Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: «Засоби автентифікації користувача в інформаційній системі через незахищене середовище»

Виконавець: студента IV курсу, групи КБ-41

_____ **Олександр БОНДАРЕНКО**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Юрій ЩЕБЛАНІН	

Нормоконтроль	Олена БОГУСЛАВСЬКА	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-41** (група) **Олександру Володимировичу Бондаренку** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Засоби автентифікації користувача в інформаційній системі через незахищене середовище

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Концепція автентифікації, її фактори і протоколи

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з теорією автентифікації, їх типовими факторами та протоколами, вразливостями з боку безпеки даних, обрати метод авторизації у систему та розробити рекомендації для посилення безпеки при авторизації

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації з вибору стандарту автентифікації і розробка рекомендацій з посилень безпеки.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Олександр БОНДАРЕНКО (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 22.01.2023	*виконано*
2	Аналіз літератури	29.01.2023 – 20.02.2023	*виконано*
3	Обґрунтування вибору рішення	24.02.2023 – 04.03.2023	*виконано*
4	Дослідження методів автентифікації	05.03.2023 – 24.03.2023	*виконано*
5	Аналіз проблем інформаційної безпеки в процесах авторизації	25.03.2023 – 07.04.2023	*виконано*
6	Дослідження вразливостей та загроз	07.04.2023 – 16.04.2023	*виконано*
7	Вироблення рекомендацій щодо вибору засобів автентифікації	16.04.2023 – 30.04.2023	*виконано*
8	Формування висновків	30.04.2023 – 10.05.2023	*виконано*
9	Оформлення пояснювальної записки	11.05.2023 – 27.05.2023	*виконано*

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Олександр БОНДАРЕНКО (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 62 сторінок основного тексту, 2 таблиці та 10 рисунків. Список використаних джерел містить 21 найменувань і займає 3 сторінки.

Методи дослідження кваліфікаційної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння.

Об'єктом дослідження є процес автентифікації користувачів в інформаційній системі.

Предметом дослідження є методи, засоби і технології захисту процесу автентифікації користувача.

В даній роботі були досліджені тенденції розвитку, а також напрямки впровадження сучасних технологій автентифікації; проаналізовані протокол, такі як Kerberos, OpenID; вироблені шляхи побудови системи ідентифікації та автентифікації.

Були розроблені рекомендації для забезпечення безпечного способу авторизації користувачів в інформаційну систему.

Ключові слова: Інформаційна система, інформаційна безпека, авторизація, автентифікація.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

НСД	–	Несанкціонований доступ
SFA	–	Однофакторна автентифікація
2FA	–	Двофакторна автентифікація
MFA	–	Багатофакторна автентифікація
CHAP	–	Challenge Handshake Authentication Protocol
PPP	–	Point-to-Point Protocol
AS	–	Authentication Server (сервер автентифікації)
TGS	–	Ticket-Granting Server (сервер надання квитків)
СЦ	–	Сертифікаційний центр
ЄСІА	–	Єдина система ідентифікації та автентифікації
ІКС	–	Інформаційно-телекомунікаційна система
SSO	–	Single Sign-On (Технологія єдиного входу)
ПЗП	–	Постійний запам’ятовуючий пристрій
ЕОМ	–	Електронно-обчислювальна машина

ЗМІСТ

ВСТУП

Актуальність даної роботи визначається тією обставиною, що на даний момент процес ідентифікації та авторизації є невід'ємною частиною роботи з безліччю програм або для отримання доступу до мережі.

Автентифікація користувачів за допомогою паролів все ще залишається домінуючою формою автентифікації, незважаючи на її відомі недоліки. Абсолютно кожний користується онлайн-сервісами, як соціальні мережі або онлайн-банкінг. І якщо хтось заволодів вашими даними для входу, то зайти може під вашим ім’ям будь-хто. Тому процедура автентифікації користувача є важливим аспектом функціонування інформаційних систем і до неї треба ставитись серйозно щоб забезпечити безпеку користувачів.

Тому **метою роботи** є розробка рекомендацій для покращення методів автентифікації користувачів.

Для досягнення поставленої мети необхідно вирішити такі *завдання***:**

- Дослідити принципи роботи сучасних засобів автентифікації;
- Проаналізувати сучасних методи і засоби автентифікації та ідентифікації;
- Побудувати систему ідентифікації та автентифікації в інформаційній системі.

Об'єктом дослідження є процес автентифікації користувачів в інформаційній системі.

Предметом дослідження є методи автентифікації користувачів в інформаційній системі.

Методи дослідження кваліфікаційної роботи бакалавра:

- аналіз літератури;
- аналіз документів;
- порівняння;
- вивчення та узагальнення національної та зарубіжної практики.

РОЗДІЛ 1
ДОСЛІДЖЕННЯ СУЧАСНИХ ТЕХНОЛОГІЙ АВТЕНТИФІКАЦІЇ ЧЕРЕЗ НЕЗАХИЩЕНЕ СЕРЕДОВИЩЕ

З популяризацією комп'ютерних технологій проблема захисту інформації в інформаційній системі стає все більш актуальною. Таким чином, проблема захисту інформації в комп’ютерних системах спрямована на ізоляцію належним чином функціонуючих інформаційних систем від НСД на захищені комп’ютерні дані третіми особами або програмне забезпечення. Створення єдиної централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури. Контроль доступу є ефективним методом захисту інформації, який може регулювати використання ресурсів інформаційної системи, для чого розроблена концепція ІБ. Метод і система захисту інформації на основі контролю доступу включають такі функції захисту інформації в ІКС:

- ідентифікація користувачів, ресурси системи ІБ;
- ідентифікація та автентифікація користувачів на основі введених облікових даних;
- дозволити доступ до певних умов роботи на основі правил, випущених для кожного користувача, що визначається захистом інформації та є основою інформаційної безпеки в більшості типових моделей ІКС;
- реєструє запити користувачів на ресурси, його IS захищає ресурси від NSD і стежить за некоректною поведінкою користувачів системи.

Можна побачити, що система ідентифікації/автентифікації є одним із важливих компонентів будь-якої інфраструктури захисту від НСД до інформаційної системи.

1.1 Поняття незахищеного середовища

Під незахищеним середовищем у сфері кібербезпеки розуміється ситуація чи стан, які становлять значний ризик для безпеки та цілісності комп’ютерних систем,

мереж, даних або цифрових активів окремих осіб. Він може включати різні фактори, які ставлять під загрозу конфіденційність, цілісність і доступність інформації, роблячи її вразливою для несанкціонованого доступу, маніпулювання або знищення.

Загальні характеристики незахищеного середовища в кібербезпеці є:

1. Недостатні або застарілі заходи безпеки: неадекватні засоби контролю безпеки, такі як слабкі паролі, невиправлене програмне забезпечення або відсутність шифрування, можуть створити вразливі місця, якими можуть скористатися зловмисники.

2. Недостатня обізнаність і навчання користувачів: коли користувачі не знають найкращих методів безпеки або не дотримуються їх, вони можуть ненавмисно створювати ризики, піддаючись фішингу, завантажуючи зловмисне програмне забезпечення або неправильно обробляючи конфіденційну інформацію.

3. Слабкий контроль доступу: погано визначені або погано забезпечений контроль доступу може призвести до того, що неавторизовані особи отримають доступ до конфіденційних систем або даних. Це може включати слабкі механізми автентифікації, неправильні дозволи користувача або незахищені віддалені точки доступу.

4. Зараження зловмисним програмним забезпеченням: наявність шкідливого програмного забезпечення, наприклад вірусів, програм-вимагачів або шпигунських програм, може значно поставити під загрозу безпеку середовища. Це може призвести до несанкціонованого доступу до даних, збою в роботі системи або навіть до крадіжки конфіденційної інформації.

5. Вразливості мережі: незахищені бездротові мережі, незахищені мережеві пристрої або неправильно налаштовані брандмауери можуть наражати середовище на несанкціонований доступ до мережі, підслуховування або перехоплення даних.

6. Відсутність можливостей моніторингу та реагування на інциденти: без належних інструментів моніторингу та процедур реагування на інциденти стає важко виявляти інциденти безпеки та швидко реагувати на них. Це може призвести до того, що тривалий час компрометація або несанкціонований доступ залишатимуться непоміченими.

7. Неадекватні механізми резервного копіювання та відновлення. Недостатні стратегії резервного копіювання даних або ненадійні плани аварійного відновлення можуть зробити середовище вразливим до втрати даних, ускладнюючи або унеможливлюючи відновлення після інцидентів безпеки або системних збоїв.

8. Внутрішні загрози: необережні користувачі, співробітники або особи з привілейованим доступом, які зловживають своїми повноваженнями, можуть становити значний ризик для безпеки середовища, навмисно чи ненавмисно скомпрометувавши системи або викравши конфіденційну інформацію.

9. Відсутність оновлень безпеки та управління виправленнями: відсутність регулярного оновлення програмного забезпечення та застосування виправлень безпеки може залишити системи під відомими вразливими місцями, якими можуть скористатися зловмисники.

Захист середовища під час процесів автентифікації має вирішальне значення для підтримки безпеки та цілісності ваших цифрових систем, мереж і даних. Автентифікація служить основою для перевірки ідентичності користувачів, які намагаються отримати доступ до ресурсів, і відіграє важливу роль у запобіганні несанкціонованому доступу та захисті конфіденційної інформації. Щоб захистити середовище під час процесів автентифікації, важливо впроваджувати безпечні методи автентифікації, регулярно оновлювати та виправляти системи автентифікації, навчати користувачів правилам використання надійних паролів, використовувати багатофакторну автентифікацію, де це необхідно, і відстежувати журнали на наявність підозрілих дій. Крім того, отримання інформації про нові технології автентифікації та передові практики може допомогти вам випереджати нові загрози та підвищити безпеку.

1.2 Поняття автентифікації та її типи

Автентифікація — процес визначення, чи хтось або щось насправді є тим, за кого себе видає. Технології автентифікації забезпечують контроль доступу до систем шляхом перевірки того, що облікові дані користувача збігаються з обліковими

даними в авторизованій базі даних користувачів або сервері автентифікації даних. При цьому автентифікація забезпечує безпеку системи, процесів і корпоративної інформації [1].

Автентифікація має багато видів і типів. Для цілей ідентифікації користувачів користувачі зазвичай ідентифікуються за їхнім ідентифікатором користувача, а автентифікація відбувається, коли користувач надає облікові дані (наприклад, пароль), які відповідають його ідентифікатору користувача. Практика вимагання ідентифікатора користувача та пароля називається однофакторною автентифікацією (SFA). В останні роки з’явилась потреба в посилені процесу автентифікації, вимагаючи додаткових факторів, таких як унікальний код, який надається користувачам через їх мобільний пристрій, коли вони намагаються увійти, або біометричний підпис, такий як сканування обличчя чи відбиток пальця. Це називається двофакторною автентифікацією (2FA).

Коефіцієнти автентифікації можуть виходити навіть далі, ніж SFA, для якого потрібні ідентифікатор користувача та пароль, або 2FA, для якого потрібні ідентифікатор користувача, пароль і біометричний підпис. Коли для автентифікації використовуються три або більше факторів підтвердження особи — наприклад, ідентифікатор користувача та пароль, біометричний підпис і, можливо, особисте запитання, на яке користувач повинен відповісти, — це називається багатофакторною автентифікацією (MFA) [2].

1.3 Фактори автентифікації

Автентифікація користувача шляхом використання ідентифікатора користувача та пароля вважається найпростішим методом. Цей процес ґрунтується на тому, що користувач повинен мати знання двох компонентів інформації: свого ідентифікатора або імені користувача та пароля. Так як цей тип автентифікації базується лише на одному факторі, його можна віднести до типу однофакторна автентифікація (Single-Factor Authentication).

Існує і більш надійна автентифікація, яка має більший рівень захищеності від атак і є більш надійною . Цей тип автентифікації використовує різноманітні фактори і методи, щоб підтвердити ідентичність користувача з високою ступенем впевненості. Це може включати використання біометричних даних, двофакторну автентифікацію, шифрування та інші технології, які забезпечують високий рівень безпеки і захисту від несанкціонованого доступу. Зрозуміло що, надійну автентифікацію використовують для зменшення ризику порушення безпеки та забезпечення захисту важливої інформації [3].

Коефіцієнт автентифікації представляє фрагмент даних або атрибут, який можна використовувати для автентифікації користувача, який запитує доступ до системи. Факторами автентифікації можуть бути те, що ви знаєте, те, що у вас є, або те, чим ви є. За останні кілька років були розроблені додаткові фактори автентифікації. У деяких випадках місце розташування може використовуватись як четвертий фактор, що враховує географічне положення користувача під час процесу автентифікації. Це може бути досягнуто шляхом використання геолокаційних технологій, які визначають фізичне місцезнаходження пристрою або користувача.

Крім того, час може використовуватись як п'ятий фактор в автентифікаційному процесі. Це означає, що час, коли здійснюється автентифікація, може бути врахований як додатковий показник для підтвердження ідентичності користувача. Наприклад, система може вимагати, щоб автентифікація здійснювалася лише певного часу або в певному вікні часу, що забезпечує додатковий рівень безпеки.

Додавання місця розташування і часу як додаткових факторів до процесу автентифікації дозволяє збільшити надійність і стійкість системи до атак, оскільки використовуються додаткові параметри, що ускладнюють можливість несанкціонованого доступу до ресурсів чи пристроїв.

