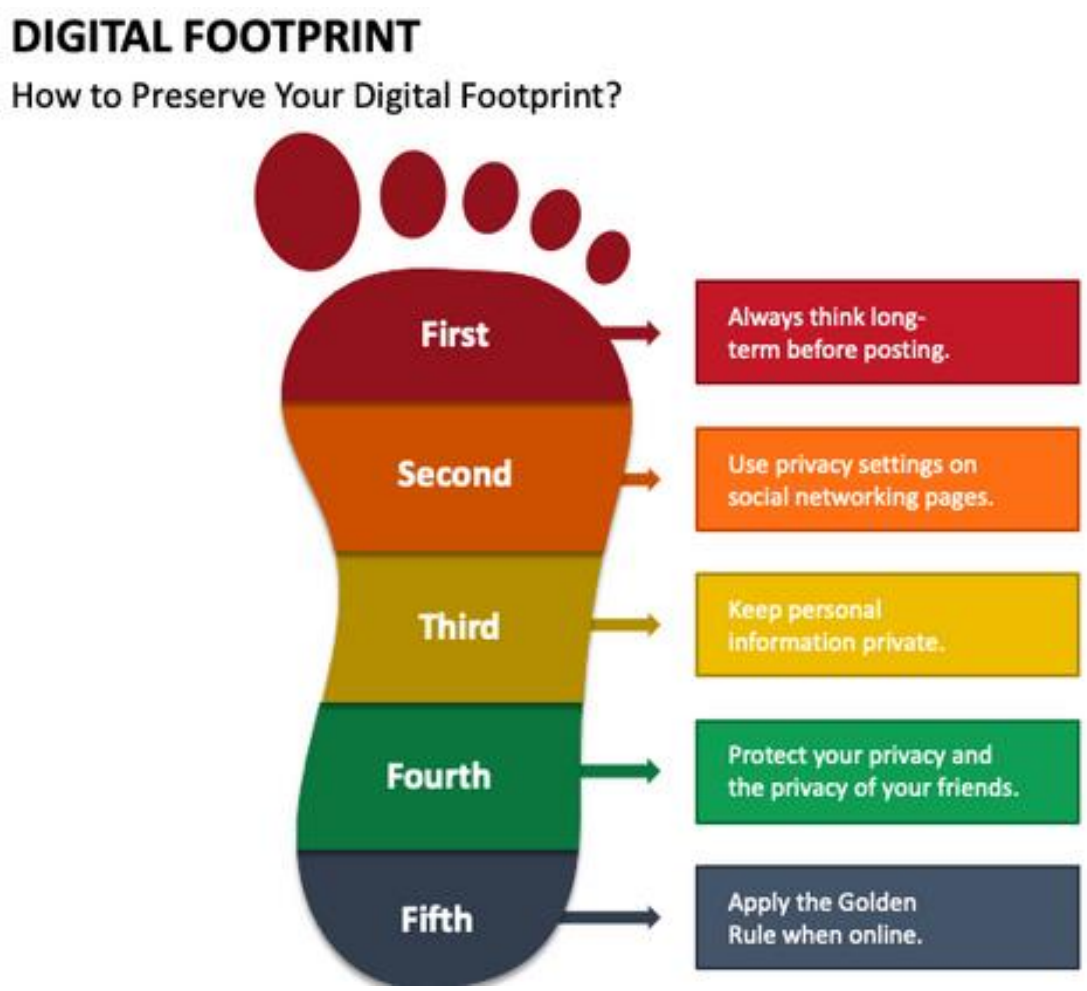
Ситуації зі збором даних не можна розглядати лише з одного боку. Дізнавшись більше інформації про користувача, рекламодавці зможуть запропонувати йому дійсно корисний продукт. Причому саме в потрібний час і в потрібному місці. Найчастіше користувачеві навіть не доводиться нічого шукати. Необхідні товари, місця і послуги приходять до нього самі. Такий підхід відмінно економить час і допомагає швидше знайти потрібну інформацію. Цей досвід можливий при дотриманні певних умов: дані повинні збиратися і зберігатися у відповідності до політики конфіденційності та законодавства.

Як зменшити цифровий слід та цифрову тінь.

1) Розділіть акаунти. Придумуйте випадкові імена акаунтів електронної пошти для особистого використання. Створюйте окремі акаунти для фінансових операцій, реєстрації в соцмережах і загального призначення. Не використовуйте справжню дату народження, не вводьте повне ім’я або використовуйте вигадані імена для кожного акаунту. Для непублічних акаунтів, використовуйте випадкові зображення профілю.

2) Не повторюйте паролі. використовуйте менеджер паролів щоб генерувати окремі паролі для кожного онлайн-сервісу. Для додаткового захисту налаштуйте двухфакторну аутентифікацію.

3) видаляйте метадані, приховуйте геолокацію.



4) Приховуйте підказки. видаляйте EXIF (якщо це не відбувається автоматично) перед публікацією фото в соцмережах. Але залишаються підказки на самому фото: силуети будівель, рекламні вивіски, відображення в дзеркалі, документи на робочому столі. Такі деталі полегшують ідентифікацію особистості, пошук місця розташування офісу або домашньої адреси, а також складають уявлення про спосіб життя цілі.

5) Навчіться мовчати. Розміщення контенту в мережі – загроза конфіденційності. Перш, ніж опублікувати коментарі або фото, подумайте: чи дає це зловмисникові інформацію для створення досьє на людину або компанію.

Перевірте налаштування конфіденційності в соцмережі: хто саме може переглядати ваші публікації та особисті дані та яку кількість інформації можуть бачити відвідувачі. У список друзів краще додавати лише людей, з якими ви особисто знайомі, бажано перевірених й надійних. Далі необхідно очистити існуючий список друзів: почніть із видалення з друзів усіх незнайомців, яких ви

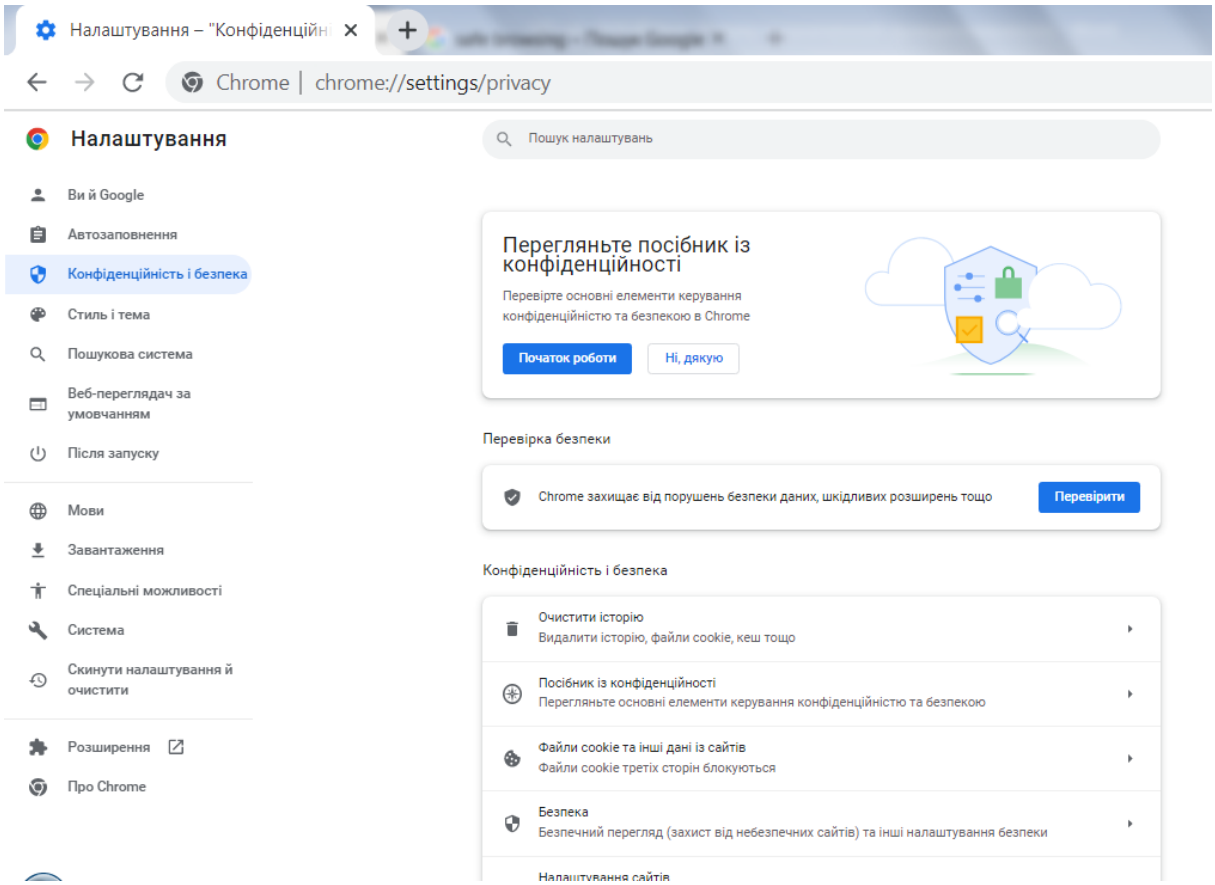
навіть не пам’ятаєте, а потім переходьте до знайомих, яких ви не дуже добре знаєте, а також до людей, з якими перестали спілкуватися.

Не ділитися таємницями за допомогою повідомлень. Дописувач може зберегти переписку з секретами і використовувати її для шантажу чи інших дій. Не відповідайте на повідомлення, які приходять від незнайомців, навіть якщо вони здаються буденними й містять фрази типу «Привіт, як справи?» Або «Нумо познайомимося». Ігноруйте навмисно образливі повідомлення, а дописувачів відразу відправляйте до чорного списку чи поскаржиться на них адміністрації сайту.

5.2. Безпека браузерів.

Google Chrome забезпечує високий захист від шкідливих сайтів, але, водночас, він збирає інформацію щодо користувачів. Із випуском Chrome 76.10 в грудні 2019 року, користувачі можуть отримувати попередження, якщо їхні паролі будуть виявлені в списках і базах, раніше зламаних хакерами та виставлених в загальний доступ. Сам Chrome гарантує, що його можна вважати найбезпечнішим браузером, завдяки своїм трьом функціям:

- безпечний перегляд сторінки, який попереджає про можливі загрози при відкритті фішингового або шкідливого вебсайту;
- режим пісочниці, який надає додатковий рівень захисту і запобігає автоматичному встановленню шкідливих програм (особливо в фоновому режимі);
- автоматичні оновлення, що дозволяють встановлювати всі оновлення і усувати недоліки безпеки;
- унікальні паролі генеруються і зберігаються у веб-браузері автоматично;
- браузер має режим інкогніто і пропонує налаштування параметрів конфіденційності вручну.



Mozilla Firefox є одним із найближчих конкурентів Google Chrome. Ще у 2017 році версія Mozilla Quantum містила такі можливості:

- Linux Sandboxing, який запобігає спробам злому;
- захист від стеження, який блокує компоненти відстеження на відвідуваних користувачем вебсайтах;
- покращений центр управління, що дозволяє отримувати доступ до численних параметрів і налаштовувати їх для забезпечення найбільш безпечних і приватних сеансів перегляду, які може запропонувати браузер;
- Contextual Feature Recommender (CFR) — система, яка рекомендує доповнення та функції, що спираються на досвід перегляду контенту користувача;
- поліпшений захист від стеження, який повністю вимикає стеження.

Opera – ще один браузер в списку «найбезпечніших браузерів». Із 2016 десктопна версія цього браузера на базі Chromium включала вбудований блок захисту від реклами. Opera пропонує кращу конфіденційність користувачів, додавши вбудовану віртуальну приватну мережу – VPN.

Інші функції безпеки, які надаються розробником:

- значки безпеки пропонують перевірену інформацію про сторінку;
- захист від шахрайства і шкідливих програм – попереджає про сайти, що становлять потенційну небезпеку;
- блокування реклами працює як будь-який інший сторонній додаток, що дозволяє блокувати рекламу.

Але браузер збирає деяку інформацію про користувачів і може ділитися нею з довіреними партнерами та компаніями.

Експерти антивірусної лабораторії Zillya! підготували список із семи кращих додатків для браузера, які допоможуть зробити Інтернет-серфінг безпечним.

Adblock Plus – один із найпопулярніших додатків для браузера. Adblock Plus дозволяє блокувати настирливу рекламу, спливаючі вікна та інші неприємні об'єкти на сторінці. Доповнення приховує не всю рекламу, а лише ту, яка не відповідає критерієм «ненав'язливості». Правильно оформлена реклама потрапляє в так званий білий список і відображається користувачеві. Підтримувані браузери: Internet Explorer, Firefox, Chrome, Opera, Safari. Офіційна сторінка доповнення: https://adblockplus.org/.

NoScript – це доповнення підвищує рівень безпеки користувача шляхом тотального блокування JavaScript, Java та іншого контенту в браузері, який завантажується з вебсайтів або запускається на ПК користувача. Таким чином NoScript захищає користувача від різноманітних скриптів, XSS-атак, хакерських маршрутизаторів, тощо. Підтримувані браузери: Firefox, SeaMonkey. Офіційна сторінка доповнення: http://noscript.net/getit.

AdwCleaner – дозволяє позбутися від рекламного ПЗ на комп'ютері. Програма сканує систему і виявляє будь-яке рекламне ПО, надбудови та програми, які підпорядковують собі комп'ютер користувача. Підтримувані браузери: Internet Explorer, Firefox, Chrome. Сторінка доповнення: http://www.bleepingcomputer.com/download/adwcleaner/.

Ghostery – це доповнення захищає конфіденційну інформацію користувача при відвідуванні сайтів в Інтернеті. Ghostery відстежує «невидиму» сторону Мережі, в якій знаходяться шпигуни, мережеві жучки і маяки, розміщені на сайтах рекламними агентами різних компаній, які дозволяють збирати дані про користувачів в Інтернеті. Доповнення Ghostery надає користувачеві інформацію про кожну виявлену компанію, доповнюючи звіт посиланнями на політики конфіденційності та налаштування збору інформації цих компаній. Підтримувані браузери: Internet Explorer, Firefox, Chrome, Opera, Safari. Офіційна сторінка доповнення: https://www.ghostery.com.

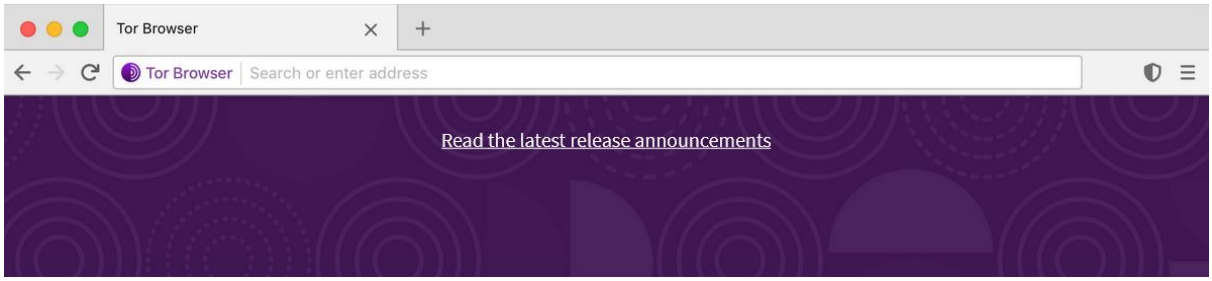
AVG PrivacyFix – це доповнення для управління налаштуваннями конфіденційності соціальних мереж, пошуковиків та вебсайтів. AVG PrivacyFix виконує сканування налаштувань профілів користувача в соціальних мережах і визначає проблеми конфіденційності. Якщо профілі налаштовані таким чином, що приватна інформація користувача наражається на небезпеку, то додаток допоможе це виправити. Доповнення AVG PrivacyFix так само, як і Ghostery, може визначити компанії, які шпигують за діяльністю користувача в Інтернеті та подивитися політику конфіденційності цих компаній. Підтримувані браузери: Firefox, Chrome. Офіційна сторінка доповнення: https://www.privacyfix.com/start/install.

