МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

КОВАЛЬ ОЛЕКСІЙ ОЛЕКСАНДРОВИЧ

Допускається до захисту:
Завідувач кафедри
інформаційних технологій,
д.т.н., доцент, Нескородєва Т. В.
«__»_____20__р.

ПЕРСОНАЛЬНА СИСТЕМА КІБЕРБЕЗПЕКИ СТРУКТУРНИЙ ПІДХІД

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Науковий керівник:
Крижановський В.Г,
професор кафедри
інформаційних технологій
д.т.н., професор

_____
(підпис)

Оцінка : _____ / _____ / _____
(бали/за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____
(підпис)

Вінниця – 2022

АНОТАЦІЯ

Коваль О. О. Персональна системи кібербезпеки структурний підхід. Спеціальність 125 «Кібербезпека». Донецький національний університет імені Василя Стуса. Вінниця, 2022.

У бакалаврській роботі запропонована унікальна персональна система кібербезпеки.

Ключові слова: кібербезпеки, система, правила користувача, АЗП, пароль.

32 сторінки, 12 рисунків, 10 джерел.

ABSTRACT

Koval OO Personal cybersecurity system structural approach. Specialty 125 «Cybersecurity». Vasyl Stus Donetsk National University. Vinnytsia, 2022.

The bachelor's thesis offers a unique personal cybersecurity system.

Keywords: cybersecurity, system, user rules, AF, password.

32 pages, 12 figures, 10 sources.

ЗМІСТ

ТЕРМІНИ ТА СКОРОЧЕННЯ

ПК – персональний комп’ютер(personal computer);

ПЗ – програмне забезпечення(software);

ШПЗ – шкідливе програмне забезпечення(malicious software (computer viruses));

АПЗ – антивірусне програмне забезпечення(antivirus software);

ВСТУП

Актуальність теми

Станом на тепер людина користується електрообчислювальними засобами повсякчас(телефон, комп'ютер, телевізор, вимірювальні прилади і тд). Такі прилади мають на меті оброблення, передавання, зберігання інформації і таким чином утворюють інформаційну систему [1] з певними інформаційними потоками всередині неї.

Ми постійно взаємодіємо з іншими людьми за допомогою вищевказаних засобів. Деякі з інформаційних потоків потребують захисту від втручання сторонніх осіб, оскільки можуть нести в собі конфіденційну, таємну та іншу інформацію, що потребує захисту.

Мета дослідження

В даній роботі ми зосередимося на захисті інформації яка належить сучасній людині за допомогою створення системи кібербезпеки для персонального використання.

Завдання дослідження

Ознайомлення та аналіз з актуальними проблемами та тенденціями в сфері особистої кібербезпеки.

На основі ознайомлення та аналізу обрати засоби, та створити систему, що дозволить підвищити стан особистої кібербезпеки користувача.

Об'єкт дослідження

Стан кібербезпеки пересічного користувача.

Предмет дослідження

Персональна система кібербезпеки для пересічного користувача.

Варто розуміти, що така система не дає стовідсоткову гарантію кібербезпеки, але вона значно її підвищує.

В даній роботі буде розглянуто яким чином можна побудувати систему кібербезпеки для персонального використання. Ця система буде функціонувати в рамках використання сучасних інформаційних технологій та засобів пересічною людиною під час її, повсякденного життя.

В даній роботі основним засобом, за допомогою якого людина буде існувати, як елемент сучасної цифрової інформаційної системи будемо вважати персональній комп'ютер. На основі вразливостей та загроз, які виникають під час використання останнього і буде будуватись система кібербезпеки.

Під інформаційною системою будем розуміти інформаційний простір, що утворений мережею інтернет. [2]

Щоб побудувати ефективну систему кібербезпеки, необхідно знати, що і де саме ми будемо захищати, це дасть змогу побудувати систему, яка буде відповідати необхідним нам потребам.

Простір у якому буде здійснюватися захист в рамках даної роботи будемо називати інформаційним простором. Оскільки загрози інформації можуть бути реалізовані не лише через мережу Інтернет, але і за допомогою фізичного, психологічного впливу потрібно буде розглянути усі аспекти у яких виникнення загроз є реальним.

Також потрібно розуміти, що захист буде здійснено в тих точках, де користувач може безпосередньо впливати на події, які впливають на стан захищеності інформації.

В РОЗДІЛ 1 буде розглянуто загальну проблематику питання та проведемо аналіз літератури, що стосується теми.

В РОЗДІЛ 2 буде здійснено вибір ПЗ та створення правил, для описаних в РОЗДІЛ 1 проблем.

В РОЗДІЛ 3 будуть проведені налаштування та випробування засобів, що використовуються.

РОЗДІЛ 1 - ТЕНДЕНЦІЇ РОЗВИТКУ ОСОБИСТОЇ КІБЕРБЕЗПЕКИ

1.1 Актуальність обраної теми в сучасних реаліях

Сьогодні питання особистої безпеки і в особливості кібербезпеки стоїть, як ніколи гостро. Окрім «звичайних» зловмисників, що бажають наживитися на людях, що не достатньо кваліфіковані в даному аспекті зросли загрози що створенні агресором для ведення «кібер війни».

Актуальність даного питання підтверджуються і статистикою так наприклад за даними Національної поліції України, кількість організованих груп і злочинних організацій, що вчиняють кримінальні правопорушення з використанням високих інформаційних технологій, за останній рік збільшилась на 36 %. Так найпоширенішими кіберзлочинами є: [3]

- Кардинг – шахрайські операції з кредитними картками (реквізитами кредитних карток), які не погоджені власником картки. Це може бути крадіжка чи незаконне отримання кредитної картки, викопіювання даних картки для подальшого її підроблення, викопіювання реквізитів картки для здійснення покупок через Інтернет без участі власника картки.

Фішинг – шахрайські дії, спрямовані на виманювання реквізитів картки у її власника. Зазвичай власник кредитної картки сам добровільно повідомляє шахраям потрібну інформацію.

Фішинг буває кількох видів:

- СМС-фішинг, коли потенційна жертва шахраїв отримує повідомлення про те, що її кредитну картку заблокував банк, а для розблокування необхідно надати реквізити, або ж про те, що власник картки отримав виграш, але потрібно заплатити за його доставку.
- Інтернет-фішинг, коли шахраї створюють фішингові (підроблені) сторінки, які імітують офіційні сторінки банків, платіжних сервісів, інтернет-магазинів тощо. На жаль, не всі уважно перевіряють назву сайта, уводячи дані кредитної картки, що на руку кібершахраям.
- Вішинг – це майже той самий фішинг, однак виманювання реквізитів картки зловмисники здійснюють за допомогою телефонних дзвінків

- Скімінг – копіювання даних платіжної картки за допомогою спеціального пристрою (скімера). Зазвичай відбувається під час здійснення карткових операцій із банкоматами.
- Шимінг – модернізований різновид скімінгу. У цьому разі шахраї використовують майже непомітний прилад, який розміщують усередині картридера.
- Піратство – протиправне розповсюдження об'єктів інтелектуальної власності в Інтернеті.
- Мальваре(Malware/ШПЗ) – створення та поширення вірусів і шкідливого програмного забезпечення.
- Протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості й насильства.
- Рефайлінг – незаконна підміна телефонного трафіку.

Таким чином якщо, ми говоримо про загрози в мережі для користувачів Інтернет можемо сказати, що фішинг та Malware є основними загрозами в Україні.

