DOI 10.15276/imms.v13.no3-4.275
УДК 004.9

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 275-281

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗБЕРІГАННЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

О.Р. Осколкова, В.В. Зоріло

Національний університет “Одеська політехніка”
1 Шевченка пр., Одеса, 65044, Україна
e-mail: vikazorilo@gmail.com

У сучасному світі дуже часто постає питання щодо збереження та захисту парольних даних. Існує чимало сервісів та інтернет-ресурсів, до яких потрібно мати певні доступи, аби потрапити до системи. Коли ресурсів і паролів багато, то виникає питання, де і в якій формі їх зберігати. Зазвичай для цього використовують програмні рішення – менеджери паролів. *Мета* даної роботи полягає у підвищенні ефективності зберігання інформації з обмеженим доступом шляхом розробки додатку з можливістю шифрування. Для досягнення мети було проведено огляд та аналіз сучасних менеджерів паролів, який показав, що в повній мірі існуючі рішення не можуть задовольнити вимоги багатьох підприємств, зокрема, підприємства «OdesSeo», яке займається комплексним інтернет-маркетингом і знаходиться у місті Одеса. Для зберігання інформації з обмеженим доступом у зашифрованому вигляді було вибрано алгоритми шифрування SHA3 для паролів до акантів працівників, та AES-256 для паролів до проектів замовників послуг. Шифри останніх переводили у формат позиційної системи числення Base64. Розроблено мобільний додаток – менеджер паролів, який було успішно впроваджено у виробництво підприємства «OdesSeo». Підвищення ефективності зберігання інформації з обмеженим доступом на підприємстві «OdesSeo» вимірюється в грошовому еквіваленті, нижня межа якого складає 50000 грн або 1200$, що за оцінками ризик-менеджерів відповідає мінімально-необхідним витратам на усунення наслідків витоку інформації чи несанкціонованого доступу до системи підприємства та проектів клієнтів.
Ключові слова: менеджер паролів, шифрування, захист інформації, кібербезпека.

Вступ. У сучасному світі дуже часто постає питання щодо збереження та захисту парольних даних. Існує чимало сервісів та інтернет-ресурсів, до яких потрібно мати певні доступи, аби потрапити до системи. Коли ресурсів і паролів багато, то виникає питання, де і в якій формі їх зберігати. На даний момент існують рішення, які закривають дане питання, але в них є деякі недоліки та особливості. Часто повний функціонал додатків можливо використовувати тільки за умовою придбання ліцензії, особливо у випадку використання у виробництві. Для великих компаній ця сума може сягати десятків і навіть сотень тисяч доларів. Також не завжди розробники менеджерів паролів мають хорошу репутацію: багато з них не вийшли з російського ринку та продовжують співпрацювати з країнами-терористами, що знижує довіру до них. Ці та інші причини спонукають компанії та підприємства шукати власні рішення для збереження такого виду інформації з обмеженим доступом, як паролі, ключі до шифроалгоритмів тощо.

Мета роботи полягає у підвищенні ефективності зберігання інформації з обмеженим доступом шляхом розробки додатку з можливістю шифрування.

Для досягнення поставленої мети необхідно вирішити наступні *задачі:*

1) огляд та аналіз сучасних рішень;

2) визначення методів зберігання інформації з обмеженим доступом;

3) розробка проекту програмного додатку;

4) реалізація програмного додатку.

Для конкретики будемо вирішувати дані задачі для підприємства «OdesSeo», не обмежуючи при цьому можливість адаптації і використання розробки для інших підприємств.

Основна частина. Підприємство «OdesSeo» займається комплексним інтернет-маркетингом, знаходиться у місті Одеса, існує на ринку вже 10 років і є лідером у своїй сфері. Послуги, які надає компанія, наступні: розробка сайтів – створення дизайну сайту, написання основного функціоналу сайту на основі розробленої CMS (розробка компанії); seo-просування та seo-оптимізація сайту; створення та реалізація комплексної маркетингової стратегії для просування бізнесу клієнта он-лайн; контекстна реклама (PPC) та реклама у соціальних мережах (SMM).

До цієї компанії звертаються різні бізнеси за послугами. Кожний бізнес має власні доступи до різних систем, сайтів, сервісів. Всі необхідні доступи бізнес має надати компанії для подальшої роботи. Ці доступи надаються певним співробітникам компанії, не усім, а тільки тим, хто буде працювати над проектом. Також варто враховувати, що в кожного співробітника є власні доступи, наприклад: корпоративна пошта, робочі акаунти в соціальних мережах і тому подібне.

