

**Методичні вказівки
до виконання лабораторних робіт
з дисципліни «Основи безпеки інтернет-технології»
зі спеціальності «Кібербезпека та захист інформації»**

Міністерство освіти і науки України
Вінницький національний технічний університет

**Методичні вказівки
до виконання лабораторних робіт
з дисципліни «Основи безпеки інтернет-технології»
зі спеціальності «Кібербезпека та захист інформації»**

Вінниця
ВНТУ
2026

Рекомендовано до видання Радою з якості освіти Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 13 від 18.06.2026 р.)

Рецензенти:

В. П. Майданюк, кандидат технічних наук, доцент

Г. Б. Ракитянська, кандидат технічних наук, доцент

Методичні вказівки до виконання лабораторних робіт з дисципліни «Основи безпеки інтернет-технологій» зі спеціальності «Кібербезпека та захист інформації» / уклад.: В. І. Маліновський, Л. М. Куперштейн, Л. О. Майданевич. Електрон. текст. дані. Вінниця : ВНТУ, 2026. 70 с.

Методичні вказівки призначені для студентів зі спеціальності «Кібербезпека та захист інформації», що навчаються за освітніми за першим рівнем освіти «бакалавр». У методичних вказівках вирішуються завдання із області використання Інтернет-технологій на комп'ютерних і мобільних пристроях та пристроях Інтернету речей. У виданні наведені завдання для рішення практичних задач у галузі кібергігієни та кібербезпеки вебтехнологій та Інтернет-сервісів на стаціонарних та мобільних інформаційних пристроїв користувачів.

ЗМІСТ

1. Лабораторна робота № 1. Основи парольної безпеки та цілісності даних користувача в інформаційних сервісах.....	4
2. Лабораторна робота № 2. Основи кібербезпеки та захисту електронної пошти (E-mail) та інших інформаційних інтернет-сервісів	13
3. Лабораторна робота № 3. Основи кібербезпеки і кібергігієни інтернет-браузера та захисту клієнської частини інтернет-сервісів.....	18
4. Лабораторна робота № 4. Кібербезпека робочого місця користувача із ПК/АРМ із виходом у мережу Інтернет.....	26
5. Лабораторна робота № 5. Основи кібербезпеки месенджерів та засобів спілкування на інтернет-ресурсах	34
6. Лабораторна робота № 6. Базові техніки кібербезпеки і кібергігієни при роботі із банківськими та іншими інтернет-сервісами	38
7. Лабораторна робота № 7. Основи кібербезпеки мобільних і персональних пристроїв користувачів в мережі Інтернет	47
8. Лабораторна робота № 8. Основи мережевого захисту серверної частини інтернет-сервісів та їх ресурсів	62

ЛАБОРАТОРНА РОБОТА № 1

Основи парольної безпеки та цілісності даних користувача в інформаційних сервісах

Мета роботи – засвоєння найпростіших прийомів роботи із створенням надійних і стабільних паролів та даних авторизації в акаунтах мережі Інтернет. Вивчення програм хешування для перевірки цілісності даних та створення надійних паролів і даних акаунта у мережі. Зрозуміти концепцію надійного пароля. Дослідити концепцію створення надійного пароля.

Необхідні ресурси: ПК або персональний пристрій з доступом до Інтернету. ПК(ПЕОМ) із доступом до Інтернет, необхідне програмне забезпечення (ПЗ), встановлені робочі середовища і операційні системи та/або персональні пристрої із цими системами і доступом до Інтернету.

Теоретичні відомості

Для вивчення теоретичних відомостей потрібно ознайомитись із теоретичним матеріалом і лекційними матеріалами за темами: «Парольна кібербезпека та кібергігієна», «Основи перевірки цілісності інформації» та «Геш-функції і їх застосування».

Порядок виконання лабораторної роботи

Ознайомитись із теоретичним матеріалом за відповідними темами.

Завдання 1. Гешування даних за допомогою Геш-функцій та перевірка цілісності даних.

- 1.1. Створіть текстовий файл із довільним паролем.
 - a. Знайдіть на своєму комп'ютері програму Блокнот (Notepad) і відкрийте її.
 - b. Введіть текст довільного пароля у програмі.
 - c. Виберіть Файл > Зберегти (File > Save).
 - d. Перейдіть до Робочого столу в ОС Windows чи Linux і подивіться властивості файлу. Там повинен бути розділ контрольні суми і геш. Зафіксуйте ці дані і збережіть у вигляді скріншоту.
 - e. Введіть Hash (Геш) у поле Ім'я файлу: (File name:) і натисніть Зберегти (Save).

1.2. Встановіть програмне забезпечення або скористайтесь онлайн-версіями ПЗ (вебверсіями) для визначення та/або генерації Геш-функцій, наприклад:

HashCalc, HashTab – модулі ПЗ під ОС MS Windows, або HashCalc Online WEB – різновиди ПЗ для визначення та/або генерації Геш-функцій, які доступні через пошук у вашому інтернет-браузері: інтернет-браузер (Ghrome/Mozilla Firefox/Opera/Edge/in)>>HashCalc, HashTab Online)>> перші доступні 4-5 вебсайтів і один-два довільних (на вибір). Все виконується безпосередньо в інтернет-браузері, у вигляді вебзастосунків безпосередньо в середовищі WEB через інтернет-браузер. Для використання Online WEB – перейдіть у інтернет-браузер (Ghrome, Mozilla Firefox, Opera, Edge, Internet Explorer) і в довільній системі WEB пошуку (google,bing, yahoo) введіть Online HashCalc та/або OnlineHashCalculator і оберіть довільні 3-4 сервіси (із результатів пошуку) і виберіть найбільш зручний, функціональний і придатний для Вас.

1.3 а. У випадку, якщо посилання з якихось причин недоступне (відсутність мережі, проблеми із сайтом, тощо) – взяти відповідні екземпляри програм ПЗ у викладача або лаборанта.

1.3 б. Натисніть Завантажити (Download) у рядку HashCalc.

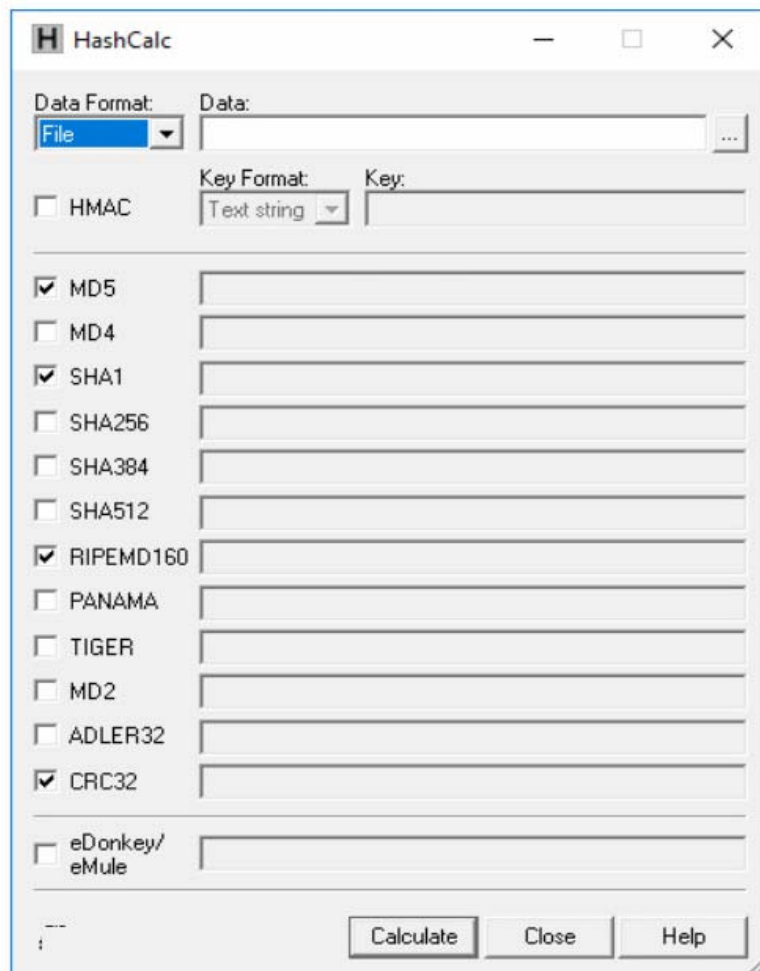
Відкрийте hashcalc.zip (hashtab.zip)файл та запустіть файл setup.exe.

1.3 с. Дотримуйтесь вказівок Майстра установки (Installation wizard), щоб встановити HashCalc(HashTab). Попросіть у викладача допомоги, якщо у вас є будь-які питання про встановлення програми.

1.3 е. Натисніть кнопку Готово (Finish) на останньому екрані та закрийте файл README, якщо він відкритий. Ви можете прочитати файл, якщо хочете.

1.3 f. HashCalc тепер встановлено та запущено.

1.4. Обчисліть геш файлу Hash.txt із паролем.



- a. Вкажіть наступні елементи у HashCalc:
 - 1) Формат даних (Data Format): Файл (File).
 - 2) Дані: Натисніть ... Поруч із полем Дані (Data), перейдіть на Робочий стіл (Desktop) і виберіть файл Hash.txt.
 - 3) Зніміть прапорець HMAC
 - 4) Зніміть усі типи хешів, крім MD5
 - b. Натисніть кнопку Обчислити (Calculate). Яке значення поряд із MD5?
- 1.4. Внесіть зміни у файл Hash.txt
- c. Перейдіть на Робочий стіл і відкрийте файл Hash.txt.
 - d. Зробіть невелику зміну тексту, наприклад, видалення літери або додавання пробілу.
 - e. Натисніть Файл > Зберегти (File > Save) та закрийте Блокнот.
- 1.5. Обчисліть новий хеш файлу Hash.txt
- a. Знову натисніть кнопку Обчислити (Calculate) в HashCalc. Яке значення поряд із MD5?
- Чи значення відрізняється від значення, що одержано на кроці 3?
- b. Встановіть прапорець біля усіх типів хеш-функцій.
 - c. Натисніть Обчислити (Calculate)
 - d. Зверніть увагу, що багато типів Хеш-функцій створюють хеш різної довжини. Поясніть чому? Онлайн калькулятори для обчислення хеш –функцій:
<https://www.fileformat.info/tool/hash.htm>
https://www.tools4noobs.com/online_tools/hash/

Завдання 2. Створення надійних паролів та концепція безпечного паролю.

1.1 Відкрийте веб-браузер і перейдіть на <http://passwordsgenerator.net>

1.2 Виберіть параметри, які відповідають політиці вибору пароля.

1.3. Згенеруйте пароль. Чи легко запам'ятати згенерований пароль?

Перевірте згенерований пароль за допомогою он лайн-інструменту перевірки надійності паролю:

<https://www.vpnmentor.com/tools/passwordmeter/> , або аналогічним.

2.4. Використовуючи онлайн-інструмент для створення паролів, створіть паролі на основі випадкових слів. Зауважте, що оскільки слова з'єднані разом, вони не розглядаються як словарні слова.

2.5. Відкрийте веб-браузер і перейдіть на <http://preshing.com/20110811/xkcd-password-generator/>

2.6. Згенеруйте новий пароль з випадкових слів, натиснувши Generate Another! у верхній частині веб-сторінки. Перевірте згенерований пароль за допомогою он лайн-інструменту перевірки надійності паролю: <https://www.vpnmentor.com/tools/passwordmeter/> , або аналогічним.

2.7. Чи легко запам'ятати згенерований пароль?

а) Знайдіть на своєму мобільному пристрої програму обробки текстових даних (Блокнот/Notepad, веб-додаток для обробки і роботи із файлами *.txt або інший додаток) і відкрийте її.

б) Введіть текст паролю у цій програмі для тесту. Згенеруйте пароль, який відповідає сучасним критеріям стабільності та надійності:

– довжина не менше 8 символів;

– в складі латинські літери, хаотично розміщені спецсимволи (регістр символів важливий). Чим вища стійкість паролю – тим краще.

а) Збережіть цей файл (File > Save).

2.8 Відкрийте веббраузер і перейдіть за посиланням: <http://preshing.com/20110811/xkcd-password-generator/>

2.9 Згенеруйте новий пароль з випадкових слів, вибравши опцію *Generate Another!* у верхній частині вебсторінки.

2.10 Чи легко запам'ятати згенерований пароль? Порівняти і зробити аналітичні висновки за отриманими результатами, які включити у звіт.

2.11 Перевірте стійкість та надійність пароля за допомогою одного із сервісів онлайн-перевірки стійкості та захищеності паролів:

<https://uk.vpnmentor.com/tools/passwordmeter/>

<https://uk.vpnmentor.com/tools/passwordmeter/>

<https://zillya.ua/check-password>

Інші сервіси для генерації паролей:

- Сервіс від Кіберполіції:

<https://www.cyberpolice.gov.ua/generate-password/>

- Сервіс від компанії ESET:

<https://www.eset.com/ua/home/generator-paroley/>

- Сервіс від компанії Avast:

<https://www.avast.ua/random-password-generator#pc>

- Програма Password Tech Portable (колишня назва PWGen) або інші програми і способи.

Зробити аналітичні висновки та проаналізувати отримані дані.

Завдання 3.

3.1. Визначити період блокування (годину, зміну, добу) введення пароля у системі автентифікації та авторизації на вебсервері за формулою (1.4), якщо задана середня кількість клієнтів, кількість спроб неправильного набору паролю та інші параметри (див. варіанти індивідуальних завдань). Показник K_p – межа "забудькуватості пароля" (вводиться згідно з таблицею по варіантах). Інформація про блокування клієнта автоматично надходить на пульт контролю системи вебсервера і журналюється. Також потрібно занести ці дані обрахунку у табл. 1.1.

Таблиця 1.1 – Вихідні дані

№	Робоча	Наявн	Показник	Фактор наявності	Макс	Питома ширина	визначення
1							
2		-					
3		-					

Згідно варіантів індивідуальних завдань обчислити період блокування інтернет-сервісу/інтернет-ресурсу для 2-х довільних випадків (2-х варіантів із параметрами).

Всі помилкові спроби увійти до системи повинні враховуватися, занотовуватися у файл журналу подій і аналізуватися через "розумний" проміжок часу. Якщо в системі передбачені можливість блокування клієнта або всієї системи після певної кількості невдалих спроб вхід цієї можливістю необхідно скористатися. Така можливість є основним бар'єром до підбору паролів повним перебором. Розумно, блокувати потенційно небезпечне підключення клієнта 3-й підряд неправильної спроби набору пароля, і, відповідно, блокувати систему невдалих спроб входу за деякий період (годину, зміну, добу).

$$\begin{aligned} K_{ed} &= \max(\text{int}(p * n_e * r) + 1; k); \\ K_{ed} &= \max(\text{int}(p * 0.1 * r) + 1; k), \end{aligned} \quad (1.4)$$

де p – середня кількість тих клієнтів, що підключаються за цей період до системи;
 r – кількість спроб вводу паролю (зазвичай $r = 3$); $n_e = 0.1 - 10\%$ (середня) – 10-ти відсоткова межа "забудькуватості пароля", r – кількість спроб і можливості введення пригадування паролю, і включення доступу по паролю, при його відновленні (для більшості систем кількість спроб на пригадування паролю, зазвичай $k = r$; $k = 3$ (ті ж самі 3)). Інформація про блокування клієнта або системи повинна автоматично надходити на пульт контролю за системою, або фіксуватися в логах серверу чи інформаційної системи моніторингу.

Варіанти індивідуальних завдань:

1. $p=2$; $ne=0.1$; $r=3$; $k=r$;
2. $p=1$; $ne=0.2$; $r=3$; $k=r$;
3. $p=2$; $ne=0.3$; $r=3$; $k=3$ $r=2$;
4. $p=1$; $ne=0.4$; $r=5$; $k=r$;
5. $p=3$; $ne=0.5$; $r=5$; $k=r$;
6. $p=2$; $ne=0.2$; $r=4$; $k=3$ $r=2$;
7. $p=2$; $ne=0.3$; $r=6$; $k=r$;
8. $p=3$; $ne=0.4$; $r=5$; $k=r$;
9. $p=3$; $ne=0.7$; $r=6$; $k=r$;
10. $p=2$; $ne=0.3$; $r=4$; $k=r$;
11. $p=2$; $ne=0.2$; $r=4$; $k=r$;
12. $p=2$; $ne=0.2$; $r=5$; $k=r$;
13. $p=1$; $ne=0.2$; $r=7$; $k=r$;
14. $p=2$; $ne=0.4$; $r=4$; $k=r$;
15. $p=1$; $ne=0.6$; $r=10$; $k=r$;
16. $p=2$; $ne=0.2$; $r=10$; $k=r$;
17. $p=3$; $ne=0.5$; $r=5$; $k=r$;
18. $p=3$; $ne=0.5$; $r=5$; $k=r$;
19. $p=5$; $ne=0.5$; $r=5$; $k=r$;
20. $p=5$; $ne=0.5$; $r=5$; $k=r$.

3.2. Описати базові параметри і ризики появи кіберзагроз для ІС (інформаційних систем) та інтернет-сервісів у різних варіантах появи. Відповідно вписати до таблиці і визначити повну кількість перебору паролів та середній час перебору для системи авторизації сервера за допомогою автентифікації та авторизації, яка має бути складною і містити цифри, символи і спец. символи клавіатури та враховувати регістр літер, виходячи з вищезазначеного переліку.

3.3. Перевірте, чи не були зламані або/та скомпроментовані ваші паролі від акаунтів (наприклад, E-mail) за допомогою одного із посилань:

<http://www.auditmvp.com;>
<http://www.pcllank.com/test;>
[http://www.hackerwatch.org/probe/.](http://www.hackerwatch.org/probe/)

або аналогічного сервісу комплексної перевірки паролів E-mail:

[http:// https://haveibeenpwned.com/](http://https://haveibeenpwned.com/)

3.4. Розрахувати і визначити питому складність, кількість комбінацій перебору пароля (методом грубої сили) за даними індивідуальних завдань. Для розрахунку потрібно ознайомитись із теоретичними відомостями з теми: «Парольна кібергігієна та кібербезпека».

Таблиця 1.2 – Вихідні дані по варіантах індивідуальних завдань

№ варіанту	Робоча довжина паролю L, символів	Наявність спец-символів	Показник обчислюв. потужності $Gplops$ $(\times 10^9)$	Фактор наявності регістру символів Аа (1-True; 0-False)	Максимальна довжина паролю, L_{max}	Питома ширина символу, M^*	Коеф-т визначення часу j
1	9	+	1,21	1	12	1	2.01
2	9	-	1,12	0	13	1	2.02
3	7	-	2,13	1	11	1	2.03
4	9	+	1,54	1	12	1	2.01
5	7	+	1,55	0	14	1	2.02
6	9	+	2,56	0	15	1	2.04
7	5	-	1,52	0	11	1	2.08
8	10	+	1,54	1	10	1	2.06
9	11	-	1,53	0	12	1	2.04
10	12	-	1,56	1	13	1	2.05

Завдання 4. Вивчення криптостійкості паролів.

4.1. Вивчення криптостійкості паролів і даних авторизації

У лабораторній роботі пропонується використовувати програму Advanced ZIP Password Recovery для дослідження криптостійкості паролів з різною кількістю символів і різними наборами символів.

4.1.1 За допомогою програми архівації даних створіть архівний файл і встановіть на нього пароль завдовжки 2 рядкових латинських символів.

4.1.2. Відкрийте створений файл в програмі Advanced ZIP Password Recovery і вкажіть використовуваний набір – рядкові латинські символи, мінімальну довжину пароля – 1, максимальну довжину пароля – 2 і виконаєте перебір. Зафіксуйте кількість перебраних паролів і час перебору в таблиці 1.3.

Таблиця 1.3 – Результати перебору паролів в програмі Advanced ZIP Password Recovery

№ п/п	Набір символів	Довжина пароля, символів	Кількість перебраних паролів	Час перебору, с	Швидкість перебору, паролей/с
-------	----------------	--------------------------	------------------------------	-----------------	-------------------------------

4.2. Повторіть дослідження архівного файлу захищеного паролями довжиною 2, 3, 4 рядкових латинських символів і занесіть результати в табл. 1.3. За допомогою програми архівації даних створіть архівний файл і встановіть на нього пароль завдовжки 2 символи з наборів рядкових латинських символів і цифр і занесіть результати в табл. 1.3.

4.3. Повторіть дослідження архівного файлу захищеного паролями 3, 4 рядкових і заголовних латинських символів; результати занесіть в табл. 1.3.

4.4. За допомогою програми архівації даних створіть архівний файл і встановіть на нього пароль завдовжки 2 символи з наборів рядкових, заголовних латинських символів і цифр, виконайте дослідження криптистійкості і занесіть результати в табл. 1.3.

4.5. Повторіть дослідження архівного файлу захищеного паролями довжин 2, 3, 4 рядкових, заголовних латинських символів і цифр, результати занесіть в табл. 1.3.

4.6. Створіть за допомогою програми архівації даних архівний файл і встановіть на нього пароль завдовжки 2 символи з наборів рядкових, заголовних латинських символів, цифр і спеціальних символів, виконайте дослідження криптистійкості і занесіть результати в табл. 1.3.

