МЕТОДИЧНИЙ ПОСІБНИК

ДЛЯ ТРЕНЕРІВ З ПИТАНЬ КІБЕРГІГІЄНИ

ОБСЄ Організація з безпеки та співробітництва в Європі
Координатор проектів в Україні

НАДС
НАЦІОНАЛЬНЕ АГЕНТСТВО УКРАЇНИ З ПИТАНЬ ДЕРЖАВНОЇ СЛУЖБИ

USG УКРАЇНСЬКА ШКОЛА УРЯДУВАННЯ

Die Bundesregierung

UKaid from the British people

МЕТОДИЧНИЙ ПОСІБНИК

ДЛЯ ТРЕНЕРІВ З ПИТАНЬ КІБЕРГІГІЄНИ

СПЕЦІАЛЬНА ПРОФЕСІЙНА (СЕРТИФІКАТНА) ПРОГРАМА ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ

Київ • 2021

УДК 004.7.056.5(072)
М54

Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікатної) програми підвищення кваліфікації: Практикум. – Київ: ВАІТЕ, 2021. – 106 с.

Автори-упорядники:

Олександр МАНЖАЙ, к.юр.н., доцент кафедри інформаційних технологій і кібербезпеки Харківського національного університету внутрішніх справ;

Віталій НОСОВ, к.т.н., професор кафедри інформаційних технологій і кібербезпеки Харківського національного університету внутрішніх справ.

Метою цього видання є підвищення рівня спроможності учасників щодо використання інтерактивних методик навчання дорослих з питань правильного поводження з інформацією у кіберсфері, а також формування в учасників навичок безпечної роботи із засобами комп'ютерної техніки в державному органі / органі місцевого самоврядування. Посібник може стати у пригоді державним службовцям категорії «Б» та «В», посадовим особам місцевого самоврядування, працівникам закладів післядипломної освіти, навчальних і наукових закладів, установ та організацій тощо, у тому числі фізичним особам, що здійснюють підвищення кваліфікації державних службовців та посадових осіб місцевого самоврядування.

Україна, 01030, Київ
вул. Стрілецька, 16
www.osce.org/ukraine

ОБСЄ Організація з безпеки та співробітництва в Європі
Координатор проектів в Україні

Опубліковано за сприяння Координатора проектів ОБСЄ в Україні у рамках проекту «Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки» за підтримки урядів Німеччини та Сполученого Королівства як частина загальної (сертифікатної) програми підвищення кваліфікації у співпраці з Національним агентством України з питань державної служби та Українською школою урядування.

Загальне керівництво проектом: Ольга Войтович, національна спеціалістка проектів Координатора проектів ОБСЄ в Україні.

ISBN 978-617-7627-15-8

ЗМІСТ

ЗАГАЛЬНІ МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

У межах цього курсу тренерам слід розглянути такі теми:

1. Соціальна інженерія.
2. Безпечне користування мережею Інтернет.
3. Безпечне користування електронною поштою.
4. Шкідливе програмне забезпечення.
5. Безпека користування соціальними мережами.
6. Безпека мобільних пристроїв.
7. Фізична безпека.
8. Убезпечення від неправдивих повідомлень.
9. Правові засади кібергігієни.

Методи викладання та інтерактивні заняття забезпечують формування навичок у слухачів і підвищують рівень їхніх знань. Стиль викладання залежить від навичок, компетенції та здатності викладача.

Для описаних тем рекомендовано використовувати такі **принципи викладання**:

Залучення. Зацікавте учасників тим, що ви робите, використовуйте мінімум нових термінів.

Дослідження. Учасники повинні вивчати предмет, ставити питання і досліджувати власні погляди та ідеї, потрібно скласти питання для аудиторії.

Пояснення. Слід надавати зміст модуля і обговорювати його з учасниками, говорити коротко та послідовно.

Закріплення. Використовуючи рольові ігри та сценарії, закріпіть пройдений матеріал, обов'язково посилайтеся на джерело.

Оцінювання. Використовуючи тести або обговорення та рецензування, оцініть успішність навчання учасників та повідомте їхні оцінки, звертайте увагу на неправильні частини відповідей.

Під час розкриття матеріалів курсу можна використовувати такі **прийоми викладання**:

Начитування. Цей прийом полягає у безпосередньому начитуванні змісту модуля, коли слухачі повинні слухати і вести відповідний конспект. Цей метод найкраще підходить для надання коротких правових або офіційних визначень і огляду плану заняття й навчальних цілей.

Обговорення на занятті. В межах цього прийому викладач залучає слухачів до обговорення їхнього розуміння та інтерпретації матеріалу. Цей метод добре підходить для тієї частини навчання, яка є складною або важкою для розуміння, і може застосовуватись для закріплення вивченого матеріалу або принципу. Цей прийом найкраще працює у поєднанні з начитуванням і є можливістю для викладача залучити слухачів до навчального процесу та заохотити всіх їх до однакової участі. Його також можна використати, щоб перевірити, що навчальні цілі повністю охоплено, та переконатись у тому, що студенти повністю зрозуміли зміст модуля.

Наведення прикладів протиправного використання. Щоб сприяти обговоренням на занятті й виконанню групової вправи, надано кілька прикладів протиправного використання певних технологій у відповідних частинах деяких модулів. Такі або аналогічні приклади слід використовувати, якщо потрібно збагатити і покращити навчальний досвід слухачів.

Групова вправа. Цей метод призначено для слухачів, які ще більше заглибились у навчальний процес, і застосовується через поділ аудиторії на групи однакового розміру. Групи обмірковують план заняття, а потім кожній із них ставляться певні питання. Тут можна навести приклади з практики, де кожен елемент теми може бути обговорений детальніше. Надайте можливість кожній групі представити свої відповіді по черзі, а решті аудиторії – ставити питання наприкінці кожної презентації.

Сценарії. Цей метод найскладніший для планування і викладання і передбачає створення «навчальних вправ», коли слухачі беруть участь у рольових іграх на

певну тему. Це дуже ефективний метод здобуття знань та досвіду, але він складний у застосуванні і вимагає підтримки і участі більше ніж одного викладача, а можливо, і використання інших «рольових акторів».

Щоб спланувати і успішно провести навчальний курс, викладач повинен вирішити, які засоби потрібні для викладання. Це можуть бути:

- ноутбуки та письмове приладдя для всіх слухачів, відповідне програмне забезпечення;
- роздатковий матеріал за темою для слухачів (включаючи матеріал, який потрібно прочитати до початку курсу);
- перекидні плакати, стійки і маркери для загального використання;
- комп'ютер та проектор для презентацій.

Проведення тренінгу із дорослими відрізняється від звичайного викладання навчального матеріалу студентам. Дорослі:

- не можуть пасивно сидіти годинами;
- привносять до аудиторії свої знання й досвід;
- мають мотивацію навчатись;
- цінять свій (дорогий) час;
- потребують практичних знань (а не теорії);
- потребують знань для негайного застосування.

Відповідно навчання дорослих буде ефективним тільки через виконання практичних вправ. За кожною темою тренінгу доцільно підготувати презентацію із коротким змістом навчання за приблизно такою структурою:

- тема;
- цілі навчання;
- від яких кіберзагроз будемо вчитися захищатися;
- коротка ідея щодо відповідних методів та засобів захисту;
- опис задачі, яку потрібно виконати;
- підсумки.

Зважаючи на різний рівень знань учасників, виконання ними усіх завдань не є обов'язковим.

На початку тренінгу тренер представляється, коротко розповідає про себе у контексті тематики тренінгу, щоб зазначити рівень своїх компетенцій. Здійснює знайомство та аналіз аудиторії:

- кількість;
- вікова група;
- освіта;
- рівень знань за тематикою тренінгу;
- мотиви присутності на тренінгу;
- які є побоювання, проблеми;
- цілі й очікування від тренінгу.

Далі на екран виводиться презентація за відповідною темою, оголошується тема, цілі, від яких кіберзагроз будемо вчитися захищатися, коротка ідея щодо відповідних методів та засобів захисту і перше завдання для виконання. Тренер починає демонструвати виконання завдання в темпі, що дозволяє учасникам слідувати за ним, робить зупинки, надає пояснення, відповідає на запитання і перевіряє результати виконання. За 5–10 хвилин до закінчення часу, відведеного на тему, підбиваються підсумки.

Кожен учасник заздалегідь має одержати електронний варіант порядку виконання практичних завдань. За наявності технічної можливості, на комп'ютерах учасників тренінгу доцільно встановити віртуальні машини та усі завдання виконувати на цих машинах, які перед проведенням тренінгу з новими учасниками легко відновлюються до початкового стану.

Для встановлення віртуальної машини необхідно мати комп'ютер із процесором, який підтримує апаратну віртуалізацію, та включити її в BIOS, якщо вона за замовчуванням вимкнена.

Відповіді на питання:

- як дізнатися, чи ввімкнена апаратна віртуалізація?

- як дізнатися, чи підтримує ваш ПК технологію віртуалізації?
- як увійти в BIOS, щоб увімкнути апаратну віртуалізацію?
- як увімкнути апаратну віртуалізацію в BIOS?

можна знайти тут: https://support.bluestacks.com/hc/en-us/articles/115003174386-How-to-enable-Virtualization-VT-on-Windows-10-for-BlueStacks-4.

Завантажити та встановити монітор віртуальних машин (гіпервізор) VirtualBox і VirtualBox Extension Pack можна за посиланням: https://www.virtualbox.org/wiki/Downloads.

Завантажити із сайту https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ архів віртуальної Windows-машини можна, обравши такі параметри:

- Virtual Machines: MSEdge on Win10 (x64) Stable ***;
- Choose a VM platform: VirtualBox.

Розпакувати архів віртуальної Windows-машини. Запустити VirtualBox та через меню «Файл» – «Імпортувати образ віртуальної машини» здійснити імпорт віртуальної Windows-машини. Зробити знімок (snapshot) віртуальної Windows-машини (комбінація клавіш Ctrl+Shift+T), який буде використовуватися для відновлення початкового стану машини.

З VirtualBox запустити віртуальну Windows-машину для користувача «IEUser» з паролем «Passw0rd!».

МОДУЛЬ № 1:

СОЦІАЛЬНА ІНЖЕНЕРІЯ

ПРАКТИЧНА ВПРАВА

«ЗАХИСТ ВІД ФІШІНГОВИХ АТАК»

Навчальна мета заняття: ознайомлення з принципами фішингових атак та протидії ним.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

Фішінг (англ. *fishing* – рибна ловля) – одержання доступу до конфіденційних даних користувачів, яке досягається шляхом проведення масових розсилань електронних листів від імені популярних брендів, наприклад, від імені соціальних мереж (Facebook, Twitter, Instagram), банків (Приватбанк, Ощадбанк), інших сервісів (Google.com). У листі часто міститься пряме посилання на сайт, який зовні складно відрізнити від справжнього. Опинившись на такому сайті, користувач може повідомити інформацію, що дозволяє одержати доступ до облікових записів тощо.

Фейк (Fake) – точна копія головної сторінки (або будь якої іншої сторінки) оригінального сайту, яка використовується для фішінгу з метою отримання конфіденційних даних користувачів.

Для демонстрації техніки фішінгу можуть бути використані декілька способів. Скористаємося одним з них.

1. Створити фейкову сторінку.

Для створення фейку сайту можна скористатися такою технікою:

- завантажити оригінальну сторінку сайту з формою авторизації;
- відкрити вихідний код оригінальної сторінки (наприклад, з використанням правої кнопки миші);

- скопіювати вихідний код сторінки в текстовий файл та назвати його index.html.

2. Для розміщення сторінки в мережі слід завантажити утиліту ngrok. Запустити її з командного рядка:

ngrok http 80

Завантажити набір Denwer для створення та управління сайтами та привести його у готовність.

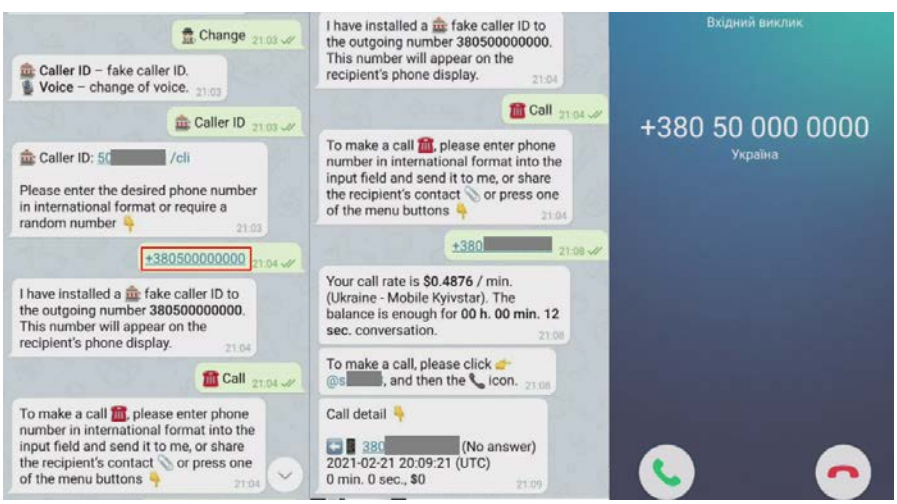
Створити в папці Denwer\Home каталог з назвою виділеної ngrok адреси, а в ньому папку www.

Розмістити в створеній папці www скрипти сайту.

Запустити Denwer.

Перевірити роботу сайту.

Одним з додаткових інструментів фішингу може бути телефонування жертві з підміненого номера (Caller ID Spoofing), приклад налаштування та результат якого зображено на зобр. 1.



Зобр. 1. Caller ID Spoofing

Для того, щоб захиститись від атак подібного виду, потрібно уважно перевіряти повідомлення, які надходять, та користуватись антифішинговими інструментами. Відповідні інструменти нерідко вбудовано у браузери.

ПРАКТИЧНА ВПРАВА

«АНАЛІЗ ПОШТОВОГО ПОВІДОМЛЕННЯ»

Навчальна мета заняття: отримати практичні навички аналізу поштового повідомлення.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

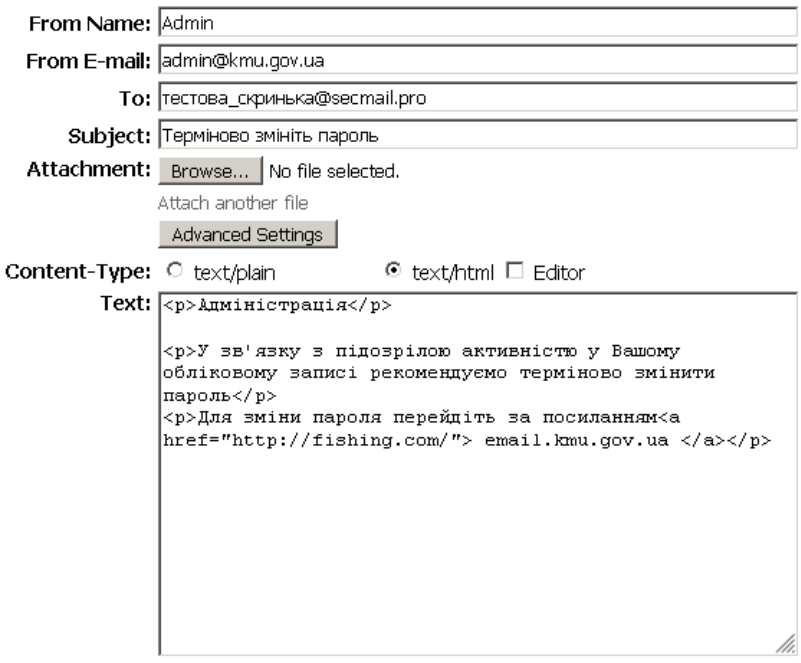
Завдання, які потрібно виконати, **підкреслено**.

Фішінгові повідомлення часто надходять користувачам за допомогою електронної пошти.

Змоделюємо ситуацію, яким чином це може відбуватися та як можна запобігти цьому негативному явищу.

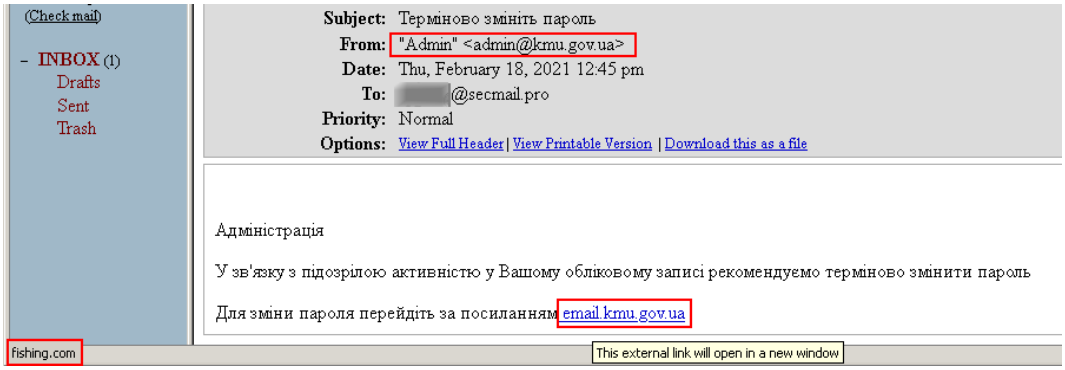
Спершу слід зареєструвати тестову поштову скриньку, на яку будемо одержувати відповідні повідомлення. Для цього можна скористатися поштовим сервісом secmail.pro, реєстрація на якому доступна через мережу TOR. Враховуючи наведене, спершу потрібно встановити на комп'ютері TOR-браузер (https://www.torproject.org/ru/download/), після чого зареєструватися за адресою http://secmailw453j7piv.onion/ або http://secmail63sex4dfw6h2nsrbmfz2z6alwxe4e3adtkpd4pcvkhht4jdad.onion/.

Після реєстрації електронної поштової скриньки слід надіслати на неї неправдиве повідомлення з підміною заголовка. Для цього можуть бути використані сервіси https://emkei.cz/, http://anonym-mail.5ymail.com, https://anonymousemail.me/ тощо. Приклад відповідним чином сформованого листа наведено на зобр. 1.



Зобр. 1. Відправлення неправдивого повідомлення

У результаті на поштову скриньку надійде лист як на зобр. 2.



Зобр. 2. Повідомлення, що надійшло

Для того, щоб виявити підробку в листі, потрібно дослідити його поштовий заголовок. Для цього слід після відкриття листа натиснути **Options:** View Full Header.

```
Return-Path: <admin@kmu.gov.ua>
Delivered-To: <тестова скринька@secmail.pro>
Received: from secmail.pro
     by secmail (Dovecot) with LMTP id zw69MqrRLmAHZgAA8Dqv6g
     for <тестова скринька@secmail.pro>; Thu, 18 Feb 2021 12:45:45 -0800
Received: by secmail.pro (Postfix, from userid 33)
     id AE93210B3120; Thu, 18 Feb 2021 12:45:45 -0800 (PST)
Received: from localhost (emkei.cz [93.99.104.210])
     by secmail.pro (Postfix) with ESMTPS id 0DEF72034F
     for <тестова скринька@secmail.pro>; Thu, 18 Feb 2021 12:45:42 -0800
(PST)
Received: by localhost (Postfix, from userid 33)
     id 8B33E222DB; Thu, 18 Feb 2021 15:45:39 -0500 (EST)
To: тестова скринька@secmail.pro
      Subject: =?UTF-
8?B?0KLQtdGA0LzRltC90L7QstC+INC30LzRltC90ZbRgtGMINC/0LDRgNC+0Ls=?=
     =?UTF-8?B?0Yw=?=
From: "Admin" <admin@kmu.gov.ua>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: admin@kmu.gov.ua
Reply-To: admin@kmu.gov.ua
Content-Type: text/html; charset=utf-8
Message-Id: <20210218204539.8B33E222DB@localhost>
Date: Thu, 18 Feb 2021 15:45:39 -0500 (EST)
```

Базовий формат поштових повідомлень (листів, messages) і статей USENET (article) визначається RFC 822 і його «спадкоємцем» RFC 2822. Кожне повідомлення (лист, message, стаття, article) складається з конверта і вмісту. Конверт зберігає адресну інформацію, необхідну для відправлення і передачі повідомлення одержувачеві. Формат конверта визначається середовищем розповсюдження. Для його автоматичного створення може використовуватися інформація з вмісту повідомлення. Стандарт визначає тільки формат вмісту повідомлення і лише у момент передачі, тобто повідомлення можуть зберігатися абсолютно в іншому форматі. Повідомлення ділиться на рядки і складається з секції заголовків і тіла повідомлення (можливо, порожнього).

Заголовок електронного поштового листа можна дослідити або вручну, або за допомогою програм чи сервісів (зобр. 3.)

IP Address	93.99.104.210
Country	Czech Republic
Region	-
City	-
ISP	Liberty Global
Organization	Liberty Global
Latitude	50.0848
Longitude	14.4112

Зобр. 3. Результат аналізу заголовка поштового листа за допомогою сервісу iplocation.net

Виходячи з даних, наведених в теоретичних відомостях:

1. Зареєструвати поштову скриньку та надіслати тестове повідомлення.
2. Проаналізувати заголовок та тіло листа зі своєї електронної поштової скриньки. Визначити адресу відправника та маршрут руху листа за допомогою сервісів http://ua.smart-ip.net/trace-email, https://toolbox.googleapps.com/apps/messageheader/analyzeheader, або https://www.iplocation.net/trace-email.

▶ Приклад. «*Розшифровка типового заголовка листа*»

Return-path:* *@ukr.net** – *зворотна адреса, вказана відправником;*

Received: from [212.9.224.21] (port=25 helo=mail-out.iptelecom.net.ua) – *лист отримано від хосту mail-out.iptelecom.net.ua з IP-адресою 212.9.224.21;*

by mx5.mail.ru – *ім'я комп'ютера, який приймав повідомлення;*

with esmtp id 1COlNS-000F0L-00 – *комп'ютер, що прийняв повідомлення, надав йому ідентифікаційний номер 1COlNS-000F0L-00;*

Tue, 18 Nov 2008 02:14:18 +0300 – *передавання листа здійснювалося у вівторок, 18 листопада 2008 року о 02:14:18 за часом третього часового поясу, який випереджає Гринвічський часовий пояс на 3 години, звідси «+0300»;*

Received-SPF: none (mx5.mail.ru: 212.9.224.21 is neither permitted nor denied by domain of ukr.net) client-ip=212.9.224.21 – *отримана відповідь на SPF-запит. Технологія SPF (Sender Policy Framework) є одним зі способів ідентифікації відправника електронного листа та надає додаткову можливість фільтрування потоку пошти на наявність у ньому повідомлень зі спамом. За допомогою SPF пошта поділяється на «дозволену» й «заборонену» відносно домену одержувача чи відправника. В цьому випадку, поштовий сервер-одержувач mx5.mail.ru здійснив SPF-запит до домену ukr.net, де було отримано відповідь про фактичну відсутність SPF-захисту (дослівно: mx5.mail.ru здійснив SPF-запит до домену ukr.net про наявність у списках IP-адреси 212.9.224.21, на що було*

отримано відповідь про те, що цю адресу не внесено ані в дозволені, ані в заборонені списки SPF домену ukr.net);

envelope-from=*@ukr.net*** *– заголовок, який додається до листа деякими поштовими програмами під час доставки кінцевому одержувачу;*

helo=mail-out.iptelecom.net.ua;

Received: from h136.246.159.dialup.iptcom.net ([213.159.246.136]:64011 «HELO copm1» ident: «NO-IDENT-SERVICE[2]» whoson: «s-m-i-t»);

by pechkin.iptelecom.net.ua with SMTP id S358789AbUKAXOS (ORCPT <rfc822;igoset@mail.ru> + 3 others);

Tue, 18 Nov 2008 01:14:18 +0200 *– час, коли одержано лист;*

Message-ID: <021501c4c068$4d89ba20$0200a8c0@copm1> *– процес одержання листа первинним провайдером для подальшого пересилання з ПК, підключеного за допомогою модемного з'єднання (h136.246.159.dialup.iptcom.net). Розшифрування є аналогічним вищевикладеному;*

From: *@ukr.net*** *– напис на «конверті», від кого лист;*

To: <**@mail.ru>, <**@ukrpost.net>, <@mail.ru>, <**@ukr.net>, <**@yahoo.co.uk>, <**@ok.ru>, <**@yandex.ru>, <****@mail.ru>, <*****@mail.ru>, <**@bk.ru>, *@ukr.net*** *– адреси доставки листа;*

Subject: =?koi8-r?B?8NLFxMzP1sXOycU=?= *– тема листа (у разі заміни кодування тема матиме вигляд напису «Предложение»);*

Date: Tue, 18 Nov 2008 00:52:14 +0200 *– дата та час створення листа (вівторок 2 листопада 2008 р., о 00:52:14 на комп'ютері зі встановленим 2-м часовим поясом);*

MIME-Version: 1.0 *– версія стандарту, відповідно до якого створено цей лист;*

Content-Type: multipart/alternative *– формат змісту листа. Визначається тип інформації в листі та спосіб її відображення. Зокрема, встановлюється кодування листа, якщо використовується який-небудь національний набір символів;*

boundary=»----=_NextPart_000_0015_01C4C076.3170DA90» *– стандартизація розбивання великих листів на декілька частин. У полі «Content-Type» після значення «multipart/<subtype>» зазначається рядок – унікальний обмежувач фрагментів «boundary=<boundary string>». А потім перед кожним фрагментом пишеться цей рядок з двома мінусами попереду, а в кінці фрагментації – ще один рядок, який завершується такими ж двома мінусами.*

X-Priority: 3 *– пріоритет листа, позначений цифрами.*

X-MSMail-Priority *– нестандартне поле Microsoft – пріоритет листа. Буває «звичайним», «невідкладним» та «не невідкладним». Зазвичай використовуються слова: «Normal», «Urgent», «Non-urgent». Може впливати на швидкість обробки та передачі листа різними проміжними поштовими системами;*

X-Mailer: Microsoft Outlook Express 5.50.4927.1200 *– інформація про поштову програму, яка використовувалася для створення листа;*

X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4927.1200 *– інформація про фірму виробника програмного забезпечення;*

X-Spam: Not detected *– лист не визначено як спам.*

МОДУЛЬ № 2:

БЕЗПЕЧНЕ КОРИСТУВАННЯ МЕРЕЖЕЮ «ІНТЕРНЕТ»

ПРАКТИЧНА ВПРАВА

«БЕЗПЕЧНИЙ ПЕРЕГЛЯД ВЕБСТОРІНОК»

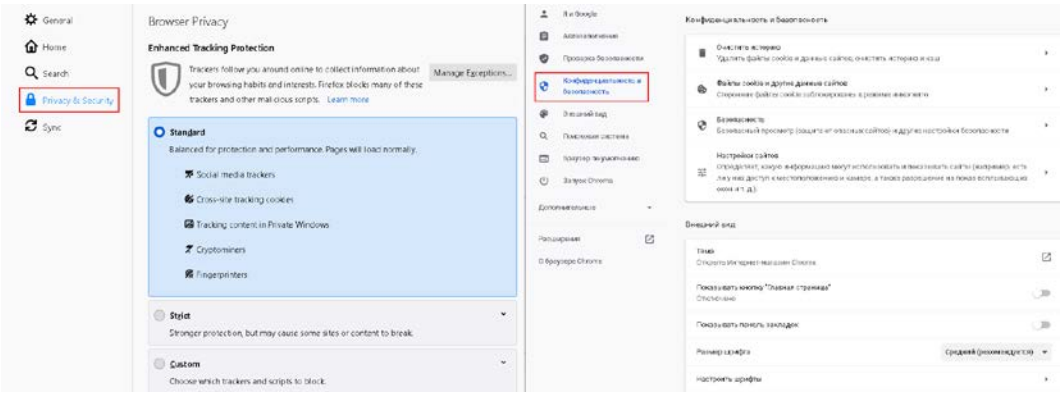
Навчальна мета заняття: здійснити налаштування браузеру та встановлення додаткових плагінів для безпечного серфінгу в мережі.

Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено.**

Перегляд вебсторінок, як правило, здійснюється за допомогою програм-браузерів, найпоширенішими серед яких є Chrome та Firefox. В усіх сучасних браузерах присутнє меню налаштувань, за допомогою якого можна здійснити налаштування безпеки та конфіденційності (зобр. 1).



Зобр. 1. Зліва направо налаштування безпеки у браузерах Firefox та Chrome

Якщо налаштування безпеки не повною мірою влаштовують користувача, можна встановити додаткові плагіни. Як приклад плагінів за напрямом безпеки можна навести:

- AdBlock для блокування спливаючих вікон (https://adblockplus.org/ru/download);

- RequestPolicy для блокування міжсайтових запитів (https://www.requestpolicy.com/);
- HideMyBack для приховування або зміни певної інформації про ідентифікатори програм і пристроїв (https://chrome.google.com/webstore/detail/hide-my-back/adkllkhpobbaieagddmffnfkgibplegi);
- Click&Clean для видалення тимчасових файлів у браузері (https://www.hotcleaner.com/).

1. Налаштуйте параметри безпеки та конфіденційності браузера. Поясніть свій вибір налаштувань.

2. Встановіть додаткові плагіни, описані в матеріалах до заняття. Опишіть порядок їх використання.

ПРАКТИЧНА ВПРАВА

«СПОСОБИ ОРГАНІЗАЦІЇ БЕЗПЕЧНОГО З'ЄДНАННЯ В МЕРЕЖІ»

Навчальна мета заняття: відпрацювати різні технології забезпечення з'єднання в мережі.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

Вхідні дані.

Перелік VPN-сервісів та проксі-серверів:

free-proxy.cz

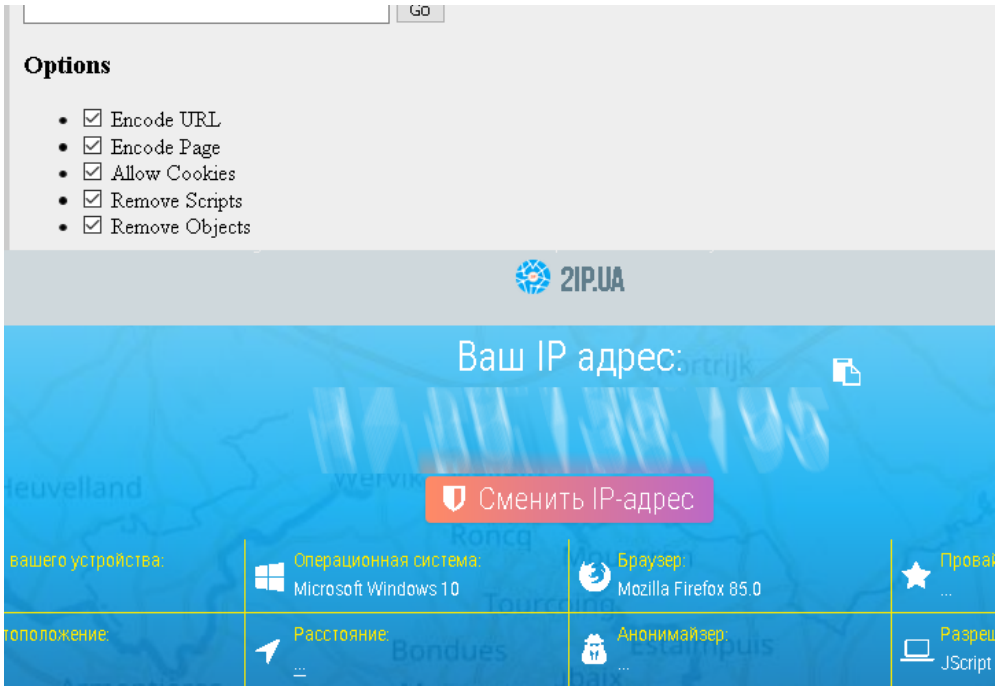
vpnbook.com

protonvpn.com

Для налагодження безпечного з'єднання з віддаленими ресурсами може бути застосовано проміжні убезпечуючі механізми, як-от: проміжні проксі- або VPN-сервери. Для демонстрації роботи таких серверів можна здійснити таке.

Проксі-сервери

Відкрити сторінку http://free-proxy.cz/en/web-proxylist/, після чого обрати будь-який проксі-вебсервер. Ввести у відповідному вікні адресу 2ip.ua. Оцінити одержані результати (зобр. 1).

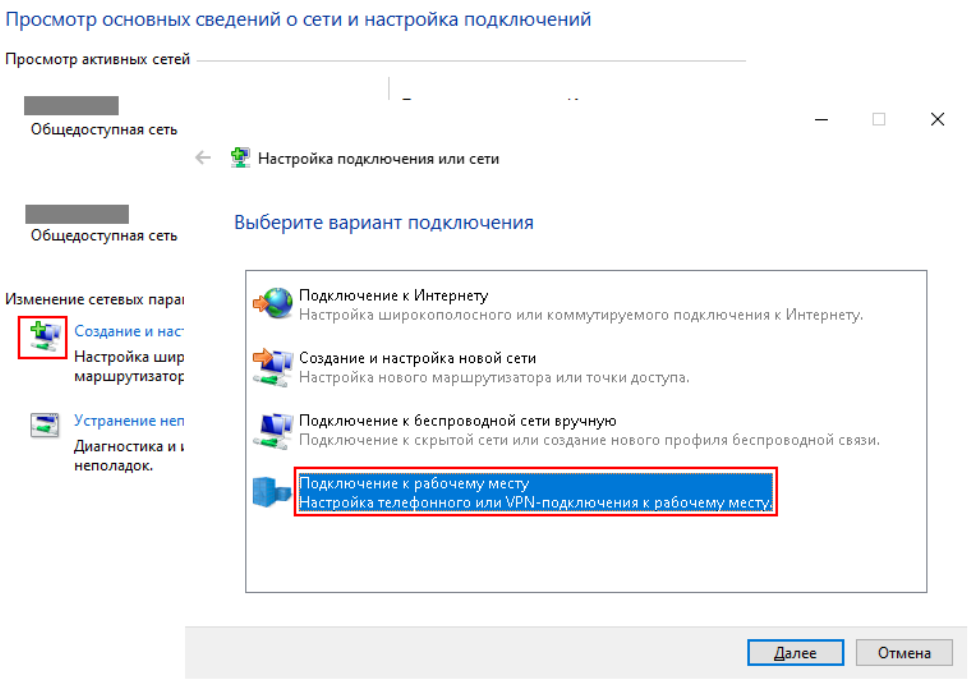


Зобр. 1. Результат використання проксі-серверу

VPN-сервери

На відміну від проксі-серверів, які працюють за окремими портами, VPN-сервери надають можливість організації повноцінного захищеного з'єднання між користувачем та відповідними ресурсами. Для користування VPN-сервером потрібно знати його налаштування та відповідні автентифікаційні дані.

Як правило, налаштувати відповідне підключення можна без необхідності встановлення додаткового програмного забезпечення. Для цього, наприклад, у системі Windows 10 слід відкрити «Центр управління мережами та спільним доступом» та створити нове з'єднання (зобр. 2).

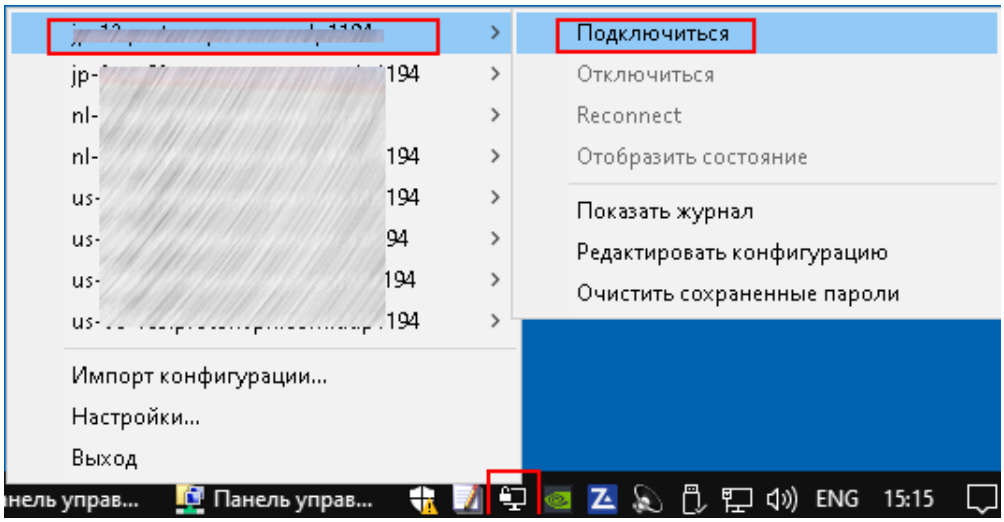


Зобр. 2. Налаштування нового з'єднання в операційній системі

Далі слід вказати адресу VPN-сервера та перейти у розділ «Зміна параметрів адаптера» та двічі натиснути на новоутвореному з'єднанні. Після цього слід ввести відповідне ім'я користувача і пароль та дочекатися з'єднання.

Більш універсальний спосіб налаштування VPN-з'єднання полягає у використанні спеціальних програм для організації такої діяльності. З цією метою може бути використано, наприклад, безкоштовний застосунок OpenVPN, який можна завантажити за адресою: https://openvpn.net/community-downloads/.

Після встановлення програми відповідні файли налаштування з'єднання записуються у папку Config програми OpenVPN. Запустивши програму слід обрати відповідну конфігурацію та під'єднатися до VPN-сервера (зобр. 3)



Зобр. 3. З'єднання з VPN-сервером за допомогою програми OpenVPN

1. Відпрацювати підключення через одиничний та ланцюжок проксі-серверів.

2. Відпрацювати принаймні два способи налаштування VPN-з'єднання: 1) через налаштування параметрів мережного підключення операційної системи та 2) за допомогою VPN Client).

3. Переконатися у зміні параметрів виходу в мережу (наприклад, скориставшись сайтом 2ip.ua).

4. Встановити Firewall та антивірус ZoneAlarm.

ПРАКТИЧНА ВПРАВА

«НАКЛАДАННЯ ЕЛЕКТРОННОГО ПІДПИСУ»

Навчальна мета заняття: відпрацювати різні технології забезпечення з'єднання в мережі.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

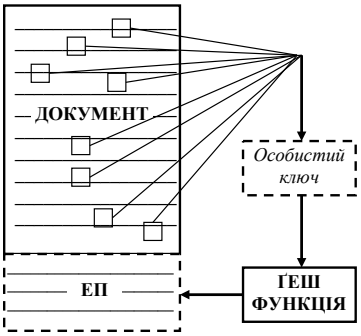
Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

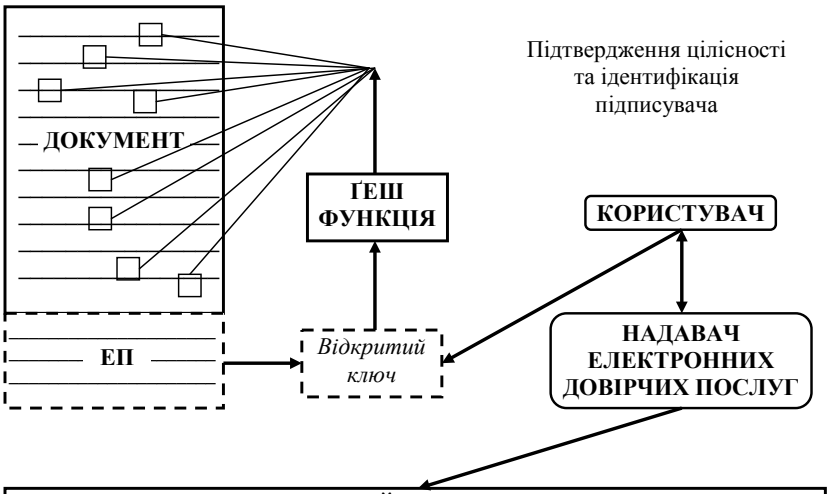
Реквізитом електронного документа є ***електронний підпис*** – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються та використовуються ним як підпис. Електронний підпис накладається за допомогою *особистого ключа* та перевіряється за допомогою *відкритого ключа*.

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

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



Зобр. 1. Приблизна модель накладання електронного підпису



КВАЛІФІКОВАНИЙ СЕРТИФІКАТ КЛЮЧА

- позначка, що сертифікат відкритого ключа виданий як кваліфікований сертифікат відкритого ключа;
- позначка, що сертифікат відкритого ключа виданий в Україні;
- ідентифікаційні дані, які однозначно визначають кваліфікованого надавача електронних довірчих послуг, засвідчувальний центр або центральний засвідчувальний орган, які видали кваліфікований сертифікат відкритого ключа;
- ідентифікаційні дані, які однозначно визначають користувача електронних довірчих послуг;
- місцезнаходження юридичної особи, якій видано кваліфікований сертифікат відкритого ключа;
- значення відкритого ключа, який відповідає особистому ключу;
- відомості про початок та закінчення строку дії кваліфікованого сертифіката відкритого ключа;
- серійний номер кваліфікованого сертифіката відкритого ключа, унікальний для суб'єкта, який видав сертифікат;
- кваліфікований електронний підпис або кваліфікована електронна печатка, створені суб'єктом, який видав сертифікат;
- відомості щодо розміщення у вільному доступі кваліфікованих сертифікатів відкритих ключів суб'єкта, який видав сертифікат;
- відомості щодо розміщення інформації, необхідної для отримання кваліфікованої електронної довірчої послуги формування, перевірки та підтвердження чинності кваліфікованих сертифікатів відкритих ключів;
- відомості про те, що особистий ключ зберігається в засобі кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);
- відомості про обмеження використання кваліфікованого електронного підпису чи печатки (для кваліфікованого сертифіката електронного підпису чи печатки);
- ім'я (імена) домену, що належить фізичній або юридичній особі, якій видано сертифікат відкритого ключа (для кваліфікованого сертифіката автентифікації веб-сайту).

Зобр. 2. Приблизна модель перевірки електронного підпису

Накладання електронного підпису не забезпечує конфіденційності документа, тобто його зміст **не шифрується**, але при цьому можна впевнитись у *цілісності* документа й *ідентифікувати його підписувача*.

Одним із швидких способів організації роботи з електронним підписом є використання у зв'язці електронного підпису від Приватбанку та програми ІІТ Користувач ЦСК-1.

Відповідний алгоритм можна описати таким чином:

1. Завантажити програму ІІТ Користувач ЦСК-1 (http://acskidd.gov.ua/korustyvach_csk) та встановити її на комп'ютері.
2. Авторизуватись в системі Приват24 та в меню Усі послуги → Бізнес → Електронний цифровий підпис → Завантажити сертифікат згенерувати відповідні файли, потрібні для безпечного електронного документообігу. При виконанні цього завдання може знадобитися встановлення додаткових плагінів для браузера Google Chrome. Завантажити відповідні сертифіката можна за адресою https://acsk.privatbank.ua/certs.
3. Імпортувати заванатажені сертифікати до програми ІІТ Користувач ЦСК-1 через відповідне меню Параметри.
4. Після вчинення відповідних дій у програмі ІІТ Користувач ЦСК-1 можна підписувати різні документи, перевіряти вже наявні підписані файли на предмет автентичності електронного підпису та цілісності документа, виконувати функції шифрування / розшифрування документів.
5. У разі відсутності потреби у використанні електронного підпису, можна відкликати сертифікат на сторінці https://acsk.privatbank.ua/service.

Порядок проведення заняття

1. Завдання: одержати ключі електронного підпису через електронний кабінет у банку.
2. З використанням ресурсу ca.informjust.ua/sign накласти електронний підпис на довільний файл трьома способами. За допомого сервісу informjust.ua/verify перевірити цілісність документа. Змінити підписаний файл. Провести повторну перевірку.
3. З використанням електронного підпису авторизуватись в онлайн-будинку юстиції (online.minjust.gov.ua/login). Одержати інформацію з державного реєстру речових прав.
4. З використанням електронного підпису авторизуватися на порталі електронних послуг пенсійного фонду (portal.pfu.gov.ua). Перевірити відомості про свої відрахування.
5. З використанням електронного підпису авторизуватися в електронному кабінеті на порталі Державної фіскальної служби України (cabinet.sfs.gov.ua). Перевірити відомості про свої доходи.
6. Відпрацювати роботу програми «ІІТ Користувач ЦСК-1» за адресою: acskidd.gov.ua/korustyvach_csk та застосунок за адресою https://acsk.privatbank.ua/program.

МОДУЛЬ № 3:

БЕЗПЕЧНЕ КОРИСТУВАННЯ ЕЛЕКТРОННОЮ ПОШТОЮ

ПРАКТИЧНА ВПРАВА

«ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ПОШТОВОГО ОБЛІКОВОГО ЗАПИСУ»

Навчальна мета заняття: відпрацювати навички налаштування двофакторної автентифікації для різних облікових записів.

Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», смартфони або телефони у слухачів, флеш-накопичувачі за кількістю слухачів.

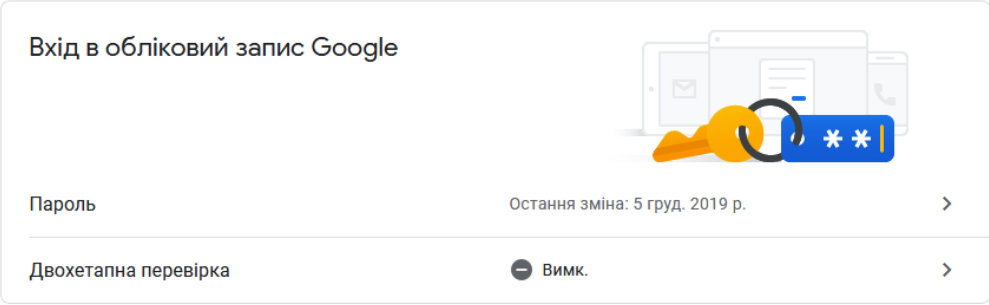
Порядок проведення заняття

Створити безкоштовні особисті поштові облікові записи в доменах gmail.com та protonmail.com.

Налаштувати двофакторну автентифікацію через Google Authenticator для облікових записів gmail.com та protonmail.com.

Для облікового запису gmail.com

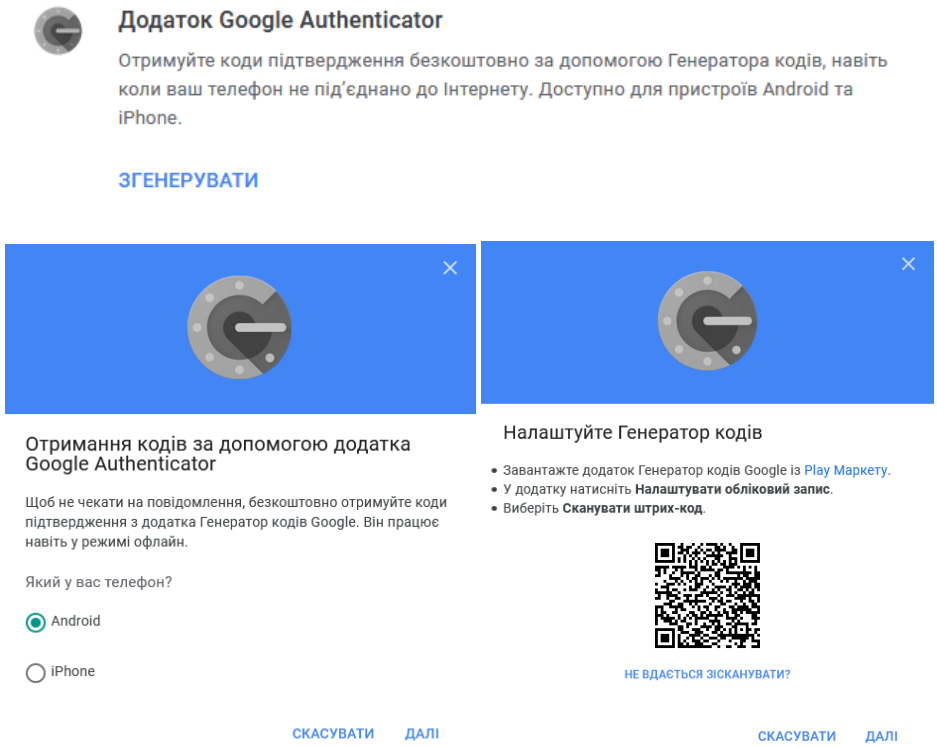
Перейти у розділ «Ваш обліковий запис» – «Безпека» – «Вхід в обліковий запис Google». Обрати «Двохетапна перевірка» – «Розпочати» (зобр. 1).



Зобр. 1. Розділ налаштувань двоетапної перевірки

Обрати автентифікацію через коротке текстове повідомлення і зареєструвати особистий телефон через отримання коду в sms і вводу його у відповідному полі налаштувань.

Знову увійти в «Безпека» – «Вхід в обліковий запис Google» – «Двоетапна перевірка» – «Розпочати» та додати інші варіанти другого етапу перевірки, щоб підтверджувати свою особу, а саме «Додаток Google Authenticator». Завантажити за наданим посиланням у смартфон додаток «Генератор кодів Google» (зобр. 2) та дотримуйтесь інструкцій щодо його налаштування.

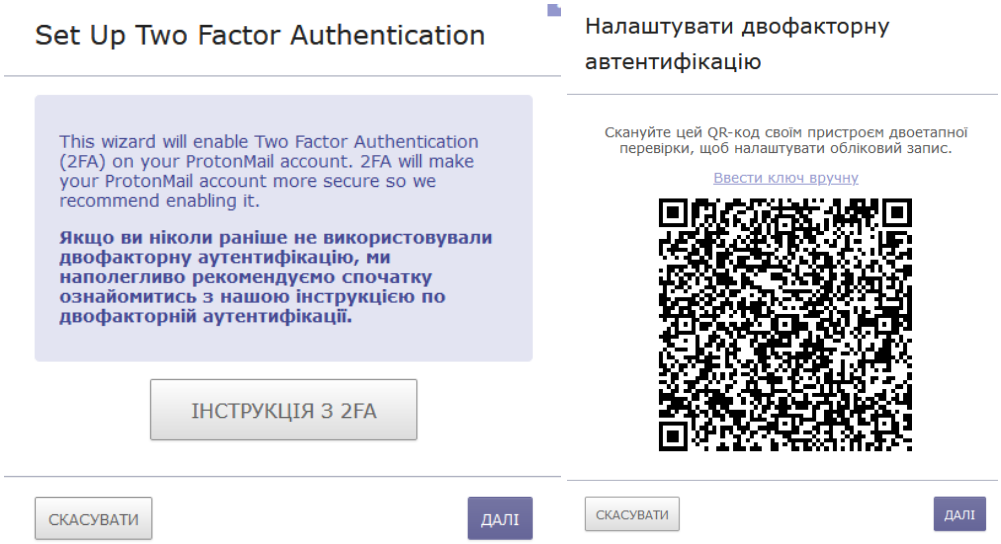


Зобр. 2. Інструкції майстру налаштувань Google Authenticator

Після закінчення налаштувань вийти із облікового запису та пройти вже двоетапну автентифікацію.

