Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Галузь знань 12 – Інформаційні технології

Спеціальність 126 – Інформаційні системи та технології

на тему: «Метод та засоби інформаційної технології забезпечення захисту персональних даних при обробці та передаванні в IT-інфраструктурі організації»

КвРІСТ. 220172.22.01.01 ПЗ

Виконав: студент 2 курсу, група ІСТм–22–1 _____ Барнич М. Б.
Підпис Ініціали, прізвище

Керівник: к.т.н. доцент _____ Гнатчук Є.Г.
Науковий ступінь, вчене звання Підпис Ініціали, прізвище

До захисту допускаю:

Зав. кафедри КІІС, д.т.н., проф.
Т.О. Говорущенко
__ _____ 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Освітній рівень магістр

Галузь знань 12 Інформаційні технології

Спеціальність 126 Інформаційні системи та технології

Освітня програма Освітньо–професійна програма «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О. Говорущенко

" 18" 12 2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Барничу Мар'яну Богдановичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод та засоби інформаційної технології забезпечення захисту персональних даних при обробці та передаванні в іт-інфраструктурі організації.
Керівник проекту (роботи) Гнатчук Є. Г.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 15.08.2023 р. №30

2. Строк подання студентом проекту (роботи) на кафедру 10.12.2023 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз відомих систем і методів захисту даних при обробці та передаванні в ІТ-інфраструктурі організації

Обгрунтування і вибір теоретичних та експериментальних методів дослідження

Розроблення та оцінка методу захисту даних в ІТ-іфраструктурі організації

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи магістра

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Лисенко С.М., професор кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання « 03 » 04 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	03.04.2023	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	03.05.2023	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	03.06.2023	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	03.07.2023	виконано
5	Робота над науковою статтею	01.10.2023	виконано
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	01.10.2023	виконано
7	Робота над розділом 4 – проектування та розробка ПЗ для вирішення поставленої задачі, експериментальна частина	01.11.2023	виконано
8	Оформлення пояснювальної записки згідно вимог	15.11.2023	виконано
9	Попередній захист ДРМ	16.11.2023	виконано
10	Захист ДРМ на засіданні ЕК	До 20.12.2023	

Студент _____ М.Б. Барнич
Підпис Ініціали, прізвище

Керівник роботи _____ Є.Г. Гнатчук
Підпис Ініціали, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Метод та засоби інформаційної технології забезпечення захисту персональних даних при обробці та передаванні в IT-інфраструктурі організації.

Автор роботи: Барнич Мар’ян Богданович.

Керівник роботи: доцент Гнатчук Є.Г.

Пояснювальна записка: 75 с., 26 рис., 5 табл., 2 дод., 67 джерел.

Перелік ключових слів: захист даних, автентифікація, біометрична ідентифікація, методи захисту, Google Authenticator, ефективність, архітектура.

Об'єктом магістерської роботи є інформаційно-технічна інфраструктура організації, яка використовується для обробки та зберігання персональних даних.

Предметом дослідження є підвищення рівня захисту персональних даних в інформаційно-технічній інфраструктурі організації при їх передаванні та обробці, зокрема шляхом дослідження, розробки та застосування методів двофакторної аутентифікації з використанням Google Authenticator.

Методи дослідження. У роботі було проаналізовано наступні теорії та засоби:

- стратегія безпеки Zero Trust;
- багатофакторна аутентифікація (MFA);
- загальний регламент ЄС про захист персональних даних (GDPR);
- Data Protection as a Service (DPaaS);
- Virtual private network (VPN);
- Microsoft Azure Active Directory.

Наукова новизна роботи:

- дослідження можливостей інтеграції двофакторної аутентифікації з іншими захисними механізмами. Найдено швидкий та ефективний метод інтеграції 2FA в проект чи систему IT-інфраструктури організації.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

API - прикладний програмний інтерфейс (англ. Application Programming Interface)

GDPR - загальний регламент ЄС про захист персональних даних

ID - ідентифікатор (англ. Identifier)

HOTP - одноразовий пароль з використанням HMAC (англ. HMAC-Based One-Time Password)

MFA - багатофакторна автентифікація (англ. Multi-Factor Authentication)

OTP - одноразовий пароль (англ. One-Time Password)

PIN - персональний ідентифікаційний номер (англ. Personal Identification Number)

SFA - однофакторна автентифікація (англ. Single-Factor Authentication)

TFA (2FA) - двофакторна автентифікація (англ. Two-Factor Authentication)

TOTP - тимчасовий одноразовий пароль (англ. Time-Based One-Time Password)

VPN - віртуальна приватна мережа.

ВСТУП

У сучасному світі, де кількість цифрових даних зростає експоненційно, захист персональних даних стає надзвичайно важливим завданням. Інтернет став неодмінною частиною нашого повсякденного життя, і ми передаємо, обмінюємося, та зберігаємо великі обсяги особистої інформації онлайн. Ця інформація може бути вельми цінною для кіберзлочинців і несанкціонованих осіб, тож захист її стає критичною проблемою.

З огляду на це, стало дедалі більше випадків кібератак, які націлені на різні сфери, включаючи бізнес, уряд та приватних громадян. Кіберзлочинці використовують різні методи та підходи для незаконного доступу до інформації, зламу систем та поширення шкідливих програм.

Інциденти кібербезпеки можуть призвести до серйозних наслідків, включаючи втрату конфіденційності даних, порушення доступності інформації, а також порушення цілісності системи. Більше того, такі інциденти можуть завдати значних фінансових збитків і пошкодити репутацію організацій та осіб.

У цьому контексті виникає нагальна потреба в розробці та впровадженні ефективних методів і засобів захисту персональних даних та інформаційних систем в цілому. Ці методи та засоби повинні включати в себе не лише технічні рішення, але й культурні та організаційні аспекти.

Запобігання та реагування на кібератаки стає складним завданням, і вимагає спільних зусиль усіх учасників інформаційно-телекомунікаційних процесів. У нашому дослідженні ми розглядаємо основні аспекти захисту персональних даних та шляхи їхнього покращення, а також розглядаємо сучасні технології та методи захисту від кібератак.

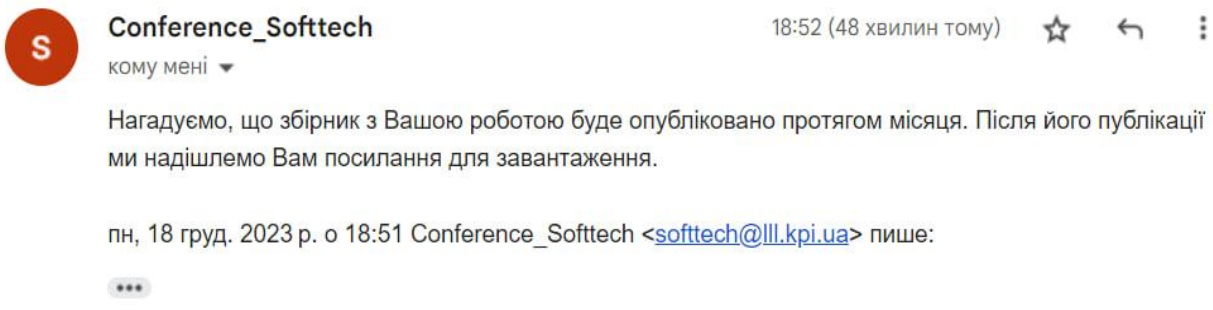
Метою магістерської роботи є розробка конкретних та ефективних методів та засобів інформаційної технології для забезпечення найвищого

рівня захисту персональних даних під час обробки та передавання в інформаційно-технологічній інфраструктурі організації.

Завданням дослідження є провести аналіз різних підходів та методів захисту інформації в інформаційно-технологічному середовищі організації, проаналізувати та вивчити сучасні технології, програмні та апаратні рішення, які можуть бути використані для захисту персональних даних, розробити конкретні рекомендації для вдосконалення системи захисту інформації в організації, провести тестування та валідацію розроблених рекомендацій на практиці для перевірки їхньої ефективності та застосовності.

Структура та об’єм дипломної роботи. Дипломна складається з вступу, чотирьох розділів, висновку та додатків, її повний зміст 93 сторінок, основний зміст викладено на сторінках, 3–х додатках, містить 23 рисунків, 5 таблиць, включає 67 найменувань вітчизняної та зарубіжної літератури.

За темою кваліфікаційної роботи магістра будуть опубліковані тези в конференції «Гнатчук Є.Г., Барнич М.Б. Метод та засоби інформаційної технології забезпечення захисту персональних даних при обробці та передаванні в іт-інфраструктурі організації. *V Міжнародна науково-практична конференція молодих вчених та студентів «Інженерія програмного забезпечення і передові інформаційні технології SoftTech-2023*.[1]



1. АНАЛІЗ ВІДОМИХ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Огляд існуючих підходів

1.1.1 Стратегія безпеки Zero Trust

Нульова довіра (ZT) - це термін для позначення еволюціонуючого набору парадигм кібербезпеки, які переносять захист зі статичних, мережевих периметрів на користувачів, активи та ресурси. Архітектура нульової довіри (ZTA) використовує принципи нульової довіри для планування промислової та корпоративної інфраструктури і робочих процесів. Нульова довіра передбачає відсутність неявної довіри до активів або облікових записів користувачів, заснованої виключно на їх фізичному або мережевому розташуванні (наприклад, локальні мережі в порівнянні з Інтернетом) або на власності активів (корпоративна або особиста власність) [56].

Автентифікація та авторизація (як суб'єкта, так і пристрою) є окремими функціями, що виконуються перед встановленням сеансу доступу до корпоративного ресурсу.

Нульова довіра - це парадигма кібербезпеки, яка фокусується на захисті ресурсів і передумові, що довіра ніколи не надається неявно, а повинна постійно оцінюватися.

Архітектура нульової довіри - це наскрізний підхід до безпеки корпоративних ресурсів і даних, який охоплює ідентифікацію (фізичних і юридичних осіб), облікові дані, управління доступом, операції, кінцеві точки, хостингові середовища і сполучну інфраструктуру [31].

Початковий фокус має бути на обмеженні ресурсів лише тими, кому потрібен доступ, і наданні лише мінімальних привілеїв (наприклад, читати, писати, видаляти), необхідних для виконання місії.

Традиційно установи (і корпоративні мережі загалом) зосереджуються на захисті периметра, а аутентифіковані суб'єкти отримують санкціонований доступ до широкої колекції ресурсів, щойно вони потрапляють до внутрішньої мережі.

У багатьох визначеннях і обговореннях ZT підкреслюється концепція усунення широкомасштабних засобів захисту периметра (наприклад, корпоративних брандмауерів) як фактору, що впливає на нього. Однак більшість з цих визначень продовжують так чи інакше визначати себе по відношенню до периметрів (наприклад, мікросегментація або мікроперіметри) як частину функціональних можливостей ZTA. Нижче наводиться спроба визначити ZT і ZTA з точки зору основних принципів, які повинні бути залучені, а не виключені. Ці принципи є ідеальною метою, хоча слід визнати, що не всі принципи можуть бути повністю реалізовані в чистому вигляді для даної стратегії.

Архітектура нульової довіри розробляється і розгортається з дотриманням наступних основних принципів нульової довіри:

1. Всі джерела даних та обчислювальні сервіси вважаються ресурсами. Мережа може складатися з декількох класів пристроїв. У мережі також можуть бути малогабаритні пристрої, які надсилають дані до агрегаторів/сховищ, програмне забезпечення як послуга (SaaS), системи, що надсилають інструкції виконавчим механізмам, та інші функції. Крім того, підприємство може вирішити класифікувати особисті пристрої як ресурси, якщо вони можуть отримати доступ до ресурсів, що належать підприємству.

2. Уся комунікація захищена незалежно від місця розташування мережі. Місцезнаходження мережі саме по собі не означає довіру. Запити

на доступ до ресурсів, розташованих у мережевій інфраструктурі підприємства (наприклад, всередині периметра застарілої мережі), повинні відповідати тим самим вимогам безпеки, що й запити на доступ і зв'язок з будь-якої іншої мережі, що не належить підприємству. Іншими словами, довіра не повинна надаватися автоматично на основі того, що пристрій знаходиться в мережевій інфраструктурі підприємства. Уся комунікація повинна здійснюватися у найбільш безпечний спосіб, захищати конфіденційність і цілісність, а також забезпечувати автентифікацію джерела.

3. Доступ до окремих ресурсів підприємства надається на основі сеансу. Перед наданням доступу оцінюється довіра до заявника. Доступ також повинен надаватися з найменшими привілеями, необхідними для виконання завдання. Це може означати лише «нещодавно» для цієї конкретної транзакції і не відбуватися безпосередньо перед ініціюванням сеансу або виконанням транзакції з ресурсом. Однак автентифікація та авторизація на одному ресурсі не надають автоматично доступ до іншого ресурсу.

4. Доступ до ресурсів визначається динамічною політикою - включаючи спостережуваний стан ідентичності клієнта, програми/сервісу та ресурсу, що запитує, - і може включати інші поведінкові та середовищні атрибути. Організація захищає ресурси, визначаючи, які ресурси вона має, хто є її членами (або можливість автентифікації користувачів з об'єднаної спільноти), і який доступ до ресурсів потрібен цим членам. Для нульової довіри ідентифікація клієнта може включати обліковий запис користувача (або ідентифікатор служби) і будь-які пов'язані з ним атрибути, призначені підприємством для цього облікового запису Політики доступу до ресурсів і дозволів на дії можуть відрізнятися залежно від чутливості ресурсу/даних.

5. Підприємство контролює та вимірює цілісність та безпеку всіх власних та пов'язаних з ними активів. Жодному активу не можна довіряти по суті. Підприємство оцінює стан безпеки активу під час оцінки запиту на отримання ресурсів. Підприємство, що впроваджує ZTA, повинно створити систему безперервної діагностики та пом'якшення наслідків (CDM) або аналогічну систему для моніторингу стану пристроїв і додатків, а також застосовувати патчі/виправлення за необхідності.

6. Вся автентифікація та авторизація ресурсів є динамічною і суворо виконується до того, як доступ буде дозволено. Це постійний цикл отримання доступу, сканування та оцінки загроз, адаптації та постійної переоцінки довіри до постійної комунікації. Очікується, що підприємство, яке впроваджує ZTA, повинно мати системи управління ідентифікацією, обліковими даними і доступом (ICAM) та управління активами. Це включає використання багатофакторної автентифікації (MFA) для доступу до деяких або всіх ресурсів підприємства.

7. Підприємство збирає якомога більше інформації про поточний стан активів, мережевої інфраструктури та комунікацій і використовує її для покращення стану безпеки. Підприємство повинно збирати дані про стан безпеки активів, мережевий трафік і запити на доступ, обробляти ці дані та використовувати отриману інформацію для покращення створення та впровадження політик [3].

Ці принципи застосовуються до роботи, що виконується всередині організації або у співпраці з однією чи кількома організаціями-партнерами, а не до анонімних публічних або орієнтованих на споживача бізнес-процесів. Організація не може нав'язувати внутрішні політики зовнішнім суб'єктам (наприклад, клієнтам або звичайним користувачам Інтернету), але може впроваджувати деякі політики, засновані на ZT, для користувачів, які не є співробітниками організації, але мають особливі

відносини з нею (наприклад, зареєстровані клієнти, утриманці співробітників і т.д.) [17].

1.1.2 Багатофакторна аутентифікація (MFA)

Багатофакторна автентифікація - це одна з найпопулярніших послуг, яку сьогодні використовують різні люди, особливо багато організацій. Люди використовують цю послугу для авторизації своїх збережених даних і доступу до них без будь-яких порушень безпеки. Оскільки використання різних систем зберігання для різних типів даних зростає, нам потрібно зосередитися на безпеці.

Будь-який вид загрози безпеці може бути великою загрозою для будь-якої компанії. Перевіряючи останні опитування з різних питань безпеки, ми виявили, що 94% організацій помірно або дуже стурбовані безпекою даних.

Згідно з дослідженням Intel, інсайдерські загрози є причиною неймовірних 43% всіх порушень. Половина з них є навмисними, а половина - випадковими.

На думку компанії Different Web Services, одного з найбільших у світі постачальників послуг безпеки, багатофакторна автентифікація є чудовим методом захисту доступу до системи, оскільки вона додає додатковий рівень безпеки до традиційної автентифікації за допомогою імені користувача та пароля.

Вони реалізують технології, які дозволяють користувачам використовувати фактори знання (ім'я користувача та пароль) на першому рівні автентифікації, а потім доповнюють їх факторами володіння, наприклад, вимагаючи від користувача створити код автентифікації на пристрої з підтримкою MFA [24].

Зважаючи на галас у галузі, це позитивний крок для постачальників послуг безпеки, щоб охопити MFA, але очевидно, що вони зосереджують основну увагу на міркуваннях володіння. Єдина проблема полягає в тому, що якщо користувач втратить свій пристрій з підтримкою MFA, його облікові дані опиняться під загрозою.

MFA - це тип автентифікації, який вимагає надання двох або більше факторів перевірки для отримання доступу до ресурсу.

Основна перевага MFA полягає в тому, що вона посилює безпеку будь-якої компанії, змушуючи користувачів ідентифікувати себе за допомогою чогось більшого, ніж просто логін і пароль. Хоча імена користувачів і паролі є важливими, вони піддаються грубому злому і можуть бути легко викрадені третіми сторонами.

Примусове використання елементів MFA, таких як відбитки пальців або фізичний апаратний ключ, підвищує впевненість вашої організації у своїй здатності захиститися від шахраїв. Одноразові паролі (OTP) є однією з найпоширеніших проблем MFA, з якими стикаються користувачі.

OTP - це чотири-восьмизначні коди, які надсилаються клієнтам електронною поштою, SMS або через різноманітні мобільні додатки. На регулярній основі або при надходженні запиту на аутентифікацію OTP генерує новий код. Більшість методів автентифікації MFA використовують один з трьох типів додаткової інформації:

1. Особиста інформація, наприклад, пароль або PIN-код [37].
2. Володіння предметом, таким як планшет або смартфон.
3. Вроджені дані, такі як розпізнавання відбитків пальців або розпізнавання голосу.

MFA є необхідним компонентом успішної політики управління ідентифікацією та доступом (IAM). У цій моделі користувачі можуть обирати між двофакторною та багатофакторною автентифікацією. Якщо високий рівень безпеки не потрібен, вони завжди можуть використовувати

двофакторну автентифікацію, яка допоможе їм використовувати менше місця для зберігання даних [42].

Схеми двофакторної автентифікації (2FA) спрямовані на посилення безпеки автентифікації на основі пароля для входу в систему за рахунок використання токенів вторинної автентифікації. У цьому контексті мобільні схеми 2FA не потребують додаткового обладнання (наприклад, смарт-картки) для зберігання та обробки токенів вторинної автентифікації, а отже, вважаються розумним компромісом між безпекою, зручністю використання та вартістю [27].

1.1.3 Біометрична ідентифікація

Біометрична ідентифікація – це спосіб ідентифікації особистості за окремими специфічними біометричними ознаками (ідентифікаторами), які властиві конкретній людині.

За принципом дії біометричні методи ідентифікації поділяються на статичні (за ознаками, даними людині з народження), динамічні (за ознаками, що набуті в процесі існування) та комбіновані (поєднання двох перших) [1].

Загальний опис BIS необхідний для кращого розуміння технологій біометричної ідентифікації [49]. Біопсихологічна теорія особистості (BIS) - це модель загальних біологічних процесів, що мають відношення до людської психології, поведінки та особистості.

Модель, запропонована психологом-дослідником Джеффрі Аланом Греєм у 1970 році, добре підтверджена подальшими дослідженнями і має загальне визнання серед професіоналів [35].

Розглянемо два біометричні методи ідентифікації.

Ідентифікація райдужної оболонки ока. Райдужна оболонка ока людини є надзвичайно цінним джерелом біометричної інформації,

оскільки являє собою дуже складну структуру, унікальну для кожної людини. Візуальний вигляд райдужної оболонки є результатом її шаруватої будови, загальна структура якої є генетично детермінованою. Однак конкретні деталі критично залежать від обставин, які є початковими умовами розвитку ембріонального попередника райдужної оболонки ока. Таким чином, дві різні райдужки не можуть бути однаковими, навіть у випадку генетичної спорідненості [40].

Ідентифікація за відбитками пальців. Ідентифікація за відбитками пальців є одним з найбільш популярних і надійних методів біометричної ідентифікації особистості. Відбитки пальців рук - це відбитки, утворені внаслідок тертя гребенів шкіри та великих пальців. Вони здавна використовуються для ідентифікації через свою незмінність та індивідуальність. Незмінність означає постійний і незмінний характер візерунка на кожному пальці. Індивідуальність - це унікальність деталей хребта у різних людей; ймовірність того, що два відбитки пальців будуть однаковими, становить приблизно 1 до 1,9x1015. Однак ручна перевірка відбитків пальців настільки виснажлива, трудомістка і дорога, що не здатна задовольнити сучасні вимоги до продуктивності. Автоматична система ідентифікації за відбитками пальців широко застосовується у багатьох сферах, таких як охорона будівель чи територій та банкомати [15].

1.1.4 GDPR

Загальний регламент ЄС про захист персональних даних (GDPR) був попередньо узгоджений у грудні 2015 року. Окільки це регламент, а не директива, його дотримання є обов'язковим і не потребує ратифікації кожною країною-членом ЄС у своєму законодавстві [58]. Загальний

регламент про захист даних (GDPR) суттєво посилив вимоги до систем обробки даних, вимагаючи проведення масштабних аудитів [12].

Очікується, що GDPR матиме значний вплив на технологічні платформи та архітектури даних, які наразі збирають, зберігають та управляють персональними даними [36].

Оскільки GDPR висуває високі вимоги до контролерів і обробників даних щодо обробки персональних даних, включаючи захист даних за замовчуванням, а також реєстрацію всіх дій з обробки, організаціям доведеться провести ретельну внутрішню оцінку своїх технологічних платформ і архітектури даних, включаючи різні інформаційні системи, веб-сайти, бази даних, сховища даних і платформи обробки даних, щоб краще зрозуміти, які персональні дані були зібрані і де існують персональні дані.

Після внутрішньої оцінки організаціям, ймовірно, доведеться внести зміни до своїх технологічних платформ та архітектури даних, щоб відповідати вимогам GDPR.

У деяких випадках, щоб зменшити ризик невідповідності GDPR, знадобиться реінжиніринг існуючих систем або платформ [16].

1.1.5 Data Protection as a Service (DPaaS)

DPaaS – це хмарна послуга, яка забезпечує комплексний захист данних, включаючи резервне копіювання, відновлення та запобігання втрати данних. Вона використовує передові технології та стратегії, щоб забезпечити безпеку, доступність та можливість відновлення ваших данних, навіть у разі атаки розшифровки данних [2].

Хмарні обчислення - це використання обчислювальних ресурсів (апаратного та програмного забезпечення), які надаються як послуга через мережу (зазвичай Інтернет).

Назва походить від використання символу у формі хмари як абстракції для складної інфраструктури, яку вона містить, на системних схемах. Хмарні обчислення довіряють віддаленим сервісам дані, програмне забезпечення та обчислення користувача.

У бізнес-моделі, що використовує програмне забезпечення як послугу, користувачам надається доступ до прикладного програмного забезпечення та баз даних.

Хмарні провайдери керують інфраструктурою та платформами, на яких працюють програми. SaaS іноді називають «програмним забезпеченням на вимогу» і, як правило, тарифікується на основі оплати за використання.

Прихильники SaaS стверджують, що SaaS дозволяє бізнесу знизити операційні витрати на IT, передаючи хмарному провайдеру обслуговування та підтримку апаратного та програмного забезпечення.

Це дозволяє бізнесу перерозподілити витрати на IT-операції з апаратного/програмного забезпечення та витрат на персонал на досягнення інших IT-цілей.

Крім того, завдяки централізованому розміщенню додатків можна випускати оновлення без необхідності встановлення нового програмного забезпечення користувачами [57].

Недоліком SaaS є те, що дані користувачів зберігаються на сервері хмарного провайдера. Як наслідок, можливий несанкціонований доступ до даних, абонентська плата.

Архітектура Secure DBaaS адаптована до хмарних платформ і не передбачає жодного проміжного проксі-сервера або брокерського сервера між клієнтом і хмарним провайдером.

Усунення будь-якого довіреного проміжного сервера дозволяє Secure DBaaS досягти тих самих рівнів доступності, надійності та еластичності, що й хмарний DBaaS.

Інші пропозиції, засновані на проміжних серверах, були визнані непрактичними для хмарних рішень, оскільки будь-який проксі-сервер є єдиною точкою відмови і вузьким місцем системи, що обмежує основні переваги (наприклад, масштабованість, доступність і еластичність) сервісу баз даних, розгорнутого на хмарній платформі.

