© Harasymchuk O., Chentsov O. Keepass as a password and data security manager // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 2, pp. 324-329. ©

DOI: 10.18372/2225-5036.30.19245

ВИКОРИСТАННЯ МЕНЕДЖЕРА ПАРОЛІВ KEEPASS ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ ДАНИХ

Олег Гарасимчук, Олег Ченцов

Національний університет «Львівська політехніка»

ГАРАСИМЧУК Олег Ігорович, к.т.н., доц.
Рік та місце народження: 1979 рік, м. Бережани, Тернопільська обл., Україна.
Освіта: Національний університет «Львівська політехніка», 2001 рік.
Посада: доцент кафедри захисту інформації з 2008 року.
Наукові інтереси: комплексні системи санкціонованого доступу, генерування псевдовипадкових чисел та послідовностей, генерування пуассонівських імпульсних послідовностей, методи і засоби захисту інформації, проектування комплексних систем захисту інформації, бази даних та знань, захист даних, сигнальні процесори в системах захисту інформації.
Публікації: більше 100 наукових публікацій, серед яких наукові статті, монографії, навчальний посібник, патенти, тези та матеріали доповідей на конференціях.
E-mail: oleh.harasymchuk@gmail.com.
Orcid ID: 0000-0002-8742-8872.

ЧЕНЦОВ Олег Олександрович, студент
Рік та місце народження: 2000 рік, м. Дрогобич, Львівської обл., Україна.
Освіта: Національний університет «Львівська політехніка», 2024 рік.
Посада: студент кафедри захисту інформації.
Наукові інтереси: кібербезпека в хмарних середовищах, захист персональних даних.
E-mail: chentsov.oleh@gmail.com.
Orcid ID: 0009-0006-5739-4364.

Анотація. *Захист даних є критично важливим аспектом сучасного інформаційного середовища, оскільки постійно зростає кількість загроз, як з боку зловмисників, так і внаслідок людських помилок, що ставить під загрозу конфіденційність і цілісність інформації. Основні принципи захисту даних включають управління доступом, шифрування, резервне копіювання та моніторинг активності. Багаторівневий підхід до безпеки, що включає фізичні, адміністративні та технічні заходи, дозволяє знизити ризики несанкціонованого доступу та втрати даних. У статті розглядається важливість безпеки паролів у сучасному цифровому середовищі. З огляду на зростаючу кількість кіберзагроз, збереження конфіденційності та захист персональних даних стали пріоритетними завданнями. Одним із ефективних інструментів для управління паролями є KeePass – програма для зберігання паролів, яка забезпечує високий рівень шифрування та безпеки. У даній роботі проаналізовані ключові функції KeePass, його переваги та недоліки в порівнянні з іншими менеджерами паролів. У статті також звертається увага на необхідність вибору надійного менеджера паролів для забезпечення багаторівневого захисту даних користувачів. Використання таких інструментів стає особливо актуальним в умовах зростання кількості кібератак та необхідності збереження конфіденційності в різних галузях, включаючи бізнес та державні установи.*

Ключові слова: *захист даних, шифрування, управління доступом, 1Password, Keeper, Enpass, KeePass.*

Постановка проблеми

Хоча багато технологій обіцяли замінити паролі, вони все ж залишаються основним засобом захисту онлайн-акаунтів. Це створює ризик для безпеки, оскільки більшість особистих даних захищені паролями, які потрібно запам'ятовувати та часто змінювати. До того ж користувачі часто ігнорують двофакторну автентифікацію та повторно використовують паролі, що підвищує ризики. Менеджери паролів пропонують вирішення цих проблем, зберігаючи паролі у безпечному зашифрованому сховищі, автоматично заповнюючи їх та генеруючи надійні.