4.7. Повторіть дослідження архівного файлу захищеного паролями довжиною 5 рядкових, заголовних латинських символів, цифр і спеціальних символів, результати занесіть в табл. 1.3.

4.8. Повторіть дослідження архівних файлів захищених паролями довжини 5 символів для методу грубої сили і методу зі словником. Використайте два варіанта пароля, з комбінацією слів та довільний набір символів. Порівняйте роботу методів відновлення пароля.

4.9. Повторіть дослідження архівних файлів захищених паролями довжиною 5 символів з використанням маски. Порівняйте наскільки використання масок пришвидшує підбір паролів.

4.10. Побудуйте два графіки: залежність кількості перебраних паролів від довжини пароля для різних використаних наборів символів і залежність часу підбору пароля від довжини пароля для різних використаних наборів символів.

5. Зміст звіту

5.1. Тема і мета роботи.

5.2. Вихідні дані для виконання роботи.

5.3. Результати виконання роботи.

5.4. Висновки.

6. Контрольні запитання:

1. Для чого призначена геш-функція?
2. Назвіть основні алгоритми обчислення геш-функції?
3. Як змінюється довжина геш-функції при зміні вхідних даних?
4. Чи можна відновити дані, коли відома геш-функція?
5. Назвіть вимоги до надійних паролів?
6. Чи змінюється складність злому пароля методом грубої сили при збільшенні довжини пароля?
7. Що таке політика вибору пароля?
8. Назвіть основні типи атак на пароль.
9. Що таке розрахункові таблиці і як вони використовуються для зламу пароля?
10. Від чого залежить стійкість і надійність пароля?
11. Від яких показників залежить кінцевий час взламу пароля методом грубої сили?
12. Яка актуальна мінімально допустима довжина пароля?
13. Які атаки і методи взламу пароля знаєте?
14. Назвіть основні алгоритми обчислення геш-функції?
15. Як змінюється довжина геш-функції при зміні вхідних даних?
16. Чи можна відновити дані, коли відома геш-функція?
17. Назвіть вимоги до надійних паролів?
18. Чи змінюється складність злому пароля методом грубої сили при збільшенні довжини пароля?
19. Що таке політика створення пароля?
20. Назвіть основні типи атак на пароль.
21. Що таке розрахункові таблиці і як вони використовуються для взламу пароля?
22. Від яких показників залежить кінцевий час зламу пароля?
23. Який пароль вважається надійним і захищеним від взламу?

ЛАБОРАТОРНА РОБОТА № 2

Основи кібербезпеки та захисту електронної пошти (E-mail) та інших інформаційних інтернет-сервісів

Мета роботи: вивчення і перевірка надійності та безпеки інформації даних, перевірка інформації, отриманої з мережі Інтернет та інших ресурсів. Опановування основних команд та основних інструментів безпеки при роботі в мережі Інтернет із вебресурсами і сервісами. Вивчення підходів кібергігієни електронної пошти. Навчитись виявляти небезпечну інформацію по E-mail. Зрозуміти концепцію надійних та безпечних даних, безпечної роботи із E-mail.

Необхідні ресурси: ПК або персональний пристрій з доступом до інтернету – ПК (ПЕОМ/АРМ), встановлені операційними системи, інтернет-браузер – ПЗ для роботи в мережі Інтернет (Mozilla Firefox, Google Chrome, Opera, Internet Explorer, EDGE) актуальної версії, персональний пристрій із цими системами і доступом до Інтернету, розширення браузерів: ADB Block Plus, Ghostery, Avast Online Security, AVG Online Security, Microsoft Defender Online Security, WEB Guard Online, VPN-plugins, Antibanner, NoScript та інші; інші окремі модулі ПЗ, що можуть надаватись до лабораторної роботи.

Теоретичні відомості

Ознайомитись із теоретичними відомостями та лекційними матеріалами за темами: «Основи кібербезпеки і кібергігієни при роботі із інформаційними даними та електронною поштою, а також іншими вебсервісами в мережі Інтернет».

Порядок виконання лабораторної роботи

Завдання 1. Вивчення безпеки даних, які передаються по каналу електронної пошти (E-mail).

2.1 Основні правила створення безпечних E-mail і аналіз файлів

2.1. Візьміть тестовий електронний файл для тестування кібербезпеки (можна взяти у викладача) і зробіть прикріплення із записом до електронного листа E-mail як вкладення на довільному поштовому сервісі або використайте свій власний. Краще використовувати сервіси із не дуже високою безпекою E-mail, відмінні від сервісів компанії google.

Можна для тесту взяти базову сигнатуру емулятора (макета) вірусу на вебсайті <https://www.eicar.org/download-anti-malware-testfile/> (download/завантажити) в розділі >>скачати файл (формати: *.exe; *.com; *.txt; *.zip; *.rar).

(!) Даний файл не є шкідливим і НЕ може нанести шкоду вашій інформаційній системі чи ОС ПК, але (!) є «індикатором» функціональності антивірусу (AV) і призначений для його тестування і контролю антивірусних

функцій інформаційних та вебсистем. Реакція існуючого антивірусного захисту (AV) в складі ОС чи MS Windows або Linux або іншої зовнішньої захисної системи на нього може бути відповідно: як на шкідливий файл.

(!) Тому для роботи із ним і подібними навчальними макетами потрібно додавати його у список дозволених програм(список виключень) на ОС Windows чи іншій ОС, або в список дозволених в складі іншого антивірусного захисту.

Також для проведення експерименту можна взяти його пряму сигнатуру:
X5O!P%@AP[4\PZX54(P^)^7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*

І додати в попередньо створений тестивий файл AV TEST *.txt у програмі блокнот (NotPad). Відкрити AV TEST *.txt >> Вставити (Ctrl+V) сигнатуру EI Car >>Зберегти. Для роботи >> додати в список дозволених програм файл AV TEST *.txt в системі антивірусу.

Зробити фіксацію реакції антивірусної системи на цей файл у вигляді скрін-шоту і додати це у звіт разом із аналітичними поясненнями.

2.2 Взяти 3 тестові файли у викладача (*.exe; *.bat; *.com TEST Files) і провести аналогічні дослідження антивірусної безпеки.

2.3 Взяти системи електронної пошти (онлайн або у вигляді ПЗ продукту – наприклад, MS Outlook, поштовий клієнт, Thunderbird , Outlook Express або інший).

2.4 Створити тестовий файл із довільним текстом (до 1000 символів) та додати до листа:

- у вигляді вкладення сигнатури безпосередньо в текст;
- у вигляді прикріплення до самого листа – файлом(файлами).

2.5 Відправити лист та протестувати реакцію поштової системи на нього. Дослідити сам процес передачі файлів у системі електронної пошти та зробити висновки про: пересилку листа без вірусної сигнатури; із нею; із вірусним тестовим файлом; про пересилку між різними потовими сервісами і скриньками (особливо важливо і між різними адресами і різними сервісами). Зробити висновки за результатами проведеного експерименту.

2.6 Аналогічно взяти попередньо надані файли у викладача (*.exe; *.bat; *.com TEST Files) і провести аналогічні дослідження із їх пересилкою через канал електронної пошти. Подивитись реакцію системи безпеки електронної пошти на них і зробити висновки, додати їх із скріншотами у звіт.

2.7 Провести вивчення і дослідження влаштованої системи і налаштувань (опцій безпеки) поштового сервісу E-mail.

Зробіть тестові висновки по зробленому прикріпленню і поведінці антивірусного алгоритму перевірки вкладень в поштовому сервісі.

Увійдіть в обліковий запис і опишіть безпеку в розділі «Налаштування»>Безпека облікового запису»(або аналогічний).

«Налаштування»>Приватність даних

«Налаштування»>Спам-фільтрація і інші окремі вкладення

Результати додайте у звіт у вигляді скріншоту із поясненнями і описом.

Зробити фіксацію результатів і налаштувань безпеки E-mail і у вигляді скрін-шоту і додати це в звіт разом із аналітичними поясненнями.

2.8. Проведіть комплексну перевірку безпеки вашого облікового запису у його налаштуваннях. Матеріали додайте до звіту.

2.9 Відкрийте веб-браузер і перейдіть за посиланням

<https://virustotal.com> – Антивірусний онлайн сервіс.

2.9.1 Оберіть довільне посилання URL для його перевірки. Вставте на командну стрічку у доступному полі на цьому URL ресурсі і перевірте посилання на предмет загроз небезпечної інформації. Наведіть приклади небезпечних посилань (довільно) і результат перевірки за допомогою комплексного аналізу на virustotal.com.

2.9.2 Оберіть файли тестових вірусів (elcar і інші) і додайте для перевірки на ресурсі <https://virustotal.com> в розділі check file

Зробіть відповідні аналітичні висновки.

2.10 Проведіть налаштування E-mail облікового запису і сервісу за допомогою Спам-Фільтрів: Mai IWashe або SpamPal (чи аналогічного). Проведіть роботу і покажіть результати по Спам-фільтрації у обліковому записі E-mail. Наведіть кількість від фільтрованої інформації та даних аналізу.

Завдання 2.

Вивчення автоматизованих інструментів захисту даних і безпеки електронної пошти (E-mail).

2.2 Встановіть один із можливих захисних екранів для E-mail у вигляді плагінів.

2.2.1 Інтернет Браузер >> сервіс E-mail >> Налаштування>> Розширення>>пошук по розширеннях (або Інтернет у магазині онлайн сервіса браузера, у хмарнову сховищі розширень Інтернет) >>AVG WEB Secure та/або Avast Online WEB Secure та/або Spy Hunter WEB security та/або Trellox Endpoint Security Web Controll та/або Microsoft Online Security>> Встановити розширення >> Ввімкнути розширення>> Налаштувати розширення.

2.2.2 Налаштувати встановлені розширення AVG WEB Secure та Avast WEB Secure: Розширення Браузера >> Налаштувати (встановити прапорці доступу і прапорці блокування шкідливих ресурсів, прапорці блокування трекерів аналітики, прапорці реклами, прапорці Cookie-файлів).

2.2.3 Встановити інші варіанти WEB-захисту (WEB Secure) та антиспам захисту для E-mail – аналогічні розширення браузерів: Mcfee WEB security; Mcfee Antispam security, або інші:

2.3 Встановіть розширення Antibanner та NoScript – для блокування файлів і впливаючих вікон й відповідно потенційних загроз у вигляді та/або у впливаючих вікнах.

2.4 Встановіть один із доступних онлайн мережевих екранів – фаєрволів браузера або використайте той, що входить до складу ОС.

Проведіть роботу і перевірте функціональність роботи цього розширення.

Зробіть аналітичні висновки по роботі.

2.4.1 Перевірте і зробіть тести безпеки розширень на базі однієї-двох вірусних тестових посилань (треба знайти довільні 1-2 вірусні посилання) та 1-2 тестових фішингових посилань. Для цього можна взяти тестові посилання URL на файлу і тестового сайту el car test file із URL: чи тестового URL:

<https://www.eicar.org/download-anti-malware-testfile/>
<https://www.kaggle.com/datasets/sid321axn/malicious-urls-dataset>
<https://www.eicar.org/download/eicar-com-2/?wpdmdl=8842&refresh=68d11d81859151758535041> або інший і в тому числі.

2.4.2 Перевірте безпеку Інтернет Браузера (мережевий кран) за допомогою одного із посилань:

[http://www.auditmvpc.com/](http://www.auditmvpc.com;);
<http://www.pcellank.com/test>;
<http://www.hackerwatch.org/probe/>, або аналогічним WEB-сервісом.

Перевірте роботу фаєрволу і розширень і матеріали (результати із скрін-шотами і описом) додайте у звіт.

2.5. Перевірте, чи була ваша електронна скринька зламана. Зробіть комплексну перевірку безпеки вашої електронної скриньки за допомогою сервісу комплексної перевірки безпеки E-mail:

<https://haveibeenpwned.com/>

Зробіть аналітичні висновки і матеріали додайте в звіт.

Завдання 3. Вивчення безпеки WEB сервісів (інтернет-сервісів)

2.3 Взяти довільні 3-4 вебсервіси для проведення експериментів і досліджень. Причому, один із них має бути або вірусним, фішинговим чи тестовим. Для цих довільних 3-х – 4-х WEB сервісів (інтернет-сервісів-WEB сайтів) проведіть:

2.3.1. Тестування на предмет наявних потенційних загроз в них WEB -сервісом безпеки <https://virustotal.com> . Зробіть аналітичні висновки і результати додайте у звіт.

2.3.2 Проведіть тестування і сканування цих 3-х – 4-х WEB ресурсів одним із наявних сканером активності і доступності :
<https://www.host-tracker.com/en> ; <https://www.foxcloud.net/monitoring.php> ;
<https://downdetector.com.ua/> , або аналогічним . Короткі результати із звітів із аналізом додайте у звіт.

2.3.3 Спробувати отримати числові мережеві показники (час затримки пакетів при передачі до інтернет-ресурсу та кількість проміжних стрибків мережі до відповідного інтернет-ресурсу) цих 3-х – 4-х WEB ресурсів командами :

ping **url.com** (або ping **url IP**) ;
tracert **url.com** (або tracert **url IP**) ;

Для запуску цих команд слід використати командний рядок CMD ОС:

Win +R >> cmd [Enter]>>start >>>comand [Enter]

Проаналізувати отримані результати (зробити висновок про доступність, якість зв'язку із цими 3–4-ма вебсервісами). Результати і аналіз додати у звіт із поясненнями.

2.3.4. Потестуйте і проведіть дослідження для цих вебсервісів автоматизованими ПЗ засобами захисту – Online екранами із п.п. 2.2.1 – 2.2.3 (у минулому, 2-му завданні).

2.4. Проаналізувати кіберризики і небезпеки, пов'язані із користуваннями інтернет-сервісами (базові), зокрема при користуванні сервісами при вивантаженні файлів Upload Files, завантаженні файлів Download Files та користуванні торент-мережами й іншими інтернет-сервісами, де вивантажуєте свої дані і файли в мережу Інтернет. Результати додати у звіт роботи з описом та поясненнями.

2.5. Зробити загальні аналітичні висновки по роботі та проаналізувати ризики кіберзагроз, які можуть існувати в каналах електронної пошти (E-mail).

3. Зміст звіту

6.1. Титульний аркуш.

6.2. Тема і мета роботи, необхідні ресурси і короткі теоретичні відомості з лабораторної роботи.

6.3. Вихідні дані для виконання роботи.

6.4. Хід роботи або Порядок виконання роботи.

6.5. Результати виконання роботи із скріншотами та даними.

6.6. Висновки (розгорнуті, аналітичні).

4. Контрольні запитання:

1. Для чого призначений інтернет-сервіс та які показники він має?

2. Назвіть основні функції і особливості інтернет-сервісу, основні його протоколи роботи?

3. В чому особливість використання і призначення електронної пошти як інтернет-сервісу? Яка історія E-mail? (коротко).

3. Як змінюється безпека інтернет-сервісу при збільшенні його функціоналу?

4. Які основні загрози існують при користуванні інтернет-сервісом?

5. Назвіть вимоги до інформації інтернет-сервісу?

6. Критерії достовірності і безпечності інформації та цифрових даних.

7. Засоби перевірки достовірності даних і цілісності даних в Інтернет.

8. Сучасні засоби, підходи та ПЗ для перевірки даних у WEB сервісах.

9. Що таке НЕ достовірна інформація (фейк)? Що таке небезпечна інформація?

10. Способи виявлення недостовірної та небезпечної інформації.

11. Чи змінюється складність виявлення шкідливих даних за допомогою технічних засобів при збільшенні їх кількості?

12. Як змінюється достовірність даних при збільшенні їх кількості?

13. Які програмні засоби контролю безпеки Ви знаєте для вебсервісів?

14. Яка інформація є критичною, важливою та які до неї вимоги?

Лабораторна робота № 3

Основи кібербезпеки і кібергігієни інтернет-браузера та захисту клієнської частини інтернет-сервісів



Мета роботи: опанування основних команд й основних інструментів безпеки при роботі в мережі Інтернет із інтернет-ресурсами і сервісами. Вивчення основних прийомів та технік кібергігієни інтернет-браузера, оволодіння приемами і методами захисту інформації при роботі у глобальній мережі Інтернет.

Необхідні ресурси: ПК (ПЕОМ/АРМ) із доступом до інтернету та встановленими операційними системами браузер роботи в Інтернет (Mozilla Firefox, Google Chrome, Opera, Internet Explorer, EDGE) актуальної версії, персональний пристрій із цими системами і доступом до Інтернету, розширення браузерів: ADB Block Plus, Ghostery, Avast Online Security, AVG Online Security, WEB Guard, VPN-plugins, Antibanner, NoScript та інші; окремі модулі ПЗ, що можуть надаватись до лабораторної роботи.

Теоретичні відомості

Ознайомитись із теоретичними відомостями та лекційними матеріалами за темою «Основи кібербезпеки і кібергігієни при роботі з інформаційними даними в мережі Інтернет та з інтернет-ресурсами у веббраузері».

Порядок виконання роботи

Завдання 1. Основи аналізу трафіку даних і підключень при роботі користувача в мережі Інтернет.

Завдання передбачає вивчення створення надійних з'єднань для систем авторизації інтернет-браузера. Для його виконання потрібно:

1.1. Відкрити інтернет-браузер (Mozilla Firefox, Google Chrome, Opera, EDGE, Internet Explorer) актуальної версії та ввести довільний вебсайт і перейти на нього, натиснувши клавішу Enter або здійснивши відповідні аналогічні дії за допомогою миші, натиснувши клавішу «Перейти». Аналогічно можна проробити на смартфоні або планшетному ПК на базі операційної системи Android або Appstore для мобільних пристроїв на базі iOS або інше хмарне сховище програм для інших мобільних пристроїв із операційними системами.

1.2. Встановити програму моніторингу трафіку мережі, наприклад Network Statistic Traffic View (або TCP IP Connection view, чи аналогічну).

Зайти в інтернет-браузер і в полі пошуку програм і знайти системну програму аналізу трафіку (Network Trafik View, Traffic Monitor, Network connection, PCAP dump) або іншу.

1.3 Встановити і запустити цю програму при відкритому інтернет-браузері. Аналогічно встановити програму моніторингу ресурсів мобільного пристрою із функцією відображення завантаженості процесора.

1.4. Запустити у веббраузері одночасно трафік із 4-8 вкладинок із різнотипним контентом із різних сайтів.

1.5. Запустити системну програму аналізу трафіку із моніторингом трафіку мережі. Провести аналіз трафіку.

1.6 Зафіксувати параметри мережевих з'єднань (в тому числі IP-адреси, протоколи і порти: сокети) і зробити скрін-шоти, які будуть потім використані для звіту. Проаналізувати ці з'єднання і проаналізувати потенційні ризики, які існують при встановленні з'єднань вашого ПК/АРМ із стороннім вебсайтом або вебресурсом і включити цей аналіз у звіт.

1.7 Перевірити ці 4-8 вебсайтів на сайті **virustotal.com** і зробити скрін-шоти із аналізом. Привести приклад небезпечного URL (знайти в мережі Інтернет небезпечний вебресурс і зафіксувати результати перевірки програмним Інтернет вебсервісом **virustotal.com**).

1.8. Запустити системну програму аналізу трафіку із моніторингом трафіку мережі. Провести аналіз трафіку.

1.9. Запустити команду із командного рядка terminal Win+R /cmd>>/netstat. Отримати статистику підключень мережі та проаналізувати активні параметри з'єднань (IP-адреси, протоколи і порти: сокети), які створюють вкладинки інтернет-браузера. Закрити частину вкладинок і залишити 1-2. Зробити аналіз повторно та проаналізувати результати. Результати занести у звіт із аналізом і аналітикою трафіку.

1.10 Закрити всі вкладинки інтернет-браузера, провести аналіз підключень, які залишились. Зробити висновки.

1.11. Повторно запустити активну консоль аналізу статистики мережі: terminal/cmd (Win+R)>>netstat Зафіксувати IP-адреси, протоколи і порти: (сокети); та terminal/cmd >>ipconfig(ifconfig).

Можна виконати цей пункт із іншого пристрою або віртуальної машини. Для цього необхідно попередньо встановити віртуальну машину (Наприклад, Virtual Box, VM Ware) чи запустити спеціальну програму з термінала командного рядка.

1.12. Подивитись активні підключення та їх дані при відвідуванні багатьох сайтів, в т.ч. із сайтами із відеоконтентом, мультимедійним контентом (youtube.com, сайти онлайн-відеоігор). Закрити сайти і зробити повторний моніторинг. Зробити аналітичні висновки. Зробити скріншоти активних з'єднань і записати/зафіксувати дані. Запустити програму аналізу трафіку в режимі реального часу і зробити аналіз систем і найбільш завантаженості каналів і мережі за типами вкладок.

1.13 Визначити статистику завантаженості процесора пристрою за відповідними програмами модуля CPU Monitor або системним монітором [Cntrl+Alt+Del]. Зробити висновки по найбільш критичних і найбільш великих і можливо ризикованих для стабільності ресурсах із точки зору впливу на стабільність і завантаженість роботи системи.