На відміну від SecureDBaaS, архітектури, що покладаються на довірений проміжний проксі-сервер, не підтримують найбільш типовий хмарний сценарій, коли географічно розподілені клієнти можуть одночасно виконувати операції читання/запису та модифікації структури даних у хмарній базі даних [25].

6. VPN (Virtual Private Network)

VPN - це віртуальна мережа, побудована на основі існуючих фізичних мереж, яка може забезпечити безпечний механізм зв'язку для даних та іншої інформації, що передається між двома кінцевими точками.

Віртуальні приватні мережі (VPN) на рівні захищених сокетів (SSL) забезпечують безпечний віддалений доступ до ресурсів організації.

Оскільки VPN можна використовувати в існуючих мережах, таких як Інтернет, вона може полегшити безпечну передачу конфіденційних даних через загальнодоступні мережі. [64]

Віртуальна приватна мережа (VPN) розширює приватну мережу через публічну мережу і дозволяє користувачам надсилати та отримувати інформацію через об'єднані або публічні мережі так, ніби їхні обчислювальні маневри безпосередньо пов'язані з замкненою системою.

Таким чином, додатки, що працюють через VPN, можуть отримати вигоду від функціональності, безпеки та управління приватною мережею.

Основна перевага VPN, з точки зору споживача, полягає в тому, що вони є значно економічно вигідними.

Альтернативою використанню технології VPN є високошвидкісна виділена лінія.

Ці лінії дорогі, їх складно адмініструвати та обслуговувати. Крім того, подумайте, що станеться, коли виділена лінія вийде з ладу. Зв'язок між двома сторонами також припиняється, поки відповідні служби не відремонтують лінію. [65]

За реалізацією існує два типи VPN, а саме: VPN з віддаленим доступом та VPN між сайтами [2].

1.1.6 VPN з віддаленим доступом

Рисунок 1.1 демонструє віддалений доступ до VPN, який також називають віртуальною комутованою (VPDN).

Рисунок 1.1 - Віддалений доступ до VPN

VPDN - це тип з'єднання між користувачем і локальною мережею, тобто з'єднання, яке з'єднує мобільного користувача з локальною мережею (LAN).

Це означає, що користувач може отримати доступ до приватної мережі з будь-якого місця.

Зазвичай VPDN використовується співробітниками, які перебувають поза офісом і потребують підключення до офісної мережі компанії.
Переважно компанії, які хочуть створити такий тип VPN-мережі, тісно співпрацюють з постачальником послуг для підприємств (Enterprise Service Provider, ESP).

ESP надає компанії сервер мережевого доступу (NAS).

ESP також надає спеціальне програмне забезпечення для комп'ютерів, що використовуються співробітниками компанії.

1.1.7 Site-to-site VPN

Site-to-site VPN використовується для з'єднання різних областей, які вже фіксовані, через пристрій, що використовує виділену VPN, з'єднані через Інтернет.

Міжсайтова VPN поділяється на дві, а саме: екстранет та інтранет. Інтранет, де VPN використовується тільки для з'єднання різних місць, які все ще є одним агентством або однією компанією.

Наприклад, центральний офіс з'єднаний з філією. Іншими словами, адміністративний контроль в контролі.

У той час як в екстранеті VPN використовується для з'єднання компанії з іншими компаніями, такими як партнери, постачальники або клієнти. Іншими словами, адміністративний контроль знаходиться під контролем деяких відповідних установ.

Принцип роботи VPN подано на рисунку 1.2.

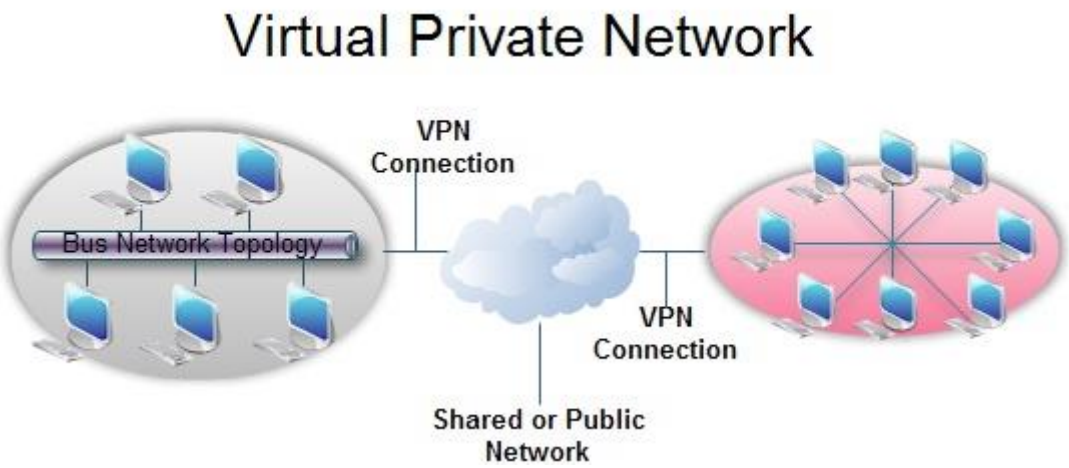


Рисунок 1.2 - Принцип роботи VPN

1.2 Виокремлення ключових тенденцій в наведених методах

Ключові тенденції в ZT:

1. Нульова довіра (ZT):

– перенесення захисту: парадигма ZT переносить захист з мережевих периметрів на користувачів, активи та ресурси;

– оцінка довіри: забезпечує відсутність неявної довіри та постійну оцінку довіри до активів та облікових записів користувачів [55].

2. Архітектура нульової довіри (ZTA):

– комплексний підхід: навколо ідентифікації, облікових даних, управління доступом, операцій, кінцевих точок, хостингових середовищ та сполучної інфраструктури;

– мінімальні привілеї: фокус на обмеженні ресурсів для користувачів та наданні лише необхідних привілеїв.

3. Традиційні підходи та ЗТ:

– зміна акценту: від важіння захисту периметра до обмеження доступу лише тим, кому це потрібно.

– мікросегментація: спроба уникнути широкомасштабних засобів захисту периметра.

4. Оцінка ЗТ і ЗТА. Оптимальні принципи: визначення ZT і ZTA через принципи, такі як перенесення захисту, оцінка довіри та комплексний підхід.

Ці тенденції вказують на перехід від традиційного захисту периметра до більш гнучких та орієнтованих на довіру стратегій, з фокусом на мінімізації привілеїв та постійній оцінці довіри до суб'єктів та пристроїв.

Ключові тенденції в MFA:

1. Широке поширення MFA. Багатофакторна автентифікація є широко використовуваною послугою, особливо в організаціях. Застосування в різних системах зберігання використовується для авторизації доступу до різних систем зберігання даних [38].

2. Безпека та загрози. Стурбованість організацій стосовно безпеки даних: організації висловлюють серйозну стурбованість щодо безпеки даних, оскільки використання різних систем зростає [33].

Інсайдерські загрози становлять значну частину всіх порушень, індикуючи потребу в ефективних заходах безпеки [19].

3. Позитивне ставлення до MFA. Додатковий рівень безпеки у MFA вважається чудовим методом захисту, додаючи додатковий рівень безпеки до традиційної автентифікації за допомогою імені користувача та пароля [20].

4. Реалізація MFA. Технологічні рішення застосовують технології, що дозволяють користувачам використовувати фактори знання на першому рівні, а потім доповнюють їх факторами володіння, такими як код автентифікації на пристрої MFA.

5. Облікові дані та загрози втрати пристрою. Ризики втрати облікових даних: потенційні ризики виникнення, якщо користувач втратить пристрій MFA, що може піддати облікові дані загрозі.

6. Типи MFA та їх використання. Одноразові паролі (OTP): широке використання, але можуть бути піддатливі атакам. Розглядаються як один з елементів MFA.

7. Надійність та безпека MFA. Необхідний компонент управління ідентифікацією та доступом (IAM): MFA розглядається як необхідний компонент для підвищення безпеки компаній.

8. Використання в моделі IAM. Вибір між двофакторною та багатофакторною автентифікацією: користувачі можуть обирати використання двофакторної чи багатофакторної автентифікації в залежності від рівня безпеки.

9. Мобільні схеми 2FA. Безпека без додаткового обладнання: мобільні схеми 2FA вважаються розумним компромісом між безпекою, зручністю використання та вартістю [22].

Ці тенденції вказують на широкий розповсюдження та позитивне ставлення до багатофакторної автентифікації, враховуючи при цьому

існуючі ризики та використання різних технологій для підвищення рівня безпеки.

Розглянемо ключові тенденції в біометричній ідентифікації.

Розрізняються статичні (за ознаками з народження) та динамічні (за ознаками, набутими в процесі існування) методи біометричної ідентифікації.

Біопсихологічна теорія особистості (BIS). Зв'язок із біометричною ідентифікацією: опис BIS використовується для кращого розуміння технологій біометричної ідентифікації, що підкреслює взаємозв'язок між біологічними процесами та особистістю.

Ідентифікація райдужної оболонки ока. Унікальність біометричного ідентифікатора: райдужна оболонка надає унікальність для ідентифікації, базуючись на генетично детермінованій структурі, що виникає внаслідок розвитку ембріонального попередника.

Ідентифікація за відбитками пальців. Незмінність та індивідуальність відбитків пальців: ідентифікація за відбитками пальців визначається їх незмінністю та індивідуальністю. Незмінність полягає в постійному та незмінному візерунку, а індивідуальність - в унікальності деталей [21].

Широке використання в різних галузях: біометричні методи ідентифікації, такі як ідентифікація райдужної оболонки та відбитків пальців, застосовуються в різних галузях, включаючи охорону будівель, територій та банкоматів [13].

Висока точність та надійність. Індивідуальність величезної кількості варіацій: ідентифікація за відбитками пальців має велику індивідуальність, що забезпечує високу точність та надійність [39].

Автоматизація для підвищення продуктивності. Використання автоматичних систем: ручна перевірка відбитків пальців є трудомісткою,

тому використання автоматичних систем ідентифікації допомагає підвищити продуктивність [39].

Інтеграція в системи безпеки. Використання в системах охорони: біометричні методи ідентифікації інтегруються в системи безпеки для забезпечення контролю та доступу.

Ці тенденції свідчать про широкі можливості та ефективність використання біометричної ідентифікації в різних сферах, підкреслюючи їхню унікальність та високий ступінь надійності.

Розглянемо ключові тенденції в контексті загального регламенту про захист даних (GDPR).

Обов'язковість та зобов'язання. Обов'язковість дотримання: GDPR встановлює обов'язкові вимоги до захисту персональних даних для всіх суб'єктів, що опрацьовують такі дані, і це не вимагає ратифікації кожною країною-членом ЄС.

Посилення вимог. Масштабні аудити та оцінки: GDPR суттєво посилив вимоги до систем обробки даних, вимагаючи проведення масштабних аудитів для визначення відповідності.

Вплив на технологічні платформи. Вплив на збір, зберігання та управління даними: очікується, що GDPR суттєво вплине на технологічні платформи та архітектури даних, особливо ті, які займаються персональними даними.

Високі вимоги до обробників та контролерів даних. Обробка даних та захист за замовчуванням: GDPR встановлює високі стандарти для контролерів і обробників даних, включаючи захист даних за замовчуванням і за замовчуванням.

Необхідність ретельної внутрішньої оцінки. Оцінка технологічних платформ: організаціям доведеться провести ретельну внутрішню оцінку своїх технологічних платформ і архітектур даних, включаючи різні інформаційні системи та веб-сайти.

Зміни та Реінжиніринг. Можливі зміни в технологічних платформах: організації можуть бути змушені вносити зміни до своїх технологічних платформ та архітектур даних для відповідності GDPR.

Ризик невідповідності та реінжиніринг. Ризик невідповідності та реінжиніринг існуючих систем: організації можуть зіткнутися з ризиком невідповідності GDPR і потребою в реінжинірингу існуючих систем або платформ для зменшення цього ризику.

Персоналізована реакція на вимоги GDPR. Адаптація до вимог GDPR: різні організації можуть взяти різні шляхи адаптації до вимог GDPR в залежності від їхніх технологічних платформ та архітектур даних.

Ці тенденції свідчать про необхідність глибокого перегляду та адаптації технологічних платформ для відповідності високим стандартам GDPR у сфері захисту персональних даних.

Ключові тенденції в методі Data Protection as a Service (DPaaS):

1. Характеристики DPaaS. Хмарна послуга для комплексного захисту даних: DPaaS надає хмарну послугу, що охоплює резервне копіювання, відновлення та запобігання втраті даних.

2. Захист від розшифрування даних. Захист від атак розшифрування: DPaaS використовує передові технології та стратегії для забезпечення безпеки, доступності та відновлення даних, включаючи сценарії атак розшифрування.

3. Хмарні обчислення та SaaS. Визначення хмарних обчислень: пояснення концепції хмарних обчислень, як використання обчислювальних ресурсів через мережу. Програмне забезпечення як послуга (SaaS): опис використання SaaS в бізнес-моделі, зокрема, передача обслуговування та підтримки апаратного та програмного забезпечення хмарному провайдеру.

4. Переваги SaaS. Зниження операційних витрат: переваги SaaS включають зниження операційних витрат на IT, централізоване

розміщення додатків та можливість випускати оновлення без перевстановлення [44].

5. Недоліки SaaS. Зберігання даних на сервері хмарного провайдера: виділення недоліків SaaS, таких як можливий несанкціонований доступ до даних та абонентська плата [46].

6. Архітектура Secure DBaaS. Безпечна послуга бази даних для хмари: Secure DBaaS адаптована до хмарних платформ та уникне проміжних серверів, що дозволяє досягти високого рівня доступності, надійності та еластичності.

7. Невикористання проміжних проксі-серверів. Обмеження проміжних проксі-серверів: Secure DBaaS не використовує проміжних серверів, уникаючи проблем, пов'язаних із їхнім використанням, такими як єдина точка відмови та вузьке місце системи.

8. Географічно розподілені клієнти. Підтримка географічно розподілених операцій: зазначення того, що архітектура Secure DBaaS підтримує географічно розподілені клієнти для одночасного виконання операцій читання/запису та модифікації даних у хмарній базі даних [32].

Ці тенденції вказують на значущі переваги та обмеження у сфері Data Protection as a Service та використання хмарних технологій для забезпечення безпеки та доступності даних [4].

На основі розгляду ключових тенденцій в областях Zero Trust (ZT), Multi-Factor Authentication (MFA), біометричної ідентифікації, регламенту про захист даних та DPaaS, обрано метод MFA як найефективніший та найлегший в імплементації для захисту даних в IT-інфраструктурі організації. Основні фактори, що підтверджують цей вибір, включають:

1. Широке поширення та позитивне ставлення до MFA. MFA є широко використовуваною послугою в організаціях, а його позитивне ставлення обумовлено як додатковим рівнем безпеки.

2. Безпека та загрози:

Стурбованість організацій стосовно безпеки даних та загрози інсайдерських атак підкреслюють важливість використання ефективних заходів безпеки, таких як MFA.

3. Використання в моделі IAM. MFA визначається як необхідний компонент управління ідентифікацією та доступом (IAM), що вказує на його ключову роль у забезпеченні безпеки компаній.

4. Типи MFA та їх використання. Різні типи MFA, такі як одноразові паролі (OTP), надають можливість користувачам вибору та використання того, що найбільше відповідає вимогам їхньої безпеки.

Висока точність та надійність MFA. Висока точність та надійність ідентифікації за допомогою MFA, зокрема за використання відбитків пальців, роблять його привабливим для використання в організаціях.

Враховуючи ці фактори, важливо провести аналіз методів автентифікації та сервісів для посилення автентифікації, з урахуванням конкретних потреб та характеристик IT-інфраструктури організації.

Розглянемо ключові тенденції в методі VPN (Virtual Private Network).

Безпека та Конфіденційність. VPN надає безпечний механізм зв'язку, що забезпечує захист конфіденційності даних між двома кінцевими точками.

Використання SSL на рівні захищених сокетів у віртуальних приватних мережах гарантує безпечний віддалений доступ до ресурсів організації.

Економічність та Ефективність. VPN є економічно вигідним засобом забезпечення безпеки, оскільки вони можуть використовувати існуючі мережі, такі як Інтернет, полегшуючи передачу конфіденційних даних.

Можливості Розширення. Віртуальна приватна мережа розширює приватну мережу через публічну і дозволяє користувачам обмінюватися

інформацією, якщо їхні обчислювальні маневри пов'язані з замкненою системою.

Типи VPN та їх Застосування. VPN з віддаленим доступом (VPDN): Забезпечує з'єднання між користувачем та локальною мережею, особливо корисний для співробітників, які працюють віддалено.

Site-to-site VPN: З'єднує різні області через віртуальну приватну мережу, що використовується для з'єднання філій або співпраці компаній.

Альтернатива технології VPN.Зазначено, що високошвидкісна виділена лінія є альтернативою технології VPN, але вона може бути витратною та важкоадміністрованою.

Розвиток Технологій. Зазначено, що VPN можна використовувати в існуючих мережах, таких як Інтернет, що вказує на постійний розвиток технологій та їхню адаптацію до змінних умов.

Співпраця з Постачальниками Послуг для Підприємств (ESP). У випадку VPN з віддаленим доступом (VPDN) відзначено співпрацю компаній з постачальниками послуг для підприємств, що підкреслює важливість спільної роботи з постачальниками для успішної імплементації.

Різні Сценарії Застосування. Зазначено, що VPN може використовуватися як для забезпечення з'єднання філій (інтранет), так і для співпраці з іншими компаніями, які є партнерами, постачальниками або клієнтами (екстранет).

На основі розгляду ключових тенденцій в областях Zero Trust (ZT), Multi-Factor Authentication (MFA), біометричної ідентифікації, регламенту про захист даних та DPaaS, VPN, обрано метод MFA як найефективніший та найлегший в імплементації для захисту даних в IT- інфраструктурі організації. Основні фактори, що підтверджують цей вибір, включають:

1. Широке поширення та позитивне ставлення до MFA. MFA є широко використовуваною послугою в організаціях, а його позитивне ставлення обумовлено як додатковим рівнем безпеки.

2. Безпека та загрози. Стурбованість організацій стосовно безпеки даних та загрози інсайдерських атак підкреслюють важливість використання ефективних заходів безпеки, таких як MFA.

3. Використання в моделі IAM. MFA визначається як необхідний компонент управління ідентифікацією та доступом (IAM), що вказує на його ключову роль у забезпеченні безпеки компаній.

4. Типи MFA та їх використання. Різні типи MFA, такі як одноразові паролі (OTP), надають можливість користувачам вибору та використання того, що найбільше відповідає вимогам їхньої безпеки.

5. Висока точність та надійність MFA. Висока точність та надійність ідентифікації за допомогою MFA, зокрема за використання відбитків пальців, роблять його привабливим для використання в організаціях.

Враховуючи ці фактори, важливо провести аналіз методів автентифікації та сервісів для посилення автентифікації, з урахуванням конкретних потреб та характеристик IT- інфраструктурі організації.

1.3 Постановка задачі дослідження

Існуючий огляд методів та засобів захисту даних в організації показав, що є велика кількість відомих рішень та сервіс мультифакторної автентифікації виявися найоптимальнішим для імплементації в IT-інфраструктуру організації.

Таким чином, постає завдання вибору оптимального методу та сервісу MFA.

Метою є аналіз методів автентифікації та сервісів для посилення автентифікації з метою вибору оптимального способу та сервісу для підвищення рівня безпеки даних в IT- інфраструктурі організації.

Кроки аналізу:

1. Аналіз існуючих методів автентифікації. Дослідження різних методів автентифікації, включаючи паролі, одноразові паролі (OTP), біометричну ідентифікацію, та інші доступні технології.

2. Оцінка сервісів для посилення автентифікації. Проведення аналізу різних сервісів, які надають рішення для підвищення рівня безпеки автентифікації, з урахуванням їхньої ефективності та можливостей.

4. Порівняння ефективності та безпеки. Порівняння різних методів та сервісів за критеріями ефективності та безпеки в контексті конкретних потреб організації.

5. Вибір найоптимальнішого способу та сервісу. Обрання та рекомендація найоптимальнішого методу та сервісу для підвищення рівня безпеки автентифікації в IT-інфраструктурі організації.

Ця задача спрямована на забезпечення вибору та імплементацію методу автентифікації, який оптимально відповідає потребам та вимогам IT- інфраструктурі організації, забезпечуючи максимальний рівень безпеки для її даних.

2. МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ДАНИХ ПРИ ОБРОБЦІ ТА ПЕРЕДАВАННІ В ІТ-ІНФРАСТРУКТУРІ ОРГАНІЗАЦІЇ

2.1 Збір та аналіз даних про методи захисту даних при обробці та передаванні в ІТ-інфраструктурі організації

2.1.1 PassWindow

PassWindow - це метод забезпечення аутентифікації за другим фактором в онлайн-середовищі.

Він включає в себе сегментні матриці - фізичний шаблон ключа, надрукований на портативній пластиковій підкладці, і цифровий складний шаблон, який відображається у вигляді зображення на звичайному електронному екрані, наприклад, на дисплеї ноутбука або мобільного пристрою.

При накладенні вони показують користувачеві унікальний одноразовий код доступу та набір цифр, характерних для певної транзакції.

Цей код використовується для онлайн-аутентифікації та перевірки транзакцій.

Специфічна інформація про транзакцію, що міститься в цих цифрах, наприклад, інформація про цільовий рахунок призначення або суму транзакції, дозволяє користувачеві візуально підтвердити мету отриманого виклику на аутентифікацію.

Ці функції роблять PassWindow одним з небагатьох доступних механізмів автентифікації, який забезпечує надійний захист від новітніх онлайн-загроз безпеки типу Man-In-the-Middle (MITM) [34].

PassWindow може використовуватись для захисту при обробці та передаванні даних, забезпечуючи аутентифікацію за другим фактором у онлайн-середовищі, рис. 2.1.

Рисунок 2.1 - Логотип PassWindow

2.1.2 SFA

Спочатку для автентифікації суб'єкта використовувався лише один фактор. Однофакторна автентифікація (Single-Factor Authentication, SFA) в основному прийнята спільнотою через її простоту і зручність для користувача . Як приклад, можна розглянути використання пароля (або PIN-коду) для підтвердження права власності на ідентифікатор користувача. Очевидно, що це найслабший рівень автентифікації [8].

Зазвичай, при використанні цього типу автентифікації слід враховувати вимогу мінімальної складності пароля. SFA зазвичай використовує один із наступних факторів:

1. Щось, що ви знаєте (Something You Know): наприклад, пароль чи PIN-код.
2. Щось, що ви маєте (Something You Have): наприклад, фізичний ключ, токен або смарт-карта.
3. Щось, що ви є (Something You Are): наприклад, біометричні дані, такі як відбиток пальця чи розпізнавання обличчя.

Спрощена природа SFA може призвести до ризику безпеки, оскільки в разі компрометації єдиного фактора зловмисники можуть отримати доступ до системи або даних.

Тому в сучасних системах інформаційної безпеки широко використовується багатофакторна аутентифікація (MFA), де використовуються комбінації різних факторів для підвищення рівня захисту та запобігання несанкціонованому доступу [48].

2.1.3 MFA

Багатофакторна автентифікація (Multi-Factor Authentication, MFA) — це метод, при якому користувач повинен надати кілька видів аутентифікаційної інформації для підтвердження своєї ідентичності перед отриманням доступу до системи чи послуги.

MFA використовує комбінації різних факторів для забезпечення вищого рівня безпеки порівняно з однофакторною автентифікацією.

Існують наступні способи впровадження MFA: генерація OTP, генерація HOTP, генерація TOTP

2.1.4 Генерація OTP

Одноразовий пароль (OTP) - це пароль, який дійсний лише для одного сеансу входу або транзакції. OTP уникають ряду недоліків, які пов'язані з традиційними (статичними) паролями.

Найважливішим недоліком OTP є те, що, на відміну від статичних паролів, вони не є вразливими до атак повторного відтворення.

Це означає, що потенційний зловмисник, якому вдасться записати OTP, що вже використовувався для входу в сервіс або для проведення

транзакції, не зможе ним зловживати, оскільки він вже не буде дійсним [10].

Запатентовано велику кількість технологій OTP, що робить стандартизацію в цій області важчою, оскільки кожна корпорація чи компанія хоче проштовхнути свою власну технологію, котра би була найбільш сприятливим для її кінчевого споживача.

Разом з тим, це великий плюс, так як, постійно виникають нові алгоритми – технологія розвивається. Стандарти, однак, існують, наприклад, TOTP і HOTP.

2.1.5 Генерація HOTP

HOTP - це алгоритм генерації одноразового пароля, який працює на основі механізму автентифікації повідомлень.