1.2 Вивчення тенденцій з питання особистої кібербезпеки

Розглянемо основні загрози, проблеми, фактори на які варто звернути, увагу, що впливають на особисту кібербезпеку та можливі варіанти вирішення, поліпшення таких, що циркулюють навколо людини у кіберпросторі.

До Вищевказаних можна віднести:

1. Соціальний інженеринг(в тому числі фішинг);
2. Зараження ШПЗ – поширена та дуже небезпечна загроза, що може стати причиною втрати ваших даних, вимагання коштів, втрати працездатності ваших пристрої, викрадання даних і тд.;
3. Відсутність АПЗ(Захист в реальному часі);
4. Встановлення легких паролів – одна з найпоширеніших проблем сучасного інформаційного простору людини. Багато з нас мають кілька десятків різних облікових записів, при цьому для кожного з них потрібен пароль небажання вигадувати щоразу новий

складний пароль призводить до повторного використання паролів, або використання занадто легких, що полегшує робото злочинцям;

5. Встановлення неліцензійного ПЗ;
6. Відсутність резервних копій даних – дехто з нас просто не створює резервних копій з оглядом на те, що з їх пристроєм все буде гаразд, саме такі користувачі страждають від втрати особистих даних;
7. Використання небезпечного Wi – Fi середовища для передачі особистих важливих даних;
8. Поширення власних особистої інформації в соцмережах та створення так званого «цифрового сліду» - будь які ваші особисті данні, що ви можете поширювати мережею:
    - Ідентифікаційна інформація (дата народження, по батькові чи дівоче прізвище, місце народження);
    - Робоче місце;
    - Відносини;
    - Хоббі та інтереси;
    - Спортивні клуби;
    - Освіта;
    - Відповіді на запитання щодо відновлення облікового запис;
9. Усвідомлення загроз особистої кібербезпеки, протидія таким, самосвідомість в питаннях кібербезпеки;
10. Відсутність визначеного набору/переліку правил поводження, застосування, праці, взаємодії користувача з іншими особами/приладами в цій системі і поза нею(якщо це може мати відношення до системи в якій необхідно забезпечити захист), як умовне узагальнення вищевказаних пунктів, що призводить до всіх вище вказаних загроз та можливості їх реалізації.

Так у роботах [4-7] деякі з наведені вище пунктів розглядаються наступним чином:

1 - Соціальна інженерія зазвичай використовується в маркетингу та політиці. Але в кіберсвіті іноді його використовують для злому та обману. Здобуваючи вашу впевненість, щоб надати їм деякі з ваших облікових даних, вони обманом змусять вас зламати ваші дані;

3 - Профілактика краще, ніж лікування. На відміну від антивірусного сканування, яке шукає шкідливі файли або програми, які вже є на вашому пристрої, захист у реальному часі виявить та зупинить зловмисне програмне забезпечення, перш ніж воно потрапить на ваш пристрій.

4 - Зловмисники використовують програмне забезпечення на основі словників, щоб спробувати з мільйонів можливих і найбільш часто використовуваних паролів;

7 - Коли ви використовуєте його, пам’ятайте, що це благодатне середовище для хакерів, щоб викрасти вашу конфіденційну інформацію або навіть отримати доступ до вашого смартфона/ноутбука

8 - Як тільки ви виходите в Інтернет, ви починаєте створювати сліди інформації про себе. Це відомо як ваш цифровий слід. Кіберзлочинці можуть використовувати цю інформацію проти вас, використовуючи її для створення переконливих шахрайств, спрямованих на вас чи когось, кого ви знаєте.

9 - Незважаючи на це, програмісти та виробники програмного забезпечення дуже обережні, щоб захистити кінцевих користувачів, але особиста кібербезпека схожа на замок ваших дверей. Крім того, кібербезпека також є обов’язком кожного.

Більшість проблем із кібербезпекою залежить від оновлення ваших знань про новітні тенденції злому та шкідливого програмного забезпечення. У багатьох випадках успіх кіберзагроз був пов’язаний із незнанням або недбалістю деяких простих порад із безпеки.

10 - Люди можуть заперечувати використання технологій безпеки, не дотримуватись протоколів безпеки, брати участь у шкідливій діяльності, яка створює значні загрози для них та організацій, і недооцінювати шанси стати жертвами порушення кібербезпеки.

1.3 Визначення напрямків роботи зі створення системи кібербезпеки

З огляду на викладені вище фактори ми можемо визначити та сформулювати основні елементи нашої системи кібербезпеки.

Оскільки ми маємо 2 тісно пов'язані пункти(Зараження ШПЗ, відсутність АПЗ), то важливою частиною нашої системи буде вибір та налаштування АПЗ.

Інше важливе питання використання паролів, так за даними[9] майже 3 з 4 споживачів використовують повторювані паролі, багато з яких не змінювалися протягом п'яти і більше років. Тому близько 40 відсотків опитаних стверджують, що минулого року у них був «інцидент з безпекою», тобто у них зламали обліковий запис, вкрали пароль або отримали повідомлення про зламану їх особисту інформацію. Також 21% людей використовує паролі, що старші за 10 років. Саме через таке ставлення є важливим покращити цю сферу безпеки. Таким чином 2 пунктом створення нашої системи буде написання програми з створення паролів, та перевірки їх надійності.

Варто розуміти, що під час проектування та подальшої побудови систем, та інших рішень в яких будуть задіяні люди, одною з основних умов забезпечення безпеки, є наявність чітко визначеного набору/переліку правил поводження, застосування, праці, взаємодії користувача з іншими особами/приладами в цій системі і поза нею та їх дотримання (якщо це може мати відношення до системи в якій необхідно забезпечити захист). Саме тому визначення таких правил буде останнім пунктів даної роботи.

Висновки за розділом 1

Таким чином в результаті пошуку тенденцій в питаннях особистої кібербезпеки, та огляду актуальних робіт покій тематиці, ми можемо стверджувати, що основними напрямками захисту варто обрати:

1) Вибір і налаштування АПЗ;
2) Написання ПЗ для створення паролів;
3) Створення правил поведінки користувача

РОЗДІЛ 2 - ІНСТРУМЕНТИ ТА ВИМОГИ ДЛЯ СТВОРЕННЯ СИСТЕМИ

2.1 Вимоги до АПЗ та вибір АПЗ

Оскільки розроблювана система є персонально і призначена для використання звичайними користувачами основними вимогами будуть:

1. Надійність АПЗ;
2. Можливість захисту в реальному часі;
3. Простота налаштування та встановлення АПЗ;
4. Дешевизна обраного АПЗ;

Під вимоги підпадає вбудований захисник Windows 10 – Microsoft Defender, саме його і будемо використовувати в побудові нашої системи.

Він є безкоштовним та пропонує наступний функціонал:

1. Захист в реальному часі;
2. Сканування пристрою на наявність ШПЗ(швидке/повне/автономна);
3. Захист у хмарі;
4. Захист від підробок;
5. Створення винятків;
6. Контрольований доступ до папок.

Детальніше про вищевказані пункти в РОЗДІЛІ 3

2.2 Вимоги для ПЗ зі створення паролів

Розробку даного виду ПЗ ми будемо здійснювати самостійно, окрім ього для захисту користувачів можна використати наступне ПЗ.

2.2.1 Keypass

KeePass — це безкоштовний менеджер паролів з відкритим кодом, який допомагає вам безпечно керувати своїми паролями. Ви можете зберігати всі свої паролі в одній базі даних, яка заблокована головним ключем. Тож вам потрібно запам’ятати лише один головний ключ, щоб розблокувати всю базу даних. Файли бази даних шифруються за допомогою найкращих і найбезпечніших алгоритмів шифрування, відомих на даний момент (AES-256, ChaCha20 і Twofish).

