Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Дослідження методів багатофакторної автентифікації та їх практичного застосування
(тема)

Виконала:
студентка 2 курсу, групи АМСЗІм-18-1
Кавуненко Я.О.
(прізвище, ініціали)
Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)
Керівник: доцент кафедри ІКІ ім. В.В. Поповського
Єпішкін С.О.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В. В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри _____
(підпис)
«_____» _____ 2020 р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентці Кавуненко Яні Олегівні .
(прізвище, ім'я, по-батькові)

1. Тема роботи: Дослідження методів багатофакторної автентифікації та їх практичного застосування затверджена наказом по університету від «17» березня 2020р. №465 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 10.05.2020р.
3. Вихідні дані до роботи: методи ідентифікації та автентифікації, методика захисту від несанкціонованого доступу до інформації шляхом використання багатофакторної автентифікації, аналітичні данні щодо різноманітних типів біометричних систем автентифікації, технологія OpenVPN, застосування USB-токенів у поєднанні з технологією OpenVPN
4. Перелік питань, що потрібно опрацювати в роботі:

1) Застосування методів та механізмів багатофакторної автентифікації
2) Порівняльний аналіз методів та протоколів автентифікації
3) Розробка захищеного методу реалізації дистанційної роботи

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: демонстраційний матеріал у вигляді ppt-презентації; узагальнена модель взаємозв'язку стандартизованих областей біометрії; концептуальна схема узагальненої біометричної системи; схема мережі з використання OpenVPN та ESMART Token; модель токену з сканером відбитку пальця.

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по-батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Єпішкін Сергії Олексійович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	17.02.2020	Виконано
2	Збір матеріалів для дослідження	15.03.2020	Виконано
3	Розробка 1 розділу	25.03.2020	Виконано
4	Розробка 2 розділу	01.04.2020	Виконано
5	Розробка 3 розділу	10.04.2020	Виконано
6	Оформлення дипломної роботи	01.05.2020	Виконано

Дата видачі завдання 17 лютого 2020 року

Студентка _____ Кавуненко Я.О.
(підпис)

Керівник роботи _____ доцент Єпішкін С.О.
(підпис)

РЕФЕРАТ

Пояснювальна записка: 89 с., 34 рис., 13 табл., 23 джерел.

АВТЕНТИФІКАЦІЯ, ІДЕНТИФІКАЦІЯ, НАДІЙНІСТЬ, КОРПОРАТИВНА МЕРЕЖА, КРИПТОАЛГОРИТМ, БІОМЕТРИКА, ПАРОЛЬ, СИСТЕМА ДОСТУПУ.

Об'єкт дослідження – процес автентифікації користувачів комп'ютерних систем і локальних мереж.

Предмет дослідження – методи й засоби автентифікації користувачів у комп'ютерних системах і локальних мережах.

Мета роботи – аналіз шляхів підвищення ефективності побудови сучасних систем автентифікації співробітників у корпоративних мережах за рахунок використання біометричних ознак користувачів.

Методи досліджень – емпіричний аналіз, формалізація та порівняння.

У цей час локальні мережі значно підвищують ефективність діяльності співробітників різних організацій. Але в умовах росту кількості вузлів у мережі виникає проблема забезпечення ефективної й надійної системи автентифікації користувачів. Особливо важливим питанням стає забезпечення захищеного доступу до мережі співробітників при роботі за межами офісу.

У роботі виконаний аналіз поточного стану систем автентифікації користувачів у локальних мережах. Розглянуто їхні достоїнства й недоліки. Особлива увага приділена використанню біометричних систем автентифікації клієнтів при побудові сучасних локальних мереж, які мають істотні переваги в порівнянні з випадком, коли як система доступу використовується парольний захист.

Розроблено модель для налаштування доступу до корпоративної мережі з встановленою двофакторною автентифікацією за технологією OpenVPN та використанням USB-токену.

