НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

28 листопада 2025 року

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ VI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

28 листопада 2025 року, м. Одеса

Одеса, 2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
National University «Odesa Law Academy»
Faculty of Cybersecurity and Information Technologies
Department of Cybersecurity

CYBERSECURITY IN TODAY'S WORLD: ACTUAL CHALLENGES

MATERIALS OF THE VI INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

November 28, 2025, Odesa

Odesa, 2025

УДК 004.056

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій, кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть учасники конференції, їхні наукові керівники, які рекомендували ці матеріали до друку.

Рекомендовано до друку
Вченою радою Національного університету
«Одеська юридична академія»
(протокол №3 від 29.11.2025 р.)

Матеріали Міжнародної науково-практичної конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с.

У конференції взяли участь студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

UDC 004.056

Editor-in-chief:

O. V. Dykyi, Dean of the Faculty of Cybersecurity and Information Technologies,
Candidate of Law, Associate Professor

The materials were published in the author's edition.
Full responsibility for the reliability and quality of the submitted material
bears the participants of the conference, their scientific supervisors,
who recommended these materials for publication.

Recommended for printing
by the Academic Council of the National University
«Odesa Law Academy»
(Minutes No. 3 dated 11/29/2025)

Materials of the International Scientific and Practical Conference «Cybersecurity in the Modern World: Current Challenges» (Odessa, November 28, 2025). Odesa, 2025. 287 p.

The conference was attended by students, postgraduates, young scientists, teachers and researchers. The conference is held at the National University «Odesa Law Academy».

VI Міжнародна науково-практична конференція

«Кібербезпека в сучасному світі: актуальні виклики»

28 листопада 2025 року

ТЕМАТИЧНІ НАПРЯМКИ КОНФЕРЕНЦІЇ:

Секція 1. Алгоритмічні та технічні аспекти кібербезпеки

Секція 2. Штучний інтелект та інформаційні технології

Секція 3. Управлінські, соціальні та психологічні аспекти взаємодії з кіберпростором

Секція 4. Нормативно-правові засади кібербезпеки та захисту інформації

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

VI International Scientific and Practical Conference

«Cybersecurity in today's world: actual challenges»

28 November 2025 year

THEMATIC DIRECTIONS OF THE CONFERENCE:

Section 1. Algorithmic and technical aspects of cybersecurity

Section 2. Artificial intelligence and information technologies

Section 3. Management, social and psychological aspects of interaction with cyberspace

Section 4. Regulatory and legal principles of cybersecurity and information protection

E-mail: kiberprostirconf@gmail.com (Для питань та тез)

ЛОКАЛЬНИЙ МЕНЕДЖЕР ПАРОЛІВ ІЗ ГЕНЕРУВАННЯМ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Тимошенко Лідія

кандидат економічних наук, доцент кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»

Вакуліна Сана

здобувач кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»

Волобуєва Ірина

здобувач кафедри кібербезпеки та програмного забезпечення Національного університету «Одеська політехніка»

Із розвитком інформаційних технологій та масовим переходом до цифрових сервісів питання захисту облікових даних користувачів набуває особливої актуальності. Паролі є найпоширенішим методом автентифікації, однак користувачі часто обирають прості комбінації або повторюють ті ж паролі в різних акаунтах. Це призводить до підвищення ризику несанкціонованого доступу до персональних даних.

Надійність пароля безпосередньо залежить від його довжини, складності та ентропії. Для підвищення рівня безпеки важливо не лише створювати складні паролі, але й оцінювати їхню стійкість до підбору. Застосунок для автоматичного генерування паролів та оцінювання надійності сприяє формуванню звичок користувачів і підвищенню загального рівня кібербезпеки.

Метою роботи є забезпечення високої швидкості генерування паролів та конфіденційності процесів шляхом локального генерування і оцінювання їх надійності.

Під час проведення огляду сучасних програм для керування паролями – LastPass, Bitwarden, KeePass та 1Password, встановлено, що більшість орієнтовані на централізоване зберігання паролів у хмарних сховищах, що створює додаткові ризики витоку даних (табл. 1) [1]. Запропонований підхід – операції з обробки паролів виконуватимуться локально на пристрої користувача.