Фактори автентифікації, що використовуються на даний момент, включають наступне:

- **Фактор знань** в автентифікації використовується для підтвердження ідентичності користувача шляхом знання конфіденційної інформації. Цей фактор включає будь-які облікові дані, які користувач повинен знати, такі як персональний

ідентифікаційний номер (PIN), ім'я користувача, пароль або відповідь на секретне запитання. Наприклад, користувач може використовувати пароль, який він встановив під час реєстрації, або відповідати на питання, яке він попередньо вказав. Ця інформація є конфіденційною і повинна бути відома лише користувачу. Під час автентифікації система перевіряє введені дані з збереженими обліковими даними, щоб визначити, чи співпадають вони. Фактор знань є поширеним методом автентифікації і може бути ефективним, якщо облікові дані користувача залишаються в таємниці. Однак, слабкі або легко вгадувані паролі, недостатньо складні запитання або використання загальновідомих інформаційних даних можуть підірвати безпеку цього фактора. Тому важливо створювати міцні паролі та використовувати надійні запитання для забезпечення ефективної автентифікації з фактором знань.

- **Фактор володіння** в автентифікації використовується для підтвердження ідентичності користувача на основі предметів, якими він володіє та носить з собою, наприклад смартфон або ключ з чіпом.

- **Фактор невід’ємності**, також відомий як фактор приналежності, використовується для автентифікації на основі біометричних даних, які є унікальними для кожної особи. Цей фактор ґрунтується на тому, "чим ви є" з точки зору фізичних характеристик. Наприклад, фактор невід’ємності може включати використання відбитків пальців, розпізнавання обличчя або сканування сітківки ока. Ці дані вимірюються та реєструються, а потім використовуються для порівняння зі збереженими у базі даних даними, щоб підтвердити особу.

- **Фактор розташування** використовується як додатковий елемент для автентифікації, який базується на місцезнаходженні користувача. Цей фактор може бути використаний як доповнення до інших факторів автентифікації для забезпечення більшої безпеки та захисту. Місцезнаходження може бути визначено за допомогою систем глобального позиціонування (наприклад, GPS) або перевіркою мережевих адрес і маршрутів. За допомогою цих засобів можна встановити прийнятну точність розташування користувача. Фактор розташування сам по собі зазвичай не використовується для автентифікації в самостійному режимі, але він може доповнювати інші фактори, що забезпечує засіб виключення певних запитів.

Наприклад, це може завадити зловмиснику, який знаходиться у віддаленій географічній зоні, намагаючись видати себе за користувача, який зазвичай входить лише зі свого дому чи офісу в країні, де розташована організація. Фактор розташування допомагає підвищити безпеку системи, але варто враховувати, що визначення розташування може бути неабсолютним і піддається певним обмеженням.

- **Фактор часу** є додатковим механізмом для автентифікації, який використовується для відсіювання зловмисників, які намагаються отримати доступ до ресурсу у неприпустимий час. Використання фактора часу може забезпечити додатковий рівень безпеки, особливо якщо поєднується з іншими факторами, наприклад, фактором розташування. Прикладом використання фактора часу є сценарій, коли користувач востаннє автентифікувався опівдні в США. Якщо через годину буде спроба автентифікації з Азії, система може відхилити запит на основі комбінації часу та місця, оскільки така зміна розташування та часу може свідчити про несанкціоновану спробу доступу [4].

1.4 Вразливості безпеки протоколів автентифікації

Основні групи атак на процес автентифікації включають наступне:

1. Атаки на користувацький інтерфейс: Ці атаки спрямовані на отримання облікових даних користувача або обман користувача для розкриття своїх автентифікаційних даних;

2. Атаки на базу даних шаблона: Ці атаки спрямовані на отримання доступу до бази даних, в якій зберігаються шаблони автентифікації, наприклад, хеші паролів;

3. Атаки на системні модулі та взаємозв’язки між модулями: Ці атаки спрямовані на вразливості у системних модулях або недостатньо захищених взаємозв’язках між модулями, включаючи атаки на протоколи комунікації. Зловмисники можуть спробувати використовувати вразливості в системі автентифікації, такі як атаки на перехоплення та підробку токенів автентифікації, маніпуляції з протоколами обміну повідомленнями або атаки на сервіси автентифікації [5];

Автентифікація є критичним етапом для забезпечення безпеки веб-додатків під час атак на користувацький інтерфейс. Коли користувач вводить своє ім'я та пароль для входу, а потім проходить перевірку правильності даних, додаток визначає права доступу, які будуть надані системі, на основі ідентифікатора, що встановлюється за наданими обліковими даними.

Існує кілька різних протоколів автентифікації, які можуть використовуватися в HTTP:

1. Базовий - використовується не зашифровані імена користувача та паролі.

2. Digest – як базовий, але вже використовуються зашифровані паролі.

3. Форма - використовується налаштована форма для введення облікових даних користувача, яка обробляється на бекенді.

4. NTLM - протокол автентифікації, який використовується в HTTP-запитах та відповідях.

5. Negotiate - протокол, який дозволяє клієнту та серверу використати будь-який тип автентифікації, зазначеному вище.

6. Клієнтські сертифікати - механізм, який дозволяє перевіряти автентичність цифрового сертифікату, наданого веб-клієнтом за допомогою SSL/TLS.

7. Microsoft Passport - це служба єдиного входу, керована Microsoft, яка дозволяє веб-сайтам автентифікувати користувачів за допомогою їх участі в службі Passport. Цей механізм використовує спільний ключ між Microsoft та партнерськими сайтами для створення файлу cookie, який ідентифікує користувача.

Всі наведені протоколи автентифікації використовуються в рамках протоколу HTTP або SSL/TLS і передають облікові дані, що вбудовані безпосередньо в трафік між клієнтом і сервером [7].

У разі, якщо хакер успішно пройшов процес автентифікації та підтвердив свою ідентичність як законний користувач, він отримує повний доступ до системи на тому самому рівні привілеїв, які були призначені цьому аккаунту користувача.

В таблиці 1.1 визначено різні атаки, які спрямовані на порушення процесу автентифікації.

Таблиця 1.1

Типи атак на процеси автентифікації

Атака	Опис
Brute-force attack	Зловмисник використовує автоматизований процес для послідовного підбіру всіх можливих комбінацій паролів, намагаючись знайти правильний пароль для автентифікації.
Перебір за словником	Ця атака використовує заздалегідь підготовлений словник або список популярних паролів, які зазвичай використовуються користувачами. Зловмисник послідовно перевіряє кожен пароль зі словника, сподіваючись знайти відповідну пару для автентифікації. Це ефективний метод для атаки на слабкі або прості паролі, які легко відгадати.
Sniffing attack	Хакер перехоплює трафік мереж та потім аналізує, що з цього може містити пароль. Якщо пароль не зашифрований то його легше виявити, тому шифрування забезпечує вищий рівень захисту від цієї атаки.
Spoofing attack	Спуфінг-атака, відома також як атака підробки, є методом, за допомогою якого зловмисник підроблює свою ідентичність або джерело даних, щоб надати обманливу інформацію або отримати незаконний доступ до системи. Це здійснюється шляхом зміни суб'єкта

	атаки (IP-адреси, електронної пошти, веб-сайту і т.д.) так, що зловмисник здається законним або довіреним джерелом. Наприклад, випадок спуфінг-атаки може включати підробку IP-адреси, щоб зловмисник з'явився як легітимний користувач або сервер, та передачу обманливих даних або запитів, які можуть привести до несанкціонованого доступу до системи або виконання шкідливих дій.
Man in the middle	Атака посередника є типом атаки, при якій зловмисник вступає між комунікаційними сторонами та перехоплює або змінює передані між ними дані. Замість прямої комунікації між двома сторонами, зловмисник підключається до мережі і перехоплює, аналізує або зламує дані, передані між ними. У такій атаці зловмисник може отримувати доступ до конфіденційних даних, таких як паролі, особисту інформацію або фінансові дані, а також може модифікувати передані дані для впливу на поведінку системи або спричинення шкоди.

Для протидії атакам на автентифікацію можна вжити такі заходи:

1. Встановлення надійної парольної політики: Застосування вимог до складності паролів, включаючи використання комбінації великих і малих літер, цифр і спеціальних символів. Також важливо вимагати регулярну зміну паролів.

2. Збереження історії паролів: Заборона використання раніше використаних паролів, щоб запобігти повторному використанню старих та потенційно компрометованих паролів.

3. Багатофакторна автентифікація: Використання двофакторної або більш складної автентифікації, яка вимагає двох або більше методів підтвердження ідентифікації, наприклад, пароль разом з кодом, отриманим на мобільний пристрій.

4. Використання строгої системи порядкової нумерації: Застосування унікальних і непередбачуваних ідентифікаторів для автентифікаційних сесій та запобігання використанню старих або відновлених ідентифікаторів.

5. Аудит кількості невдалих спроб входу в систему: Моніторинг і реєстрація кількості невдалих спроб автентифікації, що дозволяє виявляти підозрілу активність або спроби злому.

6. Контроль мережі та систем на предмет наявності інструментів перехоплення і крадіжки паролів: Використання мережевих моніторингових інструментів для виявлення можливих загроз, таких як програми перехоплення пакетів чи шкідливе програмне забезпечення.

7. Блокування облікового запису при введенні великої кількості неправильних паролів за короткий проміжок часу: Застосування заходів, що обмежують атаки перебором паролів, таких як тимчасове блокування облікового запису після декількох невдалих спроб.

Оскільки парольна автентифікація є найпопулярнішою, потрібно заохочувати посилення паролю, щоб їх не було легко вгадати або зламати:

1. Використовуйте довгі паролі: Встановіть мінімальну довжину пароля на прийнятний рівень, наприклад, не менше 8-10 символів. Чим довший пароль, тим складніше його вгадати або зламати.

2. Складність паролів: Вимагайте використання комбінації великих і малих літер, цифр та спеціальних символів у паролі. Не використовуйте очевидні комбінації, такі як "123456".

3. Унікальні паролі: Кожному обліковому запису повинен бути призначений унікальний пароль. Не використовуйте один і той самий пароль для різних сервісів або веб-сайтів.

4. Заборона використання особистої інформації: Уникайте використання особистої інформації, такої як ім'я, дата народження чи номер телефону, у паролях. Ця інформація може бути легко вгадана або знайдена зловмисниками.

5. Регулярна зміна паролів: Заохочуйте користувачів регулярно змінювати свої паролі, наприклад, кожні 3-6 місяців. Це зменшить ризик, що старий пароль буде компрометований.

Оскільки біометричні дані, які зберігаються в базі даних шаблонів, можуть піддаватися атакам, існують різні методи захисту цих шаблонів. Наприклад, скасована біометрія є такими методами. Скасована біометрія використовує повторюване спотворення прийнятого біометричного сигналу, що базується на певних перетвореннях, для захисту біометричного шаблону.

Атаки на системні модулі пов'язані зі зміною внутрішніх компонентів і можуть бути здійснені в різних модулях, таких як модулі попередньої обробки, вилучення ознак, зіставлення і прийняття рішень.

Висновки до першого розділу

Автентифікація відіграє ключову роль в забезпеченні безпеки організаційних мереж та ресурсів. Цей процес дозволяє лише правомірним користувачам отримувати доступ до захищених ресурсів, таких як комп'ютерні системи, мережі, бази даних, веб-сайти та інші мережеві програми або служби.

Авторизація включає в себе дві важливі частини. По-перше, адміністратор надає права доступу автентифікованим користувачам, щоб визначити їх привілеї. По-друге, система перевіряє дозволи користувача облікового запису, щоб переконатися,

що він має право отримувати доступ до цих ресурсів. У результатах, користувачеві надаються відповідні привілеї, які залежать від його дозволів, що зберігаються локально або на сервері автентифікації. Адміністратор встановлює всі налаштування для цих змінних середовища.

Атаки на процес автентифікації можуть бути класифіковані на три основні типи. Перш за все, атаки на користувацький інтерфейс, де зловмисники намагаються отримати доступ до облікових записів, використовуючи незаконний доступ до інтерфейсу користувача. Другий тип - атаки на базу даних шаблонів, де зловмисники намагаються змінити або вилучити біометричні дані, що зберігаються в базі даних. Нарешті, атаки на системні модулі та їх взаємозв'язки, де шкідливе програмне забезпечення може впливати на процеси обробки, вилучення ознак та прийняття рішень.

РОЗДІЛ 2
МЕТОДИ ТА ПРОТОКОЛИ АВТЕНТИФІКАЦІЇ

Усі методи автентифікації вимагають, щоб ви вказали, хто або що ви є, і передали відповідні облікові дані, щоб підтвердити, що ви є тим, за кого себе видаєте. Ці облікові дані зазвичай мають форму того, що ви знаєте, чогось у вас є або чимось, чим ви є. Те, що ви знаєте, може бути паролем. Те, що у вас є, може бути смарт-картою. Те, що ви є, відноситься до галузі біометрії, в якій складне обладнання використовується для сканування людини в певному сенсі для забезпечення автентифікації. Важливим елементом є визнання того, що різні механізми надають послуги автентифікації з різним ступенем достовірності. Вибір належної технології автентифікації значною мірою залежить від розташування об’єктів, які автентифікуються, і ступеня довіри до окремих аспектів мережі.

