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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Розробка системи захищеного допуску користувачів до роботи з інформацією з обмеженим доступом на об’єкті інформаційної діяльності»

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
_____ Оксана МАТВІЙЧУК

Виконав: здобувач вищої освіти групи СЗДМ 61
Оксана МАТВІЙЧУК

Керівник: ТУРОВСЬКИЙ Олександр
д.т.н., професор (ПРІЗВИЩЕ, Ім’я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім’я)

Київ 2025

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

Кафедра Технічних систем кіберзахисту
Ступінь вищої освіти магістр
Спеціальність 125-Кібербезпека та захист інформації
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Матвійчук Оксанаі Вікторівні
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Розробка системи захищеного допуску користувачів до роботи з інформацією з обмеженим доступом на об'єкті інформаційної діяльності»
керівник кваліфікаційної роботи ТУРОВСЬКИЙ Олександр, д.т.н., професор
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «____» _____ 2025 р. №_____

2. Строк подання кваліфікаційної роботи 20.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: об'єкті 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. Провести аналіз порядку розподілу інформації на об'єкті інформаційної діяльності, загрози інформаційній безпеці та аналіз технічних каналів витоку інформації на об'єкті інформаційної діяльності;
4.2. Проаналізувати методи і способи застосування засобів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом;
4.3. Розробити практичні рекомендацій що до вдосконалення механізмів 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 15.10.2024

КАЛЕНДАРНИЙ ПЛАН

/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
	Підбір науково-технічної літератури		
	Написання першого розділу роботи		
	Написання другого розділу роботи		
	Написання третього розділу роботи		
	Написання висновків по роботі		
	Підготовка демонстраційних матеріалів		
	Підготовка доповіді		

Здобувач вищої освіти _____ Оксана МАТВІЙЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олександр ТУРОВСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 71 сторінок, має 19 рисунків, 5 таблиць. Список використаних джерел містить 31 найменування і займає 4 сторінки.

Метою кваліфікаційної роботи є удосконалення механізмів допуску користувачів 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.

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.

Апробація:

О.В. Матвійчук, В.М. Савченко. Побудова та принципи функціонування системи захищеного допуску користувачів до роботи з інформацією з обмеженим доступом. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-комунікаційних систем*. м. Київ, 05-06 листопада 025 року, Київ: РВЦ ДУІКТ. – 2025. С.31-32. h 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.

Object of research the process of user identification and authentication when accessing and working with restricted information.

Subject of research mechanisms of user identification and authentication when accessing and working with restricted information.

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

ЗМІСТ

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 суспільного розвитку захист інформації суб'єктами інформаційної діяльності є одним із найактуальніших питань не лише в Україні, а й у всьому світі. Одним із аспектів вирішення цієї проблеми є організація та впровадження багатофакторної автентифікації та ідентифікації під час доступу користувачів до інформації з обмеженим доступом.

Це, у свою чергу, вимагає відповідних досліджень та, на їх основі, удосконалення методів та механізмів багатофакторної автентифікації та ідентифікації.

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 найважливішим компонентом 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 цілей інформаційної діяльності до зловмисників через різні фізичні канали [6,7].

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

- Радіоканали;
- Канали електричних сигналів;
- Канали акустичних сигналів;
- Канали оптичних сигналів;
- Фізичні канали сигналів [7].

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

- Джерела небезпечних сигналів включають компоненти, вузли та провідники виробничого та охоронно-технічного обладнання, а також радіо- та електронне обладнання;
- За певних умов кожне джерело небезпечного сигналу може утворювати канал витку технічної інформації;

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

- Ефект мікрофона;
- 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].

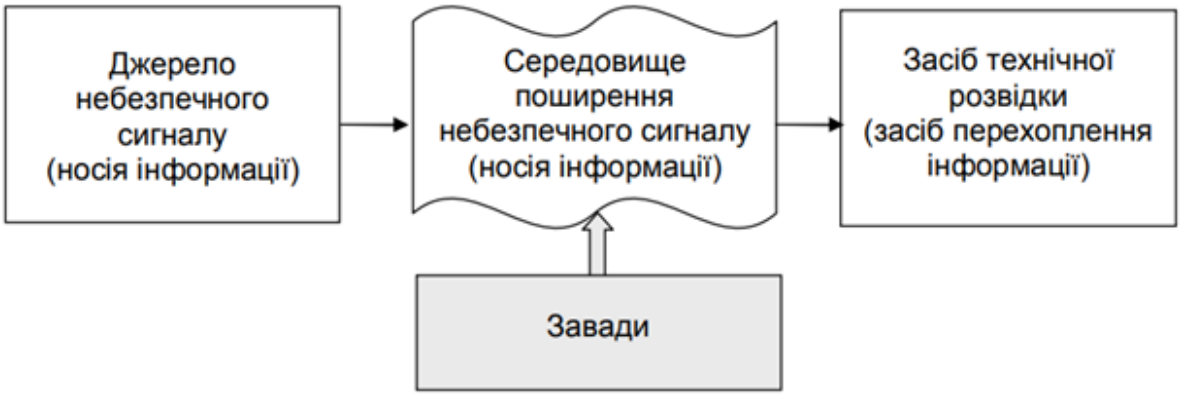


Рис. 1.2 Функціональна схема каналів технічного витоку інформації

1.2. Аналіз технічних каналів витоку інформації

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 - 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 по першому 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 проведено аналіз загроз, визначено канали витоку технічної інформації та продемонстровано структуру цих каналів.

3. 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
СИСТЕМА АВТОРИЗАЦІЇ КОРИСТУВАЧІВ ДЛЯ ДОСТУПУ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

2.1 Порядок авторизації користувачів в інформаційно-комунікаційних мережах обмеженого доступу

Через широке використання комп'ютерних технологій захист інформаційної діяльності в інформаційно-комунікаційних мережах (ІКМ) набуває все більшого значення.

