Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Григоренка Вадима Олександровича

на здобуття ступеня вищої освіти Бакалавра

Система аунтетифікації користувачів
на основі протоколу одноразових паролів

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.200128.20.01.06 ПЗ

Виконав студен 4 курсу група КБ-20-1 Вадим ГРИГОРЕНКО
Керівник канд. техн. наук, доцент Віра ТІТОВА
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

20 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Григоренко Вадиму Олександровичу

1 Тема роботи Система аутентифікації користувачів на основі протоколу одноразових паролів

Керівник роботи Тітова Віра Юріївна

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру 25.05.2024р

3 Вихідні дані до роботи Провести аналіз алгоритмів одноразових паролів та на основі цього створити програмне забезпечення

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ. Автентифікація та ідентифікація користувачів. Технології одноразових паролів. Програмна реалізація. Висновки

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Структурна схема розробленої системи автентифікації. Блок-схема роботи програми.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка проєктних рішень	Квітень	
Апробація проєктних рішень	Травень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Червень	
Захист КР	Червень	

Студент Вадим ГРИГОРЕНКО

Керівник кваліфікаційної роботи Віра ТІТОВА

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система автентифікації користувачів на основі протоколу одноразових паролів.

Автор: Григоренко Вадим Олександрович.

Керівник: Тітова Віра Юріївна.

Пояснювальна записка: 67 с., 1 додаток, 14 рис., 1 табл., 40 джерел.

Графічна частина: 3 плакати, 9 презентаційних слайдів.

ОДНОРАЗОВІ ПАРОЛІ, АВТЕНТИФІКАЦІЯ, БЕЗПЕКА, ІНФОРМАЦІЙНІ СИСТЕМИ, ПРОТОКОЛ ОТР

Кваліфікаційна робота присвячена розробці системи автентифікації користувачів на основі протоколу одноразових паролів з метою підвищення рівня безпеки інформаційних систем. В роботі проведено дослідження існуючих методів автентифікації, зокрема протоколів одноразових паролів, та аналіз їх ефективності. Було розроблено програмну реалізацію системи автентифікації, проведено її тестування та оцінку рівня безпеки.

Результати дослідження показали, що використання одноразових паролів суттєво підвищує захист інформаційних систем від несанкціонованого доступу в порівнянні з традиційними методами автентифікації. У роботі також описано створення відповідної документації, що включає технічне завдання, модель загроз та порушників, а також план захисту інформації.

20.06.2024

ABSTRACT

The topic of the qualification work: User authentication system based on the protocol of one-time passwords.

Author: Vadim Oleksandrovich Grigorenko.

Head: Titova Vira Yuriivna.

Explanatory note: 67 pp., 1 appendices, 14 figures, 1 table, 40 sources.

Graphic part: 3 posters, 9 presentation slides.

ONE-TIME PASSWORDS, AUTHENTICATION, SECURITY, INFORMATION SYSTEMS, OTP PROTOCOL

The qualification work is devoted to the development of a user authentication system based on the protocol of one-time passwords in order to increase the level of security of information systems. The paper examines existing authentication methods, in particular one-time password protocols, and analyzes their effectiveness. The software implementation of the authentication system was developed, its testing and assessment of the security level was carried out.

The results of the study showed that the use of one-time passwords significantly increases the protection of information systems against unauthorized access compared to traditional authentication methods. The work also describes the creation of relevant documentation, including a technical task, a model of threats and violators, as well as an information protection plan.

20.06.2024

ЗМІСТ

ВСТУП

У сучасному світі системи, об’єднані через мережі, все активніше стають невіддільною частиною нашого життя. Безпека таких систем є важливим аспектом, до якого ставляться так само серйозно, як і до безпеки в реальному житті. Особливо з приходом Covid-19 світ показав, що існує велика кількість вразливих систем, а також систем, не готових до обробки великої кількості користувачів. Вторгнення російської федерації в Україну у 2022 році продемонструвало, що безпека національних систем повинна бути на найвищому рівні для витримування масових та потужних атак на інфраструктуру. Такі системи не тільки повинні захищати національні інтереси, а й бути спроможними надавати послуги у межах цілих країн і націй.

Автентифікація та авторизація є першим рівнем захисту від зловмисників у будь-якій системі. Вимоги до безпеки таких систем є високими через велику кількість моделей загроз та векторів атак, починаючи від прямих атак на систему і закінчуючи перехопленням трафіку між користувачем та системою. В умовах постійного зростання кіберзагроз питання автентифікації стає критично важливим для забезпечення надійного захисту інформаційних систем.

Ця дипломна робота присвячена дослідженню та розробці систем автентифікації користувачів на основі одноразових паролів. Основною метою є підвищення рівня безпеки інформаційних систем через впровадження ефективних методів автентифікації, що відповідають сучасним вимогам та викликам кібербезпеки.

1 АВТЕНТИФІКАЦІЯ ТА ІДНЕТИФІКАЦІЯ КОРИСТУВАЧІВ

1.1 Автентифікація користувачів

Автентифікація є критичним компонентом забезпечення безпеки в інформаційних системах. Її розвиток відображає зростання складності та вразливості інформаційних технологій. Розглянемо основні етапи розвитку автентифікації. 1960-ті роки Історія автентифікації починається з використання простих паролів. Перші комп'ютерні системи використовували текстові паролі для обмеження доступу до ресурсів. Цей метод був досить ефективним на той час, коли комп'ютери були великими і дорогими машинами, доступ до яких мали лише спеціалісти Основні проблеми цього методу полягали у вразливості до атак типу "груба сила" (brute force), коли хакер послідовно підбирає всі можливі паролі, а також до соціальної інженерії, коли зловмисник отримує пароль шляхом обману користувача.

З розвитком технологій і зростанням кількості користувачів виникла потреба у захисті паролів від несанкціонованого доступу. У цей час почали використовуватися алгоритми хешування для зберігання паролів у зашифрованому вигляді. Одним з перших таких алгоритмів був DES (Data Encryption Standard). Хоча шифровані паролі значно підвищили рівень безпеки, вони все ще залишалися вразливими до атак типу "груба сила" та до випадків, коли користувачі використовували слабкі або однакові паролі для різних сервісів. 1990-ті роки: Зростання інтернету та електронної комерції призвело до появи більш складних методів автентифікації.

Двофакторна автентифікація стала популярною у цей період. Вона вимагала від користувача введення не лише пароля, але й другого фактору, такого як одноразовий пароль (OTP), що надсилався на мобільний телефон або генерувався спеціальним токеном. Основною проблемою 2FA була зручність використання.

Користувачам доводилося мати при собі додаткові пристрої (токени) або мати доступ до мобільного телефону, що не завжди було зручно. 2000-ті роки З

розвитком біометричних технологій з'явилися методи автентифікації, засновані на фізичних характеристиках користувача, таких як відбитки пальців, розпізнавання обличчя та сканування райдужки ока. Ці методи забезпечували високий рівень безпеки, оскільки біометричні дані важко підробити. Основні проблеми біометричної автентифікації включають високу вартість впровадження та ризик компрометації біометричних даних, які, на відміну від паролів, неможливо змінити у разі витоку. 2010-ті роки: Сучасні системи автентифікації почали використовувати аналіз поведінкових ознак, таких як стиль набору тексту, використання миші та інші дії користувача. Ці методи дозволяють постійно моніторити користувача і виявляти аномалії в його поведінці Недоліки цього методу включають високу складність впровадження та необхідність у великих обсягах даних для точного аналізу поведінки користувача 2020-ті роки і далі ШІ починає відігравати все більшу роль у системах автентифікації.

Використання машинного навчання дозволяє створювати більш надійні моделі, що можуть розпізнавати користувачів за складними наборами даних, включаючи біометричні та поведінкові ознаки. Це дозволяє підвищити рівень безпеки і знизити ймовірність помилкових спрацьовувань. Використання ШІ в автентифікації потребує значних обчислювальних ресурсів і може бути вразливим до атак на основі маніпуляції даними, що використовуються для навчання моделей.

Розвиток автентифікації пройшов довгий шлях від простих паролів до складних систем, що використовують біометричні дані та штучний інтелект. Кожен новий етап розвитку додавав нові рівні безпеки, але також приносив нові виклики і проблеми. В майбутньому можна очікувати подальшого розвитку технологій автентифікації з акцентом на підвищення безпеки та зручності для користувачів. Автентифікація користувача перевіряє особу користувача, який намагається отримати доступ до мережі або обчислювального ресурсу, авторизуючи передачу облікових даних від людини до машини під час взаємодії в мережі, щоб підтвердити автентичність користувача. Цей термін відрізняється від машинної автентифікації, яка є автоматизованим методом автентифікації, який не потребує

введення користувача. Автентифікація допомагає гарантувати, що лише авторизовані користувачі можуть отримати доступ до системи, запобігаючи неавторизованим користувачам отримати доступ і потенційно пошкодити системи, викрасти інформацію або спричинити інші проблеми.

Майже всі взаємодії людини з комп'ютером, крім гостьових і автоматичних облікових записів, виконують автентифікацію користувача. Він авторизує доступ як до дротових, так і до бездротових мереж, щоб забезпечити доступ до мережевих та підключених до Інтернету систем і ресурсів. Простий процес автентифікації користувача складається з трьох завдань:

– ідентифікація;
– аутентифікація;
– авторизація.

Автентифікація користувача може бути такою ж простою, як вимога до користувача ввести унікальний ідентифікатор, наприклад ідентифікатор користувача, разом із паролем для доступу до системи. Однак це також може бути складнішим - наприклад, вимагати від користувача надати інформацію про фізичні об'єкти чи навколишнє середовище або навіть виконати певні дії.

Автентифікація користувача працює, доводячи мережі або обліковому запису, що користувач, який намагається отримати доступ, є тим, за кого себе видає.

Як правило, користувач підтверджує свою особу унікальними даними для входу. Давайте детальніше розглянемо три основні етапи процесу перевірки інформації. Введення облікових даних для входу щоб отримати доступ до захищеної системи, вам потрібно ввести своє ім'я користувача, пароль або інший тип ключа доступу, який ви обрали під час реєстрації.

Порівняно облікові дані система до якої ви намагаєтеся отримати доступ, надсилає ваші облікові дані на свій сервер автентифікації, який порівнює їх із хешами облікових даних, які надійно зберігаються в базі даних системи.

Автентифікацію завершено якщо введена вами інформація для входу еквівалентна тій, що зберігається на сервері, це надає вам доступ до облікового

запису. ваш запит на автентифікацію буде відхилено, якщо ви не надасте правильні облікові дані. ваш обліковий запис також може бути позначено як підозріла активність, якщо ви невдало спробуєте ввійти кілька разів поспіль. у цьому випадку система автентифікації може надати вам додатковий етап перевірки, наприклад одноразовий пароль.

1.2 Типи автентифікації

Типи автентифікації користувача стосуються різних методів, які застосовуються для розпізнавання законного користувача. Кожен метод може використовувати інформацію різного характеру, яку знають лише сервер автентифікації та користувач. Ця інформація зазвичай поділяється на три різні категорії, які називаються факторами автентифікації.

Розглянемо кожну з них детальніше фактор знань або щось, що користувач знає, включає ім’я користувача, пароль і PIN-коди, створені користувачем фактор володіння або щось, що є у користувача, відноситься до фізичних пристроїв, включаючи телефони та брелки, або цифрових активів, таких як облікові записи електронної пошти фактор приналежності або щось, чим є користувач, тобто його біометричні дані, такі як сканування відбитків пальців або розпізнавання обличчя.

Залежно від типу автентифікації кожен фактор можна використовувати як унікальний маркер перевірки або об’єднати для більш надійних рішень автентифікації. Типи автентифікації включають різні методи перевірки користувача для доступу до системи або ресурсу. Вибір методу автентифікації залежить від рівня безпеки, який необхідно забезпечити, та специфічних вимог до користувацького досвіду.

Розглядаючи основні типи автентифікації. Найбільш поширений метод автентифікації, який передбачає введення користувачем секретного пароля або ПІН-коду. Або такі як сканування відбитків пальців або розпізнавання обличчя.

Цей метод забезпечує високий рівень безпеки завдяки унікальності біометричних даних кожної людини. паролі, які генеруються для одноразового використання і мають обмежений термін дії. Використовуються для додаткового рівня захисту, зазвичай в рамках двохфакторної автентифікації.

Також є Багатофакторна автентифікація (MFA) є методикою підвищення безпеки, яка вимагає від користувача підтвердження своєї особи за допомогою двох або більше незалежних факторів. MFA забезпечує значно вищий рівень захисту в порівнянні з традиційними методами автентифікації, оскільки для доступу до системи зловмиснику необхідно зламати декілька різних механізмів захисту. Використання декількох факторів автентифікації значно ускладнює доступ для зловмисників, навіть якщо один з факторів було скомпрометовано.

MFA забезпечує захист від фішингових атак, атаки грубою силою (brute force) та інших видів кібератак, що спрямовані на отримання доступу до системи. Багато галузей вимагають впровадження багатофакторної автентифікації для забезпечення відповідності нормативним вимогам щодо захисту даних таким чином, багатофакторна автентифікація є важливим інструментом у забезпеченні безпеки сучасних інформаційних систем. Вона значно підвищує рівень захисту, мінімізуючи ризики несанкціонованого доступу та забезпечуючи відповідність нормативним вимогам.

1.3 Методи автентифікації

Пароль є одним із найпоширеніших методів автентифікації. Зазвичай це комбінація літер, цифр і спеціальних символів, які користувач створює, щоб підтвердити свою особу, коли хоче отримати доступ до свого облікового запису. Щоб користувач належним чином захистив свої облікові записи, він повинен створити надійні паролі. Вони мають містити принаймні вісім символів і містити поєднання великих і малих літер, а також цифр і символів. Надійні паролі важче

зламати, оскільки вони складніші та менш передбачувані. Вони також більш ефективні проти атак грубої сили, які залишаються популярними серед хакерів для отримання несанкціонованого доступу до облікових записів.

У разі атаки грубою силою зловмисники перевіряють можливі комбінації паролів, доки не знайдуть правильний збіг і не отримають доступ до особистих облікових записів або конфіденційних даних. Однак практика показує, що люди схильні створювати слабкі паролі, які легко запам'ятати. Враховуючи кількість онлайн-акаунтів, якими доводиться жонглювати одній людині щодня, це цілком природно. На жаль, така практика значно загрожує безпеці користувача в Інтернеті. Крім того, користувачі схильні використовувати той самий пароль для кількох облікових записів, що робить їх більш сприйнятливими до того, щоб стати жертвами різних кіберзлочинів.

Наприклад, якщо ви використовуєте однакові облікові дані для своїх облікових записів у соціальних мережах і банку, і хакеру вдається зламати один із них, вони отримають доступ до обох облікових записів. Хакерам все частіше вдається отримати доступ до чутливих і конфіденційних даних, включаючи паролі користувачів, через витоки даних великих компаній. Якщо ви використовуєте однакові ім’я користувача та пароль для всіх своїх облікових записів в Інтернеті, витік даних одного з ваших облікових записів може мати руйнівні наслідки, оскільки хакери можуть легко отримати доступ до всіх ваших облікових записів з однаковими обліковими даними. Ось чому життєво важливо не використовувати один і той самий пароль для кількох облікових записів і не включати будь-яку особисту інформацію у свої паролі - у разі взлому хакер отримає ще одну частину вашої цінної особистої інформації. Багатофакторна аутентифікація Багатофакторна автентифікація. MFA - це метод перевірки користувача, який вимагає двох або більше факторів ідентифікації, щоб надати користувачеві доступ до свого облікового запису. Наприклад, після введення імені користувача та пароля МЗС може надіслати вам push-сповіщення або одноразовий код підтвердження для підтвердження вашого підключення Це один із способів підтвердження особи.

Іншим варіантом може бути використання біометричних даних, як відбиток пальця.

MFA часто взаємозамінно називають двофакторною автентифікацією (2FA). Однак остання є лише підмножиною MFA, яка використовує рівно два фактори для автентифікації користувачів, тоді як MFA може містити більше двох факторів для ідентифікації користувачів. Завдяки багаторівневому підходу до безпеки MFA може завадити хакерам отримати доступ до облікових записів користувачів, навіть якщо їм вдасться зламати паролі. Фактори.

Вторинної автентифікації в MFA зазвичай включають те, що є у користувача (наприклад, цифрові активи) або те, чим вони є (наприклад, біометричні дані), які потребують серйозних зусиль, щоб підробити або отримати до них доступ.