2.1 Автентифікація імені користувача та пароля

В останні роки було присвячено багато робіт вивченню захисту інформації або ресурсів від неавторизованих користувачів. Було досліджено, що автентифікація за паролем є найбільш прийнятним і добре використовуваним методом на сьогоднішній день, оскільки він простий у використанні та виконанні, має низьку вартість. Ім'я користувача та пароль часто використовуються на практиці. Це метод автентифікації, який базується на «те, що ви знаєте». Це найпростіший спосіб автентифікації, який надає кожному користувачеві унікальне ім’я користувача та секретний пароль. Це простий спосіб зазнати атаки шляхом вгадування пароля. Найбільша проблема хорошого пароля полягає в тому, що користувачі можуть легко його забути. Просити користувача згадати один ідентифікатор користувача та пароль для однієї системи може здатися розумним, але з поширенням систем – поширюється і кількість паролів, яку користувачі мають пам’ятати, або вони використовують один пароль для усіх сервісів. Поки користувач може ввести правильне ім’я користувача та пароль,

комп’ютер і система припускатимуть, що оператор, який користується комп’ютером, є офіційним або оригінальним користувачем. Насправді багато користувачів часто використовують рядок символів, який легко вгадати, як-от день народження, номер телефону або ім’я домашньої тварини як пароль, щоб запобігти забуттю свого пароля. Або вони записують пароль на папері і ховають десь, де, на їхню думку, це може бути безпечно. Таким чином, інформація може бути втрачена або викрадена. Навіть якщо можна гарантувати, що ім’я користувача та пароль не буде викрадено, це все одно не дуже безпечно. Це оскільки ім’я користувача та пароль зберігаються в статичному стані в базі даних. Таким чином, його потрібно передати на мережеву платформу та через пам’ять комп’ютерів під час процесу автентифікації. Кожного разу інформація автентифікації буде однаковою, тому наприклад програмам-шригунам легко перехватити пароль, спостерігаючи за трафіком. Таким чином, з точки зору безпеки, ім’я користувача та пароль є дуже небезпечним методом автентифікації [8].

2.2 Система PassWindow як некриптографічна технологія автентифікації

Некриптографічні алгоритми автентифікації розширюють можливості підтвердження автентичності користувача, використовуючи не лише логін та пароль, але й додаткові засоби. Ці засоби можуть включати мобільні телефони, смарт-карти, токени та інші пристрої.

Використання таких додаткових засобів дозволяє збільшити рівень безпеки і запобігти несанкціонованому доступу до системи. Наприклад, багатофакторна автентифікація вимагає введення не лише логіна та паролю, але й додаткового коду, який може бути отриманий через мобільний телефон або інший пристрій. Таким чином, навіть якщо зловмиснику вдасться дізнатися логін та пароль, він все одно не зможе отримати доступ до системи без додаткового підтвердження.

Алгоритм некриптографічної автентифікації наведено на рисунку 2.1.

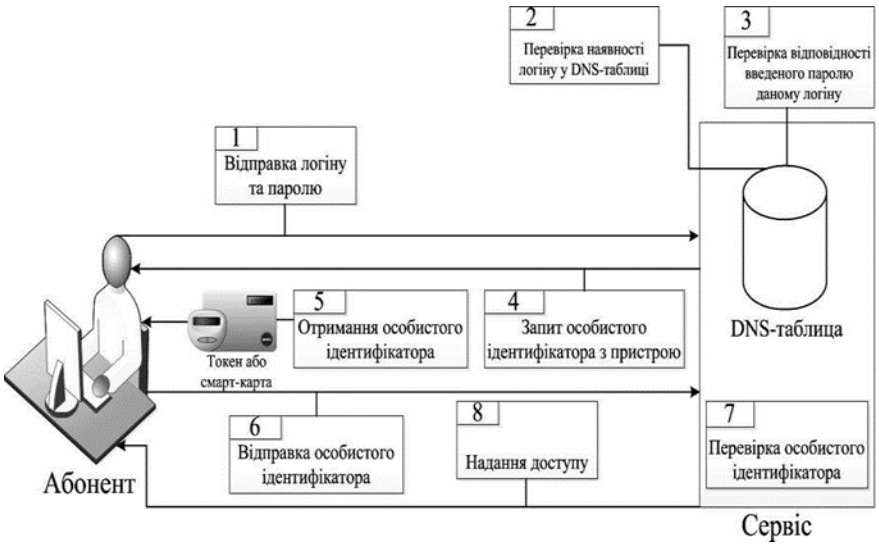

Рисунок 2.1 Схема алгоритму некриптографічної автентифікації

Система автентифікації PassWindow належить до класу двофакторних і некриптографічних методів автентифікації. Основна ідея полягає в тому, що, крім знання логіна та пароля, користувач має доступ до додаткового засобу для підтвердження своєї ідентичності. Цим засобом можуть бути електронний сертифікат на пристрої користувача, спеціальний код безпеки, що надсилається на особистий телефон або в застосунок, або навіть біометричні дані користувача.

Алгоритм PassWindow базується на створенні унікального ключа доступу. Частина цього ключа надрукована на прозорій частині стандартного ідентифікаційного документа у вигляді штрих-коду. Для формування повного унікального ключа доступу необхідно навести картку на екран монітора, термінала, мобільного телефону або планшета у певну область, де формується друга частина коду, яка також має вигляд штрих-коду.

Шаблони штрих-кодів PassWindow можуть мати форму унікальних статичних зображень символів або бути розширеною анімаційною версією шаблону. Сервер автентифікації генерує послідовності шаблонів штрих-кодів, кожна з яких є унікальною і може використовуватися тільки зі співпадаючим ключем.

PassWindow здатна надійно передавати будь-які буквено-цифрові коди, але наразі її реалізація зосереджена на передачі коротких послідовностей випадкових

цифр, які можуть бути використані як одноразові паролі у поєднанні з ідентифікуючими цифрами для перевірки справжності користувача.

Коли користувач підтверджує, що інформація, закодована у штрих-кодах, відповідає очікуваному значенню, він може закінчити транзакцію, за допомогою відповідного паролю.

PassWindow пропонує додатковий рівень безпеки та захисту при автентифікації, використовуючи унікальний процес формування ключа доступу. Ця система дозволяє забезпечити більш надійний контроль над доступом до ресурсів і зменшити ризик несанкціонованого вторгнення.

Основні етапи системи PassWindow подано на рисунку 2.2.

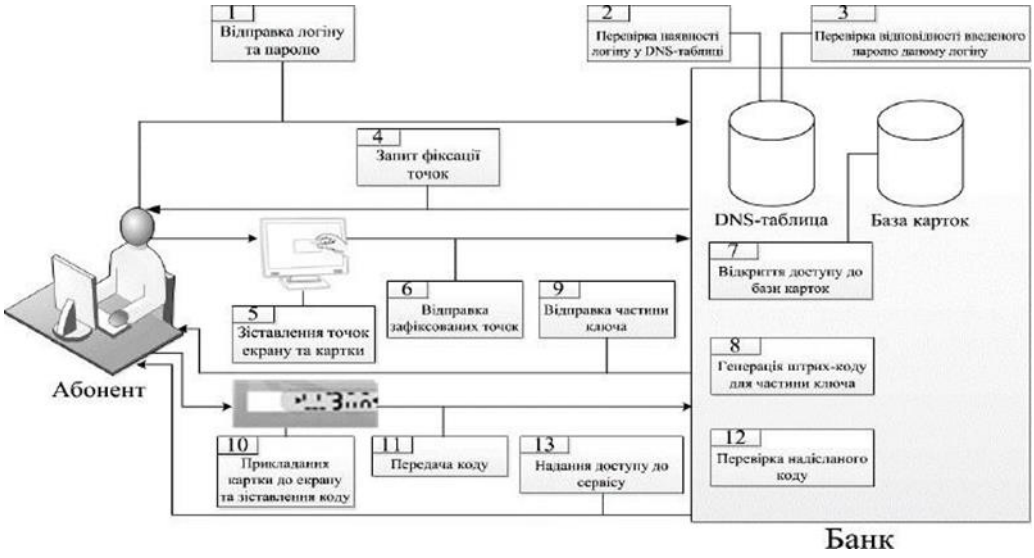

Рисунок 2.2 Схема алгоритму подвійної автентифікації PassWindow

Принцип роботи автентифікації має такий алгоритм:

1. Користувач пройшов ідентифікацію і готовий до автентифікації.

2. Перевіряється наявність логіна користувача в DNS-таблиці.

3. Проводиться перевірка введеного пароля.

4. Здійснюється запит для фіксації точок на картці.

5. Користувач прикладає свою картку до екрану, і система фіксує відповідність точок на штрих-коді картки.

6. Зафіксовані точки відправляються до сервісу для подальшого зберігання.

7. Відкривається доступ до бази даних карток для подальшої обробки.

8. Генерується штрих-код для другої частини ключа.

9. Частина ключа, яка представлена штрих-кодом, надсилається користувачеві.

10. Користувач, прикладаючи свою персональну картку до екрану свого пристрою, формує код.

11. Отриманий код надсилається до сервісу для подальшої перевірки.

12. Надісланий код перевіряється на правильність.

13. Якщо автентифікації пройшла успішно, користувачу надається доступ до сервісу.

2.3 Автентифікація за допомогою смарт-картки та USB-ключів

Смарт-картки є універсальними пристроями, які можуть зберігати та обробляти інформацію, виконувати криптографічні операції та забезпечувати безпеку даних. Вони широко використовуються в різних галузях, включаючи фінансові послуги, транспортні системи, ідентифікацію особи, контроль доступу та інші.

Смарт-картки залежно від факторів мають різні класифікації.

Залежно від типу мікросхеми смарт-картки бувають:

- З перепрограмованою енергозалежною пам'яттю: Ці картки мають можливість перезаписувати та змінювати інформацію, яку вони зберігають. Вони зазвичай використовуються для зберігання особистої інформації.
- з перепрограмованою захищеною пам'яттю: Ці картки мають механізм захисту та доступу до читання/запису, який вимагає введення спеціального коду або пароля. Вони широко використовуються у розрахункових картках або для зберігання даних, де безпека є пріоритетом.
- Багатофункціональні смарт-картки: Це картки з великим об'ємом енергозалежної перепрограмованої пам'яті, а також спеціальний мікропроцесор та вбудовану операційну систему. Вони забезпечують широкий набір функцій і можуть бути використані для різних застосунків, включаючи розрахункові системи, ідентифікацію, контроль доступу та інші послуги користувача.

За призначенням виділяють такі смарт-карти: лічильники, пам'яті, мікропроцесорні.

Карти-лічильники використовуються, коли необхідно віднімати фіксовану суму в усіх платіжних операціях.

Картки пам'яті використовуються для зберігання інформації і можуть бути двох типів: з захищеною і незахищеною пам'яттю. У незахищених картках немає обмежень для читання та запису даних.

У картках з захищеною пам'яттю є механізм, який дозволяє читати, записувати або вилучати інформацію, але для цього потрібно ввести спеціальний секретний код, іноді навіть кілька кодів. Зазвичай, картки з захищеною пам'яттю мають область, де зберігаються ідентифікаційні дані. Записані дані неможливо змінити, що необхідно для запобігання підробленню картки. Такі картки можуть використовуватися як засіб платежу та для зберігання конфіденційних даних.

Мікропроцесорні картки схожі на картки пам'яті, але мають чіп, що робить їх справжніми розумними картками. Мікропроцесор - це мікросхема або чіп, який може зберігати значну кількість інформації та виконувати арифметичні та/або логічні операції. Такі картки є своєрідними мікрокомп'ютерами з власним процесором, оперативною та постійною пам'яттю, а іноді навіть операційною системою. Зазвичай вони також мають вбудовані криптографічні засоби для шифрування інформації.

На картці встановлюється спеціалізована операційна система, яка надає широкий набір сервісних операцій та засобів безпеки. Операційна система картки підтримує файлову систему, яка дозволяє розмежовувати доступ до збереженої на картці інформації.

Смарт-карти можуть використовуватися для ідентифікації, автентифікації або авторизації користувача, зберігання на них ключової інформації, а також для здійснення криптографічних операцій [9].

Електронний ключ (ЕК) - це фізичний пристрій, який використовується для захисту програмного забезпечення та даних від несанкціонованого копіювання, поширення та незаконного використання. ЕК має форму компактного знімного USB-

пристрою, вбудованого на двошарову друковану плату. На цій платі розташовані електронні компоненти ЕК і USB-роз'єм.

Електронний ключ виконує такі функції:

- Генерацію сеансових ключів.
- Приймання, зберігання, надання доступу та знищення довільних даних користувача на ЕК.
- Автентифікацію користувача.
- Створення КЕП для даних, що завантажуються з ЕОМ за допомогою особистого ключа КЕП.
- Прийняття та зберігання загальних параметрів для алгоритмів КЕП та протоколу розподілу ключів.
- Створення спільного секретного ключа.
- Шифрування та розшифрування сеансових ключів за допомогою спільного секретного ключа.
- Приймання та зберігання двох довгострокових ключових елементів (ДКЕ), які використовуються у алгоритмі генерації випадкових бітових послідовностей.
- Знищення особистих ключів КЕП та протоколу розподілу ключів.
- Управління параметрами автентифікації користувача.
- Генерацію та зберігання особистих ключів КЕП та протоколу розподілу в зашифрованому вигляді з контролем цілісності.

Електронний ключ (ЕК) повинен мати такі функціональні компоненти:

- Процесор з вбудованими елементами: оперативною пам'яттю, постійною пам'яттю, генератором тактових сигналів та контролером шини USB.
- Генератор випадкових сигналів (ГВС).
- Стабілізатори напруги для живлення всіх компонентів ЕК.

Процесор виконує такі функції:

- Програми, які реалізують функціональні можливості ЕК.

- Зберігання особистих ключів, даних автентифікації та користувацьких даних у вбудованій постійній пам'яті.
- Організація обміну інформацією з ЕОМ за допомогою інтерфейсу USB.

