

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний університет "Житомирська політехніка"
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра на тему:
«Дослідження та послаблення вразливостей систем парольної
аутентифікації користувачів інформаційних систем»

Виконала студентка 4-го курсу групи КБ-19-2
спеціальності 125 «Кібербезпека»

 Дарина Шевчик
Керівник старший викладач кафедри КІ та КБ

 Єлизавета Байлюк

Рецензент професор кафедри КІ та КБ, д.т.н., доцент

 Володимир Воротніков

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної

інженерії та кібербезпеки

 Андрій Єфіменко

1 березня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студентка: Шевчик Дарина Анатоліївна

Тема роботи: «Дослідження та послаблення вразливостей систем парольної аутентифікації користувачів інформаційних систем»

затверджена Наказом університету від 1 березня 2023 р. № 99

Термін здачі студентом закінченої роботи 20.06.2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

- Системи парольних аутентифікацій та їх вразливості;
- Дослідження впливу парольних політик на зменшення вразливостей систем парольних аутентифікацій

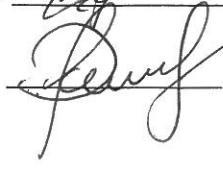
Обладнання та програмне забезпечення:

1. Kali Linux (2021.4)
2. Програмне забезпечення «VirtualBox» v. 6.1.32
3. Ubuntu (20_04 LTS)
4. Програмне забезпечення «KeePass» v. 2.54
5. Розширення для браузера «Bitwarden»

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Байлюк Є.М..	13.03.2023	13.03.2023
2	Байлюк Є.М.	01.04.2023	01.04.2023
3	Байлюк Є.М.	15.04.2023	15.04.2023
4	Байлюк Є.М.	25.04.2023	25.04.2023

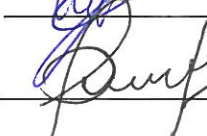
Студентка  Дарина Шевчик

Керівник  Єлизавета Байлюк

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	19.02.2023	Виконано
2	Аналіз об'єкта дослідження	10.03.2023	Виконано
3	Постановка задачі дослідження	12.03.2023	Виконано
4	Опрацювання літературних джерел	20.03.2023	Виконано
5	Пошук програмного забезпечення	10.04.2023	Виконано
6	Дослідження сучасних систем парольних аутентифікацій	15.04.2023	Виконано
7	Налагодження робочого середовища	18.04.2023	Виконано
8	Дослідження програмного забезпечення для зламу паролів	05.05.2023	Виконано
9	Тестування парольних менеджерів	10.05.2023	Виконано
10	Аналіз вразливостей систем парольних аутентифікацій	20.05.2023	Виконано
11	Розробка рекомендацій для складання парольних політик	02.06.2023	Виконано
12	Оформлення пояснювальної записки	15.06.2023	Виконано
13	Отримання відгуку керівника та рецензії на кваліфікаційну роботу		Виконано
14	Захист		Виконано

Студентка  Дарина Шевчик

Керівник  Єлизавета Байлюк

АНОТАЦІЯ

Випускна робота бакалавра складається з пояснювальної записки. Пояснювальна записка до випускної бакалаврської роботи містить 52 сторінки і 28 рисунків. Перелік посилань містить 24 літературних джерела.

Останні роки все більшої популярності набирає дистанційний формат роботи. У зв'язку з цим, з'явилася ще гостріша потреба у впровадженні надійних методів захисту систем парольних аутентифікацій.

Метою цієї кваліфікаційної роботи є дослідження методів мінімізації вразливостей систем парольних аутентифікацій шляхом впровадження парольних політик.

У першому розділі було розглянуто теоретичні відомості про поняття авторизації та аутентифікації.

У другому розділі було розглянуто сучасні системи парольних аутентифікацій, їх переваги та недоліки.

У третьому розділі було досліджено програмні засоби для зламу систем парольних аутентифікацій та методи їх роботи. Також було розглянуто популярні парольні менеджери та засоби двофакторної аутентифікації.

У четвертому розділі було досліджено вимоги, що мають бути впроваджені у системи парольних аутентифікацій для мінімізації їх вразливостей.

Ключові слова: СИСТЕМИ ПАРОЛЬНИХ АУТЕНТИФІКАЦІЙ, ПАРОЛЬНА ПОЛІТИКА, СОЦІАЛЬНА ІНЖЕНЕРІЯ, АУТЕНТИФІКАЦІЯ, ЗАХИСТ ІНФОРМАЦІЙНИХ СИСТЕМ.

					ККІКБ.КР.Б – 125 – 23 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Дослідження та послаблення вразливостей систем парольної аутентифікації користувачів інформаційних систем	Літ.	Арк.	Аркуші
Розроб.		Шевчик Д.А.		20.06.23				
Перевір.		Байлюк Є.М.		20.06.23				
Керівник								
Н. контр.								
Зав. каф		Єфіменко А.А.		20.06.23		ФІКТ Гр. КБ-19-2		

ANNOTATION

A bachelor's degree qualification work consists of an explanatory note. The explanatory note to the bachelor's thesis contains 52 pages, and 28 figures. The list of references includes 24 literary sources.

Nowadays, a remote format of working has become more popular. As a result, the inception of reliable methods of password authentication systems' protections is now a necessity.

This work aims to investigate the methodology of minimisation vulnerabilities of password authentication systems by implementing password policies.

In the first chapter, theoretical information about the concepts of authorization and authentication was considered.

In the second chapter, modern password authentication systems, their advantages, and disadvantages were considered.

In the third chapter, software tools for breaking password authentication systems and their methods of operation were investigated. Popular password managers and two-factor authentication tools were also considered.

The fourth chapter explored the requirements that should be implemented in password authentication systems to minimize their vulnerabilities.

Keywords: PASSWORD AUTHENTICATION SYSTEMS, PASSWORD POLICY, SOCIAL ENGINEERING, AUTHENTICATION, PROTECTION OF INFORMATION SYSTEMS.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ЗМІСТ

АНОТАЦІЯ	5
ANNOTATION.....	6
ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ ПАРОЛЬНИХ АУТЕНТИФІКАЦІЙ	10
1.1. Поняття аутентифікації та авторизації	10
1.2. Принципи роботи систем пароліної аутентифікації.....	12
1.3. Основні методи атак на системи пароліної аутентифікації.....	12
РОЗДІЛ 2. АНАЛІЗ ІСНУЮЧИХ СИСТЕМ ПАРОЛЬНОЇ АУТЕНТИФІКАЦІЇ ..	15
2.1. Огляд сучасних методів пароліної аутентифікації	15
2.2. Популярні системи пароліної аутентифікації, їх переваги та недоліки	15
2.3. Аналіз вразливостей сучасних систем пароліної аутентифікації	19
РОЗДІЛ 3. ДОСЛІДЖЕННЯ ОСНОВНИХ ПРОГРАМНИХ ЗАСОБІВ, ЩО ВИКОРИСТОВУЮТЬСЯ У СИСТЕМАХ ПАРОЛЬНИХ АУТЕНТИФІКАЦІЙ...	20
3.1. Огляд програмних інструментів для зламу паролів.....	20
3.1.1 John the Ripper.....	20
3.1.2 Hydra.....	22
3.2. Огляд пароліних менеджерів	27
3.2.1 Bitwarden	27
3.2.2 KeePass	31
3.3. Двофакторна аутентифікація	37
РОЗДІЛ 4. АНАЛІЗ ПРОВЕДЕНИХ ДОСЛІДЖЕНЬ ТА РОЗРОБКА ВИМОГ ДО ПАРОЛЬНИХ ПОЛІТИК.....	42
4.1. Вимоги до пароліних політик	42
4.2. Методи захисту від соціальної інженерії	45
4.3. Оцінювання захищеності системи пароліної аутентифікації.....	47
ВИСНОВОК.....	49
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	50

ВСТУП

Актуальність теми. В реаліях нашого сьогодення, все більше видів діяльності трансформуються та частково чи повністю переходять у онлайн-формат. Цьому сприяють різні фактори. Основним поштовхом до таких метаморфозів стала епідемія вірусу COVID-19, через що було введено обмеження на великі скупчення людей, в тому числі й на робочих місцях.

В результаті цього виявилось, що в деяких сферах, зокрема в сфері інформаційних технологій такий формат роботи є досить ефективним, а іноді навіть більш ефективним, ніж робота в офісі. Крім того, для підприємств дистанційна форма організації праці є вигіднішою економічно, оскільки не потрібно розподіляти частину бюджету на утримання приміщення, оренду, надання послуг таксі в нічний час тощо.

Але попри усі переваги дистанційної форми роботи, все ж є певні недоліки. Основною проблемою онлайн формату є організація безпечного процесу праці. Підприємству доводиться знаходити шляхи налагодження захищеної комунікації в середині компанії, безпечний доступ до внутрішніх систем/баз даних тощо.

На цьому фоні, було виявлено загальні тенденції вразливостей компаній. Одним з найбільших недоліком у системах захисту підприємств є людський фактор. Все більше набуває популярності серед хакерів соціальна інженерія як метод отримання доступу до внутрішніх систем компаній, зокрема – отримання особистих та корпоративних паролів.

Саме тому, впровадження якісних захисних механізмів для систем парольних аутентифікацій є однією з найважливіших задач сучасних фахівців з кібербезпеки.

Метою кваліфікаційної роботи є дослідження систем парольної аутентифікації та мінімізація вразливостей систем захисту, зокрема за рахунок парольних політик.

Для досягнення цієї мети необхідно виконати такі завдання:

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк Є.М				8
Змн.	Арк.	№ докум.	Підпис	Дата		

- вивчення поняття аутентифікації та авторизації, дослідити вразливості сучасних систем парольних аутентифікацій;
- практичне дослідження вразливостей систем парольних аутентифікацій та чим вони зумовлені;
- дослідження того, яким чином ці вразливості можна зменшити шляхом впровадження парольної політики.

Об’єктом дослідження є сучасні системи парольних аутентифікації, їх переваги та недоліки.

Предметом дослідження є парольні політики як один з методів мінімізації вразливостей систем парольних аутентифікації.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк Є.М				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ СИСТЕМ ПАРОЛЬНИХ АУТЕНТИФІКАЦІЙ

1.1. Поняття аутентифікації та авторизації

Основою будь якої системи урегулювання розміру повноважень та рівня доступу до інформації будь-якої компанії є поняття аутентифікації та авторизації.

Аутентифікація - процес перевірки ідентичності користувача, який намагається отримати доступ до системи або ресурсу, шляхом перевірки наданої користувачем інформації. Процес аутентифікації може включати різні етапи в залежності від того, яка система використовується і які механізми захисту в ній реалізовані [17]. Але загальний процес аутентифікації може бути описаний у вигляді таких етапів:

1) Надання ідентифікатора користувачем: користувач повинен представити ідентифікатор, який відповідає його обліковому запису в системі. Це може бути логін, електронна адреса або інший ідентифікатор, який було надано при реєстрації в системі.

2) Перевірка ідентифікатора: система перевіряє, чи існує користувач з таким ідентифікатором в її базі даних. Якщо такий користувач існує, відбувається перехід на наступний етап, якщо ні – процес аутентифікації припиняється.

3) Надання пароля: після успішної перевірки ідентифікатора, користувач повинен представити пароль, який пов'язаний з цим обліковим записом. Пароль може бути введений за допомогою клавіатури або інших методів, таких як сканування відбитку пальця або розпізнавання обличчя.

4) Перевірка пароля: система перевіряє, чи введений пароль відповідає такому, що зберігається в базі даних користувачів. Якщо пароль вірний, система продовжує процес аутентифікації. Якщо ні – система повідомляє про помилку і зупиняє процес аутентифікації.

5) Надання доступу: якщо ідентифікатор і пароль введені правильно, система надає користувачу доступ до ресурсів, на які він має дозвіл. Зазвичай це

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				10
Змн.	Арк.	№ докум.	Підпис	Дата		

включає додаткову перевірку прав доступу користувача до окремих ресурсів, контроль та обмеження доступу.

Існують різні види аутентифікації, серед яких:

- Аутентифікація на основі біометричних даних, таких як відбитки пальців, розпізнавання голосу або обличчя.
- Аутентифікація на основі ключів, таких як RSA-ключі.
- Аутентифікація на основі криптографічних протоколів, таких як Kerberos або SSL/TLS.

