Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Дослідження методів автентифікації та їх технічна реалізація

Виконав(ла): студент(ка) 4 курсу, групи СБ-41
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Бортник Н.В. (прізвище та ініціали)

Керівник (підпис) Скарга-Бандурова І.С. (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т.Б. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль
2023

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри

(підпис) (прізвище та ініціали)

« » 2023 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

студенту Бортнику Назарію Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження методів автентифікації та їх технічна реалізація

Керівник роботи Скарга-Бандурова Інна Сергіївна, доктор технічних наук, професор кафедри
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*03*» *квітня* 2023 року № *4\7-349*

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи персональний ноутбук з середовищем локального севрера Open Server та редактором коду Visual Studio, застосунок для двофакторної автентфиікації Google Authenticator, документація, інтернет ресурси.

4. Зміст роботи (перелік питань, які потрібно розробити)
РОЗДІЛ 1 КЛАСИЧНІ МЕТОДИ АВТЕНТИФІКАЦІЇ, РОЗДІЛ 2 СУЧАСНІ МЕТОДИ АВТЕНТИФІКАЦІЇ, РОЗДІЛ 3 ТЕХНІЧНА РЕАЛІЗАЦІЯ МЕТОДУ АВТЕНТИФІКАЦІЇ, РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності,основи охорони праці	Пилипець М.І., д.т.н. проф. кафедри МТ		

7. Дата видачі завдання 16.01.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Ознайомлення з завданням до кваліфікаційної роботи	16.01 – 21.01	*Виконано*
2	Огляд літератури про автентифікацію та її важливість	22.01 – 31.01	*Виконано*
3	Визначення цілей і завдання дослідження	01.02 - 10.02	*Виконано*
4	Дослідження різних методів автентифікації, включаючи пароль, біометрію, OTP	11.02 - 25.02	*Виконано*
5	Вивчення переваг і недоліків кожного методу	26.02 - 10.03	*Виконано*
6	Вивчення концепції двофакторної автентифікації	11.03 – 25.03	*Виконано*
7	Вивчення вимог щодо безпеки і зручності автентифікаційних систем	26.03 - 04.04	*Виконано*
8	Дослідження різних рішень і технологій для реалізації двофакторної автентифікації	05.04-20.04	*Виконано*
9	Оцінка переваг, ризиків і обмежень кожного рішення	21.04 – 30.04	*Виконано*
10	Розробка програмного коду веб-сайту	01.05- 14.05	*Виконано*
11	Інтеграція системи двохфакторної автентифікації	15.05-31.05	*Виконано*
12	Проведення тестування зі створеною системою двофакторної автентифікації	01.06-04.06	*Виконано*
13	Виконання завдання розділу «Безпека життєдіяльності, основи охорони праці»	05.06-08.06	*Виконано*
14	Оформлення кваліфікаційної роботи	09.06 – 12.06	*Виконано*
15	Проходження нормоконтролю	13.06 – 15.06	*Виконано*
16	Перевірка на плагіат	16.06 - 19.06	*Виконано*
17	Захист кваліфікаційної роботи	20.06.2023	

Студент _____ Бортник Н.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Скарга- Бандурова І.С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження методів автентифікації та їх технічна реалізація // Кваліфікаційна робота ОР «Бакалавр» // Бортник Назарій Володимирович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБ-41 // Тернопіль, 2023 // с. 57 , рис. – 12, табл. – 2, лістинги. – 3, додатки – 5.

Ключові слова: АВТЕНТИФІКАЦІЯ, СТАНДАРТИ АВТЕНТИФІКАЦІЇ, ДВОФАКТОРНА АВТЕНТИФІКАЦІЇ, БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ, СЕРВІСИ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

Основною метою даної роботи є впровадження сервісу двофакторної автентифікації. Для цього було розглянуто різні методи автентифікації, та як використовуються програми двофакторної автентифікації.

Об'єкт дослідження - процес автентифікації користувачів у інформаційно-телекомунікаційних системах.

Предмет дослідження - методи вибору сервісу для двофакторної автентифікації.

При написанні дипломної роботи, був здійснений теоретичний аналіз і виклад наукової літератури, запропонована методика вибору послуг двофакторної автентифікації.

Результатом роботи є впровадженння сервісу двофакторної автентифікації для веб-сайту.

В цій кваліфікаційній роботі проведений аналіз та порівняння різних методів автентифікації та наглядного прикладу впровадження ефективного та малозатратного способу двофакторної автентфікації.

Для реалізації даної роботи були використані програмні продукти: Visual Studio 2022, Open Server.

ABSTRACT

Study of authentication methods and their technical implementation // Qualification work of OR "Bachelor" // Bortnyk Nazarii Volodymyrovych// Ivan Pulyuy Ternopil National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, Group SB-41 // Ternopil, 2023 // p. 57 , fig. - 12, tab. – 2, listings. – 3, applications – 5.

Keywords: AUTHENTICATION, AUTHENTICATION STANDARDS, TWO-FACTOR AUTHENTICATION, MULTI-FACTOR AUTHENTICATION, TWO-FACTOR AUTHENTICATION SERVICES

The main goal of this work is to implement a two-factor authentication service. For this, various authentication methods were considered, and how they are used by two-factor authentication programs.

The object of research is the process of user authentication in information and telecommunication systems.

The subject of the study is methods of selecting a service for two-factor authentication.

When writing the thesis, a theoretical analysis was carried out and

presentation of scientific literature, proposed method of service selection

two-factor authentication.

The result of the work is the implementation of the two-factor authentication service for the website.

In this qualification work, an analysis and comparison of various authentication methods and an illustrative example of the implementation of an effective and low-cost method of two-factor authentication are carried out.

Software products were used to implement this work: Visual Studio 2022, Open Server.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ……..7
ВСТУП…….9
РОЗДІЛ 1 КЛАСИЧНІ МЕТОДИ АВТЕНТИФІКАЦІЇ……....11
1.1 Парольна автентифікація: принцип роботи, сильні та слабкі сторони, проблеми безпеки…….....11
1.2 Біометрична автентифікація: методи, переваги та ризики……..…19
РОЗДІЛ 2 СУЧАСНІ МЕТОДИ АВТЕНТИФІКАЦІЇ……..….24
2.1 Двофакторна автентифікація: використання пароля разом з іншим фактором, види та переваги…….……...24
2.2 Багатофакторна автентифікація: процеси, переваги та способи її реалізації…….....27
2.3 Роль ШІ в автентифікації: поведінкова біометрія, виявлення аномалій, безперервна та адаптивна автентифікація……..….30
РОЗДІЛ 3 ТЕХНІЧНА РЕАЛІЗАЦІЯ МЕТОДУ АВТЕНТИФІКАЦІЇ…….....34
3.1 Огляд застосунків: Authy 2FA, FreeOTP, Google Authenticator, Microsoft Authenticator…….....……34
3.2 Підключення 2FA із використаням Google Authenticator
3.3 Тестування впровадженої 2FA…….....…….41
РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ……..……..44
4.1 Долікарська допомога при пораненнях……..……...44
4.2 Вимоги до профілактичних медичних оглядів для працівників ПК……...……46
ВИСНОВКИ……..……49
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……..……51
ДОДАТКИ……..…….…..53
Додаток А Лістинг коду форми реєстрації…….……...……..53
Додаток Б Лістинг коду форми входу…...……...……54

Додаток В Лістинг коду форми профілю……..……..55
Додаток Г Лістинг коду обробки даних з форми реєстрації…….…...56
Додаток Д Лістинг обробки даних з форми входу……...…..57

ПЕРЕЛІК СКОРОЧЕНЬ І ТЕРМІНІВ

2FA(two-factor authentication) – двофакторна автентифікація

MFA (multi-factor authentication – мультифакторна автентифікація

OTP (one-time password) – одноразовий пароль

TOTP (Time-based One-Time Password Algorithm) – алгоритм одноразового пароля на основі часу

HOTP (HMAC-Based One-Time Password Algorithm) – алгоритм одноразового пароля на основі HMAC

ШІ – штучний інтелект

МН – машинне навчання

ВДТ – візуальний дисплейний термінал

ЕОМ – електронно-обчилювальна машина

ПК – персональний комп’ютер

ВСТУП

У сучасному інформаційному середовищі, де доступ до цифрової інформації стає все більш поширеним і необхідним, питання забезпечення безпеки та конфіденційності даних стає критичним. Автентифікація є важливим елементом безпеки, вона гарантує ідентифікацію та підтвердження правомочності користувачів перед наданням доступу до системи чи будь якого ресурсу.

Автентифікацію можна визначити як процес перевірки та підтвердження особи користувача, який намагається отримати доступ до певного ресурсу чи системи. Цей процес зазвичай передбачає надання користувачем підтвердження особи (наприклад, логін або ім’я користувача) та механізм автентифікації (наприклад, пароль, біометричний або інший фактор автентифікації).

Важливість автентифікації в сучасному інформаційному середовищі неможливо переоцінити. Недостатня або ненадійна автентифікація може призвести до серйозних наслідків, таких як несанкціонований доступ до конфіденційних даних, втрата або пошкодження інформації, фінансові збитки або порушення конфіденційності користувача. У зв’язку зі збільшенням кількості кібератак і технологічних розробок існує потреба постійно вдосконалювати методи автентифікації та розробляти нові рішення для запобігання атакам.

Метою цієї кваліфікаційної роботи є вивчення різних методів автентифікації, щоб з’ясувати їх сильні та слабкі сторони та можливість застосування в реальних сценаріях. Дослідження включатиме аналіз класичних методів автентифікації, таких як автентифікація за допомогою пароля та біометрична автентифікація, а також нові підходи, такі як двофакторна чи багатофакторна автентифікація.

Основною метою цього дослідження є розглянути більшість методів автентифікації, зрозуміти ефективність, надійність і зручність для

застосування в різних сферах. На основі отриманих результатів будуть сформульовані рекомендації щодо вибору і реалізації методів автентифікації, які найкраще задовольняють потреби безпеки і зручності для кінцевих користувачів та організацій.

РОЗДІЛ 1 КЛАСИЧНІ МЕТОДИ АВТЕНТИФІКАЦІЇ

1.1 Парольна автентифікація: принцип роботи, сильні та слабкі сторони, проблеми безпеки

Автентифікація - це процес перевірки користувача або пристрою перед наданням доступу до системи або ресурсу. Іншими словами, автентифікація підтверджує, що користувач є тим, за кого себе видає. Це гарантує, що доступ до захищеної системи отримають лише ті, хто має відповідні облікові дані. Коли користувач хоче отримати доступ до інформації в мережі, він повинен надати конфіденційні облікові дані, щоб підтвердити свою особу. Автентифікація дозволяє безпечно надавати доступ потрібному користувачеві в потрібний час. Однак самої лише автентифікації недостатньо.

Автентифікація є частиною триетапного процесу доступу до цифрових ресурсів

- Ідентифікація - визначення того, хто ви є.
- Автентифікація - доведення того, хто ви є.
- Авторизація - доведення того, чи є у вас дозвіл.