Біометрична автентифікація - це метод перевірки користувачів на основі їхніх унікальних фізіологічних або поведінкових характеристик. Вони можуть включати Розпізнавання відбитків пальців, обличчя, очей або голосу вважається фізіологічною біометрією. Динаміка натискання клавіш або аналіз сигнатур, розглянуті поведінкові характеристики. Цей метод автентифікації стає все більш популярним, оскільки він може забезпечити високий рівень безпеки - унікальні біологічні характеристики важко відтворити. Крім того, він забезпечує майже безперебійну роботу користувача, оскільки користувачеві потрібно просто торкнутися екрана, щоб отримати відбиток пальця або дозволити пристрою просканувати своє обличчя. Однак важливо пам’ятати, що безпомилкових онлайн-інструментів не існує, і біометрична автентифікація не є винятком. Зловмисники йдуть у ногу з технологією та запровадили такі методи, як розпізнавання зображень, щоб підробити особу людини. Ось чому біометрична автентифікація є найціннішою в поєднанні з іншими методами автентифікації.

Єдиний вхід (SSO) - це метод перевірки, який дозволяє користувачам застосовувати уніфікований набір облікових даних для кількох облікових записів. Система SSO особливо популярна в бізнесі, оскільки вона спрощує процес входу для співробітників, які можуть отримати доступ до кількох підключених додатків і

служб, увійшовши лише один раз, використовуючи один набір облікових даних.

Система SSO перевіряє облікові дані користувача щоразу, коли користувач входить до платформи, інтегрованої з SSO. Він видає маркер або цифровий сертифікат, який перевіряється, коли користувач намагається отримати доступ до іншої інтегрованої програми. Якщо він підтверджений, користувач отримує доступ до програми без повторного входу.

Система єдиного входу може забезпечити майже плавний перехід між інтегрованими програмами та службами, оскільки це допомагає користувачам скоротити облікові записи та облікові дані для входу, якими вони повинні керувати.

Однак важливо мати на увазі, що якщо хакер отримує доступ до облікових даних користувача SSO, він отримує доступ до всіх підключених програм. Це головна причина, чому SSO зазвичай використовується з MFA, отримуючи рівень безпеки на додаток до зручності роботи.

Аутентифікація на основі сертифіката – це метод перевірки, коли користувач підтверджує свою особу, надаючи цифровий сертифікат серверу автентифікації. Ці сертифікати видаються центром сертифікації (CA), третьою стороною, яка перевіряє, чи юридична особа - особа чи організація - є легітимною, перш ніж видати їй сертифікат. Цифровий сертифікат зазвичай поєднує цифрову особу користувача та цифровий підпис центру сертифікації, що підтверджує цю особу. Коли користувач намагається підключитися до облікового запису за допомогою цифрового сертифіката, сервер автентифікації спочатку перевіряє, чи сертифікат дійсний (термін дії не закінчився або не відкликаний) і чи його видано довіреним ЦС. Потім сервер надсилає криптографічне повідомлення на пристрій користувача, який повинен відповісти правильною відповіддю, пов’язаною з сертифікатом. Якщо відповідь правильна, сервер підтверджує особу користувача та надає йому доступ до облікового запису. Завдяки автентифікації на основі сертифікатів системи можуть автентифікувати користувачів із мінімальним втручанням людини, знімаючи з користувачів тягар керування численними обліковими даними для входу. З іншого боку, якщо зловмисники коли-небудь скомпрометують цифровий

сертифікат, вони можуть видати себе за користувача, щоб отримати доступ до кількох облікових записів. Інша проблема може виникнути, якщо центр сертифікації буде зламано – тоді всі сертифікати, видані ним, можуть опинитися під загрозою.

Автентифікація пристрою - це процес ідентифікації та перевірки пристрою, наприклад телефону чи комп'ютера, перед тим, як він отримає доступ до мережі чи служби.

Це допомагає переконатися, що пристрій є законним і надійним, перш ніж він підключатиметься до конфіденційних систем або даних. Автентифікація пристрою часто поєднується з іншими методами автентифікації користувача, такими як MFA, біометрична автентифікація або цифрові сертифікати. Цей тип автентифікації особливо корисний у бізнес-середовищі, коли працівникам може знадобитися підключитися до мереж або отримати конфіденційну інформацію під час віддаленої роботи. Автентифікація пристрою додає додатковий рівень безпеки, перевіряючи користувача та його пристрій, щоб лише схвалені пристрої мали доступ до корпоративних ресурсів.

1.4 Ідентифікація користувачів

Ідентифікація користувача або ідентифікатор користувача - це об'єкт, який використовується для ідентифікації користувача на веб-сайті, програмному забезпеченні, системі або в загальному IT-середовищі. Це найпоширеніший механізм автентифікації, який використовується в обчислювальних системах. Незалежно від типу користувача та його прав, кожен користувач має унікальну ідентифікацію, яка відрізняє його від інших користувачів. Системні адміністратори використовують ці ідентифікатори для призначення привілеїв, відстеження активності користувачів і керування загальними операціями в конкретній системі, мережі чи програмі. Багато аналітичних технологій не можуть ідентифікувати

унікальних користувачів, якщо вони використовують кілька пристроїв протягом кількох сеансів.

Оскільки щоразу, коли користувач робить це, зараховується новий користувач. Маючи унікальний ідентифікатор користувача, це усуває цю проблему, дозволяючи відносити всю діяльність до одного користувача в аналітичному звіті.

Ідентифікатор користувача (також ідентифікатор користувача) ідентифікує користувача за допомогою унікального ідентифікатора користувача та надає доступ до комп'ютера або мережі. Для автентифікації в мережі використовується інформація про користувача, яка є індивідуальною для кожного користувача. Для входу в систему потрібно кожного разу вводити ідентифікатор користувача, який зазвичай складається з імені або псевдоніма та пароля. Доступ до захищеної системи надається лише після правильного введення ідентифікатора користувача. Після закінчення сеансу користувач повинен знову вийти з системи. Якщо вихід з системи пропущено, доступ до захищеної області часто залишається активним. Тому з міркувань конфіденційності кожному слід звернути увагу на вихід із системи. Системний адміністратор також може примусово завершити вихід із системи після закінчення певного часу.

Ідентифікатор користувача пов'язаний з обліковим записом користувача Нині доступ до комп'ютера, а також до більшості онлайн-сервісів регулюється індивідуальним логіном. Користувач повинен спочатку увійти під своїм ідентифікатором користувача, а потім отримати доступ до захищених файлів, служб або мереж. Зокрема, в Інтернеті навряд чи будь-яка послуга може бути виконана без ідентифікатора користувача. Інтернет-банкінг, постачальники послуг електронної пошти, соціальні мережі, форуми чи веб-магазини - усі ці різні служби покладаються на ідентифікатори користувачів для чіткого призначення користувачів і захисту конфіденційних даних від несанкціонованого доступу. Ідентифікатор користувача пов'язаний з обліковим записом користувача, якому можна призначити спеціальні права.

Користувачі очікують безпеки, особливо банківських даних Контроль

доступу часто використовується в Інтернеті. У випадку з інтернет-магазинами, операторами телекомунікацій або іншими платними послугами користувачі також повинні ввести свої банківські реквізити. Це особливо цікаво для хакерів, тому провайдер повинен докладати особливих зусиль для захисту банківських даних. Створення ідентифікатора користувача супроводжується прийняттям правил користувача. Кожен, хто створює ідентифікатор користувача та вперше входить до служби, повинен ввести дійсну адресу електронної пошти. Потім на цю електронну адресу буде надіслано посилання для підтвердження для автентифікації. Лише після переходу по цьому посиланню послуга активується для користувача. Реєструючись, користувач приймає умови користування відповідним сервісом. Кожен, хто порушує ці правила, може бути назавжди виключений із мережі.

1.5 Автентифікація за допомогою одноразових паролів

Одноразовий пароль або одноразовий пароль - це код безпеки, розроблений для використання під час одноразової спроби входу або транзакції, щоб мінімізувати ризик шахрайських спроб і підтримувати високий рівень безпеки. Одноразові паролі є більш безпечними, ніж статичні паролі, створені користувачами, і їх потенційне повторне використання в кількох облікових записах. Одноразові паролі це рядок символів або цифр, які автоматично генеруються та надсилаються на телефон користувача через SMS, голосове або Push-повідомлення. Генерація зашифрованого коду OTP PIN-код, який надходить на телефон клієнта, не є зі списку та не зберігається протягом тривалого часу.

Він генерується так само, як і криптографічні ключі, які захищають банківські рахунки: «одностороння хеш-функція», що передбачає генерацію та множення великих простих чисел.

Цей метод має корисну якість такі коди відносно легко згенерувати, але практично неможливо «відстежити» або дізнатися, як код був згенерований,

дивлячись на результат.

Це означає, що одноразовий пароль, який бачить клієнт, справді непередбачуваний: навіть якщо зловмисник мав списки з мільйонів одноразових паролів, немає жодного «шаблону», який би дозволив йому отримати інформацію про те, який одноразовий пароль буде згенеровано для певного клієнта в майбутньому. OTP став стандартним методом увімкнення входу в систему за особливих обставин, як-от підтвердження нового облікового запису або підтвердження законності транзакції. Також відомий як одноразовий PIN-код, одноразовий код авторизації (OTAC) або динамічний пароль. Зазвичай це шестизначне число, яке надсилається на телефон клієнта за допомогою SMS-повідомлення, а потім вводиться клієнтом на сайті чи в додатку. вони намагаються увійти. Одноразовий пароль (OTP), також відомий як одноразовий PIN-код, одноразовий код авторизації (OTAC) або динамічний пароль, - це пароль, дійсний лише для одного сеансу входу або транзакції в комп'ютерній системі чи іншому цифровий пристрій.

Одноразові паролі уникають кількох недоліків, пов'язаних із традиційною (статичною) автентифікацією на основі пароля; ряд реалізацій також включають двофакторну автентифікацію, гарантуючи, що одноразовий пароль також вимагає доступу до чогось, що є у людини (наприклад, невеликого брелока з вбудованим калькулятором OTP, або смарт-картки, чи окремого мобільного телефону). як щось, що людина знає (наприклад, PIN-код).

Алгоритми генерації OTP зазвичай використовують псевдо випадковість або випадковість для генерації спільного ключа або початкового числа, а також криптографічні хеш-функції, які можна використовувати для отримання значення, але їх важко повернути назад, і тому зловмиснику важко отримати дані, які використовувалися для хеш. Це необхідно, оскільки інакше було б легко передбачити майбутні OTP, спостерігаючи за попередніми. Одноразові паролі обговорювалися як можлива заміна традиційних паролів, а також як покращення

звичайних користувацьких паролів.

З іншого боку, одноразові паролі можуть бути перехоплені або перенаправлені, а жорсткі маркери можуть бути втрачені, пошкоджені або вкрадені. Багато систем, які використовують одноразові паролі, не реалізують їх безпечно, і зловмисники можуть дізнатися пароль під час фішингових атак, щоб видати себе за авторизованого користувача. Protect - це приклад генератора одноразових паролів, який можна використовувати як програму на телефоні. Щоразу, коли ви отримуєте SMS із кодом, який допоможе вам увійти на веб-сайт або програму, ви використовуєте одноразовий пароль.

Щодня по всьому світу надсилаються мільйони одноразових паролів, і значна частина з них надсилається через SMS. З поважною причиною: люди тримають свої мобільні телефони під рукою 24 години на добу, і як цінне особисте майно телефоном зазвичай користується одна людина, що робить його чудовим каналом для підтвердження того, ким вони себе видають. Загальна ідея одноразового пароля полягає в тому, щоб додати другий рівень автентифікації, щоб випередити кіберзлочинність і захистити свою організацію від катастрофічних наслідків шахрайства для вашого бізнесу. Ризик шахрайства значно зменшується, якщо користувачеві не потрібно лише вводити своє ім’я користувача та пароль (щось, що він знає), а й щось, що він «є», щоб завершити вхід.

Цим «чимось» може бути телефон користувача. OTP бувають усіх форм і розмірів, але завжди додають додатковий рівень автентифікації. Одноразові паролі використовуються, коли транзакція потребує додаткового захисту або альтернативного методу підтвердження особи клієнта.

Коли виникає розпізнана ситуація клієнту потрібно нагадати пароль, банк підтверджує транзакцію, що не відповідає шаблону, і в багатьох інших випадках (див. нижче) - запит на одноразовий пароль робиться або самим клієнтом, або клієнтом. установа, з якою вони мають справу. OTP генерується автоматично як напів випадкове число або рядок символів.

Неможливо заздалегідь передбачити, яким буде OTP; також одноразові паролі

зазвичай обмежені за часом, їх можна використовувати лише протягом кількох хвилин. Одноразові паролі мають обмежений час використання Крім того, термін придатності OTP дуже короткий: рідко перевищує півгодини, а іноді лише кілька хвилин. Іншими словами, ситуація, на яку вони відповідають, дуже обмежена в часі. Це клієнт, який сидить за своїм столом і намагається увійти до свого облікового запису, або клієнт, який стоїть біля торгової стійки та підтверджує, що її платіж законний. Це ще один плюс для використання SMS через інші канали. Хоча SMS спочатку не розроблявся як технологія обміну миттєвими повідомленнями, на практиці більшість глобальних мобільних мереж передадуть текстове повідомлення від джерела до одержувача лише за кілька секунд. Є кілька способів надіслати OTP. Деякі надають можливість отримувати OTP електронною поштою, хоча це, як правило, менш безпечно. Інші постачальники навіть вмикають одноразові паролі як голосові повідомлення, повідомляючи PIN-код вголос, коли клієнт перевіряє поштову скриньку. Але найпоширенішим способом надсилання одноразових паролів є мобільне повідомлення, як правило, SMS на мобільний телефон клієнта.

1.6 Автентифікація за допомогою багаторазових паролів

Однією з поширених схем аутентифікації є проста аутентифікація, яка заснована на застосуванні традиційних багаторазових паролів з одночасним узгодженням засобів його використання і обробки. Базовий принцип «єдиного входу» передбачає достатність одноразового проходження користувачем процедури аутентифікації для доступу до всіх мережевих ресурсів. Процедура простої аутентифікації користувача в мережі полягає в наступному.

При спробі логічного входу в мережу користувач набирає на клавіатурі комп'ютера свої ідентифікатор і пароль. Ці дані надходять для обробки на сервер аутентифікації. У базі даних, що зберігається на сервері аутентифікації, за

ідентифікатором користувача знаходиться відповідний запис, з неї витягується пароль і порівнюється з тим паролем, який ввів користувач.

Якщо вони співпали, то аутентифікація пройшла успішно, користувач отримує легальний статус і ті права і доступ до ресурсів мережі, які визначені для його статусу системою авторизації. У схемі простий аутентифікації передача пароля та ідентифікатора користувача.

OTP – це одноразовий пароль, який використовується для автентифікації користувача. На відміну від звичайних паролів, OTP генерується і діє лише протягом короткого часу або для одного сеансу входу. Автентифікація за допомогою багаторазових паролів (One-Time Passwords, OTP) є важливою складовою сучасних систем безпеки. Ця технологія дозволяє значно підвищити рівень захисту користувачів від різних видів атак, таких як фішинг, атаки повторного використання паролів та інші.

Етапи роботи OTP:

– пароль генерується за допомогою спеціальних алгоритмів;

– користувач отримує одноразовий пароль на свій пристрій і вводить його в систему для підтвердження своєї особи;

– система перевіряє введений користувачем пароль на відповідність згенерованому паролю. якщо вони збігаються, користувач отримує доступ до системи.

Типи OTP:

– time-based one-time password (totp) пароль генерується на основі часу. він змінюється через певний інтервал часу;

– hmac-based one-time password (hotp) пароль генерується на основі лічильника, який збільшується кожного разу, коли генерується пароль.

1.7 Переваги та недоліки існуючих методів автентифікації

Переваги паролів. паролі легко створювати та використовувати. користувачі

вводять текстовий пароль для доступу до системи, що не вимагає спеціальних знань або навичок практично всі системи, від веб-сайтів до операційних систем, підтримують автентифікацію за допомогою паролів. це стандартний метод, який знайомий більшості користувачів паролі не вимагають додаткового обладнання або інфраструктури для їх використання, що робить їх економічно вигідним варіантом інтеграція паролів у системи безпеки є відносно простою та не потребує складних технологічних рішень.

Недоліками паролів є паролі те що можуть бути вкрадені, зламані або вгадані. зловмисники можуть використовувати атаки перебором, фішинг або соціальну інженерію для отримання паролів. користувачі часто обирають слабкі паролі, які легко вгадати користувачів.

Можна обманом змусити ввести свої паролі на фальшивих веб-сайтах або в підроблених додатках, що дозволяє зловмисникам отримати доступ до їхніх облікових записів багато користувачів використовують однакові паролі для різних облікових записів. якщо один з таких паролів буде зламано, це створює ризик для інших облікових записів користувача керування паролями користувачам важко запам’ятовувати багато різних паролів, особливо якщо вони складні та унікальні. це призводить до використання слабких паролів або їх записування, що може стати додатковим ризиком невідповідність сучасним вимогам безпеки.