Для облікового запису protonmail.com

У поштовому обліковому записі protonmail перейти у розділ «Налаштування» – «Безпека» – «Увімкнути двоетапну перевірку» – «Налаштувати двофакторну автентифікацію» (зобр. 3).



Зобр. 3. Інструкції майстра налаштувань двофакторної автентифікації

Скористатися вже встановленим у смартфоні застосунком Google Authenticator (встановлюється з Google Play або App Store) і налаштувати двоетапну автентифікацію. Вийти із облікового запису та пройти вже двоетапну автентифікацію.

ПРАКТИЧНА ВПРАВА
«ПАРОЛЬНИЙ МЕНЕДЖЕР»

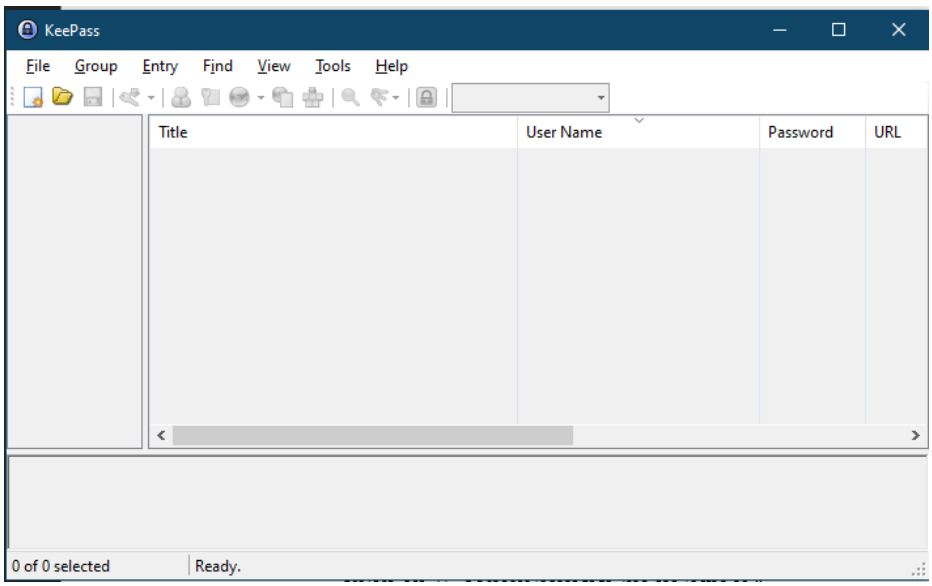
Навчальна мета заняття: встановити, налаштувати та опановувати використання парольного менеджера KeePass.

Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», смартфони або телефони у слухачів, флеш-накопичувачі за кількістю слухачів.

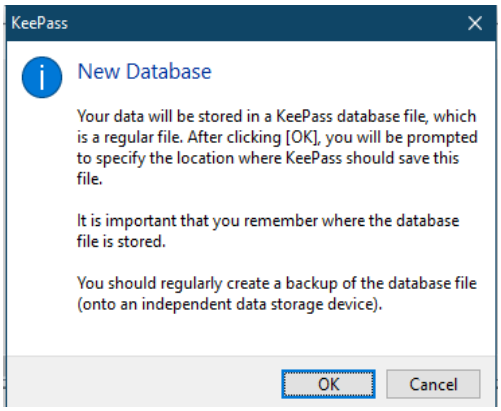
Порядок проведення заняття

Завантажити (https://keepass.info/index.html), встановити та запустити парольний менеджер KeePass Password Safe (зобр. 1).



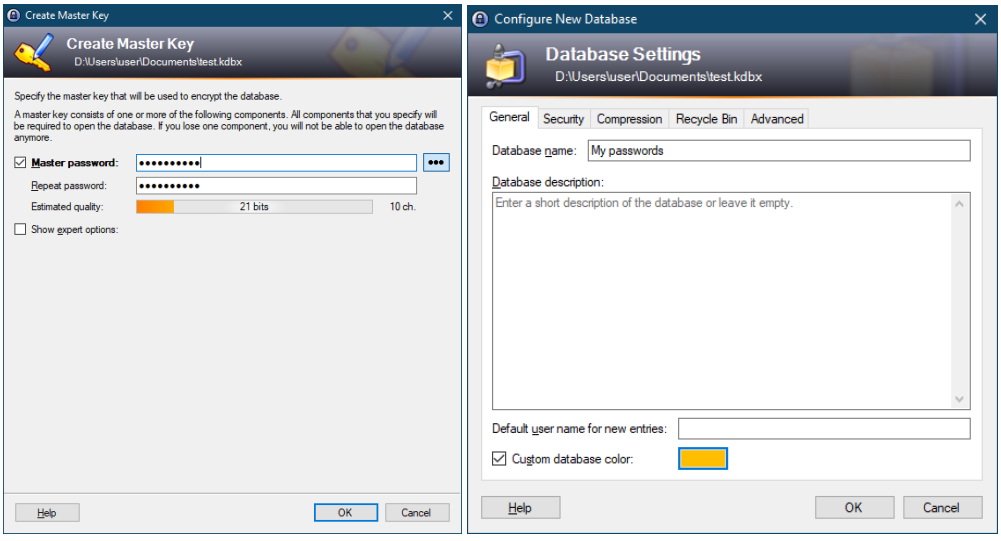
Зобр. 1. Головне вікно KeePass

Комбінацією клавіш (Ctrl+N) створити та вказати місце зберігання файлу нової бази паролів (зобр. 2).

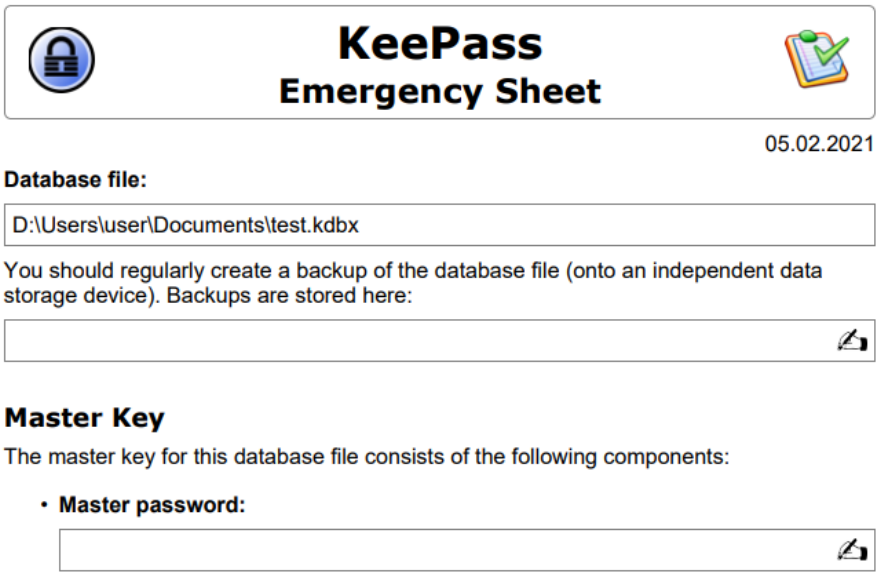


Зобр. 2. Повідомлення щодо створення нової бази паролів

Придумати та запам'ятати майстер-пароль (парольну фразу) довжиною не менше 10-ти символів із використанням маленьких та великих літер, цифр та спеціальних символів. Ввести майстер-пароль (парольну фразу) та вибрати ім'я для бази паролів (зобр. 3). Додатково можна роздрукувати основні дані щодо місця зберігання основної бази паролів, її резервної копії та підказки щодо майстер-пароля (зобр. 4).



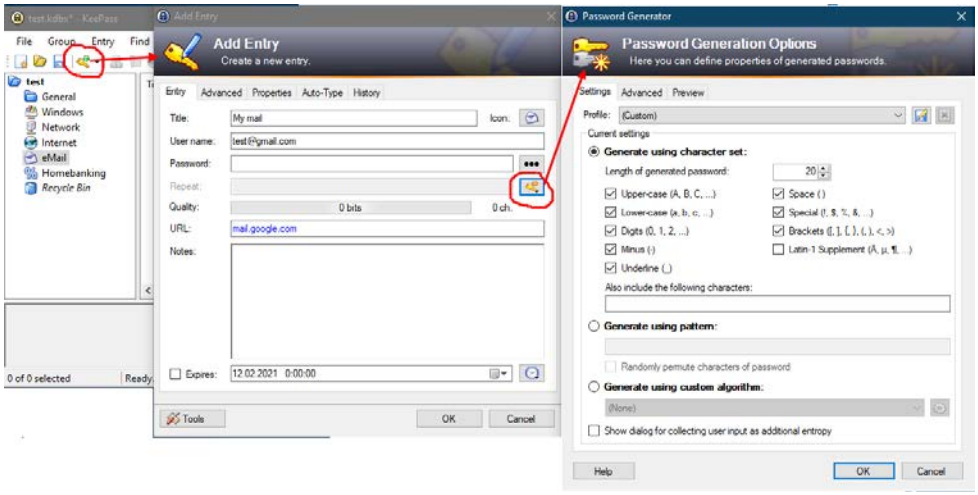
Зобр. 3. Створення майстер-паролю та налаштування бази


KeePass
Emergency Sheet
05.02.2021
Database file:
D:\Users\user\Documents\test.kdbx
You should regularly create a backup of the database file (onto an independent data storage device). Backups are stored here:
Master Key
The master key for this database file consists of the following components:
• Master password:

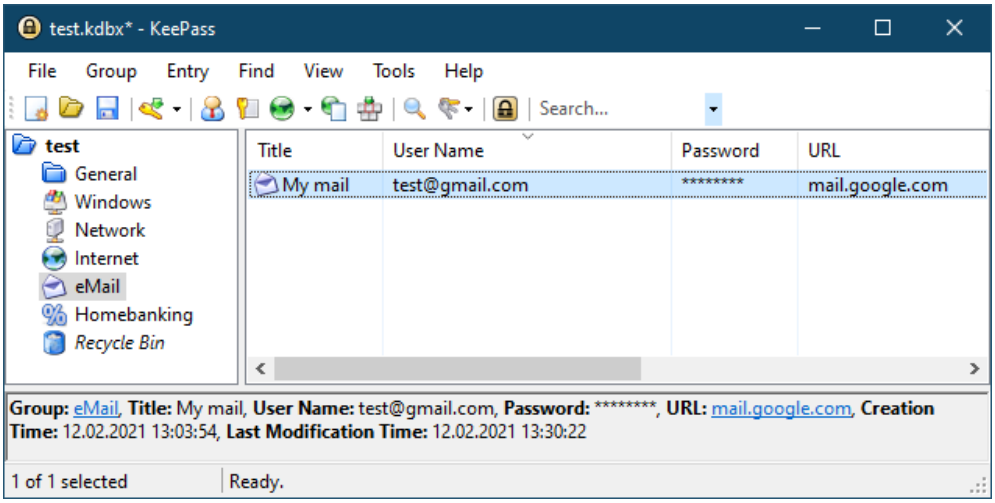
Зобр. 4. Пам'ятка щодо місця зберігання основної бази паролів, її резервної копії та підказки щодо майстер-пароля

В основному вікні KeePass зліва обрати теку «eMail», створити новий запис (комбінація клавіш Ctrl+I), заповнити поля для свого поштового облікового запису, перейти у налаштування Генератора паролів і обрати довжину пароля та абетку символів, з яких буде генеруватися пароль (зобр. 5). Завершити редагування, зберегти зміни (комбінація клавіш Ctrl+S) і переглянути створений запис (зобр. 6).

Зверніть увагу, що деякі вебсервіси забороняють наявність в паролі спеціальних символів. У такому випадку, або після генерації паролю вручну видалити спеціальні символи або виключити їх із абетки налаштувань Генератора паролів.



Зобр. 5. Створення і налаштування параметрів нового запису у базі паролів



Зобр. 6. Створений запис у базі паролів

Пройти автентифікацію в поштовому сервісі, використовуючи менеджер паролів. Для цього в KeePass обирається відповідний запис та почергово копіюється у буфер логін (комбінація клавіш Ctrl+B) та пароль (комбінація клавіш Ctrl+C), які почергово вставляються у відповідні поля форми автентифікації поштового сервісу.

ПРАКТИЧНА ВПРАВА

«ПЕРЕВІРКА ФАКТУ КОМПРОМЕТАЦІЇ ПОШТОВОЇ АДРЕСИ»

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

Час проведення: 0,25 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome».

Порядок проведення заняття

За адресами https://haveibeenpwned.com, https://monitor.firefox.com перевірити наявність власних поштових облікових записів у «зливах», де фігурують вкрадені дані автентифікації. У випадку знаходження поштових облікових записів у «зливах» терміново змінити паролі на відповідних ресурсах та, за можливості, налаштувати двофакторну автентифікацію.

ПРАКТИЧНА ВПРАВА

«ЕЛЕКТРОННИЙ ПІДПИС ТА ШИФРУВАННЯ ПОВІДОМЛЕНЬ»

Навчальна мета заняття: налаштувати утиліту gpg4usb, створити повідомлення для співрозмовника, підписати та зашифрувати повідомлення. Співрозмовнику розшифрувати і перевірити підпис у отриманому повідомленні.

Час проведення: 1,75 год. Місце проведення: комп'ютерний клас.

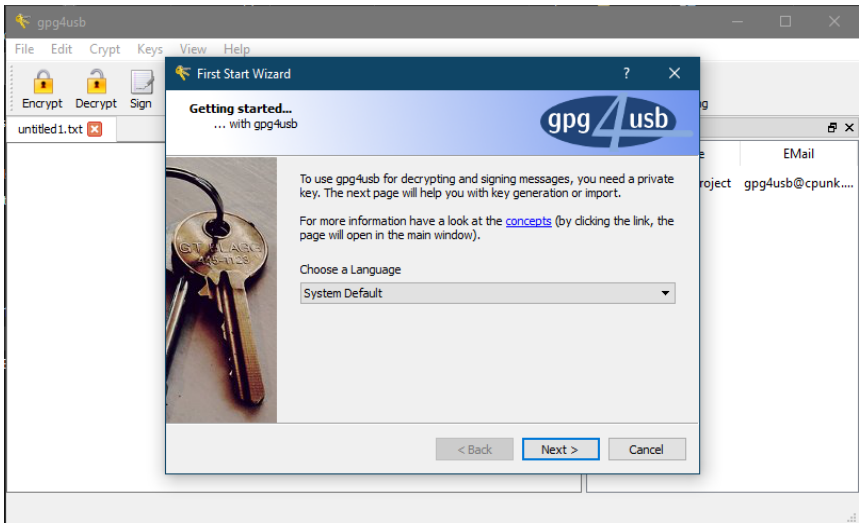
Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome».

Порядок проведення заняття

Виконати такі дії:

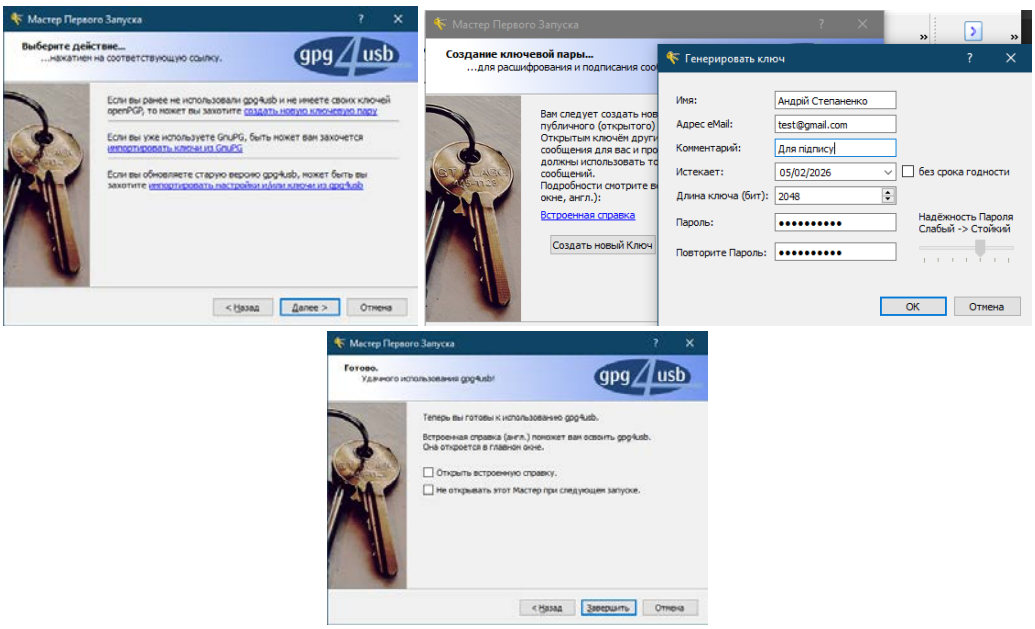
- встановити на свій флеш-накопичувач утиліту **gpg4usb**;
- згенерувати пару своїх ключів;
- експортувати свій публічний ключ в окремий файл *_pub.asc;
- обмінятися своїм публічним ключем з іншими;
- імпортувати у програму публічні ключі інших;
- створити повідомлення для співрозмовника, підписати повідомлення та зашифрувати його з використанням публічного ключа адресата;
- отримати підписане та зашифроване повідомлення, розшифрувати повідомлення та перевірити електронний підпис.

За посиланням https://www.gpg4usb.org/download.html вибрати та завантажити на особистий флеш-накопичувач архів утиліти gpg4usb. Розпакувати архів, запустити утиліту start_windows.exe та обрати зручну мову інтерфейсу (зобр. 1).



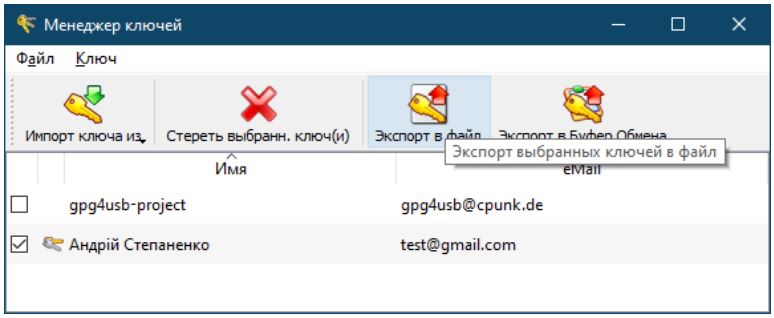
Зобр. 1. Налаштування мови інтерфейсу gpg4usb

Далі клікнути на посилання «Створити нову ключову пару», обрати «Створити новий Ключ» та заповнити відповідні поля персональними даними (пароль згенерувати та зберегти у менеджері паролів). Завершити налаштування у майстрі першого запуску (зобр. 2).



Зобр. 2. Генерування ключів у майстрі першого запуску

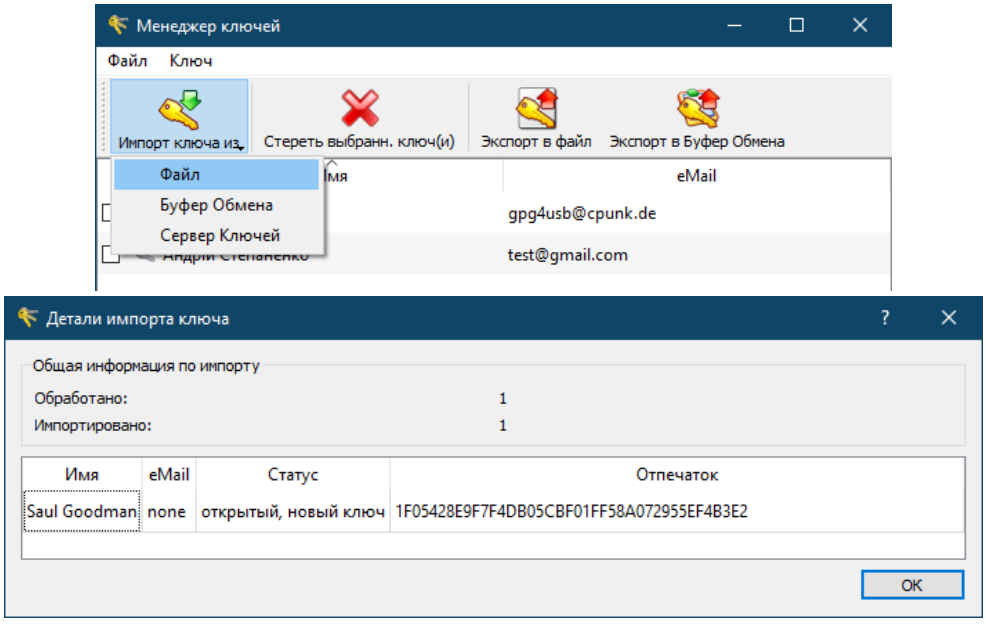
Запустити «Менеджер ключів», обрати обліковий запис своїх ключів, вибрати «Експорт обраних ключів у файл» та зберегти свій публічний ключ (наприклад, Андрій Степаненко test@gmail.com(202AA4030C558985)_pub.asc) на флеш-накопичувач (зобр. 3).



Зобр. 3. Експорт публічного ключа

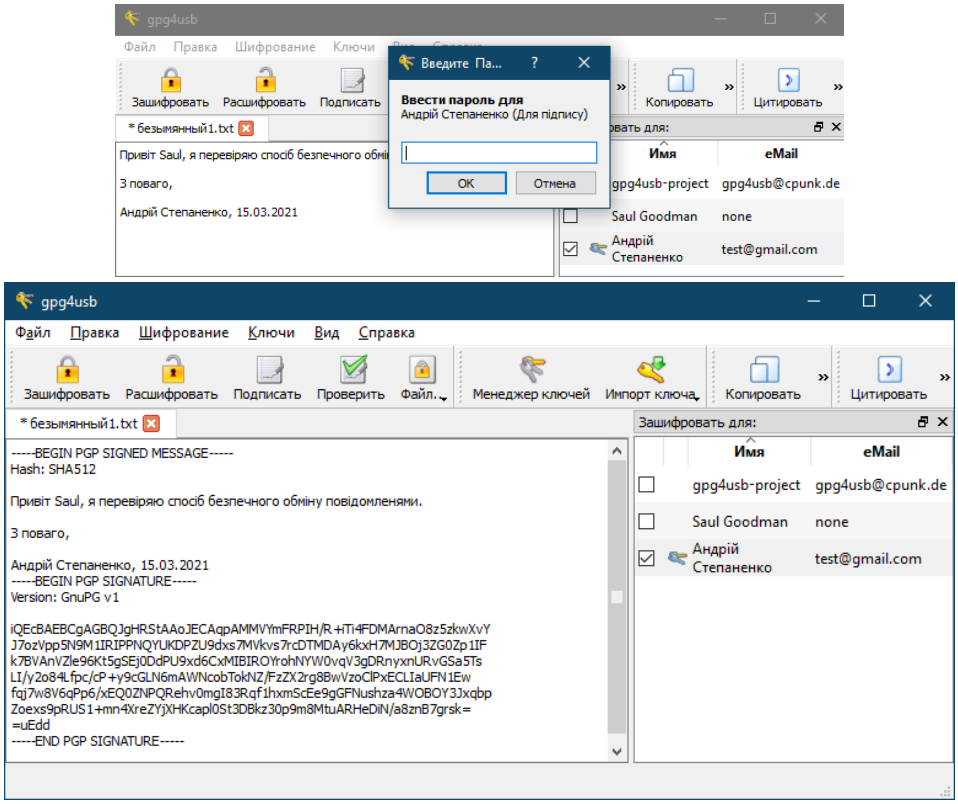
Слухачам обмінятися між собою своїми публічними ключами (Андрій Степаненко test@gmail.com(202AA4030C558985)_pub.asc) – це можна зробити пересиланням поштою або локальним копіюванням на свої носії.

У менеджері ключів здійснити імпорт у програму файлів публічних ключів, отриманих від інших слухачів (зобр. 4).



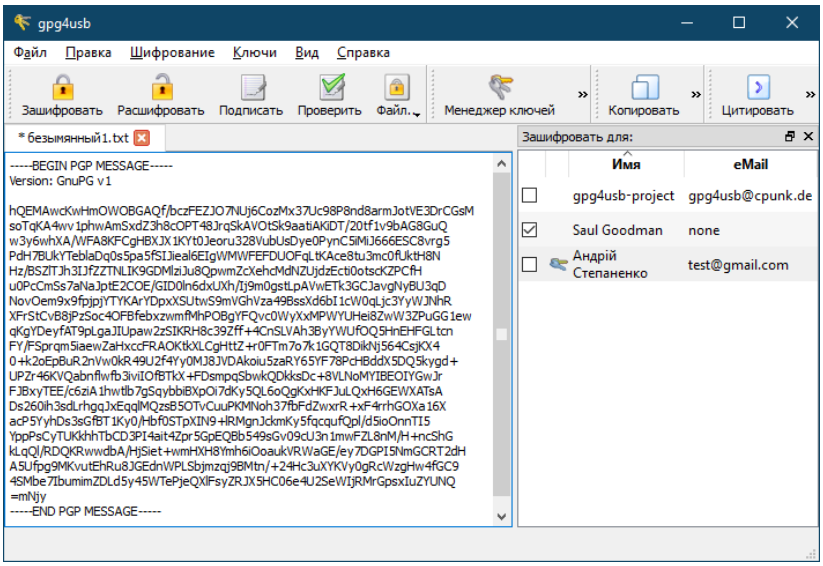
Зобр. 4. Імпорт публічних ключів співрозмовників

Створити довільне повідомлення для співрозмовника, вказати дату, час та зазначити свій ключ у правому віконці програми. Обрати «Підписати» повідомлення, ввести пароль для свого приватного ключа та отримати підпис (зобр. 5).



