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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захищеного доступу до конфіденційної інформації методами багатофакторної автентифікації користувачі»

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
_____ Владислав ДУДНИК

Виконав: здобувач вищої освіти групи СЗДМ 61
Владислав ДУДНИК

Керівник: ГАВРИЛЕНКО Олексій .
к.т.н. (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 ТСК
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дуднику Владиславу Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система захищеного доступу до конфіденційної інформації методами багатофакторної

керівник кваліфікаційної роботи ГАВРИЛЕНКО Олексій, к.т.н. .

затверджені наказом Державного університету інформаційно-комунікаційних технологій
від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 20.12.2024 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. Огляд процесів захисту інформації на об'єктах інформаційної діяльності
4.2. Аналіз методів і засобів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом
4.3. Розробка та удосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом

5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах.

6. Дата видачі завдання _____20.10.2024 ___

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 _____ Владислав ДУДНИК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олексій ГАВРИЛЕНКО .

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 69 сторінок, має 19 рисунків, 5 таблиць. Список використаних джерел містить 31 найменування і займає 4 сторінки.

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

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

Об'єкт дослідження. Процес санкціонованого доступу користувачів 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.О. Панасюк, В.О. Марченко, **В.С. Дудник.** 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. https://duikt.edu.ua/uploads/p_2661_93669247.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, mechanisms for multi-factor identification and authentication of users when accessing information with limited access are developed and improved.

Object of research. The process of authorized user access to work with restricted information.

Subject of research. Mechanisms for user identification and authentication when accessing 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 розвитку суспільства, однією з найактуальніших проблем, яка є не тільки в Україні, а й в світі, полягає в захисту інформації на об’єктах інформаційної діяльності. Одним з аспектів вирішення вказаного питання є організація та здійснення багатофакторної ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

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

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

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

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

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

– Розроблено та удосконалено механізми ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

Об’єкт дослідження. Процес санкціонованого доступу користувачів 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 одним із найважливіших у загальному комплексі заходів технічного захисту інформації (ТЗІ). Несанкціоноване ознайомлення із інформацією з метою її подальшого використання є можливим шляхом перехоплення її зловмисниками [1,5,6].

Для нелегального знімання інформації використовуються різні технічні засоби. Інформація з об'єкта надходить зловмисникові по різним фізичним каналам [6,7].

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і способів перехоплення повідомлення, технічні канали витоку можна розділити на [7,8]:

- радіоканал;
- електричний;
- акустичний;
- оптичний;
- матеріально-речовий [7].

Аналіз фізичної природи численних випромінювачів показує, що [6,7]:

- джерелами небезпечного сигналу є елементи, вузли і провідники технічних засобів забезпечення виробничої та трудової діяльності, а також радіоелектронна апаратура;
- кожне джерело небезпечного сигналу за певних умов може утворити технічний канал витоку інформації;
- кожна електронна система, що містить в собі сукупність елементів, вузлів і провідників, володіє безліччю технічних каналів витоку інформації. Радіоканали витоку інформації утворюються за рахунок:

- мікрофонного ефекту;
- магнітного поля;
- паразитної генерації;
- по ланцюгах живлення;
- по ланцюгам заземлення;
- за рахунок взаємного впливу;
- електромагнітного випромінювання;
- ВЧ нав'язування;
- із волоконно-оптичних систем зв'язку.

Структура технічного каналу витоку інформації в загальному випадку включає (Рис. 1.2) джерело сигналу або передавач, середу поширення електричного струму або електромагнітної хвилі і приймач сигналу [7].

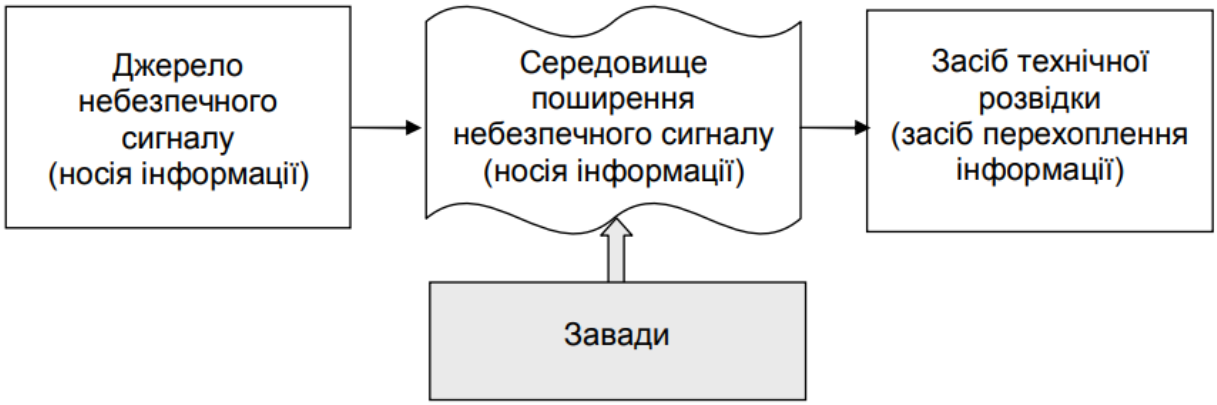


Рис. 1.2 Структура технічного каналу витоку інформації

1.2. Аналіз технічних каналів витоку інформації

Для встановлення вимог та організації захисту інформації від витоку технічними каналами здійснена їх класифікація за певними ознаками.

Зокрема відокремлені типи ТКВІ за такими ознаками [6,7]:

- за видом інформаційної діяльності на ОІД;
- за принципом (фізичним ефектом, процесом) формування небезпечного

сигналу (носія інформації);

- за середовищем поширення небезпечного сигналу;
- за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника.

За видом інформаційної діяльності на ОІД відокремлюються такі типи ТКВІ:

- технічні канали витоку мовної інформації,
- технічні канали витоку інформації, що обробляється в ОТЗС,
- технічні канали витоку візуальної інформації,
- матеріально-речовинні канали витоку інформації.

Класифікацію ТКВІ за принципом (фізичним ефектом, процесом) формування небезпечного сигналу, середовищем поширення небезпечного сигналу та способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника доцільно розглянути у межах визначених вище типів ТКВІ.

Технічні канали витоку мовної інформації за цими ознаками поділяються на такі [7,8]:

- Акустичні канали.
- Акустовібраційні (віброакустичні) канали.
- Акустооптоелектронні (лазерні акустичні) канали.
- Акустоелектричні канали.
- Відеоакустичні канали.
- Канали ВЧ нав’язування (для зняття мовної інформації).
- Канали витоку мовної інформації на основі закладних пристроїв.

Технічні канали витоку інформації, що обробляється в ОТЗС, поділяються на такі [7,8]:

- Канали побічних електромагнітних випромінювань.
- Канали побічних електромагнітних наведень.
- Канали “паразитної” модуляції сигналів ВЧ генераторів.
- Канали “паразитної” ВЧ генерації підсилювачів.

- Канали перехоплення (зняття) інформації з волоконно-оптичних ліній передачі даних.
- Канали перехоплення (зняття) інформації з каналів зв'язку.
- Канали ВЧ нав'язування (для зняття інформації, що обробляється в ОТЗС).
- Канали витоку інформації, що обробляється в ОТЗС, на основі закладних пристроїв.

Технічні канали витоку візуальної інформації поділяються на Такі [7,8]:

- Візуальні канали.
- Візуально оптичні канали.
- Канали витоку візуальної інформації на основі закладних пристроїв.

Матеріально-речовинні канали витоку інформації [7,8,9,10]:

- Добування інформації з магнітних та інших носіїв інформації засобів ЕОТ, що вийшли з ладу.
- Добування інформації з чернеток документів, з відходів виробництва, видавницької діяльності, діловодства тощо.
- Хімічні канали.

За носієм інформації та принципом формування небезпечного сигналу відокремлюються такі ТКВІ [7,8]:

1. Електромагнітні канали витоку інформації, до яких відносяться канали побічних електромагнітних випромінювань, канали "паразитної" ВЧ генерації підсилювачів, канали "паразитної" модуляції ВЧ генераторів, канали перехоплення інформації з ліній радіо- (радіорелейного, стільникового, мобільного) зв'язку та тому подібні;
2. Електричні канали витоку інформації, до яких відносяться канали побічних електромагнітних наведень на комунікації, канали зняття інформації з ліній провідного зв'язку та тому подібні;
3. Параметричні канали витоку інформації, до яких відносяться, канали ВЧ нав'язування, канали "паразитної" модуляції та тому подібні.

За місцем перехоплення інформації засобами технічної розвідки

противника відокремлюються такі типи ТКВІ [7,8,9,10]:

- канали перехоплення (зняття) інформації за межами КЗ,
- канали перехоплення (зняття) інформації за межами КЗ з активним впливом на параметри технічного каналу витоку інформації (наприклад, канал ВЧ нав'язування),
- канали зняття інформації засобами технічної розвідки, встановленими на ОІД (наприклад, технічні канали витоку інформації закладними пристроями).

Розглянута класифікація технічних каналів витоку інформації дозволяє систематизувати уявлення про них та встановити вимоги і заходи щодо захисту інформації від витоку відповідними ТКВІ.

1.3 Висновки по розділу

1. Подано порядок розподілу інформації на об'єкті інформаційної діяльності. Визначено класифікацію інформації за змістом та порядком доступу. Подано способи та режими доступу до інформації. Визначено інформацію, яка підлягає захисту та подано критерії інформаційної безпеки.

2. Проведено аналіз загроз та визначено канали витоку технічної інформації. Показана структура технічного каналу витоку інформації.

3. Здійснено аналіз технічних каналів витоку інформації та подана їх класифікація. Яка включає розподіл за видом інформаційної діяльності, принципом формування небезпечного сигналу, за середовищем поширення небезпечного сигналу, за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника.

РОЗДІЛ 2
ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

2.1 Процес ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах

У зв’язку з загальним розповсюдженням комп’ютерних технологій все гострішою встає проблема захисту інформації в інформаційно-комунікаційних мережах (ІКМ) об’єкту інформаційної діяльності.

Тому дуже актуальними є теоретичні розробки в області захисту комп’ютерної інформації та практичне їх застосування безпосередньо в певних конкретних комп’ютерних системах. Питання захисту інформації в комп’ютерних системах вирішується для того, щоб ізолювати нормально функціонуючу інформаційну систему від несанкціонованих управляючих дій і доступу сторонніх осіб або програм до комп’ютерних даних, що захищаються. Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури [1,2,3].

Управління доступом – ефективний метод захисту інформації, регулюючий використовування ресурсів інформаційної системи, для якої розроблялася концепція інформаційної безпеки (ІБ). Методи і системи захисту інформації, що спираються на управління доступом, включають наступні функції захисту інформації в ІКС [8,9,10,11]:

– ідентифікація користувачів, ресурсів і персоналу системи ІБ;

– впізнання і встановлення достовірності користувача за обліковими даними,

що вводяться (на даному принципі працює більшість моделей ІБ);

– допуск до певних умов роботи згідно регламенту, наказаному кожному

окремому користувачу, що визначається засобами захисту інформації і є

основою інформаційної безпеки більшості типових моделей ІКС;

– протоколювання звертань користувачів до ресурсів, ІБ яких захищає ресурси від НСД і відстежує некоректну поведінку користувачів системи.

Як бачимо, система ідентифікації і автентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу (НСД) до будь-якої інформаційно-комунікаційної системи. Під НСД до інформації розумітимемо доступ до інформації, що порушує встановлені правила розмежування доступу і здійснюваний з використанням штатних засобів обчислювальної техніки або автоматизованих систем.

