

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

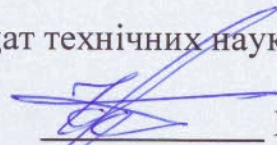
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології захисту інформації в соціальних мережах»

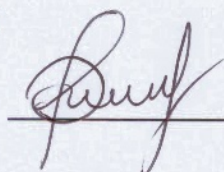
Виконала студентка 2-го курсу групи КБм-23-1
спеціальності 125 «Кібербезпека та захист інформації»

 М. О. Сябрук

Керівник доцент кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 Ю. Б. Бродський

Рецензент старший викладач кафедри комп'ютерної
інженерії та кібербезпеки

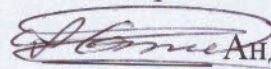
 Є. М. Трокоз

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

17 вересня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студентка: Сябрук Марія Олександрівна

Тема роботи: «Методи та технології захисту інформації в соціальних мережах»

затверджена Наказом університету від 17 вересня 2024 р. № 479/с

Термін здачі студентом закінченої роботи 25 грудня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження): методи та технології захисту інформації в соціальних мережах.

Обладнання та програмне забезпечення:

1. ОС Windows 11 (v.23H2);
2. Вбудована у ноутбук камера USB2.0 HD UVC WebCam;
3. HTML, CSS, Flask;
4. Python (v.3.11).

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	О. А. Покотило	17.09.2024	17.09.2024
2	О. А. Покотило	18.10.2024	18.10.2024
3	О. А. Покотило	18.11.2024	18.11.2024

Студентка  М. О. Сябрук

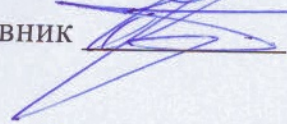
Керівник  Ю. Б. Бродський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	17.09.2024 – 23.09.2024	Виконано
2	Розробка плану роботи	24.09.2024 – 30.09.2024	Виконано
3	Пошук та аналіз наукових джерел з теми, складання списку літератури	01.10.2024 – 07.10.2024	Виконано
4	Вивчення та систематизація теоретичних аспектів інформаційної безпеки в соціальних мережах	08.10.2024 – 18.10.2024	Виконано
5	Опис основних методів захисту інформації, аналіз сучасних технологій для забезпечення захисту даних	19.10.2024 – 25.10.2024	Виконано
6	Проведення аналізу соціальних мереж (Facebook, WhatsApp, Telegram, Viber, WeChat, Signal)	26.10.2024 – 04.11.2024	Виконано
7	Визначення критеріїв для оцінки соціальних мереж, порівняння платформ за обраними критеріями	05.11.2024 – 10.11.2024	Виконано
8	Опис концепції запропонованого методу фотографування при спробі несанкціонованого доступу	11.11.2024 – 21.11.2024	Виконано
9	Опис прототипу методу фотографування, проведення тестування.	22.11.2024 – 30.11.2024	Виконано

10	Формування висновків проведеного аналізу та дослідження	01.12.2024 – 05.12.2024	Виконано
11	Написання пояснювальної записки	06.12.2024 – 20.12.2024	Виконано
12	Захист	25.12.2024	Виконано

Студентка  М. О. Сябрук

Керівник  Ю. Б. Бродський

АНОТАЦІЯ

Випускна кваліфікаційна робота магістра складається з пояснювальної записки, що містить вступ, три розділи, висновки, список використаної літератури та додатки. Текстова частина викладена на 70 сторінках друкованого тексту. Пояснювальна записка має 2 сторінки додатків. Список використаних джерел містить 21 найменування і займає 3 сторінки. В роботі наведено 13 рисунків та 4 таблиці. Загальний обсяг роботи – 87 сторінок.

Метою кваліфікаційної роботи є аналіз сучасних методів, засобів та технологій, за допомогою яких здійснюється захист інформації та обґрунтування пропозицій щодо покращення безпеки інформації в соціальних мережах.

В рамках роботи було розглянуто загальні питання організації методів і технологій захисту інформації. Проаналізовано політику захисту соціальних мереж Facebook, WhatsApp, Telegram, Viber, WeChat і Signal та проведено їх порівняння між собою. Окрему увагу приділено використанню традиційних методів захисту інформації в соціальних мережах. Обґрунтовано доцільність поєднання фізичної ідентифікації злоумисника із автоматичним сповіщенням користувача для здійснення захисту інформації в соціальних мережах. Представлено прототип та проведено тестування методу фотографування злоумисника в соціальних мережах.

КЛЮЧОВІ СЛОВА: СОЦІАЛЬНІ МЕРЕЖІ, ЗАГРОЗИ, ЗАХИСТ ІНФОРМАЦІЇ, МЕТОДИ, ТЕХНОЛОГІЇ, НАЦІОНАЛЬНА БЕЗПЕКА, КОРИСТУВАЧІ, ПРИСТРОЇ.

ANNOTATION

The final qualification work of the master consists of an explanatory note, including an introduction, three chapters, conclusions, a list of references, and appendices. The test part is set out on 70 pages of printed text. The explanatory note includes 2 pages of appendices. The list of references contains 21 sources and occupies 3 pages. The work contains 13 figures and 4 tables. The total volume of the work is 87 pages.

The purpose of the qualification thesis is to analyze modern methods, tools, and technologies for information protection and to substantiate proposals for improving information security in social networks.

The work considered general issues of organizing methods and technologies for information protection. The protection policy of social networks Facebook, WhatsApp, Telegram, Viber, WeChat and Signal was analyzed and their comparison was made. Special attention was paid to the use of traditional methods of information protection in social networks. The feasibility of combining physical identification of the attacker with automatic user notification for information protection in social networks was substantiated. A prototype of a method for photographing an attacker on social networks was presented and tested.

KEYWORDS: SOCIAL NETWORKS, THREATS, INFORMATION SECURITY, METHODS, TECHNOLOGIES, NATIONAL SECURITY, USERS, DEVICES.

ЗМІСТ

ВСТУП	10
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ	12
1.1. Методи захисту інформації	12
1.1.1. Криптографічні методи захисту: шифрування повідомлень, цифровий підпис.....	19
1.1.2. Біометричний захист інформації.....	21
1.1.3. Автентифікація користувачів. Методи автентифікації: паролі, багатофакторна автентифікація, біометричні системи	24
1.1.4. Контроль доступу до даних	27
1.2. Технології захисту інформації в соціальних мережах	29
1.2.1. Використання блокчейн-технологій для захисту даних	30
1.2.2. Моніторинг трафіку: штучний інтелект	33
РОЗДІЛ 2. ПОЛІТИКА ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ	39
2.1. Facebook Messenger	40
2.2. WhatsApp	43
2.3. Telegram	46
2.4. Viber.....	49
2.5. WeChat	53
2.6. Signal.....	56
2.7. Порівняння Facebook, WhatsApp, Telegram, Viber, WeChat, Signal.....	59
РОЗДІЛ 3. МЕТОД ФОТОГРАФУВАННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ.....	61
3.1. Використання традиційних методів захисту інформації в соціальних мережах.....	61
3.1.1. Пропозиція впровадження методу фотографування	62
3.1.2. Порівняння методу фотографування з традиційними методами захисту інформації в соціальних мережах	63
3.2. Опис методу фотографування зломисника в соціальних мережах	64
3.2.1. Алгоритм і блок-схема пропонованого методу	64
3.2.2. Практична реалізація прототипу	66

3.2.3. Тестування прототипу	69
3.2.4. Переваги методу фотографування в соціальних мережах	75
3.2.5. Недоліки методу фотографування в соціальних мережах	76
3.2.6. Пропозиції щодо подальшого розвитку методу фотографування для соціальних мереж	77
ВИСНОВКИ	80
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	82
ДОДАТКИ	85

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СМ – Соціальна мережа

КС – Комп’ютерна система

ІТЗ – Інженерно-технічний захист

DES – Data Encryption Standart

RSA – Rivest, Shamir, Adleman

ЦП – Цифровий підпис

АІ – Штучний інтелект

ВСТУП

Актуальність. Вже третій рік у нашій країні триває повномасштабна війна, яку розв'язала росія. Нині український народ стоїть на захисті територіальної цілісності та суверенітету нашої держави. Одним із ключових елементів національної безпеки України є забезпечення кібербезпеки, в якій соціальні мережі (далі СМ) відіграють значну роль. Протягом останніх років Україна стикається з наслідками гібридної війни, що ведеться російською федерацією. Кіберзброя, яка застосовується в таких конфліктах, охоплює широкий спектр технічних і програмних засобів. Основна мета кібервійни полягає у досягненні стратегічних цілей у військовій, політичній, економічній та інших сферах. Окрім того, такі дії мають яскраво виражений психологічний характер, спрямований на деморалізацію, дезорганізацію супротивника та створення хаосу всередині країни. Головними мішенями кібератак стають критично важливі та функціональні системи. Як зазначив заступник голови Держспецзв'язку Віктор Жора, «Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак проти неї» [1]. У цьому контексті соціальні мережі відіграють особливу роль, оскільки вони містять значну кількість розвідувальної інформації. До такої інформації належать маршрути пересування, місця дислокації, дані про військовослужбовців та докази злочинної діяльності. З огляду на це, захист інформації в соціальних мережах, пошук методів та технологій її захисту на сьогодні є нагальною потребою держави, що й обумовлює актуальність магістерського дослідження.

Об'єктом дослідження є існуючі процеси та системи захисту інформації в соціальних мережах.

Предметом дослідження є методи та технології захисту інформації в соціальних мережах.

Метою кваліфікаційної роботи є аналіз сучасних методів, засобів та технологій, за допомогою яких здійснюється захист інформації та

обґрунтування пропозицій щодо покращення безпеки інформації в соціальних мережах.

Мета обумовлює виконання наступних завдань:

- розглянути загальні питання організації методів і технологій захисту інформації;
- проаналізувати політику захисту соціальних мереж Facebook, WhatsApp, Telegram, Viber, WeChat і Signal;
- обґрунтувати доцільність поєднання фізичної ідентифікації злоумисника із автоматичним сповіщенням користувача для здійснення захисту інформації в соціальних мережах.

Результатом виконання кваліфікаційної роботи є виокремлення сучасних методів, засобів та технологій захисту інформації в соціальних мережах та пропозицій щодо покращення безпеки інформації в соціальних мережах.

Апробація наукових досліджень полягає в обговоренні дослідження, його рецензуванні і експертизі, оприлюдненню результатів у повідомленнях на науково-практичних конференціях: Сябрук М. О., Бродський Ю. Б. Роль соціальних мереж в забезпеченні кібербезпеки // Тези доповідей VI Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 29-30 листопада 2023 року – Житомир: Житомирська політехніка, 2023 [2]; Сябрук М. О. Система розпізнавання користувачів в соціальних мережах // Тези доповідей XIV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2024», м. Житомир, 28-29 березня 2024 року – Житомир: Житомирська політехніка, 2024 [3]; Сябрук М. О. Моніторинг нормативної бази захисту інформації в соціальних мережах // Тези доповідей VII Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 02-03 грудня 2024 року – Житомир: Житомирська політехніка, 2024 [4].

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Інформація є ключовим ресурсом у сучасному світі, який визначає конкурентоспроможність, ефективність та безпеку ділових і наукових процесів. В умовах стрімкого розвитку інформаційних технологій і цифрових комунікацій питання захисту даних набуває особливої актуальності. Конфіденційність, цілісність і доступність інформації є фундаментальними принципами, на яких базується безпека інформаційних систем.

Соціальні мережі обробляють величезні обсяги інформації, що робить їх привабливими цілями для кібератак. Злом акаунтів, витоки інформації та атаки з використанням соціальної інженерії вимагають впровадження ефективних методів та технологій захисту. Далі розглянемо їх широкий спектр.

1.1. Методи захисту інформації

Усі методи інформаційної безпеки можна умовно розділити на дві основні групи: організаційно-правові та інженерно-технічні. Останні включають фізичні, апаратні, програмні та криптографічні методи захисту (рис. 1.1).



Рисунок 1.1 - Класифікація методів захисту інформації в комп'ютерних системах [5]

До *організаційно-правових* методів захисту інформації належать комплексні заходи, спрямовані на забезпечення безпеки в процесі створення, впровадження та експлуатації комп'ютерних систем (далі КС). Ці заходи включають організаційно-технічні та організаційно-правові дії, що застосовуються на різних етапах життєвого циклу системи: під час проєктування системи, у процесі будівництва або реконструкції приміщень для розміщення обладнання, на етапі монтажу та тестування технічних і програмних компонентів, під час перевірки працездатності та надійності системи.

Ключовим елементом проведення організаційних заходів є використання та підготовка нормативних і законодавчих документів у сфері інформаційної безпеки, які регулюють доступ до інформації з боку користувачів на законодавчому рівні.

Інженерно-технічний захист інформації (далі ІТЗ) — це комплекс спеціальних заходів, технічних засобів і процедур, які спрямовані на захист конфіденційної інформації. Вони охоплюють широкий спектр рішень, що реалізуються залежно від завдань і об'єктів захисту.

Засоби інженерно-технічного захисту класифікуються за кількома ознаками: об'єкти впливу, способи реалізації, функціональне призначення, масштаби застосування, а також типи загроз, які нейтралізуються. Ця класифікація дозволяє ефективно адаптувати методи захисту до конкретних умов. Засоби ІТЗ охоплюють фізичні, апаратні, програмні та криптографічні компоненти:

1) *фізичні засоби* включають споруди і засоби, які забезпечують перешкоди фізичному доступу злоумисників до об'єктів захисту та матеріальних носіїв конфіденційної інформації, включають охоронні системи, бар'єри, замки, системи контролю доступу та захисту матеріальних засобів, фінансів, персоналу, інформації від протиправних впливів;

2) *апаратні засоби* включають пристосування, прилади та інші технічні рішення, які створені для запобігання несанкціонованого доступу,

розголошення або витоку інформації. На практиці діяльності підприємства використовується найрізноманітніша апаратура, починаючи зі звичайних засобів зв'язку до автоматизованих систем для підтримки безпеки виробничих процесів;

3) *програмні засоби* охоплюють спеціальні програми, програмні комплекси та системи захисту інформації в інформаційних системах різного призначення та засобах обробки (збирання, накопичення, зберігання, обробка та передача) даних;

4) *криптографічні засоби* базуються на математичних і алгоритмічних методах, спрямованих на шифрування інформації під час її передачі, зберігання та обробки [6].

Завдання та функції захисту інформації визначають набір методів і структуру систем, що її забезпечують. Основні методи захисту інформації представлені в таблиці 1.1.

Таблиця 1.1

Методи захисту інформації в комп'ютерних системах [7]

Методи захисту інформації в КС
Підвищення рівня достовірності інформації
Контроль доступу до внутрішнього монтажу апаратури, ліній зв'язку та органів керування
Захист від побічного випромінювання та наводок
Захист інформації при аварійних ситуаціях
Розмежування і контроль доступу до інформації
Методи ідентифікації і автентифікації
Криптографічне перетворення інформації
Контроль та облік доступу
Законодавчі міри
Обмеження доступу
Розмежування доступу
Розділення доступу (привілеї)

Одним із ключових типів загроз конфіденційності інформації, цілісності та працездатності КС є навмисні загрози, які заздалегідь плануються злоумисником з метою завдання шкоди. За способом реалізації такі загрози поділяються на дві основні категорії:

- загрози, що реалізуються за безпосередньої участі людини (зловмисника);

- загрози, які здійснюються автоматизованими програмами без участі людини.

Основні завдання системи захисту від загроз обох категорій включають наступне:

- запобігання несанкціонованому доступу до ресурсів комп'ютерних систем;
- блокування можливості несанкціонованого використання комп'ютерних ресурсів у випадках, коли доступ уже було отримано;
- швидке виявлення несанкціонованої активності, усунення причин її виникнення та мінімізація негативних наслідків.

Методи вирішення завдань захисту від несанкціонованих дій, що здійснюються людьми, суттєво відрізняються від підходів до протидії загрозам, реалізованим комп'ютерними програмами.

Основними функціями системи захисту інформації є створення бар'єрів для несанкціонованого доступу до ресурсів комп'ютерних систем. Це реалізується через процеси ідентифікації користувачів та перевірки їхніх повноважень, а також обмеження доступу до ресурсів відповідно до встановлених прав.

Особливу роль відіграє функція коректного завершення сеансів роботи користувачів, яка запобігає можливості використання облікового запису злоумисником, що маскується під санкціонованого користувача.

Захист даних від дослідження і копіювання передбачає застосування криптографічних методів, зокрема, шифрування інформації. Крім того, необхідно передбачити механізми видалення залишкової інформації та аварійного знищення даних у разі виявлення загроз.

Захист програмного забезпечення від копіювання запобігає можливості використання несанкціоновано скопійованих програм на інших пристроях. Також важливим є захист програм від дослідження, що дозволяє зберегти конфіденційність алгоритмів та інших технічних деталей їх реалізації.

Для забезпечення захисту доступу до комп'ютерних систем будь-який користувач повинен пройти такі етапи:

- ідентифікація;
- встановлення достовірності (аутентифікація);
- визначення повноважень для розмежування доступу до комп'ютерних ресурсів та подальшого контролю.

Ці етапи також повинні застосовуватися для підключення до систем віддалених робочих станцій і терміналів. Ідентифікація є важливим етапом, який забезпечує надання КС унікального ідентифікатора для кожного користувача, що звертається до неї. Це дозволяє системі здійснювати подальші захисні дії відповідно до встановлених правил.

Процес перевірки достовірності (аутентифікація) полягає у підтвердженні особи користувача, який намагається отримати доступ до системи. Для підвищення рівня безпеки можуть застосовуватися біометричні методи, що базуються на використанні унікальних фізичних характеристик людини, зокрема аналіз голосу, відбитків пальців, або структури зіниці ока.

Ефективність захисту при застосуванні парольної аутентифікації значною мірою залежить від обмежень щодо тривалості дії пароля. Чим частіше паролі оновлюються, тим вищий рівень безпеки системи.

Методи ідентифікації та аутентифікації можуть значно відрізнятися залежно від об'єктів і цілей їх застосування. Всі методи класифіковано та представлено в узагальненій формі в таблиці 1.2.