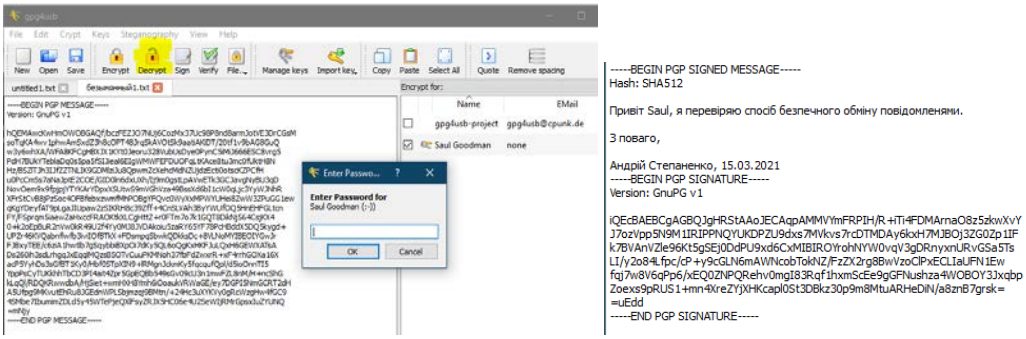
Зобр. 5. Підпис повідомлення

Зняти позначку зі свого ключа та поставити на ключі співрозмовника у правому віконці програми, обрати «Зашифрувати» (зобр. 6). Отримане зашифроване повідомлення відіслати своєму співрозмовнику.



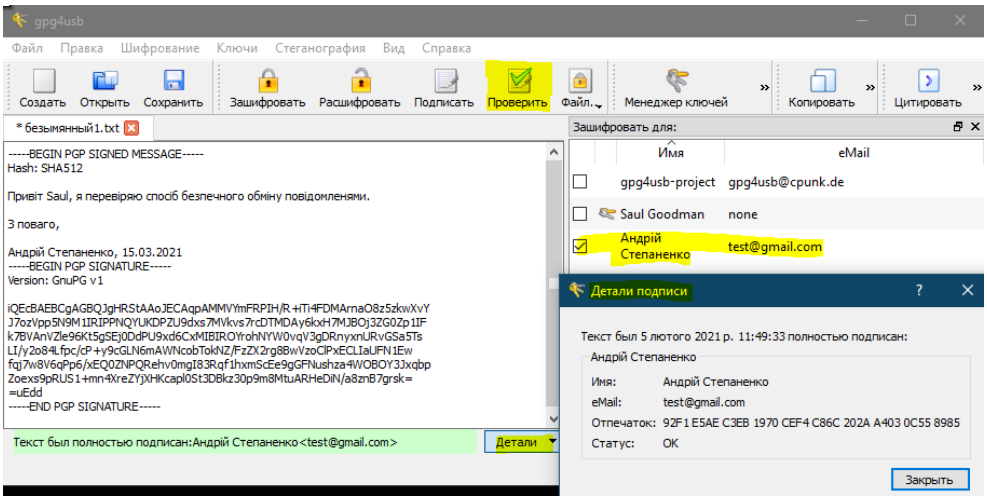
Зобр. 6. Шифрування повідомлення

Співрозмовник, отримавши зашифроване повідомлення або копіює його зміст у буфер пам'яті та вставляє у порожнє поле текстового файлу gpg4usb, або відкриває його як текстовий файл в gpg4usb. Після чого у правому полі програми позначає рядок із зазначенням своїх ключів, обирає «Розшифрувати», вводить пароль до свого приватного ключа та отримує розшифроване повідомлення (зобр. 7).

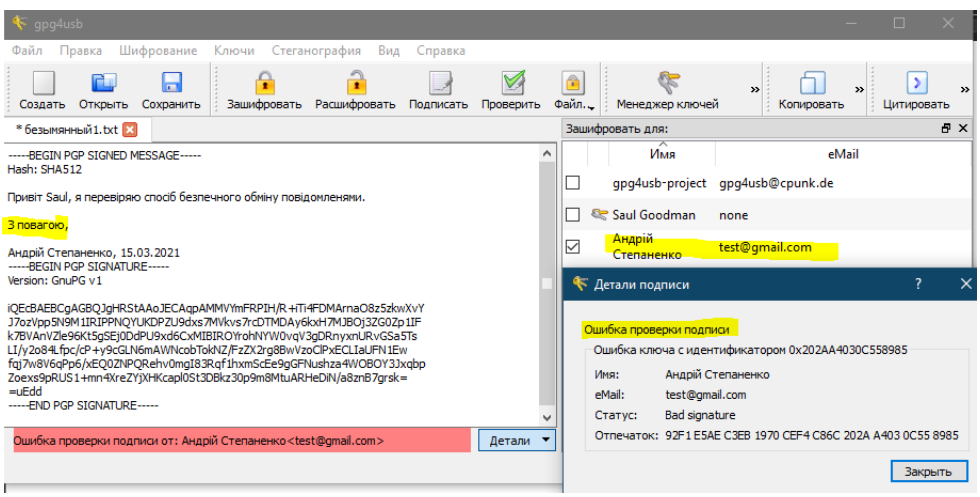


Зобр. 7. Розшифрування повідомлення

У правому полі програми співрозмовник позначає рядок із зазначенням ключа відправника, обирає «Перевірити» та «Деталі» підпису (зобр. 8). Виправити або додати у повідомленні одну літеру та повторити перевірку підпису у зміненому повідомлені (зобр. 9).



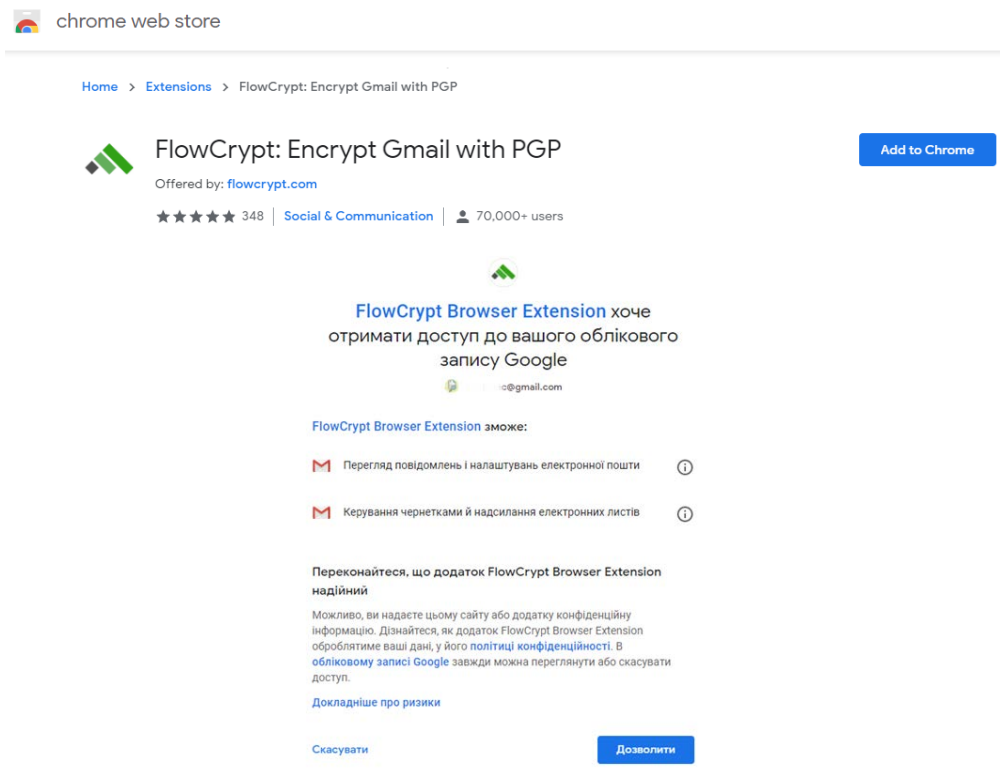
Зобр. 8. Успішна перевірка підпису відправника повідомлення



Зобр. 9. Невдала перевірка підпису відправника повідомлення

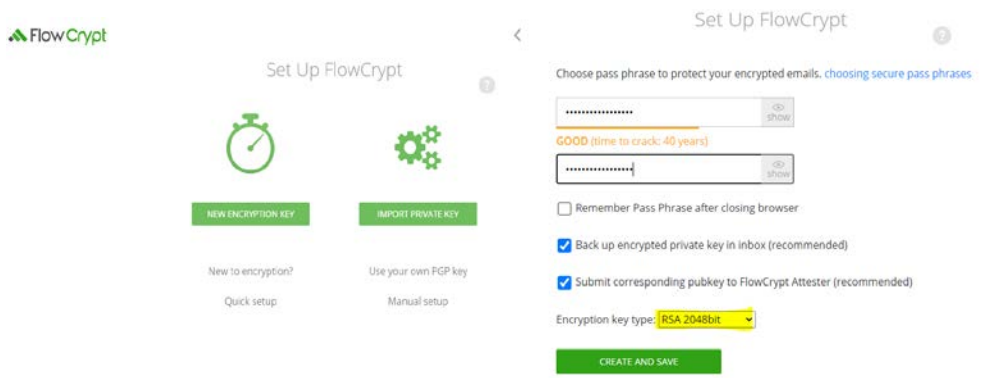
Установити і налаштувати в обліковому записі Google розширення електронного підпису та шифрування. В обліковому записі ProtonMail здійснити налаштування інтегрованого сервісу електронного підпису та шифрування листів, які спрямовуються на зовнішні поштові домени. Після налаштувань переслати підписані та зашифровані листи між поштовими доменами protonmail.com та gmail.com. Переконатися у забезпеченні конфіденційності та цілісності такого листування.

Додати в Google Chrome розширення FlowCrypt: Encrypt Gmail with PGP (https://chrome.google.com/webstore/detail/flowcrypt-encrypt-gmail-w/bnjglocicdkmhmoohhfkfkbbkejdhdgc?hl=ua), клацнути на розширення та надати дозвіл FlowCrypt отримувати доступ до облікового запису Google (зобр. 10).



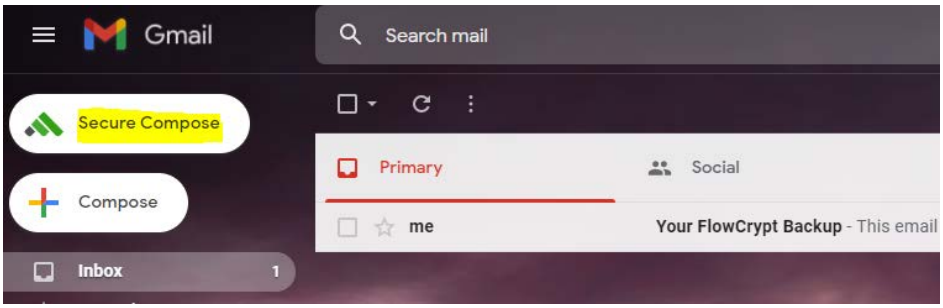
Зобр. 10. Встановлення та надання дозволу FlowCrypt

У FlowCrypt згенерувати і зберегти ключі: обрати New encryption key, Encryption key type – RSA 2048bit – Create and save (зобр. 11).



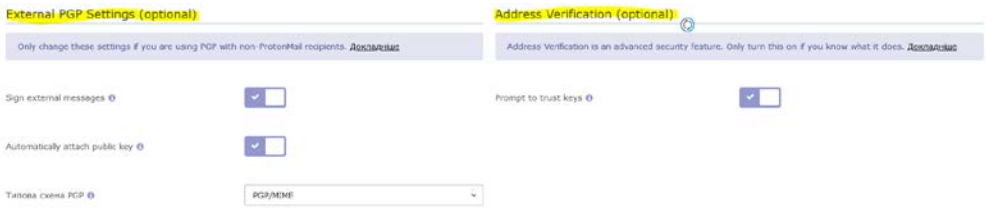
Зобр. 11. Створення і збереження ключів для облікового запису

Після налаштувань розширення в поштовому клієнті з'явиться кнопка Secure Compose (зобр. 12).



Зобр. 12. Кнопка FlowCrypt Secure Compose

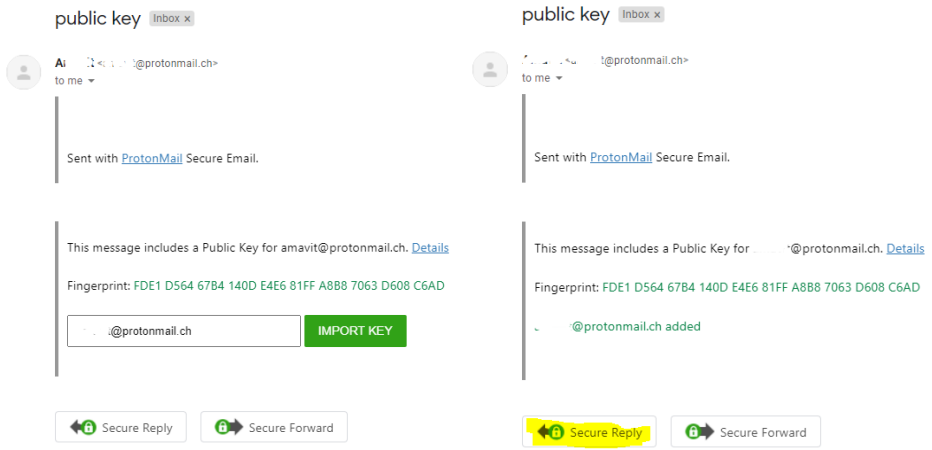
Авторизуватися у своєму обліковому записі ProtonMail. Перейти у «Налаштування» – «Безпека» і ввімкнути «External PGP Settings (optional)», Address Verification (optional) (зобр. 22).



Зобр. 13. Включення опцій підпису та шифрування

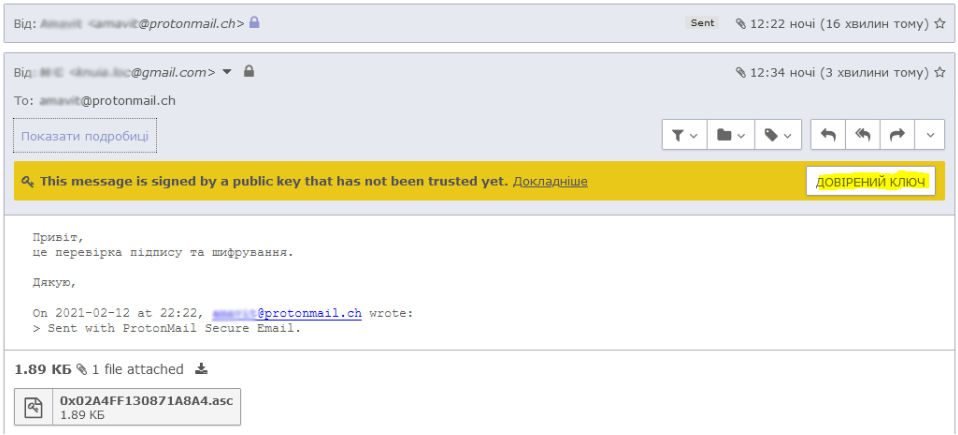
Відправити на адресу @gmail.com лист, до якого буде автоматично додано публічний ключ облікового запису @protonmail.com.

У @gmail.com після відкриття листа від @protonmail.com здійснити імпорт відкритого ключа @protonmail.com, та відповісти з підписом і шифруванням, натиснувши Secure Reply (зобр. 23).



Зобр. 14. Отримання публічного ключа та відповідь з підписом та шифруванням

У @protonmail.com буде автоматично розшифровано листа і перевірено підпис, але зазначено, що перевірка підпису була зроблена публічним ключем, який ще не є довіреним. Натиснути «ДОВІРЕНИЙ КЛЮЧ» (зобр. 15).



Зобр. 15. Розшифрований і перевірений на правдивість підпису лист з пропозицією позначити публічний ключ як довірений

Далі всі листи між обліковими записами @gmail.com і @protonmail.com будуть автоматично підписуватися і шифруватися перед відправкою, а під час отримання перевірятись та розшифровуватись.

МОДУЛЬ № 4:

ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

ПРАКТИЧНА ВПРАВА

«ВБУДОВАНА В ОС WINDOWS 10 СИСТЕМА ЗАХИСТУ ВІД ВІРУСІВ І ЗАГРОЗ»

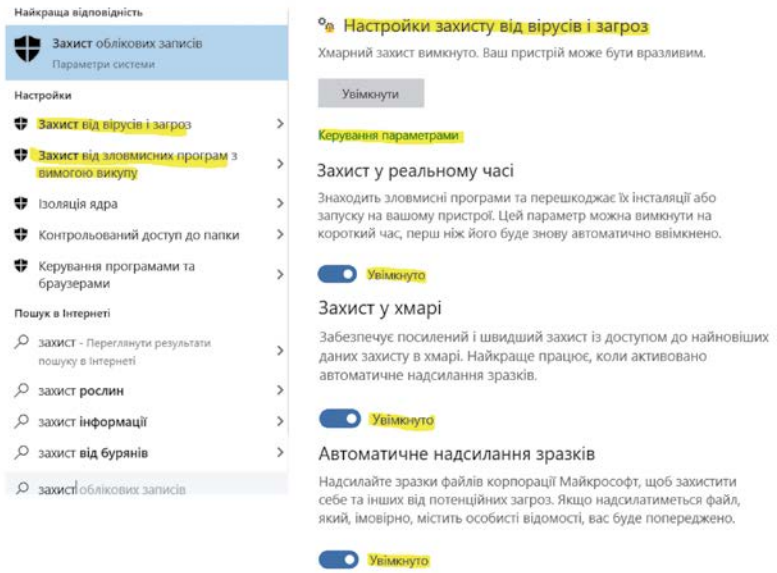
Навчальна мета заняття: налаштувати і перевірити ефективність вбудованої в ОС Windows 10 системи захисту від вірусів і загроз.

Час проведення: 1 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», тестові файли.

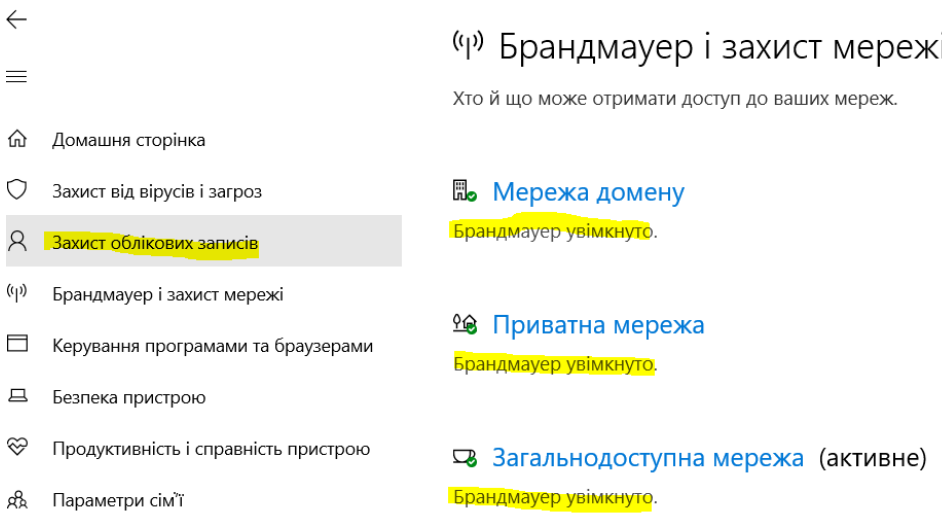
Порядок проведення заняття

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



Зобр. 1. Налаштування захисту від вірусів

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



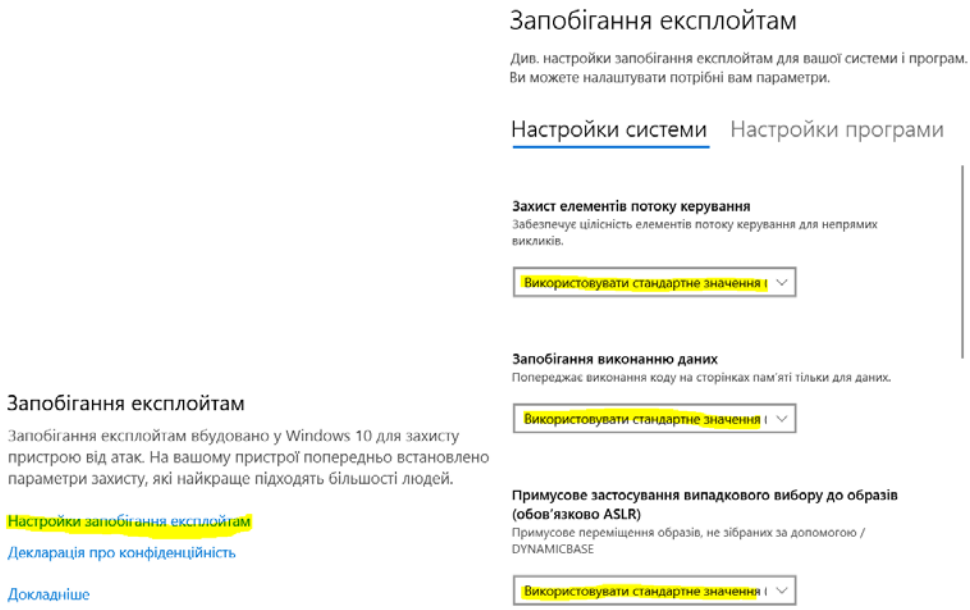
Зобр. 2. Налаштування захисту мережі

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

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

Зобр. 3. Налаштування SmartScreen

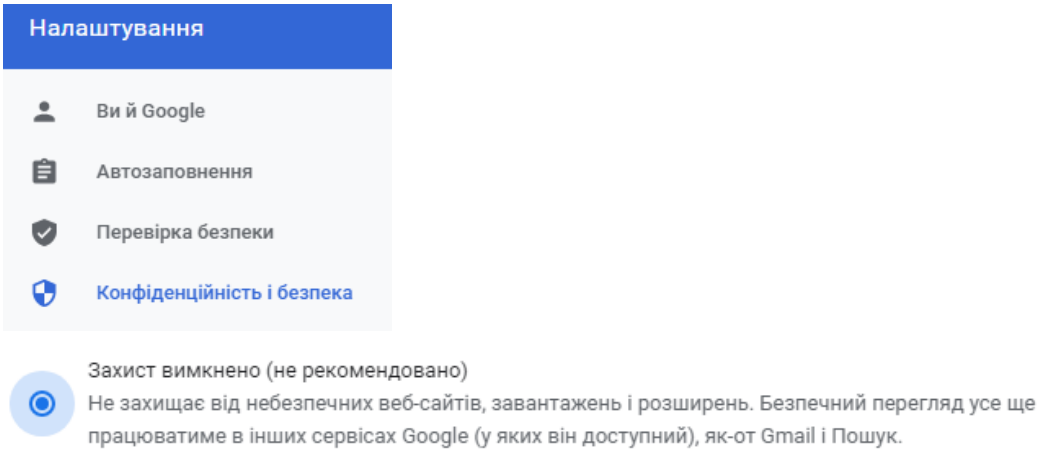
У розділі «Керування програмами та браузерами» перейти до «Налаштування запобігання експлойтам» та переконатися, що для усіх налаштувань встановлено «Використовувати стандартне значення (Увімкнуто)» (зобр. 4).



Зобр. 4. Налаштування «Настройки запобігання експлойтам»

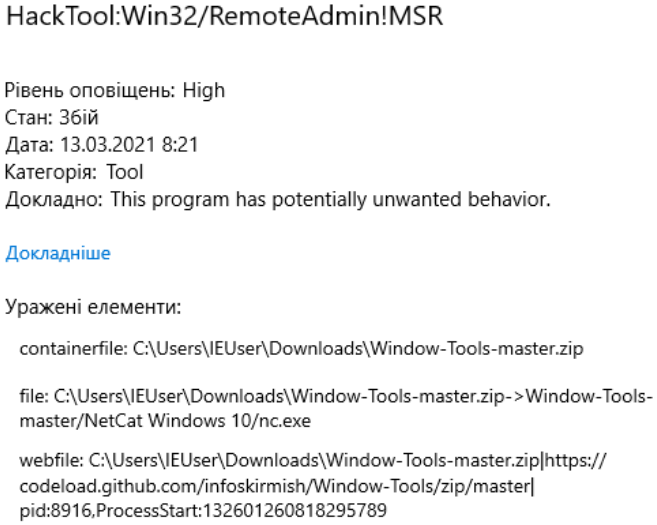
Після здійснення усіх дій вийти із меню налаштувань системи.

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



Зобр. 5. Вимкнення захисту у веббраузері Google Chrome

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



Зобр. 6. Виявлення та блокування шкідливого файлу

ПРАКТИЧНА ВПРАВА
«АНТИВІРУС ”ZILLYA!”»