Тому теоретична розробка захисту комп'ютерної інформації та його практичне застосування в конкретних комп'ютерних системах мають велике значення. Метою захисту інформації комп'ютерних систем є ізоляція нормально функціонуючих інформаційних систем та запобігання несанкціонованим адміністративним операціям та доступу до захищених комп'ютерних даних третіх осіб або програм. Створення 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 основі цього розроблена концепція інформаційної безпеки (ІБ). Методи та системи захисту інформації на основі контролю доступу в інформаційно-комунікаційних системах (ІКС) включають такі функції захисту інформації [8,9,10,11]:

– Ідентифікація користувачів, ресурсів та персоналу в інформаційній системі;

– Ідентифікація та підтвердження особи користувача на основі введених ним облікових даних (більшість моделей інформаційних систем працюють на основі цього принципу);

– Дозвіл доступу до певних умов роботи відповідно до правил, встановлених для кожного користувача. Ці правила, визначені заходами захисту інформації, складають основу інформаційної безпеки для більшості типових моделей промислових систем управління (ІСУ);

– Реєструючи доступ користувачів до ресурсів, інформаційні системи захищають ресурси від незахищеного доступу (НЗД) та контролюють неправомірні дії користувачів.

Тому системи розпізнавання та автентифікації особи є ключовим елементом інфраструктури для захисту будь-якої інформаційно-комунікаційної системи від несанкціонованого доступу (НЗД). Несанкціонований доступ – це доступ, здійснений за допомогою стандартного комп’ютерного обладнання або автоматизованих систем з порушенням встановлених обмежень доступу.

Несанкціонований доступ може бути випадковим або навмисним.

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

Розпізнавання особи означає пред’явлення користувачем свого унікального ідентифікатора (символу). Завдяки автентифікації інша сторона може бути впевнена, що суб'єкт дійсно є тим, за кого він себе видає. Іноді термін «автентифікація» також використовується як синонім [7,11]. Автентифікація — це процес перевірки того, чи має користувач дозвіл на доступ до ресурсів, і користувач повинен надати ідентифікатор, який він представляє. Ці процедури (розпізнавання особи та автентифікація) нероздільні, оскільки метод верифікації визначає, яку інформацію користувач повинен надати системі для отримання доступу [7,11].

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

¶

Рис.2.1. Структура технологічних підходів до ідентифікації та автентифікації користувачів

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 Огляд методів перевірки та автентифікації ідентичності 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].

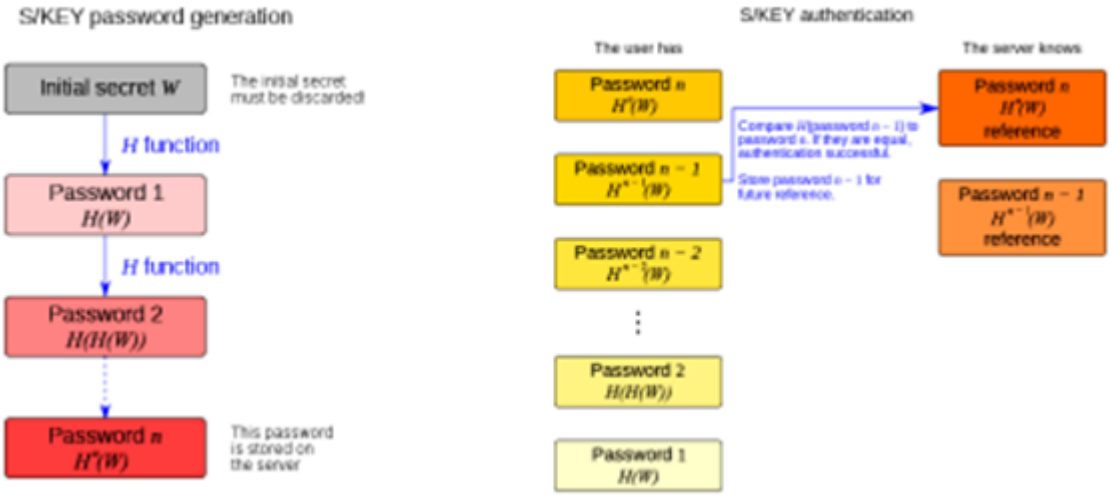


Рис.2.1Структура функціональних схем одноразових (а) та багаторазових (б) паролів

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 вкрасти;

– 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 перезапуск системи;

– 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. Ключові пристрої ідентифікації користувача - 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 стираний 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. схема формування цифрового підпису

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]:

− Сувора 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

зловмисники можуть вкрасти 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

Аналіз основних переваг і недоліків 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.
OTP-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 (OTP). 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 слабко 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 особистості людини [16].

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.

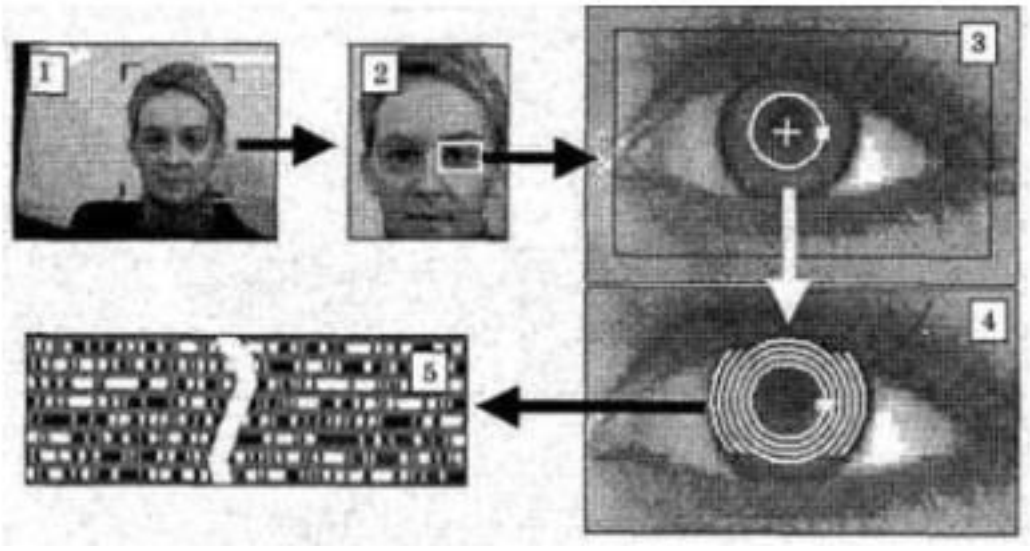


Рис. 2.6. Автентифікація за райдужною оболонкою ока

2. Розпізнавання відбитків долонь. Цей метод використовує інфрачервону камеру для зчитування інформації. Після введення інформації система генерує