ГВС має за завдання створення аналогового випадкового сигналу і його подальше перетворення у двійкову форму, що використовується при формуванні послідовностей випадкових значень.

Програми ЕК повинні включати:

- програмний комплекс тестування та конфігурування ЕК;
- внутрішні програмні компоненти ЕК;
- системні програмні компоненти.

Внутрішні програми ЕК призначені для:

- забезпечення коректного розпізнавання ЕК ОС ЕОМ;
- знищення з ПЗП особистих ключів КЕП та протоколу розподілу ключів;
- зберігання у ПЗП особистих ключів КЕП та протоколу розподілу ключів в зашифрованому вигляді з контролем цілісності;
- генерація сеансових ключів;
- передачу кодів команд та вхідних даних для виконання відповідних внутрішніх програм крипто-графічного модуля, які виконують перетворення вхідних даних у вихідні;
- зашифрування та розшифрування сеансових ключів з використанням сформованого спільного секрет-ного ключа;
- формування спільного секретного ключа за протоколом розподілу ключовими даними з використанням особистого ключа протоколу розподілу та відкритого ключа протоколу розподілу отримувача;
- генерації особистого ключа КЕП та протоколу розподілу ключів з використанням алгоритму генерації випадкових бітових послідовностей КЕП і вбудованого апаратного ГВС;
- прийому та зберігання у ПЗП загальних параметрів для алгоритму КЕП та протоколу розподілу ключів;

- прийому, запис та зберігання у ПЗП довільних даних користувача;
- управління параметрами автентифікації користувача;
- прийому та зберігання у ПЗП двох ДКЕ;
- надання доступу та знищення довільних даних користувача з ПЗП.

Системні програмні компоненти призначені для:

- отримання з ЕК результатів виконання команд та вихідних даних;
- формування КЕП від даних, що завантажуються з ЕОМ з використанням особистого ключа КЕП;
- автентифікації користувача перед початком роботи.
- Програмний комплекс тестування та конфігурування призначений для:
- форматування ЕК, що включає знищення особистих ключів та довільних даних користувача у ЕК;
- встановлення або зміни даних автентифікації користувача ЕК шляхом їх завантаження у ЕК;
- конфігурування параметрів ЕК у ОС ЕОМ;
- перевірки роботоспроможності ЕК.

До складу ключових даних ЕК повинні входити:

- особистий та відкритий ключі протоколу розподілу ключів;
- особистий та відкритий ключі КЕП;
- ДКЕ, що використовуються у алгоритмі генерації випадкових бітових послідовностей та протоколі розподілу ключових даних;
- загальні параметри КЕП та протоколу розподілу ключів.

Особисті ключі КЕП і ключі протоколу розподілу повинні генеруватися внутрішньо в ЕК. Після цього, особисті ключі мають бути збережені внутрішнім ПЗП, а відкриті ключі передаються до ЕОМ для подальшого поширення.

Захист інформації, що обробляється в ЕК, від несанкціонованого доступу має бути забезпечений наступними заходами:

- Автентифікація користувача перед початком роботи з ЕК.
- Зберігання особистих ключів в захищеному вигляді у внутрішньому ПЗП.

- Використання командного інтерфейсу взаємодії, який виключає прямий доступ до внутрішніх вузлів та програм ЕК.

Захист і контроль цілісності особистих ключів у внутрішньому ПЗП здійснюється за допомогою захищеного пароля. Особисті ключі перевіряються на цілісність шляхом порівняння виробленої хеш-суми з еталоном, що зберігається у ПЗП. Крім того, ключі захищаються шляхом кодування за допомогою режиму простої заміни.

Автентифікація користувача перед початком роботи з ЕК здійснюється шляхом передачі пароля доступу до ЕК, його хешування та порівняння з еталоном, що зберігається у внутрішньому ПЗП. На основі результату порівняння ЕК приймає рішення щодо успішності автентифікації.

2.4 Challenge handshake authentication protocol

Протокол CHAP використовується для періодичної перевірки особи партнера за допомогою тристороннього рукостискання. CHAP — це протокол автентифікації віддаленого доступу, який використовується в поєднанні з протоколом Point-to-Point для забезпечення безпеки та автентифікації користувачів віддалених ресурсів. Процес автентифікації працює таким чином:

1. Після завершення фази встановлення зв’язку автентифікатор надсилає однорангові повідомлення запити.
2. Одноранговий вузол відповідає значенням, обчисленим за допомогою функції «одностороннього хешування»
3. Автентифікатор перевіряє відповідь на власні обчислення та отримує підтвердження; інакше з’єднання має бути розірвано
4. Через випадкові проміжки часу автентифікатор надсилає новий виклик одноранговому партнеру та повторює кроки з першого по третій.

CHAP забезпечує захист від атаки відтворення з боку однорангового пристрою за допомогою використання ідентифікатора, що поступово змінюється, і змінного значення виклику. Використання повторних викликів має на меті обмежити час

впливу будь-якої окремої атаки. Автентифікатор контролює частоту та час викликів. Цей метод автентифікації залежить від «паролю», відомого лише автентифікатору та одноранговому вузлу. Паролю не надсилається за посиланням. Хоча автентифікація є лише односторонньою, шляхом узгодження CHAP в обох напрямках один і той самий секретний набір можна легко використовувати для взаємної автентифікації. Оскільки CHAP може використовуватися для автентифікації багатьох різних систем, поля імен можуть використовуватися як індекс для пошуку потрібного паролю у великій таблиці паролів. Це також дає можливість підтримувати більше ніж одну пару ім’я/секрет на систему та змінювати використовуваний пароль у будь-який час протягом сеансу. Але з іншого боку, CHAP вимагає, щоб пароль був доступний у формі звичайного тексту. Необоротно зашифровані бази даних паролів, які є загальнодоступними, не можна використовувати. Це погано для великих установок, оскільки всі можливі паролі зберігаються на обох кінцях зв’язку [10].

2.5 Автентифікація Kerberos

Протокол Kerberos використовується для перевірки автентичності у системах "клієнт-сервер" та обміну захищеною інформацією з метою створення безпечного каналу зв'язку між користувачами, що працюють у локальних або глобальних мережах. Kerberos був спеціально розроблений для мереж на основі протоколу TCP/IP і побудований на принципі довіри учасників протоколу до третьої (довіреної) сторони. Служба Kerberos забезпечує надійну перевірку автентичності в мережі з подальшою авторизацією доступу клієнта (клієнтського додатка) до ресурсів цієї ж мережі. Безпека сеансів Kerberos забезпечується застосуванням симетричних алгоритмів шифрування. Служба Kerberos розділяє спеціальний секретний ключ з кожним суб'єктом мережі, і знання цього ключа є доказом автентичності суб'єкта мережі.

Система Kerberos має структуру типу "клієнт-сервер" і складається з клієнтських компонентів, які встановлені на всіх машинах мережі, а також сервера Kerberos. Клієнтами можуть бути користувачі, а також незалежні програми, які

виконують різні дії, такі як доступ до баз даних, принтерів, отримання привілеїв адміністратора та інше [11].

Kerberos генерує сеансові ключі, які надаються лише клієнту й серверу (або двом клієнтам). Ці ключі використовуються для шифрування повідомлень, якими обмінюються сторони, і видаляються після завершення сеансу.

У системі Kerberos використовуються два типи документів: квиток (ticket) і автентифікатор (authenticator).

Отримання початкового квитка включає виділення квитка, відомого як квиток Ticket Granting Ticket (TGT), який підтверджує клієнта службі TGT. TGT зашифровується за допомогою секретного ключа TGS і містить ідентифікатори клієнта й сервера, сеансовий ключ для пари TGS-клієнт та початковий і кінцевий час дії TGT. Сервер автентифікації надсилає цей зашифрований квиток клієнту.

Таким чином, клієнт може пройти автентифікацію в TGS-сервері, використовуючи отриманий квиток TGT протягом усього терміну дії TGT.

Після цього клієнт може отримати окремий квиток для кожної необхідної йому служби. Для цього клієнт надсилає запит до служби TGS (запит відправляється автоматично без втручання користувача). Запит складається з квитка TGT і автентифікатора. Автентифікатор зашифровується за допомогою сеансового ключа, що використовується між клієнтом і TGS-сервером, і містить ідентифікатори клієнта та сервера, випадковий сеансовий ключ та мітку часу. TGS, отримавши запит, розшифровує TGT за допомогою свого секретного ключа. Потім TGS використовує вкладений у TGT сеансовий ключ для розшифрування автентифікатора. На останньому етапі проводиться порівняння інформації, яка міститься в автентифікаторі, з інформацією в квитку. Якщо всі дані вірні, то TGS дозволяє виконати запит.

Перевірка міток часу передбачає, що годинники всіх комп'ютерів і серверів мають однаковий час. Якщо час, вказаний у запиті, суттєво відрізняється від поточного часу, TGS розглядає цей запит як спробу повторного виконання.

При правильному запиті TGS надає клієнту квиток для доступу до цільового сервера. TGS також створює сеансовий ключ для клієнта й цільового сервера, який

зашифрований сеансовим ключем, що спільний для клієнта й TGS. Обидва повідомлення надсилаються клієнту. Потім клієнт розшифровує повідомлення й отримує сеансовий ключ.

Запит до служби. Тепер клієнт може підтвердити свою ідентичність цільовому серверу. Щоб успішно пройти автентифікацію на цільовому сервері, клієнт створює автентифікатор, який містить його ім'я, мережеву адресу та мітки часу. Цей автентифікатор зашифровується за допомогою сеансового ключа "клієнт-сервер" і надсилається разом з квитком, який зашифрований секретним ключем цільового сервера, який отримано від TGS. Після отримання даних від клієнта, цільовий сервер перевіряє автентифікатор. Він розшифровує його за допомогою свого секретного ключа і отримує сеансовий ключ. Квиток також перевіряється. Процедура перевірки схожа на процедуру "клієнт-TGS" - перевіряється відповідність мережних адрес і часової мітки. Якщо все в порядку, сервер переконується, що клієнт є тим, за кого він себе видає.

Якщо потрібна взаємна перевірка, сервер надсилає клієнту повідомлення, яке містить зашифровану мітку часу сеансовим ключем. Це дозволяє довести, що сервер знає правильний секретний ключ і може розшифрувати квиток і посвідчення. При необхідності клієнт і сервер можуть шифрувати наступні повідомлення загальним ключем. Керберос також може використовуватися для міждоменної автентифікації. При доступі клієнта до центру розподілу ключів (KDC) з метою отримання доступу до сервера в іншому домені, KDC видаватиме клієнту квиток пересилки (refferal ticket) для звернення до KDC того домену, в якому знаходиться необхідний сервер для користувача. На рисунку 2.3 зображен процес автентифікації за допомогою Kkerberos.

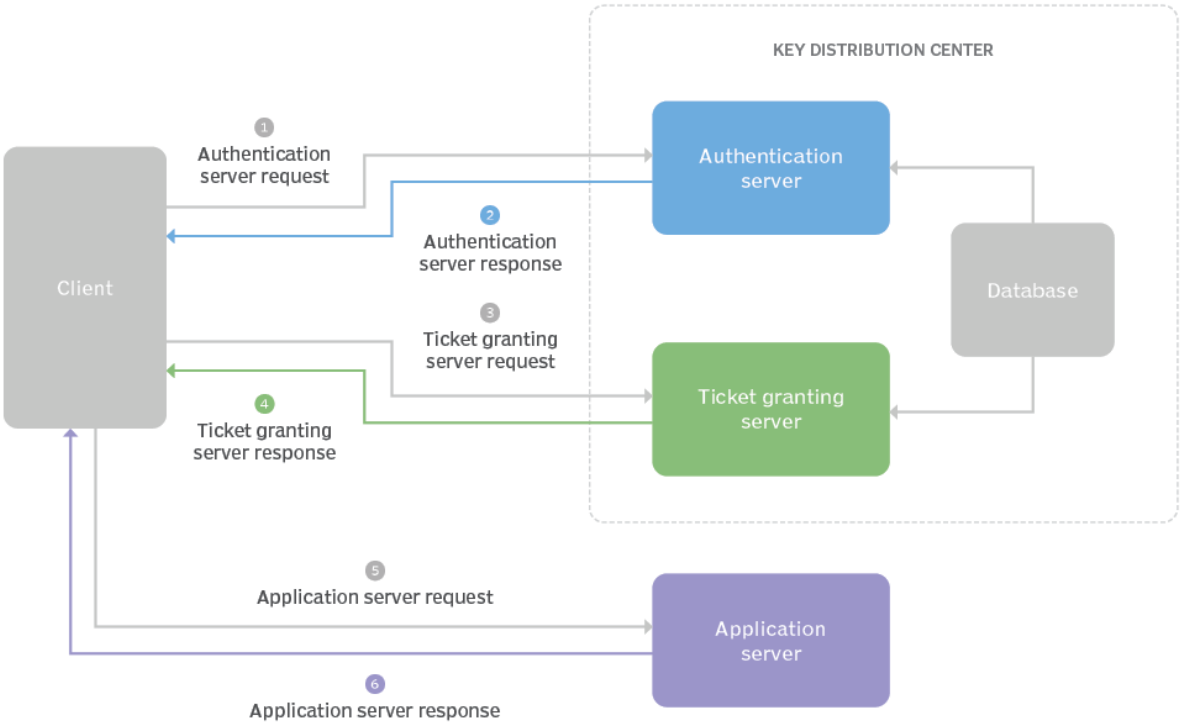

Рисунок 2.3 Процес автентифікації, використовуючі протокол Kerberos

Kerberos працює в незахищеному середовищі, тому неправильна конфігурація може призвести до витоку критичної інформації, такої як сеансові ключі, що зберігаються на жорсткому диску, або відкритих даних. Навіть зберігання ключів тільки в оперативній пам'яті може бути небезпечним при збоях в операційній системі, які дозволяють скопіювати ключі на жорсткий диск.