Авторизація - процес перевірки повноважень користувача, який вже пройшов аутентифікацію, для забезпечення доступу до конкретних ресурсів, які йому дозволено використовувати [18]. Узагальнено етапи авторизації можна описати наступним чином:

- 1) Користувач надає запит на доступ до певного ресурсу.
- 2) Система перевіряє права доступу користувача до цього ресурсу, які можуть бути збережені в базі даних системи або у відповідному файлі на сервері.
- 3) Якщо користувач має достатньо прав для доступу до ресурсу, система надає йому доступ. Якщо прав недостатньо, доступ може бути обмежений або заборонений.

У багатьох системах авторизація може бути налаштована на різні рівні доступу до ресурсів. Наприклад, в системі управління базами даних користувачі можуть мати права на читання даних, але не мати прав на їх редагування. Також можуть бути налаштовані права доступу на рівні додатків або модулів системи.

Процес авторизації зазвичай супроводжується веденням журналу доступу [8], де реєструється інформація про користувачів, які отримали доступ до ресурсу, час їхнього доступу та виконані дії. Це дозволяє системним адміністраторам відслідковувати доступ до ресурсів та виявляти можливі порушення безпеки. Наприклад, системний адміністратор має можливість відслідкувати незвичну кількість невдалих спроб авторизації певного облікового запису.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				11
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2. Принципи роботи систем пароліної аутентифікації

Принцип роботи систем пароліної аутентифікації полягає у перевірці того, що введений користувачем пароль збігається зі збереженим паролем в системі. Після введення пароля система перевіряє правильність введеного значення, порівнюючи його зі значенням, яке зберігається в базі даних або іншому джерелі. Якщо введений пароль співпадає зі збереженим, користувач отримує доступ до системи. Якщо ж паролі не співпадають, доступ до системи буде відхилений [19].

Основні принципи роботи систем пароліної аутентифікації включають:

- Захист паролів: система повинна забезпечувати захист паролів користувачів від несанкціонованого доступу, наприклад, шляхом збереження паролів у хешованому форматі.
- Контроль доступу: система повинна забезпечувати контроль доступу, який дозволяє відмежувати користувачів від інформації та функцій, які вони можуть використовувати.
- Логування: система повинна вести журнал дій користувачів, щоб мати можливість відслідковувати дії користувачів в системі.
- Політики паролів: система повинна мати встановлені правила для вибору паролів, щоб забезпечити надійний рівень захисту від несанкціонованого доступу до системи.
- Перевірка паролів: система повинна перевіряти паролі, введені користувачами, на відповідність заданим правилам та забезпечувати належну безпеку входу до системи.

1.3. Основні методи атак на системи пароліної аутентифікації

Неважко здогадатися, що системи аутентифікації регулярно стають ціллю для атак зловмисників, оскільки в результаті це дає змогу отримати доступ до виділеної частини інформації (в залежності від ролі зламаного облікового запису) та впливати на систему «з-середини».

Основними методами атак на системи пароліної аутентифікації є [20]:

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				12
Змн.	Арк.	№ докум.	Підпис	Дата		

1) Атаки «грубої сили» (Brute force атаки) – метод атаки на систему парольної аутентифікації, при якому зловмисник намагається отримати доступ до системи шляхом перебору всіх можливих комбінацій паролів, поки не буде отримано правильну комбінацію. Цей метод є одним з найпростіших, але дуже затратним по часу та неефективним.

2) Атаки «за словником» (Dictionary атаки) – це метод атаки на систему парольної аутентифікації, при якому зловмисники використовують попередньо скомпонований словник, щоб спробувати вгадати пароль користувача. У цьому методі атаки використовуються списки зі слів, фраз, чисел або комбінацій символів, які зазвичай використовуються для паролів.

3) Атаки з використанням соціальної інженерії (Social engineering) – це атаки, у яких використовуються соціальні навички для отримання доступу до конфіденційної інформації чи системи. Основною метою таких атак є залучення людини до виконання певних дій, що можуть призвести до розкриття конфіденційної інформації або надання доступу до системи. Часто такі атаки використовують людські слабкості, такі як довіра до авторитетних осіб або бажання допомогти іншим.

4) Фішингові атаки (Phishing) – це форма соціального інжинірингу, в якій зловмисник намагається отримати конфіденційну інформацію, таку як логіни, паролі, номери банківських карток, шляхом видавання себе за іншу довірену особу або організацію через електронні листи, повідомлення в соціальних мережах, SMS тощо. Часто такі атаки виглядають як офіційні повідомлення від банків, провайдерів електронної пошти, соціальних мереж, в яких запрошується негайно виконати якісь дії, такі як оновлення акаунту або перевірка безпеки.

5) Кейлогінгові атака (Keylogging) – це метод, що полягає у записуванні клавіатурного вводу користувача на комп'ютері або іншому пристрої. Для цього зловмисник може використовувати спеціальний шпигунський софт, що встановлюється на комп'ютер жертви або фізичний пристрій, який підключається до клавіатури.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				13
Змн.	Арк.	№ докум.	Підпис	Дата		

6) Сніферські атаки (Sniffing) – це метод отримання конфіденційної інформації, який полягає в перехоплюванні трафіку мережі з метою отримання паролів та інших конфіденційних даних. Для здійснення атаки зловмисники використовують програми-сніфери, які перехоплюють мережевий трафік, що протікає між комп'ютерами, маршрутизаторами та іншими мережевими пристроями.

7) Атака з використанням веселкових таблиць (Rainbow table) – це метод атаки на пароліні системи, що використовує попередньо обчислені хеш-значення паролів. У таких атаках зловмисники створюють таблицю, яка містить хеш-значення паролів з попередньо збереженими супутніми значеннями, наприклад, сіллю. Потім зловмисники можуть використовувати цю таблицю для швидкого перебору паролів, порівнюючи їх зі значеннями у таблиці. Цей метод є швидким і ефективним для паролів, які складаються зі слабких комбінацій символів або малої довжини.

8) Pass-the-hash атаки – це вид атаки, який використовується для отримання доступу до системи, необхідного для проведення злочинних дій, шляхом використання хеш-значення пароля, замість самого пароля. У такій атаці зловмисник використовує хеш пароля, який був зібраний під час аутентифікації, для авторизації свого доступу до системи, обходячи при цьому необхідність знати сам пароль. Це можливо завдяки тому, що багато систем зберігають хеш-значення пароля замість самого пароля.

Висновки до першого розділу

Отже, було коротко розглянуто поняття аутентифікації та авторизації, роботи систем пароліної аутентифікації та розглянуто основні методи атак на дані системи.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				14
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. АНАЛІЗ ІСНУЮЧИХ СИСТЕМ ПАРОЛЬНОЇ АУТЕНТИФІКАЦІЇ

2.1. Огляд сучасних методів парольної аутентифікації

Методи парольної аутентифікації з часом змінювались та удосконалювались, від традиційних паролів до біометричних та мультифакторної аутентифікації. Перші методи аутентифікації використовували прості паролі, які були збережені у вигляді тексту в базі даних системи. Згодом були введені механізми хешування паролів, при яких пароль зберігався у вигляді хеш-значення, а не відкритого тексту. Для удосконалення захисту паролів використовувались методи додавання до пароля додаткових символів та зміни формату паролів [18].

Наразі, можна виділити основні сучасні методи парольної аутентифікації:

- Використання сильних паролів: довгих та складних, з використанням різних символів, цифр та літер великих і малих регістрів;
- Двофакторна аутентифікація: використання двох різних способів аутентифікації, наприклад, пароля та SMS-коду;
- Біометрична аутентифікація: використання унікальних фізичних характеристик користувача, таких як відбиток пальця або розпізнавання обличчя;
- Мультифакторна аутентифікація: використання трьох або більше різних факторів аутентифікації, таких як пароль, біометричні дані, токен та інші;
- Автоматична аутентифікація: використання спеціального програмного забезпечення, яке запам'ятовує логіни та паролі користувачів і автоматично заповнює їх на веб-сайтах та інших сервісах.

2.2. Популярні системи парольної аутентифікації, їх переваги та недоліки

2.2.1 Сильний пароль – це пароль, який важко відгадати, і який містить комбінацію великих і малих літер, цифр і спеціальних символів. Використання сильних паролів має свої переваги та недоліки [4].

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				15
Змн.	Арк.	№ докум.	Підпис	Дата		

Переваги:

+ Захист від зловмисників: сильний пароль забезпечує відмінний захист від зловмисників, які намагаються отримати доступ до вашої системи.

+ Більша безпека для даних: використання сильних паролів зменшує ризик викрадення чутливої інформації, такої як фінансові дані, особисті контакти тощо.

Недоліки:

- Труднощі запам'ятовування: сильні паролі можуть бути складними для запам'ятовування, тому використання унікальних паролів для кожного облікового запису може бути проблематичним та вимагає використання надійних паролівних менеджерів, таких як KeePass чи LastPass.

- Можливість втрати пароля: якщо ви забули свій сильний пароль, відновлення доступу до вашого облікового запису може бути вкрай складним або навіть неможливим.

2.2.2 Двофакторна аутентифікація – це процес підтвердження ідентичності користувача за допомогою двох факторів, зазвичай чогось, що користувач знає (наприклад, пароль) та щось, що користувач має (наприклад, токен або мобільний пристрій) [17].

Переваги:

+ Зменшує ризик втрати даних: двофакторна аутентифікація допомагає зменшити ризик втрати даних, оскільки навіть якщо хакери зламають пароль, вони не зможуть отримати доступ до акаунту без другого фактора підтвердження ідентичності.

+ Підвищує безпеку: два фактори підтвердження ідентичності значно підвищують безпеку системи, оскільки для зловмисників важче зламати систему з двома факторами аутентифікації, ніж систему з одним фактором.

Недоліки:

- Складність використання: двофакторна аутентифікація може бути складною для використання, особливо для менш досвідчених користувачів.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				16
Змн.	Арк.	№ докум.	Підпис	Дата		

- Залежність від обладнання: двофакторна аутентифікація може потребувати додаткового обладнання, такого як токени або карти, що може бути незручним для користувачів.

2.2.3 Біометрична аутентифікація - це процес ідентифікації особи за допомогою її фізичних характеристик, таких як відбитки пальців, розпізнавання обличчя, сканування радужної оболонки ока тощо [12].

Переваги:

+ Легкість запам'ятовування: користувачі не потребують пам'ятати паролі або карти доступу.

+ Стійкість до взлому: біометрична аутентифікація дуже складна до підробки, оскільки фізичні характеристики користувача є унікальними.

Недоліки:

- Один з головних недоліків полягає в тому, що фізичні характеристики людини можуть змінюватися внаслідок захворювань, травм або дії відповідних процедур. Це може призвести до того, що користувач не зможе пройти процес біометричної аутентифікації.

- Вартість: така аутентифікація може бути досить дорогим методом, оскільки вона потребує коштовних пристроїв та обладнання, яке здатне зчитувати та обробляти біометричні дані.

2.2.4 Мультифакторна аутентифікація (MFA) - це процес перевірки ідентичності користувача з використанням двох або більше методів аутентифікації [10].

Переваги:

+ Надійність: зменшує ризик порушення безпеки, оскільки навіть якщо зломисник дізнається пароль, він все ще не зможе отримати доступ до системи, якщо потрібен другий фактор аутентифікації, такий як фізичний токен або відбиток пальця.

+ Відповідність вимогам безпеки: в деяких випадках MFA є обов'язковим для відповідності вимогам безпеки, таким як стандарти PCI DSS або HIPAA.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Недоліки:

- Вартість: використання MFA може бути дорожчим, оскільки вимагає придбання фізичних пристроїв або додаткового програмного забезпечення. Крім того, існує ймовірність технічних проблем, такі як неправильна робота фізичного пристрою або проблеми з мережевим зв'язком, що може створити перешкоди для користувача.

- Затримка: процес MFA може займати більше часу, особливо якщо користувач повинен ввести додатковий код або скористатися фізичним пристроєм.

2.2.5 Автоматична аутентифікація - це метод, який дозволяє автоматично ідентифікувати користувача на основі певних факторів, таких як його поведінка, голосові характеристики, місцезнаходження та інші.

Переваги:

+ Висока швидкість і зручність: користувачі можуть бути автоматично ідентифіковані без необхідності введення пароля або інших даних. Крім того, вона може відбуватися у фоновому режимі, не перериваючи роботу користувача.

+ Висока точність ідентифікації: такі фактори, як поведінка користувача, голосові характеристики, є складними для підробки або підміни.