У сучасних умовах паролі самі по собі не забезпечують достатнього рівня захисту. багато систем переходять на багатофакторну автентифікацію (mfa), що поєднує паролі з іншими методами автентифікації, щоб підвищити безпеку.

Паролі є простим і поширеним методом автентифікації, але вони мають суттєві недоліки, особливо в контексті сучасних загроз кібербезпеки. Для підвищення рівня захисту рекомендується використовувати паролі разом з іншими методами автентифікації, такими як двофакторна автентифікація (2FA) або багатофакторна автентифікація (MFA). Мультифакторна автентифікація (MFA) - є підходом, який підвищує безпеку шляхом використання кількох незалежних

методів перевірки особи користувача.

Перевагами MFA є те що підвищена безпека використання кількох факторів автентифікації значно ускладнює доступ для зловмисників, навіть якщо один з факторів буде скомпрометований. Наприклад, якщо пароль вкрадено, зловмисник все одно не зможе увійти без додаткового фактора, такого як одноразовий код або біометричні дані забезпечує захист від широкого спектра атак, таких як фішинг, атаки перебором паролів та атаки соціальної інженерії. Зловмисникам значно складніше одночасно скомпрометувати декілька факторів автентифікації; MFA дозволяє використовувати менш складні паролі без втрати рівня безпеки.

Оскільки додаткові фактори забезпечують необхідний рівень захисту покращена відповідність вимогам безпеки багато галузей, включаючи фінансові послуги та охорону здоров'я, мають нормативні вимоги щодо захисту даних, які можуть включати використання MFA для захисту конфіденційної інформації.

Недоліки MFA є те що додавання додаткових етапів автентифікації може бути незручним для користувачів, оскільки їм доводиться виконувати більше дій для доступу до своїх облікових записів.

Деякі методи MFA вимагають наявності додаткових пристроїв, таких як смартфони для отримання одноразових кодів або апаратні токени. Якщо ці пристрої втрачаються або стають недоступними, користувач може мати проблеми з входом в систему. Використання декількох факторів може призвести до технічних проблем, таких як збої в роботі серверів, проблеми з доставкою кодів через SMS або перебої.

В роботі біометричних сканерів впровадження та підтримка систем MFA може вимагати додаткових витрат на апаратне та програмне забезпечення, а також на навчання користувачів і підтримку служби технічної підтримки.

Інтеграція MFA в існуючі системи та процеси може бути складною, особливо для організацій з великою кількістю користувачів або старими системами, які не підтримують сучасні методи автентифікації. MFA - забезпечує значно вищий рівень безпеки порівняно з традиційною автентифікацією за допомогою паролів. Однак вона може додати деякі складнощі та незручності як для користувачів, так і для

адміністраторів. Незважаючи на це, у багатьох випадках переваги MFA, особливо в контексті захисту від сучасних кіберзагроз, переважають її недоліки, що робить її важливою складовою стратегії кібербезпеки. Біометрична автентифікація- використовує унікальні фізичні або поведінкові характеристики людини для перевірки її особи. Розглянемо основні переваги та недоліки цього методу.

Переваги біометричної автентифікації біометричні дані є унікальними для кожної людини, що робить їх важкими для підробки або крадіжки. Наприклад, відбитки пальців, розпізнавання обличчя або райдужної оболонки ока мають високий рівень точності для користувачів біометрична автентифікація усуває необхідність запам'ятовувати паролі або носити з собою додаткові пристрої. Користувачі можуть швидко та легко проходити автентифікацію.

За допомогою відбитка пальця або розпізнавання обличчя біометрична автентифікація може бути виконана дуже швидко, часто протягом частки секунди, що зменшує час очікування для користувачів підробити біометричні дані значно складніше, ніж інші форми автентифікації, такі як паролі або одноразові коди біометричні дані завжди при собі, їх неможливо загубити або забути, що зменшує ймовірність проблем з доступом через втрату або забування паролів.

Недоліки біометричної автентифікації проблеми з конфіденційністю збір та зберігання біометричних даних викликає занепокоєння щодо конфіденційності. Якщо біометричні дані будуть викрадені або зламані, їх не можна змінити, як це можна зробити з паролем для використання біометричної автентифікації потрібні спеціальні пристрої, такі як сканери відбитків пальців, камери для розпізнавання обличчя або інші біометричні сенсори. Це може збільшити вартість та складність впровадження біометричні системи можуть допускати помилкові відмови (false negatives) або помилкові допуски (false positives). Наприклад, відбитки пальців можуть не розпізнати через пошкодження шкіри, а розпізнавання обличчя може помилитися через зміну зовнішнього вигляду деякі користувачі можуть мати упередження проти біометричної автентифікації через занепокоєння щодо конфіденційності та безпеки своїх особистих даних якість та надійність

біометричних сенсорів може варіюватися, що впливає на загальну ефективність системи. Крім того, деякі умови навколишнього середовища, такі як погане освітлення або надмірний шум, можуть впливати на точність розпізнавання.

Біометрична автентифікація пропонує високий рівень безпеки та зручності, але також має певні недоліки, зокрема проблеми з конфіденційністю, залежність від апаратного забезпечення та можливість помилок у розпізнаванні. Успішне впровадження біометричної автентифікації потребує збалансування цих факторів та врахування специфічних вимог і ризиків конкретної системи.

Єдиний вхід (Single Sign-On, SSO) - є методом автентифікації, що дозволяє користувачам використовувати один набір облікових даних для доступу до кількох додатків або систем. Розглянемо основні переваги та недоліки SSO.

Переваги SSO покращена зручність для користувачів. користувачам потрібно запам'ятовувати лише одні облікові дані для доступу до різних систем. це зменшує кількість логінів та спрощує процес доступу.

Замість того, щоб вводити облікові дані для кожної окремої системи, користувач проходить автентифікацію один раз, що економить час та підвищує продуктивність адміністратори можуть централізовано контролювати політику безпеки, забезпечувати використання сильних паролів та регулярно їх оновлювати. це зменшує ймовірність використання слабких або повторюваних паролів управління обліковими записами стає простішим та ефективнішим, оскільки адміністратори можуть централізовано контролювати доступ користувачів до різних систем SSO зменшує кількість паролів, які потрібно запам'ятовувати, та кількість входів у різні системи, що покращує загальний користувацький досвід.

Недоліки SSO якщо система SSO виходить з ладу або стає мішенню атаки, користувачі можуть втратити доступ до всіх підключених систем та додатків. це може мати серйозні наслідки для бізнес-процесів через те, що один набір облікових даних дає доступ до кількох систем, ці облікові дані стають привабливішою ціллю для зловмисників. це робить їх більш вразливими до фішингу та взлому методом

грубої сили та інших атак впровадження.

SSO може бути складним і потребувати інтеграції з існуючими системами та додатками. це може вимагати значних зусиль та ресурсів не всі додатки та системи можуть підтримувати SSO. це може призвести до необхідності використання додаткових методів автентифікації для окремих систем, що знижує загальні переваги SSO центральне управління обліковими даними може викликати занепокоєння щодо конфіденційності. Неправильне налаштування або компрометація системи SSO може призвести до витоку чутливих даних. SSO - є потужним інструментом для підвищення зручності та ефективності управління доступом, але воно також має свої ризики та обмеження. Для успішного впровадження SSO необхідно ретельно планувати заходи безпеки, забезпечувати надійність системи та враховувати потенційні проблеми з сумісністю та конфіденційністю.

Автентифікація на основі сертифікатів - використовує цифрові сертифікати для підтвердження особи користувача або пристрою. Цифрові сертифікати видаються центрами сертифікації (Certificate Authorities, CA) і містять криптографічні ключі. Розглянемо основні переваги та недоліки цього методу автентифікації.

Переваги автентифікації на основі сертифіката цифрові сертифікати використовують асиметричне шифрування, яке забезпечує високий рівень безпеки. злом приватного ключа є дуже складним завданням, що значно ускладнює несанкціонований доступ сертифікати забезпечують аутентичність сервера і користувача, що робить їх стійкими до фішингових атак, оскільки зловмисник не може легко підробити сертифікат; автентифікація на основі сертифікатів може бути автоматизованою, що зменшує потребу в ручному введенні облікових даних і підвищує зручність для користувачів сертифікати можуть містити додаткову інформацію про права доступу та привілеї користувача.

Що дозволяє точніше керувати доступом до ресурсів використання сертифікатів усуває необхідність зберігати та вводити паролі, що знижує ризики,

пов'язані з паролями (наприклад, забування паролів або використання слабких паролів).

Недоліки автентифікації на основі сертифіката налаштування та підтримка інфраструктури відкритих ключів (pki) можуть бути складними і вимагати значних ресурсів та технічної експертизи вартість отримання та підтримки цифрових сертифікатів може бути високою, особливо якщо використовуються сертифікати від авторитетних центрів сертифікації необхідно ефективно керувати життєвим циклом сертифікатів, включаючи видачу, оновлення та відкликання сертифікатів. це може бути складним завданням, особливо в великих організаціях надійність системи автентифікації залежить від надійності та безпеки центру сертифікації. якщо центр сертифікації буде скомпрометований, це може поставити під загрозу безпеку всієї системи.

Якщо приватний ключ користувача буде втрачений або скомпрометований, користувач втратить можливість автентифікації, і зловмисники можуть отримати доступ до захищених ресурсів.

Автентифікація на основі сертифікатів забезпечує високий рівень безпеки і зручності, але вона має свої складності та витрати, пов'язані з впровадженням і управлінням. Цей метод підходить для середовищ, де необхідний високий рівень безпеки і є можливість забезпечити відповідну інфраструктуру для Сертифікатна автентифікація використовує цифрові сертифікати, які видаються центром сертифікації (CA). Кожен користувач або пристрій отримує унікальний сертифікат, який підтверджує його особу. Цифровий сертифікат містить публічний ключ користувача, який використовується для шифрування даних, та підпис центру сертифікації, що гарантує його дійсність. управління сертифікатами.

1.8 Висновок до першого розділу

У сучасному цифровому світі аутентифікація користувачів є критичною для

захисту систем та даних від несанкціонованого доступу. Існує багато різних типів і методів аутентифікації, які можна використовувати, і важливо вибрати найкращі для ваших конкретних потреб. Важливо також використовувати надійні паролі та інші фактори аутентифікації, а також регулярно оновлювати їх.

Окрім аутентифікації, важливо також використовувати методи авторизації для керування доступом користувачів до систем та даних. Авторизація визначає, до чого кожен користувач має доступ, і допомагає гарантувати, що користувачі не матимуть доступу до даних або систем, до яких їм не потрібен доступ.

Створити політику паролів вона повинна включати вимоги щодо складності паролів, їх регулярної зміни та заборону повторного використання паролів проводити навчання користувачів користувачі повинні знати про ризики кібербезпеки та кращі практики захисту своїх облікових записів застосовувати оновлення та використовувати надійні програмні забезпечення. слідкувати за активністю користувачів моніторинг активності може допомогти виявити підозрілу поведінку та вжити заходів до її припинення. Забезпечення комплексного підходу до аутентифікації, авторизації та кібербезпеки має стати пріоритетом для організацій та окремих осіб.

Це допоможе захистити конфіденційні дані, запобігти фінансовим втратам та зберегти довіру в цифровому середовищі. Кращі практики захисту облікових записів включають застосування оновлень та використання надійного програмного забезпечення. Важливо слідкувати за активністю користувачів, адже моніторинг активності може допомогти виявити підозрілу поведінку та вжити заходів для її припинення. Забезпечення комплексного підходу до аунтетифікації та авторизації та кібербезпеки повинно стати пріоритетом для організації та окремих осіб. Це сприятиме захисту конфідеційних данних, запобіганню фінансовим втратам та збереженню довіри в цифровому середовищі.

2 ТЕХНОЛОГІЇ ОДНОРАЗОВИХ ПАРОЛІВ

2.1 Аналіз OTP

Одноразовий пароль (OTP), Одноразовий пароль - це автоматично згенерований код, який надсилається на відомий пристрій, що належить користувачеві, після спроби входу. Щоб авторизуватися, користувач має ввести код, який зазвичай надсилається через текстове повідомлення або електронну пошту. На відміну від традиційних паролів, які не змінюються, одноразовий пароль дійсний лише для одного використання протягом встановленого періоду, як правило, від п’яти до 10 хвилин. також відомий як одноразовий PIN-код, одноразовий код авторизації (OTAC) або динамічний пароль, це пароль, дійсний лише для одного сеансу входу.

Одноразові паролі уникають кількох недоліків, пов’язаних із традиційною (статичною) автентифікацією на основі пароля; ряд реалізацій також включають двофакторну автентифікацію, гарантуючи, що одноразовий пароль також вимагає доступу до чогось, що є у людини (наприклад, невеликого брелока з вбудованим калькулятором OTP, або смарт-картки, чи окремого мобільного телефону). як щось, що людина знає (наприклад, PIN-код).Алгоритми генерації OTP зазвичай використовують псевдовипадковість або випадковість для генерації спільного ключа або початкового числа, а також криптографічні хеш-функції, які можна використовувати для отримання значення, але їх важко повернути назад, і тому зловмиснику важко отримати дані, які використовувалися для хеш. Це необхідно, оскільки інакше було б легко передбачити майбутні OTP, спостерігаючи за попередніми Одноразові паролі обговорювалися як можлива заміна традиційних паролів, а також як покращення традиційних паролів. З іншого боку, одноразові паролі можуть бути перехоплені або перенаправлені, а жорсткі маркери можуть бути втрачені, пошкоджені або вкрадені. Багато систем, які використовують одноразові паролі, не реалізують їх безпечно, і зловмисники можуть дізнатися пароль під час фішингових атак, щоб видати себе за авторизованого користувача.

2.2 Принцип роботи OTP

Одноразові паролі працюють як динамічний механізм автентифікації, який створює одноразові паролі для кожного сеансу або транзакції. Його функціонування включає декілька етапів, від генерації паролю до його використання і перевірки. Перший етап - генерація OTP є ключовим процесом, який забезпечує унікальність і безпеку одноразового паролю для кожного сеансу або транзакції. На цьому етапі вибирається алгоритм генерації OTP. Є всього два метода генерації HOTP та TOTP. Другий етап - це процес доставки пароля від сервера користувачу для цього використовуються один з каналів а саме:

- SMS;
- електронна пошта;
- мобільні додатки;
- токени.

Третій етап - користувач вводить отриманий одноразовий пароль у відповідне поле на веб-сайті або в додатку, де вимагається автентифікація. Останній етап - на цьому етапі сервер або автентифікаційна система перевіряє отриманий від користувача OTP та проводиться порівняння між OTP сервера та користувача як що паролі співпадають користувач проходить аунтентифікацію та отримую доступ до свого аккаунта або транзакції як що ні користувач отримає повідомлення про помилку аутентифікації. Принцип роботи одноразових паролів (OTP) базується на створенні унікальних паролів, які можна використовувати лише один раз. OTP широко використовуються в системах двофакторної автентифікації для забезпечення додаткового рівня безпеки. Вони запобігають повторному використанню захоплених паролів, що значно ускладнює роботу зловмисникам. Генерація одноразових паролів може здійснюватися різними методами.

Серед яких найпоширенішими є часова синхронізація та використання лічильників. На першому етапі сервер і клієнт обмінюються секретним ключем. Цей ключ є унікальним для кожного користувача і зберігається в захищеному

вигляді Кожен одноразовий пароль генерується на основі поточного часу, розділеного на фіксовані часові інтервали (наприклад, 30 секунд). Клієнт обчислює геш від поєднання секретного ключа і поточного часового інтервалу за допомогою алгоритму HMAC (Hash-based Message Authentication Code). Результатом є геш, який потім перетворюється у одноразовий пароль. Генерований геш перетворюється в цифровий код певної довжини (зазвичай 6 або 8 цифр), який і є одноразовим паролем.

Процес валідації одноразових паролів є критичним для забезпечення безпеки автентифікації. Сервер повинен підтвердити, що введений користувачем пароль є дійсним і був згенерований легітимним пристроєм. Користувач вводить згенерований одноразовий пароль, який передається на сервер для валідації. Сервер обчислює поточний часовий інтервал аналогічно клієнту. Сервер генерує одноразовий пароль, використовуючи той самий секретний ключ і поточний часовий інтервал. Сервер порівнює згенерований одноразовий пароль з отриманим від користувача. Якщо паролі співпадають, автентифікація вважається успішною. Додатково сервер може перевірити паролі в межах декількох часових інтервалів (наприклад, ±1 інтервал), щоб компенсувати можливі розбіжності у часі. Для забезпечення безпеки одноразових паролів застосовуються декілька заходів. Секретний ключ зберігається у зашифрованому вигляді як на сервері, так і на клієнтському пристрої. Одноразові паролі дійсні лише протягом короткого періоду часу або після одного використання, що запобігає їх повторному використанню. Сервер і клієнт можуть використовувати механізми для синхронізації часу або лічильників, щоб мінімізувати можливість розбіжностей, які можуть бути використані зловмисниками.