Таблиця 1.2

Методи, які використовуються для встановлення дійсності об'єктів захисту інформації в комп'ютерних системах [7]

Ідентифікація та встановлення дійсності		
Особи	Документів	Технічних засобів
Поділ коду пароля на дві частини: та, що запам'ятовується користувачем, та, що вводиться вручну із спеціального носія-картки.	Застосування криптографічного перетворення інформації (в мережі цифрового підпису).	Ідентифікація та встановлення дійсності терміналу з використанням контрольних значень Х. Для встановлення дійсності клієнта відносно користувача, тощо.

Продовження табл. 1.2

Особи	Документів	Технічних засобів
Присвоєння об'єкту унікального імені чи ключа-пароля та зберігання його в КС.		Ідентифікація та встановлення достовірності інформації на засобах її ідентифікації та друку.
«Запит-відповідь»		
«Рукописання»		
«Ключ-замок»		

Під час обміну інформацією рекомендується виконувати взаємну перевірку достовірності повноважень об'єктів і суб'єктів взаємодії. У разі передачі даних через мережу ця процедура стає обов'язковою для забезпечення безпеки.

Метод «запит-відповідь». У рамках цього методу у КС заздалегідь створюється спеціально захищений масив запитань. Цей масив включає як запитання загального характеру, так і персоналізовані запитання, орієнтовані на конкретного користувача. Для підтвердження автентичності система пропонує користувачеві випадкову послідовність запитань, на які той має дати правильні відповіді. У разі успішного проходження тестування користувач отримує доступ до системи.

Метод односторонніх функцій. Цей метод широко застосовується в асиметричних криптосистемах завдяки унікальній властивості: значення функції $f(x)$ легко обчислити, якщо відомо x , але обернене обчислення x за заданим $y = f(x)$ є надзвичайно складним або практично неможливим.

Метод «рукописання». Цей метод базується на функції F , яка відома лише користувачу та комп'ютерній системі. При вході в систему вона генерує випадкове число або послідовність символів X і обчислює $F(X)$. Це значення X передається користувачу, який повинен розрахувати $F(X)$ самостійно і ввести його у систему. Якщо обчислене значення збігається з розрахунком системи, доступ дозволяється.

Ідентифікація та встановлення достовірності технічних засобів забезпечується паролями, які застосовуються для перевірки як користувача, так і терміналу, з якого здійснюється доступ. Це дозволяє встановити двосторонню достовірність між користувачем і комп'ютерною системою.

Ідентифікація та встановлення достовірності документів базується на таких підходах:

- документ сформований безпосередньо в даній КС: в цьому випадку достовірність даних гарантується за допомогою засобів інформаційного захисту, таких як криптографічне шифрування, і захисту паролем.

- документ сформований з віддалених об'єктів: в цьому випадку для забезпечення достовірності використовуються методи криптографічного захисту, особливо якщо документи транспортувалися через незахищені середовища або зберігалися протягом тривалого часу в пам'яті системи.

Ідентифікація та перевірка достовірності інформації на засобах відображення і друку. Методи, що використовуються для підтвердження достовірності документів, також застосовуються до інформації, представленої на засобах її візуалізації та друку. Це забезпечує цілісність і надійність відображених даних.

Своєчасне виявлення несанкціонованих дій користувачів. Для своєчасного виявлення несанкціонованих дій необхідно реалізувати наступні функції:

- регулярний контроль цілісності інформації;
- перевірка коректності функціонування системи захисту;
- реєстрація та сигналізація.

1.1.1. Криптографічні методи захисту: шифрування повідомлень, цифровий підпис

Криптографічний захист (шифрування) інформації - це метод забезпечення безпеки даних, що базується на їхньому перетворенні за допомогою спеціальних ключів. Метою такого захисту є приховування змісту інформації, перевірка її справжності, забезпечення цілісності даних та ідентифікація автора. На відміну від тайнопису, який приховує сам факт передавання даних, шифрування дозволяє передавати зашифровані повідомлення відкрито, приховуючи лише їхній зміст.

Методи криптографії поділяють на два типи: підстановчі та перестановочні. Підстановчий метод передбачає, що кожен символ повідомлення замінюється іншим згідно із заданим правилом. Для цього часто використовується ключ — певне слово або фраза, що визначає порядок підстановки. У загальному випадку ключ у криптографії — це послідовність бітів, що використовуються для шифрування та розшифрування даних.

У випадку з перестановочним алгоритмом змінюються не символи, а порядок їх розміщення в повідомленні. Залежно від доступності ключів, які використовуються, розрізняють:

- **симетричне шифрування** — один і той самий ключ застосовується як для шифрування, так і для дешифрування даних. Такий підхід із закритим ключем широко використовується, наприклад, в архіваторах даних. Це зручно для захисту приватної інформації, але має ключовий недолік: під час передачі зашифрованого повідомлення по каналах зв'язку необхідно забезпечити безпечну передачу самого ключа, щоб одержувач міг здійснити розшифрування. Якщо ключ передати таємно, можна передати й саму інформацію без шифрування, що в певному сенсі зводить ефективність шифрування нанівець. У випадку неможливості безпечного обміну ключами застосування цього методу стає проблематичним;

* *асиметричне* — тут використовується пара ключів: відкритий (публічний) ключ для шифрування і закритий (приватний) ключ для дешифрування. Цей метод усуває потребу у таємному обміні ключами між учасниками. Знання відкритого ключа не дозволяє отримати доступ до закритого ключа чи розшифрувати дані. Основним недоліком такого підходу є необхідність адміністрування ключів: їх потрібно надійно зберігати та періодично оновлювати [8].

На даний час існує багато криптографічних алгоритмів, серед яких найбільш поширеними є стандарт шифрування даних DES (Data Encryption Standart) та алгоритм RSA (Rivest, Shamir, Adleman), названий за першими літерами прізвищ розробників, розроблені у 1970-х роках. Обидва алгоритми є державними стандартами США. DES — симетричний алгоритм шифрування, а RSA — асиметричний. Рівень захищеності при використанні цих алгоритмів напряду залежить від довжини ключа, що застосовується.

Криптографічні алгоритми застосовуються не лише для шифрування повідомлень, а й для створення *електронних (цифрових) підписів (ЦП)* — спеціальних даних, які забезпечують підтвердження цілісності електронного документа та ідентифікують особу, що його підписала.

Терміни «електронний підпис» і «цифровий підпис» часто використовуються як синоніми, але між ними є відмінність. Електронний підпис — це будь-який підпис у цифровій формі, який не обов'язково базується на криптографії (наприклад, підпис, створений за допомогою біометрії). Цифровий підпис, у свою чергу, є підвидом електронного підпису, який створюється із застосуванням криптографічних методів.

Цифровий підпис додає до повідомлення зашифровану інформацію. Найпоширенішим методом є використання асиметричного шифрування: створення підпису здійснюється за допомогою закритого ключа, доступного лише відправнику, а перевірка підпису виконується за допомогою відкритого ключа, доступного будь-якому користувачу. Разом із підписом передається публічний ключ і додаткові відомості, такі як ім'я відправника, серійний номер

підпису та дані сертифікаційного центру. В результаті, послати зашифроване повідомлення і перевірити підпис може будь-хто, але створити його або розшифрувати зашифроване повідомлення може тільки власник секретного ключа.

Загалом для забезпечення високого рівня захищеності інформації використовується криптографічна система, що являє собою сукупність засобів криптографічного захисту, необхідної нормативної, експлуатаційної і іншої документації, зокрема й такої, що визначає заходи безпеки.

Проте криптосистеми мають обмеження. Наприклад, отримавши зашифроване повідомлення парним ключем, неможливо точно визначити, хто саме його відправив. Цю проблему можна вирішити за допомогою засобів біометричного захисту (див. наступний пункт), який додає рівень перевірки на основі фізичних характеристик користувача та методом двофакторної аутентифікації (використовується й однофакторна, але вона менш надійна), тоді користувач повинен мати, наприклад, пластикову картку (смарт-картку або картку з магнітною смужкою) і знати PIN-код.

Отже, розвиток криптосистем і вдосконалення цифрових підписів, підвищення їх надійності створюють важливі передумови для відмови від паперового документообігу, заміни його електронним і переходу до проведення безпечних електронних операцій.

1.1.2. Біометричний захист інформації

Системи біометричного захисту інформації використовують унікальні для кожної людини вимірювані фізіологічні характеристики для перевірки її особи. Цей процес називається електронною аутентифікацією і має на меті підтвердити, чи дійсно індивід є тим, за кого себе видає. Це відрізняється від ідентифікації, завданням якої є перевірка того, чи відомий індивід системі

(наприклад, за допомогою введення пароля), та авторизації, яка надає доступ до певних ресурсів залежно від перевіреної особи.

Біометричні системи забезпечують найвищий рівень точності під час аутентифікації, оскільки вони перевіряють параметри, які важко або неможливо змінити чи підробити. Це значно відрізняє їх від традиційних систем, які не здатні визначити, наприклад, хто саме вводить код чи використовує смарт-картку.

Однак, незважаючи на переваги, біометричні системи мають і певні недоліки. Основна проблема полягає в тому, що для роботи таких систем необхідно зберігати унікальні конфіденційні дані кожної людини. Водночас прихильники біометрії зазначають, що насправді ці системи забезпечують вищий рівень секретності, оскільки не потребують збереження інформації про адресу, номер телефону чи банківські реквізити користувача.

Сучасний розвиток біометричних технологій дозволив значно розширити сферу їх застосування. Раніше вони були атрибутом в більшій мірі військових систем, а сьогодні ці технології впроваджуються у різних галузях. Завдяки вдосконаленню біометричних пристроїв очікується їхнє широке використання у промисловості та приватному секторі, зокрема для проведення онлайн-транзакцій, доступу до банкоматів, систем роздрібної торгівлі, управління доступом до будівель і багато іншого.

Протягом тривалого часу проводилися дослідження для визначення унікальних фізичних характеристик людини, які могли б слугувати надійним індивідуальним ідентифікатором та розпізнавалися б з високою точністю. Результати таких спроб лягли в основу сучасних біометричних технологій:

- розпізнавання відбитків пальців, започаткований у кримінології XIX століття, його основа полягає у скануванні унікального візерунка на пальцях користувача та його порівнянні з раніше записаними зразками. Технологія досягла високого рівня точності завдяки використанню як стандартних сканерів, так і пристроїв, що вимірюють електричні заряди між складками шкіри. Незважаючи на це, розвиток технології вимагає врахування можливих змін

стану шкіри та зовнішніх умов. Перевагами є простота і швидкість роботи для кінцевих користувачів;

- розпізнавання голосу базується на аналізі індивідуальних мовних характеристик за допомогою стандартних аудіозаписуючих пристроїв. Проте рівень точності при цьому дещо нижчий, оскільки залежить від якості звукового середовища та обладнання;

- аналіз геометрії руки передбачає вимірювання фізичних параметрів руки і пальців користувача. Нові пристрої створюють тривимірну карту руки, що значно підвищує точність ідентифікації, оскільки рівень точності прямо пропорційний кількості точок у записаному зразку;

- сканування сітківки ока передбачає сканування системи кровоносних судин на сітківці. Рівень точності цього підходу є одним із найвищих серед біометричних технологій, на рівні із розпізнаванням відбитків пальців;

- сканування райдужної оболонки використовується для аналізу унікальних рисунків на райдужній оболонці ока. Хоча точність методу поки що середня, очікується її зростання завдяки вдосконаленню технічних засобів;

- розпізнавання обличчя базується на створенні тривимірної моделі обличчя за допомогою стандартної цифрової камери. Точність варіюється від низької до середньої залежно від конкретного підходу;

- розпізнавання динаміки підпису під час аналізу підпису враховує не лише форму літер, а й швидкість та інтенсивність натиску під час підпису, що здійснюється спеціальним пристроєм;

- розпізнавання стилю набирання символів на клавіатурі визначає швидкість, ритм та інтенсивність натискання клавіш. Маркетингові дослідження свідчать про те, що користувачі проявляють більше довіри до систем розпізнавання відбитків пальців, а не, наприклад, до стилю введення даних. Але важливо зазначити, що другі будуть готові до масштабного впровадження набагато раніше. Для роботи не потрібне додаткове обладнання, що робить їх значно дешевшими [9].

Описані вище методи можна поділити на дві групи залежно від способу «захоплення» біометричних характеристик людини:

- безконтактні технології (наприклад, розпізнавання голосу чи обличчя), які не потребують фізичного контакту із користувачем. Вони більш зручні для застосування, але мають нижчий рівень надійності, оскільки можуть бути чутливими до зовнішніх умов, таких як акустика чи освітлення;
- контактні технології (наприклад, розпізнавання відбитків пальців або аналіз геометрії руки), які передбачають фізичну взаємодію із пристроєм. Ці методи забезпечують вищу точність, проте можуть викликати дискомфорт у користувачів.

Попри відмінності у прийнятності й надійності, біометричні технології загалом матимуть високий попит у різних сферах. Їхнє поширення залежатиме від кількох факторів, зокрема: удосконалення технічних пристроїв і програмного забезпечення, зниження вартості впровадження, підтримки на законодавчому рівні та розробки промислових стандартів, які регулюватимуть їх використання.

1.1.3. Автентифікація користувачів. Методи автентифікації: паролі, багатофакторна автентифікація, біометричні системи

Автентифікація – це процес підтвердження того, що доступ до корпоративних ресурсів отримують лише користувачі, служби та програми, які мають відповідні дозволи. Автентифікація є ключовим елементом кібербезпеки, адже зловмисники, прагнучи отримати несанкціонований доступ до систем, часто викрадають облікові дані користувачів, які вже мають доступ. Процес автентифікації зазвичай включає три основні етапи:

- Ідентифікація: встановлення особи користувача в системі, як правило, через ім'я облікового запису.

- Автентифікація: підтвердження особи користувача через щось, що відомо лише йому (наприклад, пароль). Для підвищення рівня безпеки сучасні методи додають ще один рівень — використання чогось, що належить користувачеві (наприклад, смартфон або апаратний ключ), або чогось унікального для нього (біометричні дані, як-от відбиток пальця чи зображення обличчя).
- Авторизація: перевірка прав доступу користувача до певних системних ресурсів.

У сучасних системах автентифікація дедалі частіше делегується спеціалізованим платформам ідентифікації, на відміну від традиційних методів, коли кожна система самостійно перевіряла особу користувача. Також відбулися зміни у типах способів автентифікації. Хоча ім'я користувача і пароль залишаються базовими елементами, вони дедалі частіше доповнюються додатковими рівнями захисту. Це обумовлено вдосконаленням методів викрадення облікових даних, що стимулює впровадження більш надійних технологій захисту. Фахівці з кібербезпеки активно розробляють нові рішення, які покращують захист ідентичностей та мінімізують ризики несанкціонованого доступу.

Автентифікація за паролем – це найпоширеніший метод підтвердження особи, який ґрунтується на введенні користувачем унікального пароля. Більшість програм і сервісів вимагають створення паролів із використанням комбінацій цифр, літер та спеціальних символів, що зменшує ризик їхнього вгадування зловмисниками. Однак такий підхід має недоліки, пов'язані як із безпекою, так і з користувацьким досвідом. Багатьом користувачам складно запам'ятовувати унікальні паролі для кожного облікового запису, через що паролі часто використовуються повторно. Це створює додаткові загрози, адже зловмисники застосовують різноманітні методи для вгадування, викрадення або виманювання паролів. У зв'язку з цим дедалі більше організацій переходять на більш безпечні методи автентифікації, які не залежать від паролів.

Автентифікація за сертифікатом – це шифрований метод ідентифікації, що дозволяє пристроям і користувачам підтверджувати свою особу у взаємодії з іншими пристроями чи системами. Прикладами такого підходу є використання смарт-карт або передача цифрових сертифікатів із пристрою співробітника до мережі чи сервера [10].

Автентифікація за маркером – це метод підтвердження особи, за якого пристрій і система кожні 30 секунд генерують унікальний одноразовий пароль, заснований на часових параметрах. Якщо згенеровані коди збігаються, система підтверджує наявність у користувача відповідного пристрою.

Одноразовий пароль – це тимчасовий код, який створюється для одного сеансу автентифікації та діє протягом обмеженого часу. Він може бути надісланий користувачеві через SMS, електронну пошту або апаратний ключ.

Push-сповіщення – метод автентифікації, який передбачає надсилання запиту на пристрій користувача для підтвердження чи відхилення доступу. Щоб уникнути помилкових схваленень, які можуть статися через неуважність, push-сповіщення часто комбінуються з одноразовими паролями. У такому випадку система генерує додатковий унікальний код, який користувач вводить для завершення процесу. Це забезпечує вищий рівень захисту, зокрема від фішингових атак.

Голосова автентифікація – спосіб підтвердження особи, при якому користувач відповідає на телефонний дзвінок і вводить код або проходить ідентифікацію за допомогою голосу [10].

Багатофакторна автентифікація – є одним із найефективніших методів зниження ризику компрометації облікових записів. Вона передбачає використання двох або більше рівнів автентифікації, що поєднують різні способи підтвердження особи. Для забезпечення надійного захисту рекомендується вимагати від користувачів надання будь-яких двох із наступних типів інформації:

- Щось, що знає лише користувач, наприклад пароль.

- Щось, що належить лише користувачу, як-от надійний пристрій, який складно підробити (наприклад, телефон або апаратний ключ).
- Щось, що є частиною користувача, наприклад біометричні дані (відбиток пальця або розпізнавання обличчя).

Багато організацій застосовують комбінований підхід, наприклад, запитують пароль (те, що знає користувач) і додатково надсилають SMS із одноразовим кодом на надійний пристрій (те, що належить користувачу).

1.1.4. Контроль доступу до даних

Контроль та управління правом доступу забезпечують захист об'єктів і ресурсів від несанкціонованого доступу та використання. Вибір відповідної моделі управління доступом є ключовим фактором, що визначає рівень безпеки організації та її інформаційних систем будь-якого призначення. Науково розроблені моделі та методи управління доступом враховують особливості суб'єктів і важливість безпеки об'єктів або ресурсів. Моделі управління доступом поділяються на чотири категорії:

- дискреційне (виборче) управління;
- обов'язкове (мандатне) управління;
- рольова модель управління;
- управління доступом на основі правил.