НСД може носити випадковий або навмисний характер.

Задачею систем ідентифікації і автентифікації є визначення і верифікація набору повноважень суб'єкта при доступі до інформаційної системи. Ідентифікація дозволяє суб'єкту (користувачу, процесу, діючому від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я).

Ідентифікація - це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). За допомогою автентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова "автентифікація" іноді використовують словосполучення "перевірка достовірності" [7,11].

Автентифікація – це процедура, яка перевіряє, чи має користувач з пред'явленим ідентифікатором право на доступ до ресурсу. Ці процедури (ідентифікація та автентифікація) нерозривно зв'язані між собою, оскільки спосіб перевірки визначає, яким чином і що користувач повинен пред'явити системі, щоб отримати доступ [7,11].

Сьогодні існує декілька технологій ідентифікації та автентифікації користувачів в інформаційно-комунікаційних системах (рис.2.1) [7,8,12,13].

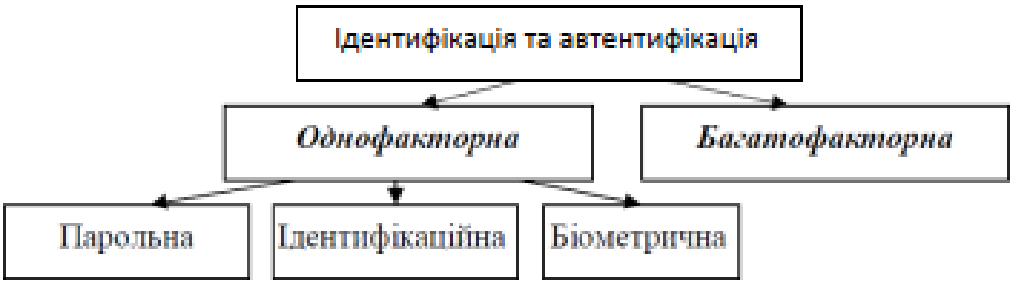


Рис.2.1. Система технологій ідентифікації та автентифікації

У кожного з них є свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних комп'ютерних системах, інші – в інших. Однак у багатьох випадках немає строго певного рішення. А тому як розроблювачам програмного забезпечення, так і користувачам приходиться самостійно вирішувати, який спосіб ідентифікації реалізовувати у власних ІКС.

2.2 Класифікація та характеристики методів ідентифікації та автентифікації користувача

Парольна ідентифікація та автентифікація користувачів.

Нещодавно парольна ідентифікація та автентифікації була ледве не єдиним способом визначення особистості користувача. І в цьому немає абсолютно нічого дивного. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні [7,14].

Суть її зводиться до наступного. Кожен зареєстрований користувач якої певної системи одержує набір персональних реквізитів (звичайно використаються пари логін-пароль).

Далі при кожній спробі входу він повинен вказати свою інформацію. Ну а оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особистість та ідентифікує її.

При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте, по сукупності характеристик їх

слід визнати найслабкішим засобом перевірки достовірності. Саме слабкий рівень парольного захисту є однією з основних причин уразливості комп'ютерних систем до спроб несанкціонованого доступу. Але поки символьний пароль – найпоширеніший спосіб ідентифікації і аутентифікації користувачів і ще довго їм залишатиметься.

Наступні заходи дозволять значно підвищити надійність парольного захисту [7,14]:

– накладання технічних обмежень: встановлення мінімальної довжини пароля, використання в паролі різних груп символів (пароль повинен містити букви, цифри, знаки пунктуації і т.п.);

– управління терміном дії паролів, їх періодична зміна;

– обмеження кількості невдалих спроб входу в систему;

– використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правилах, може генерувати тільки благозвучні паролі, що запам'ятовуються).

Для детальнішого розгляду принципів побудови парольних систем сформулюємо декілька основних визначень. Ідентифікатор користувача – деяка унікальна кількість інформації, що дозволяє розрізняти індивідуальних користувачів парольної системи (проводити їх ідентифікацію). Часто ідентифікатор також називають ім'ям користувача або ім'ям облікового запису користувача. Пароль користувача – деяка секретна кількість інформації, відома тільки користувачу і парольній системі, яке може запам'ятати користувачем і пред'явлене для проходження процедури автентифікації. Одноразовий пароль дає можливість користувачу однократно пройти автентифікацію. Багаторазовий пароль може бути використаний для перевірки достовірності повторно.

Обліковий запис користувача - сукупність його ідентифікатора і його пароля. База даних користувачів парольної системи містить облікові записи всіх користувачів даної парольної системи. Під парольною системою розумітимемо програмно-апаратний комплекс, що реалізовує системи ідентифікації і автентифікації користувачів ІКС на снові одноразових (рис.2.1,а) або

багаторазових (рис.2.1,б) паролів [13,14].

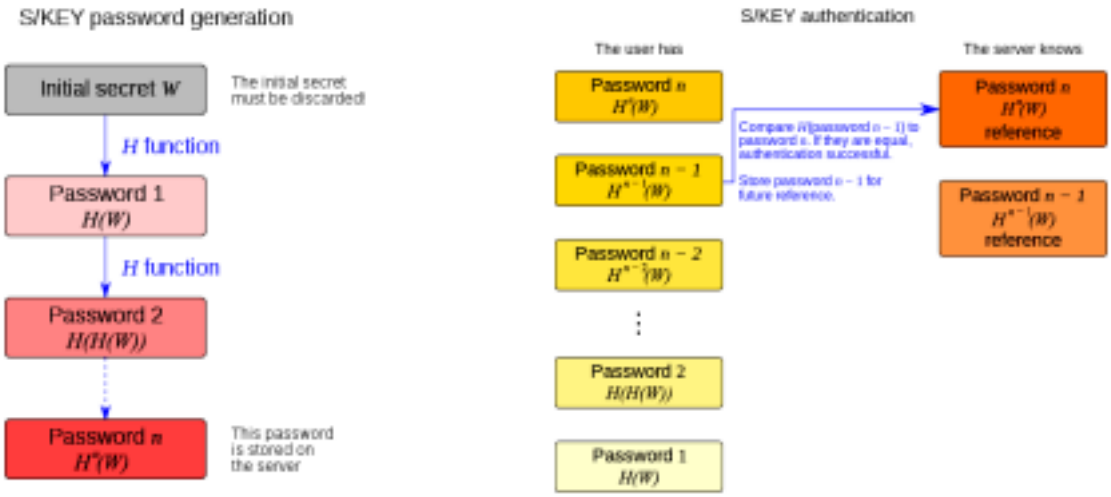


Рис.2.1. Система одноразових (а) та багаторазових (б) паролів

Як правило, такий комплекс функціонує спільно з підсистемами розмежування доступу і реєстрації подій. В окремих випадках парольна система може виконувати ряд додаткових функцій, зокрема генерацію і розподіл короткочасних (сеансових) криптографічних ключів. Основними компонентами парольної системи є [12,13,14]:

– інтерфейс користувача;

– інтерфейс адміністратора;

– модуль сполучення з іншими підсистемами безпеки;

– база даних облікових записів.

Парольна система є "переднім краєм оборони" всієї системи безпеки. Деякі її елементи (зокрема ті, що реалізують інтерфейс користувача) можуть бути розташовані в місцях, відкритих для доступу потенційному зловмиснику. Тому парольна система стає одним з перших об'єктів атаки при вторгненні зловмисника в захищену систему. Нижче перераховані типи загроз безпеки парольних систем.

1). Розголошування параметрів облікового запису через [14,15]:

– підбір в інтерактивному режимі;

– підглядання;

– навмисну передачу пароля його власником іншій особі;

– захват бази даних парольної системи;

перехоплення переданої по мережі інформації про пароль;

– зберігання пароля в доступному місці.

2). Втручання у функціонування компонентів парольної системи через:

– впровадження програмних закладок;

– виявлення і використовування помилок, допущених на стадії розробки;

– виведення з ладу парольної системи.

Деякі з перерахованих типів загроз пов'язані з наявністю так званого людського фактору, що виявляється в тому, що користувач може [14,15]:

– вибрати пароль, який легко запам'ятати і також легко підібрати;

– записати пароль, який складно запам'ятати, і покласти запис в доступному місці;

– ввести пароль так, що його зможуть побачити сторонні;

– передати пароль іншій особі навмисно або під впливом помилки.

На додаток до вище сказаного необхідно наголосити на існуванні "парадоксу людського фактору". Полягає він в тому, що користувач нерідко прагне виступати скоріш супротивником парольної системи, як, втім, і будь-якої системи безпеки, функціонування якої впливає на його робочі умови, ніж союзником системи захисту, тим самим послаблюючи її.

Важливим аспектом стійкості парольної системи є спосіб зберігання паролів в базі даних облікових записів. Можливі наступні варіанти зберігання паролів [12,13,15]:

– у відкритому виді;

– у вигляді згорток (хешування);

– зашифрованими за деяким ключем.

Найбільший інтерес представляють другий і третій способи, які мають ряд особливостей. Хешування (використання незворотної хеш-функції до будь-якої інформації перетворює її на унікальний код) не забезпечує захист від підбору

паролів по словнику у разі отримання бази даних зловмисником. При виборі алгоритму хешування, який буде використаний для розрахунку згорток паролів, необхідно гарантувати відмінність значень згорток, отриманих на основі різних паролів користувачів.

Крім того, слід передбачити механізм, що забезпечує унікальність згорток в тому випадку, якщо два користувача вибирають однакові паролі. Для цього при розрахунку кожної згортки зазвичай використовують деяку кількість "випадкової" інформації, наприклад, видаваною генератором псевдовипадкових чисел.

При шифруванні паролів особливе значення має спосіб генерації і зберігання ключа шифрування бази даних облікових записів. Перерахуємо деякі можливі варіанти [14,15]:

– ключ генерується програмно і зберігається в системі, забезпечуючи можливість її автоматичного перезавантаження;

– ключ генерується програмно і зберігається на зовнішньому носієві, з якого прочитується при кожному запуску;

– ключ генерується на основі вибраного адміністратором пароля, який вводиться в систему при кожному запуску.

У другому випадку необхідно забезпечити неможливість автоматичного перезапуску системи, навіть якщо вона виявляє носій з ключем. Для цього можна зажадати від адміністратора підтверджувати продовження процедури завантаження, наприклад, натисненням клавіші на клавіатурі. Найбільш безпечне зберігання паролів забезпечується при їх хешуванні і подальшому шифруванні отриманих згорток, тобто при комбінації другого і третього способів.

Враховуючи, що користувачі нерідко вибирають недостатньо стійкі паролі, можна зробити висновок, що отримання бази даних облікових записів або перехоплення переданого по мережі значення згортки пароля представляють серйозну загрозу безпеці парольної системи. В більшості випадків автентифікація відбувається в розподілених системах і пов'язана з передачею по

мережі інформації про параметри облікових записів користувачів. Якщо інформація, що передається по мережі в процесі автентифікації, не захищена належним чином, виникає загроза її перехоплення зловмисником і використання для порушення захисту парольної системи. Відомо, що багато комп'ютерних систем дозволяють перемикати мережевий адаптер в режим прослуховування адресованого іншим одержувачам мережевого трафіку в мережі, заснованій на передачі пакетів даних. Нагадаємо основні види захисту мережевого трафіку: фізичний захист мережі; кінцеве шифрування; шифрування пакетів.

Поширені наступні способи передачі по мережі паролів [12,13,14]:

– у відкритому вигляді;

– зашифрованими;

– у вигляді згорток;

– без безпосередньої передачі інформації про пароль ("з нульовим розголошуванням").