Таким чином, процеси генерації та валідації одноразових паролів є комплексними та включають використання криптографічних алгоритмів для забезпечення надійності та безпеки автентифікації. Вони відіграють ключову роль у сучасних системах захисту інформації, забезпечуючи додатковий рівень безпеки для користувачів та їх даних.

Всі етапи генерації OTP зображені на рисунку 2.1.

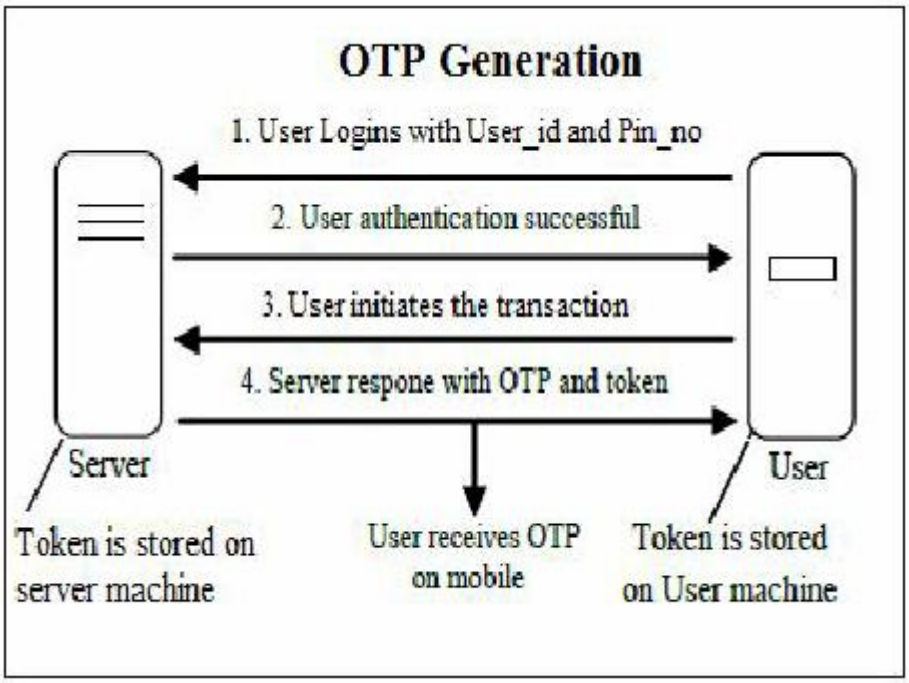


Рисунок 2.1 - Етапи генерації одноразових паролів

2.3 Принцип генерації OTP алгоритмом TOTP

Алгоритм TOTP (RFC 6238) передбачає, що OTP є продуктом двох параметрів, зашифрованих разом. Це загальне значення, яке є спільним секретним ключем або початковим числом; і змінна, в даному випадку - час роботи. Ці параметри шифруються за допомогою хеш-функції. Алгоритм TOTP відповідає відкритому стандарту, задокументованому в RFC 6238. Вхідні дані включають спільний секретний ключ і системний час.

На рисунку 2.2 нижче зображено, як програми автентифікації, такі як Google Authenticator і Server, генерують пароль без підключення до Інтернету.

Коли користувач встановлює TOTP, сервер генерує секретний ключ - набір випадкових чисел і букв. Потім він зберігає цей ключ у телефоні, зазвичай

скануючи QR-код (2D штрих-код) за допомогою програми автентифікації. (Якщо в користувача телефоні немає камери.

Замість цього маємо можливість вручну ввести довгий код.) Тепер і телефон, і сервер мають копію цього секретного ключа. Коли користувач хоче увійти, йому потрібно довести, що у нього є ключ. Для цього додатки поєднують ключ із поточним часом (з точністю до 30 секунд), щоб створити код доступу. Він робить це за допомогою так званого «безпечного хешування».

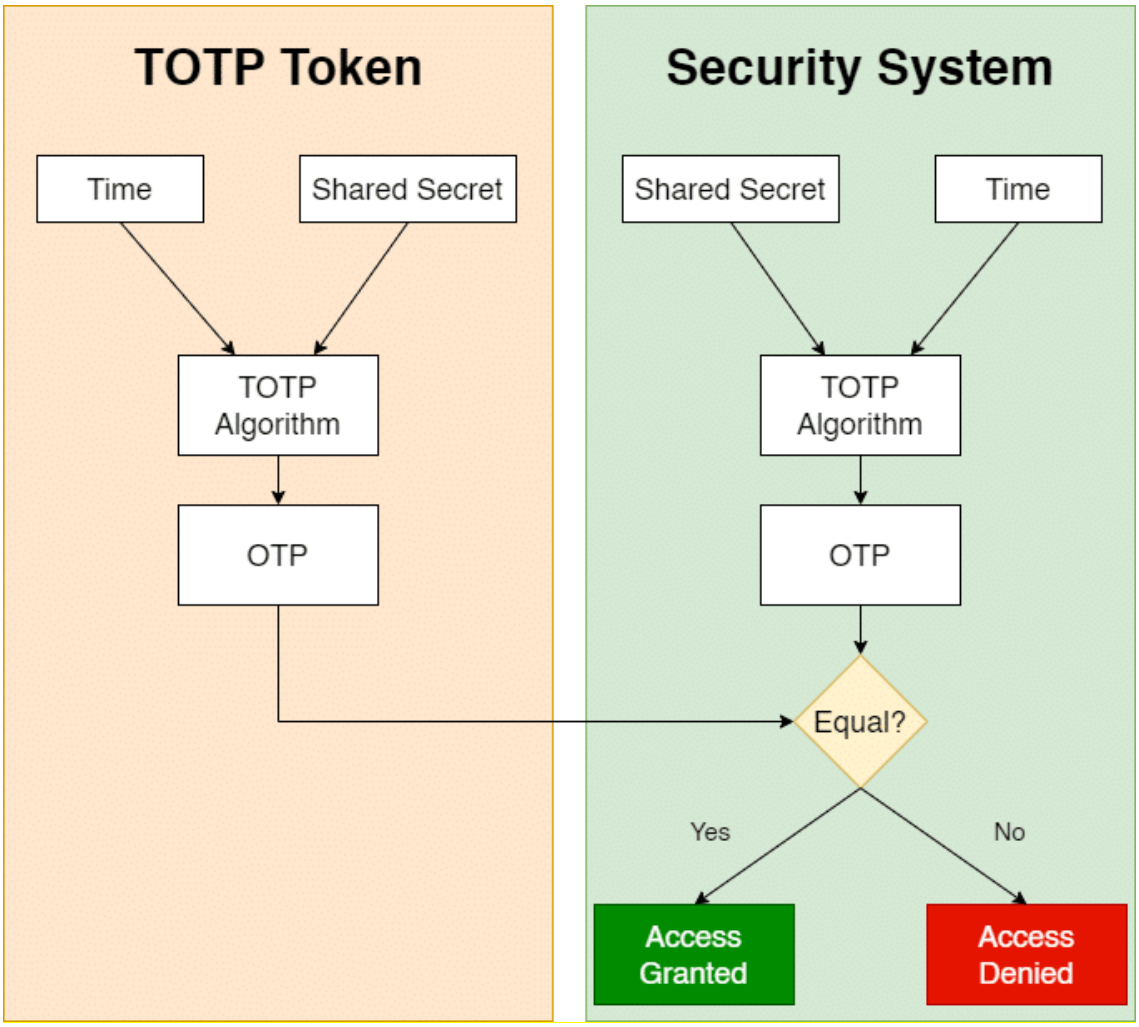


Рисунок 2.2 - Алгоритм генерації одноразових паролів за часом

З точки зору неспеціаліста, він змішує час і ключ разом, щоб отримати унікальний вихід (якщо час або ключ відрізняються бодай незначною мірою, результат буде зовсім іншим), але який неможливо повернути назад (навіть якщо

користувач знає час це не допоможе йому вгадати секретний ключ). Також Для полегшення введення код доступу скорочено до 6-значного числа.

Адміністратори часто використовують одноразові паролі (ТОТР) як другий фактор. Токени ТОТР - це випадкові цифрові коди, які генерує програма, яка автоматично оновлюється. ТОТР 2FA пропонує багато переваг безпеки, але є також кілька недоліків, які слід враховувати.

Переваги алгоритму ТОТР: організації часто використовують ТОТР 2FA через те, наскільки він доступний, більшість програм автентифікації, які генерують токени ТОТР, безкоштовні або стягують невелику плату, тож організації будь-якого розміру можуть захистити ідентифікаційні дані своїх користувачів, якщо захочуть організаціям не потрібно встановлювати нове обладнання для автентифікації користувачів у своїх IT-ресурсах, все, що їм потрібно, це програма для автентифікації на робочому столі, ноутбуці чи телефоні. Більшість постачальників додатків ТОТР пропонують 2FA для всіх цих пристроїв, тож користувачі можуть використовувати те, що відповідає їхнім потребам коли користувач вперше намагається отримати доступ до програми чи системи, його генератор токенів ТОТР зберігає та запам'ятовує.

Ця функція дозволяє користувачам отримувати свої коди без доступу до вайфай .

Стільникового зв’язку, оскільки їхні попередні спроби входу зберігаються на їхніх пристроях і постійно створюватимуться нові коди для цих ресурсів за допомогою правильного постачальника організації можуть застосовувати ТОТР 2FA у масштабі всіх своїх IT-ресурсів. це включає гетерогенні системи, широкий спектр програм, мереж і файлових серверів. Недоліки алгоритму ТОТР користувач не може отримати свій код ТОТР, якщо не має готової програми автентифікації, якщо вони забудуть свій телефон удома або розрядиться акумулятор пристрою, вони можуть не мати доступу до своїх IT-ресурсів може вимагати від користувача введення кількох кодів ТОТР, щоб увійти до закінчення терміну дії коду, що потребує додаткового часу та може призвести до блокування облікового запису,

якщо він перевищить відведену кількість спроб TOTP 2FA використовує секретний ключ, спільний між програмою автентифікації та сервером, на якому вона розміщена, якби зловмисник клонував цей секретний ключ, він міг би створити дійсні коди за бажанням і отримати доступ до облікового запису користувача

Принцип генерації одноразових паролів (OTP) алгоритмом TOTP базується на використанні часових міток для генерації паролів. Це означає, що одноразовий пароль генерується на основі поточного часу та секретного ключа, який зберігається на стороні сервера та клієнта.Основна ідея полягає в тому, що обидві сторони (сервер і клієнт) використовують поточний час як змінну для генерації пароля, що робить його дійсним лише протягом короткого проміжку часу. Такий підхід підвищує безпеку, оскільки навіть якщо пароль буде перехоплено, він стане недійсним через кілька хвилин. Що дозволяє розробляти TOTP на різних платформах. А саме мобільні додатки часто використовують TOTP для двофакторної автентифікації. Багато популярних додатків, таких як Google Authenticator, Microsoft Authenticator та Authy, підтримують генерацію одноразових паролів на основі часу.

Ці додатки забезпечують додатковий рівень безпеки для користувачів, пропонуючи генерувати паролі, які змінюються кожні 30 секунд. Користувачі додають облікові записи до додатків шляхом сканування QR-кодів або введення секретного ключа вручну. Після цього додаток генерує одноразові паролі на основі поточного часу та секретного ключа. Платформа Android надає різні бібліотеки та інструменти для розробників, які дозволяють інтегрувати функціональність TOTP у мобільні додатки. Для цього використовуються криптографічні алгоритми та часові мітки для генерації паролів, що змінюються кожні 30 секунд. Такі додатки можуть також синхронізувати годинник з сервером для точності генерації паролів. На платформі iOS також існують різні засоби для реалізації TOTP. Розробники можуть використовувати вбудовані криптографічні бібліотеки для генерації одноразових паролів. Додатки на iOS, такі як Apple ID та інші, використовують TOTP для додаткового захисту облікових записів. Також є можливість розробляти

Десктопні додатки, такі як менеджери паролів, часто інтегрують підтримку TOTP для забезпечення безпеки доступу до збережених паролів. Наприклад, програми типу 1Password, LastPass та KeePass підтримують генерацію одноразових паролів для облікових записів, додаючи додатковий рівень захисту. Десктопні додатки на Windows можуть використовувати криптографічні API для реалізації TOTP. Вони дозволяють зберігати секретні ключі та синхронізувати час з сервером для точного генерації одноразових паролів. На платформі macOS також є можливості для інтеграції TOTP у додатки. Менеджери паролів на macOS можуть використовувати вбудовані бібліотеки для генерації одноразових паролів на основі часу. Ще OTP також широко використовується у веб-сервісах для забезпечення безпеки користувачів. Багато популярних онлайн-сервісів, таких як Google, Facebook, Amazon та інші, підтримують двофакторну автентифікацію з використанням TOTP. Користувачі можуть активувати цю функцію в налаштуваннях безпеки своїх облікових записів.

Можуть використовувати додатки на своїх смартфонах для отримання одноразових паролів. Веб-сервіси можуть інтегрувати TOTP за допомогою різних криптографічних бібліотек, які забезпечують генерацію одноразових паролів на основі часу. Користувачі можуть синхронізувати свої облікові записи з додатками, які підтримують TOTP, шляхом сканування QR-коду або введення секретного ключа вручну. Це дозволяє забезпечити додатковий рівень захисту для користувачів, зменшуючи ризик несанкціонованого доступу до їхніх облікових записів. Багато веб-сервісів надають API, які дозволяють розробникам інтегрувати підтримку TOTP у свої додатки. Це забезпечує гнучкість та масштабованість для різних видів програмного забезпечення, дозволяючи використовувати TOTP у широкому спектрі застосувань. Таким чином, TOTP є ефективним та зручним способом забезпечення безпеки облікових записів, який може бути реалізований на різних платформах з використанням сучасних криптографічних методів та інструментів. ime-based One-Time Password (TOTP) є ефективним та зручним способом забезпечення безпеки облікових записів, який може бути реалізований на

різних платформах з використанням сучасних криптографічних методів та інструментів.

2.4 Принцип генерації OTP алгоритмом HOTP

Пароль на основі HMAC (або скорочено HOTP) - це алгоритм OTP на основі подій, який використовує спільний секретний ключ і лічильник подій. HMAC - механізм перевірки цілісності інформації, що передається або зберігається в ненадійному середовищі. Подібні способи є невід'ємною і необхідною частиною світу відкритих обчислень і комунікацій. HMAC використовує хеш-функцію разом з секретним ключем, що дозволяє створити унікальний код для кожного повідомлення, який можна використовувати для перевірки автентичності повідомлення. Хеш-функція використовується для створення контрольної суми повідомлення, а секретний ключ додає додатковий рівень безпеки.

Так як лише особа з доступом до секретного ключа зможе створити коректний HMAC. Механізми, які надають такі перевірки цілісності на основі секретного ключа, зазвичай називають кодом автентифікації повідомлення (MAC). Як правило, MAC використовується між двома сторонами, які поділяють секретний ключ для перевірки автентичності інформації, переданої між цими сторонами. Цей стандарт визначає MAC. Іншими словами це криптографічний метод, який включає криптографічну хеш-функцію (зазвичай SHA-1) і набір параметрів (секретний ключ, лічильник). В основі алгоритму HOTP лежить секретний ключ. Секретний ключ, який іноді називають «початковим», - це значення, яким маркер OTP і сервер обмінюються лише один раз під час ініціалізації маркера.

Потім секретний ключ надійно зберігається клієнтом і сервером і більше ніколи не надається іншим. В алгоритмі HOTP лічильник базується на подіях. Лічильник збільшується кожного разу, коли користувач натискає кнопку на маркері. Лічильник на сервері збільшується після кожної успішної автентифікації.Коди

HOTP генеруються за допомогою алгоритму одноразового пароля на основі HMAC, описаного в RFC 4226. Алгоритм генерації HOTP. Одноразовий пароль HMAC або HOTP - це одноразовий пароль на основі подій, який складається з 2 частин, а саме секретного ключа, який називається початковим, і фактора переміщення, який є лічильником для HOTP. Початкове число - це секретний ключ, який відомий лише маркеру та серверу, який перевіряє надіслані коди OTP під час ініціалізації маркера. Тоді як лічильник – це те, що зберігається в токені та на сервері. Лічильник на маркері збільшується щоразу, коли натискається кнопка на маркері, але лічильник на сервері збільшується лише тоді, коли надісланий параметр OTP успішно перевірено. Робота алгоритму HOTP зображена на рисунку 2.3.