Протокол Kerberos вимагає виконання додаткових вимог, таких як:

- Захист служб Kerberos від атак, спрямованих на відмову в обслуговуванні.
- Синхронізація системного часу між усіма учасниками системи.
- Надійний захист служб Kerberos від будь-якого несанкціонованого доступу.
- Захист отриманих клієнтом мандатів та секретних ключів від несанкціонованого доступу.

Невиконання цих вимог може стати причиною успішної атаки.

2.6 Автентифікація на основі токенів

Токен — це пристрій безпеки, який автентифікує користувача за допомогою відповідного дозволу (наприклад, пароля), вбудованого в сам токен. Суть автентифікації на основі токенів полягає в тому, що ви повинні мати маркер у своєму розпорядженні, щоб автентифікувати себе на комп'ютері. Комп'ютер не впізнає вас без токена, незалежно від того, чи було токен загублено, позичено чи вкрадено [12]. Основні властивості токенів:

- Людина повинна фізично володіти токеном, щоб ним користуватися
- Хороший токен важко скопіювати
- Людина може втратити токен і ненавмисно втрачають доступ до критичного ресурса
- Люди можуть виявити вкрадені токени, провівши інвентаризацію токенів, які вони повинні мати у своєму розпорядженні.

Токени зазвичай діляться на дві категорії: пасивні та активні. В обох випадках токен містить базовий пароль, і потрібно скопіювати базовий пароль, щоб створити робочу копію конкретного токену. Пасивний маркер — це просто пристрій зберігання базового паролю. Приклади, які ми можемо знайти навколо нас у нашому житті, наприклад: кредитні картки, механічні ключі та спеціалізовані пристрої. Активний маркер може генерувати різні результати за різних обставин. Наприклад, активний токен може брати участь у протоколі автентифікації відповіді на виклик або надавати інші функції шифрування, які використовують базовий пароль токена. Традиційно активними маркерами були комерційні маркери одноразового пароля або смарт-картки, хоча з'явилися й інші моделі, які підключаються до існуючих портів на настільних і портативних комп'ютерах.

2.7 Технологія біометричної автентифікації

Технологія біометричної автентифікації вперше була представлена в 1970-х і на початку 1980-х років. Ця технологія збирає унікальні фізіологічні чи поведінкові

характеристики людини для зберігання в базі даних або порівняння з даними, які вже є в базі даних. Біометрія «визначається як унікальна, вимірювана біологічна характеристика або ознака для автоматичного розпізнавання або перевірки особистості людини. Статистичний аналіз цих біологічних характеристик став відомий як наука про біометрію». Сьогодні біометричні технології зазвичай використовуються для аналізу характеристик людини з метою безпеки. П’ять найпоширеніших фізичних біометричних зразків, які аналізуються з метою безпеки, — це відбитки пальців, руки, очі, обличчя та голос [13]. Існує три рівні безпеки:

- Найнижчий рівень безпеки визначається як те, що ви маєте у своєму розпорядженні, наприклад бейдж із фотографією на ньому.
- Другий рівень безпеки — це те, що ви знаєте, як-от пароль, який використовується під час входу до комп’ютера, або PIN-код для використання банківської картки в банкоматах.
- Найвищий рівень безпеки – це те, ким ви є, і те, що ви робите. Це, по суті, суть біометричних технологій.

Фізіологічна біометрія

Фізіологічна біометрія використовує алгоритми та інші методи для визначення ідентичності на основі даних, зібраних шляхом прямого вимірювання людського тіла. Відбитки пальців, геометрія руки, сканування райдужної оболонки та сітківки ока, геометрія обличчя та кровоносні судини сітківки.

Відбитки пальців

Відбитки можна сканувати оптично, але необхідні громіздкі камери. Ємнісний метод використовує різницю в електричних зарядах завитків на пальці, щоб виявити ті частини пальця, які торкаються чипа, і ті, які підняті. Дані перетворюються на граф, хребти якого представлені вершинами, а вершини, що відповідають суміжним хребтам, з’єднані. Кожна вершина має номер, який приблизно дорівнює довжині

відповідного хребта. На цьому етапі визначення збігів стає проблемою зіставлення графів. Ця проблема подібна до класичної проблеми ізоморфізму графа, але через неточність у вимірюваннях граф, створений за відбитком пальця, може мати різну кількість ребер і вершин. Таким чином, алгоритм узгодження є наближенням.

Поведінкова біометрія

Поведінкова біометрія визначається шляхом аналізу конкретної дії людини. Те, як людина розмовляє, підписує своє ім’я чи друкує на клавіатурі, є методом визначення її особи, якщо її правильно проаналізувати. Крім того, біометрію можна визначити як пасивну або активну. Пасивна біометрія не вимагає активної участі користувача і може бути успішною, навіть не знаючи, що її проаналізували. Активна біометрія вимагає співпраці з особою та не працюватиме, якщо вона заперечує свою участь у процесі. Динаміка миші — це один із видів біометрії, який можна використовувати як для активного, так і для пасивного моніторингу. Хоча біометричні технології відрізняються, усі вони працюють подібним чином: користувач надсилає зразок, який є ідентифікованим, необробленим зображенням або записом фізіологічної чи поведінкової біометрії за допомогою пристрою збору даних (наприклад, сканера чи камери). Ці біометричні дані потім обробляються для отримання інформації про відмінні риси для створення пробного шаблону або шаблону перевірки.

Голос

Автентифікація за допомогою голосу передбачає розпізнавання голосових характеристик мовця або перевірку вербальної інформації. Перший використовує статистичні методи для перевірки гіпотези про те, що ідентифікація мовця відповідає заявленим. Система спочатку навчається на фіксованих парольних фразах або фонемах, які можна комбінувати. Для автентифікації диктор або вимовляє парольну фразу, або повторює слово (або набір слів). Вербальна перевірка інформації

стосується змісту висловлювання. Система задає набір запитань на кшталт "в якому місті ви народилися?" потім він перевіряє, чи збігаються промовлені відповіді з відповідями, записаними в його базі даних. Ключова відмінність полягає в тому, що методи перевірки мовця залежать від мовця, а методи перевірки вербальної інформації не залежать від мовця, відповідаючи лише на зміст відповідей.

Око

Автентифікація за характеристиками ока використовує райдужну оболонку та сітківку. Візерунки всередині райдужної оболонки унікальні для кожної людини. Отже, один із підходів перевірки полягає в статистичному порівнянні шаблонів і запиті, чи є відмінності випадковими. Другий підхід полягає у співвіднесенні зображень за допомогою статистичних тестів, щоб побачити, чи вони збігаються. Сканування сітківки покладається на унікальність візерунків, зроблених кровоносними судинами в задній частині ока. Для цього потрібен лазерний промінь на сітківку ока, який дуже інтрузивний. Цей метод зазвичай використовується лише в приміщеннях, де потребується більший захист.

Обличчя

Розпізнавання обличчя складається з кількох кроків. Спочатку розташовується обличчя. Якщо користувач розташовує своє обличчя в заздалегідь визначеному положенні (наприклад, спираючись підборіддям на опору), проблема стає дещо легшою. Однак такі риси обличчя, як волосся та окуляри, можуть ускладнити розпізнавання. Техніки для цього включають використання нейронної мережі та шаблонів. Потім отримане зображення порівнюється з відповідним зображенням у базі даних. На кореляцію впливають відмінності в освітленні між поточним зображенням і референтним зображенням, спотворення, «шум» і вигляд обличчя. Механізм кореляції необхідно «тренувати». було використано кілька різних методів кореляції з різним ступенем успіху. Альтернативний підхід полягає в тому, щоб

зосередитися на рисах обличчя, таких як відстань між носом і підборіддям і кут лінії, проведеної від одного до іншого.

Натискання клавіш

«Динаміка натискання клавіш потребує підпису на основі інтервалів натискання клавіш, тиску натискання клавіші, тривалості натискання клавіші та місця натискання клавіші (на краю чи посередині). Цей підпис вважається унікальним так само, як унікальні письмові підписи. Розпізнавання натискань клавіш може бути як статичним, так і динамічним. Статичне розпізнавання виконується один раз, під час автентифікації, і зазвичай передбачає введення фіксованого або відомого рядка».

В таблиці 2.1 наведено короткі властивості різних типів біометрії.

Таблиця 2.1

Загальний огляд біометрії

Біометрія	Пристрій збору	Зразок	Отримана особливість
Райдужна оболонка	Інфрачервона відеокамера, камера комп’ютера	Чорно-біле зображення райдужної оболонки	Смуги райдужної оболонки
Відбиток пальця	Периферійний пристрій для настільного комп’ютера, мікросхема миші або зчитувач, вбудований у клавіатуру	Зображення відбитка пальця	Розташування та напрямок закінчень хребта та біфуркацій на відбитку пальця, дрібниці
Голос	Мікрофон, телефон	Запис голосу	Частота, каденція та тривалість вокального зразку
Підпис	Фірмовий планшет, чутливий до руху стилус	Зображення підпису та запис відповідного вимірювання динаміки	Швидкість, порядок штрихів, тиск і зовнішній вигляд підпису

Обличчя	Відеокамера, камера ПК	Зображення обличчя (оптичне або теплове)	Взаємне розташування і форма носа, положення скул
Рука	Запатентований настінний пристрій	Тривимірне зображення верхньої та бокової сторони руки	Висота і ширина кісток і суглобів рук і пальців
Сітківка	Запатентований настільний або настінний пристрій	Зображення сітківки	Схеми кровоносних судин і сітківки

2.8 Сертифікати

Сертифікат — це повідомлення, підписане третьою стороною, якій довіряють публічно. Суб'єкти, які використовують сертифікати, видані цією довіреною стороною, мають довіряти центру сертифікації. Сертифікат гарантує, що відкритий ключ прив'язаний до зазначеної сутності, і, отже, гарантія ідентифікації сертифікованої сторони є важливою вимогою для методів відкритого ключа. Серед інформації сертифікат містить: версію, серійний номер, підпис, видавець, термін дії, тему, інформацію про відкритий ключ суб'єкта, унікальний ідентифікатор видавця, унікальний ідентифікатор суб'єкта, розширення, алгоритм підпису та значення підпису.

Також автентифікація сертифіката здійснюється за допомогою методу автентифікації з відкритим ключем. Замість того, щоб клієнт надсилав лише відкритий ключ, він надсилає сертифікат, що містить відкритий ключ. Автентифікація сертифіката працює таким чином: клієнт надсилає сертифікат користувача (який містить відкритий ключ користувача) на сервер. Сервер використовує сертифікат CA для перевірки дійсності сертифіката користувача. Сервер використовує сертифікат користувача, щоб перевірити зі своїх файлів зіставлення, чи дозволено вхід чи ні. Нарешті, якщо підключення дозволено, сервер перевіряє, чи має користувач дійсний закритий ключ, використовуючи виклик. Порівняно з традиційною автентифікацією за допомогою відкритого ключа цей метод

більш безпечний, оскільки система перевіряє, чи сертифікат користувача було видано довіреним СЦ. Крім того, автентифікація за сертифікатом більш зручна, оскільки на сервері не потрібна локальна база даних відкритих ключів користувачів.

2.9 Взаємна автентифікація

Взаємна автентифікація також називається двосторонньою автентифікацією, яка складається з клієнта та сервера. Клієнт повинен підтвердити свою ідентичність серверу, а сервер підтверджує свою ідентичність клієнту перед запуском будь-якої програми. Це не передбачає взаємодії користувача ні з процесом клієнта, ні з процесом сервера. Щоб клієнт міг довіряти справжньому ланцюжку сертифікації організації чи суб'єкта, і будувати зв'язок між ними [14].

Взаємна автентифікація гарантує, що людина за клавіатурою не тільки є тим, за кого себе видає, але й доводить, що сервер, з яким він спілкується, є тим, за кого себе видає. Взаємна автентифікація захищає конфіденційність конфіденційної інформації, гарантуючи, що сервіс, з яким спілкується користувач, є справжнім.

Взаємна автентифікація часто використовується в електронному бізнесі та онлайн-банкінгу. Використовуючи взаємну автентифікацію, користувачі довіряють сертифікату суб'єкта торгівлі або об'єкта в ланцюжку сертифікатів, що означає, що користувачі довіряють органам третьої сторони. Модель взаємної автентифікації зображена на рисунку 2.4.

Рисунок 2.4 Модель взаємної автентифікації

2.10 Багатофакторна автентифікація

Багатофакторна автентифікація використовується для визначення права особи на доступ до фізичного об’єкта або на доступ до даних в інформаційній системі. Існує багато широко використовуваних методів автентифікації, але окремо кожен із них має свої обмеження або на нього може легко впливати середовище. Щоб зробити кращу та надійнішу автентифікацію, ми могли б поєднати ці методи. Наприклад, коли ви користуєтеся банкоматом, вам потрібно вставити банківську картку, а потім ввести PIN-код. Банківська картка стосується того, що у вас є, а ПІН-код, відомий лише вам, стосується того, що ви знаєте. Тоді ви зможете отримати доступ до профілю свого облікового запису та зняти гроші. За допомогою методу багатофакторної автентифікації автентифікація може стати більш надійною. «Методологія багатофакторної автентифікації також може включати 5 засобів керування для зниження ризику. Успіх конкретного методу автентифікації залежить не тільки від технології. Це також залежить від відповідної політики, процедур і засобів контролю. Ефективний метод автентифікації повинен мати прийнятність клієнта, надійну продуктивність, масштабованість для зростання та взаємодію з існуючими системами та майбутніми планами» [15].