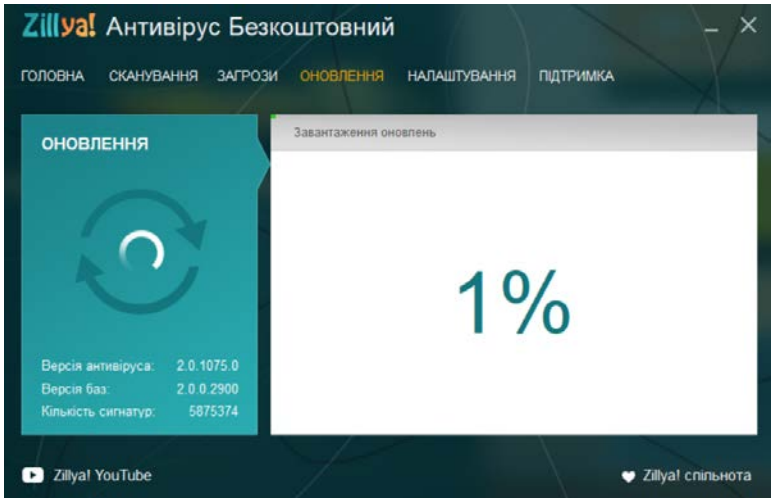
Навчальна мета заняття: встановити і перевірити ефективність сертифікованого для використання державними органами антивірусу «Zillya!».

Час проведення: 1 год. Місце проведення: комп’ютерний клас.

Устаткування: персональний комп’ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», тестові файли.

Порядок проведення заняття

Завантажити і виконати встановлення безкоштовної версії антивірусу «Zillya!» (https://zillya.ua/antivirus-free). Відкрити антивірус, в меню «Оновлення» запустити процес оновлення баз сигнатур вірусів (зобр. 1).



Зобр. 1. Оновлення баз сигнатур вірусів

Спробувати завантажити будь-який доступний у мережі файл зі шкідливим кодом, наприклад, за посиланням is.gd/7Xad5B. Встановити факт виявлення, чи не виявлення шкідливого файлу.

Самостійно виконати ті самі дії з антивірусом «ZoneAlarm» (https://www.zonealarm.com/software/free-firewall).

У налаштуваннях веббраузеру Google Chrome «Конфіденційність і безпека» – «Безпечний перегляд» обрати «Покращений захист».

МОДУЛЬ № 5:

БЕЗПЕКА КОРИСТУВАННЯ СОЦІАЛЬНИМИ МЕРЕЖАМИ

ПРАКТИЧНА ВПРАВА

«ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ОБЛІКОВОГО ЗАПИСУ FACEBOOK»

Навчальна мета заняття: налаштувати для облікового запису Facebook двофакторну автентифікацію через Google Authenticator.

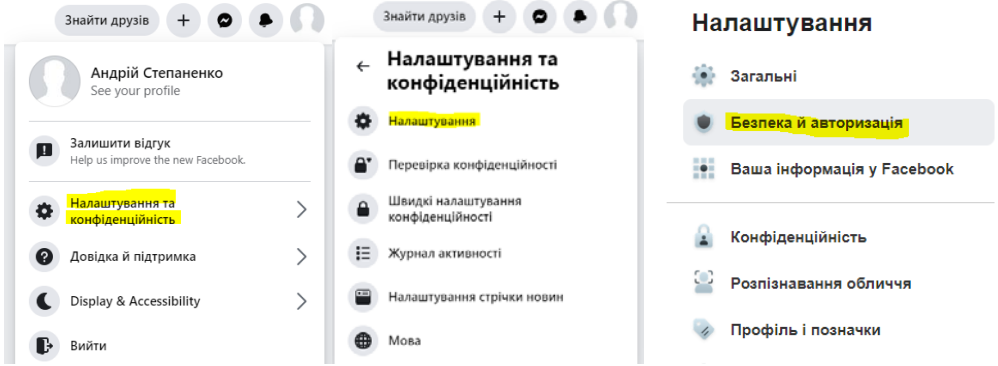
Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», особисті смартфони або телефони у слухачів, дата-кабелі підключення смартфона до комп'ютера, підготовлені файли фотозображень з метаданими.

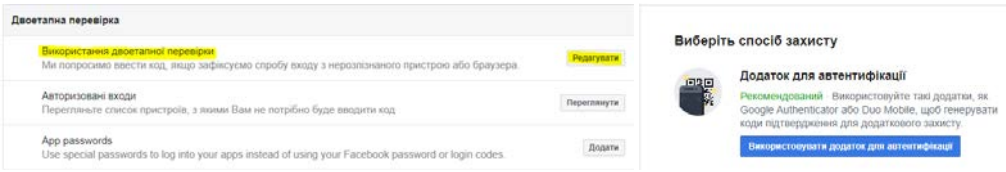
Порядок проведення заняття

Створити, якщо немає, обліковий запис у соціальній мережі «Facebook». Встановити для Facebook-облікового запису двофакторну автентифікацію через Google Authenticator.

В обліковому записі перейти в «Налаштування та конфіденційність» – «Налаштування» – «Безпека й авторизація» (зобр. 1) – «Двоетапна перевірка» – «Використання двоетапної перевірки» – «Редагувати» – «Використовувати додаток для автентифікації» (зобр. 2).

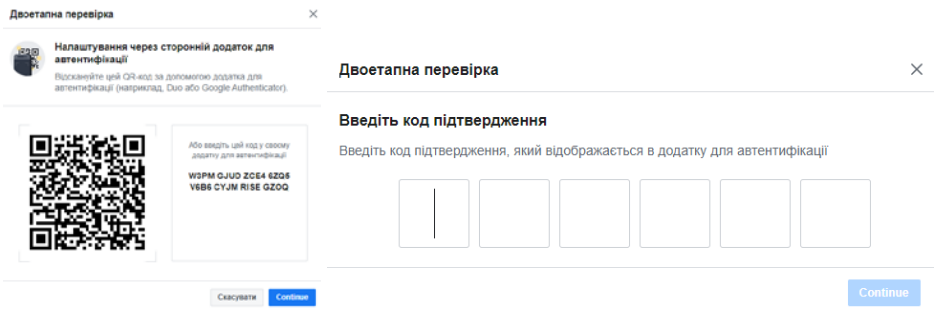


Зобр. 1. Шлях до налаштувань «Безпека й авторизація»



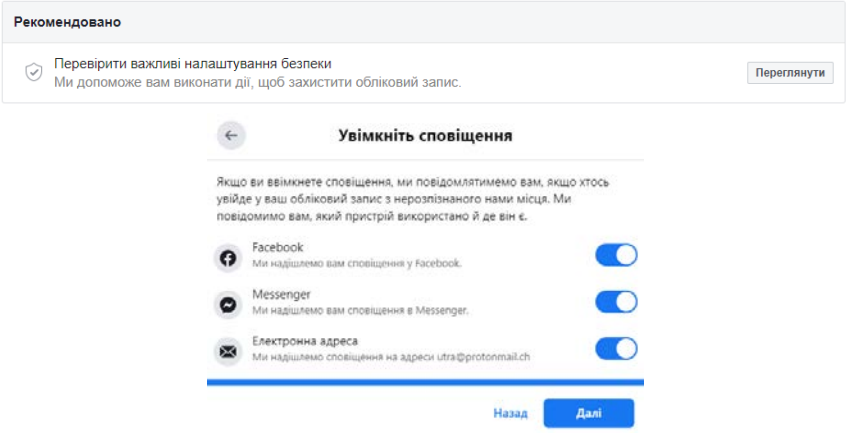
Зобр. 2. Шлях до налаштування додатка автентифікації

Переконатися, що у власному смартфоні встановлений Google Authenticator (встановлюється з Google Play або App Store), увійти до «Використовувати додаток для автентифікації», зчитати додатком смартфону Google Authenticator QR-код та ввести код підтвердження (зобр. 3).



Зобр. 3. Налаштування двоетапної перевірки

Після налаштування двоетапної перевірки повернутися у розділ «Безпека й авторизація» та переглянути важливі налаштування безпеки облікового запису, де увімкнути сповіщення про вхід у ваш обліковий запис з нерозпізнаного місця (зобр. 4).



Зобр. 4. Увімкнення сповіщення про вхід в обліковий запис з нерозпізнаного місця

Після закінчення налаштувань вийти із облікового запису та увійти з використанням двоетапної автентифікації.

ПРАКТИЧНА ВПРАВА

«ВИДАЛЕННЯ МЕТАДАНИХ ФОТОЗОБРАЖЕНЬ»

Навчальна мета заняття: навчитися перевіряти наявність метаданих у файлах фотозображень та видаляти їх.

Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», особисті смартфони або телефони у слухачів, дата-кабелі підключення смартфона до комп'ютера, підготовлені файли фотозображень з метаданими.

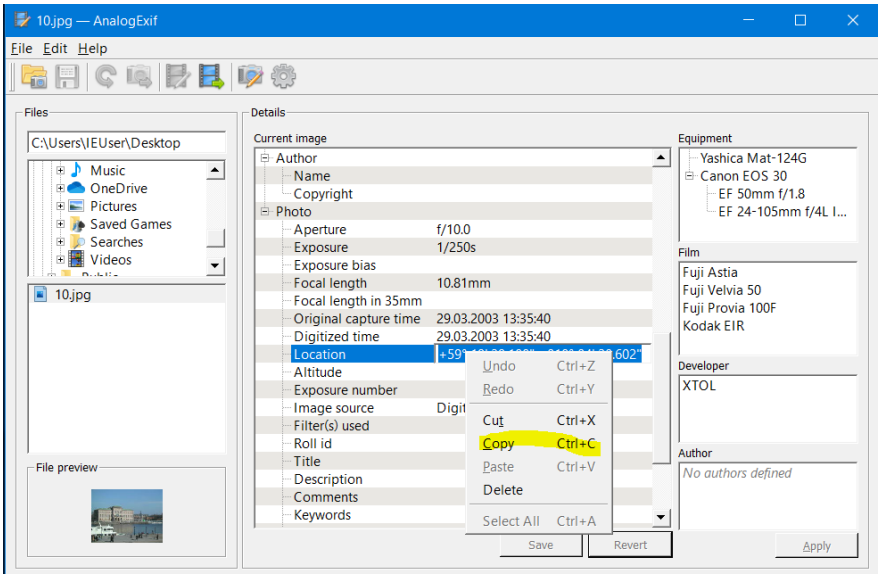
Порядок проведення заняття

В особистому смартфоні включити GPS, підійти до вікна у приміщенні й дочекатися встановлення координат свого місцезнаходження, перевіривши цей факт запуском додатку «Карти», де відобразиться точне місцезнаходження смартфона.

Зробити декілька фотознімків фотокамерою смартфона, підключити смартфон до комп'ютера та завантажити фотозображення на комп'ютер. Або скопіювати на комп'ютер підготовлені файли фотозображень з метаданими.

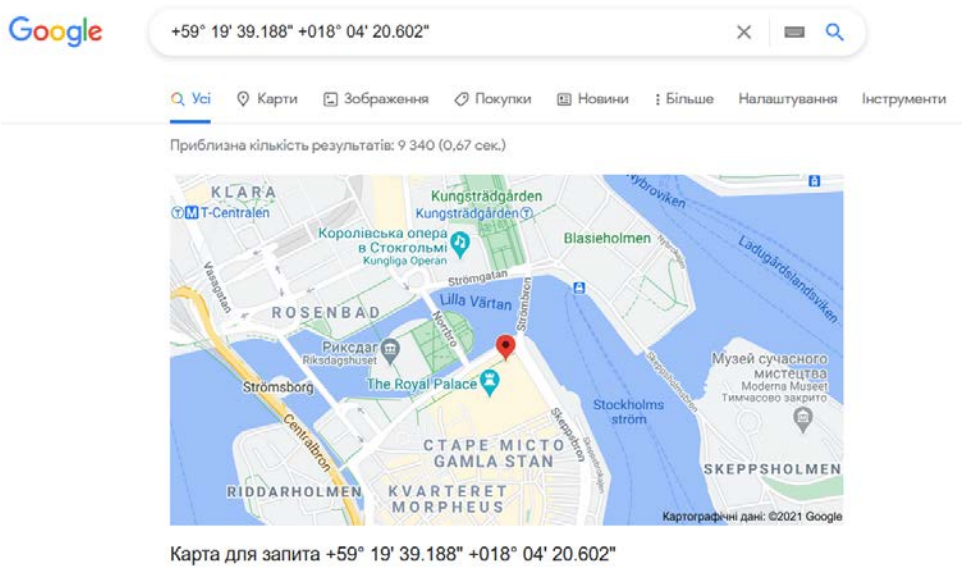
Перевірити наявність метаданих у файлах фотозображень та видалити їх.

Завантажити, встановити і запустити утиліту перегляду та редагування метаданих «AnalogExif» (https://sourceforge.net/projects/analogexif). Відкрити у AnalogExif фотозображення, переглянути метадані, двічі клацнути на поле Location та скопіювати у буфер координати (зобр. 1).



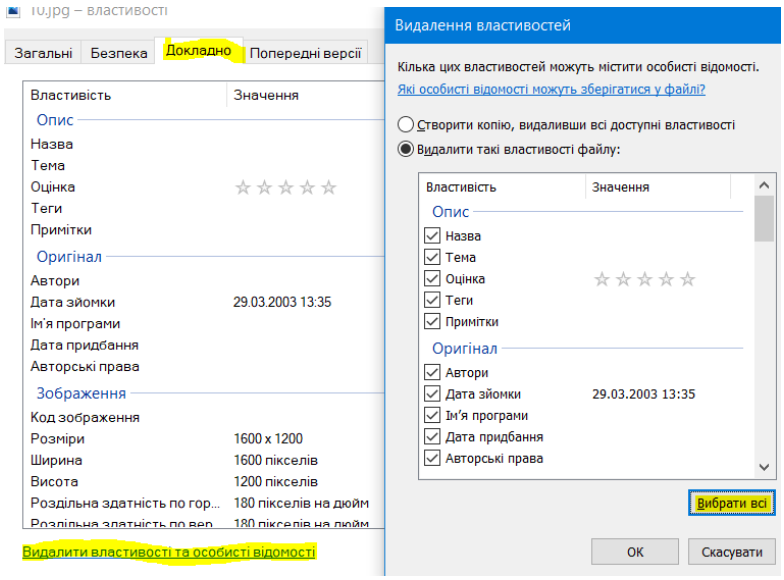
Зобр. 1. Перегляд метаданих фотозображення

Відкрити веббраузер «Google Chrome», вставити координати в адресний рядок і здійснити пошук місця фотозйомки (зобр. 2).



Зобр. 2. Пошук місця фотозйомки за координатами з метаданих фотозображення

У Провіднику файлів через контекстне меню (клацнути правою кнопкою миші) подивитися «Властивості файлу фотозображення», перейти у вкладку «Докладно» та клацнути на «Видалити властивості та особисті відомості» – «Вибрати всі» – «ОК» (зобр. 7).



Зобр. 3. Видалення метаданих фотозображень

Знову відкрити у AnalogExif фотозображення та переконатися, що метадані відсутні та можна їх безпечно завантажувати у соціальні мережі.

ПРАКТИЧНА ВПРАВА
«ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ ОБЛІКОВОГО ЗАПИСУ INSTAGRAM ТА TWITTER»

Навчальна мета заняття: налаштувати для облікового запису Instagram та Twitter двофакторну автентифікацію.

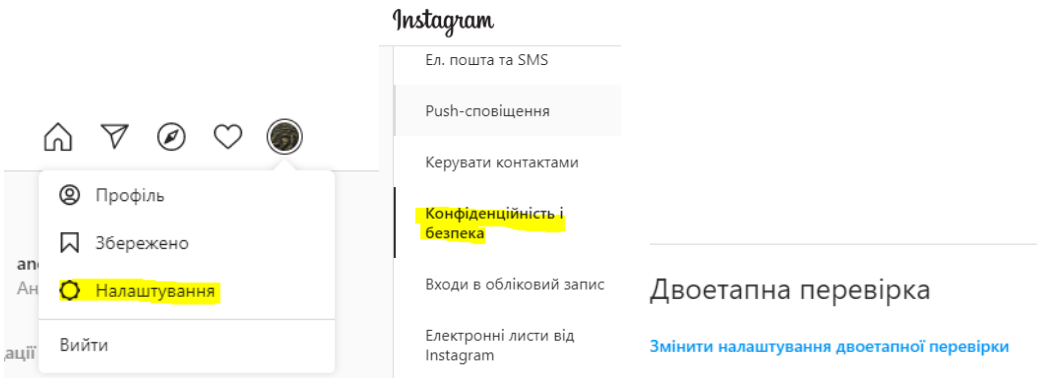
Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», особисті смартфони або телефони у слухачів, дата-кабелі підключення смартфона до комп'ютера, підготовлені файли фотозображень з метаданими.

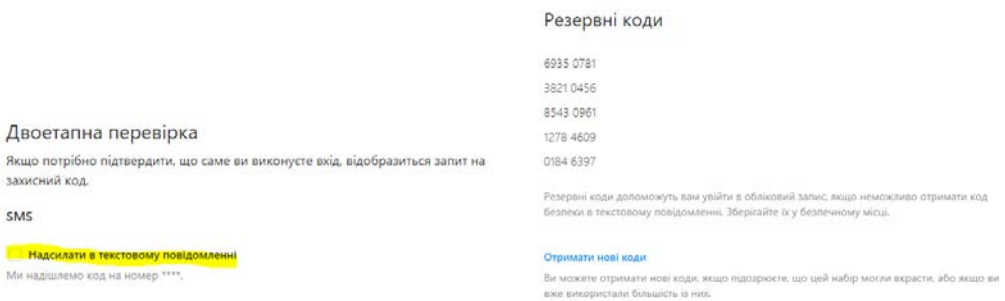
Порядок проведення заняття

Із використанням раніше створеного Facebook-облікового запису створити Instagram-обліковий запис та встановити двофакторну автентифікацію облікового запису.

Перейти «Налаштування» – «Конфіденційність і безпека» – «Змінити налаштування двоетапної перевірки» (зобр. 1). Увімкнути двоетапну перевірку «Надсилати в текстовому повідомленні» та зберегти у парольному менеджері резервні коди доступу, які можна використати за неможливості отримання текстових повідомлень.



Зобр. 1. Вхід до налаштувань двоетапної перевірки



Зобр. 2. Налаштування двоетапної перевірки

Після закінчення налаштувань вийти із облікового запису та увійти з використанням двоетапної автентифікації.

Створити обліковий запис у Twitter та, з огляду на попередньо виконані задачі, увімкнути і налаштувати двоетапну перевірку автентифікації. Після закінчення налаштувань вийти із облікового запису та увійти з використанням двоетапної автентифікації.

МОДУЛЬ № 6:

БЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ

ПРАКТИЧНА ВПРАВА

«ВИВЕДЕННЯ ІНФОРМАЦІЇ З ЕКРАНА ТЕЛЕФОНА НА ПЕРСОНАЛЬНИЙ КОМП'ЮТЕР»

Навчальна мета заняття: налаштувати виведення інформації з екрана смартфона на комп'ютер для демонстрації маніпуляцій у телефонному пристрої.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено.**

Вхідні дані

Потрібні програми:

Android → Windows, MacOS: vysor (vysor.io)

Android → MacOS, Windows, Linux: Airdroid (airdroid.com)

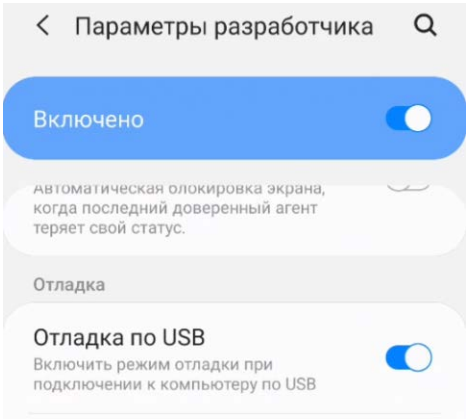
iOS → Windows: LonelyScreen (lonelyscreen.com)

iOS → MacOS: QuickTime player

Щоб продемонструвати налаштування безпеки на мобільному пристрої, може виникнути потреба виведення проекції екрану смартфона на персональний комп'ютер. Вирішення цього завдання залежить від операційної системи, встановленої на мобільному пристрої та на ПК. В окремих випадках можливості операційної системи дозволяють здійснити безпосереднє виведення інформації з екрану мобільного пристрою без необхідності встановлення додаткового програмного забезпечення. Однак такий спосіб не є універсальним та залежить від конкретного системного програмного забезпечення. У зв'язку з наведеним, пропонуємо скористатися більш перевіреним способом, у рамках якого потрібно встановити спеціальні застосунки.

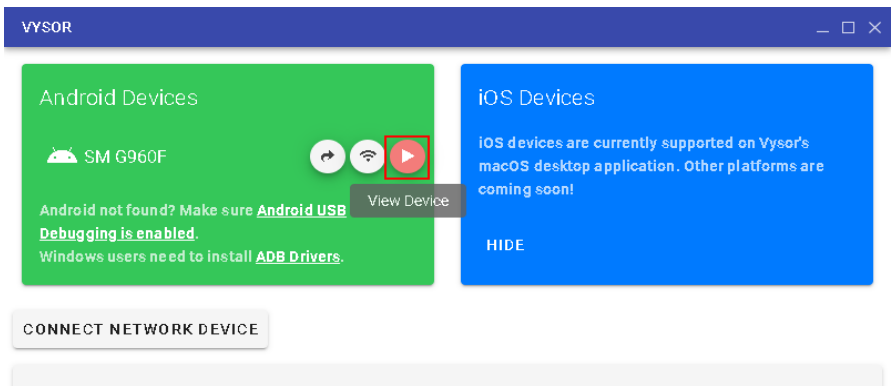
Розглянемо, яким чином виконати відповідне підключення для найбільш поширених операційних систем.

Для того, щоб здійснити демонстрацію за схемою Android → Windows, MacOS можна скористатися програмою Vysor, яку слід завантажити за посиланням https://www.vysor.io/. Після інсталяції програми потрібно приєднати Android-пристрій до персонального комп'ютера за допомогою шнура USB та у налаштуваннях Android відкрити «Налаштування» → «Відомості про телефон» → «Відомості про програмне забезпечення» та торкнутися елемента «Номер збірки» сім разів. Після цього потрібно повернутися до меню налаштувань та в меню «Параметри розробника» увімкнути параметр «Налаштування по USB» (зобр. 1).



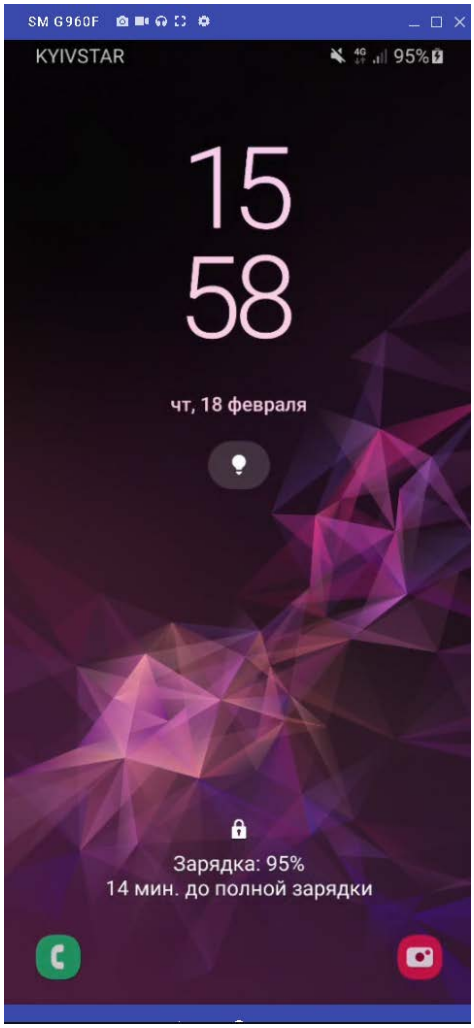
Зобр. 1. Налаштування параметрів розробника

Після виконання описаних маніпуляцій у програмі Vysor потрібно обрати пристрій для виведення відповідної проекції на екран комп'ютера (зобр. 2).



Зобр. 2. Перегляд відповідного пристрою

У результаті на моніторі комп'ютера має відобразитись зміст екрану мобільного пристрою (зобр. 3). Після проведення описаних налаштувань можна за допомогою проектора демонструвати аудиторії відповідні маніпуляції на мобільному пристрої.



Зобр. 3. Проекція екрану мобільного пристрою виведеного на ПК

Якщо потрібно вивести зображення з мобільного пристрою під управлінням iOS в системі Windows, то для цього можна скористатися застосунком LonelyScreen (http://www.lonelyscreen.com/download.html). Після запуску цієї програми слід у пристрої під управлінням iOS провести вверх екрана та відкрити «Центр управління». Далі слід торкнутися елемента «AirPlay Mirroring» та обрати «LonelyScreen».