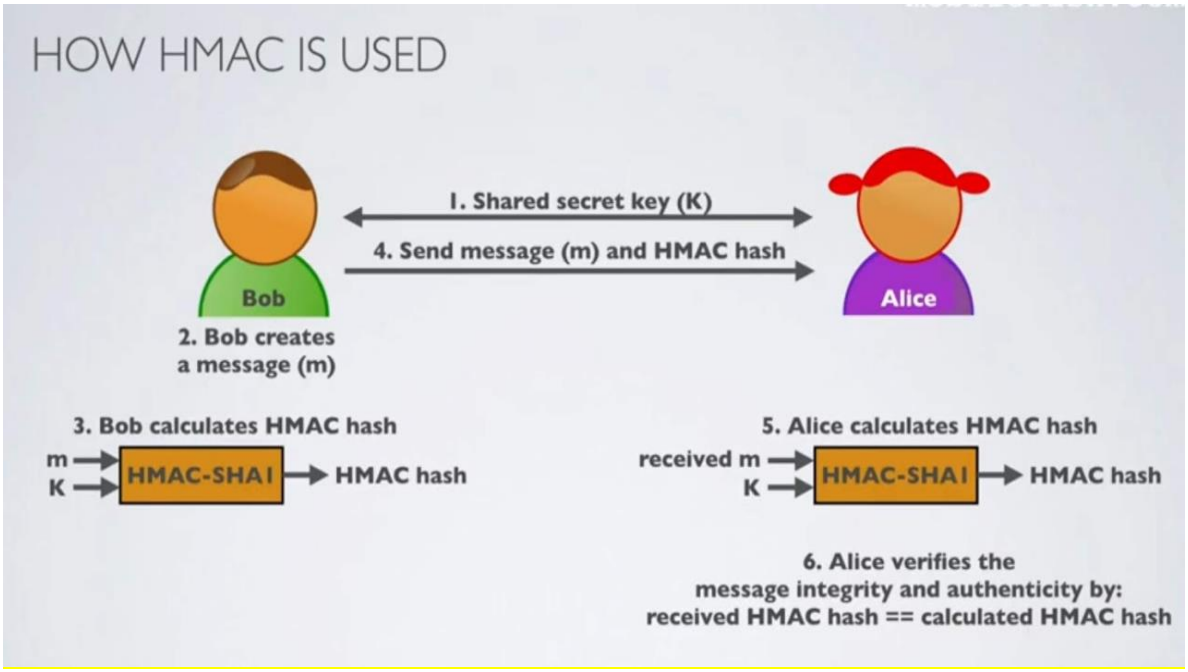


Рисунок 2.3 - Алгоритм генерації HOTP

Переваги алгоритму HOTP HOTP не обмежений терміном дії, тому це додає користувачеві певну гнучкість для введення коду будь-коли, але це також може зробити HOTP вразливим, оскільки його термін дії налаштовано на завершення лише після успішної перевірки автентифікації оскільки HOTP використовує алгоритм OTP на основі подій, він не обмежується часовими обмеженнями, це може бути дуже бажаним, якщо існує потреба в підвищеній безпеці протягом більш

тривалого періоду часу порівняно з алгоритмами OTP на основі часу, які є короткочасними HOTP легко інтегрується в існуючі системи автентифікації і може бути використаний для різних сценаріїв; використання секретного ключа і HMAC гарантує, що OTP є криптографічно стійкими та важкими для підробки.

Недоліки алгоритму HOTP якщо лічильник клієнта і сервера вийдуть з синхронізації, автентифікація може не спрацювати, це може статися, наприклад, через пропуск кількох OTP або їх невикористання користувачам необхідно вводити OTP вручну.

Що може бути незручним і схильним до помилок після кожної успішної автентифікації сервер повинен інкрементувати лічильник, що вимагає додаткових операцій і управління станом.

Принцип генерації одноразових паролів (OTP) алгоритмом HOTP (HMAC-based One-Time Password) базується на використанні криптографічного алгоритму HMAC (Hash-based Message Authentication Code) і лічильника для генерації паролів. В алгоритмі HOTP лічильник збільшується з кожною генерацією нового пароля, забезпечуючи унікальність кожного пароля.

Основною ідеєю є те, що обидві сторони (сервер і клієнт) мають синхронізований лічильник, який використовується разом із секретним ключем для створення одноразового пароля. Мобільні додатки використовують HOTP для автентифікації користувачів, забезпечуючи додатковий рівень безпеки. Багато додатків для двофакторної автентифікації, такі як Google Authenticator і Authy, підтримують HOTP, дозволяючи користувачам генерувати одноразові паролі на основі лічильника. На платформі Android розробники можуть використовувати вбудовані криптографічні бібліотеки для реалізації HOTP. Наприклад, додаток Google Authenticator генерує одноразові паролі на основі секретного ключа і лічильника, який збільшується з кожною новою генерацією пароля. Це забезпечує унікальність кожного пароля та додатковий рівень безпеки для користувачів. Подібно до Android, платформа iOS також підтримує реалізацію HOTP у мобільних додатках. Розробники можуть використовувати криптографічні бібліотеки,

доступні в iOS, для створення одноразових паролів. Додатки для двофакторної автентифікації, такі як Microsoft Authenticator, використовують HOTP для забезпечення безпеки облікових записів. Також Десктопні додатки, такі як менеджери паролів, використовують HOTP для генерації одноразових паролів, які забезпечують додатковий захист облікових записів користувачів.

Ці програми зберігають секретні ключі та синхронізують лічильники з сервером, щоб забезпечити унікальність кожного пароля. На платформі Windows існує безліч бібліотек, які дозволяють реалізувати HOTP у десктопних додатках. Менеджери паролів, такі як LastPass, підтримують генерацію одноразових паролів за допомогою HOTP, забезпечуючи додатковий рівень безпеки для збережених паролів. Подібно до Windows, платформа macOS також підтримує реалізацію HOTP у десктопних додатках. Менеджери паролів, такі як 1Password, використовують HOTP для створення одноразових паролів, які забезпечують захист облікових записів користувачів.

Також як в TOTP алгоритмі можлива розробка веб- сервісів. Веб-сервіси широко використовують HOTP для забезпечення безпеки користувачів. Багато онлайн-сервісів, такі як Google, Facebook і Amazon, підтримують двофакторну автентифікацію з використанням HOTP, дозволяючи користувачам генерувати одноразові паролі за допомогою додатків на своїх смартфонах.

Веб-сервіси можуть інтегрувати HOTP за допомогою криптографічних бібліотек, які забезпечують генерацію одноразових паролів на основі секретного ключа і лічильника. Користувачі можуть синхронізувати свої облікові записи з додатками, які підтримують HOTP, шляхом сканування QR-коду або введення секретного ключа вручну. Багато веб-сервісів надають API, які дозволяють розробникам інтегрувати підтримку HOTP у свої додатки. Це забезпечує гнучкість та масштабованість для різних видів програмного забезпечення, дозволяючи використовувати HOTP у широкому спектрі застосувань. Таким чином, HOTP є ефективним та зручним способом забезпечення безпеки облікових записів, який може бути реалізований на різних платформах з використанням сучасних

криптографічних методів та інструментів.

2.5 Порівняння алгоритмів OTP

HOTP – Одноразовий пароль на основі події OTP на основі подій (також називається HOTP, що означає одноразовий пароль на основі HMAC) – це оригінальний алгоритм одноразового пароля, який базується на двох частинах інформації. Перший – це секретний ключ, який називається засіб, який відомий лише маркеру та серверу, який перевіряє надіслані коди OTP. Друга частина інформації — це фактор переміщення, який у OTP на основі подій є лічильником. Лічильник зберігається в токені та на сервері.

Лічильник у маркері збільшується, коли натискається кнопка на маркері, тоді як лічильник на сервері збільшується лише після успішної перевірки OTP. Щоб обчислити OTP, маркер передає лічильник в алгоритм HMAC, використовуючи початкове значення маркера як ключ. HOTP використовує хеш-функцію SHA-1 у HMAC. Це створює 160-бітове значення, яке потім зменшується до 6 (або 8) десяткових цифр, які відображає маркер. TOTP: Одноразовий пароль на основі часу OTP на основі часу (скорочено TOTP) базується на HOTP, але змінним фактором є час, а не лічильник. TOTP використовує час із кроком, який називається часовим кроком, який зазвичай становить 30 або 60 секунд. Це означає, що кожен OTP дійсний протягом часового кроку. Порівняння – Обидві схеми OTP пропонують одноразові коди, але ключова відмінність полягає в тому, що в HOTP даний OTP дійсний, доки його не буде використано, або доки не буде використано наступний OTP. У HOTP є кілька дійсних кодів «наступного OTP». Це пов’язано з тим, що можна натиснути кнопку на маркері, таким чином збільшивши лічильник на маркері, без того, щоб кінцевий OTP надсилався на сервер перевірки.

З цієї причини сервери перевірки HOTP приймають ряд OTP. Зокрема, вони приймуть одноразовий пароль, згенерований лічильником, який знаходиться в

межах заданої кількості приростів від попереднього значення лічильника, що зберігається на сервері. Цей діапазон називається вікном перевірки. Якщо лічильник маркерів виходить за межі діапазону, дозволеного сервером, перевірка не вдасться, і маркер потрібно повторно синхронізувати. Отже, очевидно, що в HOTP є компроміс. Чим більше вікно перевірки, тим менша ймовірність необхідності повторно синхронізувати маркер із сервером, що незручно для користувача. Важливо, що чим більше вікно, тим більша ймовірність того, що зловмисник вгадає один із прийнятих одноразових паролів за допомогою атаки грубою силою.

Навпаки, у TOTP є лише один дійсний OTP у будь-який момент часу – той, що генерується на основі поточного часу UNIX. Вибір між HOTP і TOTP виключно з точки зору безпеки надає перевагу TOTP. Важливо, що сервер перевірки повинен бути в змозі впоратися з можливістю дрейфу в часі з маркерами TOTP, щоб мінімізувати будь-який вплив на користувачів. Також є більший вибір форм-фактора з токенами TOTP. Традиційні брелоки OTP-токенів стають меншими, і Microcosm представив картку OTP Card – OTP-токен розміром з кредитну картку з дисплеєм EPD.

2.6 Висновки до розділу

У цьому розділі було детально розглянуто технології одноразових паролів (OTP), зокрема алгоритми TOTP та HOTP, які є основними методами генерації одноразових паролів.

Одноразові паролі (OTP) представляють собою важливий інструмент для підвищення безпеки автентифікації користувачів у цифрових системах. Переваги OTP.

OTP забезпечують вищий рівень безпеки порівняно з традиційними статичними паролями, оскільки кожен пароль дійсний лише для одного сеансу або транзакції Використання OTP знижує ризик фішингових атак, оскільки навіть якщо

зловмисник отримає одноразовий пароль, він не зможе використовувати його повторно. Багато систем OTP інтегрують додатковий рівень захисту у вигляді двофакторної автентифікації, що ще більше підвищує безпеку. Недоліки OTP Одноразові паролі можуть бути перехоплені або перенаправлені зловмисниками, особливо якщо вони надсилаються через менш безпечні канали, такі як SMS Жорсткі токени або мобільні пристрої, які використовуються для генерації OTP, можуть бути втрачені, пошкоджені або вкрадені для отримання OTP користувач повинен мати доступ до свого пристрою (телефону, електронної пошти або токена). Відсутність доступу до пристрою може унеможливити автентифікацію.

Також було проведено порівняння TOTP та HOTP TOTP: Генерація OTP базується на поточному часі, що забезпечує високу безпеку, але потребує точного синхронізації часу між сервером та клієнтом. Перевагою є те, що OTP діє лише протягом короткого проміжку часу (звичайно 30 секунд), що зменшує можливість атаки грубою силою. HOTP: Генерація OTP базується на лічильнику подій, що дозволяє OTP бути дійсним доти, доки він не буде використаний. Це додає гнучкості користувачам, але також може створювати ризик десинхронізації між сервером та клієнтом. Вибір між TOTP та HOTP залежить від конкретних вимог до безпеки та зручності використання. TOTP надає перевагу з точки зору безпеки через обмежений час дії пароля, тоді як HOTP може бути більш гнучким у використанні, але потребує механізмів для уникнення десинхронізації.

Отже, використання технологій OTP є важливим кроком у підвищенні безпеки цифрових систем. Організації повинні враховувати як переваги, так і недоліки кожного алгоритму, обираючи найбільш відповідний для своїх потреб та забезпечуючи належний рівень захисту від потенційних загроз.

3 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ

3.1 Необхідність створення

Зростання загроз кібербезпеці: З кожним роком кількість кібератак та їх складність зростає. Витоки даних, фішинг, атаки на паролі - все це становить серйозну загрозу для безпеки інформації. З розвитком цифрових технологій, все більше особистих даних користувачів зберігається в онлайн-системах, що потребує надійного захисту.

Традиційні паролі часто є слабкими і легко піддаються атакам. Багато користувачів використовують прості або однакові паролі для різних сервісів, що підвищує ризик компрометації. Використання лише пароля для входу в систему вже не забезпечує достатнього рівня безпеки. Метою розробки програми є впровадження двофакторної аутентифікації (2FA) за допомогою одноразових паролів (OTP), як буде використовувати два алгоритма HOTP та TOTP що значно підвищує безпеку користувачів так як завдяки такому захисту втратити свої данні стає значно складніше так як програма буде використовувати два різних алгоритма шифрування. Необхідність створення нових підходів до захисту інформації в сучасному контексті кібербезпеки обумовлена зростаючою кількістю і складністю кібератак.

У сучасному контексті кібербезпеки ми стикаємося з різноманітними викликами, які потребують інноваційних підходів до захисту даних та інформаційних систем. Останні роки показують значне збільшення кількості кібератак, які стають все більш складними і небезпечними. Кібератаки можуть бути спрямовані на різні цілі, включаючи фінансові установи, урядові організації, приватні компанії та індивідуальних користувачів. Атаки можуть мати різні форми, такі як фішинг, шкідливе програмне забезпечення, DDoS-атаки, атаки на мережеві інфраструктури та інші. Технологічний прогрес, зокрема в області штучного інтелекту (ШІ), машинного навчання і Інтернету речей (IoT), надає нові можливості для кіберзлочинців.

Наприклад, ШІ може бути використаний для автоматизації атак, що робить їх швидшими і важче виявляти. IoT-пристрої часто мають слабку безпеку, що робить їх легкою мішенню для кібератак. Критична інфраструктура, така як енергетичні мережі, транспортні системи і медичні заклади, стає все більш залежною від інформаційних технологій. Це робить її вразливою до кібератак, які можуть мати серйозні наслідки для суспільства, включаючи перебої в постачанні електроенергії, порушення транспортних послуг і загрозу життю пацієнтів у лікарнях. Кіберзлочинці активно використовують методи соціальної інженерії для обману користувачів і отримання доступу до конфіденційної інформації.

Такі методи включають фішинг, вішинг (голосовий фішинг) та смішинг (SMS-фішинг). Зловмисники часто видають себе за легітимні організації або осіб, щоб обдурити користувачів і змусити їх розкрити свої паролі або інші конфіденційні дані. Програмне забезпечення завжди містить певні вразливості, які можуть бути використані кіберзлочинцями для здійснення атак. Важливим аспектом кібербезпеки є своєчасне виявлення та виправлення таких вразливостей через оновлення та патчі. Проте, багато організацій і користувачів не встигають вчасно оновлювати своє програмне забезпечення, що підвищує ризик атак.

З поширенням великих даних (Big Data) і зростаючою кількістю персональної інформації, що зберігається в інтернеті, зростає ризик порушення приватності. Кіберзлочинці можуть викрадати персональні дані для різних цілей, включаючи фінансові шахрайства та шантаж. Захист персональної інформації стає все більш важливим аспектом кібербезпеки. Не всі загрози походять ззовні організації. Інсайдерські загрози, які включають співробітників, що зловживають своїм доступом до інформаційних систем, також представляють серйозну проблему. Такі інсайдери можуть бути мотивовані фінансовими вигодами, образою або іншими особистими мотивами. Глобалізація призводить до ускладнення ланцюгів постачання, що створює додаткові ризики для кібербезпеки. Наприклад, вразливості в постачальників програмного забезпечення або апаратних

компонентів можуть стати точкою входу для кіберзлочинців. Забезпечення безпеки всього ланцюга постачання стає критично важливим завданням.