Недоліки:

- Низький рівень захисту: автоматична аутентифікація може бути менш безпечною, ніж інші методи, такі як двофакторна аутентифікація або біометрична ідентифікація.

- Проблеми з розпізнаванням: автоматична аутентифікація може мати проблеми з розпізнаванням користувачів, які мають фізичні обмеження, наприклад, слабкий голос, хвороби або травми, що впливають на їх поведінку.

- Висока вартість: у порівнянні з іншими методами, такими як паролі або підписи, автоматична аутентифікація може бути дорожчою у розгортанні та підтримці.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				
Змн.	Арк.	№ докум.	Підпис	Дата		18

2.3. Аналіз вразливостей сучасних систем парольної аутентифікації

Підсумовуючи проаналізовані у даному розділі дані, можна зробити висновки, що кожен з методів сучасних систем парольної аутентифікації має свої переваги та недоліки. Також варто враховувати те, що жоден з методів не є універсальним та надійним на 100%. Кожна система повинна бути розглянута окремо, щоб створити найоптимальнішу комбінацію методів аутентифікації [7].

В цілому, можна виділити такі основні вразливості сучасних систем парольної аутентифікації [13]:

- Паролі низької складності, які можуть бути легко зламані, такі як ‘password’, ‘123456’, ‘qwerty’, паролі що містять особисту інформацію про користувача (ім’я, пам’ятні дати чи місця, домашніх тварин) тощо.
- Використання одного та того ж пароля на кількох ресурсах. Це збільшує ймовірність зламу більшої кількості систем, до яких користувач має доступ.
- Використання слабких алгоритмів хешування, які дозволяють виконувати атаки типу «веселкових» таблиць.
- Недостатня довжина паролів, яка забезпечується мінімальними вимогами до складності пароля.
- Використання публічних мереж, таких як Wi-Fi, без шифрування трафіку, що може призвести до перехоплення пароля.
- Вразливість користувачів до соціального інжинірингу, який може використовуватися для отримання доступу до паролів користувачів.
- Відкритий доступ до бази даних з паролями, що забезпечує можливість виконання атак типу грубої сили та атак з використанням словників.
- Використання ненадійних технологій зберігання та передачі паролів, які можуть бути уражені атаками на середовище.

Висновки до другого розділу

Отже, у даному розділі було виконано огляд сучасних методів парольної аутентифікації, їх переваги та недоліки, та проаналізовано основні їх вразливості.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				
Змн.	Арк.	№ докум.	Підпис	Дата		19

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ОСНОВНИХ ПРОГРАМНИХ ЗАСОБІВ, ЩО ВИКОРИСТОВУЮТЬСЯ У СИСТЕМАХ ПАРОЛЬНИХ АУТЕНТИФІКАЦІЙ

3.1. Огляд програмних інструментів для зламу паролів

Для того, щоб розробити якісну парольну політику та рекомендації щодо зменшення вразливостей систем парольних аутентифікації, необхідно дослідити основні інструменти, що використовуються для зламу паролів. Це потрібно для того, щоб розуміти на які саме вразливості направлені такі атаки та яким чином можна мінімізувати ймовірність їх виконання.

Серед найпопулярніших програмних засобів для зламу паролів можна навести такі: John the Ripper, Hashcat, Hydra, Medusa, Cain and Abel, Aircrack-ng. Розглянемо детальніше деякі з них.

3.1.1 John the Ripper

John the Ripper - це інструмент з відкритим вихідним кодом для перевірки безпеки паролів і відновлення паролів, доступний для багатьох операційних систем. Має наступний функціонал [14]:

- Брутфорс атаки;
- Словникові атаки: використовує заготовлені словники більше ніж на 20ти мовах світу з можливістю використання власних словників
- Розподілені атаки: John the Ripper має можливість розподіленого обчислення, коли кілька комп'ютерів працюють разом для швидкого взлому пароля.
- Підтримка різних форматів хешів: John the Ripper може працювати з різними форматами хешів паролів, включаючи MD5, MD4, SHA1, SHA-256, SHA-512.
- Паралельне обчислення: Програма може використовувати мультипотоківість та розподілити обчислення на кілька ядер процесора, що дозволяє швидше зламувати паролі.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				20
Змн.	Арк.	№ докум.	Підпис	Дата		

– Використовується також для аналізу вразливостей систем.

Для використання застосунку, необхідно зробити копію файлу паролів:

```
umask 077  
unshadow /etc/passwd /etc/shadow > mypasswd
```

Для зламу паролів використовується команда ‘john’:

```
john mypasswd
```

Для перегляду зламаних паролів використовується команда:

```
john --show mypasswd
```

Також можна використовувати словники, встановлювати додаткові правила для зламу (такі як довжина паролю або тип хешування):

```
john --wordlist=all.lst --rules --stdout=8 | unique mangled8.lst  
john --wordlist=mangled8.lst mypasswd
```

Переглянемо роботу застосунку [14] та проведемо дослідження як довжина паролю впливає на час його зламу. Для цього використаємо віртуальну машину, що працює на дистрибутиві Linux, а саме – Ubuntu 20.04 LTS. Створимо декілька користувачів та для кожного створимо паролі. Для більшості користувачів використаємо просто паролі, такі як ‘admin’, ‘qwerty’, ‘123456’ та такі, що відповідають імені користувача (‘test2’ і ‘test3’). Для останнього юзера використаємо довгий пароль з використанням великої літери та спеціального символу – ‘longP@assword’:

```
student@student-VirtualBox:~$ sudo useradd test1  
student@student-VirtualBox:~$ sudo useradd test2  
student@student-VirtualBox:~$ sudo useradd test3  
student@student-VirtualBox:~$ sudo useradd test4  
student@student-VirtualBox:~$ sudo useradd test5  
student@student-VirtualBox:~$ sudo useradd test6  
student@student-VirtualBox:~$ sudo passwd test1  
Новий пароль :  
Повторіть новий пароль :  
passwd: пароль було успішно змінено  
student@student-VirtualBox:~$ sudo passwd test2  
Новий пароль :  
Повторіть новий пароль :  
passwd: пароль було успішно змінено  
student@student-VirtualBox:~$ sudo passwd test3  
Новий пароль :  
Повторіть новий пароль :  
passwd: пароль було успішно змінено  
student@student-VirtualBox:~$ sudo passwd test4  
Новий пароль :  
Повторіть новий пароль :  
passwd: пароль було успішно змінено  
student@student-VirtualBox:~$ sudo passwd test5  
Новий пароль :  
Повторіть новий пароль :  
passwd: пароль було успішно змінено  
student@student-VirtualBox:~$ sudo passwd test6  
Новий пароль :  
Повторіть новий пароль :  
passwd: пароль було успішно змінено  
student@student-VirtualBox:~$ unshadow /etc/passwd /etc/shadow > mypasswd
```

Рис.3.1. Створення тестових користувачів

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
–		Байлюк С.М				21
Змн.	Арк.	№ докум.	Підпис	Дата		

Після цього, встановимо John the Ripper на робочу станцію, проведемо відповідне налаштування та спробуємо зламати паролі користувачів:

```

student@student-VirtualBox:~$ sudo unshadow /etc/passwd /etc/shadow > m
ypasswd
student@student-VirtualBox:~$ johnsudo john mypasswd
johnsudo: команду не знайдено
student@student-VirtualBox:~$ sudo john mypasswd
Created directory: /root/.john
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3
) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
test2                (test2)
test3                (test3)
qwerty               (test1)
123456               (test5)
111111               (student)
admin                (test4)

```

Рис.3.2. Використання John the Ripper для зламу паролів користувачів

В результаті дослідження, усі паролі крім останнього були зламані менше ніж за 1 секунду. Пароль ‘longP@assword’ не був зламаний більш ніж за 7 годин. Використовуючи відкрите джерело <https://www.security.org/how-secure-is-my-password/> , маємо приблизний час зламу 84 тисячі років. Для порівняння, така сама комбінація без спеціального символу (‘longPassword’) буде зламана приблизно за триста років, а тільки з маленьких літер (‘longpassword’) – лише за 3 тижні.

Таким чином можна зробити висновок, що чим довший та оригінальніший пароль (велика кількість символів, використання спеціальних символів, комбінація великих та маленьких літер), тим складніше комп’ютеру його зламати.

3.1.2 Hydra

Hydra є популярним програмним інструментом для виконання атаки перебору паролів або атаки на доступ до системи з використанням підбору паролів. Основним функціоналом Hydra є [15]:

- Підтримка протоколів: Hydra підтримує багато різних мережеских протоколів, таких як HTTP, HTTPS, FTP, SMTP, POP3, IMAP, Telnet, SSH та інші. Це дозволяє використовувати Hydra для зламу паролів у різних типах систем.

- Багатопотоковість: Hydra може працювати з кількома потоками, що дозволяє виконувати паралельні спроби входу з різних обчислювальних вузлів.
- Можливість використання словникових файлів.
- Конфігураційні файли: Hydra дозволяє використовувати конфігураційні файли, щоб зручно налаштувати параметри атаки. Це включає в себе налаштування протоколів, адреси веб-сайту або сервера, порти, тип аутентифікації, параметри перебору та інші параметри.
- Гнучкість параметрів: Hydra надає широкий набір параметрів, що дозволяють налаштовувати атаку. Це включає в себе можливість вказати користувачів та паролі вручну, використовувати проксі-сервери, обмеження швидкості атаки, встановлення таймаутів, використання проксі-списків і багато іншого.
- Збереження результатів: Hydra може зберігати результати атаки, включаючи вдалі спроби входу, виключені акаунти або знайдені паролі. Це дає змогу аналізувати результати та оцінювати ефективність атаки.

Застосунок Hydra встановлений за замовчуванням на дистрибутиві Kali Linux, але може використовуватись і на інших дистрибутивах. Для огляду можливостей застосунку теж буде використано віртуальну машину на базі Kali Linux:

```

kali@kali: ~
File Actions Edit View Help

Options:
-R      restore a previous aborted/crashed session
-I      ignore an existing restore file (don't wait 10 seconds)
-S      perform an SSL connect
-s PORT if the service is on a different default port, define it here
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-x MIN:MAX:CHARSET password bruteforce generation, type "-x -h" to get help
-y      disable use of symbols in bruteforce, see above
-r      rainy mode for password generation (-x)
-e nsr  try "n" null password, "s" login as pass and/or "r" reversed login
  
```

Рис.3.3. Огляд функціоналу застосунку Hydra

```

kali@kali: ~
File Actions Edit View Help
n
-u --loop loop around users, not passwords (effective! implied with -x)
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
t
-o FILE write found login/password pairs to FILE instead of stdout
-b FORMAT specify the format for the -o FILE: text(default), json, jsonv1
-f / -F exit when a login/pass pair is found (-M: -f per host, -F global)
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-T TASKS run TASKS connects in parallel overall (for -M, default: 64)
-w / -W TIME wait time for a response (32) / between connects per thread (
0)
-c TIME wait time per login attempt over all threads (enforces -t 1)
-4 / -6 use IPv4 (default) / IPv6 addresses (put always in [] also in -M)
-v / -V / -d verbose mode / show login+pass for each attempt / debug mode
-O use old SSL v2 and v3
-K do not redo failed attempts (good for -M mass scanning)
-q do not print messages about connection errors
-U service module usage details
-m OPT options specific for a module, see -U output for information
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help
)

Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s]
http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum
icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql
mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radm
in2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum sn

```

Рис.3.4. Огляд функціоналу застосунку Hydra (продовження)

Для виконання атаки, підготуємо словник паролів (розархівуємо потрібний файл). Використаємо один з відомих словників – rockyou. Цей словник за замовчуванням встановлений на Kali Linux та містить понад 14 мільйонів популярних паролів:

```

(root@kali)-[/usr/share/wordlists]
# gzip -d rockyou.txt.gz

(root@kali)-[/usr/share/wordlists]
# ls -l
total 136644
lrwxrwxrwx 1 root root      25 Dec  2  2021 dirb → /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root      30 Dec  2  2021 dirbuster → /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root      41 Dec  2  2021 fasttrack.txt → /usr/share/set/src/fasttrack/word
list.txt
lrwxrwxrwx 1 root root      45 Dec  2  2021 fern-wifi → /usr/share/fern-wifi-cracker/extras/w
ordlists
lrwxrwxrwx 1 root root      46 Dec  2  2021 metasploit → /usr/share/metasploit-framework/data
/wordlists
lrwxrwxrwx 1 root root      41 Dec  2  2021 nmap.lst → /usr/share/nmap/nselib/data/passwords.
lst
-rw-r--r-- 1 root root 139921507 Jul 17  2019 rockyou.txt
lrwxrwxrwx 1 root root      25 Dec  2  2021 wfuzz → /usr/share/wfuzz/wordlist