Зробити висновки про паралельність впливу різних процесів на програмно-апаратну платформу інформаційного пристрою (ПК\ноутбук/АРМ).

Зробити висновки про співвідношення обчислювальних ресурсів і кількості активних сеансів зв'язку та/або підпрограм на цій платформі.

1.14. Запустити не менше 10-30 програм/додатків на пристрої ПК/АРМ/ноутбк. За допомогою програми моніторинг ресурсів пристрою визначити завантаженість системи і розхід використання обчислювальних ресурсів (ресурси і завантаженість ЦП, пам'яті, ОЗП, статичної, пам'яті та ін.).

1.15 Встановити програмне забезпечення CCleaner (або аналог із офіційного вебсайту <https://www.ccleaner.com/>) та провести:

- аналіз ресурсів та зокрема пам'яті пристрою (ОЗП, постійна пам'ять);
- провести оптимізацію і очищення сміття (в т.ч. системного) CCleaner;
- провести аналіз системи пристрою (в т.ч. його інших ресурсів) за компонентами: – пам'ять (ОЗП; і статична пам'ять (et-HDD); ресурсів процесора (%-завантаженості); активно-працюючих програм.

Зробити відповідні аналітичні висновки про вплив роботи програм, їх кількості, оптимальності на стабільність і доступність ресурсів системи і ОС.

1.16. Навести приклад небезпечного 1) ПЗ і небезпечних програм; 2) небезпечних URL, які споживають і використовують понад нормово і багато системних ресурсів. Спробувати знайти аналогічні ПЗ і сайти в URL в мережі Інтернет.

(УВАГА!) – НЕ вводити свої РЕАЛЬНІ персональні дані на фішингових чи потенційно-небезпечних ресурсах URL (!).

Проводити тестування активності таких сайтів у тестових вікнах і з включеним VPN.

Провести дії пунктів 1.6–1.9 по цих сайтах.

Подивитись і зробити скріншоти і аналіз трафку мережі.

1.17. Відкрити ресурс **virustotal.com** в інтернет-браузері. Ввести URL(URI) тестового фішингового ресурсу (попередньо знайти), або потенційно-небезпечного ресурсу в строку перевірки на **virustotal.com**. Переглянути аналіз ресурсів і статистику перевірки потенційно небезпечного посилання. Зробити висновки по роботі.

1.18. За допомогою сервісів одного із сервісів:

- <https://www.cloudfox.com/>;
- <https://www.host-tracker.com/en>,

а також утилітами Ping та Whois (із командного рядка) (!) визначити (в базовому вигляді) походження та локацію потенційно небезпечного сайту (URL(URI)). Здійснити моніторинг протягом 1-15 хв цього ресурсу. Дані та графіки з аналітики трафіку зібрати і додати у звіт. Оцінити

стабільність і безпечність ресурсів та здійснити пошук подібних сайтів у мережі Інтернет.

(Сервіс Whois відкривається в браузері безпосередньо через пошук по прямому URL).

Завдання 2. Робота із додатками веббраузерів для збору аналітики інтернет-сервісами.

2.1. Встановити додаток Ghostery веб-браузер Google Chrome.

Браузер>Налаштування > додатки та доповнення > додати із магазину>пошук> Ghostery> Ghostery for Google Chrome.

Виконати базові налаштування, направлені на блокування реклами і роботи систем аналітики ресурсів інтернет-технологій. Запустити додаток в режим блокування аналітики.

2.2. Навести дані аналітики (заблоковані ресурси/трекери/кукі/дані сайтів) для 2-4-х довільно обраних сайтів із першого списку. Скріншоти і матеріали аналізу, дані статистики додати у звіт. Проаналізувати ризики використання такого вебресурсу.

2.3. Встановити додатки Antibanner і ADB Block Plus веббраузер Google Chrome. Браузер>Налаштування > додатки та доповнення > додати із магазину>пошук> ADB Block > ADB Block for Google Chrome. Виконати базові налаштування, направлені на блокування реклами і роботи систем аналітики. Скріншоти і матеріали аналізу, дані статистики додати у звіт.

2.4. Виконати налаштування браузера для інтернет-серфінгу, направлені на блокування відстежування інтернет-технологіями на прикладі Ghrome: Браузер>Налаштування>основні>Аналітика> поставити галочку V-у полі не відстежувати у Google Chrome. Переглянути аналітику даних по попередніх додатках із цією опцією.

Зробити аналітичні висновки за результатами роботи додатків. Появи контекстної та таргетованої реклами і супровідних інформаційних матеріалів, навести і проаналізувати ризики, які несе в собі реклама і рекламні сервіси.

2.5. Навести приклади потенційно небезпечної інформації (контенту) і інтернет-сайту (вебресурсу). Знайти це в інтернет-мережі і показати.

Навести методи і способи нейтралізації потенційних загроз контенту і роботи з такою інформацією за списком. Матеріали занести у звіт.

2.6. Встановити один із сервісів VPN для стаціонарного ПК (і також для мобільного пристрою -smartphone та/або Teblet PC (Планшет)). Для мобільного пристрою: зайти в Playmarket в смартфонах або планшетних ПК на базі операційної системи Android. Appstore – для мобільних пристроїв на базі iOS (iPhone) або інше хмарне сховище – для програм до інших мобільних пристроїв із операційними системами (ОС), відмінними від зазначених.

2.7. У терміналі із мобільного пристрою запустити команду terminal>>Ipconfig(Ifconfig). Зафіксувати IP-адресу вашого пристрою і інших вебсервісів у мережі Інтернет, з якими зараз встановлені зв'язки.

2.7.1. Встановити один із доступних сервісів VPN (із переліку Free VPN) із гарним і високим рейтингом.

2.7.2. Запустити VPN.

2.7.3. У терміналі із мобільного пристрою запустити команду terminal>>Ipconfig(Ifconfig). Зафіксувати IP-адресу вашого пристрою в мережі Інтернет **ІЗ** та **БЕЗ** запущеним сервісом VPN. Зробити аналітичні висновки щодо безпеки роботи VPN і додати скріншоти IP-адрес пристрою.

2.7.4. У випадку потенційної кіберзагрози DoS/DDoS-атаки або зміни швидкого збільшення завантаженості шляхом підключень

Включити/переключити VPN-сервіс і змінити IP-адресу мобільного пристрою/обчислювальної платформи – як спосіб збільшення кіберстійкості до DDoS-атак і превентивії завантажень на мережу.

2.8. Встановити один із сервісів мережевих екранів (FireWall) для стаціонарного ПК або використати вже існуючий (Zone Alarm, Active Firewall, влаштований в ОС Windows чи інший). Для мобільного пристрою – зайти в Playmarket в смартфонах або планшетних ПК на базі операційної системи Android або Appstore для мобільних пристроїв на базі iOS або інше хмарне сховище програм для інших мобільних пристроїв із операційними системами, відмінними від зазначених. Встановити один із доступних мережевих екранів (Firewall app) із функціями відображення підключень по конкретних компонентах операційної системи/додатків. Активувати/запустити встановлений мережевий екран/фаєрвол (Firewall app).

2.8.1. Активувати мережевий екран/фаєрвол і подивитись в налаштуваннях Firewall>>settings>>rules/programs статистику і трафік встановлених мережевих програм (всіх програм в мобільній платформі). Зробити скріншоти і додати їх до звіту з аналізом результатів лабораторної роботи.

Налаштувати заборону доступу для **inbound|outbound** (вхідний/вихідний) трафіку даних всіх програм, крім тих, якими Ви користуєтесь в даний момент для виконання даних програм.

2.8.2. Запустити 2 сервіси одночасно: VPN + Firewall. Це забезпечить максимальний захист від мережевих вторгнень іззовні. Так із потенційних загроз трафіку. Або запустити VPN в складі існуючого Firewall.

2.8.3. Запустити попередньо встановлений монітор онлайн-трафіку в режимі реального часу. Подивитись статистику і зробити скріншоти графіків трафіку мережі при роботі в інтернет-браузері **ІЗ** включеними і налаштованими сервісами VPN + Firewall та попередньо **БЕЗ** них.

2.8.4. Очистити історію веббраузера і супровідні файли cookie даних сайтів перегляду, які Ви відвідували. Це забезпечить видалення слідкуючих cookie-файлів і окремих налаштувань сайту, що можуть відслідковувати ваші дії в інтернеті та провокувати витік персональної інформації.

2.8.4.1 Для цього перейти у Угорі праворуч натисніть значок Історія:

- Якщо адресний рядок унизу вікна, проведіть пальцем від нього вгору, перш ніж натиснути значок.

2.8.4.2 Знайдіть запис, який потрібно видалити.

2.8.4.3 Праворуч натисніть значок.

2.8.4.4 Щоб видалити кілька записів:

1. Натисніть і утримуйте запис.

2. Виберіть інші записи, які потрібно видалити.

3. Угорі праворуч натисніть значок.

Також Ви можете вилучити запис з історії певного сайту на його сторінці.

- Натисніть значок Останнє відвідування Вилучити .

Як видалити ескізи зі сторінки нової вкладки

Щоб переглянути найчастіше відвідувані сайти, відкрийте нову вкладку. Щоб видалити ескіз, натисніть і утримуйте його й виберіть Видалити.

Зробити відповідні висновки.

Завдання 3. Вивчення онлайн-захисту інтернет-браузера від шкідливих URL вебресурсів.

3.1. Встановити один із можливих варіантів захисту/кіберзахисту вебсистеми інтернет-перегляду (McFee; LookBit Web; Internet Sec; E-set) або в складі діючого антивірусного пакету в Trial (пробному) варіанті.

3.2. Встановити два із можливих доступних варіантів плагінів (вебдодатків до інтернет-браузера): Avast Online Security, AVG Online Security, WEB Guard або інший.

3.3. Запустити ці моделі і провести дослідження і коротку статистику даних результатів роботи і тестування 3-5 тестових вебсайтів (в тому числі тестового файлу і тестового сайту el car test file із URL: чи тестового URL:

<https://www.eicar.org/download-anti-malware-testfile/>

<https://www.kaggle.com/datasets/sid321axn/malicious-urls-dataset>

[https://www.eicar.org/download/eicar-com-](https://www.eicar.org/download/eicar-com-2/?wpdmdl=8842&refresh=68d11d81859151758535041)

[2/?wpdmdl=8842&refresh=68d11d81859151758535041](https://www.eicar.org/download/eicar-com-2/?wpdmdl=8842&refresh=68d11d81859151758535041) або інший і в тому числі проведіть тест прямою тестовою вірусною сигнатурою:

X5O!P%#@AP[4PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*) . Можна це зберегти у файли *.txt .

Перевірти файли і URL – безпосередньо затиснувши перемістивши їх курсором в поле інтернет-браузера.

Перевірти файли і URL за допомогою інструментів антивірусного сканування і перегляду інтернет-сторінок із списку. Дані занесіть до табл. 3.1.

Таблиця 3.1 – Основи тестування вебсайтів

Вебсайт	ІРадреса	Тип загрози	Ризики	Результати	Параметри
(URL)		(По резуль.AV)		сканування	URL

3.4. Коротко охарактеризувати результати про потенційні кіберзагрози або потенційного витoku інформації із браузера при роботі із цими

вебресурсами в інтернеті, якщо є, або їх потенційно можливу появу (якщо такий випадок трапляється – навести приклад) в результаті використання інтернет-технологій та інтернет-сервісів.

3.5. Візьміть довільний вебресурс, який передбачає вивантаження файлів (Upload) в мережу Інтернет (File sharing), наприклад: Photoshop Online (Photoshop.com) або Canva (Canva.com) <https://fex.net/> ; <https://www.file.io/> ; <https://www.dropbox.com/> Створіть там простий тестовий акаунт і зафікуйте простий пароль.

3.5.1. Вивантажіть туди тестовий (будь-який!) не важливий *.PDF або *.JPG- файл для тесту (! – файл із НЕ критичною інформацією).

3.5.2. Передайте доступ другу/напарнику по лаб. роботі (або зімітуйте передачу та в т.ч. зімітуйте передачу/перехоплення пароля напарником). Напарник, отримавши файли і пароль, повинен завантажити (Download) цей тестовий *.PDF - файл собі на комп'ютер. Зімітуйте передачу посилання URL вже завантаженого файлу напарнику, щоб він відкрив його на його ж комп'ютері, але в іншій вкладинці/браузері/системі. А також на іншому компютері в одній мережі.

Аналогічно можна протестувати інші вебсервіси для онлайн-обробки даних, де передбачено вивантаження файлів в інтернет.

Зробіть висновки про інформаційну і кібербезпеку при роботі із файлами і даними, які ми вивантажуємо в мережу Інтернет та вебсервіси (особливо малонадійні вебсервіси). Матеріали із скріншотами і аналітикою додати до звіту з лабораторної роботи.

Завдання 4. Налаштування безпеки інтернет-браузера.

4.1. Зайти в налаштування безпеки інтернет-браузера та у налаштування безпеки мережі стаціонарного пристрою ПК (та мобільного пристрою – як додатку до основної роботи) в загальній консолі всіх налаштувань: Settings>>programs>> safety або Settings>> safety (*- може відрізнятись в залежності від моделі моб. пристрою або операційної системи).

4.2. Переглянути налаштування і дозволи, які надаються програмам і опції безпеки відкриття різного вмісту (в т.ч. по вебсайтах і ресурсах та іншого контенту), а також переглянути правила, які встановлюються для інтернет-браузера і мережевих програм на пристрої. Передивитись налаштування по категоріях системних ресурсів.

4.3. Шляхом аналізу (☺) визначити програми і налаштування, які мають потенційні небезпеки відкриття контенту і завантаження файлів, або отримали високі дозволи доступу до ресурсів пристрою або які не є співмірні з їхнім необхідним функціоналом чи по замовчуванню. Зробити висновки по безпеці для цих технологій.

4.4. Проаналізувати програми і налаштування інтернет-браузера, які мають доступ до системних ресурсів (мікрофон, камера, сховище, куки-файли), і до місця розташування (геолокація) і ваших координат геолокації при роботі в мережі Інтернет. Зробити аналіз і проаналізувати ризики,

пов'язані з цими дозволами. Матеріали із скріншотами додати до звіту.

Обмежити доступ всіх не співмірних із необхідним технічним функціоналом програм (шляхом аналізу) до ресурсів пристрою, окрім тих, які передбачені наявними технічними функціями.

Дозволи на ті програми, які Ви не знаєте, або володієте неповною інформацією щодо них або ті, які не використовуються тільки в період використання самого інтернет-сервісу чи браузера для доступу – повинні бути відкликані. Це може призвести до часткової або повної втрати функціоналу обчислювальної платформи / мобільного персонального пристрою. Результати із висновками додати до звіту.

4.5. Провести аудит безпеки мережевих програм на ПК по всіх пунктах системи доступу до прав та інше. Матеріали додати у звіт.

4.6. Встановити (або показати наявний за допомогою скріншота) актуальний антивірусний захист із функцією щоденного оновлення антивірусних баз та функціями аналізу вебінтерфейсів і контролю моніторингу аналізу вебсерфінгу. Матеріали і скріншоти додати до звіту.

5. Зміст звіту

5.1. Титульний аркуш із темою. Мета роботи та необхідні ресурси і теоретичні відомості.

5.2. Вихідні дані для виконання роботи.

5.3. Результати виконання роботи (схема, таблиці істинності та графіки) із описом та аналізом по кожному пункту.

5.4. Висновки

6. Контрольні запитання (для самопідготовки і у звіті з лабораторної роботи НЕ наводяться)

1. Що таке кібергігієна і кібербезпека інтернет-браузера?
2. Що таке ШПЗ? Що таке ризики і їх різновиди для інтернет-сервісів?
3. Що таке інтернет-сервіс?
4. Що таке фішингове і шкідливе URL посилання? Шкідливий URL?
5. Що таке куки-файли (cookie) та які ризики вони несуть?
6. Як провести моніторинг мережі і підключень активними командами із командного рядка (Windows) чи Terminal (Linux) та ПЗ модулями?
7. Які загрози є в глобальній мережі Інтернет?
8. Які заходи кібергігієни і кібербезпеки потрібні для боротьби із ними?
9. Які ризики несе робота в мережі Інтернет? Як уберегтись користувачу?
10. Які розширення та інструменти інтернет-браузера дозволяють запобігти витокам та ризикам кіберзагроз?
11. Які заходи можна вжити для зменшення ризиків кіберзагроз безпеки користувача при роботі із інтернет-сервісами?
12. Основи безпеки при роботі із інтернет-браузером?
13. Які кіберзагрози існують у сучасній мережі Інтернет?

Лабораторна робота № 4.

Кібербезпека робочого місця користувача із ПК/АРМ із виходом у мережу Інтернет



Мета роботи: опанування основних базових практик і основних інструментів безпеки робочого місця ПК та/або АРМ при роботі в мережі Інтернет: із інтернет-ресурсами і сервісами. Вивчення основних прийомів та технік кібербезпеки на ПК/ноутбук та/або АРМ, оволодіння прийомами і методами захисту інформації при роботі на ПК та/або АРМ у глобальній мережі Інтернет.

Необхідні ресурси: ПК (ПЕОМ/АРМ) із доступом до Інтернет та встановленими операційними системами базового антивірусного захисту браузером інтернет, розширення браузерів: ADB Block Plus, Ghostery, Avast Online Security, AVG Online Security, WEB Guard, Antibanner, NoScript, Https Everywhere та інших; окремі модулі ПЗ (ПЗ модулі для роботи із технологіями: DNS, FTP, TCP), що можуть надаватись до лабораторної роботи.

Теоретичні відомості

Ознайомитись із теоретичними відомостями та лекційними матеріалами за темами: «Основи кібербезпеки і кібергігієни робочого місця ПК та/або АРМ при роботі в мережі Інтернет». Ознайомитись із основними принципами і структурою комп'ютерних систем та мереж.

Робота із DNS сервісами і клієнтами.

1. Інформація: DNS-клієнт (від англ. Domain Name System-client – програма або бібліотечна функція, призначена для надсилення запитів до DNS-серверів, таких, як визначення IP-адреси за іменем хоста, або зворотних запитів (доменні імена за вказаною IP-адресою). У операційних системах MS Windows присутня служба DNS client, призначена для локального кешування DNS-запитів. Вміст кешу можна переглянути командою `ipconfig /displaydns`. Спеціалізовані програми Для діагностики DNS використовуються спеціальні програми – nslookup и dig. Версія nslookup для Windows підтримує WINS, що може створювати плутанину у випадках, коли відповіді DNS і WINS серверів відрізняються. Окремі версії nslookup для Unix-подібних систем підтримують також і Network Information Service, що теж може ускладнювати діагностику.

Приклади роботи програми dig: dig – утиліта Unix-систем, що надає користувачеві інтерфейс командного рядка для звернення до системи DNS (DNS-клієнт). Dig англійською значить «копати», але формально – це скорочення від «domain information groper». Дозволяє задавати різні типи запитів і запитувати довільно вказувані сервера. Має більше можливостей, ніж подібна утиліта nslookup. Якщо в аргументах не вказано DNS-сервер, то буде використано перший сервер з файлу /etc/resolv.conf.

Прямий запит (Приклад)

```
$ dig google.com.ua aaaa ;; global options: +cmd ;;
Got answer: ->>HEADER<<- opcode:
QUERY, status: NOERROR, id: 2129 ;; flags: qr rd ra;
QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1 ;;
ANSWER SECTION: google.com.ua. 300 IN AAAA2a00:1450:4001:815::2003
```

Зворотній запит:

```
$ dig -x 2a00:1450:4001:815::2003 ;; global options: +cmd ;;
Got answer: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17643 ;;
flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1 ;;
ANSWER SECTION:
3.0.0.2.0.0.0.0.0.0.0.0.0.0.0.0.0.5.1.8.0.1.0.0.4.0.5.4.1.0.0.a.2.ip6.arpa. 69749 IN
PTR fra15s12- in-x03.1e100.net.
```

У наведеному прикладі видно, що доменні імена у прямому і зворотному запиті не збігаються, хоча IP-адреса одна й та сама.