Кібертероризм і діяльність державних акторів стають все більш значущими загрозами. Держави та терористичні групи можуть використовувати кіберпростір для здійснення атак на критичну інфраструктуру, крадіжки інтелектуальної власності та проведення шпигунських операцій. Незважаючи на зростання кількості кібератак, багато організацій і користувачів все ще недооцінюють ризики, пов'язані з кібербезпекою. Недостатня обізнаність про сучасні загрози і методи захисту може призводити до серйозних наслідків, включаючи втрату даних, фінансові збитки і шкоду репутації. Враховуючи всі ці виклики, стає очевидним, що необхідність створення нових підходів до забезпечення кібербезпеки є надзвичайно актуальною. Сучасні реалії вимагають від фахівців з кібербезпеки бути постійно в курсі нових загроз, використовувати інноваційні технології та розробляти комплексні стратегії захисту для забезпечення безпеки інформаційних систем та даних. Кібертероризм і діяльність державних акторів стають все більш значущими загрозами. Держави та терористичні групи можуть використовувати кіберпростір для здійснення атак на критичну інфраструктуру, крадіжки інтелектуальної власності та проведення шпигунських операцій. Незважаючи на зростання кількості кібератак, багато організацій і користувачів все ще недооцінюють ризики, пов'язані з кібербезпекою. Недостатня обізнаність про сучасні загрози і методи захисту може призводити до серйозних наслідків, включаючи втрату даних, фінансові збитки і шкоду репутації. Враховуючи всі ці виклики, стає очевидним, що необхідність створення нових підходів до забезпечення кібербезпеки є надзвичайно актуальною. Сучасні реалії вимагають від фахівців з кібербезпеки бути постійно в курсі нових загроз, використовувати інноваційні технології та розробляти комплексні стратегії захисту для забезпечення безпеки інформаційних систем та даних. икористання міжмережевих екранів (файрволів), систем виявлення та запобігання вторгнень.

3.2 Програмна реалізація

Для початку роботи програми потрібно розвернути сервер, цей процес зображено на рисунку 3.1.

Рисунок 3.1 - Запуск сервера

Після того як сервер запущений та готовий до генерації паролів потрібно запустити клієнтську частини, сама клієнтська частина зображена на малюнку 3.2. Сам сервер працює на безкоштовному фреймворку Flask який і дозволяє створити свій сервер. Після того, як сервер готовий до генерації паролів, потрібно запустити клієнтську частину, яка зображена на рисунку 3.3. Клієнтська частина інтерфейсу дозволяє користувачам зручно взаємодіяти з сервером через веб-інтерфейс. Сервер працює на безкоштовному фреймворку Flask, що забезпечує його стабільну та надійну роботу і дозволяє легко налаштовувати та розширювати функціонал за потреби проєкту. також дозволяє легко налаштовувати та розширювати функціонал за потреби проєкту, є ідеальним вибором для цього сервера. вера. Його легка конфігурація і можливості розширення дозволяють швидко адаптувати сервер до вимог проєкту.

Рисунок 3.2 - Клієнтський інтерфейс

В інтерфейсі користувача є декілька функцій. А саме декілька полів вводу інформації, кнопка згенерувати пароль, кнопка відправити HOTP та TOTP також про всяк випадок як що користувач не встигне ввести пароль є кнопка змінити пароль що заставить сервер відправити нові данні для аутентифікації. Для продовження роботи програми потрібно ввести номер телефону та електрону адресу. Після чого на пошту та номер буде надіслано код який згенерований різними алгоритмами, сам код прийде на сервер на якому вилізе сповіщення що користувач згенерував паролі зображено на рисунку 3.3.

Рисунок 3.3 - Генерація пароля сервером

Далі сервер відправить тільки що згенеровані паролі. HOTP – відправить на пошту а TOTP - відправить на номер телефона користувача використовуючи безкоштовний сервіс для відправки смс. Отримання повідомлень зображенно на рисунках 3.4 та 3.5.

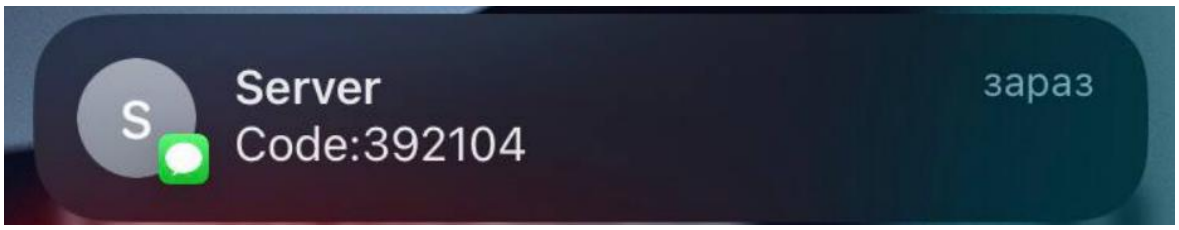


Рисунок 3.4 - Отримання коду на номер телефона.

Рисунок 3.5 - Отримання коду на пошту.

Після цього користувачу потрібно правильно ввести ці данні у свої поля. Далі сервер звірить коди введені користувачем і вирішить аутентифікувати користувача

чи ні як що обидва кода вірні сервер аутентифікує користувача, зображено на рисунку 3.6.

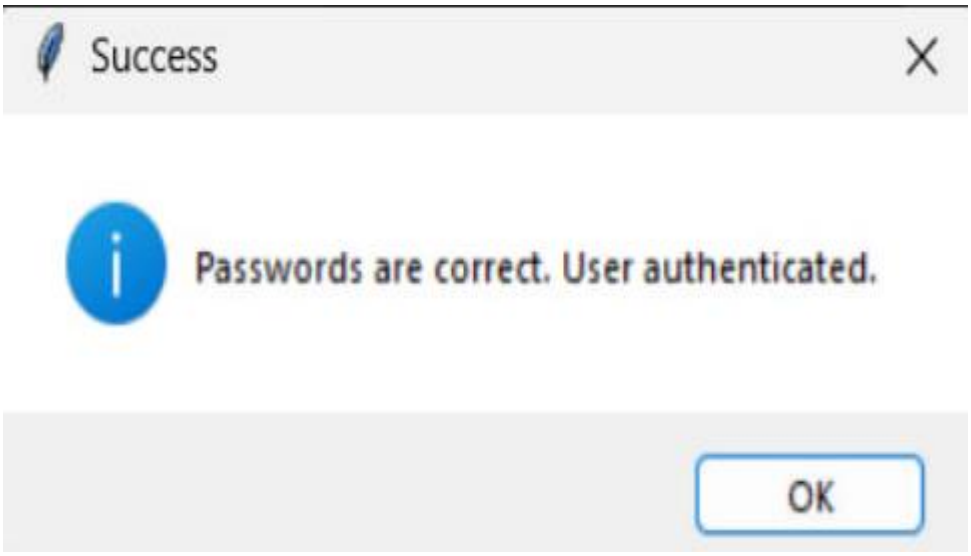


Рисунок 3.6 - Повідомлення про вірні данні.

Як що користувач введе не вірні данні які при перевірці сервер не підтвердить клієнт видасть помилку. А на сервер відправить помилку Зображено на рисунку 3.7.

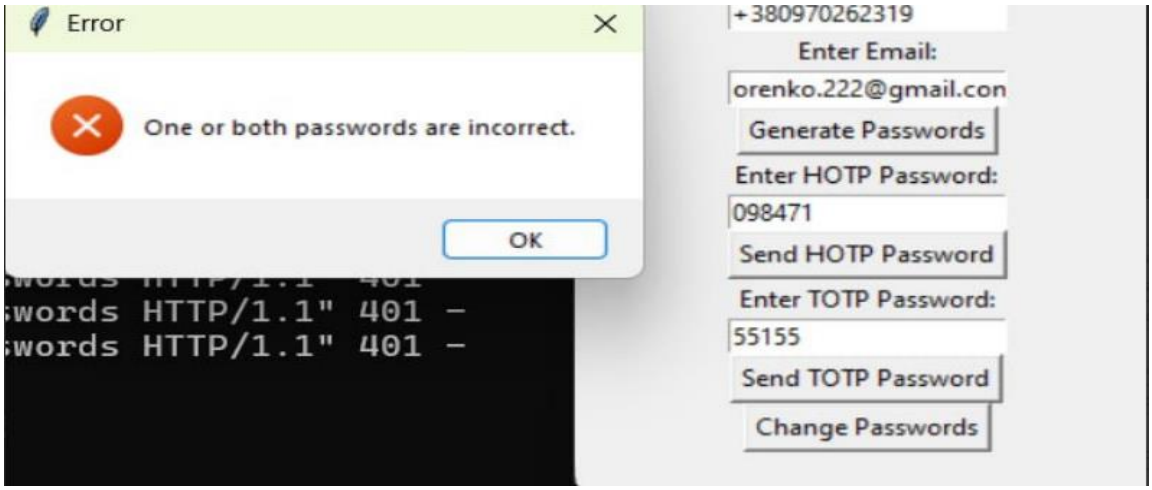


Рисунок 3.7 - Помилка при введенні невірних паролів.

Також як що один з паролів буде вірний а інший не вірний то на сервер також буде відправлено повідомлення про помилку і клієнт сповістить користувача. Зображено на малюнку 3.8.

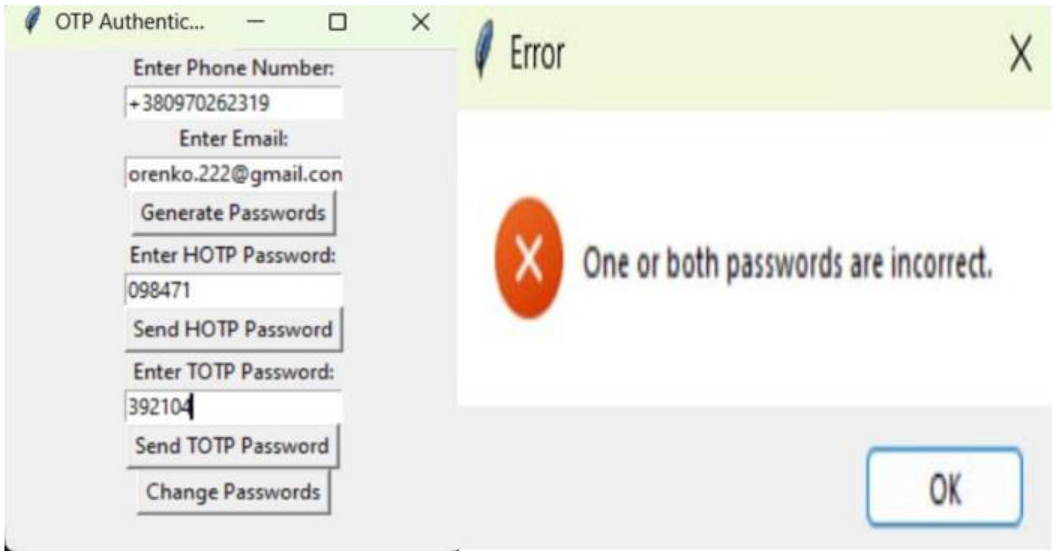


Рисунок 3.8 Помилка при введені одного невірного паролю

Також як що користувачу із за помилки сервера, мережі або іншої помилки яка може виникнути. То на таку ситуацію в програмі є кнопка змінити паролі яка негайно відправить запит на сервер про зміну паролів а сервер в свою чергу згенерує нові паролі відповідно до рисунку.3.9.

Рисунок 3.9 - Повторна генерація паролів

3.3 Відомості про розробку програми

Сама програма була написана мовою Pythone і скаладається з двох частин. А саме серверна частина яка відповідає за генерацію паролів та їх перевірку. Та клієнтська служить засобом для надання серверу інформації про те куда надсилати паролі та закритими дверима які держать зловмисників при вході а користувачів в середині. Процес розробки включав декілька етапів, кожен з яких був важливий для створення надійного та функціонального програмного забезпечення. На початковому етапі було прийнято рішення про вибір архітектури програмного забезпечення. Було обрано багатошарову архітектуру, яка включає наступні шари:

– презентаційний шар;

– логічний шар;

– шар даних.

Для кожного з шарів були обрані відповідні технології та інструменти в презентаційному Використовувалися python та різні бібліотекит для створення інтерфейсу користувача. Для динамічного оновлення даних та покращення користувацького досвіду був застосований фреймворк Flask Для реалізації бізнес-логіки також була обранна мова програмування 54ython разом з фреймворком Spring, який забезпечує зручне керування залежностями та структурування коду. Для зберігання даних використовувалася реляційна база даних PostgreSQL. Для роботи з базою даних було використано ORM (Object-Relational Mapping) фреймворк Hibernate, який спрощує взаємодію з базою даних роцес розробки включав регулярне інтеграційне тестування для забезпечення коректної роботи всіх компонентів системи. Hibernate, який спрощує взаємодію з базою даних, значно полегшує розробку програмного забезпечення, абстрагуючи складні операції SQL за допомогою об'єктно-реляційного відображення (ORM). Це дозволяє розробникам працювати з базою даних через об'єкти, що зменшує кількість коду та потенційні помилки, пов'язані з ручним написанням SQL-запитів.

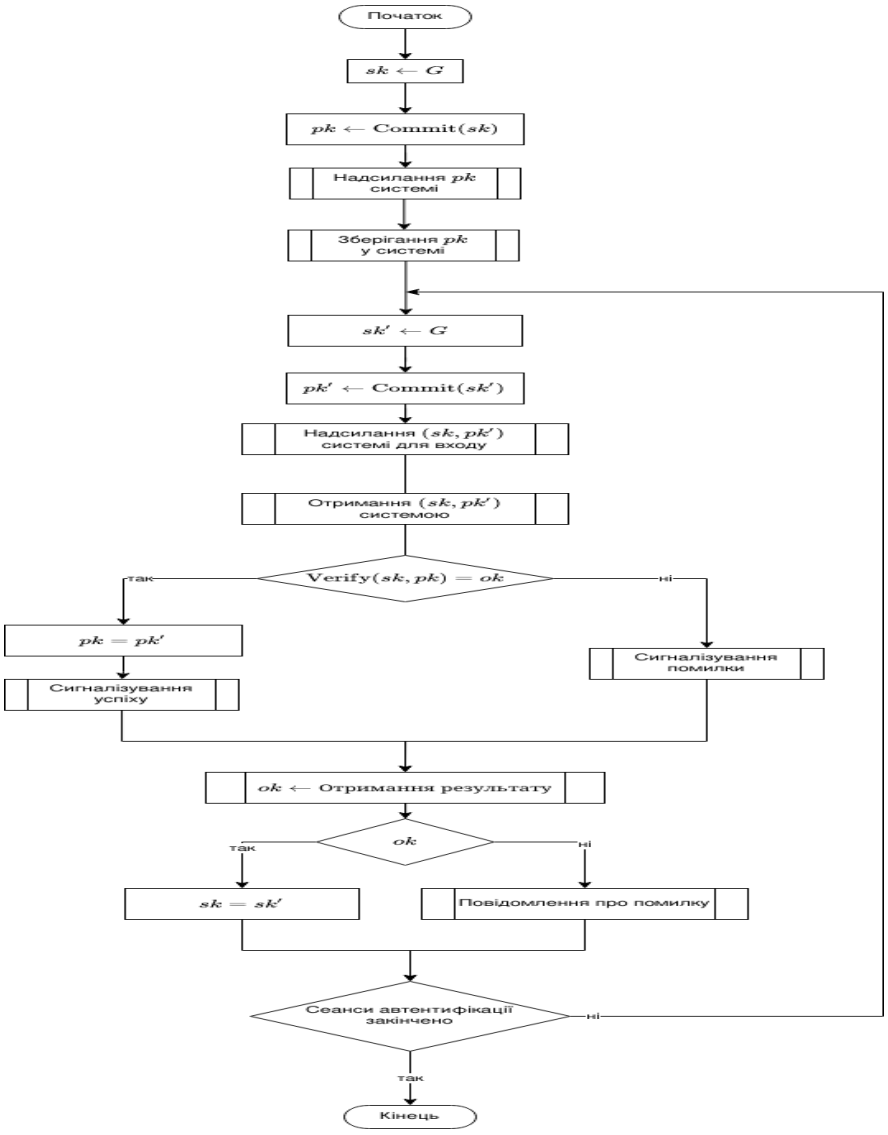


Рисунок 3.10 - Блоксхема роботи програми

3.4 Структурна схема програми

Розробка надійної системи автентифікації користувачів є важливим завданням для забезпечення безпеки інформаційних систем. Система автентифікації на основі одноразових паролів (OTP) забезпечує високий рівень захисту.

Оскільки паролі генеруються динамічно і використовуються лише один раз. Структурна схема розробленої системи автентифікації наведена на рисунку 2.5.

Вона складається з таких ключових компонентів:користувач ініціює запит на доступ до системи, вводячи свої облікові дані. на пристрої користувача (смартфон або комп’ютер) генерується одноразовий пароль (OTP) за допомогою спеціального додатку або пристрою. сервер автентифікації приймає запити від користувачів та здійснює перевірку автентичності облікових даних та OTP. Сервер також відповідає за генерацію OTP для порівняння з OTP, введеним користувачем. генератор OTP генерує одноразові паролі на основі алгоритму TOTP (Time-Based One-Time Password). Алгоритм TOTP використовує поточний час і секретний ключ, відомий лише користувачу і серверу, для генерації одноразових паролів. база даних користувачів зберігає інформацію про користувачів, їх облікові дані та налаштування для автентифікації. база даних також містить секретні ключі, які використовуються для генерації OTP.