ABSTRACT

The report contains: 89 p., 34 fig., 13 tables, 23 sources.

AUTHENTIFICATION, IDENTIFICATION, RELIABILITY, CORPORATE NETWORK, CRYPTOALGORITHM, BIOMETRICS, PASSWORD, ACCESS SYSTEM.

A research object is the process of authentication of users of computer systems and local area networks.

The subject of research is methods and means of authentication of users in computer systems and local networks.

An aim of the work is to analyze ways of improving the efficiency of building modern systems of employee authentication in corporate networks by using biometric features of users.

Methods of researches are empirical analysis, formalization and comparison.

At this time, local networks significantly increase the efficiency of employees of different organizations. However, as the number of nodes in the network grows, there is a problem of providing an efficient and reliable user authentication system. A particularly important issue is securing secure access to the employee network when working outside the office.

In this work the analysis of the current state of authentication systems of users in local networks is performed. Their advantages and disadvantages are considered. Particular attention is paid to the use of biometric customer authentication systems in the construction of modern local area networks, which have significant advantages over the case when password protection is used as an access system.

A model has been developed to set up corporate network access with two-factor OpenVPN authentication installed and using a USB token.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

АС – автоматизована система
БіоППІ – біометричний прикладний програмний інтерфейс
БХЛ – біометричні характеристики людини
ГВС – генератор випадкового сигналу
ДКЕ – довгострокові ключові елементи
ДНК – дезоксирибонуклоеїнова кислота
ЕК – електронний ключ
ЕОМ – електронно-обчислювальна машина
ЕЦП – електронний цифровий підпис
ЄС – Європейський Союз
ЄСФОБД – єдина система форматів обміну біометричними даними
ІА – інформація автентифікації
ІБ – інформаційна безпека
ІзОД – інформація з обмеженим доступом
ІС – інформаційна система
ІТС – інформаційно-телекомунікаційна система
КЗ – контрольована зона
КЗІ – криптографічний захист інформації
НДДКР – науково-дослідні та дослідно-конструкторські роботи
НСД – несанкціонований доступ
ОЗП – оперативний запам’ятовувальний пристрій
ОС – операційна система
ПЗ – програмне забезпечення
ПК – персональний комп’ютер
ПЗП – постійний запам’ятовувальний пристрій
СЗІ – система захисту інформації
СКУД – система контролю та управління доступом
ТЗІ – технічний захист інформації
ТС – телекомунікаційна система

DSA – Digital Signature Algorithm – криптографічний алгоритм з використанням відкритого ключа для створення електронного підпису, але не для шифрування

IP-адрес – Internet Protocol Address – унікальний мережевий адрес вузла в комп'ютерній мережі

ICC – Integrated Circuit Card – картка з інтегрованою схемою, щоб охопити всі пристрої, де міститься інтегральна схема

MAC-адреса – Media Access Control – управління доступом до середовища – це унікальний ідентифікатор, що зіставляється з різними типами устаткування для комп’ютерних мереж

PIN – Personal Identification Number – особистий ідентифікаційний номер

RSA – Rivest, Shamir, Adleman – криптографічний алгоритм з відкритим ключем, названий по першим літерам прізвищ авторів

SIM-картка – Subscriber Identification Module – модуль ідентифікації абонента

SMS – Short Message Service – послуга обміну короткими текстовими повідомленнями в телекомунікаційних мережах

ВСТУП

Важливим елементом забезпечення цілісності конфіденційної інформації є захист від несанкціонованого доступу до ресурсів інформаційних систем, що викликає необхідність створення надійних і зручних систем контролю доступу. Кожний користувач сучасних інформаційно-комунікаційних систем декілька разів на день стикається з процедурами ідентифікації та автентифікації. Ці процедури виконуються кожний раз, коли користувач вводить пароль для доступу до інформаційної системи, мережі, бази даних або при запуску прикладної програми. В результаті їх виконання користувач або отримує доступ до певних ресурсів інформаційної системи, або не отримує.