Уся перелічена інформація є інформацією з обмеженим доступом. В тому числі від забезпечення її конфіденційності, цілісності та доступності будуть залежати ефективність роботи підприємства та його клієнтів і партнерів, репутація підприємства, прибутки та інші важливі для підприємства показники. Тому компанія зацікавлена в надійності додатку для зберігання даної інформації.

Додаток повинен задовольняти наступним вимогам: можливість створення акаунту для кожного співробітника; можливість створення записів з паролями та інформацією про проекти у власному акаунті співробітника; можливість поділитися паролем/паролями проектів з іншим співробітником; двохфакторна автентифікація працівника; шифрування паролю для входу в акаунт; шифрування паролів проектів, які зберігаються у додатку. Також дуже важливою та принциповою вимогою є те, що компанія-розробник відповідного менеджера паролів не повинна співпрацювати з компаніями РФ.

Розглянемо наступні рішення [1-5].

LastPass. Сумісність: iOS, Mac, Linux, Windows, Android. Основні функції та переваги додатку: 256-бітове шифрування AES; PBKDF2 SHA 256 та хешування з додаванням «солі»; автоматичне заповнення паролів; редагування пароля; генератор паролів; безпечний пароль і спільний доступ до нотаток; пошук паролем або сайтом; масове додавання та збереження паролів; система авторизації. Недоліки: базові установки генератора паролів менш захищені; висока вартість ліцензії. Не вийшли з російського ринку.

Dashlane. Сумісність: iOS, Mac, Linux, Windows, Android. Основні функції та параметри додатку: автоматичне заповнення паролів; масове додавання та збереження паролів; 256-бітове шифрування AES; генератор паролів; можливість внесення додаткової інформації щодо збережених паролів; система авторизації; можливість редагування паролів; хмарний контейнер; автоматичний контроль термінів старіння паролів; надсилання повідомлень про необхідність змінити дані для доступу; можливість встановити новий персональний пароль. Недоліки: висока вартість ліцензії; «хмарний» контейнер доступний тільки у платній версії; додаток має відкритий код, будь-хто може проаналізувати цей код та виявити вразливості.

1Password. Сумісність: iOS, Mac, Linux, Windows, Android. Основні функції та параметри додатку: висока надійність; наявність вбудованого генератора паролів; можливість створення резервних копій; гібридне AES-шифрування з 128

або 256 бітною маскою; зберігання та редагування паролів; зберігання додаткової важливої інформації. Програма зберігання паролів 1Password дозволяє підключатися до комп'ютера віддалено. Синхронізує пристрої за допомогою єдиного облікового запису на смартфонах та ПК. Недоліки: висока вартість; немає можливості обмінюватися даними з користувачами; якщо не оплатити підписку, то користувач більше не матиме доступу до своїх старих паролів.

Bitwarden. Сумісність: iOS, Mac, Linux, Windows, Android. Основні функції та параметри додатку: багатофакторна автентифікація; 1гб зашифрованого файлового сховища з преміям-планами; синхронізація з хмарою; наскрізне шифрування AES 256 біт, хешування та PBKDF2 SHA-256; можливість писати та виконувати сценарії у сховищі Bitwarden. Недоліки: додаток має відкритий код.

Keeper. Сумісність: iOS, Mac, Linux, Windows, Android. Основні функції та параметри додатку: персональне сховище для кожного користувача; автоматичне заповнення паролів; кількість даних, які можна зберігати у додатку, не обмежуються; генерація паролів; підтримка імпорту даних з інших менеджерів паролів та можливість експорту до PDF, CSV або JSON. Недоліки: складна процедура відновлення доступу до облікового запису, є можливість втрати даних; висока вартість обслуговування; не вийшли з російського ринку.

Для зручності порівняння існуючих рішень скористаємося таблицею 1.