PrivDog – сканує відвідувані вебсайти щодо наявності шкідливого контенту, блокуючи непотрібні рекламні об’єкти. Також, PrivDog прискорює швидкість відкриття сайтів шляхом зменшення кількості cookies, шпигунів і реклами. Підтримувані браузери: Internet Explorer, Firefox, Chrome. Офіційна сторінка доповнення: http://www.privdog.com/.

WOT (Web of Trust) – це надбудова до браузера, яка попереджає користувача про сайти з низькою репутацією. WOT – це своєрідне співтовариство користувачів, кожен із яких, перебуваючи на тому чи іншому Інтернет-ресурсі, може поставити йому оцінку. На основі цих оцінок створюється репутація ресурсу. Рейтинги сайтів постійно оновлюються багатомільйонною аудиторією. Підтримувані браузери: Internet Explorer,

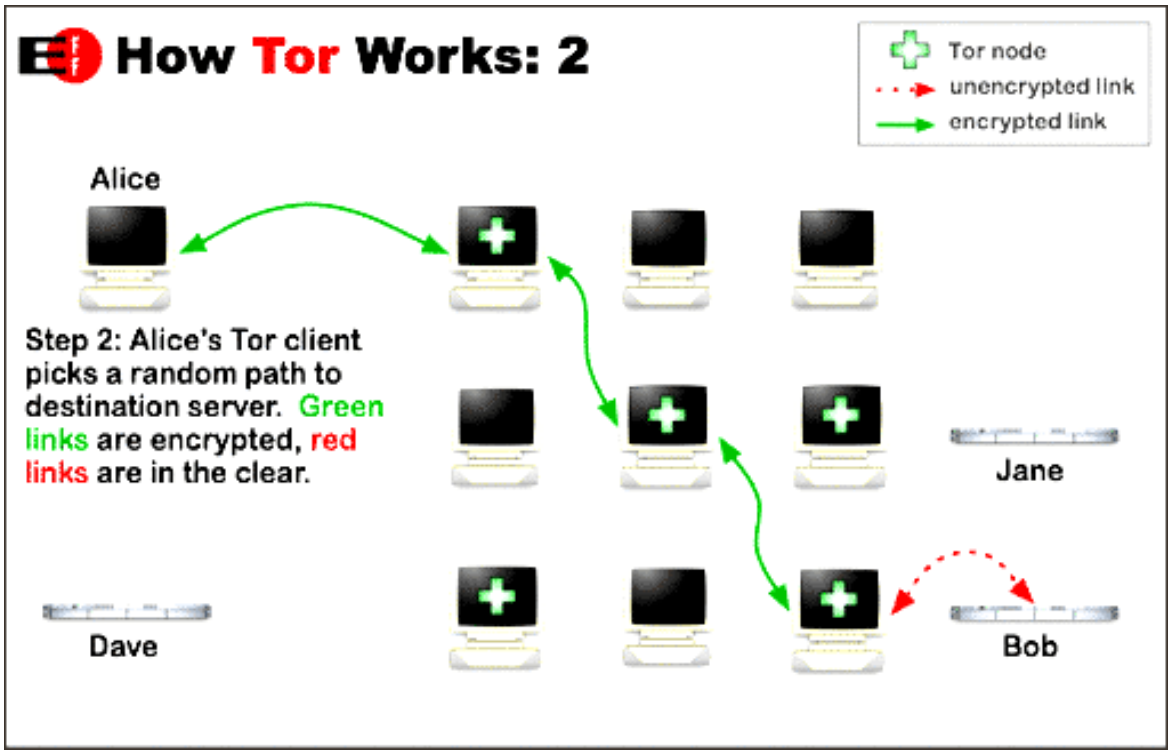
Firefox, Chrome, Opera, Safari. Офіційна сторінка доповнення: https://www.mywot.com.

Браузер Tor – безкоштовна, відкрита та некомерційна програма, яка дає користувачам анонімний доступ до Інтернету. Основна ідея проекту – забезпечити вільний та безпечний доступ до Мережі. Для звичайних користувачів – це спосіб захистити себе та свій трафік не тільки від влади, а й від провайдерів, власників публічних Wi-Fi-точок та сайтів, а також спосіб обійти блокування деяких сайтів.



Tor існує завдяки величезній мережі комп'ютерів-волонтерів, які розкидані по всьому світу. Назва Tor – The Onion Router англійською, або цибульний маршрутизатор – відсилає до принципу роботи браузера. Tor зашифровує ваш трафік тричі, ніби створюючи три шари цибулини. Зашифрований трафік прямує до комп'ютера А, який знімає перший шар шифрів і бачить адресу комп'ютера В. Комп'ютер В, знімаючи ще один шар, бачить адресу комп'ютера С, не знаючи при цьому, звідки трафік прийшов спочатку і куди він прямує зрештою. І лише через комп'ютер С ви виходите в Інтернет.

Хто б не стежив за вами чи вашим трафіком –провайдер чи влада – вони можуть дізнатися, що ви користуєтеся браузером Tor, але не вашу мету. Щоразу ви потрапляєте в Інтернет за допомогою випадкового комп'ютера-волонтера, а сам браузер за замовчуванням не зберігає історію ваших дій, тому в Інтернеті ніхто не дізнається, хто ви, і не зможе отримати інформацію про вас.



Через цибульну структуру браузер Tor уповільнює швидкість вашого Інтернет-з'єднання. Стрім відео чи музики через Tor, швидше за все, буде особливо повільним. Браузер не зможе захистити вас, якщо ви самі видаєте інформацію про себе в Інтернеті або якщо на вашому комп'ютері є віруси чи програми, які стежать за вашим Інтернет-користуванням.

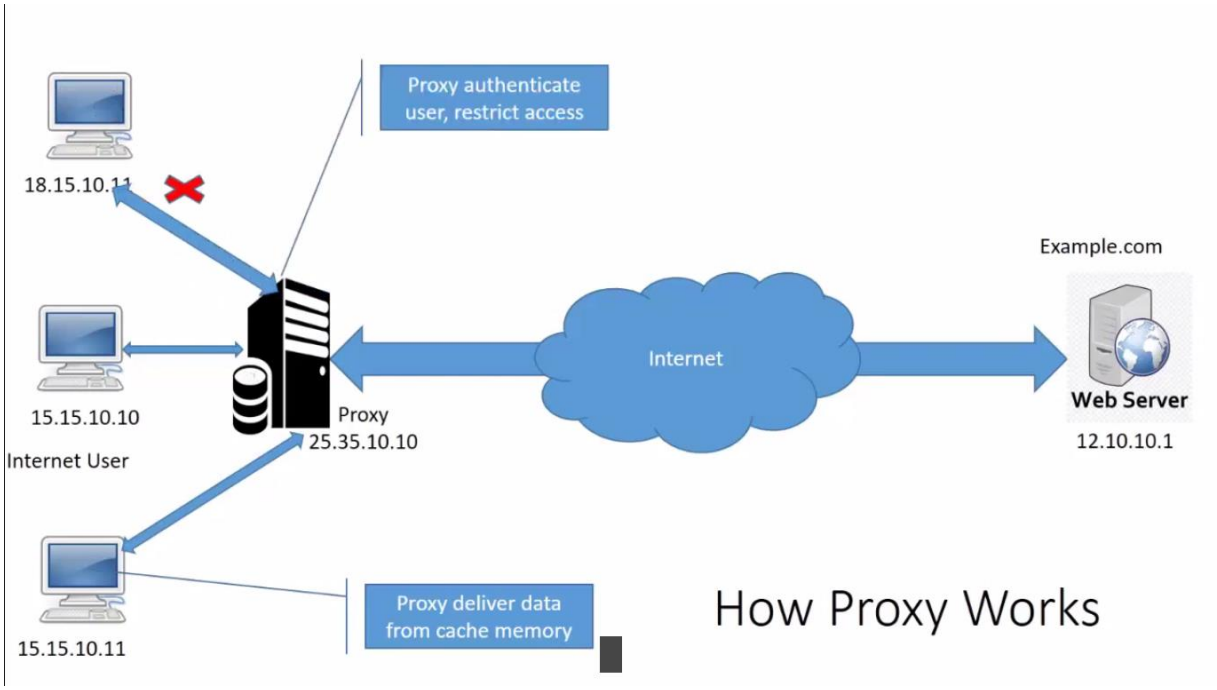
5.3. Технології Proxy, VPN, DNSFilter, Firewall, Wi-Fi.

5.3.1. Проксі сервер (proxy – «представник, уповноважений», право користуватися чимось від чужого ім'я) – це служба в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі запити до інших мережних служб. Спочатку клієнт підключається до такого сервера і запитує у нього деякий ресурс, що розташований на іншому сервері в Інтернеті. Далі сервер або підключається до вказаного сервера й отримує ресурс у нього, або надає ресурс із власного кешу.

Технологію проксі застосовують з метою:

- забезпечення доступу з комп'ютерів локальної мережі до Інтернету;
- кешування даних – якщо часто відбуваються звернення до одних і тих самих зовнішніх ресурсів, можна тримати їх копію на сервері та видавати за

запитом, знижуючи цим навантаження на канал у зовнішню мережу і прискорюючи отримання клієнтом запитаної інформації;



- стиснення даних – сервер завантажує інформацію з Інтернету та передає інформацію кінцевому користувачеві в стислому вигляді;
- захисту локальної мережі від зовнішнього доступу – наприклад, можна налаштувати сервер так, що локальні комп'ютери будуть звертатися до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звертатися до локальних взагалі;
- обмеження доступу з локальної мережі до зовнішньої – наприклад, можна заборонити доступ до певних вебсайтів, обмежити використання Інтернету певним локальним користувачам, встановлювати квоти на трафік або смугу пропускання, фільтрувати рекламу та віруси;
- анонімізації доступу до різних ресурсів. Проксі-сервер може приховувати інформацію про джерело запиту або користувача. У такому разі цільовий сервер бачить лише інформацію про сервер, наприклад IP-адресу, але не має можливості визначити справжнє джерело запиту. При звертанні до web-серверів proxy «підмінить» IP-адресу користувача на свою й зловмисник буде намагатися вторгнутися не до користувача, а на proxy-сервер (у якого набагато більш потужна система захисту).

Але не всі proxy-сервера в Internet є анонімними (підміняють IP-адресу користувача). Більшість із них призначено для прискорення доступу в Internet й не приховують вашу IP-адресу. Для пошуку анонімних проксі-серверів доцільно скористатися сервісом Proxy Checker або аналогічним.

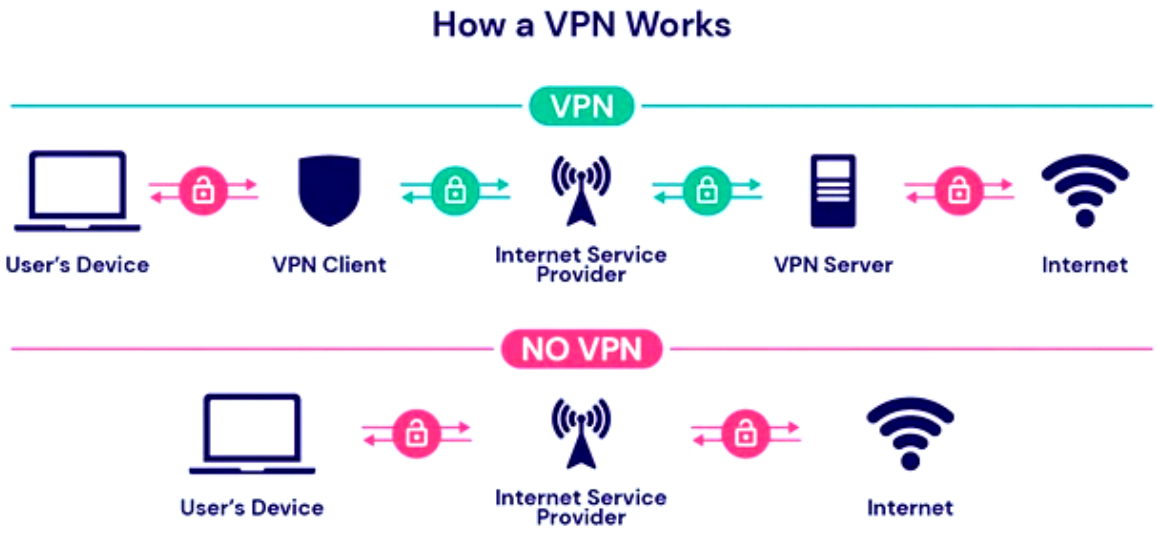
Проксі сервери бувають декількох типів:

- FTP проксі використовуються для завантаження даних на сервери FTP;
- CGI проксі (анонімайзери) допомагають відкрити будь-який вебсайт прямо у браузері. Жодних додаткових налаштувань не потрібно. Найчастіше такі проксі виконані у вигляді вебсайту, де можна ввести адресу сайту, яку необхідно відвідати;
- SMTP, POP3 та IMAP проксі використовуються для надсилання та отримання електронної пошти;
- HTTP та HTTPS проксі призначені для перегляду веб-сторінок;
- Socks проксі передає всі дані на кінцевий сервер як клієнт, тому вважається найбільш анонімним протоколом.

При роботі з будь-яким проксі ви повинні пам’ятати, що проксі сервер здатний вести логи (звіти роботи), зберігаючи всю інформацію про вашу IP-адресу та всі запити, які виконувались з неї, включаючи паролі, логіни та інші важливі конфіденційні дані. Також проксі сервера можуть бути під контролем спецслужб або зловмисників, а часом їх створюють спеціально для перехоплення та аналізу трафіку.

5.3.2. VPN (Virtual Private Network, віртуальна приватна мережа) – узагальнена назва технологій, які дозволяють створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному пристрою чи користувачу бути повноцінним учасником віддаленої мережі та користуватися її сервісами – внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет. Безпека передавання інформації через загальнодоступні мережі

реалізована за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об'єднати декілька географічно віддалених мереж (або окремих клієнтів) в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.



Коли ви підключені до VPN-серверу, то весь ваш Інтернет-трафік шифрується. Це означає, що ніхто не може відстежити, що ви робите в Інтернеті – навіть ваш Інтернет-провайдер. Окрім того, Інтернет-провайдер не зможе обмежити швидкість вашого підключення. Шифрування також запобігає отриманню хакерами доступу до вашої чутливої та важливої інформації, яку ви вводите на вебсайтах, наприклад, до паролів. використання VPN у смартфоні особливо важливо, якщо ви використовуєте відкриті публічні WiFi-мережі, оскільки кіберзлочинцям дуже просто відстежувати ваше підключення до публічних мереж.

VPN приховує вашу справжню IP- адресу. Існує декілька причин, чому варто використовувати VPN-з'єднання. По-перше, ваша IP-адреса може бути використана для визначення вашого реального місцезнаходження, що в свою чергу загрожує вашій конфіденційності, особливо в поєднанні з іншою персональною інформацією.

По-друге, багато вебсайтів, таких як Netflix, HBO, Hulu, BBC iPlayer, Amazon Prime Video та багато інших, на підставі вашої IP-адреси визначають, доступ до якого контенту ви отримаєте. Крім того, через наявність

геопросторових блоків, ви не можете отримати доступ до багатьох популярних ТВ-каналів, особливо поза межами країн їх трансляції. Єдиним способом обійти гео-просторове блокування є маскування вашої реальної IP-адреси та підміна її на іншу, а саме це й робить VPN.

Також VPN блокує підозрілі сайти, рекламу та трекери. Найкращі VPN мають вбудований захист від кібератакі та здатні запобігти завантаженню шкідливих програм і трекерів із підозрілих сайтів на ваш пристрій. Деякі з них також блокують рекламу та спливаючі вікна.

Існує два основних класи мереж VPN. Шлюз захищеного віддаленого доступу до VPN дозволяє користувачам підключитися до іншої мережі (до Інтернету або внутрішньої системи своєї компанії) за приватним зашифрованим тунелем. Інший клас – VPN типу «мережа-мережа», чи VPN між маршрутизаторами. Цей вид мережі VPN в основному використовується в корпоративному середовищі, особливо якщо підприємство має штаб-квартири з різним розташуванням. VPN типу «мережа-мережа» використовується для створення закритої внутрішньої мережі, де всі офіси можуть підключатися один до одного. Ця технологія відома як інтранет.

