DOI 10.15276/imms.v12.no1-2.15
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 1-2, pp. 15-22

РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗБЕРІГАННЯ ТА ЗАХИСТУ ДАНИХ ДЛЯ ПРИВАТНОГО ТА КОРПОРАТИВНОГО ЗАСТОСУВАННЯ

Б.В.Гаврилюк, В.В. Зоріло, Н.І.Кушніренко, О.Р.Осколкова

1, пр.Шевченка, Національний університет «Одеська політехніка», 65044, Одеса
vikazorilo@gmail.com, whiteswanhelena@gmail.com

Кажуть, що найкращий менеджер паролів – це наш мозок. У цьому твердженні є сенс, але іноді наш мозок не справляється, доводиться задіяти зовнішні ресурси. Кількість паролів на одного користувача зростає з кожним роком: нові соціальні мережі, нові банківські рахунки, нові реєстрації в різних сервісах, акаунти на різних сервісах (телевізійних, музичних, послуги інтернет-провайдерів тощо). За правилами інформаційної безпеки користуватись одним паролем для різних клієнтських сервісів не є раціональним, тому що якщо зловмисники зможуть, наприклад, підібрати пароль до вашої електронної пошти, вони спробують застосувати його і до інших ваших застосунків на кшталт інтернет-банкінг та інше. Сучасна людина розуміє, що для кожного сервісу потрібен свій унікальний пароль. Пароль має бути надійним, містити певну кількість символів, де серед цифр та літер надійність пароля підвищують спеціальні символи та зміни регістрів. Запам'ятати все це важко. Але запам'ятати один пароль – цілком під силу більшості з нас. Вибрати зручний та надійний менеджер паролів – непросте завдання. Ви маєте дійсно довіряти сервісу. Зрештою, саме він зберігатиме ваші секретні дані. В роботі протестовано два десятки менеджерів паролів і вибрано одинадцять, які є найкращими з погляду функціональності, безпеки та зручності. Проте кожен з відомих менеджерів не враховує індивідуальні особливості користувачів і потребує доповнень згідно їх потреб. Тому створення програмного забезпечення для зберігання паролів у зашифрованому вигляді є актуальним. Доступ до зашифрованих паролів може відбуватися через той один пароль, який необхідно запам'ятати. Такі програмні за стосунки було створено у даній роботі з урахуванням потреб корпоративного та приватного користування.

Ключові слова: захист даних, парольний менеджер, шифрування, криптографія.

Вступ

Причинами цього дослідження стала проблема зі зберіганням великої кількості паролів. Безліч паролів було безповоротно втрачено і доводилося створювати нові і знову втрачати. Тому постало питання зберігання всіх паролів, бажано в одному надійному місці.

Для позбавлення цієї проблеми було вирішено використовувати існуючі рішення – «менеджери паролів» або у разі, якщо існуючі рішення не підійдуть, створення свого програмного продукту.

Навіть найкращий у світі менеджер паролів буде марним, якщо він не відповідає конкретним потребам або просто занадто складний у використанні. Ось чому не слід поспішати і завантажувати менеджер паролів №1, представлений у будь-якому топ-листі – проведемо дослідження існуючих рішень.

Потрібно бути впевненим, що рішення має достатній функціонал і необхідну кількість одночасних підключень. Крім того він має мати зручний інтерфейс.

Більшість менеджерів паролів пропонують однаковий набір функцій: синхронізація, генерація паролів та двофакторна автентифікація. Для вибірки використовувалися такі критерії. Шифрування: все, що менше 256-бітного шифру AES військового рівня, є неприпустимим. Додаткові можливості: сканування даркнета, U2FA, VPN або безпечний чат – ось лише деякі з прикладів, які надають додаткову цінність продукту. Багатофакторна автентифікація: на додаток до власного

автентифікатора хороший менеджер паролів повинен пропонувати кілька інших. Біометричні дані (Touch ID та Face ID) також повинні працювати на всіх пристроях. Імпорт та експорт: від менеджера паролів не так багато користі, як від неможливості імпортувати ваше сховище з іншої служби чи браузера. Експорт також важливий у випадку, якщо ви вирішите змінити менеджер паролів. Програми та розширення для браузерів: чим більше тим краще. Співвідношення ціна-якість. Служба підтримки клієнтів: онлайн-чат або підтримка по телефону – ознака якісного обслуговування. Те саме стосується доступності 24/7.