Таблиця 1

Порівняльний аналіз існуючих аналогів

Функції	Назва мобільного додатку				
	LastPass	Dashlane	1Password	Bitwarden	Keeper
Шифрування даних	+	+	+	+	+
Система авторизації	+	+	+	+	+
Збереження та редагування паролей	+	+	+	+	+
Створення резервних копій	-	-	+	-	+
Внесення додаткових коментарів	+	+	+	-	-
Генератор паролів	+	+	-	-	-
Можливість ділитися парольними записами	-	-	-	-	+
Зручний та простий інтерфейс	-	+	+	-	+
Сучасний дизайн	-	+	+	+	+
Автономність	-	+	-	+	+
Вийшли з російського ринку	-	-	+	-	-
Вартість ліцензії на місяць на одного користувача	$10,20	Від $10	$19,95*	$20*	$45

* залежить від кількості людей

Як можемо бачити, жоден із додатків не задовольняє в повній мірі висунутим вимогам. Враховуючи важливість даних, які необхідно захистити, розробимо власне програмне забезпечення.

Для коректної роботи підприємства «OdesSeo» необхідно безпечно зберігати доступи кожного клієнта та передавати їх між співробітниками, що працюють над спільними проектами, а саме доступи до сайтів, хостингу, акаунтів соціальних мереж тощо. Втрата або витік цієї інформації на підприємстві може призвести до небажаних наслідків, матеріальних та репутаційних збитків.

База даних буде складатися з наступних таблиць: «User» для зберігання та реєстрації даних для ідентифікації, аутентифікації та авторизації працівників; «Passwords» для зберігання записів користувача, які є інформацією, наданою клієнтами/партнерами; «Receivepass» для записів про те, хто з працівників поділився паролем та з ким, і про його статус – «прочитано»/«не прочитано» (рис.1).

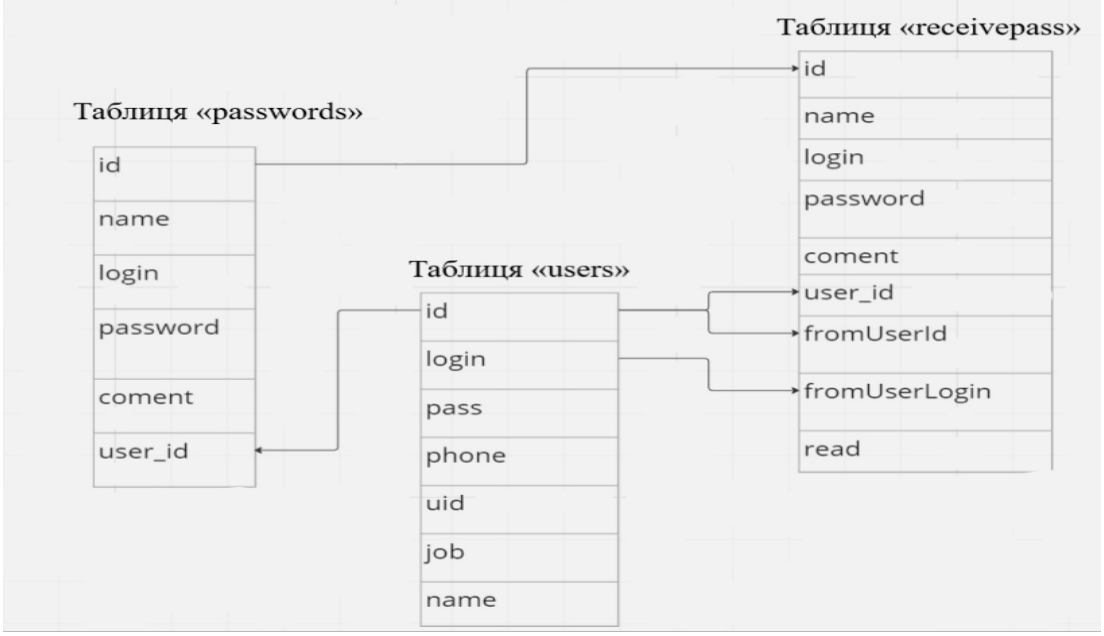

Рис. 1. Схема бази даних для серверної частини додатку

Безпека процесу реєстрації та авторизації користувачів в системі забезпечується шляхом шифрування пароля для входу в обліковий запис. Шифрування здійснюється на серверній стороні, зашифровані дані зберігаються у таблиці «User».

Для паролів працівників встановимо наступні обмеження: довжина повинна бути не менше 10 символів, пароль повинен містити хоча б одну велику літеру, хоча б одну цифру і хоча б один спеціальний знак з наступного переліку знаків {!, ?, %, &}; алфавіт має складатися з латинських літер, арабських цифр та спеціальних знаків, потужність алфавіту з врахуванням регістрів складає 66 символів. Таким чином для підбору одного символу пароля можливі 66 варіантів, а кількість усіх можливих комбінацій складає 66^{10}.