Існує кілька протоколів VPN. Найстаріший з них – PPTP (протокол тунелювання «точка-точка»), який досі застосовується, але вважається одним із найбільш ненадійних протоколів. Інші – IPSec, L2TP, SSL, TLS, SSH і OpenVPN. Багато хто віддає перевагу протоколу OpenVPN, оскільки це програмне забезпечення з відкритим вихідним кодом.

На що слід звернути увагу при виборі VPN для захисту конфіденційності та забезпечення безпеки:

- 256-бітне шифрування AES;
- автоматичне аварійне відключення. У випадку втрати підключення під час використання VPN, функція автоматичного аварійного відключення призупинить ваш трафік до тих пір, доки не буде відновлено захищене з’єднання із сервером. Без цього інструменту ви будете наражатися на

випадкові витоки даних, через що ваша конфіденційність вже не буде захищеною;

- політика відмови від реєстрації дій користувачів;
- захист від витоків даних через DNS або IPv6. Існує декілька шляхів витоку ваших даних в мережу під час використання VPN, але ці два є найбільш поширеними.

Недоліки VPN:

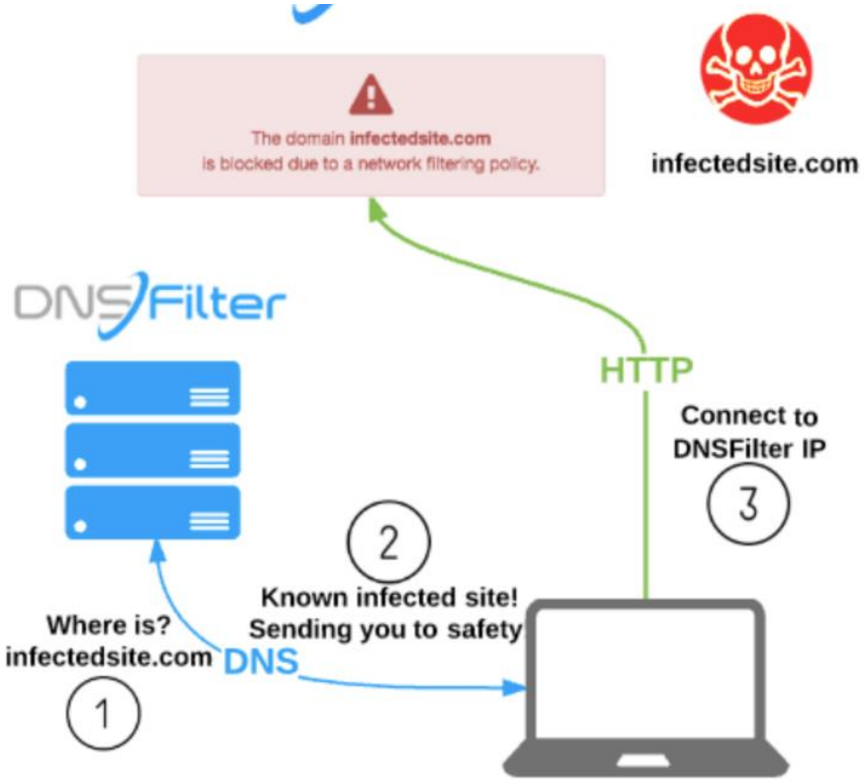
- зниження швидкості з'єднання з Інтернетом;
- неперевірені VPN можуть скомпрометувати ваш захист;
- деякі вебсайти блокують VPN.

5.3.4. DNSFilte (domain name system) – система доменних імен, яка працює за допомогою DNS-серверів. Кожен DNS-сервер за вказаною адресою сайту визначає IP-адресу веб-сервера, на якому знаходиться сайт.

DNS-фільтрація передбачає фільтрацію доменних імен та є методом запобігання доступу до певних веб-сторінок або IP-адрес, які здаються підозрілими. ви також можете заблокувати певні URL-адреси вручну. Особливо зручним цей спосіб є у випадку, коли вам потрібно захистити не один комп'ютер, а декілька, які підключені до мережі Інтернет через роутер. Окрім комп'ютерів, таким чином можна захистити інші пристрої, підключені до роутера через Wi-Fi. Якщо використовувати стандартні налаштування мережі, то всі запити до сайтів йдуть через сервер провайдера, який надає доступ до мережі Інтернет. Як правило, сервер провайдера не фільтрує запити користувачів і надає доступ до всіх затребуваних сайтів (якщо доступ до них не заборонено законодавством).

Але в мережі Інтернет існують DNS-сервери, які збирають інформацію про сайти, що містять інформацію, шкідливу для дітей, або сайти, які були

помічені в різних шахрайських схемах. Якщо в налаштуваннях свого комп'ютера або роутера вказати IP-адресу такого DNS-сервера, то всі запити до сайтів проходитимуть через цей сервер. Сервер фільтруватиме адреси затребуваних сайтів і не надаватиме доступ до заборонених сайтів.



DNS-фільтр перевіряє вхідний та вихідний трафік та блокує підозрілий, ґрунтуючись на певних заданих параметрах. Він дозволяє мережі отримувати та відправляти лише безпечний трафік. DNS-фільтр також може захистити Wi-Fi людини від експлойтів, що є чудовою додатковою функцією програми.

Можна навести наступний практичний приклад використання фільтрації DNS: якщо керівник заблокував доступ своїх користувачів до facebook.com у робочий час, і вони намагатимуться відкрити цей сайт, нічого не вийде. У робочий час їхній запит буде відхилений – сайт стане недоступним.

Переваги DNS-фільтрації:

- на деяких платформах це єдиний спосіб фільтрувати весь системний трафік. Наприклад, на iOS лише Safari підтримує блокування контенту у звичному сенсі. Фільтрувати трафік усіх інших браузерів та програм допоможе лише DNS-фільтрація;

- з деякими формами стеження (наприклад, CNAME-трекінг) може впоратися лише DNS-фільтрація;
- етап обробки DNS-запиту – перша ступінь, яка може заблокувати рекламу чи трекер. Це допомагає трохи заощадити час життя батареї та трафік.

Недоліки DNS-фільтрації:

- DNS-фільтрація – «грубий» метод. Це означає, що з її допомогою не вийде прибрати, наприклад, білі порожні блоки, що залишаються після заблокованої реклами. Багато видів складної реклами не можуть бути заблоковані на рівні DNS (точніше, можуть, але лише ціною повного блокування домену, який також використовується для інших корисних цілей);
- неможливо визначити джерело DNS-запиту, тобто ви не зможете розрізняти трафік різних програм на DNS-рівні. Це завадить веденню докладної статистики і унеможливить створення правил, що працюють лише для конкретних додатків.

Загальнодоступні DNS-фільтри.

Публічний DNS-сервер Google. Цей сервер по суті створювався не для фільтрації, а для прискорення роботи Інтернету, але він так само фільтрує фішингові та шкідливі сервери. Крім того, даний сервер вміє працювати по IPv6.

Адреси DNS Google:

IPv4 8.8.8.8, 8.8.4.4

IPv6 2001:4860:4860::8888, 2001:4860:4860::8844.

OpenDNS – мабуть найстаріший DNS-фільтр. Є платні та безкоштовні можливості. Вміє виправляти неправильно набрані адреси сайтів, а також показує сторінку з пошуком та рекламою, якщо адресу виправити не вдалося автоматично. Має профілі для батьківського контролю доступні безкоштовно після реєстрації. Без реєстрації декларується фільтрація шкідливих серверів.

Адреси DNS OpenDNS:

208.67.222.222

208.67.220.220

https://www.opendns.com/

1.1.1.1 DNS Family. Приватний сервер DNS від CloudFlare. Декларується як один із найшвидших та приватних. Є варіанти із блокуванням шкідливих сайтів та дорослого контенту.

Адреси DNS 1.1.1.1:

1.1.1.1 – швидкий приватний;

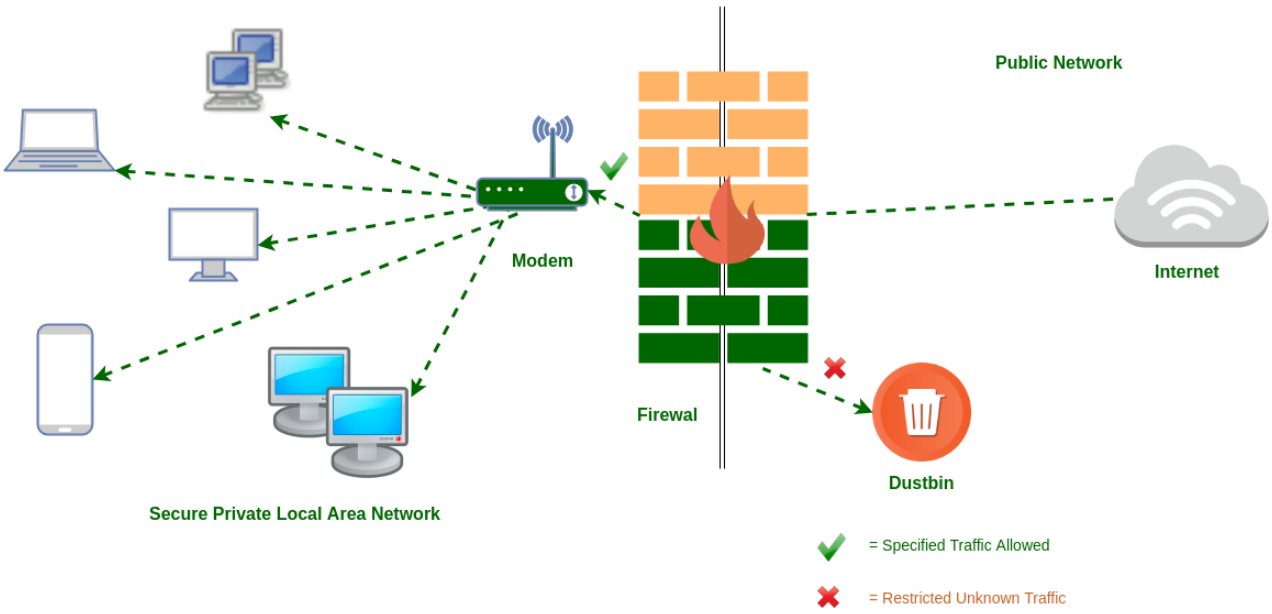
1.1.1.2, 1.0.0.2 – з блокуванням шкідливих сайтів;

1.1.1.3, 1.0.0.3 – з блокуванням шкідливих сайтів та дорослого контенту.

https://1.1.1.1/family/.

5.3.5. Мережевий екран (firewall, міжмережевий екран або мережевий екран, брандмауер) – комплекс апаратних чи програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів, які проходять через нього, відповідно до заданих правил. Термін походить від англійського слова «firewall» – протипожежна стіна, яка перешкоджає поширенню вогню.

Основним завданням мережевого екрану є захист комп'ютерних мереж або окремих вузлів від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, оскільки їх основне завдання – не пропускати (фільтрувати) пакети, що не задовольняють критерії, які визначені в конфігурації.



Деякі мережеві екрани також дозволяють здійснювати трансляцію адрес – динамічну заміну внутрішньомережевих (сірих) адрес або портів на зовнішні, які використовуються за межами локальних мереж.

Мережеві екрани поділяються на різні типи залежно від таких характеристик:

- чи забезпечує екран з'єднання між одним вузлом і мережею або між двома та більше різними мережами;
- на рівні яких мережевих протоколів відбувається контроль потоку даних;
- чи відслідковується стан активних з'єднань.

Залежно від рівня, на якому відбувається контроль доступу, існує поділ на мережеві екрани, що працюють на:

- мережевому рівні, коли фільтрація відбувається на основі адрес відправника і одержувача пакетів, номерів портів транспортного рівня моделі OSI та статичних правил, заданих адміністратором;
- сеансовом рівні (також відомі як stateful) – відстежують сеанси між додатками, не пропускають пакети, які порушують специфікації TCP/IP, та часто використовуються у зловмисних операціях – скануванні ресурсів, зломи через неправильні реалізації TCP/IP, обриви/уповільнення з'єднань, ін'єкції даних.
- рівні додатків, фільтрація на підставі аналізу даних програми, переданих всередині пакету. Такі типи екранів дозволяють блокувати передачу небажаної і потенційно небезпечної інформації на підставі політик та налаштувань.

Мережеві екрани з фільтрацією пакетів являють собою маршрутизатори або працюють на сервері програми, сконфігуровані таким чином, щоб фільтрувати вхідні та вихідні пакети. Тому такі екрани називають іноді пакетними фільтрами. Фільтрація здійснюється шляхом аналізу IP-адреси джерела і приймача, а також портів вхідних TCP- та UDP-пакетів і порівнянням їх із сконфігурованою таблицею правил. Ці мережеві екрани прості у

використанні, дешеві, надають мінімальний вплив на продуктивність обчислювальної системи. Основним недоліком є їх вразливість при підміні адрес IP. Крім того, вони складні при конфігуруванні: для їх установки потрібно знання мережевих, транспортних і прикладних протоколів.

Шлюзи сеансового рівня контролюють допустимість сеансу зв'язку. Вони стежать за підтвердженням зв'язку між авторизованим клієнтом і зовнішнім хостом (і навпаки), визначаючи, чи є запитуваний сеанс зв'язку допустимим. При фільтрації пакетів шлюз сеансового рівня грунтується на інформації, що міститься в заголовках пакетів сеансового рівня протоколу TCP, тобто функціонує на два рівні вище, ніж мережевий екран з фільтрацією пакетів. Окрім того, зазначені системи зазвичай мають функцію трансляції мережевих адрес, яка приховує внутрішні IP-адреси, тим самим, виключаючи підміну IP-адреси. Однак у таких мережевих екранах відсутній контроль вмісту пакетів, що генеруються різними службами. Для виключення зазначеного недоліку застосовуються шлюзи прикладного рівня.

Шлюзи прикладного рівня перевіряють вміст кожного пакету, який проходить через шлюз пакета і можуть фільтрувати окремі види команд або інформації в протоколах прикладного рівня. Це більш досконалий і надійний тип мережевого екрану, що використовує програми-посередники (proxies) прикладного рівня або агенти. Агенти складаються для конкретних служб мережі Інтернет (HTTP, FTP, тощо) і служать для перевірки мережевих пакетів на наявність достовірних даних.

Шлюзи прикладного рівня знижують рівень продуктивності системи через повторну обробку в програмі-посереднику. Це непомітно при роботі в Інтернеті по низькошвидкісних каналах, але істотно при роботі у внутрішній мережі.

Мережеві екрани експертного рівня поєднують у собі елементи всіх трьох описаних вище категорій. Як і мережеві екрани з фільтрацією пакетів, вони працюють на мережному рівні моделі OSI, фільтруючи вхідні та вихідні пакети на основі перевірки IP-адрес і номерів портів. Мережеві екрани експертного

рівня також виконують функції шлюзу сеансового рівня, визначаючи, чи відносяться пакети до відповідного сеансу. І, нарешті, брандмауери експертного рівня беруть на себе функції шлюзу прикладного рівня, оцінюючи вміст кожного пакета у відповідності з політикою безпеки, виробленої в конкретній організації.

Зручність firewall полягає також у можливості вести журнал мережевих підключень, що дасть повну картину використання Інтернет трафіку. Після перегляду журналу, спеціаліст або сам користувач зможе побачити всі запити, що надійшли з мережі або виходять від комп'ютера, і при необхідності дізнатися, з якої адреси була здійснена хакерська атака або підозріла мережева активність.

Мережевий екран не може запобігти вірусам, які поширюються електронною поштою та фішинговому шахрайству.

5.3.6. Бездротові мережі Wi-Fi (wireless fidelity, бездротова точність / відданість). При роботі з громадськими Wi-Fi мережами на ПК, планшетах чи смартфонах доцільно дотримуватися наступних правил.

1) Не обмінюйтесь конфіденційною інформацією. Намагайтеся не використовувати відкритий Wi-Fi для перегляду електронної пошти, входу в облікові записи, здійснення операцій в онлайн-банкінгу, відправки документів чи будь-яких інших конфіденційних даних. Усі важливі операції варто здійснювати з дому, або будь-якої іншої довіреної точки доступу, яку захищено складним та унікальним паролем та брандмауером.