Ідентифікація – процедура розпізнавання користувача в системі за допомогою наперед визначеного імені (ідентифікатора) або іншої інформації про нього, яка сприймається системою. Вона є початковою процедурою надання доступу до системи, після неї здійснюється автентифікація та авторизація.

Автентифікація – це процедура перевірки належності ідентифікатора об'єкту, тобто встановлення чи підтвердження дійсності, і перевірка чи є об'єкт або суб'єкт, що перевіряється, справді тим, за кого він себе видає.

Останнім часом все частіше застосовується, так звана, розширена або багатофакторна автентифікація. Вона побудована на спільному використанні декількох факторів автентифікації. Це значно підвищує захищеність системи.

В якості прикладу можна навести використання SIM-карт в мобільних телефонах. Суб'єкт вставляє апаратно свою картку (пристрій автентифікації) в телефон і при включенні вводить свій персональний ідентифікаційний номер (PIN-код).

Також, до прикладу, у деяких сучасних ноутбуках присутній сканер відбитка пальця. Таким чином, при вході в систему суб'єкт повинен пройти цю процедуру (біометрична автентифікація), а потім ввести пароль.

Вибираючи для системи той чи інший фактор або спосіб автентифікації необхідно насамперед відштовхуватися від необхідного ступеня захищеності, вартості побудови системи та забезпечення мобільності суб'єкта.

Актуальність теми полягає в необхідності переходу сучасних систем контролю та управління доступом (СКУД) до механізмів багатофакторної автентифікації, оскільки з розвитком технологій однофакторна автентифікація все

менш задовольняє вимогам забезпечення послуг інформаційною безпекою (ІБ). «Слабкі паролі користувачів інформаційних систем (ІС) – найбільш вразливе місце, яке використовується зловмисниками, як у великих, так і в малих компаніях. 80% інцидентів у сфері ІБ трапляється внаслідок використання слабких паролів» – до такого висновку дійшла компанія «Trustwave» за результатами власного дослідження, що охоплює ряд компаній у 18 регіонах світу. Використання біометричної автентифікації також не є панацеєю, оскільки деякі системи можна обійти за допомогою муляжів. Найраціональніший вихід з даної ситуації – поєднати декілька методів автентифікації в одній системі, тобто перейти до використання багатофакторної моделі.

Метою дослідження є вироблення та обґрунтування вимог методів багатофакторної автентифікації.

Об’єктом дослідження є інформаційна система, що містить інформацію з обмеженим доступом (ІзОД), або з інших причин має бути забезпечена засобами криптографічного захисту інформації (КЗІ).

Предметом дослідження є механізми автентифікації, що представляють одну з трьох сутностей:

- сутність знання;
- сутність володіння;
- сутність характеристики.

1 ЗАСТОСУВАННЯ МЕТОДІВ ТА МЕХАНІЗМІВ БАГАТОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

1.1 Електронний підпис та проблема створення єдиної системи ідентифікації в Україні

У зв’язку з загальним розповсюдженням комп’ютерних технологій все гострішою встає проблема захисту інформації в комп’ютерних інформаційних системах. Тому дуже актуальними є теоретичні розробки в області захисту комп’ютерної інформації та практичне їх застосування безпосередньо в конкретних комп’ютерних системах.

Питання захисту інформації в комп’ютерних системах вирішується для того, щоб ізолювати інформаційну систему від несанкціонованих 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. Управління доступом – ефективний метод захисту інформації, що регулює використовування ресурсів інформаційної системи, для якої розроблялася концепція інформаційної безпеки. Методи й системи захисту інформації, що спираються на управління доступом, включають наступні функції захисту інформації в інформаційних системах:

– ідентифікація користувачів, ресурсів і персоналу системи інформаційної безпеки;

– впізнання і встановлення вірогідність користувача за обліковими даними, що вводяться (на даному принципі працює більшість моделей інформаційної безпеки);

– допуск до певних умов роботи згідно з регламентом, наказаному кожному окремому користувачу, що визначається засобами захисту інформації і є основою інформаційної безпеки більшості типових моделей інформаційних систем;

– протоколювання звертань користувачів до ресурсів, інформаційна безпека яких захищає ресурси від несанкціонованого доступу і відстежує некоректну поведінку користувачів системи.