Перший спосіб застосовується і сьогодні в багатьох популярних додатках (наприклад, TELNET, FTP). У захищеній системі його можна застосовувати тільки у поєднанні із засобами захисту мережевого трафіку. При передачі паролів в зашифрованому вигляді або у вигляді згорток по мережі з відкритим фізичним доступом можлива реалізація наступних погроз безпеці парольної системи [14,15]:

– перехоплення і повторне використання інформації;

– перехоплення і відновлення паролів;

– модифікація інформації, що передається, з метою введення в оману контролюючої сторони;

– імітація зловмисником дій контролюючої сторони для введення в оману користувача.

Схеми автентифікації "з нульовим знанням" або "з нульовим розголошуванням" вперше з'явилися в середині 80-х – на початку 90-х років. Їх основна ідея полягає в тому, щоб забезпечити можливість одному з пари суб'єктів довести істинність деякого твердження другому, при цьому не

повідомляючи йому ніякої інформації про зміст самого твердження. Наприклад, перший суб'єкт (що "доводить") може переконати другого ("перевіряючого"), що знає певний пароль, насправді не передаючи тому жодної інформації про сам пароль. Ця ідея і відображена в визначені "доказ з нульовим розголошуванням". Стосовно парольного захисту це означає, що якщо на місці перевіряючого суб'єкта виявляється зловмисник, він не отримує ніякої інформації про доказуване твердження і, зокрема, про пароль. Загальна схема процедури автентифікації з нульовим розголошуванням складається з послідовності інформаційних обмінів (ітерацій) між двома учасниками процедури, по завершенню якої перевіряючий із заданою ймовірністю робить правильний висновок про істинність твердження, що перевіряється. Із збільшенням числа ітерацій зростає ймовірність правильного розпізнавання істинності (або помилковості) твердження.

Ще одним способом підвищення стійкості парольних систем, пов'язаної з передачею паролів по мережі, є застосування одноразових (one - time) паролів [14,15].

Загальний підхід до застосування одноразових паролів заснований на послідовному використанні хеш-функції для розрахунку чергового одноразового пароля на основі попереднього. На початку користувач одержує впорядкований список одноразових паролів, останній з яких також зберігається в системі автентифікації. При кожній реєстрації користувач вводить черговий пароль, а система розраховує його згортку і порівнює з еталоном, що зберігається у системі. У разі спів падання користувач успішно проходить автентифікацію, а введений ним пароль зберігається для використання як еталон при наступній реєстрації.

Захист від мережевого перехоплення в такій схемі заснований на властивості необоротності хеш- функції. Найбільш відомі практичні реалізації схем з одноразовими паролями - це програмний пакет S/KEY і розроблена на його основі система OPIE.

Головна перевага парольної ідентифікації – це простота реалізації й

використання.

Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований у більшості програмних продуктів. Таким чином, система захисту інформації виявляється простою і доступною. Головним недоліком парольної ідентифікації слід вважати величезну залежність надійності ідентифікації від самих користувачів, точніше, від обраних ними паролів. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. До них відносяться занадто короткі паролі, загальновідомі сполучення символів і т.д. Тому деякі фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з випадкового сполучення букв, цифр і різних символів..

Окремим видом парольної ідентифікації ‘ використання QR-коду.

Розробкою QR-коду займалася компанія Denso-Wave. Зараз позначення “QR code” є зареєстрованим товарним знаком DENSO Corporation, проте, його використання не обкладається будь-якими ліцензійними відрахуваннями. Крім цього, самі QR коди описані і опубліковані в якості стандартів ISO.

Розшифровка QR - “Quick Response”. Тобто QR код можна назвати кодом швидкого реагування (або моментального відгуку). Зараз це як ніколи відображає суть, так як для сканування не потрібно ніяких спеціальних приладів. Досить піднести до коду смартфон і можна отримати всю необхідну інформацію.

QR коди бувають різних версій і в залежності від них мають різний розмір. Від 21 на 21 пікселя без урахування полів в першій версії до 177 на 177 пікселів в сороковій версії.

Існує 4 основних типи кодувань. Серед них цифрова (для шифровки цифр), алфавітно-цифрова (цифри і символи), байтовая (дані) і кандзі, призначена для роботи з ієрогліфами.

Для виправлення помилок у QR-коді, в разі його пошкодження або нанесення додаткових малюнків, використовується код Ріда-Соломона з 8-бітовим кодовим словом. Існує чотири рівні надмірності (7%, 15%, 25% і 30%). Є й інші складні ступені захисту від помилок зчитування. Особливу важливість

вони знаходять в разі роботи з платіжними та ідентифікаційними системами. Однією з таких ступенів є перебір всіх можливих варіантів зчитування з підрахунком штрафних балів за особливими правилами для кожного з них. В результаті вибирається найвдаліший варіант, який і приймається за істинний.

Головною перевагою QR коду є його “місткість”. Цей тип коду є двовимірним на відміну від одновимірного штрих-коду. Свого часу перехід від “смужок” до “квадратиків” був обумовлений саме необхідністю шифрувати в кодах більше інформації.

Стандартний QR код може нести в собі до 4000 символів. Це дозволяє зашифрувати не тільки пару десятків символів інвентарного номера товару в магазині, але навіть цілі тексти, довгі реферальні посилання і багато іншого. Є навіть можливість шифрування JPEG, GIF і PNG. Правда, для цього вони повинні бути розміром не більше 4 КБ, а це дуже мало. Для передачі зображень куди простіше зашифрувати посилання і розмістити на спеціальній сторінці будь-зображення.

Апаратна ідентифікація та автентифікація користувачів в ІКМ.

Цей принцип ідентифікації ґрунтується на визначенні особистості користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні [9,10,14].

Зрозуміло, що мова йде не про звичні для більшості людей ключі, а про спеціальні електронні. На даний момент найбільше поширення одержали два типи пристроїв: різноманітні карти (безконтактні-карти, смарт-карти, магнітні карти і т.д.) та так званні токени (token), які підключаються безпосередньо до одного з портів комп'ютера. Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм, зазвичай невеликих розмірів для зручності його носіння з собою. До складу електронних систем ідентифікації і аутентифікації входять (рис.2.3) [9,10,14]:

Рис.2.3. Токени

1. Переносні токени [9,10,14]:

– асинхронні – користувач вводить рядок в пристрій, отримує відповідь і вводить її в комп'ютер;

– PIN/асинхронні – асинхронний метод доповнюється введенням PIN-коду в пристрій;

– синхронні – наприклад, токен синхронізований за часом з сервером і генерує для даного користувача в дану хвилину пароль, який вже і вводиться в систему;

– PIN/синхронні.

2. Різноманітні карти – це пристрої, схожі на переносні аутентифікатори, але складніші по своєму складу. Карти бувають [9,10,14]:

− пасивні (карти з пам'яттю);

− активні (інтелектуальні карти).

Останні включають CPU, мініатюрну операційну систему, годинник, програми на ROM (read-only memory – пам'ять тільки для читання), буферну пам’ять (RAM) для криптографічних розрахунків, незалежну пам'ять або EEPROM (Electrically Erasable Programmable Read-Only Memory) для зберігання цифрових ключів. За допомогою смарт-карти проводиться розрахунок одноразових паролів і здійснюється взаємодія з пристроєм через картрідер [9,10,14].

Після введення PIN-коду картрідер сам запитує смарт- карту, і подальший процес протікає без участі людини, завдяки чому можна використовувати достатньо довгі ключі.

Карт досить багато, і працюють вони по різних принципах. Так, наприклад, досить зручні у використанні безконтактні карти (їх ще називають проксіміті-

карти), які дозволяють користувачам проходити ідентифікацію як у комп'ютерних системах, так й у системах доступу в приміщення. Найбільш надійними вважаються смарт-карти – аналоги звичних багатьом людям банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-кодом і т.д.

Що таке USB-ключ, розглянемо на прикладі цифрового підпису від компанії Aladin Software. Цифровий підпис - персональний засіб аутентифікації і зберігання даних, що апаратно підтримує роботу з цифровими сертифікатами і електронними цифровими підписами (ЕЦП) [9].

Рис. 2.4. Цифрові підписи

Цифровий підпис може бути виконаний у вигляді USB-ключа або стандартної смарт-карти.

Цифровий підпис підтримує роботу і інтегрується зі всіма основними системами і додатками, що використовують технології смарт-карт або PKI (Public Key Infrastructure). Основне призначення [9,10,14,15]:

− двохфакторна adтентифікація користувачів при доступі до захищених ресурсів (комп'ютерів, мереж, додатків);

− безпечне зберігання закритих ключів цифрових сертифікатів, криптографічних ключів, профілів користувачів, налаштувань додатків і інше в незалежній пам'яті ключа;

− апаратне виконання криптографічних операцій в довіреному середовищі (генерація ключів шифрування, симетричне і асиметричне шифрування, розрахунок хеш-функції, формування ЕЦП).

Цифровий підпис як засіб аутентифікації підтримується більшістю сучасних операційних систем, бізнес-додатків і продуктів по інформаційній безпеці.

Можливості застосування [9,10,14]:

− сувора аутентифікація користувачів при доступі до серверів, баз даних, розділів Web-сайтів;

− безпечне зберігання секретної інформації: паролів, ключів шифрування, закритих ключів цифрових сертифікатів;

− захист електронної пошти (цифровий підпис і шифрування, доступ);

− системи електронної торгівлі, «клієнт-банк», «домашній банк»;

− захист комп'ютерів;

− захист мереж та каналів передачі даних за рахунок побудови VPN (virtual private network – віртуальні приватні мережі);

− клієнт-банк, home-банк.

Цифровий підпис забезпечує [14,15]:

– автентифікацію користувачів за рахунок використання криптографічних методів; безпечне зберігання ключів шифрування і ЕЦП, а також закритих ключів цифрових сертифікатів для доступу до захищених корпоративних мереж і інформаційних ресурсів;

– мобільність користувача і можливість безпечної роботи з конфіденційними даними в недовіреному середовищі (наприклад, на чужому комп'ютері) за рахунок того, що ключі шифрування і ЕЦП генеруються

цифровим ключем апаратно і не можуть бути перехоплені;

– безпечне використання - скористатися цифровим ключем може тільки його власник, що знає PIN-код ключа; реалізацію як західних та російських, так і вітчизняних стандартів на шифрування і ЕЦП; зручність роботи - ключ виконаний у вигляді брелків зі світловою індикацією режимів роботи і безпосередньо підключається до USB-портів, якими зараз оснащено 100% комп'ютерів, не вимагає спеціальних зчитувачів, блоків живлення, проводів і т.п.;

– використання одного ключа для вирішення безлічі різних завдань - входу в комп'ютер, входу в мережу, захисту каналу, шифрування інформації, ЕЦП, безпечного доступу до захищених розділів Web-сайтів, інформаційних порталів і тому подібне.

Безконтактні смарт-карти розділяються на ідентифікатори Proximity і смарт-карти, що базуються на міжнародних стандартах ISO/IEC 15693 і ISO/IEC 14443. В основі більшості пристроїв на базі безконтактних смарт-карт лежить технологія радіочастотної ідентифікації.

Основними компонентами безконтактних пристроїв є чіп і антена.

Ідентифікатори можуть бути як активними (з батареями), так і пасивними (без джерела живлення). Ідентифікатори мають унікальні 32/64 розрядні серійні номери.

Системи ідентифікації на базі Proximity криптографічно не захищені, за винятком спеціальних рекомендованих систем. USB-ключі працюють з USB-портом комп'ютера. Виготовляються у вигляді брелоків. Кожний ключ має 32/64 розрядний серійний номер.

Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. І дійсно, у пам'яті токенів можуть зберігатися ключі, підібрати які досить складно. Крім того, в них реалізовано чимало різних захисних механізмів, а вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції. Головна небезпека у застосуванні апаратної

ідентифікації криється у можливості крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані.

Другий мінус розглянутої технології - ціна. Взагалі, останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. Проте, для введення в експлуатацію системи такої ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом де які типи ключів можуть зношуватися, крім того, вони можуть бути загублені й т.д. Тобто апаратна ідентифікація вимагає деяких експлуатаційних витрат.

Основні переваги й недоліки різних типів цифрових ключів розглянемо в Табл. 2.1 [9,10,14].

Таблиця 2.1

Основні переваги й недоліки різних типів цифрових ключів

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

USB-токени з вбудованим чіпом	Високий рівень безпеки. Мобільність. Підтримка великої кількості застосунків. Очевидна приналежність токена користувачеві.	Потребує встановлення ПЗ користувача.
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.

Біометрична ідентифікація та автентифікація користувачів в ІКМ

Біометрія – це ідентифікація користувача по унікальним, властивим тільки йому біологічним ознакам. Тобто, можна сказати, що біометричні технології споконвічно розроблялися для точного встановлення особистості людини [16].

А тому рішення використати їх в області інформаційної безпеки виглядає цілком логічним. Причому даний напрямок розвивається дуже активно. Сьогодні експлуатується вже більше десятка різних біометричних ознак. Причому для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів.

Так що користувачам, що вирішили використати біометричну ідентифікацію, є із чого вибрати. Біометрична ідентифікація та автентифікації - це спосіб ідентифікації особи по окремих специфічних біометричних ознаках, властивих конкретній людині. Сучасний рівень розвитку комп'ютерних

технологій дозволив використовувати подібні ознаки як основу для ідентифікації людини і ухвалення рішення про можливість доступу до ресурсів комп'ютерних систем [16,17,18].

Серед біометричних механізмів ідентифікації можна виділити такі [16,17,18]:

1) по статичних ознаках – те, що практично не міняється з часом, починаючи з народження людини (фізіологічні характеристики);

2) по динамічних ознаках – поведінкові характеристики, тобто ті, які побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії.

Динамічні ознаки можуть змінюватися з часом, але не різко, а поступово.

Серед статичних методів в задачах ідентифікації користувача комп'ютерних систем використовуються наступні [16,17,18]:

1. Ідентифікація по відбитку пальця (рис.1.5). В основу цього методу покладена унікальність малюнка папілярних візерунок на пальцях. Ідентифікація побудована таким чином: за допомогою сканера одержують зображення відбитку, потім це зображення по складному алгоритму перетворюється на спеціальний цифровий код. Далі цей код порівнюється з еталонними кодами, які зберігаються в базі даних.

Рис.2.5. Пальцевий та долонний дактилоскопічні сканери

2. Ідентифікація по розташуванню вен на долоні. Прилад, який прочитує інформацію в цьому випадку, є інфрачервона камера. В результаті на вході програми при формуванні цифрового коду з'являється малюнок вен на руці

людини. Не потребує контакту людини з пристроєм для сканування. Має високі показники надійності і достовірності.

3. Ідентифікація по сітківці ока (рис.2.6). В даному випадку сканується малюнок кровоносних судин очного дна, який має нерухому структуру, незмінну в часі. Зрозуміло, що цей малюнок спостерігається тільки за певних умов: при скануванні людина дивиться на видалене світлове джерело і спеціальна камера сканує її очне дно, що в свою чергу може викликати неприємні відчуття у людини. Вважається одним з самих надійних біометричних методів.

4. Ідентифікація по райдужній оболонці ока (рис.2.6).

Малюнок райдужної оболонки ока - унікальний для кожної людини. В цьому методі важлива не тільки спеціальна камера, але і надійне програмне забезпечення.

Адже саме за допомогою програмного забезпечення із зображення виділяється малюнок потрібної нам райдужної оболонки. Цей метод є одним з найбільш точних серед біометричних методів.

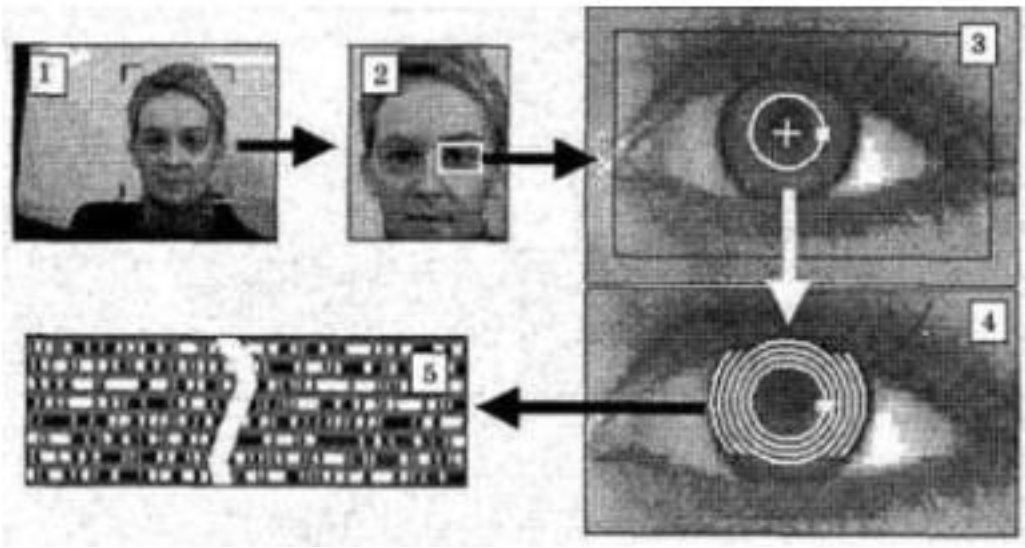


Рис. 2.6. Аутентифікація за райдужною оболонкою ока

5. Ідентифікація за формою кисті руки. Цей метод ґрунтується на розпізнаванні геометричних особливостей кисті руки. Спеціальний сканер формує тривимірний малюнок кисті. При аналізі цього малюнка виконуються

вимірювання, за допомогою яких формується відповідний цифровий код.

6. Ідентифікація за формою обличчя (рис.2.7).

На практиці використовується як двовимірне так і тривимірне зображення. Причому двовимірне розпізнавання обличчя на сьогоднішній день –один з самих неефективних методів біометрії, тому має обмежене коло застосування або використовується тільки в сукупності з іншими методами. Розпізнавання за тривимірним зображенням обличчя чимось схоже на метод ідентифікації за формою кисті руки. Тут так само будується тривимірний образ обличчя. Спеціальне програмне забезпечення виділяє з цього образу контури очей, губ і інших частин лиця. Далі проводяться точні вимірювання між заданими контурами. Саме за цими даними будується цифровий код.

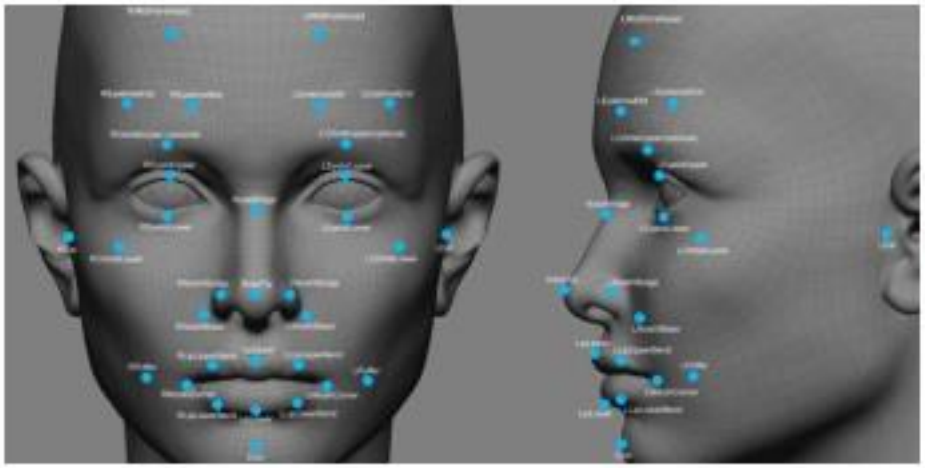


Рис. 2.7. Аутентифікація за формою обличчя

Серед динамічних методів, які використовуються для ідентифікації особи користувача, можна назвати наступні:

1. Ідентифікація по голосу. В даний час існує безліч програм по розпізнаванню голосу. В методі ідентифікації по голосу важливі частотні характеристики голосу людини. Саме по частотних характеристиках і будується цифрова модель.

2. Ідентифікація по почерку. При ідентифікації за даним методом звичайно досліджується підпис людини. Перевіряються такі динамічні характеристики, як:

графічні параметри, сила натиску на поверхню, швидкість нанесення підпису. На основі цих характеристиках і будується цифровий код.

3. Ідентифікація по клавіатурному почерку. Даний метод аналогічний ідентифікації по почерку, але замість того, щоб ставити автограф, людині необхідно надрукувати кодове слово. Цифровий код будується по динаміці набору певного слова або фрази.

При всьому теоретичному різноманітті можливих біометричних методів тих, що застосовуються на практиці серед них небагато. Основних методів три – розпізнавання по відбитку пальця, по зображенню особи (двомірному або тривимірному), по райдужній оболонці та по сітківці ока. На сьогоднішній день всі біометричні технології є імовірнісними і нерідко дана обставина служить основою для критики біометрії.

Важко не погодитися, що біометричні технології надійніші і зручніші за ті засоби захисту, які широко застосовувалися до теперішнього часу. Але, незважаючи на активну діяльність протягом останніх років у напрямку розробки та вдосконалення методів ідентифікації користувачів з метою управління доступом до ресурсів інформаційних систем, надійність та стійкість існуючих систем недостатня для потреб сьогоднішнього дня. Головним достоїнством біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує. Правда, сьогодні вже відомо кілька способів обману дактилоскопічних сканерів.

Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або може бути використана фотографія пальця зареєстрованого користувача. Втім, треба зізнатися, що сучасні пристрої значно стійкіші по відношенню до подібної фальсифікації.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входить до цієї системи, необхідно придбати власний сканер. Звичайно, останнім часом ціни на біометричні пристрої постійно знижуються [17,18].

Крім того, не дуже давно з'явилися миші й клавіатури з вбудованими

дактилоскопічними сканерами.

В розглянутих системах для визначення особи користувача використовується тільки один фактор. Однак подібні процеси сьогодні не можна назвати надійними.

Останнім часом набуває поширення комплексна або багатофакторна ідентифікація.

2.3 Вимоги та порядок організації процесів ідентифікації та автентифікації

Основним міжнародним стандартом по криптографічним протоколам аутентифікації є стандарт Міжнародної організації по стандартизації та Міжнародної електротехнічної комісії ISO / IEC 9798 - Information technology – Security techniques - Entity authentication mechanisms, що складається з п'яти частин [19,20,21]:

ISO / IEC 9798-1 - «General Model»;

ISO / EEC 9798-2 - «Mechanisms using symmetric encipherment algorithms »;

ISO / EEC 9798-3 - «Entity authentication using a public-key algorithm »;

ISO / IEC 9798-4 - «Mechanisms using a cryptographic check function»;

ISO / IEC 9798-5 - «Mechanisms using zero knowledge techniques».

В цих протоколах претендент і перевіряючий мають симетричний секретний ключ або ключі парно-вибіркового зв'язку. Для їх отримання може використовуватися довірений сервер в режимі реального часу.