```

Рис.3.5. Підготовка словника паролів до використання

Для початку протестуємо роботу брутфорсу на локальному хості. Припустимо що ми знаємо логін, під яким можна зайти у систему по SSH з'єднанню. Спробуємо підібрати до логіну пароль зі словника:

```
(root@kali)-[~]
# hydra -V -f -l u0_a150 -P /usr/share/wordlists/rockyou.txt localhost -s 22 ssh 255 x 1
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 17:47:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduc
e the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a p
revious session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
25 tries per task
[DATA] attacking ssh://localhost:22/
[ATTEMPT] target localhost - login "u0_a150" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "iloveyou" - 5 of 14344399 [child 4] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "rockyou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "nicole" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "daniel" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "babygirl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target localhost - login "u0_a150" - pass "jessica" - 16 of 14344399 [child 15] (0/0)
```

Рис.3.6. Брутфорс SSH з'єднання локального хосту

Спробуємо виконати атаку на інший сервер, що знаходиться у тій самій мережі. Візьмемо налаштований сервер, що працює на базі Ubuntu, дозволимо на ньому під'єднання по SSH. Для економії часу, створимо на сервері тестового юзера з нескладним паролем (password123), дізнаємось IP адресу мережевого адаптера на сервері:

```
kb192-16@srv-ubuntu-shevchyk:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6e:d4:0b brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.83/24 brd 192.168.50.255 scope global dynamic enp0s3
        valid_lft 60843sec preferred_lft 60843sec
    inet6 fe80::a00:27ff:fe6e:d40b/64 scope link
        valid_lft forever preferred_lft forever
kb192-16@srv-ubuntu-shevchyk:~$
```

Рис.3.7. Інформація про мережевий адаптер серверу

Тепер, знаючи що IP адреса – 192.168.50.83 а логін користувача - testuser, спробуємо підібрати дані для входу на сервер використовуючи можливості Hydra:

```
(root@kali)-[/home/kali]
# hydra -l testuser -P /usr/share/wordlists/rockyou.txt 192.168.50.83 ssh -t 4
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 18:36:35
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a p
revious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~358610
0 tries per task
[DATA] attacking ssh://192.168.50.83:22/
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 14344359 to do in 5976:49h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 14344315 to do in 8538:17h, 4 active
[STATUS] 26.29 tries/min, 184 tries in 00:07h, 14344215 to do in 9095:04h, 4 active
[STATUS] 26.80 tries/min, 402 tries in 00:15h, 14343997 to do in 8920:24h, 4 active
[STATUS] 26.10 tries/min, 809 tries in 00:31h, 14343590 to do in 9160:31h, 4 active
[STATUS] 26.04 tries/min, 1224 tries in 00:47h, 14343175 to do in 9179:20h, 4 active
[22][ssh] host: 192.168.50.83 login: testuser password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 19:30:09
```

Рис.3.8. Брутфорс SSH з'єднання

Бачимо, що атака була вдалою, пароль для входу був підібраний приблизно за 50 хвилин. Після цього, можна під'єднатися до серверу використовуючи SSH та підібрані дані:

```
(root@kali)-[/home/kali]
# ssh testuser@192.168.50.83 -p 22
testuser@192.168.50.83's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-144-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri 09 Jun 2023 01:11:08 PM UTC

System load:      0.07                Processes:         125
Usage of /home:   0.0% of 1.90GB      Users logged in:   1
Memory usage:     25%                IPv4 address for enp0s3: 192.168.50.83
Swap usage:       0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

91 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
```

Рис.3.9. Вхід на сервер зі зламаними даними

Таким чином, було ще раз підтверджено важливість створення надійних паролів, а також забезпечення захищеного з'єднання, бажано використовуючи не стандартний порт.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				26
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2. Огляд парольних менеджерів

3.2.1 Bitwarden

Bitwarden - це парольний менеджер, який забезпечує збереження та управління паролями. Основний функціонал Bitwarden включає [21]:

- Збереження паролів: Bitwarden дозволяє зберігати паролі у захищеній хмарній базі даних Microsoft Azure Cloud, що керується командою Microsoft.

- Генерація сильних паролів: має вбудований генератор сильних паролів, який допомагає створювати випадкові та складні паролі. Також можливо налаштувати параметри генерації, такі як довжина та використання різних символів.

- Автозаповнення паролів: дозволяє автоматично вводити паролі на веб-сайтах та в програмах.

- Синхронізація між пристроями: дозволяє синхронізувати базу даних паролів між різними пристроями.

- Керування пароліями: є можливість безпечно ділитися пароліями з іншими користувачами Bitwarden, що дозволяє зручно керувати спільним доступом до облікових записів.

- Групування та організація: Bitwarden дозволяє створювати категорії та папки для організації паролів, що допомагає їх структурувати.

- Аудит безпеки: парольний менеджер надає можливість перевірити безпеку паролів, виявити слабкі або повторювані паролі, і рекомендує створювати сильні паролі.

- Інтеграція з браузером та додатками: Bitwarden працює з багатьма популярними веб-браузерами і має додатки для різних платформ, що дозволяє зручно використовувати його на різних пристроях.

Розглянемо детально особливості використання Bitwarden у якості парольного менеджера, а саме використання розширення для браузера (також є можливість використання застосунку). Створимо акаунт на офіційному сайті, звернувши особливу увагу на вимоги до майстер-паролю:

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				27
Змн.	Арк.	№ докум.	Підпис	Дата		

Create an account

email address (Necessarily)
kb192_shda@student.ztu.edu.ua
The email address will be used to sign in.

Name
Daryna
What is your name?

Master password (Necessarily)
.....
Important: Your master password cannot be recovered if you forget it! Minimum characters: 12

Weak

Re-enter the master password (Necessarily)
.....

Master password hint
.....
The master password hint can help you remember it.

☒ Check known data breaches for this password

☐ By checking this box, you agree to the following:
[Terms of Use](#), [Privacy Policy](#)

Рис.3.10. Створення акаунту на Bitwarden

Додамо парольну карту для входу на освітній портал:

NEW ELEMENT

What type of element is this?
Login

Name
ztu.edu.ua

Folder

Username
kb192_shda

Password
.....

Authenticator Key (TOTP)
.....

TYPE 1
https://learn.ztu.edu.ua/login/index.php

Match detection
Default discovery method

+ New URI

Notes

Рис.3.11. Додавання парольної карти

Додамо ще декілька парольних карток та розглянемо основні можливості:

Vaults Send Tools Reports

FILTERS

Search folder

All vaults

+ New item

GO PREMIUM

Upgrade your account to a Premium membership and unlock some great additional features.

Go Premium

All items

My vault

New organization

Search folder

All vaults

Me

Me

Me

Рис.3.12. Збережені парольні карти

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
		Байлюк С.М				28
Змн.	Арк.	№ докум.	Підпис	Дата		

Можемо побачити, що є можливість створювати парольні карти, де вказувати логін, пароль, та посилання на сторінці, де відбуватиметься процес авторизації. Крім цього, можна зберігати замітки у захищеному вигляді, дані карти для оплати у Інтернеті, сортувати збережену інформацію шляхом групування у різні теки.

Для більшої зручності використання, встановимо розширення для браузера:

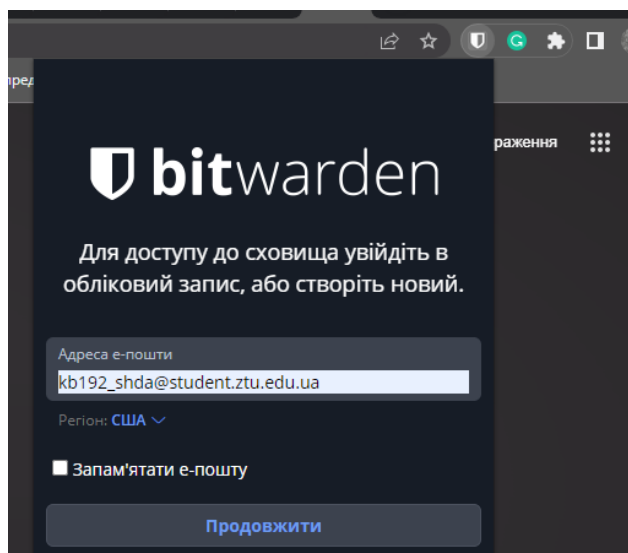


Рис.3.13. Використання розширення Bitwarden для браузера

Переглянемо додаткові налаштування розширення:

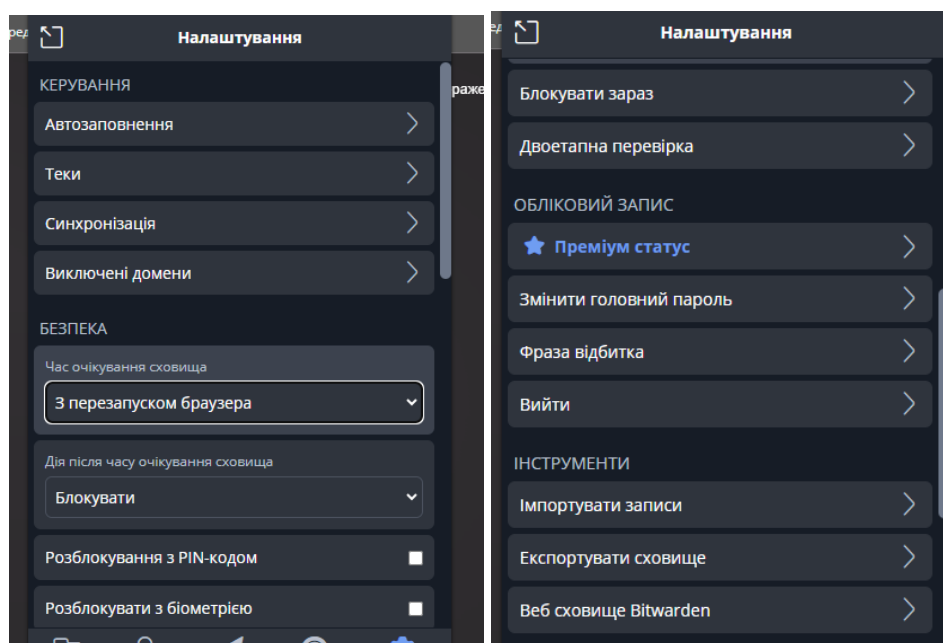


Рис.3.14. Налаштування розширення Bitwarden для браузера

Бачимо, що для додаткової безпеки можна налаштувати блокування вікна розширення через певний час використання, також можна використовувати різні

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				29
Змн.	Арк.	№ докум.	Підпис	Дата		

методи додаткової аутентифікації, такі як PIN-код, біометрія, двофакторна авторизація. Присутні декілька варіантів автозаповнення – вимкнення функції (можна виконувати вхід за допомогою натискання на парольну карту у вікні розширення), автоматичне автозаповнення при завантаженні сторінки (не рекомендовано використовувати, оскільки можливе некоректне відображення даних та введення даних входу у невідповідні поля, якщо такі присутні на сторінці) та автозаповнення шляхом комбінації клавіш CTRL+Shift+L. При спробі входу на сторінку сайту, що присутній у одній з наявних парольних карт, розширення пропонує використати необхідні дані:

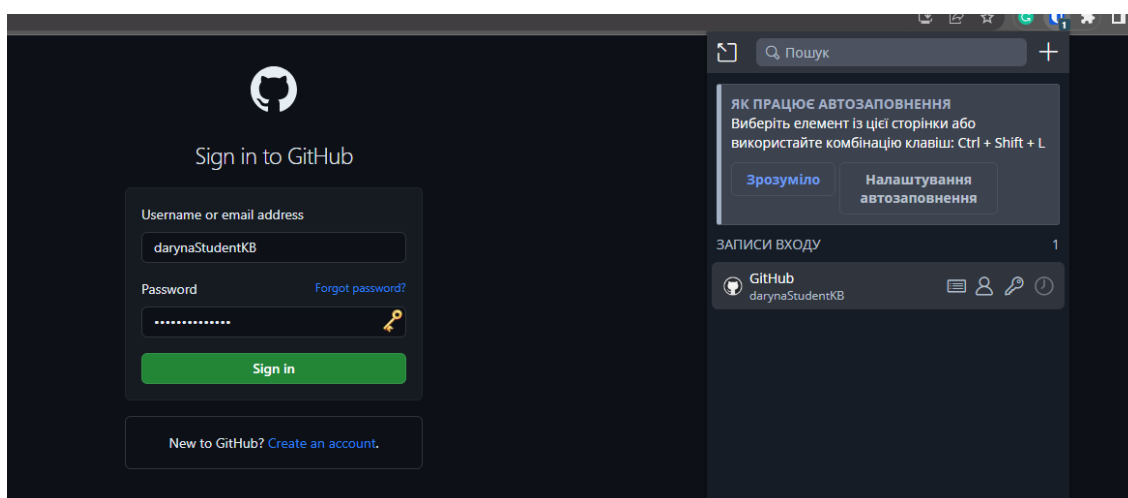


Рис.3.15. Автозаповнення даних для входу

В цілому, парольний менеджер Bitwarden є досить зручним у використанні, забезпечує високий рівень захищеності процесу авторизації й позбавляє необхідності запам'ятовувати велику кількість паролів. Проте варто відмітити, що парольний менеджер все ж має певні недоліки:

- Залежність від хмарного сервісу: у разі використання Bitwarden у хмарному середовищі, з'являється залежність від доступу до Інтернету та надійності хмарного сервісу. Якщо сервіс недоступний або виникають проблеми з хмарним сервером, отримання доступу до паролів буде ускладнене.