Як бачимо, ідентифікація користувачів є необхідним та важливим елементом і основою ефективності будь-якої системи управління доступом до інформаційних ресурсів комп'ютерних систем.

Для забезпечення довіреної передачі даних чинне законодавство в основному охоплює тільки електронні підписи. В Україні немає основ для безпечних, надійних і простих електронних операцій, що включають електронну ідентифікацію, автентифікацію і підписи. Чинне законодавство потребує покращення, розширення та прийняття на рівні Європейського союзу (ЄС).

Відповідно до політики «Кращого регламенту», у ЄС було розглянуто ряд альтернативних політик, кращим варіантом виявилося покращення правової бази, забезпечення міждержавного прийняття та визнання схем електронної ідентифікації та введення інших довірчих послуг, що допомогло б підвищити рівень безпеки та довіри громадян до електронних операцій та призвело б до збільшення ринку транскордонних електронних операцій. Громадяни та підприємства отримували б від неї користь, адже це давало б можливість використовувати засоби електронної ідентифікації, автентифікації та електронного підпису транскордонно. У 2012 році ЄС прийняв Регламент, який реалізував засади такої політики. Його впровадження знизить законодавчу фрагментацію і забезпечить правову єдність країн шляхом введення набору основних правил по безпечній передачі даних.

Для того, щоб дії ЄС були виправдані, необхідно створити умови для розв'язання проблеми міждержавної взаємодії. Разом з тим електронна ідентифікація не може розглядатися в запропонованому Регламенті загальним чином, як інші довірчі послуги, адже випуск засобів ідентифікації є національною прерогативою. Тому цей документ розглядає виключно трансграничні аспекти електронної ідентифікації.

Довірча послуга – це будь-яка електронна послуга, що входить до складу створення, перевірки, підтвердження правильності, обробки та зберігання електронних підписів, електронних печаток, електронних міток часу, електронних документів, послуг електронної доставки, підтвердження справжності сайту та електронних сертифікатів, включаючи сертифікати електронного підпису та електронних печаток.

Кваліфікована довірча послуга – це довірча послуга, яка відповідає прикладним вимогам, передбаченим у Регламенті [1]. Кожна держава-член створює, підтримує і публікує довірчі списки з інформацією, пов'язаною з

провайдерами кваліфікованих довірчих послуг, разом з інформацією про кваліфіковані довірчі послуги, які вони надають.

Наглядові органи повинні гарантувати, що дані провайдерів кваліфікованих довірчих послуг зберігаються і лишаються доступними на протязі відповідного періоду часу, навіть якщо провайдер кваліфікованих довірчих послуг перестає існувати. Провайдери довірчих послуг повинні гарантувати конфіденційність і цілісність даних, що відносяться до особи, якій надається довірча послуга. Після того, як кваліфікована довірча послуга була прийнята, вона не може бути заборонена для здійснення адміністративних процедур або через те, що вона не включена в довірчі списки, встановлені державами-членами.

Регламент, прийнятий у ЄС, гарантує, що довірчі послуги та продукти, які відповідають йому, можуть вільно циркулювати на внутрішньому ринку. Довірчі послуги та кінцеві споживчі продукти, що використовуються при наданні цих послуг, повинні бути доступні для осіб з обмеженими можливостями.

Електронний підпис – це дані в електронній формі, які приєднуються або логічно пов'язуються з іншими електронними даними, і використовуються підписувачем в якості підпису.