2. Приклади використання. В даному випадку ми опитуємо A-запис для домену wikipedia.org з першого доступного 1 сервера DNS:

```
# dig wikipedia.org A ; <<>> DiG 9.2.4 <<>> wikipedia.org a ;; global options:
printcmd ;; Got answer: ;; ->>HEADER<<- opcode:
QUERY, status: NOERROR, id: 30077 ;; flags: qr rd ra;
QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0 ;;
QUESTION SECTION: ;wikipedia.org. IN A ;;
ANSWER SECTION: wikipedia.org. 1724 IN A 208.80.152.2 ;; Query time: 14
msec ;; SERVER: 80.91.160.9#53(80.91.160.9) ;;
WHEN: Sun Aug 2 09:21:38 2009 ;; MSG SIZE rcvd: 47
```

Зараз ми опитуємо сервер DNS для домену wikipedia.org. По даній інформації можна побачити, що домен підтримується 3-ма серверами DNS (ns2.wikimedia.org, ns0.wikimedia.org, ns1.wikimedia.org):

```
# dig wikipedia.org NS ; <<>> DiG 9.2.4 <<>> wikipedia.org NS ;; global
options: printcmd ;; Got answer: ;; ->>HEADER<<- opcode:
QUERY, status: NOERROR, id: 6460 ;; flags: qr rd ra; QUERY: 1,
ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3 ;;
QUESTION SECTION: ;wikipedia.org. IN NS ;;
ANSWER SECTION: wikipedia.org. 79965 IN NS ns2.wikimedia.org.
wikipedia.org. 79965 IN NS ns0.wikimedia.org. wikipedia.org. 79965 IN NS
ns1.wikimedia.org. ;;
```

ADDITIONAL SECTION: ns0.wikimedia.org. 79965 IN A 208.80.152.130
ns2.wikimedia.org. 79965 IN A 91.198.174.4 ns1.wikimedia.org. 79965 IN A
208.80.152.142 ;; Query time: 0 msec ;;
SERVER: 80.91.160.9#53(80.91.160.9) ;; WHEN: Sun Aug 2 09:27:28 2009 ;;
MSG SIZE rcvd: 143

Наступний синтаксис команди дасть інформацію про MX-запис, який
віддає сервер DNS ns0.wikimedia.org:

```
2 dig wikipedia.org @ns0.wikimedia.org mx ; <<>> DiG 9.2.4 <<>>
wikipedia.org @ns0.wikimedia.org mx ; (1 server found) ;; global options:
printcmd ;; Got answer: ;; ->>HEADER<<- opcode:
QUERY, status: NOERROR, id: 6361 ;; flags: qr aa rd; QUERY: 1,
ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2 ;;
QUESTION SECTION: ;wikipedia.org. IN MX ;; ANSWER SECTION:
wikipedia.org. 3600 IN MX 10 mchenry.wikimedia.org. wikipedia.org. 3600 IN
MX 50 lists.wikimedia.org. ;;
ADDITIONAL SECTION: mchenry.wikimedia.org. 3600 IN A 208.80.152.186
lists.wikimedia.org. 3600 IN A 91.198.174.5 ;; Query time: 176 msec ;;
SERVER: 208.80.152.130#53(208.80.152.130) ;; WHEN: Sun Aug 2 09:32:52
2009 ;; MSG SIZE rcvd: 119
```

Приклади роботи програми nslookup nslookup (англ. name server
lookup пошук на сервері імен) – утиліта, що надає користувачеві інтерфейс
командного рядка для звернення до системи DNS. Дозволяє задавати різні
типи запитів і опитувати довільно вказані сервери. Її аналогом є утиліти
host і dig. Розроблена у складі пакету BIND (для UNIX-систем). Утиліта
адаптована для Windows безпосередньо фірмою Microsoft і йде в комплекті
з операційною системою. nslookup працює в інтерактивному або
неінтерактивному режимі. Приклад неінтерактивного режиму \$ nslookup
wikipedia.org Server:

```
192.168.1.2 Address: 192.168.1.2#53 Non-authoritative answer:
Name: wikipedia.org Address: 208.80.152.2
```

Приклад інтерактивного режиму nslookup > server 1.1.1.1

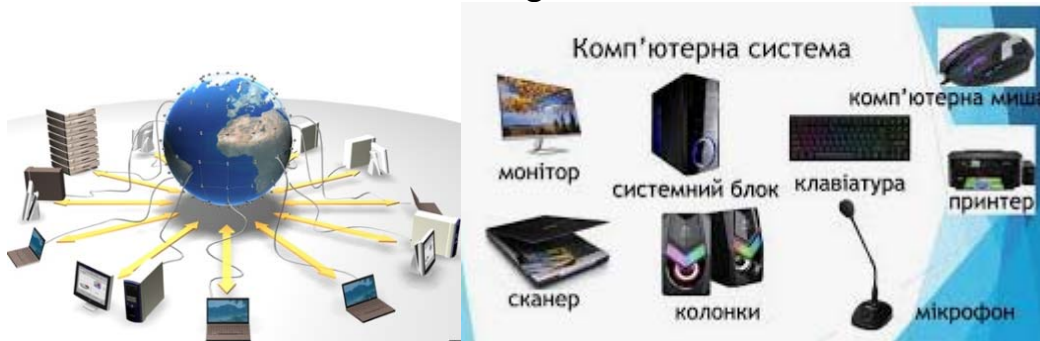
```
Default server: 1.1.1.1 3 Address: 1.1.1.1#53 > wikipedia.org Server: 1.1.1.1
Address: 1.1.1.1#53 Non-authoritative answer: Name: wikipedia.org Address:
91.198.174.192
```

В інтерактивному режимі можливо легко порівнювати відповіді
різних серверів, наприклад, після оновлення інформації про домен (зони).
Для цього спочатку перевіряємо який сервер зараз налаштовано, потім
перемикаємо на інший сервер та запитуємо інший сервер. Приклад
перевірки відповіді різних DNS серверів nslookup > server Default server:

```
127.0.0.1 Address: 127.0.0.1#53 > server 1.1.1.1 Default server: 1.1.1.1
Address: 1.1.1.1#53 > wikipedia.org Server: 1.1.1.1 Address: 1.1.1.1#53 Non-
authoritative answer: Name: wikipedia.org Address: 91.198.174.192 > server
8.8.8.8 Default server: 8.8.8.8 Address: 8.8.8.8#53 > wikipedia.org Server:
```

8.8.8.8 Address: 8.8.8.8#53 Non-authoritative answer: Name: wikipedia.org
Address: 91.198.174.192

Приклад як запитати про MX (mail exchange) запис в інтерактивному режимі nslookup > set q=MX > wikipedia.org Server: 10.1.0.252 Address: 10.1.0.252#53 Non-authoritative answer: wikipedia.org mail exchanger = 10 mx1001.wikimedia.org. 4 wikipedia.org mail exchanger = 50 mx2001.wikimedia.org. Authoritative answers can be found from: mx1001.wikimedia.org internet address = 208.80.154.76 mx1001.wikimedia.org has AAAA address 2620::861:3:208:80:154:76 mx2001.wikimedia.org internet address = 208.80.153.45 mx2001.wikimedia.org has AAAA address 2620::860:2:208:80:153:45



Структура базової комп'ютерної системи



Структура базової комп'ютерної мережі

Порядок виконання лабораторної роботи

Завдання 1.

1. Встановити і випробувати захист ОС АРМ та/або ПК(ноутбук).

1.1. Встановити систему антивірусного захисту або скористатись існуючою в складі ОС. Налаштувати параметри сканування. Встановити планове сканування. Вибрати >> сканувати всю систему і запустити сканування.

1.2 Встановити параметри антивірусного сканування в реальному часі в системі антивірусного захисту >> моніторинг і сканування і дослідження трафіку в системі реального часу (або аналогічне по назві і суті). Antivirus Traffic Monitor >> Active Scan in real time || – >> Active Scan Network connection. Також вибрати >> Antivirus Net Analyzer >> Старт. Запустити її і в режимі реального часу подивитись результати і опрацювання програми, а також споживання передачу/прийом подій в мережі за різними типами запущених і встановлених програм. Результати у вигляді скріншотів додати у звіт.

1.3. Запустити програму аналізу даних активних загроз AV Util , AV Scan Util(module) та Trojan Remover або Dr.WEB Cure It (із ліцензією у пробному та/або режимі trial) і провести сканування і моніторинг загроз і дослідити передачу в системі.

1.4. Провести аналіз і сканування тестових файлів антивірусних програм (надаються викладачем та/або надавались у минулих лаб. роботах) із запуском більшості встановлених програмних модулів аналогічними системами. Провести сканування штатними антивірусними засобами цих файлів (тестові вірусні файли і програми 3-4шт.). Аналіз із результатом додати у звіт.

1.5. Провести аналіз встановлених програм на вашому ПК/АРМ і визначити найбільш ризикові програми, по параметрах споживання максимального трафіку (особливо якщо вони працюють у фоні).

1.6. Налаштувати утиліту AV Util , AV Scan Util, або Dr.WEB Cure It або Trojan Remover (або аналогічний модуль сканування) із покращеними показниками виявлення ШПЗ та евристики і аналізу провести сканування і моніторинг загроз. Результати із аналізом додати у звіт.

1.7. Встановити і запустити програму мережевого екрану (Firewall) або використати існуючу в складі ОС (наприклад, браундмауер MS Windows) і налаштувати правила передачі трафіку для встановлених програм і програмних модулів. Провести аналіз даних активних загроз від програм і їх з'єднань до мережі Інтернет. Результати із аналізом додати у звіт.



Умовна будова глобальної мережі

Завдання 2.

2.1 Здійснити запуск активного моніторингу трафіку. Запустити програму активного моніторингу (мережевий сніфер Network Traffic Analyzer або IP/TCP Connection(Problem) View) і дослідження трафіку в системі реального часу для ПК та подивитись трафік за категоріями від різних програм і різного типу контенту. Подивитись рух пакетів і протоколи даних програм та інші дані по запуску аналізу і моніторингу

вмісту. Відкрити веббраузер і запустити довільні 2-3 сайти із підтримкою незахищеного http (НЕ https) протоколу по порту 80. Налаштувати програму активного моніторингу (сніфер) на прослуховування цього порту даного ресурсу із моніторингом вводу даних на сайт в текстовому форматі для користувача. Зробити висновки про роботу програм і їх оригінальність. Матеріали додати у звіт.



2.2 Відкрити і провести дослідження параметрів інтернет-ресурсів (3-4 довільні вебсайти) за допомогою програм:

- DNS Bench;
- DNS Inform та/або DNS Monitor;
- DnsJumper Dns Monitor ;
- Online Web-сервісу Who Is;
- FTP Use та/або FTP View(або інший модуль роботи із FTP) ;
- інших програм для аналізу вебсайтів.

2.2.1.Додатково до завдання роботи із DNS провести тестування команд dig або nslookup із терміналу або із командного рядка ОС Linux або Windows для 3-4 довільних інтернет-сайтів в різних режимах із отриманням додаткової інформації.

2.2.2. Проаналізувати і додати ці дані із описом і скріншотами у звіт по лаб. роботі № 4. 4.2.3.д. Встановити додаток DNS Client for Android (DNS Client for iOS) на мобільний пристрій (смартфон) із хмарного сховища AppStore(Playmarket). <https://play.google.com/store/apps/details?id=androdns.android.leetdreams.ch.androdns&hl=ru&pli=1>

Виконати завдання по п.п.2.2.1. і 2.2.2 для сайту localhost та google.com. Висновки і результати із аналізом додати до звіту з лабораторної роботи № 4.

Зробити висновки про безпеку інформації від онлайн-вебресурсів. Матеріали із скріншотами додати в звіт. Проаналізувати базові ризики для інтернет-ресурсів і відповідно від інтернет-ресурсів для ПК/АРМ користувача, що їх використовує.

2.3 Відкрити списки встановлених програм на ПК (або ноутбукі): Пуск >>Налаштування>>Програми і компоненти. Переглянути списки встановлених програм і наявність цих програм у меню пуск у операційній системі (ОС) Windows або аналогічно у Linux. Передивитись наявність цих

програм і їх функціонал у інших областях ОС, додаткові меню, вкладення, інше. Переглянути політики і опис цих програм. У випадку, якщо програми не виконують свій функціонал, не відповідають заявленим характеристикам, не запускаються, або мають сумнівні функції, потрібно видалити ці програми і програмні модулі (попередньо передивитись і повторно перевіривши їх оригінальність і справжність і перечитавши документацію і опис цього ПЗ). Непідтверджені або сумнівні програми можуть бути шкідливими. Зробити висновки про встановлені програми.

2.4 Для цих 3-4 довільних файлів (один із яких потрібно, щоб був вірусним, тестовим) провести дослідження на ресурсі: virustotal.com. Результати із аналізом про безпеку та скріншотами додати у звіт.

Завдання 3.

3.1. Відкрити списки встановлених програм (додатків) на пристрої: Налаштування >> Програми і компоненти>>Список програм/додатків. Переглянути списки цих встановлених програм і перевірити наявність цих програм на робочому столі. Перевірити дозволи і ресурси, які вони займають, і які критичні дозволи надані цим додатком/програмам, зайшовши у меню Налаштування (натиснувши на програму) >> спец. налаштування >>дозволи. Якщо у випадку, якщо програма не відомий (!) і не є системою програмою і має перевищені дозволи, або не працює , не відкривається, чи виконує свої функції не вірно (чи взагалі не виконує) – потрібно видалити цю програму. Зробити висновки по роботі таких програм.

Передивитись повторно наявність цих програм і їх функціонал у інших областях ОС Android (Apple ОС), додаткові меню, вкладення програм, інше. Якщо виявлено аномальну поведінку додатка чи іраціональні/неадекватні дозволи – також потрібно ретельно переглянути його. Перевірити оригінальність додатка/програми, його розробника і ліцензійні умови. Переглянути політики і опис цих програм/додатків. У випадку, якщо додатки/програми не виконують свій функціонал, не відповідають заявленим характеристикам, не запускаються, або мають сумнівні функції, походження, сумнівного постачальника/розробника, потрібно видалити ці програми і програмні модулі (попередньо передивитись і повторно перевіривши їх оригінальність і справжність та перечитавши документацію і опис цього ПЗ. Непідтверджені додатки, програми можуть мати шкідливі функції і бути ШПЗ (шкідливим програмним забезпеченням).

3.2 У інтернет-браузері, що встановлений у вашому ПК/АРМ/ноутбучі, встановити розширення:

- No Script;
- Https Everywhere.

Провести дослідження і вивчення роботи 3-4 довільних вебсайтів (вебресурсів) із цими розширеннями і зробити висновки про безпеку роботи вебсайтів та їх відкриття на ПК/АРМ.

3.3 Взяти довільний вебсайт (для тесту) із підтримкою тільки Http протоколу. Для цього можна скористатись пошуком в мережі Інтернет. І спробувати запустити цей сайт у браузері інтернет на вашому ПК/АРМ: 1) із розширенням Hhttps Everywhere ; 2) без розширення Hhttps Everywhere . Зробити висновки про безпеку роботи із таким вебсайтом і результати із скріншотами і висновками додати в звіт.

4. Зміст звіту

4.1. Титульний аркуш із темою. Мета роботи та необхідні ресурси і теоретичні відомості (коротко, 1-3 сторінки А4).

4.2. Вихідні дані для виконання роботи.

4.3. Результати виконання роботи (схема, таблиці, графіки і скріншоти) із описом, поясненнями та аналізом по кожному пункту.

4.4. Висновки.

5. Контрольні запитання (для самопідготовки і у звіті з лабораторної роботи **НЕ** наводяться)

1.Що таке кібергігієна і кібербезпека АРМ/ПК на робочому місці користувача?

2. Що таке ШПЗ? Що таке ризики і їх різновиди для інтернет-сервісів?

3. Що таке інтернет-сервіс?

4. Що таке фішингове і шкідливе URL посилання? Шкідливий URL?

5. Що таке шкідливі файли, які ризики вони несуть і які бувають?

6. Як провести моніторинг мережі і підключень вебресурсів ПЗ модулями?

7. Які загрози є для АРМ\ПК із підключенням до глобальної мережі Інтернет?

8. Які заходи кібергігієни і кібербезпеки потрібні для захисту ПК/АРМ?

9. Які ризики несе робота в мережі Інтернет? Як уберегтись користувачу?

10. Які розширення та інструменти ПЗ дозволяють запобігти витокам та ризикам кіберзагроз для АРМ/ПК на робочому місці користувача?

11. Які заходи можна вжити для зменшення ризиків кіберзагроз безпеки користувача при роботі із інтернет-сервісами?

12. Основи безпеки при роботі із інтернет-браузером?

13. Які кіберзагрози взагалі існують у сучасній мережі Інтернет в кіберпросторі?

ЛАБОРАТОРНА РОБОТА № 5

Основи кібербезпеки месенджерів та засобів спілкування на інтернет-ресурсах



Мета роботи: опановування кібергігієни при роботі із даними і технологіями в месенджерах для забезпечення приватного спілкування. Зрозуміти концепцію безпечних даних у месенджерах і чатах соціальних мереж і надійності процесів операційних систем.

Необхідні ресурси: ПК (ПЕОМ) або ноутбук із доступом до мережі Інтернет та встановленими операційними системами та месенджерами; або персональний пристрій із цими системами і доступом до інтернету; встановлені застосунки месенджерів на мобільний пристрій і ПК: Viber, Telegram, Signal, Messenger, WhatsApp, FB messenger, тощо; модулі програмного забезпечення (ПЗ), які надаються викладачем для проведення експерименту.

Теоретичні відомості

Ознайомитись із теоретичними відомостями та лекційними матеріалами за темами: «Кібербезпека та кібергігієна месенджерів та засобів спілкування, а також при транспорті інформаційних даних»; «Основи кібербезпеки каналів передачі даних та інтернет-сервісів».

Порядок виконання роботи

5.1. Встановити один із можливих варіантів захисту вебресурсів / кіберзахисту вебсистеми інтернет-перегляду (McFee; LookBit Web; Internet Sec; E-set) або в складі діючого антивірусного пакету в Trial (пробному) варіанті. Провести дослідження і коротку статистику даних кіберзахисту ПК та/або ноутбука при перегляді результатів інтернет-сторінок та при відкритих месенджерах чи аналогічних чатів відповідних соціальних мереж (Fb, Telegram, Instagram).

5.2 Провести експеримент із пересилки тестових вірусних файлів (емуляторів Test AV Files): 2-3файли по каналах соціальних мереж чи месенджерах:

- Viber;
- Telegram;

- Signal;
- FB messenger;
- Signal;
- Discord
- інший месенджер.

Мінімум 3 різні довільні месенджери.

Встановити десктопну (desktop) версію застосунку для ПК для цих месенджерів (наприклад, Viber Desktop) і для 2-х окремих месенджерів провести експеримент із залученням цієї десктопної версії ПЗ застосунку месенджера (наприклад, Viber Desktop) по пересилці вірусних емуляторів (навчальних екземплярів ПЗ). При включеному антивірусному захисті із контролем каналів цих месенджерів (або чатів соц. мереж). Також провести тестування при пересиланні цих файлів штатними засобами захисту в складі месенджерів та чатів соц. мереж. Результати занести у звіт із аналізом і описом.

5.3. Провести аналогічне дослідження по пересилці шкідливих і фішингових URL (тестових URL) месенджерами та чатами соц. мереж. Для тестування можна взяти 2-3 тестових вебсайтів (в тому числі тестовий файл (чи сигнатуру еі car) і тестовий сайту URL:

<https://www.eicar.org/download-anti-malware-testfile/> ;

<http://maliciouswebsitesetest.com/> ;

<https://www.kaggle.com/datasets/sid321axn/malicious-urls-dataset>

<https://www.eicar.org/download/eicar-com-2/?wpdmdl=8842&refresh=68d11d81859151758535041;>

<https://www.webpagetest.org/> ;

один із набору URL із переліку на: <https://caniphish.com/free-phishing-test/phishing-website-templates>, або інший.

5.4 В тому числі проведіть тест прямою тестовою вірусної сигнатури еі car:

X5O!P%@AP[4PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H* . Можна її зберегти в файлі *.txt .

Перевірити все це(в т.ч. приклади шкідливих URL) на сайтах:

<https://virustotal.com>;

<https://skysnag.com/phishing-check/>;

<https://www.phishingbox.com/phishing-test>;

<https://checkphish.bolster.ai/>

та антивірусних засобів у п.п.5.1 .

Перевірти файли і URL за допомогою інструментів антивірусного сканування і перегляду Інтернет сторінок із списку. Дані занесіть до

Таблиця 5.1 – Основи тестування вебсайтів

Вебсайт	ІРадреса	Тип загрози	Ризики	Результати	Параметри
(URL)		(По резуль.АV)		сканування	URL
файл		(По резуль.АV)		сканування	URL

5.5 Коротко охарактеризувати результати про потенційні кіберзагрози або потенційного витоку інформації із месенджерів (чатів соц. мереж) при роботі із цими вебресурсами у інтернеті, якщо є, або їх потенційно можливу появу (якщо такий випадок трапляється у лабораторній роботі – навести приклад із зазначенням*) в результаті використання інтернет-технологій.

5.6. Взяти один довільний месенджер для спілкування (Telegram, Facebook, Whatsapp, Viber, Diskord, Telegram, Signal) і встановити один із можливих варіантів захисту / кіберзахисту на нього (P2TP, L2TP, IP Sec Encryption) та налаштувати його інтерфейс. Або включити ці опції в налаштуваннях цього месенджера (чату) і навести в лабораторній роботі у вигляді скріншотів із описом.

5.7 Відправити листи довільного вмісту своєму партнерові по роботі або собі через вебсистему інтернет. Впевнитись у надійності джерел.

5.8 Створити аналогічні акаунти в цих месенджерах, схожі за нікнеймом/логіном на оригінальні акаунти партнера. А також схожим зображенням із нього (із оригіналу). Відправити лист на цей дублюючий "тестовий фішинговий" акаунт чи на акаунт товариша/партнера по роботі. Це імітація фішингового акаунту в месенджерах. Впевнитись у надійності і визначити ознаки, за якими можна розрізнити оригінал від копії акаунти, на які були відправлені листи. Навести їх у роботі з описом і аналізом. Зробити висновки по цьому пункту.