Для ідентифікації потрібен ідентифікатор користувача, наприклад, ім'я користувача. Однак без автентифікації неможливо дізнатися, чи дійсно ім'я користувача належить цій особі. Отже, автентифікація - це комбінація імені користувача та пароля або іншого фактора для перевірки імені користувача. Загальні фактори автентифікації описані нижче:

- Фактор знань (автентифікація на основі знань). У методі фактору знань користувач повинен підтвердити свою особу, розкривши інформацію, яку не знає ніхто інший. Типовими прикладами цього фактора автентифікації є секретні запитання, відповідь на які знає лише користувач, наприклад, ім'я його першого домашнього улюбленця або дівоче прізвище матері. Додатки також можуть запитувати доступ за допомогою чотиризначного PIN-коду. Ці методи безпечні, якщо ніхто інший не знає конфіденційної інформації.

Злочинці можуть проаналізувати особисту історію користувача і обманом змусити його розкрити цю інформацію. PIN-код також можна розшифрувати за допомогою методів грубої сили, які передбачають вгадування всіх можливих комбінацій з чотирьох цифр.

– Фактор власності. Метод фактору власності ідентифікує себе за тим, чим користувач унікально володіє. Наприклад це можуть бути фізичні пристрої, такі як мобільні телефони, токени безпеки, екрани, апаратні брелоки і ключі безпеки. Цифрові активи, такі як облікові записи електронної пошти та додатки для автентифікації. Система надсилає секретні коди у вигляді цифрових повідомлень на ці пристрої та активи, які користувач потім повторно вводить у систему. Якщо пристрій втрачено або вкрадено, обліковий запис може бути скомпрометований. Деякі токени безпеки долають цю проблему, підключаючись безпосередньо до системи, що унеможливлює цифровий доступ.

– Фактори успадкування. Методи успадкування використовують специфічну для користувача інформацію. Ось кілька прикладів таких факторів автентифікації:

а) Ідентифікація за відбитками пальців.

б) Сканування сітківки ока.

в) Розпізнавання мови.

г) Розпізнавання обличчя.

д) Поведінкова біометрія, наприклад, динаміка натискання клавіш.

Найпоширенішим методом автентифікації є унікальне ім'я користувача та пароль, але оскільки загрози кібербезпеки зросли в останні роки, все більше організацій використовують і рекомендують додаткові фактори автентифікації для багаторівневої безпеки. Автентифікація на основі пароля - це метод, який вимагає від користувача введення облікових даних (ім'я користувача та пароль) для підтвердження своєї особи (рис.1.1). Введені облікові дані порівнюються з обліковими даними, що зберігаються в базі даних системи, і тільки якщо вони збігаються, користувачеві надається доступ. Паролі є

елементами інформації і відомі лише користувачеві. Коли користувач намагається увійти в систему, система автентифікації порівнює облікові дані, надані користувачем, з обліковими даними, що зберігаються в базі даних. Якщо вони збігаються, користувачеві надається доступ. Якщо збігу немає, користувачеві відмовляють у доступі і можуть попросити повторно ввести інформацію або відновити забутий пароль.

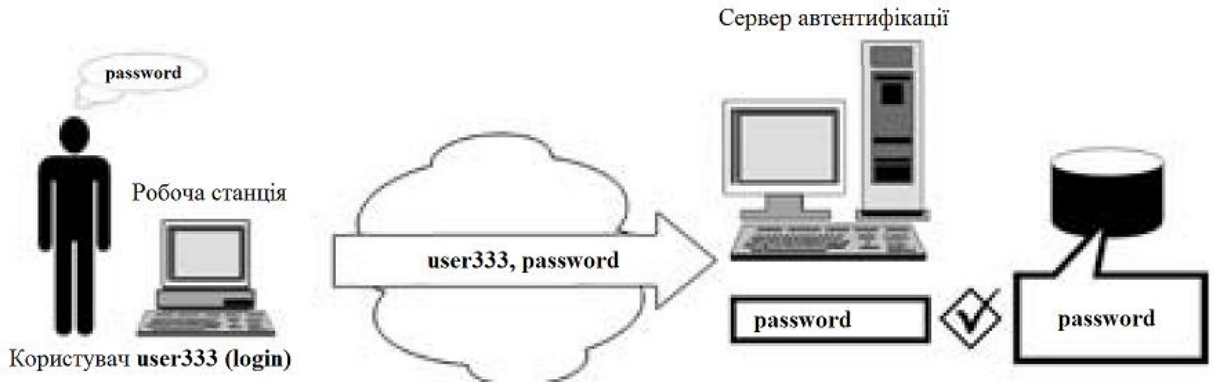


Рисунок 1.1 – Схема автентифікації на основі відкритого паролю

З перших днів існування Інтернету парольна автентифікація широко використовувалася завдяки своїй простоті та широкому розповсюдженню серед користувачів. Хоча в останні роки її популярність знизилася через проблеми з безпекою, про які йтиметься нижче, але всеодно залишаються компанії які використовують тільки парольну автентифікація, швидше за все це через те, що вона є інтуїтивно зрозумілою для користувачів і дозволяє їм отримувати доступ до сторінок і сервісів, якщо вони вводять правильні облікові дані. Також щоб збільшити захист від итоку інформації паролі можуть зберігається в базі даних системи у зашифрованому вигляді, а саме хешуються (рис 1.2).

Рисунок 1.2 – Схема автентифікації на основі хешованого паролю

Цифрові паролі використовуються щонайменше з середини 1960-х років і досі залишаються поширеними. Паролі використовуються протягом тривалого часу, частково через легкість процесу. Автентифікація на основі паролів пропонує ряд переваг як для організацій, так і для кінцевих користувачів, зокрема:

– Звичність. Паролі є найпоширенішим методом автентифікації і є звичними для середньостатистичного користувача, що призводить до більш комфортної роботи та меншої кількості запитів на підтримку.

– Зручність використання. Порівняно з деякими іншими методами автентифікації, які вимагають більш складних технологій і додаткового обладнання та програмного забезпечення, автентифікація за допомогою пароля є відносно простою і недорогою, зберігаючи при цьому базовий рівень безпеки. Це робить її популярною серед малих і середніх підприємств з обмеженими ресурсами (хоча ситуація змінюється).

– Контроль користувачів. Автентифікація на основі паролів дозволяє користувачам керувати своїми паролями, дозволяючи їм змінювати або скидати паролі в будь-який час. Це дозволяє користувачам керувати своїми паролями на власний розсуд.

Системи автентифікації на основі паролів мають деякі переваги, але вони далекі від досконалості. Окрім необхідності записувати, запам'ятовувати та використовувати менеджери паролів для зберігання десятків облікових даних, які сьогодні має середньостатистична людина, є й інші недоліки.

– Вразливість. Один з основних ризиків, пов'язаних з парольною автентифікацією, полягає в тому, що паролі можна легко вкрасти або вгадати, особливо якщо вони слабкі або повторно використовуються в декількох системах. Якщо паролі скомпрометовані, зловмисники можуть отримати доступ до облікових записів користувачів і потенційно конфіденційної інформації. Майже 80 відсотків витоків даних за останні 4 роки році були спричинені компрометацією паролів.

– Передбачуваність. Простіше кажучи, люди схильні обирати слабкі паролі. Насправді, за однією з оцінок, близько 60 відсотків користувачів використовують власні імена або дні народження. І лише третина користувачів не використовують свої паролі повторно на різних платформах. Підбірка облікових даних та атаки грубої сили використовують цю людську передбачуваність, щоб вгадати або викрасти облікові дані користувачів.

– Помилки. Люди забувають свої паролі. Комп'ютер, на якому зберігаються облікові дані, може вийти з ладу. Навіть фізичні копії інформації можуть бути втрачені або викрадені. Зазвичай користувачі можуть відновити свої паролі електронною поштою, але якщо основну електронну пошту зламано або вимкнено, вони можуть назавжди втратити доступ до свого облікового запису.

– Складність. Автентифікація на основі пароля проста, але вона може стати складною, якщо користувачам потрібно створювати складні паролі, які відповідають певним вимогам, таким як мінімальна довжина, спеціальні символи та цифри. Це призводить до розчарування користувачів, збільшує ймовірність відходу користувачів і призводить до втрачених конверсій. Крім того, завдання скидання паролів збільшує навантаження на IT-спеціалістів та

служби підтримки, які можуть витрачати свій час на інші важливі для бізнесу завдання.

Отже, паролі - це швидко і звично, але ціною цього є загроза безпеці користувачів і організації. В таблиці 1.1 наведено сім найвідоміших атак на пароль та захист від них.

Таблиця 1.1 – Найвідоміші атаки на пароль

Опис атаки	Захист від атаки
Груба сила	
Автоматизовані системи вручну намагаються створити кілька мільйонів, мільярдів або трильйонів комбінацій літер і цифр у надії випадково натрапити на пароль облікового запису.	– Використання складних паролів із комбінаціями великих і малих літер, цифр і символів може ускладнити вгадування. – Також бажано використовувати довші паролі, оскільки довші паролі додають експоненціальних рівнів складності вгадування методом грубої сили. – Увімкніть блокування облікового запису, якщо користувач забагато разів вводить неправильний пароль. Заблокований обліковий запис із обмеженим часом відновлення може перешкодити атакам грубої сили. – Впровадження багатофакторної автентифікації та рішень без пароля може зменшити ефективність атак грубої сили, оскільки вони вимагають облікових даних, які ці методи не можуть відтворити.
Фішинг	
Зловмисник розраховує на необізнаність користувачів щодо сучасних загроз безпеці та їхню довіру до офіційних електронних листів, підробляючи ці електронні листи для запиту паролів користувачів. Сам по собі фішинг є поширеною формою атаки, яка має кілька різних форм: електронна пошта, SMS тексти, голосові дзвінки, підроблені веб-сайти	– Навчання членів команди, від найманих працівників до вищого керівництва, тому, як розпізнавати фішингові атаки, коли вони їх бачать. – Реалізація попереджень електронною поштою, щоб надавати сповіщення, коли співробітники отримують електронні листи з-за меж організації.

Продовження таблиці 1.1

Словник	
Словникові атаки пробують слова з попередньо визначеного списку, намагаючись підібрати пароль облікового запису. Ці словники, хоч і містять менше загальних слів, часто зосереджуються на «звичайних» паролях, зібраних хакерами роками. Списки також можуть містити терміни зі словників, загальні назви або комбінації дат і місць	– Уникайте загальних паролів, які складаються зі зрозумілих слів, навіть якщо ви використовуєте комбінації загальних слів. – Створення паролів із випадкових або, здавалося б, випадкових комбінацій букв, цифр і символів. – Активація блокування облікового запису, якщо користувач вводить неправильний пароль забагато разів. Заблокований обліковий запис із обмеженим часом відновлення може перешкодити атакам грубої сили. – Впровадження багатофакторної автентифікації та рішень без пароля може зменшити ефективність атак грубої сили, оскільки вони вимагають облікових даних, які ці методи не можуть відтворити.
Кейлоггери	
Кейлоггери — це типи програмного забезпечення, які відстежують натискання клавіш у хост-системі та копіюють цю інформацію в текстовий файл. Ці типи програмного забезпечення можуть походити від іншого виду злому, як-от заражене вкладення електронної пошти або щось, встановлене локально на машині. Кейлоггер відкриває будь-які паролі, введені користувачем.	– Сканування систем на наявність зловмисного або іншого зловмисного програмного забезпечення за допомогою антивірусних засобів і перевірка на наявність несподівано встановленого програмного забезпечення в системі. – Підтримка повного фізичного захисту фізичних комп’ютерів, включаючи надійну автентифікацію для робочих станцій і фізичної безпеки (замки, клавіатури та камери) у будь-якому місці, де розташовані комп’ютери.