Дискреційний контроль доступу – цей метод передбачає, що власник або адміністратор об'єкта має право на основі ідентифікаційної інформації про суб'єктів (ключі доступу) визначати та контролювати всіх, у кого є доступ до системи або ресурсів. Модель є простою у налаштуванні та управлінні, сумісною з великою кількістю програмного забезпечення та операційних систем, таких як Windows і ін. Адміністратор формує списки користувачів, яким надано доступ, а також визначає рівень їхніх прав у системі.

Перевагами такого контролю доступу можна назвати те, що адміністратор може швидко і легко налаштувати дозволи з визначенням хто отримує доступ і куди. При цьому, він зосереджується на інтересах діяльності конкретної установи, поточних завданнях та режимі загальної політики безпеки організації. Натомість надмірна залежність від адміністратора є суттєвим недоліком, бо це створює ризик ненавмисного надання доступу стороннім особам, що ставить під загрозу цілісність системи безпеки організації та дає можливість розпоряджатися ресурсами без відома власника [11].

Мандатний контроль доступу – є найбільш суворою формою регулювання доступу до ресурсів, оскільки надає виключні права на управління лише власнику об'єкта або адміністратору системи. У цій моделі доступу використовується поняття мітки об'єкта (мандат), яка визначає рівень важливості ресурсу і присвоюється йому під час створення. Користувачам забороняється змінювати рівень доступу до ресурсів або перевищувати обмеження, встановлені адміністратором. Для зміни рівня доступу потрібно створювати нові профілі користувачів із відповідними обліковими даними. Адміністратор може змінювати параметри доступу виключно у межах, визначених загальною політикою безпеки організації. Мандатний контроль доступу є оптимальним для організацій і об'єктів, де необхідно забезпечити максимальний рівень безпеки. Цей підхід доцільно застосовувати у військових та урядових установах, а також у корпораціях, що потребують суворого захисту конфіденційної інформації та ресурсів і вважають необхідним застосування підвищеного рівня безпеки [11].

Модель рольового управління доступом – базується на розподілі функцій співробітників відповідно до специфіки діяльності організації, окремих підрозділів або виконуваних проектів. Цей метод передбачає встановлення рівнів доступу не для кожного користувача окремо, а для ролей, які виконують працівники. Ролі визначаються посадовими обов'язками або специфікою завдань, і доступ строго обмежується повноваженнями, що відповідають обраній ролі.

До основних переваг такого методу можна віднести: одним рівнем доступу користуватися декілька користувачів, які виконують однакову роль або навпаки — один співробітник може одночасно виконувати кілька ролей без необхідності перегляду його індивідуальних прав доступу. Якщо завдання потребує розширення доступу, адміністратор може переглянути права для конкретної ролі або користувача залежно від обставин. Така модель є оптимальною для динамічних та адаптивних середовищ, зокрема для хмарних систем управління доступом, де постійно змінюються ролі та функції співробітників.

Контроль та управління доступом на основі правил – це модель, яка схожа з рольовим методом, але передбачає встановлення чітких правил обмеження доступу, визначених власниками об'єктів або адміністраторами ресурсів. Ці правила можуть включати: обмеження доступу залежно від часу доби, надання доступу лише з певних пристроїв, визначення доступу на основі кількості попередніх спроб входу, обмеження доступу залежно від місця знаходження користувача, комбінацію зазначених параметрів, що задаються адміністраторами [11].

Ця модель є ідеальним рішенням для організацій із великою кількістю об'єктів різного рівня доступу та регламенту роботи. Її гнучкість дозволяє налаштовувати численні комбінації правил доступу, що адаптуються до змінних умов та потреб організації. Модель управління доступом на основі правил оптимально підходить для середовищ із високими вимогами до безпеки та комплексних сценаріїв доступу.

1.2. Технології захисту інформації в соціальних мережах

Соціальні медіа здійснили революцію у сфері глобальної комунікації, значною мірою змінивши способи взаємодії між людьми та інтегрувавшись у повсякденне життя. Значні обсяги особистої інформації публікуються або

передаються через ці платформи за допомогою функцій обміну повідомленнями. У цьому контексті особливу увагу слід приділити процесам збору особистих даних компаніями соціальних мереж та їх можливій передачі третім сторонам. Ці аспекти викликають занепокоєння серед захисників конфіденційності, що спричиняє значний тиск на компанії з вимогами до впровадження більш суворих заходів захисту даних. Як відповідь на ці виклики, інформаційна безпека застосунків соціальних медіа почала базуватися на впровадженні сучасних технологій захисту інформації. Ключовими інструментами захисту є: шифрування даних, системи автентифікації користувачів і моніторинг мережевого трафіку. Використання цих методів дозволяє забезпечити основні принципи інформаційної безпеки – конфіденційність, цілісність і доступність даних – водночас мінімізуючи ризики витоків або несанкціонованого доступу до інформації.

1.2.1. Використання блокчейн-технологій для захисту даних

Останніми роками зростає занепокоєння щодо надійності та безпеки платформ соціальних мереж. Технологія блокчейн постає як трансформаційна сила, здатна забезпечити підвищену безпеку шляхом розподілу даних між декількома захищеними вузлами. Незважаючи на те, що деякі сервіси обміну повідомленнями акцентують увагу на забезпеченні конфіденційності, виникають нові виклики, пов'язані з обробкою додаткових метаданих.

Соціальні мережі на основі блокчейну виходять за межі традиційної безпеки, пропонуючи інноваційні можливості, такі як інтеграція цифрових валют для проведення довірчих транзакцій, підвищений контроль користувачів над їхнім контентом та децентралізовані механізми взаємодії. Однак, на тлі поширеності основних платформ, таких як Facebook та Instagram, що пропонують безкоштовний доступ, існують постійні виклики, зокрема боротьба

з дезінформацією, негативними соціальними взаємодіями, а також з вирішенням складних питань, таких як цензура та обмеження свободи слова.

Водночас платформи електронної комерції, такі як eBay та Amazon, забезпечують віддалену торгівлю, дозволяючи користувачам здійснювати транзакції без особистих зустрічей. Проте анонімність у цих середовищах створює ризики, серед яких неправомірна поведінка, включаючи продаж контрафактної продукції або поширення недостовірної інформації.

Критичне значення для безпеки онлайн-спільнот мають системи управління довірою та репутацією, які сприяють захисту користувачів і стимулюють ефективну співпрацю. Такі системи є фундаментальними для забезпечення надійності та безпечної взаємодії в соціальних мережах, особливо у світлі нових викликів цифрового середовища.

Більшість сучасних соціальних мереж працюють на централізованих платформах, що створює суттєві ризики для безпеки користувацького контенту. Використання технології блокчейн із її децентралізованою та розподіленою структурою вирішує ці проблеми за рахунок шифрування користувацьких даних. Крім того, оцінка рівня соціальної довіри між користувачами відіграє важливу роль у багатьох веб-додатках. Інтеграція блокчейну в соціальні мережі дала поштовх до створення нових децентралізованих платформ, що дозволяють усунути обмеження традиційних централізованих систем. Однак залишається невизначеність щодо реальних переваг впровадження блокчейну в існуючі соціальні платформи [12].

Кібербезпека є однією з найперспективніших сфер застосування технології блокчейн. Використання унікальних ключів для автентифікації, які підтверджуються всіма учасниками мережі, робить систему стійкою до підробок. Будь-яка спроба підміни даних буде швидко виявлена, що дозволяє системі оперативно реагувати на можливі загрози.

Завдяки тому, що кожен учасник мережі зберігає копію даних, повне видалення інформації є практично неможливим. Це скорочує час на

відновлення системи після атак і зменшує ймовірність завдання незворотної шкоди.

Розглянемо основні проблеми блокчейну:

- масштабування: зі збільшенням обсягу даних процес запису нових блоків ускладнюється, що потребує значних ресурсів часу та обчислювальної потужності. Часткове вирішення цієї проблеми пропонують блокчейни другого рівня, створені для обробки операцій, але остаточного вирішення питання масштабування поки що немає;
- високе енергоспоживання: сумарна споживана потужність усіх майнінгових пулів світу відповідає енергетичним потребам середньостатистичної європейської країни. Уряди багатьох країн реагують на це шляхом запровадження підвищених тарифів на електроенергію, податків або навіть прямих заборон. Подальше зростання популярності блокчейну може спричинити посилення цього опору. Рішення цієї проблеми потребує переходу на альтернативні механізми роботи мереж.

При збереженні цінної інформації ключовим завданням є забезпечення її цілісності та неможливості підміни. У цифровому середовищі це досягається шляхом шифрування даних для забезпечення конфіденційності та їхнього розповсюдження серед усіх учасників мережі (вузлів). Кожен вузол отримує ідентичну копію масиву даних. У разі підозри на зміну інформації достатньо порівняти копії між собою.

Однак процес порівняння великих обсягів даних стає вкрай ресурсомістким, особливо якщо кількість учасників мережі сягає сотень тисяч. Щоб оптимізувати цей процес, у блокчейні застосовується контрольна сума (хеш). Хеш представляє собою зашифрований заголовок масиву даних, який змінюється при будь-якій модифікації навіть одного символу в масиві. Таким чином, перевірка автентичності даних здійснюється шляхом порівняння контрольних сум, що значно знижує обчислювальне навантаження.

Динамічність блокчейн-платформи дозволяє постійно додавати нову інформацію, найчастіше у вигляді транзакцій – грошових переказів між

користувачами. Водночас технологія блокчейн може бути адаптована для перевірки автентичності інших об'єктів, таких як наукові публікації, предмети мистецтва чи посвідчення особи.

Функціональність забезпечується структурою ланцюга блоків, у якій кожен новий блок прив'язаний до попереднього за допомогою хешів. Зокрема, блок №2 містить свою контрольну суму, а також хеш блоку №1. Блок №3 включає свій хеш та хеш блоку №2, і цей процес продовжується далі (рис. 1.2).

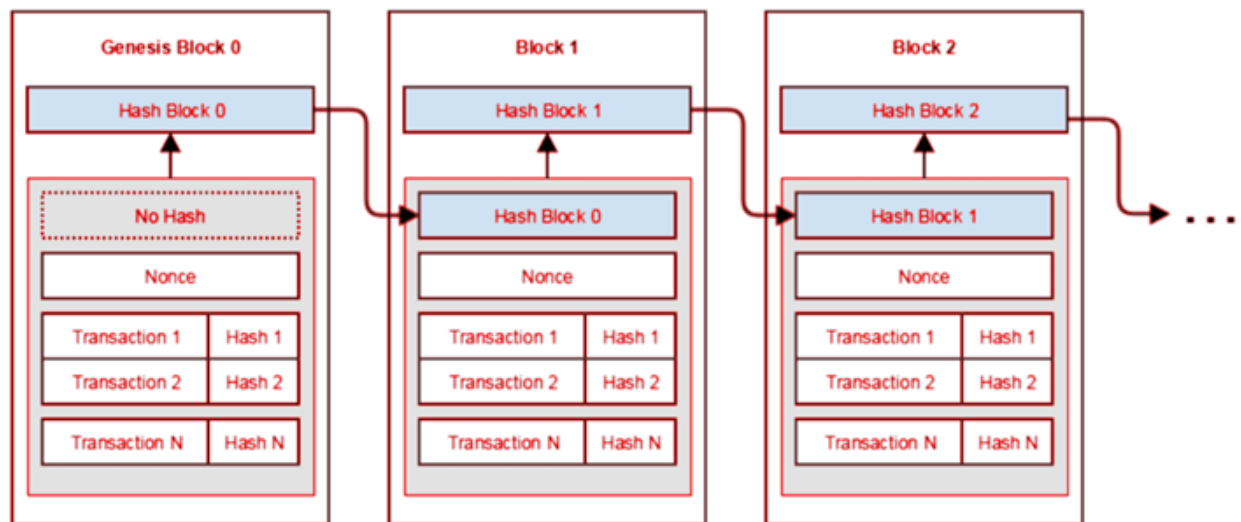


Рисунок 1.2 - Структура блоків блокчейна

Ця структура гарантує, що видалення або підміна будь-якого блоку автоматично порушить цілісність усього ланцюга, роблячи такі маніпуляції очевидними [13].

1.2.2. Моніторинг трафіку: штучний інтелект

У зв'язку зі зростанням складності кібератак компанії змушені застосовувати передові технології, щоб залишатися на крок попереду зловмисників. Штучний інтелект (далі AI) виступає потужним інструментом, який докорінно змінив підходи до виявлення, управління та реагування на кіберзагрози. Завдяки інтеграції AI команди з кібербезпеки можуть отримувати

цінну аналітичну інформацію, автоматизувати трудомісткі процеси та ухвалювати рішення швидше і з більшою точністю.

АІ в кібербезпеці використовує передові технології, такі як машинне навчання та нейронні мережі, для посилення систем захисту. Ці технології дозволяють аналізувати великі обсяги даних, виявляти шаблони та адаптуватися до нових загроз із мінімальним втручанням людини.

На відміну від традиційних інструментів кібербезпеки, які базуються на фіксованих правилах для виявлення загроз, системи, керовані АІ, мають здатність до самонавчання, що дозволяє їм прогнозувати, виявляти та ефективніше протидіяти як відомим, так і невідомим загрозам. Це значно підвищує рівень захисту та зменшує ймовірність зломів.

Етапи розвитку штучного інтелекту в кібербезпеці:

1 етап – допоміжний інтелект: спрямований на вдосконалення існуючих процесів та допомогу організаціям у виконанні поточних завдань.

2 етап – розширений інтелект: відкриває нові можливості, дозволяючи виконувати завдання, які раніше були недоступними.

3 етап – автономний інтелект: перспективна технологія, яка забезпечить повну автономність машин, включно із самостійним ухваленням рішень (наприклад, у контексті самокерованих автомобілів) [14].

Системи штучного інтелекту знаходять широке застосування у сфері кібербезпеки, охоплюючи всі етапи – від виявлення загроз до автоматизації реагування на них. У контексті соціальних мереж АІ сприяє вирішенню ключових проблем, таких як: виявлення загроз, управління загрозами, реакція на загрозу.

Виявлення загроз за допомогою АІ значно перевершує традиційні засоби безпеки, які можуть не помічати аномалії чи залишати поза увагою загрози нульового дня. Системи, базовані на штучному інтелекті, використовують методи розпізнавання образів та виявлення аномальної активності для ідентифікації потенційних атак. Крім того, АІ здатний постійно сканувати

мережі та системи, виявляючи вразливості та автоматично позначаючи потенційні точки ризику.

Після виявлення загрози AI стає ключовим інструментом автоматизації процесу управління. Зокрема, системи штучного інтелекту визначають пріоритети вразливостей на основі їх потенційного впливу, дозволяючи організаціям зосереджуватися на вирішенні найкритичніших проблем, оптимізують процес управління виправленнями, оцінюючи рівень ризику та пропонуючи найбільш ефективні стратегії реагування, автоматизують реагування в реальному часі, що дозволяє мінімізувати шкоду від атаки та скоротити час відновлення систем.

Штучний інтелект демонструє значний потенціал у кібербезпеці, зокрема у сфері автоматизації реагування на загрози. Його функціонал включає такі дії, як блокування шкідливого трафіку, ізоляція уражених систем та автоматична генерація звітів про інциденти. Завдяки здатності до адаптації та самонавчання, AI забезпечує ефективне реагування на нові загрози, що виникають.

Розглянемо рішення, які пропонує AI в забезпеченні кібербезпеки соціальних мереж: штучний інтелект здатний швидко аналізувати величезні обсяги даних, виявляти аномалії та ідентифікувати потенційні ризики. Це скорочує час, необхідний для реагування на загрози, і підвищує ефективність заходів захисту. AI дозволяє автоматизувати процеси, такі як аналіз журналів подій і сканування вразливостей, звільняючи команди безпеки для стратегічних завдань. Використовуючи аналіз шаблонів минулих атак, AI може передбачати нові загрози, допомагаючи організаціям випереджати кіберзлочинців.

До основних переваг використання систем штучного інтелекту для забезпечення захисту інформації в аспекті кібербезпеки можна віднести такі характеристики AI:

- AI може аналізувати великі обсяги даних у режимі реального часу, надаючи прогнозовану інформацію. Це дозволяє командам з кібербезпеки передбачати потенційні атаки та впроваджувати профілактичні заходи для їхнього запобігання.

- AI автоматизує процеси виявлення, аналізу та пом'якшення загроз, скорочуючи час між виявленням загрози та реагуванням на неї. Системи на основі AI також забезпечують контекст для визначення пріоритетів попереджень, сприяють швидкому реагуванню та допомагають усунути основні причини вразливостей.
- AI-системи здатні виявляти вразливі місця у мережах і системах, оцінюючи їх за критичністю та потенційним впливом. Це дозволяє визначати пріоритетність ризиків і мінімізувати помилкові спрацьовування, підвищуючи ефективність роботи команд безпеки.
- AI може прогнозувати, як і де найімовірніше станеться злам. Це дозволяє організаціям оптимально розподіляти ресурси для захисту слабких місць.
- AI пропонує рекомендації на основі аналізу даних, що сприяє ухваленню обґрунтованих рішень. Це полегшує розуміння впливу програм інформаційної безпеки та забезпечує прозорість для зацікавлених сторін, включаючи кінцевих користувачів, команди безпеки, керівництво та раду директорів [14].

Виділимо основні технології штучного інтелекту в кібербезпеці:

Машинне навчання — це форма штучного інтелекту, яка дозволяє системам навчатися на основі даних і вдосконалюватися без явного програмування. У сфері кібербезпеки типовим застосуванням машинного навчання є аналіз поведінки користувачів і суб'єктів, який аналізує моделі та поведінку для виявлення загроз. Наприклад, цей аналіз може позначати незвичайну активність входу, визначаючи аномалії в поведінці користувачів, такі як ненормальний час входу або розташування, які можуть сигналізувати про порушення безпеки та сприяти швидшій реакції. Машинне навчання відмінно справляється з такими завданнями, як виявлення аномалій мережевого трафіку та запобігання атакам, розпізнаючи нестандартну поведінку до їх ескалації.

