

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ**

КВАЛІФІКАЦІЙНА РОБОТА
на тему:

«Система багатофакторної автентифікації користувача при захищеному доступі
до конфіденційної інформації»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

*Кваліфікаційна робота містить результати власних досліджень.
Використання ідей, результатів і текстів інших авторів мають посилання на
відповідне джерело*

_____ Назар АНДРІЄНКО

Виконав: здобувач вищої освіти групи СЗДМ 61
Назар АНДРІЄНКО

Керівник: _____
к.т.н., доцент (ПРИЗВИЩЕ, Ім'я) КОТЕНКО Андрій

Рецензент: _____
(ПРИЗВИЩЕ, Ім'я)

Київ 2026

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

Кафедра Технічних систем кіберзахисту
 Ступінь вищої освіти магістр
 Спеціальність Кібербезпека та захист інформації
 Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ

Завідувач кафедри ТСК

Олександр Туровський

« » 2025 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Андрієнку Назару Андрійовичу

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:

«Система багатофакторної автентифікації користувача при захищеному доступі до конфіденційної інформації»

керівник кваліфікаційної роботи

Андрій КОТЕНКО **к.т.н., доцент**

(ПРИЗВИЩЕ Ім'я, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи

15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: об'єкти інформаційної діяльності, канали витоку інформації з обмеженим доступом на об'єкті інформаційної діяльності, методи, способи та механізми ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

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

4.1. Захист інформації на об'єктах інформаційної діяльності.

4.2. Огляд методів і засобів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

4.3. Розробка та вдосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах.

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____

(підпис)

Назар АНДРІЄНКО _____

(Ім'я, ПРИЗВИЩЕ)

Керівник роботи _____

(підпис)

Андрій КОТЕНКО _____

(Ім'я, ПРИЗВИЩЕ)

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 72 сторінок, має 19 рисунків, 5 таблиць. Список використаних джерел містить 31 найменування і займає 4 сторінки.

Метою кваліфікаційної роботи є удосконалення механізмів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

В кваліфікаційній роботі визначено порядок розподілу інформації, проведено аналіз загроз інформаційній безпеці та аналіз технічних каналів витоку інформації на об'єкті інформаційної діяльності. Проведено огляд методів і засобів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом. Досліджено шляхи, розроблено та вдосконалення механізми багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

Апробація:

Н.А. Андрієнко, І.С. Волковецький, Є. О. Васін. Принципи та методи застосування системи багатофакторної автентифікації для запобігання витоку конфіденційних даних на об'єкті інформаційної діяльності. *Всеукраїнської науково-практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.29-30. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ПАРОЛЬ, QR-КОД, БІОМЕТРИЧНІ ДАННІ, ІДЕНТИФІКАЦІЇ, АВТЕНТИФІКАЦІЯ.

ABSTRACT

The qualification work consists of an introduction, three sections, general conclusions, a list of sources used, the total volume of the work is 69 pages, has 19 figures, 5 tables. The list of sources used contains 31 names and takes up 4 pages.

The purpose of the qualification work is to improve the mechanisms for identifying and authenticating users when accessing information with limited access.

The qualification work defines the procedure for distributing information, analyzes threats to information security and analyzes technical channels for information leakage at the object of information activity. A review of methods and means of identifying and authenticating users when accessing information with limited access is conducted. Ways have been studied, developed and improved mechanisms for multi-factor identification and authentication of users when accessing information with limited access.

Approbation:

N.A. Andrienko, I.S. Volkovetsky. Principles and methods of applying a multi-factor authentication system to prevent the leakage of confidential data at the object of information activity. All-Ukrainian scientific and practical conference: Current problems of information and telecommunication systems security. Kyiv, November 5, 2025, Kyiv: DUKT Research and Development Center. – 2025. P.29-30.
https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Keywords: INFORMATION PROTECTION SYSTEMS, OBJECT OF INFORMATION ACTIVITY, PASSWORD, QR-CODE, BIOMETRIC DATA, IDENTIFICATION, AUTHENTICATION.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ	..8
ВСТУП.....	..9
РОЗДІЛ 1 ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ	10
1.1. Аналіз загроз інформаційній безпеці на об'єкті інформаційної діяльності	10
1.2. Аналіз каналів витоку інформації на об'єкті інформаційної діяльності	11
1.3 Висновки по розділу.....	15
РОЗДІЛ 2 ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ	16
2.1 Процес ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах	16
2.2 Класифікація та характеристики методів ідентифікації та автентифікації користувача	18
2.3 Вимоги та порядок організації процесів ідентифікації та автентифікації	38
2.3 Висновки по розділу	44

РОЗДІЛ 3 РОЗРОБКА МЕХАНІЗМІВ БАГАТОФАКТОРНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ	45
3.1 Зміст, характеристики та вимоги до механізму ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах	45
3.2 Моделі оцінки захищеності механізмів багатофакторної автентифікації користувачів від несанкціонованого доступу	51
3.3 Висновки по розділу	55
ВИСНОВКИ.....	56
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	58
ДОДАТОК	62

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ОІД	Об'єкт інформаційної діяльності
ІзОД	Інформація з обмеженим доступом
ТЗІ	Технічний захист інформації
ТКВІ	Технічні канали витоку інформації
ОТЗС	Об'єкт технічного захисту систем
ТЗО	Технічні засоби охорони
ТСО	Технічна система охорони
ТЗОС	Технічні засоби охоронної сигналізації
ІКМ	Інформаційно-комунікаційна мережа

ВСТУП

На сучасному етапі розвитку суспільства, однією з найактуальніших проблем, яка є не тільки в Україні, а й в світі, полягає в захисту інформації на об'єктах інформаційної діяльності. Одним з аспектів вирішення вказаного питання є організація та здійснення багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

Це, в свою чергу, вимагає проведення відповідних досліджень та на їх основі удосконалення методів та механізмів вказаної багатофакторної ідентифікації та автентифікації користувачів.

Метою кваліфікаційної роботи удосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

- Визначено порядок розподілу інформації на об'єкті інформаційної діяльності, проведено аналіз загроз інформаційній безпеці та аналіз технічних каналів витоку інформації на об'єкті інформаційної діяльності.

- Проведено методів і засобів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

- Розроблено та вдосконалено механізми ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

Об'єкт дослідження. Процес ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

Предмет дослідження. Механізми ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

РОЗДІЛ 1

ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

1.1 Аналіз загроз інформаційній безпеці на об'єкті інформаційної діяльності

Захист інформації є найважливішою частиною комплексних заходів технічного захисту інформації (ТЗІ). Зловмисники можуть перехоплювати інформацію, отримувати до неї доступ без дозволу та використовувати її для інших цілей [1,5,6].

Для незаконного викрадення інформації використовуються різні технічні засоби. Інформація передається від об'єктів до зловмисників через різні фізичні канали [6,7].

Виходячи з фізичних характеристик джерела інформаційного сигналу, середовища поширення та методів перехоплення, канали витоку технічної інформації можна класифікувати на такі категорії [7,8]:

- Радіоканали;
- Електричні канали;
- Акустичні канали;
- Оптичні канали;
- Матеріальні канали [7].

Аналіз фізичних характеристик численних джерел сигналів показує [6,7]:

- Джерела небезпечних сигналів включають компоненти, вузли та провідники виробничого та охоронного обладнання, а також радіо- та електронне обладнання;

- За певних умов кожне джерело небезпечного сигналу може утворювати канал витоку технічної інформації;

- Кожна електронна система, що містить компоненти, вузли та провідники, має кілька каналів витоку технічної інформації. Причини витоку радіоінформації включають:

- Мікрофонний ефект;
- Магнітне поле;
- Паразитний ефект;
- Уздовж кола живлення;
- Уздовж кола заземлення;
- Взаємний вплив;
- Електромагнітне випромінювання;
- Радіочастотні перешкоди;
- Від волоконно-оптичних систем зв'язку.

Структура каналу витоку технічної інформації зазвичай включає (Рисунок 1.2): джерело або передавач сигналу, середовище поширення струму або електромагнітних хвиль та приймач сигналу [7].

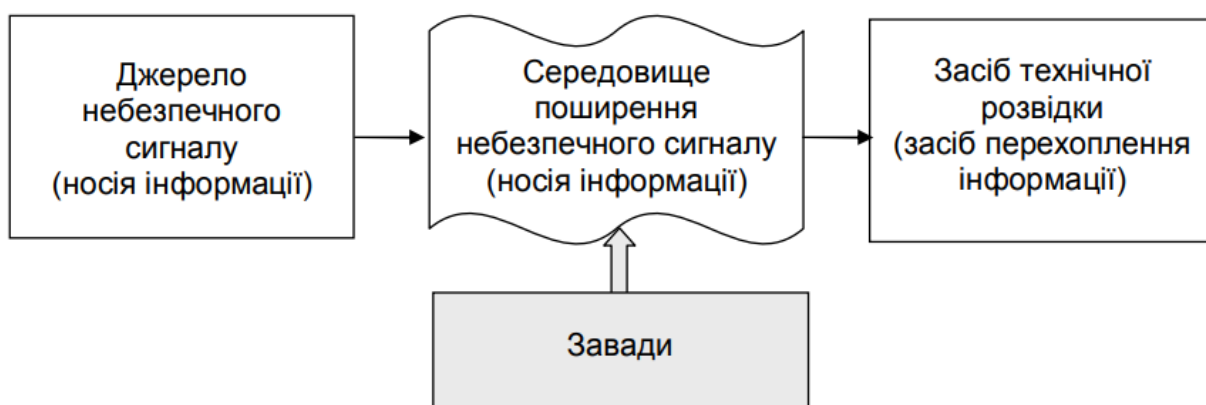


Рис. 1.2 Структура технічного каналу витоку інформації

1.2 Аналіз каналів витоку інформації на об'єкті інформаційної діяльності

Для визначення вимог до каналів технологій витоку інформації та організації захисту інформації ці канали були класифіковані за певними характеристиками.

Зокрема, види витоку технічної інформації розрізняються за такими характеристиками [6,7]:

- На основі типу інформаційної активності на ОІД;
- На основі принципу (фізичного ефекту, процесу) формування сигналу небезпеки (носія інформації);
- На основі середовища поширення сигналу небезпеки;
- На основі методу, за допомогою якого технічна розвідка противника перехоплює (ліквідує) сигнал небезпеки.

Виходячи з типу інформаційної активності на ОІД, витік технічної інформації можна розділити на такі типи:

- Технічні канали витоку голосової інформації;
- Технічні канали витоку інформації, що обробляється в ОТЗС;
- Технічні канали витоку візуальної інформації;
- Канали витоку матеріальної інформації.

Рекомендується класифікувати ТКВІ за вищезазначеними типами ТКВІ на основі принципу (фізичного ефекту, процесу) формування сигналу небезпеки, середовища поширення сигналу небезпеки та методу, за допомогою якого технічна розвідка противника перехоплює (ліквідує) сигнал небезпеки.

Виходячи з цих характеристик, технічні канали витоку голосової інформації можна класифікувати наступним чином [7,8]:

- Акустичні канали.
- Вібраційні (вібраційні акустичні) канали.
- Акустооптичні (лазерні акустичні) канали.
- Електроакустичні канали.
- Аудіовізуальні канали.

- Канали радіочастотних перешкод (використовуються для ліквідації голосової інформації).

- Канали витоку голосової інформації на основі вбудованих пристроїв.

Технічні канали витоку інформації, що обробляються ОТЗС, можна класифікувати наступним чином [7,8]:

- Канали бічного електромагнітного випромінювання.
- Канали бічних електромагнітних перешкод.
- Канали паразитної модуляції радіочастотних сигналів генератора.
- Канали паразитної генерації радіочастот підсилювачів.
- Канали перехоплення (видалення) інформації з волоконно-оптичних ліній передачі даних.
- Канали перехоплення (видалення) інформації з каналів зв'язку.
- Канали радіочастотних перешкод (використовуються для видалення інформації, обробленої ОТЗС).
- Канали витоку інформації обробки ОТЗС на основі вбудованих пристроїв.

Технічні канали витоку візуальної інформації можна класифікувати наступним чином [7,8]:

- Візуальні канали.
- Оптичні візуальні канали.
- Канали витоку візуальної інформації на основі вбудованих пристроїв.

Матеріальні канали витоку інформації [7,8,9,10]:

- Вилучення інформації з магнітних властивостей або інших носіїв інформації несправних пристроїв ЕОТ.
- Вилучення інформації з чернеток документів, виробництва, публікацій, офісних відходів тощо.
- Хімічні канали.
- Виходячи з носія інформації та принципу формування сигналу небезпеки, можна виділити такі ТКВІ [7,8]:

1. Канали витоку електромагнітної інформації, включаючи канали бічного електромагнітного випромінювання, канали генерації високої частоти "паразитного" підсилювача, канали модуляції високочастотного генератора "паразитного" типу та канали перехоплення інформації ліній радіозв'язку (радіорелейного, стільникового, мобільного) тощо;

2. Канали витоку інформації електричних сигналів, включаючи канали електромагнітних перешкод для зв'язку та канали вилучення інформації з дротових ліній зв'язку;

3. Канали витоку інформації за параметрами, включаючи канали радіочастотних перешкод та канали "паразитної" модуляції.