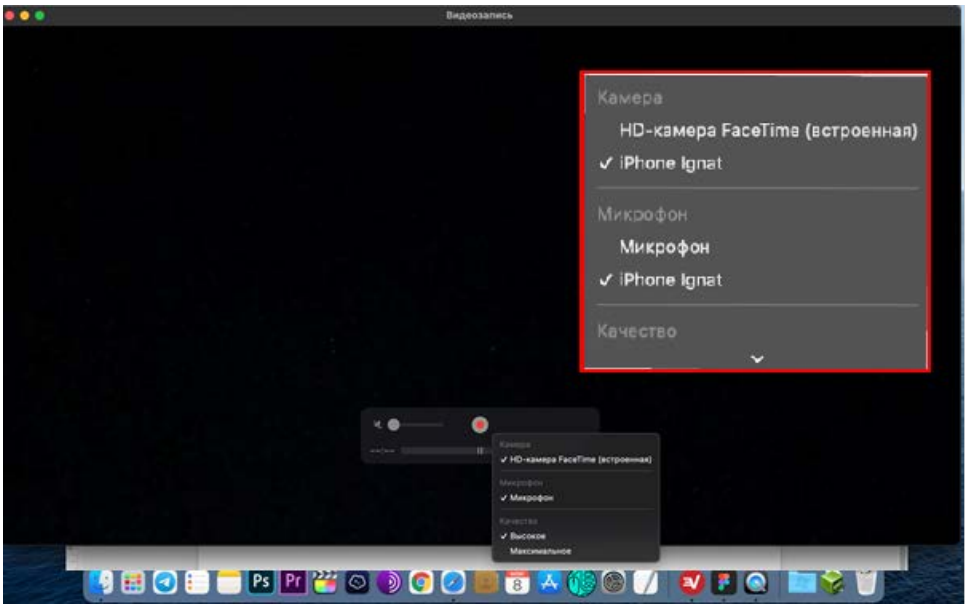
У разі необхідності виведення зображення з пристрою під управлінням iOS на пристрій під управлінням MacOS можна скористатися таким алгоритмом.

Спершу слід приєднати смартфон до персонального комп'ютера за допомогою кабелю «Lighting». Якщо телефон приєднується вперше, потрібно розблокувати пристрій та натиснути «Довіряти».

Після цього на персональному комп'ютері потрібно відкрити програму «QuickTime Player», та обрати в меню «Файл» → «Новий відеозапис» (зобр. 4).

Зобр. 4. Налаштування QuickTime Player

У вікні, що з'явилося, потрібно натиснути стрілку поряд з кнопкою запису та обрати в як камеру назву телефона.



Зобр. 5. Налаштування QuickTime Player

Якщо всі налаштування зроблено правильно, то на екрані персонального комп'ютера має з'явитися зображення з екрана смартфона.

Зверніть увагу! Якщо кабель «Lighting» неякісний, то зображення може не передаватись.

Існують випадки, коли демонстрація роботи певних програм безпосередньо зі смартфона є недоцільною. В такому випадку можна встановити на комп'ютері віртуальну систему Android. Для виконання цього завдання можна використати, наприклад, застосунок Bluestacks (https://www.bluestacks.com/download.html).

1. Приєднати смартфон до персонального комп'ютера за допомогою шнура USB.

2. Налаштувати виведення зображення екрана смартфона на монітор персонального комп'ютера.

3. Самостійно встановити застосунок Bluestacks та проінсталювати у віртуальній системі Android програму Telegram.

ПРАКТИЧНА ВПРАВА
«НАЛАШТУВАННЯ ЗАХИСНИХ МЕХАНІЗМІВ У МОБІЛЬНОМУ ПРИСТРОЇ»

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

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

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

Завдання, які потрібно виконати, **підкреслено**.

Вхідні дані

Потрібні програми:

Telegram

Viber

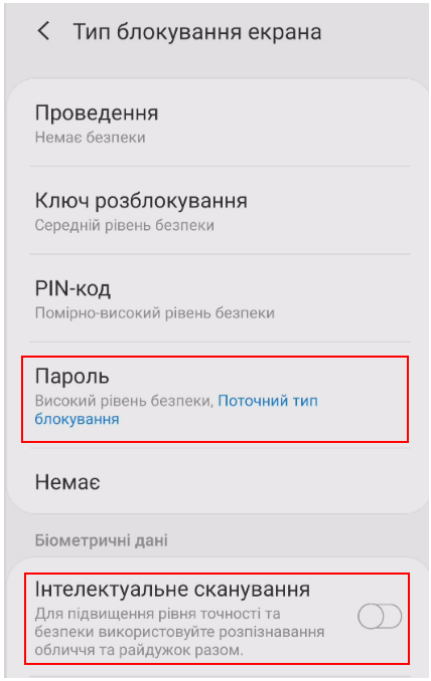
WhatsApp

Налаштування безпеки мобільного пристрою слід організовувати за двома головними напрямами:

1) налаштування операційної системи мобільного пристрою;

2) налаштування прикладних програм.

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

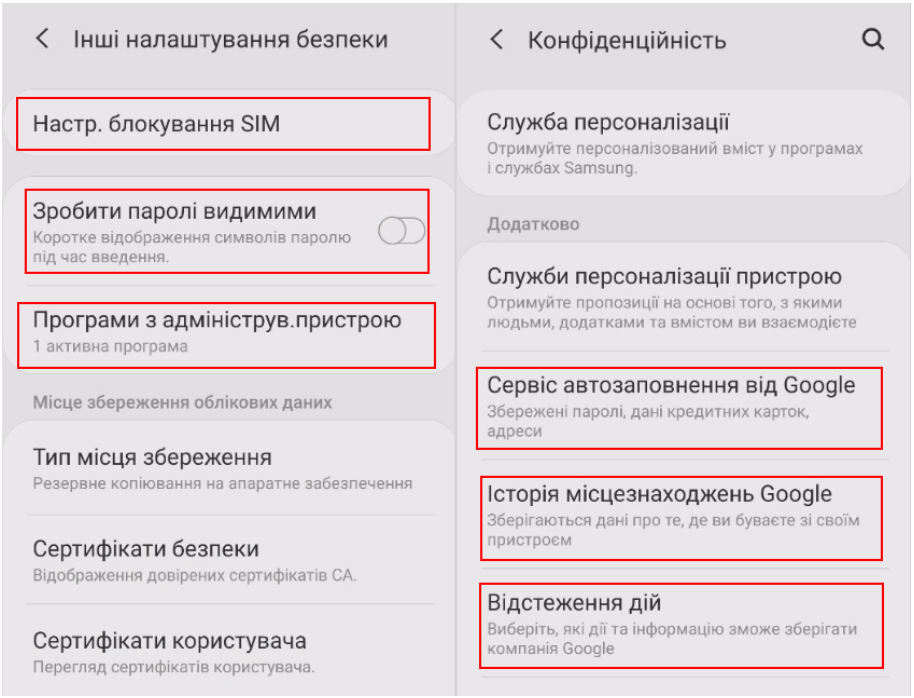


Зобр. 1. Налаштування паролю для розблокування пристрою

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

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

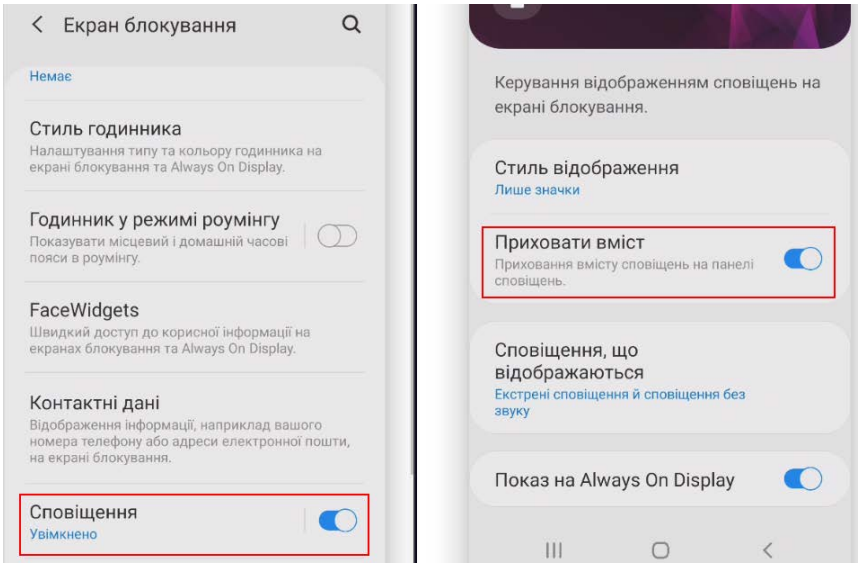
Крім наведеного, слід переглянути інші налаштування безпеки та встановити їх таким чином, щоб вони відповідали потрібному рівню захисту (зобр. 2).



Зобр. 2. Налаштування параметрів безпеки та конфіденційності

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

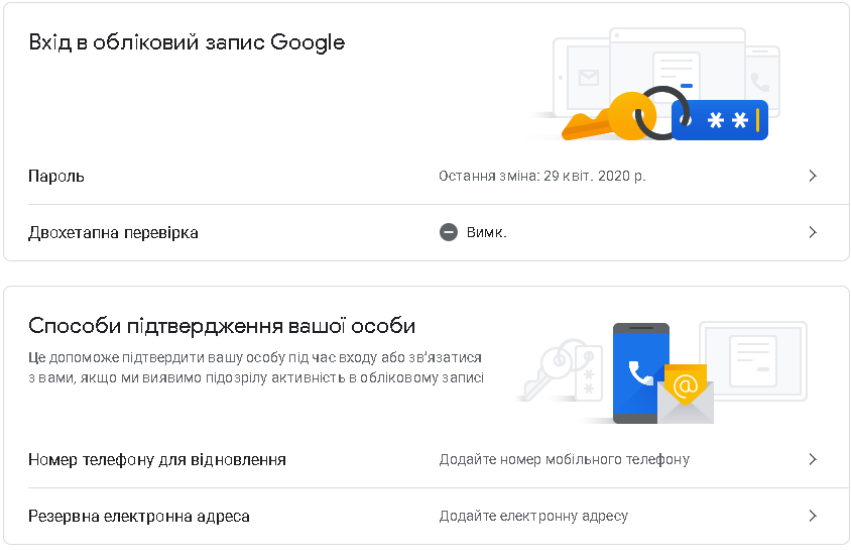
Для виконання розглянутого завдання на iPhone: «Налаштування» → «Пароль» → «Доступ з блокуванням екрану»; «Налаштування» → «Сповіщення» → «Показ мініатюр» → «Без блокування».



Зобр. 3. Вимкнення повідомлень

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

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

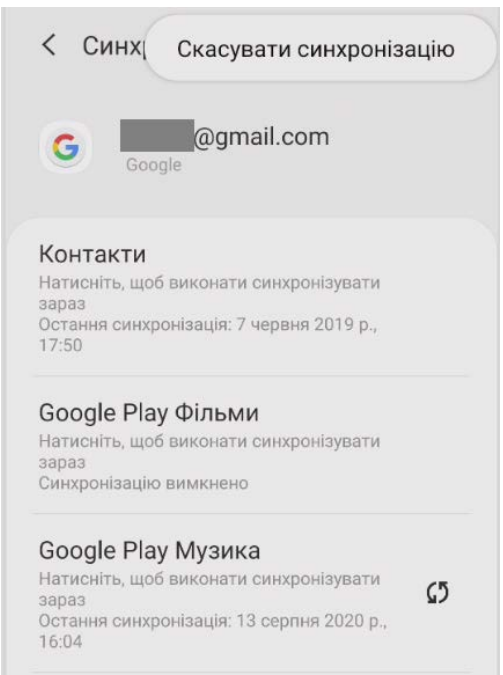


Зобр. 3. Налаштування безпеки облікового запису

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

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

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

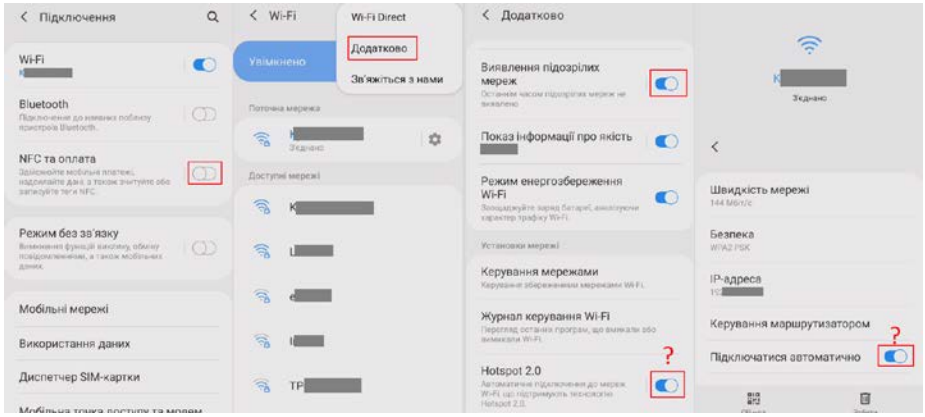


Зобр. 4. Налаштування синхронізації

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

Крім наведеного, слід також вимкнути автоматичне підключення до Wi-Fi мереж (зобр. 5). Якщо у Вас налаштоване автопідключення до відомих точок доступу Wi-Fi, то Ви так само автоматично можете бути під'єднаним до підробленої точки доступу.

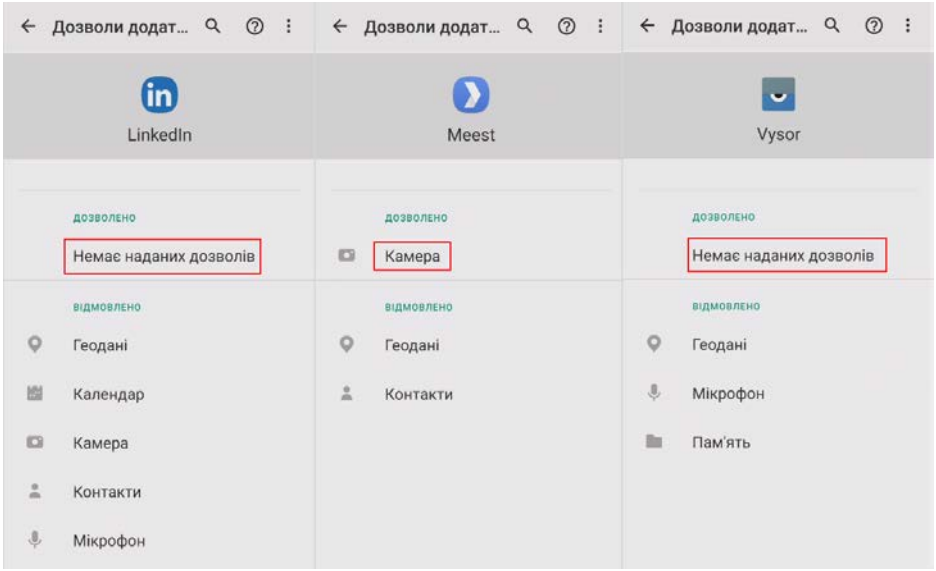
У подальшому весь трафік Інтернет може бути пропущений через обладнання зловмисника. Це дозволяє порушнику примусово перенаправляти запити з Вашого пристрою на свої ресурси. При цьому Ви можете навіть нічого не помітити.



Зобр. 5. Налаштування Wi-Fi

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

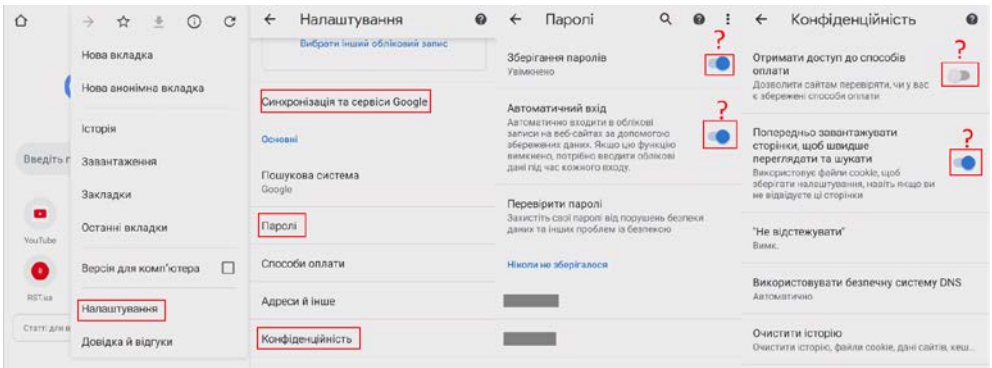
Що стосується налаштувань окремих застосунків, то тут слід передусім звернути увагу на обмеження їх доступу до чутливих даних: файлів на телефоні, контактів, геолокації тощо (зобр. 6).



Зобр. 6. Налаштування прав доступу для застосунків

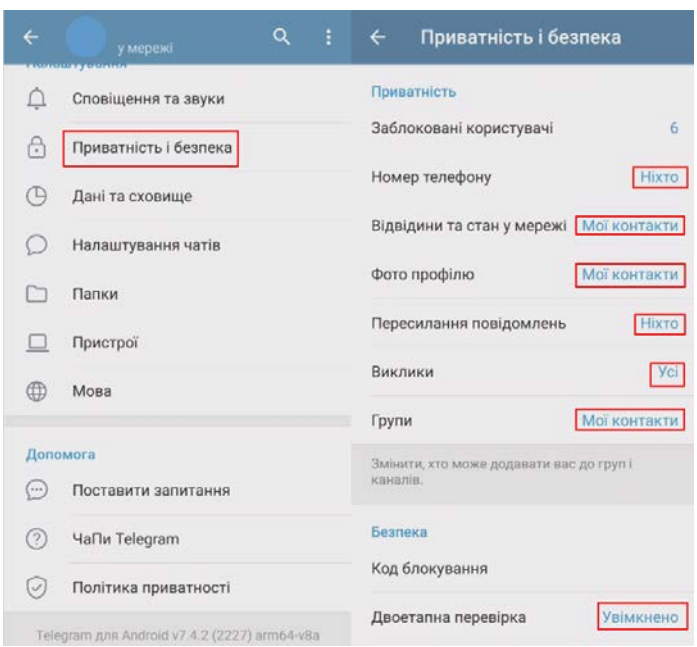
Для виконання розглянутого завдання на iPhone: «Налаштування» → «Конфіденційність» → «Геолокація», «Відслідковування» → поставити «Вимкнути» у налаштуваннях відповідних застосунків.

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

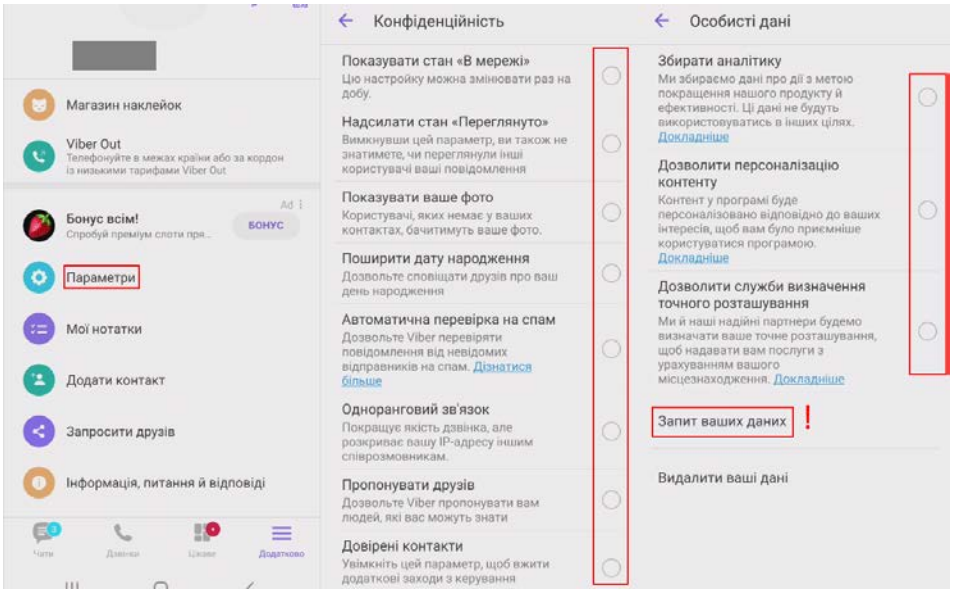


Зобр. 7. Налаштування безпеки браузера

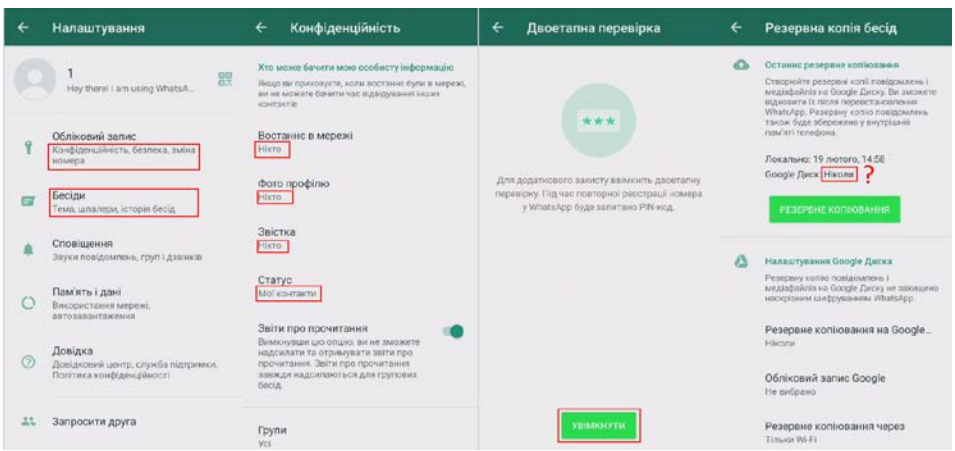
Важливою частиною захисту мобільного пристрою є правильне налаштування програм для спілкування (месенджерів). Найбільш поширеними такими рішеннями на теперішній час є Telegram (зобр. 8), Viber (зобр. 9), WhatsApp (зобр. 10).



Зобр. 8. Налаштування безпеки Telegram



Зобр. 9. Налаштування безпеки Viber



Зобр. 10. Налаштування безпеки WhatsApp

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

Завдання

1. Налаштуйте параметри безпеки для:

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

МОДУЛЬ № 7:

ФІЗИЧНА БЕЗПЕКА

ПРАКТИЧНА ВПРАВА

«СТВОРЕННЯ ЗАХИЩЕНОГО ФЛЕШ-НАКОПИЧУВАЧА»

Навчальна мета заняття: створити захищений флеш-накопичувач за допомогою вбудованого в ОС Windows 7/10 Pro/10 Enterprise сервісу BitLocker To Go та програми VeraCrypt.

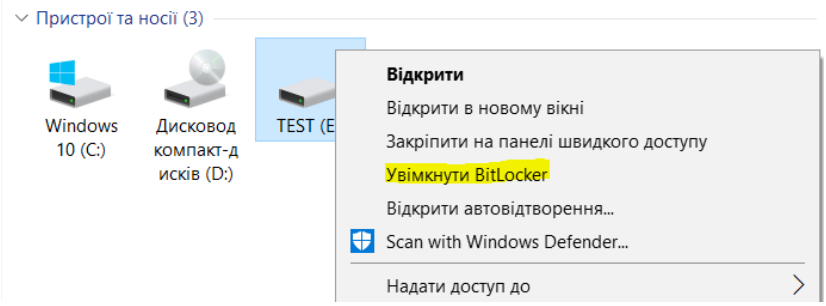
Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

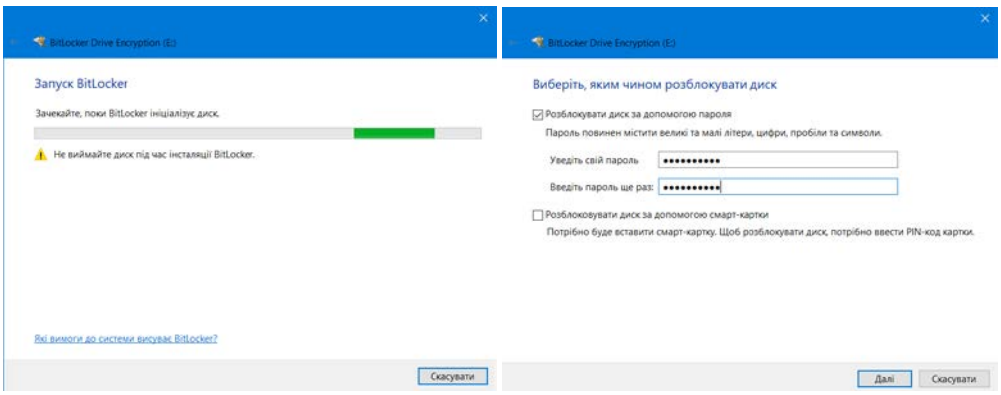
Створити захищений флеш-накопичувач за допомогою вбудованого в ОС Windows 7/10 Pro/10 Enterprise сервісу BitLocker To Go, який повністю шифрує вміст флеш-накопичувача на рівні файлової системи. У випадку фізичної втрати флеш-накопичувача дані залишаться недоступними для читання.

Вставити флеш-накопичувач у USB порт та відкрити «Провідник файлів». Увімкнути BitLocker для диску флеш-накопичувача: клацнути правою кнопкою миші диск у вікні «Провідника файлів», а потім вибрати команду «Увімкнути BitLocker». Якщо немає цього параметра у контекстному меню, то, ймовірно, у вас не Windows Pro або Enterprise, і знадобиться шукати інше рішення для шифрування (зобр. 1).