цифровий код і відображає візерунки вен на руці суб'єкта під час процесу введення. Контакт між суб'єктом та скануючим пристроєм не потрібен. Цей метод може похвалитися високою надійністю та точністю.

3. Розпізнавання сітківки (Рисунок 2.6). Цей метод сканує та записує візерунки вен сітківки. Очевидно, що ці візерунки можна спостерігати лише за певних умов: під час сканування суб'єкт дивиться на віддалене джерело світла, поки спеціалізована камера сканує його сітківку, що може викликати дискомфорт. Цей метод вважається одним із найнадійніших біометричних методів.

4. Розпізнавання райдужної оболонки ока (Рисунок 2.6).

Візерунок райдужної оболонки ока кожної людини унікальний. Цей метод вимагає не лише спеціалізованої камери, але й надійного програмного забезпечення.

Зрештою, програмне забезпечення використовується для вилучення потрібних візерунків райдужної оболонки ока з зображення. Цей метод наразі є одним із найточніших біометричних методів.

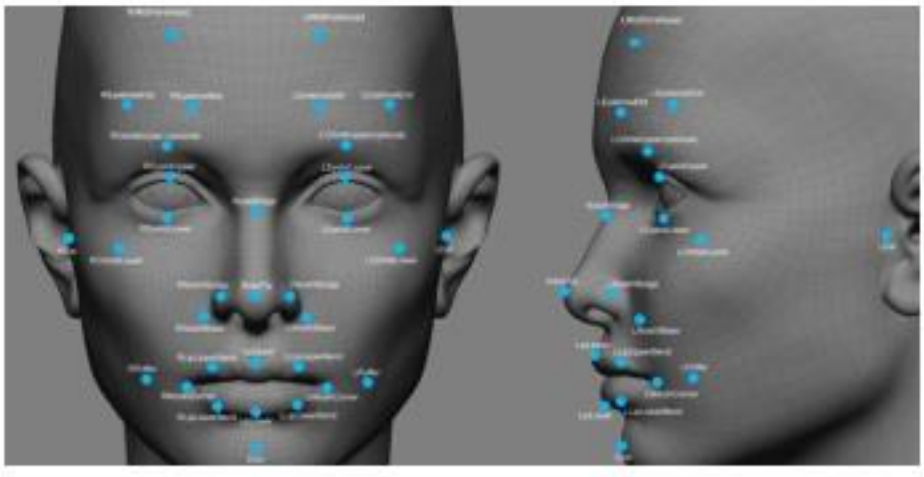


Рис. 2.7. Аутентифікація за формою обличчя

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 з'явилися лише нещодавно.

У системі, що обговорюється в цій статті, для визначення особи користувача використовується лише один фактор. Однак надійність цього методу все ще потребує покращення.

В останні роки широкого поширення набула складна або багатофакторна автентифікація.

2.3 Вимоги та процедури розпізнавання та автентифікації особи

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 запитувач і верифікатор мають симетричний ключ або попарно вибірковий ключ зв'язку. Ці ключі можна отримати в режимі реального часу за допомогою довіреного сервера.

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

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

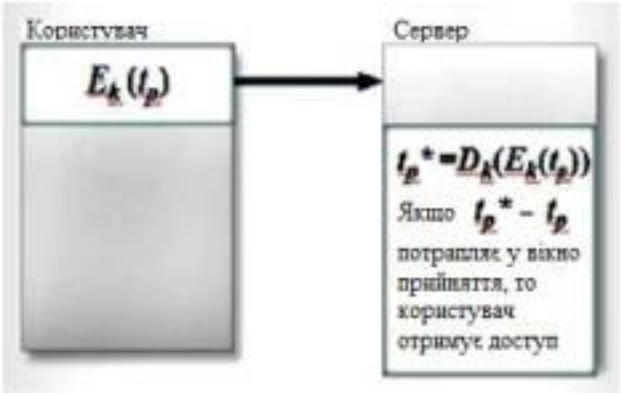


Рис. 2.9. Одностороння автентифікація, заснована на мітці часу

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.

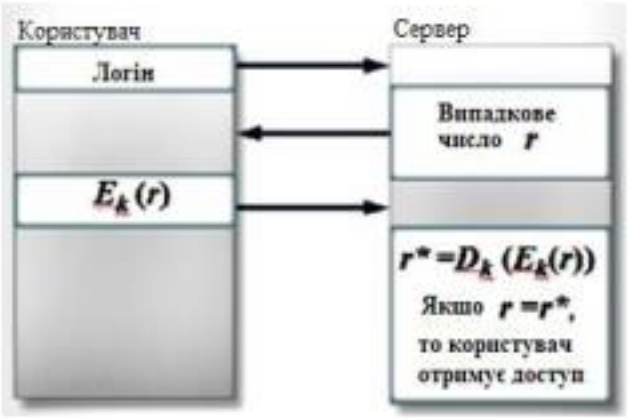


Рис. 2.10. Технологія односторонньої автентифікації з використанням випадкових чисел

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 рукостискання. 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.