Продовження таблиці 1.1

Наповнення облікових даних	
Зазвичай хакер, зламавши один обліковий запис, намагається використати ці облікові дані для кількох інших облікових записів. Подібним чином хакери, які викрадають паролі (наприклад, шляхом зламу бази даних), чекатимуть і з часом спробують знову використати ці облікові дані як в інших системах, так і в тій самій системі.	– Змушення користувачів змінювати паролі після злому. Обов'язкова зміна може зменшити загрозу старих паролів, які можуть спричинити проблему. – Вимагати від користувачів регулярно змінювати свої паролі та робити так, щоб вони не могли повторно використовувати попередні комбінації імені користувача та пароля. – Зробити менеджери паролів обов'язковими, якщо дотримуватись паролів як основного підходу безпеки.
Розпилення пароля	
Атака розпилення потребує кількох поширених паролів (наприклад, атака за словником), але покладається на звичайні шаблони, як-от добре відомі параметри за замовчуванням, дати народження або прості фрази, як-от комбінації цифр і слова «пароль», і намагається підібрати кілька облікових записів одночасно. Цей «розпилювальний підхід» не матиме такого ж рівня успіху, як спеціальна словникова атака. Натомість він розраховує на гру чисел: у сотнях облікових записів принаймні один із них використовує слабкий пароль.	– Уникайте загальних паролів, які складаються зі зрозумілих слів, навіть якщо ви використовуєте комбінації загальних слів. – Створення паролів із випадкових або, здавалося б, випадкових комбінацій букв, цифр і символів. – Вимагати від користувачів регулярно змінювати свої паролі та робити так, щоб вони не могли повторно використовувати попередні комбінації імені користувача та пароля. – Зробити менеджери паролів обов'язковими, якщо дотримуватись паролів як основного підходу безпеки. – Впровадження багатофакторної автентифікації та рішень без пароля може зменшити ефективність атак грубої сили, оскільки вони вимагають облікових даних, які ці методи не можуть відтворити.

Продовження таблиці 1.1

Людина посередині	
Атаки типу Man-in-the-middle відбуваються, коли хакер отримує контроль над системою-посередником між двома сторонами, наприклад користувачем і платформою автентифікації, і викрадає інформацію, коли вона переміщується вперед і назад між ними (включаючи паролі). Незахищені канали зв'язку можуть зробити цю інформацію легко читаною, і будь-який зловмисник може прочитати інформацію, не попереджаючи жодну зі сторін про загрозу.	– Шифрування даних, що входять до організації та виходять з неї, а також уникнення надсилання будь-якої інформації, включаючи облікові дані для входу, через відкритий текст. – Використання віртуальних приватних мереж для віддалених користувачів, які отримують доступ до критично важливих систем.

Розглянувши найвідоміші атаки ми бачимо які є слабкі сторони в такої автентифікації. Для більшості атак хорошим захистом є впровадження багатофакторної автентифікації, що ми і розглянемо в наступних розділах.

1.2 Біометрична автентифікація: методи, переваги та ризики

Біометрична автентифікація - це процес кібербезпеки, який використовує унікальні біологічні характеристики, такі як відбитки пальців, голос, сітківка ока або обличчя, для підтвердження особи користувача. Системи біометричної автентифікації зберігають цю інформацію і перевіряють, чи є користувач тим, за кого він себе видає, коли отримує доступ до свого облікового запису. Цей тип автентифікації, як правило, більш безпечний, ніж традиційна багатофакторна автентифікація.

Нижче перераховані загальні методи біометричної автентифікації, що використовуються в мережевій безпеці для боротьби з кіберзлочинністю. Крім

того, деякі з наступних методів біометричної автентифікації використовуються щодня:

– Розпізнавання обличчя: система, яка використовує унікальні риси обличчя людини для її ідентифікації. Використовується в різних сферах, включаючи смартфони, платежі кредитними картками та правоохоронні органи.

– Автентифікація за відбитками пальців: автентифікація за відбитками пальців використовує унікальні відбитки пальців для визначення особи людини. Вона може використовуватися для захисту всього, від мобільних пристроїв до автомобілів і будівель, і є найпоширенішою технологією біометричної автентифікації.

– Очна автентифікація: очна автентифікація використовує унікальний візерунок райдужної оболонки ока або сітківки для ідентифікації особи. Цей тип біометричної автентифікації складно реалізувати, і тому він менш поширений, ніж інші варіанти біометричної автентифікації. Щоб ідентифікація за райдужною оболонкою ока була точною, потрібне джерело інфрачервоного світла, камера, яка може бачити інфрачервоне світло, і мінімальне світлове забруднення. Однак, коли ці умови дотримані, це одна з найточніших доступних систем біометричної автентифікації. Розпізнавання погляду широко використовується в ситуаціях, де безпека є найбільш важливою, наприклад, на ядерних дослідницьких об'єктах.

– Розпізнавання мови: розпізнавання мови використовує унікальний тон, висоту і частоту голосу людини для ідентифікації цієї людини. Це найпоширеніший біометричний метод ідентифікації користувачів при зверненні в колл-центри для підтримки клієнтів (наприклад, в онлайн-банкінгу).

– Автентифікація за ходою: Автентифікація за ходою ґрунтується на визначенні манери ходи людини. Оскільки кожна людина ходить по-різному, ефективним засобом ідентифікації є те, як людина ходить, виставляючи одну ногу перед іншою. Хоча це ще не дуже поширений метод автентифікації,

очікується, що він стане більш поширеним у міру того, як методи автентифікації стануть більш поширеними.

– Автентифікація за венами: Використовує малюнок кровоносних судин на руках і пальцях для підтвердження особи. Цей тип біометрії використовує інфрачервоне світло для створення карти вен під шкірою руки або пальця. Автентифікація за венами є набагато точнішою, ніж автентифікація за сітківкою/райдужною оболонкою ока.

Переваги та ризики біометричної автентифікації

Переваги:

– Страхування ідентичності: біометрична автентифікація відповідає на питання "що є або чого немає у людини" і допомагає підтвердити особу. Біометрична автентифікація забезпечує високий рівень довіри для кінцевих користувачів. Її складне програмне забезпечення дозволяє постачальникам знати, що людина є тією, за кого себе видає, завдяки видимим, реальним характеристикам. Навіть якщо кіберзлочинець знає пароль користувача або відповідь на секретне запитання, він не може скопіювати відбиток пальця або сканування райдужної оболонки ока.

– Простота використання: Хоча біометрія - це більше технічний аспект серверного процесу, з точки зору користувача вона часто є простішою і швидшою. Використання сканера відбитків пальців або розпізнавання обличчя для розблокування облікового запису може зменшити кількість входів за допомогою довгих паролів з декількома обмежувачами, які легко забути. Apple досягла значного прогресу в біометричній автентифікації, використовуючи на своїх пристроях як відбитки пальців, так і обличчя Apple досягла значного прогресу в біометричній автентифікації, використовуючи на своїх пристроях як відбитки пальців, так і обличчя.

– Виявлення шахрайства: Біометричні дані майже неможливо підробити. Їх важко скопіювати або вкрасти, а ймовірність того, що ваш відбиток пальця точно збігається з чиїмось іншим, становить 1 до 64

мільярдів. Шанси хакера отримати доступ до будь-чого, що захищене біометрично, надзвичайно низькі.

Ризики:

– Потенціал злому: біометричні дані можуть бути зламані. Компанії та уряди, які збирають і зберігають персональні дані, постійно перебувають під загрозою з боку хакерів. Однак біометричні дані незамінні в разі витоку даних, і організаціям необхідно поводитися з біометричними даними користувачів дуже відповідально.

– Нерозпізнавання реального користувача: коли ви реєструєтесь у системі розпізнавання обличчя, ви реєструєте певний ракурс і вираз обличчя. Однак система має дані лише на момент реєстрації, тому щоразу, коли користувач одягає окуляри, макіяж або навіть посміхається, системі розпізнавання обличчя складно розпізнати користувача, що може ускладнити процес входу в систему.

– Упередженість: Системи розпізнавання облич можуть бути менш точними в розпізнаванні людей з іншим кольором шкіри, раси, тощо. Багато біометричних систем навчаються переважно на фотографіях світлошкірих або темношкірих чоловіків. Це призводить до вроджених упереджень, які ускладнюють розпізнавання жінок і людей з іншим кольором шкіри. Неправильне застосування або навмисне зловживання технологією може призвести до дискримінації.

– Занепокоєння щодо обміну біометричними даними: чи є прийнятним для компаній продавати або обмінюватися біометричними даними з іншими особами, такими як правоохоронні органи, імміграційні служби та репресивні іноземні уряди. Ці проблеми конфіденційності призвели до прийняття законів про захист біометричних даних у багатьох штатах США. Коли біометричні дані зберігаються у форматі даних, користувачі ризикують залишити постійний цифровий запис, який може бути відстежений зловмисниками, особливо в місцях і країнах із суворими заходами спостереження.

– Зберігання даних: де б не зберігалися біометричні дані, вони повинні зберігатися надійно. Біометричні дані не можна скинути, як паролі. Якщо біометричні дані перехоплені, користувач нічого не може з цим зробити, оскільки він не може змінити свій відбиток пальця або райдужну оболонку ока.

Найвідоміші атаки на системи, що використовують біометричну автентифікацію:

– Підміна характеристик. Зловмисники копіюють біометричні характеристики законного користувача і подають їх біометричному датчику. Захист: висока деталізація зчитування.

– Копіювання поведінки користувача. Зловмисник записує поведінкові характеристики користувача та відтворює їх на біометричному датчику. Захист від: модифікації поведінки.

– Перехоплення біометричних показників. Зловмисник перехоплює біометричні дані легітимного користувача під час передачі між пристроями. Захист: шифрування біометричних даних.

– Тиражування біометричних "підписів". Зловмисник копіює показання біометричних датчиків ("підписи") і обробляє їх у системі так, ніби вони належать реальній людині. Захист: автентифікації біометричних "підписів".

РОЗДІЛ 2 СУЧАСНІ МЕТОДИ АВТЕНТИФІКАЦІЇ

2.1 Двофакторна автентифікація: використання пароля разом з іншим фактором, види та переваги

Хоч і паролі захищають цифрові активи, але цього недостатньо. Досвідчені кіберзлочинці активно намагаються розкрити паролі. Дізнавшись пароль, вони потенційно можуть отримати доступ до кількох облікових записів, в яких користувач повторно використовував цей пароль. Двофакторна та багатофакторна автентифікація - найкращий спосіб запобігти цьому.