Кваліфіковані сертифікати електронного підпису повинні містити:

– вказівку, принаймні у формі, придатній для автоматизованої обробки, що сертифікат був виданий в якості кваліфікованого сертифіката електронного підпису;

– набір даних, які однозначно визначають провайдера кваліфікованих довірчих послуг, що видав кваліфіковані сертифікати, і містить, принаймні, найменування держави-члена, в якій провайдер розташований, та: для юридичної особи: найменування та реєстраційний номер, які наводяться в офіційних документах, для фізичної особи: ім'я особи;

– набір даних, що однозначно визначають підписувача, якому видано сертифікат, включаючи, принаймні, ім'я підписувача або псевдонім;

– дані для перевірки електронного підпису, які відповідають даним для створення електронного підпису;

– відомості про початок і кінець періоду дії сертифікату;

– ідентифікуючий код сертифікату, що має бути унікальним для провайдера кваліфікованих довірчих послуг;

– вдосконалений електронний підпис провайдера кваліфікованих довірчих послуг, що видав сертифікат;

– місце, де підтримується сертифікат вдосконаленого електронного підпису або, доступне безкоштовно;

– місце розташування послуги перевірки статусу дійсності сертифіката;

– відповідну індикацію того факту, що на кваліфікованому пристрої для створення електронного підпису розташовані дані для створення електронного підпису, які пов'язані з даними для перевірки електронного підпису.

Основною проблемою впровадження системи Регламенту в Україні є відсутність сучасної нормативно-правової бази. При розробці нормативно-правової бази електронного цифрового підпису (ЕЦП), в першу чергу закону «Про ЕЦП» [2], в суттєвій мірі орієнтувалась на Директиву ЄС 1999/93 ЄС. Але інформаційні технології розвиваються швидше з кожним роком, тож необхідно поновлювати та вдосконалювати цю базу, а також переходити на транскордонний рівень забезпечення задач інформаційної безпеки.

1.2 Класифікація засобів та методів ідентифікації та автентифікації

Ідентифікацію та автентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів.

Ідентифікація дозволяє суб'єкту (користувачеві, процесу, чи іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я). Шляхом автентифікації друга сторона переконується, що суб'єкт дійсно є тим, за кого себе видає.

Суб'єкт може підтвердити свою справжність, представивши щонайменше одну з наступних сутностей (для однофакторної автентифікації).

1) Щось, що він знає – пароль. Це секретна інформація, якою має володіти тільки авторизований суб'єкт. Паролем може бути голосове або текстове повідомлення, комбінація для замка або PIN-коду.

2) Щось, що йому належить – засіб автентифікації. Важливим фактом є володіння унікальним предметом. Це може бути особиста печатка, ключ, файл даних, що містить характеристику. Дана характеристика часто інтегрується у спеціальний пристрій автентифікації, наприклад, смарт-картку.

3) Щось, що є частиною суб'єкта – біометрика. Характеристикою є фізична особливість суб'єкта. Це може бути портрет, відбиток пальця або долоні, голос або райдужка ока.

Загальна процедура ідентифікації та автентифікації користувача при наданні доступу до АС наведена на рисунку 1.1. Якщо в процесі автентифікації справжність суб'єкта встановлено, система захисту інформації (СЗІ) повинна визначити його повноваження (сукупність прав). Це необхідно для подальшого розмежування доступу до ресурсів [3].