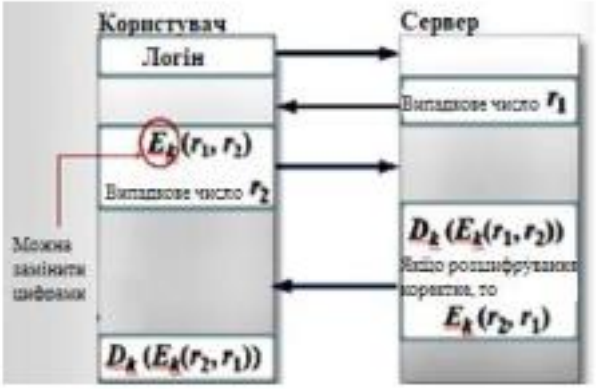


Рис. 2.11. Зустрічна автентифікація з використанням випадкових чисел

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.

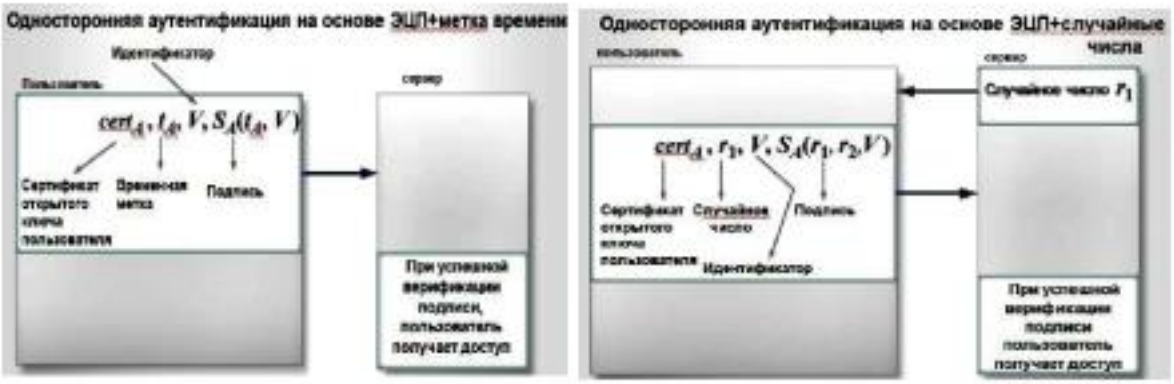


Рис. 2.12. Протоколи з використанням схем-цифрового підпису

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 невиправлені 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. Протоколи 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 – зловмисник перехоплює комунікаційний трафік, намагаючись отримати інформацію про довгострокові ключі.

Атаки на протоколи автентифікації та контрзаходи

Таблиця 2.2

Практична реалізації 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 цього 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
МЕХАНІЗМИ АВТОРИЗАЦІЇ КОРИСТУВАЧІВ ДЛЯ ДОСТУПУ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

3.1 Порядок реалізації механізмів ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах

У системі автентифікації зазвичай можна виділити кілька елементів [16,19,23]:

- Суб'єкт, який підлягає автентифікації;

- Характеристики суб'єкта — його унікальні особливості;

- Особа, відповідальна за систему автентифікації, яка відповідає за контроль її роботи;

- Механізм автентифікації, тобто принцип роботи системи;

- Механізм надання або скасування певних дозволів на доступ для суб'єкта.

Задовго до появи комп'ютерів люди використовували різні унікальні особливості суб'єктів. Зараз тип функції, що використовується в 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, кодовими замками або персональними ідентифікаційними номерами (PIN).

Механізми паролів легко впроваджувати та є недорогими. Однак, вони також мають суттєві недоліки: конфіденційність паролів часто є складною проблемою, і зловмисники постійно розробляють нові методи крадіжки, злому та підбору паролів (див. "Криптографія бандитів").

2. Ще один метод, який ми маємо, – це пристрої автентифікації. У цьому випадку вирішальним є той факт, що суб'єкт володіє якимось унікальним предметом. 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 отримати такі пристрої набагато складніше, ніж зламати паролі, 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. Частина нас самих – біометрія.

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

Багатофакторна автентифікація. Один із методів автентифікації комп'ютерної системи передбачає введення ідентифікатора користувача (зазвичай відомого як «ім'я користувача») та пароля (деяка конфіденційна інформація) [24,25]. Дійсні (довідкові) пари логін-пароль 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 еталонними даними;

- Якщо дані збігаються з еталонними 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);

- За допомогою шифрування або односторонньої хеш-функції;

У цьому випадку унікальні дані, введені користувачем, передаються мережею безпечно. Для максимальної безпеки під час зберігання та передачі пароля слід використовувати односторонню функцію. Як правило, для цих цілей використовуються криптографічно стійкі хеш-функції. У цьому випадку на сервері зберігається лише зображення пароля. Після того, як система отримає пароль та хешує його, вона порівнює результат із еталонним зображенням, що зберігається в ньому. Якщо вони однакові, пароль збігається. Зловмиснику, який отримав зображення, практично неможливо самостійно обчислити пароль. Використання кількох паролів має кілька суттєвих недоліків. По-перше, сам еталонний пароль або його хеш-образ зберігається на сервері автентифікації. У більшості випадків пароль зберігається в системних файлах без шифрування.

Як тільки зловмисник отримує доступ до цих файлів, він може легко отримати конфіденційну інформацію. По-друге, користувачі змушені запам'ятовувати (або записувати) кілька паролів. Зловмисники можуть отримати цю інформацію, використовуючи лише методи соціальної інженерії, без будь-яких технічних засобів. Крім того, безпека системи значно знижується, якщо користувачі самі вибирають паролі. У більшості випадків користувачі вибирають слово або комбінацію слів, що існує в словнику. Маючи достатньо часу, зловмисники можуть зламати пароль за допомогою простих атак методом перебору. Рішення цієї проблеми включають використання випадкових паролів або обмеження терміну дії паролів користувачів, після якого пароль необхідно змінити.