5.9 Відправити тестовий варіант прикріпленого емулятора вірусного файлу оригіналу адресанту-«двійнику» (дублюючий акаунт або собі), прикріпивши це вкладення/прикріплення. Подивитись реакцію антивірусного захисту (локального на ОС і в складі месенджерів) і зробити висновки по цьому пункту лабораторній роботі.

5.10. Продемонструвати можливості витоку інформації особистого спілкування й інформації шляхом імітації НСД (несанкціонованого доступу, із зазначенням точок і місць реалізації доступу до акаунту), що додається у прикріпленнях у демонстраційному режимі. Зробити висновки із додаванням скріншотів результатів.

5.11. Організувати і налаштувати правила і налаштування безпечного спілкування і передачі інформації у цих месенджерах. Зробити аудит налаштувань месенджерів і по максимуму включити захист: 2FA/MFA; шифрування P-to-P(P2P) encryption; security; authority; privacy та ін. Налаштування, результати із скріншотами привести в звіт.

5.12. Написати 3-4 пункти політики кібергігієни при спілкуванні і передачі інформації у приватних чатах соц. мереж і месенджерах. Матеріали додати до звіту.

5.12. Протестувати процеси блокування посилань URL месенджерів і визначення цілісності цих посилань програмами:

- Broken Link Detector;
- URL Disabler;
- URL Checker.

Зробити висновки і включити матеріали у звіт.

6. Зміст звіту

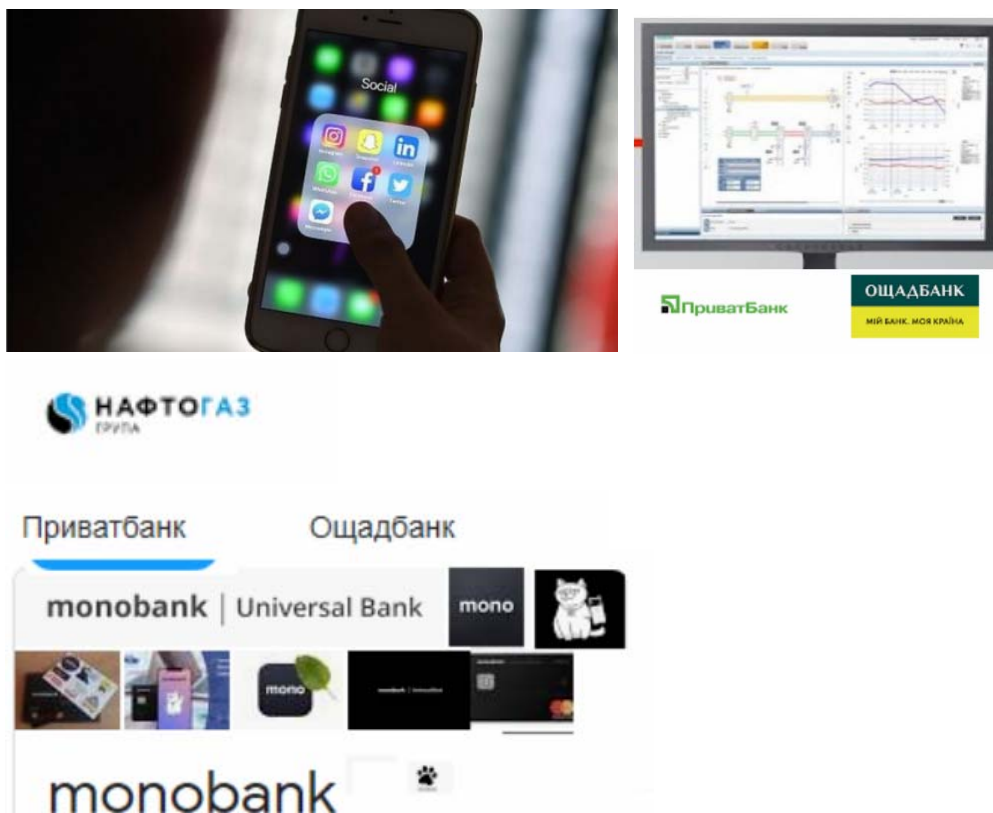
1. Тема і мета роботи.
2. Вихідні дані для виконання роботи.
3. Результати виконання роботи (схема, таблиці істинності та часові діаграми).
4. Висновки.

7. Контрольні запитання (для самопідготовки, до звіту з лабораторної роботи відповіді на них включати НЕ потрібно!)

1. Сучасні методи, підходи та програмне забезпечення для перевірки цілісності та кібербезпеки даних.
2. Що таке НЕ достовірні та достовірні інформації в месенджерах?
3. Способи виявлення та ознаки потенційно небезпечної і шкідливої інформації у месенджерах і чатах.
4. Що таке дані інтернет-аналітики і як вони проявляються в месенджерах?
5. Що таке основи політики і менеджменту ризиків у виборі політики безпеки у месенджерах?
6. Які способи підвищення кіберзахисту та кібергігієни месенджерів на ПК і ПЗ та моб. пристрої при використанні сучасних інтернет-технологій Ви знаєте?
7. Базові способи перевірки кіберзахисту даних та виявлення небезпечного контенту.
8. Базові способи перевірки кіберзахисту даних у месенджерах та середовищах спілкування та підходи виявлення небезпечного контенту.
9. Основні ризики і витoki даних у месенджерах та середовищах спілкування.
10. Основні правила кібергігієни месенджерів та середовищ спілкування.
11. Що треба зробити, щоб підвищити безпеку месенджерів та середовищ спілкування?
12. Основні ризики та кіберзагрози при спілкуванні у месенджерах та середовищах передачі повідомлень та іншої інформації.
13. Основи захисту приватності у месенджерах та середовищах спілкування.
14. Кібербезпека месенджерів, чатів та середовищ спілкування.
15. Базові технології і практики кіберзахисту даних у месенджерах, чатах та інших середовищах спілкування.

ЛАБОРАТОРНА РОБОТА № 6

Базові техніки кібербезпеки і кібергігієни при роботі із банківськими та іншими інтернет-сервісами



Мета роботи: опановування основних прийомів автоматизованого доступу до даних, програмами доступу. Вивчення основних прийомів кібергігієни роботи із банківською та економічною інформацією, приватною інформацією при роботі в мережі Інтернет і перегляді вебсторінок.

Необхідні ресурси: ПК (ПЕОМ) із доступом до мережі Інтернет та встановленими операційними системами Windows та/або Linux; мобільний персональний пристрій із мобільними операційними системами і доступом до інтернету; зразок банківської карти (!! НЕ оригінальної)); створені тестові (! НЕ оригінальні) криптогаманці; встановлені застосунки месенджерів на мобільний пристрій і ПК: Viber, Telegram, Signal, Messenger, WhatsApp, FB messenger, тощо; модулі програмного забезпечення (ПЗ), які надаються викладачем для проведення експерименту.

Теоретичні відомості

Ознайомитись із теоретичними відомостями та лекційними матеріалами за темами: «Кібергігієна при роботі із банківською і приватною інформацією», «Кібергігієна автоматизованого робочого місця (АРМ) оператора» та «Кібергігієна і кібербезпека інтернет-браузера».

Порядок виконання роботи

Завдання 1.

1.1. Встановити один із можливих варіантів захисту / кіберзахисту вебсистеми інтернет-перегляду (McFee; LookBit Web; Internet Sec; E-set) або в складі діючого антивірусного пакету в Trial (пробному) варіанті.

1.2. Робота із додатками захисту веббраузера від інформаційних втручань та попередження збору даних аналітики інтернет-сервісами:

1.2.1. Встановити захист на веббраузер для безпечної роботи із мережею Інтернет.

1.2.2. Встановити додаток Ghostery веббраузер Google Chrome(Mozilla Firefox). Для цього потрібно зайти Браузер>Налаштування > додатки та/або розширення (доповнення) > додати із Вебмагазину>пошук по назві> Ghostery> Ghostery for Google Chrome (Mozilla Firefox).

Виконати базові налаштування додатка, направлені на блокування реклами, трекінгу (відслідковування) і роботи систем аналітики ресурсів інтернет-технологій. Запустити додаток в режим блокування аналітики. Дослідити 2-3 банківські сайти та 2-3 криптогаманці (головна сторінка) та вставити матеріали із описом у звіт.

1.2.3. Встановити додаток ADB Block Plus веббраузер Google Chrome(Mozilla Firefox).

1.2.4. Встановити один із можливих варіантів захисту Microsoft Defender Online Browser Security Avast WEB Secure / AVG WEB Secure Online / Malewarebytes security Online / Online WebShield для кіберзахисту вебсистеми інтернет-браузера. Для безпечного перегляду інтернет-ресурсів та запобіганню фішингу.

Також можливий один із наступних додатків: McFee Online; LookBit Web Online; E-set Internet Security; E-set Internet Safety або інший) або в складі діючого антивірусного пакету в Trial (пробному) варіанті.

1.2.5. Виконати налаштування браузера для інтернет-серфінгу, направлені на блокування відстежування інтернет-технологіями.

1.2.6. Браузер>Налаштування > додатки та доповнення > додати із магазину>пошук> ADB Block > ADB Block for Google Chrome. Виконати базові налаштування, направлені на блокування реклами і роботи систем аналітики. Скріншоти і матеріали, які це підтверджують, потрібно додати у звіт, а також дані аналізу та майбутні дані статистики додати у звіт.

1.3. Виконати налаштування браузера для інтернет-перегляду, направлені на блокування відстежування інтернет-технологіями. Браузер>Налаштування>основні>Аналітика> поставити галочку V-у полі не відстежувати у Google Chrome. Переглянути аналітичні дані даних за попередніми додатками із цієї опцією.

1.3.1. Вся подальша робота із критичною інформацією буде відбуватись у захищеному режимі: «Режим Інкогніто» у веббраузері. Виконати налаштування веббраузера при перегляді інтернет-контенту,

направлені на блокування відстежування зовнішніми вебтехнологіями, а також (!) – на заборону роботи розширень/додатків в режимі: «Режим Інкогніто».

1.3.2. Дозволити вищевстановленим розширенням але (!) тільки із найбільш відомим розширенням, із високим рейтингом працювати в режимі «Режим Інкогніто».

1.3.3. Всі вкладки для роботи із критичною, банківською інформацією будуть відкриватись у цьому режимі. Браузер>>нова вкладка в режимі «Режим Інкогніто».

1.4. Блокування аналітики і захищений електронний банкінг. Провести дослідження і коротку статистику даних результатів перегляду інтернет-сторінок і зокрема довільних сайтів інтернет-банкінгу. Коротко охарактеризувати результати про потенційні кіберзагрози, якщо є, або їх потенційно можливу появу (якщо такий випадок трапляється) в результаті використання інтернет-технологій та інтернет-серфінгу.

1.4.1. Провести аналітику даних (заблоковані ресурси/трекери/кукі/дані сайтів) для 4-х довільно обраних сайтів, в т.ч. сайтів інтернет-банкінгу із першого списку). Скріншоти і матеріали аналізу, дані статистики додати у звіт. Зробити аналітичні висновки по роботі розширень браузера, а також щодо появи контекстної та таргетованої реклами і супровідних інформаційних матеріалів.

1.5. Навести приклади роботи із ЕЦП банку (Електронний цифровий підпис) при інтернет-банкінгу і політику захищеного зберігання і доступу до ключів ЕЦП та токенів (як фізичних, так і логічних – паролів) при захищеному інтернет-банкінгу.

1.6 Провести аналіз ризиків потенційних теоретичних кіберзагроз при використанні технології ЕЦП та суміжних електронних фінансових сервісів (FinTech), наприклад, при використанні електронних криптогаманців (в т.ч. апаратних.). Навести приклади таких сервісів у вигляді скріншотів.

Завдання 2.

2.1 Навести приклади потенційно небезпечних вебресурсів (інтернет-сайтів) та фішингової і шкідливої інформації із шкідливим контентом від них (2-3 приклади) із реакцією антивірусних інструментів на них – 1.)AV Online Web Security; 2.) AV антивірусного захисту в складі ОС чи окремого. Скріншоти додати у звіт у вигляді картинок: в складі контенту. Навести методи, способи і практичні інструменти нейтралізації потенційних загроз контенту і роботи із такою інформацією. Навести основні прийоми роботи із потенційно небезпечною інформацією і потенційно небезпечним медіа-контентом (на прикладі наведених картинок) – у вигляді списку.

УВАГА (!!). При пошуку фішингових сайтів в мережі Інтернет будьте обережними, включіть вебзахист та ні в якому разі НЕ вводьте туди свої персональні дані, дані карток та іншу інформацію, тільки потрібно зробити скріншоти.

Для прикладу, дані фішингових сайтів (тестові URL):
<http://maliciouswebsitesetest.com/> ;
<https://www.kaggle.com/datasets/sid321axn/malicious-urls-dataset>
<https://www.webpagetest.org/> ;
 один із набору URL із переліку на: <https://caniphish.com/free-phishing-test/phishing-website-templates>.

2.2. В тому числі проведіть тест прямою тестовою вірусної сигнатури єї car: X5O!P%@AP[4PZX54(P^7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H* . Можна її зберегти в файлі *.txt .

2.3. Перевірити фішингові ці посилання (в т.ч. приклади шкідливих URL) на сайті:

<https://virustotal.com>;
<https://skysnag.com/phishing-check/>;
<https://www.phishingbox.com/phishing-test>;
<https://checkphish.bolster.ai/>

та антивірусних засобів у п.п.6.1.

Перевірти файли і URL за допомогою інструментів антивірусного сканування і перегляду інтернет-сторінок із списку. Дані занесіть до таблиці 6.1.

Таблиця 6.1 – Основи тестування вебсайтів

Вебсайт	ІАдреса	Тип загрози	Ризики	Результати	Параметри
(URL)		(По резуль.АV)		сканування	URL
файл		(По резуль.АV)		сканування	URL

2.4. Коротко охарактеризувати результати про потенційні кіберзагрози або потенційного витоку інформації із месенджерів (чатів соц. мереж) при роботі із цими вебресурсами в інтернеті, якщо є, або їх потенційно можливу появу (якщо такий випадок трапляється у лабораторній роботі – навести приклад із зазначенням*) в результаті використання інтернет-технологій та інтернет-сервісів.

Завдання 3.

3.1. Взяти довільну (НЕ діючу (!) і НЕ актуальну (!) банківську карту). Можна взяти тестовий зразок у викладача. Уважно її оглянути.

3.2 Визначити критичні елементи та критичну (!) інфомрацію, яку містить ця банківська карта. До критичної інформації належать зокрема: код CVV/CVV2 (на звороті картки); дата і термін дії хх/хх(місяць/рік), вторинно – номер картки; персональна інформація власника (П.І.Б.) на картці.

3.3 Зробити висновки при передачі цих даних третім сторонам у випадках:

– втрати картки;

- тимчасового заволодіння карткою (наприклад, коли дали на декілька хв/сек. другу/подрузі/знайомому; офіціанту в закладі; іншій особі);
- у випадку фото-, відеофіксації цих даних фото/відео-каналами (фото/відеокамера, яка встановлена, наприклад, під касою і т.п.);
- інших випадках заволодіння даними картки чи самою карткою, наприклад, коли Ви самі ввели їх на фішинговому сайті.

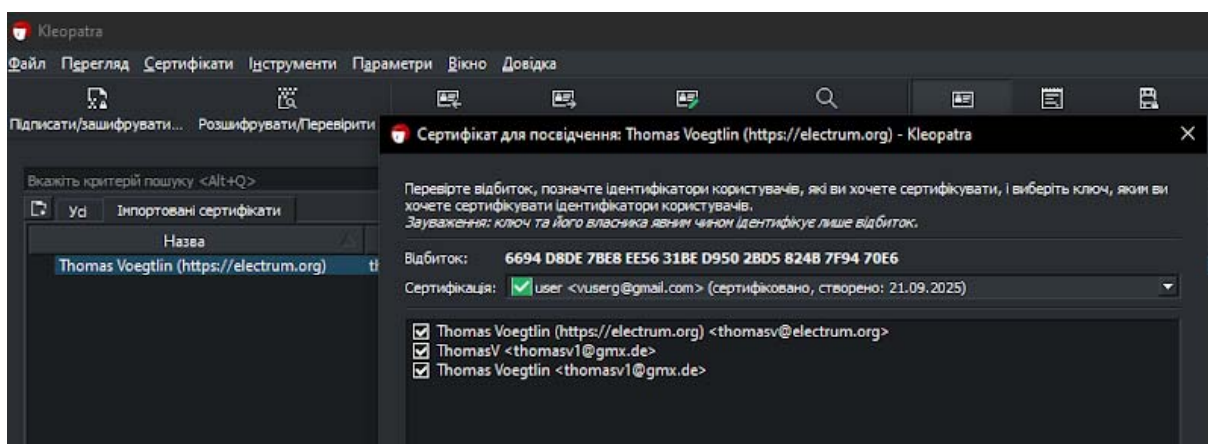
3.4. Провести експеримент: змодельовати ситуацію втрати даних банківської картки (!! Увага, - НЕ брати для експерименту свої оригінальні чи діючі банківські картки).

3.5. Для цього:

- ввести дані картки (! НЕ оригінальної) на фішинговому сайті, у формі чи на сайті опитування, чи отримання фінансових ресурсів на картці;
- ввести дані і спробувати придбати товар на будь-якому одному інтернет-магазині, аналогічно показати ситуацію, коли інтернет-магазин є фішинговим. Зробити звіт про ризики та кіберзагрози про роботі із даними картки.

3.6. Взяти довільні 2 криптогаманці, наприклад:

1) Electrum (<https://electrum.org/#download>Завантажити)
портативна версія Electrum;



2) Monero getmonero.org.

Встановити та отримати тестові версії криптогаманців та електронних підписів до них для експерименту.

3.6.1 Перевірити самі криптогаманці і їх електронні підписи гаманців:

1) Завантажити публічний ключ Thomas Voegtlin
(<https://electrum.org>) <thomasv@electrum.org>.

<https://raw.githubusercontent.com/spesmilo/electrum/master/pubkeys/ThomasV.asc>

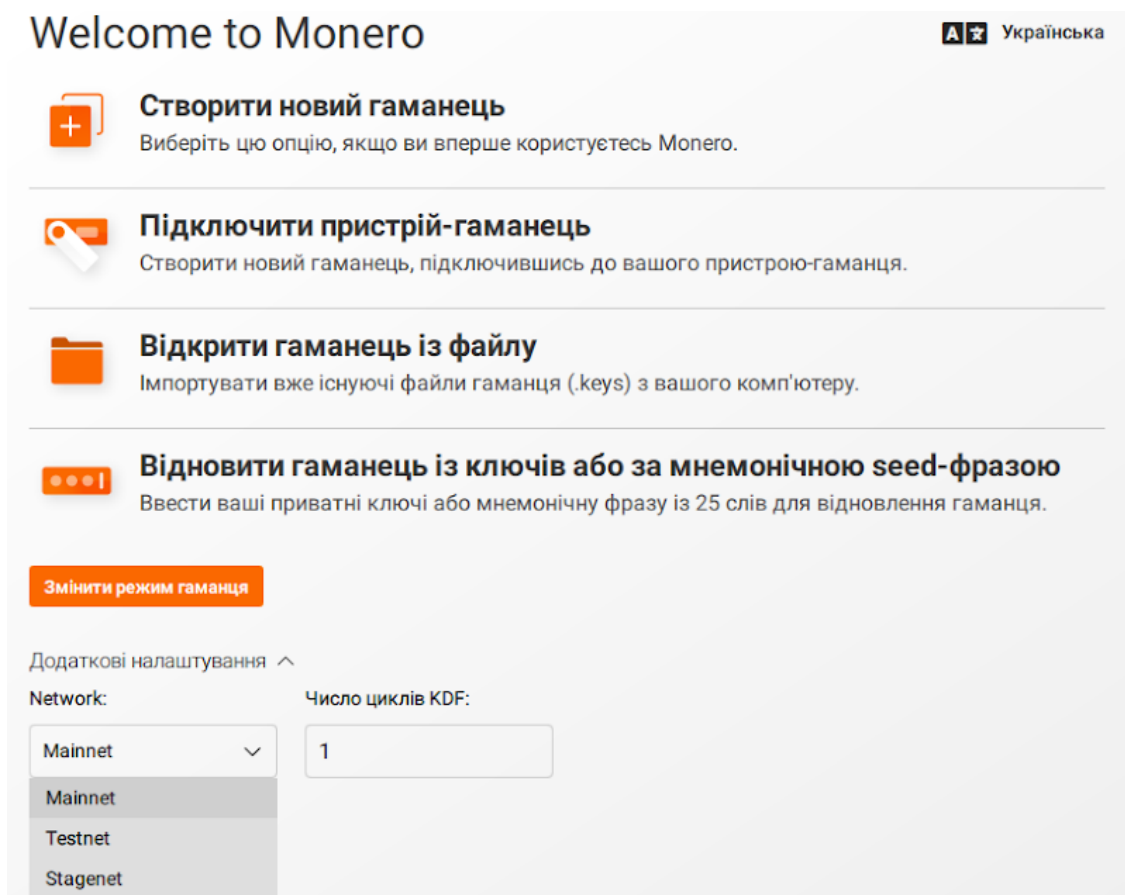
Зафіксувати геш публічного ключа Thomas Voegtlin.