Він може бути реалізований будь-яким розробником апаратного або програмного забезпечення для створення сумісного пристрою або програмного забезпечення для автентифікації.

Для генерації одноразових паролів використовується інкрементний лічильник і статичний симетричний ключ, відомий лише пристрою безпеки та серверу верифікації.

Для значення HOTP використовується алгоритм HMAC-SHA-1, який приймає довільно великий набір даних і повертає значення певної довжини 160 біт як вихідне значення:

$$HOTP(K, counter) = HMAC - SHA\text{-}1(K, counter) \quad (2.1)$$

де K - загальний секрет між клієнтом і сервером, а counter - 8-байтне значення лічильника. Цей лічильник повинен бути синхронізований між генератором HOTP (клієнт) і валідатором HOTP (сервер) [7].

2.1.6 Генерація TOTP

Алгоритм Time-based One Time Password (TOTP) - один з найпоширеніших алгоритмів двофакторної автентифікації.

Він був застосований при розробці веб-додатку для відстеження електронних відпусток для покращення безпеки та автентифікації при доступі до додатку.

Він забезпечує додаткову функцію безпеки, яка полягає в тому, що навіть якщо пароль користувача викрадений або скомпрометований, зловмисник не може отримати доступ до цього облікового запису без пароля, згенерованого TOTP, який змінюється кожні 30-60 секунд.

Концептуальна основа дослідження була розроблена на основі багатофакторної автентифікації, зокрема алгоритму TOTP, моделі швидкої розробки додатків - цикли прототипування слугували основою в процесі розробки системи [54].

Дослідження складається з трьох основних компонентів: розробка веб-додатку для відстеження електронних відпусток, тестування функціональних можливостей з точки зору автентифікації користувачів та відновлення облікових записів, а також технічна оцінка з точки зору сумісності, надійності та безпеки.

Веб-додаток показав, що алгоритм TOTP заслуговує на похвалу з точки зору автентифікації, відновлення та безпеки користувачів [45].

2.1.7 Google Authenticator

Google Authenticator забезпечує двоетапну процедуру автентифікації за допомогою одноразових паролів (OTP).

Додаток для генерації OTP доступний для iOS, Android та Blackberry. Механізм автентифікації інтегрується в систему Linux PAM.

У цьому посібнику описано встановлення та налаштування цього механізму [11].

Автентифікатор представляє 6-ти або 8-мизначний одноразовий цифровий пароль, який користувач повинен надати в додаток до імені користувача і пароля, щоб увійти в Google або інших сервісів. Автентифікатор також може генерувати коди для сторонніх додатків, такі як менеджери паролів або послуг хостингу файлів. Попередні версії програми були доступні з відкритим вихідним кодом на GitHub, але останні випуски є приватною власністю Google [29].

2.1.8 Microsoft Authenticator

Microsoft Authenticator - це технологія двофакторної автентифікації (2FA), яку також називають двоетапною перевіркою або двоетапною автентифікацією, при вході в облікові записи або програми.

Microsoft Authenticator можна завантажити як додаток на Android та iOS і отримати одноразові коди доступу не лише до облікових записів і продуктів Microsoft, а й до інших сайтів і продуктів, які використовують двофакторну автентифікацію.

Він також забезпечує безпарольний вхід до продуктів і сайтів Microsoft та керування обліковими записами для кількох сайтів або програм одночасно [52].

Microsoft Authenticator генерує шестизначний пароль, який відображається для кожного доданого облікового запису.

Пароль дійсний протягом 30 секунд, що запобігає використанню коду кілька разів.

Щоб ініціалізувати обліковий запис можна скористатись можливістю сканування QR-коду або ввести коду вручну.

2.1.9 Twillio Authy

Twillio Authy – мобільний застосунок, котрий забезпечує генерацію одноразових паролів на основі алгоритму TOTP.

Додаток має змогу працювати офлайн. Twillio Authy генерує шестизначний пароль, котрий дійсний протягом 30 секунд. Ініціалізація облікового запису проходить шляхом сканування QR-коду або введення коду вручну.

Авторизувавшись на сервері Twillio Authy за номером телефону, додаток дає змогу використовувати застосунок одночасно на декількох пристроях, котрі будуть синхронізовані. В разі втрати пристрою, як фактора власності, можна деавторизувати його з будь-якого іншого авторизованого пристрою.

Authy розроблений та доступний для мобільних пристроїв, які працюють під системою IOS, Android чи Windows, та для розумних годинників.

Conditional Access і Azure Active Directory. Azure Active Directory (Azure AD) - це хмарна служба від корпорації Microsoft для управління ідентифікацією і доступом як послуга (IDaaS), яке поєднує в собі можливості єдиного доступу до будь-якого хмарного чи локального додатку з розширеним захистом.

Це дає користувачам єдине посвідчення для доступу до потрібних їм додатків і спільної роботи з будь-якої платформи і пристрою. Оскільки Azure AD заснована на масштабованих можливостях управління і правилах доступу з урахуванням ризиків, Azure AD допомагає забезпечити безпеку і оптимізувати IT-процеси [59].

Служба надає такі функції:

1. Управління додатками. Керування хмарними і локальними додатками за допомогою Application Proxy, єдиного входу, порталу "Мої додатки" (також званого панеллю доступу) і додатків SaaS. Azure AD вже працює з величезною кількістю комерційних і користувацьких додатків, наприклад Office 365, Saleforce.com, Box і Workday. Або ж ви можете підключити додатки, яких ще немає в базі, наприклад, розроблені вашою компанією, використовуючи готовий набір шаблонів і бібліотек.

2. Автентифікація. Адміністрування самостійного скидання пароля, багатофакторної перевірки автентичності, що налаштовується, списку заборонених паролів і смарт-блокування в Azure Active Directory.

3. Умовний доступ. Управління доступом до хмарних додатків.

4. Управління пристроями.Управління тим, як хмарні і локальні пристрої отримують доступ до корпоративних даних.

5. Доменні служби. Приєднання віртуальних машин Azure до домену без використання контролерів домену. Служба Domain Controller as a Service для перенесення традиційних додатків на Azure IaaS, для віртуальних машин Windows і Linux.

6. Користувачі Enterprise. Управління призначенням ліцензій, доступом до додатків і налаштування делегатів з використанням груп і ролей адміністратора.

7. Гібридне посвідчення. Використання Azure Active Directory Connect і Connect Health для надання одного ідентифікатора користувача для аутентифікації і авторизації в усіх ресурсах, незалежно від розташування (локально або в хмарі).

8. Захист ідентифікації. Визначення потенційних вразливостей, що впливають на посвідчення організації, налаштування політик для відповіді на підозрілу активність і виконання відповідних дій для її усунення [53].

Conditional Access (CA) - це механізм перевірки кожного процесу під'єднання до системи на основі налаштованого сценарію і рішення, що встановлює, що робити з цим під'єднанням. А його можна заборонити, дозволити без умов або дозволити з умовами.

Є компонентом Azure AD.

Assignments - у яких випадках сценарій має спрацьовувати.

Access controls - що потрібно зробити.

Users and groups - які користувачі потрапляють під дію політики. Це можуть бути всі користувачі в Azure AD або конкретні групи/користувачі. Окремо можна вказати винятки. Ви можете застосувати політику для всіх користувачів за винятком окремої групи.

Cloud apps - сценарії можуть застосовуватися до будь-якого додатка, зареєстрованого в Azure AD. Тобто ви не обмежені роботою тільки з додатками Office 365.

Conditions - додаткові умови.

Sign-in risk - можливість використання механізму оцінювання ризику авторизації. Оцінюється звідки, в який час, з використанням якого клієнта, наскільки ця поведінка звичайна тощо.

Device platforms - можливо вказати, до якої платформи буде застосовна політика. Наприклад, створення політики тільки для мобільних клієнтів або тільки для Windows машин.

Locations - мають на увазі мережеві локації. Можна використовувати список довірених IP-адрес.

Client apps (preview) - оцінює тип клієнта. Можливо використовувати, щоб створити політику тільки для браузера або EAS (Exchange Active Sync). Для тих, хто захоче закрити використання OWA на мобільних пристроях, але залишити опцію для настільних комп'ютерів.

Device state (preview) - дає можливість виключити пристрої в певному статусі.

Grant - саме тут відбувається налаштування сценарію: блокування доступу або вимога додаткових заходів безпеки.

Session - здійснення контролю в самій сесії. Поки що можливе використання тільки з Exchange Online і Sharepoint Online, рис. 2.2.

Рисунок 2.2 - Логотип Azure Active Directory

2.2 Вибір методів та їх обґрунтування

2.2.1 Переваги методу 2FA

В магістерській роботі обрано метод 2FA (двофакторної аутентифікації) для забезпечення захисту персональних даних в IT-організації.

В контексті безпеки даних, методи багатофакторної автентифікації (MFA) можуть також використовуватись для захисту інформації при обробці та передаванні через технологію PassWindow.

Це можливо зважаючи на перелічені фактори [51]:

1. Додатковий рівень автентифікації. MFA може додати додатковий рівень автентифікації до процесу обробки та передавання даних. У випадку PassWindow це може включати використання фізичних ознак користувача, які є унікальними для кожного індивіда, разом з штрих-кодами для створення комбінації, доступної тільки автентифікованому користувачеві.

2. Захист від перехоплення. Так, як PassWindow використовує штрих-коди для передавання інформації, подібно до того, як MFA використовує додаткові фактори, це може забезпечити додатковий захист від перехоплення даних. Зловмисники, які намагаються перехопити інформацію, матимуть складність у розкодуванні та використанні даних без належної автентифікації.

3. Одноразові паролі. В тексті зазначено, що PassWindow може використовувати короткі рядки випадкових чисел, які використовуються як одноразові паролі. Це концепція, що вже є стандартним підходом у багатьох системах MFA для забезпечення безпеки під час автентифікаційних транзакцій.

4. Відсутність заздалегідь збережених даних. MFA, подібно до PassWindow, може допомагати уникнути заздалегідь збережених даних або однозначних інформаційних патернів, зменшуючи тим самим ризик несанкціонованого доступу до даних.

Таким чином, використання 2FA в сучасних системах автентифікації може інтегрувати подібні концепції для захисту даних під час їхньої обробки та передавання.

Застосування додаткових факторів, таких як фізичні ознаки та одноразові паролі, може зробити системи ще більш надійними та відповідними високим стандартам безпеки.

Використання кількох факторів автентифікації для підтвердження своєї особи базується на передумові, що несанкційований користувач навряд чи зможе надати фактори, необхідні для доступу.

Якщо під час спроби автентифікації хоча б один із компонентів відсутній або поданий неправильно, ідентифікація користувача не встановлюється з достатньою достовірністю, і доступ до об’єкта, котрий захищається багатофакторною автентифікацією, тоді залишається заблокованим. 2FA значно піднімає планку для зловмисника [9].

Двофакторна автентифікація захищає організацію від компрометації облікових записів користувачів, але додає додатковий крок до виконання критично важливих завдань [14].

Сервіс багатофакторної автентифікації - це ефективний механізм контролю доступу уповноважених осіб до цінних ресурсів, таких як програмне забезпечення, мережевий сервер або обчислювальний пристрій.

У цьому механізмі користувач повинен представити більше одного облікового запису для автентифікації.

Ці облікові дані або фактори автентифікації змінюються залежно від потреб програми в безпеці.

Користувач повинен послідовно подавати до системи безпеки кілька факторів автентифікації [5].

Ці фактори повинні бути незалежними, щоб уникнути порушення всієї системи безпеки у випадку компрометації одного з цих облікових даних [41].

Розглянемо переваги та обґрунтування вибору 2FA.

Висока безпека. 2FA забезпечує високий рівень безпеки, оскільки для отримання доступу необхідно підтвердити ідентичність користувача двома або більше способами. Це робить практично неможливим несанкціонований доступ навіть у випадках витоку одного елемента ідентифікації.

Простота впровадження. Одним із головних плюсів вибору 2FA є його простота впровадження. Зазвичай, цей метод може бути легко інтегрований в існуючі системи без значних труднощів та витрат на оновлення.

Підвищена зручність. Введення двох чи більше елементів для аутентифікації може бути здійснено швидко та зручно. Пароль та одне додаткове підтвердження часто є менш обтяжливими для користувачів, порівняно з іншими складнішими методами.

Масштабованість. 2FA легко масштабується для великих корпоративних середовищ. Він може бути використаний для захисту доступу до різних рівнів систем та сервісів.

Зменшення впливу витоків даних. У випадку витоку одного елемента аутентифікації (наприклад, пароля), інший елемент взаємодії залишається непорушеним, що додає додатковий шар безпеки [26].

2.2.2 Ефективність методу 2FA

Двофакторна автентифікація може бути особливо корисною для галузей з високим рівнем ризику, які сильно покладаються на захист даних.

Розглянемо ризики безпеки, з якими стикаються різні галузі, і як двофакторна автентифікація може допомогти їх уникнути (див. рисунок 2.5).

Фінансова галузь. Клієнти покладаються на фінансові установи в питанні захисту своїх даних. Однак ці установи також у 300 разів частіше стикаються з кібератаками.

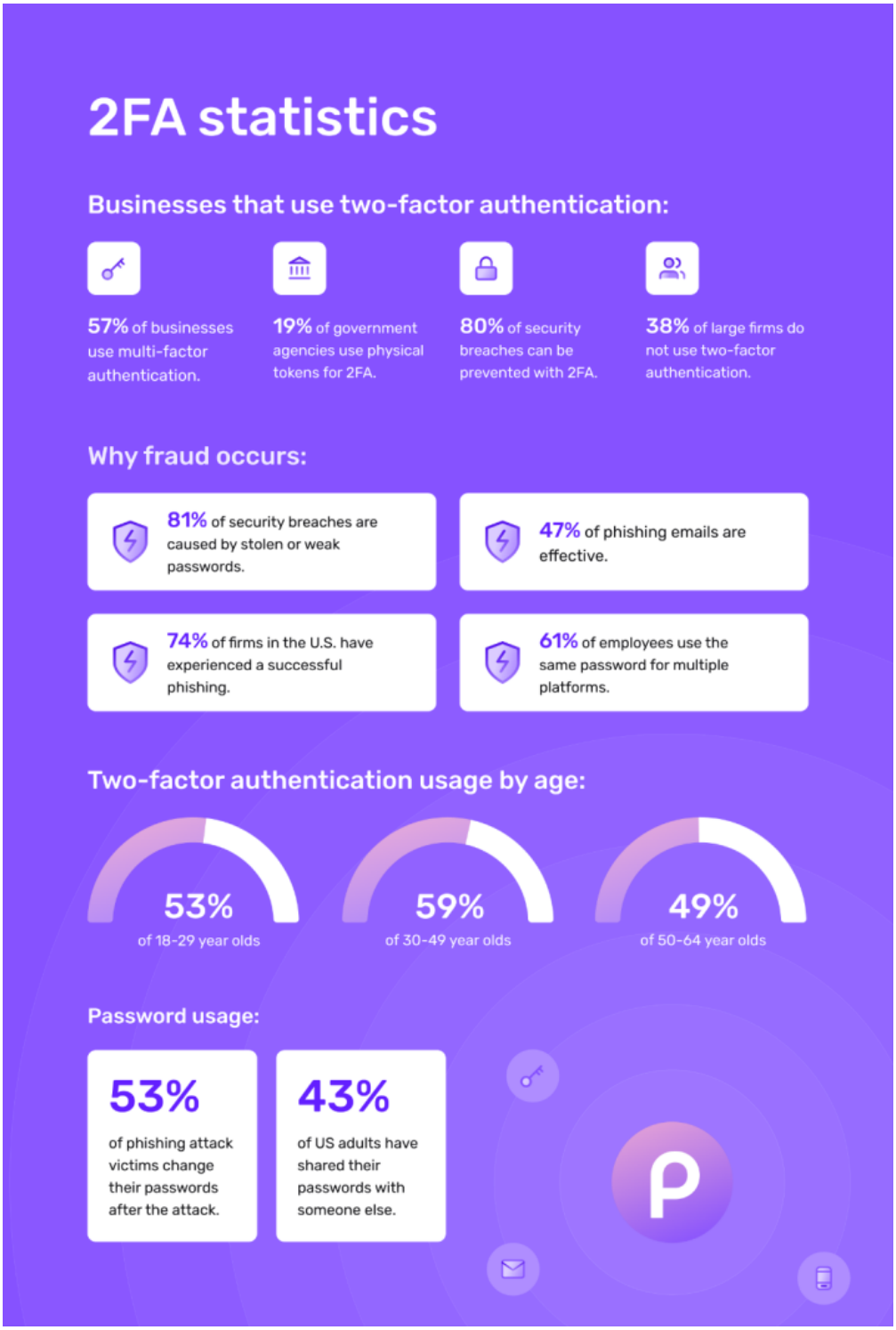


Рисунок 2.5 - Статистика ефективності використання 2FA

Порушення безпеки даних у фінансових установах дає кіберзлочинцям доступ до конфіденційної інформації, такої як дані

кредитних карток, номери соціального страхування та персональні дані користувачів.

Потім зловмисники можуть використати цю інформацію для здійснення шахрайських дій із заволодіння обліковими записами, які в середньому займають 16 годин.

Ось чому для фінансових послуг важливо використовувати двофакторну систему автентифікації для захисту облікових записів користувачів.

38% респондентів, які надають фінансові послуги, вважають, що розвиток технологій збільшив ризики інформаційної безпеки.

Однак організації можуть захистити себе від несанкціонованих входів, внутрішніх загроз і зовнішніх атак за допомогою двофакторної автентифікації.

Завдяки двофакторній автентифікації компанії, що надають фінансові послуги, покращують відносини з клієнтами, зміцнюючи їхню довіру.

Галузь охорони здоров'я також приваблює кібератаки, оскільки має справу з конфіденційною інформацією про пацієнтів, такою як медичні записи та дані кредитних карток.

Дослідження показують, що приблизно 79% всіх зареєстрованих витоків даних були здійснені в секторі охорони здоров'я, і очікується, що ця галузь зазнає збитків на суму понад 6 трильйонів доларів США в період з 2017 по 2020 рік.

Двофакторна автентифікація може допомогти медичним установам уникнути витоку даних, оскільки хакеру знадобиться як пароль, так і код або символ, надісланий на телефон авторизованого користувача.

Ця система може бути корисною для захисту персональних даних пацієнтів та працівників галузі охорони здоров'я.

Індустрія електронної комерції. Зі зростанням індустрії електронної комерції зростає і кількість кібератак та витоків даних.

Статистика показує, що роздрібні торговці електронною комерцією стикаються в середньому з 206 000 веб-атаками на місяць, а збитки від шахрайства в електронній комерції, як очікується, досягнуть 6,4 мільярда доларів до 2021 року.[62]

Підприємства електронної комерції можуть отримати значну вигоду від двофакторної системи автентифікації, якою можуть користуватися як клієнти, так і співробітники. Окрім захисту конфіденційної інформації, двофакторна автентифікація може допомогти зміцнити довіру клієнтів і ускладнити хакерські атаки.

Державний сектор надзвичайно вразливий до кібератак, оскільки урядові установи мають доступ до великої кількості конфіденційної інформації, включаючи фінансові та військові дані.

Лише у 2018 році 1,2 мільярда урядових записів було порушено через кібератаки.

Не дивно, що в 2020 році американські урядові організації витратили 18,88 мільярда доларів на відновлення та простої після кібератаки.

Завдяки двофакторній автентифікації уряд може захистити акаунти співробітників від внутрішніх і зовнішніх загроз, насамперед від злому акаунтів і фішингових атак.

Двофакторна автентифікація захищає організації, зменшуючи ймовірність несанкціонованого доступу, який може статися, коли користувачі діляться паролями або стають жертвами фішингових атак чи витоку даних.

За даними Google, використання двофакторної автентифікації блокує 100% автоматизованих хакерських атак ботів [62].

Використання цієї практики також полегшує віддалену роботу бізнесу, оскільки співробітники можуть безпечно отримати доступ до систем компанії з будь-якого місця.

Крім того, двофакторна автентифікація може допомогти компаніям заощадити час і гроші, зменшуючи ймовірність витоку даних - станом на 2020 рік середня вартість витоку даних становила 3,86 мільйона доларів, а також може суттєво вплинути на репутацію компанії.

Дослідження показують, що 49% клієнтів відмовляються реєструватися в онлайн-сервісі, який зазнав кібератаки.

Саме тут може допомогти двофакторна автентифікація. Оскільки 2FA зменшує ймовірність несанкціонованого доступу, ваша компанія може краще захистити персональні дані клієнтів.

Обрання 2FA в дослідженні обгрунтовано не лише його технічною ефективністю, але і практичністю використання.

Його простота впровадження, висока безпека та зручність для користувачів роблять його оптимальним вибором для забезпечення захисту персональних даних в IT-інфраструктурі організації.

2.3.1 Переваги сервісу Azure Active Directory

Розглянемо основні переваги Azure Active Directory (Azure AD) на основі наданого тексту.

Єдиний Доступ та Спільна Робота. Azure AD забезпечує єдине посвідчення для доступу до різноманітних додатків, незалежно від їхнього типу (хмарні чи локальні), що полегшує користувачам спільну роботу з будь-якої платформи та пристрою.

Azure AD базується на масштабованих можливостях управління та правил доступу з урахуванням ризиків, що дозволяє оптимізувати IT-процеси та забезпечує високий рівень безпеки.

Управління Додатками. Послуга Azure AD дозволяє керувати як хмарними, так і локальними додатками, використовуючи різні інструменти, такі як Application Proxy, єдиний вхід, портал "Мої додатки" та додатки SaaS.

Azure AD вже інтегровано з великою кількістю комерційних і користувацьких додатків, таких як Office 365, Salesforce.com, Box і Workday, що робить його універсальним для використання.

Можливості Автентифікації. Azure AD надає ряд можливостей автентифікації, таких як самостійне скидання пароля, багатофакторна перевірка автентичності, налаштовується списки заборонених паролів та смарт-блокування.

Умовний Доступ. Використання функції Conditional Access дозволяє управляти доступом до хмарних додатків, налаштовуючи умови та правила для безпечного з'єднання.

Управління Принтерами та Просторами. Azure AD може бути використаний для приєднання віртуальних машин Azure до домену без використання контролерів домену та надає Domain Controller as a Service для перенесення традиційних додатків на Azure IaaS.

Управління Користувачами Enterprise. Azure AD дозволяє ефективно керувати призначенням ліцензій, доступом до додатків та конфігуруванням делегатів за допомогою груп і ролей адміністратора.

Інтеграція з Іншими Сервісами. Azure AD інтегрується з іншими сервісами, такими як Azure Active Directory Connect і Connect Health, що дозволяє надати один ідентифікатор користувача для аутентифікації та авторизації в усіх ресурсах, незалежно від їхнього розташування.

2.3.2 Ефективність Azure Active Directory

Хоча хмарове обчислювальне середовище є дуже ефективним та економічно вигідним для великих організацій, однак однією з найважливіших проблем у хмаровому середовищі є безпека.

Хмарні постачальники не завжди повністю орієнтовані на конкретні потреби організацій у справах безпеки та конфіденційності.

Важливо, щоб хмарове середовище було налаштовано для задоволення вимог організацій.

Організації вимагають, щоб будь-яке обране рішення хмарового обчислення було налаштоване, розгорнуте та управлялося з урахуванням їхніх потреб у справах безпеки, конфіденційності та інших вимог.

Однією з ключових загроз хмаровому середовищу є несанкціонований доступ до даних, додатків чи інфраструктури.

Для ефективної реалізації цього ми повинні мати потужний механізм управління доступом в хмаровому середовищі.

Управління ідентифікацією та контролем доступу (IAM) визначається як методи, що надають достатній рівень захисту для ресурсів та даних організації через правила та політики, які застосовуються до користувачів за допомогою різних технік, таких як забезпечення пароля входу, надання привілеїв користувачам та надання облікових записів користувачів.

У хмаровому середовищі основні загрози походять від веб-браузерів, що використовуються для клієнтського доступу до послуг хмарового обчислення. Різноманітні доступні додатки та розширення для веб-браузерів - це основні причини їхніх проблем із безпекою.

Багато додатків для веб-браузерів також не надають автоматичних оновлень, що підвищує стійкість існуючих вразливостей.

Однак, з огляду на безпеку, Azure Active Directory (Azure AD) виявляється ефективним рішенням.

Воно надає механізми управління ідентифікацією та контролю доступу, які враховують специфіку хмарового середовища.

Реалізовані механізми аутентифікації та авторизації враховують динаміку хмарового середовища та забезпечують високий рівень захисту.

Azure AD підтримує управління доступом на рівні сервера з урахуванням безпеки та конфіденційності даних.