Огляд сучасних рішень

На сьогоднішній день існує безліч програм, які мають певну систему авторизації. Важливою метою є зберігання та забезпечення захисту тих даних, що стосуються авторизації певної людини чи підприємства.

До основної мети забезпечення та зберігання даних відноситься наявність усіх доступів до систем, які має певна людина чи організація. Важливо зберігати усю інформацію щодо авторизації до різних систем. Адже втрата конфіденційної інформації конкретного користувача або підприємства може призвести до дуже тяжких та іноді до незворотних наслідків. Для вирішення даного питання використовують спеціально призначені системи для збереження парольної інформації користувача або цілого підприємства. Так як існує багато систем, які спрямовані на вирішення даного питання, перед користувачем або організацією постає вибір: яку саме систему варто обрати. Для того, щоб обрати одну з систем, необхідно провести аналіз та огляд сучасних систем, що спрямовані на вирішення даного питання. Існують наступні програми, які надають можливість користувачам зберігати свої парольні дані:

1) LastPass
2) Dashlane
3) 1Password
4) Bitwarden
5) Keeper
6) NordPass
7) Enpass
8) RoboForm
9) RememBear
10) Zoho Vault
11) Passbolt

LastPass – надійний менеджер паролів. Він є однією з найдешевших систем у використанні (3 долари на місяць).

Цей менеджер паролів використовує багатофакторну автентифікацію (MFA), яка може змінюватись від «вашого пристрою» (смартфон) до біометричних даних (відбиток пальця). Можливе використання не тільки власного автентифікатора, але й автентифікатора від YubiKey, Sesame, Google або Microsoft.

Цей менеджер паролів можна встановити на всіх основних платформах і в багатьох браузерах. LastPass має розширення для Chrome, Firefox, Safari, Opera, Edge та Edge Legacy. Але в той же час він не підтримує Vivaldi або Brave. У цій системі присутні функції автозаповнення та автозбереження.

Користуватися даною системою можна і безкоштовно, але в такому випадку користувач не матиме можливості використовувати весь функціонал системи. Без платної підписки користувачеві не доступні такі функції як: оперативне спілкування з техпідтримкою, функція аварійного доступу (коли користувач може надати довіреній особі своє сховище з паролями), обмін паролем через мережу з іншими користувачами, не доступна опція багатофакторної автентифікації для захисту парольних даних. При цьому для звичайного користувача захист даних здійснюється 256-бітовим шифруванням.

Dashlane підтримує три методи аутентифікації, перший з яких – двофакторна аутентифікація (2FA). Це чудовий спосіб захистити обліковий запис, навіть якщо хтось отримає ваш майстер-ключ. Другим фактором може бути інформація, яку знаєте тільки ви (PIN-код), або ваш смартфон або біометрична інформація (наприклад, Face ID).

Преміум-план доступний за ціною $4,99 і пропонує універсальну двофакторну автентифікацію (U2FA). Це безпечніша версія 2FA, в якій пристрій USB або NFC можна підключити до будь-якого комп'ютера для миттєвого доступу до ваших паролів. У той же час U2FA простіша у використанні, пристрій обмінюється даними з комп'ютером за протоколом HID.

Також є біометричний логін, який можна використовувати замість майстер-паролю. Dashlane підтримує як Touch ID, так і Face ID, тому все залежить від пристрою користувача.