З міркувань безпеки паролі на сервері будуть зберігатися у вигляді хешу, згенерованого засобами алгоритму SHA3. До пароля при шифруванні буде додаватись «сіль». Разом з іншими даними про працівника пароль потрапляє на сервер, де створюється новий запис у таблиці «Users».

Для додаткового захисту використаємо двохфакторну автентифікацію, де другий фактор захисту буде реалізовано через корпоративний номер телефону працівника: для авторизації чи реєстрації користувачів необхідно отримати підтвердження у вигляді коду, який буде надіслано як SMS-повідомлення на вказаний номер телефону. При реєстрації код надсилається лише у випадку, якщо користувача ще немає у системі. При авторизації код відправляється тільки у випадку, якщо вказаний користувач вже зареєстрований у системі.

Під час роботи з проектами замовників послуг працівники «OdesSeo» створюють у застосунку записи про клієнтів з наступною інформацією: назва проекту, логін, пароль та коментар для конкретного запису. Ці дані зберігаються у базі даних у таблиці «Passwords». Пароль також зберігається у зашифрованому вигляді. Шифрування відбувається на пристрої працівника ще до того, як

відправити їх до бази даних.

При створенні працівником запису про клієнта поле з паролем проекту шифрується алгоритмом симетричного шифрування AES-256 за допомогою унікального для кожного проекту ключа шифрування, що зберігається у файлах додатка та разом з іншими даними відправляється до бази даних. Ключ зберігається в базі даних у таблиці «passwords» зашифрованому вигляді.

Для того, щоб розшифрувати пароль, необхідно щоб користувач у полі для вводу ввів власний ключ шифрування (рис. 2). Не знаючи ключ шифрування, побачити пароль в дешифрованому вигляді не можливо.

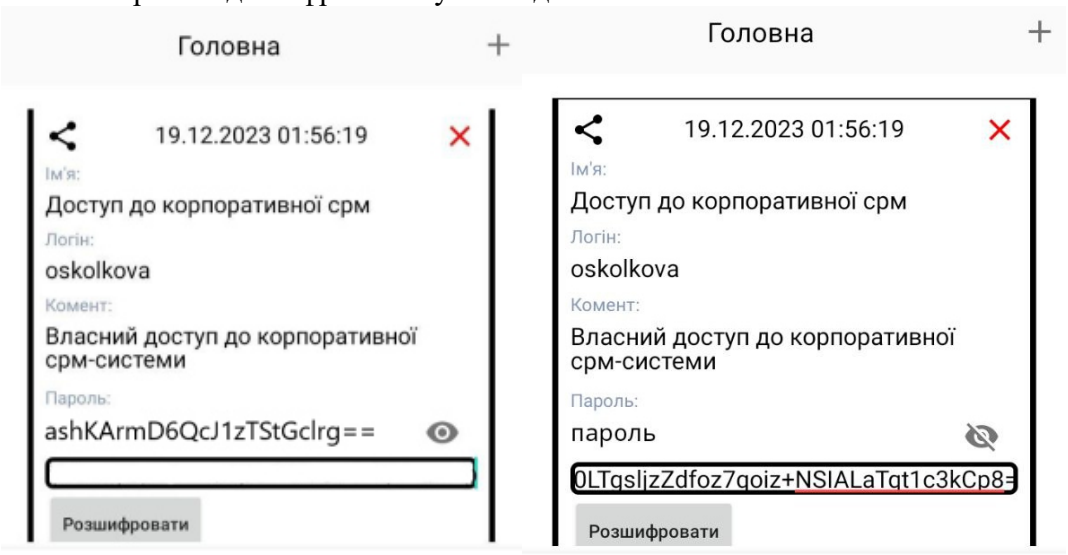

Рис.2. Дешифрування паролю

Процес генерації ключа шифрування було удосконалено шляхом додавання логіну користувача та конвертації ключа з шифру AES-256 у представлення в позиційній системі числення Base64. Обрана комбінація симетричного шифрування пароля з додаванням логіна працівника та солі та представлення шифру у Base64 забезпечує достатній рівень безпеки, прийнятну швидкість шифрування, ефективність та зручність в роботі з ключем шифрування.