- Відповідальність за майстер-пароль: майстер-пароль відіграє вирішальну роль у безпеці бази даних паролів. Він має високі вимоги до рівня складності щоб зменшити ймовірність його взлому, адже у такому разі (при відсутності додаткових методів автентифікації), це означатиме отримання доступу до усіх

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				30
Змн.	Арк.	№ докум.	Підпис	Дата		

даних для авторизації, якими володіє користувач. Крім того, у разі втрати майстер-паролю відновити його неможливо, результатом чого буде втрата доступу до усіх збережених на акаунті даних.

3.2.2 KeePass

KeePass - це парольний менеджер, який забезпечує зберігання та управління паролями. Основний функціонал KeePass включає [5]:

- Збереження паролів;
- Генерація сильних паролів: крім зберігання паролів, KeePass також надає можливість генерувати сильні, випадкові паролі;
- Категорії та організація: є можливість створювати категорії та папки для організації паролів;
- Автозаповнення паролів: KeePass має функцію автозаповнення, яка дозволяє автоматично вводити ваші паролі на веб-сайтах або в програмах;
- Інтеграція з веб-браузерами: KeePass може інтегруватися з різними веб-браузерами і автоматично заповнювати паролі на веб-сторінках;
- Резервне копіювання та відновлення: KeePass надає можливість резервувати свою базу даних паролів і відновлювати її у разі втрати або пошкодження. Це гарантує, що паролі завжди будуть безпечними та доступними.
- Розширення та налаштування: KeePass має велику кількість розширень та налаштувань, що забезпечує гнучкість налаштувань його під свої потреби та розширення його функціоналу.

Навідміну від Bitwarden, де паролі зберігаються у хмарному сховищі, для користування KeePass необхідно створити локальний файл бази даних, де будуть зберігатися усі паролі. База даних захищається майстер-паролем, за збереження його несе відповідальність власник-користувач базою. Відповідно, майстер-пароль потребує дотримання певних вимог, такі як довжина паролу, наявність спеціальних символів, довжини тощо.

Оглянемо функціонал парольного менеджера на практиці. Для початку, створимо нову базу даних та майстер-пароль до неї:

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				31
Змн.	Арк.	№ докум.	Підпис	Дата		

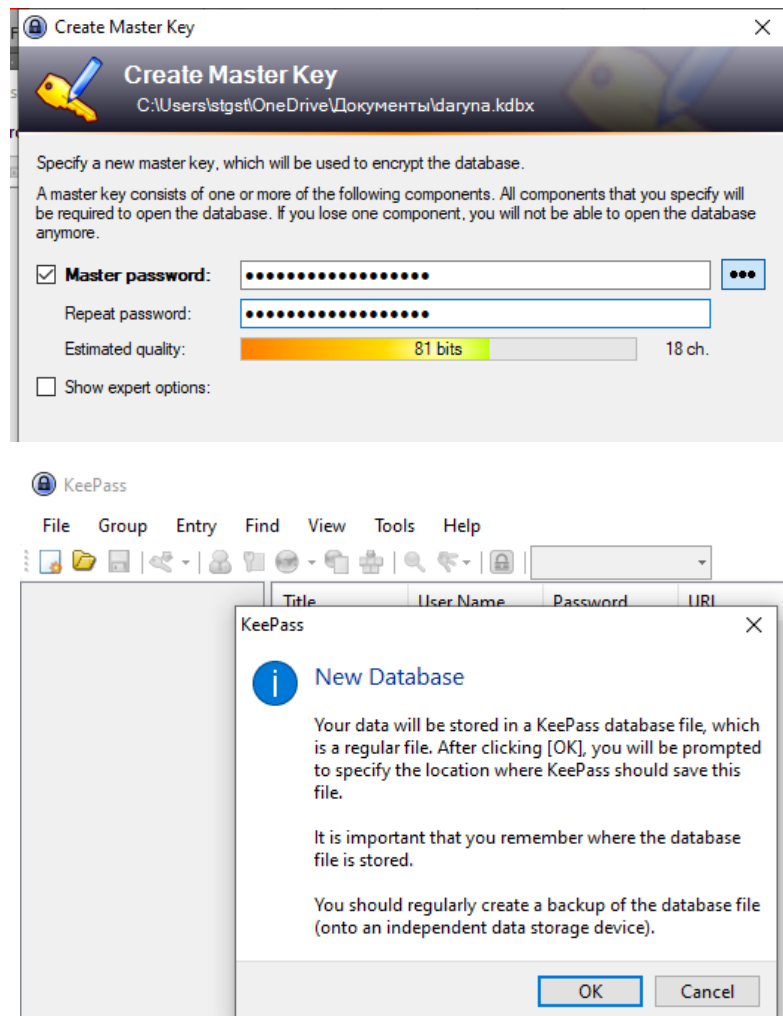


Рис.3.16 Створення бази даних та майстер-пароллю

Оглянемо основний функціонал:

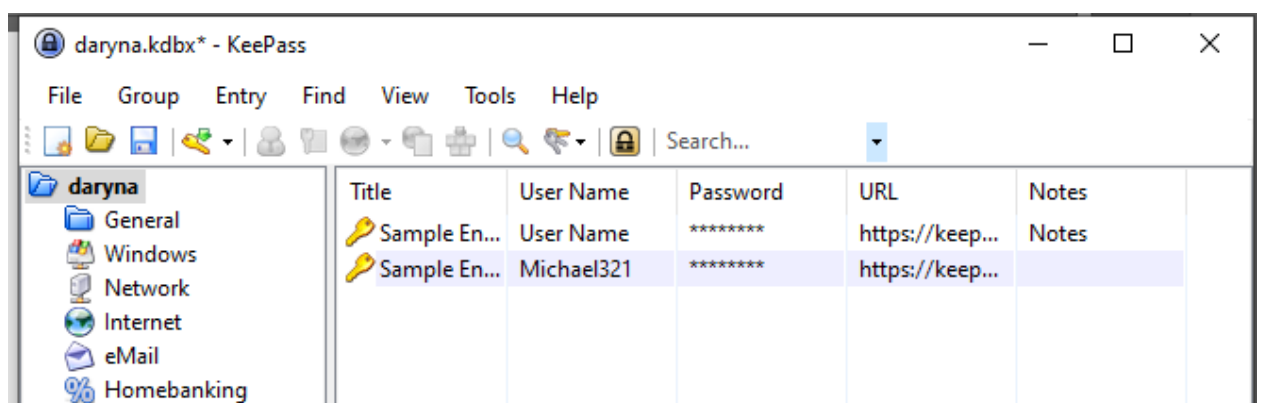


Рис.3.17 Огляд функціоналу KeePass

Бачимо, що є можливість додавати пароль карти, додатково прописувати захищену замітку. Також є можливість групувати пароль карти в різні теки для кращої організації. Спробуємо створити паролську карту та розглянемо надані можливості:

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				32
Змн.	Арк.	№ докум.	Підпис	Дата		

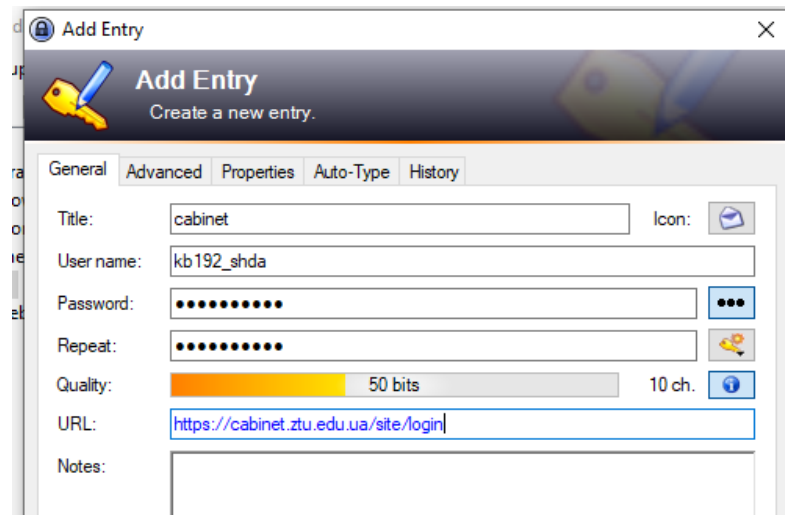


Рис.3.18 Створення паролної карти в KeePass

Бачимо, що створення паролної карти подібне до аналогічного у Bitwarden. Корисною додатковою функцією є аналіз якості створеного паролю та можливість згенерувати надійний пароль згідно заданих вимог. Розглянемо налаштування безпеки:

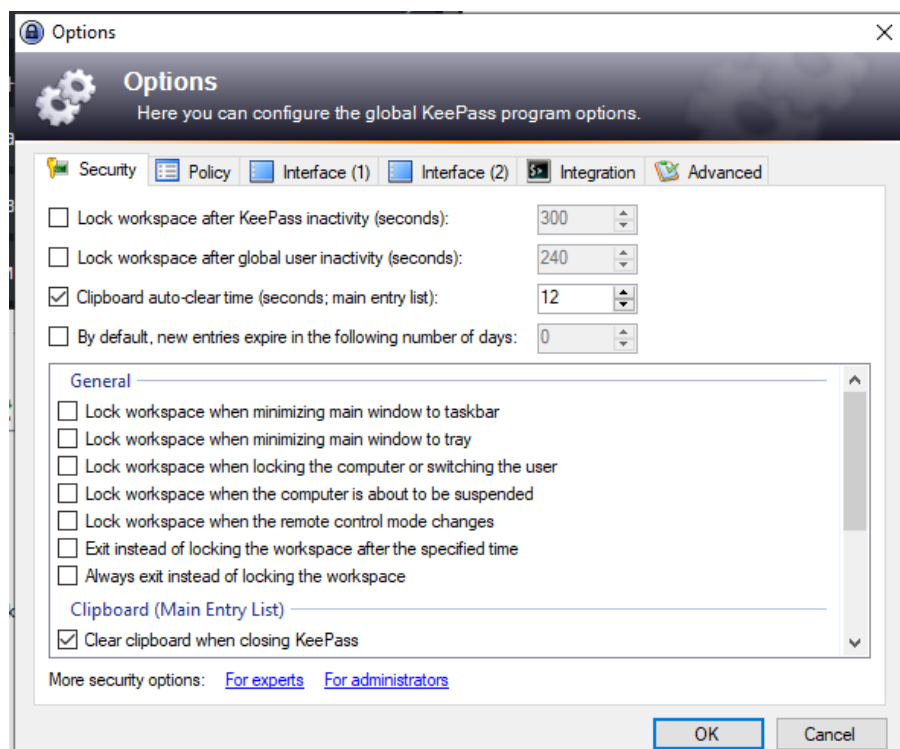


Рис.3.19 Налаштування безпеки KeePass

Як бачимо, KeePass надає можливість блокування активного вікна за різних умов та для різних користувачів, налаштувати нагадування про зміни паролю через певний проміжок часу тощо. На відміну від Bitwarden, для можливості використання автозаповнення даних у браузері, а не копіювання їх з вікна