2) вибирайте мережу вручну. Переконайтеся, що ваш пристрій налаштовано на вибір Wi-Fi вручну, а не на автоматичне підключення. Якщо ви вже використовували певну точку доступу раніше, ваш пристрій може автоматично підключитися до неї. Саме тому для відкритих Wi-Fi варто використовувати функцію «Забути мережу» – це дозволить уникнути непомітного для користувача підключення до Інтернету.

3) використовуйте VPN.

4) використовуйте додаткові інструменти захисту. Наприклад, Tor, VPN та DoNotTrack.

5) Увімкніть двофакторну аутентифікацію для всіх облікових записів, де це можливо. Цей крок додає ще один рівень безпеки, тому, якщо навіть зловмисники матимуть логін та пароль, дані користувача будуть захищені від несанкціонованого доступу.

6) Завершуйте активні сеанси в облікових записах. Спеціалісти рекомендують під час доступу до відкритих Wi-Fi завжди виходити з акаунтів, щоб уникнути їх компрометації. Крім цього, використовуйте функцію «Переглянути активні сеанси», яка доступна у більшості месенджерів та Інтернет-спільнот. Вона дозволяє перевірити де, коли та з яких пристроїв здійснювався вхід до вашого облікового запису.

7) вимикайте підключення до Інтернету, якщо він не використовується. Якщо ви вже виконали всі необхідні дії в Інтернеті та підключення до відкритого Wi-Fi вам більше не потрібне, просто вимкніть його. Це забезпечить захист від несанкціонованого доступу зловмисників. Чим довше ви будете підключені до відкритої мережі, тим більша імовірність того, що кіберзлочинці намагатимуться отримати доступ до ваших даних.

При розгортанні домашньої мережі Wi-Fi варто дотримуватися наступних порад.

1) Встановіть унікальний пароль для вашого облікового запису адміністратора Wi-Fi та маршрутизатора. Не залишайте маршрутизатор з паролями Wi-Fi та адміністратора, які встановлені за замовчуванням. Хакери постійно намагаються прорватися на пристрої, використовуючи ці загальновідомі облікові дані. Також корисно регулярно змінювати пароль.

2) Постійно оновлюйте прошивку. Маршрутизатор з автоматичними оновленнями – найкращий варіант, але потрібно переконатися, що ви їх включили.

3) Створіть гостьову мережу. Гостьова мережа достатньо ізольована від домашньої локальної мережі, відвідувачі отримують доступ до Інтернету без

можливості потрапити у ваші приватні дані. ви можете додатково приховати домашній Wi-Fi SSID, підключивши до домашньої мережі лише надійні пристрої та періодично перевіряючи наявність нових підключених пристроїв, щоб запобігти несанкціонованому доступу.

4) вимкнути функції WPS та UPnP. Деякі маршрутизатори Wi-Fi мають кнопку сполучення (кнопку WPS) для полегшення з'єднання, оскільки вона дозволяє уникнути вводу паролю, щоб додати нові пристрої до мережі. Але цю функцію можна використати для отримання доступу до вашої домашньої мережі. UPnP (Universal Plug and Play) призначена для полегшення підключення пристроїв без складної конфігурації – таких як смарт-телевізори. Але деякі шкідливі програми спрямовані на UPnP, щоб отримати доступ до вашої домашньої мережі.

5) Встановлення MAC-фільтрів. Щоб зробити вашу мережу ще більш безпечною, ви можете встановити режим фільтрації MAC-адрес – дозволити підключатися лише домашнім гаджетам. MAC-адресу кожного пристрою з мережним адаптером можна подивитися в його налаштуваннях. Також в розділі MAC-фільтрів вашого маршрутизатора можна заборонити доступ певних пристроїв. Це стане в нагоді, якщо ви, наприклад, давали тимчасовий доступ гостю або сусідові, але далі не хочете, щоб він використовував вашу мережу.

6) Оберіть безпечний маршрутизатор. Підчас розгортання мережі Wi-Fi ви можете стикнутися з декількома варіантами безпеки роутера. Нижче наведено список протоколів, які ранжовані за ступенем безпеки (вгорі – найбезпечніші):

WPA3,

WPA2 Enterprise,

WPA2 Personal WPA + AES,

WPA + TKIP,

WEP,

Open Network (no security implemented).

Системи, які все ще використовують WEP, не є безпечними. Для покращення функцій WEP у 2003 році було створено протокол Wi-Fi Protected Access або WPA. Цей покращений протокол, як і раніше, мав відносно низьку безпеку, але його легше було налаштувати. WPA, на відміну від WEP, використовує протокол Temporary Key Integrity Protocol (TKIP) для безпечнішого шифрування. Оскільки Wi-Fi Alliance зробив перехід із WEP на більш просунутий протокол WPA, вони мали зберегти деякі елементи WEP, щоб старі пристрої все ще були сумісні. На жаль, це означає, що такі вразливості, як функція налаштування WiFi Protected, яку можна зламати відносно легко, ще присутні в оновленій версії WPA.

Роком пізніше, в 2004 році, стала доступна нова версія протоколу Wi-Fi Protected Access 2. WPA2 має більш високий рівень безпеки, а також він простіше налаштовується в порівнянні з попередніми версіями. Основна відмінність WPA2 полягає в тому, що він використовує покращений стандарт шифрування Advanced Encryption Standard (AES) замість TKIP. Єдина помітна вразливість WPA2 полягає в тому, що за умови отримання доступу до мережі, зловмисник може атакувати інші пристрої, підключені до цієї мережі.

ЛАБОРАТОРНА РОБОТА №5. МЕРЕЖЕВА КІБЕРБЕЗПЕКА

Мета вивчення: отримати практичні навички налаштування браузера та встановлення додатків для підвищення захисту від ШПЗ, видалення рекламного та потенційно небезпечного ПЗ; дослідити власний цифровий слід; дослідити способи використання проксі-серверів та віртуальної приватної мережі.

Обсяг навчального часу: 2 години.

Обладнання: комп'ютер (планшет, смартфон), наявність підключення до мережі Інтернет.

План заняття:

1. Налаштування браузерів для безпечної роботи.

2. Встановлення у браузерах розширень для блокування спливаючих вікон, реклами тощо.

3. Дослідження цифрового сліду.

4. Видалення рекламного та потенційно небезпечного програмного забезпечення.

5. Знайомство з технологіями проксі та VPN.

Інформаційні джерела:

довідкові системи браузерів Google Chrome, Mozilla Firefox, Opera:

- https://support.google.com/chrome/?p=help&ctx=settings#topic=9796470,
- https://support.mozilla.org/uk/products/firefox?as=u&utm_source=inproduct,
- https://help.opera.com/ru/latest/;

додатки для браузерів Google Chrome, Mozilla Firefox, Opera:

- https://chrome.google.com/webstore/category/extensions?hl=uk,
- https://addons.mozilla.org/uk/firefox/,
- https://addons.opera.com/uk/extensions/;

довідка веб-магазину Chrome:

https://support.google.com/chrome_webstore/answer/2664769?hl=uk;

додаткові фільтри для блокувальника uBlock Origin: https://github.com/search?q=uBlock-filters;

довідник поштових скриньок, які потрапили до баз даних у мережі: https://haveibeenpwned.com;

тест браузера на рівень інформаційної ентропії: https://coveryourtracks.eff.org;

як браузер фіксує інформацію щодо переміщення курсора миші: https://clickclickclick.click/#ab8459dff2c433c3f59108d42618bc9b;

демонстрація даних, які збирає браузер про комп'ютер користувача: https://webkay.robinlinus.com/

програма Malwarebytes AdwCleaner для видалення рекламного, потенційно небажаного ПЗ: https://malwarebytes.com/adwcleaner/;

проксі-сервери:

- https://www.hidemyass.com/uk-ua/proxy,
- https://www.kproxy.com/,
- https://www.4everproxy.com/,
- http://dontfilter.us/.

ЗАВДАННЯ:

1. Налаштувати параметри безпеки в деякому браузері.

2. Встановити в браузер додаток uBlock Origin та налаштувати його.

2.1. Додайте сайт https://ddpu.edu.ua/ до білого списку додатку.

2.2. Заблокуйте деякі елементу довільного сайту за Вашим вибором. Вимкніть на цьому сайті JavaScript.

2.3. Створіть власний фільтр для певного елементу вебсайту. Видаліть власний фільтр.

2.4. Додайте фільтр користувача до uBlock Origin.

3.1. За допомогою Диспетчера задач деактивуйте попередньо відкритий браузер чи будь-яку іншу програму.

3.2. Зробіть скріншот вкладки автозавантаження, за необхідності видаліть небажані програми.

3.3. Виконайте перевірку та виправлення реєстру за допомогою програми Ccleaner.

3.4. Виконайте перевірку комп'ютера за допомогою програми AdwCleaner.

4.1. Перевірте, чи була скомпрометована Ваша поштова скринька. Визначте рівень інформаційної ентропії браузера.

4.2. Встановіть й налаштуйте додаток у браузері для підвищення конфіденційності.

5.1. За допомогою безкоштовних проксі-сервесів відвідайте сторінку пошукової системи Google та офіційний вебсайт Донбаського державного педагогічного університету.

5.2. Налаштуйте в браузері Opera технологію VPN та скористайтеся нею.

ВИМОГИ ДО ЗВІТУ:

1. Скрін екрану з налаштуванням параметрів безпеки в браузері.

2. Скрін екрану з встановленим у браузер додатком uBlock Origin, вимкненим на сайті JavaScript.

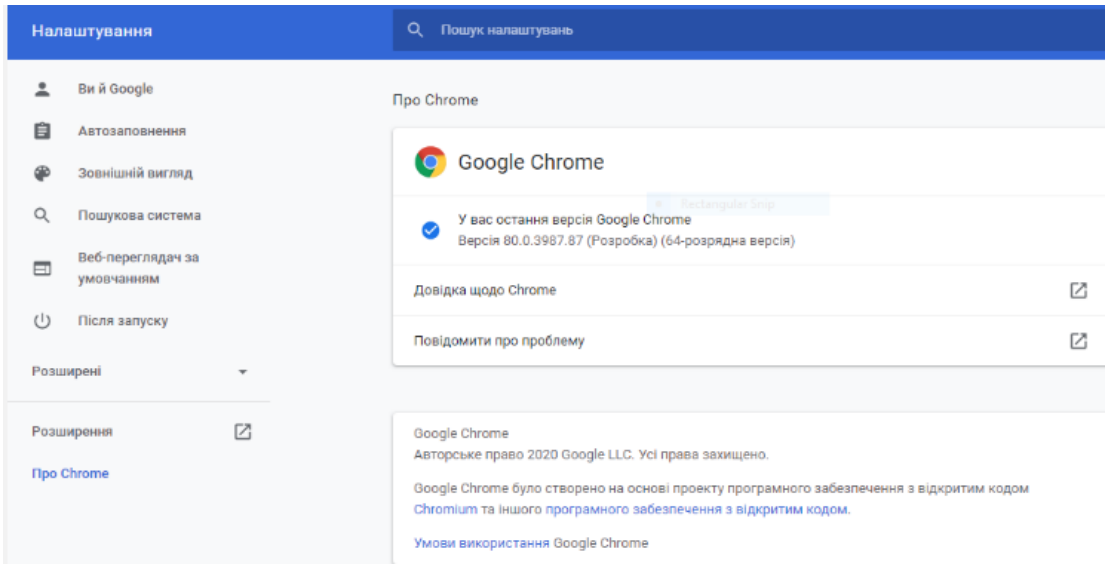
3. Скрін екрану з встановленим додатком у браузері для підвищення конфіденційності (за Вашим вибором).

4. Скрін екрану з безкоштовним проксі-сервісом.

ХІД РОБОТИ.

1. Налаштування браузерів для безпечної роботи.

Кожен браузер трохи відрізняється за механізмом встановлення оновлень. Google Chrome: нові оновлення запускатимуться автоматично, коли ви закриєте браузер. Щоб перевірити, чи оновлений Chrome, перейдіть на Chrome – Про Google Chrome у верхньому лівому куті браузера.



Mozilla Firefox дозволяє вмикати та вимикати автоматичні оновлення в розділі Firefox – Налаштування. Для перевірки версії Firefox, перейдіть до Firefox – Про Firefox у верхньому лівому куті браузера.

Microsoft Edge: оновлення поширюються автоматично. Щоб перевірити свою версію, відкрийте Edge, клацніть на 3 крапки у верхньому правому куті, а потім виберіть Про Edge.

Використання приватного режиму (чи режиму інкогніто) запобігає збереженню історії веб-пошуку, кешу браузера, даних форм та файлів cookie після виходу з браузера, який треба обов'язково **повністю закрити**. Але перегляд у приватному режимі не надає повної конфіденційності – IP-адресу та дії користувача можна відстежувати.

Налаштування параметрів конфіденційності є однією з найважливіших речей для захисту веб-браузера. За замовчуванням багато налаштувань браузера залишають відкритими особисті дані. Насамперед, необхідно:

- вимкнути спливаючі вікна та перенаправлення, які також можуть використовуватися для поширення шкідливого програмного забезпечення;
- не дозволяти автоматичне завантаження. Автоматичне завантаження може містити шкідливе програмне забезпечення. Доцільно отримати запит перед тим, як щось завантажувати;
- видаліть файли cookie після перегляду та вимкніть сторонній доступ до файлів cookie;
- обмежте доступ до свого місцезнаходження, камери та мікрофона. Налаштуйте браузер запитувати дозвіл перед тим, як отримати доступ до цих функцій;
- деактивуйте ActiveX. ActiveX вважається застарілою технологією й створює ризики для безпеки. Також розгляньте можливість вимкнення Flash та Javascript;
- увімкніть функцію «Надіслати запит Не відстежувати». Це допоможе запобігти вебсайтам відстежувати вас, але повноцінна гарантія цього відсутня.

Налаштування конфіденційності Chrome: клацніть на три вертикальні крапки у верхньому правому куті браузера. Клацніть Налаштування, опуститься сторінкою вниз й натисніть Розширений щоб отримати доступ до налаштувань конфіденційності.

Налаштування конфіденційності Firefox: клацніть на три вертикальні лінії у верхньому правому куті браузера, виберіть Налаштування, потім натисніть Приватність та безпека.

Microsoft Edge: клацніть три крапки у верхньому лівому куті браузера. Перейти до Конфіденційність і Безпека.

2. Розширення для блокування спливаючих вікон, реклами тощо.

Розширення для веб-браузера вперше з’явились у четвертій версії Internet Explorer від Microsoft у 1999 році й називалися «Панелі провідника». Це були спеціалізовані панелі інструментів, які можна було додати до інтерфейсу.

Браузер Mozilla Firefox був наступним, який почав підтримувати розширення в 2004 році, за ним послідувала Opera в 2009 році, і нарешті, в 2010 році, Google Chrome та Safari. Браузер Microsoft Edge також підтримує розширення.

На жаль, деякі розширення можуть створювати проблеми для безпеки та конфіденційності. Це пов'язано з дозволами, які вони отримують під час їх встановлення. Наприклад, майже всі розширення для Google Chrome можуть читати та змінювати дані користувача на вебсайтах. Встановлювати браузерні розширення треба лише з офіційних магазинів, зокрема, Chrome Web Store та Mozilla Addons for Firefox. Це не гарантує відсутності зловмисних програм, але їхня кількість в офіційних магазинах суттєво менша, ніж на сторонніх вебсайтах. Якщо ви користуєтеся Firefox, то доцільно використовувати лише розширення зі списку Рекомендованих: їх додатково перевіряють на відповідність стандартам.

