МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ВОЛОДИМИРА ДАЛЯ

МЕТОДИЧНІ ВКАЗІВКИ

щодо виконання практичних завдань з курсу:
Кібербезпека в аспекті інформатизації
та діджиталізації суспільства

для здобувачів вищої освіти,
усіх спеціальностей та рівнів підготовки

(електронне видання)

Затверджено
на засіданні кафедри
"Інформаційних технологій та програмування"
Протокол № 07 від 14.03.2025

Київ 2025

УДК 004.01

Методичні вказівки щодо виконання практичних завдань з курсу «Кібербезпека в аспекті інформатизації та діджиталізації суспільства» для здобувачів вищої освіти, усіх спеціальностей та рівнів підготовки (електронне видання) / Розр: О.І. Захожай. – Київ: Вид-во СНУ ім. В. Даля, 2025. – 63 с.

У методичних вказівках наведена необхідна теоретична база, а також практичні рекомендації для виконання практичних завдань. Матеріали методичних вказівок можуть бути використані для виконання практичних занять як в аудиторному форматі із застосуванням обладнання лабораторій та комп'ютерних класів, так і самостійно у віддаленому режимі.

Розробник	О.І. Захожай, зав. кафедри, д.т.н.
Відп. за видання	О.І. Захожай, зав. кафедри, д.т.н
Рецензент	Д.М. Марченко, професор, д.т.н.

ЗМІСТ

ВСТУП

Курс «Кібербезпека в аспекті інформатизації та діджиталізації суспільства» розроблений спільно з Perdue University (США) в рамках співпраці в освітній сфері та підвищення інформаційної обізнаності майбутніх фахівців незалежно від їх сфери професійної діяльності.

Метою курсу є опанування сучасними фахівцями-користувачами інформаційних систем, технологій та сервісів основних аспектів інформаційної та кібербезпеки. Курс направлений на те, щоб надати майбутнім фахівцям знання та вміння організувати власну безпечну взаємодію в сучасному цифровому світі. Відомо, що стрімкий розвиток комп'ютерних систем та інформаційних технологій утворює нові виклики та загрози, пов'язані з безпечністю та приватністю особистих «цифрових» даних, випадками «цифрового» шахрайства тощо. Цей курс спрямований навчити безпечній взаємодії користувачів в цифровому світі.

Практичні завдання охоплюють найпоширеніші кейси цифрової взаємодії, які пов'язані з можливими негативними наслідками інформаційної та кібер небезпеки. Кожне практичне завдання представляє опрацювання ефективних сценаріїв убезпечення власних цифрових даних та приватності під час різноманітних застосувань цифрових сервісів, як то: парольна політика та безпечний менеджмент паролів власних цифрових акаунтів, забезпечення безпечності електронного листування, електронний документообіг, основи криптування та цифрові підписи, а також інструменти цифрового спостереження за діями користувачів.

ПРАКТИЧНЕ ЗАВДАННЯ 1.
ПАРОЛЬНА ПОЛІТИКА ТА ВИКОРИСТАННЯ МЕНЕДЖЕРІВ ПАРОЛІВ

1. Короткі відомості

Одна з найважливіших складових запобігання компрометації особистих даних - це розуміння того, як кіберзлочинці можуть намагатися отримати доступ до критично важливих даних.

Методи атак продовжують розвиватися і ставати все більш витонченими, надаючи кіберзлочинцям великий інструментарій, який можна використовувати проти користувачів у кіберпросторі.

Надалі наводиться перелік найпоширеніших прийомів несанкціонованого отримання паролів користувачів, на які слід звернути увагу.

1) Вразливості протоколів доступу.

Іноді програмний код має недоліки, які використовуються для обміну або шифрування паролів. Атакуючі можуть використовувати ці вразливості для злому паролів.

В якості прикладу, можна навести метод зламування паролів WEP, хоча, фактично, це використання вразливості ключів шифрування застарілого на сьогодні протоколу WEP, який колись використовувалися для захисту бездротових мереж. Щоб мінімізувати ризик отримання паролів через цей напрямок, треба переконатися, що апаратно-програмне забезпечення оновлено. Так використання застарілих WiFi-роутерів, які не підтримують протоколи WPA2, а працюють з протоколами WEP дозволять бездротове підключення до мережі, але дані, що будуть передаватися таким чином (в тому числі і паролі підчас аутентифікації) будуть у небезпеці. На даний час WEP технологія є застарілою, оскільки її злом може бути здійснений лише за кілька хвилин. Тим не менш, вона продовжує широко використовуватися. Деякі виробники маршрутизаторів, як і раніше, надають WEP як опцію шифрування і можна в найсучаснішому роутері, навіть по необережності обрати саме такий протокол. Замість WEP необхідно використовувати WPA/WPA2, який загалом безпечний.

На жаль, зловмисники виявляють і використовують уразливості, перш ніж цей факт стане відомим. З цієї причини не можна ніколи бути впевненими, що вразливість нашого апаратно-програмного забезпечення не зазнала атаки.

2) Повний перебір (або метод «грубої сили», англ. brute force)

Повний перебір відноситься до практики спроби підбору всіх можливих комбінацій букв і цифр, доки не підбереться той, який відповідає паролю.

Найкращий спосіб пом'якшити атаки з використанням грубої сили - це зробити так, щоб паролі були складними. Як правило, пропонується використання довгих паролів (вісім або десять символів) які містять непов’язану послідовність прописних та рядкових букв, числа, а також додаткових символів (?, !, _, @ та ін.). При цьому категорично не рекомендується використовували будь-які смислові комбінації: слова або фрази.

Уникаючи слів і фраз ми гарантуємо, що наш пароль не може бути підібраний, запуском списку спільних паролів. Атакуючі часто використовують ці списки під час атак грубої сили, для того щоб зменшити кількість необхідних повторів підбору та зменшити час визначення парольної послідовності. Проте, обчислювальна потужність комп'ютерних систем зростає дедалі більше, як і здатність атакуючих розгортати подібні атаки. Те, що вважається досить довгим паролем сьогодні, може бути небезпечним у майбутньому, тому що завтра комп'ютери зможуть перевіряти можливі паролі швидше, ніж сьогодні.

Чим довше ваш пароль, тим більше кількість можливих комбінацій, які атакуючий повинен спробувати, щоб підібрати пароль. В цьому випадку, час підбору паролю значно збільшується і, в ідеальному випадку, зміна паролю частіше, ніж час його підбору – унеможливлює успішну кібератаку.

Але, складність паролю має і зворотній бік. В цьому випадку ускладнюється швидке введення його з клавіатури, що дозволяє візуально фіксувати послідовність натискань клавіш і, відповідно, парольну комбінацію. Тому, найбезпечніший це такий пароль, який користувач, незважаючи на його складність, може швидко вводити.

Підміна – спуфінг (англ. spoofing)

Зловмисник може «обманювати» користувача підставляючи підробний сайт з авторизацією, дизайн якого повністю відповідає оригінальному сайту. Таким чином, користувач, нічого не підозрюючи, заповнює поля логіну і паролю на підробному сайті і сам власноруч надає власні облікові дані зловмисникові.

Атаки за допомогою спуфінгу простіше виконати, ніж може здатися на перший погляд. Будь-хто, хто контролює налаштування конфігурації мережі, може легко перенаправити відвідувачів на підроблену версію будь-якого сайту, який він забажає, змінивши конфігурації DNS.

Іноді також можливо "отруювати" кеші DNS в мережах, щоб виконувати атаки спуфінгу, навіть без прямого управління мережними налаштуваннями.

Найкращий спосіб уникнути атаки за допомогою спуфінгу - це підключення тільки до мереж, яким ви довіряєте. Наприклад, атаки спуфінгу це одна з причин, чому не рекомендується підключатися до випадкових мереж у публічних місцях: аеропортах, вокзали, парки відпочинку тощо.

Додаткова небезпека криється в тому, що гаджети мають функцію запам'ятовувати дані входу мереж до яких колись було під'єднання, тому зловмисник може створити точку доступу з CCID і паролем як загальновідома і наш пристрій потрапляючи до зони дії цієї мережі автоматично підключається до неї і стає мішенню для спуфінгу. При цьому, користувач може навіть не підозрювати про таке небезпечне підключення. Так, проходячи з власним смартфоном в кишені в зоні дії небезпечної мережі він і не підозрює, що смартфон, з включеним wifi і пошуком доступної мережи, автоматично приєднується до цієї мережи.

Будь-який користувач може налаштувати точку доступу з таким мережевим ім'ям, як Free Wifi, а потім використовувати spoofing для крадіжки паролів.

Можна власноруч допомогти усунути «отруєння» DNS та інші вразливості, постійно оновлюючи свої маршрутизатори та інше мережеве програмне забезпечення, а також запускаючи програмне забезпечення для виявлення вторгнень у мережі.

Також дуже важливим є відслідковування вмісту файлу “hosts” до якого операційна система першочергово звертається для розрішення імен веб ресурсів (англ. resolve), а потім, якщо не знаходить відповідності, вже звертається до вказаного в мережевій конфігурації DNS серверу. Таким чином, зловмисник може зробити додатковий запис до цього файлу та перенаправити користувача на небезпечний сайт. Цей файл є в різних операційних системах. Так, наприклад, в Microsoft Windows, за замовчуванням, він розташований у C:\Windows\System32\drivers\etc, в операційних системах сімейства Linux - /etc/hosts.

Нарешті, треба серйозно ставитися до попереджень у своєму веб-браузері про недійсні сертифікати при відвідуванні сайтів з професійним обслуговуванням, сертифікати яких повинні бути правильно налаштовані.

Зазвичай проблеми з сертифікатами зустрічаються на багатьох веб-сайтах, що погано обслуговуються, просто тому, що адміністратори не створюють правильні сертифікати, а не через фактичну заміну.

З цієї причини користувачі, на жаль, звикли ігнорувати попередження про проблеми із сертифікатами, які часто є ознакою атаки-підміни.

3) Атаки соціальної інженерії – фішінг (англ. fishing)

Такі атаки як фішинг базуються на тому, що за допомогою електронних листів та текстів, користувачів обманом змушують надати свої облікові дані, клацнути шкідливі посилання або вкладення, перейти на шкідливі веб-сайти тощо. Іноді фішинг та спуфінг використовуються разом.

У фішинговій атаці зловмисник використовує соціальну інженерію, щоб переконати користувача клацнути посилання або завантажити програмне забезпечення, яке краде паролі, або може призвести до хаосу іншими способами. Наприклад, електронний лист подібного вмісту: «Вітаємо, ви щойно виграли приз у 1 000 000 долларів США! Для отримання призу, перейдіть за посиланням ….».

На жаль, немає ніяких стійких до відмови технічних інструментів, які можна використовувати для запобігання фішингу. Найкращий захист полягає в тому, щоб навчати себе та інших користувачів, щоб ретельно замислюватися, перш ніж натискати посилання або приймати завантаження, навіть якщо воно, здається, із легального джерела і дуже заманливе.

4) Атаки за словником

При цьому різновиді атак зловмисник використовує список спільних слів, званий словником, щоб спробувати отримати доступ до паролів, очікуючи, що люди використовували спільні слова або короткі паролі. Їх методика також включає додавання чисел до і/або після загальних слів, щоб врахувати людей, які думають, що просте додавання чисел до і/або після утруднює вгадування пароля. В цьому випадку, як вже згадувалося раніше, важливим є дотримання політики складних паролів.

5) Атаки з розпиленням паролів

Розпилення паролів: форма атаки методом грубої сили, націленої на кілька облікових записів. При традиційній атаці методом грубої сили зловмисники намагаються кілька разів вгадати пароль одного облікового запису, що часто призводить до блокування облікового запису. При розпиленні паролів зловмисник пробує лише кілька найбільш поширених паролів для кількох облікових записів користувачів, намагаючись ідентифікувати людину, яка використовує пароль за замовчуванням або пароль, що легко вгадується. В цьому випадку також використовується, нажаль, дуже поширений підхід використання одного й того самого паролю для різних сервісів з аргументацією – «так легше запам'ятати». Категорично не рекомендується використовувати схожі облікові данні для аутентифікації до різних сервісів.

6) Атака із реєстрацією ключів

При цьому виді атаки зловмисник, встановлюючи програмне забезпечення для реєстрації ключів на пристрої жертви, як правило, за допомогою фішинг-атаки електронною поштою чи месенджерів, може перехоплювати натискання клавіш жертви, щоб отримати її логіни та паролі для різних облікових записів.

7) Атака через перехоплення трафіку

В таких атаках кіберзлочинці використовують програмне забезпечення, таке як аналізатори пакетів, для відстеження та перехоплення мережного трафіку, що містить інформацію про паролі. Якщо трафік не зашифрований або використовує слабкі алгоритми шифрування, захоплення паролів стає ще простішим. В цьому випадку, найнебезпечнішим і, нажаль, дуже поширеним є авторизація на веб ресурсах, які працюють на звичайному протоколі http, а не використовують захищене ssl з'єднання по протоколу https. Так логін і пароль пересилається від клієнта до сервера у відкритому, незашифрованому вигляді. Приклад такого сайту наведено на рисунку 1.1.

І, на останок, сценарій добровільного фішингу дуже складного і захищеного паролю, для того, щоб зловмисники не дуже напружувалися з брутфорсом нашого паролю☺ – подивіться як «чудово» це вирішується на рисунку 1.2

Послухалися рекомендацій вище, створили велику кількість паролів окремо для кожного сервісу! Як запам'ятати? – Нема проблем ☺ – як вам такий варіант, що представлений на рисунку 1.3?.

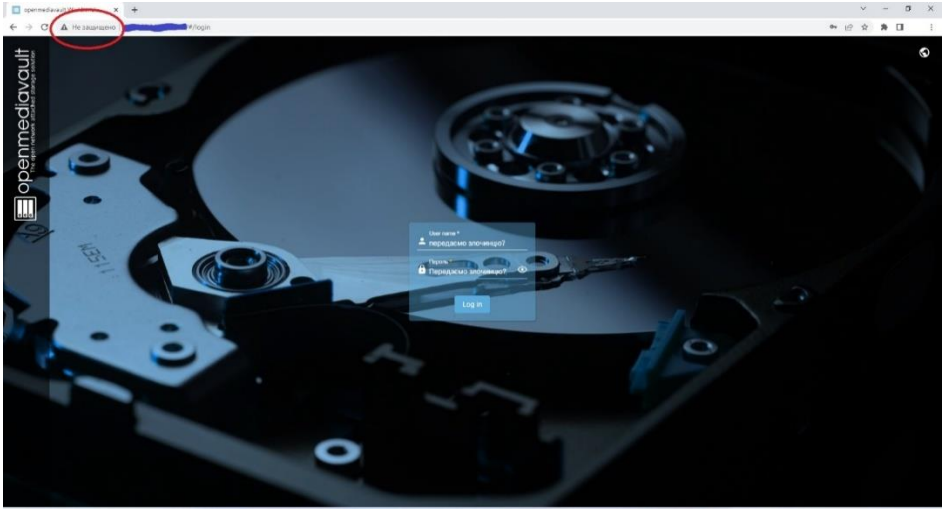


Рисунок 1.1 – Приклад веб-ресурсу, що використовує незахищене з’єднання за протоколом http

Рисунок 1.2 – Приклад «чудового» підходу до менеджменту паролів 😊
(фото з відкритих джерел)

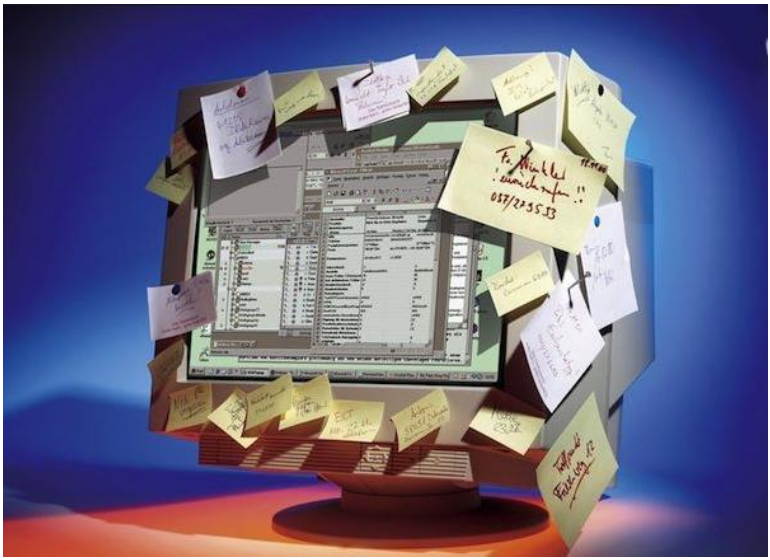


Рисунок 1.3 – Ось тепер точно надійно ☺ – для кожного сервісу – власний пароль! (фото з відкритих джерел)

2. Можливі сценарії уникнення компрометації паролів

Користувачі можуть використовувати ряд сценаріїв, щоб зловмисники не могли скомпрометувати їхню особисту інформацію за допомогою описаних вище методів. Серед них: надійні паролі, багатофакторна автентифікація та можливості єдиного входу. На додаток до цього, підкованість у сфері кібербезпеки має вирішальне значення для захисту.

Створення сильного пароля

Важливо розробити паролі, які неможливо забути і важко вгадати навіть для людини, яка може знати такі особисті деталі вашого життя, як назва вулиці, на якій ви виросли, або ім'я вашого першого собаки. Хоча додавання цифр і спеціальних символів до звичайних слів може здаватися привабливим, але кіберзлочинці вміють використовувати низку методів атаки, щоб зламати такі паролі. Уникайте використання наступних особистих даних у паролях:

- дні народження;
- телефонні номери;
- інформація про місце роботи.
- словосполучення, що включають назви фільмів, спортивних команд, пам’ятних місць тощо.
- просте заплутування загально відомого слова, наприклад: «P@$$w0rd».

Найкращими підходами до забезпечення надійності парольних комбінацій є:

- використання малоймовірні або випадкових комбінацій великих і малих літер, цифр і символів, за умови, що довжина комбінації - не менша за десять символів;

- зберігання парольної комбінації в таємниці, не розголошуючи її, а також не використовуючи для збереження паперові носії інформації, а також звичайні електронні (будь то флешки, жорсткі диски та ін.) - якщо збереження здійснюється в нешифрованому вигляді;
- не слід використовувати той самий пароль для декількох облікових записів, це збільшує обсяг інформації, до якої може отримати доступ кіберзлочинець, якщо йому вдасться зламати пароль;
- треба змінювати пароль кожні три місяці, щоб знизити ймовірність зламування облікового запису.

Додаткові заходи безпеки парольного доступу

Поодинока лінія захисту не ефективна для стримування передових кібератак. Щоб забезпечити надійний захист, потрібно використовувати кілька тактик. В якості додаткових інструментів забезпечення кіберзахищеності парольного доступу є використання багатофакторної аутентифікації та технології єдиного входу.

Багатофакторна аутентифікація (англ. MFA - Multi-Factor Authentication) полягає у підтвердженні особистості користувача, додаючи додатковий крок до процесу аутентифікації, чи то за допомогою фізичних чи мобільних токенів на основі додатків. Це гарантує, що навіть у разі злому пароля зловмисники не зможуть отримати доступ до інформації, так як для цього їм треба також отримати в своє розпорядження, наприклад, смартфон користувача і, навіть якщо й це вийшло – доступ до смартфону також може бути обмежений додатковими засобами захисту.

Єдиний вхід (SSO): дозволяє користувачам використовувати єдине безпечне ім'я користувача та пароль для кількох сервісів.

Оскільки поточні події змушують людей збільшувати кількість часу, який вони проводять у Мережі для роботи, електронного навчання та спілкування з сім'єю та друзями, а кіберзлочинці посилюють атаки, націлені на користувачів, важливо виконати перевірку стану безпеки для всіх облікових записів – оновити слабкі та застарілі паролі по мірі необхідності.

3. Практичний кейс

До вирішення надається наступна задача. Організувати роботу з сукупністю облікових даних для різних сервісів за умови використання усіх безпекових аспектів, викладених вище.

Умови вирішення наступні.

1) паролі повинні бути складні, що унеможливлює запам’ятовування усіх розрізнених комбінацій символів.

2) паролів може бути багато (в сучасному цифровому світі у кожного користувача кількість облікових записів на сервісах часто перевищує 100), що також унеможливлює запам’ятовування.

3) паролі треба періодично змінювати – що ще більше унемоджливлює запам’ятовування.

4) Якщо паролі неможливо запам’ятати – їх треба зберігати. Але неможна доля цього використовувати звичайні паперові носії, або створення текстових файлів на електронних носіях з переліком облікових записів.

Варіантом забезпечення вказаних умов є використання спеціального програмного забезпечення – менеджерів паролів.

Менеджери паролів призначені для створення унікальних, довгих, складних, легкозмінних паролів для всіх онлайн-облікових записів та безпечного зашифрованого зберігання паролів у локальному або хмарному сховищі. Це спростить вам завдання - потрібно буде тільки запам'ятати один пароль до сховища.

Поставимо додаткову умову – мінімізація фінансових витрат на організацію парольного менеджменту, а також можливість його використання на різних пристроях, які територіально розосереджені.