Окремо кожен із цих підходів має свої обмеження. «Щось, що у вас є», можна вкрасти, тоді як «щось, що ви знаєте», можна здогадатися, поділитися чи забути. «Щось, що ти є» – це, як правило, найсильніший підхід, але його впровадження може бути дорогим. Щоб посилити автентифікацію, ми можемо комбінувати методи, які часто називають багатофакторною або сильною автентифікацією. Найпоширенішим типом є двофакторна автентифікація, наприклад використання PIN-коду, а також токену SecureID для входу в мережу (рисунок 2.5). Прикладом двофакторної автентифікації, з якою ми, напевно, найбільше знайомі, є наша картка банкомату: ми вставляємо картку (щось у вас) у банкомат і вводимо PIN-код (те, що ви знаєте), щоб отримати доступ до номера нашого рахунку та виконати транзакції. Ми також можемо використовувати трифакторну автентифікацію. Наприклад, якщо ми використовуємо біометричні дані для автентифікації користувачів у мережі, ми

можемо зберігати інформацію про відбитки пальців у системній базі даних, яка доступна лише за допомогою PIN-коду користувача. А без PIN-коду та сканування відбитків пальців користувач не може отримати доступ до системи.

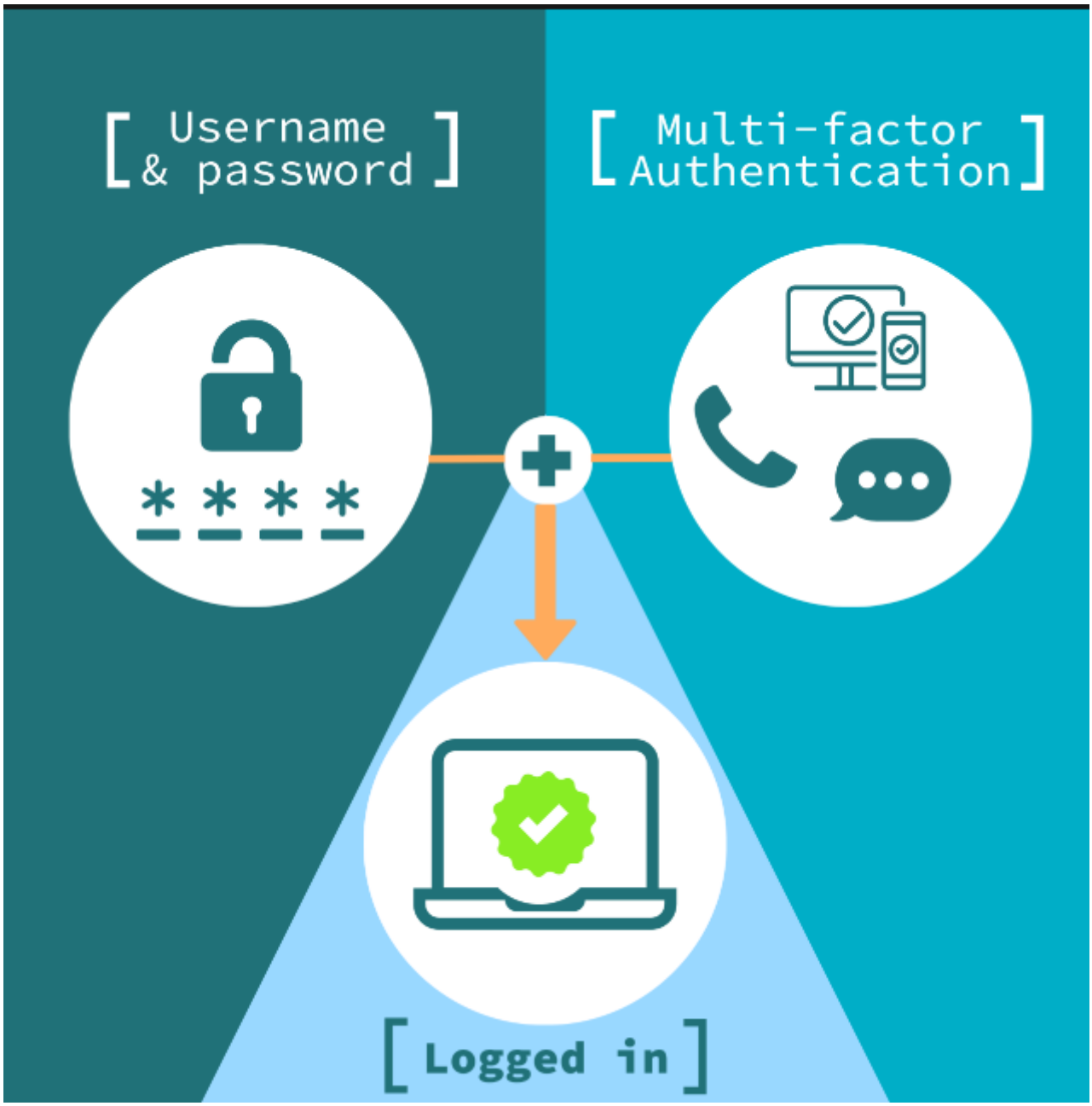

Рисунок 2.5 Загальна схема багатофакторної аутентифікації

Висновки до другого розділу

Дослідження, яке було проведено, показало, що майже всі системи використовують криптографічні алгоритми та піддаються традиційним атакам та соціальну інженерію. Однак, особливе місце серед них займає система двофакторної

автентифікації PassWindow, яка використовує штрих-коди для створення ефективного автентифікатора та більш ефективно захищається від сучасних онлайн-атак. Новий алгоритм моніторингу системи PassWindow дозволяє отримати унікальний штрих-код картки користувача після проведення 3-5 сесій передачі одноразових паролів (OTP).

Досягнення найбільшої ефективності, використання спеціального коду є ключовим механізмом. Цей підхід дозволяє уникнути передачі банківських реквізитів через Інтернет безпосередньо продавцеві. Головним перевагою є можливість змінювати цей код для кожної нової трансакції. Втім, це передбачає значні витрати для банківської установи, а також потребу в створенні окремого підрозділу для постійного супроводження та генерації цих кодів.

РОЗДІЛ 3
СТВОРЕННЯ СИСТЕМИ ПЕРЕВІРКИ ПРОЦЕСУ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ

3.1 Рекомендації до використання протоколу Kerberos

Kerberos — це протокол для автентифікації запитів на обслуговування між надійними хостами в ненадійній мережі, наприклад Інтернеті. Підтримка Kerberos вбудована в усі основні комп'ютерні операційні системи, включаючи Microsoft Windows, Apple macOS, FreeBSD і Linux.

Для забезпечення безпечного процесу автентифікації в одному домені в локальній мереж рекомендується використовувати протокол Kerberos. Протокол добре працює в локальних мережах, надійний і його майже неможливо зламати, коли облікові дані адміністратора справді заблоковані. Але Kerberos непридатний для роботи у публічному Інтернеті, оскільки він обмежений одним доменом і дуже чутливий до часу.

Система Kerberos виконує наступні заходи захисту:

- Паролі ніколи не можна передавати через мережу.
- Паролі ніколи не повинні зберігатися в клієнтських системах і завжди повинні становитися недійсними після їх використання.
- Паролі ніколи не зберігаються у вигляді відкритого тексту, навіть на серверах автентифікації.
- Пароль вводиться лише один раз за сеанс. Це рання форма автентифікації єдиного входу, і означає, що користувачі можуть автентифікувати себе лише один раз, і будуть мають доступ до будь-якої системи, для якої вони авторизовані.
- Уся інформація автентифікації зберігається на централізованому сервері автентифікації. Самі сервери додатків не зберігають жодної інформації автентифікації. Це дозволяє використовувати такі функції:

- Адміністратор може вимкнути авторизацію користувача на використання будь-якого сервера додатків із централізованого сервера автентифікації. Для відкликання авторизації не потрібен доступ до окремих серверів.
- Для доступу до всіх служб Kerberos достатньо одного пароля користувача. Користувач може скинути свій пароль лише один раз, незалежно від того, скільки служб він автентифікований для використання.
- Захист інформації користувача спрощується, оскільки вся інформація автентифікації користувача зберігається на одному централізованому сервері автентифікації, а не на всіх окремих серверах, які користувач має право використовувати.

- Усі сторони – користувачі, а також сервери додатків – повинні пройти автентифікацію, коли буде запропоновано. Під час входу користувачі проходять автентифікацію. Службам програми може знадобитися автентифікація для клієнта.
- Kerberos надає клієнтам і серверам механізм для налаштування шифрованого каналу, щоб мережеве спілкування було приватним.

Приклад систем, у яких вбудована або доступна підтримка Kerberos:

- Веб-сервіси Amazon
- Apple macOS
- Google Cloud
- Hewlett Packard Unix
- IBM Advanced Interactive eXecutive
- Microsoft Azure
- Microsoft Windows Server і AD
- Oracle Solaris
- Red Hat Linux
- FreeBSD
- OpenBSD

Протокол Kerberos був розроблений давно та оновлений багато разів, тому він вважається безпечним механізмом автентифікації користувачів. Хоч Kerberos і

використовує криптографію, він як і всі методи безпеки не є 100% стійким до атак. Протокол вразливий до атак Kerberoasting, Golden Ticket і Silver Ticket, а також атак з передачі квитка.

Kerberoasting

Kerberoasting це атака, яку використовують хакери, щоб скомпрометувати облікові дані користувачів.

Для облікових записів служби, які мають старі або слабкі паролі, Kerberoasting є потужною технікою атаки.

Оскільки в процесі автентифікації Kerberos контролер домену не відстежує, чи дійсно користувачі підключаються до служби після запиту квитка, хакери можуть запитувати сотні квитків, щоб спробувати зламати — без генерування трафіку до цільової служби, який може викликати попередження. Крім того, зловмиснику не потрібно мати облікові дані адміністратора, щоб розпочати атаку, достатньо зламати облікові дані звичайного користувача.

Підробка квитків

Автентифікація Kerberos базується на припущенні, що будь-який TGT, зашифрований за допомогою хешу пароля KRBTGT, є законним. Таким чином, будь-який зловмисник, який може створити підроблені квитки, має практично необмежену владу в домені. Ця атака називається Золотий квиток.

Щоб підробити TGT, хакерам потрібні чотири ключові відомості:

- Повне доменне ім’я (FQDN)
- Ідентифікатор безпеки домену (SID)
- Ім’я користувача облікового запису, який вони хочуть видати
- Хеш пароля KRBTGT

З усіма чотирма частинами інформації під рукою хакер може створити квиток Kerberos, щоб видати себе за будь-якого користувача AD, включно з

високопривілейованим адміністратором домену. Крім того, вони можуть зробити ці квитки дійсними скільки завгодно довго, навіть якщо це порушує налаштування політики обмеження часу організації.

Атаки на передачу квитка

Окрім підробки квитків, хакери також можуть викрасти законні квитки TGS або TGT, видані користувачеві KDS. З цими квитками в руках вони отримують доступ до IT-ресурсів так, ніби вони є цим користувачем, навіть не дізнаючись пароль користувача.

Якщо хакер зламав обліковий запис певного користувача, він може отримати TGT і всі квитки TGS для цього користувача. Але зловмисник, якому вдається викрасти адміністративні привілеї, може отримати всі квитки TGT і TGS, збережені в системі.

Для зменшення ризику атак Kerberoasting для початку можна переконатися, що облікові записи служб мають довгі паролі, які регулярно змінюються. Загальна рекомендація полягає в тому, щоб паролі мали довжину не менше 25 символів і змінювали їх кожні 30 днів. Навіть із сучасним апаратним забезпеченням і інструментами для злому паролів хакерам буде важко підібрати паролі до того, як вони будуть змінені. Треба запровадити належне управління: уважно відстежувати, які облікові записи служби є та як вони використовуються, суворо дотримуватись принципу найменших привілеїв для всіх.

Довжина пароля набагато важливіша для запобігання хакерам, ніж складність пароля. Обмежте доступ до пароля облікового запису KRBTGT і регулярно змінюйте його.

Основною стратегією захисту від атак Golden Ticket є дотримання наріжного принципу безпеки: найменші привілеї. Зводячи до мінімуму, хто має доступ до хешу пароля KRBTGT, ви обмежуєте свою вразливість до атак Golden Ticket.

Також варто зауважити, що наявність надійної стратегії аварійного відновлення Active Directory є важливою.

3.2 Процес автентифікації з використанням стандарту OpenID Connect

Майбутнім напрямком розвитку ідентифікаційних та автентифікаційних систем є створення комплексної системи, яка забезпечуватиме надійний доступ до систем для користувачів. Її функціями є:

- реєстрація користувачів в інформаційній системі;
- перевірка користувача при реєстрації;
- забезпечення актуальності даних та підтримка їх оновлень;
- надання користувачем керованого доступу до своїх даних відповідно до запитів ІКС;

Архітектура єдиної системи ідентифікації та автентифікації подана на рисунку 3.1.