2)Завантажити останню офіційну версію Monero GUI Wallet з домену getmonero.org, наприклад, у вигляді архіву.

<https://www.getmonero.org/resources/user-guides/verification-allos-advanced.html#:~:text=Binary%20Verification%20on%20Windows>

Завантажити версію публічного ключа:

https://raw.githubusercontent.com/monero-project/monero/master/utls/gpg_keys/binaryfate.asc



Перевірити цілісність завантаженого архіву через обчислення гешу і порівняння його із зазначеним на сайті. Завантажити публічний ключ для перевірки електронного підпису, встановити Gpg4win та перевірити електронний підпис архіву Monero GUI Wallet.
<https://pgp4win.org/download.html>

Розпакувати архів і запустити основний файл гаманця monero-wallet-gui.exe, після чого відкриється вікно майстра налаштування, де слід вибрати відповідну мову інтерфейсу, «Розширений режим» - «Додаткові налаштування» і у спадному списку - Stagenet (рис. 1).

Завантажити файл інсталяції Gpg4win і перевірити його цілісність за SHA256. Обчислити Геш-функцію Геш-калькулятором або безпосередньо у командному рядку

Обчислення Геша в командному рядку

>Terminal/ cmd> certutil -hashfile <file> SHA256

Для цього записати значення гешу, що опубліковано на сайті, і самостійно обчислений у два текстові файли, а потім у cmd порівняти їх вміст (створити каталог із своїм прізвищем в ньому):

> fc /C sha256site.txt sha256my.txt >nul && echo Файли однакові || echo Файли різні cmd.exe оператори

&& і || працюють як логічні зв'язки між командами:

&& → виконати наступну команду, якщо попередня завершилася успішно (код виходу = 0)

|| → виконати наступну команду, якщо попередня завершилася з помилкою (код виходу ≠ 0)

Обчислення геша в командному рядку

> certutil -hashfile <file> SHA256

Імпортувати та експортувати і показати свої публічні ключі. За яким алгоритмом вони були створені?

Надрукувати і показати публічний і приватний ключі.

Видалити свої ключі і продемонструвати їх відновлення.

Зробити висновки по роботі із цілісністю даних електронних ключів вебсервісів криптогаманців і даних доступу до криптогаманців та можливими ризиками кіберзагроз по них.

Імпортувати з кожного із цих сервісів публічні ключі і скопіювати їх в буфер обміну. Також скопіювати значення гешу публічного ключа.

Провести експеримент: змінити/підмінити ключі і вставити на етапі передачі іншій стороні чи з буфера обміну в поле авторизації на сервісі.

Аналогічно провести експеримент: змінити/підмінити адресу криптогаманця на етапі фото передачі стороні В чи на етапі викопіювання з буфера обміну.

(!) Експеримент проводити виключно в навчальних цілях із метою оцінки ризиків та їх вивчення.

3.7 Провести дослідження електронних криптогаманців при користуванні вебсервісами, при відкритті їх напряму у веббраузері (Google Chrome, Mozilla Firefox та інш.). Проаналізувати можливості витоків даних і критичної інформації: адрес і ключів криптогаманців, а також паролів доступу до них. Описати та проаналізувати всі ризики, які існують і виникають при роботі із критичними фінансовими даними та дотичними до них другорядними даними (наприклад, ключами і паролями криптогаманців).

Для демонстраційних цілей описати ризики і навести скріншоти експериментів із поясненнями в лабораторній роботі.

Завдання 4.

4.1. Встановити комплексний інформаційний захист (один із антивірусних продуктів): ESET Internet Security, Avast / AVG Internet Security, Norton Internet Security, Dr.WEB Internet Security. Будьте уважними, в назві продукту повинно бути слово: Internet Security (що вказує на наявність у даного антивірусного пакету функція захисту при роботі із мережею Інтернет). Встановити можна на свій власний ПК у тріал/демо режимі (із 15-ти чи 30-ти денною ліцензією). Цього достатньо для виконання завдань лабораторної роботи.

4.2. У встановлених антивірусного пакету (в опціях) повинен бути функціонал: Safety Banking/Safety Internet Banking/Захищений банкінг. Потрібно знайти цю опцію у меню антивірусного пакету і активувати.

4.2.1. Після запуску даної опції (Safety Internet Banking/Захищений банкінг) у вас відкриється окрема захищена оболонка окремого інтернет-браузера з відсутністю і потенційними ризикам кіберзагроз та інформаційних витоків, яка буде працювати в ізольованому режимі з віртуалізацією ресурсів (технологія Віртуалізації і контеризації даних, що чимось схожа на технологію створення віртуальних машин ПК: VM Ware, VM Box). Саме в цьому режимі відсутні всі потенційні і реальні трекінгові механізми збору даних, відсутня можливість ін'єкції шкідливих скриптів, експлойтів, перехресних XSS- ВЕБ атак, втручання вірусів та запобігання зняття даних кей-логерами і сніферами. Трафік шифрований при роботі із цими ресурсами в складі антивірусного пакету.

Але зауважте (!), дана технологія не завжди може запобігти витoku даних через шкідливий фішинговий сайт. Де користувач довірившись чи введений в оману, сам введе свої дані, а також не завжди може запобігти атакам типу MITM (Man in the Middle-людина посередині, що дозволяє перехопити дані на ненадійному з'єднанні чи інтернет-провайдері і розшифрувати). Також захищений браузерінг (Safety Internet Brouvsing) не захищає користувача від атак типу: «Підглядання пароля та прямого видивляння пароля з клавіатури. Хоча в більшості технологія перекриває і запобігає ризикам інформаційних загроз на 80-90%.

Інші ризики залежать від поведінки і обізнаності самого користувача.

4.2.2. Здійснити перегляд і опис роботи загальних сторінок інтернет-банкінгу чи криптобірж 2-3 сторінки в захищеному режимі. Протестувати роботу ізольованої програмної оболонки окремого браузера в складі антивірусного пакету.

Результати додати у звіт.

4.2.3. Запустіть кілька екземплярів веббраузера.

Протестувати процеси блокування посилань URL месенджерів і визначення цілісності цих посилань програмами:

- Broken Link Detector;
- URL Disabler.

Зробіть висновки.

5. Зміст звіту

1. Тема і мета роботи.
2. Вихідні дані для виконання роботи.
3. Результати виконання роботи (схема, таблиці істинності та часові діаграми.
4. Висновки.

6. Контрольні запитання (для самопідготовки, до звіту з лабораторної роботи включати НЕ потрібно!)

1. Сучасні методи, підходи та програмне забезпечення для перевірки цілісності та кібербезпеки даних.
2. Що таке НЕ достовірні та достовірні інформація в месенджерах?
3. Способи виявлення та ознаки потенційно небезпечної і шкідливої інформації у месенджерах і чатах.

4. Що таке дані інтернет-аналітики і як вони проявляються?
5. Що таке основи політики і менеджменту ризиків у виборі політики безпеки у месенджерах?
6. Які способи підвищення кіберзахисту та кібергігієни банківської інформації існують на ПК і ПЗ та моб. пристрої при використанні сучасних інтернет-технологій Ви знаєте?
7. Базові способи перевірки кіберзахисту даних та виявлення небезпечного контенту.
8. Базові способи перевірки кіберзахисту даних у критичних даних у веббраузері та середовищах спілкування та підходи виявлення небезпечного контенту.
9. Назвіть вимоги до стабільності програмного забезпечення ЕОМ та окремих інтернет-сервісів для банківської інформації.
10. Що таке і які критерії скомпрометованого ПЗ чи інтернет-сервісу?
11. Методи перевірки безпеки і стабільності даних інтернет-сервісів.
12. За допомогою якої утиліти по заданому доменному імені хоста можна визначити його IP-адресу? Визначте IP-адресу хоста www.privatbank.ua; www.oshadbank.ua ; <https://monobank.ua/> .
13. Що таке інтернет-банкінг?
14. Що таке інтернет-серфінг?
15. Що таке захищений інтернет-банкінг?
16. Що таке захищений інтернет-серфінг?
17. Основні ризики при роботі в Інтернеті?
18. Основні ризики при роботі в режимі інтернет-банкінгу?
19. Яка інформація та дані є найбільш критичними при інтернет-серфінгу?
20. Як захистити дані при роботі в мережі Інтернет?
21. Як здійснити та налаштувати захищений інтернет-банкінг (базові правила)?
22. Як вберегтись при роботі з даними в мережі Інтернет?
23. Як вберегтись при роботі з даними банкінгу і шопінгу в мережі Інтернет від фішингу, ШПЗ і кібератак?
24. Як захистити свої дані при роботі із критичними даними карток при інтернет-банкінгу та інтернет-шопінгу в глобальній мережі?
25. Як організувати захищений інтернет-банкінг? Правила кібергігієни.

Лабораторна робота № 7

Основи кібербезпеки мобільних і персональних пристроїв користувачів в мережі Інтернет

Мета роботи: вивчити і ознайомитись із особливостями забезпечення кібербезпеки мобільних та персональних пристроїв користувачів, опанувати навички і базові практики їх кіберзахисту. Дослідити кібербезпеку свого мобільного пристрою та налаштувати базовий захист.

Вивчити і практично ознайомитись із основними правилами і практиками кібергігієни та кібербезпеки мобільних персональних пристроїв, мережі.

До мети також можна віднести опанування навичок аналізу і оцінки показників віддалених інтернет-ресурсів, географічно-розподілених ресурсів і серверів мережі Інтернет, навчитись оцінювати затримку віддалених ресурсів мережі за певний час, складати наочні приклади типової активності мережі.

Необхідні ресурси: ПК і мобільний пристрій (смартфон) або персональний пристрій із доступом до мережі Інтернет, відкритим акантом Google (Playmarket чи Applestore) та встановленими ОС Windows, Linux, Android, iOS.

Теоретичні відомості

Ознайомитись із теоретичними відомостями та лекційними матеріалами за темами: «Парольна кібергігієна», «Кібергігієна автоматизованого робочого місця (АРМ) оператора» та «Кібергігієна та основи кібербезпеки мобільних і персональних пристроїв», «Основи тестування та мережевих команд операційних систем. Тестування та аналіз ресурсів мережі Інтернет».

Кібергігієна мобільного пристрою при роботі в Інтернет

Дотримання правил кібергігієни, обачливе використання смартфонів – усе це особливо важливо в сучасному високоризикованому кіберпросторі, із великою кількістю кіберзагроз, особливо але й інколи – у військовий час, адже йдеться не тільки про безпеку особистих даних, а часто і про збереження життя. Повинні існувати спеціальні правила поведінки на мобільних пристроях у кіберпросторі, для безпечного користування телефонами та мережею Інтернет.

Щоб убезпечити себе та своїх колег, вимикайте телефон повністю або вмикайте «режим польоту», коли використовуєте еротичні дані і не перевірені мережі, або перебуваєте у ризикованих зонах. Під час спілкування телефоном змінюйте або вимикайте геолокації у потенційно небезпечних місцях.

Під час використання мережі Інтернет на смартфоні застосовуйте захищений тунель (VPN) та мережевий екран (Firewall).

Не під'єднуйтеся до невідомих і відкритих (без пароля) Wi-Fi-мереж або інших Bluetooth-пристроїв, які «роздають» інтернет безкоштовно. Бажано не «роздавати» інтернет зі свого смартфона.

Налаштуйте мобільні пристрої, зокрема і месенджери, так, щоб приймати дзвінки та повідомлення лише від осіб, які є у списку контактів.

Виконайте в телефоні всі безпечні налаштування: від блокування телефона до вимкнення функції геолокації.

Будьте обережні під час використання соціальних мереж.

Не переходьте за небезпечними і підозрілими сумнівними посиланнями URL (без попередньої їх перевірки, наприклад, на ресурсі: virustotal.com) та не завантажуйте неперевірені та ризиковані файли із мережі Інтернет, і тим більше, не встановлюйте додатки із сторонніх джерел із низькою (або відсутньою взагалі) репутацією, статистикою встановлення та відгуками.

Це базові правила кібергігієни смартфона.

Для забезпечення базової кібербезпеки смартфона потрібно встановлювати антивірус, використовувати мережевий екран Firewall та захищений тунель VPN.

Порядок виконання роботи

Частина 1. Робота із мережевими ресурсами мережі Інтернет.

Завдання 1. Базові налаштування мобільного пристрою (смартфона).

1.1 Виконайте в телефоні всі безпечні налаштування: від блокування телефона до вимкнення функції геолокації. Будьте обережні під час використання соціальних мереж.

1.2. Для цього проаналізуєте затримку віддаленого комп'ютера (та у смартфоні, поперельно встановивши термінал чи програму аналізу мережі, Term, queue) за допомогою команди ping.

1.3. Реєстрація затримки мережі за допомогою утиліти «ping». Використовуючи час затримки в мілісекундах(мс), обчисліть середню затримку і діапазон (мінімальне і максимальне значення) тривалості затримки. У частині 1 вам потрібно проаналізувати і обчислити затримку мережі і швидкодію мережі (біт.с) при зверненні до кількох вебсайтів, розташованих в різних країнах світу – географічно віддалених інтернет-ресурсах.

Цю процедуру можна використовувати на пристрої в корпоративній (робочій) чи домашній мережі університету для формування базового рівня аналізу мережі і оцінки її продуктивності. Для цього виконайте:

Крок 1: Перевірка підключення. Для перевірки підключення відправте наступні ехо-запити за допомогою команди ping на вебсайти регіонального інтернет-реєстру (RIR):

```
C: \ Users \ User1> ping www.arin.net
```

```
C: \ Users \ User1> ping www.lacnic.net
```

```
C: \ Users \ User1> ping www.afrinic.net
```

```
C: \ Users \ User1> ping www.apnic.net
```

```
та C: \ Users \ User1> ping www.ripe.net (для прикладу)
```

*Примітка. Оскільки деякі вебсайти (наприклад, www.ripe.net) не відповідають на запити ICMP, їх можна не використовувати в цій лабораторній роботі із вказанням причин і додаванням скріншоту. Але можна використати інші сайти.



Географічна мапа місця розташування інтернет-ресурсів

Крок 2: Зберіть мережеві дані. Вам необхідно зібрати достатню кількість даних для підрахунку статистики застосування команди ping, відправивши по 25 ехо-запитів на кожен адресу, вказану в кроці 1.

Збережіть результати роботи зі всіма вебсайтами у текстові файли із описом, додатковим аналізом і скріншотами.

Завдання 2. Тестування ехо-запитів і фіксація затримки мережі.

2.1. У вікні командного рядка введіть ping для отримання списку доступних параметрів.

```
C:\Users\User1> ping Usage: ping
```

```
Або C:\Users\User1> ping Usage: ping -h (ping -help )
```

```
C:\Users\User1> ping Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i  
TTL] [-v TOS] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout]  
[-R] [-S srcaddr] [-4] [-6] target_name Options: -t Ping the specified host until  
stopped.
```

To see statistics and continue - type Control-Break; To stop - type Control-C. -a Resolve addresses to hostnames. -n count Number of echo requests to send. -l size Send buffer size. -f Set Don't Fragment flag in packet (IPv4-only). -i TTL Time To Live. -v TOS Type Of Service (IPv4-only).

2.2. Відправка ехо-запитів.

Використовуючи команду `ping` із розширеною функцією підрахунку, відправте 25 ехо-запитів на вузол призначення, як показано нижче.

При цьому в цій папці буде створено файл з ім'ям `arin.txt`.

Цей текстовий файл буде містити результати ехо-запитів за допомогою команди `ping`.

```
C:\Users\User1> ping -n 25 www.arin.net> arin.txt
```

*Примітка. Поле терміналу залишається порожнім до повного виконання команди, так як її результати перенаправляються в текстовий файл `arin.txt` (в даному прикладі). Символ `>` використовується для перенаправлення виведених на екрані даних в текстовий файл і перезапису цього файлу, якщо він вже існує. Якщо у файлі необхідно зберегти кілька результатів, в рядку команди замініть `>` на `>>`.

2.3. Виконайте команду `ping` для інших вебсайтів.

```
C:\Users\User1> ping -n 25 www.afrinic.net > afrinic.txt
```

```
C:\Users\User1> ping -n 25 www.apnic.net > apnic.txt
```

```
C:\Users\User1> ping -n 25 www.lacnic.net > lacnic.txt
```

Крок 3: Перевірте зібрані дані. Для перегляду результатів, збережених у створеному файлі, у вікні командного рядка введіть `more`.

```
C:\Users\User1> more arin.txt
```

```
Pinging www.arin.net [192.149.252.76] with 32 bytes of data:
```

```
Reply from 192.149.252.76: bytes=32 time=108ms TTL=45
```

```
Reply from 192.149.252.76: bytes=32 time=114ms TTL=45
```

```
Reply from 192.149.252.76: bytes=32 time=112ms TTL=45
```

```
Reply from 192.149.252.75: bytes=32 time=111ms TTL=45
```

```
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45
```

```
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45
```

```
Ping statistics for 192.149.252.75:
```

```
Packets: Sent = 25,
```

```
Received = 25,
```

```
Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds: Minimum = 107ms,
```

```
Maximum = 121ms, Average = 111ms
```

Примітка. Натисніть ПРОБІЛ (SPACE), щоб відобразити іншу частину файлу, або клавішу `q`, щоб вийти.

Щоб перевірити, чи створені необхідні файли, введіть команду `dir`, яка виводить на екран список усіх файлів у папці. Щоб відобразити тільки текстові файли, можна використовувати спеціальний символ `*`.

```
C:\Users\User1> dir *.txt Volume in drive C is OS Volume Serial
Number is 0A97-D265 Directory of C:\Users\User1 02/07/2013 12:59 PM
1,642 afrinic.txt 02/07/2013 01:00 PM 1,615 apnic.txt 02/07/2013 12:40 PM
1,641 arin.txt 02/07/2013 12:58 PM 1,589 lacnic.txt 4 File(s) 6,487 bytes 0
Dir(s) 34,391,453,696 bytes free
```

Внесіть отримані результати в наведену нижче таблицю.

	Мінімальне	Максимальне	Середнє
www.afrinic.net			
www.apnic.net			
www.arin.net			
www.lacnic.net			

Порівняйте результати затримки. Наскільки час затримки залежить від географічного розташування? Аналітичні результати разом із скріншотами додайте у звіт.

2.4. Потестуйте тестовий ресурс webtestpage.com/ webtestpage.org (або аналогічний ресурс, призначений для тестування безпеки) утилітою `hping`, для цього виконайте запит:

```
C:\Users\User1> hping -n 25 www.webtestpage.com > webtestpage.txt
```

```
C:\Users\User1> hping -n 25 www.webtestpage.org > webtestpage.txt
```

Потестуйте можливості команди `hping` (!!), але обережно і тільки на тестових експериментальних ресурсах).

Завдання 3: Реєстрація затримки мережі за допомогою утиліти «`tracert`» та «`tracert`».

Залежно від зони охоплення вашого інтернет-провайдера і розташування вузлів джерела і призначення, відслідковувані маршрути можуть перетинати безліч переходів і мереж. Для визначення затримки мережі можна також використовувати команду `tracert`.

3.1. У частині 2 команда `tracert` застосовується для відстеження шляху до тих же вузлів призначення, що і в частині 1. Для цієї мети команда `tracert` використовує пакети з повідомленням ICMP TTL Exceed (Час життя пакету перевищено) і ехо-відгуки ICMP.

1: Скористайтесь командою «`tracert`» і збережіть отримані результати в текстові файли. Скопіюйте наступні команди, щоб створити файли відстеження маршруту для кожного вузла:

```
C:\Users\User1> tracert www.arin.net > traceroute_arin.txt
```

```
C:\Users\User1> tracert www.lacnic.net > traceroute_lacnic.txt
```

```
C:\Users\User1> tracert www.afrinic.net > traceroute_afrinic.txt
```

```
C:\Users\User1> tracert www.apnic.net > traceroute_apnic.txt
```

Та

```
C:\Users\User1> tracert www.arin.net > tracert _arin.txt
C:\Users\User1> tracert www.lacnic.net > tracert _lacnic.txt
C:\Users\User1> tracert www.afrinic.net > tracert _afrinic.txt
C:\Users\User1> tracert www.apnic.net > tracert _apnic.txt 2:
```

Введіть команду «more», щоб перевірити відстежені маршрути.