Можливі альтернативи:

1) використання хмарних сервісів менеджменту паролів;
2) використання локальних менеджерів паролів.

Хмарні сервіси менеджменту паролів повністю дозволяють забезпечети виконання основних умов 1-4. Також, хмарні рішення частково вирішують додаткову умову - розміщення програмного забезпечення менеджменту паролів на хмарі забезпечує доступ до нього з будь якої точки світу, будь якого пристрою і в режимі 24/7. Але, абсолютна більшість таких сервісів не є безкоштовними та потребують абонентської плати.

Локальні менеджери паролів також дозволяють забезпечити виконання основних умов 1-4, а також в інтернет просторі є безкоштовні рішення, що частково вирішує додаткову умову безкоштовності. Але, локальне збереження бази паролів не дозволяє забезпечити одночасне використання з багатьох пристроїв в режимі 24/7.

Рішення, що повністю задовольняє усім умовам – використання локального менеджеру паролів з додатковим налаштуванням синхронізації бази даних через безкоштовну хмару з довільною кількістю клієнтів на різних пристроях.

Алгоритм вирішення задачі.

В якості однієї з наявних альтернатив застосуємо програмне забезпечення локального менеджеру паролів Keepas. Keepas-клієнт використовує захищену та зашифровану базу даних облікових записів, що зберігається локально на одному пристрої з клієнтом. Це рішення є безкоштовним та має клієнти для різних платформ та операційних систем.

В якості хмари для синхронізації бази даних паролів можна використати будь-які рішення, що дозволяють встановити локально на довільній кількості пристроїв клієнти синхронізації. В якості прикладу використаємо хмару Microsoft OneDrive. У випадку реєстрації аккаунту Microsoft користувачу надається безкоштовно 5 Гбайт для збереження даних.

1. Якщо є Microsoft account – пропускаємо цей пункт. Для створення акаунту перейдемо на ресурс Microsoft за посиланням: https://account.microsoft.com/. Головна сторінка представлена нижче на рисунку 1.4.

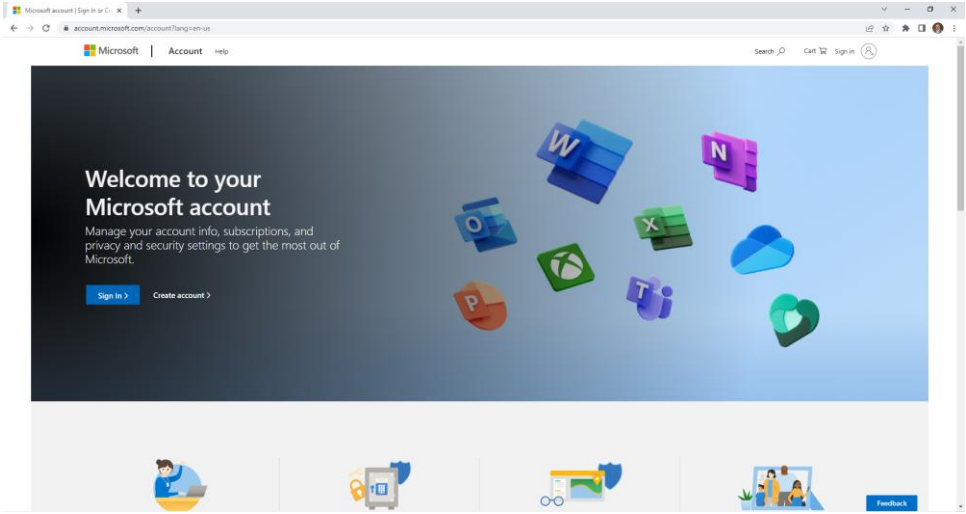


Рисунок 1.4 – Головна сторінка доступу до власних акаунтів Microsoft

Натискаємо на посилання “Create account” і далі відкривається вікно введення адреси електронної пошти, представлене нижче на рисунку 1.5.

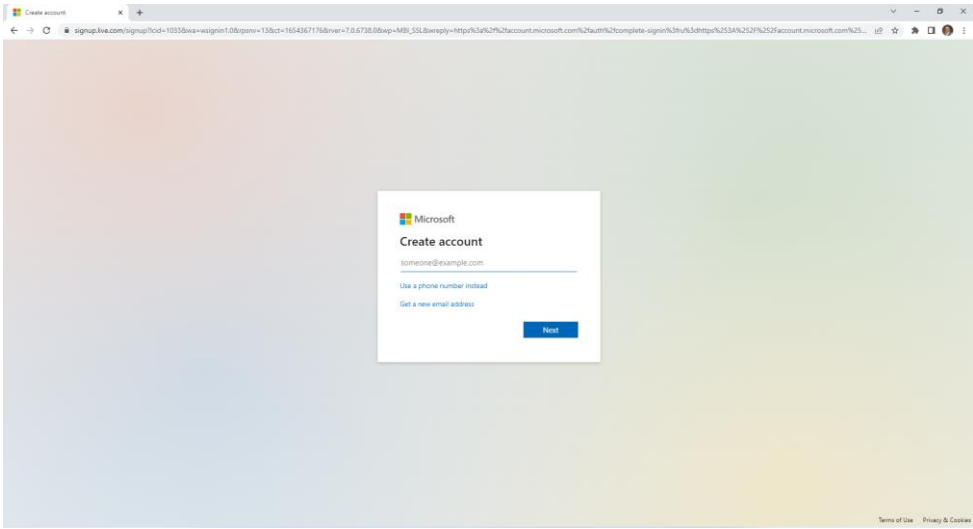


Рисунок 1.5 – сторінка авторизації на сервісі Microsoft

В цьому вікні треба задати адресу електронної пошти, яка буде використовуватися для створення акаунту. Можна використати або існуючу адресу

електронної пошти або створити нову, натиснувши на посилання “Get a new email address”. Нову адресу пропонується створити в одному з двох доменів Microsoft: @outlook.com або @hotmail.com. Після зазначення адреси йде запит на створення паролю акаунту і потім – процедура підтвердження валідності пошти – запит на введення коду, що автоматично надсилається на вказану адресу електронної пошти.

2. Налаштуємо клієнт синхронізації хмари Microsoft OneDrive. Перейдемо за посиланням https://www.microsoft.com/uk-ua/microsoft-365/onedrive/download, завантажимо звідси інсталяційний пакет та встановимо клієнт. Після встановлення, автоматично з’явиться вікно налаштувань, яке проілюстровано далі на рисунку 1.6.

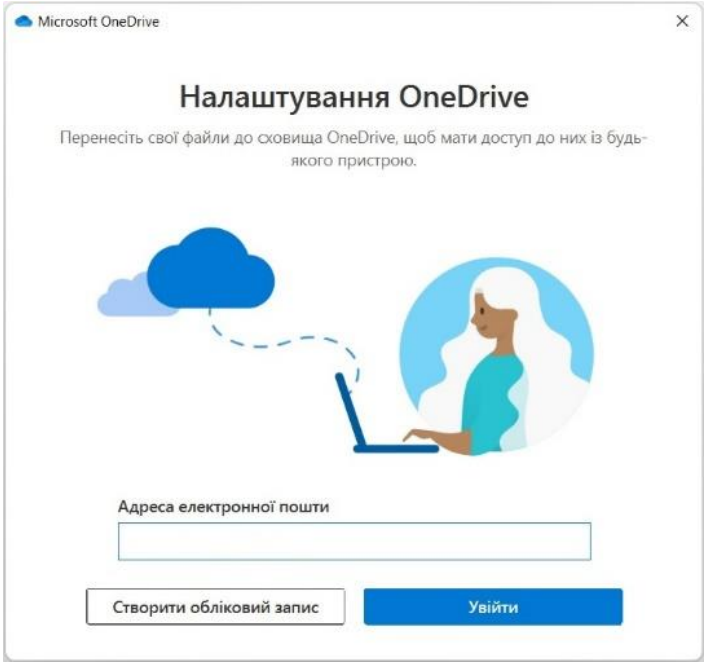


Рисунок 1.6 – Авторизація в клієнті синхронізації з хмарних сервісом Microsoft OneDrive

Після введення логіна і пароля облікового запису Microsoft, з’являється вікно запиту на шлях до локальної папки, яка буде використовуватися для синхронізації з хмарою, яке проілюстровано на рисунку 1.7.

Вказавши бажану папку, можна далі погоджуватися з наведеною інформацією в серії вікон. На завершальному етапі буде запропоновано встановити чи ні застосунок синхронізації OneDrive на мобільний телефон і після завершення інсталяції з’явиться вікно, показане на рисунку 1.8.

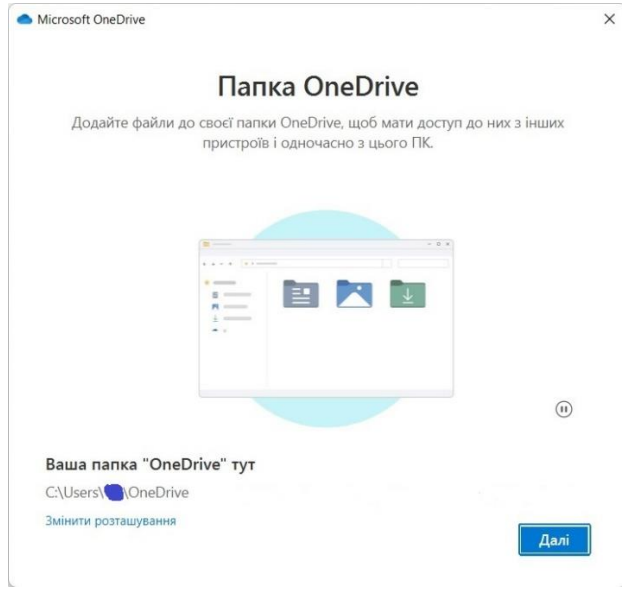


Рисунок 1.7 – Вікно налаштувань шляху для теки, яка буду використовуватися для синхронізації з хмарним сервісом OneDrive

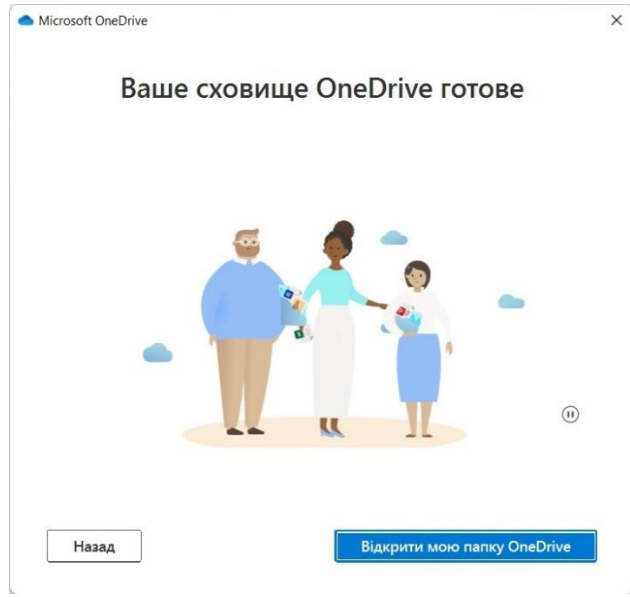


Рисунок 1.8 – Вікно завершення налаштування клієнта синхронізації з хмарним сервісом OneDrive

Тепер увесь вміст локальної папки буде синхронізований з хмарним простором зберігання даних відповідного акаунту Microsoft.

3. Тепер все готове для встановлення та налаштування застосунку менеджменту паролів Keepass. Для установки в середовищі Windows існує два варіанта – використання інсталяційного пакету або portable-версія. Відповідні завантаження можна зробити з сайту проєкту за посиланням: https://keepass.info/download.html. Вигляд сторінки представлений нижче на рисунку 1.9.

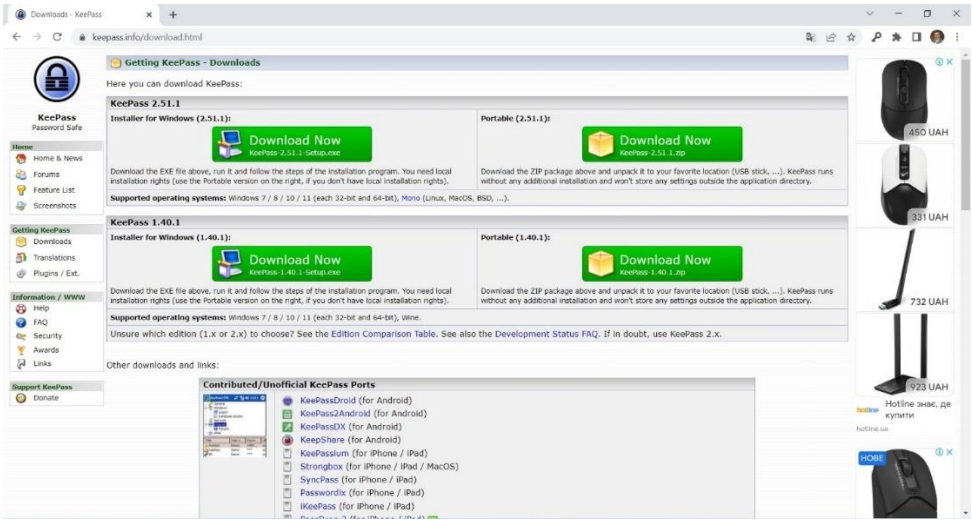


Рисунок 1.9 – Вигляд вікна завантаження інсталяційних пакетів менеджеру паролів Keepass

Рекомендується завантажувати останню версію (на ілюстрації це 2.51.1). Також нижче на сторінці доступний перелік клієнтських програм для різних операційних систем та різних архітектур. Вигляд сторінки завантаження інсталяційних пакетів для різних архітектур і операційних систем представлений на рисунку 1.10.

Також, в боковому меню сторінки можна перейти за посиланням “Translations” та завантажити необхідні мовні пакети для відображення інтерфейсу програми. До завантаження, в тому числі, доступна українська. Для завантаження треба обирати пакет, який відповідає обраній версії. Приклад сторінки обрання локалізації інсталяційного пакету представлений на рисунку 1.11.

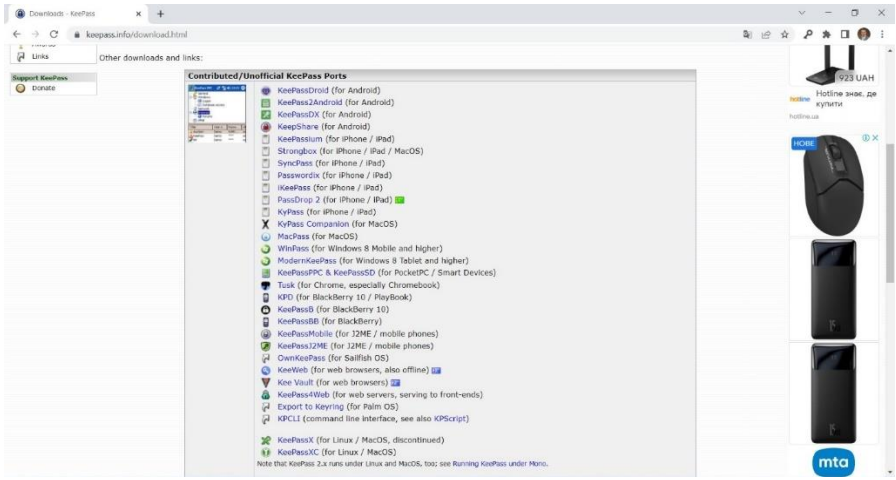


Рисунок 1.10 – Вигляд вікна обрання інсталяційного пакету для різних архітектур і операційних систем

Рисунок 1.11 -Сторінка обрання

Після установки / розпаковки (у випадку застосування portable-версії) і запуску програми, з'являється запит на активацію чи відключення автоматичного пошуку та встановлення оновлень. Вибір можна зробити на власний розсуд, але треба пам'ятати, що оновлення можуть стосуватися безпекових питань, тому якщо автоматичне оновлення виключене, то треба періодично перевіряти наявні оновлення власноруч. Вигляд вікна оновлення версії програмного забезпечення наведено на рисунку 1.12.

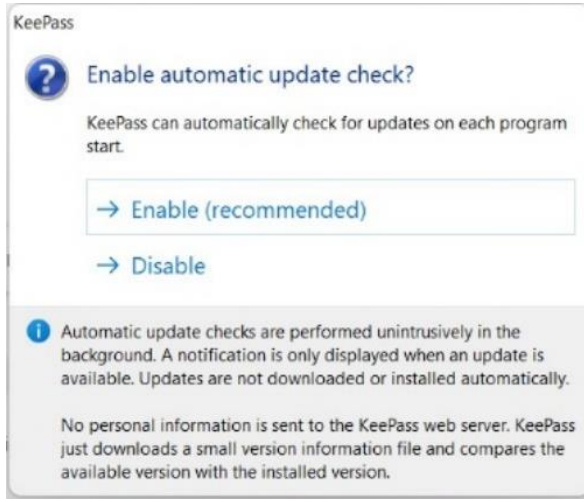


Рисунок 1.12 – Вигляд вікна оновлення версії програмного забезпечення

Якщо мовні пакети не було застосовано, то інтерфейс програми буде виглядати так, як показано нижче на рисунку 1.13.

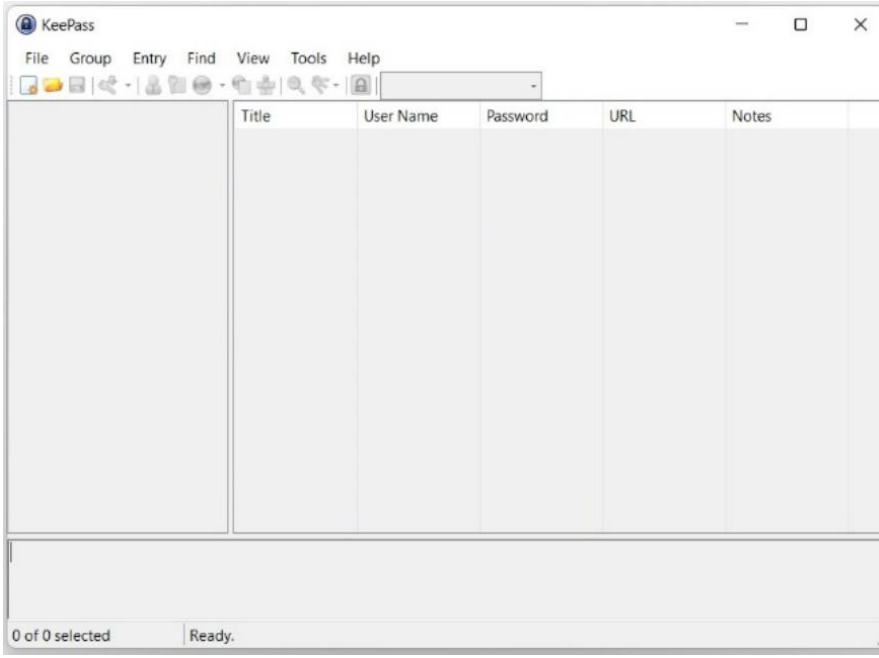


Рисунок 1.13 – Вигляд головного вікна без застосованого мовного пакету

У випадку використання мовних пакетів файл локалізації з завантаженого архіву треба скопіювати у папку “Languages”, яка знаходиться в папці програми.

Для активації мовного пакету треба перейти в меню “View” – “Change language” і у вікні, проілюстрованому нижче на рисунку 1.14, обрати потрібну мову. На рисунку 1.14, як приклад, показана додаткова встановлена мова – українська.

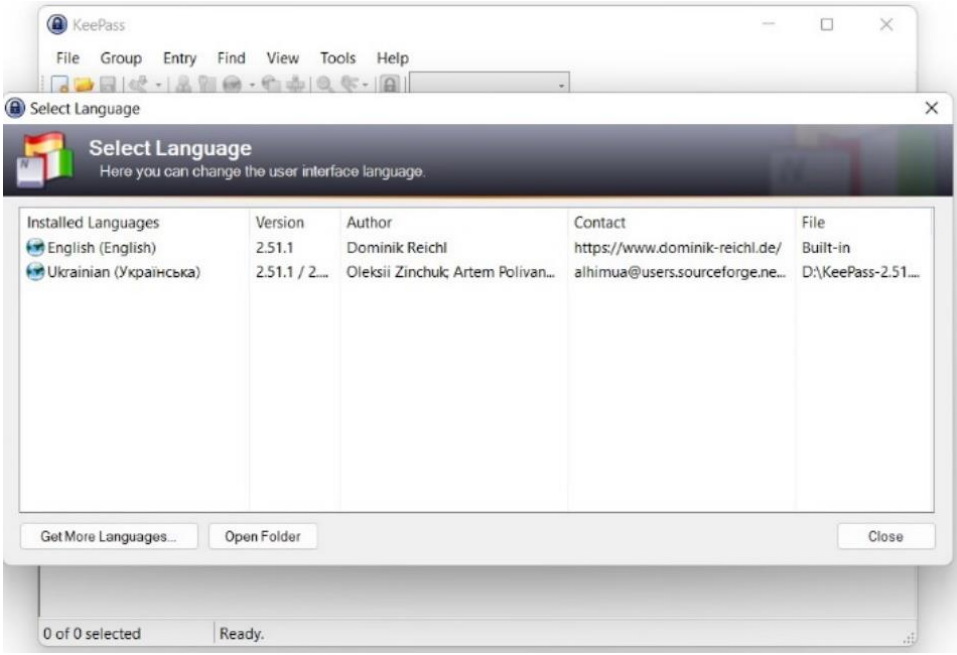


Рисунок 1.14 – Застосування мовного пакету на прикладі української мови

Зміна локалізації програми відбудеться після її перезапуску.