Окрім того, воно інтегрується з різними хмаровими платформами, такими як Google, Amazon та Microsoft Azure. Azure Active Directory є однією з найефективніших хмарових платформ, а його служби активного каталогу дозволяють реалізувати надійний та безпечний доступ до хмарових ресурсів.

Розглянемо основні переваги Azure Active Directory (Azure AD).

Єдина точка входу. Azure AD надає єдину точку входу (Single Sign-On), що дозволяє користувачам отримувати доступ до різноманітних хмарових та локальних додатків, використовуючи лише один обліковий запис та пароль.

Інтеграція з існуючими службами Microsoft. Для організацій, які використовують інші продукти Microsoft, Azure AD ідеально інтегрується з їхнім екосистемами, такими як Office 365, SharePoint, інші облікові записи корпоративних служб.

Механізми безпеки. Azure AD пропонує різноманітні механізми безпеки, такі як багатофакторна аутентифікація, контроль умовного доступу, виявлення ризику та інші, що роблять його ефективним для забезпечення безпеки корпоративних ресурсів.

Гнучкість управління доступом. Azure AD дозволяє настроювати політики доступу, визначати, хто, як і коли може отримувати доступ до різних ресурсів.

Підтримка стандартів безпеки. Підтримка промислових стандартів безпеки, таких як OAuth та OpenID Connect, робить Azure AD сумісним із сторонніми додатками та службами.

Основними недоліками Azure Active Directory (Azure AD) насьогодні можна вважати:

1. Залежність від інтернет-з'єднання: Для повного функціонування Azure AD потрібне постійне інтернет-з'єднання, що може становити проблему в умовах непостійного доступу до мережі.

2. Специфічність для екосистеми Microsoft. Хоча Azure AD інтегрується добре з продуктами Microsoft, він може виявитися менш універсальним, якщо організація використовує інші екосистеми або має різноманіття технологій.

3. Вартість. Деякі функції та розширені можливості Azure AD можуть бути пов'язані з додатковими витратами, що робить його менш доступним для менших компаній з обмеженими бюджетами.

4. Необхідність налаштування. Для досягнення оптимального використання Azure AD, організації можуть потребувати певного часу та експертизи для налаштування та управління сервісом.

5. Обмежені можливості в безкоштовному варіанті. Безкоштовний варіант Azure AD (Azure AD Free) має обмежені можливості порівняно з платними планами, що може бути недостатнім для певних великих організацій.

2.4.1 Переваги методу VPN

Технологія віртуальних приватних мереж (VPN) стала невід'ємним компонентом сучасних стратегій кібербезпеки.

VPN забезпечують безпечний віддалений доступ до мережі та ресурсів компанії з будь-якого місця.

Це дозволяє співробітникам працювати з дому або в дорозі, маючи при цьому доступ до критично важливих бізнес-додатків і даних.

VPN також дозволяють компаніям розширювати свою мережу до віддалених офісів, постачальників і партнерів, забезпечуючи безпечне і надійне з'єднання між різними місцями [66].

Розглянемо переваги та обґрунтування вибору VPN.

VPN використовує передові алгоритми шифрування для захисту усього мережевого трафіку, що ускладнює можливість зловживання та крадіжки інформації.

Забезпечення Віддаленого Доступу. VPN надає безпечний віддалений доступ до мережі та ресурсів компанії з будь-якого місця, що дозволяє співробітникам працювати з дому чи в русі та одночасно мати доступ до важливих бізнес-додатків та даних.

Розширення Мережі. VPN дозволяє компаніям розширювати свою мережу до віддалених офісів, постачальників та партнерів, забезпечуючи безпечне та надійне з'єднання між різними місцями.

Масштабованість. VPN можна легко масштабувати для задоволення потреб ростучого бізнесу, додавши нових співробітників чи розташувань і миттєво адаптуючись до збільшеного попиту.

Гнучкість Налаштувань. VPN може бути налаштований відповідно до конкретних потреб організації, включаючи правила маршрутизації, політики контролю доступу та методи аутентифікації.

Більшість рішень VPN включають функції звітності та логування, які дозволяють відслідковувати використання мережі, моніторити активність користувачів та виявляти потенційні загрози безпеки.

2.4.2 Ефективність методу VPN

У 2022 році світовий ринок віртуальних приватних мереж (VPN) склав 45 мільярдів доларів США і, за прогнозами, досягне 350 мільярдів доларів США до 2032 року.

Віртуальні приватні мережі призначені для безпечного розширення мережі з приватного місця, такого як офіс або будинок, через публічну мережу, так, як якщо б мережа була безпосередньо підключена.

VPN популярні серед споживачів для приховування свого реального місцезнаходження, чи то для доступу до географічно заблокованих сервісів, чи то для обходу цензури або інших обмежень.

На підприємствах VPN часто створюють для того, щоб працівники мали доступ до корпоративних інтрамереж під час подорожей, віддаленої роботи або роботи з дому [67].

Для промисловості найбільшою причиною використання VPN все ще залишається захист системи, оскільки все більше організацій покладаються на керовані системи VPN для захисту своєї інформації.

Зростання попиту на VPN призвело до того, що все більше компаній, які займаються кібербезпекою, приєднуються до боротьби, що ще більше розширює ринок [66].

Розмір світового ринку мереж VPN у 2022 році порівняно з 2032 роком подано на рисунку 2.6.

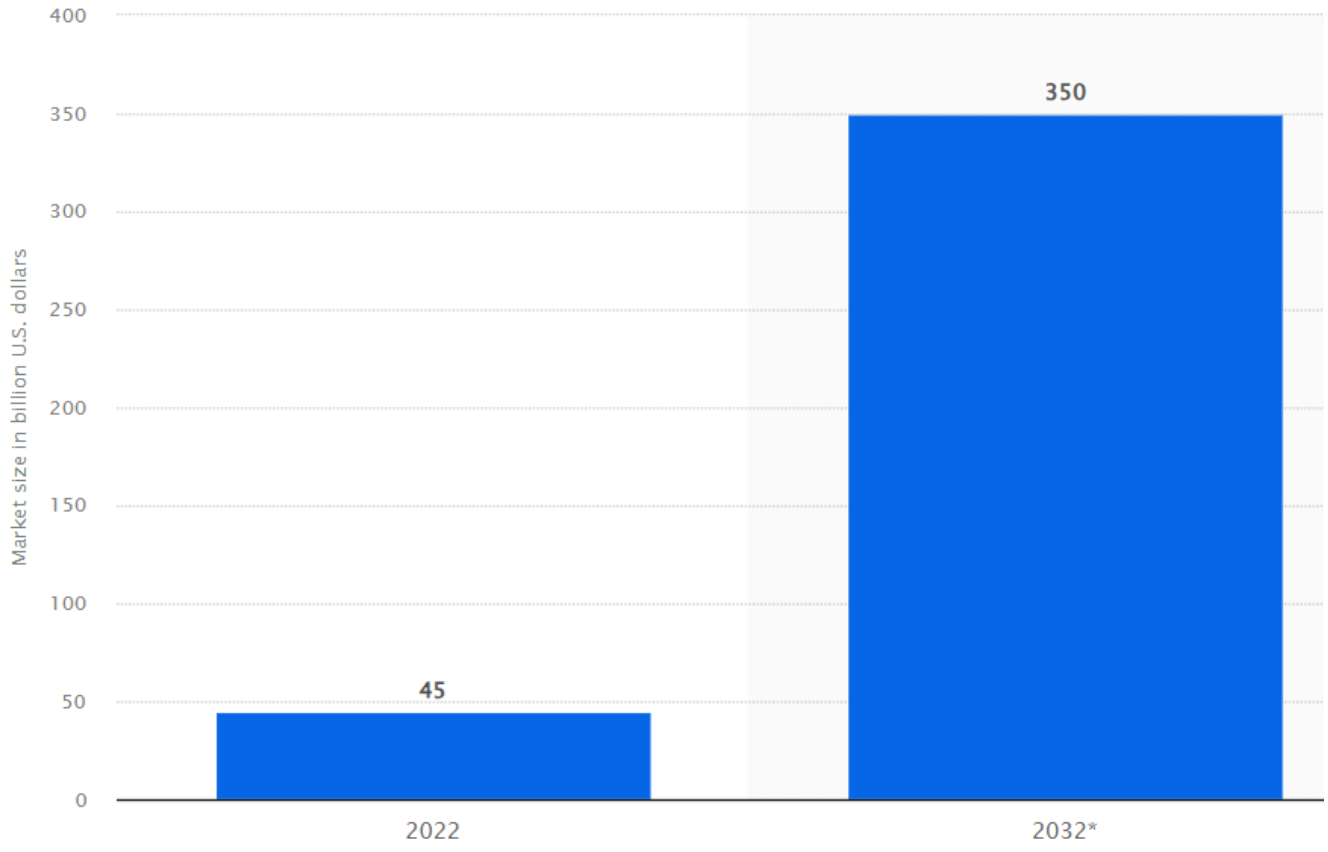


Рисунок 2.6 - Розмір світового ринку мереж VPN у 2022 році порівняно з 2032 роком

Однією з ключових переваг VPN є його здатність ефективно шифрувати весь мережевий трафік, що робить його важким для перехоплення та викрадення.

Використання високорівневих алгоритмів шифрування забезпечує конфіденційність та безпеку навіть у випадках обробки чутливої інформації або комерційної власності.

Статистика використання VPN поднано на рисунку 2.7.

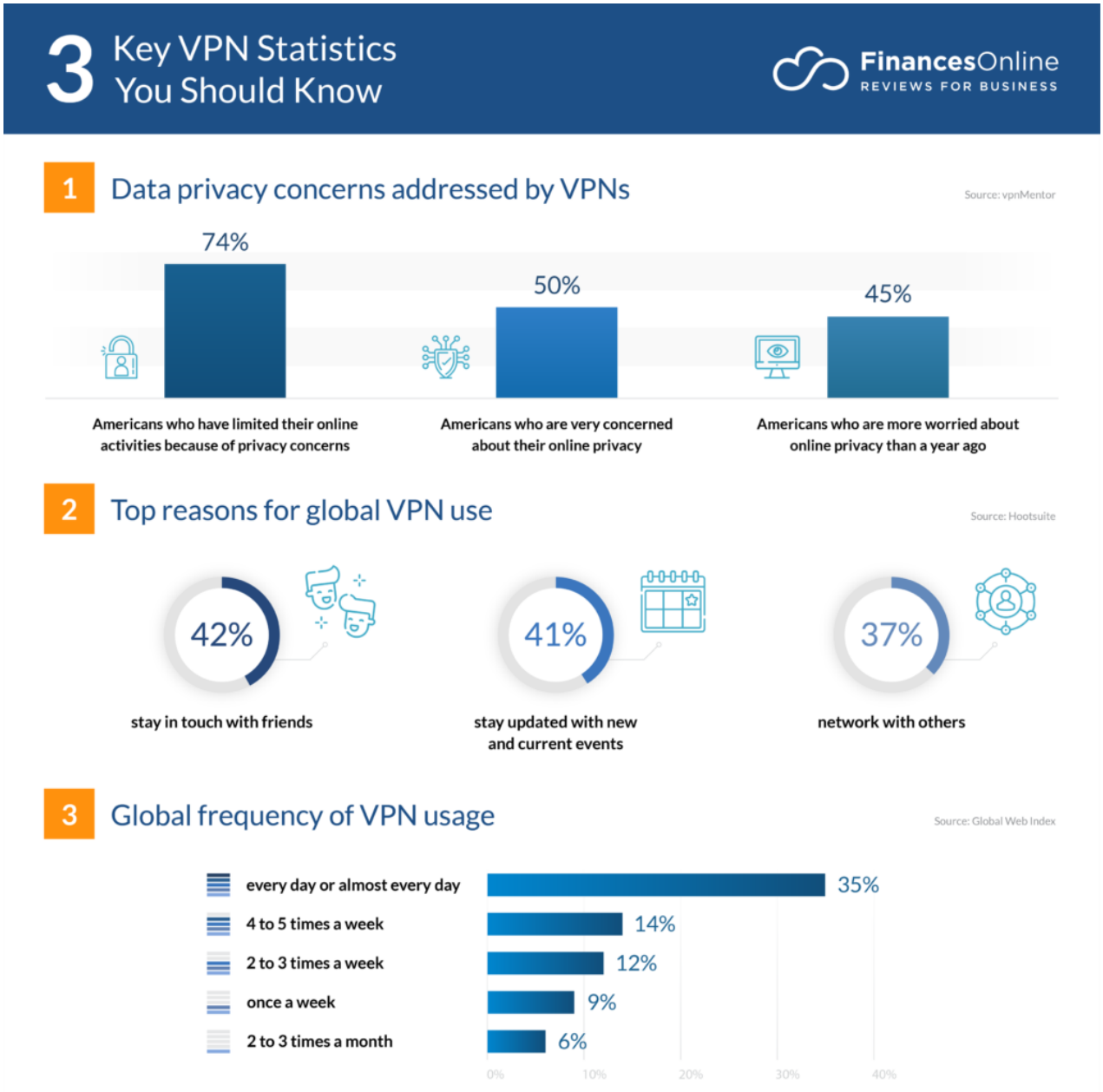


Рисунок 2.7 – Статистика використання VPN

2.5 Висновки

У ході дослідження було проведено аналіз переваг та недоліків трьох ключових сервісів: двофакторної аутентифікації (2FA), Azure Active Directory (Azure AD) та віртуальних приватних мереж (VPN).

В розділі приведено обгрунтування вибору 2FA як ефективного та легкозастосовного методу в інфраструктурі організації, здійснене на основі аналізу вказаних переваг кожного сервісу.

Двофакторна аутентифікація (2FA) забезпечує високий рівень безпеки, оскільки вимагає подвійної ідентифікації користувача.

При використанні двох або більше елементів, таких як пароль та додаткове підтвердження, навіть у випадку витоку одного елемента ідентифікації, доступ залишається практично неможливим для несанкціонованих осіб.

Важливою перевагою 2FA є його легкість впровадження, оскільки метод легко інтегрується в існуючі системи без значних труднощів та витрат на оновлення, що робить його привабливим вибором для швидкого підняття рівня безпеки.

2FA легко масштабується для великих корпоративних середовищ і може використовуватися для захисту доступу до різних рівнів систем та сервісів у великих організаціях.

3. ТЕХНОЛОГІЯ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ ЗАХИСТУ ДАНИХ ПРИ ОБРОБЦІ ТА ПЕРЕДАВАННІ В ІТ-ІНФРАСТРУКТУРІ ОРГАНІЗАЦІЇ

3.1 2FHA як сервіс

Двофакторна автентифікація (2FHA) - це захід безпеки, який вимагає від користувачів надання двох форм ідентифікації для доступу до облікового запису або системи.

Однією формою ідентифікації зазвичай є пароль, а іншою - унікальний, прив'язаний до часу одноразовий пароль (OTP), який генерується і надсилається на телефон користувача за допомогою SMS-повідомлення [60].

Двофакторна автентифікація (2FA) як послуга - це рішення безпеки, яке дозволяє компаніям додати додатковий рівень захисту до процесу автентифікації користувачів.

Зазвичай вона надається як хмарний сервіс і може бути інтегрована в існуючі системи та інфраструктуру організації [47].

За допомогою 2FA користувачі повинні надати дві форми ідентифікації при вході в систему або додаток: перша - це традиційна форма автентифікації, наприклад, пароль, а друга - унікальний, одноразовий код, згенерований пристроєм або сервісом, наприклад, мобільним додатком або текстовим повідомленням.

Крім того, механізм 2FHA може бути запропонований як послуга компаніям від компанії, основною послугою якої є створення множинних OTP для клієнтів (назвемо цю компанію «Factorization of Authentication: FofA»).

Компанії, які користуються послугами FofA, можна розділити на дві групи: до першої групи належать компанії, які мають власний механізм

2FA (система аутентифікації: TOTP-сервер і хешовані паролі), а до другої групи - компанії, які не мають жодної системи 2FA [28].

3.1.1 2FA з SMS-кодом

Двофакторна автентифікація на основі SMS-повідомлень (2FA) є найбільш поширеним механізмом 2FA, незважаючи на те, що SMS-повідомлення, як відомо, вразливі до атак перенаправлення, і незважаючи на наявність альтернатив, які можуть бути більш безпечними.

Це пов'язано з двома причинами:

1. По-перше, він дуже ефективний на практиці, про що свідчать звіти Google та Microsoft.
2. По-друге, користувачі віддають перевагу SMS, а не альтернативам, оскільки обмін текстовими повідомленнями вже є частиною їхнього щоденного спілкування [43].

Двофакторна аутентифікація з використанням СМС є ефективним методом захисту облікових записів та персональної інформації, який використовує два різних фактори для підтвердження ідентичності кінцевого користувача.

У цьому методі одним з факторів є звичайний пароль, а другим - одноразовий код, який користувач отримує через короткий текстовий повідомлення (СМС) на свій мобільний телефон [18].

Як працює двофакторна аутентифікація (2FA) з SMS:

1. Активація 2FA: користувач активує 2FA для свого облікового запису та обирає метод отримання одноразових кодів через СМС.
2. Реєстрація номеру телефону: користувач пов'язує свій номер телефону з обліковим записом.
3. Генерація одноразових кодів:

– при вході в систему або виконанні важливих операцій користувач вводить свій звичайний пароль;

– система генерує і відправляє користувачеві унікальний одноразовий код через СМС на зазначений номер телефону;

– введення одноразового коду: користувач вводить отриманий одноразовий код разом із своїм звичайним паролем;

– автентифікація та доступ: якщо введені дані вірні, користувач має доступ до свого облікового запису чи виконує запитану операцію;

– ахист від несанкціонованого доступу: в разі втрати чи небажаного доступу до мобільного телефону навіть знання пароля не дасть зловмиснику повного доступу до облікового запису без одноразового коду (див. рисунок 3.1) [6].

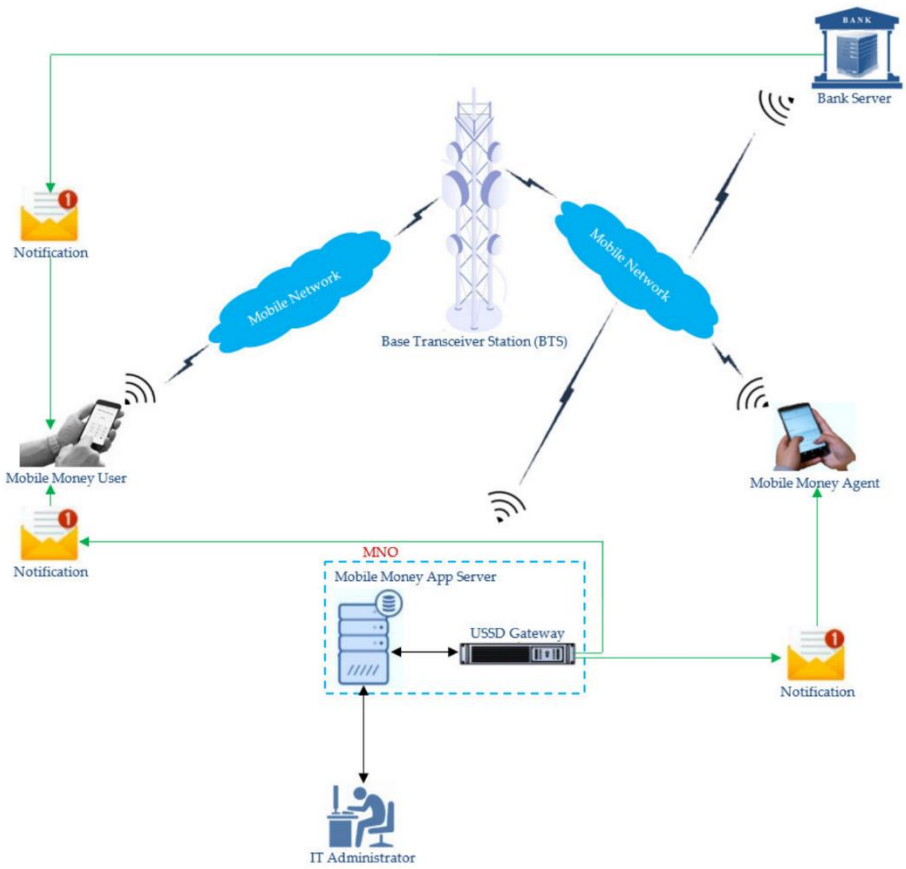


Рисунок 3.1 - Принцип роботи 2FA з SMS-кодом

Переваги 2FA з СМС:

1. Широкий застосунок: доступний для користувачів без використання спеціальних пристроїв чи додатків.

2. Доступність: майже кожен користувач має доступ до телефону, що робить цей метод доступним для широкого кола аудиторії.

3. Додатковий шар захисту: зменшує ризик несанкціонованого доступу, оскільки для вторинного підтвердження потрібно мати доступ до фізичного пристрою (телефону).

Недоліки 2FA з СМС::

1. Затримка у доставці: залежність від мережі та можливість затримки у доставці СМС може призвести до часових ускладнень.

2. Збір та використання даних: існує ризик перехоплення СМС або збору інформації з них.

3. Вартість для оператора: у деяких випадках вартість відправлення СМС може покладатися на оператора мобільного зв'язку чи користувача [23].

3.1.2 Статистика 2FA з SMS-кодом

У 2021 році 57,8% компаній використовували застосунки Authenticator Apps для багатофакторної автентифікації.

Водночас SMS-код і вторинна електронна пошта становили 39,1% і 14,7% використання MFA компаніями відповідно. 57,8% компаній використовували додатки-автентифікатори.

Методи для MFA подано в таблиці 3.1 [63].

3.1.3 2FA з Google Authenticator

Включення Google Authenticator, широко використовуваної технології двофакторної автентифікації, забезпечує додатковий рівень безпеки, що практично унеможливлює несанкціонований доступ [30].

Цей інтегрований метод простий у використанні навіть для людей, які не є технічно підкованими, і пропонує максимальний захист від основних загроз, таких як підміна SIM-карти, програми-сталкери та атаки з побічних каналів [28].

Таблиця 3.1 – таблиця методів для MFA

Multi-Factor Authentication Type	Share of Companies Using It
Authenticator application	57.8%
SMS code	39.1%
One Time Password (OTP)	37.4%
Hardware security key	30%
Secondary Email	14.7%
Other	7.3%

Як працює двофакторна аутентифікація (2FA) з Google Authenticator:

1. Активація 2FA. Користувач активує 2FA для свого облікового запису, зазвичай за допомогою мобільного додатку, такого як Google Authenticator. Під час активації генерується унікальний код або сканується QR-код.

2. QR-код і секретний ключ. QR-код містить інформацію, яка додається до додатку Google Authenticator. Також користувач отримує секретний ключ, який може бути введений вручну, якщо немає можливості сканувати QR-код.

3. Генерація одноразових паролів. Додаток Google Authenticator генерує одноразові шестизначні паролі (OTP), які змінюються кожні 30 секунд.

Ці OTP використовуються для вторинного підтвердження особи під час входу в систему або виконання важливих операцій.

4. Двофакторний вхід. Під час входу в систему, окрім стандартного пароля, користувач вводить поточний OTP, що генерується додатком.

5. Безпека та захист. 2FA додає значний рівень безпеки, оскільки навіть якщо зловмисник здобуде пароль, йому все одно потрібно мати фізичний доступ до мобільного пристрою для отримання поточного OTP.

6. Застосування в онлайн-сервісах. 2FA широко використовується в онлайн-сервісах, таких як електронні поштові скриньки, соціальні мережі, банківські системи і багато інших, для захисту особистої інформації користувачів.

Принцип роботи Google Authenticator [65] подано на рисунку 3.2.

Розглянемо переваги 2FA з Google Authenticator:

1. Високий рівень безпеки завдяки використанню факторів, які важко піддаються підробці.

2. Зручність та простота використання мобільного додатку.

3. Застосовується в різних сферах, забезпечуючи універсальний метод захисту.

3.1.4 Статистика 2FA з Google Authenticator

До кінця 2021 року Google автоматично зареєстрував 150 мільйонів користувачів у своїй системі перевірки безпеки з двофакторною автентифікацією.

Статистика двофакторної автентифікації за галузями: Станом на квітень 2023 року 158 компаній у всьому світі використовують Google Authenticator як інструмент двофакторної автентифікації.

Наразі частка ринку Google Authenticator становить 5,20%.

Найбільше його використовують у таких галузях, як штучний інтелект, машинне навчання та хмарні обчислення. Інші три галузі включають фінтех, охорону здоров'я та Інтернет речей [63].