Можливість поділитися парольним записом з іншим працівником в застосунку реалізовано у вигляді функції вибору конкретного працівника та передачі конкретного запису з паролем. В таблиці «Receivepass» при цьому буде створено запис з інформацією про: проектну назву, логін, пароль та коментар; ідентифікатор та логін відправника; ідентифікатор отримувача; статус запису «прочитано»/«не прочитано».

Під час реєстрації працівнику надається можливість заповнити спеціальну форму, яка включає наступні поля: прізвище; ім'я; по-батькові; логін; номер телефону; посада в компанії; пароль. Після заповнення форми та натискання кнопки «Зареєструватися» дані відправляються на сервер для перевірки наявності в базі даних. Якщо збіг знайдений, користувач отримує повідомлення про існуючий акаунт і неможливість реєстрації з заданими параметрами. Інакше система переходить до наступного етапу – перевірка за вказаним номером телефону – надсилання повідомлення з кодом підтвердження (рис. 3), відсіювання ботів через проходження капчі (рис. 4).

В результаті успішного проходження останнього етапу створюється новий запис у базі даних з інформацією про працівника та його унікальним ідентифікатором. Ці заходи значно підвищують рівень безпеки реєстрації та збереження даних користувачів у системі.

Авторизація працівника передбачає введення даних: логін, номер

телефону, пароль, унікальний ключ для шифрування, який зберігається на пристрої користувача. Після заповнення всіх полів пароль піддається хешуванню з сіллю, що дозволяє зменшити ризики атак з використанням «райдужних таблиць», відбувається пошук отриманого хешу на сервері. Якщо запис знайдено, користувач авторизується в системі. Інакше відбувається відмова в авторизації, а після певної кількості невдалих спроб – блокування акаунта. Це дозволяє протистояти можливій атаці перебору паролів «грубою силою».

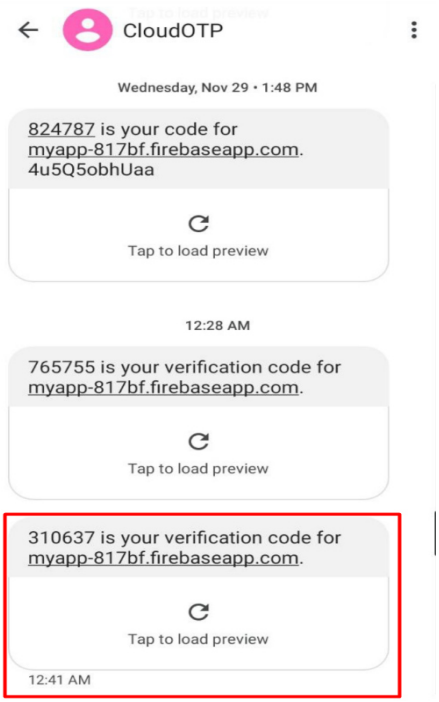

Рис.3. Надсилання повідомлення з кодом підтвердження

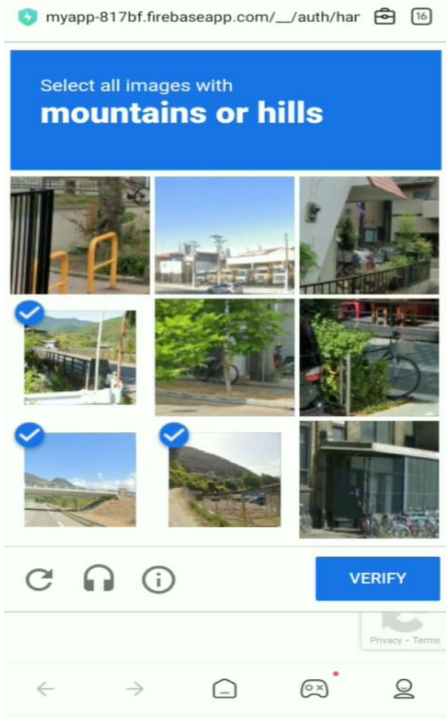

Рис. 4. Приклад проходження капчі

Для виводу на сторінці працівника доступних йому проектних записів система за ідентифікатором працівника створює запит до бази даних до таблиці «Passwords» та повертає дані, що належать користувачеві. Він може їх видаляти, редагувати, створювати нові, або надсилати їх колезі. Пароль доступу до проекту буде відображатись у зашифрованому вигляді. Для розшифрування необхідно ввести ключ.