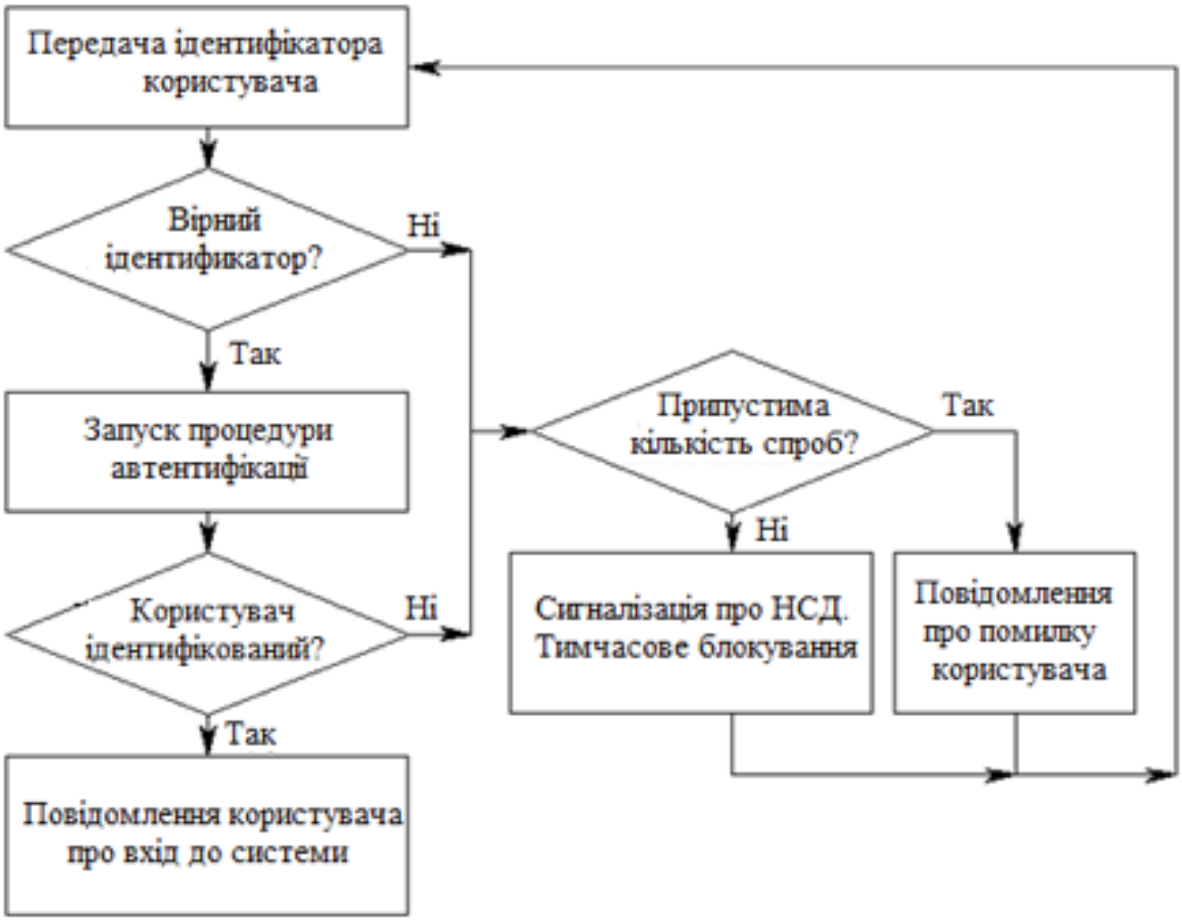

Рисунок 1.1 – Класична процедура ідентифікації та автентифікації

За контрольованим компонентом системи способи автентифікації можна розділити на автентифікацію партнерів за бесідою та автентифікацію джерела даних. Автентифікація партнерів за бесідою використовується при встановленні (та періодичній перевірці) з'єднання під час сеансу. Вона використовується для запобігання таких загроз, як маскарад та повторення попереднього сеансу зв'язку.

Автентифікація джерела даних – підтвердження справжності джерела окремої порції даних.

Автентифікація буває односторонньою, наприклад, коли клієнт доказує свою справжність серверу, та двосторонньою (взаємною). Приклад односторонньої автентифікації – процедура входу користувача до системи.

Процес автентифікації користувача системою можна розділити на два етапи:

– підготовчий – виконується при реєстрації користувача у системі. Саме тоді у користувача запитується зразок автентифікаційної інформації, наприклад, пароль чи контрольний відбиток пальця, який в подальшому розглядатиметься системою як еталон при автентифікації;

– штатний – зразок автентифікаційної інформації запитується у користувача і порівнюється з еталоном. Якщо зразок схожий на еталон із заданою точністю, користувач вважається опізнаним.