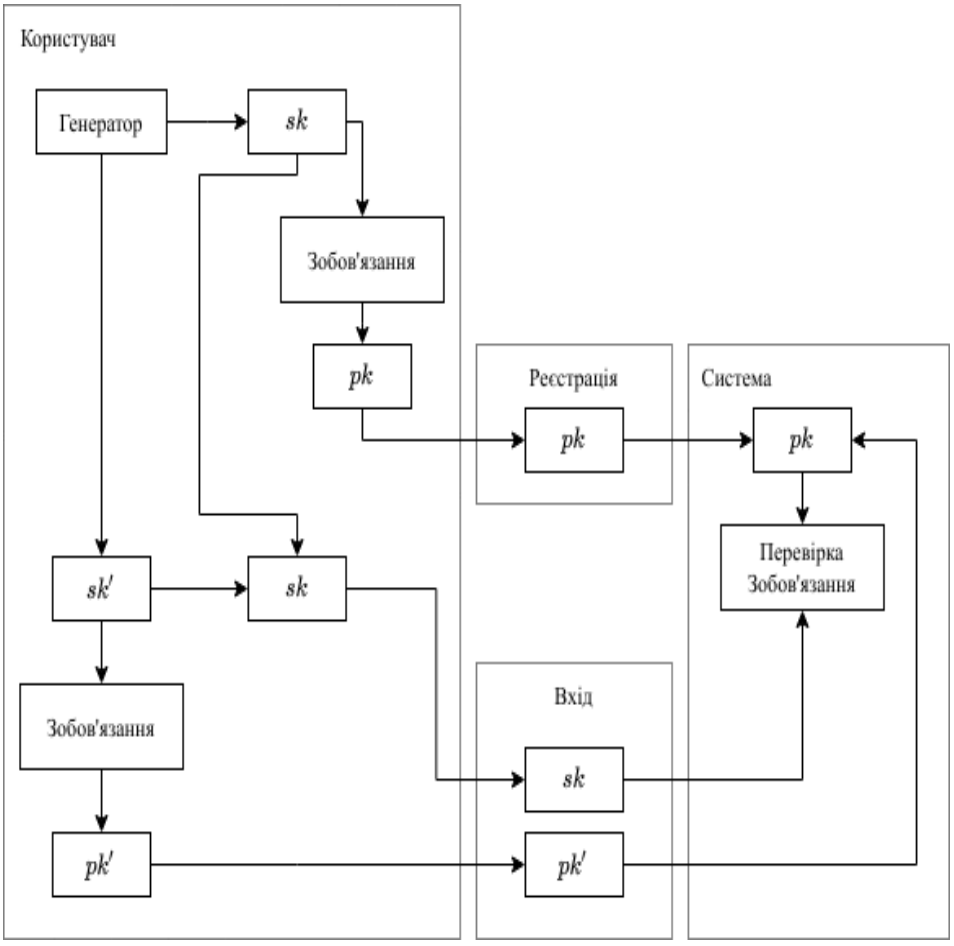


Рисунок 3.11 - Структурна схема розробленої системи автентифікації

3.5 Оцінка ефективності

Для оцінки ефективності розробленої системи було проведено порівняння з існуючими методами автентифікації. Основними критеріями оцінки були надійність, швидкість автентифікації, зручність використання та вартість впровадження. Оцінка ефективності системи автентифікації зображена на малюнку 2.6.

Таблиця 3.1 – Оцінка ефективності системи автентифікації

Критерії	Паролі	Сертифікати	Одноразові паролі
Надійність	Середня	Висока	Висока
Швидкість автентифікації	Висока	Середня	Висока
Зручність використання	Середня	Низька	Висока
Вартість впровадження	Низька	Висока	Середня

Одноразові паролі забезпечують високий рівень безпеки завдяки унікальності кожного паролю і короткому часу їх дії. Це знижує ризик компрометації паролів у порівнянні зі статичними паролями. Система OTP забезпечує високу швидкість автентифікації завдяки простоті і швидкості генерації паролів. Це дозволяє користувачам швидко і безпечно отримувати доступ до системи. Використання одноразових паролів є зручним для користувачів, оскільки вони не потребують запам'ятовування складних паролів.

Достатньо мати доступ до пристрою, який генерує OTP. Вартість впровадження системи OTP є середньою в порівнянні з іншими методами, такими як сертифікати, що потребують складної інфраструктури. Однак, вона вища за використання статичних паролів, що обумовлено необхідністю додаткового

обладнання або програмного забезпечення для генерації OTP. Отже звідси випливає висновок що Було розроблено структурну схему системи автентифікації на основі одноразових паролів та проведено її оцінювання в порівнянні з існуючими методами автентифікації. Проведений аналіз показав, що запропонована система забезпечує високий рівень безпеки, зручність використання та швидкість автентифікації, що робить її оптимальним рішенням для захисту інформаційних систем. Враховуючи сучасні вимоги до кібербезпеки, впровадження такої системи є доцільним та ефективним заходом для зниження ризиків несанкціонованого доступу до інформаційних ресурсів.

3.6 Висновки до розділу

У даному розділі було представлено розробку та реалізацію програми, що використовує два алгоритми одноразових паролів (OTP) - HOTP та TOTP - для підвищення безпеки аутентифікації користувачів. Програма забезпечує двофакторну аутентифікацію, де сервер генерує два одноразових паролі: один з яких відправляється на електронну пошту користувача (HOTP), а інший - на номер його телефону (TOTP). Клієнтська частина програми дозволяє користувачеві ввести отримані паролі, які потім перевіряються сервером для визначення автентичності користувача. Основними результатами програми стали Було успішно впроваджено два алгоритми одноразових паролів. HOTP використовує лічильник, що інкрементується, тоді як TOTP базується на поточному часі.

Це дозволяє забезпечити як відносно тривалі одноразові паролі, так і короткочасні, що знижує ймовірність компрометації. Серверна частина програми генерує одноразові паролі та відправляє їх користувачеві через два різні канали - електронну пошту та SMS.

Це підвищує безпеку, оскільки зловмисник має отримати доступ до обох каналів, щоб скомпрометувати аутентифікацію. Клієнтська частина програми

дозволяє користувачеві зручно ввести отримані коди та передати їх серверу для перевірки. Сервер здійснює перевірку відповідності введених кодів згенерованим і приймає рішення щодо автентичності користувача. Впровадження двофакторної аутентифікації з використанням HOTP та TOTP значно підвищує рівень безпеки системи. Навіть у разі компрометації основного пароля, додатковий рівень захисту у вигляді OTP ускладнює несанкціонований доступ.

Запропонована система двофакторної аутентифікації з використанням HOTP та TOTP. ґрунтується на використанні секретного ключа та лічильника, який збільшується при кожному запиті на новий пароль. HOTP паролі залишаються дійсними до моменту використання, що забезпечує гнучкість у випадках, коли точний час синхронізації не може бути гарантований. ефективно вирішує проблему ненадійності традиційних паролів та забезпечує високий рівень безпеки для користувачів. Одноразові паролі (OTP), які генеруються за допомогою HOTP і TOTP, значно підвищують рівень безпеки, оскільки кожен пароль використовується лише один раз і стає недійсним після використання або після закінчення короткого проміжку часу. Це робить перехоплення паролів марним для зловмисників. Поєднання двох різних алгоритмів OTP і використання двох окремих каналів для передачі паролів підвищує стійкість системи до кібератак. Різноманітність методів генерації паролів: Використання двох різних алгоритмів (HOTP і TOTP) додає додатковий рівень складності для зловмисників. Навіть якщо один алгоритм буде скомпрометований, інший забезпечить додатковий захист.Успішна реалізація даного підходу демонструє практичну цінність двофакторної аутентифікації та її важливість у сучасних умовах підвищеної загрози кібербезпеці. В подальшому розробка може бути вдосконалена шляхом додавання додаткових методів аутентифікації та інтеграції з іншими системами захисту даних та інтеграції з іншими системами захисту даних. Це дозволить значно підвищити рівень безпеки та забезпечити ще більшу стійкість системи до кібератак.

ВИСНОВКИ

В дипломній роботі було розглянуто різні аспекти автентифікації та ідентифікації користувачів, аналіз технологій одноразових паролів, та розроблено програмну реалізацію системи автентифікації. Основною метою роботи було підвищення рівня безпеки інформаційних систем за рахунок використання ефективних методів автентифікації. Розглянувши різні методи автентифікації, зокрема паролі, одноразові паролі та автентифікацію на основі сертифікатів, було визначено їх переваги та недоліки. Встановлено, що для забезпечення належного рівня безпеки слід застосовувати багатофакторну автентифікацію, яка поєднує кілька методів одночасно.

Технології одноразових паролів (OTP) детально аналізувались, особлива увага була приділена алгоритмам HOTP та TOTP. На основі проведеного аналізу було визначено, що алгоритм TOTP є більш гнучким і надійним для використання у сучасних інформаційних системах. Програмна реалізація системи автентифікації продемонструвала високу ефективність та здатність інтегруватися з існуючими інформаційними системами. В результаті тестування програмного продукту було встановлено його відповідність вимогам безпеки та функціональності. Отже, виконана робота підтверджує, що використання сучасних методів автентифікації, зокрема одноразових паролів, є ефективним засобом підвищення безпеки інформаційних систем. Запропоновані рішення можуть бути використані для захисту інформаційних ресурсів від несанкціонованого доступу, що є особливо важливим у контексті зростаючих кіберзагроз.

Висновки до розділу включають аналіз досягнень та можливих напрямків подальшого розвитку в галузі одноразових паролів (OTP). Розглядаючи досягнення та перспективи розвитку, можна зробити кілька важливих висновків.

OTP знайшли широке застосування у різних сферах, включаючи банківські послуги, електронну комерцію, корпоративні мережі та інші галузі, де безпека є критично важливою.

Багато компаній та організацій успішно інтегрували OTP у свої системи безпеки, що дозволило значно знизити кількість успішних кібератак. Було розроблено і впроваджено кілька важливих стандартів, таких як TOTP (Time-based One-Time Password) та HOTP (HMAC-based One-Time Password), які стали основою для багатьох сучасних рішень у галузі одноразових паролів. Ці стандарти забезпечують сумісність та інтероперабельність між різними системами і платформами. Сучасні рішення з використанням OTP стали більш зручними для користувачів. Інтеграція OTP у мобільні додатки, використання QR-кодів для швидкої ініціалізації, а також автоматичне введення паролів значно спростили процес аутентифікації.

Таким чином, аналіз досягнень у сфері одноразових паролів показує значний прогрес у підвищенні безпеки аутентифікації. Однак, існують ще багато перспективних напрямків для подальшого розвитку, які можуть забезпечити ще більший рівень захисту інформації в майбутньому.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Миронович В. Все у безпеці: навіщо вашому бізнесу двофакторна аутентифікація. Speka - онлайн медіа про технології та підприємництво | SPEKA.media | SPEKA.media. URL: https://speka.media/vse-u-bezpeci-navishho-vasomu-biznesu-dvofaktorna-autentifikaciya-p1o3xv?utm_source=google&utm_medium=cpc&utm_campaign=20972733776&gad_source=1 (дата звернення: 21.05.2024).
2. Учасники проектів Вікімедіа. Автентифікація – вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Автентифікація (дата звернення: 21.05.2024).
3. Что такое аутентификация | Unisender. Unisender. URL: https://www.unisender.com/ru/glossary/chto-takoe-email-autentifikaciya/ (дата звернення: 21.05.2024).
4. 1С-Битрикс Разработчикам - SSL аунтефикация. URL: https://dev.1c-bitrix.ru/community/forums/forum6/topic5303/ (дата звернення: 21.05.2024).
5. Digital A. Что такое аутентификация? - Альфа Банк URL: https://www.alfabank.by/about/wiki/banks/authentication/ (дата звернення: 21.05.2024).
6. Oteir N. У чому різниця між аутентифікацією та авторизацією?. INTROSERV. URL: https://introserv.com/ua/blog/u-chomu-rizniczya-mizh-autentifikaczieyu-taavtorizaczieyu/?gad_source=1&gclid=Cj0KCQjw6auyBhDzARIsALIo6v_TUEn3Gj7sniUBxncAiKItKIBxzBWPa_paVnPEnI00DViCzp5B-4IaAuyoEALw_wcB (дата звернення: 21.05.2024).
7. Толчёнова М. Идентификация, аутентификация, авторизация: чем они различаются. skillbox.ru. URL: https://skillbox.ru/media/code/identifikatsiya-autentifikatsiya-avtorizatsiya-chem-oni-razlichayutsya/ (дата звернення: 21.05.2024)
8. Аутентифікація і авторизація: що це і в чому відмінність. QualityAssuranceGroup.

URL: https://qagroup.com.ua/publications/autentyfikatciia-i-avtoryzatciia/ (дата звернення: 21.05.2024).

9. Учасники проектів Вікімедіа. Автентифікація (веб) – вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Автентифікація_(веб) (дата звернення: 21.05.2024).

10. Що таке аутентифікація: визначення | SendPulse UA. SendPulse. URL: https://sendpulse.ua/support/glossary/authentication (дата звернення: 21.05.2024).

11. Що таке двохфакторна автентифікація? | Захисний комплекс Microsoft. Your request has been blocked. This could be due to several reasons. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-two-factor-authentication-2fa (дата звернення: 21.05.2024).

12. Ідентифікація, автентифікація та авторизація – у чому різниця?. UKEY WAF - Надійний захист веб-сайту. URL: https://ukeywaf.com/identyfikacziya-avtentyfikacziya-ta-avtoryzacziya-u-chomu-riznyczya/ (дата звернення: 21.05.2024).

13. Ідентифікація, автентифікація та авторизація – не дай керувати зловмисникам. ТОВ "Зе Кернел". URL: https://thekernel.ua/identyfikatsiia-avtentyfikatsiia-ta-avtoryzatsiia/ (дата звернення: 21.05.2024).

14. Аутентифікація та Авторизація: Ключові поняття » CyberSecureFox. CyberSecureFox. URL: https://cybersecurefox.com/uk/autentyfikatsiia-avtoryzatsiia-v-kiberbezpetsi/ (дата звернення: 21.05.2024).

15. Автентифікація. www.wikidata.uk-ua.nina.az. URL: https://www.wikidata.uk-ua.nina.az/Автентифікація.html (дата звернення: 21.05.2024).

16. Що таке двофакторна автентифікація?. How Dropbox Empowers You and Your Teams to Find and Use Your Content More Easily - Dropbox. URL: https://experience.dropbox.com/uk-ua/resources/what-is-2fa (дата звернення: 21.05.2024).

17. Різниця між аутентифікацією та авторизацією: порівняння. FoxmindEd. URL: https://foxminded.ua/riznytsia-mizh-avtentyfikatsiieiu-ta-avtoryzatsiieiu/ (дата звернення: 21.05.2024).

18. Що таке двоетапна автентифікація та чим вона відрізняється від двохфакторної. YubiKey - Україна. URL: https://yubikey.com.ua/shcho-take-dvoetapna-avtentyfikatsiia (дата звернення: 21.05.2024).

19. Що таке двофакторна автентифікація користувача | блог ssl.com.ua. Блог SSL.com.ua. URL: https://ssl.com.ua/blog/ukr/what-is-2fa/ (дата звернення: 21.05.2024).

20. Що таке Двофакторна аутентифікація (2FA) - цеКрипто. цеКрипто. URL: https://tsecrypto.com/article/shho-take-dvofaktorna-autentyfikacziya-2fa/ (дата звернення: 21.05.2024).

21. Аспракі Я.-Т. Автентифікуйте свій домен. просто. зробіть. це. - викидайло. Вишибала. URL: https://www.usebouncer.com/uk/автентифікація-вашого-домену-просто/ (дата звернення: 21.05.2024).

22. Двофакторна автентифікація | PeopleForce База знань. PeopleForce help center. URL: https://help.peopleforce.io/uk/articles/6628189-двофакторна-автентифікація (дата звернення: 21.05.2024).

23. Oteir N. У чому різниця між аутентифікацією та авторизацією?. INTROSERV. URL: https://introserv.com/ua/blog/u-chomu-rizniczya-mizh-autentifikaczieyu-ta-avtorizaczieyu/?gad_source=1&gclid=Cj0KCQjw6auyBhDzARIsALIo6v_FWEetd7wTAQhCB0_RFfWIGONLzqiZ62pe9SMuwrWGWtTBgqImpYoaAuzqEALw_wcB (дата звернення: 21.05.2024).