Стандартом ISO / IEC 9798-2 передбачені три способи автентифікації [19,20]:

1. Одностороння аутентифікація, заснована на мітці часу (рис.2.9). Якщо у претендента і перевіряючого є системний годинник, немає необхідності надсилати запит. претендент відразу може направити повідомлення з включеною в нього міткою часу, а перевіряючий звірити мітку з показаннями свого годинника.

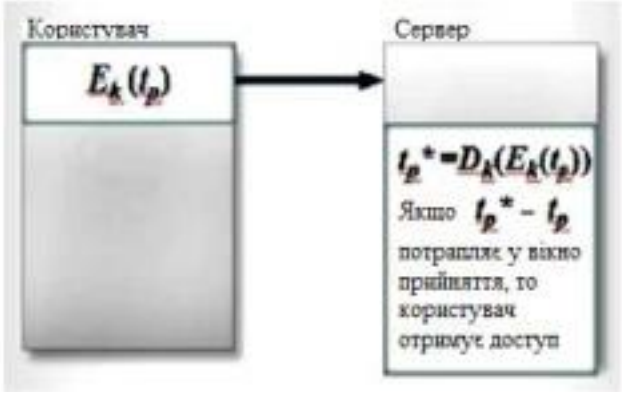


Рис. 2.9. Одностороння автентифікація, заснована на мітці часу

2. Одностороння аутентифікація з використанням випадкових чисел (рис.2.10). В якості запиту перевіряючий посилає випадкове число, згенероване за допомогою генератора псевдовипадкових чисел. Отримавши запит, претендент обчислює відповідь на нього - зашифровує з допомогою алгоритму симетричного шифрування отримане випадкове число і (якщо необхідно) ідентифікатор, перевіряючий розшифровує отриманий шифр-текст і перевіряє структуру запиту.

Якщо вона вірна, він приймає претендента.

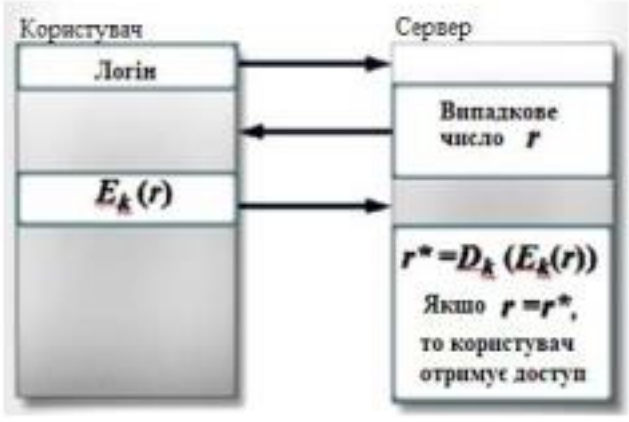


Рис. 2.10. Одностороння автентифікація з використанням випадкових чисел

3. Взаємна автентифікація з використанням випадкових чисел (рис.2.11). Відмінність цього протоколу від попереднього в тому, що тут кожен з учасників

по черзі виконує ролі перевіряючого і претендента, перевіряючи автентичність один-одного.

Протокол взаємної автентифікації - це по суті два протоколи односторонньої автентифікації, «упаковані» в три пересилання повідомлення. Подібного роду протоколи в силу їх симетричності називаються протоколами рукостискання. цей протокол допускає заміну шифру на хеш-функцію з ключем, як зазначено в стандарті ISO / IEC 9798-4. Для підвищення стійкості протоколу до переданим повідомленням можна додати мітки часу.

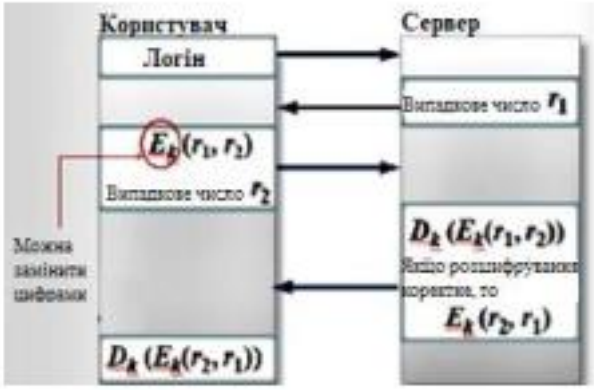


Рис. 2.11. Взаємна автентифікація з використанням випадкових чисел

4 Протоколи «запит - відповідь» з використанням асиметричних криптосхем.

Такі протоколи можна розділити на дві групи: протоколи з використанням ЕЦП і протоколи з використанням схем відкритого шифрування. В стандарті ISO / IEC9798-3 рекомендовані:

1) Протоколи з використанням схем-цифрового підпису (рис.2.12).

В описах протоколів зустрічаються позначення certA сертифікатів відкритих ключів цифрового підпису відповідних учасників протоколу, тобто структури даних, містять їх ідентифікатори, відкриті ключі і іншу службову інформацію, завірену цифровим підписом засвідчувального центру. Детальніше метод сертифікації відкритих ключів буде розглянуто пізніше. Протоколи, подібні описаним вище, використовуються також в стандарті Міжнародного

телекомунікаційного союзу ITU X.509. У ньому описані протоколи автентифікації, суміщені з протоколами обміну ключами.

Рис. 2.12. Протоколи з використанням схем-цифрового підпису

2) Протоколи з використанням схем відкритого шифрування (рис.2.13).

Загрози безпеки ІКС можна поділити на мережеві атаки (інформація, яка надходить з віддаленого клієнта) і локальні атаки, які походять від шкідливих програм, вже встановлених на системі клієнта, наприклад, троянів, руткітів тощо.

Часто оцінки безпеки автентифікації зосереджені переважно на мережевих атаках, припускають, що користувальницький термінал (тобто настільний комп'ютер, ноутбук або мобільний пристрій) є захищеною платформою. Проте нерідко зловмисник отримує повний доступ до ПК жертви через приховані процеси зв'язку, які залишилися від шкідливих програм, що використовують невиправлені діри в безпеці ліцензійного програмного забезпечення.

Типовими методами атак на протоколи автентифікації є [19,20,21]:

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 аутентифікаційного обміну (Interleaving attack) - зловмисник в ході атаки має можливість модифікувати проходить через нього

трафік.

Рис. 2.13. Протоколи з використанням схем відкритого шифрування

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.

Атаки на протоколи автентифікації та шляхи їх поводження

Таблиця 2.2

Рекомендації стосовно заходів проти поширених типів атак на протоколи аутентифікації

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

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

2.4 Висновки по розділу

1. Проведено огляд існуючих технологій ідентифікації та автентифікації користувача в інформаційно-комунікаційних системах об’єкту інформаційної діяльності. Визначені основні поняття та функції доступу до інформації з обмеженим доступом. Подана система технологій ідентифікації та автентифікації користувачів.

2. Розглянуто зміст, особливості застосування, переваги та недоліки парольної, апаратної, біометричної ідентифікації та автентифікації користувачів

в інформаційно - комунікаційних системах.

4. Подано вимоги та порядок організації процесів ідентифікації та автентифікації.

Розділ 3
РОЗРОБКА МЕХАНІЗМІВ БАГАТОФАКТОРНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

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

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

- суб'єкт, який буде проходити процедуру автентифікації;
- характеристика суб'єкта – його відмінна риса;
- керівник системи автентифікації, що несе відповідальність контролює її роботу;
- механізм автентифікації, тобто принцип роботи системи;
- механізм, який надає або позбавляє суб'єкта певних прав доступу.

Ще до появи комп'ютерів використовувалися різні відмінні риси суб'єкта, його характеристики. Зараз використання тієї чи іншої характеристики в системі залежить від необхідної надійності, захищеності та вартості впровадження. Виділяють 3 фактора автентифікації [24,25]:

1. Щось, що ми знаємо - пароль. Це секретна інформація, якою повинен володіти тільки авторизований суб'єкт. Паролем може бути мовне слово, текстове слово, комбінація для замка або персональний ідентифікаційний номер (PIN).

Парольний механізм може бути досить легко реалізований і має низьку вартість. Але має суттєві мінуси: зберегти пароль в секреті часто буває проблематично, зловмисники постійно придумують нові методи крадіжки, злому і підбору пароля (див. бандитський криптоаналіз).

2. Щось, що ми маємо - пристрій автентифікації. Тут важливий факт володіння суб'єктом якимось унікальним предметом. Це може бути особиста

печатка, ключ від замка, для комп'ютера це файл даних, що містять характеристику. Характеристика часто вбудовується в спеціальний пристрій автентифікації, наприклад, пластикова картка, смарт-карта. Для зловмисника дістати такий пристрій стає більш проблематично, ніж зламати пароль, а суб'єкт може відразу ж повідомити в разі крадіжки пристрою. Це робить даний метод більш захищеним, ніж парольний механізм, однак, вартість такої системи вища.

3. Щось, що є частиною нас - біометрика.

Характеристикою є фізична особливість суб'єкта. Це може бути портрет, відбиток пальця або долоні, голос чи особливість очі. З точки зору суб'єкта, даний метод є найбільш простим: не треба ні запам'ятовувати пароль, ні переносити з собою пристрій автентифікації. Однак, біометрична система повинна володіти високою чутливістю, щоб підтверджувати авторизованого користувача, але відкидати зловмисника зі схожими біометричними параметрами. Також вартість такої системи досить велика. Але незважаючи на свої мінуси, біометрика залишається досить перспективним фактором.

Автентифікація по багаторазовим паролям. Один із способів автентифікації в комп'ютерній системі полягає у введенні вашого користувацького ідентифікатора, в просторіччі званого «логіном» (англ. login - реєстраційне ім'я користувача) і пароля - якоїсь конфіденційної інформації [24,25]. Достовірна (еталонна) пара логін-пароль зберігається в спеціальній базі даних.

Проста автентифікація має такий загальний алгоритм [24,25]:

- суб'єкт запитує доступ до системи і вводить особистий ідентифікатор та пароль;

- ведені унікальні дані надходять на сервер автентифікації, де порівнюютьс з еталонними;

- при збігу даних з еталонними, автентифікація визнається успішною, при відмінності - суб'єкт переміщується до 1-го кроку.

Введений суб'єктом пароль може передаватися в мережі двома способами:

- незашифрованому, у відкритому вигляді, на основі протоколу парольного

аутентифікації (Password Authentication Protocol, PAP);

- з використанням шифрування або односпрямованих хеш-функцій;

В цьому випадку унікальні дані, введені суб'єктом передаються по мережі захищено. З точки зору максимальної захищеності, при зберіганні і передачі паролів слід використовувати односпрямовані функції. Зазвичай для цих цілей використовуються криптографічно стійкі хеш-функції. У цьому випадку на сервері зберігається тільки образ пароля. Отримавши пароль та виконавши його хеш-перетворення, система порівнює отриманий результат з еталонним чином, що зберігаються в ній. При їх ідентичності, паролі збігаються. Для зловмисника, який отримав доступ до образу, обчислити сам пароль практично неможливо. Використання багаторазових паролів має ряд істотних мінусів. По-перше, сам еталонний пароль або його хешірованних образ зберігаються на сервері автентифікації. Найчастіше зберігання пароля проводиться без криптографічних перетворень, в системних файлах.

Отримавши доступ до них, зловмисник легко добереться до конфіденційної інформації. По-друге, суб'єкт змушений запам'ятовувати (або записувати) свій багаторазовий пароль. Зловмисник може отримати його, просто застосувавши навички соціальної інженерії, без всяких технічних засобів. Крім того, сильно знижується захищеність системи у випадку, коли суб'єкт сам вибирає собі пароль. Найчастіше це виявляється якесь слово чи комбінація слів, присутні в словнику. При достатній кількості часу зловмисник може зламати пароль простим перебором. Вирішенням цієї проблеми є використання випадкових паролів або обмеженість за часом дії пароля суб'єкта, після закінчення якого пароль необхідно поміняти.