Загалом варто керуватися такими правилами:

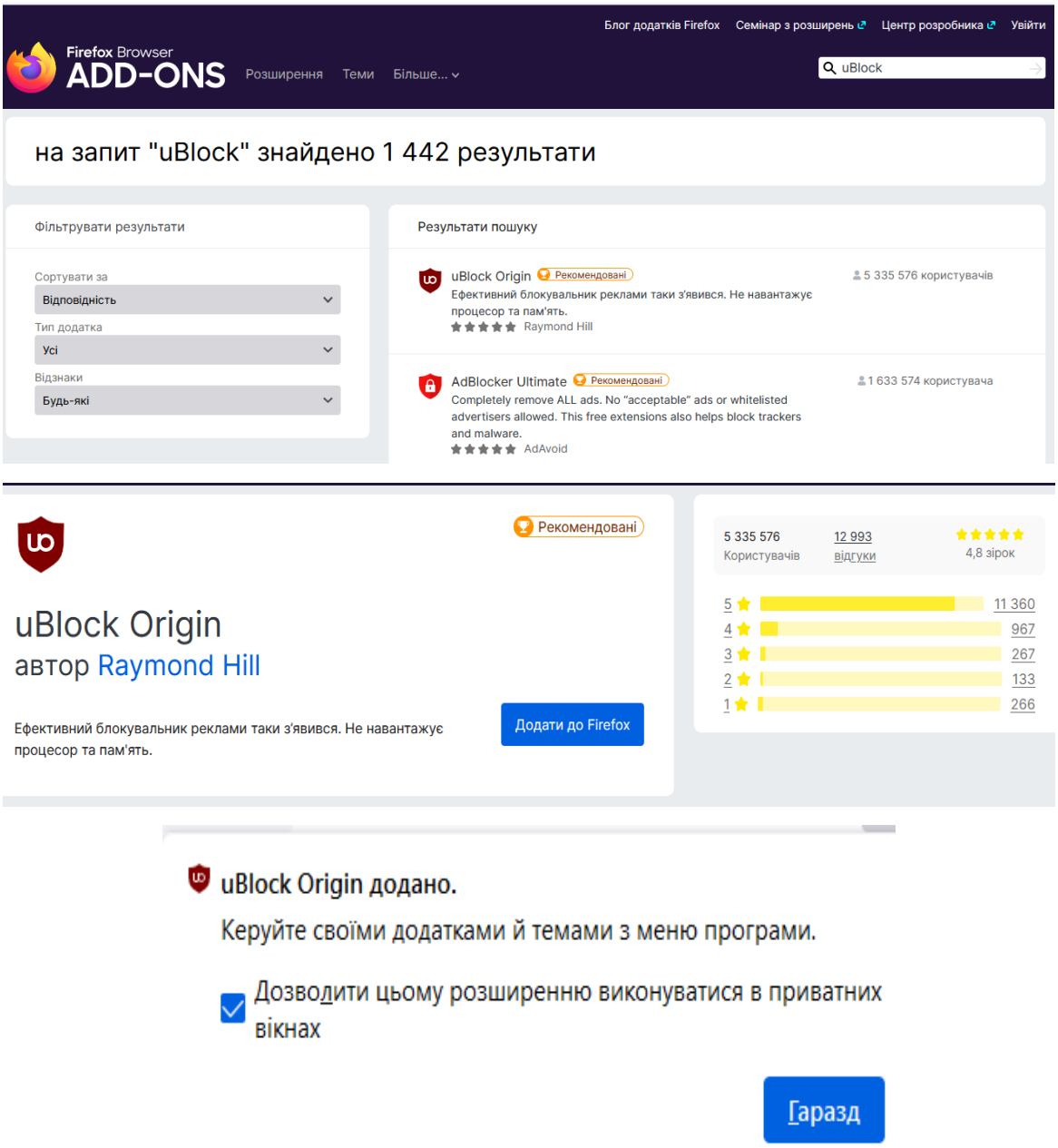
- використовуйте лише ті розширення, яким ви довіряєте і якими постійно користуєтеся;
- видаляйте всі розширення, якими ви не користуєтеся, не впевнені в їхній потребі або мету встановлення яких ви не пам'ятаєте.

Для встановлення додатків у Firefox натисніть кнопку меню ≡ й виберіть Додатки та теми (або введіть about:addons у новій вкладці), щоб відкрити менеджер додатків. виберіть панель із типом додатків, якими ви хочете керувати, а саме Розширення або Теми. У меню, що з'явиться, оберіть «Доповнення» (Add-Ons) – запуститься вкладка, в якій відобразяться усі встановлені в браузер плагіни. В пошуковому рядку цієї вкладки введіть ключові слова для пошуку доповнення. Наприклад, це може бути блокувальник реклами uBlock. Відкриється репозиторій Mozilla зі списком знайдених по ключовому слову посилань. Оберіть розширення, яке вам потрібне чи подобається найбільше та перейдіть на його сторінку.

На сторінці додатка клацніть кнопку «Додати в Firefox» (Add to Firefox). З'явиться спливаюче меню із запитом дозволів. Натисніть кнопку «Додати» для

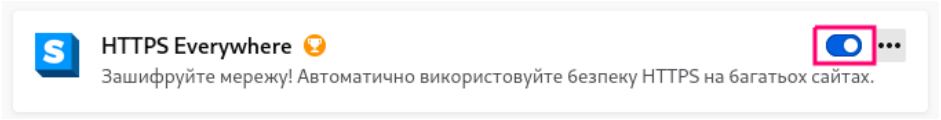
продовження установки. Доцільно надати встановленому додатку дозвіл виконуватися в режимі інкогніто чи у приватних вікнах.

Також можна встановити додатки з файлу. Для цього необхідно завантажити файл інсталятора на комп'ютер (наприклад, файл .xpi або .jar) та встановити додаток за допомогою значка шестерні ⚙ у верхньому правому кутку панелі Розширення менеджера додатків. Оберіть Встановити додаток з файлу..., далі знайдіть та виберіть необхідний файл.



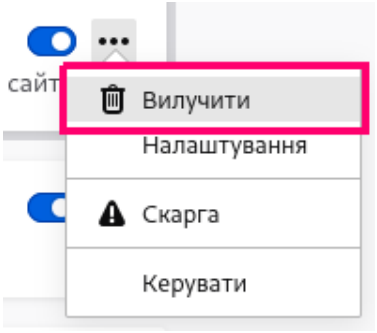
Вимкнення розширень. Розширення, яке має статус «вимкнено» не вилучається з браузера, а просто припиняє свою роботу. Натисніть кнопку меню ≡, відкрийте Додатки й теми 🧩 та оберіть Extensions. Прогорніть перелік

розширень. Натисніть на синій перемикач біля розширення, яке хочете вимкнути.



Для увімкнення розширення, знайдіть його в переліку розширень та натисніть на перемикач біля відповідного розширення.

Вилучення розширення. Натисніть кнопку меню ≡, відкрийте Додатки й теми та оберіть Extensions. Прогорніть перелік розширень. Натисніть піктограму еліпсис (3 крапки) біля розширення та виберіть вилучити.

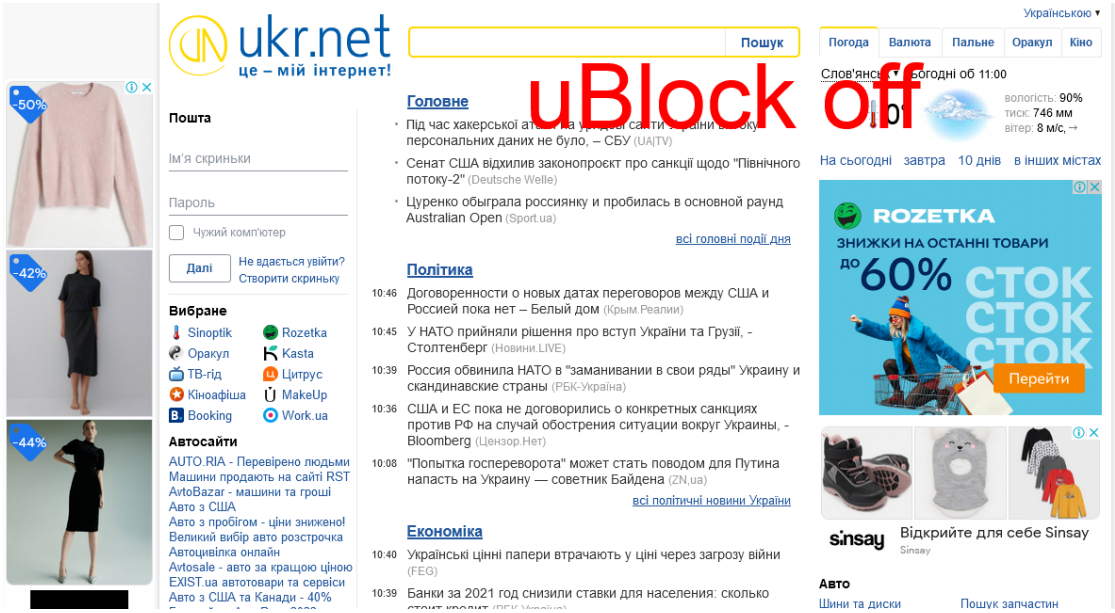


uBlock Origin – це безкоштовний (проект принципово відмовляється від пожертв) блокувальник Інтернет-реклами, який поширюється у вигляді розширення для браузерів і приховує більшість видів спливаючих банерів та рекламних відеороликів. uBlock Origin блокує рекламу на сторінках вебсайтів за допомогою механізму фільтрів. При цьому розширення використовує як вбудовані правила фільтрації так і створені безпосередньо користувачем. Завдяки приховуванню реклами доповнення збільшує швидкість завантаження сторінок в Інтернет-браузері, звільняє місце на екрані для корисного контенту, а також блокує деякі види шкідливих програм. Відповідно до заяв Реймонда Хіла, розробника проекту, і коментарів деяких користувачів, uBlock Origin відрізняється від аналогів тим, що споживає менше пам’яті та ресурсів процесора.

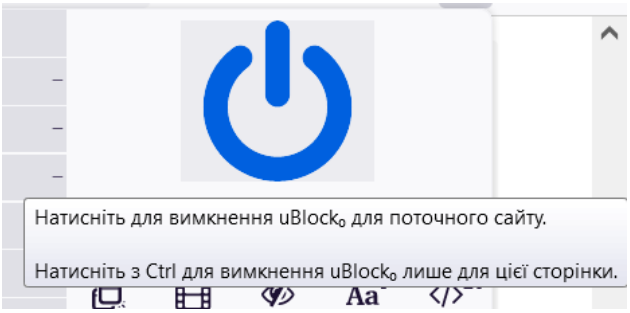
Переваги uBlock Origin: безкоштовне розповсюдження продукту; підтримка популярних браузерів; наявність вбудованого анти-трекера; можливість створення власних фільтрів; підтримка функції білого списку;

підтримка української мови інтерфейсу. Версія uBlock Origin для Firefox має додаткову функцію, яка допомагає відхилити спроби вебсайтів обійти блокувальники реклами.

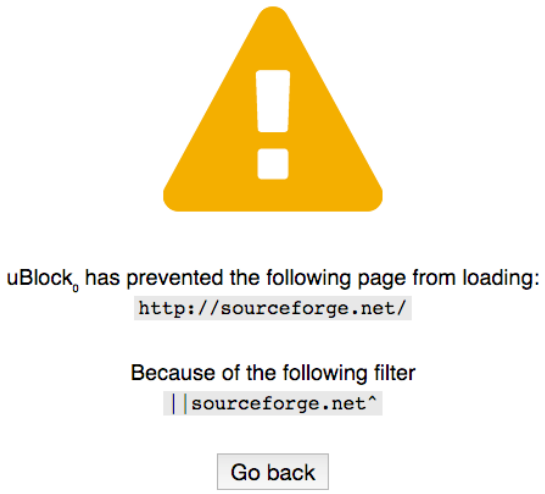
Інтерфейс uBlock Origin зводиться до невеликого меню в браузері. У ньому відображається кількість рекламних повідомлень, прихованих програмою, а також здійснюється її конфігурація. Сторінка налаштувань пропонує користувачеві можливість створення власних фільтрів, внесення ресурсів до переліку довірених, а також коротку інформацію щодо використання модуля.



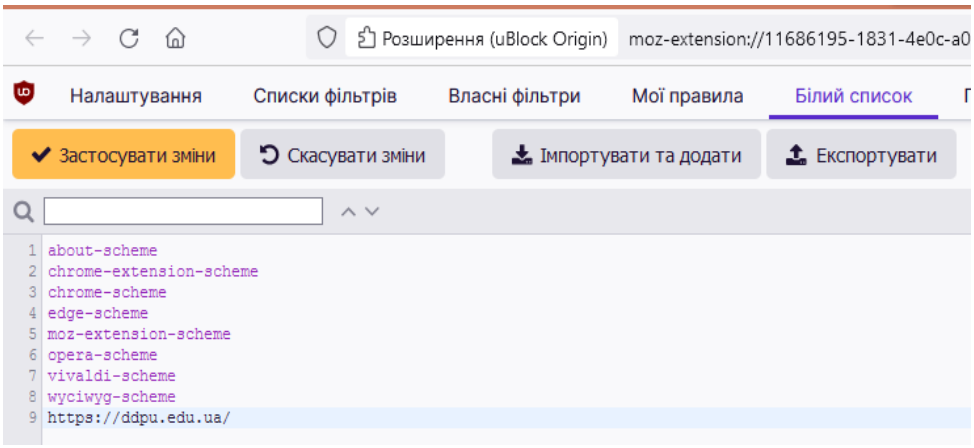
Деактивувати uBlock Origin для певного ресурсу можна натискаючи на його позначку в меню браузера та натискаючи відповідну кнопку.



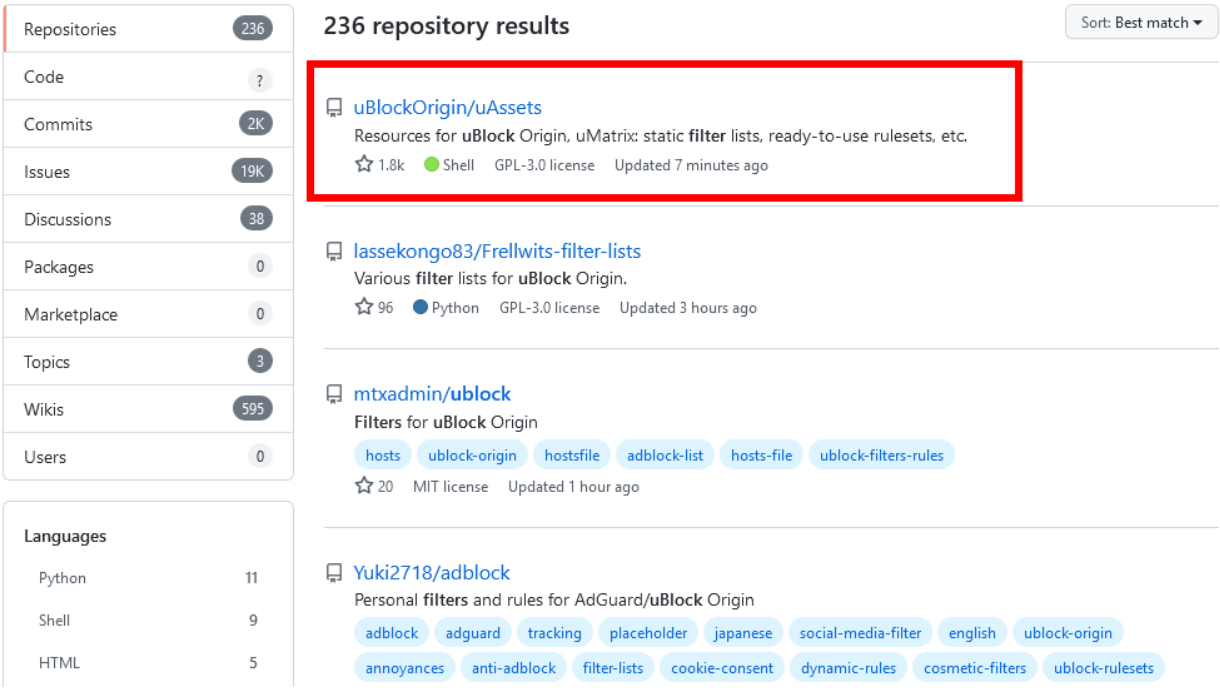
Іноді розширення блокує всю сторінку та демонструє повідомлення «uBlock Origin запобіг завантаженню наступної сторінки», наприклад, спробуйте відвідати http://ublock.org/ із увімкненим додатком uBlock Origin.