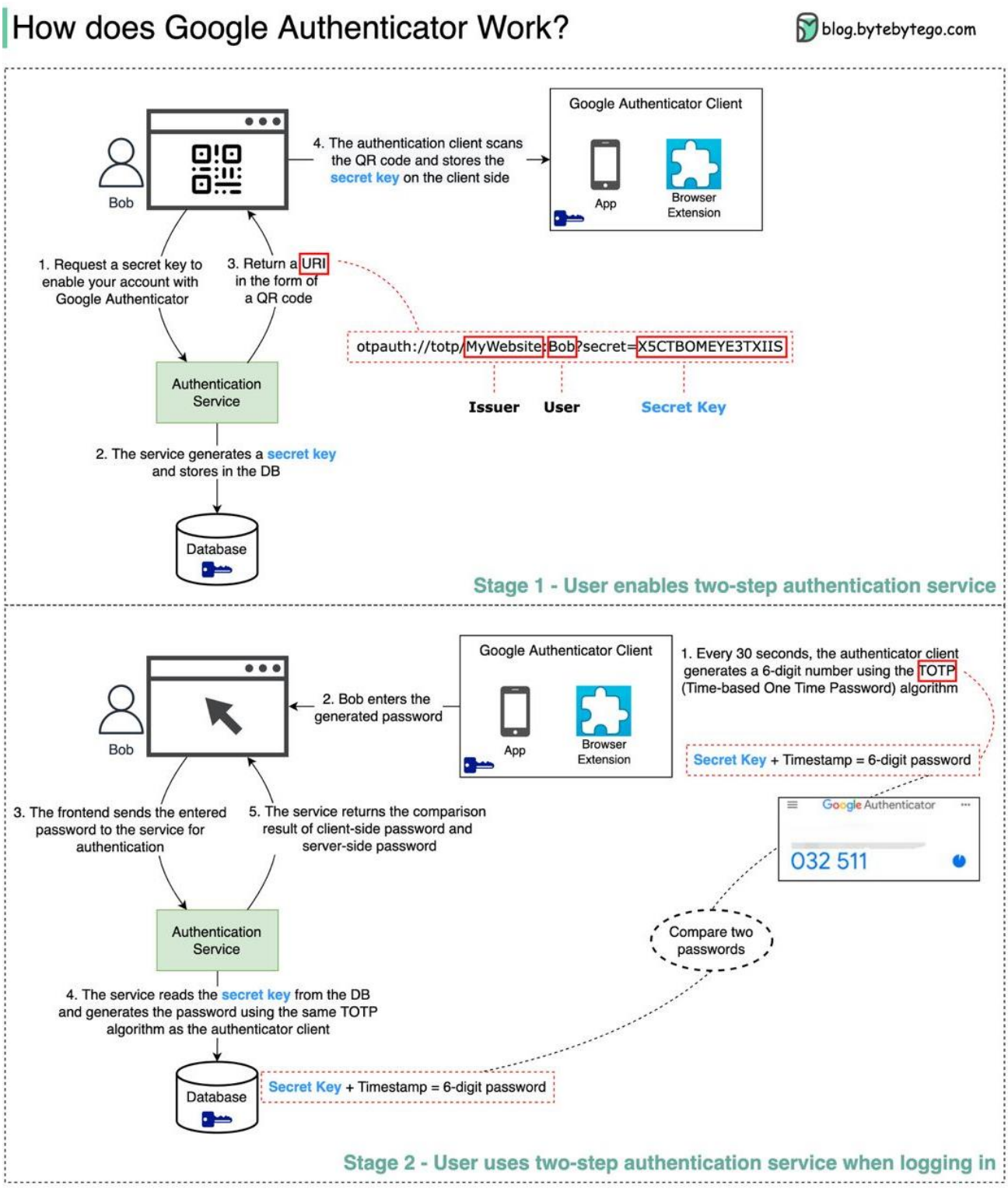


Рисунок 3.2 - Принцип роботи Google Authenticator [65]

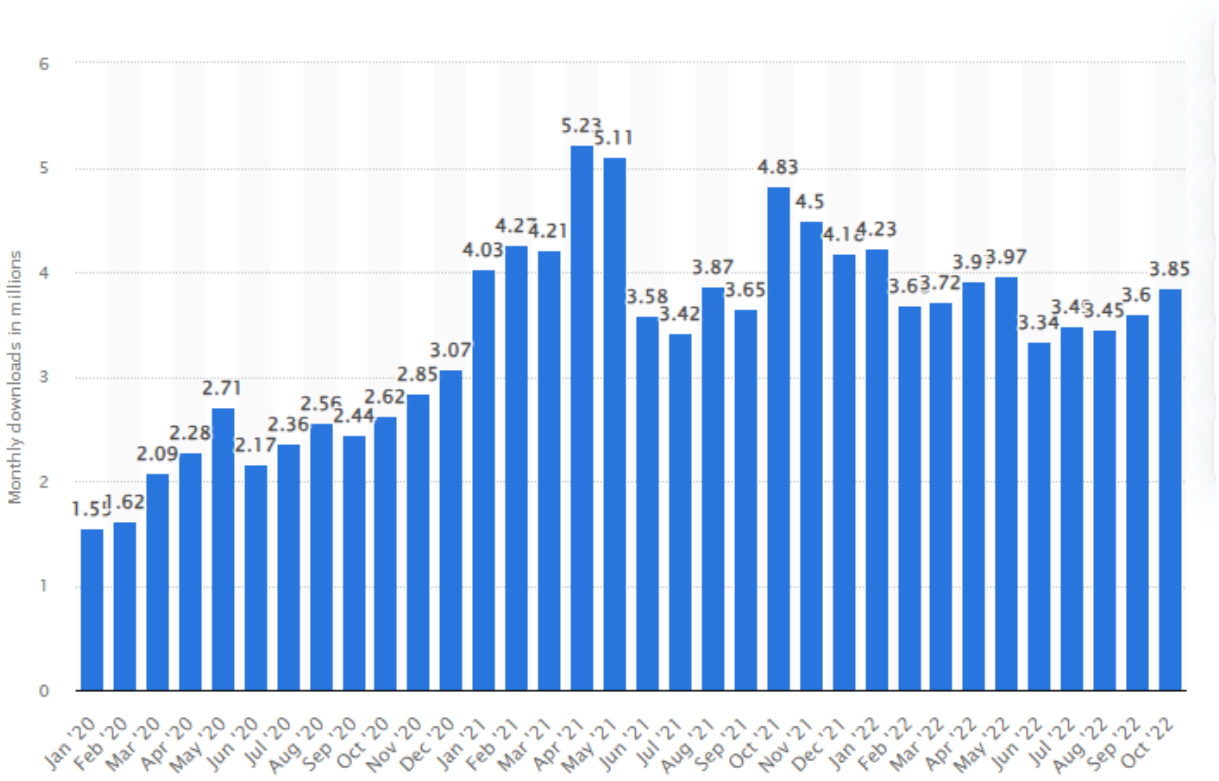


Рисунок. 3.3 - Щомісячне завантаження додатку Google Authenticator по всьому світу з січня 2020 року по жовтень 2022 року

3.2 Вибір сервісу двофакторної автентифікації для захисту даних при їх обробці та передаванні в IT-інфраструктурі організації

На основі отриманої інформації було обрано метод 2FA з Google Authenticator як найефективніший і найпростіший в імплементації в структуру IT-інфраструктурі організації сервіс для захисту даних при їх обробці та передаванні.

Обрання методу 2FA з Google Authenticator для захисту даних при обробці та передаванні в IT-інфраструктурі організації обгрунтоване наступним чином:

1. Високий рівень безпеки: Google Authenticator надає високий рівень безпеки завдяки використанню одноразових паролів (OTP), які генеруються кожні 30 секунд. Це робить систему важкою для атак, орієнтованих на отримання паролів.
2. Надійність та захист від атак: оскільки OTP змінюються кожні 30 секунд, а сам додаток зберігається на фізичному пристрої користувача, система стає стійкою до атак, таких як перенаправлення SIM-карти чи атаки з побічних каналів.
3. Зручність у використанні: Google Authenticator - простий та зручний для використання мобільний додаток. Користувачам легко активувати та імплементувати його в свої облікові записи.
4. Універсальність застосування: Google Authenticator широко використовується в різних сферах, таких як електронні поштові скриньки, соціальні мережі, банківські системи і багато інших. Це робить його універсальним методом захисту.
5. Простота імплементації: імплементація 2FA з Google Authenticator в структуру IT-інфраструктурі організації відносно проста та не вимагає значних витрат часу та ресурсів.
6. Відсутність залежності від мережі: використання Google Authenticator не залежить від мобільного зв'язку чи інтернет-підключення. Це робить його надійним у різних умовах роботи.

3.3 Аналіз ринку MFA

Світовий ринок багатофакторної автентифікації станом на 2023 рік зріс до 13 мільярдів.

Загальний ринок MFA зріс з низького рівня в $2,82 млрд у 2016 році до високого в 12,9 млрд у 2022 році.

Прогнозується, що ринок зросте до 26,7 мільярдів у 2027 році.

Дані щодо світового ринку багатофакторної автентифікації подано в таблиці 3.2.

Таблиця 3.2 – Світовий ринок багатофакторної автентифікації

Year	Global MFA Market Size, млрд
2016	$2.82
2017	$3.92
2018	$5.51
2019	$7.59
2020	$9.45
2021	$11.37
2022	$12.9

80% організацій у регіоні EMEA у 2022 році вже впровадили багатофакторну автентифікацію. У регіонах APAC та NA впровадження MFA склало 76% та 72% відповідно

Дані щодо впровадження багатофакторної автентифікаці подано в таблиці 3.3.

Таблиця 3.3 – Впровадження багатофакторної автентифікаці

Region	Implemented MFA	Implementing MFA in the Next 12 to 18 Months
APAC	76%	27%
EMEA	80%	25%
NA	72%	29%

У 2021 році 57,8% компаній використовували додатки Authenticator для багатофакторної автентифікації.

У той же час, SMS-код та вторинна електронна пошта становили 39,1% та 14,7% використання MFA компаніями відповідно. 57,8% компаній використовували додатки-автентифікатори

Дані щодо впровадження мультифакторної автентифікаці подано в таблиці 3.4.

Таблиця 3.4 – Впровадження мультифакторної автентифікаці

Multi-Factor Authentication Type	Share of Companies Using It
Authenticator application	57.8%
SMS code	39.1%
One Time Password (OTP)	37.4%
Hardware security key	30%
Secondary Email	14.7%
Other	7.3%

У табл. 3.5. відображено порівняльний аналіз між Google Authenticator та SMS-повідомленнями для 2FA.

Таблиця 3.5 – Порівняльний аналіз між Google Authenticator та SMS-повідомленнями для 2FA.

Критерії	Google Authenticator (2FA)	2FA на основі SMS-повідомлень
Надійність	Висока, оскільки коди генеруються локально на пристрої.	Низька, оскільки SMS може бути перехоплено або вкрадено.
Безпека	Висока, оскільки коди не відправляються через відкриті мережі.	Низька, оскільки SMS-повідомлення може бути перехоплене або викрадене.
Вартість	Безкоштовно, оскільки	Вартість пов'язана з вартістю SMS-

	Google Authenticator - безкоштовний.	повідомлень, що може бути високою для користувачів, які подорожують.

Кінець таблиці 3.5 – Порівняльний аналіз між Google Authenticator та SMS-повідомленнями для 2FA

Доступність	Потребує смартфон або планшет для генерації кодів.	Можливо використовувати з будь-яким телефоном, здатним приймати SMS.
Простота використання	Зручно використовувати, проте потрібно зберігати секретні ключі.	Простий процес, оскільки коди надсилаються через SMS. Проте, важливо не втрачати телефон або SIM-карту.
Підтримка без Інтернету	Працює без Інтернет-з'єднання під час генерації кодів.	Залежить від наявності Інтернет-з'єднання для отримання SMS.
Швидкість	Швидка генерація кодів без затримок на доставку повідомлень.	Залежить від роботи оператора та швидкості доставки SMS.
Можливість втрати доступу	Висока безпека, але втрата пристрою або секретного ключа може призвести до втрати доступу.	Ризик втрати доступу при втраті телефону або SIM-карти.

3.4 Висновки

З наведеної інформації випливає, що двофакторна автентифікація (2FA) на основі SMS-повідомлень широко використовується через свою ефективність та повсякденність для користувачів.

Цей метод забезпечує захист облікових записів за допомогою пароля та одноразового коду, який надходить через SMS на мобільний телефон.

Його перевагами є широкий застосунок, доступність для більшості користувачів та додатковий шар захисту.

З іншого боку, існують певні недоліки, такі як можливість затримок у доставці SMS та ризик перехоплення чи використання даних. Однак незважаючи на ці обмеження, 2FA з SMS залишається популярним вибором.

У порівнянні з 2FA з Google Authenticator, який використовує одноразові паролі, змінюються кожні 30 секунд, і додаток забезпечує високий рівень безпеки. Google Authenticator є простим у використанні, універсальним для різних сервісів та не залежить від мережі. Його вибір для захисту даних у IT- інфраструктурі організації обґрунтовується його надійністю, зручністю та високим рівнем безпеки.

4. РОЗРОБКА ТЕХНОЛОГІЇ 2FA ДЛЯ ЗАХИСТУ ДАНИХ ПРИ ЇХ ОБРОБЦІ ТА ПЕРЕДАВАННІ В ІТ-ІНФРАСТРУКТУРІ ОРГАНІЗАЦІЇ.

4.1 Інструменти і діаграми для системи 2FA

Після ретельного аналізу патернів проектування веб-додатків та огляду сучасних технологій розробки веб-додатків було прийнято рішення прийняти розгалужену архітектуру з реалізацією патерну проектування MVC.

На рівні інтерфейсу використовується HTML та Razor для простого представлення.

Для реалізації бізнес-логіки використовується MVC-фреймворк ASP.NET Core, який надає можливість створювати API з використанням шаблонів ASP.NET Core Web API.

На рівні доступу до даних було вирішено використовувати об'єктно-реляційне відображення, в якості системи управління базами даних обрано Microsoft SQL SERVER.

Діаграма послідовності (англ. Sequence Diagram) - це вид діаграми в моделюванні систем, що відображає взаємодії між об'єктами в рамках конкретного сценарію або викликів функцій у ході виконання програми або операційної діяльності. Цей графічний інструмент дозволяє відобразити порядок виконання різних об'єктів та їх взаємодію на протязі часу [50].

На основі діаграми можна викласти опис того, як працює послідовність процесу доступу до даних з двофакторною автентифікацією на основі подій:

1. Ініціювання запиту на вхід: User → Client: користувач починає процес, ініціюючи запит на вхід.

2. Передача запиту на автентифікацію: Client → AuthSystem: клієнт передає запит на систему автентифікації.

3. Перевірка інформації в БД: AuthSystem → Database: система автентифікації перевіряє інформацію в базі даних.

4. Передача результатів перевірки: Database → AuthSystem: База даних повертає результати перевірки системі автентифікації.

5. Надсилання запиту на додаткові фактори: AuthSystem → Client: якщо основна аутентифікація успішна, система автентифікації може вимагати додаткових факторів для підтвердження.

6. Запит на введення додаткових факторів: Client → User: клієнт передає запит на введення додаткових факторів користувачеві.

7. Надсилання додаткових факторів: User → Client: користувач надсилає додаткові фактори через клієнта.

8. Передача додаткових факторів для перевірки: Client → AuthSystem: клієнт передає додаткові фактори системі автентифікації для перевірки.

9. Перевірка додаткових факторів в БД: AuthSystem → Database: система автентифікації перевіряє додаткові фактори в базі даних.

10. Передача результатів перевірки додаткових факторів Database → AuthSystem: база даних повертає результати перевірки додаткових факторів системі автентифікації.

11. Надсилання результатів автентифікації: AuthSystem → Client: система автентифікації повертає результати автентифікації клієнту.

12. Повідомлення користувачеві: Client → User: клієнт повідомляє користувача про результати автентифікації.

Тепер зобразимо діаграму послідовності входу користувача в систему, рис. 4.1.

На основі діаграми послідовності входу користувача в систему можна викласти опис того, як працює процес аутентифікації користувача в систему:

1. Клієнт ініціює запит на вхід: клієнт ініціює процес аутентифікації, відправляючи запит на вхід до компонента "Авторизація".

2. Авторизація перевіряє підтвердження: компонент "Авторизація" взаємодіє з базою даних ("БД"), викликаючи метод "перевіритиПідтвердження()". База даних перевіряє наявність коректних облікових даних (логін, пароль) та повертає результати перевірки ("Результати перевірки") назад в компонент "Авторизація".

3. Авторизація перевіряє додаткові фактори: компонент "Авторизація" викликає метод "перевірити Додаткові Фактори()" у компонента "БАФ" (Безпека Авторизації Факторів). Компонент "БАФ" проводить перевірку додаткових аутентифікаційних факторів, таких як двофакторна автентифікація, та повертає результати ("Результати БАФ") у компонент "Авторизація".

4. Відповідь для Клієнта: компонент "Авторизація" формує HTTP відповідь, що містить результати проходження обох етапів аутентифікації. Ця відповідь передається назад клієнту.

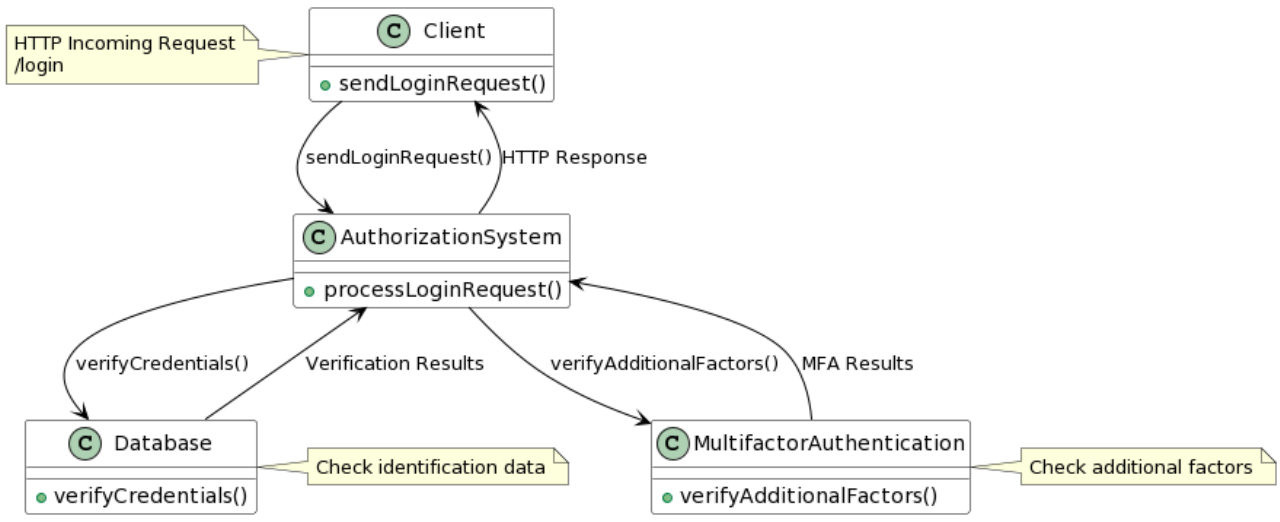


Рисунок 4.1- Послідовність процесу аутентифікації користувача в систему. Процес завершується, і клієнт отримує відповідь щодо свого запиту на вхід в систему.

У разі успішної аутентифікації йому надається доступ до ресурсів системи, в іншому випадку йому може бути відмовлено у доступі, рис. 4.2.

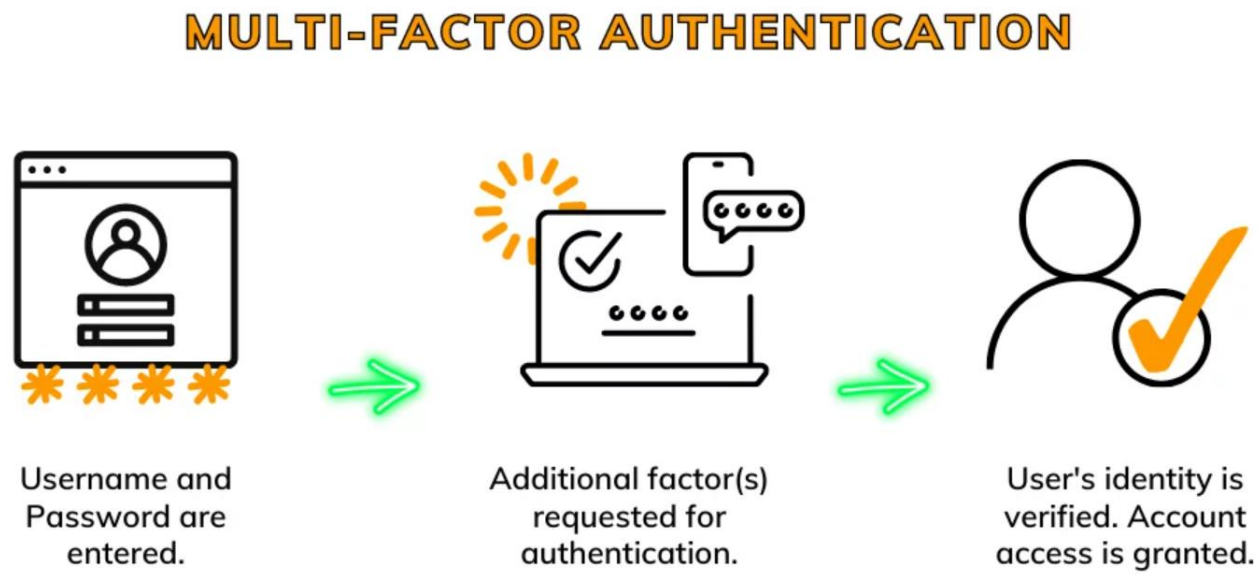


Рисунок 4.2 - Принцип роботи MFA

4.2 Опис функціонування проекту

Проект заснований на архітектурному шаблоні MVC (Model-View-Controller), що дозволяє розділити логіку додатку на три основні компоненти: модель, вид та контролер, а забезпечує доступ до даних – Entity Framework, котрий потрібно інтегрувати до проєкту.

Для забезпечення функціоналу двофакторної аутентифікації використовується NuGet-пакет Google Authenticator.

Цей пакет дозволяє імплементувати сервіс у проект та генерувати і перевіряти двофакторні коди згідно з алгоритмом, використовуваним Google Authenticator.

Основним файлом конфігурації додатку є Web.config, в якому вказані певні чутливі дані, які використовуються в роботі застосунку (такі як адреса підключеної бази даних, логін та пароль доступу до неї чи секретний ключ для підпису JWT-токенів).

В теці Controllers знаходяться контролери, які приймають ввід користувача і передають зміни до моделі. Сутності бази даних розміщені в теці Models, рис. 4.3.

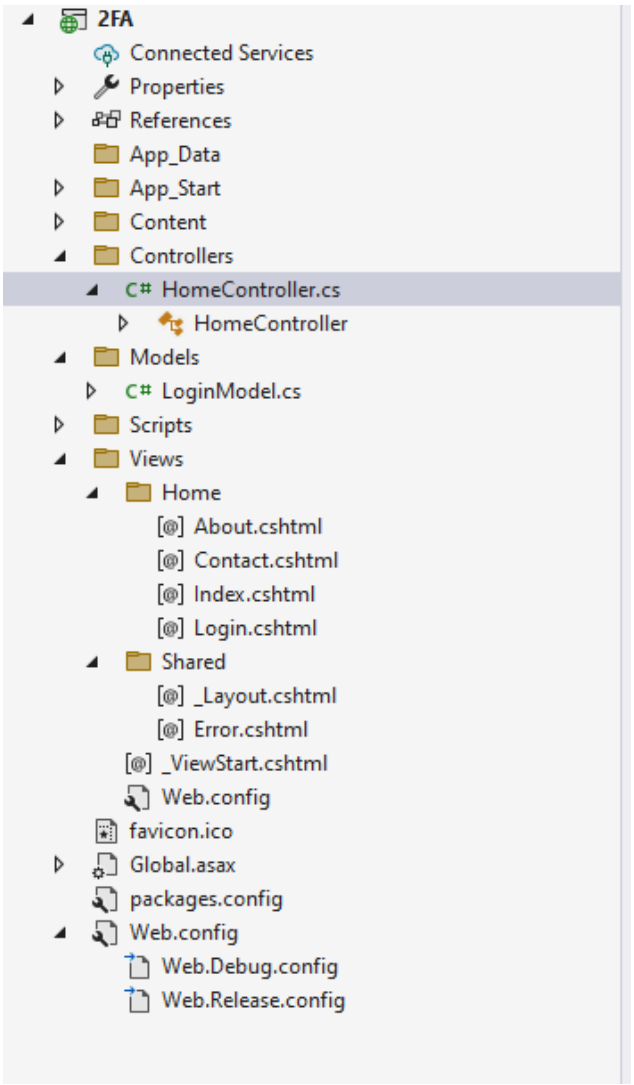


Рисунок 4.3 - Структура проєкту

4.3. Опис клієнтської частини проєкту

Клієнтська частина розробленої програми призначена виключно для демонстрації роботи сервісу багатофакторної автентифікації, тому в ній не реалізовані розширені функціональності для повноцінного використання веб-застосунку (локалізація, адаптивність, сучасний дизайн тощо).