Двофакторна автентифікація (2FA) - це додатковий рівень безпеки, який використовується для перевірки того, що особа, яка намагається отримати доступ до онлайн-акаунту, є тією, за кого себе видає. Спочатку користувач вводить ім'я користувача та пароль. Потім він повинен надати іншу інформацію для того, щоб отримати доступ. Методи двофакторної та багатофакторної автентифікації ґрунтуються на принципах "що ви знаєте", "що ви маєте" та "що існує".

Згідно з 2FA, навіть якщо тільки один з факторів автентифікації (п.1.1 розділу 1) скомпрометований, обліковий запис не може бути розблокований. Отже, якщо ваш пароль буде викрадений або мобільний телефон загублений, шанси того, що хтось інший отримає доступ до вашої вторинної інформації, дуже низькі. Іншими словами, якщо споживачі правильно використовують 2FA, веб-сайти та додатки можуть безпечніше ідентифікувати користувачів і розблоковувати їхні облікові записи.

Сьогодні існують різні типи двофакторної автентифікації, деякі з них надійніші та складніші за інші, але всі вони забезпечують кращий захист, ніж паролі. У цьому розділі розглядаються найпоширеніші форми 2FA.

– 2FA з апаратними токенами

Можливо, найстаріша форма 2FA, апаратні токени розміром з брелок для ключів, які генерують новий цифровий код кожні 30 секунд. Коли

користувач намагається отримати доступ до свого облікового запису, він дивиться на пристрій і повторно вводить відображений 2FA-код на веб-сайті або в додатку. Інші версії апаратних токенів автоматично передають 2FA-код при підключенні до USB-порту комп'ютера.

Однак це має кілька недоліків. Це дорого коштує компаніям для розгортання. Користувачі також вважають, що його можна легко загубити через його розмір. Найголовніше, він не є повністю стійким до хакерів.

– SMS та голосові 2FA

SMS 2FA взаємодіє безпосередньо з мобільним телефоном користувача. Після отримання імені користувача та пароля сайт надсилає користувачеві унікальний одноразовий пароль (OTP) за допомогою текстового повідомлення. Подібно до процесу для апаратних токенів, користувач повинен повторно ввести OTP в додаток, перш ніж отримати доступ до нього. Аналогічно, голосова 2FA автоматично набирає номер телефону користувача і усно надсилає 2FA-код.

Для онлайн-активностей з низьким рівнем ризику текстової або голосової автентифікації може бути достатньо. Однак для веб-сайтів, де зберігається особиста інформація (наприклад, енергетичні компанії, банки, електронні поштові скриньки), цей рівень 2FA може бути недостатньо безпечним. Насправді, SMS вважається найменш безпечним методом аутентифікації користувачів. Тому багато компаній виходять за рамки 2FA на основі SMS, щоб підвищити рівень безпеки.

– Програмні токени для 2FA

Найпоширеніша форма двофакторної автентифікації (і краща альтернатива SMS і голосу) використовує одноразові паролі, згенеровані програмним забезпеченням (також відомі як TOTP або "програмні токени").

Спочатку користувачі повинні завантажити та встановити додаток 2FA на свій смартфон або комп'ютер. Потім додаток можна використовувати на будь-якому сайті, який підтримує цей тип автентифікації. При вході в систему користувачі спочатку вводять своє ім'я користувача та пароль, а потім код,

який відображається в додатку, коли з'являється відповідний запит. Як і у випадку з апаратними токенами, термін дії програмних токенів зазвичай закінчується менш ніж за хвилину. Крім того, оскільки код генерується і відображається на одному і тому ж пристрої, програмні токени виключають можливість перехоплення хакерами. Це є основною проблемою для SMS та голосових методів передачі даних.

Основна привабливість рішень 2FA на основі додатків полягає в тому, що їх можна використовувати на мобільних та інших платформах і навіть в автономному режимі, що дозволяє здійснювати автентифікацію користувачів практично в будь-якому місці.

– Push-сповіщення для 2FA

Замість того, щоб покладатися на те, що користувач отримає і введе токен 2FA, веб-сайти і додатки тепер можуть надсилати користувачам push-сповіщення при спробі автентифікації. Власник пристрою може переглянути вміст і схвалити або заборонити доступ одним дотиком. Це безпарольна автентифікація без необхідності введення коду або додаткової взаємодії.

Push-сповіщення забезпечують пряме безпечне з'єднання між продавцем, 2FA-сервісом і пристроєм, що виключає можливість фішингу, атак типу "людина посередині" і несанкціонованого доступу. Однак це стосується лише пристроїв, підключених до Інтернету, які можна використовувати для встановлення додатків. SMS 2FA може бути кращим варіантом у регіонах з низьким рівнем мережі.

– Біометричний 2FA.

Цей метод використовує відбитки пальців, малюнок сітківки ока та розпізнавання обличчя для підтвердження особи. Також оцінюються навколишній шум, частота серцевих скорочень, шаблони набору тексту і відбитки голосу.

2.2 Багатофакторна автентифікація: процеси, переваги та способи її реалізації

Багатофакторна автентифікація (БФА) - це багатоетапний процес, який вимагає від користувача введення додаткової інформації, окрім пароля та другого фактору автентифікації. Наприклад, крім пароля, користувача можуть попросити ввести код, надісланий на електронну пошту, відповісти на секретне запитання або відсканувати відбиток пальця. Цей метод ще надійніший за двофакторну автентифікацію.

Багатофакторна автентифікація діє як додатковий рівень безпеки, щоб запобігти доступу неавторизованих користувачів до цих облікових записів, навіть якщо пароль буде викрадено. Компанії можуть використовувати багатофакторну автентифікацію для перевірки особи користувачів і надання швидкого та простого доступу авторизованим користувачам. Переваги багатофакторної автентифікації включають

– Зниження ризиків безпеки. Багатофакторна автентифікація мінімізує ризики, пов'язані з людськими помилками, неправильними паролями та втратою пристроїв.

– Сприяє цифровим ініціативам. Організації можуть впевнено впроваджувати цифрові ініціативи. Організації можуть убезпечити свою онлайн-взаємодію та транзакції, використовуючи багатофакторну автентифікацію для захисту корпоративних і користувацьких даних.

– Покращене реагування на загрози. Системи багатофакторної автентифікації можна налаштувати на проактивне надсилання сповіщень у разі виявлення підозрілого входу. Це дозволяє компаніям і приватним особам швидко реагувати на кібератаки та мінімізувати потенційні збитки.

Багатофакторна автентифікація працює, запитуючи у користувача кілька ідентифікаторів під час реєстрації облікового запису. Система зберігає цей ідентифікатор та інформацію про користувача і перевіряє його під час наступного входу в систему. Вхід - це багатоетапний процес, в якому разом з

паролем перевіряються інші ідентифікатори. Етапи процесу багатофакторної автентифікації такі:

– Реєстрація. Користувач створює обліковий запис з ім'ям користувача та паролем. Потім він прив'язує до свого облікового запису інші об'єкти, такі як мобільний телефон або фізичний апаратний брелок. Існують також віртуальні об'єкти, такі як адреси електронної пошти, номери мобільних телефонів і коди додатків для автентифікації. Всі ці елементи слугують для унікальної ідентифікації користувача і не повинні передаватися іншим особам.

– Автентифікація. Коли користувач з MFA входить на веб-сайт, йому пропонується ввести ім'я користувача та пароль (перший елемент - це те, що користувач знає), а також відповідь на автентифікацію від пристрою MFA (другий елемент - це те, що користувач має). Після того, як система перевірить пароль, вона підключається до інших елементів. Наприклад, цифровий код може бути виданий на апаратний пристрій або код може бути надісланий за допомогою SMS на мобільний пристрій користувача.

– Відповідь. Користувач завершує процес автентифікації, перевіряючи інші елементи. Наприклад, він може ввести отриманий код або натиснути кнопку на апаратному пристрої. Користувач отримує доступ до системи тільки після того, як вся інша інформація буде перевірена.

– Реалізація процесу.

Багатофакторна автентифікація може бути реалізована різними способами. Приклади наведені нижче:

– Система вимагає лише пароль та інший ідентифікатор. Це називається двофакторною або двоетапною автентифікацією.

– Замість цього сторонній додаток, який називається автентифікатором, перевіряє особу користувача. Користувач вводить пароль в автентифікатор, який аутентифікує користувача в системі.

– Під час автентифікації користувач вводить біометричні дані, скануючи частину тіла, наприклад, відбиток пальця або сітківку ока.

– Система може вимагати багаторазову автентифікацію лише при першому доступі до нового пристрою. Після цього система запам'ятовує пристрій і вимагає лише введення пароля.

Нижче наведено приклади того, як компанія може використовувати багатофакторну автентифікацію.

– Віддалений доступ для співробітників

Компанія хоче надати своїм співробітникам віддалений доступ до ресурсів. Багатофакторну автентифікацію можна налаштувати так, щоб вона вимагала входу в систему, використання апаратного брелока та сканування відбитків пальців на ноутбуках компанії, які працівники беруть із собою додому. Залежно від IP-адреси працівника, компанія може встановити правила, які вимагатимуть від нього використання двофакторної автентифікації під час роботи вдома. Однак, коли працівник працює в іншій мережі Wi-Fi, може знадобитися трифакторна автентифікація.

– Доступ до системи можуть мати лише співробітники на місці.

Лікарня хоче надати всім працівникам доступ до медичних програм і даних пацієнтів. Лікарня видає працівникам безконтактні бейджі, щоб вони могли отримати доступ до цих додатків під час чергування. На початку кожної зміни працівники повинні увійти в систему і прив'язати свої бейджі до центральної системи. Один дотик до бейджа протягом зміни забезпечує доступ до всіх ресурсів без будь-яких додаткових вимог до входу в систему. Наприкінці зміни права доступу в один дотик втрачають чинність. Це мінімізує ризик несанкціонованого доступу через втрату бейджів.

Додатки повинні збирати та зберігати цю інформацію разом з паролями під час реєстрації. Компанії, що використовують додатки, повинні захищати біометричну інформацію. Для цього компанії повинні розробити політику обмеження доступу до цифрових ресурсів та їхнього захисту. Нижче наведено кілька найкращих практик контролю доступу.

– Ролі користувачів.

Розподіл користувачів на ролі дозволяє вам точно налаштувати політику контролю доступу. Наприклад, привілейованим адміністраторам можна надати більше прав доступу, ніж кінцевим користувачам.

– Надійна політика паролів.

Незалежно від того, чи використовуєте ви трифакторну або чотирифакторну автентифікацію, вам все одно потрібно впровадити надійну політику. Правила можна застосовувати для створення паролів, які поєднують великі та малі літери, спеціальні символи та цифри.

– Ротація облікових даних безпеки

Належною практикою є прохання до користувачів регулярно змінювати свої паролі. Цей процес можна автоматизувати, заблокувавши доступ до системи до зміни пароля.