Цей менеджер паролів простий у встановленні та використанні, працює на всіх основних платформах і має розширення для браузерів Chrome, Firefox, Safari, Internet Explorer та Edge. Можна імпортувати паролі з більшості браузерів, за винятком мобільних.

Наступним у списку можливостей Dashlane йде сканер даркнета. За бажанням користувача система може використовувати електронну пошту, щоб перевірити, чи немає витоків паролів чи банківських реквізитів. Враховуючи, що кожен день з'являються мільйони нових записів, сканер даркнета може стати чудовим інструментом для запобігання крадіжці особистих даних. Також є вбудований VPN.

1Password – потужний інструмент для зберігання, створення та керування паролями користувача або організації.

Для роботи потрібен майстер-пароль, проте замість цього можна використовувати біометричний логін, як використовується відбиток пальця або обличчя. Інший варіант 2FA – використовувати телефон користувача для створення одноразового пароля.

Крім всіх основних платформ, 1Password підтримує Chrome OS та командний рядок. Що стосується розширень браузера, можливо обрати Chrome, Firefox, Edge та Brave.

Цей менеджер паролів має автозаповнення та синхронізує дані користувача на всіх пристроях. Це також спрощує обмін паролями рахунок створення гостьових облікових записів. 1Password не має обмежень на кількість людей, які можуть користуватися вашим обліковим записом, що робить його доступним для використання у рамках підприємства.

У 1Password має функцію під назвою: «Сторожова вежа». Це веб-сканер, однак він також перевіряє, чи підтримує веб-сайт 2FA і чи використовує HTTPS. А також має функцію «Режим подорожі». Вона потрібна для приховування конфіденційної інформації на телефоні. Якщо користувач втрате телефон або хтось викраде його, можливо можете бути впевненим, що вся особиста інформація в безпеці.

Перейти до 1Password дуже просто, адже у системі можливо імпортувати дані з Chrome, звичайного CSV та інших популярних менеджерів паролів, включаючи LastPass та Dashlane.

Увесь функціонал системи доступний для використання з платною підпискою: 2,99 долара на місяць для одного користувача та є тарифний план на 5 користувачів, який коштує 4,99 долара на місяць.

Програма Bitwarden допомагає зберігати та обмінюватися конфіденційними даними з будь-якого пристрою. Програмою користуються по всьому світу, тому що вона працює 40 мовами. У сервісі можна створювати унікальні паролі, а постійний аудит безпеки робить Bitwarden надійним менеджером для зберігання паролів.

Keeper надає персональне сховище кожному користувачу для того, щоб зберігати та управляти власними паролями, файлами, обліковими даними тощо. Дане сховище представлене у зашифрованому вигляді.

Keeper — надійний та безпечний менеджер паролів, який використовує підхід із нульовою довірою. Це означає, що дані користувача зашифровані не на сервері, а на пристрої, і тільки ви можете їх розшифрувати.

Усі менеджери паролів мають двофакторну автентифікацію, а в Keeper їх безліч. Можливо використовувати SMS, автентифікатор Google та Microsoft (TOTP), RSA SecurID, Duo Security, U2F (YubiKey) та KeeperDNA. Останній є запатентованим варіантом 2FA, який дозволяє біометричну автентифікацію за допомогою смартфона або розумного годинника.

У Keeper є програми для Windows, macOS, Linux, Android та iOS. Щодо розширень браузера, вони використовуються лише для автоматичного заповнення облікових даних. Звичайно, це покращує сумісність - так званий KeeperFill працює з Chrome, Firefox, Opera, Edge та IE.

Цей менеджер паролів є багатофункціональним. Деякі функції недоступні в жодному іншому менеджері паролів. Наприклад, KeeperChat – безпечна система обміну повідомленнями із самознищуючими повідомленнями та медіа-галереєю для приватних фотосесій та музичних кліпів. Або Security Audit, який перевіряє всі паролі користувача, оцінює їхню надійність і пропонує змінити слабкі. Також є сканер даркнета під назвою Breach Watch, який перевіряє, чи не були викрадені імена користувачів чи паролі.