Нажаль, надійна ідентифікація та автентифікація ускладнена через ряд принципових причин.

По-перше, комп’ютерна система посилається на інформацію в тому вигляді, в якому вона була отримана, тобто джерело інформації залишається невідомим. Наприклад, зловмисник може скористатися раніше перехопленими даними. Отже необхідно прийняти міри для безпечного вводу та передачі ідентифікаційної та автентифікаційної інформації, що достатньо важко зробити у мережевому середовищі.

По-друге, майже всі автентифікаційні сутності можна викрасти або підробити.

По-третє, наявне протиріччя між надійністю автентифікації з одного боку та зручністю для користувача з іншого. Так, з міркувань безпеки необхідно з певною періодичність просити користувача повторно вводити автентифікаційну інформацію.

В-четверте, чим надійніше засіб захисту, тим він дорожчий [4].

Таким чином, необхідно шукати компроміс між надійністю, доступністю за ціною і зручністю використання та адміністрування засобів ідентифікації та автентифікації.

Сучасні програмно-апаратні засоби ідентифікації та автентифікації за видом ідентифікаційних ознак можна поділити на електронні, біометричні та

комбіновані. До окремої групи, у зв'язку зі специфічним застосуванням, можна виділити системи одноразових паролів, що входять до складу електронних.

Класифікація програмно-апаратних систем ідентифікації та автентифікації представлена на рисунку 1.2 [5].

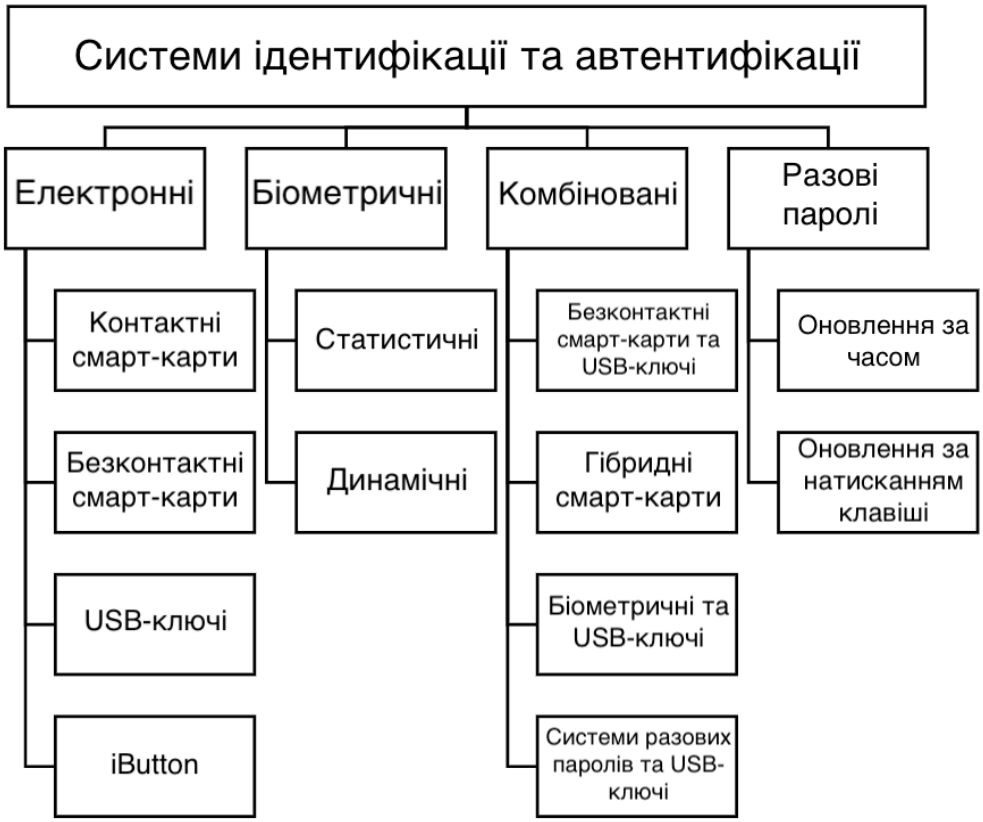

Рисунок 1.2 – Класифікація програмно-апаратних систем ідентифікації та автентифікації