Після активації української локалізації, програма прийме вигляд, показаний на рисунку 1.15.

4. Наступним етапом – потрібно створити базу для зберігання облікових даних. Таких баз може бути довільна кількість або все можна містити в одній базі. Для створення нової бази треба обрати в меню: “ Файл” – “Створити”. Після чого з'являється повідомлення, показане на рисунку 1.16.

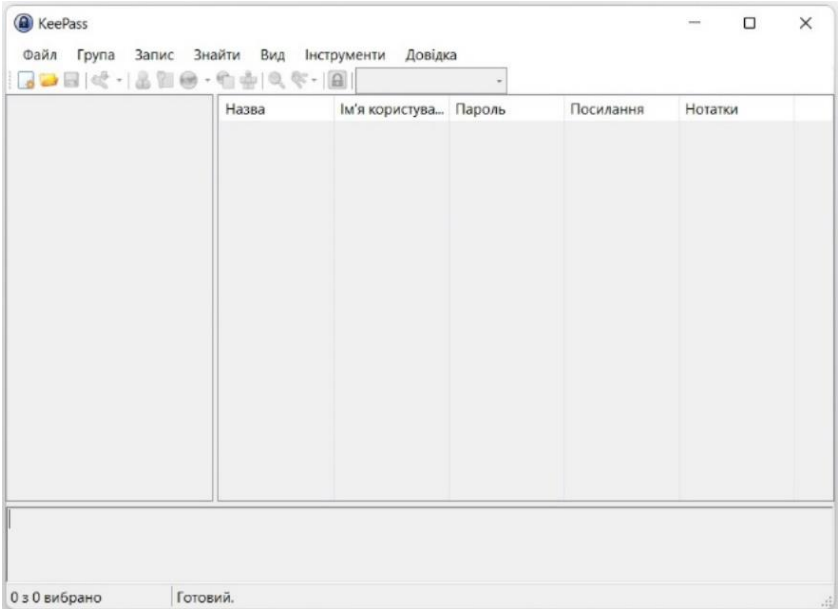


Рисунок 1.15 – Вигляд головного вікна із застосованою українською локалізацією

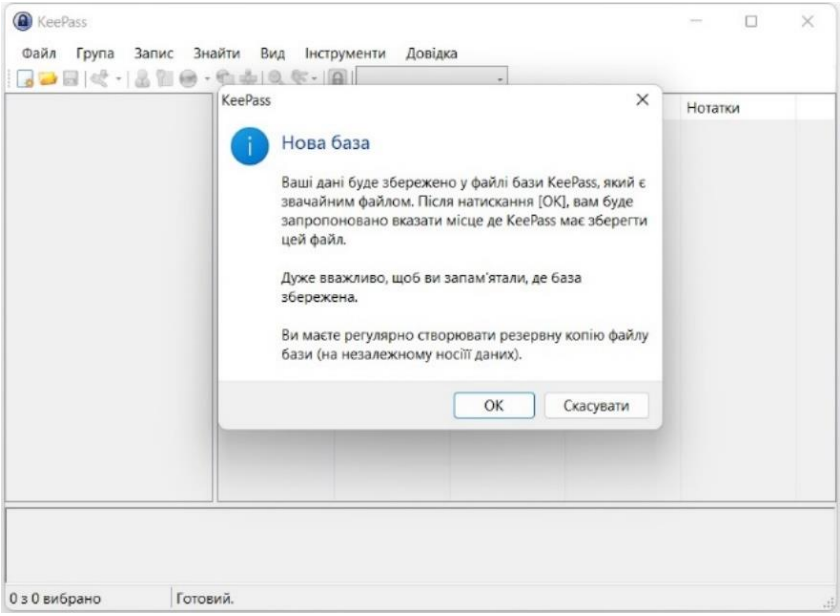


Рисунок 1.16 – Створення нової бази для зберігання облікових даних

Після натискання кнопки “ОК” з’являється діалогове вікно вказання шляху та імені файла бази облікових записів. З метою використання синхронізованого стану бази та використання його на різних пристроях треба вказати шлях зберігання файлу в папці, яка була синхронізована з хмарою Microsoft OneDrive (показано нажче на рисунку 1.17).

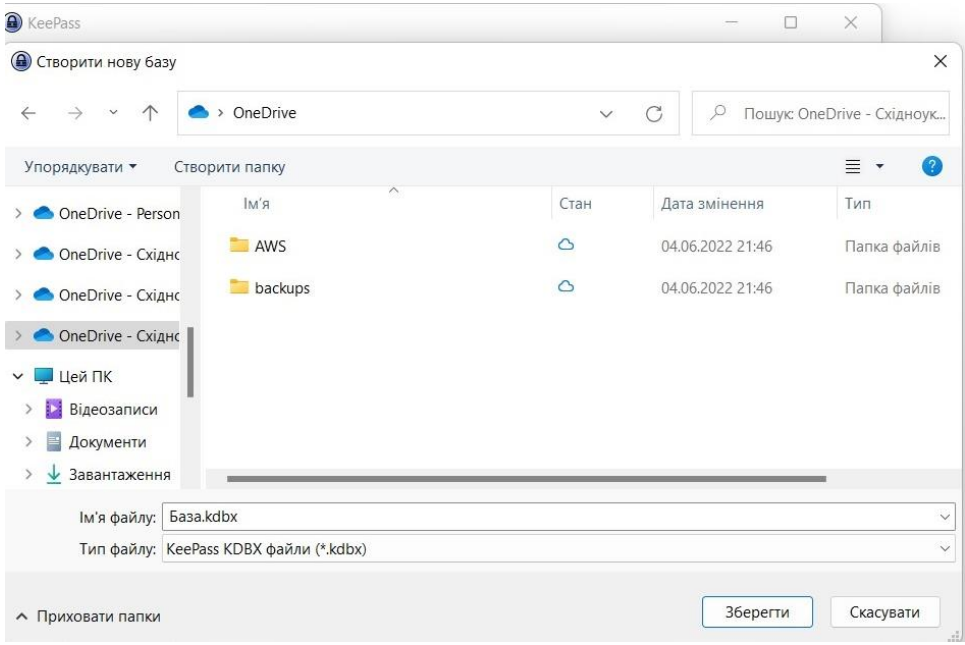
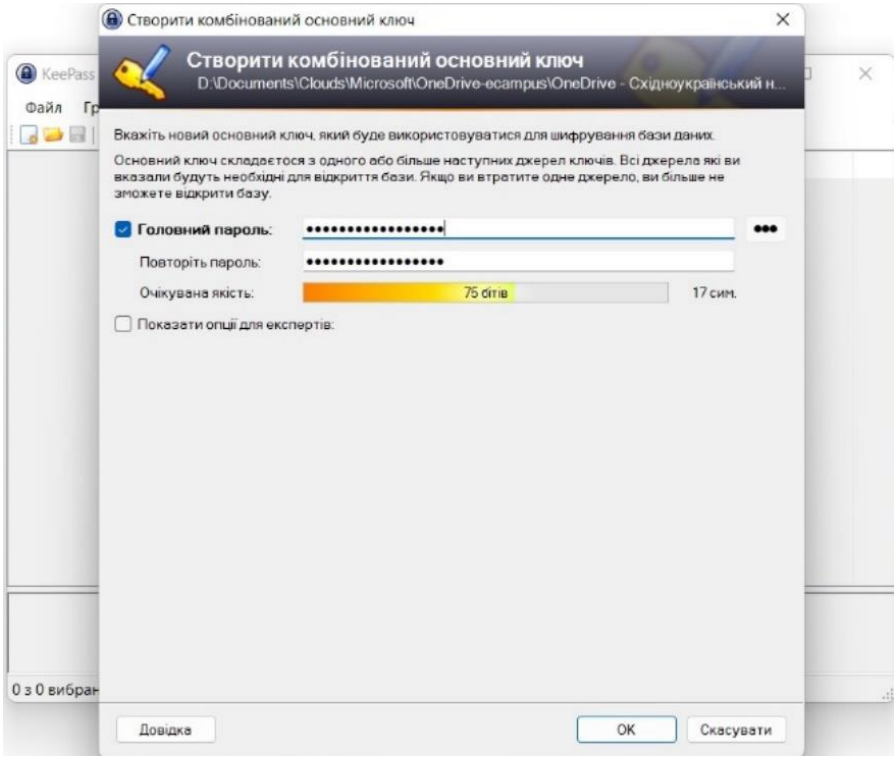


Рисунок 1.17 – Розташування файлу бази облікових даних в синхронізованій теці Microsoft OneDrive для використання на різних пристроях

Наступним етапом буде запит на створення мастер-паролю доступу до бази даних. Фактично, це один пароль, який потрібно буде запам’ятати в процесі використання менеджеру паролів. Відповідно, так як він є ключем до усіх облікових даних, що зберігаються в базі, потрібно забезпечити його нерозголошення. Вікно встановлення мастер-паролю проілюстроване на рисунку 1.18.



Рисбунок 1.18 – Встановлення мастер-паролю для бази обліковиз даних

В процесі введення паролю можна відслідковувати його поточну складність в бітах. Чим вища складність, тим більш високий ступень захисту буде забезпечений.

Надалі, з'являється вікно налаштування створеної бази, поділене на вкладинки. Перша вкладинка дозволяє завдати назву бази, яка буде відображатися в інтерфейсі програми, а також опис бази (за необхідністю). Вигляд цієї вкладенки наведений на рисунку 1.19.

Наступна вкладка дозволяє обрати метод шифрування даних в базі, а також кількість ітерації під час одержання ключа. Слід зазначити, що чим більше ітерацій, тим більш надійніший буде захист бази від можливих брут-форс атак. Однак, збільшення кількості ітерацій також призводить до збільшення часу доступу до бази. Тому визначення цього параметру залежить від співвідношення припустимої затримки на звернення та бажаного ступеню захисту. Визначені параметри можна протестувати і визначити час доступу до бази на поточній конфігурації комп'ютера. Також є опція виставлення значення ітерацій з яким на поточній системі запит буде тривати 1 секунда (вважається середньо-статистичним прийнятним варіантом). Налаштування цих параметрів та результати тесту для 30000000 ітерацій наведені на рисунках 1.20 і 1.21.

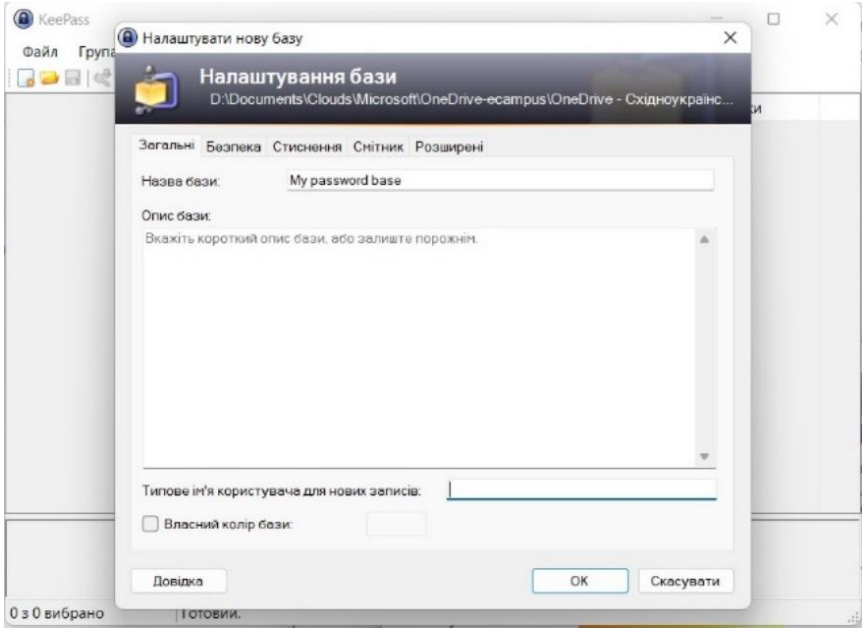


Рисунок 1.19 – Вкладинка загальних налаштувань бази облікових даних

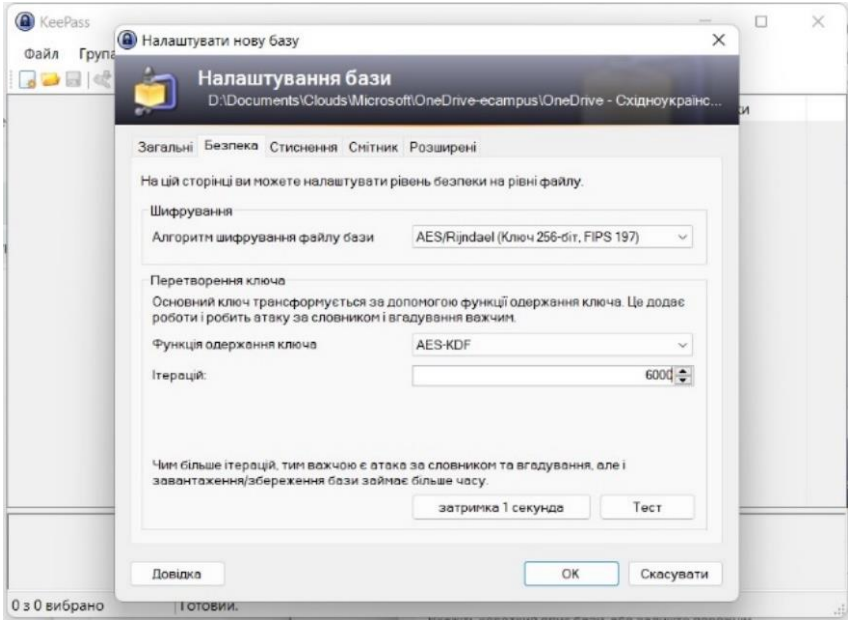


Рисунок 1.20 – Налаштування алгоритму шифрування бази облікових даних

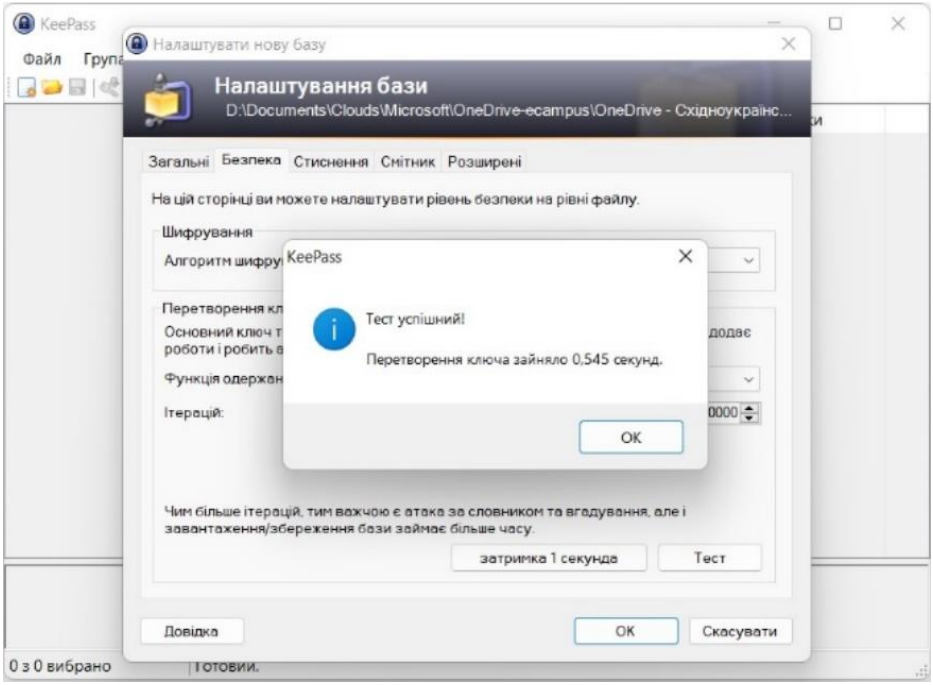


Рисунок 1.21 – Результат перевірки часу виконання ітерацій під час шифрування бази облікових даних

Наступна вкладка дозволяє визначити опцію архівування бази. Слід зазначити, що враховуючи потужність сучасник мікропроцесорів, збереження даних в архівованому стані є бажаним, так як в деяких випажках призводить навіть до збільшення швидкості обробки, так як читання файлу більшого обсягу з зовнішнього накопичувача займає більше часу ніж розпакування даних на потужному сучасному мікропроцесорі. Серед опцій архівування доцільне обрання формату Gzip, так як він є достатньо швидкодіючий. Налаштування варіанту застосування архівування бази облікових даних проілюстроване на рисунку 1.22.

Наступна вкладка дозволяє активувати чи деактивувати смітник в який будуть додаватися видалені записи та групи записів. Вигляд вікна цього налаштування навеадений на рисунку 1.23.

Наступна вкладка розширених налаштувань дозволяє визначити шаблони записів, а також історію записів. Шаблони записів доцільно використовувати, коли велика кількість записів має однакові значення, наприклад, повторюєть логін, або адреса веб ресурсу тощо. Тоді підчас створення нового запису, повторювані дані з шаблону будуть одразу додаватися до відповідних полів. Вигляд налаштувань на цій вкладці проілюстрований на рисунку 1.24

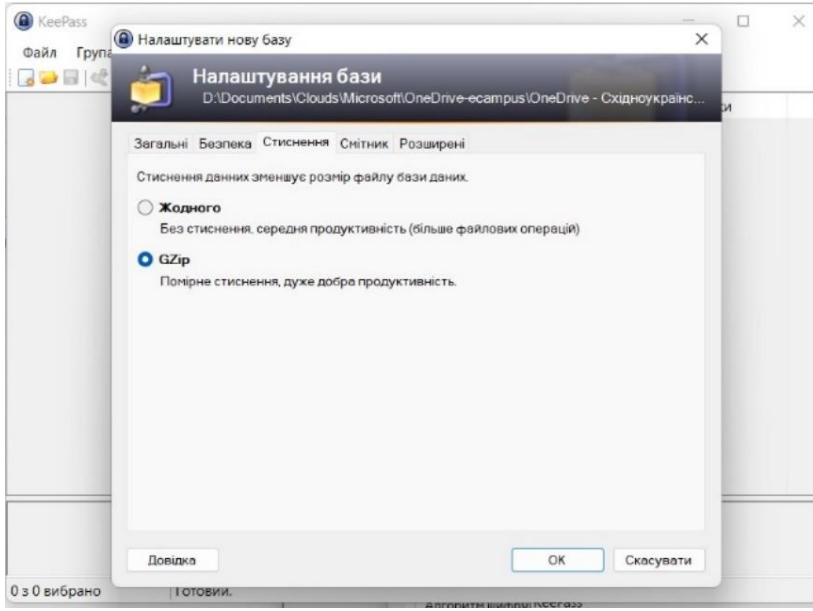


Рисунок 1.22 – Нашалштування застусування архівації бази облікових даних

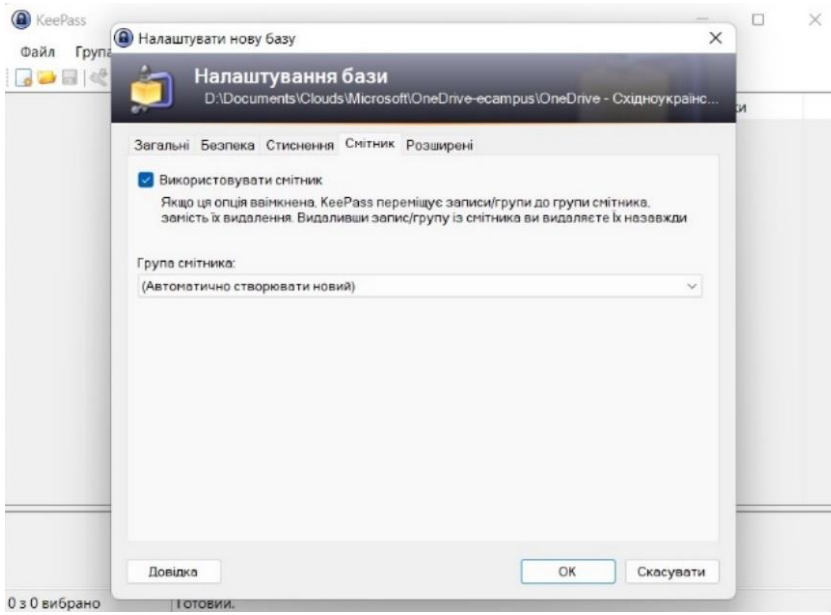


Рисунок 1.23 – Налаштування застосування смітника для видалдених даних з бази

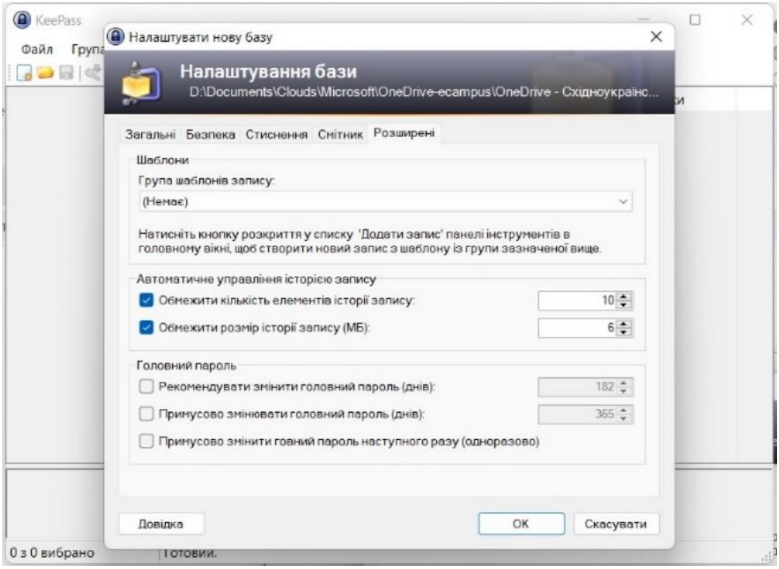


Рисунок 1.24 – Вигляд вкладки розширених налаштувань для бази облікових даних

Останнім етапом створення нової бази є друк пам’ятки, яка містить основні налаштування бази, майстер-пароль. Вигляд цього вікна наведений на рисунку 1.25.