2.1 Введіть команду more, щоб переглянути вміст цих файлів:

```
C:\Users\User1> more traceroute_arin.txt
C:\Users\User1> more tracert_arin.txt
```

Tracing route to www.arin.net [192.149.252.75] over a maximum of 30 hops: 1

```
Tracing route to www.arin.net [192.149.252.75]
over a maximum of 30 hops:
 1  <1 ms  <1 ms  <1 ms  192.168.1.1
 2  11 ms   12 ms   11 ms  10.39.0.1
 3  10 ms   15 ms   11 ms  172.21.0.116
 4  19 ms   10 ms   11 ms  70.169.73.90
 5  13 ms   10 ms   11 ms  chnddsrj01-ae2.0.rd.ph.cox.net
    [70.169.76.229]
 6  72 ms   71 ms   70 ms  mrfddsrj02-ae0.0.rd.dc.cox.net [68.1.1.7]
 7  72 ms   71 ms   72 ms  68.100.0.146
 8  74 ms   83 ms   73 ms  172.22.66.29
 9  75 ms   71 ms   73 ms  172.22.66.29
10  74 ms   75 ms   73 ms  wsip-98-172-152-14.dc.dc.cox.net
    [98.172.152.14]
11  71 ms   71 ms   71 ms  host-252-131.arin.net [192.149.252.131]
12  73 ms   71 ms   71 ms  www.arin.net [192.149.252.75]
Trace complete.
```

У цьому прикладі отримання відповіді від основного шлюзу зайняло менше 1 мс (192.168.1.1).

В рядку лічильника переходів 6 зазначено, що шлях до вузла 68.1.1.7 і назад зайняв в середньому 71 мс. Шлях до кінцевого вузла www.arin.net і назад зайняв в середньому 72 мс. Між рядками 5 і 6 спостерігається велика затримка в мережі, про що свідчить збільшення середнього часу проходження сигналу туди і назад з 11 до 71 мс.

3.2. Аналогічним чином проаналізуйте інші результати застосування команди tracert. Який висновок можна зробити про залежність часу проходження сигналу в обох напрямках і географічного місцезнаходження вузла?

Завдання 4. Перегляд мережевих налаштувань

4.1. За допомогою утиліти ipconfig (запускається в командному рядку командою ipconfig) визначите IP-адресу й маску підмережі для свого комп'ютера.

4.2. Визначте клас підмережі, в якій перебуває ваш комп'ютер без використання маски підмережі й по масці підмережі.

4.3. Визначте адресу підмережі, в якій перебуває ваш комп'ютер, з використанням функції "Логічне І" (Logic AND) або логічне множення над IP-адресою й маскою підмережі. Слід мати на увазі, що операція "Логічне І" повинна проводитися із двійковим значенням операндів, наприклад:

10101010. 10101010. 10101010. 10101010

AND

00100010.10101010. 10101010. 10101010

Result:

Завдання 5. За допомогою утиліти ping –n10 перевірте показник доступності віддалених вебхостів, мінімальний, середній і максимальний час приймання-передачі ICMP пакетів до них. Можна розглянути хости, наприклад, у наступній послідовності:

5.1. Сервер вашого безпосереднього провайдера або сервера вашої підмережі;

5.2. Який-небудь сервер вашого регіону;

5.3. Вебсервер Університету в Кембриджі: www.cam.ac.uk ;

5.4. Вебсервер Інтернет Університету інформаційних технологій: www.intuit.com ;

5.5. Вебсервер Університету в Каліфорнії: www.ucla.edu ;

5.6. Вебсервер Університету в Токіо: www.u-tokio.ac.jp ;

5.7. Вебсервер компанії Майкрософт: www.microsoft.com.

Зверніть увагу, що в останньому випадку Ісmp-пакети блокуються вебсервером. Внесіть отримані результати в таблицю:

	Мінімальне	Максимальне	Середнє
Сервер вашої підмережі			
www.cam.ac.uk			
www.intuit.com .			
www.ucla.edu			
www.u-tokio.ac.jp ;			
www.microsoft.com .			

Частина 2. Робота з мобільними пристроями в мережі Інтернет.

Завдання 6. Визначення трафіку даних мережі мобільного пристрою. Робота із персональними мобільними пристроями.

а. Відкрити Playmarket (AppStore або SamsungStore) на смартфонах або планшетних ПК на базі ОС Android , iOS або Samsung OS. Інше хмарне сховище програм для моб. пристроїв із цими операційними системами – НЕ варто використовувати.

b. Зайти в пошук программ і знайти системну програму аналізу трафіку (Wi-Fi Analyzer, NetAnaliser, Fing). Встановити і запустити цей додаток (програму).

с. В залежності від функціоналу запустити консоль аналізу трафіку мережі та параметрів завантаженості операційної системи мобільного пристрою (% завантаженості ЦП, використання пам'яті і ресурсів мережі із консолі).

Подивитись параметри мобільного персонального пристрою:

– трафіку даних різних застосунків та трафіку загального із запуском хмарних сервісів окремо і паралельно із програмою/додатком аналізу:
- потокового відео; - потокового аудіо; - музики і голосових повідомлень; - інших системних застосунків; -іншого.

– параметрів завантаженості центрального процесора ЦП CPU (% ,GHz);
– параметрів завантаженості оперативної пам'яті ОЗП RAM (% ,Mb);
– параметрів завантаженості оперативної стаціонарної постійної пам'яті сховище ROM FLASH (Mb).

Запустити не менше 7-8 програм/додатків на мобільному пристрої. За допомогою програми моніторингу ресурсів пристрою визначити завантаженість системи і розходження обчислювальних ресурсів (ресурси і завантаженість ЦП, пам'яті, ОЗП, статичної, пам'яті та інше). Встановити CCleaner із Playmarket чи AppStore та провести оптимізацію (очищення) системи мобільного пристрою за компонентами: - пам'ять ОЗП; - статична пам'ять (et-HDD); ресурсів процесора (%-завантаженості); активнопрацюючих програм.

Зробити відповідні аналітичні висновки про вплив роботи додатків на ресурси ОС мобільного персонального пристрою.

d. Зробити скрінні графіків/векторних діаграм трафіку за різними програмами за період (1 сеанс (із запуском різного контенту: 3-х типів) день/тиждень/місяць)). Порівняти їх із графіками попередньо встановленої програми аналізу трафіку даних, додати їх у звіт із аналітичними оцінками і описом.

е. Встановити систему моніторингу і дослідження інтерфейсів мережі Net view. Запустити її і в режимі реального часу подивитись мережеві параметри інтерфейсу мобільного пристрою та його можливості. Подивитись споживання передачу/прийом трафіку мережі за різними типами запущених і встановлених програм.

f. Визначити найбільш ризикові і найбільш активні програми, за параметрами споживання максимального трафіку (особливо якщо вони працюють у фоні).

Завдання 7. Робота із системами безпеки додатковим опціоналом мобільних персональних пристроїв.

7.1. Аналіз шкідливого трафіку і виявлення DDoS-трафіку. В залежності від функціоналу запустити консоль аналізу трафіку мережі.

Подивитись параметри: – трафіку даних різних застоснків та трафіку загального із запуском хмарних сервісів окремо і паралельно із програмою/додатком аналізу. Провести аналітику і попередньо визначити потенційно-ризиковані з'єднання і трафік даних від різних додатків.

Зробити побудову аналітичних графіків контентного трафіку по видах типу даних контенту та графіка загального потоку даних

Зробити скріншоти (screenshoots) цих графіків і даних аналізу трафіку та додати із аналітичним описом у звіт.

7.2. Відкрити у своєму пристрої консоль «налаштування». Перейти «налаштування» >> передача даних (або мережі/трафік мережі та/або аналогічне) >>трафік/ данні програм>>показати * * в залежності від функціоналу і опціональних налаштувань операційних систем мобільних пристроїв, різних графічних інтерфейсів в різних пристроях дані можуть відрізнятись. Зробити пошук трафіку із подібних/однакових ресурсів - як потенційно ризикових із точки зору DDoS. Зробити висновки і занести відповідні матеріали у звіт. показ даних трафіку по різних програмах. Зробити скріншоти і додати їх із аналітичним описом у звіт. Побудувати кругову діаграму в одній із текстових або табличних систем обробки даних за цими даними.

7.3 Робота із терміналом і VPN на мобільному пристрої.

Для цього Зайти в Playmarket в смартфонах або планшетних ПК на базі операційної системи Android або Appstore для моб. пристроїв на базі iOS або інше хмарне сховище програм для інших моб. пристроїв із операційними системами, відмінними від зазначених.

7.3.1. У терміналі із мобільного пристрою запустити команду terminal>>Ipconfig. Зафіксувати IP-адресу вашого пристрою в мережі Інтернет.

7.3.2.Встановити один із доступних сервісів VPN (Free VPN) із хорошим рейтингом. Запустити VPN (Free VPN).

7.3.3 У терміналі із мобільного пристрою запустити команду terminal>>Ipconfig. Зафіксувати IP-адресу вашого пристрою в мережі Інтернет із запущеним сервісом VPN. Зробити аналітичні висновки і скріншоти про IP-адреси пристрою.

7.3.4. У випадку потенційної кіберзагрози DDoS-атаки або зміни експотенційного збільшення завантаженості шляхом підключень включити/переключити VPN-сервіс і змінити IP-адресу мобільного пристрою/обчислювальної платформи – як спосіб збільшення кіберстійкості до DDoS-атак і превентації завантажень на мережу.

7.3.5. Зайти в Playmarket в смартфонах або планшетних ПК на базі операційної системи Android або Appstore для моб. пристроїв на базі iOS або інше хмарне сховище програм для інших моб. пристроїв із операційними системами, відмінними від зазначених. Встановити один із доступних мережевих екранів: Firewall. Активувати/запустити встановлений мережевий екран/фаєрвол.

7.3.6. Активувати мережевий екран/фаєрвол і подивитись в налаштуваннях Firewall>>settings>>rules/programs статистику і трафік встановлених мережевих програм (всіх програм в мобільній платформі). Налаштувати заборону доступу для inbound| outbound трафіку всіх програм, крім тих, якими Ви користуєтесь в даний момент для виконання даних програм.

7.3.7. Запустити два сервіса одночасно: VPN + Firewall. Це забезпечить як максимальний захист від мережевих вторгнень іззовні, так і від потенційних загроз трафіку.

7.3.8. Запустити попередньо встановлений монітор онлайн-трафіку в режимі реального часу. Подивитись статистику і зробити скріншоти графіків трафіку мережі із включеними і налаштованими сервісами VPN + Firewall та попередньо без них. Зробити відповідні висновки.

7.4 Робота із антивірусною системою захисту на мобільному пристрої. Встановити актуальний антивірусний захист із функцією оновлення щоденно антивірусних баз та функціями аналізу вебінтерфейсів і контролю моніторингу аналізу вебсерфінгу. Встановити один із можливих варіантів захисту/кіберзахисту вебсистеми інтернет-перегляду (McFee; LookBit Web; Internet Sec; E-set, Dr.WEB, McAfee, AVG,AVAST antivirus) або в складі діючого антивірусного пакету в Trial (пробному) варіанті.

7.4.1. Для цього зайти в Playmarket в смартфонах або планшетних ПК на базі операційної системи Android або Appstore для моб. пристроїв на базі iOS або інше хмарне сховище програм для інших моб. пристроїв із операційними системами, відмінними від зазначених. У даному хмарному сховищі із мобільного пристрою зробити пошук довільного антивірусного пакету під вашу мобільну платформу.

Встановити антивірусний пакет і запустити його.

Виконати необхідні налаштування антивірусного сканера в налаштуваннях антивірусного пакету. Виконати оновлення антивірусних баз до актуального стану.

7.4.2. Виконати сканування мобільного пристрою на наявність загроз і шкідливих додатків, виконавши відповідну команду terminal>>Ipconfig. Зафіксувати IP-адресу вашого пристрою в мережі Інтернет.

7.4.3. Встановити один із доступних додаткових сервісів антивірусного сканування (Free AntivirusVPN) із хорошим рейтингом.

7.4.4. Запустити цей додатковий сервіс антивірусного сканування і виконати дії, аналогічні пунктів 7.4.2 і 7.4.3.

7.4.5. Просканувати мобільний пристрій повторно за допомогою додаткового сервісу антивірусного сканування (AV scanner). Провести дослідження і коротку статистику аналізу даних в результаті сканування і перегляду інтернет-сторінок із таблиць у п.2.3 (с.53) та п.5.7(с.55).

Матеріали і скріншоти додати у звіт.

Завдання 8. Робота з безпекою додатків мобільних пристроїв.

8.1. Безпека додатків мобільного пристрою.

8.1.1. Зайти в налаштування безпеки мобільного пристрою в загальній консолі всіх налаштувань: Settings>>programs>> safety або Settings>> safety (*- може відрізнятись в залежності від моделі моб. пристрою або операційної системи).

8.1.2. Переглянути дозволи, які надаються програмам (в т.ч. службовим), які встановлюються у мобільному телефоні/смартфоні/моб. пристрою.

8.1.3. Шляхом евристичного синтезу і евристичного аналізу («* розумом і аналітикою ☺») визначити додатки моб. пристрою, які отримали непотрібні та неадекватні функціоналу дозволи до ресурсів цього мобільного пристрою, які не співмірні з їхнім необхідним технічним функціоналом.

Наприклад. У смартфоні на базі Android, в консолі GPS та Геолокація наявна програма Текстовий блокнот («Modern notepad») із доступом до цих ресурсів, місця розташування і координат геолокації. Виникає логічне питання: навіщо простому блокноту необхідний доступ до даних географічного місця розташування? Це пряма загроза безпеці і витоку даних в мережу.

8.1.4. Обмежити доступ всіх не співмірних із необхідним технічним функціоналом програм до ресурсів мобільного пристрою, окрім тих, які передбачені наявними технічними функціями. Дозволи на ті програми, які Ви не знаєте, або володієте неповною інформацією щодо їх прав доступу – «чіпати» не можна. Це може призвести до часткової або повної втрати функціоналу мобільної обчислювальної платформи мобільного персонального пристрою.

8.1.5. Провести аудит безпеки моб. пристрою по всіх пунктах системи доступу до прав та інше.

8.1.6. Коротко охарактеризувати результати про потенційні кіберзагрози і мережеві атаки, в т.ч. потенційної DDoS-атаки, якщо є, або їх потенційно можливу появу (якщо такий випадок трапляється) в результаті використання інтернет-технологій та інтернет-серфінгу. Визначити які ресурси і дані моб. пристрою потрібно берегти для уникнення DDoS-атак.

8.2. Подивитись дозволи і розміри пам'яті додатків. Після проведення аналізу зробити оптимізацію: повидаляти не потрібні дозволи і почистити пам'ять мобільних додатків. Можливо повидаляти не потрібні додатки.

Завдання 9. Робота зі спеціальними дозволами додатків мобільних пристроїв.

9.1 Переглянути доступ додатків до геолокації мобільних пристроїв. Провести аналіз і визначити потенційно ризиковані додатки, які мають «понаднормовий» і «неоднозначний» доступ до геоданих, геолокації.

9.2 Повідкликати дозволи геолокації ризикованих і неперевіраних додатків.

9.3. Встановити один із можливих додатків для спуфінгу геолокації моб. пристрою (lockito, geospy, geosafe та/або інші). Запустити та змінити актуальну геолокацію моб. пристрою. Результати занести у звіт із аналізом, скріншотами та описом, із зазначенням досягнення і мап/місць зміни геолокації.

9.4 Відкрити налаштування камери мобільного пристрою Камера>>Налаштування. Знайти там пункт додати/додавати геомітку (геоположення) до метаданих фото. * Може називатись по-іншому в різних моделях і версіях ОС моб. пристроїв. Знайти і вимкнути цю опцію. Ця опція дозволяє додавати для метаданих фото/відеоконтенту геоположення, де була здійснена фотографія, таким чином порушуючи безпеку.

9.5 Аналогічно провести аналіз дозволів додатків, які мають дозволи доступу до камери та мікрофона мобільного пристрою. Виконати дії п.п. 9.1.-9.2 по відношенню до дозволів доступу додатків до мікрофона та відеокамери мобільного пристрою.

Завдання 10. Основи створення надійного захисту підтримуючої мережевої інфраструктури для мобільних пристроїв.

Основна мета – навчитись створювати надійний захист пристроїв пограничного рівня для доступу до сервісів мобільних пристроїв та Інтернету речей.

10.1 За допомогою системи моделювання та/або візуалізації графіки створити базову схему комп'ютерної мережі із моб. пристроєм і роутером. Намалювати приблизну схему домашньої мережі із ПК і мобільним пристроєм. Налаштувати бездротовий маршрутизатор в будинку, зазначити на ній: поле (консоль) змінити пароль у мережевому обладнанні; обладнання із назвою мережі – стандартним SSID; безпеку із використанням WPA/WPA2/WPA3 Personal як метод захисту; використання фільтрації IP та MAC для підвищення безпеки в мережевих пристроях мережі.

10.2 Створення домашньої мережі за допомогою бездротового маршрутизатора.

10.2.1. Налаштуйте сервер та маршрутизатор Сервер: / Маршрутизатор: / комутатор/ точку доступу. Перевірте підключення до роутера за його адресою з сервера: / 192.168.1.1 (або аналогічн.) – із веббраузера в стрічці URL.

10.2.2. Налаштувати мережу ПК/ноутбука і AV ПЗ на перевірку підключення до сервера за його адресою: / IP IoT-вебсервісу: / 192.168.1. (або localhost(127.0.0.1)).

10.2.3. Підключити кінцеві пристрої із IP в конфігурацію сканування кінцевих пристроїв: // Network / Add End-Point Devices Ip .

10.3. Включити функції безпеки даних у пограничному пристрої: IP Spoofing, AntiHacking, AntiDDoS, Firewall та CyberSec, якщо вони є в

консолі управління безпекою у відповідному підменю у контрольній адміністративній панелі інтерфейсу управління пристроєм.

10.4. Створити захист домашньої мережі за допомогою безпечного бездротового маршрутизатора шляхом первинних налаштувань безпеки.

10.4.1. Змінити пароль за замовчуванням / Доступ до маршрутизатора із ноутбука/ПК.

10.4.2. Змінити ім'я маршрутизатора SSID (яке використовується за замовчуванням) та вимкнути функцію трансляції SSID при встановленні зв'язку ПК/ноутбука і кінцевих пристроїв.

10.4.3. Налаштуйте безпеку WPA2.0 на бездротовому маршрутизаторі шляхом включення відповідних функцій.

10.4.4. Налаштувати мобільний пристрій або ПК (наприклад, Laptop0) як бездротовий клієнт. Переналаштувати кінцеві пристрої:

10.4.4.1 Перевірте можливість з'єднання з маршрутизатором/комутатором та сервером із іншого пристрою (ноутбук/ПК) чи віддалений ноутбук. Доступ зі стороннього ноутбука до сервера чи маршрутизатора повинен бути відсутній, щоб зв'язатись з маршрутизатором.

10.5. Налаштуйте маршрутизатор для підтримки фільтрації MAC-адрес.

10.6. Перевірте MAC-фільтр Маршрутизатор буде видно для ноутбука та інших кінцевих пристроїв, якщо їх MAC-адреси будуть у списку дозволених MAC-адрес маршрутизатора. У хакера/зловмисника/стороннього користувача зв'язок із маршрутизатором відсутній .

10.7 Зробити аналітичні висновки по виконаному завданню: про налаштування домашньої мережі і зв'язку із кінцевими пристроями на пограничному рівні, про налаштування кінцевих пристроїв і маршрутизатора, безпеки на них. Навести отриману базову аналітику даних по забезпеченню захисту домашньої мережі налаштуванням маршрутизатора. Встановлення захисту WPA2-PSK + AES/DES унеможливило доступ зловмисника до мережі. А фільтрування IP/MAC-адрес (або IP+MAC) забезпечує додатковий рівень захисту шляхом заборони доступу для пристроїв, MAC-адреси яких відсутні в дозволеному (Permit) списку маршрутизатора.

10.8 Налаштування безпеки пристроїв пограничного рівня.

10.8.1. Зайти в пошук програм на стаціонарному ПК і знайти в мережі Інтернет системну програму аналізу трафіку (Network Trafik View, або аналогічну), а також програму LAnSpy. Встановити і запустити програму.

10.8.2. В залежності від функціоналу запустити консоль аналізу мережі. Подивитись параметри оточуючого середовища і пристроїв мережі, зокрема: IP-адреси, MAC-адреси. Сформулювати таблиці і занести ці дані по мережі.

10.8.3. Зробити побудову аналітичних графіків за допомогою програми Wi-Fi network analyzer (яка попередньо встановлена на мобільному пристрої) по підключених пристроях Wi-Fi в мережі і контентного трафіку. Зробити скріншоти, які потім занести у звіт. За типами і якістю сигналу даних контенту сформулювати пріоритетність систем доступу відалених Wi-Fi пристроїв. Скріншоти графіків сторонніх пристроїв Wi-Fi загального потоку даних занести у звіт. Зробити скріншоти (screenshots) параметрів цих пристроїв даних аналізу трафіку від них.

10.9 Провести базовий аудит безпеки. Провести аудит безпеки по всіх пунктах системи доступу до інтернету. Описати це пунктами та включити у звіт.