Таблиця 1 – Огляд програм для керування паролями

Назва	Основна ідея	Переваги	Недоліки
LastPass	Хмарний менеджер паролів. Зберігає зашифровані паролі, синхронізується між пристроями.	Зручний інтерфейс, багато функцій, автозаповнення, 2FA.	Мав витоки даних, залежність від мережі, лазівки безпеки (автозаповнення, браузерні плагіни) можуть бути вразливими.
Bit warden	Відкритий (open source) менеджер, з хмарною або самостійною (self-hosted) опцією.	Більше прозорості через відкритий код, можливість самостійного хостингу, сильне шифрування.	Деякі функції обмежені у безкоштовній версії; залежність від інтернету, якщо в хмарі; не всі частини інтерфейсу шифруються однаково у деяких менеджерах.
KeePass	Відкритий офлайн-менеджер. Дані зберігаються локально (файл бази), без необхідності серверів.	Повний контроль над даними, автономність, можна без мережі.	Менше зручностей (синхронізація через сторонні сервіси, ручне оновлення, UI), складніше для початківців.
1 Pass-word	Комбінація хмарного сховища й сильних еханізмів захисту, зручний інтерфейс, багатофакторна аутентифікація.	Нові високі стандарти безпеки, користувацький досвід, регулярні аудити, зручність + функції.	Часто платний, залежить від сервісів (хмарне зберігання), можуть бути витрати, якщо потрібно багато пристроїв або сімейний план.

Локальна система складається з трьох основних модулів.

1. Модуль генерації паролів:

– генерація рандомних комбінацій символів на основі заданих параметрів: довжина пароля, типи символів (літери, цифри, спеціальні знаки);

– можливість користувачу вказати потрібну довжину пароля;

– функція корекції згенерованого пароля користувачем.

2. Модуль оцінки надійності:

– перевірка введеного або згенерованого пароля за критеріями довжини, різноманітності символів та наявності повторів;

– використання списку з приблизно 200-от найпопулярніших паролів, які автоматично оцінюються як «слабкі»;

– результат оцінки надійності відображається у вигляді символів.

3. Модуль візуалізації результатів:

– відображення рівня надійності та ентропії пароля;

– надання рекомендацій щодо покращення пароля.

На рис. 1 наведено схему локального застосунку для генерування паролів від введення або генерації пароля, його модифікації, оцінки надійності до відображення результату користувачу.