Одночасно з цим на пристрої працівника-відправника виконується генерація ключа шифрування, що буде використовуватися для шифрування і дешифрування паролів, які користувач буде створювати і зберігати у додатку.

Для того, щоб поділитися паролем, необхідно обрати запис з паролем та існуючого користувача зі списку. Отримані доступи від інших користувачів зберігаються в окремому вікні, де можна побачити запис з паролем та від кого був отриманий запис. Для дешифрування отриманих записів необхідно отримати ключ того працівника-відправника. Згідно встановленої на підприємстві політики безпеки даний ключ можна отримати за оформленим запитом до адміністратора, який має схвалити керівник проекту.

Висновки. Проведено огляд та аналіз сучасних рішень збереження паролів, в результаті якого виявлено, що існуючі менеджери паролів попри свої переваги мають ряд недоліків, які для конкретних підприємств можуть виявитись неприпустимими та спонукати до розробки власних рішень.

Дану роботу було виконано для підприємства «OdesSeo», яке займається комплексним інтернет-маркетингом і яке потребує особливої уваги у питанні

збереження паролів.

Розроблено програмний додаток – менеджер паролів. Основним функціоналом програмного додатку є реєстрація, авторизація користувачів, можливість створювати та ділитися парольними даними і захист паролів від атак зловмисників. Переваги розробленого застосунку у порівнянні з існуючими аналогами полягають у вдосконалені процесу генерації ключа шифрування для паролів, що зберігаються у додатку, шляхом додавання логіну користувача та конвертації шифру ключа, виконаного алгоритмом AES-256, до виду позиційної системи числення Base64. Паролі доступу до акантів працівників зберігаються на сервері у вигляді хешу. Хешування відбувається алгоритмом SHA3 з додаванням солі.

Підвищення ефективності зберігання інформації з обмеженим доступом на підприємстві «OdesSeo» вимірюється в грошовому еквіваленті, нижня межа якого складає 50000 грн або 1200$, що за оцінками ризик-менеджерів відповідає мінімально-необхідним витратам на усунення наслідків витоку інформації чи несанкціонованого доступу до системи підприємства та проектів клієнтів.

Список літератури

1. Ahlgren M. Lastpass VS Dashlane (Password Manager Comparison). URL: https://www.websiterating.com/password-managers/lastpass-vs-dashlane/
2. Усама З. 5 найкращих менеджерів паролів для Windows в 2024. URL: https://uk.wizcase.com/blog/найкращі-менеджери-паролів-для-windows/
3. Шевченко Л. П’ять найкращих менеджерів паролів для вашої безпеки. URL: https://processer.media/ua/pass-managers/
4. Гарг Д. Огляд Keeper Password Manager 2023: чи він найкращий для керування паролями та секретами? URL: https://jitendra.co/uk/keeper-password-manager-review/

ENHANCING THE EFFICIENCY OF STORING RESTRICTED INFORMATION

O.R. Oskolkova, V.V. Zorilo

National Odesa Polytechnic University
1, Shevchenko Ave, Odesa, 65044
email vikazorilo@gmail.com

In the contemporary world, there is a frequent concern regarding the preservation and protection of password data. Numerous services and internet resources require specific accesses to enter their systems. When dealing with a multitude of resources and passwords, the question arises as to where and in what form to store them. Typically, software solutions, namely password managers, are employed for this purpose. The objective of this study is to enhance the efficiency of storing restricted-access information by developing an application with encryption capabilities. To achieve this goal, a review and analysis of modern password managers were conducted, revealing that existing solutions fail to meet the requirements of many enterprises, including 'OdesSeo,' a comprehensive internet marketing enterprise located in the city of Odesa. For the secure storage of restricted-access information, SHA3 encryption algorithms were chosen for employee account passwords, while AES-256 was selected for project passwords of service clients. The latter ciphers were translated into Base64 positional numeral system format. A mobile password manager application was developed and successfully implemented in the production environment of 'OdesSeo.' The increase in the efficiency of storing restricted-access information at 'OdesSeo' is measured in monetary terms, with the lower threshold being 50,000 UAH or 1,200 USD, representing the minimum necessary expenses, according to risk managers' estimates, to mitigate the consequences of information leaks or unauthorized access to the enterprise system and client projects.

Keywords: password manager, encryption, information protection, cyber security.