Залежно від місця перехоплення інформації технічною розвідкою противника, можна виділити такі типи каналів витоку технічної інформації [7,8,9,10]:

- Канали перехоплення (видалення) інформації поза зоною контакту;
- Канали перехоплення (видалення) інформації поза зоною контакту, але які позитивно впливають на параметри каналу витоку технічної інформації (наприклад, канали радіочастотних перешкод);
- Канали вилучення інформації через засоби технічної розвідки, встановлені на цільових пристроях (OID) (наприклад, канали витоку інформації вбудованих пристроїв).

Наведена вище класифікація каналів витоку технічної інформації допомагає нам систематично зрозуміти їх та сформулювати відповідні вимоги та заходи захисту каналів витоку технічної інформації.

1.3 Висновок цього розділу

1. У цьому розділі описано процедуру розповсюдження інформації об'єктів інформаційної діяльності, визначено класифікацію інформації за змістом та порядком доступу, а також описано методи та схеми доступу до інформації. У цьому розділі також визначено обсяг захищеної інформації та наведено стандарти інформаційної безпеки.

2. У цьому розділі проаналізовано канали витоку технічної інформації та наведено їх класифікацію. Класифікація базується на типі інформаційної діяльності, принципах формування сигналів небезпеки, середовищі, через яке поширюються сигнали небезпеки, та методах перехоплення (або ліквідації) сигналів небезпеки за допомогою технічної розвідки противника.

РОЗДІЛ 2

ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

2.1 Процес ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах

З популяризацією комп'ютерних технологій питання захисту інформації для об'єктів інформаційної діяльності в інформаційно-комунікаційних мережах (ІКМ) стає все більш актуальним.

Тому теоретична розробка захисту комп'ютерної інформації та його практичне застосування в конкретних комп'ютерних системах мають велике значення. Захист інформації комп'ютерних систем має на меті запобігти несанкціонованій поведінці управління та доступу до захищених комп'ютерних даних третіх осіб або програм, тим самим забезпечуючи безпеку нормально працюючих інформаційних систем. Побудова єдиної централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури [1,2,3].

Контроль доступу є ефективним методом захисту інформації; він регулює використання ресурсів інформаційної системи, і на цьому базується концепція інформаційної безпеки (ІБ). Методи та системи захисту інформації, засновані на контролі доступу, включають такі функції захисту інформації в інформаційних системах (ІС) [8,9,10,11]:

- Ідентифікація користувачів, ресурсів та персоналу в інформаційній системі;

- Ідентифікація та перевірка особи користувача на основі введених облікових даних (більшість моделей інформаційних систем базуються на цьому принципі);
- Дозвіл доступу до певних умов роботи відповідно до правил, встановлених для кожного користувача. Ці правила, визначені заходами захисту інформації, складають основу інформаційної безпеки в більшості типових моделей інформаційних систем;
- Реєстрація доступу користувачів до ресурсів. Інформаційна система використовує ці журнали для захисту ресурсів від вразливостей мережевої безпеки (NSDs) та для моніторингу неналежної поведінки користувачів.

Тому системи розпізнавання та автентифікації особи є одним з ключових елементів інфраструктури для захисту будь-якої інформаційно-комунікаційної системи від несанкціонованого доступу (AAA). Несанкціонований доступ означає доступ до інформації за допомогою стандартного комп'ютерного обладнання або автоматизованих систем з порушенням встановлених правил обмеження доступу.

Несанкціонований доступ може бути випадковим або навмисним.

Завданням систем розпізнавання та автентифікації особи є визначення та перевірка дозволів, якими володіє суб'єкт під час доступу до інформаційної системи. Перевірка особи дозволяє суб'єкту (користувачеві, процесу, що працює від імені певного користувача, або іншим апаратним та програмним компонентам) ідентифікувати себе (повідомити своє ім'я).

Перевірка особи означає відображення користувачем свого унікального ідентифікатора (символу). Завдяки автентифікації інша сторона може бути впевнена, що суб'єкт дійсно є тим, за кого він себе видає. Термін «автентифікація» іноді є синонімом «перевірки особи» [7,11].

Автентифікація – це процес перевірки того, чи має користувач право доступу до ресурсів на основі наданої ідентифікаційної особи. Розпізнавання

ідентифікаційної особи та автентифікація нероздільні, оскільки метод автентифікації визначає, яку інформацію користувач повинен надати системі, щоб отримати доступ [7,11].

Сьогодні в інформаційно-комунікаційних системах існують різні технології розпізнавання та автентифікації ідентифікаційних осіб користувачів (рис. 2.1) [7,8,12,13].

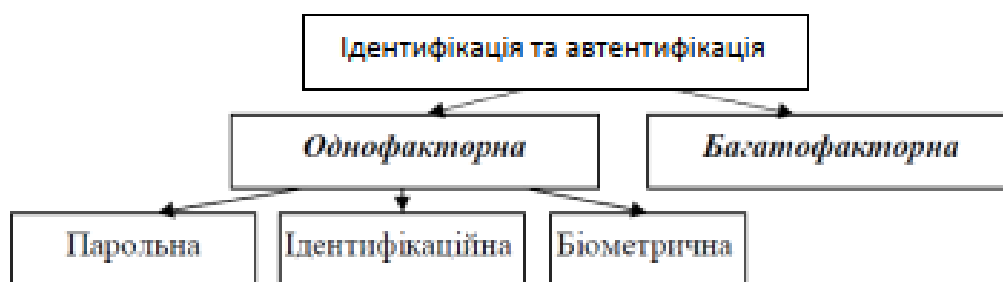


Рис.2.1. Система технологій ідентифікації та автентифікації

Кожен метод має свої переваги та недоліки, тому деякі методи підходять для певних комп'ютерних систем, а інші - для інших. Однак у багатьох випадках не існує чітко визначеного рішення. Тому розробники програмного забезпечення та користувачі повинні самостійно вирішувати, який метод перевірки ідентичності впроваджувати у своїх промислових системах керування (ІКС).

2.2 Класифікація та характеристики методів ідентифікації та автентифікації користувача

Перевірка та автентифікація пароля

В останні роки перевірка та автентифікація пароля стали майже єдиним методом визначення ідентичності користувача. Це не дивно. Насправді, перевірка пароля є найпростішою як у реалізації, так і у використанні [7,14].

Її суть полягає в наступному: кожен зареєстрований користувач певної системи отримує набір персональної інформації (зазвичай пару ім'я користувача-пароль).

Потім, кожного разу, коли користувач входить у систему, він повинен вводити свою інформацію. Оскільки пароль кожного користувача унікальний, система робить висновок та ідентифікує користувача на основі цього.

За умови правильного використання паролі можуть забезпечити прийнятний рівень безпеки для багатьох організацій. Однак, враховуючи всі свої характеристики, паролі слід вважати найслабшим засобом перевірки ідентичності. Слабкий захист паролем є однією з основних причин, чому комп'ютерні системи вразливі до атак несанкціонованого доступу. Однак наразі символічні паролі залишаються найпоширенішим методом ідентифікації та перевірки особистості користувачів, і це, ймовірно, триватиме ще довго.

Наступні заходи значно покращать надійність захисту паролем [7,14]:

- Встановлення технічних обмежень: встановлення мінімальної довжини пароля та використання різних комбінацій символів у паролі (паролі повинні містити літери, цифри, розділові знаки тощо);
- Керування термінами дії паролів та регулярна зміна паролів;
- Обмеження кількості невдалих спроб входу;
- Використовування програмних генераторів паролів (такі програми базуються на простих правилах і можуть генерувати лише ті паролі, які легко запам'ятати).

Щоб детальніше дослідити принципи побудови системи паролів, спочатку наведемо кілька основних визначень. Ідентифікатор користувача — унікальна інформація, що використовується для розрізнення кожного користувача в системі паролів (використовується для ідентифікації особистості користувача). Цей ідентифікатор часто також називають іменем користувача або іменем облікового запису користувача. Пароль користувача — секретна інформація, відома лише користувачеві та системі паролів; Користувач може запам'ятати цю інформацію та надати її під час процесу автентифікації.

Одноразові паролі дозволяють користувачеві пройти автентифікацію один раз. Паролі для багаторазової перевірки можна використовувати для багаторазової перевірки особи.

Обліковий запис користувача складається з його ідентифікатора та пароля. База даних користувачів криптографічної системи містить облікові записи всіх користувачів криптографічної системи. Криптографічна система – це апаратно-програмний комплекс, що реалізує ідентифікацію та автентифікацію користувачів ІКС на основі одноразових шифрів (рисунок 2.1, а) або кількох шифрів (рисунок 2.1, б) [13,14].

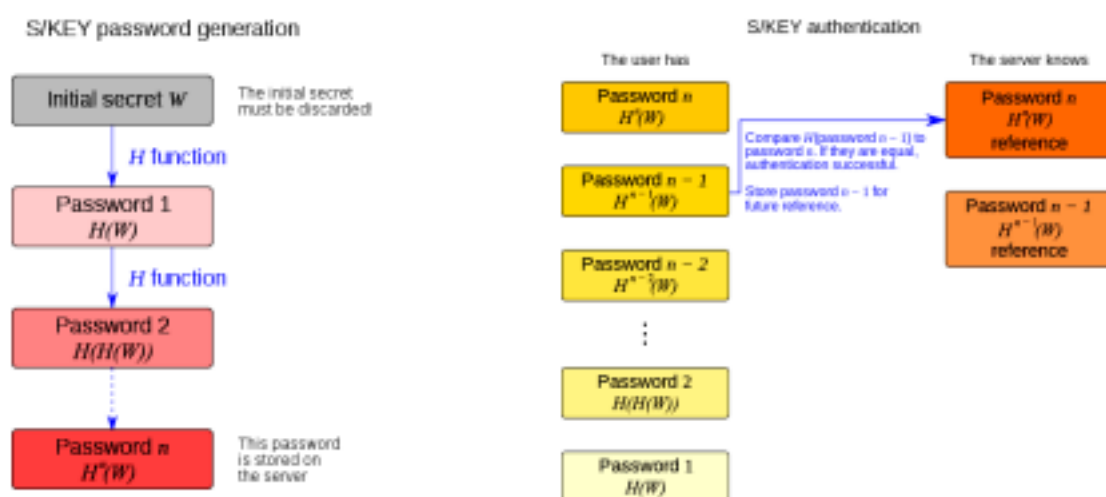


Рис.2.1. Система одноразових (а) та багаторазових (б) паролів

Зазвичай ця складна функціональність працює разом із підсистемами обмеження доступу та реєстрації подій. У деяких випадках криптографічна система також може виконувати додаткові функції, зокрема генерувати та розповсюджувати короткострокові (сесійні) ключі шифрування. Основні компоненти криптографічної системи включають [12,13,14]:

- Інтерфейс користувача;
- Інтерфейс адміністратора;
- Модулі для зв'язку з іншими підсистемами безпеки;
- База даних облікових записів.

Криптографічна система є «першою лінією захисту» в загальній системі безпеки. Деякі з її компонентів (особливо ті, що реалізують інтерфейс користувача) можуть бути розташовані в місцях, доступних потенційним зловмисникам. Тому, коли зловмисники компрометують захищену систему, криптографічна система стає однією з основних цілей. Типи загроз безпеці, з якими стикаються криптографічні системи, такі:

1) Розкриття параметрів облікового запису [14,15] шляхом:

- Вибір в інтерактивному режимі;
- Підслуховування;
- Власники паролів навмисно передають паролі іншим особам;
- Захоплення бази даних криптографічної системи;
- Перехоплення інформації про паролі, що передається мережею;
- Зберігання паролів у легкодоступному місці.

2) Втручання в роботу компонентів криптографічної системи за допомогою таких методів:

- Впровадження закладок програмного забезпечення;
- Виявлення та використання помилок під час розробки;
- Вимкнення криптографічної системи.

Деякі з вищезазначених типів загроз стосуються так званого «людського фактора», який потенційно проявляється у [14,15]:

- Вибір пароля, який легко запам'ятати та легко вкрати;
- Записування пароля, який важко запам'ятати, та розміщення запису в легкодоступному місці;
- Введення пароля таким чином, щоб його могли побачити сторонні;
- Навмисне або під впливом помилки розголошення пароля іншим.

Крім того, слід підкреслити існування «парадоксу людського фактора». Користувачі, як правило, є противниками криптографічної системи, а не

союзниками в її захисті, тим самим послаблюючи її безпеку. Фактично, робота будь-якої захищеної системи впливає на умови роботи користувачів.

Важливим аспектом стабільності криптографічної системи є те, як паролі зберігаються в базі даних облікових записів. Ось деякі можливі методи зберігання паролів [12,13,15]:

- Зберігання у відкритому тексті;
- Зберігання у згортковій (хеш-) формі;
- Шифрування за допомогою певного ключа.

Другий і третій методи є найважливішими та пропонують численні переваги. Хешування (використання незворотної хеш-функції для перетворення будь-якої інформації в унікальний код) не може перешкодити зловмисникам вибрати паролі зі словника після отримання доступу до бази даних. Вибираючи алгоритм хешування для обчислення згортки паролів, важливо забезпечити, щоб значення згортки, отримані на основі різних паролів користувачів, були різними.

Крім того, має бути передбачений механізм, що забезпечує унікальність згортки за таких умов: Проблеми виникають, якщо два користувачі обирають однаковий пароль. Тому під час обчислення кожної згортки зазвичай використовується певна кількість «випадкової» інформації, такої як інформація, згенерована генератором псевдовипадкових чисел.