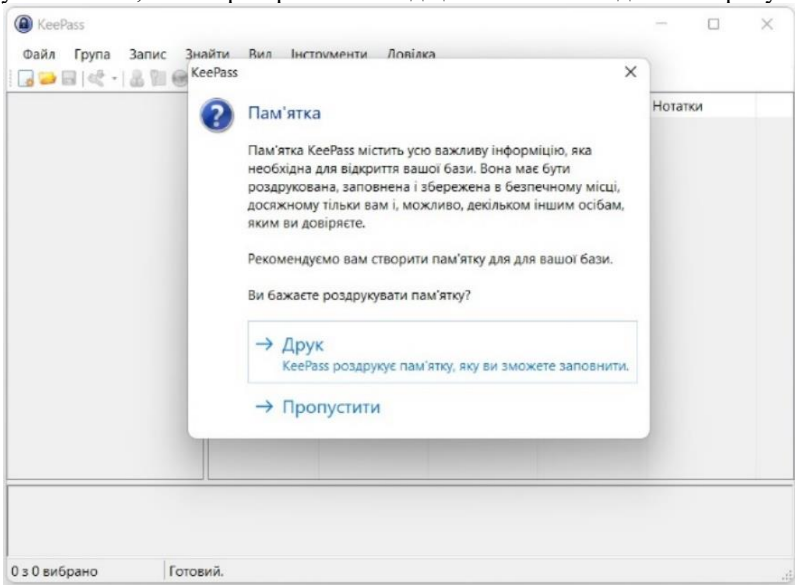


Рисунок 1.25 – Вікно друку основних даних новоутвореної бази обликових даних

Ця пам’ятка потрібна у випадку необхідності відновлення доступу до бази. Звичайно, цю пам’ятку потрібно зберігати в надійному місці, так як інформація з неї дозволяє отримати повний доступ до бази паролів. Ілюстрація зовнішнього вигляду пам’ятки представлена нижче на рисунку 1.26.

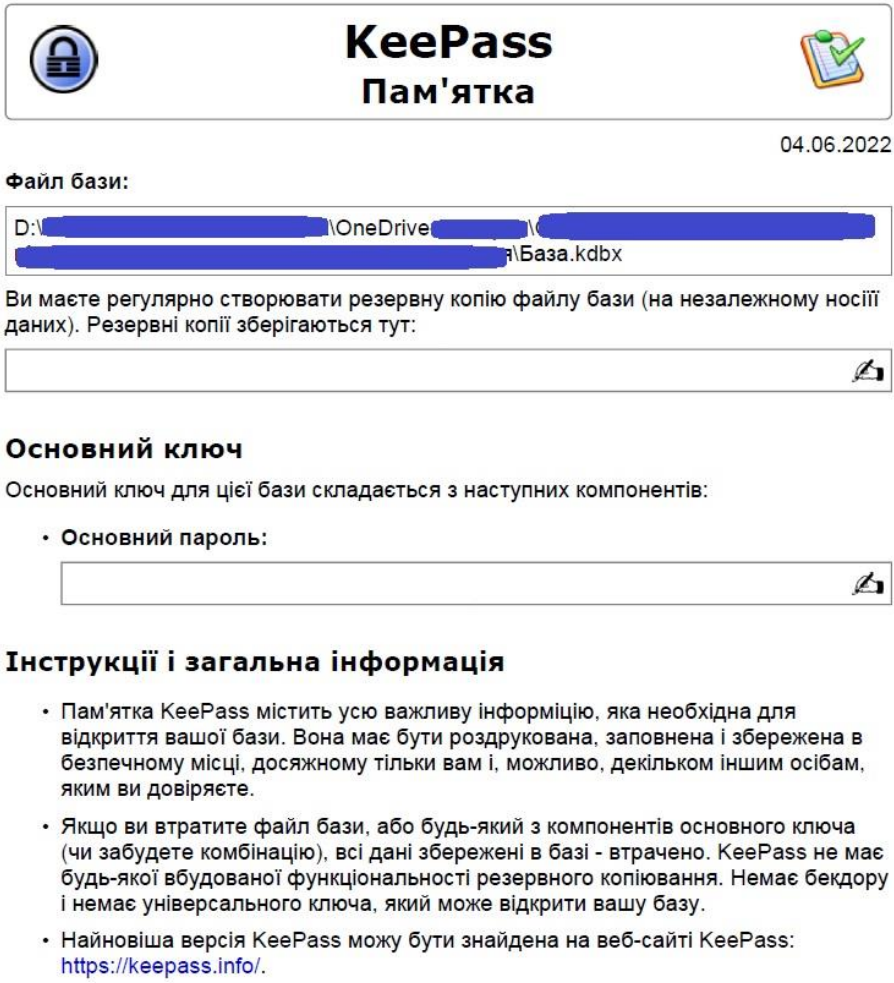


Рисунок 1.26 – Вигляд пам’ятки налаштувань бази облікових даних

5. Після завершення формування бази даних можна переходити до створення записів та редагування груп записів. За замовчанням в базі утворюються групи, які можна редагувати та додавати нові. Для створення запису треба в меню

обрати: “Запис” – “Додати запис”. Після чого, з'являється вікно з вкладками налаштувань, показане нижче на рисунку 1.27.

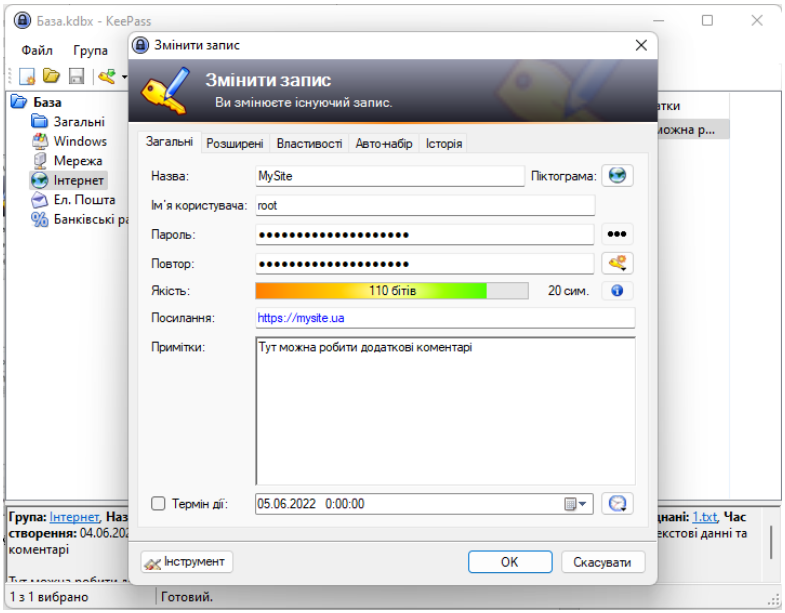


Рисунок 1.27 – Вигляд вікна створення нового запису облікових даних

На вкладці загальних налаштувань додається назва запису, зазначається ім’я користувача (пароль облікового запису), а також пароль. Підчас завдання паролю можна відслідковувати його якість. Також, за бажанням можна додати примітки та визначити термін черезщ який цей пароль повинен бути змінений. Сід зазначити, що система сама може генерувати паролі, які можна потім використовувати під час реєстрації.

На наступній вкладці “Розширені” до запису можна додати додаткові текстові поля, а також будь-які файли. Слід зазначити, що менеджер паролів можна використовувати не тільки для захищеного зберігання облікових даних, а також і будь-яких файлів. При чому їх зберігання буду здійснюватися в зашифрованому вигляді. Зовнішній вигляд вкладки “Розширені” наведений на рисунку 1.28.

Вкладка “Властивості” дозволяє налаштувати колір тексту запису, зазначити мітки чи URL певного синтаксису (обирається з розкриваючого списку). Вигляд цієї вкладки наведений на рисунку 1.29.

Вкладка “Автонабір” дозволяє автоматизувати дії підчас введення облікових даних у відповідних полях, включаючи табуляції для переходу від одного поля введення до іншого. Налаштування цієї вкладки наведені на рисунку 1.30.

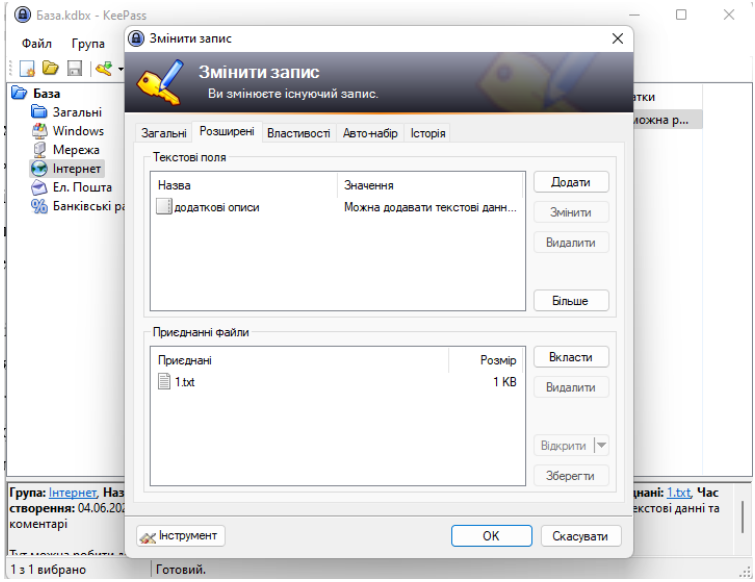


Рисунок 1.28 – Вигляд вкладки ризширених налашщтувань при створенні або редагуванні облікового запису в базі

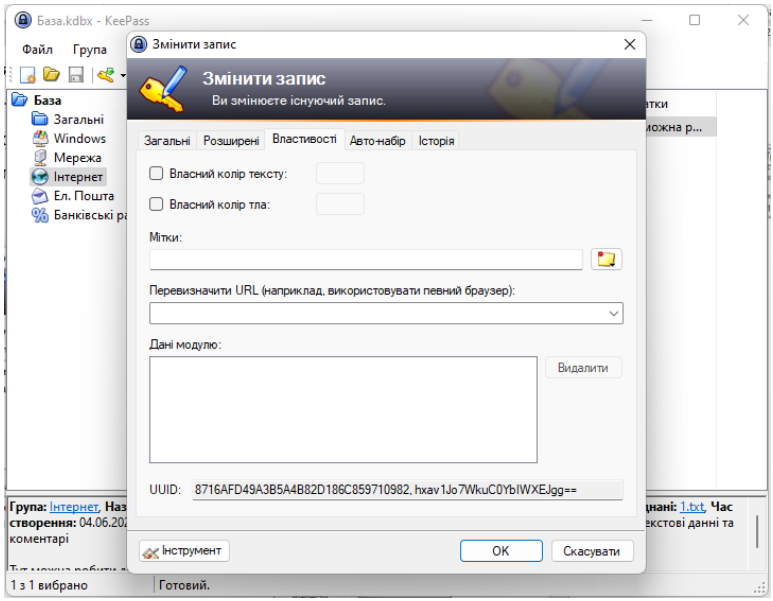


Рисунок 1.29 – Вигляд вкладки налаштування URL для застосування облікового запису

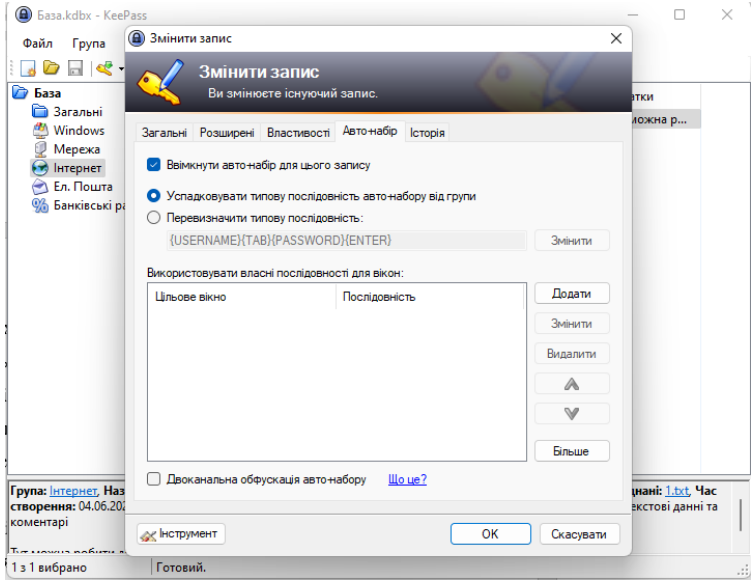


Рисунок 1.30 – Налаштування на вкладці автоматизації дій з обліковими даними

Вкладка “Історія” зберігає історію змін запису, що дозволяє відслідковувати його версії. Її вигляд наведений на рисунку 1.31.

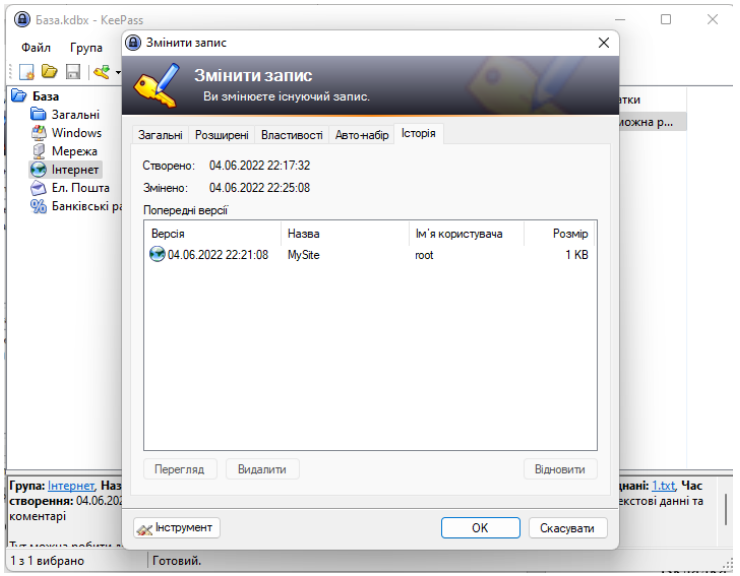


Рисунок 1.31 – Налаштування вкладки історі змін облікового запису

Після внесення усіх опцій запису, він з’являється у списку відповідної групи, як показано на рисунку1.32.

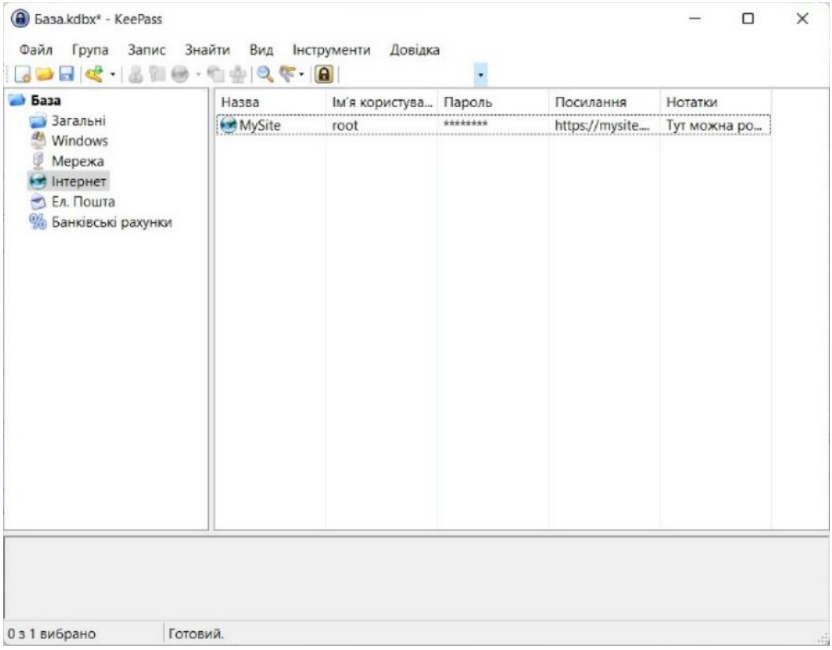


Рисунок 1.32 – Головне вікно програми з доданим облікових записом

6. Для настройки роботи менеджера паролів на інших пристроях. Треба провести налаштування синхронізації локальної папки з хмарним сховищем, згідно пункту 2 цього алгоритму. Після цього, в локальній папці з’явиться синхронізований файл бази даних, створений підчас налаштування на першому комп’ютері. Після цього, треба встановити (або розпакувати) програму менеджеру паролів, за необхідності провести налаштування локалізації, згідно пункту 3 цього алгоритму. Надалі, базу даних вже створювати не треба, а залишається тільки підключити існуючу з синхронізованої папки. Це робиться через пункт меню “Файл” - ”Відкрити” – ”Відкрити файл …”. Окрім цього, також існує варіант розміщення бази не на хмарі, а на FTP сервері, але такий варіант не підходить широкій аудиторії користувачів, у яких відсутні у вільному доступі власні сервери з FTP доступом для читання і запису.

4. Додаткові завдання

1) Проведіть аналіз часової складності алгоритмів шифрування проводячи їх тестування при однакових значеннях ітерацій.

2) Проведіть налаштування програмного забезпечення менеджеру паролів на пристрої з іншою операційною системою, наприклад на Android-смартфоні.

3) Встановіть інший варіант менеджеру паролів – KeepassXC (https://keepassxc.org/download/) та зробіть їх порівняльний аналіз.

ПРАКТИЧНЕ ЗАВДАННЯ 2.
КЕЙЛОГЕРИ

1. Короткі відомості

Кейлогери створені для реєстрації натискань клавіш - створення записів про все, що набирається на клавіатурі комп'ютера або мобільного телефону. Вони використовуються для прихованого спостереження за комп'ютерною активністю, доки людина використовуєте свої пристрої у звичайному режимі. Кейлогери використовуються у законних цілях, таких як зворотний зв'язок для розробки програмного забезпечення, але злочинці можуть використовувати їх не за призначенням для крадіжки даних.

Реєстрація натискань клавіш — це відстеження та запис кожного натискання клавіші, зробленого на комп’ютері, часто без дозволу чи відома користувача. «Натискання клавіші» — це будь-яка взаємодія, яку здійснює людина за допомогою кнопки на клавіатурі. Кожне натискання клавіші передає сигнал, який повідомляє комп’ютерним програмам, що ви хочете, щоб вони робили. Такі команди можуть включати:

- довжину натискання клавіші;
- час натискання клавіші;
- швидкість натискання клавіші;
- назву використовуваного ключа.

Під час реєстрації вся ця інформація схожа на прослуховування приватної розмови. Ви вважаєте, що лише «розмовляєте» зі своїм пристроєм, але інша людина слухала і записувала все, що ви сказали. Оскільки наше життя стає все більш цифровим, ми ділимося великою кількістю дуже конфіденційної інформації на наших пристроях.

Поведінку користувачів і особисті дані можна легко зібрати з зареєстрованих натискань клавіш. Все, від доступу до онлайн-банкінгу до номерів соціального страхування, вводиться в комп’ютери. Соціальні мережі, електронна пошта, відвідані веб-сайти і навіть надіслані текстові повідомлення можуть бути дуже показовими.

Інструменти кейлогера можуть бути апаратними або програмними, призначеними для автоматизації процесу реєстрації натискань клавіш. Ці інструменти записують дані, надіслані кожним натисканням клавіші, у текстовий файл, щоб отримати пізніше. Деякі інструменти можуть записувати все в буфер обміну, дзвінки, дані GPS і навіть відео з мікрофона або камери.

Кейлогери — це інструмент спостереження, який законно використовується для особистого або професійного моніторингу IT. Деякі з цих видів використання входять в етично сумнівну сіру зону. Однак інші види використання кейлогерів є явно злочинними.