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

може читати 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 робило його дуже небезпечним [24,25]. На комп'ютерах з операційними системами 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 цією базою даних є Active Directory. Якщо необхідно забезпечити роботу співробітників на різних комп'ютерах,Комп'ютери (оснащені системою безпеки) використовують апаратні та програмні системи, які дозволяють зберігати дані автентифікації та ключі шифрування на серверах організації. Користувачі можуть вільно працювати на будь-якому комп'ютері (робочій станції) та отримувати доступ до своїх даних автентифікації та ключів шифрування [24,25].

Після того, як зловмисник отримає багатоцільовий пароль користувача, він може отримати постійний доступ до викраденої конфіденційної інформації. Цю проблему можна вирішити за допомогою одноразових паролів (OTP).

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 користувача, так і для системи.

- Використання позначок часу та одноразової системи.

- Використання бази даних випадкових паролів, унікальної як для користувача, так і для системи.

Перший метод використовує генератор псевдовипадкових чисел, який використовує однакове значення як для суб'єкта, так і для системи. Пароль, згенерований суб'єктом, може передаватися до системи послідовно за допомогою односторонньої функції або ж він може передаватися з кожним новим запитом на основі унікальної інформації з попереднього запиту.

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

Автентифікація на основі генерації випадкових чисел через певні інтервали часу має такий 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, і на апаратному пристрої відображається випадкове число. Система порівнює введений PIN-код з ключем суб'єкта у своїй базі даних і генерує випадкове число на основі параметрів ключа та поточного часу. Далі система перевіряє, чи збігається згенероване число з числом, введеним суб'єктом [20,21,25].

Третій метод базується на єдиній базі даних паролів, що використовується користувачем і системою, що забезпечує високоточну синхронізацію між ними. У цьому випадку кожен пароль у наборі паролів можна використовувати лише один раз. Тому, навіть якщо зловмисник перехопить пароль, який використовує користувач, цей пароль буде недійсним. Одноразові паролі забезпечують вищу безпеку порівняно з використанням кількох паролів.

В останні роки все ширше використовується так звана технологія розширеної або багатофакторної автентифікації. Вона базується на комбінованому використанні кількох факторів автентифікації, що значно покращує безпеку системи. Наприклад, типовим прикладом є використання SIM-картки в мобільному телефоні.

Після ввімкнення користувач вставляє картку (пристрій автентифікації) в телефон і вводить PIN-код (пароль). Крім того, деякі сучасні ноутбуки оснащені сканерами відбитків пальців. Тому під час входу в систему користувач повинен

спочатку виконати біометричну автентифікацію, перш ніж вводити пароль [18,24,25].

Вибираючи конкретні фактори або методи автентифікації для системи, необхідно враховувати необхідну безпеку, складність системи та забезпечення мобільності користувача.

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

Таблиця 3.1

Оцінка методів автентифікації по критерію ризику

Рівень ризику	Вимоги до системи	Технологія аутентифікації	Приклади застосування
Низький	Потрібно здійснити аутентифікацію для доступу до системи, причому крадіжка, злом, розголошення конфіденційної інформації не матиме значних наслідків	Рекомендується мінімальна вимога використання багаторазових паролів	Реєстрація на порталі в мережі Інтернет
Середній	Потрібно здійснити аутенифікацію 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 аутентифікацію для доступу до системи, причому крадіжка, лом, розголошення конфіденційної інформації завдасть значної шкоди	Рекомендується мінімальна вимога - використання багатофакторної аутентифікації	Проведення великий міжбанківськ их операцій керівним апаратом

3.2 Модель оцінки безпеки механізмів багатофакторної автентифікації (запобігання несанкціонованому доступу)

Ми розглядаємо модель оцінки безпеки механізмів багатофакторної 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 багатофакторної автентифікації є простим.

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

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

Де:

P_i^n – ймовірність точної роботи механізму паролювання;

P_i^k – ймовірність точної застосування механізму особистого ключа;

P_i^k – ймовірність точної 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

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

Визначимо ймовірність правильної роботи механізму автентифації $P^n_{зах}$. Це буде спостерігатись, якщо ні по одному каналу введення паролю не буде спостерігатися НСД. Тоді, згідно (3.3) [23,25, 27]:

$$P^n_{НСД} = 1 - P^n_{зах} = 1 - P^n_1 P^n_2 \cdots P^n_j = 1 - \prod_{i=1}^{j} P^n_i \tag{3.4}$$

Де $P^n_1, P^n_2 \ldots P^n_j$ 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]:

$$P^k_{НСД} = 1 - P^k_{зах} = 1 - P^k_1 P^k_2 \cdots P^k_\varepsilon = 1 - \prod_{i=1}^{\varepsilon} P^k_i \tag{3.5}$$

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

$$P^b_{НСД} = 1 - P^b_{зах} = 1 - P^b_1 P^b_2 \cdots P^b_\varepsilon = 1 - \prod_{i=1}^{\mu} P^b_i \tag{3.6}$$

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

$$P_{НСД} = \prod_{i=1}^{j} P^n_i \prod_{i=1}^{\varepsilon} P^k_i \prod_{i=1}^{\mu} P^b_i \tag{3.7}$$

Практичне значення також мають окремі випадки, коли застосовується два або один з трьох факторів а автентифікації.

У Табл. 2 наведені окремі випадки моделей оцінки для трьох варіантів двофакторних механізмів [23,25,28].

Ймовірність НСД в послідовній моделі необхідно визначати по теоремі перемноження ймовірностей. Для цього випадку ймовірність добутку декількох незалежних подій рівні добутку ймовірності цих подій.

Що визначається виразом [23,27]:

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

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 $P_{НСД}^n$ ($P_{Зах}^n$) механізмів комбінованої двухфакторної автентифікації

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

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

$$P_{Зах} = 1 - P_{НСД} = 1 - (1 - P_n)(1 - P_k)(1 - P_b) \qquad (3.9)$$

Також важливе значення мають певні випадки, коли застосовується один чи два фактора автентифікації.