Метод генерації та зберігання ключа шифрування для бази даних облікових записів особливо важливий під час шифрування паролів. Деякі можливі варіанти наведено нижче [14,15]:

- Ключ генерується програмно та зберігається в системі, що забезпечує автоматичний– Ключ генерується програмно та зберігається на зовнішньому носії, зчитується з нього кожного разу під час завантаження системи;
- Ключ генерується на основі пароля, обраного адміністратором, який вводиться в систему кожного разу під час завантаження системи.

У другому випадку необхідно забезпечити, щоб система не могла автоматично перезавантажитися, навіть якщо вона виявить носій, що містить ключ. Цього можна досягти, вимагаючи від адміністратора підтвердження, чи продовжувати процес завантаження, наприклад, натисканням клавіші на клавіатурі. Найбезпечніший спосіб зберігання паролів – хешувати пароль, а потім шифрувати отриманий хеш, поєднуючи другий та третій методи.

Враховуючи, що користувачі часто обирають недостатньо сильні паролі, можна зробити висновок, що доступ до бази даних облікових записів або перехоплення хешів паролів, що передаються мережею, становить серйозну загрозу безпеці системи паролів. У більшості випадків автентифікація відбувається в розподілених системах і передбачає передачу інформації про параметри облікового запису користувача мережею. Якщо інформація, що передається мережею під час автентифікації, не захищена належним чином, вона ризикує бути перехопленою зловмисниками та використаною для порушення безпеки системи паролів. Загальновідомо, що багато комп'ютерних систем дозволяють комутувати мережеві адаптери для моніторингу мережевого трафіку інших одержувачів у мережі, таким чином досягаючи пакетного захисту. Розглянемо основні типи захисту мережевого трафіку: фізичний захист мережі; наскрізне шифрування; та пакетне шифрування.

Нижче наведено поширені методи передачі паролів мережею [12,13,14]:

- Передача відкритого тексту;
- Зашифрована передача;
- Згорткова передача;
- Відсутність прямої передачі інформації про пароль («нульовий витік»).

Перший метод досі використовується багатьма популярними програмами (такими як TELNET, FTP). У захищеній системі його можна використовувати лише разом із засобами захисту мережевого трафіку. Коли криптографічні системи передають шифри в зашифрованій або згортковій формі через мережі з відкритим фізичним доступом, безпеці цих систем може загрожувати наступне [14,15]:

- Інформація перехоплюється та повторно використовується;
- Шифри перехоплюються та відновлюються;
- Передана інформація підроблюється, щоб ввести в оману контролюючу сторону;

Зловмисники імітують поведінку контролюючої сторони, щоб ввести користувачів в оману.

Схеми автентифікації з «нульовим знанням» або «нульовим розкриттям» вперше з'явилися в середині 1980-х та на початку 1990-х років. Основна ідея полягає в тому, щоб дозволити одній стороні з пари сторін довести істинність твердження іншій, не розкриваючи жодної інформації про зміст твердження. Наприклад, перша сторона («доказувач») може переконати другу сторону («верифікатор»), що вона знає пароль, фактично не розкриваючи жодної інформації про сам пароль. Ця ідея втілена у визначенні «доказу з нульовим розкриттям». З точки зору захисту паролем це означає, що якщо зловмисник знаходиться на місці верифікатора, він не зможе отримати жодної інформації про твердження, яке доводиться, особливо про пароль. Загальна схема процесу автентифікації з нульовим розкриттям включає серію обмінів інформацією (ітерацій) між двома учасниками, після чого верифікатор правильно робить висновок про істинність перевіреного твердження з заданою ймовірністю. Ймовірність правильного визначення істинності чи хибності твердження зростає з кількістю ітерацій.

Ще одним методом покращення стабільності систем передачі мережевих паролів є використання одноразових шифрів [14,15].

Загальний підхід до використання одноразових шифрів полягає в обчисленні наступного одноразового шифру за допомогою хеш-функції, що базується на попередньому одноразовому шифрі. Спочатку користувачі отримують упорядкований список одноразових паролів, причому останній

пароль також зберігається в системі автентифікації. Щоразу, коли користувач реєструється та вводить наступний пароль, система обчислює його згортку та порівнює її зі стандартним паролем, що зберігається в системі. Якщо вони збігаються, користувач успішно автентифікований, а введений пароль зберігається для подальшого використання.

Механізм протидії мережевому перехопленню цієї схеми спирається на незворотність хеш-функцій. Найвідомішим практичним застосуванням схем одноразових паролів є програмний пакет S/KEY та його похідна система OPIE.

Основною перевагою розпізнавання паролів є простота реалізації та використання.

Крім того, введення інформації для розпізнавання паролів є абсолютно безкоштовним: більшість програмних продуктів реалізували цю функціональність. Таким чином, система захисту інформації є одночасно простою та економічно ефективною. Основним недоліком розпізнавання паролів є те, що його надійність сильно залежить від користувача, а точніше, від пароля, обраного користувачем. Фактично, більшість використовуваних паролів є ненадійними та легко підбираються. Ці паролі включають надто короткі паролі, поширені комбінації символів тощо. Тому деякі експерти з інформаційної безпеки рекомендують використовувати довгі паролі, що складаються з випадкових комбінацій літер, цифр та різних символів.

Ще одним методом ідентифікації пароля є використання QR-кодів.

QR-коди були розроблені компанією Denso-Wave. Наразі «QR-код» є зареєстрованою торговою маркою корпорації Denso, але його використання не підлягає жодним ліцензійним зборам. Крім того, самі QR-коди відповідають стандартам ISO та публікуються відповідно до них.

QR розшифровується як «Quick Response» (швидка відповідь). Тобто QR-код можна назвати кодом швидкої відповіді (або кодом миттєвої відповіді). Ця термінологія сьогодні точніша, ніж будь-коли, оскільки сканування QR-коду не

вимагає спеціального обладнання. Просто піднесіть смартфон близько до QR-коду, щоб отримати всю необхідну інформацію.

QR-коди бувають різних версій та розмірів, починаючи від початкових 21×21 пікселів (без рамки) до 177×177 пікселів 40-ї версії.

Існує чотири основні типи кодування для QR-кодів. До них належать числові коди (для шифрування чисел), буквено-цифрові коди (для чисел та символів), байт-код (для даних) та коди китайських символів (для обробки піктограм).

Для виправлення помилок у QR-кодах, наприклад, коли QR-код пошкоджений або потрібно додати додаткові шаблони, використовується 8-бітний код Ріда-Соломона. Він має чотири рівні надмірності (7%, 15%, 25% та 30%). Крім того, існують інші, більш складні заходи захисту від неправильного зчитування. Ці заходи особливо важливі в системах оплати та перевірки особи. Одним із таких заходів є перерахування всіх можливих варіантів зчитування та розрахунок штрафного балу на основі певних правил для кожного варіанта. Зрештою, система вибирає найвдаліший варіант і вважає його правильним.

Головна перевага QR-кодів полягає в їхній «місткості». Цей тип коду є двовимірним, на відміну від одновимірних штрих-кодів. Перехід від «смуг» до «квадратів» колись був пов'язаний з необхідністю шифрувати більше інформації в коді.

Стандартний QR-код може містити до 4000 символів. Це може шифрувати не лише десятки символів інвентарного номера товару в магазині, але й цілі абзаци тексту, довгі посилання тощо. Він навіть може шифрувати зображення JPEG, GIF та PNG. Звичайно, це залежить від того, чи розмір цих зображень не перевищує 4 КБ, що дуже мало. Під час передачі зображень шифрування посилання та розміщення зображення на окремій сторінці набагато простіше.

Апаратна ідентифікація та автентифікація користувача в РСМ.

Цей принцип ідентифікації базується на визначенні особи користувача за допомогою деякого об'єкта (ключа), який доступний лише користувачеві [9,10,14].

Очевидно, що мова йде не про фізичний ключ, з яким знайома більшість людей, а про спеціальний електронний ключ. Наразі двома найпоширенішими пристроями є різні картки (безконтактні картки, смарт-картки, картки з магнітною смугою тощо) та так звані токени, які безпосередньо підключаються до порту комп'ютера. Кожен апаратний (електронний) ідентифікатор – це фізичний пристрій, зазвичай невеликий за розміром та портативний. Системи електронної ідентифікації та автентифікації включають (рисунок 2.3) [9,10,14]:



Рис.2.3. Токени

1. Портативні токени [9,10,14]:

- Асинхронні – Користувач вводить рядок у пристрій, отримує відповідь та вводить її в комп'ютер;
- PIN/Асинхронні – На основі асинхронного методу користувачеві потрібно ввести PIN-код у пристрій;
- Синхронні – Наприклад, токен синхронізується із сервером і генерує пароль для певного користувача у заданий час, який було введено в систему;
- PIN/Синхронні.

2. Різні картки – це пристрої, подібні до портативних автентифікаторів, але зі складнішим складом. Картки класифікуються [9,10,14]:

- Пасивні (карта пам'яті);
- Активні (смарт-карта).

Останні містять процесор, мініатюрну операційну систему, годинник, програму в ROM (постійному пам'яті), буферну пам'ять (ОЗП) для криптографічних обчислень, окрему пам'ять або EEPROM (електрично стираєний програмований постійний пам'ять) для зберігання цифрових ключів. Використовуючи смарт-картку, система обчислює одноразовий пароль та взаємодіє з пристроєм через зчитувач карток [9,10,14].

Після введення PIN-коду зчитувач карток автоматично зчитує смарт-картку, і наступний процес може бути виконаний без ручного втручання, що дозволяє використовувати достатньо довгий пароль.

Існує багато типів смарт-карток, і принципи їхньої роботи також відрізняються. Наприклад, безконтактні картки (також відомі як картки проксимісного доступу) дуже зручні у використанні, і користувачі можуть використовувати їх у комп'ютерних системах або системах контролю доступу для автентифікації. Смарт-картки вважаються найнадійнішими, подібно до банківських карток, з якими знайомі багато людей. Крім того, є деякі картки, які дешевші, але менш стійкі до злому, такі як картки з магнітною смугою та картки зі штрих-кодом.

Що таке USB-ключ? Як приклад для пояснення ми використаємо цифровий підпис Aladin Software. Цифровий підпис – це метод особистої автентифікації та зберігання даних, а апаратне забезпечення підтримує використання цифрових сертифікатів та електронних цифрових підписів (ЕЦП) [9].

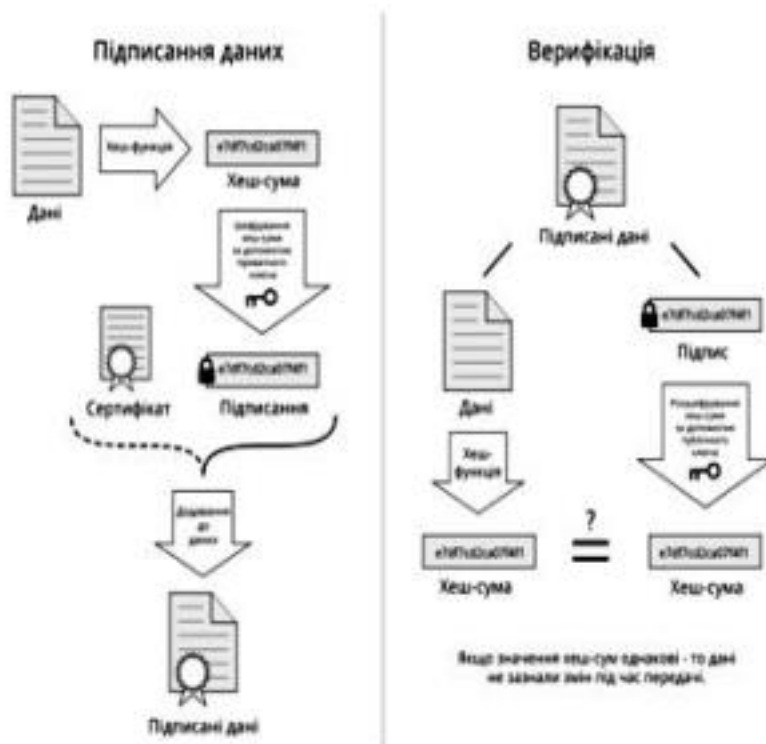


Рис. 2.4. Цифрові підписи

Цифрові підписи можна реалізувати за допомогою USB-флеш-накопичувача або стандартної смарт-картки.

Цифрові підписи підтримують та інтегруються з усіма основними системами та програмами, що використовують смарт-картки або технологію інфраструктури відкритих ключів (PKI). Їх основне використання [9,10,14,15] включає:

- Двофакторна автентифікація, коли користувачі отримують доступ до захищених ресурсів (комп'ютери, мережі, програми);
- Безпечне зберігання закритого ключа цифрового сертифіката, ключа шифрування, профілю користувача, налаштувань програми тощо на спеціальному пристрої зберігання даних;
- Виконання криптографічних операцій у надійному середовищі (генерація ключів шифрування, симетричне та асиметричне шифрування, обчислення хеш-функцій, генерація EDS).

Більшість сучасних операційних систем, комерційних програм та продуктів інформаційної безпеки підтримують цифрові підписи як засіб автентифікації.