Незалежно від використання, кейлогери часто використовуються без повної згоди користувача, а також можуть використовуються з припущенням, що користувачі повинні вести себе як зазвичай.

На сьогодні поширені дві форми кейлогерів: програмні та апаратні.

Програмні кейлогери – це комп'ютерні програми, які встановлюються на жорсткий диск пристрою. Поширені типи програмного забезпечення кейлогерів можуть включати:

- *Кейлогери на основі API*. Такі кейлогери безпосередньо підслуховують сигнали, що надсилаються від кожного натискання клавіші до програми, у яку вводиться текст. Інтерфейси прикладного програмування (API) дозволяють розробникам програмного забезпечення та виробникам апаратного забезпечення говорити однією «мовою» та інтегруватися один з одним. Кейлогери API тихо перехоплюють API клавіатури, реєструючи кожне натискання клавіші в системному файлі.
- *Кейлогери на основі «захоплення форм»* підслуховують весь текст, введений у форми веб-сайту, коли ви надсилаєте його на сервер. Дані записуються локально, перш ніж передаватися в режимі онлайн на веб-сервер.

- *Кейлогери на основі ядра* проникають в ядро системи для отримання дозволів на рівні адміністратора. Ці реєстратори можуть обійти й отримати необмежений доступ до всього, що введено у системі.

Апаратні кейлогери – це фізичні компоненти, вбудовані або підключені до вашого пристрою (наприклад, рисунок 2.1). Деякі апаратні методи можуть відстежувати натискання клавіш навіть без підключення до пристрою.

Рисунок 2.1 – Приклад апаратного кейлогеру

До найбільш поширених апаратних кейлогерів відносять:

- *Апаратні кейлогери клавіатури*, які можна розташувати поруч із з'єднувальним кабелем клавіатури або вбудувати в саму клавіатуру. Це найбільш пряма форма перехоплення ваших сигналів друку.

- *Кейлогери прихованої камери*. Такі кейлогери можна розміщувати в громадських місцях, наприклад бібліотеках, для візуального відстеження натискань клавіш.
- *Кейлогери, завантажені на USB-диск*. Вони можуть бути фізичним троянським конем, який доставляє шкідливе програмне забезпечення для реєстрації натискань клавіш після підключення до пристрою.

2. Використання кейлогерів

У тій чи іншій формі кейлогери використовувалися протягом десятиліть, починаючи з прихованих операцій КДБ у 1970-х роках. Сьогодні кейлогери є шостою за поширеністю формою корпоративного шкідливого програмного забезпечення. Проте варто зазначити, що крім несанкціонованого використання, кейлогери також можуть використовуватися в санкціонованих умовах.

Санкціоноване використання кейлогерів. При законному або санкціонованому використанні кейлогера від особи або організації вимагається:

- Не використовувати дані для злочинних дій.
- Бути власником продукту, виробником або законним опікуном дитини, яка володіє продуктом.
- Використовувати кейлогер відповідно до чинних законів свого місця розташування.

Нижче наведено кілька поширених законних застосувань кейлогерів:

- Усунення неполадок IT — для збору інформації про проблеми користувачів і їх точного вирішення.
- Розробка комп'ютерного продукту — для збору відгуків користувачів і покращення продуктів.
- Моніторинг бізнес-серверів — для спостереження за несанкціонованою діяльністю користувачів на веб-серверах.
- Спостереження співробітників — для цілодобового нагляду за безпечним використанням майна компанії.

Крім того, користувачі кейлоггера може відстежувати комп'ютерні продукти, якими вони володіють або виготовляють. Вони навіть можуть легально контролювати пристрої своїх дітей. Але вони не можуть стежити за пристроями за межами їхньої власності.

Без згоди людини та організації можуть використовувати кейлогери для:

- Батьківського нагляду за дітьми — щоб захистити дитину в онлайн-діяльності та в соціальних мережах.
- Відстеження подружжя — для збору активності на пристрої, яким володіє користувач, для підтвердження зради.
- Моніторингу продуктивності співробітників — щоб стежити за використанням часу компанії.

Несанкціоноване використання кейлогерів. Незаконне використання кейлогера повністю ігнорує згоду, закони та право власності на продукт на користь

негідного використання. Експерти з кібербезпеки зазвичай посилаються на цей варіант використання, коли обговорюють кейлогери.

При використанні в злочинних цілях кейлогери служать шкідливим шпигунським програмним забезпеченням, призначеним для захоплення конфіденційної інформації. Вони записують такі дані, як паролі або фінансову інформацію, яка потім надсилається третій стороні для злочинної експлуатації.

Загрози кейлогерів можуть випливати з багатьох проблем, пов'язаних зі збором конфіденційних даних.

Якщо ви не знаєте, що все, що ви вводите на клавіатурі комп'ютера, записується, ви можете ненавмисно розкрити свої паролі; номери кредитних карток; номери фінансових рахунків тощо.

Така конфіденційна інформація дуже цінна для третіх сторін, включаючи рекламодавців і злочинців. Після збору та збереження ці дані стають легкою мішенню для крадіжки.

3. Приклади санкціонованих кейлогерів

Колись кейлогери були апаратними засобами, які були розроблені для запису натискань клавіш у певній системі. Згодом програмні рішення стали більш популярними, ніж апаратні аналоги, завдяки їх легшій реалізації та більшій доступності. Сучасні так звані програми кейлогерів здатні набагато більше, ніж записувати натискання клавіш.

Kidlogger. KidLogger (рисунок 2.2) пропонує безкоштовну версію, «Базовий обліковий запис» і два інших плани на основі підписки: «Стандартний» і «Професійний». Безкоштовна програма записує натискання клавіш, робить знімки екрана через задані проміжки часу та реєструє використання програм, щоб можна було дізнатися, що було набрано на комп'ютері та що було видно на екрані, а також якими програмами користувалася людина.

Як і більшість інших безкоштовних програм для кейлоггерів, KidLogger пропонує звіти у вигляді файлів HTML. Він також може створювати журнали у форматах CSV та JSON. Однак особливість цього безкоштовного кейлоггера полягає в тому, що він дозволяє переглядати звіти через його веб-портал, який можна налаштувати за допомогою своєї електронної адреси. KidLogger завантажує журнали на 9 МБ дискового простору, яке було виділено на своїх серверах, і зберігає дані протягом 9 днів.

Best Free Keylogger. Best Free Keylogger (рисунок 2.3) здатний записувати натискання клавіш, буфер обміну, знімки екрана, дії в Інтернеті та програми; це також може бути програмне забезпечення батьківського контролю. Він може фільтрувати веб-вміст на основі його текстового вмісту або категорії, якщо він потрапляє до невідповідної категорії, як-от порнографія, наркотики, азартні ігри тощо. Крім того, він здатний встановлювати обмеження на програми, і дозволяє надавати доступ до Інтернету лише протягом певного періоду часу. Best Free Keylogger можна використовувати як у домашніх умовах, так і на робочих місцях.

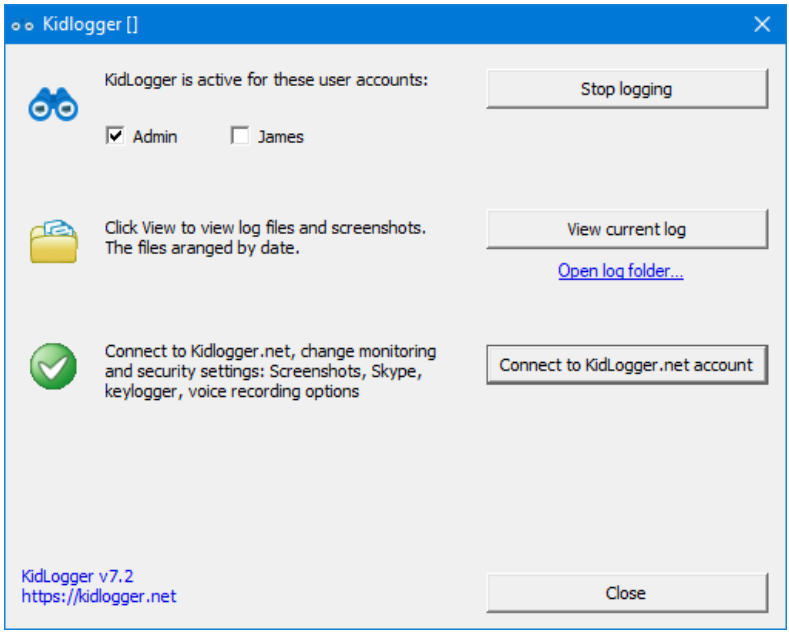


Рисунок 2.2 – Вигляд санкціонованого кейлогера Kidlogger

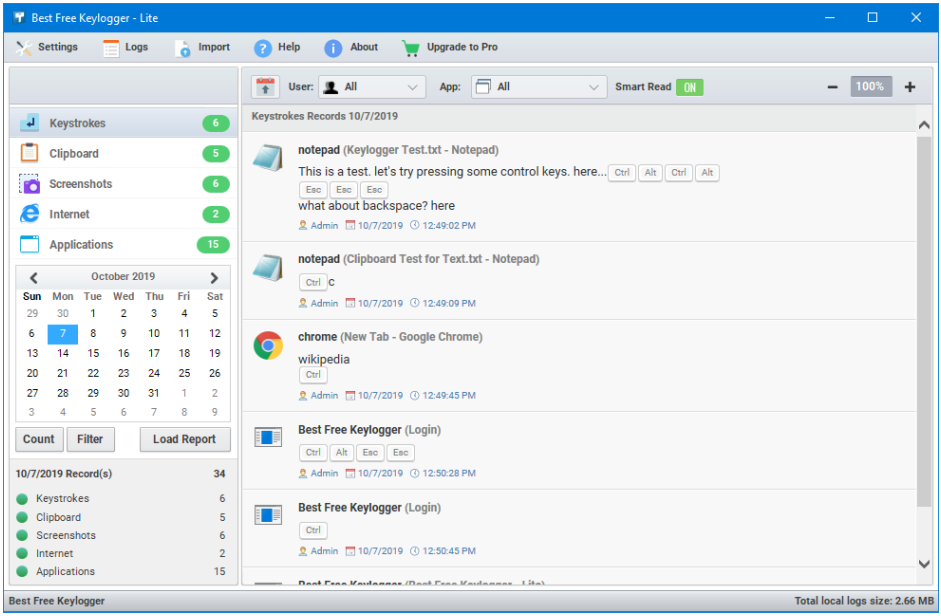


Рисунок 2.3 – Зовнішній вигляд кейлогеру Best Free Keylogger

Інтерфейс Best Free Keylogger інтуїтивно зрозумілий і зручний для користувача з багатьма корисними налаштуваннями. Наприклад, під час перегляду записів про натискання клавіш є опція «Smart Read», яка дозволяє інтелектуально відфільтрувати такі натискання клавіш, як Backspace, Enter тощо. На додаток до Smart Read, можна фільтрувати записи за датою, користувачем, програмою, текстом тощо, або сортувати журнали за датою в порядку зростання або спадання. Ці прості, але потужні інструменти, а також те, як записи представлені в засобі перегляду звітів у відповідних кольорах і піктограмах, полегшують читання та розуміння, ніж перегляди таблиць, які можна побачити в більшості інших безкоштовних програм клавіатури.

Даний кейлогер є одним з найкращих безкоштовних кейлогерів з його потужними функціями за простим і привабливим інтерфейсом є популярним вибором серед батьків, а також системних адміністраторів, які віддають перевагу додаткам, які прості у використанні.

Windows Keylogger. Windows Keylogger, як випливає з назви, призначений для комп'ютерів під керуванням ОС Windows. Існує безкоштовна версія, а також платна версія цього програмного забезпечення кейлогера. Windows Keylogger (рисунок 2.4) записує натискання клавіш, буфер обміну, роботу в Інтернеті та використання програм, за винятком знімків екрана, які доступні лише в платній версії.

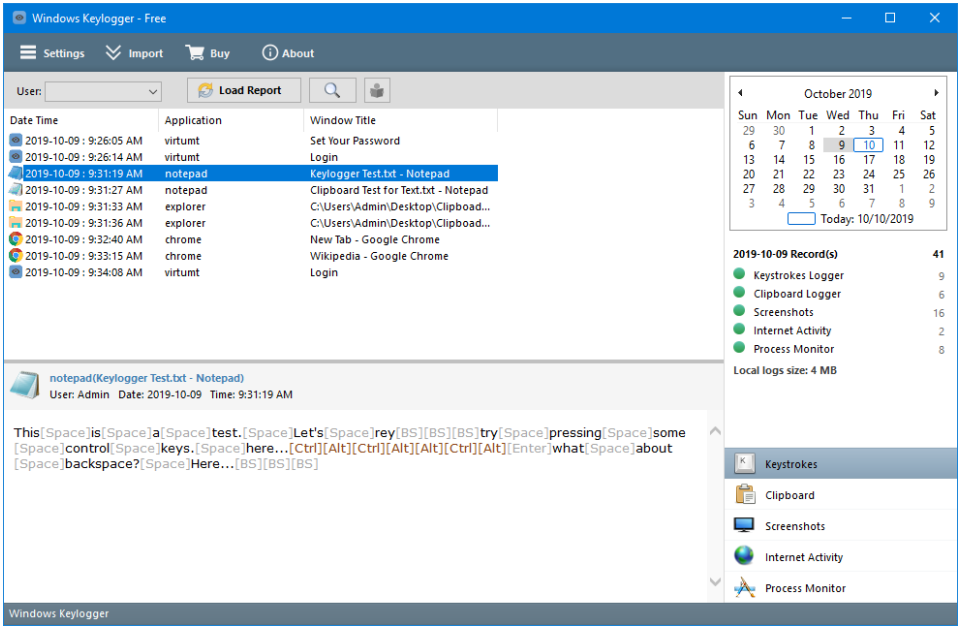


Рисунок 2.4 – Зовнішній вигляд програмного забезпечення Windows Keylogger

Цей безкоштовний кейлогер пропонує вам бічні панелі праворуч, що показує календар і кількість записів, доступних для кожної дати. Це та додавання відповідного значка програми перед кожним записом полегшують користувачам розуміння звітів у засобі перегляду звітів. Доставка звітів доступна лише в платній версії Windows Keylogger.

Refog Personal Monitor — ще одне програмне забезпечення для кейлогерів (рисунок 2.5). Він здатний записувати натискання клавіш, знімки екрана, інтернет-активність, використання додатків і може відстежувати файли.

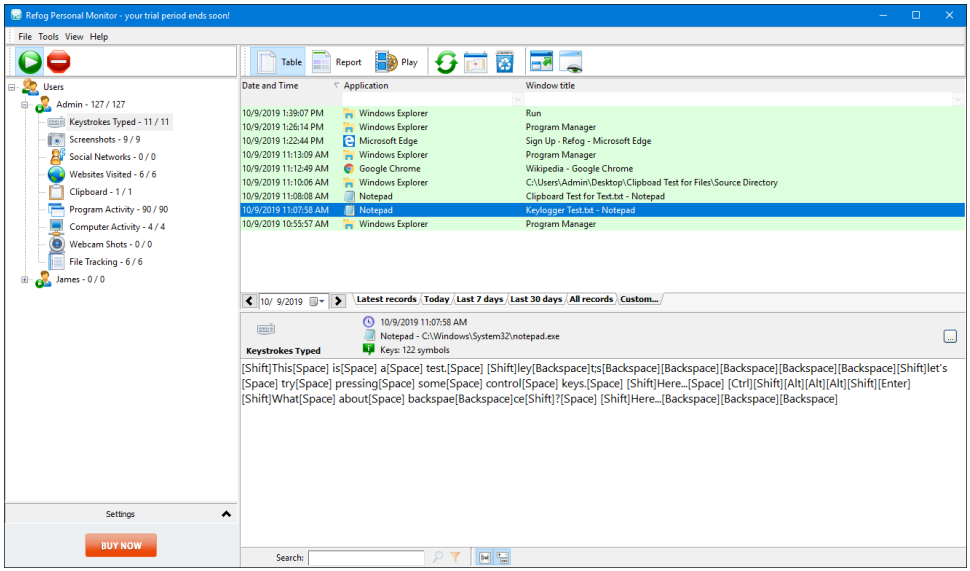


Рисунок 2.5 – Зовнішній вигляд програмного забезпечення Refog Personal Monitor

У порівнянні з більшістю інших безкоштовних програм для кейлогерів, Refog Personal Monitor має дещо привабливіший інтерфейс користувача, проте він не може обмежувати будь-яку діяльність в Інтернеті чи комп'ютері, як деякі з його конкурентів.

Spyrix Free Keylogger. Spyrix Free Keylogger — це безкоштовна версія більш складного кейлогера, точніше, платного програмного забезпечення для моніторингу, Spyrix Personal Monitor. Він має можливість записувати натискання клавіш, знімки екрана та використання програми (рисунок 2.6). Деякі загальні функції, доступні в іншому безкоштовному програмному забезпеченні кейлогерів, як-от можливість запису буфера обміну та моніторингу активності в Інтернеті, обмежені платною версією програмного забезпечення.

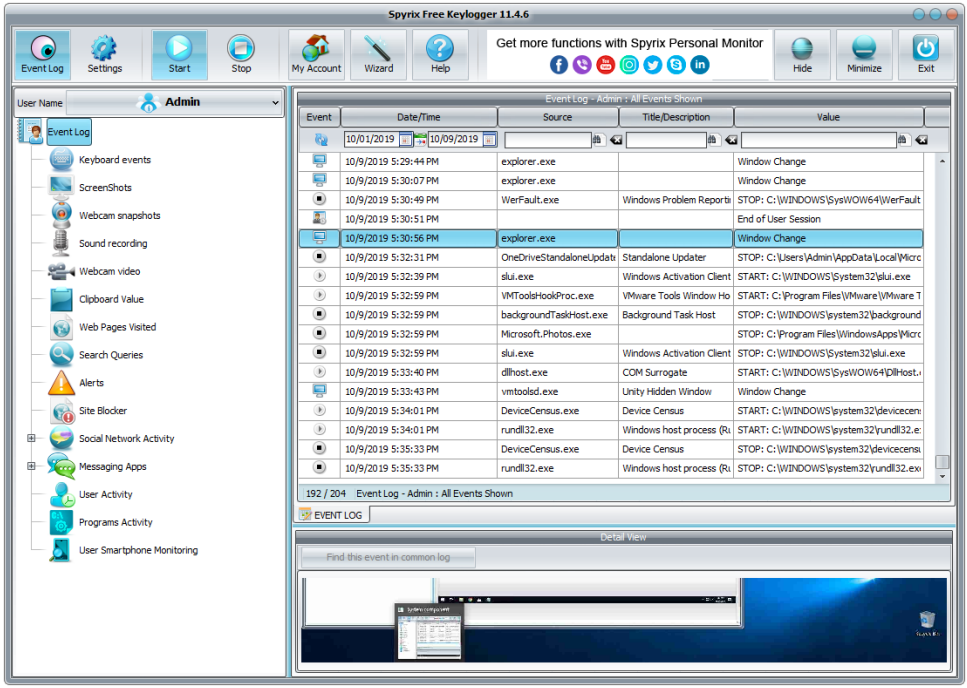


Рисунок 2.6 – Зовнішній вигляд програмного забезпечення Spyrix Free Keylogger

Доставка звітів, яка дозволяє програмному забезпеченню доставляти вам записані журнали за допомогою такого засобу, як електронна пошта або FTP, доступний лише у версії Pro. Однак одна головна функція, завдяки якій Spyrix Free Keylogger випереджає інші програми в цьому списку найкращого безкоштовного програмного забезпечення для кейлоггерів, — це опція Live View. Це дозволяє бачити, що відбувається на цільовому комп'ютері через онлайн-панель у обліковому записі Spyrix.

4. Практичний кейс

До вирішення надається наступна задача. Організувати роботу комп'ютера з використанням кейлогера.

Умови вирішення наступні.

1) необхідно налаштувати відслідковування локальних додатків;
2) ввести обмеження за користувачем чи додатком;
3) налаштувати веб-фільтр;
4) заблокувати додатки, які непотрібні користувачу комп'ютера під час виконання роботи.

Алгоритм вирішення задачі.

В якості однієї з наявних альтернатив застосуємо програмне забезпечення Iwantsoft Free Keylogger. Даний кейлогер дозволить відслідковувати роботу співробітників, а також блокувати інтернет та додатки за необхідності. Це рішення є безкоштовним.

1. Перед початком завантаження та встановлення кейлогера рекомендується вимкнути антивірус та додати у виключення папку, в яку кейлогер буде завантажено.
2. Завантажуємо кейлогер за посиланням: https://www.iwantsoft.com/download/.
3. Запускаємо кейлогер після встановлення. Програма буде просити встановити пароль для користування програмою, як цн показано нижче на рисунку 2.7.