Keeper підтримує імпорт даних з Dashlane, 1Password, ZOHO та інших менеджерів паролів. Що стосується браузерів, можна імпортувати їх з Chrome, Firefox, Opera, Edge і навіть з Internet Explorer. Доступний експорт до PDF, CSV або JSON.

Безкоштовної версії немає. Середня ціна Keeper складає 2,91 долара США на місяць за річної оплати. Проте KeepChat та моніторинг Dark Web вимагають додаткових витрат. Крім того, існують особисті, сімейні, студентські, ділові та корпоративні плани, тому остаточна ціна залежить від цілі використання системи.

Основні функції та параметри додатку. Keeper надає персональне сховище кожному користувачу для того, щоб зберігати та управляти власними паролями, файлами, обліковими даними тощо. Дане сховище представлене у зашифрованому вигляді. Існує можливість автоматичного заповнення паролів. Кількість даних, які можна зберігати у додатку, не обмежуються. Він надає функції консолі адміністратора, контроль версій, рольовий доступ та історію записів та звітування.

Програма спрямована на те, щоб зберігати паролі та особисту інформацію. Keeper працює на будь-якому мобільному пристрої та ПК, де можливе створення власного зашифрованого сховища. Сервіс швидко вигадує нові та надійні паролі та одночасно застосовує їх до підключених облікових записів у додатках та на веб-сайтах. Крім паролів, у менеджері зберігають паспортні дані, посвідчення водія, важливі фотографії, документи та інші типи файлів.

Диспетчер паролів NordPass є частиною пакету онлайн безпеки, який включає шифратор NordLocker і NordVPN.

NordPass використовує майстер-пароль для захисту сховища користувача та синхронізує всі дані між пристроями. Також можна використовувати Touch ID або Face ID (тільки для iOS). Для двофакторної автентифікації знадобиться додаток для автентифікації та електронний лист, на який буде надіслано шестизначний код.

Цей менеджер паролів може працювати на Windows, MacOS, Linux, Android та iOS. Також можливо встановити розширення NordPass у Chrome, Firefox, Safari, Opera, Brave, Vivaldi та Edge.

NordPass враховує всі особливості та потреби користувача. Можливо генерувати паролі та оцінювати їхню надійність, використовувати автозаповнення та автозбереження, а також ділитися обліковими даними для входу.

NordPass має деякі унікальні особливості. Користувачеві надається можливість впорядкувати дані в папках для полегшення доступу та використовувати OCR для автоматичного сканування текстової інформації з кредитних карток, документів та фотографій. Крім того, автономний режим дозволить користувачу отримати доступ до свого сховища, навіть якщо немає підключення до Інтернету.

NordPass також пропонує безліч можливостей для імпорту паролів. Сюди входять найпопулярніші менеджери паролів, крім Zoho Vault, та найпопулярніші браузери, крім Safari. Проте, користувачеві доведеться вручну перевіряти, чи експортований файл відповідає критеріям NordPass.

NordPass пропонує шифрування XChaCha20 наступного покоління з використанням Argon 2 для отримання ключів.

NordPass має відмінну службу підтримки, яка включає цілодобовий чат, електронну пошту і базу знань, що постійно зростає.

Безкоштовна версія потужна, але дозволяє використовувати лише один активний пристрій та не передбачає можливість безпечного обміну та довірених контактів. Коштує 2,49 доларів США на місяць (при покупці на 2 роки).

Enpass – це мінімалістичний менеджер паролів. Він є крос-платформний, але насамперед призначений для автономного використання. Користувач може налаштувати параметри синхронізації між різними пристроями за допомогою сторонніх платформ хмарного хостингу, таких як OneDrive, Dropbox, iCloud і т.д.