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				33
Змн.	Арк.	№ докум.	Підпис	Дата		

парольного менеджера вручну, необхідно здійснити додаткові налаштування. Для початку, потрібно завантажити плагін «KeePassHttp» для застосунку KeePass через офіційний репозиторій на GitHub та встановити його (у даному прикладі це було виконано з використанням Chocolatey за допомогою команди ‘choco install keepass-keepasshttp’) [16]:

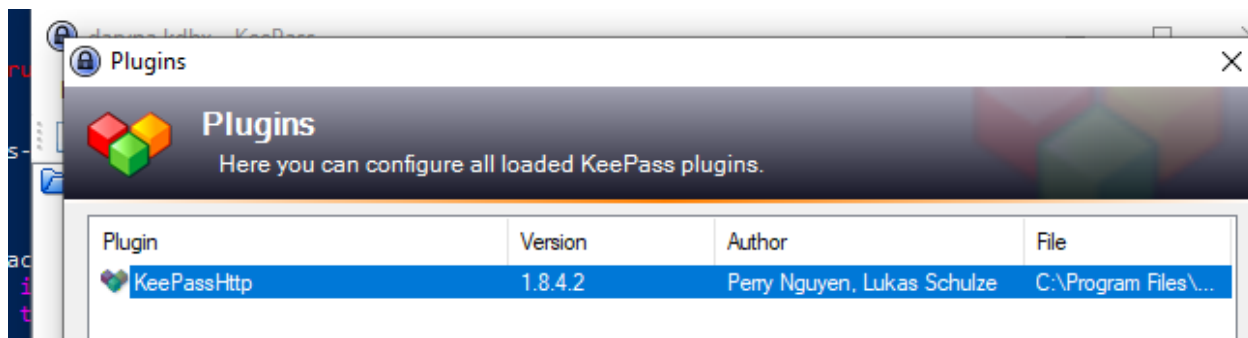


Рис.3.20 Встановлення плагіну «KeePassHttp»

Після цього, завантажимо розширення KeePassHttp-Connector для браузера. Подальші додаткові налаштування не обов’язкові, достатньо натиснути кнопку «Connect» у розширенні і відбудеться спроба з’єднання з базою даних на комп’ютері (база при цьому має бути відкрита то розблокована паролем):

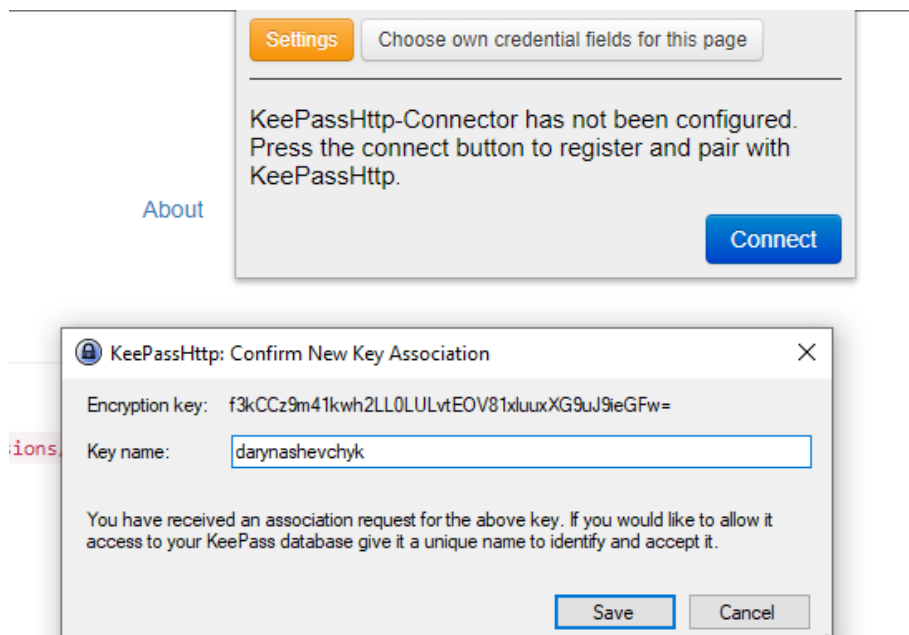


Рис.3.21 З’єднання розширення для браузера та локальної бази даних паролів

Після цього, у KeePass створиться новий запис з інформацією про ключ з’єднання, а розширення для браузера відображатиме назву ключа поточного з’єднання:

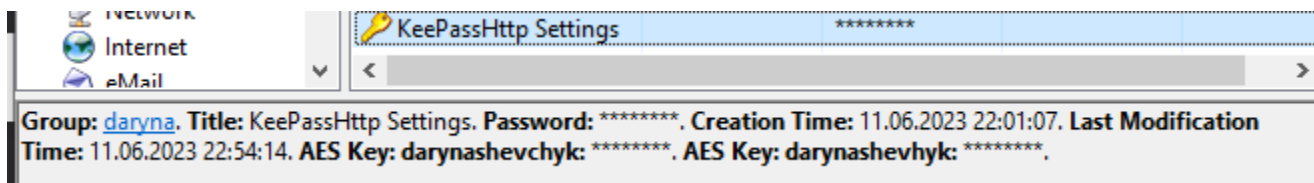


Рис.3.22 Інформація про ключ з'єднання у KeePass

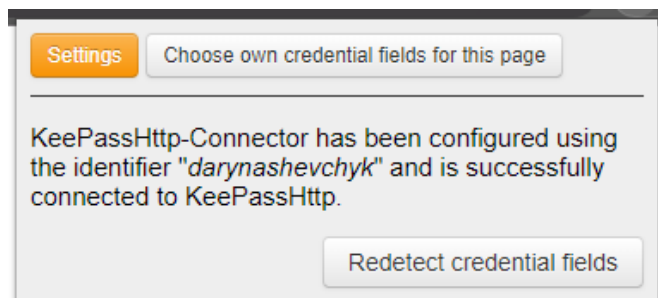


Рис.3.23 Інформація про ключ з'єднання у розширенні для браузера

Виконавши налаштування розширення для браузера то встановивши його з'єднання з базою даних паролів, парольний менеджер пропонуватиме використати дані для входу збережених парольних карт:

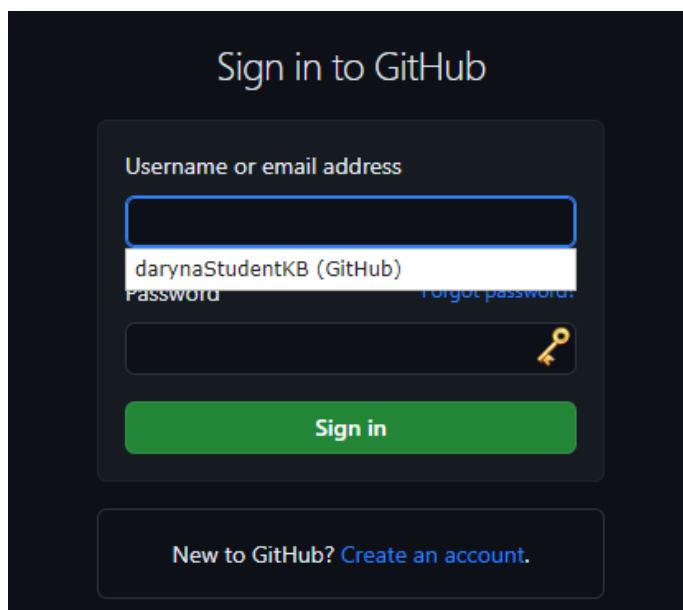


Рис.3.24 Створення тестових користувачів

Протягом використання розширення для браузера, передача даних між застосунком та власне розширенням шляхом симетричного шифрування AES у режимі CBC, повідомлення шифрується з використанням ключа довжиною 256 біт. За замовчуванням, комунікація відбувається через `http://localhost` на порт 19455, що прослуховується розширенням. Проте для забезпечення більшого рівня захищеності, є можливість налаштувати власний порт для прослуховування. Для

цього необхідно встановити власний порт у застосунку та налаштуваннях розширення:

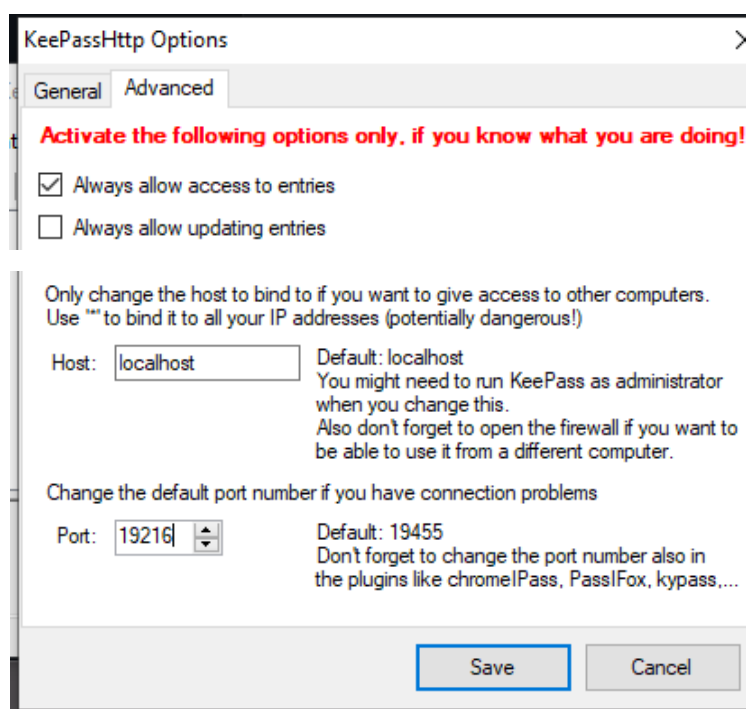


Рис.3.25 Налаштування порту у застосунку KeePass

Hostname:

localhost Save

Default: localhost

Port:

19216 Save

Change the port if you have trouble with running KeePassHTTP on the default port.
You have to set the same port number in KeePassHTTP options!
Default: 19455

☒ **Supress warnings and errors via alert.**
Disables communicating errors and warnings via JavaScript alert.

☐ **Respect maxlength="" attribute on inputs.**
Limit the field filled in to the maximum number of characters allowed by maxlength=
There is a possibility of this causing issues with sites that have decreased this value
and the password stored in keepass itself is longer than maxlength.

Рис.3.26 Налаштування порту у розширення для браузера

Це є дуже корисною опцією для великих компаній, що дає можливість налаштувати власний сервер та створити окремі бази даних для кожного працівника, задавши для кожного певний ідентифікатор (наприклад ID) та встановлення з'єднання кожного працівника на окремий порт, що дає можливість

розмежування доступу та мінімізації негативних наслідків у разі зламу бази окремого користувача.

Попри все вище описане, парольний менеджер KeePass має певні недоліки:

- Вимагає уваги до майстер-пароля: втрата майстер-пароля може призвести до неможливості отримати доступ до всіх збережених паролів. Тому необхідно стежити за безпекою майстер-пароля і регулярно робити його резервну копію.

- Необхідність ручного введення майстер-пароля: при кожному запуску KeePass вимагає введення майстер-пароля вручну, що певною мірою зменшує захищеність даних для входу у разі використання зловмисником засобів захоплення клавіатури (keylogger);

- Вимога до самостійного керування: KeePass не синхронізується автоматично з іншими пристроями, тому потрібно самостійно забезпечити синхронізацію бази даних паролів між пристроями. Крім того, на відміну від Bitwarden, KeePass вимагає більше технічних знань для його базового налаштування.

Таким чином, можна підсумувати, що як Bitwarden, так і KeePass, мають певні переваги та недоліки. Кожна компанія має приймати рішення щодо вибору парольного менеджера в залежності від своїх потреб.

3.3. Двофакторна аутентифікація

Як вже було згадано раніше у цій роботі, двофакторна аутентифікація має на увазі підтвердження ідентичності користувача з використанням додаткового фактору. Найбільш популярним є використання двофакторної аутентифікації з використанням шестизначного коду, що надсилається на пошту користувача або генерується у мобільному додатку.