Зобр. 1. Увімкнення BitLocker

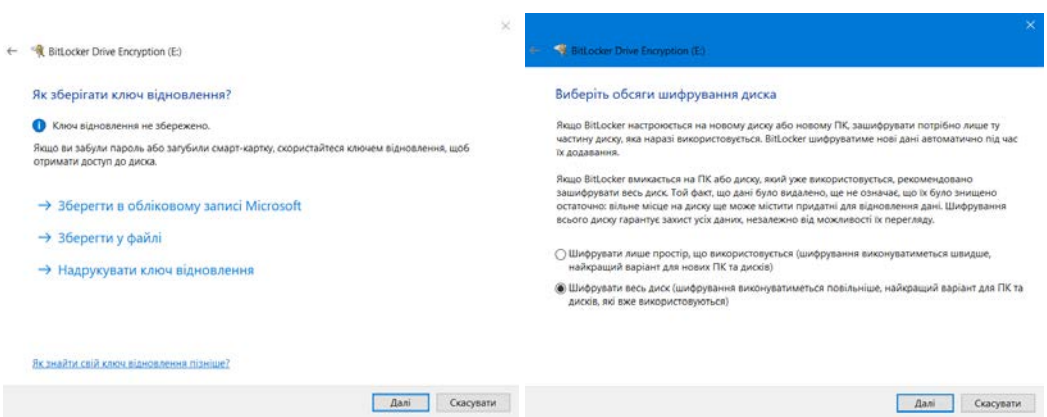
Зачекати, поки BitLocker здійснить ініціалізацію диску, далі обрати спосіб розблокування диску – за допомогою паролю, обрати надій пароль (зобр. 2).



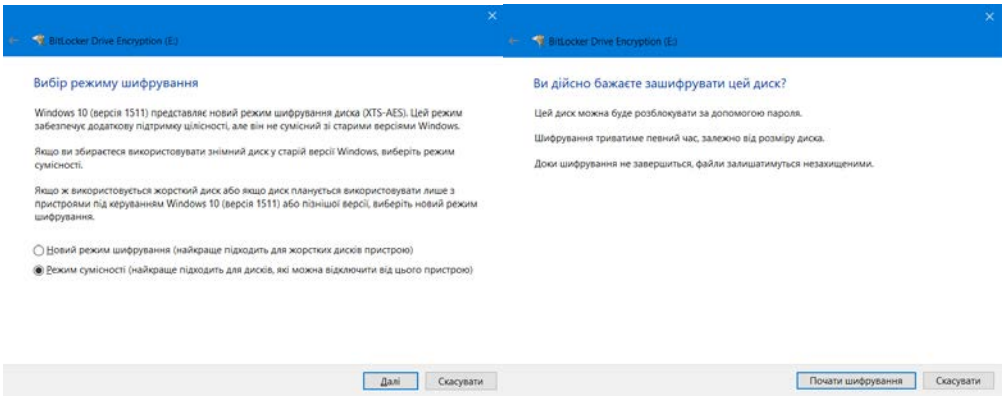
Зобр. 2. Ініціалізація BitLocker та вибір способу розблокування диску

Далі BitLocker надає можливість створити ключ відновлення, який можна використовувати для доступу до зашифрованих файлів, якщо ви, наприклад, забудете пароль (зобр. 3). Ключ відновлення можна зберегти у своєму обліковому записі Microsoft, на диску USB, файлі або навіть роздрукувати. Ці параметри є однаковими, якщо ви шифруєте системний або несистемний диск. Зберегти ключ відновлення у файл – зміст цього файлу можна скопіювати у парольний менеджер та видалити файл.

Далі обрати шифрування всього диску (зобр. 3), режим сумісності для різних версій Windows та запустити шифрування диску (зобр. 4).

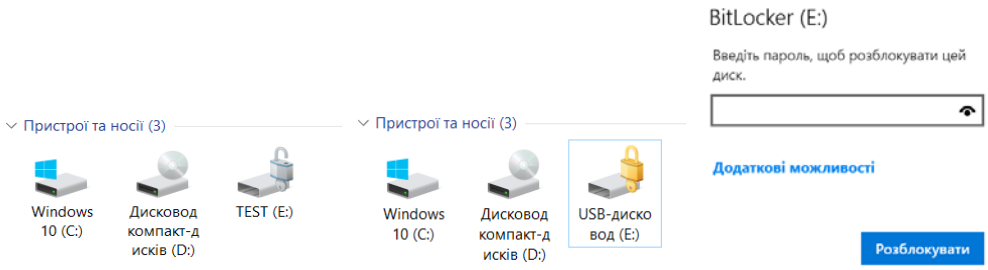


Зобр. 3. Збереження ключа відновлення та вибір обсягу шифрування диску



Зобр. 4. Вибір режиму шифрування та початок шифрування

Після завершення шифрування у «Провіднику файлів» з'явися відповідна піктограма розшифрованого диску, яка зміниться, якщо витягти диск і знову вставити, а також з'явиться запрошення ввести пароль для розшифрування диску (зобр. 5).



Зобр. 5. Піктограми розшифрованого та зашифрованого диску, запрошення ввести пароль

Записати на розшифрований диск довільні файли, витягнути флеш-накопичувач та повторити процедуру розблокування, щоб переконатися у цілісності файлів після розшифрування.

Створити захищений флеш-накопичувач за допомогою безкоштовної утиліти з відкритим кодом «VeraCrypt», яка побудована на базі останньої версії TrueCrypt.

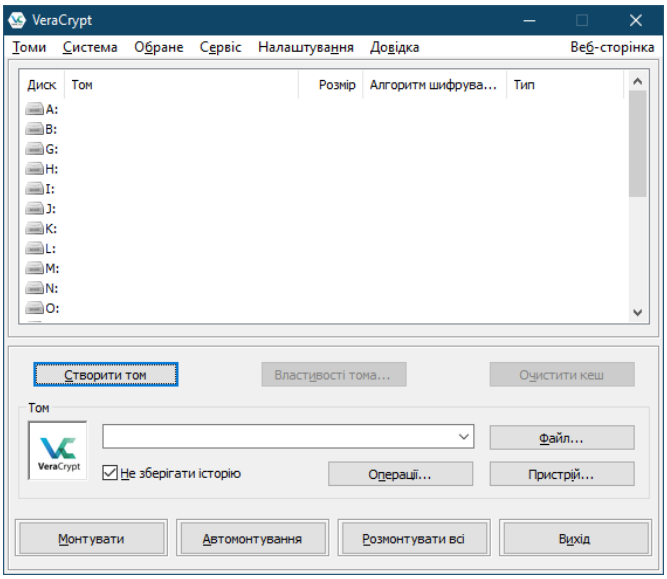
VeraCrypt використовує так званий контейнер. Стосовно VeraCrypt, контейнер – це оболонка, в якій у зашифрованому вигляді зберігаються всі файли. Фізично контейнер – це один файл. Отримати доступ до файлів, які лежать всередині контейнера-оболонки можна тільки одним способом – ввівши правильний пароль.

Процедура введення пароля і підключення контейнера називається «монтуванням».

Файли у VeraCrypt шифруються не по одному, а контейнерами. Коли програма підключає контейнер (монтує його), то контейнер виглядає як флешка – з'являється новий диск, з яким можна робити будь-які операції – копіювати туди файли, відкривати файли, видаляти файли, редагувати файли. Роблячи це, не потрібно думати про шифрування – все, що всередині контейнера, вже надійно зашифровано і зберігається / шифрується в реальному часі. І як тільки вимкнути контейнер, то вхід до нього надійно закриється.

Завантажити архів портативної версії утиліти (portable version for Windows, https://www.veracrypt.fr/en/Downloads.html) та запустити розпакування.

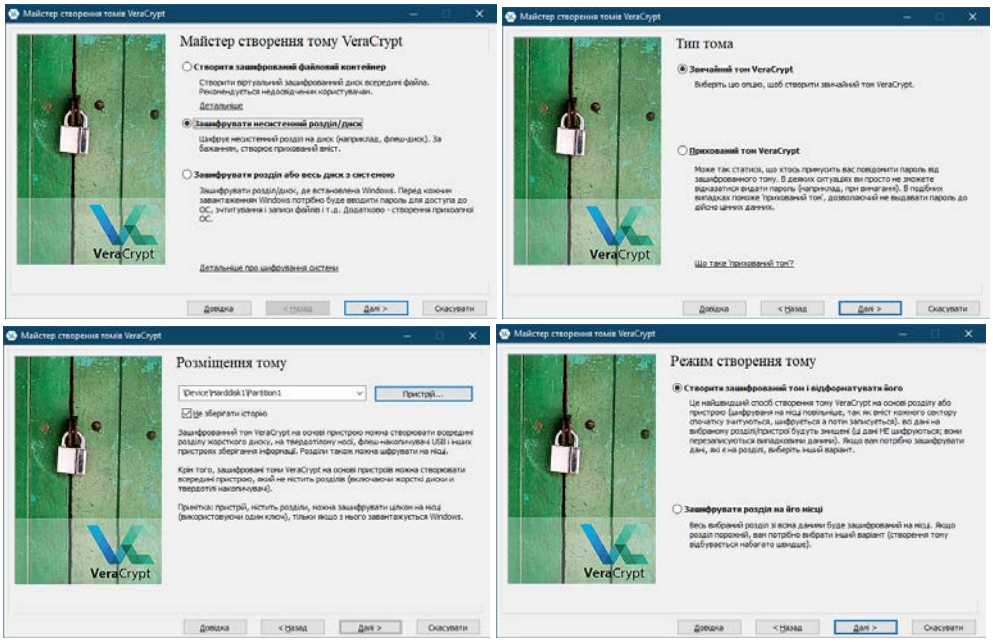
З теки VeraCrypt запустити файл VeraCrypt-x64.exe та у меню 'Settings' змінити мову програми на українську. Для цього клацнути на меню 'Settings', там вибрати 'Language ...' та обрати «Українська». Далі натиснути «Створити том» (том – це те ж саме що і контейнер) (зобр. 6).



Зобр. 6. Головне вікно VeraCrypt

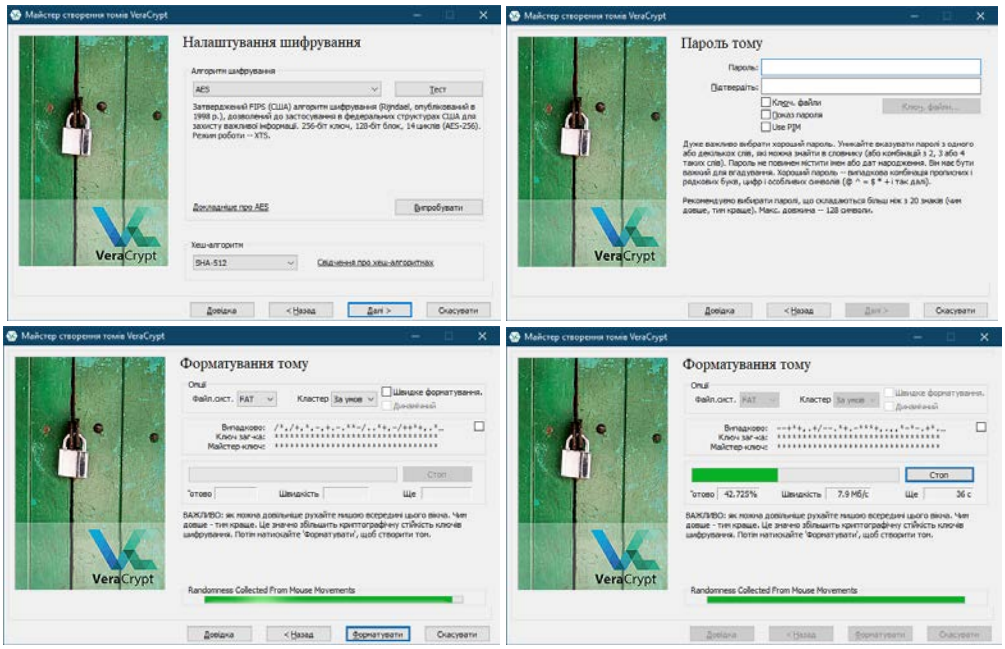
Обрати «Зашифрувати несистемний розділ/диск», «Звичайний том VeraCrypt». Вибрати розміщення тому, вказавши як пристрій флеш-накопичувач. **ВАЖЛИВО: перевірити правильність вибору пристрою, який потім буде форматуватися.**

Вибрати режим створення тому «Створити зашифрований том і відформатувати його» (зобр. 7).



Зобр. 7. Майстер створення тому

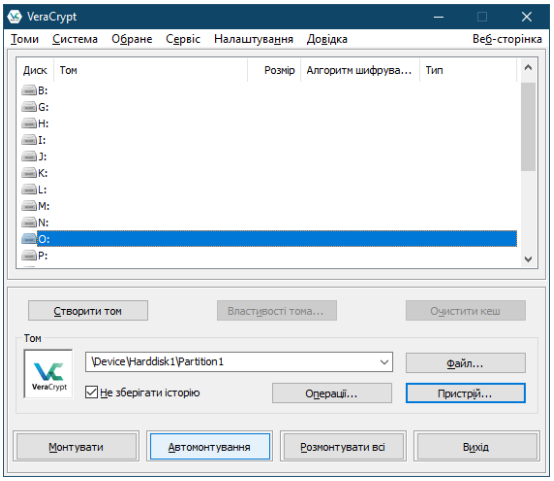
Налаштування шифрування залишити за замовчуванням. Встановити пароль тому дотримуючись рекомендацій, що будуть запропоновані у вікні вибору паролю. Важливо запам'ятати пароль і ніде не записувати. Як рекомендація – взяти перші (останні) літери улюбленої довгої фрази із заміною деяких літер цифрами і символами. Для форматування тому випадковим чином рухати мишею деякий час, а потім ініціювати форматування носія.



Зобр. 8. Налаштування шифрування та форматування тому

Після форматування ознайомитися із порядком монтування тому. Захищений флеш-накопичувач створено.

Для користуванням захищеним носієм у головному вікні VeraCrypt вибрати у розділі «Пристрій» диск флеш-накопичувача, вільну літеру для диску, що буде змонтований, та натиснути «Монтувати» або «Автомонтування» (зобр. 9).



Зобр. 9. Підключення зашифрованого диску

На запит ввести пароль і буде створений новий логічний диск, з яким можна працювати: записувати і редагувати файли, запускати програми.

По закінченні роботи із змонтованим диском у головному вікні VeraCrypt натиснути «Розмонтувати всі».

Перевірити надійність захисту інформації здійснити шляхом обміну змінними носіями і спробою відкрити диски.

ПРАКТИЧНА ВПРАВА
«БЛОКУВАННЯ ДОСТУПУ ДО ОПЕРАЦІЙНОЇ СИСТЕМИ ЗА ВІДСУТНОСТІ АКТИВНОСТІ»

Навчальна мета заняття: налаштувати блокування ОС Windows за відсутності активності.

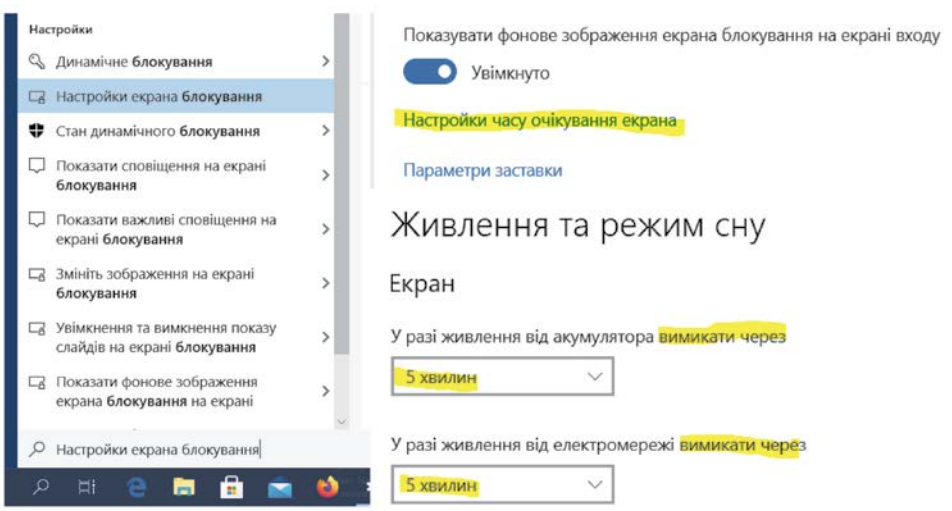
Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

Налаштувати та перевірити функціонування автоматичного блокування ОС Windows після 5 хвилин відсутності активності.

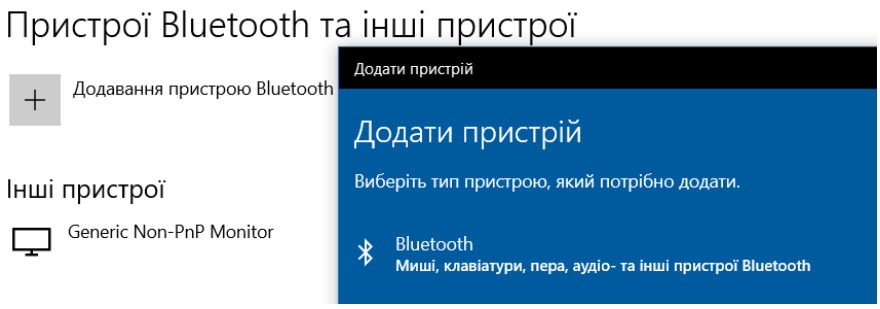
На панелі задач у полі пошуку ввести запит «блокування», вибрати «Налаштування екрана блокування» – «Налаштування часу очікування екрана» та встановити «…вимикати через 5 хвилин» (зобр. 1).



Зобр. 1. Налаштування автоматичного блокування ОС Windows після 5 хвилин відсутності активності

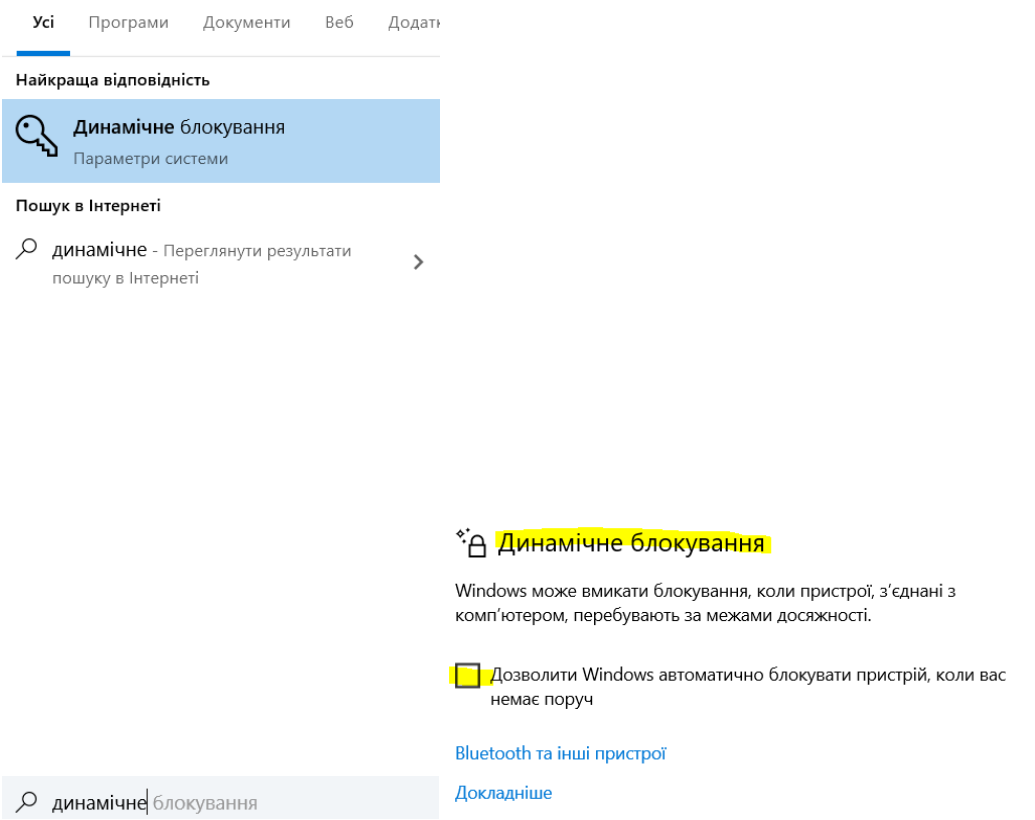
Налаштувати та перевірити роботу функції «Динамічне блокування» Windows, яка буде вмикати блокування, коли пристрої, з'єднанні з комп'ютером, опиняться за межами досяжності.

У смартфоні та комп'ютері включити Bluetooth, з'єднати пристрої між собою через відповідні налаштування Bluetooth (зобр. 2). Шляхом тестової передачі довільного файлу зі смартфона до комп'ютера переконатися у встановленому з'єднанні.



Зобр. 2. Підключення Bluetooth пристрою до комп'ютеру

На панелі задач у полі пошуку ввести запит «динамічне», обрати «Динамічне блокування» та ввімкнути «Дозволити Windows автоматично блокувати пристрій, коли вас немає поруч» (зобр. 3). Дочекатися, коли система знайде і відобразить графічно встановлене Bluetooth-підключення зі смартфоном.



Зобр. 3. Налаштування «Динамічне блокування» Windows

Розірвати з'єднання смартфона з комп'ютером, відключивши Bluetooth-адаптер смартфона, і дочекатися автоматичного блокування екрана (приблизно через 1 хвилину).

ПРАКТИЧНА ВПРАВА
«АВТОВІДТВОРЕННЯ ПІД ЧАС ПІДКЛЮЧЕННЯ ЗНІМНИХ НОСІЇВ»

Навчальна мета заняття: налаштувати блокування ОС Windows за відсутності активності.

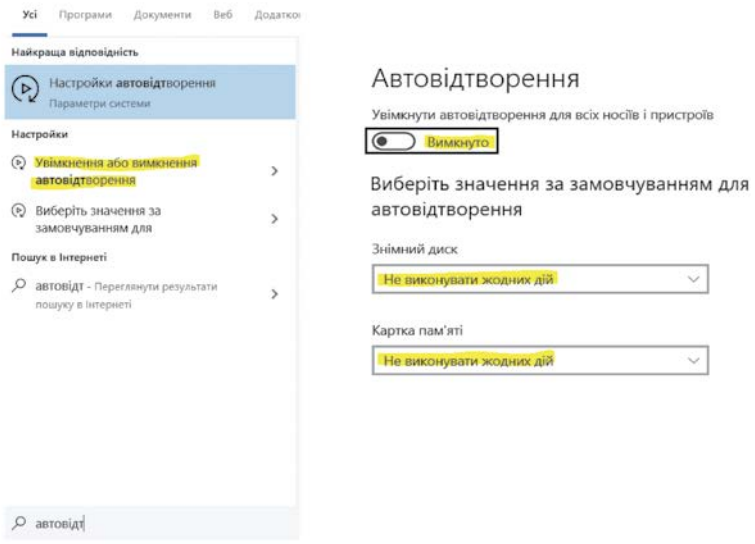
Час проведення: 0,1 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 10 Pro або вище та доступом до мережі «Інтернет», веббраузер «Google Chrome», флеш-накопичувачі за кількістю слухачів, особисті смартфони у слухачів.

Порядок проведення заняття

Для захисту від так званого «стілеру» (stealer), який використовує для крадіжки даних функцію автовідтворення під час підключення знімних носіїв, вимкнути функцію автовідтворення в ОС Windows.

На панелі задач у полі пошуку ввести запит «автовідтворення», обрати «Увімкнення або вимкнення автовідтворення» та вимкнути цю функцію (зобр. 1).



Зобр. 1. Вимкнення функції автовідтворення для всіх носіїв і пристроїв

Підключити знімний носій до комп'ютера та переконатися у відсутності автоматичного відтворення змінного носія.

МОДУЛЬ № 8:

УБЕЗПЕЧЕННЯ ВІД НЕПРАВДИВИХ ПОВІДОМЛЕНЬ

ПРАКТИЧНА ВПРАВА

«ІНСТРУМЕНТИ ВИЯВЛЕННЯ НЕПРАВДИВИХ ПОВІДОМЛЕНЬ»

Навчальна мета заняття: навчитися перевіряти окремі відомості в мережі Інтернет на достовірність.