– Політика найменших привілеїв.

Завжди створюйте нових користувачів з найнижчими привілеями та правами доступу в системі. Ви можете надавати привілеї вручну або поступово підвищувати їх у міру того, як зростає довіра користувача до автентифікованих облікових даних.

2.3 Роль ШІ в автентифікації: поведінкова біометрія, виявлення аномалій, безперервна та адаптивна автентифікація

Штучний інтелект (ШІ) відіграє важливу роль у створенні більш безпечних систем автентифікації; ШІ здатен вдосконалити системи автентифікації, використовуючи такі можливості, як аналіз даних, розпізнавання образів і машинне навчання.

Одним із способів, як ШІ може революціонізувати автентифікацію, є поведінкова біометрія. Поведінкова біометрія аналізує поведінкові патерни людей, такі як швидкість набору тексту, рухи миші та активність на сенсорному екрані, щоб створити унікальні профілі користувачів. Алгоритми штучного інтелекту можуть аналізувати ці дані в режимі реального часу і

порівнювати їх з відомою поведінкою користувача, щоб підтвердити його особу. Такий підхід додає додатковий рівень безпеки, оскільки зловмиснику складно точно імітувати унікальну поведінку людини.

Виявлення аномалій на основі штучного інтелекту - потужний спосіб побудови безпечних систем автентифікації. Він аналізує дані про поведінку користувача, щоб виявити аномалії, які відхиляються від звичайних шаблонів користувача. Наприклад, якщо користувач, який зазвичай входить в систему з певного місця, раптом намагається увійти з іншого місця, система може вважати це аномалією і вимагати додаткової перевірки, адже алгоритми ШІ можуть швидко аналізувати великі обсяги даних і виявляти аномалії в режимі реального часу, забезпечуючи додатковий рівень захисту від шахрайства.

Розпізнавання облич - ще одна сфера, де ШІ досягає значних успіхів в аутентифікації: Системи розпізнавання облич на основі ШІ використовують алгоритми глибокого навчання для аналізу рис обличчя і створення біометричних шаблонів. Потім ці шаблони порівнюються зі збереженими даними про обличчя користувача, щоб підтвердити його особу. Розпізнавання обличчя - це ненав'язливий і зручний метод автентифікації, який можна використовувати в різних сферах - від розблокування смартфонів до доступу до захищених об'єктів.

ШІ також використовується для розпізнавання голосу, ще однієї форми біометричної автентифікації, де алгоритми ШІ аналізують характеристики голосу, такі як висота, тон і особливості мовлення, щоб створити унікальний голосовий відбиток для кожного користувача. Цей голосовий відбиток порівнюється із записаними голосовими даними користувача, після чого виконується автентифікація. Розпізнавання голосу набуло популярності в таких додатках, як автентифікація в колл-центрах і голосові асистенти, завдяки простоті використання і точності.

Безперервна автентифікація - це новий тренд, який використовує ШІ для забезпечення безперервної автентифікації протягом усього сеансу роботи користувача або транзакції. На відміну від традиційних методів

автентифікації, які застосовуються лише під час входу в систему, безперервна автентифікація відстежує та аналізує дані про поведінку користувача протягом усього сеансу, щоб гарантувати, що його особистість захищена. Алгоритми штучного інтелекту можуть виявляти зміни в поведінці користувача і запускати додаткові етапи автентифікації, коли це необхідно, забезпечуючи динамічний і надійний механізм автентифікації.

Розглянемо, що таке адаптивна багатофакторна автентифікація і яке значення в ній має штучний інтелект. Вона використовує бізнес-правила та інформацію про користувача, щоб визначити, які фактори автентифікації слід застосовувати. Компанії використовують адаптивну автентифікацію, щоб збалансувати вимоги до безпеки та користувацького досвіду.

Рішення для адаптивної автентифікації використовують штучний інтелект (ШІ) та машинне навчання (МН) для аналізу тенденцій доступу та виявлення підозрілої поведінки. Ці рішення можуть відстежувати поведінку користувачів протягом тривалого часу для виявлення шаблонів, створення базових профілів користувачів і виявлення незвичайної поведінки, наприклад

– Кількість невдалих спроб входу.

– Географічне розташування користувача.

– Географічна швидкість або фізична відстань між послідовними спробами входу.

– Пристрій, що використовується для входу.

– День тижня та час спроби входу.

– Операційна система.

– Вихідна IP-адреса.

– Роль користувача.

Алгоритм машинного навчання присвоює підозрілим подіям оцінку ризику і в режимі реального часу коригує численні фактори автентифікації відповідно до бізнес-політики. Наприклад, якщо поведінка класифікується як низький ризик, користувач може увійти в систему, використовуючи лише ім'я користувача та пароль. З іншого боку, поведінка середнього рівня ризику

вимагає введення SMS-коду, а якщо поведінка є високоризикованою, користувачеві взагалі відмовляють у доступі.

РОЗДІЛ 3 ТЕХНІЧНА РЕАЛІЗАЦІЯ МЕТОДУ АВТЕНТИФІКАЦІЇ

3.1 Огляд застосунків: Authy 2FA, FreeOTP, Google Authenticator, Microsoft Authenticator

В попередніх розділах було розглянути всі методи автентифікації, як ми вже довели, парольна автентифікація є занадто слабкою і легко піддається атакам, тому її потрібно підсилити другим фактором при вході в систему. Вибір другого фактора складав між біометричною і OTP, але визначивши що є декілька значних мінусів в біометричної, а саме високі ризики, тому що біометричні дані незамінні і в разі витоку даних, зловмисник може отримати біометрику користувачів, що може бути набагато небезпечнішим ніж розкриття пароля. Також є можливість нерозпізнавання реального користувача, навіть не велика зміна може не співпадати з тою що була при реєстрації і система не надасть доступ реальному користувачу. Та ще один вагомий недолік, це можливість занепокоєння користувачів щодо надавання своїх біометричних даних, через що організація може втратити потенційних користувачів та відповідно прибуток.

Отже двофакторна автентифікація за допомогою біометрики підійде для добре захищених компаній з високою довірою від користувачів. Тому далі я огляну програми для двофакторної автентифікації із OTP паролем, на мою думку це є одним з найкращих рішень для малих та середніх організацій по відношенню зручність та безпека. Розглянемо та порівняємо 4 застосунки для двофакторної автентифікації, а саме Google Authenticator, Microsoft Authenticator, Authy 2FA, FreeOTP і виберемо одну для її технічної реалізації. Для зручності порівняння всю інформацію про додатки наведемо в таблиці нижче. Варто зауважити, що ці всі застосунки є безкоштовними та ними може скористуватись кожен користувач.

Таблиця 3.1 – Порівняльний аналіз застосунків для 2FA

Назва застосунку	Google Authenticator	Microsoft Authenticator	Authy 2FA	FreeOTP
Алгоритми генерації одноразових паролів	TOTP, HOTP	TOTP	TOTP	TOTP, HOTP
Приницп роботи	6-ти або 8-мизначний одноразовий пароль в якості другого фактора	1)6-ти або 8- ми значний одноразовий пароль в якості другого фактора 2)розпізнавання облич, сканер відбитку або введення пін, замість паролю 3) підтвердження в застосунку в якості другого фактора	1)6-ти або 8- ми значний одноразовий пароль в якості другого фактора 2)розпізнавання облич, сканер відбитку або введення пін, замість паролю 3)підтвердження в застосунку в якості другого фактора	6-ти або 8-мизначний одноразовий пароль в якості другого фактора
Розробник застосунку	Google	Microsoft	Authy	Red Hat
Відкрите програмне забезпечення	Так	Ні	Ні	Так

Продовження таблиці 3.1

Онлайн синхронізація	Так	Так	Так	Ні
Хеш	Ні	Ні	Ні	Так
Підтримувані операційні системи	Android,iOS, BlackBerry, J2ME	Android, iOS	Windows, MacOS, Linux, iOS, Android	Android, iOS
Оцінка на Google Play	3,4	4,8	3,1	4,4
Розмір застосунку	7.11 Мб	41 Мб	26 Мб	5,6 Мб
Кількість завантажень на Google Play	100млн+	50млн+	10млн+	1млн+

Результати аналізу додатків для автентифікації представлені в таблиці 3.1. Видно, що деякі з проаналізованих додатків можуть використовувати особливі фактори (наприклад, відбитки пальців чи біометрчині дані) як другий фактор, окрім OTP автентифікації. Для технічної реалізації було обрано додаток Google Authenticator.

3.2 Підключення 2FA із використаням Google Authenticator

В ході технічної реалізації двофакторної автентифікації було створено сайт з регістрацією та авторизацією та підключення 2FA із використаням Google Authenticator, для цього використовувались наступні технології: html, php, MySQL.

Реалізація сервера була здійснена за домогою програмне середовище Open Server, яка надає змогу зробити свій локальний сервер. Для підключення бази даних до проєкту був створений файл connect.php із наступним кодом (див. лістинг 3.1).

Лістинг 3.1 – Підключення проєкту до бази даних

```
<?php

    $connect = mysqli_connect('localhost', 'root', '', 
'test');

    if (!$connect)
    {
        die('Error connect to DataBase');
    }
?>
```

Наступним кроком було написання коду вигляду сайту, а саме сторінки з реєстрацією (див. рис. 3.1), входом (див. рис. 3.2) та профілем(див. рис. 3.3):

– register.php – форма реєстрації. Додаток А

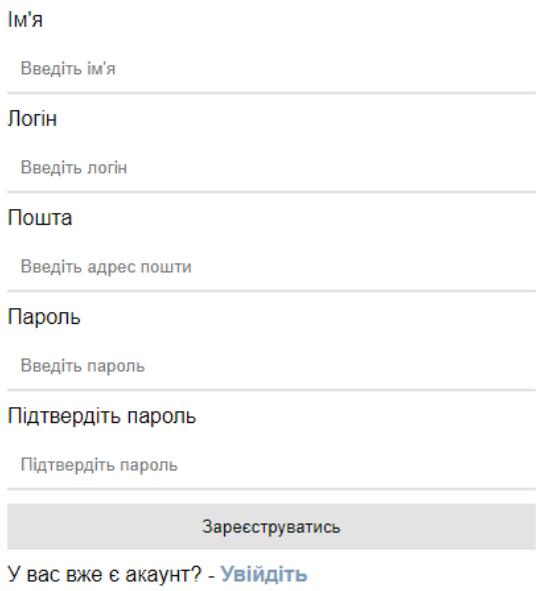


Рисунок 3.1 – Вигляд форми реєстрації

– index.php – форма входу. Додаток Б

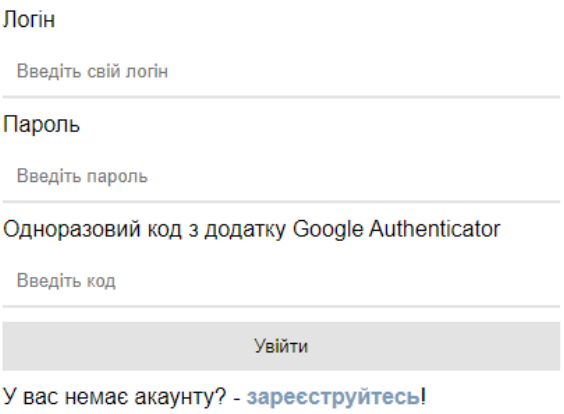


Рисунок 3.2 – Вигляд форми входу

– profile.php – форма профілю. Додаток В

Рисунок 3.3 – Вигляд форми профілю

Далі було створено таблицю в базі даних (див. рис. 3.4). Написано код (Додаток Г) для обробки даних з форми реєстрації та їх завантаження в базу даних..