Використання двофакторної аутентифікації шляхом надсилання коду на пошту є меншим надійним, оскільки існує більша ймовірність зламу пошти для отримання коду, оскільки такий код діє триваліший час ніж згенерований код у мобільному додатку.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк Є.М				37
Змн.	Арк.	№ докум.	Підпис	Дата		

Найбільш популярними мобільними застосунками для двофакторної аутентифікації є Google Authenticator [22] та Microsoft Authenticator [23]. На жаль, продемонструвати роботу застосунків на власних паролях немає можливості, оскільки вони є захищеними й зробити знімок екрану під час їх роботи неможливо. Базовий функціонал застосунків однаковий – на обраному сайті, що підтримує двофакторну аутентифікацію, необхідно згенерувати унікальний ідентифікатор або QR-код, після чого зчитати його у мобільному застосунку. Після цього, застосунок генеруватиме одноразовий шестизначний код на основі TOTP (Time-based One-Time Password), що є дійсним 30 секунд та вводиться під час входу на сайт у разі успішно пройденого першого етапу аутентифікації (валідні логін та пароль). Виглядають ці застосунки таким чином (взято з відкритого джерела – сторінок застосунків у Google Play Store):

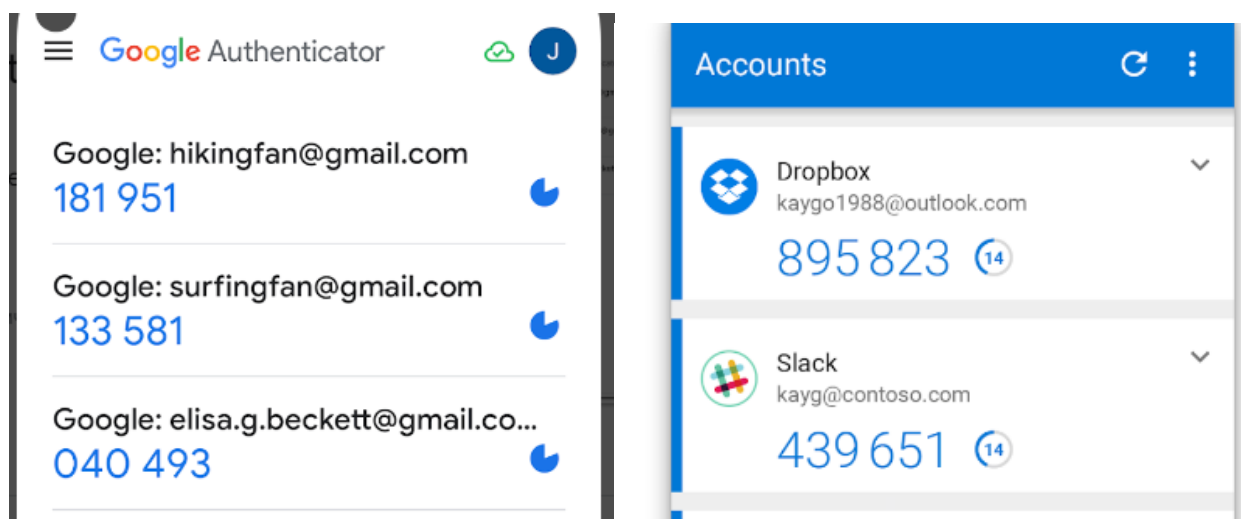


Рис.3.27 Вигляд Google Authenticator та Microsoft Authenticator

Ще одним популярним засобом двофакторної аутентифікації, принцип якого відрізняється від вище згаданих рішень від Google та Microsoft, є YubiKey. Це фізичний апаратний пристрій, розроблений компанією Yubico [24], який забезпечує безпеку та багатофакторну аутентифікацію. Він є одним з найпопулярніших та надійних засобів для захисту цифрових ідентифікаторів, аутентифікації користувачів та підтвердження транзакцій. Даний ідентифікатор є досить коштовним і виглядає наступним чином (ключ безпеки Yubikey 5 NFC, ціна одного екземпляру близько 3400 гривень):

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				38
Змн.	Арк.	№ докум.	Підпис	Дата		



Рис.3.28 Ключ безпеки Yubikey 5 NFC

Проведемо детальне порівняння Google Authenticator, Microsoft Authenticator та Yubikey.

1) Функціонал:

- Google Authenticator: забезпечує генерацію одноразових паролів (ОТР) на основі Time-based One-Time Password (TOTP) для багатофакторної аутентифікації. Він може використовуватись з багатьма онлайн-сервісами, які підтримують TOTP.

- Microsoft Authenticator: надає генерацію одноразових паролів (ОТР) на основі TOTP. Додатково, він підтримує Push-сповіщення, що дозволяє підтверджувати вхід без необхідності введення пароля або ОТР. Також використовується для аутентифікації з обліковими записами Microsoft і іншими сервісами.

- YubiKey: фізичний апаратний пристрій, що генерує одноразові паролі, підтримка різних протоколів аутентифікації.

2) Кросплатформеність:

- Google Authenticator: доступний для Android і iOS пристроїв. Додаток можна синхронізувати між різними пристроями через QR-код або налаштування облікового запису Google.

- Microsoft Authenticator: підтримує як Android, так і iOS пристрої. Додаток також синхронізується між різними пристроями через налаштування облікового запису Microsoft.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
–		Байлюк Є.М				39
Змн.	Арк.	№ докум.	Підпис	Дата		

– YubiKey: сумісний з різними операційними системами, включаючи Windows, macOS, Linux, Android та iOS. Він підтримує браузери Chrome, Firefox, Safari та інші.

3) Додаткові функції:

– Google Authenticator: не має додаткових функцій, крім генерації одноразових паролів на основі TOTP.

– Microsoft Authenticator: підтримує Push-сповіщення для підтвердження входу без введення пароля або OTP. Також може використовуватися для входу в облікові записи Microsoft за допомогою біометричних даних.

– YubiKey: захист від фішингу, можливість підтвердження операцій, безпарольна аутентифікація, можливість шифрування.

4) Інтеграція зі службами:

– Google Authenticator: можна використовувати з будь-якими онлайн-сервісами, які підтримують TOTP.

– Microsoft Authenticator: широко використовується для входу в облікові записи Microsoft, включаючи Outlook, Office 365, OneDrive, Azure та інші.

– YubiKey: підтримується багатьма сервісами, що підтримують безпарольну аутентифікацію або U2F/FIDO2 протоколи.

5) Безпека:

– Google Authenticator: генерація OTP на пристрої, відсутність зв'язку з мережею, що підвищує безпеку.

– Microsoft Authenticator: генерація OTP на пристрої, відсутність зв'язку з мережею, можливість підтверджувати вхід за допомогою біометричних даних (залежно від пристрою).

– YubiKey: Фізична безпека (наявність унікального фізичного ключа), використання апаратного шифрування, захист від фішингу.

6) Налаштування:

– Google Authenticator: простий процес додавання облікових записів на основі QR-кодів.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
–		Байлюк С.М				40
Змн.	Арк.	№ докум.	Підпис	Дата		

– Microsoft Authenticator: простий процес додавання облікових записів на основі QR-кодів.

– YubiKey: необхідність налаштування у кожному сервісі, який підтримує YubiKey, шляхом реєстрації ключа.

7) Вартість:

– Google Authenticator: безкоштовний

– Microsoft Authenticator: безкоштовний.

– YubiKey: вартість залежить від моделі.

Враховуючи вказані критерії, кожен інструмент має свої особливості і підходить для різних вимог. Google Authenticator та Microsoft Authenticator є мобільними додатками, які зручно використовувати на смартфонах, тоді як YubiKey забезпечує фізичну безпеку та розширений функціонал. Вибір залежить від потреб у безпеці, зручності використання та підтримки потрібних протоколів.

Висновки до третього розділу

Отже, було коротко розглянуто основні приклади програмного забезпечення для зламу систем парольних аутентифікації, досліджено функціонали популярних парольних менеджерів та засобів двофакторної аутентифікації.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк Є.М				41
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 4. АНАЛІЗ ПРОВЕДЕНИХ ДОСЛІДЖЕНЬ ТА РОЗРОБКА ВИМОГ ДО ПАРОЛЬНИХ ПОЛІТИК

4.1. Вимоги до парольних політик

В даній роботі було розглянуто різні аспекти вразливостей систем парольних аутентифікацій та їх причини. Коротко підсумуємо виявлені вразливості:

- слабкі паролі;
- використання однофакторної аутентифікації;
- недостатнє приділення уваги до зберігання та передачі паролів і їх хешів;
- вплив соціальної інженерії;

Велику частину досліджених вразливостей можна мінімізувати приділивши достатньо уваги створенню коректної парольної політики [10].

Парольна політика - це набір правил та вимог, які встановлюються в організації для створення, збереження та використання паролів для захисту конфіденційної інформації та ресурсів. Ці правила можуть включати вимоги до довжини паролів, використання різних символів та чисел, зміни паролів через певний період часу, обмеження використання одного пароля на декілька ресурсів тощо. Парольна політика допомагає зменшити ризик несанкціонованого доступу до інформації та зберегти конфіденційність даних [7].

Парольні політики регулюються міжнародними стандартами [1]. Серед основних:

- ISO/IEC 27001: Information security management systems. Requirements - Системи менеджменту інформаційною безпекою. Вимоги.
- NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations. Контроль безпеки та конфіденційності для інформаційних систем і організацій.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				42
Змн.	Арк.	№ докум.	Підпис	Дата		

– PCI DSS: Payment Card Industry Data Security Standard. Сукупність вимог щодо забезпечення безпеки даних власників платіжних карток, які зберігаються, передаються та/або обробляються в інформаційній інфраструктурі організацій.

Враховуючи досліджені вразливості систем парольних аутентифікації, для їх зменшення парольні політики мають містити такі вимоги:

1. Довжина пароля: паролі мають містити принаймні 8, а краще хоча б 12 символів і не перевищувати 25 символів.

2. Складність пароля: паролі повинні містити комбінацію великих і малих літер, цифр і спеціальних символів таких як <*&(^%\$>!.>

3. Створення паролів: варто уникати онлайн генераторів паролів через їх ненадійність (зазвичай вони не надають інформацію про методи обробки введеної користувачем інформації). Якщо є необхідність у використанні генератора паролю, краще надати перевагу надійним менеджерам паролів, таким як KeePass, Bitwarden чи LastPass.

4. Заборонено використовувати очевидні паролі типу “qwerty”, “admin”, “password”, “11111111”, “12345678” і т.п. Також заборонено включати до паролю особисту інформацію, таку як ім’я, дата народження/інші визначні дати, місце народження і т.д.

5. Термін дії пароля: паролі потрібно змінювати кожні 90 днів. Користувачі та співробітники отримають сповіщення за 14 днів до закінчення терміну дії пароля.

6. Історія паролів: користувачі та співробітники не можуть повторно використовувати свої останні 5 паролів.

7. Зберігання паролів: паролі повинні зберігатися в зашифрованому форматі. Обов’язкове використання шифрування не гірше ніж MD5, краще надати перевагу SSH256 чи SSH512. Бажано використовувати систему додавання «солі» до хешу для підвищення захищеності.

8. Спільний доступ до пароля: користувачам та співробітникам заборонено повідомляти свої паролі будь-кому, включаючи членів сім’ї, колег (в тому числі працівникам ІТ-відділу) та друзів.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				43
Змн.	Арк.	№ докум.	Підпис	Дата		

9. Скидання пароля: користувачі можуть скинути свої паролі за допомогою безпечного процесу скидання пароля. Цей процес включає відповіді на таємні запитання або отримання одноразового пароля електронною поштою чи текстовим повідомленням.

10. Таємні питання: у якості таємних питань рекомендовано не використовувати загальні питання, відповідь на які можна легко знайти у Інтернет-ресурсах (в основному – соціальні мережі). До них відносять:

- Питання про місто народження/проживання
- Імена домашніх улюбленців
- Власна дата народження чи близьких людей
- Улюблений колір/фільм/жанр музики тощо

Якщо уникнути таких питань неможливо (через обмеження системи), варто давати на них неправдиву, лише вам відому інформацію.

11. Захист паролем: користувачі повинні зберігати свої паролі в безпеці, не записувати їх і не зберігати в незахищеному місці (на власному/робочому пристрої у незахищеному вигляді). Рекомендовано використовувати надійні менеджери паролів, такі як KeePass, Bitwarden чи LastPass

12. Під час використання менеджерів паролів краще надати перевагу копіюванню даних для в ходу безпосередньо з менеджера або за допомогою автоматичних офіційних розширень для браузера. Не рекомендовано вводити паролі вручну для уникнення ймовірності перехоплення даних за допомогою зчитувачів клавіатури.