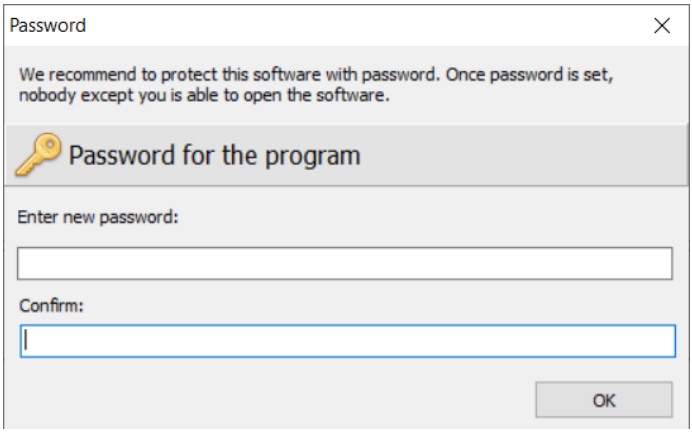


Рисунок 2.7 – Вікно запиту встановлення паролю користувача кейлогера

4. Налаштовуємо мову інтерфейсу кейлогера. Для цього заходимо в Tools / Language і обираємо одну з запропонованих мов. Обрання мови інтерфейсу проілюстровано на рисунку 2.8.
5. З лівої сторони інтерфейсу можна побачити журнал (Log), який буде зберігати інформацію про додатки, натискання клавіш, буфер обміну, веб-перегляд, месенджери, соціальні мережі, USB – пристрої, друк документів, вивантажені файли, файлові операції, знімки екранів, пристрої перехоплення. Крім того можна побачити різні повідомлення та аналітику.
6. Для налаштування виключаючих правил необхідно зайти в налаштування, як то показано на рисунку 2.9.

Для того, щоб визначити які функції необхідно задати кейлогеру, необхідно поставити відмітки перед кожною дією. Також можна налаштувати для якого користувача є необхідність використання кейлогера. Для цього необхідно перейти на вкладку Users, як то показано на рисунку 2.10

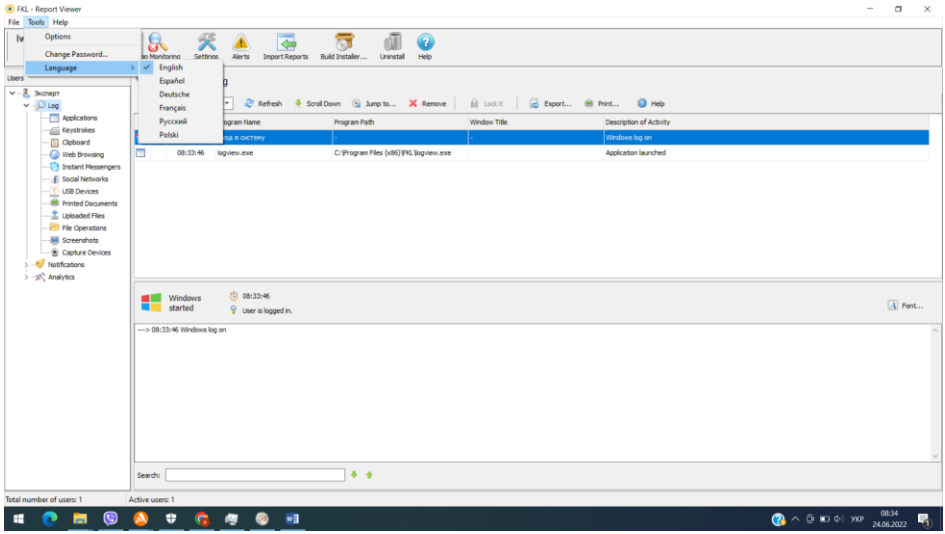


Рисунок 2.8 – Вибір мови відображення інтерфейсу кейлогера

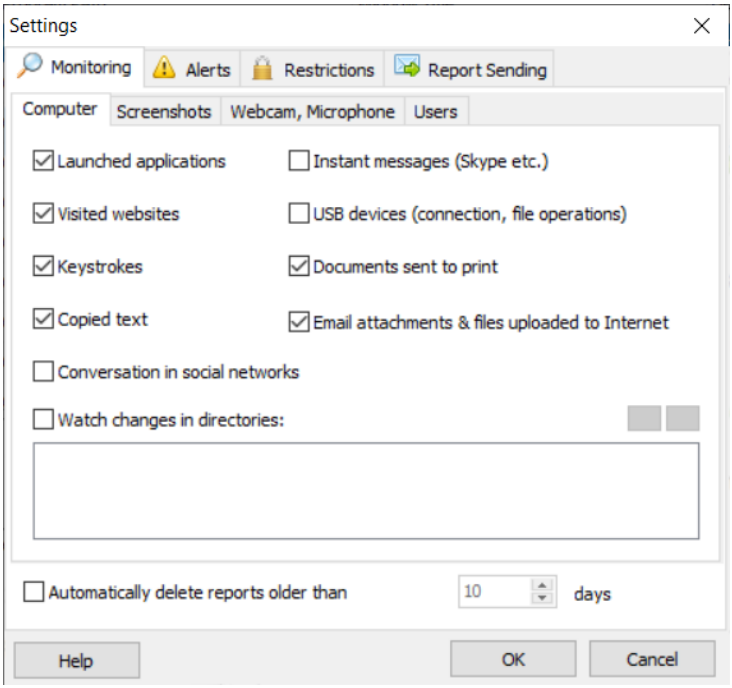


Рисунок 2.9 – Вигляд вікна налаштувань програми кейлогера

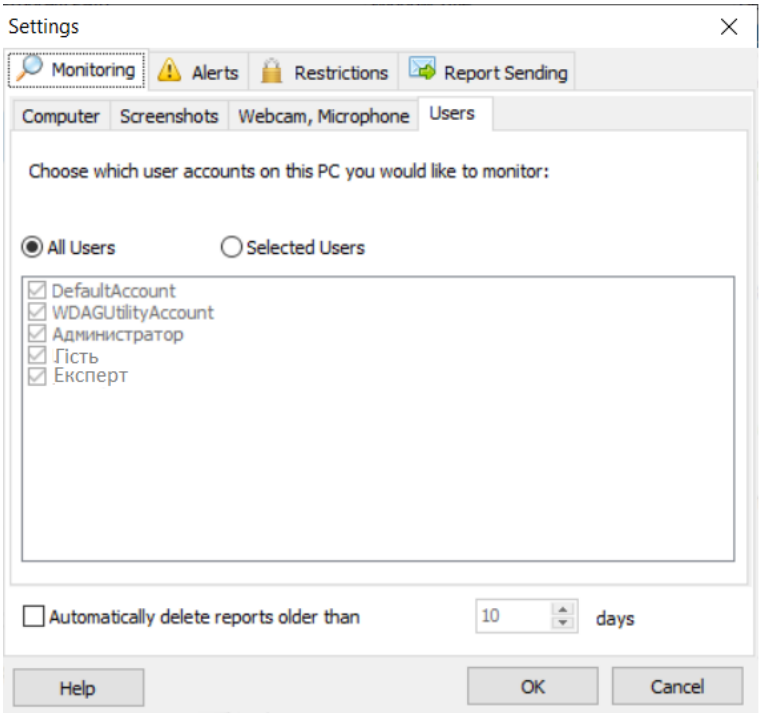


Рисунок 2.10 – Вкладка налаштувань призначення для користувачів

7. Для запобіганню витоку інформації стосовно паролей або будь-якого іншого тексту можна налаштувати отримання попереджень при появі в тексті або повідомлень користувача якогось тексту. Для цього в налаштуваннях заходимо в меню Alerts і прописуємо ключову фразу, на яку необхідно реагувати (рисунок 2.11).

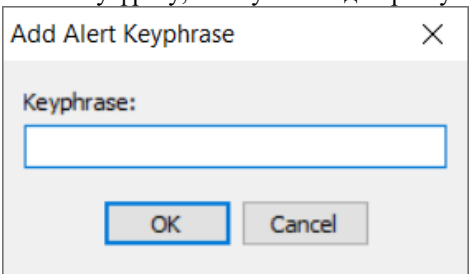


Рисунок 2.11 – Завдання ключової фрази

8. При налаштуванні обмежень на використання необхідно розуміти, що можна додатково налаштувати обмеження на використання як додатків, так і веб-сайтів. Але при блокуванні веб-сайтів треба розуміти чи не буде необхідності

заходити на якусь визначену сторінку веб-сайту, адже даний кейлогер блокує безпосередньо сайт, а не визначені сторінки сайтів.

9. При блокуванні додатків у налаштування програми заходимо до Restrictions / Lock Applications. Далі, використовуючи знак «+» біля фрази «Block access to the following applications» прописуємо додатки, які необхідно буде заблокувати. Крім того, можна обрати час коли дані додатки заблоковані не будуть (рисунок 2.12 – представлене включення блокування для прикладної програми блокноту).

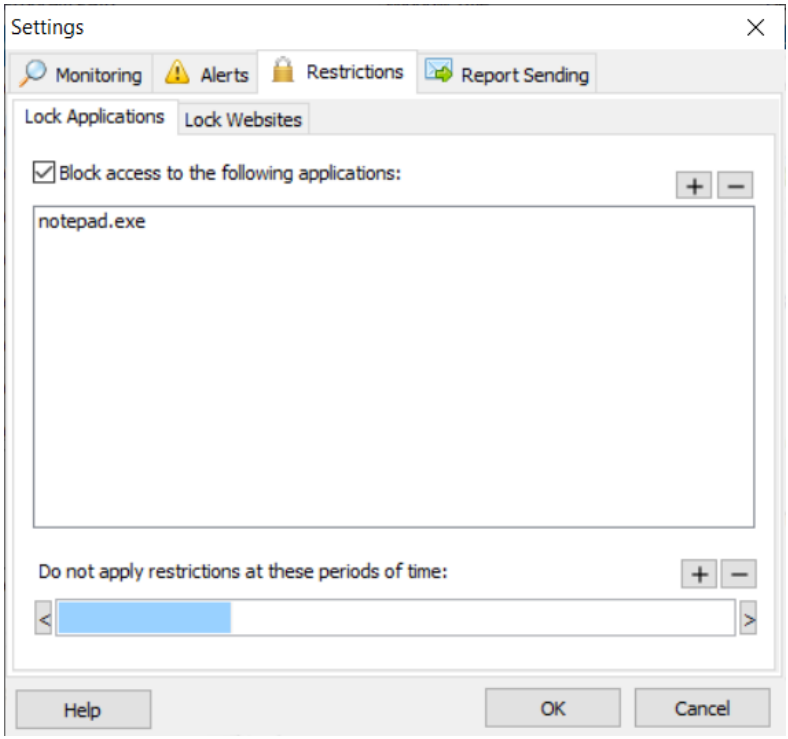


Рисунок 2.12 – Налаштування блокування прикладних програм (на прикладі блокнота)

10. Використовуючи інформацію, описану в п. 9, можна таким самим чином заблокувати різного роду веб-сайти. Приклад такого налаштування для сайту YouTube наведено на рисунку 2.13.

11. Після внесення інформації про блокування додатків та веб-сайтів, вони не будуть відкриватися на пристрої і в меню Blocking можна буде ознайомитися з інформацією коли саме користувач намагався їх відкрити. Приклад виведення реєстру блокування наведений на рисунку 2.14.

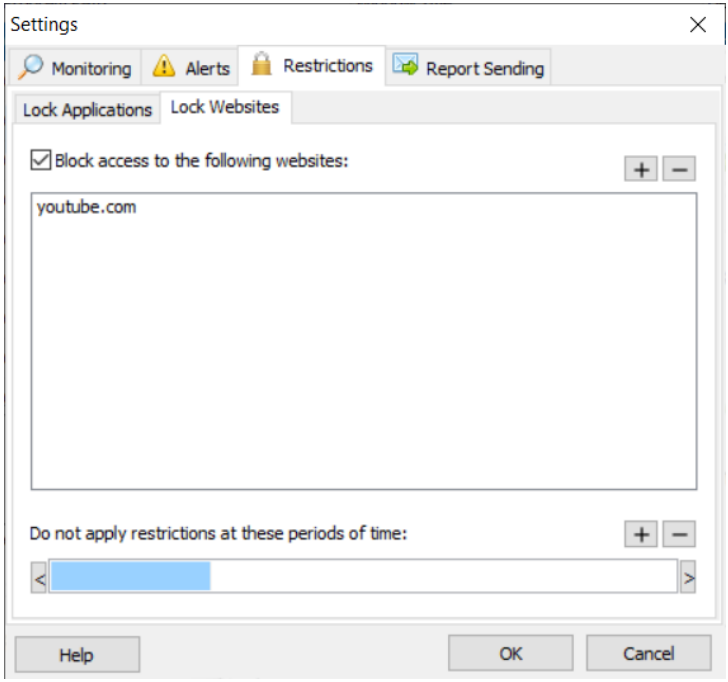


Рисунок 2.13 – Налаштування блокування веб-сайтів (на прикладі сайту YouTube)

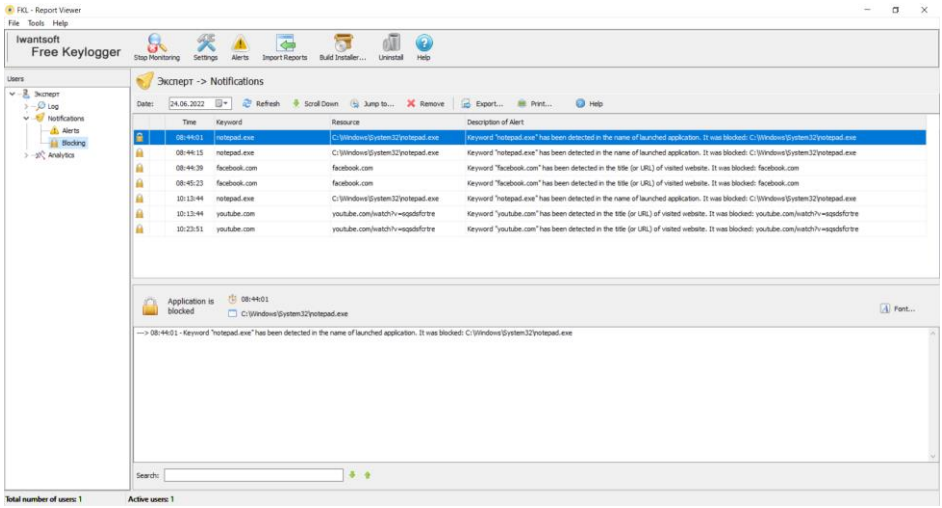


Рисунок 2.14 – Виведення інформації про блокування

12. Інформація про натискання клавіш буде відображатися так як показано далі на рисунку 2.15.

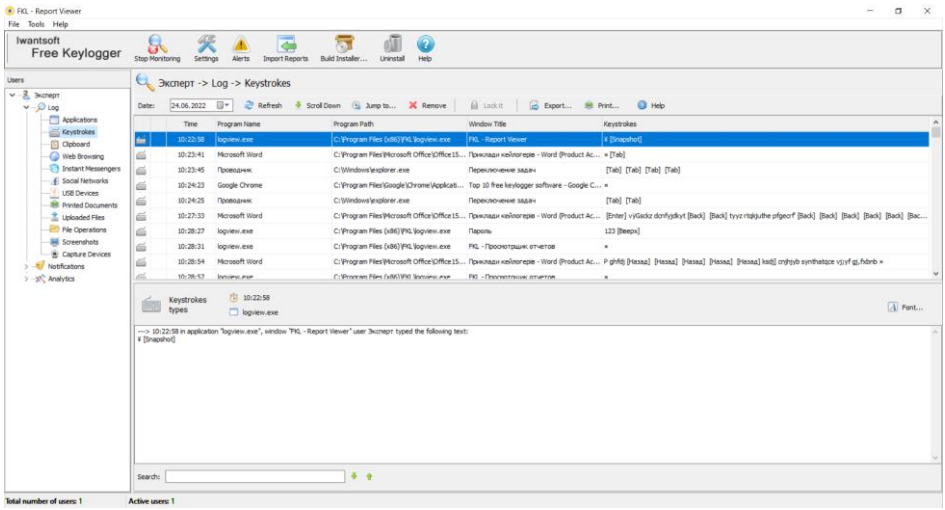


Рисунок 2.15 – Інформація про натиснуті клавіші

13. Аналітика стосовно користування додатками та веб-сайтами представляється у графічному вигляді, як то показано на рисунку 2.16.

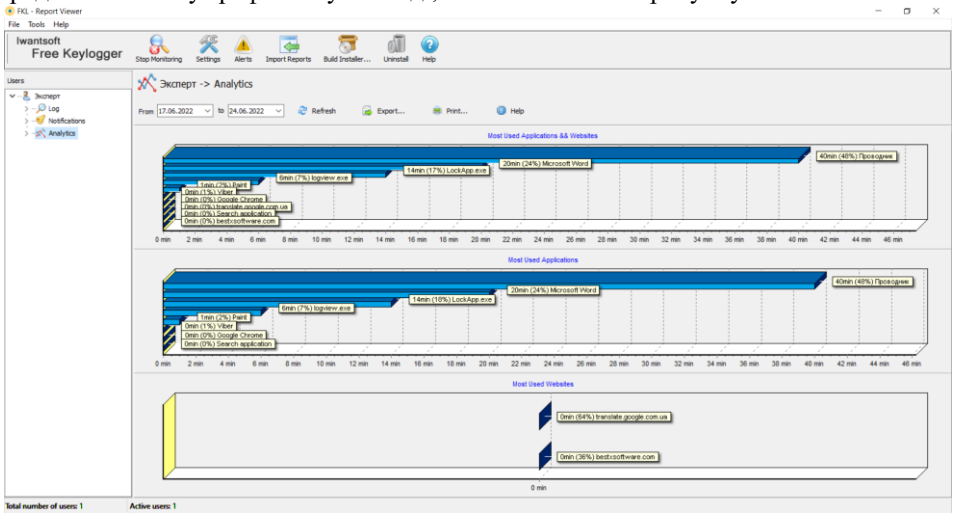


Рисунок 2.16 – Виведення аналітики щодо подій, що відстежуються

14. Якщо натиснути клавішу закриття кейлогеру, то він буде працювати у фоновому режимі. Для того, щоб знову його викликати достатньо натиснути комбінацію клавіш Ctrl+Alt+Shift+U. В процесі закрития вікна та переходу в фоновий режим з'являється вікно попередження вигляду, як представлено на рисунку 2.17

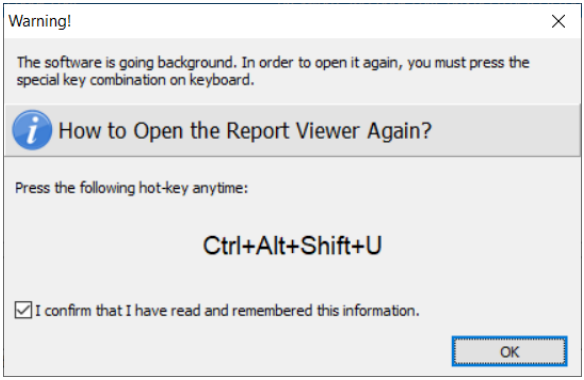


Рисунок 2.17 – Вікно попередження при переході у фоновий режим роботи

5. Додаткові завдання

1) Проведіть налаштування програмного забезпечення як вважаєте за потрібне.

2) Встановіть інший варіант кейлогеру, наприклад Spyrix Free Keylogger (https://www.spyrix.com/) та зробіть їх порівняльний аналіз.

3) Для коректної роботи в подальшому, приберіть всі правила виключення, які були задані для обох кейлогерів.

ПРАКТИЧНЕ ЗАВДАННЯ 3.
ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС ТА ШИФРУВАННЯ ДОКУМЕНТІВ

1. Короткі відомості.

Електронний цифровий підпис, або ЕЦП — універсальна сучасна можливість для ведення справ з мінімальними витратами часу. Сьогодні для того, щоб підписати договір, вести звітність, отримувати та надавати послуги, не треба їхати на зустрічі чи стояти в чергах.

Цей насправді зовсім не складний інструмент, який можна отримати за 5 хв, може врятувати підприємцю десятки годин. Хочете започаткувати справу? Можна зареєструватися в «Дії». Треба сплатити податки? Можна увійти в Електронний кабінет платника податків. Треба підписати договір? Можна підписати його з ЕЦП.

Загалом, мати його є сенс для всіх категорій населення: підприємців, клієнтів банків, споживачів фінансових послуг та навіть пенсіонерів.

Варто зазначити та запам'ятати: «електронний підпис» не дорівнює «електронний цифровий підпис». Перший — це цифрове зображення звичайного підпису, а другий фактично складається з закодованої інформації про громадянина. ЕЦП — це надійний засіб ведення справ, а е-підпис можна відтворити навіть в Paint. Саме та лише ЕЦП згідно зі законом прирівнюється до власноручного підпису.

Сучасна альтернатива традиційного підпису — це файл, у якому закодована інформація про підписанта. Також його називають «особистий ключ». Також є «відкритий ключ» — простою грубою мовою це інформація про «особистий ключ» на сервері. Коли ви, наприклад, хочете заплатити податки онлайн, ви входите з «особистим ключем» — прикріпляєте файл та вводите пароль. Коли ви натискаєте «зчитати», інформація «особистого ключа» підтверджується «серверним» «відкритим» і ви входите в сервіс.