Enpass захищає ідентифікаційні дані користувача, інформацію про кредитну картку та багато іншого. Для захисту паролів використовується інструмент моніторингу. Він допомагає оцінити надійність паролів і змінити їх у разі повторного використання пароля. Також є генератор паролів find-secure.

Шифрування даних виконується за допомогою шифру AES-256 з розширенням SQLCIPHER.

Програма безкоштовна, якщо використовуватимете тільки настільну версію. Якщо потрібно перемикатися між настільними та мобільними обліковими записами, користувачу необхідна сплатити ліцензію.

RoboForm - один із найстаріших менеджерів паролів. Він існував ще до того, як менеджери паролів стали важливими продуктами безпеки. Цільова аудиторія - бізнес. Розробники пропонують самостійний хостинг для безкоштовних користувачів, але якщо обрати преміум-план, користувач зможе використати їхню безшовну синхронізацію. Це означає, що користувач, що придбав преміум-план може отримати доступ до всіх паролів на всіх своїх пристроях.

RoboForm має кілька функцій, які можуть бути корисними. Він має стандартний генератор паролів із змінними, які можна змінити.

Також можливо поділитись своїми обліковими даними з іншими користувачами RoboForm. Є також класичні менеджери паролів, такі як безпечне хмарне сховище та спільні папки.

Всі дані, які користувач завантажує, захищені шифруванням AES-256.

Ціна на преміум-опцію починається з 1,66 долара на місяць під час оплати кожні п'ять років.

RememBear – це менеджер паролів, який зберігає, синхронізує та генерує паролі. Також можливо зберігати нотатки, кредитні картки та логіни, які пізніше можна використовувати для автозаповнення. Як і всі інші програми, RememBear підтримує двофакторну автентифікацію та біометрію (відбиток пальця та обличчя).

Даний сервіс має програми для Windows, macOS, Android та iOS. Існують також розширення для браузерів Chrome, Firefox та Safari, але вони не є автономними.

RememBear також може імпортувати із Chrome, з 1Password та LastPass.

Безкоштовна версія демонструє лише частину функцій RememBear. З безкоштовною версією не можливо створити резервну копію своїх паролів, тобто доведеться зберігати другу копію в іншому місці. Крім того, синхронізація між пристроями не дозволена. У тому числі безкоштовна версія не має пріоритетної підтримки, тому отримання відповіді може забрати деякий час.

RememBear коштує від 2,5 доларів на місяць.

Більшість найкращих менеджерів паролів орієнтовані на споживача. Навіть якщо вони мають бізнес-рішення, сегмент B2C збільшує їх дохід. Це не стосується Zoho Vault, яке знаходиться десь між споживачем та бізнесом. Компанія позиціонує Vault як менеджер паролів для команд.

Zoho Vault не має класичного інсталятора, замість цього використовується веб-додаток. Але є клієнти для Android та iOS. Що ж до розширень для браузера, то вибір досить широкий. Можливо обрати з Chrome, Firefox, Safari, Edge, Brave та Vivaldi.

Деякі менеджери паролів є частиною пакету онлайн-безпеки, який включає VPN або інструмент для шифрування файлів. Zoho має величезний список додатків, які інтегруються з Vault, що є лише одним з безлічі доступних сервісів. Крім того, цей менеджер паролів пропонує єдиний вхід для Office 365, Windows AD, Dropbox та ZenDesk.

Цей менеджер паролів підтримує понад 400 сайтів. Zoho Vault має складну систему обміну паролями, яка надає користувачу багаторівневі фільтри, доступ з обмеженням часу і підтвердження або відгук одним клацанням миші.

Можливо імпортувати в Zoho Vault з більш ніж 20 додатків та браузерів, включаючи Dashlane, LastPass, 1Password та Keeper. Проте, імпорт із Safari або Edge недоступний. Експорт доступний або у простому .csv, або у форматі, що відповідає формату Zoho Vault.