На комп'ютерах з ОС сімейства UNIX, базою є файл / etc / master.passwd (в дистрибутивах Linux зазвичай файл / etc / shadow, доступний для читання лише root), в якому паролі користувачів зберігаються у вигляді хеш-функцій від відкритих паролів, крім цього в цьому ж файлі зберігається інформація про права користувача. Спочатку в Unix-системах пароль (в зашифрованому вигляді) зберігався у файлі / etc / passwd, доступному для читання всім користувачам, що

було небезпечно [24,25].

На комп'ютерах з операційною системою Windows NT/2000/XP/2003/2008 (не входять в домен Windows) така база даних називається SAM (Security Account Manager - Диспетчер захисту облікових записів). База SAM зберігає облікові записи користувачів, що включають в себе всі дані, необхідні системі захисту для функціонування. Знаходиться в директорії % windir% \ system32\config\ [24,25].

В доменах Windows Server 2000/2003/2008 такою базою є Active Directory. При необхідності забезпечення роботи співробітників на різних комп'ютерах (з підтримкою системи безпеки) використовують апаратно-програмні системи, що дозволяють зберігати аутентифікаційні дані і криптографічні ключі на сервері організації. Користувачі вільно можуть працювати на будь-якому комп'ютері (робочої станції), маючи доступ до своїх аутентифікаційні даними і криптографічним ключам [24,25].

Отримавши одного разу багаторазовий пароль суб'єкта, зловмисник має постійний доступ до зламаної конфіденційної інформації. Ця проблема вирішується застосуванням одноразових паролів (OTP - One Time Password).

Суть цього методу - пароль дійсний тільки для одного входу в систему, при кожному наступному запиті доступу - потрібен новий пароль. Реалізовано механізм аутентифікації по одноразовим паролів може бути як апаратно, так і програмно.

Технології використання одноразових паролів можна розділити на [14,24,25]:

- використання генератора псевдовипадкових чисел, єдиного для суб'єкта і системи.

- використання тимчасових міток разом з системою єдиного часу;

- використання бази випадкових паролів, єдиного для суб'єкта і для системи.

У першому методі використовується генератор псевдовипадкових чисел з однаковим значенням для суб'єкта і для системи. Згенерований суб'єктом пароль

може передаватися системі при послідовному використанні односторонньої функції або при кожному новому запиті, грунтуючись на унікальної інформації з попереднього запиту.

У другому методі використовуються тимчасові мітки. Як приклад такої технології можна привести SecurID. Вона заснована на використанні апаратні ключів і синхронізації за часом.

Автентифікація, заснована на генерації випадкових чисел через певні тимчасові інтервали має наступний механізм реалізації. Унікальний секретний ключ зберігається тільки в базі системи і в апаратній пристрої суб'єкта. Коли суб'єкт запитує доступ до системи, йому пропонується ввести PIN-код, а також випадково генерується число, відображуваного в цей момент на апаратній пристрої. Система порівнює введений PIN-код і секретний ключ суб'єкта зі своєї бази і генерує випадкове число, грунтуючись на параметрах секретного ключа з бази і поточного часу. Далі перевіряється ідентичність згенерованого числа і числа, введеного суб'єктом [20,21,25].

Третій метод заснований на єдиній базі паролів для суб'єкта і системи та високоточної синхронізації між ними. При цьому кожен пароль з набору може бути використаний тільки один раз. Завдяки цьому, навіть якщо зловмисник перехопить використовуваний суб'єктом пароль, то він вже буде недійсний. По порівнянні з використанням багаторазових паролів, одноразові паролі надають більш високу ступінь захисту.

Останнім часом все частіше застосовується, так звана, розширена або багатофакторна автентифікація. Вона побудована на спільному використанні декількох факторів автентифікації. Це значно підвищує захищеність системи. Як приклад можна привести використання SIM-карт в мобільних телефонах.

Суб'єкт вставляє апаратно свою карту (пристрій аутентифікації) в телефон і при включенні вводить свій PIN-код(пароль). Також, наприклад в деяких сучасних ноутбуках присутній сканер відбитка пальця. Таким чином, при вході в систему суб'єкт повинен пройти цю процедуру (біометрика), а потім ввести пароль [18,24,25].

Вибираючи для системи той чи інший фактор або спосіб автентифікації необхідно перш за все відштовхуватися від необхідного ступеня захищеності, артості побудови системи, забезпечення мобільності суб'єкта.

У таблиці 3.1 наведено порівняння методів автентифікації по критерію ризику [19,20,22].

Таблиця 3.1

Порівняння 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 школи	Рекомендується мінімальна вимога - використання багатофакторної аутентифікації	Проведення великий міжбанківськ их операцій керівним апаратом

3.2 Моделі оцінки захищеності механізмів багатофакторної автентифікації користувачів від несанкціонованого доступу

Розглянемо модель оцінки захищеності багатофакторної автентифікації користувачів від несанкціонованого доступу для випадку механізму трифакторної автентифікації, розуміючи, що механізми двох і одне факторної автентифікації є окремими випадками, а від трифакторної автентифікації легко перейти до багатофакторні.

Імовірність НСД для механізму автентифікації, наведеного на Рис. 3.1, визначається за формулою [23,25, 27]:

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

Де:

P_i^n – ймовірність правильної роботи механізму паролювання;

P_i^k – ймовірність правильного застосування механізму особистого ключа;

P_i^k – ймовірність правильного застосування механізму біометричного признака.

Доказ вищеподаного співвідношення зводиться до наступного.

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

$$P_{НСД}^n + P_{Зах}^n = 1 \tag{3.2}$$

Далі

$$P_{НСД}^n = 1 - P_{Зах}^n \tag{3.3}$$

Визначимо ймовірність вірної 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]:

$$P^n_{НСД} = 1 - P^n_{Зах} = 1 - P^n_1 P^n_2 \cdots P^n_j = 1 - \prod_{i=1}^{j} P^n_i \quad (3.4)$$

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]:

$$P^k_{НСД} = 1 - P^k_{Зах} = 1 - P^k_1 P^k_2 \cdots P^k_\varepsilon = 1 - \prod_{i=1}^{\varepsilon} P^k_i \quad (3.5)$$

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

$$P^b_{НСД} = 1 - P^b_{Зах} = 1 - P^b_1 P^b_2 \cdots P^b_\varepsilon = 1 - \prod_{i=1}^{\mu} P^b_i \quad (3.6)$$

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

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

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

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

Також практичне значення мають окремі 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	$P_{НСД} = (1 - P_k)(1 - P_b)$	$P_{Зах} = 1 - (1 - P_k)(1 - P_b)$

Таким чином, запропоновано математичні моделі оцінки механізмів багатофакторної автентифікації, при використання яких можна оцінити ймовірності здійснення НСД на основі комбінованих та послідовних механізмів автентифікації. Розроблені математичні моделі можуть бути розповсюджені на довільний розмір простору автентифікації і мають загальний характер.

При їх застосуванні необхідно прийняти наступний підхід. У процесі побудови системи захисту від НСД спочатку бажано визначити перелік факторів, які можна застосувати для здійснення багатофакторної автентифікації. Потім для

кожного з факторів визначити повний перелік атак з існуючих і відомих або потенційних джерел і дати їм оцінки. Після цього можна приймати рішення щодо вибраних факторів та порядку їх застосування [23,29,30,31].

3.3 Висновки по розділу

1. Узагальнено порядок реалізації процедури ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах. Виділені елементи вказаного процесу, його фактори: пароль, пристрій автентифікації, біометрика користувача. Описано алгоритм автентифікації, та порядок користування паролем в різних операційних системах.

Наведено порівняння методів автентифікації по критерію ризику.

2. Запропоновано математичні моделі оцінки захищеності механізмів багатофакторної автентифікації користувачів від несанкціонованого доступу.

Вказані моделі враховують ймовірність виникнення випадку несанкціонованого доступу в мережу та ймовірність захисту мережі від вказаного випадку та дозволяють оцінити загальну захищеність з врахуванням часткових ймовірностей захищеності, які забезпечуються різними факторами автентифікації на основі комбінованих та послідовних механізмів побудови.

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи були виконані 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 огляд методів і засобів ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

– Розроблено та удосконалено механізми ідентифікації та автентифікації користувачів при доступі до роботи з інформацією з обмеженим доступом.

1. У першому розділі кваліфікаційної роботи проведено аналіз загроз та визначено канали витоку технічної інформації. Показана структура технічного каналу витоку інформації. Здійснено аналіз технічних каналів витоку інформації та подана їх класифікація. А саме: розподіл за видом інформаційної діяльності, принципом формування небезпечного сигналу, за середовищем поширення небезпечного сигналу, за способом перехоплення (зняття) небезпечного сигналу засобами технічної розвідки противника.

2. У другому розділі кваліфікаційної роботи проведено огляд існуючих технологій ідентифікації та автентифікації користувача в інформаційно-комунікаційних системах об’єкту інформаційної діяльності. Розглянуто зміст, особливості застосування, переваги та недоліки парольної, апаратної, біометричної ідентифікації та автентифікації користувачів в інформаційно - комунікаційних системах. Подано вимоги до процесів ідентифікації та автентифікації та зміст атак на них.

3. У третьому розділі кваліфікаційної роботи узагальнено порядок реалізації процедури ідентифікації та автентифікації користувачів в інформаційно-комунікаційних мережах. Виділені елементи вказаного процесу, його фактори: пароль, пристрій автентифікації, біометрика користувача. Описано алгоритм автентифікації, та порядок користування паролем в різних

операційних системах. Наведено порівняння методів автентифікації по критерію ризику. Запропоновано математичні моделі оцінки захищеності механізмів багатофакторної автентифікації користувачів від несанкціонованого доступу. Вказані моделі враховують ймовірність виникнення випадку несанкціонованого доступу в мережу та ймовірність захисту мережі від вказаного випадку та дозволяють оцінити загальну захищеність з врахуванням часткових ймовірностей захищеності, які забезпечуються різними факторами автентифікації на основі комбінованих та послідовних механізмів побудови.