Ця частина системи складається з односторінкового застосунку на AngularJS. У файловій структурі рівня сирцевого коду, так само як і в серверній частині, присутній файл зі наявними змінними оточення, package.json і Web.config.

Основний файл клієнтської частини - це app.js, в якому відбувається ініціалізація та створення основного компонента, в який будуть вставлятись інші.

Тека «content» буде містити використовувані стилі, «scripts» - модулі. Скрипт бібліотеки angular.min.js та всі інші необхідні скрипти підключаються безпосередньо в файлі index.html.

Контролери: HomeController: відповідає за обробку запитів для сторінок, таких як Index, About, Contact, Login, TwoFactorAuthenticate та Logoff.

Вигляд контроллера HomeController подано на рисунку 4.4.

LoginController: відповідає за обробку логіну користувачів, реєстрації та двофакторної аутентифікації.

Вигляд контроллера LoginController поднано на рисунку 4.5.

```
using _2FA.Models;
using Google.Authenticator;
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Web;
using System.Web.Configuration;
using System.Web.Mvc;
using System.Web.Security;

namespace _2FA.Controllers
{
    0 references
    public class HomeController : Controller
    {
        0 references
        public ActionResult Index()
        {
            if (Session["Username"] == null || Session["IsValidTwoFactorAuthentication"] == null || !(bool)Session["IsValidTwoFactorAuthentication"])
            {
                return RedirectToAction("Login");
            }
            return View();
        }

        0 references
        public ActionResult About()
        {
            if (Session["Username"] == null || Session["IsValidTwoFactorAuthentication"] == null || !(bool)Session["IsValidTwoFactorAuthentication"])
            {
                return RedirectToAction("Login");
            }

            ViewBag.Message = "Your application description page.";
            return View();
        }

        0 references
        public ActionResult Contact()
        {
```

Рисунок 4.4 - Вигляд контроллера HomeController

```
0 references
public ActionResult Login()
{
    Session["UserName"] = null;
    Session["IsValidTwoFactorAuthentication"] = null;
    return View();
}

[HttpPost]
0 references
public ActionResult Login(LoginModel login)
{
    bool status = false;

    if (Session["Username"] == null || Session["IsValidTwoFactorAuthentication"] == null || !(bool)Session["IsValidTwoFactorAuthentication"])
    {
        string googleAuthKey = WebConfigurationManager.AppSettings["GoogleAuthKey"];
        string UserUniqu                                              uthKey);
                          (local variable) string googleAuthKey

        //Take UserName And Password As Static - Marian As User And Pass As Password
        if (login.UserName == "Marian" && login.Password == "Pass")
        {
            Session["UserName"] = login.UserName;

            //Two Factor Authentication Setup
            TwoFactorAuthenticator TwoFacAuth = new TwoFactorAuthenticator();
            var setupInfo = TwoFacAuth.GenerateSetupCode("UdayDodiyaAuthDemo.com", login.UserName, ConvertSecretToBytes(UserUniqueKey, false), 300);
            Session["UserUniqueKey"] = UserUniqueKey;
            ViewBag.BarcodeImageUrl = setupInfo.QrCodeSetupImageUrl;
            ViewBag.SetupCode = setupInfo.ManualEntryKey;
            status = true;
        }
    }
    else
    {
        return RedirectToAction("Index");
    }
    ViewBag.Status = status;
    return View();
}
```

Рисунок 4.5 - Вигляд контроллера LoginController

Моделі: LoginModel: Модель для передачі даних форми логіну, яка містить властивості UserName та Password (рис. 4.6).

```
1   using System;
2   using System.Collections.Generic;
3   using System.Linq;
4   using System.Web;
5
6   namespace _2FA.Models
7   {
        3 references
8       public class LoginModel
9       {
            5 references
10          public string UserName { get; set; }
11
            2 references
12          public string Password { get; set; }
13      }
14  }
```

Рисунок 4.6 - Вигляд моделі LoginModel

Автентифікація:

1. При запуску проекту відображається перший фактор, логін та пароль, який потрібно ввести.

2. Після успішного входу генерується QR код та ключ, котрий треба ввести в додатку Google Authenticator, щоб той в свою чергу згенерував пароль для другого фактору, рис. 4.7.- 4.8.

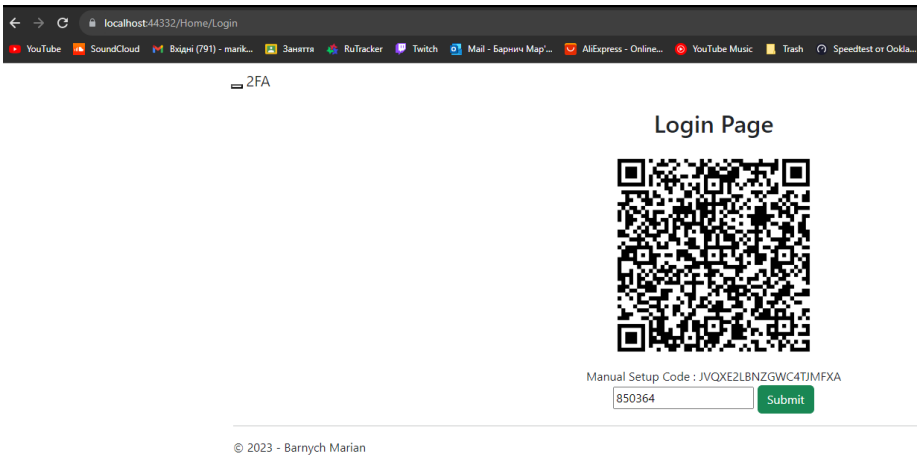


Рисунок 4.7 - Вигляд сторінки другого фактору

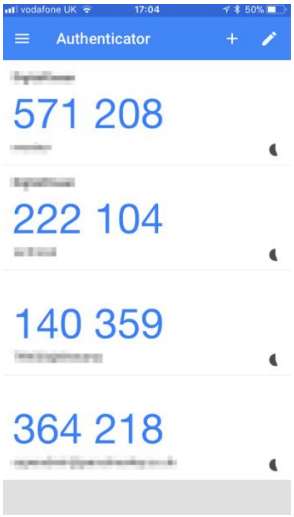


Рисунок 4.8 - Вигляд додатка Google Authenticator

4. Після введення паролю другого фактору, нас впускає на основну сторінку, де знаходяться потрібні нам дані (рис 4.9).
5. Сесії та вихід. Використовуються сесії для відстеження інформації про користувача, такої як ім'я користувача та стан двофакторної аутентифікації. Виходить з акаунта при використанні функції Logoff.

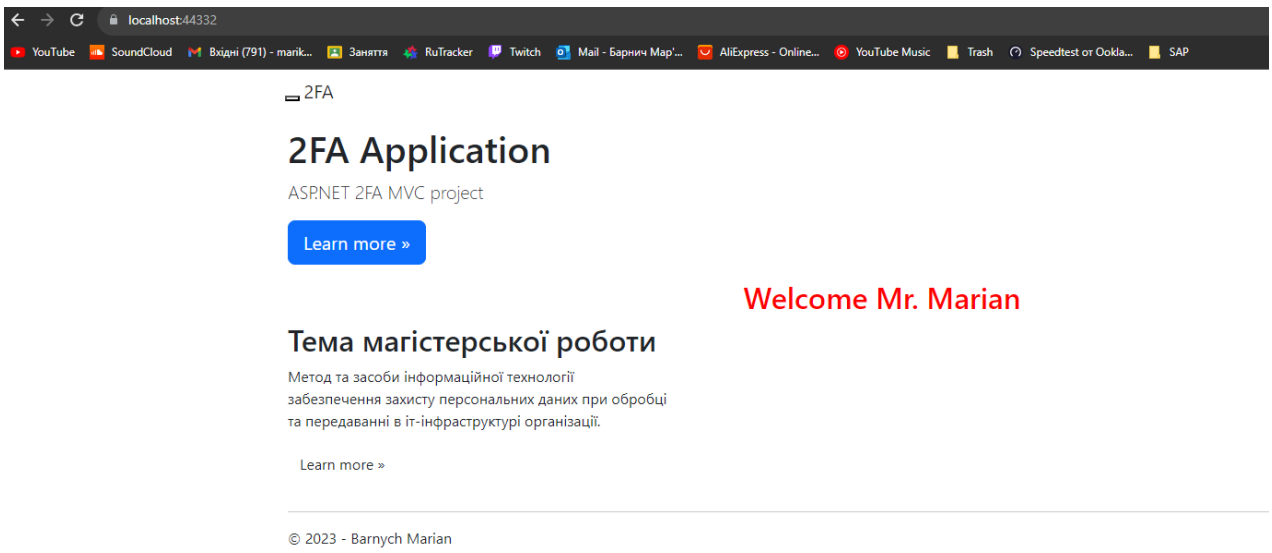


Рисунок 4.9 - Вигляд сторінки Index

4.4 Графічний інтерфейс

Додаток використовує HTML та Razor для відображення сторінок та форм.

Отже, проект на основі шаблону MVC використовує двофакторну аутентифікацію з допомогою Google Authenticator.

Користувачі вводять логін та пароль (перший фактор), а після успішного входу генерується QR-код та ключ для додатку Google Authenticator (другий фактор). Після введення коду користувач отримує доступ до системи.

Проект використовує сесії для відстеження інформації про користувача та надає можливість вийти з акаунта.

Графічний інтерфейс створений за допомогою HTML та Razor, рис. 4.10.

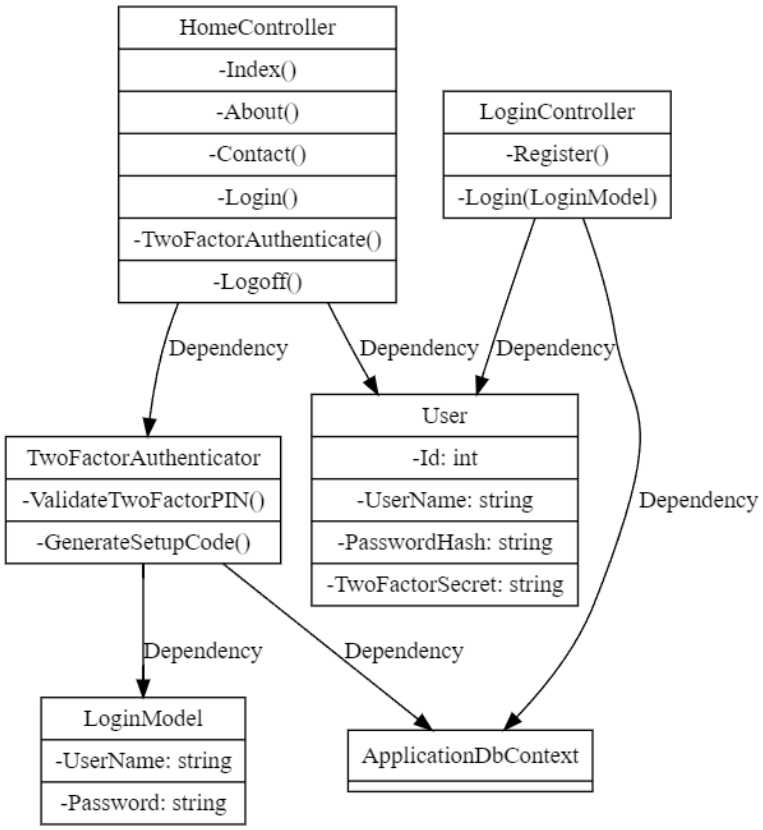


Рисунок 4.10 - Діаграма класів проекту

4.4 Оцінка ефективності двофакторної аутентифікації для захисту даних в IT-інфраструктурі організації

Ефективність проекту можна оцінити за кількома основними ознаками:

1. Складність взлому. Висока складність: використання двофакторної аутентифікації з Google Authenticator робить взлом системи складнішим. Крім того, використання сесій та інших заходів безпеки в MVC може зробити систему більш стійкою до атак.

2. Швидкість доступу. Висока швидкість: додавання двофакторної автентифікації трошки затримало процес входу, оскільки користувач повинен ввести код з додатку. Однак це невелика затримка в порівнянні з отриманою збільшеною безпекою(біля 7 секунд).

3. Зручність. Висока зручність: двофакторна автентифікація може створювати додаткові кроки, але Google Authenticator дозволяє швидко та зручно генерувати коди для входу.

Впровадження двофакторної автентифікації, зокрема за допомогою Google Authenticator та використання заходів безпеки в MVC, виявилось ефективним заходом для підвищення безпеки в IT-інфраструктурі організації. Складність взлому системи значно зростає завдяки використанню цього методу, що ускладнює завдання потенційним зловмисникам.

При цьому, затримка у швидкості доступу, є невеликою і займає біля 7 секунд додаткового часу.

Зручність для користувачів також забезпечується за рахунок швидкого та зручного генерування кодів за допомогою Google Authenticator.

Додаток є зручним, доступним на всіх мобільних платформах і зрозуміли в користуванні.

Такий комплекс заходів забезпечив би високий рівень захисту даних для організації, роблячи доступ до даних складним для несанкціонованих осіб і забезпечив надійність в управлінні інформацією.

4.5 Висновки

В розділі представлено опис проекту розробки технології двофакторної аутентифікації (2FA) для захисту даних в інформаційно-технологічній інфраструктурі організації. Здійснено аналіз патернів проектування веб-додатків та використано сучасні технології розробки веб-додатків.

Основна архітектура проекту ґрунтується на шаблоні Model-View-Controller (MVC), де HTML та Razor використовуються для подання інтерфейсу, а ASP.NET Core виступає фреймворком для бізнес-логіки. Для забезпечення функціоналу двофакторної аутентифікації використовується NuGet-пакет Google Authenticator.

Під час автентифікації використовується два фактори: спочатку вводиться логін та пароль, після чого генерується QR-код та ключ для додатку Google Authenticator, який використовується для генерації другого фактора. Проект забезпечує використання сесій для відстеження інформації про користувача та можливість вийти з акаунта.

Ефективність проекту оцінюється за такими критеріями, як складність взлому, швидкість доступу та зручність використання. Взлому системи ускладнено використанням 2FA, і система виявляється стійкою до атак. Затримка у швидкості доступу (близько 7 секунд) компенсується отриманою збільшеною безпекою. Зручність для користувачів

підтримується швидкістю та зручністю генерації кодів за допомогою Google Authenticator.

Отже, розроблена технологія 2FA на основі шаблону MVC з використанням Google Authenticator виявилася ефективною для підвищення рівня безпеки в інформаційно-технологічній інфраструктурі організації. Застосовані заходи ускладнюють взлом системи, забезпечуючи високий рівень захисту даних.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було досліджено проблематику захисту інформації в інформаційно-технологічних організаціях у сучасному світі. Основний акцент роботи був зроблений на аспектах обробки та передавання даних в цих організаціях.

У ході аналізу було розглянуто різноманітні стратегії та методи захисту інформації, такі як Zero Trust, Багатофакторна аутентифікація (MFA), Біометрична ідентифікація, а також враховано вимоги GDPR та використання Data Protection as a Service (DPaaS). Кожен метод був проаналізований з урахуванням його переваг та недоліків.

Висновки досліджень дозволили визначити, що впровадження методу двофакторної аутентифікації (2FA) з використанням Google Authenticator для IT-організацій є найбільш ефективним та простим у впровадженні в інформаційні системи. Вибір цього методу обумовлено його високою складністю взлому системи, швидкістю доступу для користувачів та загальною зручністю використання.

Створений проект, базований на обраному методі 2FA, успішно пройшов тестування та отримав позитивну оцінку щодо його ефективності. Результати свідчать про те, що впровадження обраного методу значно підвищило рівень безпеки інформації в організації, зменшивши ризик несанкціонованого доступу та підвищивши надійність у керуванні даними.

Отже, вибір методу 2FA виявився оптимальним кроком для забезпечення високого рівня безпеки та ефективності в інформаційно-технологічних організаціях.

Таким чином, висновок полягає в тому, що вибір методу 2FA виявився вдалим кроком у забезпеченні безпеки даних в інформаційно-технологічних організаціях.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Гнатчук Є.Г., Барнич М.Б. Метод та засоби інформаційної технології забезпечення захисту персональних даних при обробці та передаванні в іт-інфраструктурі організації. *V Міжнародна науково-практична конференція молодих вчених та студентів «Інженерія програмного забезпечення і передові інформаційні технології SoftTech-2023*. (19 грудня 2023 р.) (прийнято до друку).

2. Злепко С., Новіцький Г., Коваль Л., Крекотень Є. Методи і технології біометричної ідентифікації. *Вчені записки ТНУ імені В.І. Вернадського*. Серія: технічні науки, 2019. URL: https://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf (дата звернення: 12/12/2023).

3. Фронкевич М. Як DPaaS може допомогти захистити вашу компанію від атак розшифровки данних: Вичерпний посібник. *TS2 Space*: News, 2023. URL: https://ts2.space/uk/як-dpaas-може-допомогти-захистити-вашу-ком/#gsc.tab=0 (дата звернення: 14/12/2023).

5. Aggrawal, N. Authentication methods: A review. *Productivity*: Volume 52, 2012. URL: https://www.proquest.com/openview/9b68b79bb205d237f279e4c618ea74f0/1?pq-origsite=gscholar&cbl=506334 (дата звернення: 14/12/2023).

5. Ahmat M., Ates M., Fayolle J., Ravet S. An identity-centric internet: Identity in the cloud, identity as a service and other delights. *Sixth International Conference on Availability, Reliability and Security: IEEE*, 2011, pp. 555–560. URL:

https://www.researchgate.net/publication/221326733_An_Identity-Centric_Internet_Identity_in_the_Cloud_Identity_as_a_Service_and_Other_Delights (дата звернення: 14/12/2023).

6. Alsop A., Shechtman G., Strouble D. Productivity and Usability Effects of Using a Two-Factor Security System. *SAIS Proceedings*. URL:

https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1036&context=sais2009 (дата звернення: 14/12/2023).

7. Anand P. R., Bhaskar V., Indu I. Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal:* 2018. Volume 21, Issue 4. URL: https://www.sciencedirect.com/science/article/pii/S2215098617316750 (дата звернення: 14/12/2023).

8. Andonov S., Dimitrova V., Dobreva J., Lumburovska L., Mihajloska-Trpcheska H. A Comparative Analysis of HOTP and TOTP Authentication Algorithms. Which one to choose? *Cyril and Methodius University*: Faculty of Computer Science & Eng. Ss. 2021. URL: https://repository.ukim.mk/bitstream/20.500.12188/17185/1/confsec-2021-4-131%20A%20Comparative%20Analysis%20of%20HOTP%20and%20TOTP%20Authentication%20Algorithms.%20Which%20one%20to%20choose_.pdf (дата звернення: 14/12/2023).

9. Andreev S., Bezzateev S., Koucheryavy Y., Mäkitalo N., Mikkonen T., Ometov A. Multi-Factor Authentication: A Survey. *MDPI: Cryptography*, 2018. URL: https://www.mdpi.com/2410-387X/2/1/1 (дата звернення: 13/12/2023).

10. Athanasopoulos E., Ioannidis S., Petsas T., Tsirantonakis G. Two-factor authentication: is the world ready? *Proceedings of the Eighth European Workshop on System Security*, 2015.

URL: https://dl.acm.org/doi/abs/10.1145/2751323.2751327 (дата звернення: 14/12/2023).

11. Aravindhan K., Karthiga R. One-time Password: A Survey. *International Journal of Emerging Trends in Engineering and Development*: Volume 1, Issue 3, 2013.

URL: https://www.researchgate.net/profile/Aravindhan-Kurunthachalam/publication/344518837_One-

time_Password_A_Survey/links/5f7dd49592851c14bcb60412/One-time-Password-A-Survey.pdf (дата звернення: 15/12/2023).

12. Arch Linux, Google Authenticator. URL: https://wiki.archlinux.org/title/Google_Authenticator (дата звернення: 15/12/2023).

12. Arfelt E., Basin D., Debois S. Monitoring the GDPR. European Symposium on Research in Computer Security: *Computer Security,* 2019, pp 681–699. URL: https://link.springer.com/chapter/10.1007/978-3-030-29959-0_33 (дата звернення: 16/12/2023).

13. Arya K., Bhadoria R. The Biometric Computing: Recognition and Registration, 2019. URL:

https://www.google.pl/books/edition/The_Biometric_Computing/7Ui8DwAAQBAJ?hl=en&gbpv=1&dq=biometric+identification+systems&printsec=frontcover (дата звернення: 14/12/2023).

14. Bailey M., Barnes J., Egelman S., Judd T., Mason J., Reynolds J., Samarin N. Empirical Measurement of Systemic 2FA Usability. *29th Usenix Seciruty Symposium,* 2020. URL:

https://www.usenix.org/conference/usenixsecurity20/presentation/reynolds (дата звернення: 14/12/2023).

15. Barua K., Bhattacharya S., Mali K. Fingerprint Identification. *Global Journal of Computer Science & Technology:* Volume 11, 2011. URL: https://www.researchgate.net/profile/Dr-Mali/publication/229026251_Fingerprint_Identification/links/551bd7430cf20d5fbde21784/Fingerprint-Identification.pdfs (дата звернення: 17/12/2023).

16. Beacham, J. Is your practice GDPR ready*? In Practice*: 40(3), pp 124–125, 2018. URL: https://bvajournals.onlinelibrary.wiley.com/doi/abs/10.1136/inp.k1281 (дата звернення: 17/12/2023).

17. Borchert O., Connelly S., Mitchell S., Rose S. Zero Trust Architecture. *National Institute of Standards and Technology*, U.S. Department of Commerce, 2020. URL: https://doi.org/10.6028/nist.sp.800-207 (дата звернення: 16/12/2023).

18. Braz C., Jean-Marc R. Security and Usability: The Case of the User Authentication Methods, in IHM. Conference*: Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine*, Montreal, Quebec, Canada. URL: https://www.researchgate.net/publication/220745779_Security_and_usability_the_case_of_the_user_authentication_methods (дата звернення: 17/12/2023).

19. Burt J. Multi-factor auth fatigue is real – and it's why you may be in the headlines next. *The register: Security*, 2021. URL: https://www.theregister.com/2022/11/03/mfa_fatigue_enterprise_threat/ (дата звернення: 14/12/2023).

20. Cao L., Ge W. Analysis and improvement of a multi-factor biometric authentication scheme: Analysis and improvement of a MFBA scheme. *Security and Communication Networks*: Volume 8, Issue 4, 2015, pp 617–625. URL: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1010.

21. Cheng H., Han C., Fan K., Lin C. Personal authentication using palm-print features. Pattern Recognition: Volume 36, Issue 2, 2013. URL: https://www.sciencedirect.com/science/article/abs/pii/S0031320302000377 (дата звернення: 15/12/2023).

22. Chen Y., Liu H., Liu J., Wang C., Wang Y. User authentication on mobile devices: Approaches, threats and trends. *Computer Networks*: Volume 170, 2020. URL: https://doi.org/10.1016/j.comnet.2020.107118 (дата звернення: 14/12/2023).

23. Choyi V., Shah Y., Subramanian L. Multi-factor authentication as a Service. *3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering*, 2015. URL:

https://www.researchgate.net/publication/314087191_Multi-factor_Authentication_as_a_Service (дата звернення: 17/12/2023).

24. Dasgupta D., Roy A., Nag, A. Advances in User Authentication. *Springer:* Cham, Switzerland, 2017. URL: https://link.springer.com/book/10.1007/978-3-319-58808-7 (дата звернення: 15/12/2023).

25. Dasua K., Mangi K. A Novel System for Cloud Data Storage & Data Protection in Cloud Through Encryption. *International Journal of Scientific Engineering and Technology Research*: Volume 4, Issue 39, 2015. URL: https://ijsetr.com/uploads/264153IJSETR7149-1450.pdf (дата звернення: 17/12/2023).

26. Dhange M., Ghorpade V., Rajani S. Multi-factor authentication as a Service for Cloud Data Security. *International Journal of Computer Sciences and Engineering:* Volume 4, 2016. URL: https://www.researchgate.net/publication/313647475_Multi-factor_Authentication_as_a_Service_for_Cloud_Data_Security (дата звернення: 15/12/2023).

27. Dmitrienko A., Liebchen C., Rossow C., Sadeghi A. On the (In)Security of Mobile Two-Factor Authentication. *International Conference on Financial Cryptography and Data Security*, 2014, pp 365-383. URL: https://link.springer.com/chapter/10.1007/978-3-662-45472-5_24 (дата звернення: 14/12/2023).