Сценарії застосування [9,10,14]:

- Суворі автентифікація користувача під час доступу до серверів, баз даних або певних частин веб-сайту;
- Безпечне зберігання конфіденційної інформації: паролів, ключів шифрування та закритих ключів для цифрових сертифікатів;
- Захист електронної пошти (цифрові підписи та шифрування, контроль доступу);
- Системи електронної комерції, «банки клієнтів», «власний банк»;
- Захист комп'ютерів;
- Захист мереж та каналів передачі даних шляхом побудови VPN (віртуальних приватних мереж);
- Банки клієнтів, власний банк.

Цифрові підписи пропонують такі можливості [14,15]:

- Автентифікація користувачів за допомогою криптографічних методів; безпечне зберігання ключів шифрування та ЕЦП, а також закритих ключів цифрових сертифікатів для доступу до захищених корпоративних мереж та інформаційних ресурсів;
- Мобільність користувачів та можливість безпечної обробки конфіденційних даних у ненадійних середовищах (наприклад, на чужому комп'ютері), оскільки ключі шифрування та ЕЦП генеруються з цифрових ключів на апаратному забезпеченні та не можуть бути перехоплені;
- Безпечне використання – Цифровим ключем може користуватися лише власник, який знає PIN-код ключа; впровадження західних, російських та вітчизняних стандартів шифрування та ЕЦП; простота використання – ключ має форму брелока з індикатором режиму роботи та може бути безпосередньо

підключений до USB-порту, який зараз є на всіх комп'ютерах, що усуває потребу в спеціалізованих зчитувачах карт, блоках живлення, кабелях тощо;

- Багатозадачність одним кліком – вхід у комп'ютери, вхід у мережі, захист каналів, шифрування інформації, EDS (посилена безпека даних), безпечний доступ до захищених частин веб-сайтів, інформаційних порталів тощо.

Безконтактні смарт-картки класифікуються на проксимальні картки та смарт-картки відповідно до міжнародних стандартів ISO/IEC 15693 та ISO/IEC 14443. Більшість пристроїв безконтактних смарт-карток базуються на технології радіочастотної ідентифікації (RFID).

Основними компонентами безконтактних пристроїв є чіпи та антени.

Ідентифікатори можуть бути активними (живляться від батареї) або пасивними (без живлення). Кожен ідентифікатор має унікальний 32/64-бітний серійний номер.

Системи ідентифікації на основі близькості зазвичай не мають захисту шифруванням, за деякими винятками. USB-ключі працюють через USB-порт комп'ютера та нагадують брелоки. Кожен ключ має 32/64-бітний серійний номер.

Основною перевагою апаратної ідентифікації є її висока надійність. Фактично, ключ може зберігатися в пам'яті токена, що ускладнює його крадіжку. Крім того, вони реалізують різні механізми безпеки, а вбудований мікропроцесор дозволяє електронному ключу не лише брати участь у процесі автентифікації користувача, але й виконувати інші практичні функції. Основний ризик використання апаратної ідентифікації полягає в тому, що зломисники можуть вкрати токени або картки зареєстрованих користувачів. Їх також можна втратити, передати або скопіювати.

Другим недоліком цієї технології є її вища вартість. Загалом, вартість самого електронного ключа та супутнього програмного забезпечення значно знизилася за останні роки. Однак, для введення в експлуатацію такої системи

ідентифікації все ще потрібні певні інвестиції. Зрештою, кожен зареєстрований користувач повинен мати персональний токен. Крім того, ключі можуть зношуватися або губитися з часом. Іншими словами, апаратна ідентифікація вимагає певного рівня експлуатаційних витрат. У таблиці 2.1 [9,10,14] перераховано основні переваги та недоліки різних типів цифрових ключів.

Таблиця 2.1

Основні переваги й недоліки різних типів цифрових ключів

Продукт	Основні переваги	Основні недоліки
USB- токени	Мобільність - токен можна використовувати на будь-якому комп'ютері, де є USB-порт. Підтримка великої кількості застосунків IT-безпеки. Очевидна приналежність токена певному користувачеві.	Потребує встановлення ПЗ користувача.
Смарт-карти	Високий рівень безпеки. Компактність. Підтримка великої кількості застосунків.	Потребує встановлення ПЗ користувача. Потребує зчитувального пристрою.

USB-токени з вбудованим чіпом	Високий рівень безпеки. Мобільність. Підтримка великої кількості застосунків. Очевидна приналежність токена користувачеві.	Потребує встановлення ПЗ користувача.
ОТР-токени	Мобільність. Простота в користуванні. Не потребує встановлення ПЗ користувача.	Обмежене коло підтримуваних застосунків. Потребує сервера аутентифікації. Обмежений час експлуатації у зв'язку з використанням батарейки.
Гібридні-токени	Мобільність. Підтримка великої кількості застосунків. Не потребує встановлення ПЗ користувача для застосування одноразових паролів (ОТР). Очевидна приналежність токена користувачу.	Обмежений час експлуатації у зв'язку з використанням батарейки (Крім випадків, коли користувач може замінити батарейку самостійно).
Програмні токени	Не потребує апаратного пристрою.	Секретний ключ слабо захищений. Обмежене коло підтримуваних застосунків. Потрібно сервер аутентифікації.

Біометрія та автентифікація в РСМ

Біометрія стосується використання унікальних біологічних характеристик, які існують лише у користувача, для його ідентифікації. Іншими словами, можна сказати, що біометрія спочатку була розроблена для точного визначення. Тому її застосування до галузі інформаційної безпеки видається логічним. Крім того, ця галузь швидко розвивається. Наразі використовується понад десяток різних біометричних характеристик. Більше того, для найпоширеніших біометричних характеристик (відбитків пальців та райдужної оболонки ока) доступно багато різних типів сканерів.

Тому користувачі мають багато варіантів вибору при використанні біометрії. Біометрія та автентифікація – це метод ідентифікації осіб за допомогою унікальних біологічних характеристик. Розвиток сучасних

комп'ютерних технологій дозволив використовувати ці характеристики як основу для ідентифікації осіб та визначення їх доступу до ресурсів комп'ютерної системи [16,17,18]. У механізмах біометричної ідентифікації можна виділити такі типи [16,17,18]:

1) Статичні характеристики – характеристики, які майже не змінюються з часом від народження (фізіологічні особливості);

2) Динамічні ознаки – поведінкові ознаки, тобто ознаки, побудовані на основі характеристик підсвідомих дій, які формуються під час повторення будь-якої дії.

Динамічні ознаки змінюються з часом, але зміни відбуваються не раптово, а поступово.

Серед статичних методів, що використовуються для ідентифікації користувача в комп'ютерних системах, зазвичай використовуються такі методи [16,17,18]:

1. Розпізнавання відбитків пальців (рис. 1.5). Цей метод базується на унікальності візерунків сосків на пальцях. Процес розпізнавання виглядає наступним чином: зображення відбитка пальця отримується за допомогою сканера, а потім за допомогою складного алгоритму зображення перетворюється на спеціальний цифровий код. Нарешті, цей код порівнюється з еталонним кодом, що зберігається в базі даних.



Рис.2.5. Пальцевий та долонний дактилоскопічні сканери

2. Ідентифікація за відбитком долоні. У цьому випадку для зчитування інформації використовується інфрачервона камера. Після введення програми

генерується цифровий код, і під час введення відображається візерунок вен на руці людини. Контакт між людиною та скануючим пристроєм не потрібен. Він має високу надійність та точність.

3. Ідентифікація за сітківкою (Рисунок 2.6). У цьому випадку сканується візерунок кровоносних судин на очному дні, і його структура фіксується. Очевидно, що цей візерунок можна спостерігати лише за певних умов: під час сканування людина, яку сканують, дивиться на віддалене джерело світла, а спеціальна камера сканує її очне дно, що може спричинити дискомфорт у людини, яку сканують. Це вважається одним із найнадійніших біометричних методів.

4. Ідентифікація за райдужкою ока (Рисунок 2.6).

Візерунок райдужки кожної людини унікальний. Цей метод вимагає не лише спеціальної камери, але й надійного програмного забезпечення.

Зрештою, нам потрібно використовувати програмне забезпечення, щоб витягти потрібний візерунок райдужки з зображення. Цей метод є одним із найточніших біометричних методів.

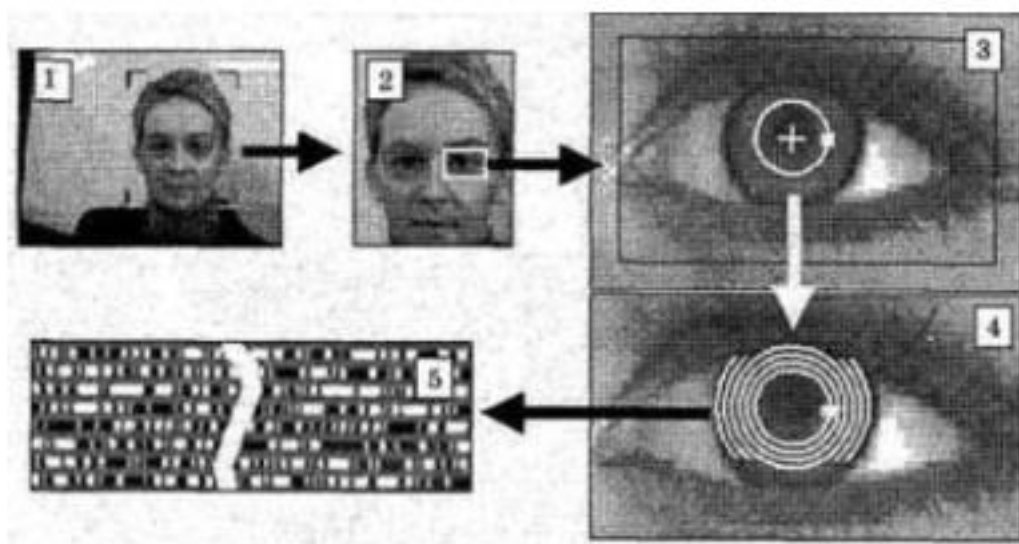


Рис. 2.6. Аутентифікація за райдужною оболонкою ока

5. Розпізнавання руки. Цей метод базується на розпізнаванні геометричних рис руки. Спеціалізований сканер генерує 3D-зображення руки. Під час аналізу цього зображення проводяться вимірювання, і відповідно генерується відповідний цифровий код.

6. Розпізнавання обличчя (Рис. 2.7).

На практиці використовуються як 2D, так і 3D-зображення. Однак 2D-розпізнавання обличчя наразі є одним з найменш ефективних методів у біометрії, тому його застосування обмежене або використовується лише в поєднанні з іншими методами. 3D-розпізнавання зображень обличчя дещо схоже на розпізнавання руки. Цей метод також створює 3D-зображення обличчя. Спеціалізоване програмне забезпечення витягує контури очей, губ та інших рис обличчя з цього зображення. Потім ці контури точно вимірюються. На основі цих даних генерується цифровий код.

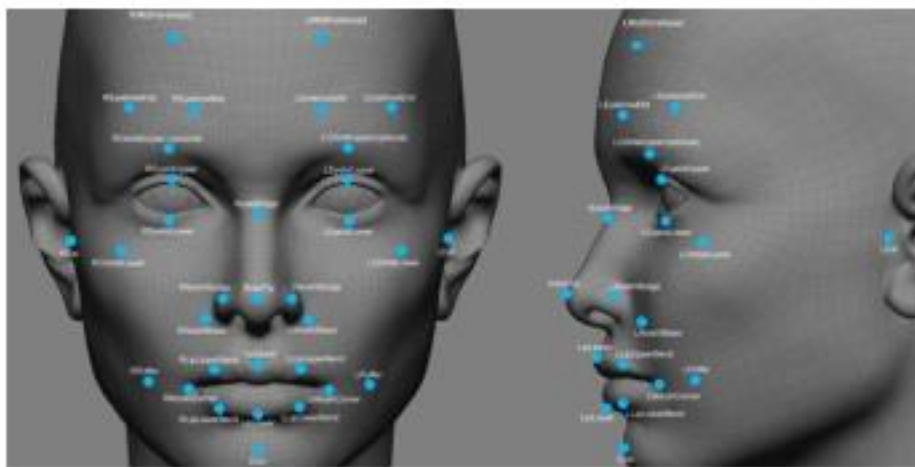


Рис. 2.7. Аутентифікація за формою обличчя

Динамічні методи, що використовуються для ідентифікації користувача, включають наступне:

1. Розпізнавання мовлення. Існує багато програм розпізнавання мовлення. У розпізнаванні мовлення частотні характеристики людського голосу є вирішальними. Цифрові моделі будуються на основі цих частотних характеристик.

2. Розпізнавання почерку. Під час використання цього методу ідентифікації зазвичай перевіряється підпис користувача. Система досліджує динамічні характеристики, такі як графічні параметри, тиск почерку та швидкість підпису. На основі цих характеристик генерується цифровий код.

3. Розпізнавання почерку з клавіатури. Цей метод схожий на розпізнавання почерку, але замість підпису користувач вводить закодоване слово. Цифровий код генерується на основі динамічних характеристик введеного конкретного слова або фрази.