24. Кафедра прикладної математики і фізики. URL: http://pmf.uad.lviv.ua/storage/uploads/лекції%201%20інформаційна%20безпека.pdf (дата звернення: 21.05.2024).

25. Аутентифікація. LivingFo – Портал LivingFo – найкращі новини. URL: https://livingfo.com/autentyfikatsiia/ (дата звернення: 21.05.2024).

26. Ti40. TI40. URL: https://pupenasan.github.io/TI40/Лекц/cloudauth.html (date of access: 21.05.2024).

27. Shapiro V. What Is Single-Factor Authentication? SFA pros and cons. Hideez. URL: https://hideez.com/en-eu/blogs/news/single-factor-authentication (date of access: 21.05.2024).

28. Двофакторна аутентифікація: посилення безпеки онлайн-облікових записів. ClearVPN. URL: https://clearvpn.com/blog/ua/shcho-take-dvofaktorna-autentyfykatsiia/ (дата звернення: 21.05.2024).

29. Багатофакторна автентифікація (MFA). UKEY WAF - Надійний захист веб-сайту. URL: https://ukeywaf.com/baza/bagatofaktorna-avtentyfikacziya-mfa/ (дата звернення: 21.05.2024).

30. Різниця між ідентифікація та автентифікація. REPORTER | Information portal. URL: https://reporter.zp.ua/riznytsya-mizh-identyfikatsiya-ta-avtentyfikatsiya.html (дата звернення: 21.05.2024).

31. How can we help? | Tor Project | Support. URL: https://support.torproject.org/uk/onionservices/client-auth/ (date of access: 21.05.2024).

32. ShieldSquare captcha. ShieldSquare Captcha. URL: https://www.kmu.gov.ua/news/roziasnennia-derzhspetszviazku-iak-pratsiuie-dvofaktorna-avtentyfikatsiia (date of access: 21.05.2024).

33. Що таке MFA – багатофакторна аутентифікація? - datami. datami. URL: https://datami.ua/shho-take-mfa-bagatofaktorna-autentifikatsiya/ (дата звернення: 21.05.2024).

34. Що таке багатофакторна автентифікація (MFA)? - Cloud. Cloud. URL: https://cloud.smart-it.com/news-post/what-is-mfa/ (дата звернення: 21.05.2024).

35. Авторизація без пароля: що це таке і чому важливо. Acer Corner. URL: https://blog.acer.com/ua/discussion/927/avtorizaciya-bez-parolya-scho-ce-take-i-chomu-vazhlivo (дата звернення: 21.05.2024).

36. Wikiwand - Автентифікація повідомлень. Wikiwand. URL: https://www.wikiwand.com/uk/Автентифікація_повідомлень (дата звернення: 21.05.2024).

37. Все про AAA: автентифікація, авторизація та облік - polaridad.es. Polaridad.es. URL: https://polaridad.es/uk/все-про-авторизацію-автентифікації-aaa-та-облік/ (дата звернення: 21.05.2024).

38. Український психологічний ХАБ. Ідентифікація це | Український психологічний ХАБ | ПСИХОЛОГ. ПСИХОЛОГ. URL: https://www.psykholoh.com/post/ідентифікація-це (дата звернення: 21.05.2024).

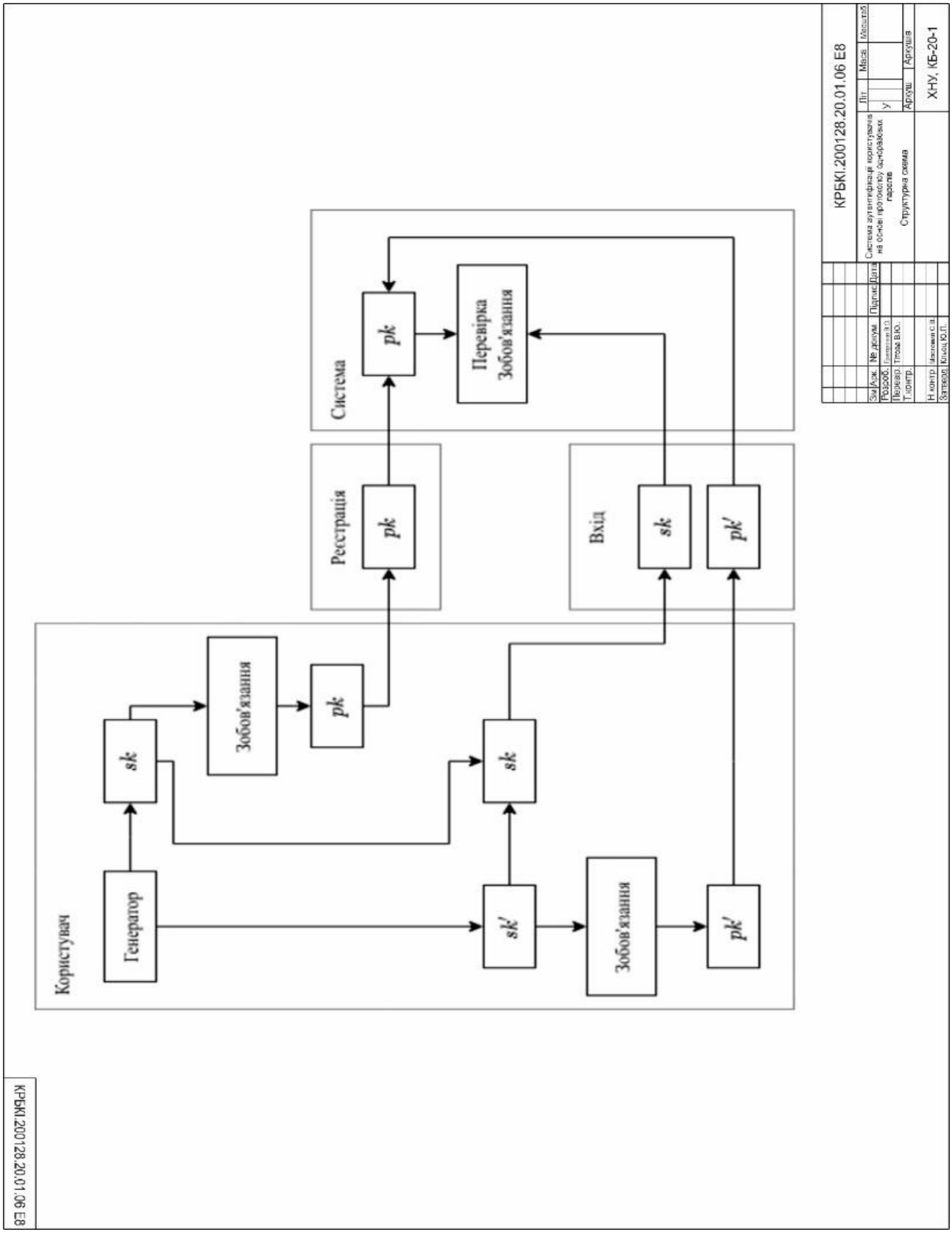
39. Аутентифікація, авторизація та ідентифікація. Онлайн-курси від компанії QATestLab | Головна сторінка. URL: https://training.qatestlab.com/blog/technical-articles/authentication-authorization-and-identification/ (дата звернення: 21.05.2024).

40. Ідентифікація та верифікація клієнта стаття від TAS life. TAS life. URL: https://taslife.com.ua/blog/identyfikacziya-ta-veryfikacziya-kliyenta (дата звернення: 21.05.2024).

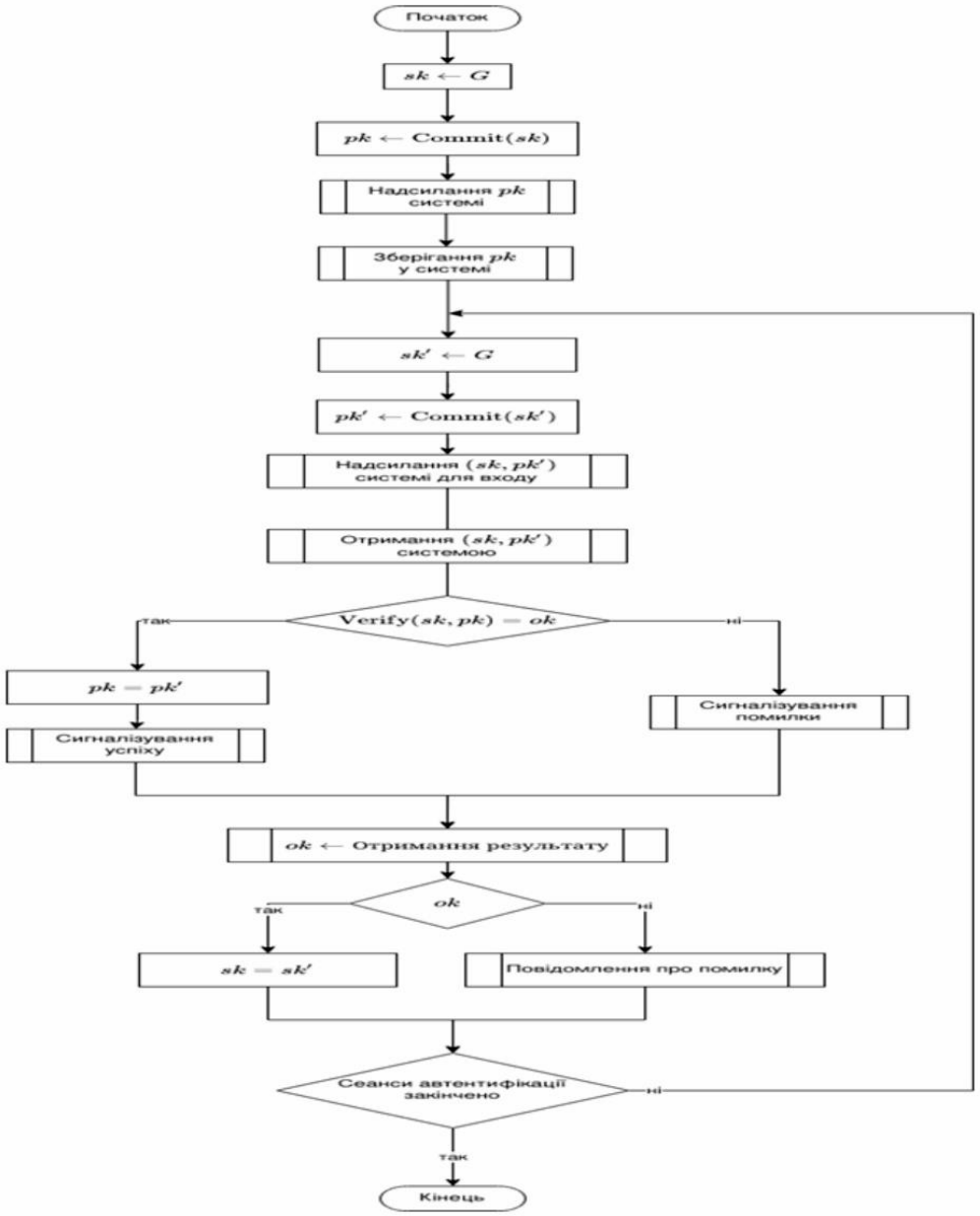
ДОДАТОК А

(Обов’язковий)

Копія графічної частини



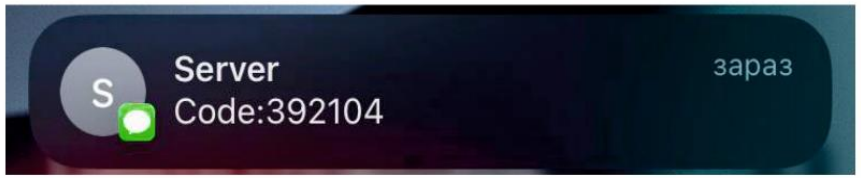
КРБКІ.200128.20.01.06 Е8

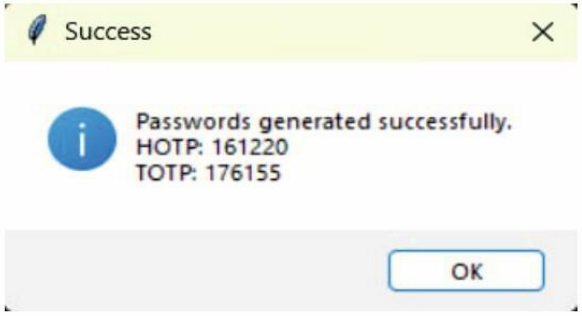


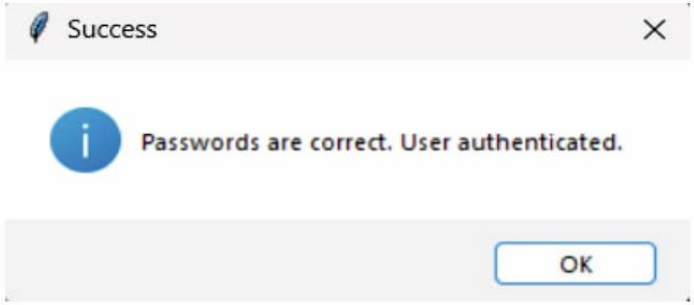
				КРБКІ.200128.20.01.06 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Система аутентифікації користувачів на основі протоколоу одноразових паролів
Розроб.		Григоренко В.О.			Алгоритм роботи програми
Перевір.		Тітова В.Ю..			
Т.контр.					
Н.контр.		Мостовий С.Б.			
Затверд.		Кільоц Ю.П.			

Літ	Маса	Масштаб
У		
Аркуш	Аркушів	
ХНУ, КБ-20-1		

```
Sending SMS to +380970262319: Your TOTP code is: 392104127.0.0.1 - - [14/Jun/2024 13:47:15] "POST /generate_passwords HT
TP/1.1" 200 -
```







					КРБКІ.200128.20.01.06 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Система аутентифікації користувачів на основі протоколу одноразових паролів	Літ	Маса / Масштаб
Розроб.		Григоренко В.О.				У	
Перевір.		Тітова В.Ю..					
Т.контр.					Графічна частина	Аркуш	Аркушів
Н.контр.		Мостовий С.В.				ХНУ, КБ-20-1	
Затверд.		Кльоц Ю.П.					

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Григоренка Вадима Олександровича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений 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.

15.06.2024
дата

підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016368244

Дата перевірки:
17.06.2024 14:58:05 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
17.06.2024 22:25:20 EEST

ID користувача:
100008300

Назва документа: **Григоренко_плагіат**

Кількість сторінок: **61** Кількість слів: **11377** Кількість символів: **88371** Розмір файлу: **1.01 MB** ID файлу: **1016174944**

4.08%
Схожість

Найбільша схожість: **1.08%** з Інтернет-джерелом (http://um.co.ua/12/12-1/12-15509.html)

3.66% Джерела з Інтернету	107	Сторінка 63
0.84% Джерела з Бібліотеки	38	Сторінка 63

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

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

Замінені символи	1

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

	Документ		Сумарний збіг по Базі Даних	
ID: 131000 Назва: Система аутентифікації користувачів на основі протоколу одноразових паролів Додано в БД: 2024-06-17 Автора: Григоренко В.О. Керівники: Тітова В.Ю. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	76683	1164	490 (1%)	5 (0%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Назва: Система аунтетифікації користувачів на основі протоколу одноразових паролів

Автор: Григоренко Вадим Олександрович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Тітова Віра Юріївна, канд. техн. наук, доцент

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:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 95,92%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Григоренко Вадим Олександрович
Тема: «Система аунтетифікації користувачів на основі протоколу одноразових паролів»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 125 «*Кібербезпека*» Освітня програма «Кібербезпека»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 64;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена розробці системи автентифікації користувачів на основі протоколу одноразових паролів з метою підвищення рівня безпеки інформаційних систем. В роботі проведено дослідження існуючих методів автентифікації, зокрема протоколів одноразових паролів, та аналіз їх ефективності. Було розроблено програмну реалізацію системи автентифікації, проведено її тестування та оцінку рівня безпеки.

2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Кібербезпека», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було розглянуто існуючі методи автентифікації та іднетифікації користувачів, проведено їх порівняльний аналіз. У другому розділі було проаналізовано технології одноразових паролів, визначено переваги та недоліки різних алгоритмів генерації, обґрунтовано вибір алгоритму в залежності від вирішуваної задачі. У третьому розділі наведено реалізацію системи аунтетифікації користувачів на основі протоколу одноразових паролів, проведено оцінювання її ефективності.

4. Позитивні сторони кваліфікаційної роботи полягають у тому що, у процесі реалізації системи було визначено, що використання одноразових паролів суттєво підвищує захист інформаційних систем від несанкціонованого доступу в порівнянні з традиційними методами автентифікації.

5. Негативні сторони кваліфікаційної роботи: не визначено ефективність розробленої системи в порівнянні з відомими програмними аналогами

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, д.т.н., професор Мартинюк Валерій Володимирович

« 18 » червня 2024 . (підпис)