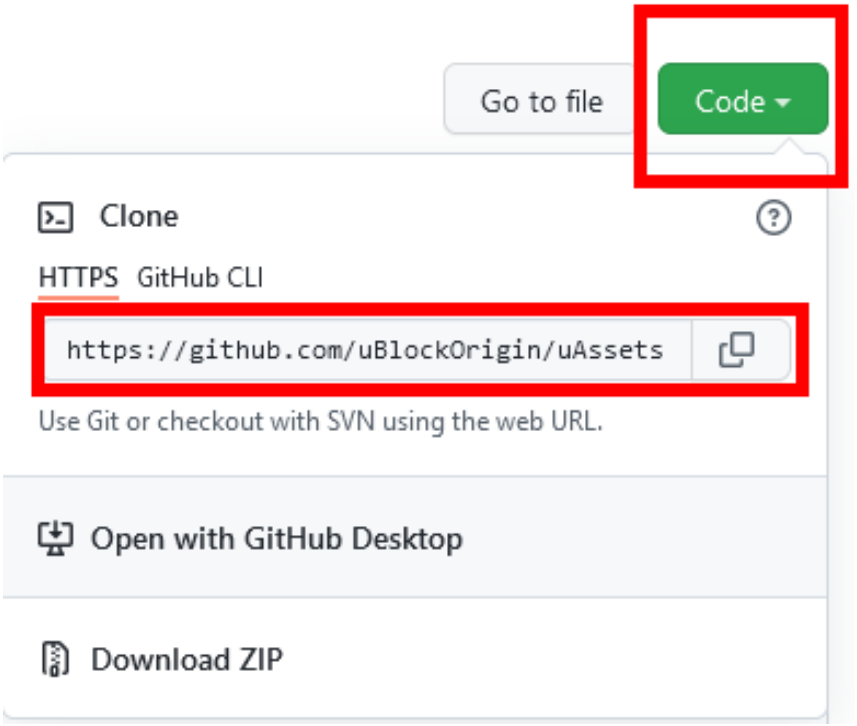


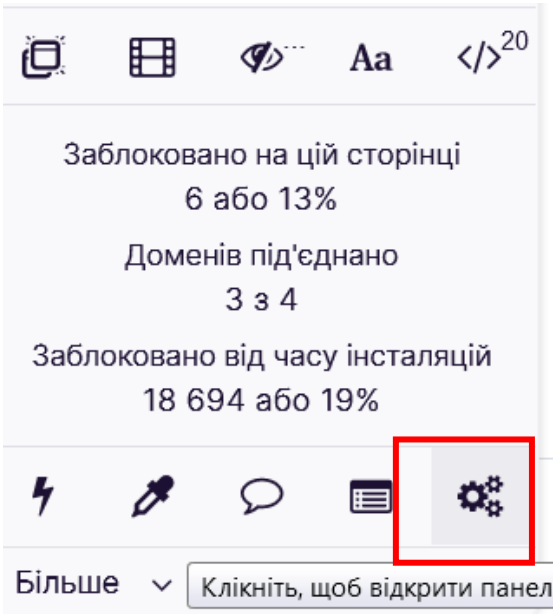
Причина появи цієї помилки полягає у тому, що uBlock Origin за замовчуванням блокує весь сайт у випадку, коли URL-адреса відповідає списку, яких є присутнім у списку домену шкідливого програмного забезпечення. Такий спосіб блокування оголошень зазвичай називають суворим блокуванням. За необхідності відвідати заблокований ресурс додайте його до білого списку. Для цього користувачеві необхідно скористатися меню налаштувань розширення.



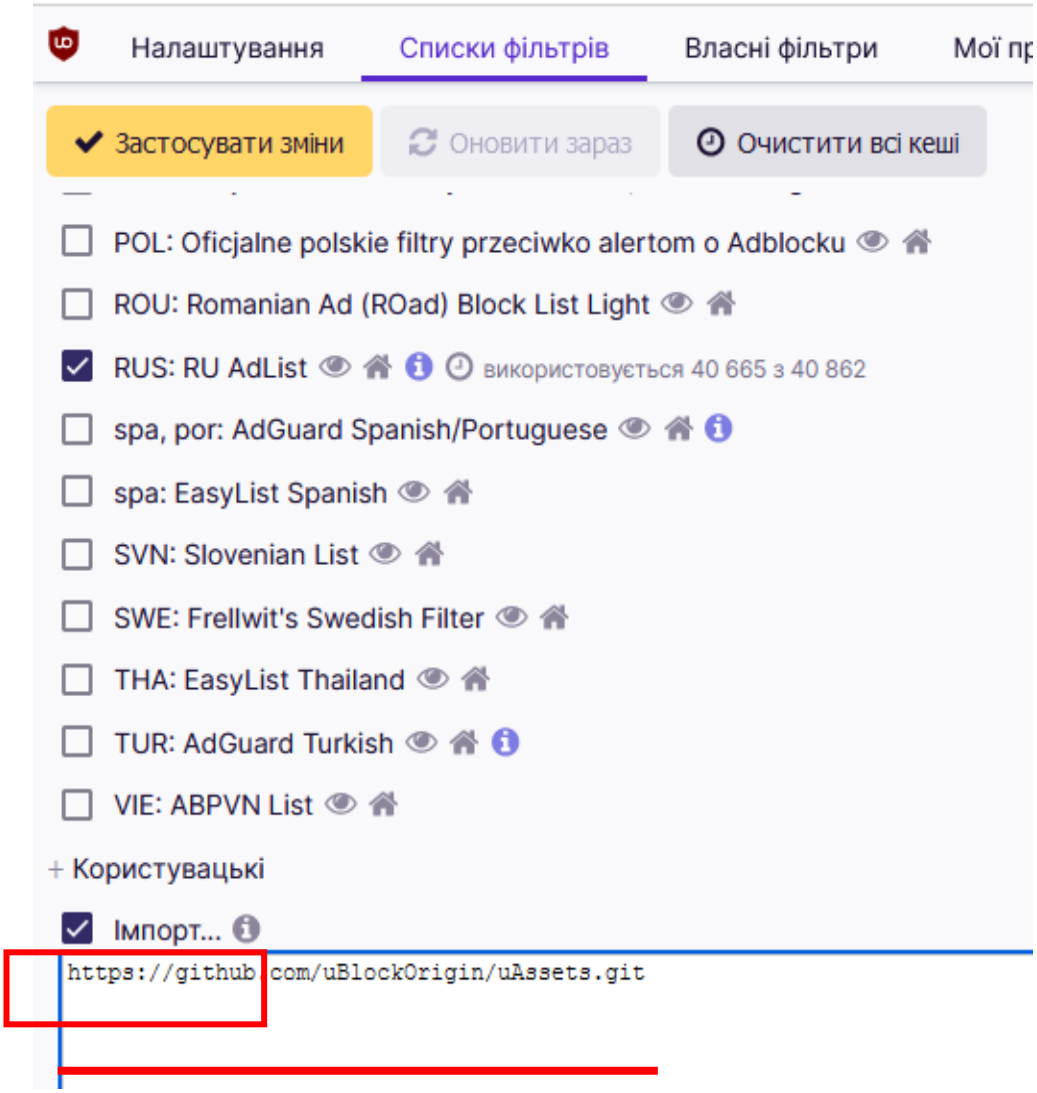
Знайдіть на ресурсі GitHub https://github.com/search?q=uBlock-filters (один із найбільших веб-сервісів для спільної розробки програмного забезпечення) додаткові фільтри для додатку та встановіть один із них в uBlock Origin. Для цього оберіть потрібний вам та перейдіть за відповідним посиланням. Сторінка містить інформацію щодо фільтру та зелену кнопку для завантаження фільтра. Скопіюйте URL-адресу й перейдіть до панелі керування uBlock Origin.







У пункті меню Списки фільтрів прокрутить до останнього пункту Імпорт, оберіть цей пункт та вставте URL-адресу фільтру. Застосуйте внесені зміни. Новий фільтр буде додано до категорії Користувацькі.



Для видалення вашого фільтру знайдіть його та натисніть піктограму баку для сміття. Застосуйте зміни.

3. Видалення рекламного та потенційно небезпечного програмного забезпечення в браузері.

Існує шкідливе програмне забезпечення, яке націлено саме на спотворення роботи браузера, зокрема:

hijacker або викрадач браузерів – замінює домашню (стартову) сторінку в браузерах, прописує посилання на вірусний чи рекламний сайт або фейковий пошуковик. Окремі екземпляри хайджекерів автоматично запускають браузер із заданої сторінки;

adware (рекламне програмне забезпечення) – при завантаженні вебсторінок вбудовує в них свій скрипт, що відображає різноманітні банери. Іноді завантажує додаткові панелі в Інтернет-магазинах, оглядових статтях із рекомендаціями покупки товарів.

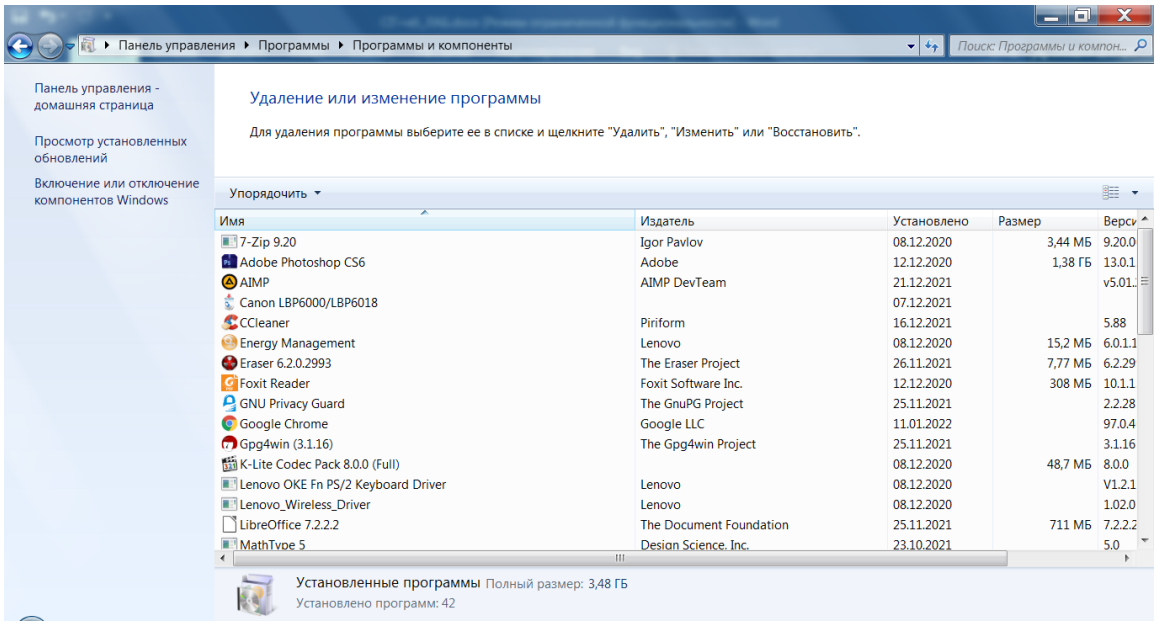
Щоб перевірити, чи заражений ваш браузер вірусною рекламою, зайдіть на той самий сайт із іншого пристрою (планшета, смартфона). Якщо й там з'явилася спливаюча панель із оголошеннями, це означає, що даний контент від власників ресурсу, якщо ж його немає – браузер, скоріш за все, інфікований.

Основні методи боротьби зі шкідливим програмним забезпеченням у браузері.

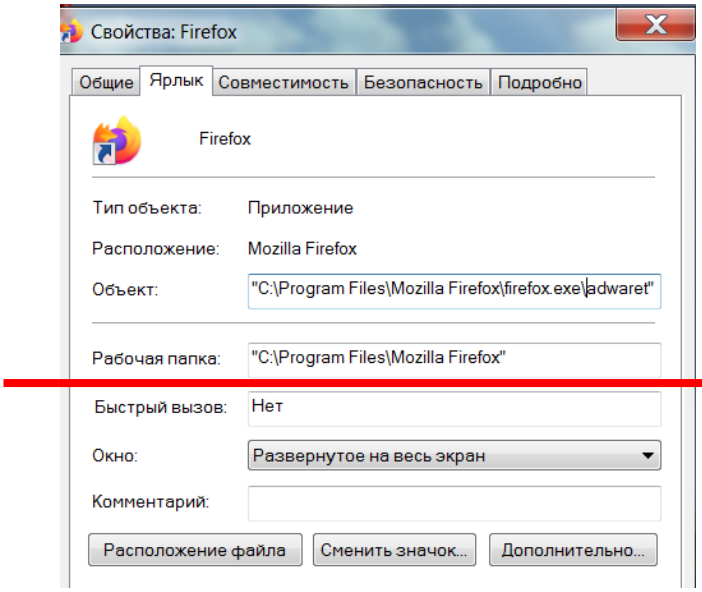
1. Запустіть повну перевірку комп'ютера антивірусом. Зверніть увагу на те, що під час цієї процедури браузер повинен бути закритим. Рекомендується взагалі не працювати за комп'ютером, поки йде перевірка.

2. Виконайте діагностику та профілактику браузерів – очистіть кеш, історію, кукі, налаштуйте стартову сторінку. Перевірте доповнення в браузері. Деякі розширення встановлюються приховано. Тому зайдіть в браузер і перевірте, чи є там доповнення, які ви не ставили. Також рекомендується видалити ті з них, якими не користуєтеся.

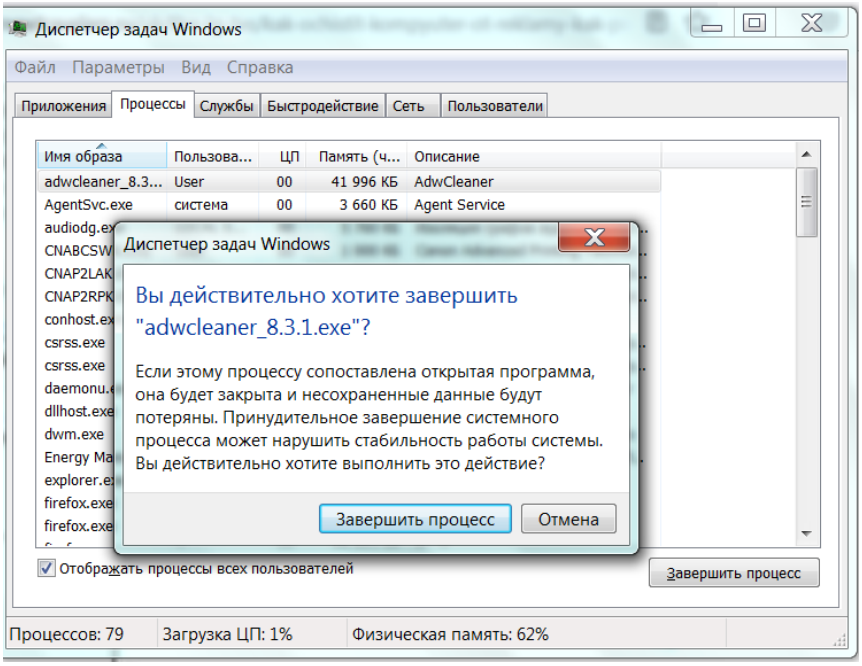
3. Іноді шкідливі модулі встановлюються як звичайний софт. У такому випадку перейдіть у Пуск – Панель управління – Програми та засоби, знайдіть та видаліть підозрілу програму.



4. Перевірте ярлик браузера. Якщо після запуску відразу відкривається сторінка рекламного сайту, то, швидше за все, проблема в ярлику. Іноді віруси прописують у властивостях ярлика (у полі «Об'єкт») адресу сайту, який відкривається підчас запуску браузера. Щоб вирішити цю проблему, видаліть ярлик та створіть новий.