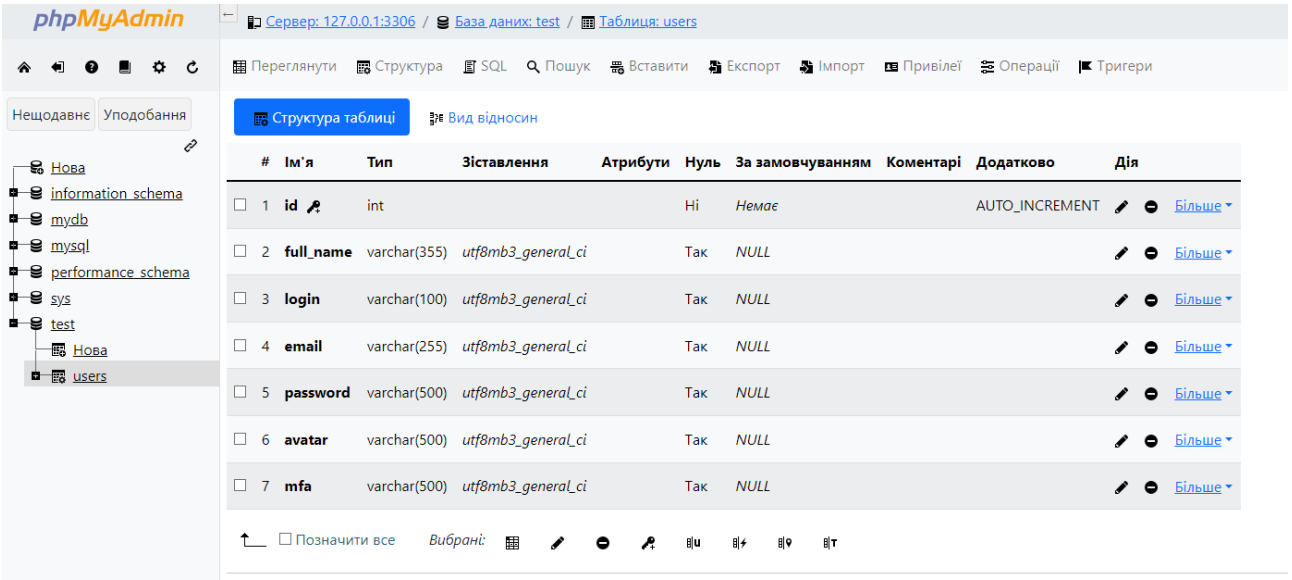


Рисунок 3.4 – Вигляд таблиці в базі даних

Для підключення 2FA було використано клас PHPGangsta_GoogleAuthenticator, що реалізує TOTP стандарт, який було взято з відкритиго проєкту на GitHub[13]. Нижче в лістингу 3.2 наведено уривок коду для підключення класу який може створювати секрети, генерувати коди, перевіряти коди та представляти QR-код для сканування секрету. Він реалізує TOTP відповідно до RFC6238.

Лістинг 3.2 – Код для підключення 2FA

```
require_once 'GoogleAuthenticator.php';
$ga = new PHPGangsta_GoogleAuthenticator();
$mfa = $ga->createSecret();
$qrCodeUrl = $ga->getQRCodeGoogleUrl($email, $mfa);
echo "<p>Додайте даний ключ в додатку Google Authenticator: 
".$mfa."</p>";
echo '<p>Або проскануйте QR code через додаток:</p><img 
src="'.$qrCodeUrl.'">';
```

Останнім кроком було написання коду для обробки даних входу з перевіркою логіну, паролю та одноразового коду із застосунку Google Authenticator. Код для перевірки OTP наведено в Лістингу 3.3. У випадку коректно введених даних перенаправляє на сторінку профілю користувача. В іншому випадку висвітлює повідомлення, про невірно введені дані входу. Додаток Д.

Лістинг 3.3 – Код для перевірки OTP

```
$secret=$user['mfa'];
$ga = new PHPGangsta_GoogleAuthenticator();
$checkResult = $ga->verifyCode($secret, $mfa, 2);
if ($checkResult)
   {
      header('Location: ../profile.php');
   }else
     {
$_SESSION['message'] = 'Код введено не вірно, спробуйте ще раз';
      header('Location: ../index.php');
      }
```

3.3 Тестування впровадженої 2FA

В цьому розділі буде проведене тестування впровадженої 2FA на коректність роботи, першим кроком стала перевірка реєстрації.
Вводимо коректну інформацію у відповідну форму (Рисунок 3.5).

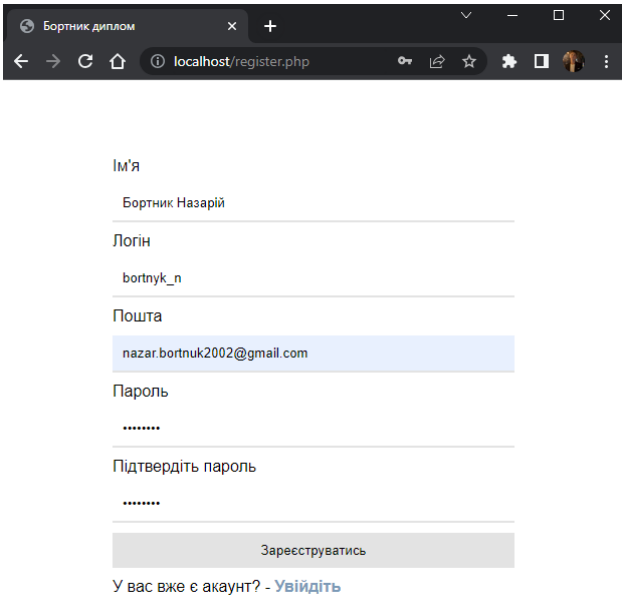


Рисунок 3.5 – Заповнена форма реєстрації

За допомогою застосунку на смартфоні вводим секретний ключ або скануємо QR-код (Рисунок 3.6).

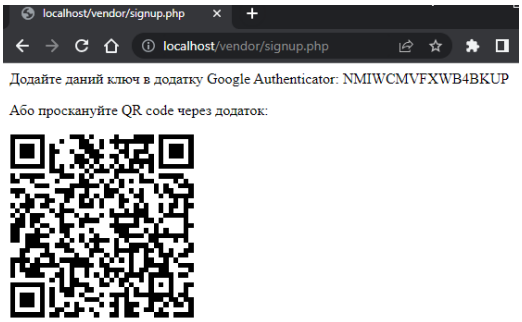
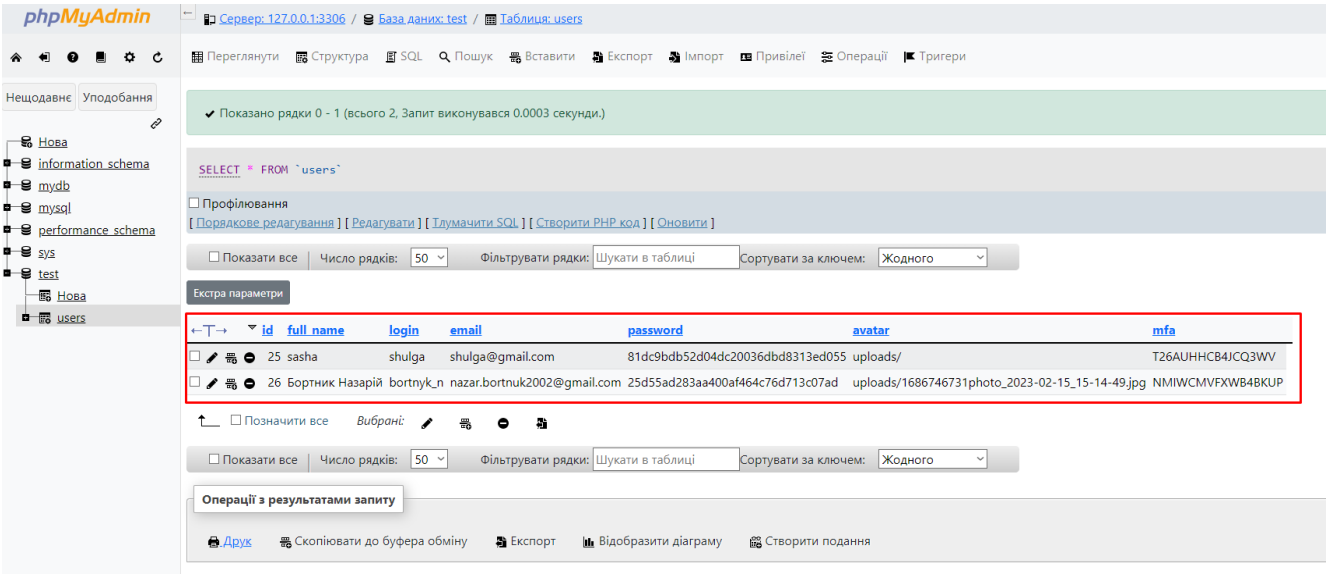


Рисунок 3.6 – Вигляд форми під’єднання 2FA

Перевіримо чи записались всі дані користувача в базу даних (див. рис. 3.7)



Рисунко 3.7 – Таблиця в базі даних

Перевірка входу. Вводим логін, пароль і одноразовий код (Рисунок 3.8).