Хоча теоретично існують різні біометричні методи, мало хто з них фактично використовується. Існує три основні методи: розпізнавання відбитків пальців, розпізнавання зображень обличчя (двовимірне або тривимірне), розпізнавання райдужної оболонки ока та розпізнавання сітківки. Наразі всі біометричні технології базуються на ймовірності, характеристиці, яка часто стає джерелом критики біометричних технологій.

Безперечно, біометричні технології є більш надійними та зручними, ніж інші широко використовувані заходи безпеки. Однак, незважаючи на нещодавні зусилля щодо розробки та вдосконалення методів ідентифікації користувачів для кращого управління доступом до ресурсів інформаційної системи, надійність та стабільність існуючих систем все ще не відповідають сучасним вимогам. Головна перевага біометричної технології полягає в її надзвичайно високій надійності. Дійсно, добре відомо, що в природі немає двох людей з абсолютно однаковими відбитками пальців. Щоправда, зараз існують різні методи обману сканерів відбитків пальців.

Наприклад, потрібний відбиток пальця можна перенести на плівку або використовувати фотографію відбитка пальця зареєстрованого користувача. Однак, слід визнати, що сучасні пристрої набагато стійкіші до такої підробки.

Основним недоліком біометрії є висока вартість обладнання. Адже кожен комп'ютер у системі повинен бути оснащений незалежним сканером. Звичайно, ціна на біометричні пристрої постійно знижується в останні роки [17,18].

Крім того, миші та клавіатури з вбудованими сканерами відбитків пальців стали доступні лише нещодавно.

У обговорюваній системі для визначення особи користувача використовується лише один фактор. Однак надійність цього методу все ще потребує покращення.

В останні роки широко застосовується комплексна або багатофакторна автентифікація.

2.3 Вимоги та порядок організації процесів ідентифікації та автентифікації

Основним міжнародним стандартом для протоколів криптографічної автентифікації є ISO/IEC 9798 — Інформаційні технології — Технології безпеки — Механізми автентифікації об'єктів, стандарт Міжнародної організації зі стандартизації та Міжнародної електротехнічної комісії (ISO/IEC). Цей стандарт складається з п'яти частин [19,20,21]:

ISO/IEC 9798-1 — «Загальна модель»;

ISO/IEC 9798-2 — «Механізми, що використовують симетричні алгоритми шифрування»;

ISO/IEC 9798-3 — «Автентифікація об'єктів з використанням алгоритмів з відкритим ключем»;

ISO/IEC 9798-4 — «Механізми, що використовують функції криптографічної верифікації»;

ISO/IEC 9798-5 — «Механізми, що використовують методи нульового розголошення».

У цих протоколах заявник і верифікатор мають симетричний ключ або попарно вибіркового ключ зв'язку. Для отримання цих ключів у режимі реального часу можна використовувати довірений сервер.

Стандарт ISO/IEC 9798-2 надає три методи автентифікації [19,20]:

1. Одностороння автентифікація на основі позначки часу (рис. 2.9). Якщо і запитувач, і валідатор мають системний годинник, запит надсилати не потрібно. Запитувач може безпосередньо надіслати повідомлення, що містить позначку часу, яку валідатор потім може порівняти зі своїми показниками годинника.

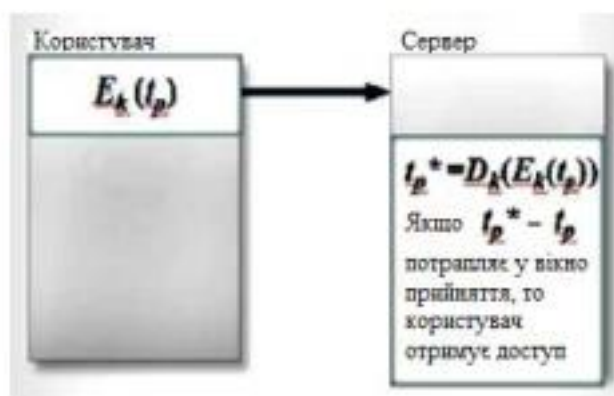


Рис. 2.9. Одностороння автентифікація, заснована на мітці часу

2. Одностороння автентифікація з використанням випадкових чисел (рис. 2.10). Верифікатор надсилає випадкове число, згенероване генератором псевдовипадкових чисел, як запит. Після отримання запиту заявник обчислює відповідь — шифруючи отримане випадкове число та (за необхідності) ідентифікатор за допомогою симетричного алгоритму шифрування. Верифікатор розшифровує отриманий шифротекст та перевіряє структуру запиту.

Якщо структура правильна, верифікатор приймає заявника.

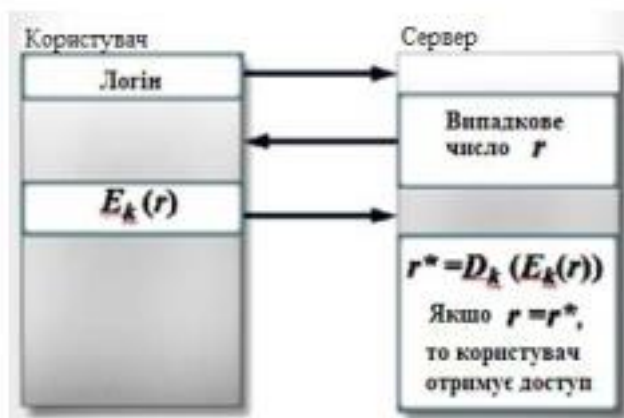


Рис. 2.10. Одностороння автентифікація з використанням випадкових чисел

3. Двостороння автентифікація з використанням випадкових чисел (рис. 2.11). Цей протокол відрізняється від попереднього тим, що учасники по черзі виступають у ролі верифікаторів та оскаржувачів, взаємно перевіряючи ідентичності один одного.

Протокол двосторонньої автентифікації по суті «упаковує» два протоколи односторонньої автентифікації в три передачі повідомлень. Завдяки своїй симетрії цей тип протоколу називається протоколом рукошлякування. Цей протокол дозволяє використовувати хеш-функції ключів, що відповідають стандарту ISO/IEC 9798-4, замість криптографії. Для підвищення стабільності протоколу до переданих повідомлень можна додавати позначки часу.



Рис. 2.11. Взаємна автентифікація з використанням випадкових чисел

4. Протоколи запиту-відповіді з використанням асиметричних схем шифрування.

Ці протоколи можна розділити на дві категорії: протоколи з використанням EDS та протоколи з використанням відкритих схем шифрування. Стандарт ISO/IEC 9798-3 рекомендує:

1) Протоколи з використанням схем цифрового підпису (Рисунок 2.12).

В описі протоколу certA представляє сертифікат відкритого ключа цифрового підпису відповідного учасника протоколу, тобто структуру даних, що містить його ідентифікатор, відкритий ключ та іншу службову інформацію, і має цифровий підпис та автентифікацію центру сертифікації. Методи автентифікації за відкритим ключем будуть детально розглянуті пізніше. Подібні протоколи також використовуються у стандарті Міжнародного союзу електрозв'язку ITU X.509. Цей стандарт описує протоколи, що поєднують протоколи автентифікації з протоколами обміну ключами.



Рис. 2.12. Протоколи з використанням схем-цифрового підпису

2) Протоколи, що використовують відкриті схеми шифрування (рис. 2.13).

Загрози безпеці промислових систем керування (ІКС) можна розділити на кібератаки (інформація від віддалених клієнтів) та локальні атаки (що виникають від шкідливого програмного забезпечення, вже встановленого на клієнтській системі, такого як трояни, руткіти тощо).

Як правило, оцінки безпеки автентифікації в першу чергу зосереджуються на кібератаках та припускають, що термінал користувача (тобто настільний комп'ютер, ноутбук або мобільний пристрій) є захищеною платформою. Однак нерідко зловмисники отримують повний доступ до комп'ютера жертви через приховані комунікаційні процеси, залишені шкідливим програмним забезпеченням, яке використовує не виправлені вразливості безпеки в ліцензованому програмному забезпеченні.

Типові методи атаки проти протоколів автентифікації включають [19,20,21]:

1. Атака уособлення - один користувач намагається видати себе за іншого користувача.
2. Атака повторної передачі (атака повторного відтворення) - будь-який користувач повторно передає раніше автентифіковані дані.
3. Атака чергування - під час атаки зловмисник може змінити трафік, що проходить через нього.



Рис. 2.13. Протоколы з використанням схем відкритого шифрування

4. Атака відбиття – варіант атаки підміни, коли зловмисник за певних обставин надсилає перехоплену інформацію назад цілі.
5. Атака вимушеної затримки – зловмисник перехоплює певну інформацію та надсилає її через певний проміжок часу.

6. Атака вибраного тексту – зломисник перехоплює комунікаційний трафік, намагаючись отримати інформацію про довгострокові ключі.

Атаки на протоколи автентифікації та контрзаходи

Таблиця 2.2

Рекомендації стосовно заходів проти поширених типів атак на протоколи автентифікації

Тип атаки	Контрзаходи
Повторна передача	Використання протоколів "запит-відповідь", міток часу, випадкових чисел, вставок ідентифікуючої інформації у відповіді.
Підміна сторони	З'єднання всіх повідомлень в межах однієї сесії протоколу (наприклад, використовуючи одноразовий і унікальний ідентифікатор в усіх повідомленнях).
Відбиття	Використання ідентифікаторів сторін в повідомленнях, що передаються, і побудова протоколу таким чином, щоб кожне повідомлення мало відмінну від інших форму.

Тип атаки	Контрзаходи
Вибірка тексту	Використання протоколу, які мають властивості доказів з нульовим розголошенням, включення в кожне повідомлення випадкових чисел.
Затримка передачі	Комбінація міток і випадкових чисел.

2.4 Висновки по розділу

1. У цьому розділі розглядаються існуючі технології ідентифікації та автентифікації користувачів в інформаційно-комунікаційних системах для об'єктів інформаційної діяльності. Визначено основні концепції та функції інформації з обмеженим доступом та запропоновано систему технологій ідентифікації та автентифікації користувачів.
2. У цьому розділі розглядаються зміст, характеристики застосування, переваги та недоліки методів ідентифікації та автентифікації користувачів в інформаційно-комунікаційних системах, включаючи криптографію, апаратне забезпечення та біометрію.
4. У цьому розділі запропоновано вимоги та процедури для організації процесу ідентифікації та автентифікації.

РОЗДІЛ 3

РОЗРОБКА МЕХАНІЗМІВ БАГАТОФАКТОРНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

3.1 Зміст, характеристики та вимоги до механізму ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах

У системі автентифікації зазвичай можна виділити такі елементи [16,19,23]:

- Суб'єкт, який приймає автентифікацію;
- Характеристики суб'єкта — його унікальні особливості;
- Особа, відповідальна за систему автентифікації, яка відповідає за керування роботою системи;
- Механізм автентифікації, тобто принцип роботи системи;
- Механізм надання або позбавлення суб'єктів певних дозволів на доступ.

Задовго до появи комп'ютерів люди використовували різні унікальні особливості суб'єктів. Сьогодні використання певних функцій у системі залежить від необхідної надійності, безпеки та вартості впровадження. Існує три фактори автентифікації [24,25]:

1. Інформація, яку ми знаємо — паролі. Це секретна інформація, яку можуть знати лише авторизовані суб'єкти. Паролі можуть бути вимовленими словами, текстовими словами, комбінаціями замків або персональними ідентифікаційними номерами (PIN-кодами).

Механізми паролів легко реалізувати та недорого. Однак вони також мають суттєві недоліки: секретність паролів часто складна, і зловмисники постійно розробляють нові методи крадіжки, злому та вибору паролів (див. Аналіз шифрів грабіжників).

2. Інформація, якою ми володіємо – пристрої автентифікації. Той факт, що суб'єкт володіє чимось унікальним, має вирішальне значення. Це може бути особиста печатка, ключ від замка або, для комп'ютера, файл даних, що містить характеристики. Ці характеристики зазвичай вбудовані в спеціальні пристрої автентифікації, такі як пластикові картки або смарт-картки. Для зловмисників отримання таких пристроїв є складнішим, ніж злом паролів, і якщо пристрій викрадено, суб'єкт може негайно повідомити про це. Це робить цей метод безпечнішим, ніж механізми паролів, але такі системи також дорожчі.

3. Біометрія – частина нас самих.

Біометрія стосується фізіологічних характеристик суб'єкта. Це може бути портрет, відбиток пальця або долоні, голос або риси очей. З точки зору суб'єкта, цей метод є найпростішим: немає потреби запам'ятовувати паролі чи носити з собою пристрої автентифікації. Однак біометричні системи повинні бути дуже чутливими, щоб підтверджувати авторизованих користувачів, відкидаючи зловмисників зі схожими біометричними параметрами. Крім того, такі системи досить дорогі. Незважаючи на ці недоліки, біометрія залишається дуже перспективною.

Багатофакторна автентифікація. Одним із методів автентифікації комп'ютерної системи є введення ідентифікатора користувача (зазвичай відомого як «ім'я користувача») та пароля (деяка конфіденційна інформація) [24,25]. Надійна (еталонна) комбінація логіна та пароля. Паролі зберігаються у спеціальній базі даних.

Загальний алгоритм простої автентифікації такий [24,25]:

- Користувач запитує доступ до системи та вводить персональний ідентифікатор і пароль;
- Введені унікальні дані надсилаються на сервер автентифікації та порівнюються з опорними даними;
- Якщо дані збігаються з опорними даними, автентифікація успішна; в іншому випадку користувач повертається до кроку 1.