В Табл.3.3 подано окремі випадки моделей оцінки для трьох варіантів двухфакторних механізмів автентифікації. Використавши подані співвідношення можна оцінити $P^n_{НСД}$ ($P^n_{Зах}$) механізмів послідовної двухфакторної автентифікації [23,26, 28].

В Табл.3.2 і 3.3 подані аналітичні співвідношення, які можна використовувати при оцінці захищеності від НСД в випадку паралельного чи послідовного застосування одного фактору автентифікації.

Таблиця 3.3.

Співвідношення для оцінки $P^n_{НСД}$ ($P^n_{Зах}$) механізмів послідовної двухфакторної автентифікації

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

Тому було запропоновано математичні моделі для оцінки механізмів багатофакторної автентифікації, які можна використовувати для оцінки ймовірності реалізації NSD на основі комбінаційних 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 третьому 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.

У цьому розділі порівнюються методи автентифікації на основі критеріїв ризику.

2. У цьому розділі запропоновано математичні моделі для оцінки безпеки механізмів багатофакторної автентифікації від несанкціонованого доступу.

Ці моделі враховують ймовірність несанкціонованого доступу до мережі та ймовірність захисту мережі від такого доступу, а також дозволяють оцінити загальну безпеку на основі комбінаційного та послідовного механізму побудови, який включає часткові ймовірності безпеки, що забезпечуються різними факторами автентифікації.

ВИСНОВКИ

Під час підготовки до кваліфікаційного огляду було виконано такі завдання:

– Визначено процес розподілу інформації об'єкта інформаційної діяльності, проаналізовано загрози інформаційній безпеці та проаналізовано технічні канали витоку інформації об'єкта інформаційної діяльності.

– Розглянуто методи ідентифікації та автентифікації користувачів та засоби доступу до інформації з обмеженим доступом.

– Розроблено та вдосконалено механізми ідентифікації та автентифікації користувачів для доступу до інформації з обмеженим доступом.

1. У першій частині кваліфікаційного огляду було проведено аналіз загроз, виявлено канали витоку технічної інформації та продемонстровано структуру цих каналів. Було проаналізовано та класифіковано канали витоку технічної інформації. Зокрема, це включало: розподіл за типом інформаційної діяльності, принцип формування сигналів небезпеки, середовище сигналів небезпеки та методи перехоплення (ліквідації) сигналів небезпеки за допомогою технічної розвідки противника.

2. У другій частині кваліфікаційного огляду було розглянуто існуючі технології ідентифікації та автентифікації користувачів в інформаційно-комунікаційних системах об'єкта інформаційної діяльності. У цій статті розглядається зміст, характеристики застосування, переваги та недоліки ідентифікації та автентифікації користувачів в інформаційно-комунікаційних системах, а також переваги та недоліки криптографічної, апаратної та біометричної ідентифікації та автентифікації. У статті описано вимоги до процесів ідентифікації та автентифікації, а також зміст атак, спрямованих на ці процеси.

3. У третій частині цього дослідження окреслено етапи впровадження процесів ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах. У ній виділено ключові елементи цього процесу та

фактори, що впливають на них: криптографія, пристрої автентифікації та біометрія користувача. У статті описано алгоритми автентифікації та етапи використання криптографії в різних операційних системах. Крім того, порівнюються методи автентифікації на основі критеріїв ризику. Запропоновано математичні моделі для оцінки безпеки механізмів багатофакторної автентифікації від несанкціонованого доступу. Ці моделі враховують ймовірність несанкціонованого доступу до мережі та ймовірність захисту мережі від таких подій, а також дозволяють оцінити загальну безпеку на основі комбінаційних та послідовних механізмів 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 И. 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. Штабалюк. – К: НТУУ «КПІ», 2014. – 212 с. − Бібліогр.: с.205. − 300пр.

28. Горбенко И. 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. Браіловський 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

4

ПЕРШИЙ РЕЗУЛЬТАТ

Порядок захисту інформації на об'єктах інформаційної діяльності

Режим доступу до інформації

5

ПЕРШИЙ РЕЗУЛЬТАТ

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

6

ПЕРШИЙ РЕЗУЛЬТАТ

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. Радіоканал;
2. Електричний;
3. Аакустичний;
4. Оптичний;
5. Матеріально-