Глибоке навчання — підмножина машинного навчання, використовує нейронні мережі для аналізу складних даних і є дуже ефективним у виявленні складних загроз кібербезпеки, таких як еволюція штамів зловмисного програмного забезпечення. У сфері кібербезпеки глибоке навчання використовується для виявлення поліморфного шкідливого програмного забезпечення, яке постійно змінює свій код, щоб уникнути традиційних методів виявлення.

Моделі глибокого навчання можуть аналізувати величезні обсяги даних і розпізнавати основні закономірності в поведінці зловмисного програмного забезпечення, навіть якщо код відрізняється. Наприклад, глибоке навчання може виявити аномалії у взаємодії файлів із системою, позначаючи зловмисний намір, навіть якщо зловмисне програмне забезпечення ніколи раніше не зустрічалося.

Ця здатність вивчати тонкі моделі поведінки значно покращує час виявлення та реакції на раніше невидимі загрози, що робить глибоке навчання необхідним для того, щоб випереджати складні кібератаки.

Нейронні мережі — це моделі штучного інтелекту, натхненні структурою людського мозку. У них вузли обробляють дані за допомогою зважених вхідних даних. Кожен вузол оцінює свій вхід, регулюючи ваги для підвищення точності. Кінцевий результат базується на сумі цих оцінок. У сфері кібербезпеки нейронні мережі допомагають аналізувати величезні масиви даних, наприклад журнали брандмауера, для виявлення закономірностей і прогнозування потенційних загроз, що робить їх потужним інструментом для виявлення загроз.

Великі мовні моделі — представляють ще одну важливу технологію AI в кібербезпеці. Вони спеціалізуються на обробці та розумінні людської мови, що робить їх дуже корисними для автоматизації аналізу загроз і покращення реагування безпеки. Ці моделі можуть аналізувати величезну кількість текстових даних, таких як звіти про загрози, журнали та документація, щоб визначити потенційні ризики та шаблони, які можуть сигналізувати про атаку.

Вони також допомагають із такими завданнями, як виявлення фішингу, створення зрозумілих людині звітів про загрози та автоматизація реагування на інциденти безпеки [14].

Висновки до першого розділу

Соціальні мережі відіграють важливу роль у контексті конфіденційності та кібербезпеки, що набуває особливого значення в умовах зростання кількості користувачів. У цьому розділі розглянуто класифікацію методів захисту інформації, зокрема організаційно-правові, інженерно-технічні, криптографічні та біометричні методи, а також автентифікацію та контроль доступу. Особливу увагу приділено перевагам шифрування як найнадійнішого методу захисту даних, зокрема у платформах обміну повідомленнями, які використовують передові криптографічні примітиви.

Доведено, що двофакторна автентифікація є ключовим заходом безпеки, який забезпечує баланс між захищеністю та зручністю використання, а її економічно ефективне впровадження підвищує цілісність систем.

Проаналізовано концепцію соціальних мереж із підтримкою блокчейну, які характеризуються децентралізацією, автономним управлінням та використанням заздалегідь визначених протоколів, що робить їх перспективною організаційною формою.

Зазначено, що розвиток штучного інтелекту значно підсилює можливості кібербезпеки. AI здатний аналізувати загрози в реальному часі, автоматизувати складні процеси безпеки та створювати динамічні середовища для введення кіберзловмисників в оману. Це дозволяє організаціям бути на крок попереду кіберзлочинців і ефективніше захищати свої системи.

Отже, сучасні технології, такі як блокчейн, криптографія та штучний інтелект, є критично важливими для забезпечення надійності та стійкості соціальних мереж у сучасному кіберпросторі.

РОЗДІЛ 2. ПОЛІТИКА ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

У сучасному цифровому світі соціальні мережі стали невід'ємною частиною нашого життя. Вони об'єднують людей, спрощують обмін інформацією та відкривають нові можливості для спілкування. Однак із зростанням популярності цих платформ все більше уваги приділяється питанням конфіденційності та безпеки даних користувачів. Важливим є аналіз політики конфіденційності соціальних мереж, їхніх підходів до обробки даних, механізмів захисту інформації та можливостей користувачів щодо контролю над своїми персональними даними. У цьому розділі будуть розглянуті ключові аспекти, пов'язані з обробкою даних соціальними мережами, зокрема:

- збір та використання даних: чи обмежується обробка даних бізнес-цілями компанії, чи вони також продаються або купуються у брокерів даних;
- контроль користувачів над своїми даними: які інструменти надаються для управління конфіденційністю;
- політика захисту даних: репутація компанії у сфері забезпечення безпеки користувачів.

Особливу увагу буде приділено мінімальним стандартам безпеки, які, на нашу думку, повинні бути реалізовані на цих платформах, включаючи:

1. Шифрування даних для забезпечення конфіденційності комунікацій.
2. Оновлення безпеки, які автоматично захищають від відомих вразливостей.
3. Надійні паролі, що запобігають атакам методом вгадування.
4. Управління вразливостями, включаючи програми повідомлення про помилки.
5. Прозора політика конфіденційності, яка інформує користувачів про використання їхніх даних.

Цей аналіз дозволяє виявити потенційні ризики конфіденційності та безпеки, а також оцінити відповідність соціальних мереж сучасним вимогам у

сфері захисту даних. До розгляду візьмемо шість найбільш популярних СМ в Україні: Facebook Messenger, WhatsApp, Telegram, Viber, WeChat, Signal.

2.1. Facebook Messenger

Facebook Messenger має такі функції, як відеочат, можливість запису голосових повідомлень, текстових чатів, групових чатів, обміну фотографіями та відео, а також функцію під назвою Messenger Rooms, яка дозволяє до 50 людей спілкуватися по відео одночасно навіть без облікового запису Facebook. Facebook досить добре відомий тим, що збирає особисті дані користувачів, зокрема вказуючи у своїй політиці конфіденційності, що може використовувати функцію камери для збору цих даних.

Розглянемо ризики та наслідки порушень конфіденційності компанії. Нажаль, користувачі завжди схвильовані роботою застосунків, що належать Facebook. Він має довгу історію необережного поводження з особистими даними людей. Facebook каже, що не використовує вміст повідомлень, щоб вибрати, яку рекламу показувати, але він не робить подібних заяв щодо інших типів інформації, що міститься у вашому застосунку — з ким ви розмовляєте, коли та інше. Facebook збирає велику кількість таких даних, щоб використовувати їх для націлювання реклами, і залишає за собою право ділитися ними з численними третіми сторонами.

Категорії даних, які збираються Facebook:

- особисті: ім'я, адреса електронної пошти, місцезнаходження, геолокація на фотографіях, сімейний стан, місто проживання, робота та освіта, номер телефону, аудіодані, відеодані;
- соціальні: люди або облікові записи, з якими ви взаємодієте, а також час, частота та тривалість діяльності; зміст комунікацій.

Механізм використання цих даних компанією: Facebook стверджує, що не продає свої дані, але ділиться ними з численними третіми сторонами, такими як

партнери, які використовують їхні аналітичні служби, рекламодавці, партнери, що пропонують товари та послуги, постачальники, дослідники та науковці, правоохоронні органи та юридичні запити.

Відповідно до цього розглянемо інструменти управління персональними даними користувачів: Facebook стверджує, що зберігає дані до тих пір, поки більше не буде потрібно надавати їхні послуги та продукти Facebook, або поки ваш обліковий запис не буде видалено – залежно від того, що станеться раніше. Тому єдиним зрозумілим способом видалення даних є видалення профілю Facebook. Видалення даних може тривати до 90 днів [15].

Важливим елементом для розуміння рівня захищеності соціальної мережі в аспекті кібербезпеки є репутація компанії у сфері захисту даних. Розглянемо декілька реальних випадків:

Ймовірно, найбільший скандал щодо конфіденційності Facebook пов'язаний з розголошенням даних про 87 мільйонів користувачів політичній консалтинговій фірмі Cambridge Analytica. Ця британська фірма обробки даних, яка працювала під час президентської кампанії Дональда Трампа в 2016 році, зібрала мільйони профілів американських виборців у Facebook і використала їх для створення потужного програмного забезпечення для прогнозування та формування вибору під час голосування.

Один із найзначніших витоків даних у Facebook стався у квітні 2019 року, коли було розкрито понад 540 мільйонів записів користувачів. Дані були скомпрометовані після того, як їх надали стороннім програмам, які використовували незахищені сервери.

Найзначніший витік даних Facebook у 2021 році стався в квітні внаслідок уразливості системи безпеки, яку Facebook усунув у 2019 році. Аварія виявила такі деталі, як імена, номери телефонів, ідентифікатори Facebook, електронні листи, статуси стосунків і місцезнаходження 533 мільйонів користувачів Facebook зі 106 країн. Ці дані були знайдені на хакерському форумі, звідки їх можна було завантажити безкоштовно.

У жовтні 2023 року зловмисник на ім'я «алгоатсон» нібито вкрав базу даних у підрядника, відповідального за керування хмарними сервісами Facebook. Однак база даних була оприлюднена лише в лютому 2024 року, коли з Facebook Marketplace витік 200 000 записів користувачів. Цей витік даних у Facebook відкрив особисту інформацію користувачів, включаючи номери телефонів і адреси електронної пошти, на форумі хакерів.

Виходячи з цього, розглянемо, які, з описаних нами вище, мінімальних стандартів безпеки реалізовані у Facebook: Messenger до 2022 року використовував шифрування, але не використовував наскрізне шифрування за замовчуванням. Люди, які використовували програму Messenger на iOS та Android до того часу, могли увімкнути «Секретні розмови», які дійсно використовували наскрізне шифрування для текстових, аудіо- та відеочатів. Пізніше компанія заявила, що наскрізне шифрування стає галузевим стандартом і працює як замок і ключ, де тільки користувач та його співрозмовник в чаті або виклику мають доступ до розмови. Вміст повідомлень і дзвінків у наскрізній зашифрованій розмові захищено з моменту, коли вони покидають ваш пристрій, до моменту, коли вони досягають пристрою одержувача. Це означає, що ніхто інший, включаючи Facebook, не зможе побачити або прослухати те, що надіслано або сказано. Також вони наполегливо рекомендують увімкнути безпечне сховище, щоб створити резервну копію історії чату та відновити її на будь-якому новому пристрої. Якщо цього сховища не буде, всі повідомлення та мультимедійні дані можуть бути назавжди втрачені при втраті пристрою. Facebook підтримує оновлення безпеки, керує вразливістю, має загальнодоступну політику конфіденційності та для входу в Messenger потрібен надійний пароль, однак дзвінки неможливо захистити паролем. А також Facebook використовує «штучний інтелект для виявлення незвичайних моделей поведінки, пов'язаних із фішингом, шахрайством та іншими шкідливими діями, щоб видалити їх із платформи» [15].

2.2. WhatsApp

WhatsApp — одна з найпопулярніших програм для обміну повідомленнями у світі, яка налічує близько 2,2 мільярдів користувачів у всьому світі. Застосунок належить Facebook. WhatsApp дозволяє здійснювати дзвінки один на один і групові дзвінки до восьми людей. Треба бути обережним, у WhatsApp є досить відома проблема дезінформації.

Розглянемо ризики та наслідки порушень конфіденційності компанії. На початку 2021 року WhatsApp, що належить Facebook, викликав неабияку суперечку, коли поскаржився на мітки конфіденційності магазину додатків Apple, які показують усі дані, які додаток використовує. Тоді WhatsApp оновив свою політику конфіденційності таким чином, що налякав людей, виправдано чи ні, що спричинило величезний перехід користувачів WhatsApp до таких програм, як Telegram і Signal. А потім Ірландія наклала на WhatsApp рекордний штраф у розмірі 266 мільйонів доларів за нібито відсутність прозорості щодо того, як він ділиться даними з Facebook. WhatsApp використовує надмічне наскрізне шифрування для всіх текстових повідомлень, чатів і відеодзвінків. Він не може читати ваші повідомлення чи бачити ваші дзвінки. Зворотний бік цього полягає в тому, що Facebook — компанія, відома своїм величезним і сумнівно етичним збором великої кількості даних — володіє WhatsApp. Це означає, що багато метаданих, як-от історія покупок, місцезнаходження, ідентифікатор пристрою тощо, можна отримувати та ділитися з компаніями, які рекламують у WhatsApp. Крім обміну повідомленнями, варто розглянути роль WhatsApp у поширенні дезінформації. У 2020 році WhatsApp став головним джерелом дезінформації про коронавірус. WhatsApp дійсно вжив заходів, щоб спробувати зупинити потік дезінформації, коли почав обмежувати кількість разів, коли люди можуть передавати часто пересиланий вміст до п'яти чатів одночасно. Сьогодні проблема дезінформації — це проблема, яку кожен має знати та робити все можливе, щоб не погіршити ситуацію.

Категорії даних, які збираються WhatsApp:

- особисті: ім'я профілю на вибір користувача, номер телефону;
- соціальні: метадані, включаючи контакти, інформацію про вашу діяльність, зокрема те, як ви використовуєте Сервіси WhatsApp, ваші налаштування Сервісів, як ви взаємодієте з іншими, використовуючи Сервіси (зокрема, коли ви взаємодієте з компанією), а також час, частоту та тривалість вашої діяльності і взаємодії.

Механізм використання цих даних компанією: існує складний ланцюжок переміщення даних між WhatsApp і Facebook, а потім до багатьох третіх сторін. Якщо ви використовуєте WhatsApp для спілкування з компаніями, програма обміну повідомленнями, що належить Facebook, може ділитися даними профілю користувача з Facebook. У політиці зазначено: «Ми співпрацюємо зі сторонніми постачальниками послуг та іншими компаніями Facebook, щоб допомогти нам працювати, надавати, покращувати, розуміти, налаштовувати, підтримувати та продавати наші Сервіси». Ця інформація може бути використана Facebook та іншими її продуктами, щоб надавати вам пропозиції, персоналізувати функції та вміст, допомагати вам здійснювати покупки та транзакції, а також показувати відповідні пропозиції та рекламу в продуктах компанії Facebook.

Відповідно до цього розглянемо інструменти управління персональними даними користувачів: єдиний спосіб видалення особистих даних, згаданий у політиці WhatsApp, — це повне видалення облікового запису. Видалення облікового запису призведе до видалення інформації облікового запису та фотографії профілю, видалення вас із усіх груп WhatsApp і видалення історії повідомлень WhatsApp. Видалення даних може тривати до 90 днів. Копії вашої інформації також можуть залишатися в резервному сховищі протягом 90 днів «для відновлення у разі аварії, помилки програмного забезпечення або іншої події втрати даних» [16].

Важливим елементом для розуміння рівня захищеності соціальної мережі в аспекті кібербезпеки є репутація компанії у сфері захисту даних. Розглянемо декілька реальних випадків: у 2022 році було виявлено, що база даних із

номерами телефонів 487 мільйонів користувачів WhatsApp з 84 країн з'явилася на продаж на хакерському форумі. Витік містив дані, які могли бути використані для фішингу, спаму та інших зловмисних дій. WhatsApp заявив, що дані могли походити з витоків, пов'язаних із сторонніми платформами, а не з їхніх серверів.

Зловмисники могли використовувати шкідливий файл для запуску коду на пристроях Android користувачів через WhatsApp. Компанія швидко випустила оновлення, щоб виправити проблему, але вразливість підкреслила важливість постійного оновлення програмного забезпечення.

WhatsApp неодноразово ставав об'єктом фішингових атак, що використовували довіру до платформи. Наприклад, злочинці часто надсилали підроблені повідомлення для отримання доступу до облікових записів користувачів.

Виходячи з цього, розглянемо, які, з описаних нами вище, мінімальних стандартів безпеки реалізовані у WhatsApp: усі повідомлення та дзвінки за замовчуванням мають наскрізне шифрування. Наскрізне шифрування гарантує, що ваші повідомлення доступні для читання та прослуховування тільки вам і вашому співрозмовнику – і більше нікому, навіть WhatsApp. Наскрізне шифрування – це унікальний замок, який захищає ваші повідомлення, і тільки в отримувача та у вас є спеціальний ключ, який необхідний, щоб розблокувати й прочитати ваші повідомлення. Усе це відбувається автоматично: вам не потрібно вмикати спеціальні налаштування, щоб забезпечити захист своїх повідомлень. Зауважте, що метадані не шифруються та не надаються в групі Facebook. Усі повідомлення WhatsApp захищені одним і тим самим протоколом шифрування Signal, який захищає повідомлення перед надсиланням із вашого пристрою. Коли ви надсилаєте повідомлення обліковому запису компанії у WhatsApp, доставка вашого повідомлення здійснюється безпечним способом на пристрій, вибраний компанією. Примітка. Процес перевірки для захищених наскрізним шифруванням чатів не є обов'язковим і використовується тільки для того, щоб переконатися, що надіслані повідомлення та вихідні виклики

зашифровані наскрізним шифруванням. WhatsApp підтримує оновлення безпеки, керує вразливістю, більше того, має програму винагороди за знайдені помилки у вразливості безпеки, має загальнодоступну політику конфіденційності.

Для виклику у WhatsApp не потрібно вводити пароль. Він дозволяє користувачам налаштувати блокування відбитками пальців або faceID як додатковий рівень безпеки, хоча це не ввімкнено за замовчуванням і лише для iPhone [16].

2.3. Telegram

У 2021 році Telegram став одним із найбільш завантажуваних додатків у світі, і зараз його активними користувачами є понад 900 мільйонів щомісяця. Завдяки таким функціям, як секретні чати, які можуть самознищуватися, можливість надсилати повідомлення до 200 000 людей у групі, групові відеодзвінки і канали з одностороннім обміном повідомленнями, Telegram став улюбленцем, але, нажаль, він також став улюбленим місцем для людей, які діляться дезінформацією, ненавистю, дитячим порно, і викраденими персональними даними. Telegram охоче називає себе однією з найбільш приватних і безпечних програм, але це іноді викликає сумніви.