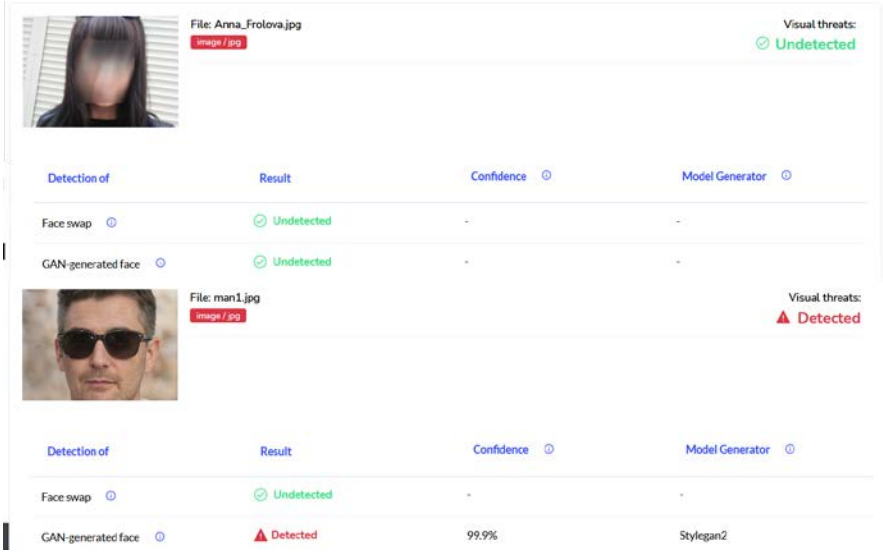
Час проведення: 0,5 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

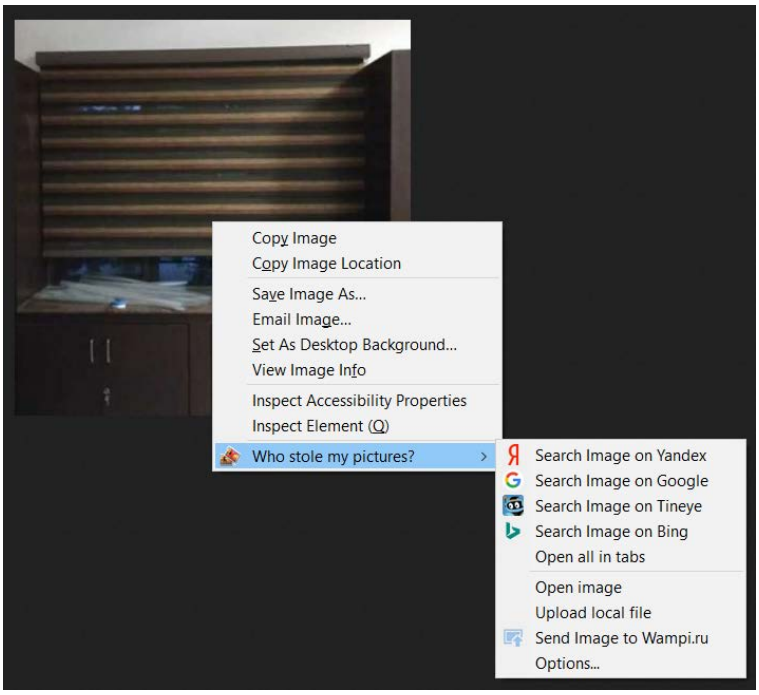
Для перевірки повідомлень та інших матеріалів на предмет їх актуальності та достовірності можуть бути використані різні аналітичні методи. Для полегшення цього процесу також варто застосовувати і низку технічних рішень. Серед подібних інструментів можна виділити такі.

Deepfake detection – це інструмент, який дозволяє виявляти підробку у різних мультимедійних файлах. Для використання цього продукту достатньо перейти за вказаним посиланням https://platform.sensity.ai/deepfake-detection#, авторизуватися. Після цього стають доступними функції завантаження мультимедійного документа для перевірки (зобр. 1).



Зобр. 1. Перевірка зображень на предмет маніпуляцій

Зображення можуть не мати ознак маніпуляцій, проте використовуватися у неправдивих повідомленнях у різних контекстах. Для того, щоб знайти першоджерело відповідних малюнків можна використовувати розширення Who stole my pictures (зобр. 2).



Зобр. 2. Використання розширення для пошуку зображень

Завантажити описане розширення можна за адресами:

- для браузеру «Chrome» (https://chrome.google.com/webstore/detail/who-stole-my-pictures/mcdbnfhkikiofkkicppioekloflmaibd);
- для браузеру «Firefox» (https://addons.mozilla.org/ru/firefox/addon/who-stole-my-pictures/).

1. Створіть декілька зображень за допомогою ресурсу thispersondoesnotexist.com, а також завантажте декілька медіафайлів із соціальних мереж.

2. Дослідіть роботу описаних програмних інструментів.

ПРАКТИЧНА ВПРАВА

«СТВОРЕННЯ ВЕБКВЕСТУ»

Навчальна мета заняття: навчитися створювати вебквести для проведення навчання.

Час проведення: 2 год. Місце проведення: комп'ютерний клас.

Устаткування: персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі «Інтернет».

Завдання, які потрібно виконати, **підкреслено**.

Особливостями вебквестів є те, що під час їх проходження учасникам:

- дозволяється *користуватися будь-якими джерелами* інформації;
- потрібно надати відповідь на конкретні *питання, без яких неможливо пройти подальші завдання*;
- на основі шаблонів документів *складаються конкретні процесуальні документи*;
- засвоюються *типові алгоритми дій* в різних ситуаціях.

Таким чином, особа занурюється у віртуальну реальність та з використанням тренажерів засвоює матеріал.

Для створення вебквестів можуть бути використані різні інструменти. Одним з таких є платформа для навчання «Google Classroom».

Google Classroom об'єднує в собі:

- Google Drive для створення завдань і обміну ними,
- Google Docs, Sheets and Slides для написання,
- Gmail для спілкування і
- Google Calendar для розкладу.

Учасники можуть бути запрошені до класу через приватний код чи автоматично імпортуватися з навчального сайту. Кожен клас створює окрему папку на Google

диску відповідного користувача Google Drive, куди учасник може подати роботу, яку оцінює викладач.

Корисні поради:

- доступ до завдань потрібно відкривати послідовно та пояснювати помилки на кожному етапі;
- тестові питання мають бути радше маленькими завданнями, по завершенні виконання яких потрібно ввести результат як відповідь;
- усі документи, використовувані в завданнях, повинні відповідати реальним за формою;
- квест має охоплювати якомога більше елементів реального розслідування;
- завдання повинні бути якомога цікавішими.

1. Група поділяється на декілька команд, кожна з яких має ознайомитися із:

- методикою перевірки фактів, викладеною за адресою gijn.org/2018/08/20/шесть-способов-создания-фейковых-нов-2/;
- ресурсами spotdeepfakes.org/en-US, scamspotter.org/quiz, phishingquiz.withgoogle.com, - spotthetroll.org, getbadnews.com/#play.

2. Проаналізувати одну зі статей на пропагандистському ресурсі. Виявити ознаки маніпуляції, викривлення фактів тощо.

3. Команді слід увійти до облікового запису Google. На основі вивчених даних створити квестове завдання з виявлення неправдивих повідомлень.

4. Презентація результатів командами.

МОДУЛЬ № 9:

ПРАВОВІ ЗАСАДИ КІБЕРГІГІЄНИ

ПРАКТИЧНА ВПРАВА

«ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ»

Навчальна мета заняття: провести гру «Дебати» за темою для виявлення та закріплення знань.

Час проведення: 1 год. Місце проведення: навчальна аудиторія.

Устаткування: ручка, зошит.

Короткі теоретичні відомості

У контексті вивчення кібіргігієни працівниками органів державної влади та місцевого самоврядування потрібно розуміти окремі аспекти вітчизняного законодавства, яке має давні традиції унормування правил безпечної роботи з інформацією.

У національних нормативно-правових актах на сьогодні відсутнє безпосереднє згадування такої категорії як кібергігієна. Водночас найбільш дотичними термінами у досліджуваному контексті є «інформаційна безпека» та «кібербезпека».

Згідно зі статтею 17 Конституції України, забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу.

25 лютого 2016 р. Указом Президента України № 47/2017 було затверджено Доктрину інформаційної безпеки України, в якій зазначено, що комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту і розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Інформаційна безпека та кібербезпека держави є складовою частиною її національної безпеки. В Україні питанню забезпечення національної безпеки традиційно приділяють велику увагу. Здійснивши екскурс в історію, можна побачити, що від самого початку становлення України як незалежної держави методично ухвалювалися нормативно-правові акти, які містили безпосередні вказівки для того чи іншого напряму забезпечення національної безпеки.

У зв'язку з появою нових системних загроз національній безпеці 21 червня 2018 р. було ухвалено новий Закон України «Про національну безпеку України», який відобразив сучасні безпекові реалії та стратегічні напрямки розвитку сектору безпеки України.

Відповідно до п. 9 ч. 1 ст. 1 цього Закону, ***національна безпека*** – це захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів України від реальних і потенційних загроз.

Складові частини національної безпеки можна представити як на зобр. 1.

Зобр. 1. Структура національної безпеки України

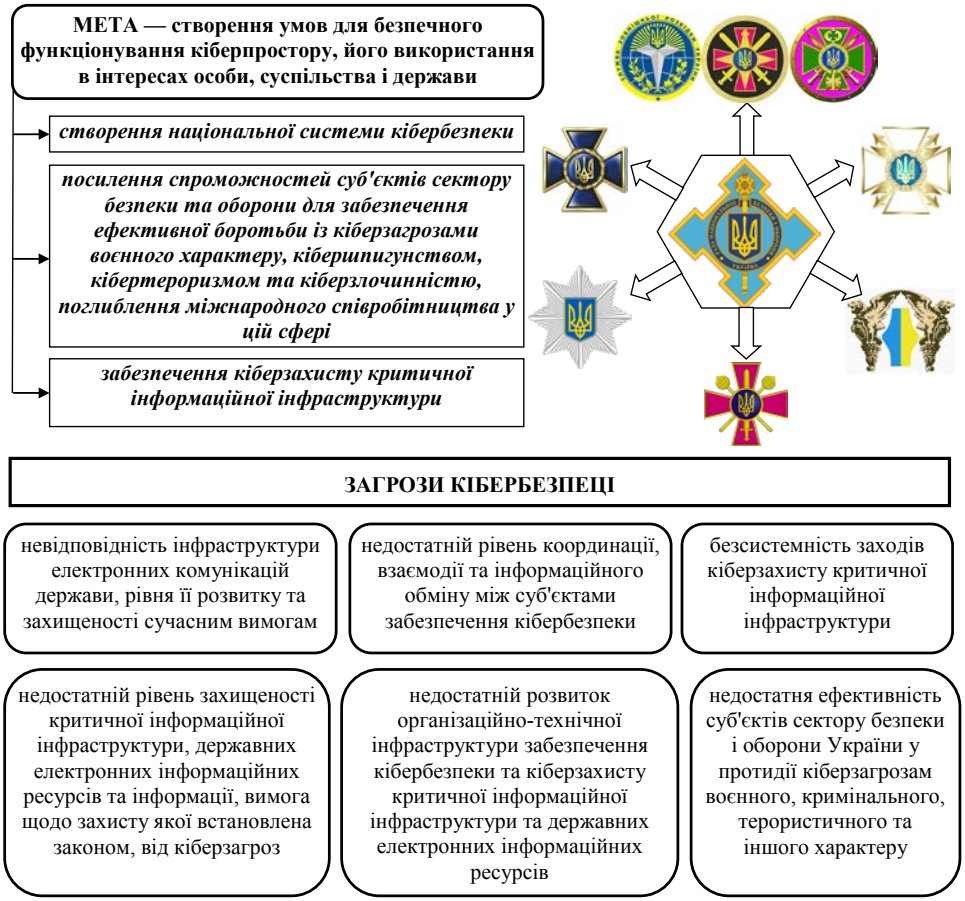
За вказаними напрямами безпеки здійснюється планування. Документи, що містять довгострокові плани, отримали назву стратегії. Відповідно, в законі описуються в загальному вигляді стратегії національної безпеки, воєнної безпеки, громадської безпеки та цивільного захисту України тощо.

Окремим нормативним актом затверджено ***Стратегію кібербезпеки України*** – документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Більш докладно структуру вказаного документа зображено на зобр. 2.

Слід наголосити, що в Законі України «Про національну безпеку України» не надається визначення термінів «інформаційна безпека» та «кібербезпека». На законодавчому рівні їх закріпили законами України «Про основні засади

забезпечення кібербезпеки України» від 05.10.2017 та «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007.

Зокрема, ***кібербезпека*** – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.



Зобр. 2. Основні елементи стратегії кібербезпеки України

Об'єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

Кібергігієна є важливим елементом кібербезпеки, проте ці поняття не є тотожними. Якщо кібербезпека пов'язана з об'єктивним оцінюванням дій, спрямованих на підтримку безпеки та дотримання захисту від кібератак, то кібергігієна асоціюється зі знаннями про безпеку в Інтернеті та правилами покращення кібербезпеки[1]. Також кібергігієна передбачає дотримання правил поведінки, що стосуються інформаційної безпеки.

Згідно з п. 13 розділу III Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки під ***інформаційною безпекою*** розуміється стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

- створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;
- підвищення рівня координації діяльності державних органів щодо виявлення, оцінки та прогнозування загроз інформаційній безпеці, запобігання таким загрозам і забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;
- вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній

[1] Neigel A. R., Claypoole V. L., Waldfogle G. E., Acharya S., Hancock G. M. Holistic Cyber Hygiene Education: Accounting for the Human Factors. *Computers & Security.* 2020. Vol. 92. 101731 (DOI: 10.1016/j.cose.2020.101731).

злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

- розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Виходячи зі змісту Доктрини інформаційної безпеки України, на зобр. 3 представлено основні пріоритети державної політики в інформаційній сфері щодо забезпечення інформаційної безпеки.

Суб'єктами забезпечення інформаційної безпеки як складової національної безпеки України є:

- громадяни України та їх об'єднання;
- Верховна Рада України, яка, серед іншого, ухвалює закони у сфері інформаційної безпеки, визначаючи тим самим державну політику в цій сфері;
- Президент України, який забезпечує послідовне проведення державної інформаційної політики, інформаційний суверенітет та інформаційну безпеку України;
- Кабінет Міністрів України, який організовує діяльність виконавчої влади щодо забезпечення інформаційної безпеки;
- Рада національної безпеки і оборони України, яку очолює Президент України, координує та контролює діяльність органів виконавчої влади у сфері інформаційної безпеки України;
- інші центральні органи виконавчої влади та органи сектору безпеки і оборони України;
- засоби масової інформації та інші суб'єкти, які здійснюють інформаційну діяльність;
- наукові установи та навчальні заклади, які, серед іншого, проводять наукові дослідження та здійснюють підготовку фахівців з інформаційної безпеки.

Зобр. 3. Основні пріоритети забезпечення інформаційної безпеки

Залежно від конкретного виду інформації встановлюються різні рівні її захисту. Для визначення конкретних захисних механізмів використовується принцип поділу інформації за порядком доступу на відкриту та з обмеженим доступом. Загальна структура такого поділу наведена на зобр. 4.

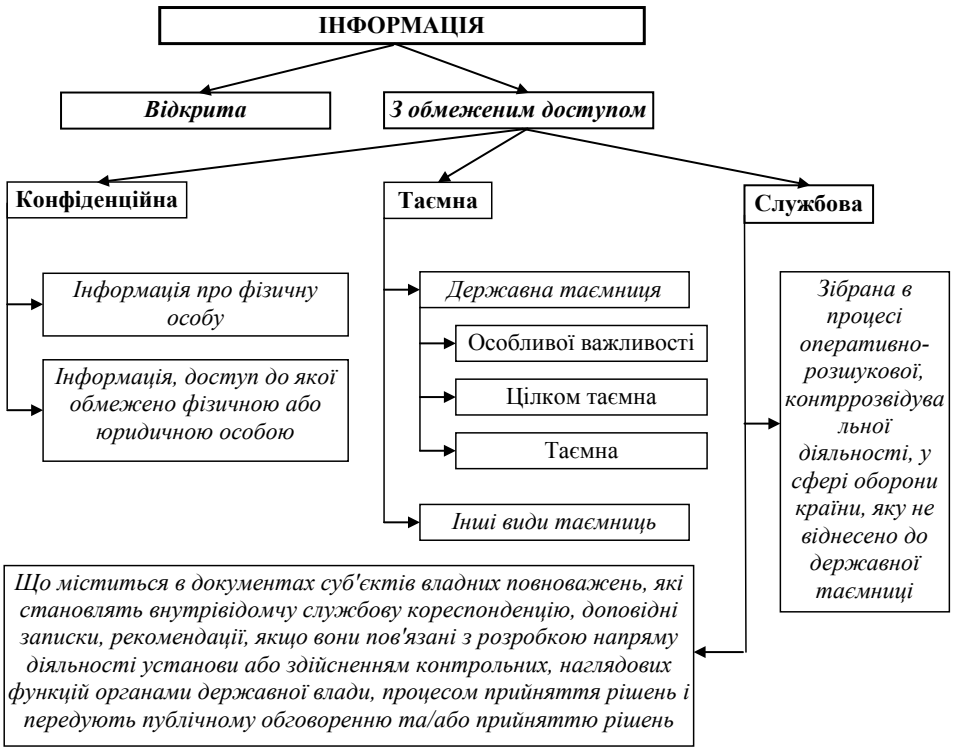
Захист відкритої інформації в державних органах регламентують:

1. Концепція технічного захисту інформації в Україні, затверджена Постановою Кабінету Міністрів України від 08.10.1997 № 1126[2].

[2] Концепція технічного захисту інформації в Україні: постанова Кабінету Міністрів України № 1126 від 8.10.1997 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/1126-97-%D0%BF (дата звернення: 12.07.2017).

2. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29.03.2006 № 373[3].

Захисту потребують такі властивості відкритої інформації, як *цілісність і доступність.*



Зобр. 4. Класифікація інформації за порядком доступу

Будь-яка інформація є **відкритою**, крім тієї, що віднесена законом до інформації з обмеженим доступом. До відкритої інформації, що підлягає захисту, відносять інформацію, яка належить до державних інформаційних ресурсів, а також про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами.

[3] Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України № 373 від 29.03.06; [із змінами і доповненнями]. *Офіційний вісник України.* 2006. № 13 (12.04.2006), стор. 164, стаття 878.

Відповідно до ч. 2 ст. 21 Закону України «Про інформацію»[4], ***конфіденційною*** є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.

Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи *у визначеному* нею *порядку* відповідно до *передбачених* нею *умов*, а також *в інших випадках, визначених законом*. Встановлення системи захисту є правом, а не обов'язком власника. Конфіденційна та службова інформація належать до інформації з обмеженим доступом, але не всяка інформація може бути визнана такою. Законодавець встановлює з цього приводу певні обмеження.

За розголошення конфіденційної інформації, що не є власністю держави, може наступати адміністративна відповідальність у порядку, визначеному ст. 164-3 Кодексу України про адміністративні правопорушення (КУпАП) від 07.12.1984. Крім того, адміністративна відповідальність може наставати також за порушення порядку використання конфіденційної інформації (ст. 186-3 КУпАП).

Більш урегульованими з правової точки зору є питання захисту службової інформації. Порядок ведення обліку, зберігання, використання та знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, детально прописаний у Типовій інструкції, затвердженій Постановою Кабінету Міністрів України від 19.10.2016 № 736[5].

За порушення роботи зі службовою інформацією передбачена адміністративна, а в окремих випадках – кримінальна відповідальність. Так, згідно зі ст. 212-5 КУпАП, порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, що призвело до розголошення такої інформації, тягне за собою накладення штрафу на громадян від двадцяти до сорока неоподатковуваних

[4] Про інформацію: закон України від 02.10.1992 р.; [із змінами і доповненнями]. *Відомості Верховної Ради України*. 1992. № 48 (01.12.1992). ст. 650.

[5] Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена Постановою Кабінету міністрів України від 19.10.2016 № 736. *Офіційний вісник України*. 2016. № 85 (04.11.2016), стор. 102, стаття 2783.

мінімумів доходів громадян і на посадових осіб – від шістдесяти до ста шістдесяти неоподатковуваних мінімумів доходів громадян. Повторне вчинення правопорушення збільшує розмір штрафу.

Кримінальна відповідальність встановлюється за розголошення службової інформації (зібраної у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни) *нерезидентам* України (іноземним підприємствам, установам, організаціям або їх представникам) (ст. 330 Кримінального кодексу України).

Також належать до інформації з обмеженим доступом ***персональні дані*** – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Наразі в Україні діє Закон України «Про захист персональних даних» від 01.06.2010, яким унормовано порядок роботи з інформацією, що містить персональні дані[6].

Таку інформацію можна поділити на:

- **загальну**, яка є відкритою і може використовуватися іншими особами. Це, наприклад, ім'я фізичної особи, право на використання якого відповідно до п. 3 ст. 296 Цивільного кодексу України допускається без її згоди, з метою висвітлення діяльності особи або діяльності організації, в якій вона працює чи навчається, що ґрунтується на відповідних документах (звітах, стенограмах, протоколах, аудіо-, відеозаписах, архівних матеріалах тощо);
- **вразливі персональні дані (конфіденційна інформація про особу)**, що є інформацією з обмеженим доступом. Саме про такі дані йдеться у ст. 32 Конституції України та у ст. 302 Цивільного кодексу України: «Збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». До таких даних належать, зокрема, персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, засудження до

[6] Про захист персональних даних: закон України від 01.06.2010; [із змінами і доповненнями]. *Офіційний вісник України.* 2010. № 49 (09.07.2010), стор. 199, стаття 1604.

кримінального покарання. Також згідно з Рішенням Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997, *до конфіденційної інформації про особу*, зокрема, належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані).

У 2012 році Конституційний суд України додатково розтлумачив, що інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовій, інтимній, товариській, професійній, діловій та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за їх згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини[7].

Враховуючи викладене, відповідно до Закону України «Про захист персональних даних», Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29.03.2006 № 373 та інших нормативних актів у сфері захисту інформації, **загальна інформація про особу**, що зберігається в інформаційних системах держави, повинна бути захищена як відкрита інформація, а **вразливі персональні дані –** як службова інформація, відповідно до вимог чинного законодавства у державних органах, або як окремий вид інформації, згідно з вимогами Закону України «Про захист персональних даних» від 01.06.2010.

[7] Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. *Офіційний вісник України*. 2012. № 9 (10.02.2012), стор. 106, стаття 332.

Захист інформації, яка становить державну таємницю, регламентується, перш за все, Конституцією України, кількома міжнародними договорами, ратифікованими Верховною Радою України, Законом України «Про державну таємницю» від 21.01.1994[8], Кримінальним кодексом України та низкою підзаконних актів.

Згідно зі ст. 1 Закону України «Про державну таємницю», ***державна таємниця*** – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому законом, державною таємницею і підлягають охороні державою.

Організаційну структуру охорони державної таємниці умовно можна представити як на зобр. 5.

Зобр. 5. Компетенція органів державної влади, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

[8] Про державну таємницю: закон України від 21.01.1994; [із змінами і доповненнями]. *Відомості Верховної Ради України*. 1994. № 16 (19.04.1994). стор. 422. ст. 93.

За порушення законодавства про державну таємницю передбачена дисциплінарна, адміністративна (ст. 212-2 КУпАП) та кримінальна відповідальність (ст. ст. 111, 114, 328, 329, 422 Кримінального кодексу України).

Порядок проведення заняття

1. Слухачі заздалегідь отримують матеріали для підготовки та ознайомлюються з правилами гри.
2. Групу розділяють на три команди: «Доповідачі», «Опоненти», «Рецензенти» (Арбітром є тренер).
3. Команда доповідачів називає будь яке число у межах кількості питань для підготовки. Після цього тренер ставить питання, номер якого відповідає названому доповідачами числу у списку питань тренера. Далі команда доповідачів протягом однієї хвилини розмірковує, чи приймає вона питання. Якщо команда питання не приймає, то вона має право ще на одну спробу вибору питання.
4. Далі команда доповідачів протягом 3-х хвилин готує розгорнуту відповідь на поставлене тренером питання. У цей час команда опонентів починає готувати питання для команди доповідачів, а команда рецензентів починає готувати питання для обох інших команд, з метою оцінки їх відповідей. Максимальна кількість запитань від кожної команди – 10.
5. Після цього доповідачі відповідають на питання тренера протягом 5-ти хвилин. Опоненти та рецензенти в цей час корегують свої питання відповідно до відповіді доповідачів.
6. Опоненти ставлять питання доповідачам. Доповідачі розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
7. Рецензенти ставлять питання доповідачам і опонентам. Ті розмірковують протягом 40 секунд та відповідають. Час відповіді необмежений.
8. Рецензенти протягом 3-х хвилин дають оцінку обом командам.
9. Полеміка між командами протягом 5-ти хвилин.
10. Тренер ставить контрольне питання за розглянутим питанням кожній з команд.
11. Тренер оцінює якість роботи кожної з команд.

Критерії оцінювання (за п'ятибальною шкалою кожний):

- повнота та аргументованість відповідей;
- робота в команді;
- дотримання правил етикету.

12. Після оцінювання команд вони змінюють свій статус і гра продовжується. Так три раунди.
13. По закінченні гри підбиваються підсумки.

ВИСНОВКИ

Цей курс призначено для майбутніх тренерів з кібергігієни. Він містить достатньо інформації та структуру, необхідні для планування та викладання кількаденного курсу з основ кібергігієни для представників органів державної влади та місцевого самоврядування.

За результатами вивчення матеріалу цієї роботи слухачі повинні навчитися не просто дотримуватись правил кібергігієни, але й доносити відповідні методи убезпечення до слухачів. Для цього майбутнім тренерам слід уважно вивчити запропоновані вправи та не соромитись ставити питання впродовж їх виконання.

По завершенні даного курсу слід провести оцінку засвоєння матеріалу шляхом проведення невеликого тестування, результати якого стануть індикатором успішності чи неуспішності проходження навчання.

Follow OSCE Project Co-ordinator in Ukraine

Україна, 01030, Київ,

вул. Стрілецька, 16

info-pcu@osce.org

www.osce.org/ukraine

ОБСЄ Організація з безпеки та співробітництва в Європі
Координатор проектів в Україні