Пароль, введений користувачем, може бути переданий мережею двома способами:

- Передача у відкритому тексті (незашифрований) на основі протоколу автентифікації пароля (PAP);
- Використання шифрування або односторонньої хеш-функції;

У цьому випадку унікальні дані, введені користувачем, передаються мережею безпечно. З точки зору максимальної безпеки, під час зберігання та передачі паролів слід використовувати односторонню функцію. Як правило, для цієї мети використовується криптографічно стійка хеш-функція. У цьому випадку на сервері зберігається лише образ пароля. Після того, як система отримає пароль та хешує його, вона порівнює результат з опорним образом, що зберігається в системі. Якщо вони однакові, пароль збігається. Навіть якщо зломисник отримає доступ до образу, практично неможливо обчислити сам пароль. Використання кількох паролів має кілька суттєвих недоліків. По-перше, сам еталонний пароль або його хеш-образ зберігається на сервері автентифікації. У більшості випадків паролі зберігаються в системних файлах без шифрування.

Зломисники можуть легко отримати конфіденційну інформацію, отримавши доступ до цих файлів. По-друге, користувачі змушені запам'ятовувати (або записувати) свої часто використовувані паролі. Зломисники можуть отримати ці паролі за допомогою методів соціальної інженерії без будь-яких технічних засобів. Крім того, безпека системи значно знижується, якщо користувачі вибирають свої власні паролі. У більшості випадків паролі - це слова або комбінації слів, що існують у словнику. За наявності достатнього часу зломисники можуть зламати паролі за допомогою простих атак методом перебору. Рішення цієї проблеми включають використання випадкових паролів або обмеження терміну дії паролів користувачів, після чого їх необхідно змінити.

В операційних системах на базі UNIX база даних – це файл `/etc/master.passwd` (у дистрибутивах Linux це зазвичай файл `/etc/shadow`,

доступний для читання лише root), який зберігає хеші паролів користувачів та інформацію про дозволи користувачів. Спочатку в системах UNIX паролі (у зашифрованому вигляді) зберігалися у файлі `/etc/passwd`, який був доступний для читання всім користувачам, що створювало вразливість безпеки [24,25]. На комп'ютерах під керуванням операційних систем Windows NT/2000/XP/2003/2008 (які не входять до домену Windows) цей тип бази даних називається SAM (Security Account Manager). База даних SAM зберігає облікові записи користувачів, що містять усі дані, необхідні для функціонування системи безпеки. Вона розташована в каталозі `%windir%\system32\config\` [24,25].

У доменах Windows Server 2000/2003/2008 Active Directory слугує основою. Щоб забезпечити можливість роботи співробітників на різних комп'ютерах (за підтримки захищеної системи), необхідні апаратні та програмні системи для зберігання даних автентифікації та ключів шифрування на серверах організації. Користувачі можуть вільно працювати на будь-якому комп'ютері (робочій станції), який зберігає їхні дані автентифікації та ключі шифрування [24,25].

Зловмисник, отримавши пароль багаторазового використання суб'єкта, може отримати постійний доступ до викраденої конфіденційної інформації. Цю проблему можна вирішити за допомогою одноразових паролів (ОТР).

Суть цього методу полягає в тому, що пароль дійсний лише для одного входу в систему, і для кожного наступного запиту на доступ потрібен новий пароль. Механізми автентифікації за одноразовим паролем можуть бути реалізовані за допомогою апаратного та програмного забезпечення.

Технології, що використовують одноразові паролі, можна класифікувати наступним чином [14,24,25]:

- Використання генератора псевдовипадкових чисел, унікального як для суб'єкта, так і для системи.
- Використання позначок часу та одноразової системи;

- Використання бази даних випадкових паролів, унікальної як для суб'єкта, так і для системи.

Перший метод використовує генератор псевдовипадкових чисел з однаковим значенням як для суб'єкта, так і для системи. Пароль, згенерований суб'єктом, може передаватися до системи послідовно через односторонню функцію, або ж він може передаватися з кожним новим запитом на основі унікальної інформації з попереднього запиту.

Другий метод використовує позначки часу. SecurID є прикладом цієї технології. Вона базується на апаратних ключах та синхронізації часу.

Автентифікація на основі генерації випадкових чисел через певні інтервали часу має наступний механізм реалізації: Унікальний ключ зберігається лише в базі даних системи та на апаратному пристрої суб'єкта. Коли суб'єкт запитує доступ до системи, система запитує PIN-код та генерує випадкове число, яке одразу відображається на апаратному пристрої. Система порівнює введений PIN-код з ключем суб'єкта у своїй базі даних та генерує випадкове число на основі параметрів ключа в базі даних та поточного часу. Далі система перевіряє, чи збігається згенероване число з числом, введеним користувачем [20, 21, 25].

Третій метод базується на базі даних паролів, спільній для користувача та системи, що забезпечує високоточну синхронізацію між ними. У цьому випадку кожен пароль у наборі паролів можна використовувати лише один раз. Тому, навіть якщо злоумисник перехопить пароль, який використовує користувач, цей пароль вже буде недійсним. Одноразові паролі забезпечують більшу безпеку порівняно з використанням кількох паролів.

В останні роки все ширше використовується так звана розширена або багатофакторна автентифікація. Вона значно покращує безпеку системи, поєднуючи кілька факторів автентифікації. Наприклад, використання SIM-картки в мобільному телефоні є одним із таких прикладів.

Користувачі вставляють SIM-картку (пристрій автентифікації) у свій телефон і вводять PIN-код (пароль) після ввімкнення. Крім того, деякі сучасні

ноутбуки оснащені сканерами відбитків пальців. Тому користувачі повинні спочатку виконати розпізнавання відбитків пальців (біометрію), перш ніж вводити пароль під час входу в систему [18,24,25].

Вибираючи певний фактор або метод автентифікації для системи, необхідно враховувати необхідний рівень безпеки, складність архітектури системи та забезпечення мобільності користувачів.

У таблиці 3.1 порівнюються методи автентифікації за критеріями ризику [19,20,22].

Таблиця 3.1

Порівняння методів автентифікації по критерію ризику

Рівень ризику	Вимоги до системи	Технологія автентифікації	Приклади застосування
Низький	Потрібно здійснити автентифікацію	Рекомендується мінімальна вимога	Реєстрація на порталі в

	для доступу до системи, причому крадіжка, злом, розголошення конфіденційної інформації не матиме значних наслідків	використання багаторазових паролів	мережі Інтернет
Середній	Потрібно здійснити автентифікацію для доступу до системи, причому крадіжка, злом, розголошення конфіденційної інформації заподіє невеликий збиток	Рекомендується мінімальна вимога - використання одноразових паролів	Проведення суб'єктом банківських операцій
Високий	Потрібно здійснити автентифікацію для доступу до системи, причому крадіжка, лом, розголошення конфіденційної інформації завдасть значної школи	Рекомендується мінімальна вимога - використання багатофакторної автентифікації	Проведення великий міжбанківських операцій керівним апаратом

3.2 Моделі оцінки захищеності механізмів багатфакторної автентифікації користувачів від несанкціонованого доступу

Ми розглядаємо модель оцінки безпеки механізмів багатфакторної автентифікації для оцінки ризику несанкціонованого доступу користувачів за допомогою трифакторного механізму автентифікації. Важливо зазначити, що двофакторна та однофакторна автентифікація – це два різні випадки, і перехід від трифакторної до багатфакторної автентифікації є простим.

Ймовірність NSD механізму автентифікації, показаного на рисунку 3.1, визначається формулами [23,25,27]:

$$P_{НСД} = \left(1 - \prod_{i=1}^j P_i^n\right) \left(1 - \prod_{i=1}^{\varepsilon} P_i^k\right) \left(1 - \prod_{i=1}^{\mu} P_i^b\right) \quad (3.1)$$

Де:

P_i^n – ймовірність правильної роботи механізму паролювання;

P_i^k – ймовірність правильного застосування механізму особистого ключа;

P_i^b – ймовірність правильного застосування механізму біометричного признака.

Доказ вищеподаного співвідношення зводиться до наступного.

Для схеми Рис. 1 ймовірності $P_{НСД}^n$ та $P_{Зах}^n$ в випадку застосування паролю мають вид [23,25, 27]:

$$P_{НСД}^n + P_{Зах}^n = 1 \quad (3.2)$$

Далі

$$P_{НСД}^n = 1 - P_{3ax}^n \quad (3.3)$$

Визначимо ймовірність вірної роботи механізму автентифікації P_{3ax}^n . Це буде спостерігатись, якщо ні по одному каналу введення паролю не буде спостерігатися НСД. Тоді, згідно (3.3) [23,25, 27]:

$$P_{НСД}^n = 1 - P_{3ax}^n = 1 - P_1^n P_2^n \dots P_j^n = 1 - \prod_{i=1}^j P_i^n \quad (3.4)$$

Де $P_1^n, P_2^n \dots P_j^n$ відповідно відказ НСД при дозволі застосування паролів всіх j користувачів.

По аналогу для випадку оцінки НСД за рахунок застосування особистих ключів отримаємо [23,25, 27]:

$$P_{НСД}^k = 1 - P_{3ax}^k = 1 - P_1^k P_2^k \dots P_\varepsilon^k = 1 - \prod_{i=1}^{\varepsilon} P_i^k \quad (3.5)$$

Для оцінки ймовірності НСД за рахунок застосування біометричних при знаків [23,28]:

$$P_{НСД}^b = 1 - P_{3ax}^b = 1 - P_1^b P_2^b \dots P_\mu^b = 1 - \prod_{i=1}^{\mu} P_i^b \quad (3.6)$$

Якщо події отримання НСД по всім трьом факторам незалежні, то загальна ймовірність $P_{НСД}^n$ буде визначатися як [23-28]:

$$P_{НСД} = \prod_{i=1}^j P_i^n \prod_{i=1}^{\varepsilon} P_i^k \prod_{i=1}^{\mu} P_i^b \quad (3.7)$$

Особливі випадки існують, коли використовуються лише два або один із трьох факторів автентифікації.

Таблиця 3.2 ілюструє ці особливі випадки для моделей оцінки трьох варіантів двофакторного механізму [23,25,28].

У послідовній моделі ймовірність НСР має визначатися теоремою множення ймовірностей. У цьому випадку добуток ймовірностей кількох незалежних подій дорівнює добутку ймовірностей цих подій.

Це визначається наступним виразом [23,27]:

$$P_{НСД} = P_n^{НСД} P_k^{НСД} P_b^{НСД} = 1 - (1 - P_n)(1 - P_k)(1 - P_b) \quad (3.8)$$

Де:

P_n – ймовірність правильного застосування паролю;

P_k – ймовірність правильного застосування ключа;

P_b – ймовірність правильного застосування біометричного признаку;

$P_n^{НСД}$ – ймовірність підроблення паролю;

$P_k^{НСД}$ – ймовірність підроблення ключа;

$P_b^{НСД}$ – ймовірність підроблення біометричного признаку;

Таблиця 3.2.

Співвідношення для оцінки $P_{НСД}^n (P_{Зax}^n)$ механізмів комбінованої
двофакторної автентифікації

Механізм пароль/ключ	$P_{НСД} = \left(1 - \prod_{i=1}^j P_i^n\right) \left(1 - \prod_{d=1}^{\varepsilon} P_d^k\right)$	$P_{Зax} = \left(\prod_{i=1}^{\varepsilon} P_i^k\right) \left(\prod_{l=1}^{\mu} P_l^b\right)$
Механізм пароль/біометрія	$P_{НСД} = \left(1 - \prod_{i=1}^j P_i^n\right) \left(1 - \prod_{l=1}^{\mu} P_l^b\right)$	$P_{Зax} = \left(\prod_{i=1}^j P_i^n\right) \left(\prod_{l=1}^{\mu} P_l^b\right)$

Механізм ключ/біометрія	$P_{НСД} = \left(1 - \prod_{d=1}^{\varepsilon} P_d^k\right) \left(1 - \prod_{l=1}^{\mu} P_l^b\right)$	$P_{3ax} = \left(\prod_{d=1}^{\varepsilon} P_d^k\right) \left(\prod_{l=1}^{\mu} P_l^b\right)$
----------------------------	---	---

В подальшому, ймовірність безвідмовної роботи послідовної структури для випадку, що зображений на Рис.4 буде визначатися по виразу [23,27]:

$$P_{3ax} = 1 - P_{НСД} = 1 - (1 - P_n)(1 - P_k)(1 - P_b) \quad (3.9)$$

Окремі випадки використання одного або двох факторів автентифікації також мають практичне значення.

У таблиці 3.3 наведено окремі випадки моделей оцінки для трьох механізмів двофакторної автентифікації. Використовуючи коефіцієнти, наведені в таблиці, можна оцінити послідовних механізмів двофакторної автентифікації [23,26,28].

У таблицях 3.2 та 3.3 наведено аналітичні коефіцієнти, які можна використовувати для оцінки стійкості до атак NSD при паралельному або послідовному використанні одного фактора автентифікації..

Таблиця 3.3.