Розглянемо ризики та наслідки порушень конфіденційності компанії. Хороші моменти: відеодзвінки (та голосові) шифруються наскрізно, що робить їх приватними та безпечними від початку до кінця.

Погані моменти: текстові повідомлення та файли не шифруються наскрізно за замовчуванням. Це означає, що якщо користувачі не вибрали функцію «секретного чату» Telegram, яка використовує наскрізне шифрування, ця інформація може бути вразливою для перехоплювачів. Схоже, у Telegram також є проблема стороннього AI-бота. Ці AI-боти можуть робити цікаві речі, наприклад, відповідати на повідомлення та планувати нагадування. Можливі ще

жахливі речі: бот штучного інтелекту створював образливі фейки оголених зображень жінок і дівчат. І що ще гірше, дослідники стверджують, що спочатку Telegram не дуже реагував на видалення цього огидного бота. Інші погані новини: у Telegram було кілька досить серйозних хакерів і недоліків у безпеці.

Категорії даних, які збираються Telegram:

- особисті: номер телефону, ім'я користувача, зображення профілю (необов'язково), інформація «про» (необов'язково), електронна пошта (необов'язково, для двоетапної перевірки), відеодані;
- соціальні: за замовчуванням: контакти, метадані, повідомлення, фотографії, аудіо, відео та файли, файли cookie. Додатково: місцезнаходження та поточне місцезнаходження.

Механізм використання цих даних компанією: вона стверджує, що не продає дані та використовує їх лише з метою надання основних послуг і пов'язаного з ними досвіду користувачів.

Відповідно до цього розглянемо інструменти управління персональними даними користувачів: що стосується Telegram, то персональні дані, які ви їм надаєте, зберігатимуться лише до тих пір, поки це необхідно для виконання їхніх зобов'язань щодо надання Послуг. Видалення облікового запису видаляє всі повідомлення, медіа, контакти та всі інші дані, які ви зберігаєте в хмарі Telegram. Цю дію потрібно підтвердити через обліковий запис Telegram. Будь-яка сторона може видалити будь-які повідомлення в чатах один на один, як надіслані, так і отримані, для обох сторін і без обмеження часу [17].

Важливим елементом для розуміння рівня захищеності соціальної мережі в аспекті кібербезпеки є репутація компанії у сфері захисту даних. Розглянемо декілька реальних випадків: іранська хакерська група Rocket Kitten у 2016 році використала уразливість у функції експорту контактів, що призвело до витоку даних 15 мільйонів користувачів, включаючи електронні адреси, номери телефонів та списки контактів. Більшість постраждалих користувачів були з Ірану та Росії. Telegram після цього посилив свої заходи безпеки, хоча подробиці про покращення не розкривалися.

У 2019 році Telegram став об'єктом масштабної DDoS-атаки, яка за твердженням засновника Павла Дурова, походила з Китаю. Атака була пов'язана з протестами в Гонконзі, що координувалися через платформу. Telegram зміг стабілізувати роботу сервісу, але подія підкреслила його вразливість до атак державного масштабу.

Хоч Telegram сам не був зламаний, платформа часто використовується кіберзлочинцями для обміну великими базами даних. Наприклад, у 2024 році через Telegram поширювали 361 мільйон електронних адрес, викрадених за допомогою шкідливого ПЗ. Це підняло питання про контроль за контентом на платформі.

Виходячи з цього, розглянемо, які, з описаних нами вище, мінімальних стандартів безпеки реалізовані у Telegram: якщо ви зареєструвалися з Європи, ваші дані зберігаються в дата-центрах у Нідерландах. Ці дата-центри належать стороннім організаціям, у яких Telegram орендує призначений простір. Однак сервери та мережі, які знаходяться в цих дата-центрах і на яких зберігаються ваші персональні дані, належать Telegram. Вони не передають ваші персональні дані таким дата-центрам. Усі дані зберігаються в надійно зашифрованому вигляді, тому місцевий технічний персонал Telegram або зловмисники (наприклад, у разі проникнення до дата-центру) не можуть отримати до них доступ.

Ваші повідомлення, мультимедіа та інші файли із секретних чатів, а також вміст ваших дзвінків і дані, які ви зберігаєте у своєму Telegram Passport, обробляються тільки на вашому пристрої та на пристрої співрозмовника. Перш ніж ці дані потрапляють на наші сервери, вони шифруються за допомогою ключа, відомого тільки вам і одержувачу. Хоча сервери Telegram обробляють ці наскрізно зашифровані дані, щоб доставити їх одержувачу — або, у випадку з Telegram Passport, щоб зберегти їх, — вони не мають технічної можливості розшифрувати їх. Тому у цьому разі вони не зберігають й не обробляють ваші персональні дані як такі, а зберігають й обробляють випадкові послідовності символів, які не мають ніякого значення без ключів — яких вони не мають.

Сервіс регулярно надає оновлення безпеки. У Telegram є спеціальна команда, яка виправляє деякі відомі вразливості безпеки в програмі досить швидко, має загальнодоступну політику конфіденційності. А також Telegram використовує авторизацію через SMS, для чатів можна додати пароль як додатковий рівень безпеки. Telegram використовує штучний інтелект, але має негативний досвід. У жовтні 2020 року регулятори із захисту даних в Італії розпочали розслідування щодо бота *deepfake* у Telegram, який, імовірно, створив понад 100 000 образливих зображень жінок, у т.ч. неповнолітніх. На iOS від Apple було обмежено доступ до бота. У звітах з Америки, Південної Кореї та Ізраїлю також детально описано, як Telegram використовувався для поширення образливих зображень протягом 2020 року. Telegram ніколи публічно не коментував шкоду, завдану роботом Telegram, або його постійну позицію, яка дозволяє йому працювати [17].

2.4. Viber

Голосові дзвінки, відеодзвінки, групові чати, стікери, соціальні канали, чати, що самознищуються, наскрізне шифрування, багато спаму та цільова реклама. Viber пропонує всі найкращі хіти світу програм обміну повідомленнями. Це величезна платформа, яка схожа на суміш WhatsApp і Telegram. Під час пандемії Viber розширив функції групового відеочату, щоб дозволити більше користувачів, що призвело до появи цікавих речей, як-от вчителі в Угорщині використовували його, щоб підтримувати зв'язок зі своїми учнями.

Розглянемо ризики та наслідки порушень конфіденційності компанії. Здається, Viber досить добре захищає конфіденційність і безпеку своїх користувачів. Особливо в порівнянні з іншими подібними програмами обміну повідомленнями, такими як Telegram і Whatsapp. Все не ідеально, але він використовує наскрізне шифрування за замовчуванням з 2016 року. Ще одна

хороша річ, яку він робить: щойно повідомлення доставлено, воно видаляється з серверів Viber, тому ваші повідомлення не залишаються там, де інші потенційно можуть отримати до них доступ, і ви можете вибрати, щоб приховати себе від будь-якого з контактів у вашому списку контактів. Деякі моменти у Viber викликають розчарування: коли ви приєднуєтеся до групи, ваш номер телефону бачитимуть усі учасники групи, а це може бути багато людей. Крім того, Viber мав проблеми з людьми, які надсилали багато спаму та вірусів, треба дуже уважно читати або завантажувати матеріали від сторонніх людей. Повідомляється, що близько 20% доходу Viber приносить реклама. Вони збирають інформацію про місцезнаходження IP-адреси, стать і вік користувачів, щоб націлити ці оголошення, хоча користувачі можуть відмовитися від націлювання за статтю та віком, якщо знайдуть час, щоб змінити свої налаштування. Їхні рекламні партнери також можуть поєднувати дані, зібрані про вас під час використання Viber, зі своїми зовнішніми записами для ще більшого націлювання. Чудовою новиною є те, що у 2020 році Viber приєднався до кампанії #StopHateForProfit і розірвали всі ділові зв'язки з Facebook. Тепер це компанія, яка виступає проти ненависті, дезінформації та неетичної практики конфіденційності.

Категорії даних, які збираються Viber:

- особисті: ім'я, електронна адреса, дата народження, вік, номер телефону та, якщо необхідно, платіжна інформація. Місцезнаходження (дані про місцезнаходження WPS) - якщо дозволено в налаштуваннях;
- соціальні: копія телефонних номерів та імен усіх ваших контактів. Якщо реєстрація через третіх осіб (наприклад, Facebook) - ваш загальнодоступний профіль, список друзів, облікові записи, на які ви підписані або які підписалися на вас, електронна адреса, день народження, історія роботи, історія освіти, інтереси, поточне місто та перегляд відео.

Механізм використання цих даних компанією: Viber використовує файли cookie та технології відстеження рекламодавцями (включаючи Google, Twitter, тощо). Таким чином, вони вмикають цільову рекламу у власному додатку Viber,

а також дозволяють численним третім особам поєднувати інформацію, яку вони збирають із Viber, з іншою інформацією, яку вони самостійно зібрали стосовно діяльності вашого веб-браузера в їхній мережі веб-сайтів. Інформація, яку Viber збирає, може поєднуватися з інформацією із зовнішніх записів (наприклад, демографічною інформацією та додатковою контактною інформацією), яку вони «отримали відповідно до закону». Коли ви приєднуєтеся до Viber, контакти у вашій адресній книзі, які вже є учасниками Viber, можуть отримувати інформацію про те, що ви тепер також у Viber.

Відповідно до цього розглянемо інструменти управління персональними даними користувачів: доки обліковий запис не буде деактивовано, усі пов'язані дані можуть зберігатися протягом невизначеного часу. Після деактивації вашого облікового запису Viber обіцяє звести до мінімуму особисті дані, які вони зберігають про вас, лише до тих даних, які вони повинні зберігати для дотримання законів або інших юридичних причин. Вони можуть зберігати дані про діяльність без ідентифікації, щоб покращити свої послуги (не передбачено жодних способів деідентифікації). Ваші публікації в загальнодоступних облікових записах, спільнотах і каналах можуть залишатися доступними, якщо ви їх не видалите [18].

Важливим елементом для розуміння рівня захищеності соціальної мережі в аспекті кібербезпеки є репутація компанії у сфері захисту даних. Розглянемо декілька реальних випадків: у 2013 році через фішинг-атаку зловмисники отримали доступ до двох систем Viber, що дозволило зламати сайт служби підтримки та отримати доступ до деяких даних. Компанія стверджувала, що дані користувачів не були скомпрометовані, але випадок підкреслив слабкість захисту від соціальної інженерії.

Виявлена вразливість у 2015 році дозволяла зловмисникам обійти механізми безпеки Viber на мобільних пристроях. Це створювало ризик несанкціонованого доступу до облікових записів через експлуатацію слабких місць у програмному забезпеченні. Проблема було вирішено через оновлення безпеки.

Пропалестинська хактивістська група у 2024 році заявила, що викрала 740 ГБ даних з серверів Viber, включаючи вихідний код, журнали викликів, особисті повідомлення та фінансову інформацію. Група вимагала викуп у 8 біткоїнів (приблизно 540 000 доларів США). Однак Viber заявив, що не знайшов доказів зламу, але проводить розслідування. Рекомендовано змінювати паролі та уникати підозрілих посилань.

Виходячи з цього, розглянемо, які, з описаних нами вище, мінімальних стандартів безпеки реалізовані у Viber: Viber за замовчуванням забезпечує наскрізне шифрування для приватних, групових чатів і дзвінків 1-на-1. Повідомлення шифруються під час надсилання з вашого пристрою і розшифровуються лише на пристрої одержувача. Ключі шифрування розташовані лише на пристроях користувачів і більше ніде. Ніхто — навіть Viber — не може прочитати ваші повідомлення. Групові виклики шифруються лише під час передачі. Для входу у Viber не потрібен пароль, під час реєстрації користувачі повинні підтвердити свій номер телефону. Користувачі мають можливість додати код безпеки, також можуть увімкнути захищені паролем секретні чати у Viber із таймером самознищення. Коли ви знайомитеся з новими людьми в спільнотах або знаходите їх по імені у Viber, починайте спілкування безпечно, не розкриваючи свої номери телефонів. Ви також можете контролювати, чи бачитимуть інші, що ви зараз онлайн або вже прочитали їхні повідомлення. У разі будь-якої вразливості системи безпеки оновлення програми Viber буде виконано негайно та надіслано в рамках звичайного процесу оновлення програми. Він також співпрацює із зовнішніми сторонами, які допомагають знайти такі вразливості та перевірити, чи їх виправлення виправляють проблеми. Має загальнодоступну політику конфіденційності. Viber використовує кілька систем штучного інтелекту та машинного навчання у своїх серверних системах для таких речей, як виявлення спаму, модерація спільноти, мовний переклад тощо. Viber стверджує, що відкритий доступ до алгоритму AI фактично завадить їхній меті (наприклад, спамери знатимуть, як обійти їхні системи та атакувати користувачів) [18].

2.5. WeChat

WeChat — надзвичайно популярна програма для соціальних мереж і обміну повідомленнями, належить китайському технологічному гіганту. І коли ми говоримо про популярність, ми маємо на увазі, що це одна з найбільш завантажуваних програм у світі, з понад мільярдом активних користувачів. Це також одна з найменших програм для обміну приватними повідомленнями. Вона пропонує всі функції — текстовий чат, відео- та голосовий чат, обмін інформацією про місцезнаходження, наклейки, ігри, WeChat Pay і навіть способи тренуватися з друзями.

Розглянемо ризики та наслідки порушень конфіденційності компанії. WeChat не тільки поганий щодо конфіденційності, але й буває лякає. Відсутність наскрізного шифрування, витік сотень мільйонів журналів приватних чатів, повідомлення про нещодавню заборону дружніх до ЛГБТ і феміністичних акаунтів, ймовірне іноземне стеження та цензура — це все дуже насторожує. Так, WeChat дуже популярний і багатофункціональний, але це не переважає поганий досвід WeChat щодо конфіденційності та безпеки.

Категорії даних, які збираються WeChat:

- особисті: ім'я, псевдонім користувача, номер мобільного телефону, пароль, стаття, IP-адреса, докладні дані про місцезнаходження (з GPS, IP-адреси, компаса, акселерометра або загальнодоступних публікацій, які містять інформацію про місцезнаходження). Додатково: екстрені контакти, керовані пристрої, адреса електронної пошти і, якщо ви виберете: номер кредитної картки, картографування/розпізнавання обличчя та/або вхід через Apple. Будь-яка інформація, яку ви включаєте у свій загальнодоступний профіль WeChat, яка може включати ідентифікатор вашого профілю, ім'я та фотографію;
- соціальні: уся інформація, яку ви надаєте іншим користувачам через WeChat. Вміст спілкування між вами та іншим користувачем або групою користувачів. Ваш список контактів на пристрої. Використані терміни веб-пошуку, відвідані профілі в соціальних мережах та деталі іншої інформації та

вмісту, до яких ви отримували доступ або запитували під час використання WeChat.

Механізм використання цих даних компанією: WeChat може передавати будь-які дані (включаючи вміст зв'язку) урядовим, громадським, регулятивним, судовим і правоохоронним органам або органам влади, коли це необхідно. Крім того, даними WeChat можна ділитися з низкою компаній групи. WeChat також каже, що вони можуть ділитися даними користувачів із низкою третіх сторін. Усім користувачам WeChat варто зауважити, що Tencent також керує Weixin, службою, сумісною з WeChat, орієнтованою на користувачів у материковому Китаї. У політиці конфіденційності WeChat вони зазначають: «Коли ви взаємодієте з користувачем Weixin або використовуєте чи отримуєте сповіщення від будь-якої функції, якою керує Weixin, майте на увазі, що ваша інформація може збиратися, зберігатися, ділитися та/або зберігатися Weixin у відповідно до Рекомендацій із захисту конфіденційності Weixin, а не цієї Політики конфіденційності». Отже, якщо ви, як користувач WeChat, взаємодієте з користувачем Weixin (і можете не знати, хто в службі є користувачами Weixin, а не WeChat), ваші права на конфіденційність будуть захищені лише в межах політики конфіденційності Weixin, яка ще менш захищена.

Відповідно до цього розглянемо інструменти управління персональними даними користувачів: WeChat каже, що ви можете видалити свій обліковий запис або певну особисту інформацію, увійшовши в обліковий запис WeChat і дотримуючись інструкцій щодо видалення облікового запису. Компанія надає чіткі терміни зберігання всіх даних. Відповідно до статті дослідників Массачусетського технологічного інституту від 2019 року, коли користувач видаляв голосове або текстове повідомлення замість того, щоб видаляти дані з локальної бази даних, WeChat просто видаляв сховище ключів для даних. Однак, оскільки ці дані залишалися в локальному сховищі, дані фактично не були видалені. WeChat зазначив, що зараз, коли користувач видаляє повідомлення з чату, додаток WeChat негайно видаляє як ключ повідомлення, так і вміст цього повідомлення з локального сховища користувача [19].

Важливим елементом для розуміння рівня захищеності соціальної мережі в аспекті кібербезпеки є репутація компанії у сфері захисту даних. Розглянемо декілька реальних випадків: WeChat ніби-то автоматично цензурує приватні розмови в реальному житті як для китайських, так і для некитайських користувачів. У березні 2019 року в Інтернеті виявили базу даних із 364 мільйонами записів користувачів із Китаю. Кожен запис також містив персональні ідентифікаційні номери громадянина Китаю, фотографії, адреси, дані про місцезнаходження GPS та інформацію про тип використовуваного пристрою. База даних також надсилала дані на 17 віддалених серверів у різних провінціях Китаю. Є підозри, що дані розповсюджуються між відділками поліції. Як повідомляється, у липні 2021 року WeChat також закрити сотні дружніх до ЛГБТ облікових записів.

Пізніше хакери, як повідомляється, злили приблизно 1,4 мільярда облікових записів користувачів Tencent, великого китайського багатонаціонального конгломерату з величезним портфоліо, включаючи соціальні мережі, ігри та фінансові технології. Це порушення викликало серйозні занепокоєння щодо безпеки даних і потенційного впливу на користувачів у всьому світі.