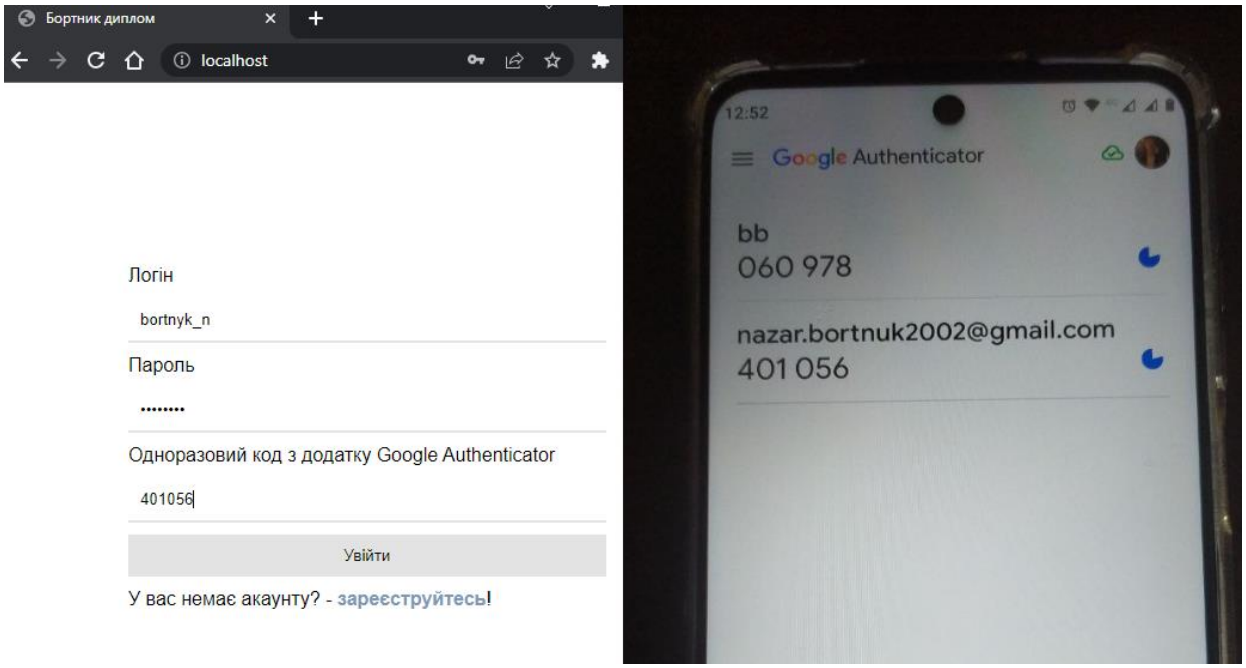


Рисунок 3.8 – Вигляд автентифікації із 2FA

Потрапляємо на сторінку профілю користувача (Рисунок 3.9).

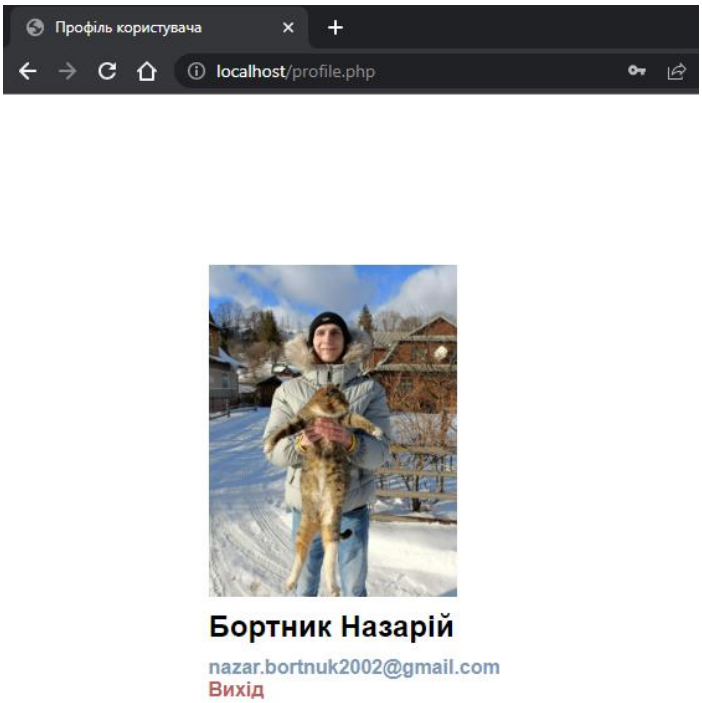


Рисунок 3.9 – Вигляд профілю користувача

Якщо введимо некоректнний одноразовий пароль ми побачимо повідомлення про відмову в автентфиікації (див. рис. 3.10).

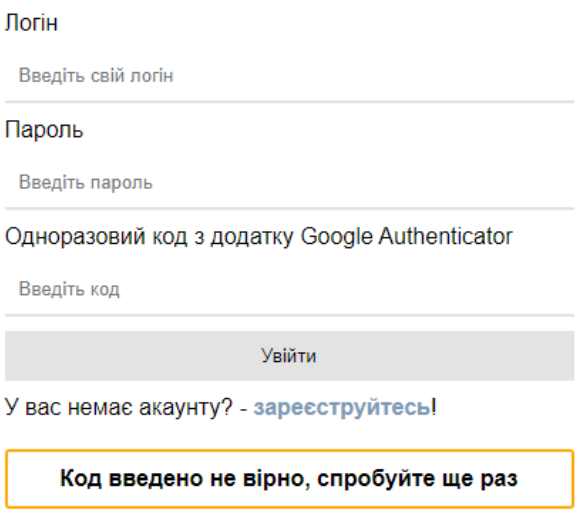


Рисунок 3.10 – Вигляд сторінки з сповіщенням про відмову в автентифікації

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Долікарська допомога при пораненнях.

Всі працівники які займаються автентифікацією та її технічною реалізацією повинні вміти надавати першу медичну допомогу при травмах. Якщо цілісність шкіри або глибоких тканин порушена, шкіру навколо рани слід обробити йодом або спиртом. Не рекомендується промивати рану водою або дезінфікуючими засобами. Після обробки рани слід накласти стерильну пов'язку. Пов'язка захищає рану від забруднення та інфекції, полегшує біль і заспокоює пацієнта, коли він бачить перев'язану рану, це викликає відчуття захищеності.

Догляд за ранами вимагає дотримання наступних правил:

– Перед обробкою рани вимити руки (протерти спиртом).

– Після обробки навколишньої шкіри йодом або перекисом водню, невеликі рани та виразки слід закрити лейкопластиром або медичним клеєм БФ-6.

– Не видаляйте з рани сторонні предмети або бруд, оскільки це може пошкодити кровоносні судини і викликати кровотечу.

– Очистіть шкіру навколо рани, протираючи її від країв назовні марлею, бинтом або бавовняною тканиною, змоченою спиртом або спиртово-йодним розчином.

– Зробіть пов'язку або окремий тканинний мішечок, щоб покрити всю рану, накладіть його на рану і обмотайте або закрийте смужкою бинта.

– Якщо видно внутрішні органи, мозок або сухожилля, рану слід ретельно закрити стерильною пов'язкою або накрити стерильним матеріалом, щоб запобігти інфікуванню.

У випадку проникаючих поранень метою першої допомоги є запобігання інфікуванню. Проникаючі поранення грудей можуть бути пов'язані з

пневмотораксом і кровохарканням, коли повітря потрапляє в підшкірну клітковину і виглядає як згусток, але при дотику видає звук потріскування.

Пневмоторакс - це скупчення в грудній порожнині повітря, яке потрапило через рану в грудях (відкритий пневмоторакс) або через пошкодження легень чи бронхів (закритий пневмоторакс). Він призводить до виснаження органів середостіння і супроводжується порушенням дихання і кровообігу.

При проникаючих ранах грудної клітки перша допомога повинна бути спрямована на запобігання пневмотораксу, шоку та інфікуванню поверхні рани. Постраждалого слід покласти в напівсидяче положення і накласти герметичну пов'язку, щоб запобігти потраплянню повітря в плевральну порожнину. Для цього після обробки рану слід накрити лейкопластиром. Для фіксації рани на грудній клітці лейкопластиром можна також використовувати обгортки від туалетного пакета, клейонку, целофанові пакети або серветки, змащені вазеліном.

Перша допомога при пораненнях, що проникають у черевну порожнину. Зазвичай це вогнепальні або колото-різані поранення. Всі поранення живота характеризуються сильним болем у животі, напруженням м'язів черевної стінки (живіт діє як "тарілка"), ознаками внутрішньої кровотечі, шоком і колапсом. Великі крововиливи супроводжуються пошкодженням твердих органів (печінки, селезінки, нирок). З'являються характерні ознаки крововиливу: підвищена слабкість, загальна блідість, нудота, блювання, холодні кінцівки. Пульс рідкий і слабкий, артеріальний тиск падає. Поранення шлунково-кишкового тракту призводить до швидкого прогресування перитоніту з виходом кишкового вмісту у вільну черевну порожнину та її інфікуванням (перитоніт).

У всіх випадках проникаючих поранень черевини необхідна перев'язка рани та стерильні перев'язувальні матеріали. Слід запобігати потраплянню в порожнину черевини кишкових петель і сальника, опущених у рану. Анальгетики не слід призначати за відсутності чітких симптомів

проникаючого поранення живота. Категорично заборонено вживати воду та їжу. Люди з проникаючими пораненнями живота повинні бути негайно госпіталізовані і транспортуватися на ношах. Проникаючі поранення живота потребують невідкладного хірургічного втручання протягом перших кількох годин, поки не розвинулася інфекція або кровотеча.

4.2 Вимоги до профілактичних медичних оглядів для працівників ПК

Профілактичні медичні огляди важливі для всіх, хто працює з візуальними дисплейними терміналами (ВДТ), відповідно до вимог щодо профілактичних медичних оглядів згідно ДСанПІН 3.3.2.007-98 „Державні санітарні правила і норми роботи з візуальними дисплейними терміналами (ВДТ) електронно-обчислювальних машин".

Працівники, які працюють з ВДТ, зобов'язані проходити попередні (під час прийняття на роботу) та періодичні (протягом трудової діяльності) медичні огляди відповідно до наказу Міністерства охорони здоров'я України. Періодичні методичні огляди повинні проводитися кожні два роки комісією у складі терапевта, офтальмолога і невропатолога. Комісія, що проводить попередні та періодичні огляди, може в разі потреби (за наявності медичних показань) залучати до обстеження лікарів інших спеціальностей. Головними критеріями оцінки придатності до роботи з ВДТ є показники стану органів зору: рефракція, гострота зору, акомодація та стан бінокулярного апарату. Стан організму також повинен бути врахований.

Для жінок, які працюють у ВДТ з комп'ютерами та ПК, слід враховувати наступне. Вони повинні проходити огляд у акушера-гінеколога кожні два роки. Жінки в період вагітності та годування груддю, перед виконанням будь-якої роботи, пов'язаної з використанням ПК або ВДТ.

Протипоказання, пов'язані із зоровою системою:

– Скоригована гострота зору повинна бути не менше 0,5 на одне око і 0,2 на обидва ока.

– Рефракція: короткозорість не менше 6,0 дптр та далекозорість не менше 4,0 дптр, астигматизм (будь-якого типу) 3,0 дптр або більше.

– Відсутність гостроти зору на обох очах.

– Лагофтальм.

– Хронічні захворювання переднього відділу ока.

– Захворювання сітківки ока і зорового нерва.

– Глаукома.

– Загальні (фізичні) протипоказання.

– Вроджені проблеми органів з сильними порушеннями функцій.

– Захворювання центральної нервової системи з вираженими порушеннями її функцій.

– Хронічні психічні та психогенні розлади, при яких пацієнт підлягає обов'язковому динамічному спостереженню в психоневрологічному диспансері; Тяжкі прикордонні психічні розлади. У випадках тяжких пограничних психічних розладів відповідне питання про придатність до роботи вирішується комісією лікарів-психіатрів.

– Ендокринні захворювання з вираженими порушеннями функції ендокринних залоз.

– Злоякісні новоутворення (придатність до роботи після лікування визначається індивідуально).