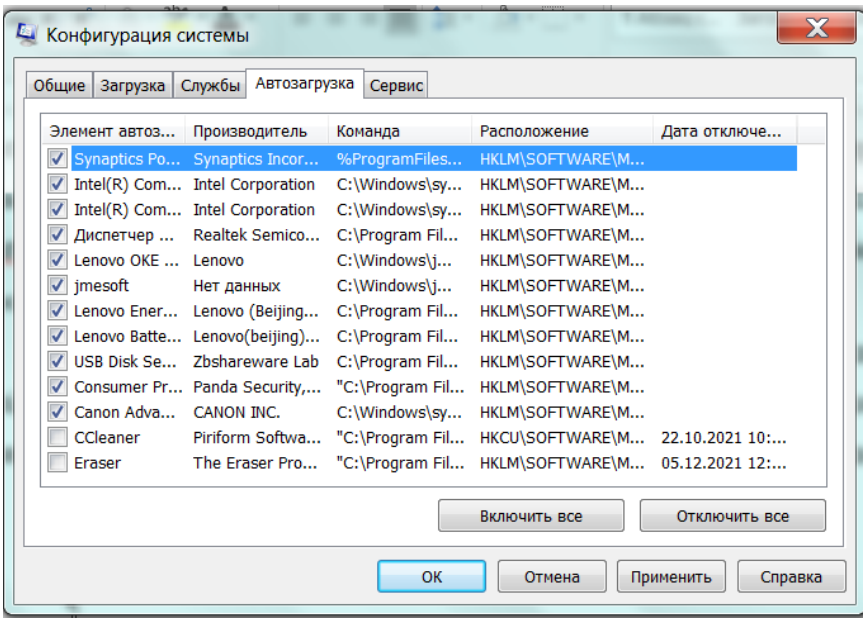


5.1. Запустить Диспетчер задач Віндоус – натисніть одночасно клавіші Ctrl+Shift+Esc. На вкладці «Процеси» перегляньте всі активні елементи. Підозрілі (з дивними назвами та підписами чи такі, що використовують багато ресурсів системи) проаналізуйте й деактивуйте: клік правою кнопкою – Властивості – Шлях до об'єкта (запам'ятайте чи запишіть); знову клік правою кнопкою по цьому ж об'єкту – Завершити процес.

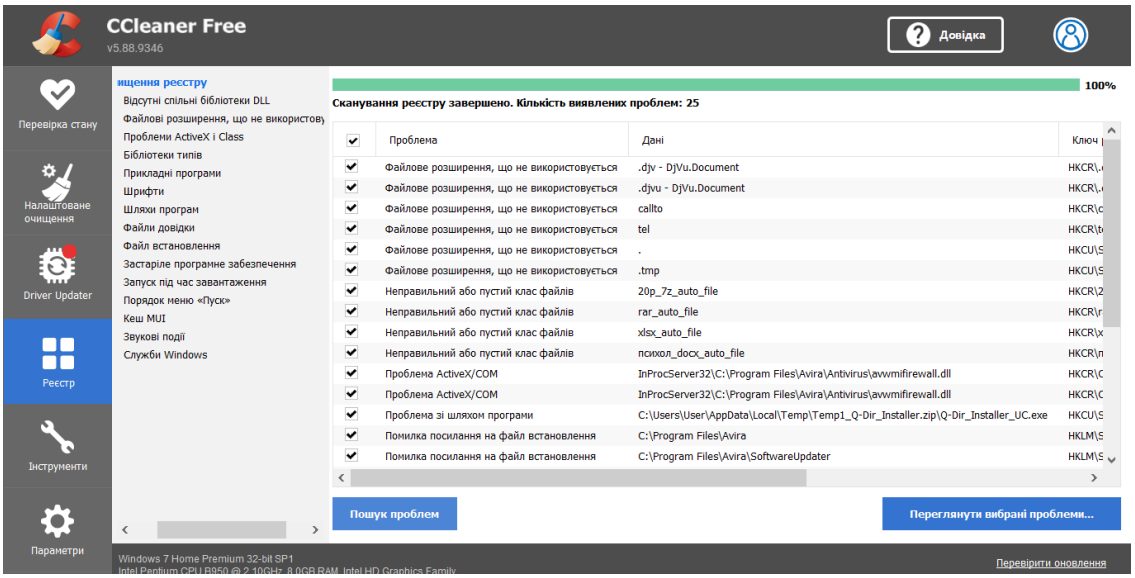


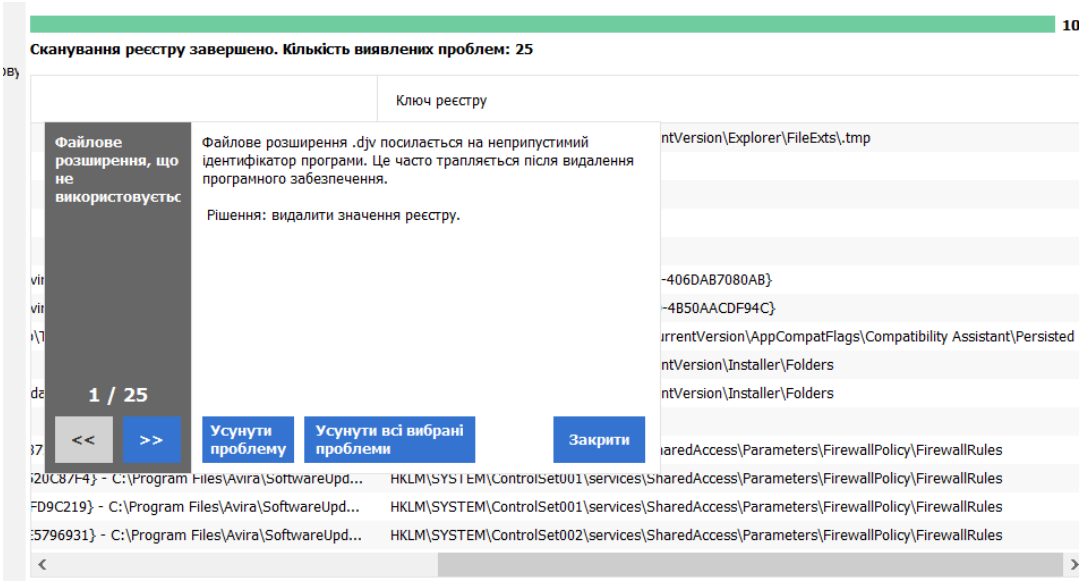
5.2. Перевірте автозавантаження: в рядку «Пуск» введіть команду msconfig, натисніть «Enter»; на вкладці «Автозавантаження» зніміть «галочки» біля підозрілих елементів (особливу увагу приділяйте директивам, які звертаються із запитом сторінки через командний рядок – CMD.EXE .... http // ... вірусний сайт); також зафіксуйте шлях до елементів (їх розташування на диску); клікніть: Застосувати – ОК.

5.3. Відкрийте послідовно всі виявлені у пунктах 5.1 та 5.2 директорії підозрілих файлів, папок, а потім видаліть їх (якщо ви точно впевнені, що це ШПЗ, а не, наприклад, деяка утиліта операційної системи). Якщо об’єкти не видаляються, використовуйте утиліту Unlocker або її аналоги для розблокування доступу.



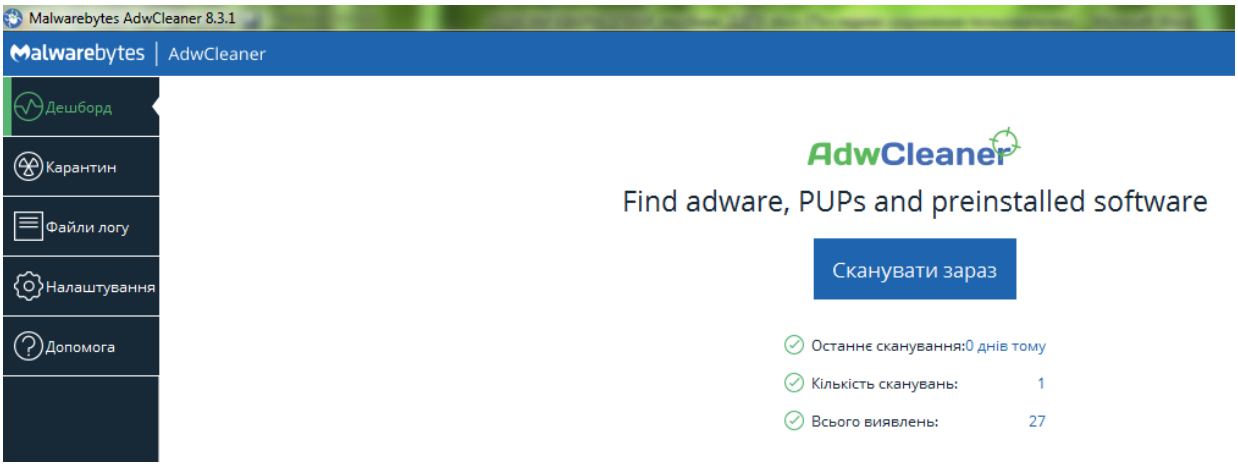
6. Виконайте перевірку та виправлення реєстру за допомогою програми Ccleaner.



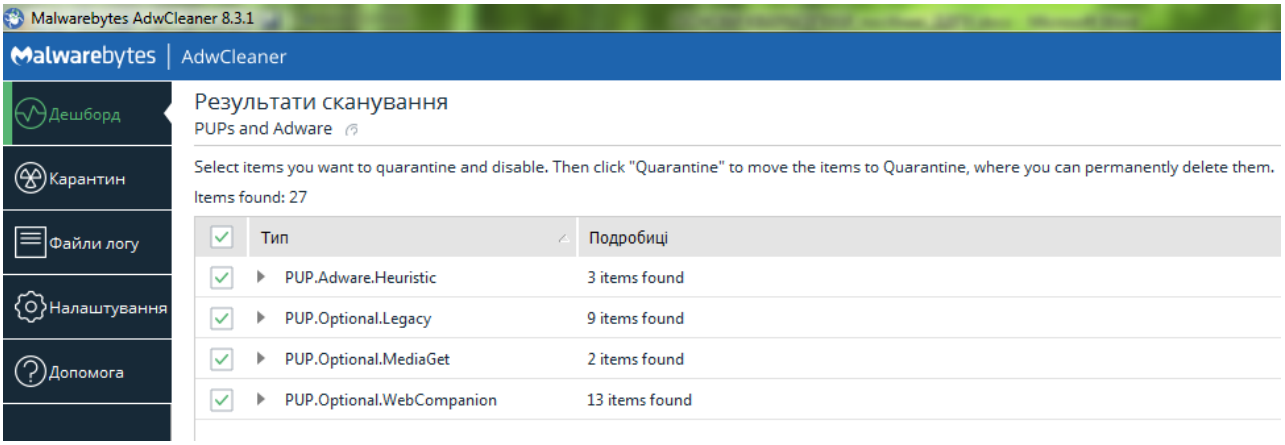


7. Скористайтеся спеціалізованим програмним засобом для видалення шкідливого ПЗ.

Програма AdwCleaner не вимагає установки на комп'ютер. Вона може запускатися з будь-якого місця на комп'ютері, з підключеного диска або флешки. AdwCleaner виконає сканування комп'ютера на наявність рекламного і потенційно небезпечного софту. Далі ви отримаєте звіт, у якому буде запропоновано видалити знайдені рекламні, шкідливі та інші потенційно небажані програми після перезавантаження комп'ютера. AdwCleaner успішно видаляє тулбари, панелі інструментів, рекламні блоки, hijacker-програми, тощо.

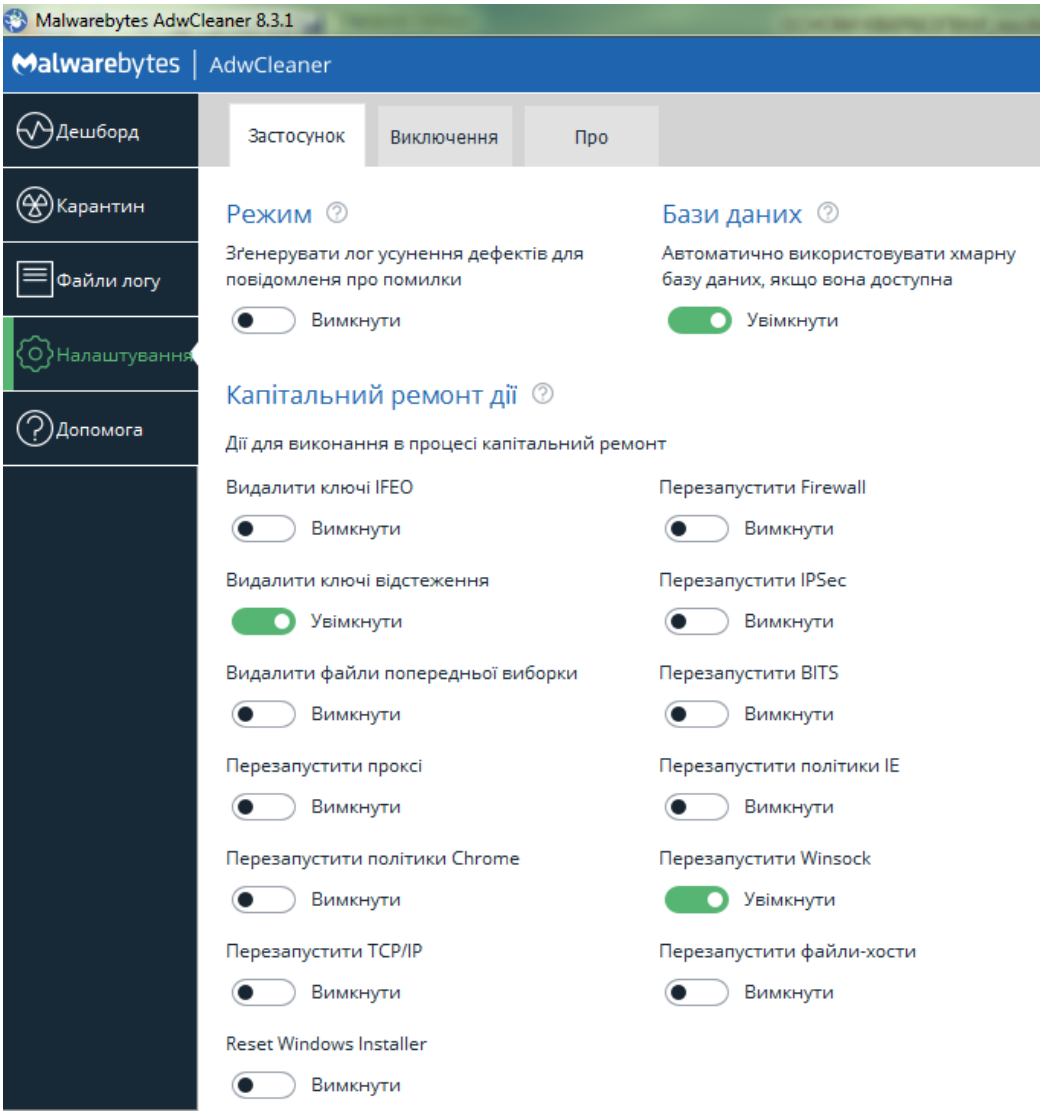


Уважно ознайомтеся з результатом сканування в кожній вкладці. Програма може пропонувати для видалення папки і файли, які не слід видаляти з комп'ютера. Перед видаленням елементів, зніміть прапорці навпроти відповідних пунктів, щоб запобігти видаленню потрібних вам програм.



Щоб змінити установки програми, відкрийте розділ «Налаштування». У розділі «Налаштування» є три вкладки: «Додаток», «виключення», «Подробиці». У вкладці «Додаток» знаходяться опції для застосування тих чи

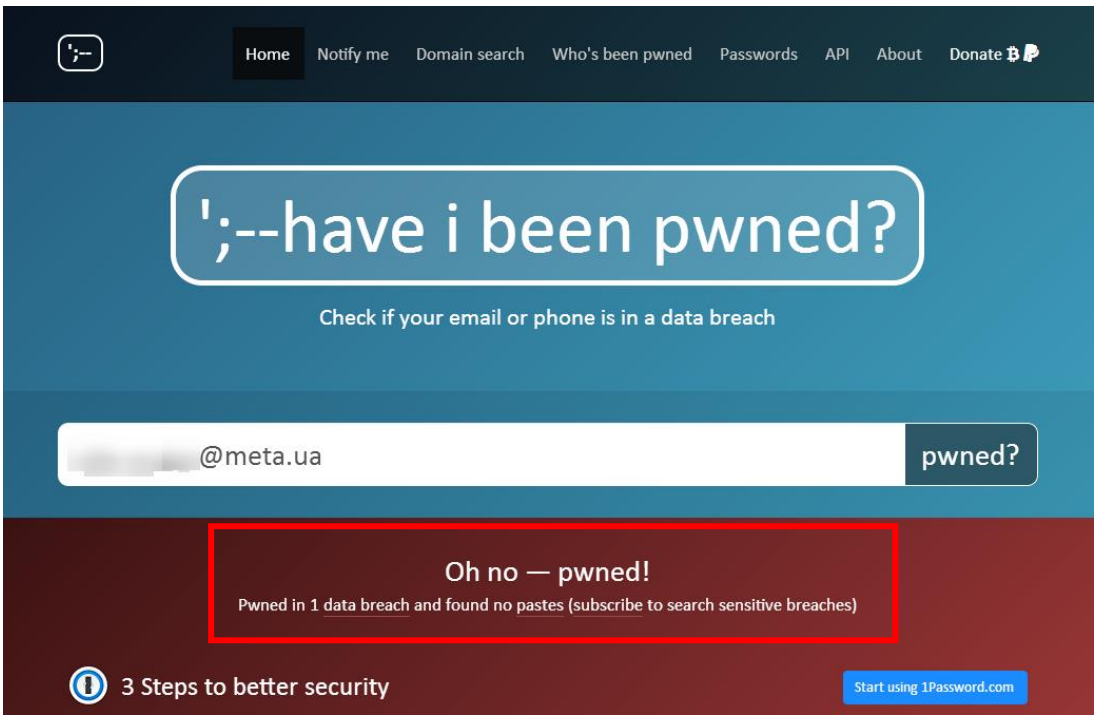
інших параметрів програми, при відновленні під час базової очищення системи. Тут є можливість задати більш строгі правила для сканування і очищення системи, в залежності від ступеня проблем, які виникли на даному комп'ютері. Звідси можна видалити AdwCleaner.