Співвідношення для оцінки $P_{НСД}^n$ (P_{3ax}^n) механізмів послідовної
двофакторної автентифікації

Механізм пароль/ключ	$P_{НСД} = (1 - P_n)(1 - P_k)$	$P_{3ax} = 1 - (1 - P_n)(1 - P_k)$
Механізм пароль/біометрія	$P_{НСД} = (1 - P_n)(1 - P_b)$	$P_{3ax} = 1 - (1 - P_n)(1 - P_b)$
Механізм ключ/біометрія	$P_{НСД} = (1 - P_k)(1 - P_b)$	$P_{3ax} = 1 - (1 - P_k)(1 - P_b)$

Тому було запропоновано математичні моделі для оцінки механізмів багатофакторної автентифікації, які можна використовувати для оцінки ймовірності реалізації NSD на основі комбінованих та послідовних механізмів автентифікації. Розроблені математичні моделі можуть бути поширені на простори автентифікації довільного розміру та є універсальними.

Під час застосування цих моделей необхідно дотримуватися наступного підходу. При побудові системи захисту NSD спочатку необхідно визначити перелік факторів, які можна використовувати для реалізації багатофакторної автентифікації. Потім для кожного фактора визначається та оцінюється повний перелік атак з існуючих відомих або потенційних джерел. Після цього можна приймати рішення щодо вибраних факторів та порядку їх застосування [23,29,30,31].

3.3 Висновок по розділу

1. У цьому розділі окреслено процес ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах. Виділено елементи та фактори цього процесу: паролі, пристрої автентифікації та біометрія користувача. Крім того, описано алгоритми автентифікації та процеси використання паролів у різних операційних системах.

2. У цій статті запропоновано математичні моделі для оцінки безпеки механізмів багатофакторної автентифікації користувачів для запобігання несанкціонованому доступу.

Ці моделі враховують ймовірність несанкціонованого доступу до мережі та ймовірність захисту мережі від конкретних ситуацій, що дозволяє оцінити загальну безпеку на основі комбінаційних та послідовних механізмів побудови, включаючи часткові ймовірності безпеки, що забезпечуються різними факторами автентифікації.

ВИСНОВКИ

Під час процесу підготовки кваліфікації було виконано такі завдання:

- Виявлено процес розподілу інформації для цілей інформаційної діяльності, а також проаналізовано загрози інформаційній безпеці та технічні канали витоку інформації.

- Розглянуто методи та засоби ідентифікації та автентифікації користувачів під час доступу до інформації з обмеженим доступом.

- Розроблено та вдосконалено механізми ідентифікації та автентифікації користувачів під час доступу до інформації з обмеженим доступом.

1. У першій частині кваліфікаційної роботи було проведено аналіз загроз та визначено канали витоку технічної інформації. Було продемонстровано структуру каналів витоку технічної інформації. Було проаналізовано канали витоку технічної інформації та запропоновано їх класифікацію. Зокрема, критерії класифікації включали: тип інформаційної діяльності, принцип формування сигналів небезпеки, середовище сигналів небезпеки та методи перехоплення (ліквідації) сигналів небезпеки технічною розвідкою противника.

2. У другій частині роботи з перевірки кваліфікації було розглянуто існуючі технології ідентифікації та автентифікації. Ця стаття зосереджена на користувачах в інформаційно-комунікаційних системах. У ній досліджується зміст, характеристики застосування, переваги та недоліки ідентифікації та автентифікації користувачів у цих системах, а також переваги та недоліки криптографічної, апаратної та біометричної ідентифікації та автентифікації. У статті окреслено вимоги до процесів ідентифікації та автентифікації та методи атак, спрямовані на ці процеси.

3. У третій частині оціночної роботи окреслено етапи реалізації процесів ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах. Виділено ключові елементи цього процесу та фактори, що впливають на них: криптографія, пристрої автентифікації та біометрія користувача.

Описано алгоритми автентифікації та етапи використання криптографії в різних операційних системах. Методи автентифікації порівнюються відповідно до критеріїв ризику. Запропоновано математичні моделі для оцінки безпеки механізмів багатофакторної автентифікації для запобігання несанкціонованому доступу. Ці моделі враховують ймовірність несанкціонованого доступу до мережі та ймовірність захисту мережі від таких подій, а також дозволяють оцінити загальну безпеку на основі механізмів комбінованої та послідовної побудови, що поєднують часткові ймовірності безпеки, що забезпечуються різними факторами автентифікації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Головань С.М. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.
2. Садердинов А.А., Трайнёв В.А., Федулов А.А. Информационная безопасность предприятия/ ИТК Дашков и К. –М., 2005. —336 с.
3. www.ik.3dscorpion.com.ua
4. www.factor-ltd.by
5. Інформаційно-психологічна протидія в Національній гвардії України (психологічний аспект) [Текст] : монографія / І. В. Воробйова, Я. В. Мацегора, І. І. Приходько та ін.; за заг. ред. проф. І.І. Приходька; 2-ге вид. – Х.: Національна акад. НГУ, 2016. – 265 с.
6. Кормич Б.А. Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник для студ. вищих навч. закл. / Б.А. Кормич. –К.: Кондор, 2004. – 384 с.
7. Термінологічний довідник з питань технічного захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
8. Каторин Ю.Ф. Большая энциклопедия промышленного шпионажа / Ю.Ф.Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко. – СПб.: ООО «Издательство Полигон», 2000. – 896 с.
9. Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013. – [Second edition 2013-10-01]. – Geneva, 2013. – P. 23.
10. Information technology. Security techniques. Information security risk management: ISO/IEC 27005:2011. – [Second edition 2011-06-01]. – Geneva, 2011. – P. 68.
11. Про електронні документи та електронний документообіг: закон України від 22 травня 2003 р. № 851-IV // Урядовий кур'єр — 2003. — №119 – 2 липня. – С. 1– 6.

12. Сарбуков А. Аутентификация В Компьютерных Системах / А. Сарбуков А. Грушо // Системы безопасности. – 2003. - №5 (53). – С. 25-29.
13. Чепиков О. Особенности применения Двухфактор-Ной аутентификации / О. Чепиков // Информационная безопасность. – 2005. – №3. – С.35-41.
14. Конахович Г.Ф., Корченко О.Г., Юдін О.К., Захист інформації в мережах передачі даних: Підручник. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с., іл.
15. Шрамко В. Н. Защита компьютеров: электронные Системы идентификации и аутентификации / В. Н. Шрамко // PCWeek/RE. – 2004. - №12.
16. ГОСТ Р ИСО/МЭК 19794-6-2006. Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. – Ч. 6: Данные изображения радужной оболочки глаза. – М.: ИПК Изд-во стандартов, 2006. – 27 с.
17. Горбенко И. Д. Методы биометрической аутентификации для использования в паспортной системе / И. Д. Горбенко, И. В. Олешко // Прикладная радиоэлектроника: научно-техн. журнал. – 2011. – Том 10, № 2. – С. 255 – 258.
18. Олешко І. В. Порівняльний аналіз методів біометричної автентифікації на основі критерію відносної ентропії / І. В. Олешко // Вісник національного університету “Львівська політехніка”. – 2012. – С. 170 – 175.
19. Горбенко Ю. И. Модели и методы оценки защищенности механизмов многофакторной аутентификации / Ю. И. Горбенко, И. В. Олешко // Восточно-европейский журнал передовых технологий: научный журнал. – 2012. – № 6/2(66). – С. 4 – 10.
20. Олешко І. В. Сравнительный анализ протоколов строгой аутентификации [Текст] / И. В. Олешко, И. Д. Горбенко // Радиотехника. – 2012. – №3 – С. 198 – 210.
21. Фесьоха В.В, Фесьоха Н.О., Доброштан О.С. Аналіз існуючих рішень автентифікації користувачів інформаційних систем та мереж спеціального

призначення. Збірник наукових праць ВІТІ № 3 – 2020. С. 129-136.

22. Субач І.Ю., Фесьоха В.В., Фесьоха Н.О. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, відкритих на основі загальнодоступних ліцензій. *Information Technology and Security*. 2017. № 1. С. 29 – 41.

23. Горбенко Ю. И. Модели и методы оценки защищенности механизмов многофакторной аутентификации / Ю. И. Горбенко, И. В. Олешко // Восточно-европейский журнал передовых технологий: научный журнал. – 2012. – № 6/2(66). – С. 4 – 10.

24. Горбенко, І. Д. Прикладна криптологія. [Текст]: монографія / І. Д. Горбенко, Ю. І. Горбенко; ХНУРЕ. – Х.: Форт, 2012. - 868 с.

25. Горбенко, Ю. І. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика [Текст] / Ю. І. Горбенко, І. Д. Горбенко. – Х.: Форт, 2010. – 593 с.

26. Чепиков О. Особенности применения двухфакторной аутентификации / О. Чепиков // Информационная безопасность. – 2005. – №3. – С.35-41.

27. Кушлик-Дивульська О. І. Теорія ймовірностей та математична статистика: навч. посіб./ О. І. Кушлик-Дивульська, Н. В. Поліщук, Б. П. Орел, П. І. Штабальук. – К: НТУУ «КП», 2014. – 212 с. – Бібліогр.: с.205. – 300пр.

28. Горбенко І. Д. Метод оценки относительной энтропии и сравнительный анализ источников биометрической информации [Текст] / И. Д. Горбенко, И. В. Олешко // Прикладная радиоэлектроника: Научно-техн. журнал. - 2012. - Том 11, № 2. - С. 255-261

29. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння [Текст]. – введ. 2002 - 28 - 12. - К.: Госпотребстандарт, 2002. – 38 с.

30. ДСТУ ISO/IEC 9798-3-2002 Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 3. Механізми з використанням методу цифрового підпису [Текст]. – введ. 2005 – 09 - 2005. - К.: Госпотребстандарт,

2005. – 17 с.

31. П. Браїловський М.М., Головень СМ. та інші. - Технічний захист інформації на об'єктах

ДОДАТОК

Оформлення слайдів та роздаткового матеріалу

2

АКТУАЛЬНІСТЬ РОБОТИ

1. Лавиноподібний розвиток інформаційних технологій та систем передачі даних;
2. Розвиток технологій та методів здобування інформації та масовані спроби несанкціанованого заволодіння інформацією з обмеженим доступом;
3. Актуальність розвитку та удосконалення методів та механізмів багатофакторної автентифікації на основі нових технологій.



Мета кваліфікаційної роботи:

удосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

Об'єкт дослідження:

процес ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

Предмет дослідження:

механізми багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

3

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

1. РОЗДІЛ 1: Порядок захисту інформації на об'єктах інформаційної діяльності

2. РОЗДІЛ 2: Методи і засоби ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

3. РОЗДІЛ 3: Розробка механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

3. ВИСНОВКИ: Узагальнено одержані результати

ПЕРШИЙ РЕЗУЛЬТАТ

Порядок захисту інформації на об'єктах інформаційної діяльності

Режим доступу до інформації



ПЕРШИЙ РЕЗУЛЬТАТ

5

Критерії інформаційної безпеки :

1. **Цілісність** - властивість інформації бути захищеною від несанкціонованого знищення, модифікації;
2. **Конфіденційність** - властивість інформації бути захищеною від несанкціонованого ознайомлення;
3. **Доступність** - властивість інформації бути захищеною від несанкціонованого доступу.

Технічні канали витоку інформації:



Структура технічного каналу витоку інформації

ПЕРШИЙ РЕЗУЛЬТАТ

6

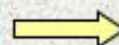
Класифікація технічних каналів витоку інформації :

1. **За видом інформаційної діяльності на ОІД**

2. **За принципом** (фізичним ефектом, процесом) формування небезпечного сигналу (носія інформації)

3. **За середовищем** поширення небезпечного сигналу

4. **За способом** перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника



1. Радіока
нал;
2. Електр
ичний;
3. Аакусти
чний;
4. Оптичн
ий;
5. Матері
ально-

ДРУГИЙ РЕЗУЛЬТАТ

7

Методи і засоби ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

ПОРЯДОК ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

Ідентифікація користувачів, ресурсів і персоналу системи ІБ

Впізнання і встановлення достовірності користувача за обліковими даними

Автентифікація - допуск до обособлених умов роботи згідно регламенту, визначеному кожному окремому користувачу

Протоколювання звертань користувачів до ресурсів, ІБ яких захищає ресурси від НСД

ДРУГИЙ РЕЗУЛЬТАТ

8

СИСТЕМА ТЕХНОЛОГІЙ АВТЕНТИФІКАЦІЇ



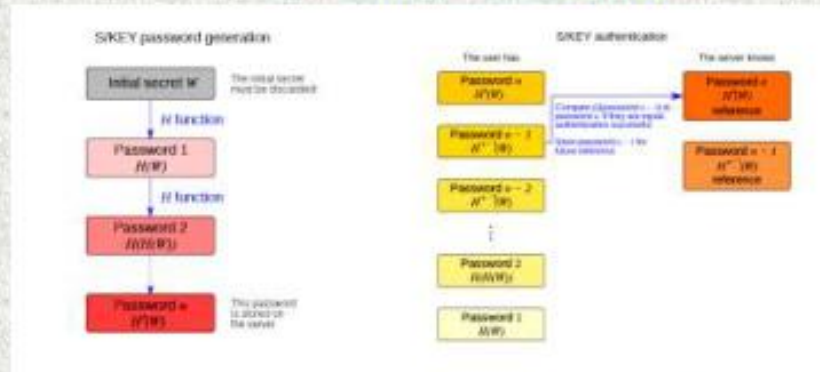
ДРУГИЙ РЕЗУЛЬТАТ

9

ЗМІСТ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

ПАРОЛЬНА:

zareєстрований користувач якої певної системи одержує набір персональних реквізитів (QR-код)