Можливості:

- Підтримка багатьох стандартів шифрування(AES, Rijndael, SHA-256 і т.д);
- Можливість збереження великої кількості паролів;
- Портативність платформ;
- Експорт у файли;
- Імпорт з файлів;
- Підтримка груп паролів;
- Підтримка автоматичного введення;
- Пошук та сортування;
- Генератор випадкових паролів;

Можна побачити, що дане ПЗ має багато можливостей та функцій, але як було згадано раніше основним є можливість автоматичного створення паролів. Саме ця функція буде основною в майбутній програмі.

Основними функціями для програми будуть:

- Можливість створення паролю;
- Можливість створення парольної фрази
- Можливість налаштувань при створенні паролів;
- Можливість перевірки надійності паролю(але не парольної фрази);
- Збереження паролів у файл(опціонально).

2.2.2 Розробка ПЗ для створення паролів

1. Створення паролів буде відбуватись за допомогою вбудованих словників з визначеним набором символів;
2. Створення парольних фраз буде відбуватись за допомогою введенням користувачем тексту, що буде використаний для цього;
3. Перевірка паролю проводиться за наступним алгоритмом:
    1. L – довжина пароля.
    Якщо довжина пароля $L \leq 4$, то U=0
    інакше, якщо $5 \leq L \leq 7$, то U=6
    інакше, якщо $8 \leq L \leq 15$, то U=12
    інакше, якщо $16 \leq L$, то U=18

2. Якщо в паролі є букви, але тільки в одному регістрі, то U=U+5 інакше, якщо в паролі є букви в обох регістрах, то U=U+7
3. Нехай N - число цифр в паролі.
   Якщо число цифр в паролі $1 \leq N \leq 2$, то U=U+5
   інакше, якщо $3 \leq N$, то U=U+7
4. Нехай S - число спецсимволів (#$%@) в паролі.
   Якщо $1 \leq S < 2$, то U=U+5
   інакше, якщо $2 \leq S$, то U=U+10.
5. Якщо в паролі є букви в обох регістрах, спецсимволи і цифри, то U=U+6
   інакше, якщо тільки одного з цього немає, U=U+4.
6. Якщо $U < 16$ - пароль дуже слабкий
   інакше, якщо $15 < U < 25$ – слабкий
   інакше, якщо $24 < U < 35$ – середній
   інакше, якщо $34 < U < 45$ – сильний
   інакше, якщо $44 < U$ – дуже сильний

Блок схема створеного алгоритму виглядає наступним чином:

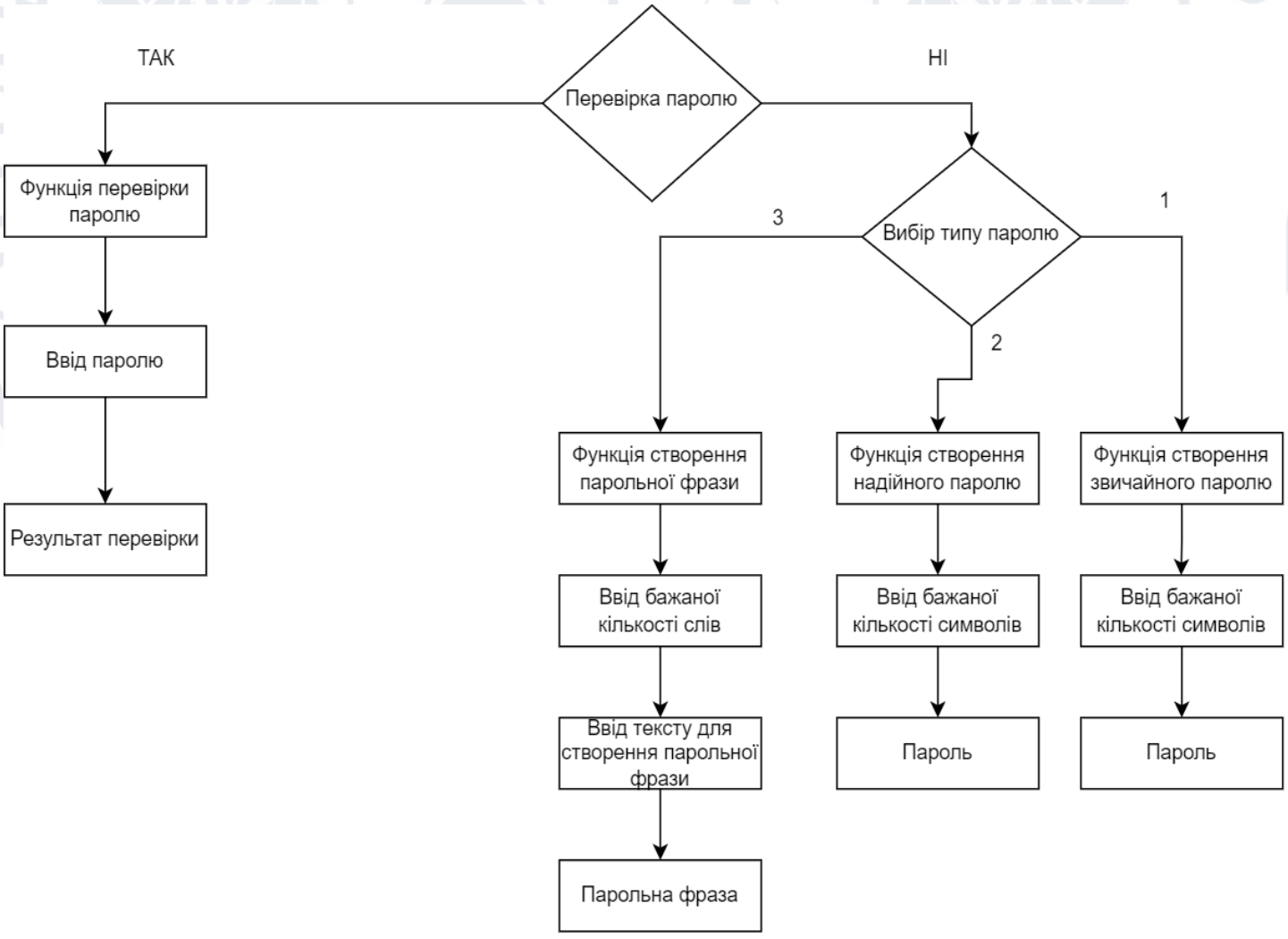

Рис. 2.1 – Блок схема алгоритму для створення та перевірки паролів

Як можна помітити дана схема не є складною, як і програма, що створена нами. Попри це алгоритм цілком виконує своє завдання див. розділ 3.1 .

Варто розуміти, що даний алгоритм являє собою мінімальний набір функціоналу, що необхідний для підвищення безпеки паролів на достатній для звичайного користувача рівень. Алгоритм, що буде приведений в ДОДАТКУ А, можна значним чином покращити пропозиції будуть наведені в РОЗДІЛІ 3.

2.3 Правила поводження для користувача

Як було згадано вище, основною умовою персональної безпеки є особиста відповідальність в даному питанні. Саме тому створення подібних правил є необхідною умовою для успішного функціонування системи. Залежність безпеки системи можна побачити на рисунку нижче.