ЕЦП може бути звичайним або посиленим. Останній роблять представникам органів влади, самоврядування та держпідприємств тощо. Для простих фізичних осіб роблять звичайний цифровий підпис через BankID. Найшвидше та безкоштовно його робить «ПриватБанк».

Для чого потрібний ЕЦП?

Для всіх онлайн-сервісів надання державних послуг, для сплати податків онлайн, для ведення звітності онлайн, отримання довідок онлайн, ведення справ та підписання документів онлайн тощо. Декількома словами: для економії часу.

Хочеш започаткувати справу? Це можна зробити онлайн через сервіс «Дія» та «вживу» через державного реєстратора — ЦНАП. Треба заплатити податки та надати податкову звітність? Це можна зробити в Електронному кабінеті платника податків. На новій роботі питають про довідку про відсутність судимості? Це можна зробити на сайті МВС.

Також ряд електронних послуг надає Пенсійний фонд. З ЕЦП можна отримати довідку про трудовий та страховий стаж, подивитися заробітну плату та суму, яка зараховується для пенсії тощо.

Тож, електронний цифровий підпис може зекономити час всім категоріям населення. А кількість сервісів, авторизація на яких відбувається з ЕЦП, з часом буде тільки збільшуватися.

ЕЦП можна отримати в будь-якому зручному акредитованого центру сертифікації ключів з цього списку. Більшість АЦСК потребують заповнення заяв, особисту присутність з документами та надають платні послуги його створення. Однак, єдиним зручним, швидким та безкоштовним надавачем ЕЦП є «ПриватБанк».

2. Практичний кейс

1. В приват 24 можна завантажити сертифікат для фізичної особи виконавши усі кроки за інструкцією https://acsk.privatbank.ua/arch/docs/instruction.pdf

Також на сайті є текстова версія інструкції https://docs.google.com/document/d/1y6TBhCn5v8NnrnCyQjjmM2vm-Q3ECXloaepNoW2E7Ts/edit

2. В результаті збережений файл-сертифікат з іменем, для прикладу, pb_2951312618.jks де перелік цифр є реєстраційним номером облікової картки платника податків того, хто реєструється.

3. Наступний крок – знайомство з програмою «ІІТ Користувач ЦСК-1.3.1» оскільки саме ця версія програми на даний час є на офіційному сайті – https://acskidd.gov.ua/korustyvach_csk

На сайті, окрім дистрибутиву самої програми є файл-інструкція для використання програми, яка містить усю необхідну інформацію по роботі із програмою - https://acskidd.gov.ua/download/manual/EU13OManualDPS.zip

4. За замовчуванням програма «ІІТ Користувач ЦСК-1.3.1» не працює із КЕП від Приватбанку. Але можливість така існує. За наступним посиланням є інструкція для прив'язки сертифікату Приватбанку до програми: http://moodle2.snu.edu.ua/mod/page/view.php?id=88529

Також є відеоінструкція щодо базового користування програмою та ЕЦП від Приватбанку: https://www.youtube.com/watch?v=ws85gPMXrnM

Після прив'язки сертифікату Приватбанку програму можна повноцінно використовувати для підписання чи перевірки підпису та шифрування файлів згідно вищевказаних інструкцій.

Рекомендація – використовувати для підписання файли формату PDF.

PS.

Підписання:

Підписаний pdf-файл отримує нове розширення – p7s. Після цього не відкривається штатними програмами перегляду. Після видалення розширення файл залишається підписаним і відкривається. Проте підписаний файл після корегування розширення піддається правкам у програмах, які такі правки дозволяють. ЕЦП після внесення правок видаляється.

Шифрування:

Зашифрований файл отримує розширення – p7e. Після видалення розширення файл перестає відкриватися.

ПРАКТИЧНЕ ЗАВДАННННЯ 4.
ШИФРУВАННЯ ЕЛЕКТРОННОЇ ПОШТИ

1. Короткі відомості

Електронна пошта може бути однією з найменш безпечних платформ. Щодня люди вільно обмінюються особистою інформацією, не переймаючись тим, хто може її побачити або в чиї руки вона може потрапити.

Багато людей знайомі з кількома стандартними порадами з безпеки, такими як використання надійних паролів та уникнення шпигунських програм. Однак більшість недооцінюють важливість використання зашифрованої електронної пошти.

Шифрування електронної пошти – це процес маскування вмісту електронних повідомлень, щоб захистити їх від прочитання небажаними сторонами. Конфіденційна інформація, як-от номери соціального страхування, паролі, облікові дані для входу та номери банківських рахунків, є вразливою під час надсилання електронною поштою.

Шифрування електронної пошти означає процес шифрування, надсилання та дешифрування електронної пошти, що робить її практично нечитабельною для небажаних третіх сторін. Лише призначений одержувач зможе прочитати зашифроване повідомлення, оскільки лише він матиме правильні ключі для його розшифровки. Деякі служби електронної пошти мають цю функцію, яка автоматично шифрує та розшифровує повідомлення, тоді як інші покладаються на більш складні методи захисту електронної пошти.

Можливо, ви пам'ятаєте кілька великих витоків даних: Facebook, LinkedIn, Marriott International та особливо Equifax. У великого бізнесу найбільше грошей і даних, тому цілком логічно, що хакери націлюватимуться на них. Однак найбільшому ризику можуть наражатися стартапи і невеликі компанії.

Невеликі компанії особливо вразливі, тому що часто не вистачає персоналу або ресурсів, необхідних для захисту або відновлення після атаки. Шифрування електронної пошти ускладнює хакеру доступ до особистої інформації, що знижує ризик злому.

У більшості країн діє безліч всеосяжних законів про конфіденційність, які вимагають від компаній захищати конфіденційну інформацію від хакерів. Це включає:

- *Каліфорнійський закон про захист прав споживачів* від 2018 р. (CCPA): компанії, які відповідають певним умовам, повинні шифрувати дані та дотримуватися «розумних процедур безпеки», інакше вони ризикують бути притягнутими до відповідальності у разі компрометації даних.
- *Вимоги кібербезпеки Департаменту фінансових послуг штату Нью-Йорк для компаній,* що надають фінансові послуги: цей закон застосовується до більшості банкірів, страхових компаній та інших фінансових установ. Ці встановлені державою вимоги гарантують, що фінансові компанії шифрують особисті дані (або вживають інших заходів для пом'якшення наслідків, якщо вони не можуть використовувати шифрування) та регулярно видаляють непотрібні дані.
- *Закон про перенесення та підзвітність медичного страхування* (HIPAA): Підписаний Біллом Клінтоном у 1996 році закон HIPAA вимагає, щоб медичні установи не передавали та не продавали дані пацієнтів.
- *Європейське банківське управління* (EBA): фінансові установи та організації, що надають платіжні послуги, повинні шифрувати особисті дані. Крім того, інтернет-магазини не можуть зберігати незахищені дані.
- *Загальне положення щодо захисту даних* (GDPR): Компанії, які зберігають особисту інформацію про клієнтів, повинні належним чином захищати такі дані від сторонніх. Крім того, громадяни ЄС мають «право на доступ» до своїх даних, а також «право на забуття» та «право на отримання інформації».

Шифрування електронної пошти по суті змішує вміст електронної пошти, тому воно стає загадкою, ключ до розгадки якої є тільки у вас. Інфраструктура відкритого ключа (PKI) використовується для шифрування та розшифровування електронної пошти. Кожній людині надається відкритий та закритий ключ у вигляді цифрового коду.

Відкритий ключ зберігається на сервері ключів разом з ім'ям та адресою електронної пошти людини, і будь-хто може отримати доступ до нього. Цей відкритий ключ використовується для шифрування електронної пошти. Якщо хтось захоче надіслати вам електронний лист із конфіденційною інформацією, він скористається вашим відкритим ключем для її шифрування. Закритий ключ використовується для розшифровування електронних листів. Він зберігається у безпечному та конфіденційному місці на комп'ютері людини, і лише ця людина має до неї доступ. Закритий ключ також можна використовувати для цифрового підпису повідомлення, щоб одержувач знав, що воно прийшло від вас.

2. Типи протоколів для шифрування електронної пошти

Розробники систем, спрямованих на захист електронної пошти, на власному досвіді знають, що миттєве вирішення проблеми захисту таких систем неможливе, оскільки хакери, творці та розповсюджувачі вірусів винахідливі, що спонукає постійно розвивати та вдосконалювати методи захисту. Слід також враховувати, що для забезпечення найвищого рівня захисту, необхідно застосовувати комплексний та систематичний підхід, з урахуванням всіх загроз та ризиків щодо безпеки пересилання електронних листів.

На сьогодні популярним є використання таких протоколів, як PGP (від англ. Pretty Good Privacy - «Досить хороша приватність») та S/MIME (від англ. Secure/Multipurpose Internet Mail Extensions – «Безпечне/багатоцільове розширення для електронної пошти»).

PGP – це бібліотека функцій, що дозволяє виконувати операції шифрування та цифрового підпису повідомлень, файлів та іншої інформації, що представлена в електронному вигляді, в тому числі прозоре шифрування даних на запам’ятовуючих пристроях, наприклад, на жорсткому диску.

До переваг PGP слід віднести:

1) наявність сервера ключів, який дозволяє користувачам обмінюватись ключами та усуває необхідність публікації ключів, або передавати їх кожному адресату в особистому порядку;

2) система опрацьовує трафік, шифрує повідомлення, що надсилаються і автоматично розшифровує вхідні повідомлення.

До недоліків протоколу PGP відносять:

1) вже розшифровані повідомлення залишаються незахищеними в клієнті;

2) якщо поштовий клієнт вже отримав повідомлення, а PGP Desktop не було запущено, то дешифрування листа стає непосильною задачею.

S/MIME — це стандарт для шифрування і підпису в електронній пошті за допомогою відкритого ключа. Під час роботи реалізується класична схема асиметричного шифрування з усіма її недоліками та перевагами. Користувач генерує

відкритий та закритий ключ, налаштовує свій поштовий клієнт і надсилає відкритий ключ всім бажаючим, які шифрують свої листи отриманим ключем і дешифруються лише закритим ключем.

Переваги S/MIME:

1) листи в поштовому клієнті лишаються зашифрованими до тих пір, доки користувач сам їх не розшифрує. Для здійснення операції дешифрування необхідне введення паролю, що вказується під час створення ключової пари (відкритого/закритого ключа);

2) на відміну від PGP Desktop, дешифрування відбувається поштовим клієнтом, а не окремою програмою, тому розшифрувати лист можна за будь-якої нагоди;

3) підтримка більшості поштових клієнтів (в тому числі мобільних).

Недоліки S/MIME:

1) постає питання про програму, яка згенерувала б сертифікат;

2) необхідно обдумати питання реалізації обміну ключами між учасниками.

Для забезпечення більш надійного захисту конфіденційності даних в ідеалі рекомендується використовувати S/MIME, надійність якого полягає в тому, що повідомлення зберігаються в поштовому клієнті в зашифрованому вигляді і розшифровуються лише при зверненні до них.

3. Приклади сервісів шифрування пошти

Шифрування - це метод перетворення даних у нерозбірливий формат, щоб отримати доступ до інформації лише уповноважені сторони. Зміст листа може прочитати тільки одержувач. Лист шифрується відкритим ключем одержувача і може бути розшифрований тільки закритим ключем. Зміст листа може прочитати тільки одержувач. Лист шифрується відкритим ключем одержувача і може бути розшифрований тільки закритим ключем одержувача. Текст листа не можна змінити "по дорозі". Відкритий ключ відправника пересилається разом з листом.

Для реалізації таких дій на сьогодні є низка популярних сервісів шифрування.

Tutanota – система, яка дозволяє шифрувати всі повідомлення, включаючи тему та заголовки (рисунок 4.1). При використанні даної системи код повністю з відкритим вихідним кодом. Рівень безкоштовного користування не має обмежень на кількість повідомлень. Функціонує повноцінний календар та безпечний пошук зашифрованих повідомлень.

Є можливість використовувати Tutanota безкоштовно але з деякими обмеження. Безкоштовна версія дозволяє надсилати та отримувати будь-які захищені повідомлення, а також включає захищений календар. Пошук у зашифрованій електронній пошті обмежений — у безкоштовній версії ви можете шукати лише повідомлення не старші за місяць. Оплата підписки за 12 євро на рік знімає це обмеження пошуку, дозволяє вам мати кілька календарів та додає функції, включаючи правила фільтрації та п'ять псевдонімів адрес електронної пошти.

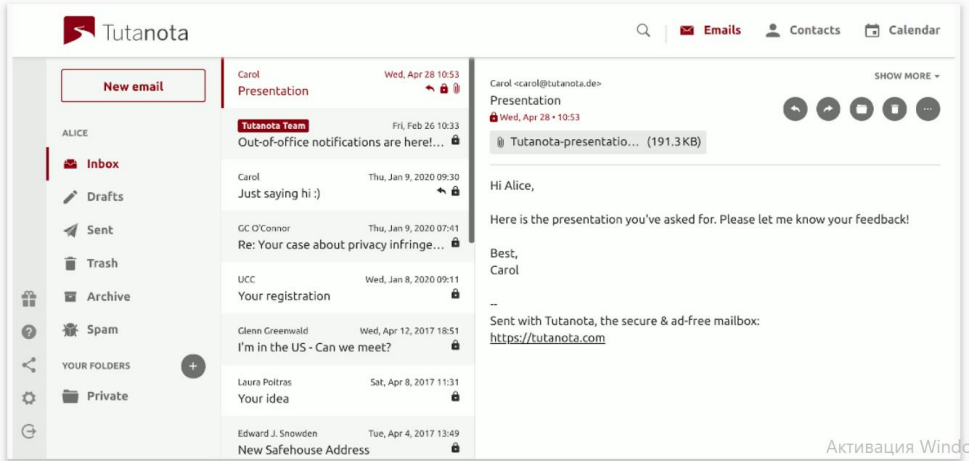


Рисунок 4.1 – Зовнішній вигляд системи Tutanota

ProtonMail – це простий сервіс веб-пошти (рисунок 4.2), який захищає ваш архів повідомлень за допомогою шифрування з нульовим доступом та пропонує наскрізне шифрування для надсилання повідомлень. Цей продукт також включає безпечний календар і (бета-версію) систему зберігання файлів.

ProtonMail зберігає дані, використовуючи шифрування з нульовим доступом, що означає, що ніхто, крім вас, не може отримати доступ до них. Коли ви спілкуєтеся з іншими користувачами ProtonMail, ви отримуєте наскрізне шифрування.

Virtru захищає та зберігає повідомлення електронної пошти для гігантських корпорацій. Virtru Email Protection для Gmail надає споживачам таке саме першокласне шифрування безкоштовно. Зовнішній вигляд інтерфейсу програми Virtru проілюстрований на рисунку 4.3.

Всесвітня система електронної пошти, на яку ми всі покладаємося, була винайдена багато десятиліть тому, і її винахідники просто не приділяли багато уваги захисту конфіденційності електронної пошти. Проте на сьогодні омпанії не тільки повинні стежити за тим, щоб їх повідомлення електронної пошти не були перехоплені не тими людьми, вони зобов'язані зберігати всі такі повідомлення відповідно до законів про відповідність. Virtru забезпечує безпеку та зберігання даних для великих компаній, але й приватні особи можуть скористатися перевагами цієї високорівневої технології, встановивши Virtru Email Protection для Gmail. На споживчому рівні ця служба шифрування електронної пошти безкоштовна.

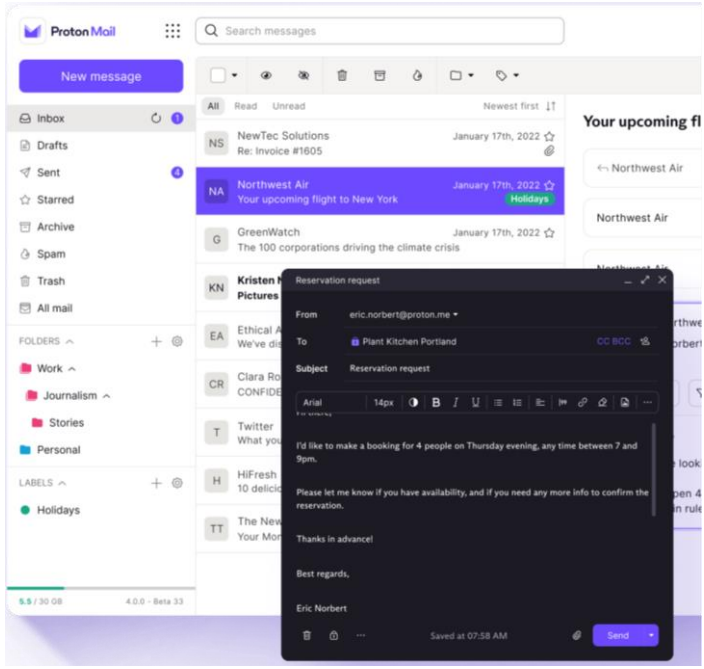


Рисунок 4.2 – Зовнішній вигляд сервісу ProtonMail

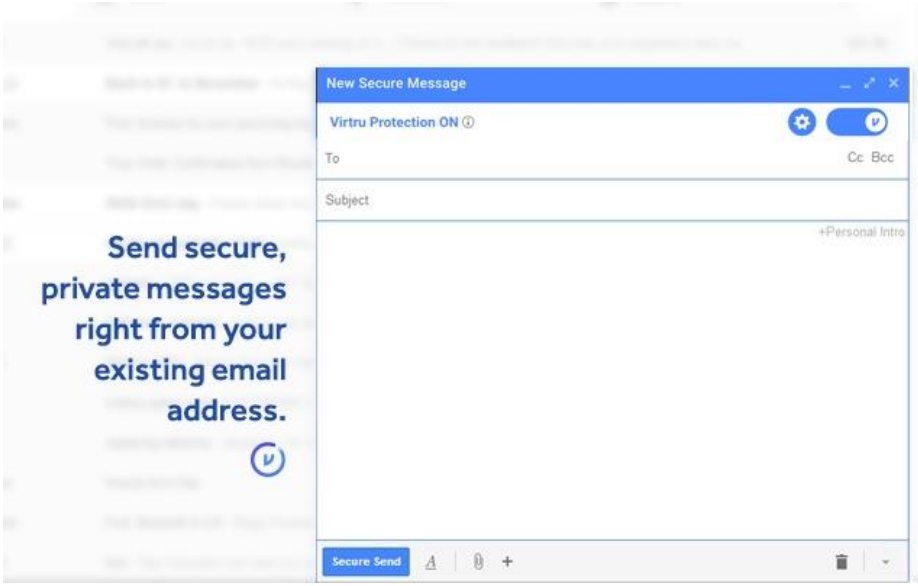


Рисунок 4.3 – Приклад використання Virtru

4. Практичний кейс

До вирішення надається наступна задача. Налаштувати сервіс шифрування електронної пошти.

Умови вирішення наступні.

5) необхідно встановити протокол шифрування пошти;

6) налаштувати роботу пошти за допомогою встановленого протоколу шифрування.

Алгоритм вирішення задачі.

Для того, щоб налаштувати шифрування електронної пошти, було обрано використовувати сертифікат S/MIME. Як варіант сертифікату застосуємо безкоштовну версію для особистої електронної пошти від компанії Actalis.

1. Заходимо на сайт компанії Actalis за посиланням: https://www.actalis.com/s-mime-certificates.aspx та обираємо обрати безкоштовний сертифікат (рисунок 4.4).

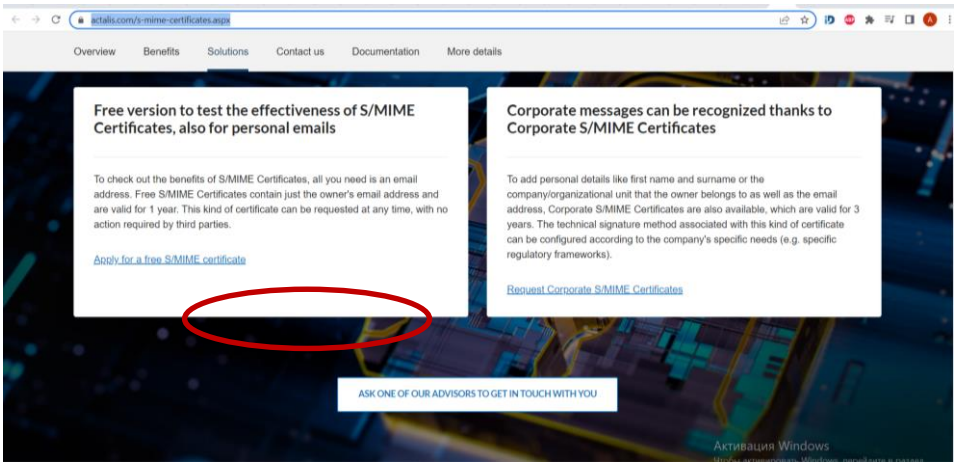


Рисунок 4.4 – Сайт для отримання безкоштовного сертифікату шифрування

2. При використанні даного сертифікату є один недолік: він працює виключно для поштових адрес типу xxx@xxx.xxx, тобто не можна використовувати корпоративну студентську пошту, як то наприклад, xxx@snu.edu.ua. Отже для шифрування пошти обираємо особисту некорпоративну пошту.