Система одноразових (а) та багаторазових (б) паролів

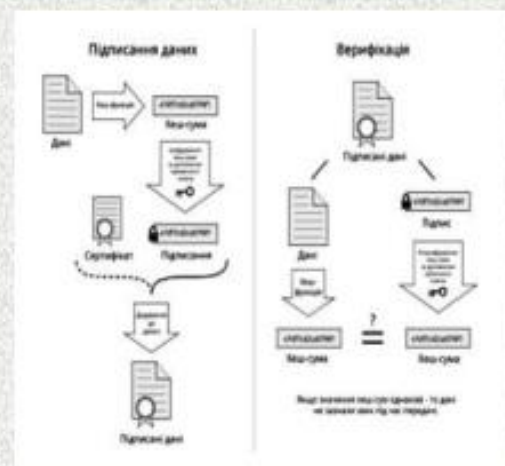
ДРУГИЙ РЕЗУЛЬТАТ

АПАРАТНА:

визначення особистості користувача по матеріальному носію (ключу), що перебуває в його ексклюзивному користуванні



Переносні токени



Цифрові підписи

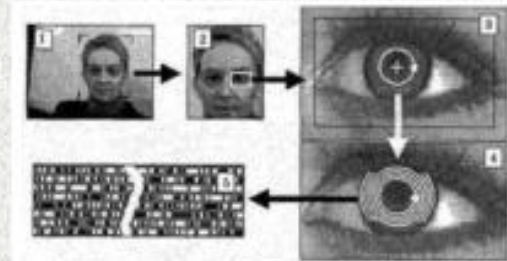
ДРУГИЙ РЕЗУЛЬТАТ

БІОМЕТРИЧНА :

визначення особистості користувача по унікальним, властивим тільки йому біологічним ознакам



Відбитки пальців



Райдужна оболонка

Динамічні методи:

- по почерку;
- по клавіатурному почерку;
- по голосу.



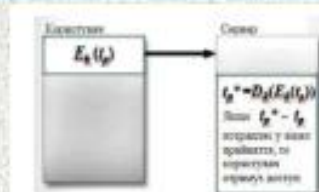
Форма обличчя

ДРУГИЙ РЕЗУЛЬТАТ

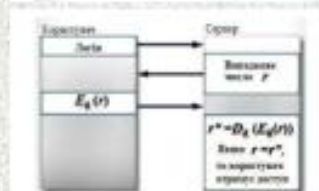
СТАНДАРТИЗАЦІЯ ПРОЦЕСІВ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

Протоколи - *ISO / IEC 9798 - Information technology – Security techniques - Entity authentication mechanisms*

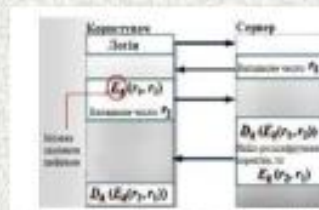
Одностороння автентифікація,
заснована на мітці часу



Одностороння автентифікація
з використанням
випадкових чисел



Взаємна автентифікація з
використанням випадкових
чисел



ДРУГИЙ РЕЗУЛЬТАТ

ВИДИ АТАК НА ПРОТОКОЛИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

1. **Самозванство (impersonation)** - один користувач намагається видати себе за іншого.
2. **Повторна передача (a replay attack)** - повторна передача колишніх аутентифікаційних даних будь-яким користувачем.
3. **Підміна боку автентифікаційного обміну (Interleaving attack)** - зломисник в ході атаки має можливість модифікувати проходить через нього трафік.
4. **Відображення передачі (reflection attack)** - один з варіантів атаки підміни, коли в рамках даного сенсу зломисник пересилає назад перехоплену інформацію.
5. **Вимушена затримка (forced delay)** - зломисник перехоплює деяку інформацію і передає її через деякий час.
6. **Атака з вибіркою тексту (chosen-text attack)** - зломисник перехоплює трафік і намагається отримати інформацію про довготривалі ключі.

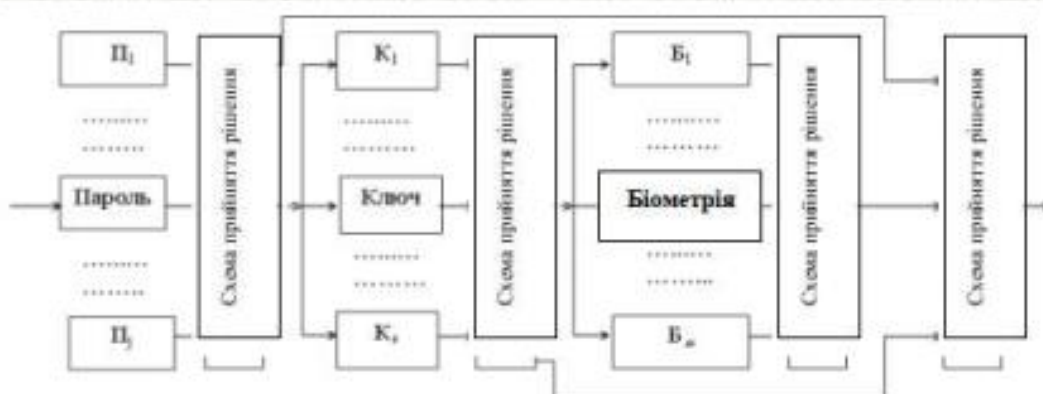
ТРЕТІЙ РЕЗУЛЬТАТ

10

Розробка механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

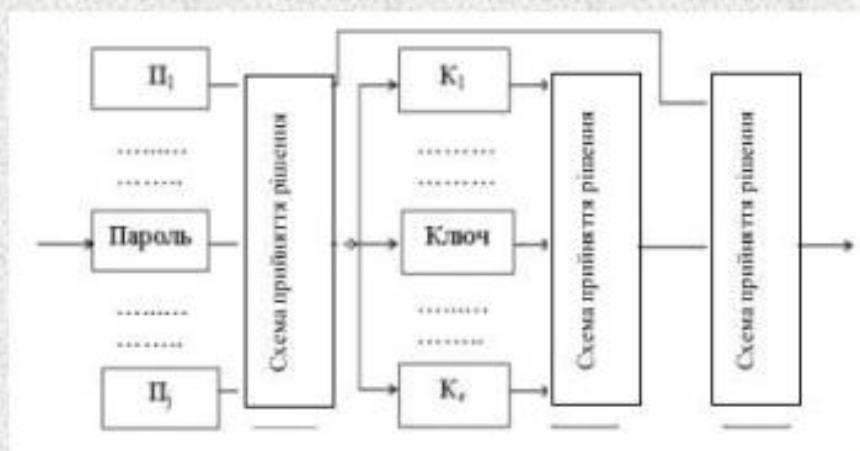
БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ

Комбінований механізм трьох факторної автентифікації
«пароль – ключ – біометрія»



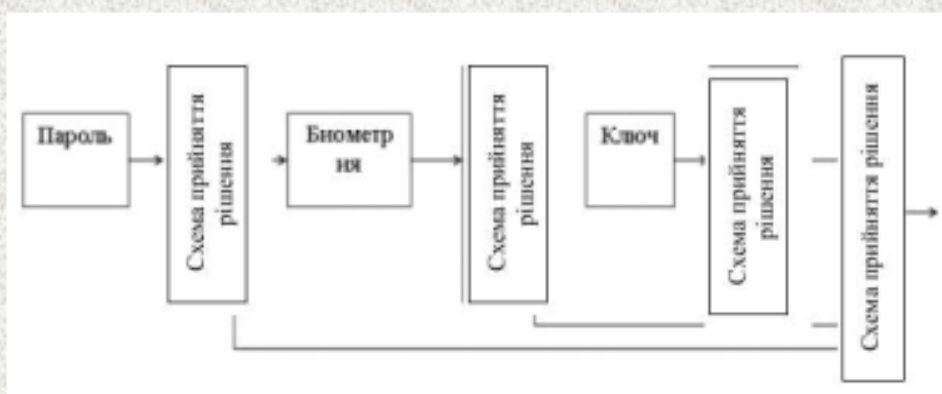
ТРЕТІЙ РЕЗУЛЬТАТ

Комбінований механізм двох факторної автентифікації «пароль – ключ»

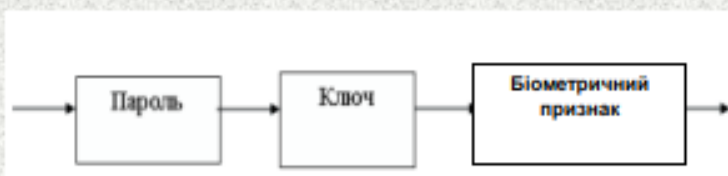


ТРЕТІЙ РЕЗУЛЬТАТ

Послідовно – паралельний механізм трифакторної автентифікації «пароль – біометрія – ключ»



Послідовне з'єднання три факторного механізму захисту від НСД



ТРЕТІЙ РЕЗУЛЬТАТ

14

ВИЗНАЧЕННЯ ЙМОВІРНІСТЕЙ НЕСАНКЦІОНОВАНОГО ДОСТУПУ: (комбінований механізм автентифікації)

Трьохфакторна ідентифікація

$$P_{НСД} = \left(1 - \prod_{i=1}^j P_i^n\right) \left(1 - \prod_{i=1}^{\varepsilon} P_i^k\right) \left(1 - \prod_{i=1}^{\mu} P_i^b\right)$$

Парольна ідентифікація

$$P_{НСД}^n = 1 - P_{зах}^n = 1 - P_1^n P_2^n \dots P_j^n = 1 - \prod_{i=1}^j P_i^n$$

Апаратна ідентифікація

$$P_{НСД}^k = 1 - P_{зах}^k = 1 - P_1^k P_2^k \dots P_{\varepsilon}^k = 1 - \prod_{i=1}^{\varepsilon} P_i^k$$

Біометрична ідентифікація

$$P_{НСД}^b = 1 - P_{зах}^b = 1 - P_1^b P_2^b \dots P_{\mu}^b = 1 - \prod_{i=1}^{\mu} P_i^b$$

ТРЕТІЙ РЕЗУЛЬТАТ

13

ЗАГАЛЬНА ЙМОВІРНІСТЬ НЕСАНКЦІОНОВАНОГО ДОСТУПУ:

$$P_{НСД} = \prod_{i=1}^j P_i^n \prod_{i=1}^{\varepsilon} P_i^k \prod_{i=1}^{\mu} P_i^b$$

$$P_{НСД}^n = 1 - P_{зах}^n$$

Співвідношення для оцінки механізмів комбінованої
двухфакторної автентифікації

Механізм пароль/ключ	$P_{НСД} = \left(1 - \prod_{i=1}^j P_i^n\right) \left(1 - \prod_{i=1}^{\varepsilon} P_i^k\right)$	$P_{зах} = \left(\prod_{i=1}^{\varepsilon} P_i^k\right) \left(\prod_{i=1}^{\mu} P_i^b\right)$
Механізм пароль/біометрія	$P_{НСД} = \left(1 - \prod_{i=1}^j P_i^n\right) \left(1 - \prod_{i=1}^{\mu} P_i^b\right)$	$P_{зах} = \left(\prod_{i=1}^j P_i^n\right) \left(\prod_{i=1}^{\varepsilon} P_i^k\right)$
Механізм ключ/біометрія	$P_{НСД} = \left(1 - \prod_{i=1}^{\varepsilon} P_i^k\right) \left(1 - \prod_{i=1}^{\mu} P_i^b\right)$	$P_{зах} = \left(\prod_{i=1}^j P_i^n\right) \left(\prod_{i=1}^{\varepsilon} P_i^k\right)$

ТРЕТІЙ РЕЗУЛЬТАТ

14

ВИЗНАЧЕННЯ ЙМОВІРНІСТЕЙ НЕСАНКЦІОНОВАНОГО ДОСТУПУ: (послідовний механізм автентифікації)

Загальна ймовірність
несанкціонованого доступу $P_{\text{зах}} = 1 - P_{\text{НСД}} = 1 - (1 - P_n)(1 - P_k)(1 - P_b)$

Співвідношення для оцінки механізмів послідовної
двухфакторної автентифікації

Механізм пароль/ключ	$P_{\text{НСД}} = (-P_n)(-P_k)$	$P_{\text{зах}} = 1 - (-P_n)(-P_k)$
Механізм пароль/біометрія	$P_{\text{НСД}} = (-P_n)(-P_b)$	$P_{\text{зах}} = 1 - (-P_n)(-P_b)$
Механізм ключ/біометрія	$P_{\text{НСД}} = (-P_k)(-P_b)$	$P_{\text{зах}} = 1 - (-P_k)(-P_b)$

ВИСНОВКИ:

16

**У процесі підготовки кваліфікаційної роботи були
виконані наступні задачі:**

1. Визначено порядок розподілу інформації на об'єкті інформаційної діяльності, проведено аналіз загроз інформаційній безпеці та аналіз технічних каналів витоку інформації на об'єкті інформаційної діяльності.
2. Проведено методів і засобів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.
3. Розроблено та вдосконалено механізми багатфакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

ДЯКУЮ ЗА УВАГУ!