28. Douligeris C., Ferrag A., Janicke H., Papaspirou V., Papathanasaki M., Maglaras L., Kantzavelou I. A Novel Authentication Method That Combines Honeytokens and Google Authenticator. *Design Automation, Computer Engineering, Computer Networks and Social Media Conference*: Information, 2022. URL: https://www.mdpi.com/2078-2489/14/7/386 (дата звернення: 16/12/2023).

29. Douligeris C., Ferrag M., Janicke H., Papaspirou V., Papathanasaki M., Maglaras L., Kantzavelou I. Security Revisited: Honeytokens meet Google Authenticator. *7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference* 2022. URL: https://ieeexplore.ieee.org/abstract/document/9932907 (дата звернення: 11/12/2023).

30. Farik M., Sharma N. Security Gaps in Authentication Factor Credentials. *International Journal of Scientific & Technology Research:* Volume 5, Issue 11, 2016. URL: https://www.researchgate.net/publication/311513572_Security_Gaps_In_Authentication_Factor_Credentials (дата звернення: 14/12/2023).

31. Fischer-Hellmann K.-P., Fuhrmann W., Furnell S., Vo T. H. Identityas-a-service: An adaptive security infrastructure and privacy-preserving user identity for the cloud environment. *Future Internet:* Volume 11, Issue 5, p. 116, 2019. URL: https://www.mdpi.com/1999-5903/11/5/116 (дата звернення: 15/12/2023).

32. Fischer-Hellmann K.-P., Fuhrmann W., Vo T. H. How to adapt authentication and authorization infrastructure of applications for the cloud. *IEEE 5th International Conference on Future Internet of Things and Cloud,* 2017. URL: https://www.researchgate.net/publication/321160178_How_to_Adapt_Authentication_and_Authorization_Infrastructure_of_Applications_for_the_Cloud (дата звернення: 12/12/2023).

33. Furman S., Spickard Prettyman S., Stanton B., Theofanos M. F. Security Fatigue. *IT Professional*: Volume 11, Issue 5, 2016. URL: https://doi.org/10.1109/MITP.2016.84 (дата звернення: 14/12/2023).

34. Gadescu H., O'Neil S., Slyman M., Van Der Merwe B. An evaluation of hypothetical attacks against the PassWindow authentication method. *PassWindow White Paper*, 2014. URL:

https://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.pdf (дата звернення: 13/12/2023).

35. Gilliland, K., Matthews, G. The personality theories of H.J. Eysenck and J.A. Gray: A comparative review. *Personality and Individual Differences:* Volume 26, Issue 4, 1999, pp 583-626. URL: https://doi.org/10.1016/S0191-8869(98)00158-5 (дата звернення: 14/12/2023).

36. He W., Li H., Yu L. The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management:* Volume 22, Issue 1, pp 1-6, 2019. URL: https://doi.org/10.1080/1097198X.2019.1569186 (дата звернення: 14512/2023).

37. Hwang T., Lin C.-L. A password authentication scheme with secure password updating. *Computers & Security*: Volume 22, Issue 1, pp. 68–72, 2003. URL: https://www.sciencedirect.com/science/article/abs/pii/S0167404803001147 (дата звернення: 14/12/2023).

38. Jacomme, C., Kremer, S. An Extensive Formal Analysis of Multi-factor Authentication Protocols. ACM Transactions on Privacy and Security. New York City: *Association for Computing Machinery*, pp 1–34, 2021. URL: https://dl.acm.org/doi/10.1145/3440712 (дата звернення: 13/12/2023).

39. Jaswal G., Kaul A., Nath R. Advances in Unconstrained Handprint Biometrics. *The Biometric Computing*: Part 1, 2019. URL: https://www.google.pl/books/edition/The_Biometric_Computing/7Ui8DwAAQBAJ?hl=en&gbpv=1&dq=biometric+identification+systems&printsec=frontcover (дата звернення: 14/12/2023).

40. Jeberson Retna Raj R., Malathi R. An integrated approach of physical biometric authentication system. *Procedia Computer Science*: Volume 85, 2016. URL:

https://www.sciencedirect.com/science/article/pii/S1877050916306214 (дата звернення: 11/12/2023).

41. Jonsson K., Kittler J., Matas K., Ramos Sánchez M. U. Combining evidence in personal identity verification systems. *Pattern Recognition Letters*: Volume 18, Issue 9, 1997. URL: https://doi.org/10.1016/S0167-8655(97)00062-7.

42. Kaiser T., Siddiqua R., Hasan M. A multi-layer security system for data access control, authentication, and authorization. *Department of Computer Science and Engineering*. Brac University, 2022. URL: https://dspace.bracu.ac.bd/xmlui/handle/10361/17566 (дата звернення: 11/12/2023).

43. Olszewski D., Munyaka Imani N., Patton C., Peeters C., Traynor P., Shrimpton T. SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication. *Asia Conference on Computer and Communications Security*, 2022. URL: https://dl.acm.org/doi/abs/10.1145/3488932.3497756 (дата звернення: 11/12/2023).

44. Orhanou G., Tachihante T., Tebaa M., Zkik K. A new authentication and homomorphic encryption as a service model for preserving privacy in clouds. *Journal of Computer Science*: Volume 13, Issue 12, 2017. URL: https://www.researchgate.net/publication/322447029_A_new_authentication_and_homomorphic_encryption_as_a_service_model_for_preserving_privacy_in_clouds (дата звернення: 12/12/2023).

45. Plata I. Application of Time-Based One Time Password (TOTP) Algorithm For Human Resource E-Leave Tracking Web App. *International Journal of Scientific & Technology Research*: Volume 9, Issue 3, 2020. URL: https://www.researchgate.net/profile/Irma-Plata-2/publication/341980938_Application_Of_Time-Based_One_Time_Password_TOTP_Algorithm_For_Human_Resource_E-

Leave_Tracking_Web_App/links/5edc276445851529453faae1/Application-Of-Time-Based-One-Time-Password-TOTP-Algorithm-For-Human-Resource-E-Leave-Tracking-Web-App.pdf (дата звернення: 14/12/2023).

46. Leandros L., Kantzavelou I. Cybersecurity Issues in Emerging Technologies. *CRC Press*: Boca Raton, FL, USA, 2021. URL: https://books.google.pl/books?hl=en&lr=&id=QiRAEAAAQBAJ&oi=fnd&pg=PP1&ots=KyteG4lerB&sig=r9zD6DJ6CqIqCBpKyMaYvoKsgpM&redir_esc=y#v=onepage&q&f=false (дата звернення: 17/12/2023).

47. Lee H.-J., Lee S., Lim H.-T., Ong I. Two factor authentication for cloud computing. *Journal of information and communication convergence engineering:* Volume 8, Issue 4, pp. 427–432, 2010. URL: https://ocean.kisti.re.kr/downfile/volume/kimics/E1ICAW/2010/v8n4/E1ICAW_2010_v8n4_427.pdf (дата звернення: 15/12/2023).

48. Liu D., Liu Q., Shen J., Sun X., Zhang Y. Secure authentication in cloud big data with hierarchical attribute authorization structure. *IEEE Transactions on Big Data*: Volume 7, Issue 4, 2017. URL: https://ieeexplore.ieee.org/document/7930440 (дата звернення: 10/12/2023).

49. Luis-García R., Alberola-López C., Aghzout O., Ruiz-Alzola J. Biometric identification systems. *Signal Processing*: Volume 83, Issue 12, 2003. URL: https://doi.org/10.1016/j.sigpro.2003.08.001 (дата звернення: 15/12/2023).

50. Mahnken S. Today's authentication options: The need for adaptive multifactor authentication. *Biometric Technology Today:* Volume. 2014, Issue 7, 2014. URL: https://www.sciencedirect.com/science/article/abs/pii/S0969476514701262?via%3Dihub (дата звернення: 14/12/2023).

51. Mehfuz S., R. Rai, Sahoo G. Securing software as a service model of cloud computing: Issues and solutions. *International Journal on Cloud Computing Services and Architecture:* Volume 3, Isuue 4, 2013. URL:

https://www.researchgate.net/publication/256476904_Securing_Software_as_a_Service_Model_of_Cloud_Computing_Issues_and_Solutions (дата звернення: 14/12/2023).

52. Microsoft Authenticator. URL: https://golden.com/wiki/Microsoft_Authenticator-3VW3DR5 (дата звернення: 02/12/2023).

53. Moniz H. Azure Active Directory and identity management. *Skillzcafe*: retrieved 15.12.2023. URL: https://www.skillzcafe.com/blog/microsoft/azure/azure-active-directory-and-identity-management (дата звернення: 14/12/2023).

54. M'Raihi D., Machani S., Pei M., Rydell J. TOTP: Time-Based One-Time Password Algorithm. *RFC Editor*, 2011. URL: https://www.rfc-editor.org/info/rfc6238; Enscript Output URL: https://www.rfc-editor.org/rfc/pdfrfc/rfc6238.txt.pdf (дата звернення: 06/12/2023).

55. Simon R., Zurko M. User-Centered Security. *The Pen Group Research Institute*, Cambridge, 1997. URL: https://www.nspw.org/papers/1996/nspw1996-zurko.pdf (дата звернення: 15/12/2023).

56. Smith R. Authentication: From Passwords to Public Keys. *Addison-Wesley* 2002, 1st edition (US). URL: https://archive.org/details/authenticationfr0000smit (дата звернення: 13/12/2023).

57. Sun Y., Zhang J., Zhu G., Xiong Y. Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*: Volume. 10, Issue 7, 2014. URL: https://www.researchgate.net/publication/274230804_Data_Security_and_Privacy_in_Cloud_Computing (дата звернення: 15/12/2023).

58. Tankard C. What the GDPR means for businesses. *Network Security:* Issue 6, 2016, Pages 5-8. URL:

https://www.sciencedirect.com/science/article/abs/pii/S1353485816300563 (дата звернення: 11/12/2023).

59. Veeraragavan N., Design and implementation of authentication as a service (aaas) in windows azure cloud platform. *Journal of Physics*: Conference Series: IOP Publishing, Volume 1142, 2018. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1142/1/012016 (дата звернення: 12/12/2023).

60. Wang D., Wang P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. *IEEE Transactions on Dependable and Secure Computing*: Volume 15, Issue: 4, 2018. URL: https://ieeexplore.ieee.org/document/7558124 (дата звернення: 14/12/2023).

61. ZIPPIA RESEARCH. URL: https://www.zippia.com/advice/mfa-statistics/ (дата звернення: 15/12/2023).

62. Bonderud D. Two-factor authentication (2FA) statistics. *Persona.* URL: https://withpersona.com/blog/two-factor-authentication-statistics (дата звернення: 15/12/2023).

65. Joan Telo. A Comparative Analysis of Network Security Technologies for Small and Large Enterprises. URL: https://research.tensorgate.org/index.php/IJBIBDA/article/view/14/13

66. Size of the virtual private network (VPN) market worldwide from in 2022 versus 2032. Statista. URL: https://www.statista.com/statistics/542817/worldwide-virtual-private-network-market/

67. 75 Key VPN Statistics: 2023 Analysis of Trends, Data and Market Share. FinancesOnline. URL:

https://financesonline.com/30-key-vpn-statistics-2019-analysis-of-trends-data-and-market-share.

ДОДАТОК А. ЛІСТИНГ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ТЕХНОЛОГІЇ АВТЕНТИФІКАЦІЇ МЕТОДОМ 2FA

```
using _2FA.Models;
using Google.Authenticator;
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.Web;
using System.Web.Configuration;
using System.Web.Mvc;
using System.Web.Security;

namespace _2FA.Controllers
{
   public class HomeController : Controller
   {
      public ActionResult Index()
      {
         if (Session["Username"] == null || Session["IsValidTwoFactorAuthentication"] == null
|| !(bool)Session["IsValidTwoFactorAuthentication"])
         {
            return RedirectToAction("Login");
         }
         return View();
      }

      public ActionResult About()
      {
         if (Session["Username"] == null || Session["IsValidTwoFactorAuthentication"] == null
|| !(bool)Session["IsValidTwoFactorAuthentication"])
         {
            return RedirectToAction("Login");
         }

         ViewBag.Message = "Your application description page.";
         return View();
      }

      public ActionResult Contact()
      {
         if (Session["Username"] == null || Session["IsValidTwoFactorAuthentication"] == null
|| !(bool)Session["IsValidTwoFactorAuthentication"])
         {
            return RedirectToAction("Login");
```

```
        }

        ViewBag.Message = "Your contact page.";
        return View();
    }

    public ActionResult Login()
    {
        Session["UserName"] = null;
        Session["IsValidTwoFactorAuthentication"] = null;
        return View();
    }

    [HttpPost]
    public ActionResult Login(LoginModel login)
    {
        bool status = false;

        if (Session["Username"] == null || Session["IsValidTwoFactorAuthentication"] == null
|| !(bool)Session["IsValidTwoFactorAuthentication"])
        {
            string googleAuthKey = WebConfigurationManager.AppSettings["GoogleAuthKey"];
            string UserUniqueKey = (login.UserName + googleAuthKey);

            //Take UserName And Password As Static - Marian As User And Pass As Password
            if (login.UserName == "Marian" && login.Password == "Pass")
            {
                Session["UserName"] = login.UserName;

                //Two Factor Authentication Setup
                TwoFactorAuthenticator TwoFacAuth = new TwoFactorAuthenticator();
                var setupInfo = TwoFacAuth.GenerateSetupCode("UdayDodiyaAuthDemo.com",
login.UserName, ConvertSecretToBytes(UserUniqueKey, false), 300);
                Session["UserUniqueKey"] = UserUniqueKey;
                ViewBag.BarcodeImageUrl = setupInfo.QrCodeSetupImageUrl;
                ViewBag.SetupCode = setupInfo.ManualEntryKey;
                status = true;
            }
        }
        else
        {
            return RedirectToAction("Index");
        }
        ViewBag.Status = status;
        return View();
    }
```

```
        private static byte[] ConvertSecretToBytes(string secret, bool secretIsBase32) =>
          secretIsBase32 ? Base32Encoding.ToBytes(secret) : Encoding.UTF8.GetBytes(secret);

        public ActionResult TwoFactorAuthenticate()
        {
            var token = Request["CodeDigit"];
            TwoFactorAuthenticator TwoFacAuth = new TwoFactorAuthenticator();
            string UserUniqueKey = Session["UserUniqueKey"].ToString();
            bool isValid = TwoFacAuth.ValidateTwoFactorPIN(UserUniqueKey, token, false);
            if (isValid)
            {
                HttpCookie TwoFCookie = new HttpCookie("TwoFCookie");
                string UserCode =
Convert.ToBase64String(MachineKey.Protect(Encoding.UTF8.GetBytes(UserUniqueKey)));

                Session["IsValidTwoFactorAuthentication"] = true;
                return RedirectToAction("Index");
            }

            ViewBag.Message = "Google Two Factor PIN is expired or wrong";
            return RedirectToAction("Login");
        }

        public ActionResult Logoff()
        {
            Session["UserName"] = null;
            Session["IsValidTwoFactorAuthentication"] = null;
            return RedirectToAction("Login");
        }


    }
}

using System;

using System.Collections.Generic;

using System.Linq;

using System.Web;


namespace _2FA.Models

{

    public class LoginModel
```

```
    {
        public string UserName { get; set; }

        public string Password { get; set; }
    }
}
@model _2FA.Models.LoginModel
@{
    ViewBag.Title = "Login";
}

<center>
    <h2>Login Page</h2>
    @if (ViewBag.Status == null || !ViewBag.Status)
    {
        <div>@ViewBag.Message</div>
        <div>
            @using (Html.BeginForm())
            {
                <div class="form-group">
                    <label for="UserName">UserName : </label>
                    @Html.TextBoxFor(a => a.UserName, new { @class = "form-control" })
                </div>
                <div class="form-group">
                    <label for="Password">Password : </label>
                    @Html.TextBoxFor(a => a.Password, new { @class = "form-control", type =
"password" })
                </div>
                <input type="submit" value="Login" class="btn btn-default" />
            }
```

```
        </div>
    }
    else
    {

        <div>@ViewBag.Message</div>
        <div>
            <img src="@ViewBag.BarcodeImageUrl" width="300" height="300" />

        </div>
        <div>
            Manual Setup Code : @ViewBag.SetupCode
        </div>
        <div>
            @using (Html.BeginForm("TwoFactorAuthenticate", "Home", FormMethod.Post))
            {
                <input type="text" name="CodeDigit" />
                <input type="submit" class="btn btn-success" />
            }
        </div>
    }
</center>

<?xml version="1.0" encoding="utf-8"?>
<!--
  For more information on how to configure your ASP.NET application, please visit
  https://go.microsoft.com/fwlink/?LinkId=301880
  -->
<configuration>
```

```
 <appSettings>
  <add key="webpages:Version" value="3.0.0.0" />
  <add key="webpages:Enabled" value="false" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />

       <add key="GoogleAuthKey" value="Marian" />
 </appSettings>
 <system.web>
  <compilation debug="true" targetFramework="4.7.2" />
  <httpRuntime targetFramework="4.7.2" />
 </system.web>
 <runtime>
  <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
   <dependentAssembly>
    <assemblyIdentity name="Antlr3.Runtime" publicKeyToken="eb42632606e9261f" />
    <bindingRedirect oldVersion="0.0.0.0-3.5.0.2" newVersion="3.5.0.2" />
   </dependentAssembly>
   <dependentAssembly>
    <assemblyIdentity name="Microsoft.Web.Infrastructure"
publicKeyToken="31bf3856ad364e35" />
    <bindingRedirect oldVersion="0.0.0.0-2.0.1.0" newVersion="2.0.1.0" />
   </dependentAssembly>
   <dependentAssembly>
    <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" />
    <bindingRedirect oldVersion="0.0.0.0-12.0.0.0" newVersion="12.0.0.0" />
   </dependentAssembly>
   <dependentAssembly>
    <assemblyIdentity name="System.Web.Optimization"
publicKeyToken="31bf3856ad364e35" />
```

```
      <bindingRedirect oldVersion="1.0.0.0-1.1.0.0" newVersion="1.1.0.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="WebGrease" publicKeyToken="31bf3856ad364e35" />
      <bindingRedirect oldVersion="0.0.0.0-1.6.5135.21930" newVersion="1.6.5135.21930"
/>
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="System.Web.Helpers" publicKeyToken="31bf3856ad364e35"
/>
      <bindingRedirect oldVersion="1.0.0.0-3.0.0.0" newVersion="3.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="System.Web.WebPages"
publicKeyToken="31bf3856ad364e35" />
      <bindingRedirect oldVersion="1.0.0.0-3.0.0.0" newVersion="3.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
      <assemblyIdentity name="System.Web.Mvc" publicKeyToken="31bf3856ad364e35" />
      <bindingRedirect oldVersion="1.0.0.0-5.2.9.0" newVersion="5.2.9.0" />
    </dependentAssembly>
  </assemblyBinding>
 </runtime>
 <system.codedom>
  <compilers>
    <compiler language="c#;cs;csharp" extension=".cs"
type="Microsoft.CodeDom.Providers.DotNetCompilerPlatform.CSharpCodeProvider,
Microsoft.CodeDom.Providers.DotNetCompilerPlatform, Version=2.0.1.0, Culture=neutral,
PublicKeyToken=31bf3856ad364e35" warningLevel="4"
compilerOptions="/langversion:default /nowarn:1659;1699;1701" />
    <compiler language="vb;vbs;visualbasic;vbscript" extension=".vb"
type="Microsoft.CodeDom.Providers.DotNetCompilerPlatform.VBCodeProvider,
```

Microsoft.CodeDom.Providers.DotNetCompilerPlatform, Version=2.0.1.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35" warningLevel="4" compilerOptions="/langversion:default /nowarn:41008 /define:_MYTYPE=\"Web\" /optionInfer+" />

</compilers>

</system.codedom>

</configuration>

ДОДАТОК Б. КОПІЯ ТЕЗ ДОПОВІДІ

УДК 004.056.5

Барнич Мар'ян Богданович, здобувач вищої освіти

Хмельницький Національний Університет, Україна

Науковий керівник: Гнатчук Єлизавета Геннадіївна, *Кандидат технічних наук*

Хмельницький Національний Університет, Україна

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ОБРОБЦІ ТА ПЕРЕДАВАННІ В ІТ-ІНФРАСТРУКТУРІ ОРГАНІЗАЦІЇ

Анотація. Актуальність задачі захисту інформації в комп'ютерних системах на сьогоднішній день невіддільна від загального розповсюдження цих систем та поширення комп'ютерних мереж, які обмінюють великі обсяги інформації. Забезпечення безпечної діяльності комп'ютерних систем стало критично важливим для різноманітних підприємств та установ, від державних організацій до невеликих приватних фірм. Незалежно від сфери діяльності, забезпечення конфіденційності та цілісності інформації вимагає розробки та впровадження ефективних методів та засобів безпеки, з урахуванням різноманітних викликів та потреб різних типів організацій. Розходження в цьому питанні полягає в застосуванні різних засобів та методів, а також в обсязі заходів, призначених для забезпечення найвищого рівня безпеки в конкретних умовах використання комп'ютерних систем.

КЛЮЧОВІ СЛОВА: захисту інформації, комп'ютерних системах, актуальність, конфіденційність та цілісність інформації.

Abstract. The relevance of information security in computer systems today is inseparable from the widespread use of these systems and the expansion of computer networks that transmit large volumes of information. Ensuring the secure operation of computer systems has become critically important for various enterprises and institutions, ranging from government organizations to small private firms. Regardless of the field of activity, safeguarding the confidentiality and integrity of information requires the development and implementation of effective security methods and tools, taking into account the diverse challenges and needs of different types of organizations. The divergence in this matter lies in the application of various means and methods, as well as the scope

of measures aimed at ensuring the highest level of security under specific conditions of computer system usage.

KEY WORDS: information security, computer systems, actuality, effective security methods.

Вступ. Питання інформаційної безпеки займають особливе місце в зв'язку із зростаючою роллю в житті суспільства і вимагають до себе все більше уваги. Як відомо, всі виробничі процеси мають в своєму складі матеріальну і нематеріальну складові. Перша – це необхідне для виробництва устаткування, матеріали, енергія і т.д. Друга – технологія виробництва. В останні роки з'явилось багато галузей виробництва, які майже на 100% складаються із однієї інформації. Наприклад, дизайн, створення програмного забезпечення, реклама та інше. Із підвищенням важливості та цінності інформації відповідно росте і роль її захисту. Тому предметом захисту є інформація, яка зберігається, обробляється, передається в комп'ютерних системах (КС). Об'єктом захисту інформації є комп'ютерна система або автоматизована система обробки інформації (АСОІ). [1].

Основна частина. Сучасні підходи до захисту персональних даних базуються на передових інформаційних технологіях, спрямованих на забезпечення високого рівня конфіденційності та цілісності інформації. Використання механізмів шифрування дозволяє ефективно захищати дані в процесі їх передавання та зберігання. Методи аутентифікації, такі як біометричні ідентифікатори та двофакторна аутентифікація, забезпечують додатковий рівень безпеки.

Багатофакторна аутентифікація — це метод аутентифікації (ідентифікації), який вимагає від користувача надання двох або більше доказів особистості, щоб отримати доступ і увійти у свій обліковий запис. І тільки після введення всієї цієї необхідної інформації Ви отримаєте доступ до свого облікового запису. Це може бути номер телефону, адреса електронної пошти або відповідь на якесь (відоме лише Вам) секретне питання. Хоча MFA об'єднує будь-яку кількість факторів аутентифікації, найбільш поширеним з них є двофакторна аутентифікація (2FA). Необхідність MFA також може бути викликана невдалою ідентифікацією у 2FA або підозрілими діями передбачуваної особистості. Це характерно для систем 2FA, здатних переходити у MFA. [2]

Використовують такі сервіси двофакторної авторизації:

1. Google Authenticator— додаток для двохетапної аутентифікації за допомогою Time-based One-time Password Algorithm (TOTP) і HMAC-based One-time Password Algorithm (HOTP) від Google. [3]

2. Microsoft Authenticator - це мобільний додаток, який забезпечує безпечний доступ до облікового запису за допомогою двоетапної аутентифікації. Microsoft Authenticator підтримує функцію введення одноразових паролів (OTP), які обмежені за часом. Іншими словами, при вході у свій обліковий запис на сервісі (що підтримує OTP) в додатку під цим обліковим записом буде створений пароль, що діє протягом 30 секунд, після чого він буде змінений.[4]

Біометрична ідентифікація – це спосіб ідентифікації особистості за окремими специфічними біометричними ознаками (ідентифікаторами), які властиві конкретній людині.