ПЕРЕЛІК ПОСИЛАНЬ

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

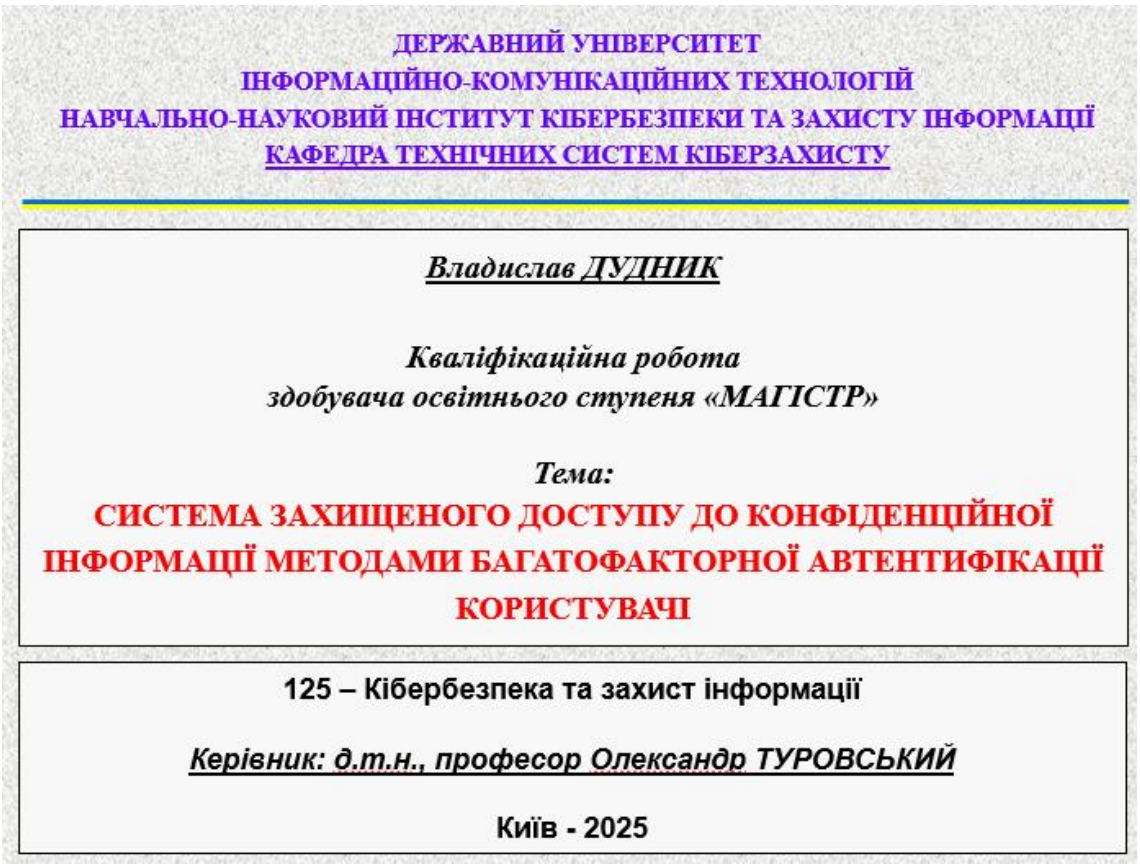
29. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння [Текст]. – введ. 2002 - 28 - 12. - К.: Госпотребстандарт, 2002. – 38 с.

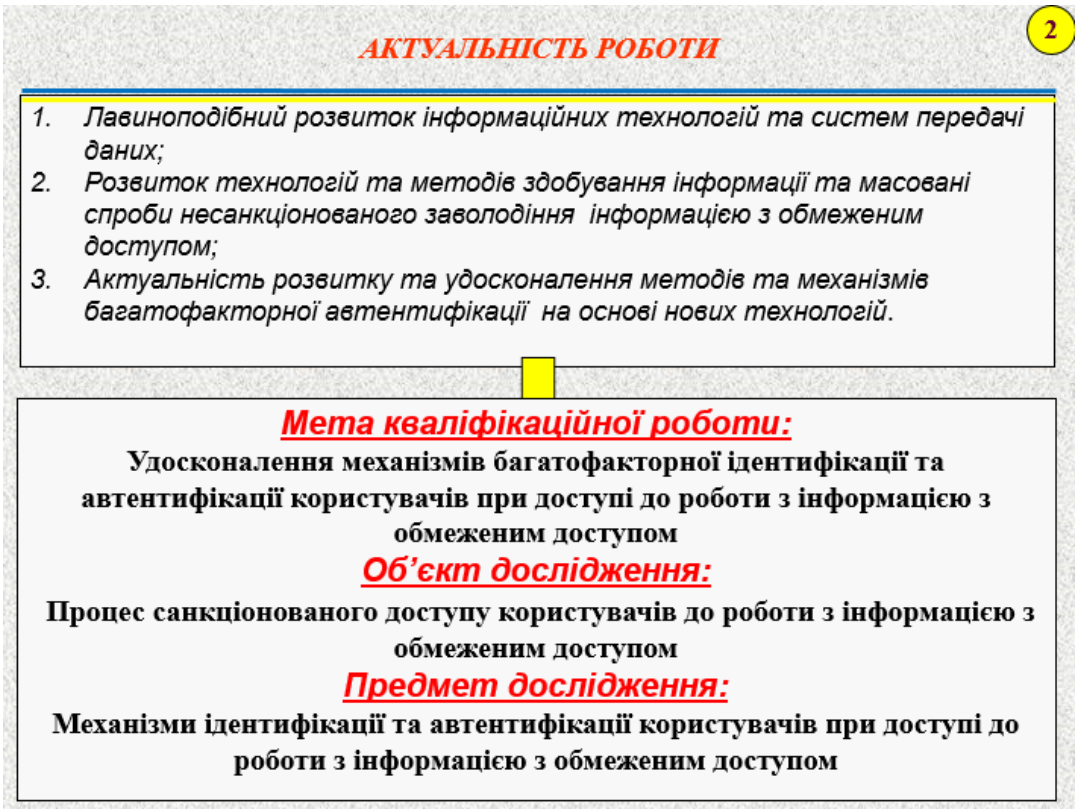
30. ДСТУ ISO/IEC 9798-3-2002 Інформаційні технології. Методи захисту. Автентифікація суб’єктів. Частина 3. Механізми з використанням методу цифрового підпису [Текст]. – введ. 2005 – 09 - 2005. - К.: Госпотребстандарт, 2005. – 17 с.

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

ДОДАТОК

Оформлення слайдів та роздаткового матеріалу





ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

3

1. **РОЗДІЛ 1**: ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

2. **РОЗДІЛ 2**: ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

3. **РОЗДІЛ 3**: РОЗРОБКА МЕХАНІЗМІВ БАГАТОФАКТОРНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ПРИ ДОСТУПІ ДО РОБОТИ З ІНФОРМАЦІЄЮ З ОБМЕЖЕНИМ ДОСТУПОМ

3. **ВИСНОВКИ**: Узагальнено одержані результати

ПЕРШИЙ РЕЗУЛЬТАТ

4

ЗАХИСТ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

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:

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

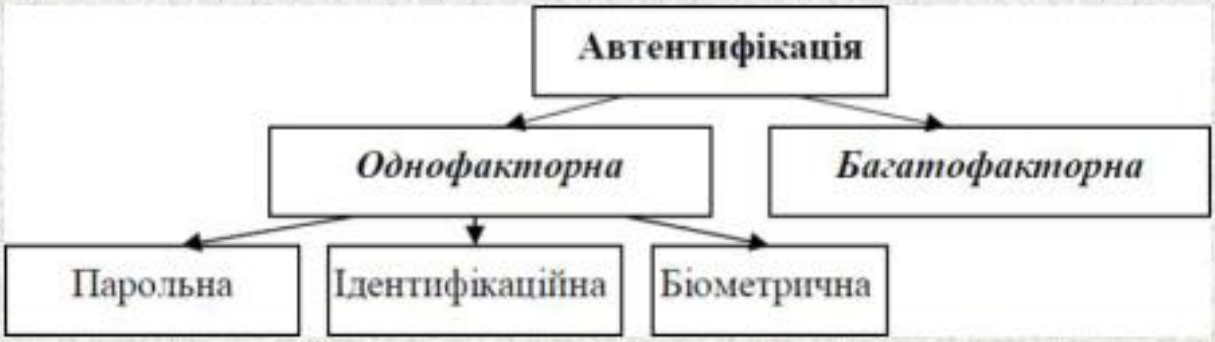
⇩

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

8

ДРУГИЙ РЕЗУЛЬТАТ

СИСТЕМА ТЕХНОЛОГІЙ АВТЕНТИФІКАЦІЇ

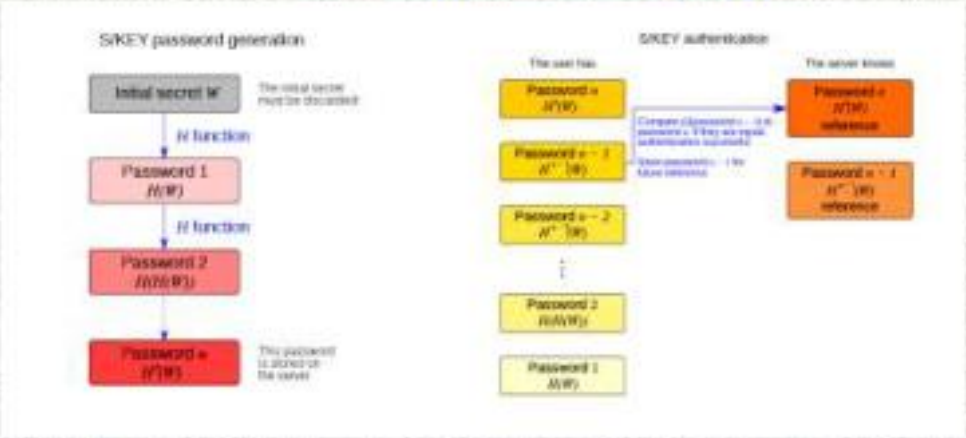


9

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

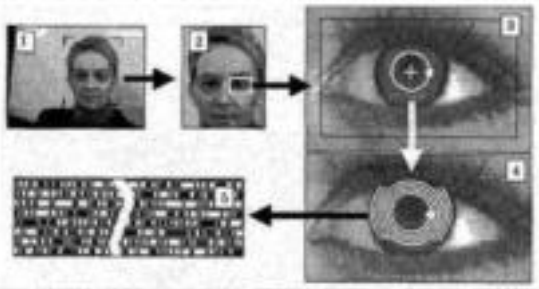
Переносні токени

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.

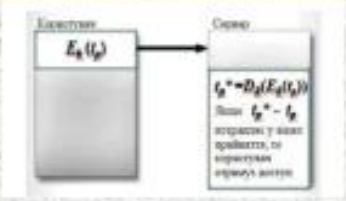
Форма обличчя

ДРУГИЙ РЕЗУЛЬТАТ

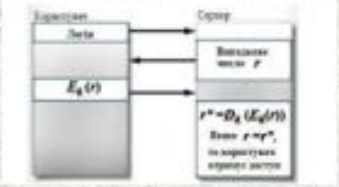
СТАНДАРТИЗАЦІЯ ПРОЦЕСІВ ІНДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

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

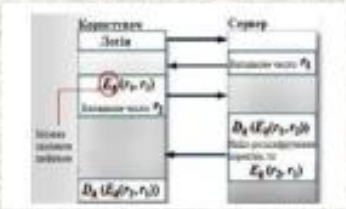
Одностороння автентифікація, заснована на мітці часу



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.