– Всі захворювання органів кровотворення (незалежно від стадії).

– Гіпертонічна хвороба III стадії.

– Хронічні захворювання легень з вираженою серцево-легеневою недостатністю.

– Тяжка бронхіальна астма. Функціональні розлади дихання та кровообігу.

– Активний туберкульоз у будь-якій локалізації.

– Виразкова хвороба шлунка та дванадцятипалої кишки з хронічними рецидивуючими виразками.

– Цироз печінки та активний хронічний гепатит.

– Хронічні форми захворювань нервової системи.

– Хронічні захворювання нирок з симптомами ниркової недостатності.

– Захворювання хребетної нервової системи (корінцевий синдром на шийному та попереково-крижовому рівнях).

– Колагенові захворювання.

– Вагітність і лактація.

– Аномалії розвитку плода в анамнезі жінок, які планують мати дітей.

Виявлені хронічні неспецифічні захворювання (гіпертонічна хвороба, виразка шлунка, виразка дванадцятипалої кишки, хронічні захворювання бронхо-легеневої та гепатобіліарно-панкреатичної систем) виявлені, особи, які використовують комп'ютери та ПК з ВДТ, повинні виконувати систематичні медичні огляди та лікування.

ВИСНОВКИ

У ході даної кваліфікаційної роботи було проведено дослідження методів автентифікації та їх технічна реалізація. Були розглянуті різні методи автентифікації, включаючи використання пароля, біометрії, push-сповіщень, мобільних додатків та апаратних токенів.

Зокрема, було зосереджено увагу на двофакторній автентифікації з використанням одноразових паролів (OTP). Використання OTP забезпечує додатковий рівень безпеки, оскільки для автентифікації необхідно мати не тільки пароль, але й фізичний пристрій для знання одноразового пароля. Це дозволяє ускладнити процес несанкціонованого доступу до облікових записів та захистити дані користувачів.

В рамках роботи була проведена технічна реалізація двофакторної автентифікації з використанням OTP для веб-сайту. Було розроблено відповідний код з інтеграцією Google Authenticator API, який включає створення та перевірку одноразових паролі при вході на веб-сайт.

Однак варто відзначити, що розглянуті методи автентифікації та їх технічна реалізація мають свої переваги та ризики. Вибір конкретного методу повинен залежати від потреб організації та користувачів, рівня безпеки, зручності використання, вартості та інших факторів.

Загалом, впровадження двофакторної автентифікації з OTP є ефективним заходом для підвищення рівня безпеки в інформаційному середовищі. Враховуючи зростаючі загрози в сфері кібербезпеки, використання двофакторної автентифікації може допомогти уникнути несанкціонованого доступу та зберегти конфіденційні дані.

Однак слід пам'ятати, що безпека - це постійний процес, і важливо постійно оновлювати та вдосконалювати методи автентифікації, щоб залишатися кроком попереду зловмисників. Тому перспективи проведення подальших досліджень у галузі автентифікації будуть завжди. Технології стрімко розвиваються і це ж стосується автентифікації, дослідження в цій

галузі можуть допомогти виявити нові підходи, методи та інновації для покращення безпеки і зручності автентифікаційних систем. Законодавство щодо захисту даних та безпеки постійно змінюється, і організації повинні відповідати цим вимогам. Тому дослідження в галузі автентифікації також можуть спрямовуватись на розробку методів, які відповідають новим правилам та вимогам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Балацька, В., Полотай, О., & Пузир, А. (2022). Автентифікація як один з механізмів забезпечення безпеки операційних систем, 288.

2. Бондаренко, О. В., & Карпінець, В. В. (2020). Двофакторна аутентифікація в системах контролю і управління доступом (Doctoral dissertation, ВНТУ).

3. Білан, Л. О. (2021). Методи двофакторної автентифікації користувачів в мобільних пристроях.

4. Горбенко, О. В., Горбенко, Ю. Л., Горбенко, А. Ю., & Сівоха, О. М. (2020). Захист інформаційних систем за допомогою використання методів автентифікації. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського, 79-85.

5. Діденко, К. О., & Мілінчук, Ю. А. (2020). Класифікація видів автентифікації.

6. Поворознюк, А. І., Поворознюк, О. А., & Філатова, Г. Є. (2021). Багатокритеріальна оцінка альтернатив при проєктуванні двохфакторної автентифікації суб'єктів-користувачів в системах захисту інформації.

7. Wijayarathna, C., & Arachchilage, N. A. (2019). An empirical usability analysis of the google authentication api. In Proceedings of the evaluation and assessment on software engineering (pp. 268-274).

8. Ibrokhimov, S., Hui, K. L., Al-Absi, A. A., & Sain, M. (2019, February). Multi-factor authentication in cyber physical system: A state of art survey. In 2019 21st international conference on advanced communication technology (ICACT) (pp. 279-284). IEEE.

9. Bartłomiejczyk, M., & Kurkowski, M. (2019). Протокол багатофакторної автентифікації в мобільному середовищі. IEEE Access , 7 , 157185-157199.

10. Jalbani, K. B., Jalbani, A. H., & Soomro, S. S. (2020). IoT Security: To Secure IoT Devices with Two-Factor Authentication by Using a Secure Protocol.

In Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital (pp. 98-118). IGI Global.

11. What is the Microsoft Authenticator app? [Електронний ресурс] – Режим доступу до ресурсу: Використання програми Microsoft Authenticator - Підтримка від Microsoft

12. TouchID, PIN, Password, Encryption [Електронний ресурс] // Authy. – 2019. – Режим доступу до ресурсу: https://authy.com/features/secure/

13. Google Authenticator PHP class [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/PHPGangsta/GoogleAuthenticator

ДОДАТКИ

Додаток А Лістинг коду форми реєстрації

```
<?php
   session_start();
   if ($_SESSION['user']) {
      header('Location: profile.php');
   }
?>
<!doctype html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <title>Бортник диплом</title>
   <link rel="stylesheet" href="assets/css/main.css">
</head>
<body>
   <!-- Форма реєстрації -->
   <form action="vendor/signup.php" method="post" enctype="multipart/form-data">
      <label>Ім'я</label>
      <input type="text" name="full_name" placeholder="Введіть ім'я">
      <label>Логін</label>
      <input type="text" name="login" placeholder="Введіть логін">
      <label>Пошта</label>
      <input type="email" name="email" placeholder="Введіть адрес пошти">
      <label>Пароль</label>
      <input type="password" name="password" placeholder="Введіть пароль">
      <label>Підтвердіть пароль</label>
      <input type="password" name="password_confirm" placeholder="Підтвердіть пароль">
      <button type="submit">Зареєструватись</button>
      <p>
         У вас вже є акаунт? - <a href="/">Увійдіть</a>
      </p>
      <?php
         if ($_SESSION['message']) {
            echo '<p class="msg"> ' . $_SESSION['message'] . ' </p>';
         }
         unset($_SESSION['message']);
      ?>
   </form>

</body>
</html>
```

Додаток Б Лістинг коду форми входу

```
<?php
session_start();

if ($_SESSION['user']) {
    header('Location: profile.php');
}

?>

<!doctype html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Бортник диплом</title>
    <link rel="stylesheet" href="assets/css/main.css">
</head>
<body>

<!-- Форма авторизації -->

    <form action="vendor/signin.php" method="post">
        <label>Логін</label>
        <input type="text" name="login" placeholder="Введіть свій логін">
        <label>Пароль</label>
        <input type="password" name="password" placeholder="Введіть пароль">
        <label>Одноразовий код з додатку Google Authenticator</label>
        <input type="text" name="mfa" placeholder="Введіть код">
        <button type="submit">Увійти</button>
        <p>
            У вас немає акаунту? - <a href="/register.php">зареєструйтесь</a>!
        </p>
        <?php
            if ($_SESSION['message']) {
                echo '<p class="msg"> ' . $_SESSION['message'] . ' </p>';
            }
            unset($_SESSION['message']);
        ?>
    </form>

</body>
</html>
```

Додаток В Лістинг коду форми профілю

```
<?php
session_start();
if (!$_SESSION['user']) {
    header('Location: /');
}
?>

<!doctype html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Профіль користувача</title>
    <link rel="stylesheet" href="assets/css/main.css">
</head>
<body>

    <!-- Профіль -->

    <form>
        <img src="<?= $_SESSION['user']['avatar'] ?>" width="200" alt="">
        <h2 style="margin: 10px 0;"><?= $_SESSION['user']['full_name'] ?></h2>
        <a href="#"><?= $_SESSION['user']['email'] ?></a>
        <a href="vendor/logout.php" class="logout">Вихід</a>
    </form>

</body>
</html>
```

Додаток Г Лістинг коду обробки даних з форми реєстрації

```
<?php

    session_start();
    require_once 'connect.php';
    require_once 'GoogleAuthenticator.php';

    $full_name = $_POST['full_name'];
    $login = $_POST['login'];
    $email = $_POST['email'];
    $password = $_POST['password'];
    $password_confirm = $_POST['password_confirm'];


    if ($password === $password_confirm) {

        $path = 'uploads/';
        $password = md5($password);
        $ga = new PHPGangsta_GoogleAuthenticator();
        $mfa = $ga->createSecret();
        $qrCodeUrl = $ga->getQRCodeGoogleUrl($email, $mfa);
        echo "<p>Додайте даний ключ в додатку Google Authenticator:
".$mfa."</p>";
        echo '<p>Або проскануйте QR code через додаток:</p><img
src="'.$qrCodeUrl.'">';

        mysqli_query($connect, "INSERT INTO `users` (`full_name`, `login`, `email`,
`password`, `avatar`, `mfa`) VALUES ('$full_name', '$login', '$email', '$password',
'$path', '$mfa')");


    } else
    {
        $_SESSION['message'] = 'Пароли не совпадают';
    }
?>
```

Додаток Д Лістинг обробки даних з форми входу

```
<?php

   session_start();
   require_once 'connect.php';
   require_once 'GoogleAuthenticator.php';

   $login = $_POST['login'];
   $password = md5($_POST['password']);
   $mfa=$_POST['mfa'];


   $check_user = mysqli_query($connect, "SELECT * FROM `users` WHERE
`login` = '$login' AND `password` = '$password'");
   if (mysqli_num_rows($check_user) > 0) {

      $user = mysqli_fetch_assoc($check_user);

      $_SESSION['user'] = [
         "id" => $user['id'],
         "full_name" => $user['full_name'],
         "avatar" => $user['avatar'],
         "email" => $user['email']
      ];
      $secret=$user['mfa'];
      $ga = new PHPGangsta_GoogleAuthenticator();
      $checkResult = $ga->verifyCode($secret, $mfa, 2);
      if ($checkResult)
      {
         header('Location: ../profile.php');
      }else
         {
         $_SESSION['message'] = 'Код введено не вірно, спробуйте ще раз';
         header('Location: ../index.php');
         }


   }else
   {
      $_SESSION['message'] = 'Пароль введено не вірно, спробуйте ще раз';
      header('Location: ../index.php');
   }
   ?>
```