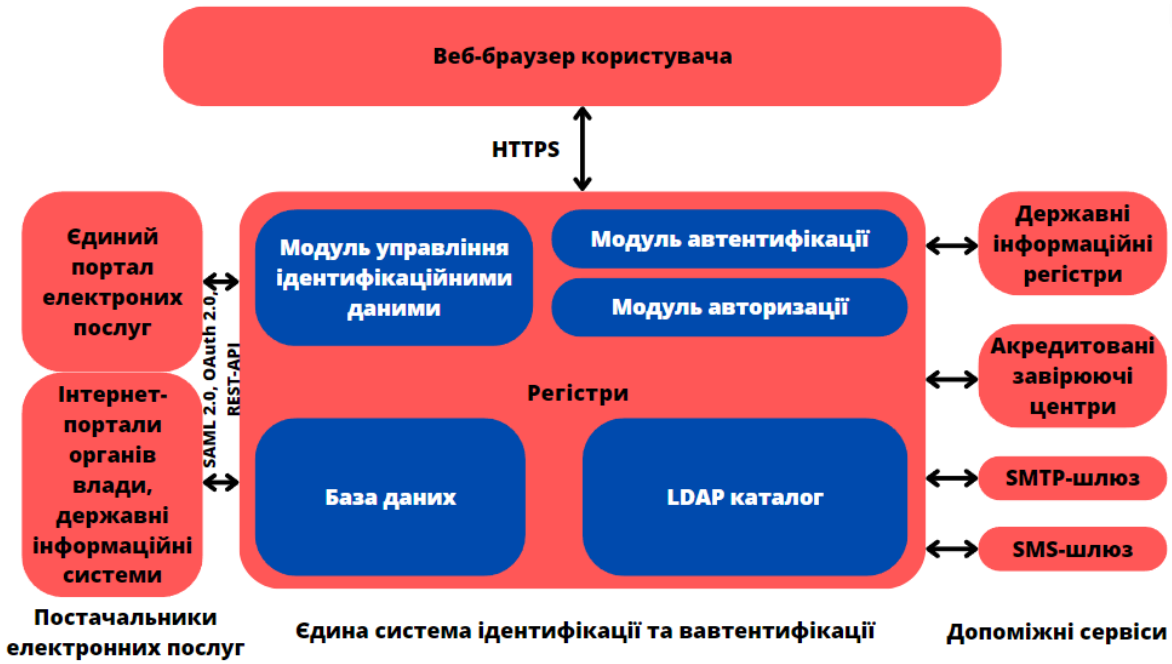

Рисунок 3.1 Архітектура ЄСІА

ЄСІА може використовувати додаткові сервіси, такі як перевірка даних користувачів, перевірка сертифікатів електронного цифрового підпису і надсилання повідомлень.

Користувачам надається можливість одноразової автентифікації, що означає, що після проходження процедури автентифікації в ЄСІА, користувач може увійти до кількох систем протягом одного сеансу роботи, не потребуючи повторного введення логіна та пароля.

Заради забезпечення функціоналу, в ЄСІА рекомендується впровадження механізму, заснованому на моделі OpenID Connect (рисунок 3.2).

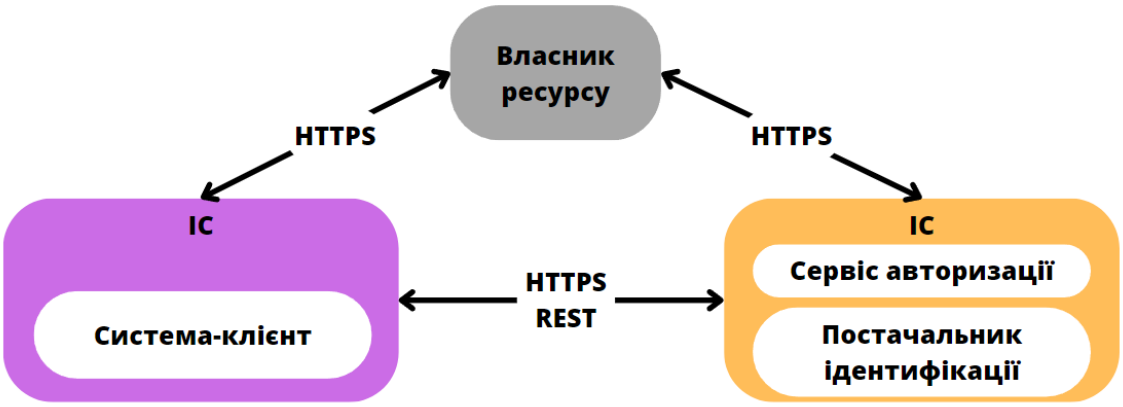

Рисунок 3.2 Схема взаємодії ІКС з ЄСІА з використанням стандарту OpenID

OpenID - це відкритий стандарт для децентралізованої системи автентифікації, який дозволяє створити єдиний обліковий запис для входу на безліч незалежних інтернет-ресурсів за допомогою послуг третіх осіб. Основною функцією OpenID є надання портативного, орієнтованого на клієнта, цифрового ідентифікатора для вільного та децентралізованого використання.

OpenID-Connect, на відміну від Kerberos, дозволяє виконувати багатодоменний єдиний вхід(MDSSO). MDSSO є набагато потужнішою технікою, ніж однодоменний єдиний вхід (SDSSO), оскільки вона дозволяє перекласти керування ідентифікацією та паролем на так званого «постачальника ідентифікаційної інформації», наприклад, Google.

OpenID-Connect, як і інші протоколи MDSSO, створено для всесвітньої мережі та найкраще працює там. Завдяки цьому стандарту користувач може використовувати один ідентифікатор для автентифікації на різних веб-ресурсах, що полегшує процес входу та забезпечує зручність та безпеку для користувача.

Процес роботи:

1. Користувач, який бажає автентифікуватися на інтернет-сервісі, починає процес шляхом введення пропонованого ідентифікатора в форму входу, яка доступна на веб-сайті;

2. За допомогою ідентифікатора, інтернет-сервіс встановлює URL-адресу OpenID провайдера, яку користувач використовує. Ідентифікатор може містити лише ідентифікатор провайдера, і в такому випадку користувач вказує свій ідентифікатор під час взаємодії з провайдером;

3. Інтернет-сервіс та OpenID провайдер створюють спільний секретний ключ для коду автентифікації. За допомогою цього ключа інтернет-сервіс може перевірити автентичність повідомлення від провайдера без необхідності додаткових запитів для перевірки автентичності;

4. У режимі "checkid_setup" інтернет-сервіс перенаправляє браузер користувача на веб-сайт провайдера для проведення процедури автентифікації. У режимі "checkid_immediate" комунікація між браузером і провайдером відбувається непомітно для користувача. В цьому режимі провайдер негайно перевіряє, чи може користувач бути автентифікованим без необхідності перенаправлення на свій веб-сайт. Якщо автентифікація можлива, інтернет-сервіс отримає підтвердження автентичності від провайдера, не роблячи видимих змін у браузері користувача;

5. Після перенаправлення на веб-сайт провайдера, провайдер перевіряє, чи є користувач авторизованим на своєму сервері. Також провайдер перевіряє, чи бажає користувач автентифікуватися на конкретному інтернет-сервісі;

6. Після успішної автентифікації провайдер перенаправляє браузер користувача назад до інтернет-сервісу. При цьому провайдер передає результати автентифікації в інтернет-сервіс;

7. Після отримання інформації від провайдера, інтернет-сервіс перевіряє її достовірність. Якщо на кроці 3 був створений спільний секретний ключ, перевірка виконується з його використанням. У випадку, коли ключ не був створений, інтернет-сервіс надсилає додатковий запит провайдеру (check_authentication). В першому випадку інтернет-сервіс називається залежною стороною без пам'яті (stateless), а в другому - німий (dumb).

8. Після успішної перевірки інформації, інтернет-сервіс підтверджує автентифікацію користувача.

ЄСІА дозволяє проводити автентифікацію користувача як представника організації. Для цього ІКС повинна:

- запросити від ЄСІА не лише ідентифікаційний токен, але й токен доступу (для отримання даних користувача);
- за допомогою маркера доступу та REST-інтерфейсу ЄСІА, звернутися до системи та отримати інформацію про працівника організації.

Система ЄСІА має можливість надавати інформацію системі-клієнту, що дозволяє проводити авторизацію автентифікованого користувача. Система, до якої користувач намагається отримати доступ, самостійно вирішує, чи має він авторизацію. Для отримання авторизаційних даних рекомендується використовувати програмний інтерфейс. У такому випадку система може запитати в користувача маркер доступу, щоб отримати необхідні авторизаційні дані. Після отримання маркера доступу система може отримати інформацію про користувача і, на основі цих даних, вирішити, чи надати користувачеві доступ до своїх ресурсів. Загальна схема реєстрації користувача зображена на рисунку 3.3.

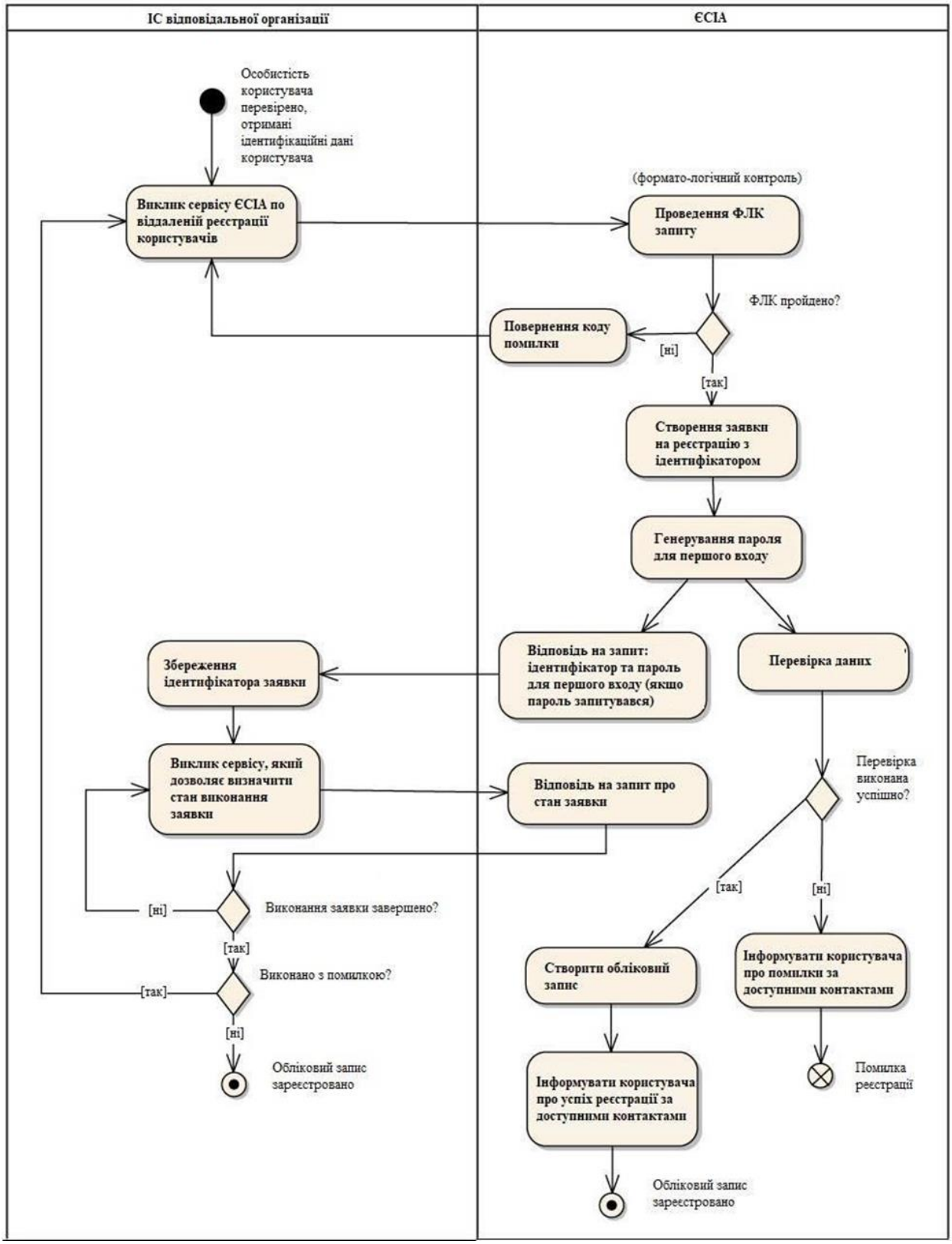

Рисунок 3.3 Схема реєстрації користувача

3.3 Процес багатофакторної автентифікації на трансакційному ідентифікаційному коді та службі коротких повідомлень

Для створення додаткового рівня безпеки у багатофакторній автентифікаційній системі використовуються трансакційні ідентифікаційні коди (TIC) та служба коротких повідомлень (SMS). TIC-коди подібні до одноразових паролів (OTP), але забезпечують ще більшу надійність. Вони служать для підтвердження того, що поточна трансакція, пов'язана з банківською карткою, зроблена самим власником рахунку, а не шахрайськими особами. TIC-коди генеруються банком як псевдовипадкові послідовності цифр або буквено-цифрових символів. Кожна трансакція вимагає унікального коду, який може бути використаний лише один раз. Механізм генерації кодів є суворим і контролюється банком. Крім того, банк зберігає номер телефону клієнта, щоб надсилати SMS-повідомлення для підтвердження трансакції. Цей додатковий етап підтвердження захищає власника рахунку від несанкціонованих трансакцій та допомагає уникнути фінансових шахрайств.

Багатофакторна автентифікація використовується для перевірки ідентичності покупця та автентифікації транзакцій, дотримуючись наступних етапів:

1. Початкова автентифікація: Логін на веб-сервер користувача за допомогою його унікального імені та пароля для здійснення початкової перевірки.
2. TIC-перевірка: Після успішної початкової автентифікації користувача, веб-сервер звертається до нього для введення TIC як другого рівня перевірки.
3. Підтвердження за допомогою SMS: Після успішної TIC-перевірки, третім рівнем автентифікації є підтвердження через SMS. Користувач отримує текстове повідомлення з деталями транзакції, які необхідні для ідентифікації та перевірки особи, що ініціює транзакцію.