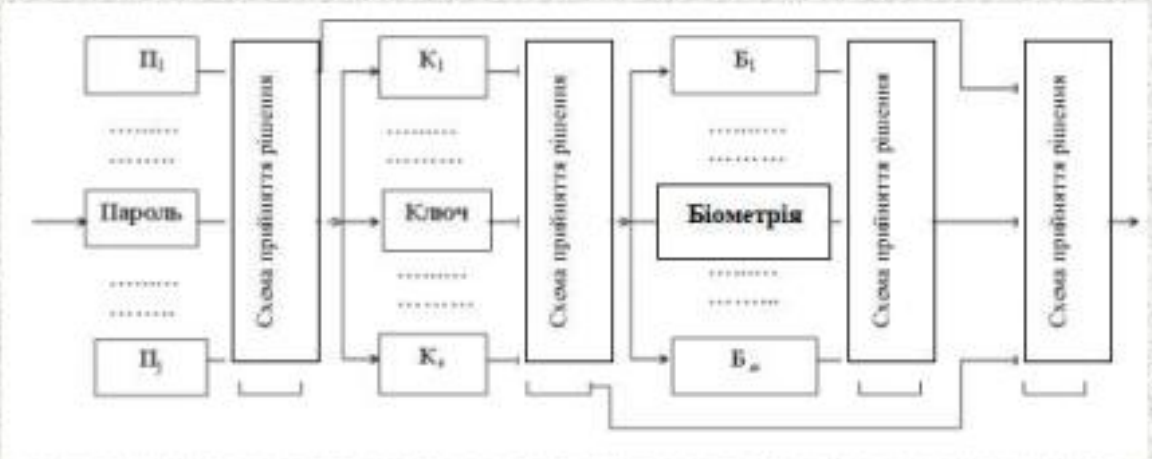
10

ТРЕТІЙ РЕЗУЛЬТАТ

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

БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ

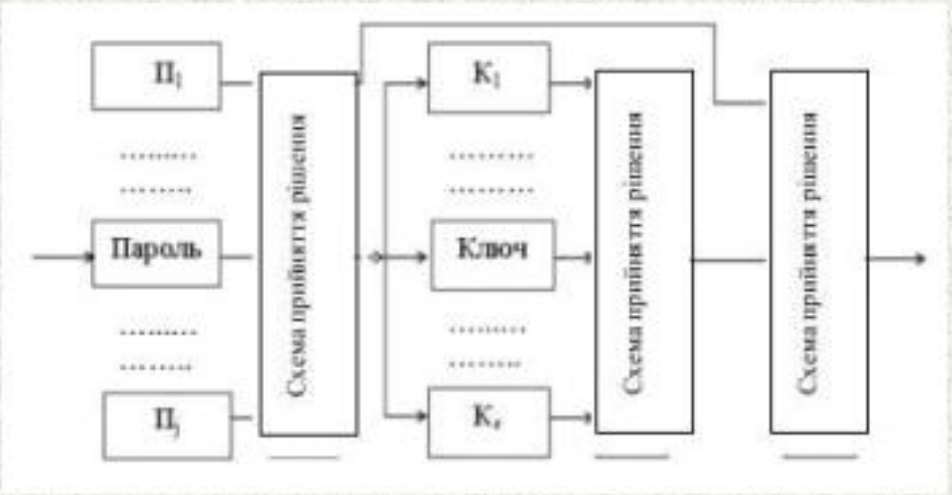
Комбінований механізм трьох факторної автентифікації «пароль – ключ – біометрія»



11

ТРЕТІЙ РЕЗУЛЬТАТ

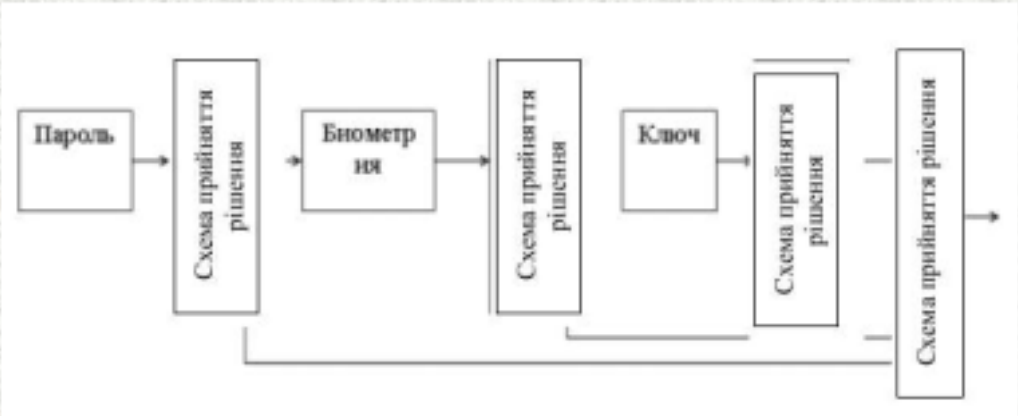
Комбінований механізм двох факторної автентифікації «пароль – ключ»



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

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

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 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 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, **В.Р.Дудник. 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 !

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

Кваліфікаційна робота здобувача освітнього ступеня «МАГІСТР»

СИСТЕМА ЗАХИЩЕНОГО ДОСТУПУ ДО КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ МЕТОДАМИ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Владислав ДУДНИК

Керівник: к.т.н. Олексій ГАВРИЛЕНКО

Київ - 2025

АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

- Актуальність роботи зумовлена необхідністю захисту інформації на об’єктах інформаційної діяльності та протидії несанкціонованому доступу.
- Об’єкт дослідження - процес санкціонованого доступу користувачів до роботи з інформацією з обмеженим доступом.
- Предмет дослідження - механізми ідентифікації та автентифікації користувачів при доступі до інформації з обмеженим доступом.
- Мета роботи - удосконалення механізмів багатофакторної ідентифікації та автентифікації користувачів.
- Завдання: аналіз загроз і каналів витоку; огляд методів і засобів автентифікації; розробка механізму багатофакторного доступу.

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ

1	**РОЗДІЛ 1**	Визначено порядок розподілу інформації, проаналізовано загрози та технічні канали витоку інформації на ОІД.
2	**РОЗДІЛ 2**	Проведено огляд парольних, апаратних і біометричних методів ідентифікації та автентифікації користувачів.
3	**РОЗДІЛ 3**	Розроблено та удосконалено механізми багатофакторної ідентифікації й автентифікації користувачів.
4	**ВИСНОВКИ**	Сформовано практичні рекомендації щодо підвищення захищеності доступу до інформації з обмеженим доступом.

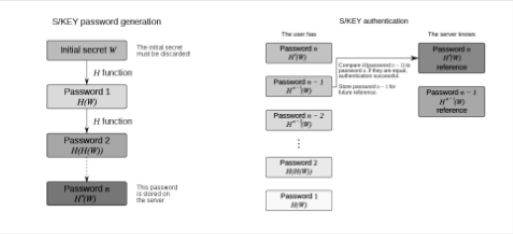
ЗАХИСТ ІНФОРМАЦІЇ НА ОБ’ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

- Визначено загрози інформаційній безпеці та технічні канали витоку інформації на об’єкті інформаційної діяльності.
- Технічний канал витоку включає джерело небезпечного сигналу, середовище його поширення та засіб перехоплення.
- Розглянуто радіоканали, електричні, акустичні, оптичні та матеріально-речовинні канали витоку інформації.

ТЕХНОЛОГІЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

- Ідентифікація дає змогу користувачу назвати себе через унікальний ідентифікатор.
- Автентифікація перевіряє достовірність заявленої особи та право доступу до ресурсу.
- Технології поділяються на однофакторні та багатофакторні, зокрема парольні, апаратні та біометричні.

ПАРОЛЬНА ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

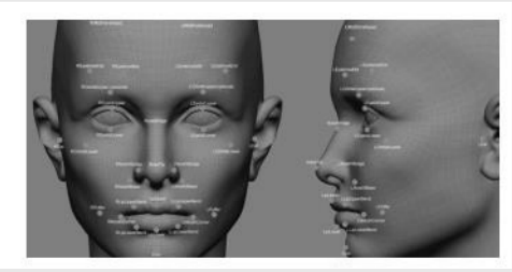


- Парольні системи залишаються найпоширенішим способом перевірки користувача в інформаційно-комунікаційних системах.
- Для підвищення надійності застосовують мінімальну довжину пароля, складність символів, обмеження спроб входу та періодичну зміну паролів.
- Одноразові паролі зменшують ризик повторного використання перехоплених облікових даних.

АПАРАТНА ІДЕНТИФІКАЦІЯ: ТОКЕНИ ТА СМАРТ-КАРТИ

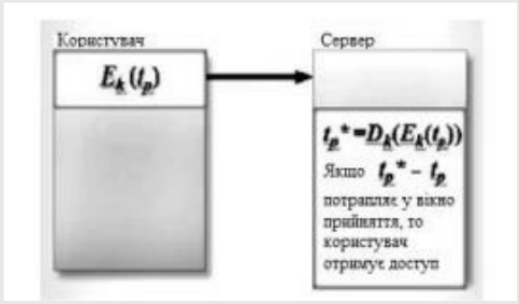
- Апаратна автентифікація ґрунтується на володінні користувачем унікальним пристроєм або електронним ключем.
- Використовуються переносні токени, смарт-карти, безконтактні карти та інші ідентифікатори.
- Токени можуть працювати в асинхронному, PIN/асинхронному, синхронному та PIN/синхронному режимах.

БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ



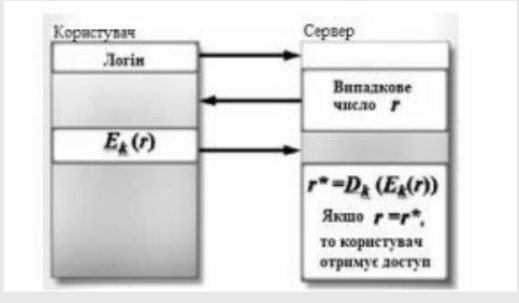
- Біометрична автентифікація ґрунтується на унікальних біологічних характеристиках людини.
- До поширених ознак належать відбитки пальців, райдужна оболонка ока, сітківка, голос, форма обличчя та геометрія руки.
- Перевага біометрії полягає у складності передачі або викрадення ознаки порівняно зі звичайним паролем.

ПРОТОКОЛИ АВТЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ МІТКИ ЧАСУ



- Мітка часу використовується для підтвердження актуальності повідомлення та зменшення ризику повторного використання перехоплених даних.
- Одностороння автентифікація дозволяє перевіряючій стороні встановити достовірність претендента.
- Такі протоколи потребують синхронізації часу та контролю допустимого інтервалу приймання повідомлень.

АВТЕНТИФІКАЦІЯ З ВИКОРИСТАННЯМ ВИПАДКОВИХ ЧИСЕЛ



- Випадкові числа застосовуються як запит, на який претендент формує криптографічно захищену відповідь.
- Перевіряючий розшифровує відповідь і контролює правильність структури запиту.
- У взаємній автентифікації кожна сторона послідовно виконує роль і претендента, і перевіряючого.

АТАКИ НА ПРОТОКОЛИ АВТЕНТИФІКАЦІЇ ТА ЗАХОДИ ЗАХИСТУ

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.

- До типових атак належать повторна передача, підміна повідомлень, перехоплення облікових даних і відображення передачі.
- Ефективними протидіями є мітки часу, випадкові числа, шифрування, контроль цілісності та взаємна перевірка сторін.
- Захист протоколів має поєднувати криптографічні механізми та організаційні правила управління доступом.

МЕХАНІЗМИ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

	для доступу до системи, причому краджка, злом, розголошення конфіденційної інформації не матиме значних наслідків	використання багаторазових паролів	мережі Інтернет
Середній	Потрібно здійснити аутенифікацію для доступу до системи, причому краджка, 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 краджка, лом, розголошення конфіденційної інформації завдасть значної школи	Рекомендується мінімальна вимога - використання багатофакторної аутентифікації	Проведення великий міжбанківськ их операцій керівним апаратом

- У роботі виділено три основні фактори автентифікації: те, що користувач знає, має та чим він є.
- Багатофакторний підхід поєднує пароль, пристрій автентифікації та біометричну ознаку.
- Таке поєднання підвищує стійкість системи до несанкціонованого доступу порівняно з однофакторною схемою.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ПРАКТИЧНЕ ЗНАЧЕННЯ

- Систематизовано технічні канали витоку інформації та загрози на об’єктах інформаційної діяльності.
- Проаналізовано парольні, апаратні та біометричні технології ідентифікації й автентифікації користувачів.
- Удосконалено підхід до багатофакторної автентифікації користувачів при доступі до інформації з обмеженим доступом.
- Запропонований механізм дозволяє підвищити рівень санкціонованого доступу та знизити ймовірність несанкціонованого доступу.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Владислав ДУДНИК

Тема: «Система захищеного доступу до конфіденційної інформації»

Київ - 2025