7

ДРУГИЙ РЕЗУЛЬТАТ

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

ПОРЯДОК ІНДЕНТИФІКАЦІЇ 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

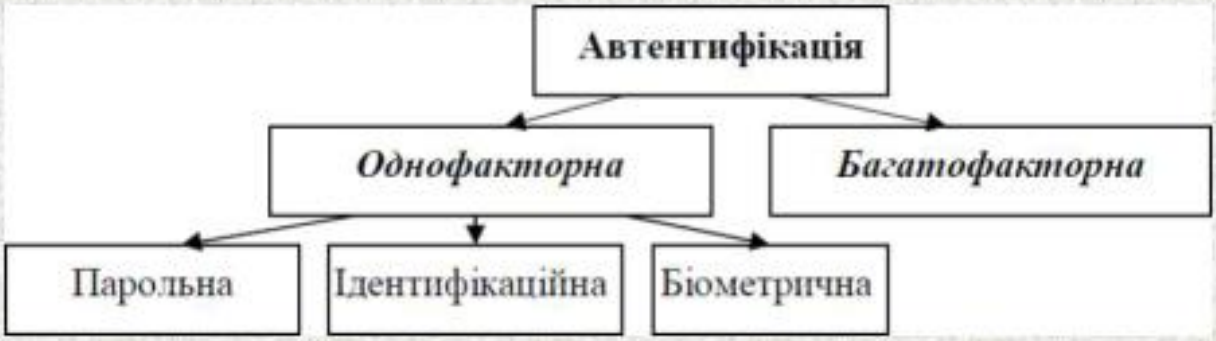
⇩

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

8

ДРУГИЙ РЕЗУЛЬТАТ

СИСТЕМА ТЕХНОЛОГІЙ АВТЕНТИФІКАЦІЇ

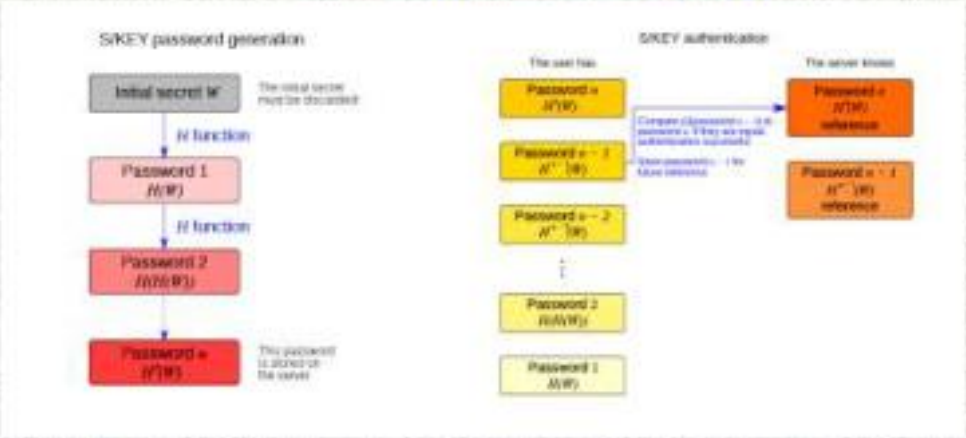


9

ДРУГИЙ РЕЗУЛЬТАТ

ЗМІСТ ІНДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

ПАРОЛЬНА:
зареєстрований 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

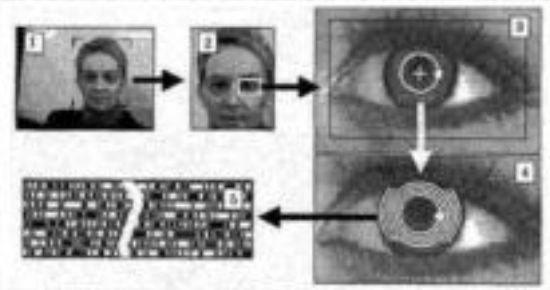
Переносні токени

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.

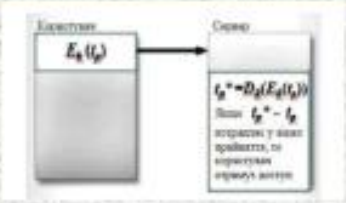
Форма обличчя

ДРУГИЙ РЕЗУЛЬТАТ

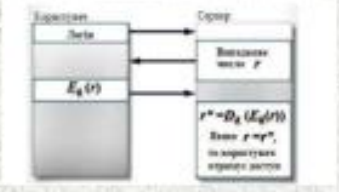
СТАНДАРТИЗАЦІЯ ПРОЦЕСІВ ІНДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

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

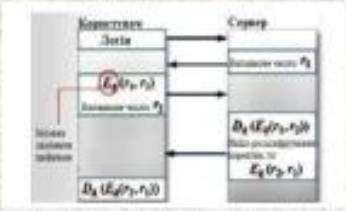
Одностороння автентифікація, заснована на мітці часу



Одностороння автентифікація з використанням випадкових чисел



Взаємна автентифікація з використанням випадкових чисел



ДРУГИЙ РЕЗУЛЬТАТ

ВИДИ АТАК НА ПРОТОКОЛИ ІНДЕНТИФІКАЦІЇ 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)** - зловмисник 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 зловмисник пересилає назад перехоплену інформацію.
5. **Вимушена затримка (forced delay)** - зловмисник перехоплює деяку інформацію і передає її через деякий час.
6. **Атака з вибіркою тексту (chosen-text attack)** - зловмисник перехоплює трафік і намагається отримати інформацію про довготривалі ключі.