Механізм багатофакторної автентифікації включає такі етапи:

1. Клієнт отримує свої логін та пароль від свого банку під час відкриття рахунку або реєстрації в цьому банку.

2. Покупець заходить на веб-сервер свого банку за допомогою GPRS-з'єднання, використовуючи свій логін та пароль. Ця перша автентифікація призначена для ідентифікації покупця веб-сервером.

3. Після успішної першої автентифікації покупець отримує можливість розпочати транзакцію з вхідним повідомленням та ідентифікатором сесії.

4. Покупець обирає спосіб оплати, наприклад, кредитною карткою, дебетною карткою або електронним переказом. У випадку оплати карткою протокол вимагає введення дійсних реквізитів платіжного засобу.

5. Покупець вводить деталі платежу, такі як суму та отримувача платежу.

6. Для здійснення транзакції клієнт повинен мати доступ до ТІС. Варто зазначити, що ТІС захищений паролем на мобільному телефоні, і цей пароль буде розшифрований за допомогою одного з шифрів ТІС перед використанням у транзакції.

7. Усі трансакційні записи разом з ТІС будуть зашифровані та передані на сервер для подальшої обробки.

8. Сервер автентифікації банку розшифровує отриману інформацію про транзакцію та вилучає ТІС. Сервер перевіряє отриманий від покупця код, порівнюючи його з кодом, який збережений разом з інформацією про рахунок клієнта, а також з вибраним кодом з бази даних сервера. Якщо обидва коди збігаються, використаний код автоматично видаляється з бази даних. У разі, якщо коди не збігаються, автентифікаційний сервер скасовує будь-які подальші транзакції клієнта та надсилає повідомлення про помилку.

9. Якщо автентифікація ТІС пройшла успішно, авторизаційний сервер генерує текстове повідомлення та надсилає його до SMS-шлюзу/адаптера для передачі через мобільну мережу.

10. Покупець підтверджує транзакцію, за допомогою SMS.

Механізм багатофакторної автентифікації зображен на рисунку 3.4.

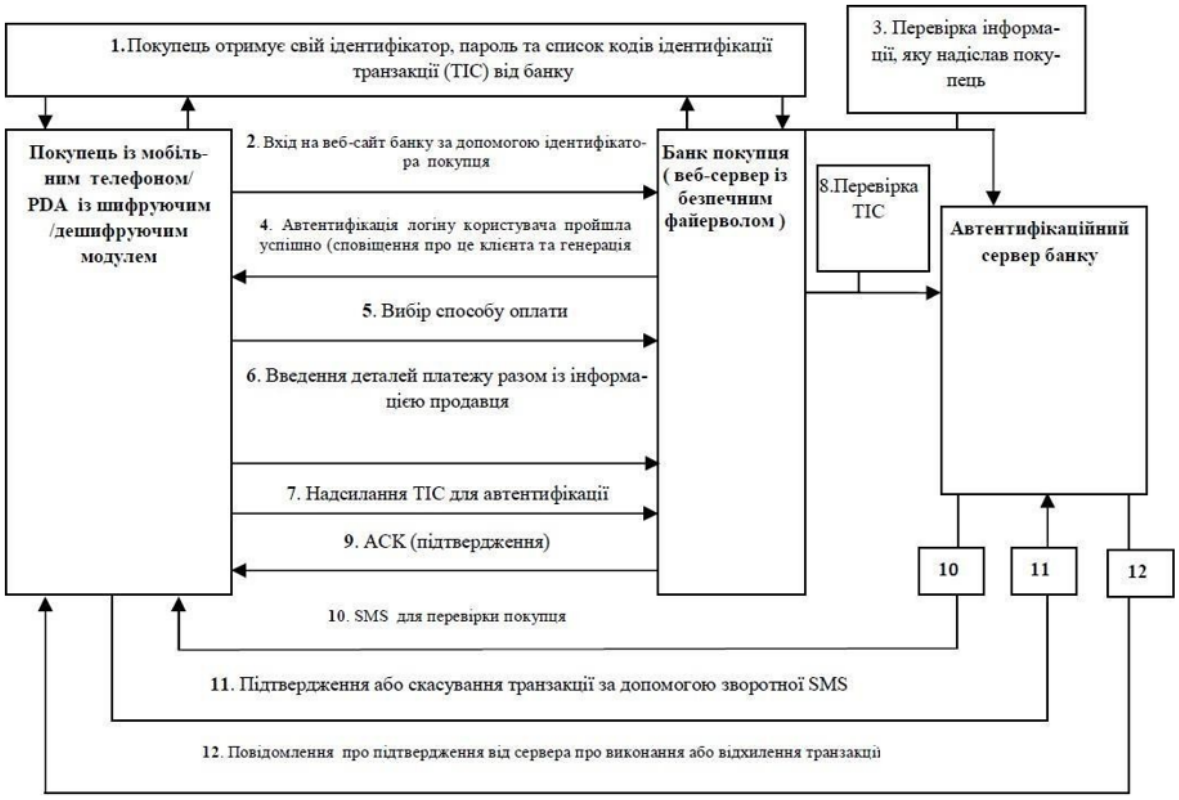

Рисунок 3.4 Схема протоколу багатофакторної автентифікації

ТІС-коди є найбільш вразливою інформацією, яка зберігається на мобільних телефонах або КПК. Щоб забезпечити їх безпеку, вони знаходяться в зашифрованому форматі та захищені паролем(рисунок 3.5). Користувач вводить локальний пароль для отримання доступу до списку ТІС-кодів і обирає потрібний код для початку трансакції. При цьому обраний код автоматично розшифровується та відображається на екрані користувача. Також цей обраний код переміщується зі списку в середовище клієнта. Локальний пароль виступає як ключ для розшифрування ТІС-коду і відомий тільки клієнту.

Рисунок 3.5 Шифрування ТІС коду

Висновки до третього розділу

Автентифікація означає перевірку ідентичності особи або програмного процесу. Цей процес використовує різні типи інформації, яка може бути представлена у різних формах. Починаючи з паролю, електронного ключа, закінчуючи смарт-картками та різними біометричними характеристиками людини.

Автентифікація в сучасному цифровому світі відіграє вирішальну роль у забезпеченні безпеки та захисту інформації. Вона є необхідною для перевірки і підтвердження ідентичності користувачів, щоб гарантувати, що доступ до системи або конкретних ресурсів отримують лише вповноважені особи. Автентифікація дозволяє перевірити, що користувач є тим, за кого він себе видає, та перешкоджає несанкціонованому доступу та зловживанню інформацією. Захист від кібератак і порушень безпеки значно підвищується завдяки використанню сучасних методів автентифікації, таких як біометричні дані або мультифакторна автентифікація.

При виборі методу автентифікації необхідно враховувати різні фактори, такі як вартість і цінність інформації, продуктивність системи. Вартість, якість і надійність засобів автентифікації повинні бути пропорційними важливості інформації. Крім того, підвищення продуктивності і надійності комплексу, зазвичай, вимагає додаткових витрат.

ВИСНОВКИ

Основними цілями забезпечення безпеки інформації в комп'ютерних системах є збереження конфіденційності, доступності та цілісності даних, а також забезпечення автентифікації та керування доступом. Автентифікація дозволяє перевірити, що особа, яка намагається отримати доступ, є тим, за кого вона себе видає. Зазвичай для підтвердження особи користувача використовуються паролі. Сучасні методи автентифікації дозволяють уникнути передачі пароля в незашифрованому вигляді.

Авторизація визначає права та дії, які авторизований користувач може здійснювати з об'єктами у системі. Цей процес базується на списку контролю доступу, пов'язаному з об'єктами, і списку дозволених дій, пов'язаних з окремими користувачами.

Для забезпечення надійної інформаційної безпеки користувачів під час процесу автентифікації в незахищених середовищах та мережах використовуються різноманітні технології безпеки, такі як біометрична автентифікація, автентифікація за допомогою токенів, протокол Kerberos.

Використання нових технологій та підходів, таких як біометрична автентифікація, мультифакторна автентифікація, автентифікація на основі поведінки будуть забезпечувати більш високий рівень безпеки та захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shacklett M. What is authentication? [Електронний ресурс] / Mary E. Shacklett // techtarget.com – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/authentication.

2. Yan J. Continuous authentication based on computer security [Електронний ресурс] / Jing Yan // Lulea University of Technology. – 2008. – Режим доступу до ресурсу: http://www.diva-portal.org/smash/get/diva2:1025705/FULLTEXT01.pdf.

3. A Review on Authentication Methods [Електронний ресурс] / S.Zulkarnain Syed Idrus, E. Cherrier, C. Rosenberger, J. Schwartzmann // researchgate.net. – 2013. – Режим доступу до ресурсу: https://www.researchgate.net/publication/281109747_A_Review_on_Authentication_Methods.

4. Belhadj F. Biometric system for identification and authentication [Електронний ресурс] / Foudil Belhadj // researchgate.net. – 2017. – Режим доступу до ресурсу: https://www.researchgate.net/publication/313614446_Biometric_system_for_identification_and_authentication.

5. An evaluation of hypothetical attacks against the PassWindow authentication method [Електронний ресурс] / M.Slyman, S. O'Neil, G. Horatiu Nicolae, B. van der Merwe // passwindow.com – Режим доступу до ресурсу: https://www.passwindow.com/evaluation_of_hypothetical_attacks_against_passwindow.pdf.

6. Schneier B. Hacking Two-Factor Authentication [Електронний ресурс] / Bruce Schneier // Schneier on Security. – 2009. – Режим доступу до ресурсу: https://www.schneier.com/blog/archives/2009/09/hacking_two-fac.html.

7. Assaad F. Transformation based Score Fusion Algorithm for Multi-modal Biometric User Authentication through Ensemble Classification [Електронний ресурс] / F. Assaad, G. Serpen // researchgate.net. – 2015. – Режим доступу до ресурсу:

https://www.researchgate.net/publication/283155701_Transformation_based_Score_Fusion_Algorithm_for_Multi-modal_Biometric_User_Authentication_through_Ensemble_Classification.

8. Brocardo M. Toward a Framework for Continuous Authentication Using Stylometry [Електронний ресурс] / M. Brocardo, I. Traore, I. Woungang // researchgate.net. – 2013. – Режим доступу до ресурсу: https://www.researchgate.net/publication/264043677_Toward_a_Framework_for_Continuous_Authentication_Using_Stylometry.

9. Understanding smart card authentication [Електронний ресурс] // access.redhat.com – Режим доступу до ресурсу: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/managing_smart_card_authentication/assembly_understanding-smart-card-authentication_managing-smart-card-authentication.

10. Leduc G. Verification of two versions of the Challenge Handshake Authentication Protocol (CHAP) [Електронний ресурс] / Guy Leduc // researchgate.net. – 2000. – Режим доступу до ресурсу: https://www.researchgate.net/publication/2542176_Verification_of_two_versions_of_the_Challenge_Handshake_Authentication_Protocol_CHAP.

11. Loshi P. Kerberos Overview [Електронний ресурс] / Peter Loshi // techtarget.com – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/Kerberos.

12. Authentication Token [Електронний ресурс] // fortinet.com – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/authentication-token

13. Julien B. Anonymous identification with cancelable biometrics [Електронний ресурс] / B. Julien, H. Chabanne, B. Kindarji // researchgate.net. – 2009. – Режим доступу до ресурсу: https://www.researchgate.net/publication/224607996_Anonymous_identification_with_cancelable_biometrics.

14. Lars Skaar Kulseng. Lightweight mutual authentication [Електронний ресурс] / Lars Skaar Kulseng // Iowa State University. – 2009. – Режим доступу до ресурсу: https://core.ac.uk/download/pdf/38925024.pdf.

15. Markus Fält. Multi-factor Authentication [Електронний ресурс] / Markus Fält. – 2020. – Режим доступу до ресурсу: https://www.diva-portal.org/smash/get/diva2:1442569/FULLTEXT01.pdf.

16. Smart cards and the fingerprint: A framework for user identification and authentication [Електронний ресурс] // Journal of Information and Communication Technology (JICT). – 2003. – Режим доступу до ресурсу: https://myjurnal.mohe.gov.my/public/article-view.php?id=4472.

17. A New Smart Cards Based Model for Securing Services [Електронний ресурс] // Journal of Computer Science IJCSIS. – 2019. – Режим доступу до ресурсу: https://www.academia.edu/38372087/A_New_Smart_Cards_Based_Model_for_Securing_Services.

18. Закон України "Про електронні довірчі послуги" [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2155-19/ed20171005#n9.

19. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу [Електронний ресурс]. – 2003. – Режим доступу до ресурсу: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi.

20. Rafi M. Multifactor authentication: biometric methods used to secure information systems [Електронний ресурс] / Mohammed Rafi // academia.edu. – 2014. – Режим доступу до ресурсу: https://www.academia.edu/13447896/MULTIFACTOR_AUTHENTICATION_BIOMETRIC_METHODS_USED_TO_SECURE_INFORMATION_SYSTEMS.

21. THE STUDY OF DIGITAL SIGNATURE AUTHENTICATION PROCESS [Електронний ресурс] / I.Patel, U. Patel, A. Patel, F. Suthar // researchgate.net. – 2019. – Режим доступу до ресурсу: https://www.researchgate.net/publication/336603564_THE_STUDY_OF_DIGITAL_SIGNATURE_AUTHENTICATION_PROCESS.