Виходячи з цього, розглянемо, які, з описаних нами вище, мінімальних стандартів безпеки реалізовані у WeChat: він використовує шифрування, але не наскрізне. Для створення облікового запису потрібен пароль. Пароль має складатися з 8-16 символів і містити як цифри, так і літери/спеціальні символи. З моменту запуску в 2011 році вийшло понад 100 оновлень за стосунку. Має загальнодоступну політику конфіденційності та керований центр безпеки. Що стосується використання штучного інтелекту, то WeChat керує центром WeChat AI, який відкрито зосереджується на таких програмах, як розпізнавання мовлення та аудіо, обробка природної мови, розпізнавання облич, розуміння вмісту тощо. Основне занепокоєння полягає в тому, що цей штучний інтелект дозволяє цензуру, блокування посилань, зображень, тем або аудіо [19].

2.6. Signal

Signal належить некомерційній організації. Їхня місія полягає в «розробці технології конфіденційності з відкритим кодом, яка захищає свободу вираження поглядів і забезпечує безпечне глобальне спілкування». Це означає, що Signal – це безкоштовна програма для обміну повідомленнями та відеочату з відкритим вихідним кодом, орієнтована на конфіденційність, яка абсолютно вражає. Наприкінці 2020 року вони навіть додали підтримку для групових відеодзвінків. Signal не має реклами та не відстежує ваші дані, щоб будь-яким чином заробити на вас гроші. Вони покладаються на пожертви щедрих користувачів, щоб зберегти свій додаток відкритим і безкоштовним для всіх.

Розглянемо ризики та наслідки порушень конфіденційності компанії. Раніше у 2021 році, коли WhatsApp (належить Facebook) оголосив про зміни у своїй політиці конфіденційності, багато користувачів, які піклуються про конфіденційність, перейшли на Signal (тоді Signal намагався збільшити потужність свого сервера, щоб деякий час обслуговувати всіх нових користувачів). Користувачі, які перейшли з WhatsApp на Signal, зробили вдалий крок. Наскрізне шифрування Signal із відкритим вихідним кодом виділяють багато фахівців із безпеки. І Signal не відстежуватиме вас і не продаватиме ваші дані незнайомцям, які можуть використати їх для націлювання на вас дивних оголошень. До речі, нещодавно навіть повідомлялося, що генеральний директор Facebook Марк Цукерберг сам використовує Signal. Це багато про що говорить.

Категорії даних, які збираються Signal:

- особисті: номер телефону. Ім'я та фотографія необов'язкові та зашифровані наскрізно, тобто Signal не може їх отримати;
- соціальні: не збираються.

Механізм використання цих даних компанією: відповідно до Signal, він «ні в якому разі не продає, не здає в оренду та не монетизує ваші особисті дані чи контент». Signal реалізує принципи мінімізації даних - лише номер телефону

використовується як джерело даних - і захисту даних за замовчуванням і за проектом.

Відповідно до цього розглянемо інструменти управління персональними даними користувачів: ви можете скасувати реєстрацію свого номера телефону, але вам знадобиться доступ до нього, і ви можете зробити це лише через додаток. Ви також можете керувати видаленням повідомлень і чатів, щоб інші користувачі більше не мали до них доступу [20].

Важливим елементом для розуміння рівня захищеності соціальної мережі в аспекті кібербезпеки є репутація компанії у сфері захисту даних. Розглянемо декілька реальних випадків: у січні 2021 року дослідниця безпеки Google Project Zero Наталі Сільванович виявила помилку в Signal, яка дозволяла передавати аудіо без згоди користувача. Помилка була оперативно виправлена. Якщо хтось користується їхніми послугами, Signal дізнається номер телефону. Якщо хтось із ваших контактів приєднається до служби, ви зможете це побачити, якщо ви також є користувачем. Це корисна функція, якщо ви хочете знати, з ким можна спілкуватися в додатку, але може дратувати (і потенційно небезпечно), якщо ви хочете бути там таємно або якщо ваш уряд заборонив Signal.

Один значний інцидент, пов'язаний із безпекою даних Signal, стався через злом у Twilio, постачальнику Signal для перевірки телефонних номерів. У 2022 році зловмисники отримали доступ до системи підтримки клієнтів Twilio за допомогою фішингових методів. В результаті постраждали приблизно 1900 користувачів Signal. Зловмисники виявили телефонні номери та коди підтвердження SMS, що дозволило зловмисникам потенційно перереєструвати облікові записи Signal на різних пристроях. Однак надійна архітектура безпеки Signal гарантувала, що історія повідомлень, контакти чи дані профілю не були скомпрометовані, оскільки вони зберігаються локально на пристроях користувачів, а не на серверах Signal.

Signal пом'якшив вплив, скасувавши реєстрацію постраждалих облікових записів, сповістивши користувачів і заохочуючи їх увімкнути «Блокування

реєстрації», щоб запобігти неавторизованій повторній реєстрації. Цей інцидент також підкреслив вразливі місця під час використання номерів телефонів для підтвердження особи та підкреслив важливість безпеки сторонніх партнерів.

Виходячи з цього, розглянемо, які, з описаних нами вище, мінімальних стандартів безпеки реалізовані у Signal: ви реєструєте номер телефону під час створення облікового запису Signal. Номери телефонів використовуються для надання наших Послуг вам та іншим користувачам Signal. За бажанням ви можете додати до свого облікового запису іншу інформацію, наприклад ім'я та зображення профілю. Ця інформація зашифрована наскрізним шифруванням. Signal використовує повне наскрізне шифрування. Крім того, Signal використовує чудову практику наскрізного шифрування даних профілю. Це означає, що навіть якщо ви вирішите надати інформацію свого профілю, Signal не матиме до неї доступу – її буде надано лише вашим контактам / кому ви вибрали. Ще одна хороше рішення — безпечне виявлення того, хто з ваших контактів користується застосунком (знову ж таки, необов'язково). Для цього інформація з контактів на вашому пристрої може бути криптографічно хешована та передана на сервер, щоб визначити, які з ваших контактів зареєстровано. Є можливість заблокувати програму Signal за допомогою пароля. Signal забезпечує конфіденційність і не має доступу до ваших повідомлень. Ви несете відповідальність за безпеку свого пристрою та облікового запису Signal. Якщо ви втратите телефон, виконайте дії на їх сайті підтримки, щоб повторно зареєструватися для надання Послуг. Коли ви зареєструєтеся на новому пристрої, ваш старий пристрій перестане отримувати всі повідомлення та дзвінки.

У разі будь-якої вразливості системи безпеки оновлення програми Signal буде виконано негайно. Signal керує вразливими місцями безпеки і взагалі кожен може повідомити про вразливість. Має загальнодоступну політику конфіденційності [20].

2.7. Порівняння Facebook, WhatsApp, Telegram, Viber, WeChat, Signal

З огляду на вище описані характеристики соціальних мереж Facebook, WhatsApp, Telegram, Viber, WeChat і Signal, можна виділити декілька ключових критеріїв, за якими зробимо порівняння:

1. Збір даних.

Facebook та WeChat вирізняються масштабним збором даних для персоналізації реклами та аналітики, що може викликати занепокоєння у користувачів, які цінують конфіденційність. WhatsApp, як дочірня компанія Facebook, також передає певні метадані материнській компанії. У протиполог їм Signal і Telegram пропонують мінімальний збір даних, надаючи перевагу приватності користувачів.

2. Рівень захисту даних.

Signal і Telegram демонструють високі стандарти захисту завдяки наскрізному шифруванню та обмеженню збору даних. У той час Facebook та WeChat використовують дані для аналітики та реклами, що робить їх менш привабливими для користувачів, орієнтованих на конфіденційність.

3. Шифрування.

Signal забезпечує найвищий рівень захисту, використовуючи повне наскрізне шифрування без винятків. Viber і WhatsApp також використовують це шифрування повідомлень, але їхні платформи збирають більше метаданих. У Telegram наскрізне шифрування доступне лише в "секретних чатах", тоді як звичайні повідомлення менш захищені. WeChat має найслабший рівень захисту даних, що робить його вразливим до стороннього доступу.

4. Правові вимоги та прозорість.

Facebook і WhatsApp підпорядковуються суворішим нормам у Європейському Союзі, але демонструють меншу прозорість у інших регіонах. WeChat діє відповідно до китайського законодавства, що значно обмежує конфіденційність. Signal виділяється своєю прозорістю та відданістю захисту даних користувачів.

5. Роль користувача у захисті приватності.

Незалежно від політики соціальних мереж, користувачі самі можуть підвищити рівень конфіденційності, використовуючи налаштування приватності, обмежуючи обсяг розміщеної інформації та обираючи платформи з більш прозорою політикою.

Усі ці аспекти підкреслюють важливість свідомого вибору платформи для комунікації залежно від потреб у безпеці та конфіденційності. Підходити до цього вибору потрібно з урахуванням як функціоналу, так і ризиків. З огляду на це, Signal залишається лідером за рівнем конфіденційності та безпеки, тоді як WeChat демонструє найменший захист.

Висновки до другого розділу

Результати порівняння соціальних мереж підкреслюють значні відмінності у підходах до захисту даних та забезпечення конфіденційності користувачів. Прозорість у роботі суттєво залежить як від технічної реалізації безпеки, так і від регіональних правових вимог. Важливо зазначити, що платформи, які приділяють більше уваги захисту приватності, не лише підвищують рівень довіри, але й отримують конкурентну перевагу на ринку.

Користувачам слід свідомо підходити до вибору платформи, враховуючи функціонал, ризики та рівень захисту даних. Порівняння соціальних мереж Facebook, WhatsApp, Telegram, Viber, WeChat, Signal за рівнем збору даних, захисту інформації, використанням шифрування, дотриманням правових вимог та прозорістю політики конфіденційності довело, що Signal є лідером у захисті приватності, тоді як WeChat демонструє найменший рівень безпеки. Інші платформи займають проміжні позиції, балансують між комерційними інтересами та захистом даних користувачів.

РОЗДІЛ 3. МЕТОД ФОТОГРАФУВАННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

3.1. Використання традиційних методів захисту інформації в соціальних мережах

На сьогоднішній день соціальні мережі для підвищення рівня безпеки даних використовують не просто один метод, а комбінацію традиційних та сучасних методів і технологій захисту інформації, щоб якомога краще забезпечити конфіденційність, цілісність і доступність даних користувачів. Розглянемо основні аспекти – це шифрування даних, аутентифікація користувачів, контроль доступу, системи виявлення аномалій, політика конфіденційності, оновлення безпеки.

Шифрування даних - застосовується для захисту передавання та зберігання інформації, зокрема наскрізне шифрування. Воно використовується в месенджерах, таких як WhatsApp, Signal і Viber, для захисту комунікацій між користувачами.

Аутентифікація користувачів - соціальні мережі застосовують двофакторну автентифікацію, яка додає додатковий рівень безпеки до традиційних паролів. Це знижує ризик несанкціонованого доступу.

Контроль доступу - використовуються традиційні моделі управління доступом, такі як рольовий або дискреційний контроль, що забезпечують обмеження доступу до даних залежно від прав користувача.

Системи виявлення аномалій - завдяки інтеграції машинного навчання платформи можуть виявляти підозрілі дії, такі як несанкціонований вхід чи спроби фішингу.

Політика конфіденційності - соціальні мережі формують політику конфіденційності, яка пояснює, як збираються, зберігаються та використовуються дані. Її прозорість залежить від платформи.

Оновлення безпеки - регулярні оновлення програмного забезпечення допомагають усувати відомі вразливості, забезпечуючи захист від нових загроз.

Хоча традиційні методи забезпечують основу кібербезпеки, соціальні мережі активно впроваджують новітні технології, такі як штучний інтелект і блокчейн, щоб підвищити ефективність захисту та відповідати сучасним загрозам.

3.1.1. Пропозиція впровадження методу фотографування

Традиційні методи захисту інформації в соціальних мережах забезпечують базовий рівень кібербезпеки. Вони допомагають виявляти та запобігати загрозам, але мають обмеження, особливо коли йдеться про ідентифікацію зломисників, які вже отримали доступ до системи.

Один із ключових викликів сучасної кібербезпеки – це фішинг, викрадення облікових даних і несанкціонований доступ до облікових записів. У таких випадках традиційні методи захисту часто не дозволяють точно ідентифікувати зломисника.

Для вирішення цієї проблеми необхідно розширити традиційні підходи, впроваджуючи нові методи, які дозволяють не лише блокувати доступ, але й ідентифікувати зломисників. Одним із перспективних рішень є використання фотографування зломисника в момент несанкціонованого доступу.

Такий інтегрований підхід сприятиме створенню більш стійкої системи захисту, яка не лише запобігає доступу, але й забезпечує виявлення потенційних загроз [21].

3.1.2. Порівняння методу фотографування з традиційними методами захисту інформації в соціальних мережах

Порівняння методу фотографування зловмисника при несанкціонованому доступі із традиційними методами захисту інформації в соціальних мережах дозволяє зрозуміти його сильні та слабкі сторони. Основні аспекти для аналізу наведено в таблиці 3.1.

Таблиця 3.1

Порівняння методу фотографування із традиційними методами захисту інформації в соціальних мережах

Критерій	Метод фотографування	Традиційні методи
Ідентифікація зловмисника	Фотографування дозволяє зафіксувати фізичну особу.	Зазвичай обмежується IP-адресою, MAC-адресою або логами дій.
Швидкість реакції	Сповіщення надсилається миттєво після спроби злому.	Залежить від налаштувань моніторингу та аналізу подій.
Додатковий рівень безпеки	Захищає в реальному часі на фізичному рівні (при доступі до пристрою).	Базується на автентифікації паролем або багатофакторних рішеннях.
Використання апаратури	Вимагає веб-камери для роботи.	Не потребує додаткового обладнання.
Масштабованість	Підходить для локальних систем, але важко впроваджується на великі платформи.	Легко масштабується для великих соціальних мереж.
Конфіденційність	Може порушувати права користувача через зберігання/обробку фото.	Зазвичай відповідає стандартам конфіденційності.

Пропонований метод можна інтегрувати з традиційними методами для досягнення максимального рівня захисту. Така комбінація дозволить:

1. Збирати візуальні докази спроб доступу.
2. Підвищити рівень відповідальності користувачів та зловмисників, знаючи, що система здійснює фіксацію обличчя.

3. Допомогти швидше ідентифікувати порушника та вжити відповідних заходів.

3.2. Опис методу фотографування зловмисника в соціальних мережах

Метод передбачає автоматичне фотографування особи, яка намагається здійснити несанкціонований доступ до облікового запису в соціальній мережі. Потім це фото надсилається на електронну пошту власника облікового запису. Цей підхід поєднує механізми виявлення аномальної поведінки з використанням вбудованої камери пристрою.

Основна мета — ідентифікація зловмисника та забезпечення додаткового рівня захисту облікового запису. Припустимо, що до системи має доступ хтось інший. У цьому випадку існуючий користувач може виконати необхідні дії для протидії атаці, відключивши Інтернет, вийшовши з веб-сайтів соціальних мереж тощо [3].

3.2.1. Алгоритм і блок-схема пропонованого методу

Пункт 1. Ініціація:

Користувач вводить логін і пароль для доступу до облікового запису.

Пункт 2. Перевірка даних:

Система перевіряє, чи введено правильний пароль та інші дані.

Пункт 3. Виявлення аномалії:

Якщо пароль неправильний або запит надходить із невідомого пристрою/IP, система фіксує спробу як потенційно зловмисну.

Пункт 4. Фотографування:

Камера активується для зйомки користувача перед пристроєм.

Пункт 5. Розпізнавання обличчя:

Алгоритм AI виділяє ключові риси обличчя (контури, розташування очей, носа, рота тощо). Зображення порівнюється з наявними шаблонами обличчя власника облікового запису, які були збережені під час попередньої авторизації або реєстрації.

Пункт 6. Надсилання фото:

Фотографія автоматично надсилається користувачу на e-mail.

Пункт 7. Блокування доступу:

Система блокує подальші спроби доступу, доки власник акаунту не перевірить ситуацію.

Таким чином ключові етапи на блок-схемі будуть такими:

1. Введення логіну та пароля:

- Користувач вводить облікові дані.
- Дані передаються для перевірки.

2. Перевірка правильності облікових даних:

Якщо логін і пароль правильні:

- Користувач отримує доступ і відображається сторінка привітання.

Якщо неправильні:

- Активується захисний механізм.

3. Захисний механізм:

- Веб-камера робить фотографію зломисника.
- Зображення порівнюється з шаблоном обличчя власника:

Якщо зображення і шаблон співпадають:

- Повторне введення логіну та пароля.

Якщо не співпадають:

- Надсилається електронний лист власнику акаунта з фото.

4. Заборона доступу:

- Відображається повідомлення про несанкціонований доступ.