4. Дослідження цифрового сліду.

HaveIBeenPwned (https://haveibeenpwned.com) – онлайн-сервіс, який містить інформацію про зламані вебсайти, бази даних яких потрапили до мережі. За допомогою даного сайту ви можете перевірити, чи знаходиться Ваша поштова скринька в одній з вкрадених баз даних. Якщо ваш e-mail потрапив до згаданих баз даних, доцільним буде видалити з пошти конфіденційне листування, змінити пароль пошти та паролі облікових записів,

які зареєстровані на цю пошту. За наявності, увімкніть двохфакторну автентифікацію.



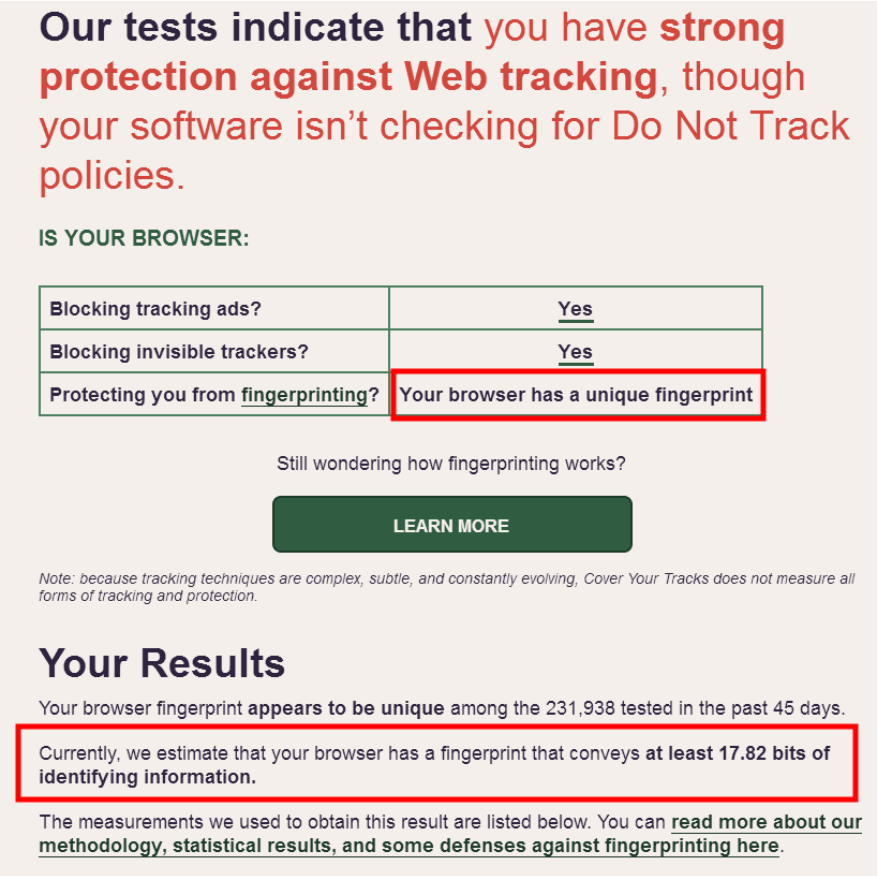
Відвідуючи вебсайти, ви залишаєте багато відомостей щодо конфігурації комп'ютера, сукупність яких є цифровими «відбитками пальців» (фінгерпринтінг), та які здатні допомогти ідентифікувати вас та ваш комп'ютер. Зокрема, фахівці з реклами використовують цю технологію в комерційних цілях.

Сервіс Panopticlick, який створила Electronic Frontier Foundation (міжнародна некомерційна юридична організація, що спеціалізується на захисті громадянських прав в галузі цифрового права, США) в основу оцінки цифрових відбитків поклав поняття інформаційної ентропії – математичну величину, що вимірюється в бітах, і яка оцінює міру хаотичності інформації. Чим більша ентропія, тим меншою є можливість ідентифікації окремо взятого комп'ютера. Оскільки на Землі живе близько 7 млрд. жителів, то вченими було встановлено, що ентропія у 33 біти дозволяє залишатися анонімним користувачем.

Чим більше конкретної інформації про комп'ютер, тобто чим менша ентропія, тим більше шансів встановлення особистих відбитків. Дослідники EFF вважають, що веб-браузер залишає достатню кількість унікальної інформації, включаючи обліковий запис, IP-адресу, cookies, інформацію, яка

міститься в рядку User Agent (щодо браузера та його версії, операційної системи, мови) – все це використовувати для ідентифікації користувача. Експеримент показав, що інформація в User Agent надає від 5 до 15 біт ідентифікуючої інформації, тому, у середньому, близько 1500 користувачів матиме такий же User Agent, як і ви. У поєднанні зі знанням географічного часового поясу, роздільної здатності екрану, глибини кольору, системних шрифтів, плагінів та деякої іншої інформації, ентропія знижується, а отже, ризик бути виявленим й упізнаним, набагато збільшується.

Якщо ви пройшли тест https://coveryourtracks.eff.org та він показав низьку ентропію, а отже, високу індивідуальність, EFF пропонує кілька рішень, які допоможуть запобігти ідентифікації вашого веб-браузера: використовувати технологію NoScript, оскільки вона блокує виявлення вебсайтами плагінів, шрифтів та cookies; перейти на більш популярний та поширений веб-браузер; використовувати найпоширенішу операційну систему, наприклад, Windows; використовувати лише ті параметри браузера, які встановлені за замовчуванням.



Ghostery – це безкоштовне розширення для браузера з можливістю антитрекінгу і блокування реклами. Модуль підтримується найпопулярнішими браузерами, серед яких Google Chrome, Mozilla Firefox, Opera, Safari, Microsoft Edge і Internet Explorer. В процесі своєї роботи Ghostery виявляє на сторінках сайтів так звані жучки, до яких розробники розширення відносять рекламу, віджети, кнопки «Поділитися» соціальних мереж, засоби аналізу дій користувача та інші небажані й відволікаючі увагу елементи, і передає контроль над ними в руки користувача. Той, у свою чергу, може залишити сторінку без змін або вибірково видалити будь-який трекер із числа виявлених програмою.

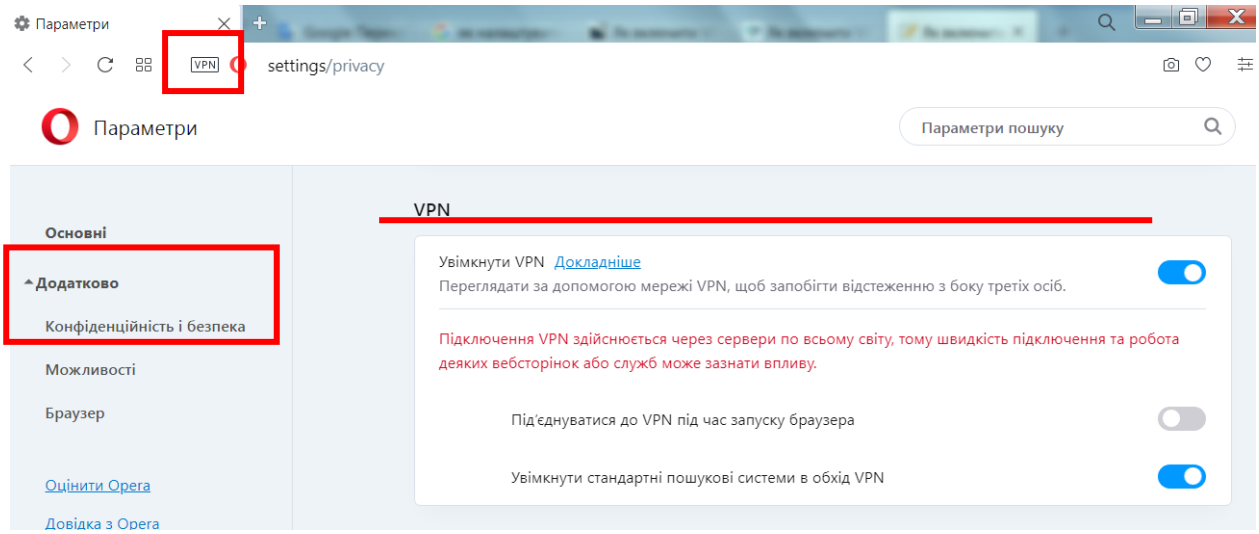
Переваги Ghostery: поширення продукту на безкоштовній основі; наявність двох режимів перегляду трекерів – простого та детального; можливість створення облікового запису користувача з метою синхронізації налаштувань Ghostery на інших пристроях; можливість експорту/імпорту налаштувань розширення; підтримка найбільш популярних браузерів; підтримка механізму створення білого й чорного списку веб-ресурсів.

Недоліки Ghostery: відсутність підтримки української мови; відсутність можливості створення власних фільтрів.

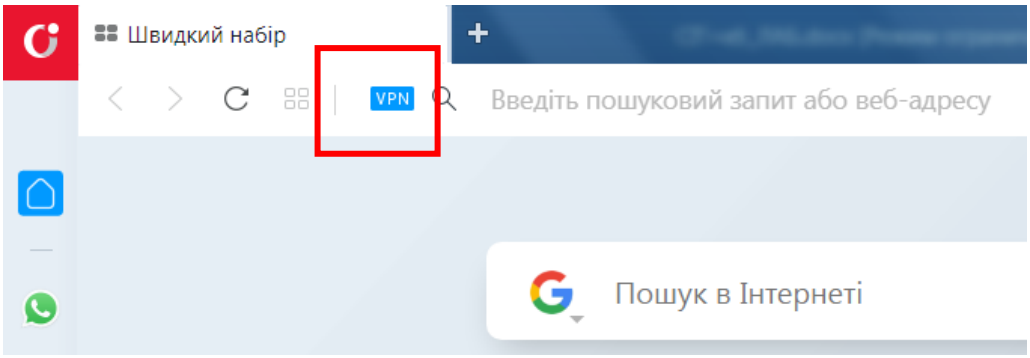
5. Знайомство з технологіями proxy та VPN.

Послуга VPN захищає вашу конфіденційність та безпеку в Інтернеті трьома важливими способами: маскує IP-адресу та місцезнаходження; інкапсулює веб-трафік; шифрує веб.

Мабуть, найбільш доступний, надійний та простий у використанні сервіс такого роду є безкоштовний VPN у браузері Opera. Запускаємо програму та заходимо в Налаштування (Setting). Зробити це можна кількома способами: натискаємо в верхньому лівому кутку червоний значок Опери та в меню вибираємо «Налаштування»; або натискаємо Alt + P; як варіант – уводимо в адресний рядок opera://settings/ та тиснемо Enter.



В адресному рядку зліва з'явиться невеликий значок VPN. Якщо він має синій колір – VPN включений та працює. Сірий колір – VPN неактивний. Натиснувши на сам значок нього можна переглянути статистику щодо трафіку.



РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Золотар О. О. Інформаційна безпека людини: теорія і практика. Монографія. / Київ: ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

2. Лісовська, Ю. П. Кібербезпека: ризики та заходи: навчальний посібник – Київ: Кондор, 2019. – 272 с.

3. Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту: навчальний посібник для студентів вищих навчальних закладів. – Львів: «Новий Світ-2000», 2020. – 678 с.

4. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.

5. Тарнавський, Ю. А. Технології захисту інформації [Електронний ресурс] – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.

ІНФОРМАЦІЙНІ РЕСУРСИ

Генератори паролів:

- https://www.avast.ua/random-password-generator;
- https://1password.com/password-generator/;
- https://axcrypt.net/information/password-generator;

Створення карти паролів: https://www.savernova.com/;

Перевірка надійності паролів:

- https://exploit.in/passcheck/;
- https://www.security.org/how-secure-is-my-password/;
- https://zillya.ua/check-password;

Бази паролів, які були скомпрометовані:

- https://breachalarm.com/?;
- https://pwnedlist.com/query;
- https://haveibeenpwned.com/Passwords;

Хмарне сховище Mega:

- https://mega.io/help;
- https://www.youtube.com/watch?v=v09UAmsXZeA;
- https://www.youtube.com/watch?v=wrer5w7GOFE;

Посібник для самостійного вивчення LibreOffice:

http://lpk.ucoz.ua/Informatika/LibreOfficee_posibnik_ua.pdf;

Документація та підтримка LibreOfficee:

- https://documentation.libreoffice.org/en/english-documentation/;
- https://help.libreoffice.org/6.3/uk/text/shared/05/new_help.html;

Сервіси відновлення втрачених паролів:

- https://www.lostmypass.com;
- https://www.password-find.com/;

Статті щодо антивірусного програмного забезпечення: https://itech.co.ua/?s=%D0%B0%D0%BD%D1%82%D0%B8%D0%B2%D1%96%D1%80%D1%83%D1%81;

Тести антивірусного програмного забезпечення:

- https://www.av-test.org/en/antivirus/home-users/;
- https://www.av-comparatives.org/;

Хмарні антивірусні сервіси:

- https://www.virustotal.com/gui/home/upload;
- https://www.hybrid-analysis.com/;
- https://metadefender.opswat.com;

Онлайн антивірусні сканери:

- https://www.eset.com/ua-ru/home/online-scanner;
- https://zillya.ua/zillya-skaner;
- https://www.trendmicro.com/ru_ru/forHome/products/housecall.html;

Довідкові системи браузерів Google Chrome, Mozilla Firefox, Opera:

- https://support.google.com/chrome/?p=help&ctx=settings#topic=9796470;
- https://support.mozilla.org/uk/products/firefox?as=u&utm_source=inproduct;
- https://help.opera.com/ru/latest/;

Додатки для браузерів Google Chrome, Mozilla Firefox, Opera:

- https://chrome.google.com/webstore/category/extensions?hl=uk;
- https://addons.mozilla.org/uk/firefox/;
- https://addons.opera.com/uk/extensions/;

Довідка вебмагазину Chrome:

https://support.google.com/chrome_webstore/answer/2664769?hl=uk;

Додаткові фільтри для блокувальника uBlock Origin: https://github.com/search?q=uBlock-filters;

Довідник поштових скриньок, які потрапили до баз даних у мережі: https://haveibeenpwned.com;

Тест браузера на рівень інформаційної ентропії: https://coveryourtracks.eff.org;

Як браузер фіксує інформацію щодо переміщення курсора миші: https://clickclickclick.click/#ab8459dff2c433c3f59108d42618bc9b;

Демонстрація даних, які збирає браузер про комп'ютер користувача: https://webkay.robinlinus.com/;

Програма Malwarebytes AdwCleaner для видалення рекламного, потенційно небажаного ПЗ: https://ru.malwarebytes.com/adwcleaner/;

Проксі-сервери:

- https://www.hidemyass.com/uk-ua/proxy;
- https://www.kproxy.com/;
- https://www.4everproxy.com/;
- http://dontfilter.us/;

Аналітика з технологій VPN: https://uk.vpnmentor.com/;

Політика інформаційної безпеки: https://pages.nist.gov/800-63-3/sp800-63-3.html – Nist 800.