Рис.2.3 – відображення важливості втілення і використання певних засобів при створення безпечного середовища для користувача

Для створення коректного та корисного набору правил вони мають мати такі властивості:

- Актуальність –правила мають бути актуальними для визначеної в них ситуації;

- Охоплюваність – іншими словами кількість правил для предметної області, вона має бути оптимальною;
- Визначеність – правила мають бути чітко визначеними;
- Однозначність – правила мають мати єдине трактування;
- Несуперечність – правила не повинні суперечити одне одному;
- Зрозумілість – правила повинні бути зрозумілими користувачу;
- Адекватність – правила мають висувати вимоги, що є можливими для користування, в деяких умовах зручними для користувача;
- Оновлюваність – правила мають переглядатись з певною періодичністю для підтримки їх актуальності.

Якщо дотримуватися вищевказаних вимог, можна створити корисний і зручний набір правил, що послугує для забезпечення високого рівня захисту з боку користувача.

Самі правила будуть наведені в РОЗІЛ 3.

Висновки за розділом 2

Отже, тепер ми маємо чітке уявлення, якими саме будуть елементи нашої системи, та які вимоги ми висуваємо до них. За допомогою вищевказаного була проведена розробка і створено парольне ПЗ, та визначені необхідні умови для створення ефективних та актуальних правил для користувача.

РОЗДІЛ 3 – НАЛАШТУВАННЯ ТА ВИПРОБУВАННЯ ОБРАНИХ МЕТОДІВ ТА ЗАСОБІВ

3.1 Налаштування Windows 10 – Microsoft Defender

Нижче будуть описані кроки для налаштування Windows 10 – Microsoft Defender, що дадуть змогу підвищити рівень безпеки пристрою.

1) Зайти в «Настройки від захисту і загроз»
2) Увімкнути такі функції – «Захист у реальному часі», «Захист у хмарі», «Автоматичне надсилання зразків», «Захист від підробок» див. рисунок 3.1

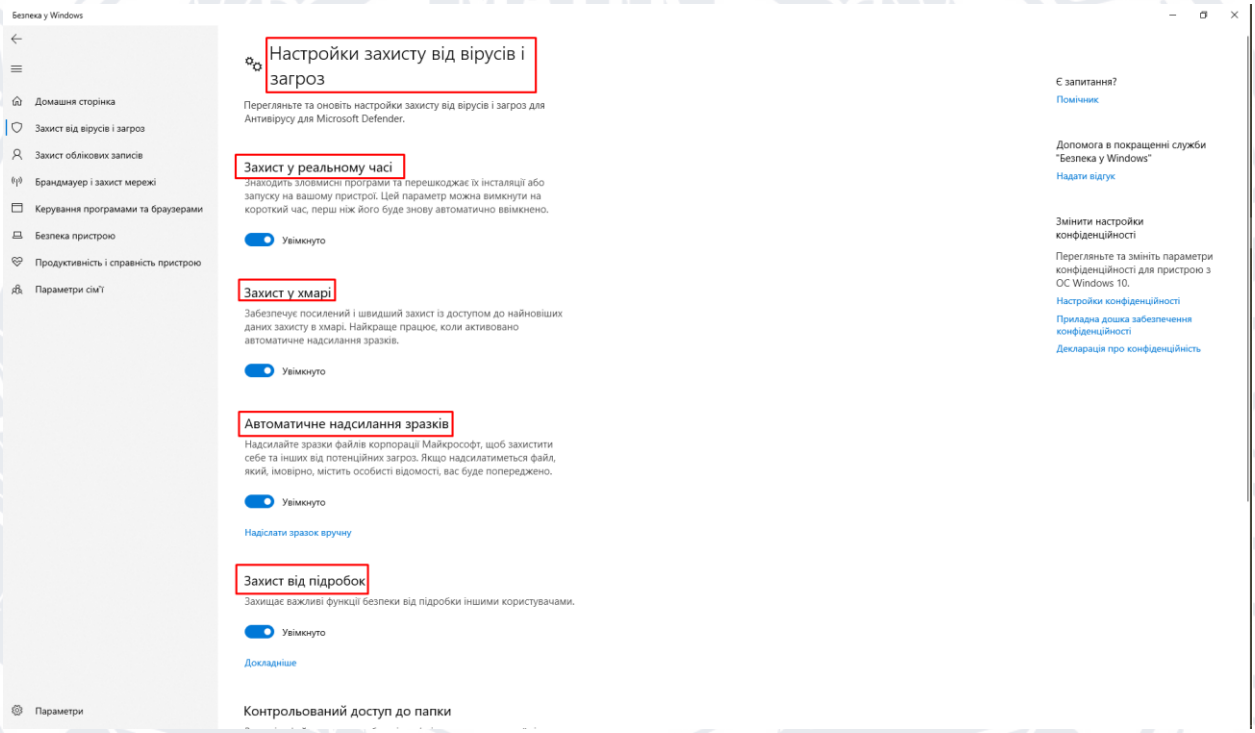

Рис. 3.1 - необхідні параметри захисту

3) При підозрі на віруси зайти в «параметри сканування», натиснути «Повна перевірка», якщо нічого не було знайдено, повторно запустити сканування з параметром «Перевірка автономним модулем Microsoft Defender» див. рисунок 3.2

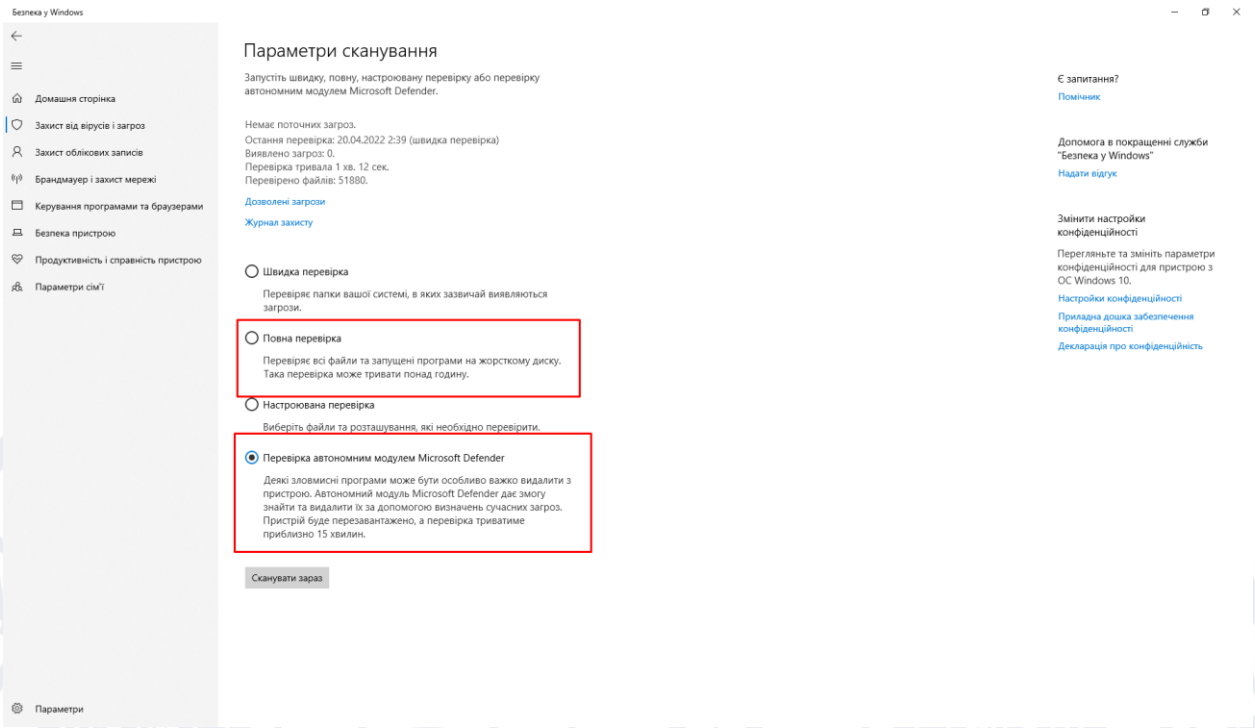

Рис.3.2 – параметри сканування

Тепер коли захист в реальному часі увімкнено можна перевірити чи працює дане ПЗ. Для цього в безпечному середовищі спробуємо запустити ШПЗ.