Вибір надійного менеджера паролів є важливим для забезпечення безпеки і зручності управління паролями. Саме тому у цифровому світі, де безліч облікових записів та паролів є нормою, менеджери паролів стають

незамінними інструментами для забезпечення безпеки та ефективності. Менеджер паролів – це програмне забезпечення, яке допомагає користувачам створювати, зберігати та керувати унікальними паролями для різних онлайн-сервісів. Цей інструмент важливий не тільки для забезпечення безпеки особистих даних, але й для оптимізації робочого процесу. За допомогою менеджера паролів користувач може забути про потребу запам'ятовувати безліч складних комбінацій, оскільки він зберігає всі паролі в зашифрованому сховищі, доступ до якого можливий лише з одним майстер-паролем. Крім того, багато менеджерів паролів пропонують функцію генерації випадкових та надійних паролів, що є критично важливим для захисту облікових записів від злому. Це зменшує ризики, пов'язані з використанням одного та того ж пароля для декількох сайтів, що є поширеною проблемою в кібербезпеці та призводить до значної кількості інцидентів та втрат даних.

Аналіз останніх досліджень та публікацій

Менеджери паролів також часто володіють додатковими функціями безпеки, такими як двофакторна автентифікація, шифрування end-to-end та автоматичне заповнення форм, що дозволяє користувачам не тільки захищати свої паролі, але й спрощувати процес їх використання [1-3]. Ці інструменти важливі не тільки для індивідуальних користувачів, але й для бізнесу, де управління великою кількістю облікових записів та забезпечення їх безпеки є ключовим аспектом захисту важливої корпоративної інформації. Використання менеджера паролів значно знижує ризики пов'язані з кіберзлочинністю, такі як фішинг, хакерські атаки та витік даних, забезпечуючи надійний захист цифрової ідентичності користувача. На сьогоднішній день існує цілий ряд праць та матеріалів, що присвячені різним менеджерам паролів, формам їх реалізації, сферам використання, а також підходам і принципам, що лежать в основі їх роботи [4-8] і класифікаціям. Зокрема можна виділити чотири основні групи менеджерів паролів.

1. Менеджери паролів вбудовані у веб-браузері. Дана група менеджерів паролів може здаватися найбільш зручною, оскільки вони безкоштовні та не потребують додаткового програмного забезпечення. Однак у них є кілька важливих недоліків у плані безпеки та функціональності. Найбільш очевидний недолік – ці менеджери прив'язані до конкретного браузера. Хоча можна перенести паролі, автоматична синхронізація між різними браузерами недоступна. Крім того, вони можуть некоректно працювати з деякими додатками при заповненні паролів. Також у таких інструментах часто відсутні важливі функції, такі як генерація паролів, оцінка їх надійності, моніторинг темної мережі або підтримка двофакторної автентифікації. На сьогоднішній день це дуже важливі інструменти для захисту, тому варто подумати про перехід на більш функціональний менеджер паролів, якщо ви досі користуєтесь браузерним.

2. Хмарні менеджери паролів. Оскільки більшість людей використовує паролі на різних пристроях, хмарні менеджери паролів стають стандартом для управління паролями. Ці сервіси дозволяють зберігати паролі у хмарі та автоматично синхронізувати їх між всіма пристроями користувачів. Хмарні менеджери мають більше можливостей порівняно з браузерними, зокрема спрощений доступ при використанні нових пристроїв, додатків чи браузерів. Основний ризик полягає в тому, що дані користувачів зберігаються в Інтернеті, що зменшує контроль над їхньою безпекою. Хоча ці сервіси зазвичай надійні, вони не повністю захищені від потенційних зломів.

3. Офлайн-менеджери паролів. Деякі менеджери паролів дозволяють зберігати паролі лише в автономному режимі, без синхронізації з хмарою. У цьому випадку паролі користувачів будуть доступні лише на конкретному пристрої, без можливості автоматичного переносу між іншими. Такий підхід виключає ризик перехоплення даних під час передачі через Інтернет і надає користувачам повний контроль над їхнім зберіганням. Однак, щоб не втратити дані у разі пошкодження чи втрати пристрою, користувачу доведеться самостійно робити резервні копії.

4. Мобільні менеджери паролів. Хоча для мобільних пристроїв доступно багато хмарних програм для керування паролями, iOS і Android пропонують власні менеджери паролів, такі як Apple Keychain і Google Password Manager, що дозволяє користувачам безпечно зберігати паролі на своїх мобільних пристроях. Мобільні менеджери паролів — це додатки, які дозволяють зберігати та автоматично вводити паролі на смартфонах і планшетах. Вони забезпечують зручний доступ до ваших облікових даних на ходу, синхронізуючи паролі між пристроями через хмару. Вони також допомагають, автоматично заповнюючи паролі на веб-сайтах і в мобільних додатках. Багато з них також пропонують додаткові функції, такі як двофакторна автентифікація, генерація надійних паролів та моніторинг безпеки, що робить їх важливими інструментами для захисту мобільних користувачів.