3. Після обрання корпоративної пошти на неї повинен прийти код верифікації, який необхідно буде ввести на другому етапі отримання сертифікату (рисунок 4.5).

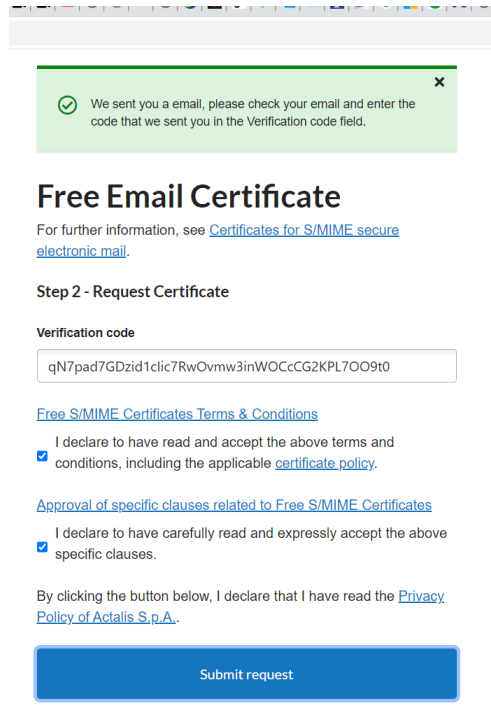


Рисунок 4.5 – Отримання сертифікату для шифрування

3. Після цього ви побачите повідомлення про отримання сертифікату на пошту і побачите пароль, який необхідно буде використати.

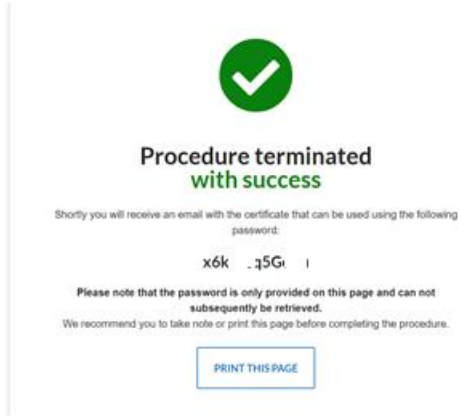
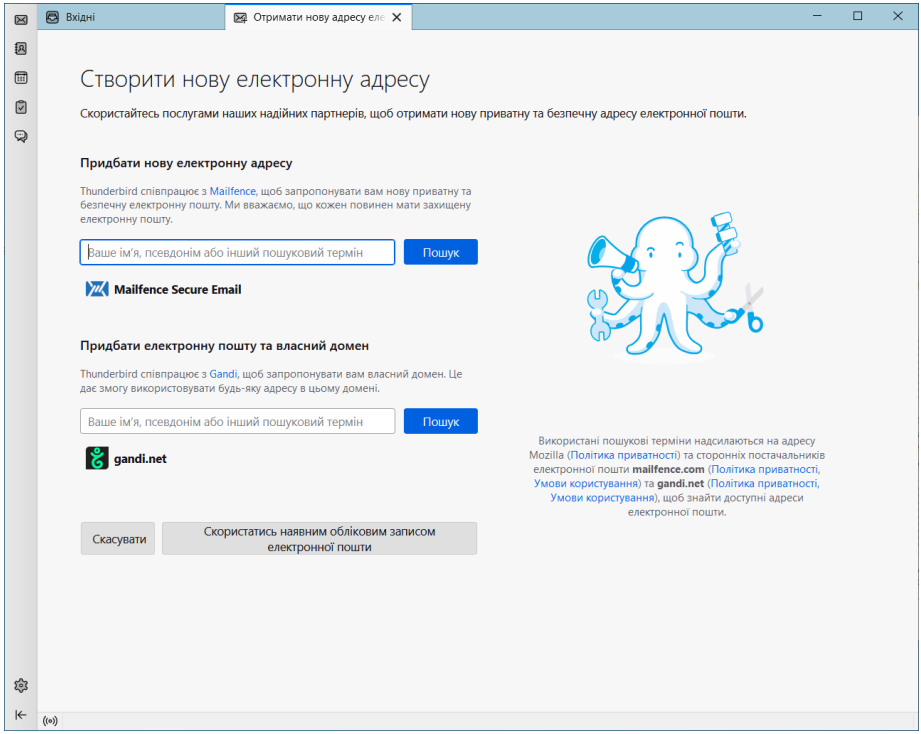


Рисунок 4.6 – Вікно завершення генерації сертифікату

Зверніть увагу!!! Пароль записано виключно на сторінці про отримання сертифікату і більше ніде його немає. Тому рекомендуємо спочатку запам'ятати пароль. В інакшому випадку не буде можливості встановити сертифікат до поштового сервісу.

5. В якості поштового сервісу запропоновано використовувати безкоштовний сервіс Thunderbird. Завантажити його можна за посиланням https://www.thunderbird.net/uk/.

6. Для налаштування своєї електронної пошти оберіть пункт «Скористатись наявним обліковим записом електронної пошти», якто то показано на рисунку 4.7.



Рисбунок 4.7 – Вікно створення електронної пошти

Після чого можна буде ввести адресу своєї пошти та пароль для роботи у сервісі (рисунок 4.8).

7. Перед початком роботи за допомогою меню «Інструменти / Налаштування» є змогу змінити мову для показу меню та сповіщень у Thunderbird (рисунок 4.9).

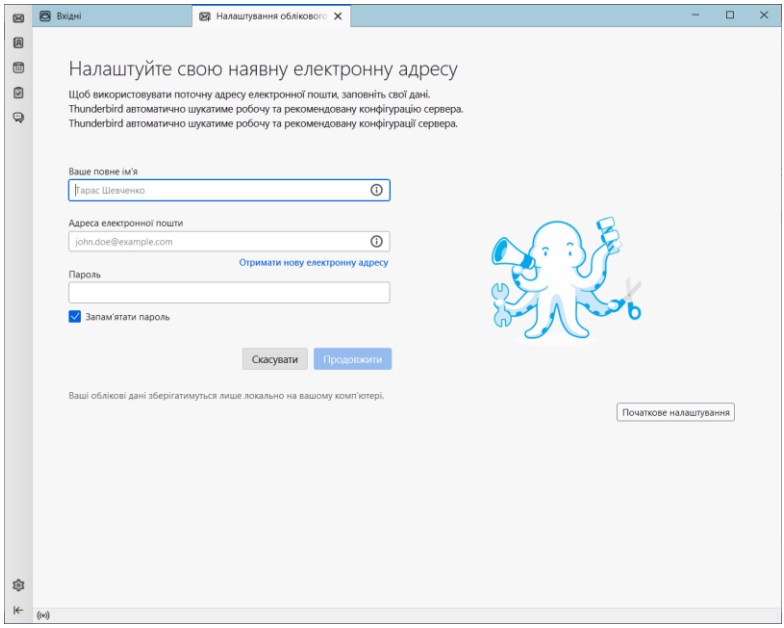


Рисунок 4.8 – Налаштування електронної пошти

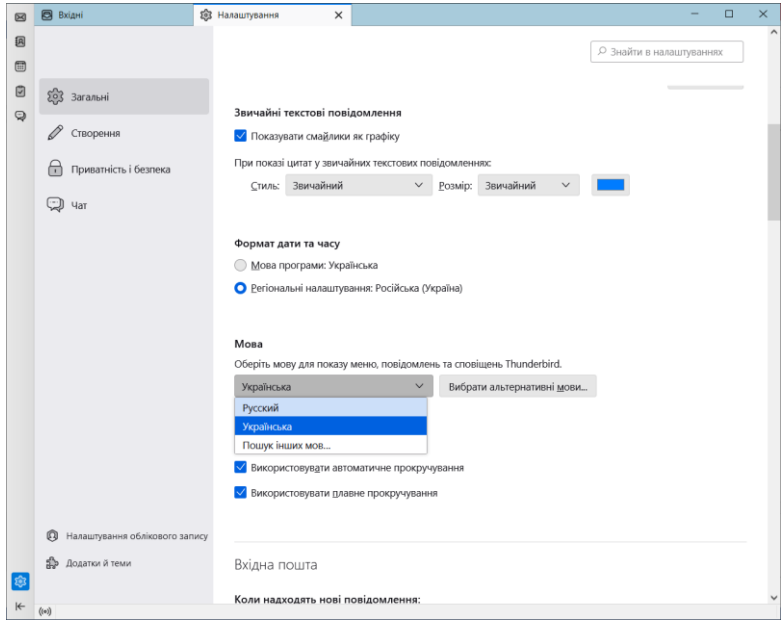


Рисунок 4.9 – Налаштування мови інтерфейсу

8. Для налаштування шифрування пошти в меню «Інструменти» обираємо «Налаштування облікового запису» та переходимо у підменю «Наскрізне шифрування».

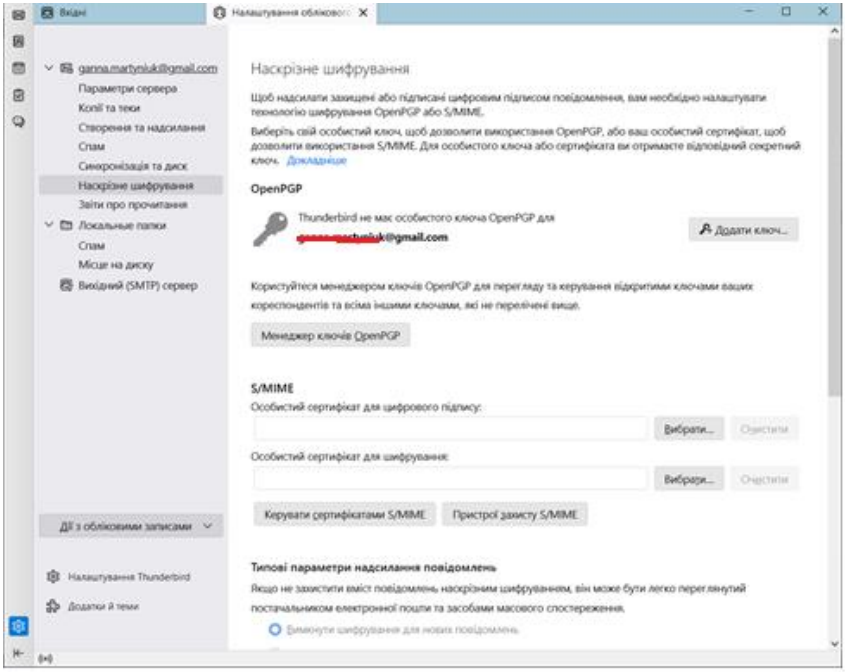


Рисунок 4.10 - Налаштування наскрізного шифрування

9. Натискаємо кнопку «Керувати сертифікатами S/MIME» після чого у підменю «Ваші сертифікати» нажимаємо кнопку «Імпорт…», як то показано на рисунку 4.11.

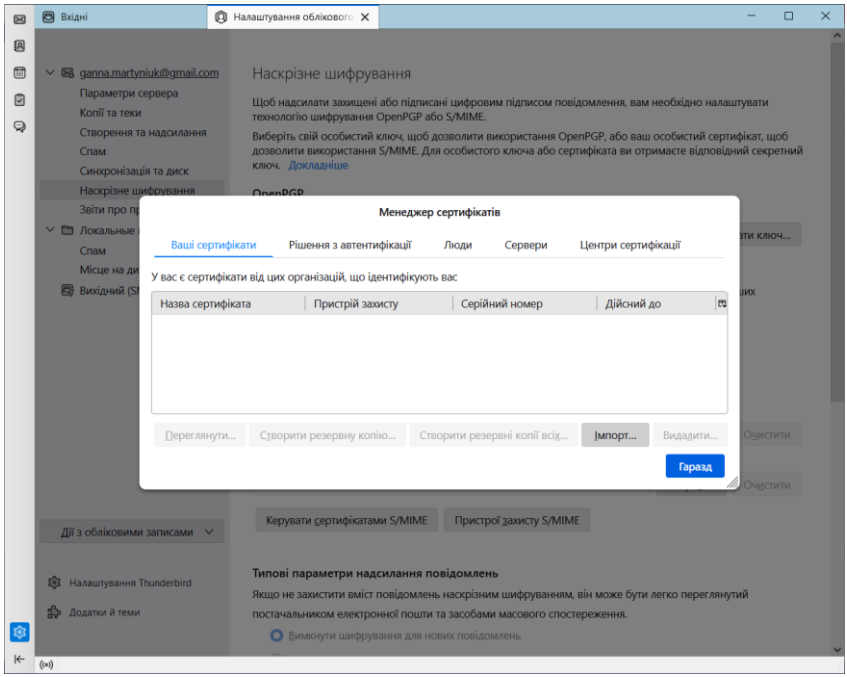


Рисунок 4.11 – Вікно менеджера створених сертифікатів

10. Імпортуємо отриманий у п.4 сертифікат, як показано на рисунку 4.12.

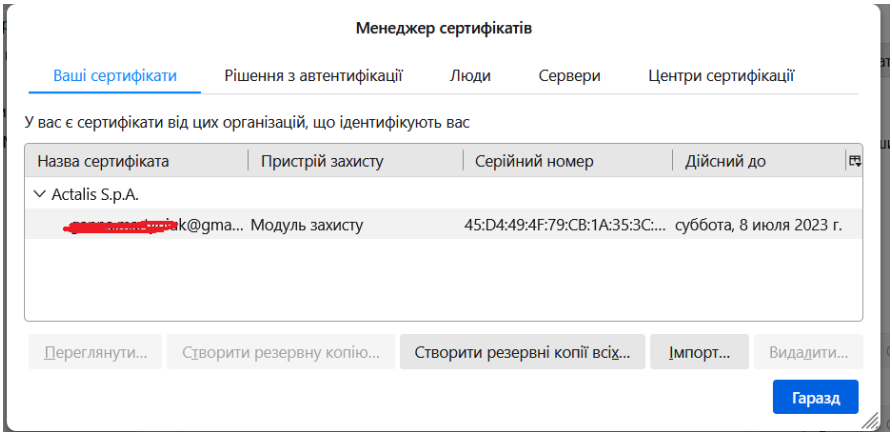


Рисунок 4.12 – Імпортування отриманого сертифікату

11. Далі обираємо отриманий сертифікат, натиснувши кнопку «Вибрати» у пункті «Особистий сертифікат для шифрування» та налаштовуємо інші параметри шифрування.

12. Далі створення електронного листа буде виглядати так, як проілюстровано на рисунку 4.13.

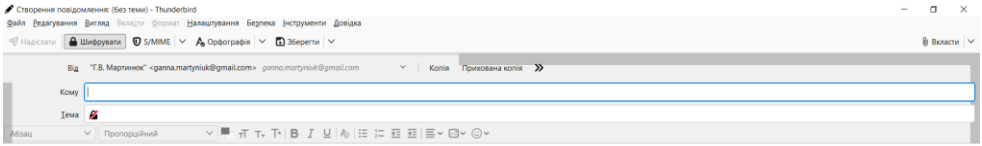


Рисунок 4.13 – Створення електронного листа

Як видно з рисунку 4.13, зараз активна кнопка шифрування і для всіх листів буде використовуватися наскрізне шифрування. Для того, щоб його прибрати, доцільно буде ще раз натиснути на кнопку «Шифрувати».

5. Додаткові завдання

1) Налаштувати наскрізне шифрування особистої пошти.

2) Описати ситуацію відправки листа людині, яка не має протоколу наскрізного шифрування.

3) Відправити листа одногрупнику, який вже також налаштував наскрізне шифрування та пояснити результат відправки.

НАВЧАЛЬНО-МЕТОДИЧНЕ ТА ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ НАУКОВО-ДОСЛІДНОЇ ПРАКТИКИ

1. 1. The United Nations E-Government Survey 2018: Gearing E-Government to Support Transformation towards sustainable and resilient societies URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-GovernmentSurvey-2018.

2. Кохан В.П., Єгорова-Луценко Т.П. Стан розвитку електронних адміністративних послуг: огляд впровадження на державному рівні. Право та інноваційне суспільство, 2018, №2 (11) 12 с. URL: http://apir.org.ua/wp-content/uploads/2018/12/Kokhan_Egorova-Lutcenko11.pdf.

3. The United Nations E-Government Survey 2014: E-Government for the Future We Want. URL: https:// publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2014.

4. The United Nations E-Government Survey 2016: E-Government in Support of Sustainable Development. URL: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016.

5. Полярна В.Л., Рябець В.В. Європейські практики надання електронних послуг в правоохоронній діяльності та перспективи їх провадження в Україні, 36 с. URL:http://ktpu.kpi.ua/wp-content/uploads/2017/02/Ryabets_ Polyarna_Derzhavne-upravlinnya.pdf.

6. Правове регулювання відносин у мережі Інтернет : монографія /[А. П. Гетьман, Ю. Є. Атаманова, В. С. Мілаш та ін.] ; за ред. С. В. Глібка, К. В. Єфремової. Харків : Право, 2016. 360 с.

7. Про схвалення Концепції розвитку системи електронних послуг в Україні: розпорядженням Кабінету Міністрів України від 16.11.2016 р. № 918-р. Офіційний вісник України. 2016 р. № 99. Стор. 259. Стаття 3234.

8. Про адміністративні послуги: Закон України від 6.09.2012р. № 5203-VI. URL: http://zakon.rada.gov.ua/laws/ show/5203-17.

9. Єдиний державний портал адміністративних послуг. URL: https://poslugy.gov.ua.

10. Про затвердження Примірного положення про центр надання адміністративних послуг: постанова Кабінету міністрів України від 20.02.2013 р. № 118. URL: http://zakon.rada.gov.ua/laws/show/118-2013-%D0%BF.

11. Про Стратегію сталого розвитку «Україна – 2020»: Указ Президента України від 12.01.2015 р. № 5/2015. URL: http://zakon2.rada.gov.ua/laws/show/5/2015.

12. Деякі питання реформування державного управління України»: розпорядження КМУ від 24.06.2016 р. № 474 р. URL: http://zakon.rada.gov.ua/laws/show/474-2016-%D1%80.

13. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження КМУ від 20.09.2017 р. № 649-р. URL: http://zakon.rada.gov.ua/laws/show/649-2017-%D1%80.

14. Про електронні документи та електронний документообіг: Закон України від 22.05.2003р. N 851-IV. URL: http://zakon.rada.gov.ua/laws/show/851-15.

15. Про електронні довірчі послуги: Закон України від 5.10.2017 р. № 2155-VIII. URL: http://zakon.rada.gov.ua/ laws/show/2155-19.

16. Веб-ресурс електронних послуг Державної служби України з питань геодезії, картографії та кадастру. URL: https://e.land.gov.ua.

17. Про затвердження Порядку ведення Єдиного державного порталу адміністративних послуг: постанова КМУ від 3.01.2013 р. № 13. URL: http://zakon.rada.gov.ua/laws/show/13-2013-%D0%BF.

18. Про затвердження Положення про Систему BankID Національного банку України: постанова правління Національного банку України 30.08.2016 р. № 378. URL: http://zakon.rada.gov.ua/laws/show/v0378500-16.

19. НБУ розширив можливості системи BankID. URL: https://www.epravda.com.ua/news/2018/10/10/641481/.

20. Glibko S. Problems of legal provision of innovative banking. European political and law discourse. Vol. 3. Issue 3. 2016. 168–173.

21. Електронна система здійснення декларативних процедур у будівництві. URL: https://e-dabi.gov.ua/.

22. Інструкція з отримання електронної послуги. URL: https://e-dabi.gov.ua/images/dabi_instr.pdf.

23. Електронні адміністративні послуги Міністерства екології та природних ресурсів України URL: e-eco.gov.ua.

24. Кабінет електронних сервісів Міністерства юстиції України. URL: https://kap.minjust.gov.ua.

25. Веб-портал «Звернення у сфері державної реєстрації актів цивільного стану». URL: https://dracs.minjust.gov. ua.

26. Електронні сервіси Державної фіскальної служби України. URL: http://sfs.gov.ua/diyalnist-/elektronnyi-servisi.

27. Портал електронних послуг Пенсійного фонду України. URL: https://portal.pfu.gov.ua.

Навчальне видання

МЕТОДИЧНІ ВКАЗІВКИ

щодо виконання практичних завдань з курсу «Кібербезпека в аспекті інформатизації та діджиталізації суспільства» для здобувачів вищої освіти, усіх спеціальностей та рівнів підготовки (електронне видання)

Укладач:
Захожай Олег Ігорович

Редактор О.*І. Захожай*
Техн. редактор *О.І. Захожай*
Оригінал - макет *О.І. Захожай*

Підписано до друку _____
Формат $60 \times 84\ 1/16$. Папір типограф. Гарнитура *Times*.
Друк офсетний. Ум. друк. арк.___. Обл.-вид.арк._____.
Тираж ___ прим. Вид. №_____. Замовл. №_____. Ціна договірна.

Видавництво Східноукраїнського національного університету імені Володимира Даля

Свідоцтво про реєстрацію: серія ДК № 1620 від 18.12.03 р.
Адреса університету: вул. Іоанна Павла II, 17,
м. Київ, 01042, Україна
e-mail: vidavnictvoSNU.ua@gmail.com.