А сама блок-схема матиме наступний вигляд (рис. 3.1):

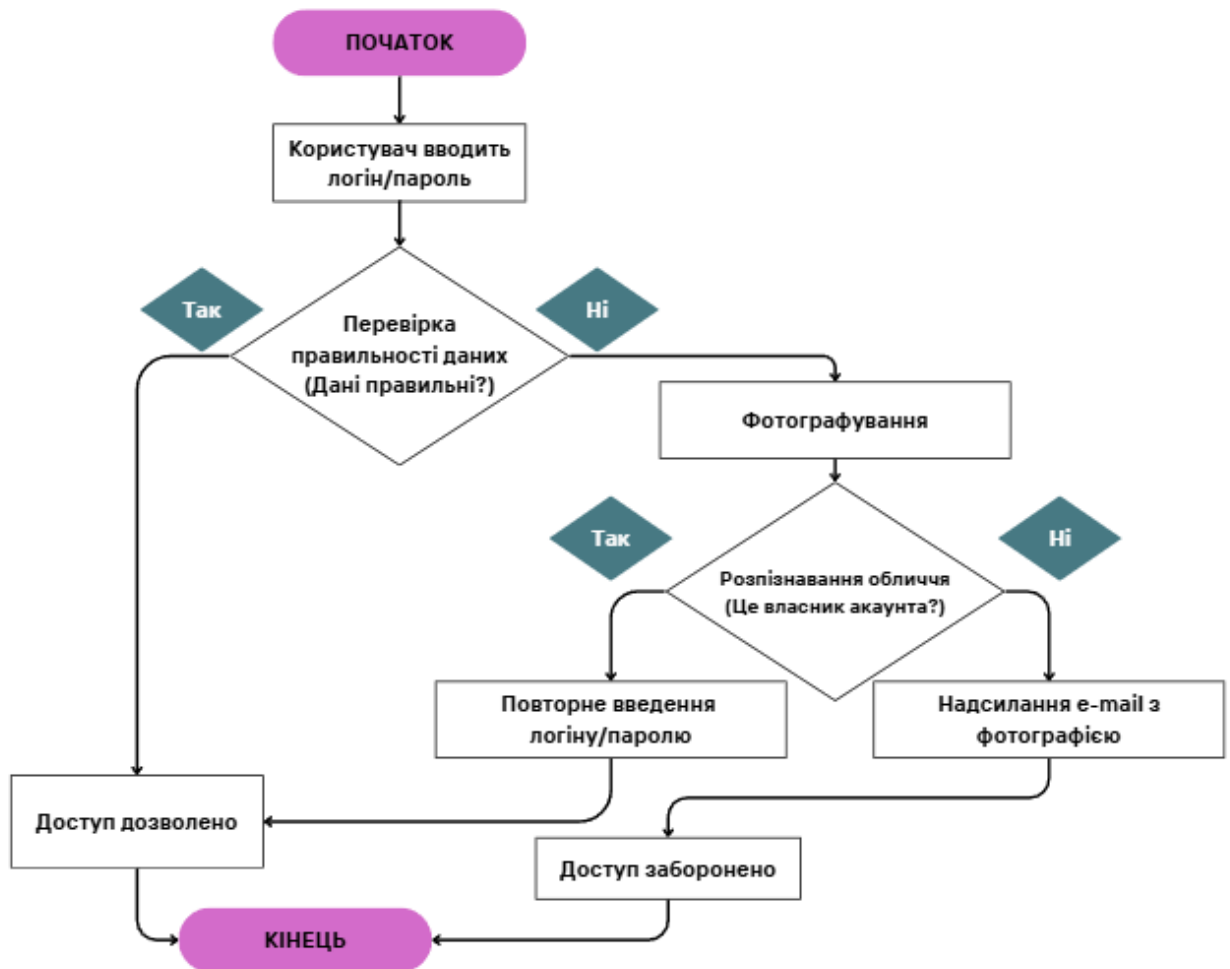


Рисунок 3.1 - Блок-схема запропонованого методу.

3.2.2. Практична реалізація прототипу

Розробимо прототип системи, яка виявляє спроби несанкціонованого доступу, ідентифікує зломисника за допомогою веб-камери, та автоматично сповіщає користувача через електронну пошту із вкладенням фотографії.

Система складається з трьох основних компонентів:

1. Веб-додаток:
 - Розроблено на основі фреймворку Flask.
 - Використовується для отримання даних логіну і пароля від користувача.
2. Модуль роботи з камерою:
 - Реалізовано за допомогою бібліотеки OpenCV.

- Забезпечує активацію веб-камери, створення фотографії та збереження її у локальному сховищі.

3. Модуль надсилання повідомлень:

- Використовує бібліотеку `smtplib` для надсилання електронного листа із вкладенням.

Для реалізації прототипу будемо використовувати наступні технології:

- Python — основна мова програмування.
- Flask — мікрофреймворк для веб-розробки (додаток А).
- OpenCV — бібліотека для роботи з камерою та зображеннями.
- `smtplib` і `email.mime` — модулі для роботи з електронною поштою.
- HTML/CSS — для створення веб-інтерфейсу (додаток Б).
- SMTP-сервер Gmail — для надсилання повідомлень.

3.2.2.1. Реалізація компонентів

Веб-додаток надає інтерфейс для введення логіну та пароля. Він складається з двох частин:

1. Головна сторінка (`index.html`):
 - Містить форму для авторизації.
 - Дані логіну та пароля надсилаються методом POST на сервер.
2. Обробка авторизації:
 - Сервер перевіряє введені дані та у разі помилки активує захисний механізм.

Захисний механізм:

1. Фотографування злоумисника:
 - Функція `capture_photo()` активує веб-камеру.
 - Фото зберігається у локальному каталозі з назвою `intruder.jpg`.
2. Надсилання електронного листа:

- Функція `send_email_with_photo()` формує лист, додає фото до вкладення та надсилає його адміністратору через SMTP-сервер.

3. Видалення фото:

- Після успішного відправлення фото видаляється для запобігання накопиченню файлів.

Якщо логін і пароль вказані правильно:

1. Користувач отримує доступ і бачить повідомлення "Ласкаво просимо!".
2. Жодних додаткових дій (фотографування чи надсилання сповіщень) не виконується.

3.2.2.2. Код основних компонентів

Функція фотографування

- Функція `capture_photo()`:
- Підключається до камери через `cv2.VideoCapture(0)`.
- Робить знімок і зберігає його локально.
- Після завершення камера звільняється методом `cam.release()`.

```
def capture_photo():
    cam = cv2.VideoCapture(0)
    result, image = cam.read()
    if result:
        cv2.imwrite("intruder.jpg", image)
    cam.release()
```

Рисунок 3.2 – Код функції фотографування

Функція надсилання електронного листа

- Функція `send_email_with_photo()`:
1. Встановлює з'єднання зі SMTP-сервером Gmail (smtp.gmail.com, порт 587).
 2. Використовує вказаний e-mail та пароль для авторизації на сервері.
 3. Формує лист:

- Тема: "Спроба несанкціонованого доступу".
- Текст: "Виявлено спробу несанкціонованого доступу. Фото додається."
- Вкладення: файл **intruder.jpg**.

4. Відправляє лист і закриває з'єднання.

```
def send_email_with_photo():
    email_user = 'mag24.email@gmail.com'
    email_password = 'kqggq zbkf juol zfhe'
    email_send = 'mariia.siawork@gmail.com'

    subject = 'Спроба несанкціонованого доступу'

    msg = MIMEMultipart()
    msg['From'] = email_user
    msg['To'] = email_send
    msg['Subject'] = subject

    body = 'Виявлено спробу несанкціонованого доступу. Фото додається.'
    msg.attach(MIMEText(body, 'plain'))

    filename = 'intruder.jpg'
    attachment = open(filename, 'rb')

    part = MIMEBase('application', 'octet-stream')
    part.set_payload((attachment).read())
    encoders.encode_base64(part)
    part.add_header('Content-Disposition', f"attachment; filename= {filename}")
    attachment.close()

    msg.attach(part)
    text = msg.as_string()

    server = smtplib.SMTP('smtp.gmail.com', 587)
    server.starttls()
    server.login(email_user, email_password)

    server.sendmail(email_user, email_send, text)
    server.quit()
```

Рисунок 3.3 – Код функції надсилання e-mail

3.2.3. Тестування прототипу

Оцінимо коректність роботи системи при декількох сценаріях:

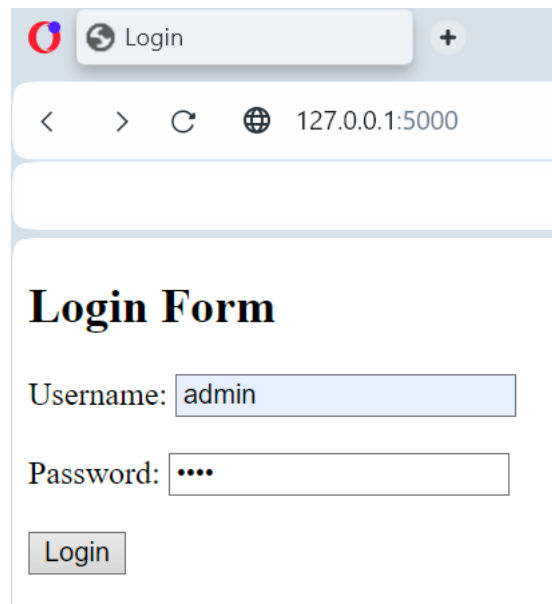
Сценарій 1: Успішна авторизація

Користувач вводить правильний логін і пароль (рис. 3.4).

Очікуваний результат:

- Доступ надано (рис. 3.5).
- Камера не активується.

- Повідомлення про несанкціонований доступ не надсилається.



The screenshot shows a web browser window with the address bar displaying '127.0.0.1:5000'. The page title is 'Login'. The main content area contains a 'Login Form' with the following elements:

- A 'Username:' label followed by a text input field containing the text 'admin'.
- A 'Password:' label followed by a password input field with masked characters (dots).
- A 'Login' button located below the password field.

Рисунок 3.4 – Введення коректних логіну та пароля

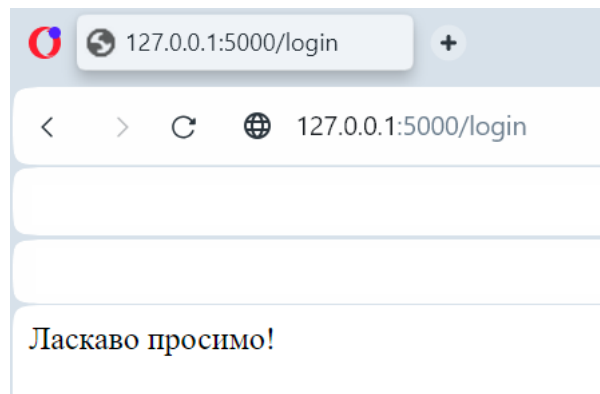


Рисунок 3.5 – Доступ надано

Сценарій 2: Несанкціонований доступ

Користувач вводить некоректний логін або пароль (рис. 3.6).

Очікуваний результат:

- Камера активується і робить знімок.
- Фото зломисника зберігається.
- Сповіщення із фотографією надсилається користувачу (рис. 3.8; 3.9).
- Після відправки фото видаляється.

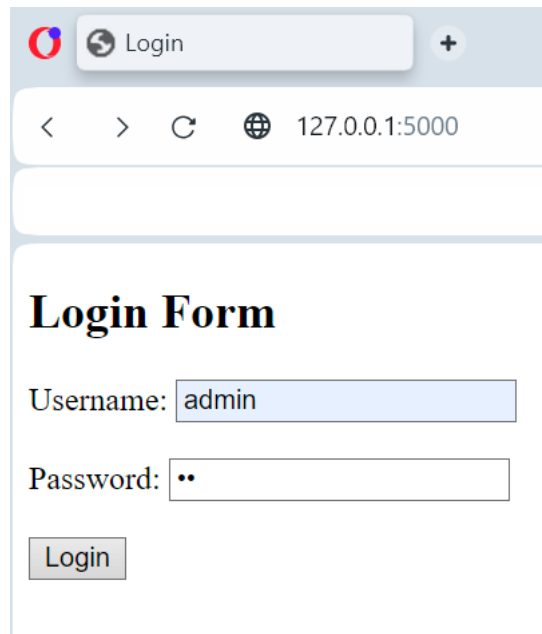


Рисунок 3.6 – Введення некоректних логіну та пароля

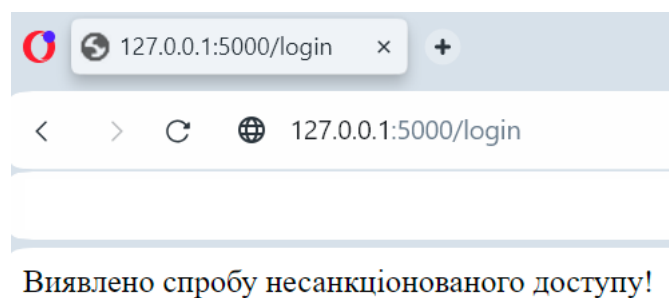


Рисунок 3.7 – Доступ заблоковано

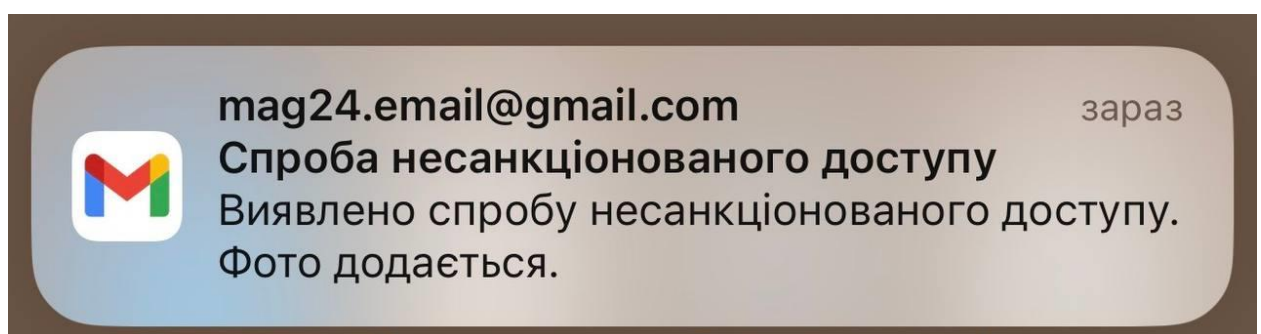


Рисунок 3.8 – Сповіщення про лист із фотографією на пошту

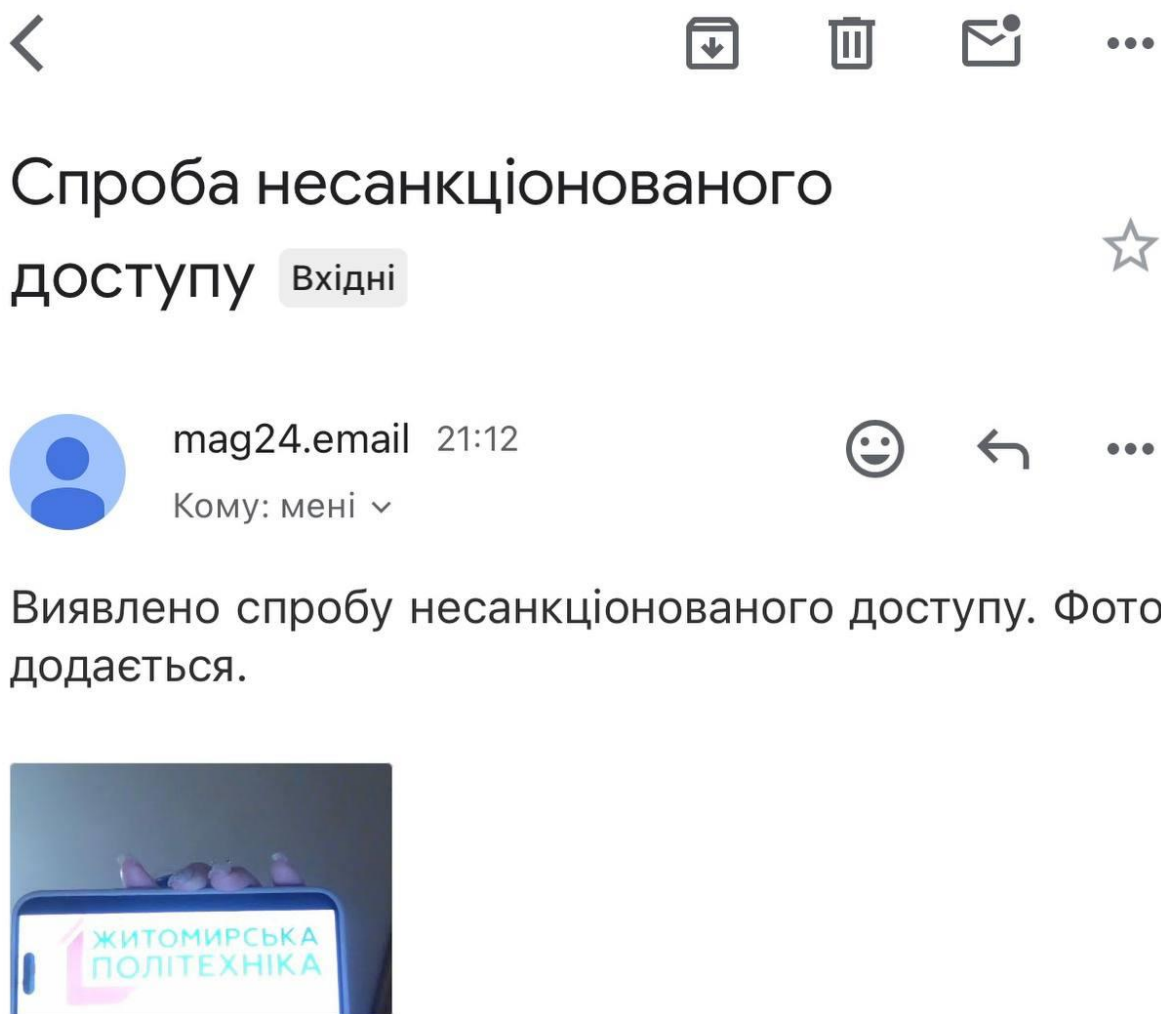


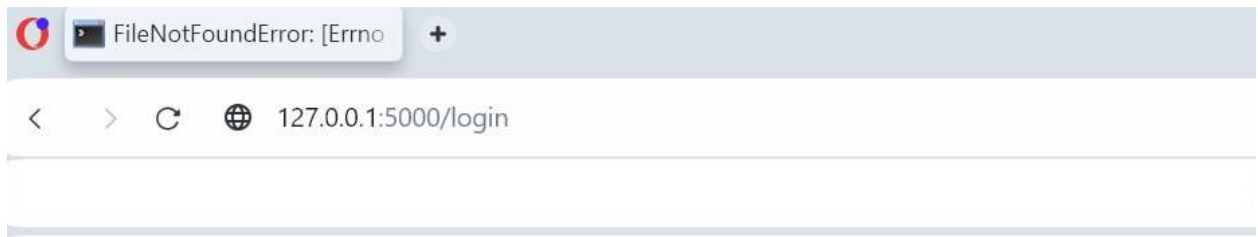
Рисунок 3.9 – Лист на пошті із фотографією зловмисника

Сценарій 3: Відсутність камери

Перевірити систему без підключеної камери.

Очікуваний результат:

- Система повідомляє про помилку роботи камери, але залишається стабільною (рис. 3.10).