13. Навчання політиці паролів: усі співробітники та підрядники повинні пройти навчання щодо політики паролів і важливості підтримки надійних паролів. Підприємству необхідно забезпечити контроль дотримання парольної політики усіма співробітниками.

14. Блокування пароля: після 5 послідовних невдалих спроб входу облікові записи користувачів буде заблоковано на 30 хвилин. Користувачі можуть звернутися до ІТ-відділу, щоб розблокувати свої облікові записи. Крім того, окрім безпосередньо блокування облікового запису, необхідно додатково вести аудит

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				44
Змн.	Арк.	№ докум.	Підпис	Дата		

невдалих спроб аутентифікації для виявлення потенційної спроби зламу системи аутентифікації з-за меж компанії.

15. Багатофакторна аутентифікація: рекомендовано використання багатофакторної аутентифікації для віддаленого доступу до мережі та систем компанії. Це можуть бути як застосунки для отримання додаткового коду, так і інші види додаткової аутентифікації, такі як біометрія чи фізичний ключ, в залежності від потреб та бюджету компанії.

16. Заборонено використовувати один й той самий пароль для облікових записів на інших ресурсах – для кожного має бути свій унікальний пароль.

4.2. Методи захисту від соціальної інженерії

Окрім впровадження сильних паролів, їх захищеного використання та зберігання, вкрай важливим є захист від соціальних інженерів. Злам складного захищеного паролю може займати не один рік і вимагати значних витрат на комп'ютерне обладнання для обчислення. Отримання паролю шлях використання методів соціальної інженерії може займати всього декілька хвилин [3].

Щоб зменшити вплив атак соціальної інженерії на системи аутентифікацій, варто дотримуватись таких рекомендацій [9]:

1. Підтримання актуальності програмного забезпечення: варто переконатися, що все програмне забезпечення та системи оновлені з останніми виправленнями безпеки та оновленнями.

2. Моніторинг активності: необхідно відстежувати мережеву активність і поведінку користувачів на наявність будь-яких ознак підозрілої активності.

3. Створення плану реагування на інциденти: необхідно розробити і запровадити план реагування на інциденти, щоб швидко реагувати на будь-які атаки соціальної інженерії та мінімізувати шкоду.

4. Створення системи звітності: варто створити систему звітності, куди співробітники мають повідомляти у разі виявлення спроб атаки з використанням соціальної інженерії.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				45
Змн.	Арк.	№ докум.	Підпис	Дата		

5. Якщо працівник працює віддалено, варто налагодити віддалений доступ до робочої станції, захищений VPN з'єднанням.

6. Навчання співробітників: необхідно навчати співробітників виявляти атаки соціальної інженерії та реагувати на них. Організації повинні проводити регулярну навчання та інформування користувачів про загрози соціальної інженерії, розповідати про типові схеми атак і надавати поради щодо попередження.

7. Резервне копіювання та відновлення даних: необхідно регулярно робити резервні копії своїх даних та перевіряти процедури відновлення.

8. Підвищення обізнаності: потрібно повідомляти користувачів про потенційні загрози, такі як фішингові електронні листи, телефонні дзвінки або відвідувачі особистої інформації.

9. Необхідно запровадити систему звітування для користувачів, яка включає звіти не лише про ситуації, що вже сталися (користувач перейшов за невідомим посиланням, завантажив скрипт і т.п.), але й про потенційні загрози, щоб уникнути їх виконання у майбутньому.

10. Варто впровадити правила що регулюють перевірку ресурсів, що надають клієнти компанії – перевірка файлів на наявність зловмисного вмісту програмним шляхом (наприклад, з використанням VirusTotal), усі посилання мають перевірятися спочатку на віртуальній машині.

11. Захист фізичного доступу: фізичний доступ до приміщень та обладнання, яке містить конфіденційну інформацію, має бути захищений. Можливе застосування механізмів контролю доступу, такі як картки доступу, біометричні сканери або фізичні бар'єри.

12. Резервне копіювання та відновлення даних: обов'язкове регулярне створення резервних копій даних та перевірка процедури відновлення.

13. Обмеження доступу: необхідне встановлення обмежень доступу до конфіденційних інформаційних ресурсів, включаючи фізичні та логічні обмеження. Кожен користувач системи повинен мати доступ лише до тієї частини даних системи, які необхідні йому для прямого виконання робочих зобов'язань.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				46
Змн.	Арк.	№ докум.	Підпис	Дата		

4.3. Оцінювання захищеності системи парольної аутентифікації

Окрім створення нової парольної політики та впровадження нових заходів щодо зменшення вразливостей системи, спеціаліст з кібербезпеки має вміти оцінювати якість існуючих рішень компанії. Оцінка якості системи парольної аутентифікації може проводитись за допомогою різних критеріїв і метрик. Ось декілька способів, якими можна оцінити якість системи парольної аутентифікації [18]:

1. Складність паролів: оцініть, наскільки система вимагає використання складних паролів. Чи вимагається використання різних типів символів, таких як великі літери, малі літери, цифри та спеціальні символи? Оцініть мінімальну та максимальну довжину паролів, яку дозволяє система.

2. Розгляньте, чи підтримує система використання додаткових факторів аутентифікації, таких як двофакторна аутентифікація або біометричні дані.

3. Зберігання паролів: дізнайтеся, як система зберігає паролі. Чи використовується надійне шифрування для захисту паролів у базі даних? Чи має система захист від витоку паролів?

4. Заходи проти атак: дослідіть, які заходи використовуються для запобігання різним видам атак, таким як Brute force, Dictionary атаки, Phishing і т. д. Чи існують обмеження на кількість невдалих спроб входу, а також блокування облікового запису після певної кількості невдалих спроб?

5. Моніторинг та журналювання: переконайтеся, що система здатна вести журнал подій, пов'язаних з аутентифікацією, і забезпечує можливість моніторингу та виявлення підозрілих дій або несправних спроб входу.

6. Керування доступом: розгляньте наявність функцій керування доступом, таких як рівні привілеїв, ролі та можливість налаштування обмежень доступу для користувачів.

7. Аудит безпеки: перевірте, чи проводяться регулярні аудити безпеки системи парольної аутентифікації. Це може включати перевірку наявності

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				47
Змн.	Арк.	№ докум.	Підпис	Дата		

оновлень, перевірку наслідків виявлених вразливостей і вжиття відповідних заходів.

Крім цього, для оцінювання захищеності системи парольної аутентифікації можна використовувати різні програмні засоби, які допоможуть виявити потенційні вразливості та забезпечити належний рівень безпеки. Ось декілька таких інструментів:

- Open Web Application Security Project (OWASP);
- Nmap;
- John the Ripper;
- Hashcat;
- Burp Suite;
- Wireshark.

Ці програмні засоби надають різноманітні функції для тестування безпеки системи парольної аутентифікації. Проте варто пам'ятати, що використання цих інструментів повинно відбуватися відповідно до законодавства та з метою забезпечення безпеки тільки в рамках власних або авторизованих тестових середовищ.

Висновки до четвертого розділу

Отже, було коротко розглянуто основні вимоги, що має містити парольна політика, заходи для зменшення впливу атак соціальної інженерії, критерії оцінювання якості захищеності системи парольної аутентифікації.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк Є.М				48
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВОК

В результаті виконання цієї роботи було досліджено основні системи парольних аутентифікації та їх вразливості.

У першому розділі було розглянуто поняття аутентифікації та авторизації, принципи їх роботи та основні відмінності.

У другому розділі було виконано огляд сучасних методів парольної аутентифікації, їх переваги та недоліки, та проаналізовано основні їх вразливості.

У третьому розділі було коротко розглянуто основні приклади програмного забезпечення для зламу систем парольних аутентифікації, досліджено функціонали популярних парольних менеджерів та засобів двофакторної аутентифікації.

У четвертому розділі було визначено основні вимоги до парольних політик та методи оцінювання захищеності систем парольних аутентифікації.

Таким чином, в цій роботі було проведено дослідження основні вразливості систем парольних аутентифікації та яким чином можна зменшити їх вплив шляхом впровадження якісної парольної політики.

Отже, мета кваліфікаційної роботи була досягнута.

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк Є.М				49
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Нова версія стандарту ISO/IEC 27001:2022. [Електронний ресурс] Режим доступу до ресурсу: <https://ain.ua/2022/12/06/nova-versiya-standartu-iso-iec-270012022-chym-it-kompaniyam-korysnyj-czej-standart-ta-yak-jogo-vprovadyty/>
- [2] Password policy (Wikipedia). [Електронний ресурс] Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Password_policy#:~:text=A%20password%20policy%20is%20a,part%20of%20security%20awareness%20training.
- [3] Methods for Understanding and Reducing Social Engineering Attack [Електронний ресурс] Режим доступу до ресурсу: <https://www.sans.org/white-papers/36972/>
- [4] Create a strong password & a more secure account [Електронний ресурс] Режим доступу до ресурсу: <https://support.google.com/accounts/answer/32040?hl=en>
- [5] KeePass Password Safe [Електронний ресурс] Режим доступу до ресурсу: <https://keepass.info/>
- [6] Vulnerability Disclosure Cheat Sheet [Електронний ресурс] Режим доступу до ресурсу: https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html
- [7] «ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ» С.Г. СЕМЕНОВ, А.О.ПОДОРОЖНЯК, О.І.БАЛЕНКО, С.Ю.ГАВРИЛЕНКО, 2014 – 252 с.
- [8] «ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ» В.Д. КОЗЮРА, В.О. ХОРОШКО, М.Є. ШЕЛЕСТ, Ю.М. ТКАЧ, О.О.БАЛЮНОВ, 2020 – 118 с.
- [9] Ways to avoid social engineering attacks [Електронний ресурс] Режим доступу до ресурсу: <https://www.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks>

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				50
Змн.	Арк.	№ докум.	Підпис	Дата		

[10] CIS Password Policy Guide [Електронний ресурс] Режим доступу до ресурсу: [CIS_Benchmarks_Password_Policy_Guide_v21.12.pdf](#)

[11] Florencio D., et al. (2007). Do Strong Web Passwords Accomplish Anything? [Електронний ресурс] Режим доступу до ресурсу: <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/tr-2007-64.pdf>

[12] Grimes R. (2019, January 04). 6 reasons biometrics are bad authenticators (and 1 acceptable use) [Електронний ресурс] Режим доступу до ресурсу: <https://www.csoonline.com/article/3330695/6-reasons-biometricsare-bad-authenticators-and-1-acceptable-use.html>

[13] Walters, R. (2015, April 07). Insecure Passwords or Insecure People? [Електронний ресурс] Режим доступу до ресурсу: www.infosecurity-magazine.com/opinions/insecure-passwords-insecure-people/

[14] [Електронний ресурс] Режим доступу до ресурсу: <https://www.openwall.com/john/doc/>

[15] [Електронний ресурс] Режим доступу до ресурсу: <https://www.kali.org/tools/hydra/>

[16] [Електронний ресурс] Режим доступу до ресурсу: <https://github.com/smorks/keepasshttp-connector/blob/master/documentation/KeePassHttp-Connector.md#9-security>

[17] [Електронний ресурс] Режим доступу до ресурсу: <https://www.kaspersky.com/blog/identification-authentication-authorization-difference/37143/>

[18] [Електронний ресурс] Режим доступу до ресурсу: <https://auth0.com/docs/get-started/identity-fundamentals/authentication-and-authorization>

[19] [Електронний ресурс] Режим доступу до ресурсу: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

[20] [Електронний ресурс] Режим доступу до ресурсу: https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				51
Змн.	Арк.	№ докум.	Підпис	Дата		

[21] [Електронний ресурс] Режим доступу до ресурсу:
<https://bitwarden.com/help/data-storage/#:~:text=Bitwarden%20processes%20and%20stores%20all,by%20the%20team%20at%20Microsoft.>

[22] [Електронний ресурс] Режим доступу до ресурсу:
<https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=en>

[23] [Електронний ресурс] Режим доступу до ресурсу:
<https://www.microsoft.com/en-us/security/mobile-authenticator-app>

[24] [Електронний ресурс] Режим доступу до ресурсу:
<https://www.yubico.com/products/yubico-authenticator/>

		Шевчик Д.А.			ККІКБ.КР.Б – 125 – 23 – ПЗ	Арк.
—		Байлюк С.М				52
Змн.	Арк.	№ докум.	Підпис	Дата		