10.9.1. Встановити актуальний антивірусний захист на ПК (бажано ENDPoint- рівня: 3 складові: файловий антивірус, мережевий екран (фаєрволл), WEB-антивірус), який функціонує із актуальними оновленнями антивірусних баз та функціональними модулями для аналізу вебінтерфейсів і контролю моніторингу аналізу вебсерфінгу. Налаштувати антивірус із врахуванням максимального захисту. Матеріали і скріншоти додати у звіт.

10.10. Провести повне сканування вашого мобільного пристрою на предмет виявлення загроз і потенційних ризиків ШПЗ. Встановити один із можливих варіантів захисту/кіберзахисту вебсистеми інтернет-перегляду, або в складі діючого антивірусного пакету в Trial (пробному) варіанті. Провести дослідження і коротку статистику даних результатів антивірусного сканування і перегляду Інтернет (матеріали у звіт).

Коротко охарактеризувати результати про потенційні кіберзагрози або потенційної атаки, якщо є, або їх потенційно можливу появу (якщо такий випадок трапляється) в результаті використання інтернет-технологій та інтернет-серфінгу.

11. Зміст звіту

1. Титульний аркуш.
2. Тема і мета роботи.
3. Вихідні дані для виконання роботи.
4. Результати виконання роботи (схема, таблиці істинності та часові діаграми).
5. Висновки.

* У звіті необхідно представляти власні й оригінальні результати роботи, плагіат і копіювання – недопустимі.

12. Контрольні запитання

1. Результати використання команд tracert і ping можуть дати важливу інформацію про затримку мережі. Що необхідно для того, щоб отримати точну картину основних даних по затримках мережі?

2. Як можна використовувати отримані основні показники?
3. За допомогою якої утиліти по заданому доменному імені хоста можна визначити його IP-адресу? Визначте IP-адресу хоста www.kyivstar.ua (або іншого, аналогічного).
4. З допомогою утиліти telnet визначте, який вебсервер встановлений на хості www.ukr.net (або іншого, аналогічного).
5. Визначте маршрут проходження ICMP пакетів до хоста www.ttt.com. Визначте географічну локалізацію хоста.
6. Що таке мобільний пристрій користувача? Які його відмінності і особливості використання у порівнянні з ПК?
7. Особливості безпеки мобільних пристроїв користувача? Які його відмінності і особливості застосування технологій кібербезпеки у мобільних пристроях користувача у порівняння із ПК?
8. Використання засобів у мобільних пристроях користувача?
9. Основні теоретичні засади і практики кібергігієни мобільних пристроїв користувачів.
10. Основні теоретичні засади і практики кібербезпеки мобільних пристроїв користувачів.
11. Безпека при використанні додатків на мобільних пристроях користувачів.

Лабораторна робота № 8.

Основи мережевого захисту серверної частини інтернет-сервісів та їх ресурсів

Мета: вивчення безпеки і основних мережевих команд керування для аналізу показників інтернет-технологій та інформаційних сервісів. Опановування основних мережевих команд й основних інструментів операційних систем Windows та Linux. Опановування основних прийомів роботи із службовими командами для інтернет-сервісів та інформаційних систем та прийомами захисту вебсервера.



Необхідні ресурси: ПК (ПЕОМ) із доступом до інтернету та встановленими операційними оболонками CMD, NC, актуальної версії ОС Windows та Linux, персональний мобільний пристрій (смартфон) із встановленим додатком – «термінал» (Terminal\$ xTerm; Termux) на базі мобільної ОС Android iOS і доступом до мережі Інтернет.

Порядок виконання роботи

Завдання 1. Робота із мережею терміналом і командною строкою в ОС

- 1.1. Відкрийте вікно CLI.
- 1.2. Визначте вашу версію DOS або Windows.
- 1.3. Визначте дату й час системи. Якщо вони невірні, виправте.
- 1.4. Визначте файли та папки на диску c:\ в корневому каталозі ☺ .
- 1.5. Створіть папку c:\cs\lab2. Скопіюйте туди файли з розширенням .sys, або з розширенням ini , які є на диску c:\ . Які файли Ви знайшли?
- 1.6. Визначте IP-адресу вашого комп'ютера.
Визначте IP-адресу довільного вебсервера.
- 1.7. Простежте маршрут до вебсерверу сайту www.google.com (або іншого вебсайту).
- 1.8. Визначте кількість IP-адрес проміжних маршрутизаторів до довільного Тестового сервера www.google.com (або іншого вебсайту)
==.

Завдання 2. Робота із мережевими командами ОС в інтерфейсі командної стрічки.

Після виконання першої частини лабораторної роботи з командами Windows Ви повинні знати:

- загальні команди Linux;
- основні мережні командами й інструменти, такі як:

ping
tracert/traceroute
netstat
ifconfig /ipconfig
route

2.1. Визначите власника файлу passwd або іншого довільного файлу в складі ОС із використанням мережесих команд. (Зверніть увагу: спочатку визначите розташування файлу і відповідно шлях до нього).

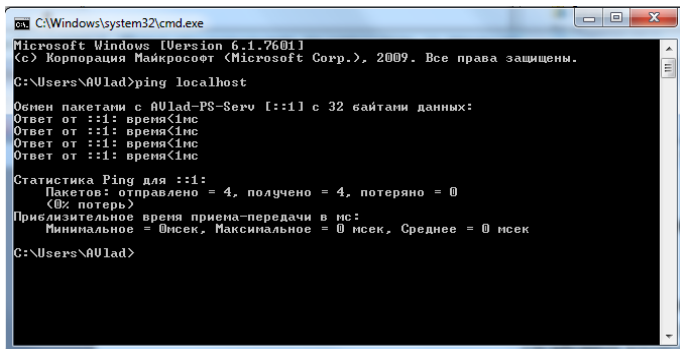
2.2 Створіть каталог work у вашому власному домашньому каталозі (наприклад, якщо Ваш логін – fred, створіть каталог в /home/fred), і скопіюйте файл passwd у каталог work, що Ви тільки що створили. Визначите власника копії passwd.

2.3 Створіть каталог .hide у каталозі work (Зверніть увагу, що ім'я файлу починається із крапки). Подивіться вміст цього каталогу. Що Ви повинні зробити, щоб побачити вміст каталогу .hide?

2.4 Створіть файл test1 зі змістом “Цей файл test1” у каталозі work. Створіть файл test2 зі змістом “Це файл test2” у каталозі work. Скопіюйте у файл із ім'ям test зміст обох попередніх файлів.

Завдання 3. Робота зі службовими мережевими програмами доступу до даних.

CMD>>n -r -l - 1234



Ознайомтесь із основами роботи протоколу НТТР за допомогою утиліти telnet

3.1. Запустіть сеанс telnet (запускається в командному рядку командою telnet). При цьому з'явиться підказка Microsoft Telnet>. З повним списком команд можна ознайомитися за допомогою команди help.

3.2. Дозвольте режим відображення символів, що вводяться із клавіатури, за допомогою команди set localecho.

3.3. Відповідно до протоколу НТТР необхідно встановити з'єднання з вебсервером. Для цього за допомогою команди open встановлюється

з'єднання, наприклад: open www.google.com.ua: 80 (протокол http) (приклад). open www.google.com.ua: 443 (протокол https).

3.4. Сформууйте клієнтський запит. Як мінімум він повинен містити рядок стану, наприклад:

GET ЗАПИТИ HTTP:

GET HTTP://WWW.TESTPAGE.ORG /INDEX.HTML HTTP/1.0

GET HTTP://WWW.GOOGLE.COM.UA/INDEX.HTML HTTP/1.0

Якщо поля запиту відсутні, то введення закінчується двома натисканнями клавіші <ENTER> для вставки порожнього рядка після заголовка.

Слід звернути увагу на те, що при введенні не можна допускати помилок, оскільки при спробі їх виправити за допомогою клавіші <BACKSPACE>, її натискання інтерпретується як частина запиту.

Сформууйте інший запит:

PUT [HTTP://WWW.TESTPAGE.ORG/INDEX.HTML](http://www.testpage.org/index.html) HTTP/1.0

DELETE [HTTP://WWW.TESTPAGE.ORG/INDEX.HTML](http://www.testpage.org/index.html) HTTP/1.0

Проаналізуйте відповіді та додайте у звіт з аналізом.

3.5. Вивчіть отриману відповідь сервера. Зверніть увагу на код відповіді в рядку стану відповіді вебсервера в рядку стану й поля заголовка відповіді. Якщо відповідь сервера дуже велика (у першу чергу через розмір документа в тілі відповіді), то вміст відповіді сервера у вікні інтерпретатора командного рядка обрізується з початку. У цьому випадку рекомендується для перегляду заголовка замість методу GET використовувати метод HEAD.

Завдання 4. Робота із серверними мережевими інструментами.

Для того, щоб виконати ці вправи, Вам знадобиться системна програма netcat (утиліта) (nc). У дистрибутиві (BackTrack) Kali Linux вона є за умовчанням, проте її легко можна завантажити і встановити і на інші операційні системи, і в т.ч. Windows (дивитись по назві NetCat або nc).

4.1. Запуск NetCat. Для цього у консолі наберіть (Зауважте, для роботи ця утиліта повинна бути встановлена вже в ОС):

nc -h

Ця команда відобразить опції, які доступні в netcat.

4.2. Для створення простого серверу в Linux / Windows, наберіть:

nc -l -p 1234

Ви тільки що запустили сервер, що прослуховує порт 1234.

4.3. Відкрийте друге вікно в консолі та наберіть:

netstat -a

Так Ви перевірите, що з'явився новий сервіс, що прослуховує порт 1234.

Щоб встановити зв'язок із сервером, потрібно використовувати клієнт!

4.4 У другому вікні консолі наберіть:

nc localhost 1234 (1234 -приклад порту, який прослуховує)

Дана команда створить з'єднання із сервером на порт 1234.
Тепер все, що друкується в одному з відкритих вікон консолі, буде відображатися і в іншому.

Як можна використати подібну службу, аби зламати вашу систему?
Netcat пересилає весь трафік у відкритому вигляді.
Чи існує безпечна альтернатива?

4.5. Зупиніть сервер, повернувшись в перше вікно консолі і натиснувши **Ctrl + C**.

4.6. Тепер створіть текстовий файл (.txt) і назвіть його «test». Запишіть у текстовий файл фразу: “Welcome to my server!”

Як тільки закінчите, подивіться на команду і розберіться в ній і розкажіть викладачеві, що робить кожна з її опцій.

Наберіть:

nc -l -p 1234 < test

4.7 З іншого вікна консолі підключіться до серверу, набравши:

nc localhost 1234

Коли клієнт підключиться до серверу, Ви повинні побачити вміст файлу test.

4.8 Включіть розширення **https everywhere**, яке попередньо встановлено в інтернет-браузері.

Проаналізуйте трафік від/до сервера nc на localhost ,

- із включеним розширенням https everywhere
- без нього.

Результати із описом, аналізом та скріншотами додати у звіт.

4.9. Запуск серверу на порті 80 та 443.

Запустіть nc на порті 80 :

\$ nc -l 80 nc

Таким чином nc «слухає» порт 80.

На другій консолі (або на другій машині) з'єднуємося з машиною на порт, який прослуховується: \$ nc 127.0.0.1 80 Повинно відбутися з'єднання між портами. Все, що буде набрано на другій консолі, буде відображено на першій і навпаки. Після того, як буде встановлено з'єднання, nc не хвилює, яка зі сторін буде використовуватися, як 'server', а яка, як 'client'.

Аналогічно зробіть це на порті 443.

\$ nc -l 443 nc

Зафіксуйте реакцію системи.

З'єднання може бути перервано використовуючи ESC.

4.10. Передача даних в nc. Попередній приклад може бути розширений для побудови передачі даних. Будь-яка інформація спрямована в одну зі сторін з'єднання буде отримана на іншому кінці.

Введення і виведення легко можуть бути побудовані в такій послідовності, щоб емулювати передачу даних.

4.11. Почніть, використовуючи nc для прослуховування порту, з перенаправленням з нього файлу:

```
$ nc -l 80> filename.out  
$ nc -l 443> filename.out
```

Використовуйте другу машину, для підключення до слухача процесу nc, з перенаправленням в нього передається файлу.

```
$ nc -l 80< filename.in  
$ nc -l 443< filename.in
```

Після передачі файлу, з'єднання автоматично закриється.

Використовуйте другу машину, для підключення до слухача процесу nc, з перенаправленням в нього передається файлу.

```
$ nc host.example.com 80  
$ nc host.example.com 443
```

*Примітка: URL - host.example.com – вибраний для тесту в якості прикладу. Для експерименту візьміть інший, реальний (!), але тестовий URL , наприклад, www.testpage.org

4.12. Сканування портів в nc. Корисно знати які порти відкриті і які сервіси запуснені на досліджуваній машині. Прапор -z може бути використаний, щоб дізнатися про відкриті порту не ініціюючи з'єднання. Наприклад:

```
$ nc -z host.example.com 20-30  
Connection to host.example.com 22 port [tcp / ssh] succeeded!  
Connection to host.example.com 25 port [tcp / smtp] succeeded!  
Був вказаний діапазон портів 20 - 30.
```

Також це може бути використано, щоб дізнатися який серверний софт запуснений, і його версія. Цю інформацію містить вітальне повідомлення. Як правило, щоб зробити це, спочатку необхідно ініціювати з'єднання, потім обірвати його, коли буде отримано вітання.

Це може бути виконано зазначенням маленького тайм ауту за допомогою прапора -w, або можна використовувати команду "QUIT" на сервері:

```
$ Echo "QUIT" | nc host.example.com 20-30  
SSH-1.99-OpenSSH_3.6.1p2  
Protocol mismatch.  
220 host.example.com IMS SMTP Receiver Version 0.84 Ready
```

*Примітка: URL - host.example.com – вибраний для тесту в якості прикладу. Для експерименту візьміть інший, реальний (!!), але ТІЛЬКИ тестовий URL , наприклад, www.testpage.org .

4.13. Безпека з'єднань між хостами і в моделі клієнт-сервер.

Очевидно, що при подібному використанні netcat інформація передається по мережі в вихідному нешифрованому вигляді. Для передачі некритичних даних це цілком прийнятно, але при передачі будь-якої цінної інформації розумно використовувати netcat в поєднанні з SSH-тунелем. Використання SSH-тунелю має дві переваги: - інформація передається всередині зашифрованого тунелю, так що вона добре захищена; - на

сервері не потрібно відкривати ніяких додаткових портів в конфігурації брандмауера, оскільки з'єднання буде встановлено через SSH. Використовуючи команди, вивчені в лабораторній роботі 1, дізнайтеся IP-адресу Вашого комп'ютера, мережеву маску, DNS-ім'я хоста і MAC-адресу. Порівняйте інформацію отриману Вами, з інформацією, отриманою Вашим напарником за сусіднім комп'ютером. У чому схожість і в чому різниця? Які IP-адреси використовуються в мережі: публічні або приватні?

Встановіть програму Putty для ОС Windows/

Протестуйте можливості безпечного підключення до тестового сервера Localhost за допомогою програми Putty. Результати занесіть у таблицю.

Таблиця

Хост	IP адреса	Протокол (SSH /TELNET)	Порт(Port)	Рівень безпеки

Результати із аналізом і описом додайте у звіт.

Також при запусчених програмах протестуйте мережевий трафік. Командою

\$ netstat

в ОС для аналізу мережевих з'єднань Команда netstat відображає мережеву статистику: з ким Ви з'єднані, як довго працює мережа і т.п. Якщо ви хочете, щоб з'єднання відображали адреси і номери портів в числовому форматі, наберіть:

\$ netstat -n

Щоб запустити утиліту в Linux або Windows потрібно зайти в консоль операційної системи і набрати: netstat У консолі Ви побачите список встановлених з'єднань.

У консолі побачите список встановлених з'єднань.

Имя	Локальный адрес	Внешний адрес	Состояние
TCP	127.0.0.1:44430	DESKTOP-R30NBMU:62701	ESTABLISHED
TCP	127.0.0.1:49677	DESKTOP-R30NBMU:49678	ESTABLISHED
TCP	127.0.0.1:49678	DESKTOP-R30NBMU:49677	ESTABLISHED
TCP	127.0.0.1:61917	DESKTOP-R30NBMU:61918	ESTABLISHED
TCP	127.0.0.1:61918	DESKTOP-R30NBMU:61917	ESTABLISHED
TCP	127.0.0.1:61919	DESKTOP-R30NBMU:61920	ESTABLISHED
TCP	127.0.0.1:61920	DESKTOP-R30NBMU:61919	ESTABLISHED
TCP	127.0.0.1:61934	DESKTOP-R30NBMU:61935	ESTABLISHED
TCP	127.0.0.1:61935	DESKTOP-R30NBMU:61934	ESTABLISHED
TCP	127.0.0.1:61936	DESKTOP-R30NBMU:61937	ESTABLISHED
TCP	127.0.0.1:61937	DESKTOP-R30NBMU:61936	ESTABLISHED
TCP	127.0.0.1:62045	DESKTOP-R30NBMU:62046	ESTABLISHED
TCP	127.0.0.1:62046	DESKTOP-R30NBMU:62045	ESTABLISHED
TCP	127.0.0.1:62047	DESKTOP-R30NBMU:62048	ESTABLISHED
TCP	127.0.0.1:62048	DESKTOP-R30NBMU:62047	ESTABLISHED
TCP	127.0.0.1:62052	DESKTOP-R30NBMU:62053	ESTABLISHED
TCP	127.0.0.1:62053	DESKTOP-R30NBMU:62052	ESTABLISHED
TCP	127.0.0.1:62701	DESKTOP-R30NBMU:44430	ESTABLISHED
TCP	127.0.0.1:62789	DESKTOP-R30NBMU:62790	ESTABLISHED
TCP	127.0.0.1:62790	DESKTOP-R30NBMU:62789	ESTABLISHED

5. Зміст звіту

1. Титульний аркуш.
2. Тема і мета роботи.
3. Вихідні дані для виконання роботи.
4. Результати виконання роботи (схема, таблиці істинності та часові діаграми).
5. Висновки.

6. Контрольні запитання

1. Назвіть призначення програми **ping**.
2. Назвіть призначення програми **tracert/traceroute**.
3. Назвіть призначення програми **netstat**.
4. Назвіть призначення утиліти **ipconfig**.
5. Назвіть призначення утиліти **route**.
6. Назвіть призначення програми **ping в Linux**.
7. Назвіть призначення програми **tracert/traceroute в Linux**.
8. Програми **netstat в Linux**.
9. Призначення утиліти **ipconfig в Linux**.
10. Яке значення та функціонал мають утиліти **route в Linux**?
11. За допомогою якої утиліти по заданому доменному імені хоста можна визначити його IP-адресу? Визначте IP-адресу хоста www.kyivstar.ua.
12. З допомогою утиліти **telnet** визначте який вебсервер встановлений на хості www.ukr.net.
13. Визначте маршрут проходження ICMP пакетів до хоста www.ttt.com. Визначте географічну локалізацію хоста.
14. Назвіть основні застосування утиліти **netstat**.
15. Що таке порт?
16. Чому порти, які використовуються віддаленими адресами відрізняються від портів, які використовують локальні адреси?
17. Коли відкрито кілька вкладок в одному браузері, як він може зрозуміти, якій з них передавати отриману інформацію?
18. Чому відбувається так, що коли використовується браузер, то зникають порти, що знаходяться в процесі прослуховування?
19. Який протокол використовується для підключення до серверу?
20. Чи дозволяє **netcat** Вам це змінити?
21. Якщо так, то яким чином?
22. Назвіть вимоги до стабільності ПЗ ЕОМ та окремих процесів.
23. Що таке і які критерії скомпрометованого програмного забезпечення?
24. Методи перевірки цілісності і стабільності даних.
25. За допомогою якої утиліти по заданому доменному імені хоста можна визначити його IP-адресу? Визначте IP-адресу хоста www.kyivstar.ua.

26. З допомогою утиліти telnet визначте, який вебсервер встановлений на хості www.ukr.net. 27. Визначте маршрут проходження ICMP пакетів до хоста www.ttt.com. Визначте географічну локалізацію хоста.

27. Назвіть основні застосування утиліту netstat. Що таке порт?

32. Основні ризики при роботі в Інтернеті?

33. Яка інформація та дані є найбільш критичними при інтернет-серфінгу?

34. Як захистити дані при роботі в мережі Інтернет?

Електронне навчальне видання

**Вадим Ігоревич Маліновський
Леонід Михайлович Куперштейн
Леонід Олександрович Майданевич**

**Методичні вказівки до виконання лабораторних робіт
з дисципліни «Основи безпеки інтернет-технології»
зі спеціальності «Кібербезпека та захист інформації»**

Рукопис оформив *В. Маліновський*

Редактор *Н. Кравчук*

Оригінал-макет виготовлено в *PBB ВНТУ*

Підписано до видання 03.09.2026 р.
Гарнітура Times New Roman.
Зам. № P2026-119

Видавець та виготовлювач
Вінницький національний технічний університет,
Редакційно-видавничий відділ.
ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95,
м. Вінниця, 21021.
press.vntu.edu.ua;
[Email: rvv.vntu@gmail.com](mailto:rvv.vntu@gmail.com)
Свідectво суб'єкта видавничої справи
серія ДК No 3516 від 01.07.2009 р.