Сервіс використовує шифрування військового рівня та архітектуру з нульовим рівнем довіри. Майстер-пароль користувача захищений алгоритмом PBKDF2, який надає йому більшої надійності.

Zoho Vault пропонує підтримку через email, через форму зворотного зв'язку або по телефону.

Дана система має застарілий інтерфейс веб-застосунку, що може перешкоджати якісному та швидкому користування системою.

Вартість ліцензії сягає 3,6 доларів на місяць, з цим можна отримати можливість використовувати п'ять пристроїв для кожного облікового запису на додаток до спільних папок та звітів про доступ за паролем.

Passbolt — один із небагатьох менеджерів паролів із відкритим вихідним кодом. Він призначений для підприємств та промислових підприємств.

Passbolt вимагає використання майстер-паролю у поєднанні із закритим ключем.

Основним недоліком є залежність від закритого ключа чи ключової фрази. Якщо користувач втрачає будь-кого з них, сховище стане недоступним. Незважаючи на те, що це найбезпечніший метод налаштування, йому не вистачає зручності для користувача. Крім того, для зміни ключової фрази, знадобиться базове розуміння роботи з кодом.

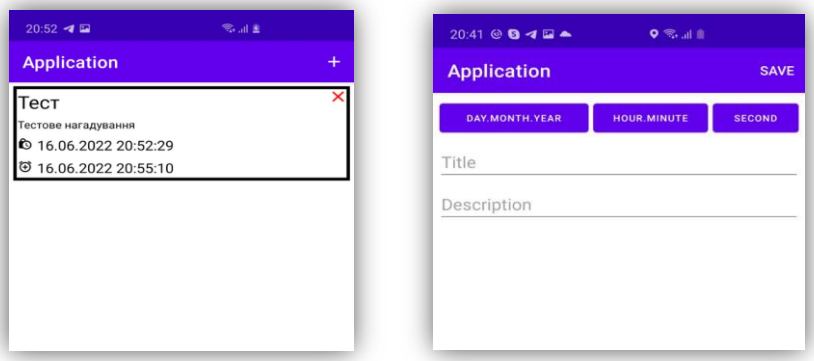
Сервери Passbolt не мають доступу до даних у вигляді відкритого тексту. Паролі завантажуються у хмару лише у зашифрованому вигляді.

Passbolt може бути абсолютно безкоштовним способом керування паролями, хоча це не найзручніший менеджер паролів для не надто технічно підкованих користувачів.

У ході огляду та аналізу існуючих аналогів, які є одними з найкращих рішень на сьогоднішній момент, немає жодного лідера, що не мав би певних недоліків.

Розробка

Для покращення даних аналогів була реалізована розробка нового застосунку, який спрямований на вирішення задач підприємства. Однією з головних задач для даного програмного застосунку є авторизація певного користувача в системі, зберігання та керування парольною інформацією. Для даного застосунку був вирішений недолік, що характерний для кожної з систем, а саме: це можливість користуватися повним функціоналом системи без придбання платної ліцензії. У якості удосконалення застосунку була запроваджена та реалізована система нагадувань, що дозволяє користувачеві створювати власні робочі нагадування. Під час огляду сучасних рішень проблеми, було виявлено, що в жодної з системи немає даного функціоналу, який дозволяв би користувачу створювати власні нагадування та визначати їх час надходження у вигляді сповіщення. Даний функціонал є дуже важливим аспектом для роботи підприємства, адже він забезпечує виконання робочих процесів вчасно, що допомагає підприємству будувати якісну онлайн-інфраструктуру бізнесу.
Інтерфейс програми показано на рисунку 1.



а) системи нагадування б) створення запису

Рис.1. Інтерфейс

Відпрацювання нагадування у вигляді push-сповіщення показано на рис. 2.