За принципом дії біометричні методи ідентифікації поділяються на статичні (за ознаками, даними людині з народження), динамічні (за ознаками, що набуті в процесі існування) та комбіновані (поєднання двох перших)

Фізіологічні (статичні) методи біометричної

ідентифікації:

– сканування райдужної оболонки ока;

– сканування сітківки ока;

– сканування рисунку вен долоні;

– геометрія кисті руки (відбитки пальців – дактилоскопія, розмір, довжина і ширина долонь);

– розпізнавання рис обличчя (контур, форма;

розташування очей і носа);

– структура ДНК-сигнатури.

Поведінкові (динамічні) методи;

– аналіз підпису (форма букв, манера письма,

натиск);

– аналіз тембру голосу;

– аналіз клавіатурного почерку тощо[5]

Сучасні стратегії захисту персональних даних ґрунтуються на передових інформаційних технологіях для забезпечення конфіденційності та цілісності інформації. Шифрування використовується для ефективного захисту даних під час їх передавання та зберігання. Однак наріжною частиною захисту є також аутентифікація, зокрема біометричні ідентифікатори та двофакторна аутентифікація, які забезпечують додатковий рівень безпеки. Багатофакторна аутентифікація, зокрема двофакторна, вимагає подання двох або більше доказів особистості для доступу до облікового запису.

Біометрична ідентифікація, ґрунтуючись на унікальних фізіологічних та поведінкових рисах, доповнює ці заходи, забезпечуючи повний спектр захисту особистої інформації.

Висновки. Загальна зростаюча роль сучасних технологій та комп'ютеризації у суспільстві вимагає особливої уваги до питань інформаційної безпеки. Разом із швидким розвитком інформаційних технологій, відзначається поява галузей, де інформація є визначальним елементом виробничих процесів. Захист персональних даних набуває критичного значення, особливо в сферах, де інформація становить основний актив.

Отже, інтеграція передових інформаційних технологій у сферу захисту персональних даних є необхідною та актуальною відповіддю на зростаючі виклики та загрози інформаційної безпеки в епоху цифрового розвитку.

Список інформаційних джерел

1. Гапак О. М. Глебена М. І Горват П.П.Захист інформації в комп'ютерних системах. URL:

https://www.uzhnu.edu.ua/uk/infocentre/get/42935

2. Илья Онищенко. захист персональних даних: деякі практичні аспекти. Asters. URL: https://www.asterslaw.com/ua/press_center/publications/personal_data_protection_some_practical_aspects/

3. Google Authenticator. Wikipedia. URL:

https://uk.wikipedia.org/wiki/Google_Authenticator

4. Microsoft Authenticator що це? Simpla. URL:

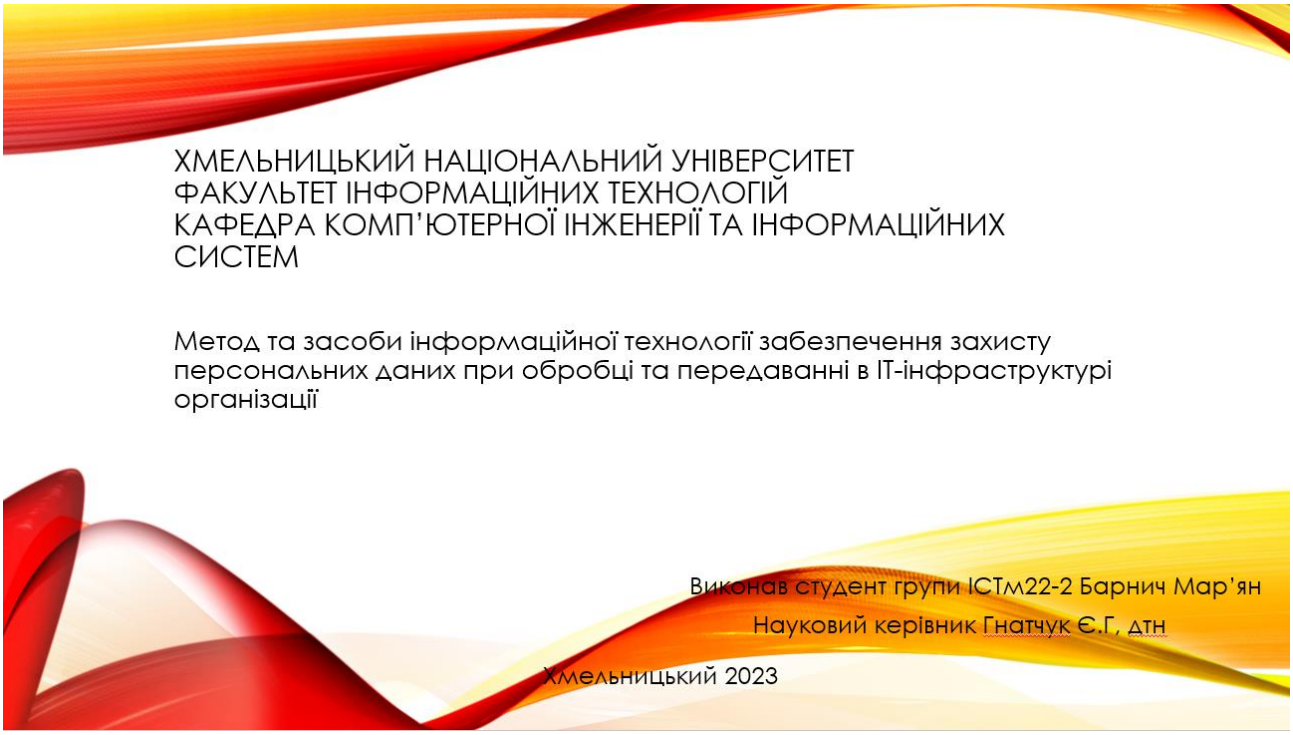
https://simpla.com.ua/blog/microsoft-authenticator-shcho-ce

5. Методи і технології біометричної ідентифікації

за результатами літературних джерел Коваль Л.Г. Злепко С.М. Новіцький Г.М. Крекотень Є.Г. URL:

https://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf

ДОДАТОК В. ПРЕЗЕНТАЦІЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ



Метою є аналіз методів автентифікації та сервісів для посилення автентифікації з метою вибору оптимального способу та сервісу для підвищення рівня безпеки даних в IT- інфраструктурі організації.

- Предметом дослідження є підвищення рівня захисту персональних даних в інформаційно-технічній інфраструктурі організації при їх передаванні та обробці, зокрема шляхом дослідження, розробки та застосування методів двофакторної аутентифікації з використанням Google Authenticator.

- Методи дослідження. У роботі було проаналізовано наступні теорії та засоби:
  - стратегія безпеки Zero Trust;
  - багатофакторна аутентифікація (MFA);
  - загальний регламент ЄС про захист персональних даних (GDPR);
  - Data Protection as a Service (DPaaS);
  - Virtual private network (VPN);
  - Microsoft Azure Active Directory.

НАУКОВА НОВИЗНА ОТРИМАНИХ РЕЗУЛЬТАТІВ

Наукова новизна роботи:

- дослідження можливостей інтеграції двофакторної аутентифікації з іншими захисними механізмами.
- Найдено швидкий та ефективний метод інтеграції 2FA в проект чи систему IT-інфраструктури організації.

ПРАКТИЧНЕ ЗНАЧЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Дослідження полягає у аналізі методів захисту даних для IT-інфраструктури при їх отриманні і передавані.

Актуальність дослідження

Актуальність дослідження полягає у виборі найефективнішого і найлегшого в інтеграції методу захисту даних для IT-інфраструктури організації.

ОГЛЯД ІСНУЮЧИХ ПІДХОДІВ ЗАХИСТУ ДАНИХ

- Нульова довіра (ZT) - це термін для позначення еволюціонуючого набору парадигм кібербезпеки, які переносять захист зі статичних, мережевих периметрів на користувачів, активи та ресурси.
- Багатофакторна автентифікація(MFA) - це одна з найпопулярніших послуг, яку сьогодні використовують різні люди, особливо багато організацій. Люди використовують цю послугу для авторизації своїх збережених даних і доступу до них без будь-яких порушень безпеки
- Біометрична ідентифікація – це спосіб ідентифікації особистості за окремими специфічними біометричними ознаками (ідентифікаторами), які властиві конкретній людині.

- Загальний регламент ЄС про захист персональних даних (GDPR) — регламент в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. DPaaS – це хмарна послуга, яка забезпечує комплексний захист данних, включаючи резервне копіювання, відновлення та запобігання втрати данних. Вона використовує передові технології та стратегії, щоб забезпечити безпеку, доступність та можливість відновлення ваших данних, навіть у разі атаки розшифровки данних .
- VPN - це віртуальна мережа, побудована на основі існуючих фізичних мереж, яка може забезпечити безпечний механізм зв'язку для даних та іншої інформації, що передається між двома кінцевими точками.
- Віртуальні приватні мережі (VPN) на рівні захищених сокетів (SSL) забезпечують безпечний віддалений доступ до ресурсів організації.

ВИОКРЕМЛЕННЯ КЛЮЧОВИХ ТЕНДЕНЦІЙ МЕТОДІ ZEROTRUST

- перенесення захисту: парадигма ZT переносить захист з мережевих периметрів на користувачів, активи та ресурси;
- оцінка довіри: забезпечує відсутність неявної довіри та постійну оцінку довіри до активів та облікових записів користувачів.

Архітектура нульової довіри (ZTA)

- комплексний підхід:
  - навколо ідентифікації, облікових даних, управління доступом, операцій, кінцевих точок, хостингових середовищ та сполучної інфраструктури;
- мінімальні привілеї:
  - фокус на обмеженні ресурсів для користувачів та наданні лише необхідних привілеїв.

ВИОКРЕМЛЕННЯ КЛЮЧОВИХ ТЕНДЕНЦІЙ МЕТОДІ MFA

- Широке поширення MFA. Багатофакторна автентифікація є широко використовуваною послугою, особливо в організаціях. Застосування в різних системах зберігання використовується для авторизації доступу до різних систем зберігання даних .
- Надійність та безпека MFA. Необхідний компонент управління ідентифікацією та доступом (IAM): MFA розглядається як необхідний компонент для підвищення безпеки компаній.
- Використання в моделі IAM. Вибір між двофакторною та багатофакторною автентифікацією: користувачі можуть обирати використання двофакторної чи багатофакторної автентифікації в залежності від рівня безпеки.

ВИОКРЕМЛЕННЯ КЛЮЧОВИХ ТЕНДЕНЦІЙ В МЕТОДІ БІОМЕТРИЧНОЇ АВТОРИЗАЦІЇ

- Широке використання в різних галузях: біометричні методи ідентифікації, такі як ідентифікація райдужної оболонки та відбитків пальців, застосовуються в різних галузях, включаючи охорону будівель, територій та банкоматів.
- Висока точність та надійність. Індивідуальність величезної кількості варіацій: ідентифікація за відбитками пальців має велику індивідуальність, що забезпечує високу точність та надійність.
- Автоматизація для підвищення продуктивності. Використання автоматичних систем: ручна перевірка відбитків пальців є трудомісткою, тому використання автоматичних систем ідентифікації допомагає підвищити продуктивність.

ВИОКРЕМЛЕННЯ КЛЮЧОВИХ ТЕНДЕНЦІЙ В МЕТОДІ DPAAS

- Хмарна послуга для комплексного захисту даних: DPaaS надає хмарну послугу, що охоплює резервне копіювання, відновлення та запобігання втраті даних.
- Захист від розшифрування даних. Захист від атак розшифрування: DPaaS використовує передові технології та стратегії для забезпечення безпеки, доступності та відновлення даних, включаючи сценарії атак розшифрування.
- Хмарні обчислення та SaaS, визначення хмарних обчислень: пояснення концепції хмарних обчислень, як використання обчислювальних ресурсів через мережу. Програмне забезпечення як послуга (SaaS): опис використання SaaS в бізнес-моделі, зокрема, передача обслуговування та підтримки апаратного та програмного забезпечення хмарному провайдеру.

ВИБІР ТЕХНОЛОГІЇ НА ОСНОВІ АНАЛІЗУ МЕТОДІВ ЗАХИСТУ

На основі розгляду ключових тенденцій в областях Zero Trust (ZT), Multi-Factor Authentication (MFA), біометричної ідентифікації, регламенту про захист даних та DPaaS, обрано метод MFA як найефективніший та найлегший в імплементації для захисту даних в IT-інфраструктурі організації.

Основні фактори, що підтверджують цей вибір

1. Широке поширення та позитивне ставлення до MFA. MFA є широко використовуваною послугою в організаціях, а його позитивне ставлення обумовлено як додатковим рівнем безпеки.
2. Стурбованість організацій стосовно безпеки даних та загрози інсайдерських атак підкреслюють важливість використання ефективних заходів безпеки, таких як MFA.
3. Типи MFA та їх використання. Різні типи MFA, такі як одноразові паролі (OTP), надають можливість користувачам вибору та використання того, що найбільше відповідає вимогам їхньої безпеки.

ТЕХНОЛОГІЯ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ ДЛЯ ЗАХИСТУ ДАНИХ ПРИ ОБРОБЦІ ТА ПЕРЕДАВАННІ В IT-ІНФРАСТРУКТУРІ ОРГАНІЗАЦІЇ

Двофакторна автентифікація (2FHA) - це захід безпеки, який вимагає від користувачів надання двох форм ідентифікації для доступу до облікового запису або системи.

Однією формою ідентифікації зазвичай є пароль, а іншою - унікальний, прив'язаний до часу одноразовий пароль (OTP), який генерується і надсилається на телефон користувача за допомогою SMS-повідомлення.

Двофакторна автентифікація (2FA) як послуга - це рішення безпеки, яке дозволяє компаніям додати додатковий рівень захисту до процесу автентифікації користувачів.

Зазвичай вона надається як хмарний сервіс і може бути інтегрована в існуючі системи та інфраструктуру організації.

За допомогою 2FA користувачі повинні надати дві форми ідентифікації при вході в систему або додаток: перша - це традиційна форма автентифікації, наприклад, пароль, а друга - унікальний, одноразовий код, згенерований пристроєм або сервісом, наприклад, мобільним додатком або текстовим повідомленням.

ТИПИ 2FA: 2FA З SMS-КОДОМ

Двофакторна автентифікація на основі SMS-повідомлень (2FA) є найбільш поширеним механізмом 2FA, незважаючи на те, що SMS-повідомлення, як відомо, вразливі до атак перенаправлення, і незважаючи на наявність альтернатив, які можуть бути більш безпечними.

Це пов'язано з двома причинами:

- По-перше, він дуже ефективний на практиці, про що свідчать звіти Google та Microsoft.
- По-друге, користувачі віддають перевагу SMS, а не альтернативам, оскільки обмін текстовими повідомленнями вже є частиною їхнього щоденного спілкування.

Недоліки 2FA з СМС:

- Затримка у доставці: залежність від мережі та можливість затримки у доставці СМС може призвести до часових ускладнень.
- Збір та використання даних: існує ризик перехоплення СМС або збору інформації з них.
- Вартість для оператора: у деяких випадках вартість відправлення СМС може покладатися на оператора мобільного зв'язку чи користувача.

ТИПИ 2FA: 2FA З GOOGLE AUTHENTICATOR

Google Authenticator широко використовувана технологія двофакторної автентифікації, забезпечує додатковий рівень безпеки, що практично унеможливлює несанкціонований доступ.

Цей інтегрований метод простий у використанні навіть для людей, які не є технічно підкованими, і пропонує максимальний захист від основних загроз, таких як підміна SIM-карти, програми-сталкери та атаки з побічних каналів.

Як працює двофакторна аутентифікація (2FA) з Google Authenticator:

1. Активація 2FA. Користувач активує 2FA для свого облікового запису, зазвичай за допомогою мобільного додатку, такого як Google Authenticator. Під час активації генерується унікальний код або сканується QR-код.
2. QR-код і секретний ключ. QR-код містить інформацію, яка додається до додатку Google Authenticator. Також користувач отримує секретний ключ, який може бути введений вручну, якщо немає можливості сканувати QR-код.
3. Генерація одноразових паролів. Додаток Google Authenticator генерує одноразові шестизначні паролі (OTP), які змінюються кожні 30 секунд.

РОЗРОБКА ТЕХНОЛОГІЇ 2FA ДЛЯ ЗАХИСТУ ДАНИХ ПРИ ЇХ ОБРОБЦІ ТА ПЕРЕДАВАННІ В IT-ІНФРАСТРУКТУРІ ОРГАНІЗАЦІЇ.

Після ретельного аналізу патернів проектування веб-додатків та огляду сучасних технологій розробки веб-додатків було прийнято рішення прийняти розгалужену архітектуру з реалізацією патерну проектування MVC.

На рівні інтерфейсу використовується HTML та Razor для простого представлення.

Для реалізації бізнес-логіки використовується MVC-фреймворк ASP.NET Core, який надає можливість створювати API з використанням шаблонів ASP.NET Core Web API.

На рівні доступу до даних було вирішено використовувати об'єктно-реляційне відображення, в якості системи управління базами даних обрано Microsoft SQL SERVER.

ОПИС ФУНКЦІОНУВАННЯ ПРОЕКТУ

Проект заснований на архітектурному шаблоні MVC (Model-View-Controller), що дозволяє розділити логіку додатку на три основні компоненти: модель, вид та контролер, а забезпечує доступ до даних – Entity Framework, котрий потрібно інтегрувати до проєкту.

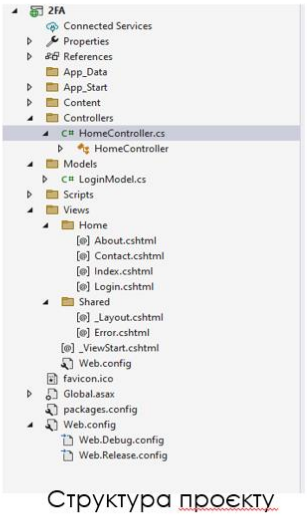
Для забезпечення функціоналу двофакторної аутентифікації використовується NuGet-пакет Google Authenticator.

Цей пакет дозволяє імплементувати сервіс у проект та генерувати і перевіряти двофакторні коди згідно з алгоритмом, використовуваним Google Authenticator.

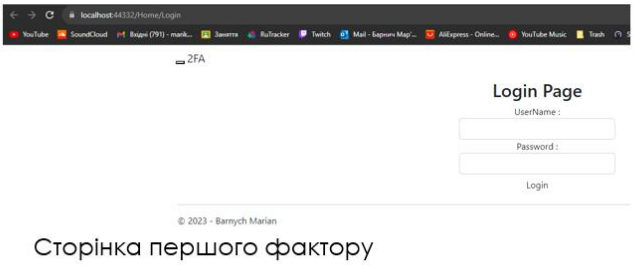
Основним файлом конфігурації додатку є Web.config, в якому вказані певні чутливі дані, які використовуються в роботі застосунку (такі як адреса підключеної бази даних, логін та пароль доступу до неї чи секретний ключ для підпису JWT-токенів).

В теці Controllers знаходяться контролери, які приймають ввід користувача і передають зміни до моделі. Сутності бази даних розміщені в теці Models

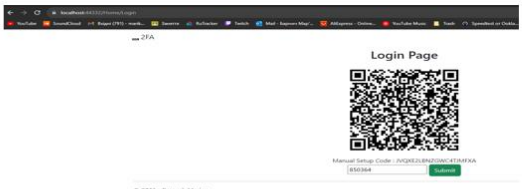
ЗНІМКИ СТРУКТУРИ ПРОЄКТУ



Структура проєкту



Сторінка першого фактору



Сторінка другого фактору

Вигляд додатка Google Authenticator

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було досліджено проблематику захисту інформації в інформаційно-технологічних організаціях у сучасному світі. Основний акцент роботи був зроблений на аспектах обробки та передавання даних в цих організаціях.

У ході аналізу було розглянуто різноманітні стратегії та методи захисту інформації, такі як Zero Trust, Багатофакторна аутентифікація (MFA), Біометрична ідентифікація, а також враховано вимоги GDPR та використання Data Protection as a Service (DPaaS). Кожен метод був проаналізований з урахуванням його переваг та недоліків.

Висновки досліджень дозволили визначити, що впровадження методу двофакторної аутентифікації (2FA) з використанням Google Authenticator для IT-організацій є найбільш ефективним та простим у впровадженні в інформаційні системи. Вибір цього методу обумовлено його високою складністю взлому системи, швидкістю доступу для користувачів та загальною зручністю використання.

Створений проект, базований на обраному методі 2FA, успішно пройшов тестування та отримав позитивну оцінку щодо його ефективності. Результати свідчать про те, що впровадження обраного методу значно підвищило рівень безпеки інформації в організації, зменшивши ризик несанкціонованого доступу та підвищивши надійність у керуванні даними.

Отже, вибір методу 2FA виявився оптимальним кроком для забезпечення високого рівня безпеки та ефективності в інформаційно-технологічних організаціях.

Таким чином, висновок полягає в тому, що вибір методу 2FA виявився вдалим кроком у забезпеченні безпеки даних в інформаційно-технологічних організаціях.

Mon Dec 18 17:45:15 EET 2023, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 12%**

ID: 123765 Назва: ДП Метод та засоби інформаційної технології забезпечення захисту персональних даних при обробці та передаванні в IT-інфраструктурі організації Додано в БД: 2023-12-18 Автора: Барнич М. Б. Керівники: Гнатчук Є.Г. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	105265	830	734 (1%)	10 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра КІ

ID перевірки:
1016018714

Дата перевірки:
19.12.2023 02:25:15 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
19.12.2023 07:20:26 EET

ID користувача:
100005591

Назва документа: **Квал ф кац и на_робота_Барнич_плаг ат**

Кількість сторінок: **88** Кількість слів: **16052** Кількість символів: **124999** Розмір файлу: **2.82 MB** ID файлу: **1015706507**

11.2%
Схожість

Найбільша схожість: **2.95%** з Інтернет-джерелом (https://ela.kpi.ua/handle/123456789/41819)

11% Джерела з Інтернету	752	Сторінка 90
1.21% Джерела з Бібліотеки	87	Сторінка 95

0.9% Цитат

Цитати	6	Сторінка 96
Посилання	1	Сторінка 96

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	3

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Здобувач: Барнич Мар'ян Богданович

Тема: Метод та засоби інформаційної технології ідентифікації залишкових дефектів у програмному забезпеченні

Спеціальність: 126 «Інформаційні системи та технології»

Обсяг кваліфікаційної роботи:

Кількість листів креслень – ; кількість сторінок записки 75

1. Короткий зміст роботи та прийнятих рішень У роботі запропоновано розробку технології 2FA для захисту даних при їх обробці та передаванні в іт-інфраструктурі організації.

2. Висновок про відповідність роботи дипломному завданню Кваліфікаційна робота магістра відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено аналіз відомих методів та засобів захисту інформації поставлена мета аналіз методів автентифікації та сервісів для посилення автентифікації з метою вибору оптимального способу та сервісу для підвищення рівня безпеки даних в IT-інфраструктурі організації. У четвертому розділі було прийнято рішення розробки архітектури з реалізацією 2FA на паттерні проектування MVC.

4. Позитивні сторони роботи: Запропонована система є ефективна для захисту даних IT-інфраструктури організації та легка в імплементації у IT-інфраструктуру.

5. Негативні сторони роботи: В роботі присутні певні логічні помилки у деяких аналізах ефективності засобів захиисту інформації.

6. Оцінка графічного оформлення та пояснювальної записки роботи: –

7. Відгук про роботу в цілому: В загальному робота виконана на достатньому рівні.

8. Інші зауваження: –

9. Оцінка кваліфікаційної роботи:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи вважаю, що робота заслуговує оцінки «задовільно» 3.00 (E)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Мартиюк В.В., звідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки Хмельницького Національного Університету

"18 грудня" 2023р.

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т.О.

Барнич Мар'ян Богданович
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи ІСТм-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлена. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщена та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

19 грудня 2023 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод та засоби інформаційної технології ідентифікації залишкових дефектів у програмному забезпеченні

Автор: Барнич Мар'ян Богданович

Спеціальність: 126 – Інформаційні системи та технології

Освітня програма: Інформаційні системи та технології

Науковий керівник: Гнатчук Єлизавета Геннадіївна, к.т.н, професор

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;
3) в якості запозичень в окремих місцях системою зафіксовано послідовності чотирьохрозряних двійкових кодів, які є вхідними даними до великої кількості задач і не можуть розглядатися як об'єкт авторських прав і, відповідно, їх порушення;
4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.(Тут текст можна і треба модифікувати)

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості Unicheck, складає 11.2% і адресується до 259 першоджерел; та системою Anti-Plagiarism складає 1%, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Є. Г. Гнатчук

Гарант ОП _____ О. О. Павлова

Завідувач кафедри КІС _____ Т. О. Говорущенко