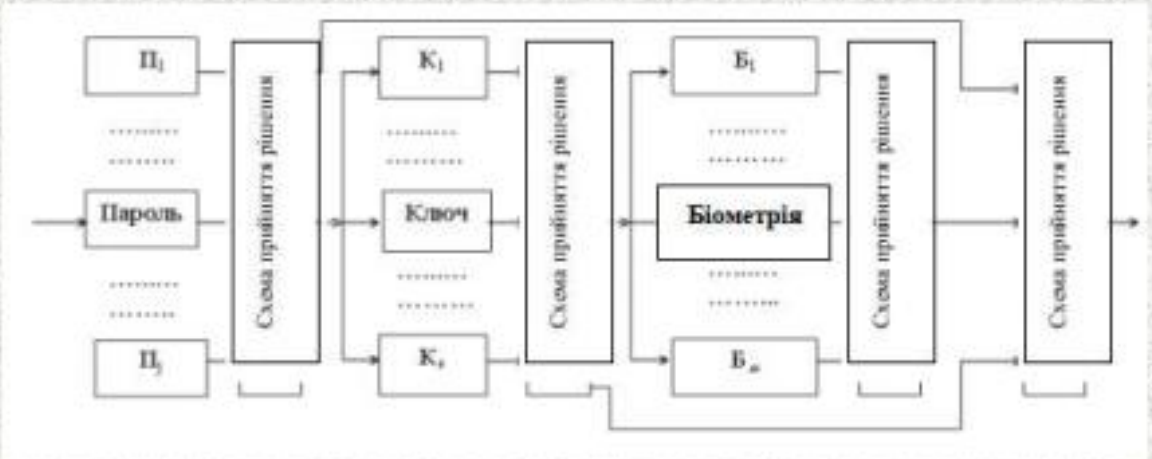
10

ТРЕТІЙ РЕЗУЛЬТАТ

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

БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ

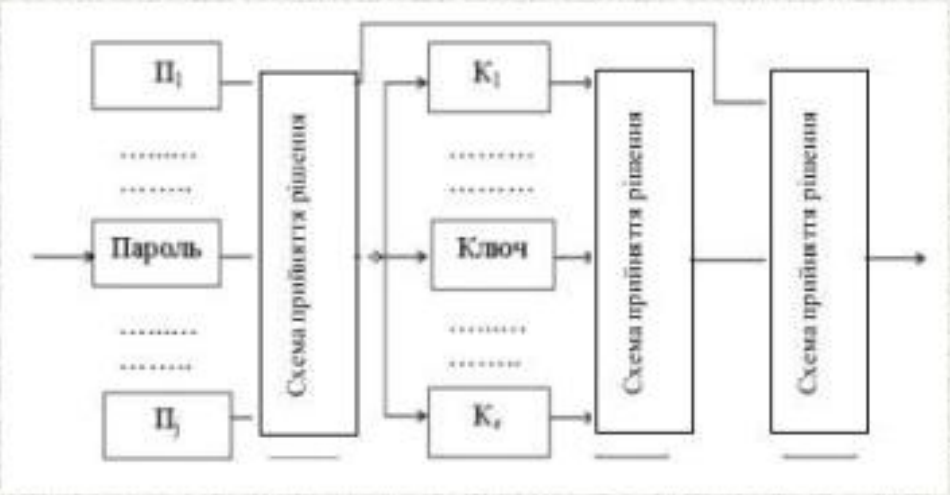
Комбінований механізм трьох факторної автентифікації «пароль – ключ – біометрія»



11

ТРЕТІЙ РЕЗУЛЬТАТ

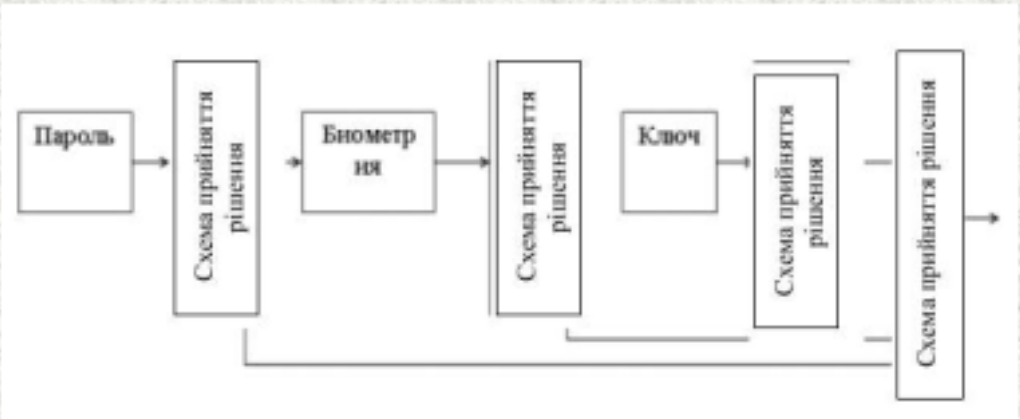
Комбінований механізм двох факторної автентифікації «пароль – ключ»



12

ТРЕТІЙ РЕЗУЛЬТАТ

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



Послідовне з'єднання три факторного механізму захисту від НСД

14

ТРЕТІЙ РЕЗУЛЬТАТ

ВИЗНАЧЕННЯ ЙМОВІРНІСТЕЙ НЕСАНКЦІОНОВАНОГО ДОСТУПУ:

(комбінований механіз автентифікації)

Трьохфакторна індетифікація

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

Парольна індетифікація

$$P^n_{НСД}=1-P^n_{Зах}=1-P_1^nP_2^n\cdots P_j^n=1-\prod_{i=1}^{j}P_i^n$$

Апараптна індетифікація

$$P^k_{НСД}=1-P^k_{Зах}=1-P_1^kP_2^k\cdots P_\varepsilon^k=1-\prod_{i=1}^{\varepsilon}P_i^k$$

Біометрична індетифікація

$$P^b_{НСД}=1-P^b_{Зах}=1-P_1^bP_2^b\cdots P_\varepsilon^b=1-\prod_{i=1}^{\mu}P_i^b$$

13

ТРЕТІЙ РЕЗУЛЬТАТ

ЗАГАЛЬНА ЙМОВІРНІСТЬ НЕСАНКЦІОНОВАНОГО ДОСТУПУ:

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

$$P^n_{НСД}=1-P^n_{Зах}$$

Співвідношення для оцінки механізмів комбінованої двухфакторної автентифікації

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

14

ТРЕТІЙ РЕЗУЛЬТАТ

ВИЗНАЧЕННЯ ЙМОВІРНІСТЕЙ НЕСАНКЦІОНОВАНОГО ДОСТУПУ:

(послідовний механіз автентифікації)

Загальна ймовірність несанкціонованого доступу $P_{Зах} = 1 - P_{НСД} = 1 - (1 - P_п)(1 - P_к)(1 - P_б)$

Співвідношення для оцінки механізмів послідовної двухфакторної автентифікації

Механізм пароль/ключ	$P_{НСД} = (-P_п)(-P_к)$	$P_{Зах} = 1-(-P_п)(-P_к)$
Механізм пароль/біометрія	$P_{НСД} = (-P_п)(-P_б)$	$P_{Зах} = 1-(-P_п)(-P_б)$
Механізм ключ/біометрія	$P_{НСД} = (-P_к)(-P_б)$	$P_{Зах} = 1-(-P_к)(-P_б)$

16

ВИСНОВКИ:

У процесі підготовки кваліфікаційної роботи були виконані наступні завдання:

– 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 огляд 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

АПРОБАЦІЯ:

О.О. Панасюк, В.О. Марченко, Р.В. Скоробагатько. **Технології ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.** *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.83-84.

ДЯКУЮ ЗА УВАГУ !