Результати:

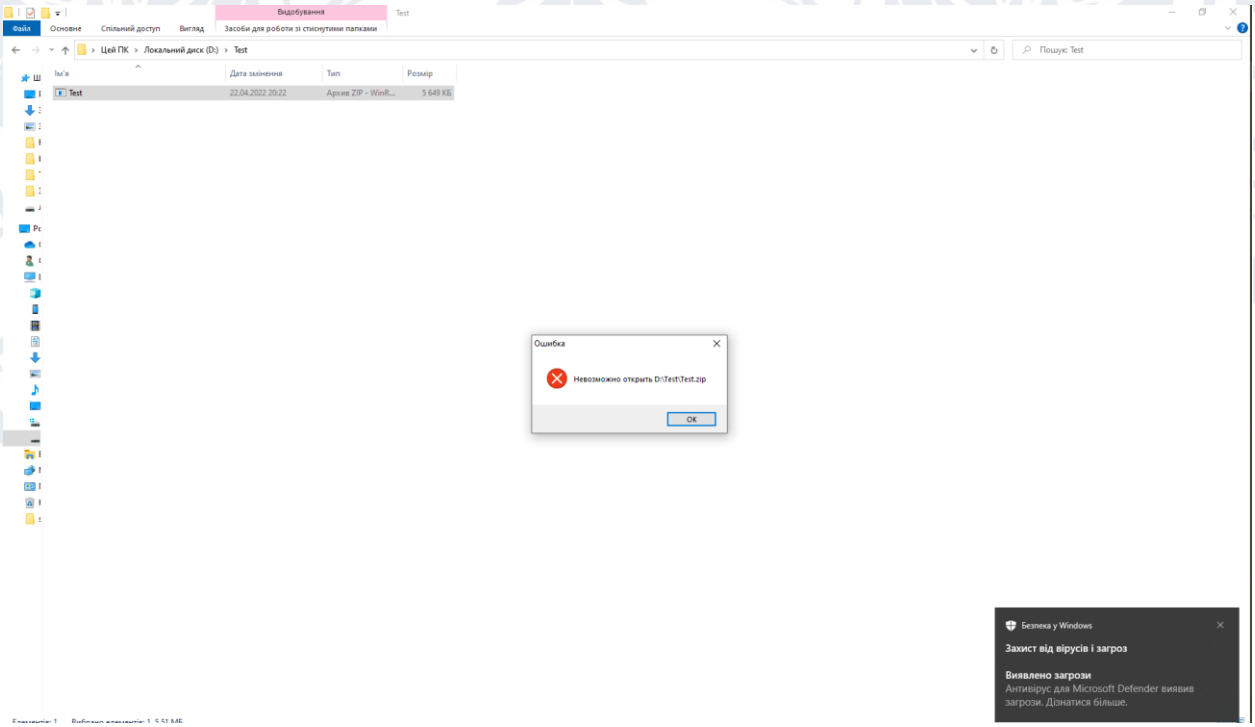

Рис.3.3 - Результат спроби запуску файлу

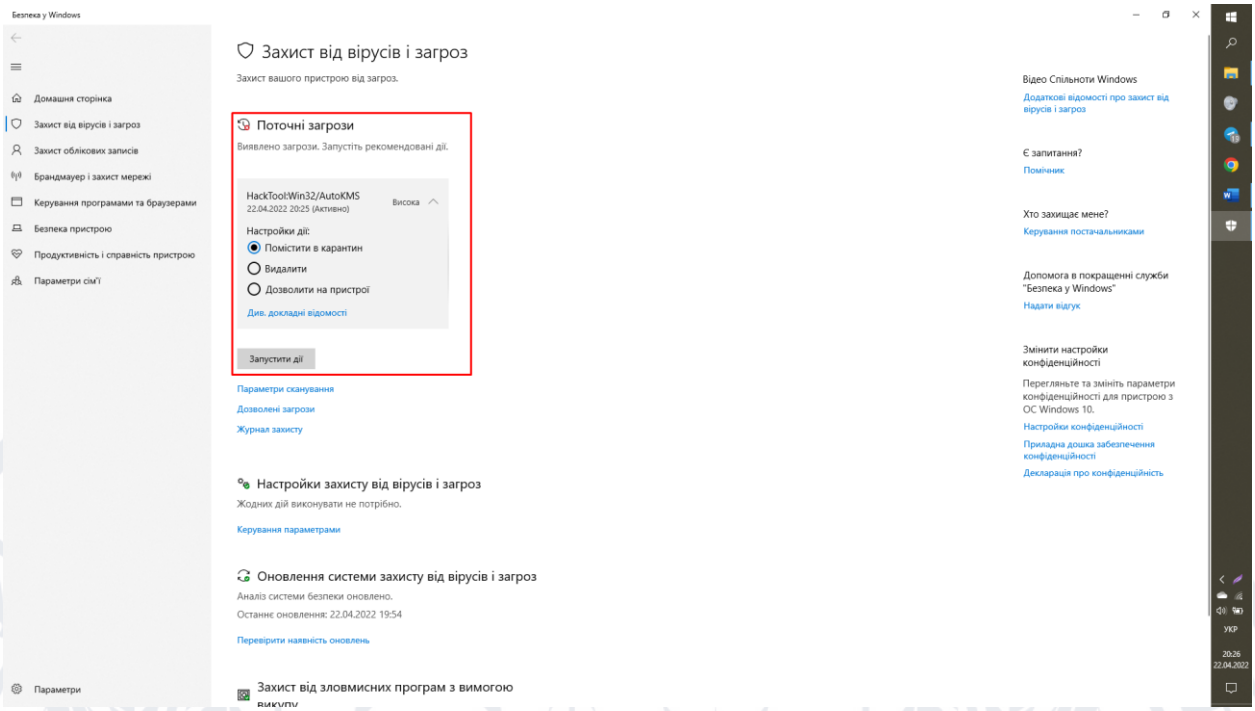

Рис.3.4 – Можливі дії відносно ШПЗ

«Помістити в карантин» - ізолювати ПЗ

«Видалити» - видалити ПЗ з пристрою(бажана дія, якщо є будь які сумніви, щодо ПЗ»

«Дозволити на пристрої» - дозволити використання даного ПЗ на пристрої(якщо є повна впевненість в ПЗ»

За допомогою вищенаведених налаштувань можна забезпечити себе від можливих загроз, що можуть потрапити на ваш ПК.

3.2 Практичні можливості ПЗ для створення паролів

Тут ми наведемо приклади використання створеного нами ПЗ, та наведемо можливі рекомендації його покращення.

3.2.1 Функція перевірки паролів

Використаємо 3 паролі – слабкий, сильний та дуже сильний створений програмно.

Слабкий – qsefth

Сильний - i7vVMGSSR.4TSjC

Дуже сильний - 94,~8398q~R#{9g26.