Мета та постановка завдання

Основною метою роботи є порівняльний аналіз популярних менеджерів паролів з метою полегшення обрання найбільш зручного у використанні для потреб кінцевого користувача та максимально ефективного використання його можливостей. Важливим завданням є також оцінка рівня безпеки, функціональності та зручності синхронізації між пристроями для кожного з розглянутих інструментів, щоб забезпечити надійний захист даних користувача.

Виклад основного матеріалу дослідження

Порівняльна характеристика популярних менеджерів паролів

1Password

1Password – це безпечний спосіб входу на вебсайти з максимальною безпекою, оскільки не потрібно вводити нові паролі самостійно [9], а також він по-

казує спливаюче вікно щоразу, коли хтось реєструється на новому веб-сайті. Також можна обрати опції збереження пароля. 1Password може зберігати необмежену кількість паролів, навіть для користувачів, що не оформили підписку. 1Password використовує безпечне 256-бітове шифрування AES для зберігання особистої інформації. Усі криптографічні ключі генеруються на пристроях користувача, а усе шифрування виконується локально. В даному менеджері не зберігається нічого що можна зламати. Також передбачена можливість ділитися паролями з родиною та діловими партнерами. Значною перевагою цього менеджера паролів є дуже інтуїтивний та зручний інтерфейс та здатність генерувати надійні та унікальні паролі. Функціонально передбачено, що менеджер не дозволить повторювати пароль. Цей фактор є важливим моментом з точки зору безпеки. 1Password може працювати на будь-яких пристроях, включаючи Linux. Хоча, не дивлячись на наявні переваги він містить ряд недоліків:

– вартість, яка може бути вищою ніж у конкурентів;

– не є менеджером з відкритим вихідним кодом;

– обмеження на кількість користувачів у сімейному плані;

– необхідність підключення до інтернету для роботи окремих функцій;

– обмежена підтримка для деяких платформ;

– для автоматичного заповнення форм на Android може знадобитися змінити клавіатуру за замовчуванням;

– складне налаштування мультифакторної автентифікації;

– даний менеджер не є open source продуктом.

Keeper

Менеджер паролів Keeper [10-11] забезпечує високий рівень безпеки завдяки шифруванню AES-256 і підтримці двофакторної аутентифікації. Він синхронізує паролі між пристроями, дозволяє зберігати файли у зашифрованому сховищі та пропонує моніторинг темної мережі для виявлення можливих загроз. Keeper підходить як для особистого використання, так і для бізнесу, пропонуючи гнучкі рішення для управління паролями. Keeper надає можливість детального налаштування рівнів доступу у організації для критично важливих даних як для окремих осіб так і для команд. В даному менеджері паролів використовується управління доступом на основі ролей (RBAC) для підтримки доступу із найменшими привілеями. Можна відстежувати активності користувачів із будь-якого місця та на кожному пристрої. При втраті одного зі своїх облікових записів у соціальних мережах існує можливість відновлення через історію записів. Це дуже важливо, оскільки дає змогу відновити профіль, особливо після того, як було забуті більшість його деталей. Для цього у Keeper є опція «Перегляд історії записів», яка дає змогу побачити зміни, внесені в зазначені облікові записи аж до декількох років. Отримавши доступ, людина має можливість миттєво захистити свій профіль за допомогою коду від Keeper's Password Generator.

У разі можливих витоків даних Keeper тимчасово приховає особисту інформацію користувача доти, доки проблему не буде вирішено. Також варто зазначити, що Keeper пропонує повний резервний захист сховища і додатково захищає його за допомогою додаткових елементів управління конфіденційністю. Але варто пам'ятати, що й Keepass володіє схожими функціями.