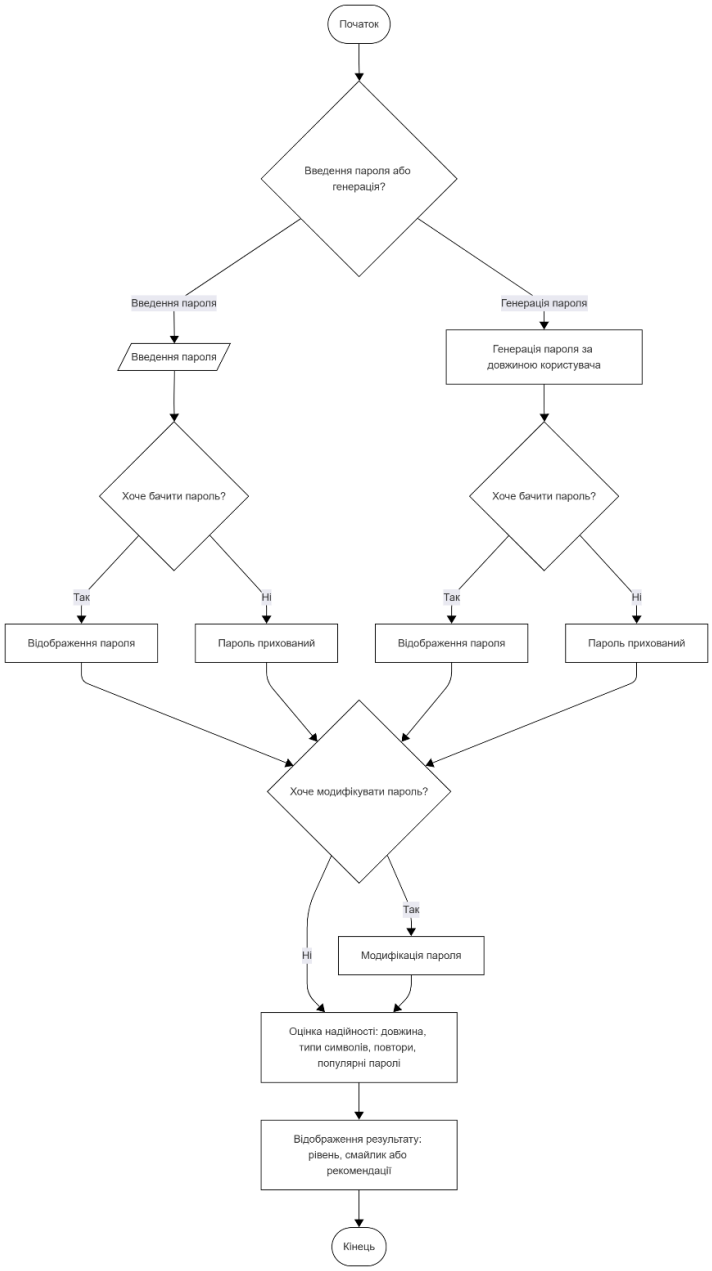

Рис.1. Схема локального застосунку для генерування паролів

Особливостями роботи системи є те, що всі обчислення виконуються локально на пристрої користувача, без обміну даними із зовнішніми сервісами, робота в офлайн-режимі для забезпечення безпеки та конфіденційності.

Розробку мобільного застосунку планується виконати у Android Studio з використанням мови Kotlin та фреймворку Android SDK для створення локального графічного інтерфейсу.

Для оцінки надійності пароля застосовуватимемо ентропійну модель, де рівень стійкості визначається за формулою [2]:

$$H = L \cdot log_2(N) \quad (1)$$

де L – довжина пароля,

N – кількість можливих символів у вибраному наборі.

На основі значення H пароль класифікують за рівнями стійкості:

– до 28 біт дуже слабкий;
– 28–36 біт слабкий;
– 36–60 біт середній;
– понад 60 біт сильний.

Результат оцінки відображатиметься користувачеві у графічній формі, наприклад, у вигляді смайлика або кольорового індикатора надійності.

Висновки. У результаті виконання роботи розроблено концепцію та прототип локального застосунку для генерування та оцінки надійності паролів на мобільних пристроях. Система працює автономно, без підключення до інтернету. Застосунок може бути інструментом навчання користувачів та частиною комплексних систем захисту інформації. Подальший розвиток проєкту – інтеграція модулів перевірки паролів за локальними словниками витоків, додавання рекомендацій із кібергігієни та впровадження адаптивних алгоритмів оцінювання на основі штучного інтелекту.

Список використаної літератури:

1. Alsharaya H. Password managers: a critical review of security, usability, and innovative designs. Journal of Computer Sciences Institute,2025, Т.36, №9, с. 28-35.
2. Oesch S., Ruoti S. Evaluating Password Managers Against Real-World Phishing Pages. IJCT Journal, 2025.

Ключові слова: пароль, застосунок, надійність, мобільний пристрій.
Keywords: password, application, reliability, mobile device

СУЧАСНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ІНТЕЛЕКТУАЛЬНИХ ЖИТЛОВИХ СИСТЕМАХ

Неділенко Валерій

аспірант кафедри безпеки інформаційних технологій
Національного університету «Львівська політехніка»

Вступ

Сучасні технології Інтернету речей (IoT) розвиваються з надзвичайною швидкістю, що створює нові виклики у сфері безпеки інформаційних систем. Одним із актуальних напрямів є захист розумних пристроїв та систем IoT, які активно інтегруються у побутові, промислові та енергетичні рішення. Пристрої IoT можуть містити різні бінарні дані, пов’язані з безпекою, для того щоб уможливити використання відповідних протоколів, наприклад, сертифікати

ЗМІСТ