Рис. 3.5 - результат перевірки слабкого паролю

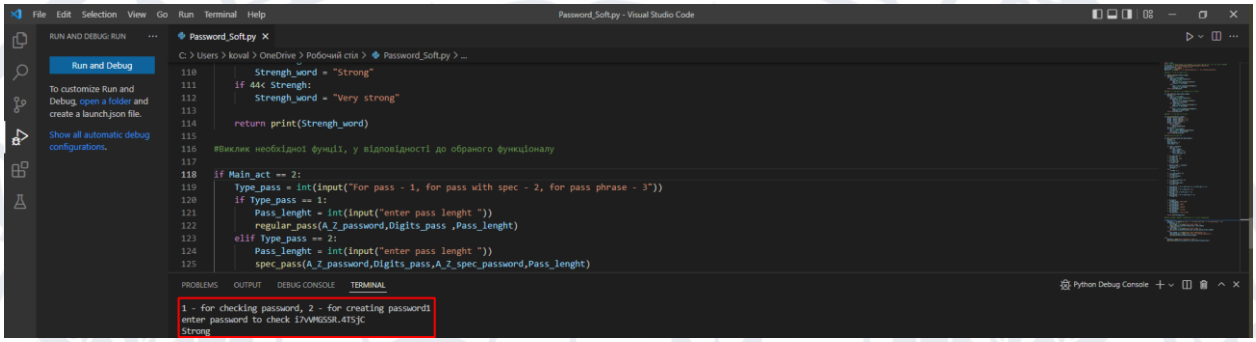

Рис. 3.6 – результат перевірки сильного паролю

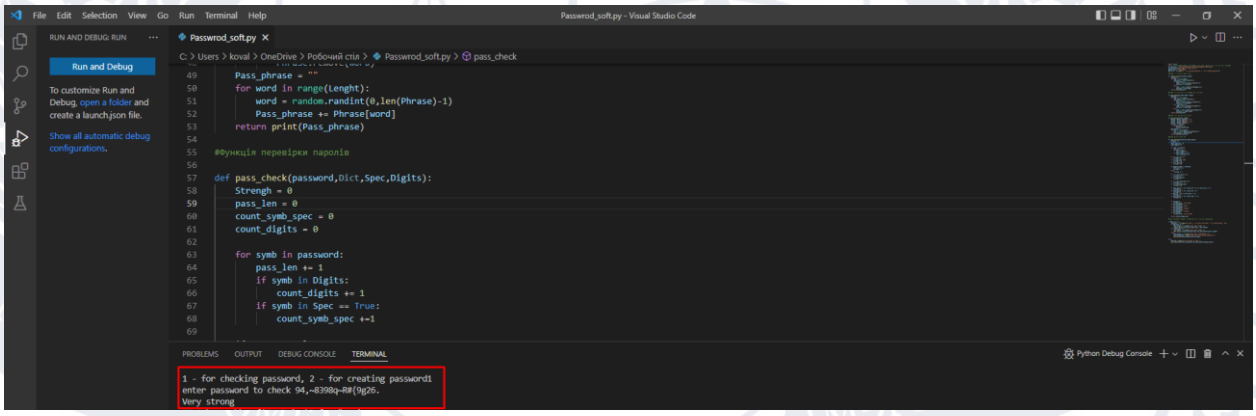

Рис. 3.7 – результат перевірки дуже сильного паролю створеного нашим ПЗ

3.2.2 Функції створення паролів та парольної фрази

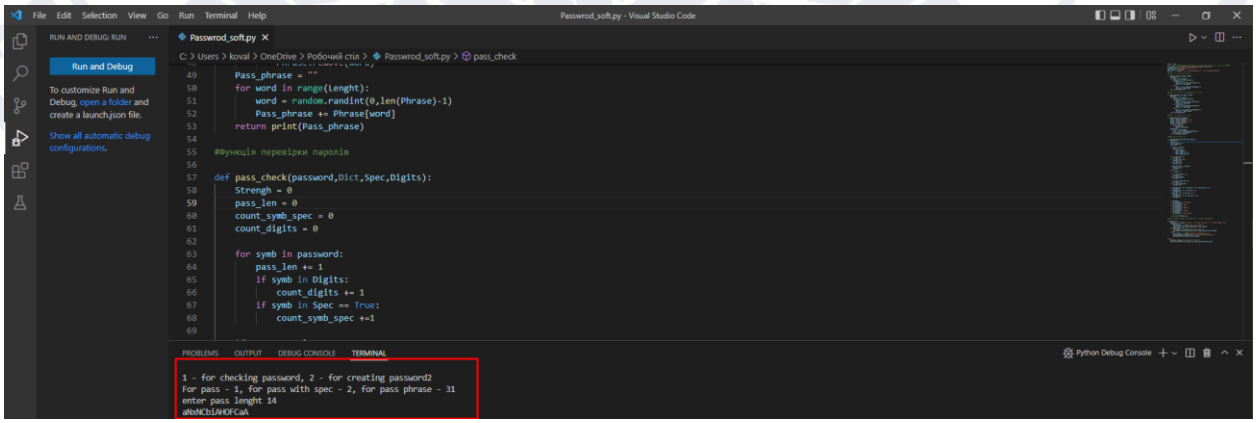

Рис. 3.8 – результат створення звичайного паролю, лише з букв

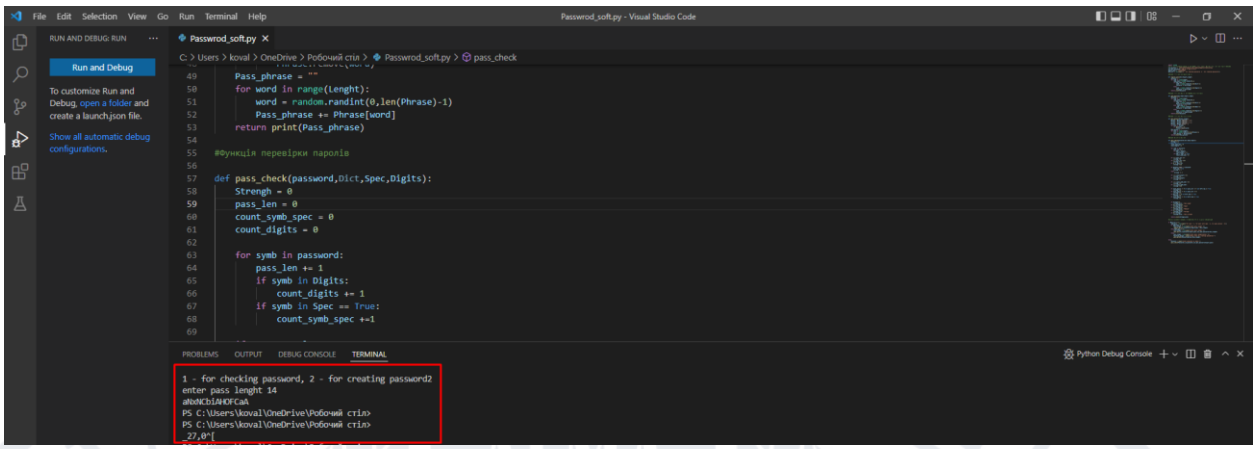

Рис. 3.9 – результат створення паролю зі спеціальними символами

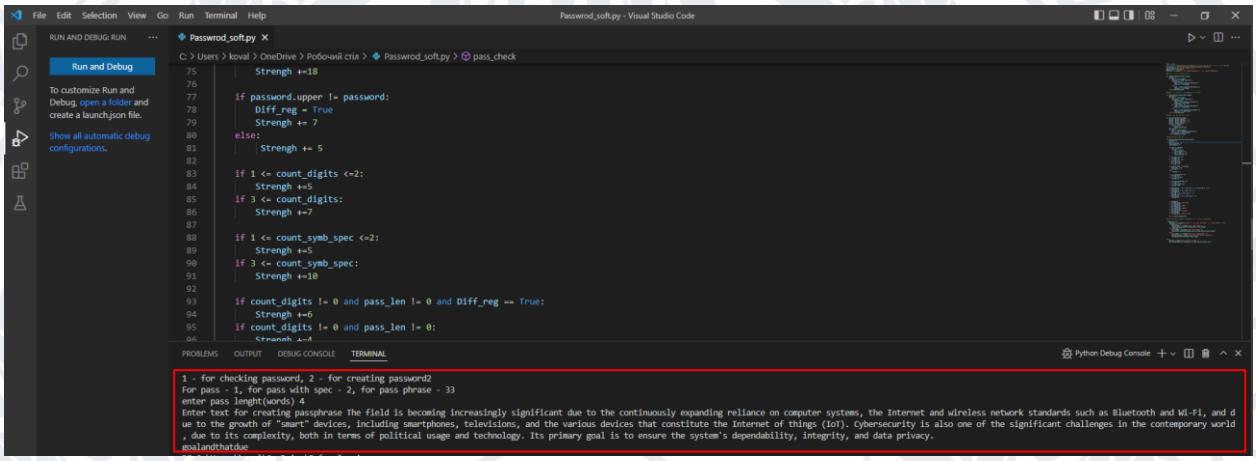

Рис. 3.10 – результат створення фрази на 4 слова з заданого тексту

Рекомендації з можливого покращення ПЗ:

- Створення перевірок для коректного вводу даних користувачем(пусті поля, хибні типи змінних і тд.);
- Можливість збереження паролів(у документ, на хмару);
- Розширення фунціоналу, шляхом використання додаткових бібліотек;
- Покращення процесу створення парольних фраз, шляхом заміни легких, популярних слів на їх іншомовні аналоги, заміни слів на певні символи «перший – 1» і тд.

3.3 Написання правил для користувача

Нижче будуть наведені правила, що мають на меті забезпечити кібербезпеку користувача.

1) Умови використання ПК:
    a. На пристроях повинно бути встановлено АПЗ;
    b. ПЗ на пристроях повинно бути оновлене до останньої версії;
    c. Відсутність неліцензійного ПЗ;

d. Остання перевірка на ШПЗ повинна бути не пізніше 5 днів.
e. Намагатись використовувати ПК за відсутності третіх осіб поряд.

2) Поводження з ПК:
   a. Не залишати без нагляду в місцях, де до пристрою можуть отримати доступ треті особи;
   b. Не передавати пристрої третім особам без необхідності;
   c. При передачі третім особам(ремонт і тд.) пристрій не повинен містити інформації з обмеженим доступом;
   d. Не зчитувати пристроєм невідомі носії інформації(флеш-карти, компакт диски і тд.);
   e. При необхідності використання невідомих носіїв інформації використати гостьовий обліковий запис, попередньо перевіривши носій інформації на АПЗ;
   f. Не вимикати/змінювати налаштування безпеки, якщо це може призвести до збільшення вірогідності компроментаціїданих.

3) Поводження з паролями паролів:
   a. Довжина паролю повинна становити 8 і більше символів;
   b. Використовувати спеціальні символи при створені паролю(тильда, знак оклику, фігурні дужки та ін.)
   c. Змінювати налаштування паролю для входу в систему примиинанні один раз на місяць, або при їх компрометації.
   d. Не передавити паролі третім особам;
   e. Не зберігати дані про пароль, в місцях, де він може бути скомпрометований(записи на робочому місці і тд.);
   f. Не використовувати один і той самий пароль двічі, або для доступу для різних облікових записів;
   g. Не використовувати паролі, що містять особисту, легкодоступну інформацію(дата народження);
   h. Не використовувати паролі, що легко вгадати(password1);

i. Використовувати багатофакторну автентифікацію, де це можливо.

4) Поводження в мережі:

a. Уникати фішингових листів;

Ознаки фішингових листів[13]:

- Відправники вперше або нечасті;
- Орфографія та погана граматика;
- Загальні привітання(Організація, яка працює з вами, повинна знати ваше ім’я, і сьогодні легко персоналізувати електронний лист);
- Підозрілі посилання або неочікувані вкладення;
- Невідповідні домени електронної пошти.

Дії при отримані підозрілого листа

- Ніколи не натискайте жодних посилань або вкладень у підозрілих електронних листах
- Якщо підозріле повідомлення надійшло від вашої знайомої особи, зв’яжіться з нею іншим способом, наприклад текстовим повідомленням або телефонним дзвінком, щоб підтвердити його.
- Видаліть його.

b. Не завантажувати підозрілого ПЗ, яке може пропонуватись;

c. Не розкривати особистих даних невідомим особам, навіть якщо вони викликають довіру. Якщо особа представилась наприклад робітником банку спочатку перевірте цю інформацію/самостійно зв’яжіться банком.

d. Уникати фішингових сайтів

Ознаки фішингових сайтів:

- На сайті відсутнє безпечне з’єднання (домен сторінки оплати безпечного сайту має починатися з починається з https:\\ а не з http:\\).
- Сайт зареєстрований на ненадійному домені, створений на конструкторі сайтів, в адресному рядку відображається однакова адреса для всіх сторінок. І навпаки, якщо сайт зареєстрований на домені національного рівня .UA, – ресурсу можна довіряти.
- Наявність нульових комісій та інших неймовірних пропозицій. Деякі пропозиції занадто добрі, щоб бути правдою.
- Наявність контентних погрішностей. Граматичні та синтаксичні помилки у тексті, контенті, неактуальна інформація, сумнівний зовнішній вигляд.
- Легітимні сайти маскують введення карткових реквізитів (наприклад, зірочками) або використовують віртуальну клавіатуру, фішингові сайти – ні.

5) Поводження при здійсненні онлайн покупок :
   a. Намагатись здійснювати покупки з відомих, надійних інтернет – магазинів;
   b. При здійсненні покупки в ненадійному магазині користуватись післяплатою.
6) Інші настанови:
   a. Завжди бути уважним, щодо відвідуваних сторінок;
   b. Фільтрувати і аналізувати інформацію, яку отримуєте під час взаємодії з іншими користувачами;
   c. Якщо контент, сайт або співрозмовник здається підозрілим перепинити взаємодію з цим об’єктом;
   d. Слідкувати за новинами в сфері комп’ютерної безпеки;
   e. Намагатись розташовувати маршрутизатор в центрі приміщення.

Висновки за розділом 3

В результаті робіт проведених в РОЗДІЛ 3 було показано, як налаштувати вбудоване АПЗ, та його використання. Протестовано та продемонстровано деякий функціонал створеного ПЗ, надані рекомендації з його майбутнього покращення. Були створенні правила(настанови) користувачу, що доповнюють роботу та надають їй повноти в сенсі системи захисту.

Варто відмітити, що в рамках забезпечення безпеки були застосовані програмні засоби(зазвичай їх достатньо, щоб забезпечити достатній захист інформації, при правильному використанні таких), які є в наявності в пересічного користувача, та були використані додаткові спеціалізовані засоби, створенні власноруч.