Основні недоліки Keeper:

– деякі доповнення мають щомісячну плату;

– складність налаштування та використання, особливо для новачків;

– обмежена підтримка деяких платформ (менш поширених операційних систем чи браузерів);

– недостатня інтеграція з браузерами;

– додаток Keeper для Android працює повільно і може здаватися занадто згрупованим;

– складнощі з відновленням доступу у випадку, коли користувач забуде свій основний пароль;

– проблеми з безпекою, оскільки незважаючи на загалом високий рівень безпеки, були випадки, коли виникали проблеми з вразливістю або зловмисниками, які намагалися зламати системи.

Enpass

Enpass [12] дозволяє зберігати будь яку інформацію (паролі, логіни, банківські рахунки тощо) за допомогою шаблонів надійно шифруючи усі дані головним паролем. Користувацький інтерфейс служби управління паролями завжди є, був і буде головним пріоритетом. Саме в Enpass він є надзвичайно функціональним. Користувач може отримувати всі свої найбільш відвідувані веб-сайти, перераховані в розділі «Моє вибране».

Бічні панелі безпосередньо включають такі категорії, як паролі, захищені записи, банківські рахунки, кредитні картки та ліцензії. Це простий спосіб знайти потрібну інформацію саме тоді, коли вона потрібна. Також в даному менеджері паролів передбачена можливість одноразової покупки, що дозволяє уникнути підписок та щомісячних платежів. Це може бути економічно вигідно в довгостроковій перспективі. Крім того пропонується безкоштовна версія з обмеженим функціоналом, що дозволяє користувачам спробувати програму перед покупкою. Enpass підтримує різні платформи, включаючи Windows, macOS, Linux, Android та iOS, що забезпечує зручність використання на різних пристроях.

В даному менеджері паролів модель безпеки з нульовим розголошенням. Як підказує досвід роботи зі старими і новими менеджерами паролів, ті, які включали цю конкретну архітектуру, були найнадійнішими.

Модель безпеки з нульовим розголошенням означає, що диспетчер паролів не може отримати доступ до паролів користувача, елементів сховища і найголовнішого пароля. Шифрування забезпечується за допомогою 256-бітного AES [13].

В Enpass присутній ряд недоліків:

– багато функцій доволі важко налаштувати та використовувати;

– оскільки Enpass є офлайн-менеджером паролів, користувачам потрібно синхронізуватись через Wi-Fi або підписатися на сторонню хмарну службу, щоб мати можливість створювати резервні копії та синхронізувати паролі на різних пристроях [14];

– неможливість відновлення майстер-пароля;

– Enpass не має веб-інтерфейсу для доступу до паролів, що може бути незручним для користувачів, які звикли до цього формату;

– обмежена документація, що ускладнює процес налаштування та використання програми;

– імпорт паролів з інших менеджерів паролів може бути не таким простим, як у конкурентів, і може вимагати додаткових налаштувань;

– дорогі підписки.

KeePass

KeePass — це [15-19] безкоштовний менеджер паролів із відкритим вихідним кодом, який дозволяє безпечно керувати своїми паролями. Паролі можна зберігати в одній базі даних, яка закривається головним ключем. Файли бази даних зашифровано за допомогою найкращих і найбезпечніших алгоритмів шифрування, відомих на даний момент (AES-256, ChaCha20 і Twofish) [20-21].

Основні переваги KeePass:

– в порівнянні з іншими менеджерами паролів є безкомпромісна безпека. Той факт, що KeePass не використовує стороннє хмарне сховище для делікатного контенту – значно підвищує захищеність;.

– усі інструменти безпеки абсолютно безкоштовні;

– безкоштовна версія для мобільних пристроїв;

– ідеально підходить для будь-якої операційної системи;

– зберігає дані на власному комп'ютері користувача;

– простий користувацький інтерфейс із можливістю перетягування.

Основні недоліки KeePass:

– важко освоїти та незручно користуватися;

– функція автозаповнення не включена;

– необхідність ручного керування базою даних паролів, що може бути не зручним для користувачів з великою кількістю облікових записів;

– Auto-Type трохи недосконалий;

– параметри багатофакторної автентифікації завантажуються окремо;

– дизайн виглядає трохи застарілим;

– обмежена сумісність з мобільними платформами, що може ускладнювати доступ до паролів на різних пристроях.