FileNotFoundError

FileNotFoundError: [Errno 2] No such file or directory: 'intruder.jpg'

Рисунок 3.10 – Сповіщення про помилку – відсутність камери

Сценарій 4: Помилка SMTP-сервера

Перевірити систему без доступу до інтернету перед спробою відправлення сповіщення.

Очікуваний результат:

- Система повідомляє про помилку надсилання листа (рис. 3.11).
- Фотографія зберігається для подальшого ручного опрацювання.



Рисунок 3.11 – Сповіщення про помилку надсилання листа

3.2.3.1. План проведення тестування

Підготовка: налаштувати веб-додаток. Перевірити доступність веб-камери та підключення до SMTP-сервера.

Проведення тестів: запросити 7 учасників. Успішно авторизуватися 3 особам. Імітувати несанкціонований доступ (некоректний логін/пароль) 4 особам.

Запис результатів: фіксувати час реакції системи, роботу камери (чи зберігається фото), надсилання листів (перевірити вхідні повідомлення власника акаунта) (табл. 3.2).

Перевірка виняткових ситуацій: відключити камеру або інтернет для тестування стабільності.

Таблиця 3.2

Результати тестування

№	Учасник	Сценарій	Фото зроблено	Лист надіслано	Час реакції (с)	Коментар
1	Успішний вхід	Успішна авторизація	Ні	Ні	0.5	Система працює коректно.
2	Зловмисник 1	Несанкціонований доступ	Так	Так	2.0	Фото і лист успішно відправлені.
3	Зловмисник 2	Несанкціонований доступ	Так	Ні	1.8	Проблема з SMTP-сервером.
4	Успішний вхід	Успішна авторизація	Ні	Ні	0.5	Система працює коректно.
5	Зловмисник 3	Відсутність камери	Ні	Ні	0.3	Камера не підключена.
6	Зловмисник 4	Несанкціонований доступ	Так	Так	2.1	Система працює коректно.

Продовження табл. 3.2

№	Учасник	Сценарій	Фото зроблено	Лист надіслано	Час реакції (с)	Коментар
7	Успішний вхід	Успішна авторизація	Ні	Ні	0.5	Система працює коректно.

3.2.3.2. Аналіз результатів

На основі проведеного тестування і отриманої таблиці можна зробити такі висновки:

1. Система коректно розпізнає успішні входи.
2. Камера активується при несанкціонованому доступі, а фотографії створюються без помилок.
3. Листи надсилаються успішно, за винятком випадків відсутності інтернету або проблем із SMTP-сервером.
4. Виняткові ситуації (відсутність камери, проблеми із сервером) не спричиняють краху системи.

3.2.4. Переваги методу фотографування в соціальних мережах

Метод виявлення несанкціонованого доступу з використанням камери та автоматичного сповіщення власника облікового запису має низку переваг у сфері інформаційної безпеки соціальних мереж:

- Система дозволяє ідентифікувати особу, яка намагалася здійснити несанкціонований доступ до облікового запису або конфіденційних даних.
- Користувач отримує оперативне сповіщення про інцидент, що сприяє швидкому реагуванню.
- Активація системи відбувається в момент виявлення аномалії (наприклад, неправильного пароля).

- Фотографія підозрілої особи надсилається в реальному часі, що дозволяє вжити заходів для блокування облікового запису.
- Метод особливо ефективний у середовищах із спільним доступом до пристроїв або робочих місць.
- Авторизований вхід здійснюється без затримок, оскільки система активується лише у разі виявлення некоректного введення даних.
- Фотографії можуть слугувати доказами для подальшого юридичного переслідування кіберзлочинців.
- Система може бути застосована для великої кількості облікових записів і платформ.
- Хмарна інтеграція забезпечує гнучке зберігання та обробку даних.
- Можливість налаштування сповіщень через електронну пошту, SMS або месенджери забезпечує зручність використання.

3.2.5. Недоліки методу фотографування в соціальних мережах

Попри численні переваги, метод фотографування зловмисника має низку недоліків, які варто враховувати при його впровадженні в соціальних мережах. Нижче наведено основні:

- Неможливість використання на пристроях без камер (наприклад, деякі настільні ПК).
- Нестабільне інтернет-з'єднання може спричинити затримки або невідправлення сповіщень.
- Технічні несправності серверів можуть призвести до втрати критичних даних.
- Навіть при видаленні фото після надсилання залишається ризик його перехоплення.
- Електронна пошта може бути недостатньо захищеною, якщо не використовується шифрування.

- Камери низької якості можуть створювати нечіткі зображення, непридатні для ідентифікації.
- Фізичне закриття або пошкодження камери зловмисником робить метод неефективним.
- Робота камери та обробка фотографій підвищує навантаження на ресурси пристрою.
- Зберігання даних вимагає додаткових обсягів пам'яті.
- У деяких країнах метод може порушувати законодавство про захист персональних даних.

3.2.6. Пропозиції щодо подальшого розвитку методу фотографування для соціальних мереж

Для підвищення ефективності, надійності та масштабованості запропонованого методу захисту інформації в соціальних мережах пропонується низка вдосконалень, спрямованих на поліпшення його архітектури, функціональності та відповідності сучасним стандартам безпеки:

1. Покращення архітектури системи

- Інтеграція бази даних для реєстрації всіх спроб авторизації.
- Додавання метаданих (наприклад, часу, IP-адреси, геолокації) до фотографій для підвищення їх інформативності.
- Оптимізація розміру зображень за допомогою бібліотек стиснення для економії місця без втрати якості.
- Використання алгоритмів для шифрування фотографій перед їх передачею, що забезпечить захист від перехоплення даних.
- Хешування паролів користувачів із використанням стійких алгоритмів для унеможливлення їхнього відновлення у разі компрометації.

2. Підвищення стійкості системи

- Розробка механізмів обробки критичних помилок, які можуть виникати під час виконання методу, зокрема: відсутність доступу до камери, проблеми з інтернет-з'єднанням, збій у відправленні електронних листів через SMTP.
- Впровадження механізмів, які активують захисний механізм лише після кількох невдалих спроб авторизації (наприклад, блокування після 3 помилкових введень пароля).

3. Розширення функціональних можливостей

- Використання хмарних сервісів для зберігання, обробки фотографій та надсилання сповіщень, що сприятиме збільшенню масштабованості та надійності системи.
- Розширення каналів сповіщення через месенджери (наприклад, Telegram, WhatsApp) або SMS для забезпечення оперативного інформування власника акаунта.

4. Рекомендації для реального використання

- Впровадження системи як додаткового рівня безпеки поряд із традиційними методами, такими як двофакторна автентифікація.
- Використання алгоритмів аналізу поведінки користувачів для виявлення аномальних дій.
- Забезпечення відповідності системи законам про захист персональних даних, шляхом дотримання вимог щодо збереження та передачі даних.
- Реалізація механізмів отримання інформованої згоди користувача на використання його даних (зокрема фотографій).

Реалізація запропонованих удосконалень дозволить підвищити функціональність, безпеку та зручність використання системи. Інтеграція сучасних технологій, таких як хмарні сервіси, механізми шифрування та розширені можливості сповіщення, забезпечить масштабованість і відповідність актуальним потребам користувачів та вимогам законодавства.

Висновки до третього розділу

Отже, використання камери для автоматичного фотографування зломисників під час спроби злому є новим підходом у захисті соціальних мереж. Його основна ідея полягає в поєднанні фізичної ідентифікації зломисника із автоматичним сповіщенням користувача, що дозволяє швидко реагувати на загрози та мінімізувати ризики злому. Особливістю цього методу є можливість надання доказів (фотографій), які можуть бути використані як юридичні свідчення. Нажаль, досі лишається можливим перехоплення таких даних, але захист фотографій та журналів дій за допомогою алгоритмів шифрування може мінімізувати цей ризик. Дана система дозволяє ідентифікувати зломисника прямо в момент атаки, а також забезпечує оперативне реагування через автоматичні сповіщення. Метод не вимагає складних технологій і може бути інтегрований у вже існуючі платформи. Натомість в цьому випадку можливі етичні та юридичні питання щодо збереження та обробки фотографій, метод залежить від апаратного забезпечення, а також на даному етапі можливі помилкові спрацювання. Це можна виправити, впровадивши додаткові рівні перевірки (наприклад, обмеження кількості спроб входу). Метод ефективний для локальних або невеликих систем, але має обмеження для використання на великих платформах через значні вимоги до обробки та зберігання даних. У зв'язку з цим рекомендується використовувати хмарні сервіси. Для підвищення ефективності рекомендовано інтегрувати метод із традиційними підходами, такими як: двофакторна автентифікація (2FA) для підвищення стійкості до атак, аналіз поведінкових факторів, включаючи IP-адреси та геолокацію, розпізнавання облич для точнішої ідентифікації користувачів.

ВИСНОВКИ

1. Розглянуто загальні питання організації методів і технологій захисту інформації. Дано класифікацію методів захисту інформації, досліджено основні напрямки їх використання. Класифікація методів захисту інформації включає в себе організаційно - правові, інженерно-технічні методи, які, своєю чергою, складаються з фізичних, апаратних, програмних і криптографічних методів. Окремо розглянуто криптографічні та біометричні методи захисту інформації, методи автентифікації та контроль доступу до даних.

Показано, що двофакторна автентифікація є важливим заходом безпеки, який слід застосовувати в соціальних мережах. Оцінено переваги двофакторної автентифікації та доведено, що вони переважають недоліки її застосування.

Розглянуто концепцію соціальних мереж із підтримкою блокчейну, які завдяки децентралізації, автономності та використанню попередньо визначених протоколів пропонують нові перспективи для організаційної структури цифрових платформ.

Підкреслено, що інтеграція штучного інтелекту відкриває додаткові можливості у сфері кібербезпеки. Завдяки здатності оперативно виявляти загрози, автоматизувати процеси захисту та створювати адаптивні механізми протидії зловмисникам, штучний інтелект дозволяє організаціям зміцнити свої системи захисту, мінімізуючи ризики кіберзлочинів.

2. Проаналізовано політику конфіденційності кількох популярних соціальних мереж, звертаючи увагу на їхні принципи роботи з даними, доступ користувачів до інформації про себе та можливі ризики. Це допомогло зрозуміти, як свідоміше підходити до використання цих платформ. Також розглянуто такі аспекти: як компанія використовує дані користувачів, які вона збирає, як користувачі можуть контролювати свої дані, який відомий досвід компанії щодо захисту даних користувачів та в загальному політику конфіденційності.

Аналіз соціальних мереж Facebook, WhatsApp, Telegram, Viber, WeChat та Signal показав, що кожна з платформ має свої сильні та слабкі сторони у сфері захисту приватності. Signal виділяється як платформа з найбільш зосередженим підходом до конфіденційності, тоді як WeChat більше орієнтований на інтеграцію сервісів, навіть ціною зниження рівня безпеки. Інші платформи прагнуть знайти баланс між потребами користувачів і комерційними цілями.

3. Обґрунтовано метод фотографування для здійснення захисту інформації в соціальних мережах, а саме: використання камери для автоматичного фотографування зломисників під час спроби несанкціонованого доступу. Основна ідея такого методу полягає в поєднанні фізичної ідентифікації зломисника із автоматичним сповіщенням користувача, що дозволяє швидко реагувати на загрози та мінімізувати ризики злому. Його особливістю є можливість надання доказів (фотографій), які можуть бути використані як юридичні свідчення. Дана система дозволяє ідентифікувати зломисника прямо в момент атаки, а також забезпечує оперативне реагування через автоматичні сповіщення. Метод ефективний для локальних або невеликих систем, але має перспективи використання на великих платформах. Експериментально доведено, що такий метод відіграє свою суттєву роль в забезпеченні кібербезпеки в соціальних мережах та його можна інтегрувати з традиційними методами для досягнення максимального рівня захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ексклюзивне інтерв'ю із заступником голови Держспецзв'язку України з питань цифрового розвитку, цифрових трансформацій і цифровізації Віктором Жорою агентству "Інтерфакс-Україна". URL: <https://interfax.com.ua/news/interview/911979.html>. (дата звернення: 08.11.2024).
2. Сябрук М. О., Бродський Ю. Б. Роль соціальних мереж в забезпеченні кібербезпеки // Тези доповідей VI Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 29-30 листопада 2023 року – Житомир: Житомирська політехніка, 2023.
3. Сябрук М. О. Система розпізнавання користувачів в соціальних мережах // Тези доповідей XIV Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології – 2024», м. Житомир, 28-29 березня 2024 року – Житомир: Житомирська політехніка, 2024.
4. Сябрук М. О. Моніторинг нормативної бази захисту інформації в соціальних мережах // Тези доповідей VII Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 02-03 грудня 2024 року – Житомир: Житомирська політехніка, 2024.
5. Методи та засоби захисту інформації. URL: <https://journals.nupp.edu.ua/sunz/article/view/3265/2687>. (дата звернення: 10.11.2024).
6. Методологія і технології захисту інформації: навчальний посібник / А. Н. Аль-Амморі, Н. М. Наумова, П. В. Дяченко, Р. М. Іщенко, М. М. Дехтяр, А. Є. Клочан. Київ : НТУ, 2020. 147 с.
7. Методи і системи захисту інформації. URL: <http://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf>. (дата звернення: 14.11.2024).
8. Методи криптографічного захисту. [URL: <https://www.uzhnu.edu.ua/uk/infocentre/get/4186>. (дата звернення: 18.11.2024).

9. Біометричний захист інформації. URL: <https://www.uzhnu.edu.ua/uk/infocentre/get/4186>. (дата звернення: 18.11.2024).
- 10.Що таке автентифікація? URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-authentication>. (дата звернення: 20.11.2024).
- 11.Моделі та методи контролю доступу. URL: <https://worldvision.com.ua/modeli-i-metody-kontrolya-dostupa-cho-vam-podkhodit/>.(дата звернення: 22.11.2024).
12. Blockchain solutions for trustworthy decentralization in social networks. URL: <https://www.sciencedirect.com/science/article/abs/pii/S1389128624001683>. (дата звернення: 23.11.2024).
13. Блокчейн: що це, навіщо він нам потрібний і в чому його небезпека? URL: <https://compX.ua/blokcheyn-shcho-tse-navishcho-vin-nam-potribniy-i-v-chomu-yogo-nebezpeka/>.(дата звернення: 28.11.2024).
14. Artificial intelligence for cybersecurity: Literature review and future research directions. URL: <https://www.sciencedirect.com/science/article/pii/S1566253523001136>. (дата звернення: 02.12.2024).
- 15.Mozilla research Privacy Not Included. Facebook. URL: <https://foundation.mozilla.org/en/privacynotincluded/facebook-messenger-and-facebook-messenger-kids/>.(дата звернення: 08.12.2024).
- 16.Mozilla research Privacy Not Included. Whatsapp. URL: <https://foundation.mozilla.org/en/privacynotincluded/whatsapp/>. (дата звернення: 12.12.2024).
- 17.Mozilla research Privacy Not Included. Telegram. URL: <https://foundation.mozilla.org/en/privacynotincluded/telegram/>. (дата звернення: 14.12.2024).
- 18.Mozilla research Privacy Not Included. Viber. URL: <https://foundation.mozilla.org/en/privacynotincluded/viber/>. (дата звернення: 15.12.2024).

19. Mozilla research Privacy Not Included. WeChat. URL: <https://foundation.mozilla.org/en/privacynotincluded/wechat/>. (дата звернення: 16.12.2024).

20. Mozilla research Privacy Not Included. Signal. URL: <https://foundation.mozilla.org/en/privacynotincluded/signal/>. (дата звернення: 17.12.2024).

21. The Development of a Secure Online System to Protect Social Networking Platforms from Security Attacks. URL: <https://www.mdpi.com/2076-3417/13/21/11731>. (дата звернення: 18.12.2024).

ДОДАТКИ

Додаток А
Бекенд

```

from flask import Flask, request, render_template
import cv2
import smtplib
from email.mime.text import MIMEText
from email.mime.multipart import MIMEMultipart
from email.mime.base import MIMEBase
from email import encoders
import os

app = Flask(__name__)

@app.route('/')
def home():
    return render_template('index.html')

@app.route('/login', methods=['POST'])
def login():
    username = request.form['username']
    password = request.form['password']

    # Простий приклад перевірки
    if username == "admin" and password == "1234":
        return "Ласкаво просимо!"
    else:
        capture_photo()
        send_email_with_photo()
        return "Виявлено спробу несанкціонованого доступу!"

def capture_photo():
    cam = cv2.VideoCapture(0)
    result, image = cam.read()
    if result:
        cv2.imwrite("intruder.jpg", image)
    cam.release()

def send_email_with_photo():
    email_user = 'mag24.email@gmail.com'
```

```

email_password = 'kqgq zbkf juol zfhe'
email_send = 'mariia.siawork@gmail.com'

subject = 'Спроба несанкціонованого доступу'

msg = MIMEMultipart()
msg['From'] = email_user
msg['To'] = email_send
msg['Subject'] = subject

body = 'Виявлено спробу несанкціонованого доступу. Фото додається.'
msg.attach(MIMEText(body, 'plain'))

filename = 'intruder.jpg'
attachment = open(filename, 'rb')

part = MIMEBase('application', 'octet-stream')
part.set_payload((attachment).read())
encoders.encode_base64(part)
part.add_header('Content-Disposition', f'attachment; filename= {filename}')
attachment.close()

msg.attach(part)
text = msg.as_string()

server = smtplib.SMTP('smtp.gmail.com', 587)
server.starttls()
server.login(email_user, email_password)

server.sendmail(email_user, email_send, text)
server.quit()

# Видалити фото після відправки
os.remove(filename)

if __name__ == '__main__':
    app.run(debug=True)

```

```
<!DOCTYPE html>

<html>

<head>

  <title>Login</title>

</head>

<body>

  <h2>Login Form</h2>

  <form action="/login" method="POST">

    <label for="username">Username:</label>

    <input type="text" id="username" name="username" required><br><br>

    <label for="password">Password:</label>

    <input type="password" id="password" name="password" required><br><br>

    <button type="submit">Login</button>

  </form>

</body>

</html>
```