Унікальність даної системи не полягає в унікальності окремих її компонентів, можна знайти безліч окремих порад для покращення стану кібербезпеки, але вони є окремими одне від одного. Її унікальність полягає в саме об'єднанні необхідних і достатніх компонентів в такий набір, що буде здатний значно збільшити рівень кібербезпеки користувачів, що будуть її застосовувати. За умови використання простих та зрозумілих кроків та вимог(зазвичай готові рішення мають в собі багато складових, які є надлишковими для звичайного користувача).

Варто тепер коли система готова в повній мірі важливим пунктом є її всебічна підтримка та розвиток, дана тематика не буде висвітлена в рамках цієї роботи, але є необхідною для згадування, так як саме вищевказані роботи будуть підтримувати безпеку на належному рівні.

ВИСНОВКИ

В роботі було:

1. Визначено, що найнеобхіднішим пунктом персонального кіберзахисту є створення набору правил для користувача;
2. Розглянуто поведінку з ПЗ. В тому числі створеним і протестованим власноруч ПЗ для створення паролів;
3. Створено та застосовано правила поводження для користувачів.

ВИКОРИСТАНІ ДЖЕРЕЛА

1) ЗАКОН УКРАЇНИ Про захист інформації в інформаційно-телекомуніка-ційних системах – 1994.
2) Єжова Л. Ф. Інформаційний маркетинг: Навч. посібник. / Л. Ф. Єжова. – Київ, 2002. – 560 с
3) Кібер злочинність в Україні Ера цифрових технологій – ера нових зло-чинів. – Режим доступу до ресурсу: https://uz.ligazakon.ua/ua/magazine_article/EA013606
4) Zaher T. 10 Most Important Basics of Personal Cyber Security You Must Know [Електронний ресурс] / Talab Zaher. – 2021. – Режим доступу до ресурсу: https://geekflare.com/basics-of-personal-cybersecurity/.
5) The Personal Cyber Security: First Steps. [Електронний ресурс] // Australian Cyber Security Centre – Режим доступу до ресурсу: https://www.cyber.gov.au/acsc/view-all-content/guidance/personal-cyber-security-first-steps-guide.
6) Personal Cyber Security: Next Steps Guide. [Електронний ресурс] // Australian Cyber Security Centre – Режим доступу до ресурсу: https://www.cyber.gov.au/acsc/view-all-content/guidance/personal-cyber-security-next-steps-guide
7) Kadena E. Human factors in cybersecurity: Risk and impacts : дис. канд. / Kadena Esmeralda, 2021. – 14 с.
8) Carly O. Password Statistics: The Bad, the Worse and the Ugly (Infographic) [Електронний ресурс] / Okyle Carly // entrepreneur. – 2015. – Режим дос-тупу до ресурсу: https://www.entrepreneur.com/article/246902
9) Cybersecurisy for you(passwords) [Електронний ресурс] // The Ohio State University – Режим доступу до ресурсу: https://cybersecurity.osu.edu/cybersecurity-you/passwords-authentication/passwords.
10) ЗОЛОТАР О. О. ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ЛЮ-ДИНИ : стаття. канд. / ЗОЛОТАР О. О., 2014. – 10 с.

ДОДАТОК А

Нижче буде приведений програмний код на мові Python, для створення паролів та парольних фраз

```
import random
# Створюємо неохідні змінні, з яких будуть створюватись паролі. Створюємо меня вибору функцій
A_Z_password = 'AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvXxYyZz'
A_Z_spec_password = "@#_-$.%^,}&*:{>~]?<["
Digits_pass = "1234567890"
Main_act = int(input("1 - for checking password, 2 - for creating password"))

#Функція створення звичайного паролю

def regular_pass(Dict,Digits,Lengh):
    Password = ""
    for symb in range(Lengh):
        type_symb = random.randint(0,1)
        if type_symb == 0:
            symb = random.randint(0,len(Dict)-1)
            Password += Dict[symb]
        else:
            symb = random.randint(0,len(Digits)-1)
            Password += Dict[symb]
    return print(Password)

#Функція створення паролю зі спеціальними символами

def spec_pass(Dict,Spec,Digits,Lengh):
    Password = ""
    for symb in range(Lengh):
        type_symb = random.randint(0,2)
        if type_symb == 0:
            symb = random.randint(0,len(Dict)-1)
            Password += Dict[symb]
        elif type_symb == 1:
            symb = random.randint(0,len(Spec)-1)
            Password += Spec[symb]
        else:
            symb = random.randint(0,len(Digits)-1)
            Password += Digits[symb]
    return print(Password)

#Функція створення парольної фрази

def pass_phrase(Phrase,Lenght):
    Phrase = Phrase.replace(",","")
    Phrase = Phrase.replace(".","")
    Phrase = Phrase.replace("!","")
    Phrase = Phrase.split(" ")
```

```
    for word in Phrase:
        if len(word) < 3:
            Phrase.remove(word)
    Pass_phrase = ""
    for word in range(Lenght):
        word = random.randint(0,len(Phrase)-1)
        Pass_phrase += Phrase[word]
    return print(Pass_phrase)

#Функція перевірки паролів

def pass_check(password,Dict,Spec,Digits):
    Strengh = 0
    pass_len = 0
    count_symb_spec = 0
    count_digits = 0

    for symb in password:
        pass_len += 1
        if symb in Digits:
            count_digits += 1
        if symb in Spec == True:
            count_symb_spec +=1

    if 5 <= pass_len <=7:
        Strengh +=6
    if 8 <= pass_len <=15:
        Strengh +=12
    if 16 <= pass_len:
        Strengh +=18

    if password.upper != password:
        Diff_reg = True
        Strengh += 7
    else:
         Strengh += 5

    if 1 <= count_digits <=2:
        Strengh +=5
    if 3 <= count_digits:
        Strengh +=7

    if 1 <= count_symb_spec <=2:
        Strengh +=5
    if 3 <= count_symb_spec:
        Strengh +=10

    if count_digits != 0 and pass_len != 0 and Diff_reg == True:
        Strengh +=6
    if count_digits != 0 and pass_len != 0:
        Strengh +=4
```

```
    if pass_len != 0 and Diff_reg == True:
        Strengh +=4
    if count_digits != 0 and Diff_reg == True:
        Strengh +=4


    if Strengh<15:
        Strengh_word = "Very weak"
    if 15< Strengh<25:
        Strengh_word = "Weak"
    if 26< Strengh<35:
        Strengh_word = "Medium"
    if 34< Strengh<45:
        Strengh_word = "Strong"
    if 44< Strengh:
        Strengh_word = "Very strong"

    return print(Strengh_word)

#Виклик необхідної фунції, у відповідності до обраного функціоналу

if Main_act == 2:
    Type_pass = int(input("For pass - 1, for pass with spec - 2, for pass phrase - 3"))
    if Type_pass == 1:
        Pass_lenght = int(input("enter pass lenght "))
        regular_pass(A_Z_password,Digits_pass ,Pass_lenght)
    elif Type_pass == 2:
        Pass_lenght = int(input("enter pass lenght "))
        spec_pass(A_Z_password,Digits_pass,A_Z_spec_password,Pass_lenght)
    else:
        Pass_lenght = int(input("enter pass lenght(words) "))
        Password_phrase = input("Enter text for creating passphrase ")
        pass_phrase(Password_phrase,Pass_lenght)

else:
    Password = input("enter password to check ")
    pass_check(Password,A_Z_password,A_Z_spec_password,Digits_pass)
```