Захист даних та управлінням паролями за допомогою KeePass: аналіз та огляд

Для доступу до бази даних всіх паролів, що зберігаються у зашифрованому вигляді потрібен лише один основний пароль або інший метод аутентифікації, такий як ключ файлу. Крім того, KeePass має ряд додаткових функцій, таких як генератор паролів та можливість використання ключів USB для автоматичного входу. Аналіз досліджень у галузі безпечного управління паролями свідчить про широке використання KeePass [22-24] у спільноті інтернет-користувачів. Велика кількість досліджень демонструє високу оцінку безпеки та ефективності цієї програми.

Ще одним аспектом, який варто враховувати, є те, що KeePass – це open-source проект, тобто він розробляється і підтримується громадськістю. Це означає, що програма постійно оновлюється та вдосконалюється за допомогою внесків від різних розробників, але також це може призвести до виникнення певних проблем з безпекою та стабільністю програми.

Завдяки підтримці великої кількості плагінів та додаткових модулів, KeePass може бути інтегрований у різні системи та розширювати свою функціональність відповідно до потреб користувача. Це дозволяє легко додавати такі функції, як резервне копіювання бази даних та використання апаратних токенів для підвищення рівня безпеки тощо. Попри це, KeePass вимагає певного рівня технічних знань для налаштування і оптимального використання, що може стати викликом для новачків. Тим не менш, його гнучкість та висока надійність роблять його популярним рішенням серед досвідчених користувачів та професіоналів у галузі кібербезпеки. Основні характеристики KeePass в порівнянні з іншими менеджерами паролів:

– Надійність: Це безкоштовний, відкритий менеджер паролів, який не зберігає дані на своїх серверах, що забезпечує повний контроль над даними користувача. Завдяки можливості локального зберігання паролів, KeePass є дуже надійним.

– Захищеність: Keepass використовує AES-256 шифрування, що є стандартом безпеки. Крім того, можна використовувати плагіни для двофакторної автентифікації, що підвищує рівень захисту.

– Комфорт: Хоча KeePass має багато функцій, його інтерфейс може бути складним для нових користувачів, що знижує рівень комфорту.

Усі ці фактори слід враховувати при виборі програмного забезпечення для управління паролями. За умови правильного використання та збереження основного пароля, KeePass може бути потужним інструментом для захисту особистих даних у цифровому світі.

Як видно з даної порівняльної таблиці KeePass володіє певними перевагами стосовно інших менеджерів паролів.

Варто зазначити, що KeePass є найбільш доцільним для використання в середовищах, де потрібен високий рівень контролю над даними, оскільки він не зберігає паролі у хмарі та дозволяє користувачам повністю керувати базою даних локально. Це робить його ідеальним для організацій, де пріоритетом є максимальна конфіденційність та захист від потенційних загроз, пов'язаних з онлайн-сервісами.

Таблиця 1

Порівняльна таблиця основних менеджерів паролів

Ознака	KeePass	1Password	Keeper	Enpass
Ліцензія	Відкритий код (Open Source)	Пропрієтарна (Платна)	Пропрієтарна (Платна)	Пропрієтарна (Платна)
Вартість	Безкоштовний	Підписка	Підписка	Одноразова оплата або підписка
Зберігання даних	Локальне зберігання	Хмарне зберігання	Хмарне зберігання	Локальне або хмарне зберігання
Синхронізація між пристроями	Мануальна (через сторонні сервіси)	Автоматична	Автоматична	Автоматична
Відкритий код	Так	Ні	Ні	Ні
Мультиплатформенність	Windows, macOS, Linux, Android, iOS	Windows, macOS, Linux, Android, iOS	Windows, macOS, Linux, Android, iOS	Windows, macOS, Linux, Android, iOS
Безпека	Висока (через локальне зберігання, шифрування AES-256)	Висока (AES-256, Zero-knowledge)	Висока (AES-256, Zero-knowledge)	Висока (AES-256)
Автоматичне заповнення	Обмежено через плагіни	Повне	Повне	Повне
Двохфакторна автентифікація	Ні	Так	Так	Так
Масштабованість для команд	Обмежено	Так	Так	Так
Резервне копіювання	Мануальне (локальне)	Автоматичне (хмарне)	Автоматичне (хмарне)	Автоматичне або мануальне

Крім того, KeePass є хорошим варіантом для технічно підкованих користувачів, які цінують можливість кастомізації через плагіни та розширення функціональності, роблячи його ще більш універсальним рішенням. Завдяки відкритому коду, даний менеджер паролів можуть використовувати дослідники та професіонали з кібербезпеки для створення спеціалізованих рішень під конкретні потреби.