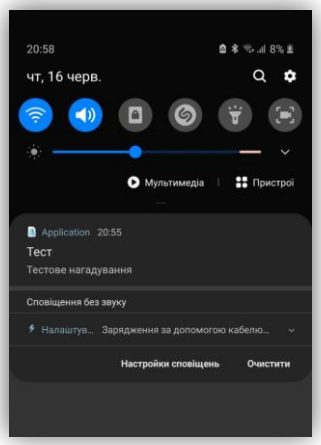


Рис. 2. Відпрацювання нагадування

Переваги розробленого застосунку у порівнянні з існуючими аналогами полягають у наявності системи корпоративних нагадувань. Застосунок має зручний та зрозумілий для користувача інтерфейс. Можливе автономне використання функціоналу нагадувань; додаток є безкоштовним та не потребує придбання ліцензії.

Висновки

У статті виконано фундаментальний огляд найкращих існуючих менеджерів паролів на думку авторів. Кожен з 11 менеджерів паролів унікальний і вибір того, який краще використовувати залежить тільки від користувача: його потреб і фінансових можливостей. Також з даного огляду можна побачити, що в кожній системі є власні переваги та недоліки. Розробка індивідуальних менеджерів згідно з цим є актуальною задачею. Згідно з цим була проведена розробка нового програмного застосунку, який удосконалює існуючі системи та задовольняє саме ті потреби організації, що не наявні у повному складі в жодній із наведених систем.

Список літератури

1. Dashlane URL: https://www.dashlane.com
2. NordPass URL: https://nordpass.com/?gclid=CjwKCAjwh-CVBhB8EiwAjFEPGe6X3Ez9NDz7tjHQspDReZASWuyQRWECogirTWCpGYhulGZxsWC2WxoCkOsQAvD_BwE
3. 1Password URL: https://1password.com/ru/
4. Keeper URL: https://www.keepersecurity.com/ru_RU/
5. Enpass URL: https://www.enpass.io
6. RoboForm URL: https://www.roboform.com/ru
7. LastPass URL: https://www.lastpass.com
8. RememBear URL: https://www.remembear.com
9. Zoho Vault URL: https://www.zoho.com/vault/
10. Passbolt URL: https://www.passbolt.com
11. Bitwarden URL: https://bitwarden.com

DEVELOPMENT OF DATA STORAGE AND PROTECTION SOFTWARE FOR PRIVATE AND CORPORATE APPLICATIONS

B.V. Gavrilyuk, V.V. Zorilo, N.I. Kushnirenko, O.R. Oskolkova

1, Shevchenko Ave., National Odessa Polytechnic University, 65044, Odesa Ukraine
vikazorilo@gmail.com, whiteswanhelena@gmail.com

It is said that the best password manager is our brain. This statement makes sense, but sometimes our brain does not cope, we have to use external resources. The number of passwords per user is growing every year: new social networks, new bank accounts, new registrations in various services, accounts on various services (television, music, Internet service providers, etc.). According to the rules of information security, using the same password for different client services is not rational, because if attackers can, for example, choose a password for your e-mail, they will try to apply it to your other applications such as Internet banking and more. Modern man understands that each service needs its own unique password. The password must be strong, contain a certain number of characters, where among the numbers and letters the reliability of the password is increased by special characters and case changes. It's hard to remember. But remembering one password is beyond the power of most of us. Choosing a convenient and reliable password manager is not an easy task. You really have to trust the service. In the end, it is he who will store your confidential information. In this paper, two dozen password managers were tested and eleven were selected, which are the best in terms of functionality, security and convenience. However, each of the well-known managers does not take into account the individual characteristics of users and needs additions according to their needs. Therefore, the creation of software for storing passwords in encrypted form is relevant. Encrypted passwords can be accessed through the one password you need to remember. Such relationship software was created in this paper, taking into account the needs of corporate and private use.

Keywords: data protection, password manager, encryption, cryptography.