Перспективи розвитку KeePass залежать від активності спільноти розробників, яка може продовжувати вдосконалювати безпеку та функціональність продукту через регулярні оновлення. У міру збільшення уваги до захисту даних у різних галузях, KeePass має всі шанси залишатися важливим інструментом для тих, хто прагне максимального контролю та безпеки своїх паролів та захисту даних.

Висновки. Отже, підсумовуючи, варто зазначити, що в умовах стрімкого розвитку цифрових технологій менеджери паролів відіграють критичну роль у забезпеченні надійного захисту інформації та конфіденційних даних. KeePass, попри деякі технічні обмеження, є прикладом того, як невеликі групи розробників можуть створювати ефективні та безпечні рішення, що відповідають найвищим стандартам кібербезпеки. Його можливості локального зберігання та надійного шифрування роблять його привабливим вибором для користувачів, які прагнуть повного контролю над своїми даними без ризику компрометації через хмарні сервіси. Завдяки своїй гнучкості та підтримці великої кількості плагінів, KeePass також забезпечує ефективне управління паролями для широкого спектра онлайн-акаунтів, що особливо важливо в сучасному світі зростаючих кіберзагроз. Однак, використання KeePass або будь-якого іншого інструменту управління паролями повинно бути частиною комплексного підходу до кібербезпеки. Це включає дотримання найкращих практик щодо створення складних паролів, своєчасного оновлення програмного забезпечення та захисту пристроїв від шкідливих програм.

Таким чином, впровадження KeePass у повсякденне використання може стати важливою складовою стратегії захисту персональних даних у сучасному інформаційному середовищі.

Список літератури

[1]. P. Pandare, S. Uniyal, R. Vani, S. Mali and P. Rumao, "Enhanced Password Manager using Hybrid Approach," 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 1793-1798, doi: 10.1109/ICICT57646.2023.10134398.

[2]. E. Halim, T. Dwiangraini, D. Wiryawan and M. Hebrard, "Implementation of Password Manager to Improve Data Security for Social Media Account," 2023 International Conference on Information Management and Technology (ICIMTech), Malang, Indonesia, 2023, pp. 754-759, doi: 10.1109/ICIMTech59029.2023.10277793.

[3]. R. Dhanalakshmi, N. Vijayaraghavan, S. Narasimhan and S. Basha, "Password Manager with Multi-Factor Authentication," 2023 International Conference on Networking and Communications (ICNWC), Chennai, India, 2023, pp. 1-5, doi: 10.1109/ICNWC57852.2023.10127424.

[4]. Марія Хомік, Олег Гарасимчук. Застосування генераторів псевдовипадкових чисел та послідовностей в кібербезпеці, методи їх побудови та оцінки якості // Захист інформації. 2023. Т. 25, № 3. С. 147-159.

[5]. Хомік М. А., Гарасимчук О. І. Аналіз загроз для генераторів псевдовипадкових чисел і псевдовипадкових послідовностей та заходи захисту // Захист інформації. 2024. Т. 25, № 4. С. 172-184.

[6]. Password Security: How to Keep Your Accounts Safe. [Електронний ресурс]: https://lifelock.norton.com / learn/internet-security-password-security.

[7]. Managing Your Passwords: A Comprehensive Guide. [Електронний ресурс]: https: // medium.com / @CyberGain/mastering-password-management-a-comprehensive-guide-b59b9ec0ef96.

[8]. Password Management: A Practical Guide. [Електронний ресурс]: https: // www.dashlane.com/ blog/password-security-best-practices.

[9]. 1Password Security Design [Електронний ресурс]: https: // 1passwordstatic.com / files / security / 1password-white-paper.pdf.

[10]. M. O. Sandonís, "Keeper: A tool for management and automated deployment of CMS web services," 2013 IEEE Nuclear Science Symposium and Medical Imaging Conference (2013 NSS/MIC), Seoul, Korea (South), 2013, pp. 1-5, doi: 10.1109/NSSMIC.2013.6829559.

[11]. Keeper: Password Manager Manual [Електронний ресурс]: https://www.acg-solutions.com/pdf/keeper-documentation.pdf.

[12]. Enpass Technologies careers [Електронний ресурс]: https://wellfound.com/company/sinew-software-systems.

[13]. Daemen, J., & Rijmen, V. (2002). "The Design of Rijndael: AES - The Advanced Encryption Standard." Springer Science & Business Media.

[14]. Enpass Review 2024: Is It a Good Password Manager? [Електронний ресурс]: https://www.safety-detectives.com/best-password-managers/enpass/.

[15]. Hengwei Zhang, Jingxin Hong and Jun Hu, "Analysis of encryption mechanism in KeePass Password Safe 2.30," 2016 10th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), Xiamen, 2016, pp. 43-46, doi: 10.1109 / ICASID.2016.787-3914.

[16]. Bonneau, J., et al. (2015). "The Security of KeePass." IEEE Security & Privacy, 13(4), pp. 65-69.

[17]. KeePass Password Safe. [Електронний ресурс]: https://keepass.info/.

[18]. Password Manager KeePass 2.55 warns users about weak security settings. [Електронний ресурс]: https://www.ghacks.net/2023/10/13/password-manager-keepass-2-55-warns-users-about-weak-security-settings/.

[19]. Software Requirements Specification for KeePass Password Safe [Електронний ресурс]: https://keepass. info / extensions / v1/docs/SoftwareRequirements-Specification-KeePass-1.10.pdf.

[20]. Schneier, B. (1999). "The Twofish Encryption Algorithm." [Електронний ресурс]: https://www.schneier.com/books/twofish/.

[21]. Bernstein, D. J. (2008). "ChaCha, a variant of Salsa20." [Електронний ресурс]: https://cr.yp.to/chacha /chacha-20080128.pdf.

[22]. KeePass Discussion [Електронний ресурс]: https://sourceforge.net/p/keepass/discussion/.

[23]. Як легко користуватися KeePass. [Електронний ресурс]: https: // tucha.ua /uk/blog/instructions/ yak-lehko-korystuvatysya-keepass.

[24]. F. Yu and H. Yin, "A Security Analysis of the Authentication Mechanism of Password Managers," 2021 IEEE 21st International Conference on Communication Technology (ICCT), Tianjin, China, 2021, pp. 865-869, doi: 10.1109/ICCT52962.2021.9657969.

УДК 004.056

Harasymchuk O., Chentsov O. Keepass as a password and data security manager

Abstract. *Data protection is a critical aspect of today's information environment, as the number of threats, both from attackers and as a result of human error, is constantly increasing, putting the confidentiality and integrity of information at risk. Basic data protection principles include access control, encryption, backup and activity monitoring. A multi-level approach to security, including physical, administrative and technical measures, reduces the risks of unauthorized access and data loss. The article examines the importance of password security in today's digital environment. Given the growing number of cyber threats, maintaining privacy and protecting personal data has become a priority. One of the effective password management tools is KeePass, a password storage program that provides a high level of encryption and security. This paper analyzes the key features of KeePass, its advantages and disadvantages compared to other password managers. The article also draws attention to the need to choose a reliable password manager to ensure multi-level protection of user data. The use of such tools becomes especially relevant in the context of the growing number of cyber-attacks and the need to preserve confidentiality in various industries, including business and government institutions.*

Keywords*: Data protection, Encryption, access control, 1Password, Keeper, Enpass, KeePass.*

Гарасимчук Олег Ігорович, к.т.н., доцент, доцент кафедри захисту інформації Національного університету «Львівська політехніка».
Oleh Harasymchuk, Ph.D., Associate Professor at the Department of Information Security, National University "Lviv Polytechnic".

Ченцов Олег Олександрович, студент спеціальності «Кібербезпека та захист інформації» Національного університету «Львівська політехніка».
Oleh Chentsov, student of the "Cybersecurity" specialty of the National University "Lviv Polytechnic".

Отримано *14 червня 2024 року*, затверджено редколегією *26 червня 2024 року*