Усі механізми автентифікації можна класифікувати відносно стійкості до атак, яким вони можуть протистояти. В основному, атаки здійснюються в момент передачі інформації автентифікації. Механізми автентифікації засновані на принципі «дещо відомо». Усі такі механізми можливо застосовувати відносно об'єктів автентифікації, а механізми з цифровим підписом – ще й для автентифікації джерела даних.

Основні класи механізмів автентифікації можна визначити таким чином.

1) Клас 0: Незахищений.

2) Клас 1: Захищений від розкриття заявленої інформації автентифікації (ІА).

3) Клас 2: Захищений від розкриття заявленої ІА та атаки типу «повторення» на різних перевірників.

4) Клас 3: Захищений від розкриття заявленої ІА та атаки типу «повторення» на одного перевірника.

5) Клас 4: Захищений від розкриття заявленої ІА та атаки типу «повторення» на одного перевірника або різних перевірників.

Класи механізмів автентифікації де пред'явник є ініціатором.

Клас 0 (Незахищений). У механізмах класу 0 ІА відправляється разом з розпізнавальним ідентифікатором від пред'явника до перевірника. Цей клас є випадком симетричної автентифікації. Механізми цього класу уразливі до розкриття інформації автентифікації та атаки типу «повторення».

Клас 1 (захищений від розкриття заявленої ІА). Даний клас механізмів автентифікації забезпечує захист від розкриття заявленої ІА і може застосовуватися для автентифікації джерела даних та об'єкта. Механізми даного класу використовують функцію перетворення. При цьому інформація автентифікації може поєднуватись із розпізнавальним ідентифікатором, потім застосовується функція перетворення і результат разом з розпізнавальним ідентифікатором передається до перевіряючого.

Основними механізмами даного класу є наступні:

– передача паролю, який в свою чергу був перетворений за допомогою односпрямованої функції (наприклад криптографічне контрольне значення, або хеш-значення);

– передача цифрового відбитку, який зашифровано на таємному ключі;

– передача паролю, який зашифровано на конфіденційному ключі;

– передача цифрового відбитку, який сформовано з використанням особистого ключа.

Механізми автентифікації класу 1 уразливі до атаки типу «повторення». Так, пароль, що передається можна відтворити на рівні протоколу обміну. При цьому відкритий пароль, який використовується на рівні системного інтерфейсу, не розкривається.

Клас 2 (захищений від розкриття заявленої ІА та атаки типу «повторення» на різних перевірників). Даний клас механізмів захищений від розкриття заявленої ІА та атаки типу повтор на різних перевірників. Вразливий даний клас до атаки типу «повторення» на одного перевіряючого. Даний клас ідентичний

класу 1. Додатково на вхід функції перетворення подається унікальна характеристика обраного перевіряючого. Це робиться для додаткового захисту.

Клас 3 (захищений від розкриття заявленої ІА та атаки типу «повторення» на одного перевірника). Механізми даного класу забезпечують захист від розкриття заявленої ІА та атаки типу «повтор» на одного перевіряючого. Для захисту від атаки типу «повторення» функція перетворення використовується разом із унікальною інформацією. Такою унікальною інформацією може бути:

– випадкове або псевдовипадкове число;
– випадкове або псевдовипадкове число певної довжини;
– позначка (мітка) часу;
– лічильник;
– криптографічне зв’язування (значення, отримане зі змісту попередніх даних в деякий момент часу).

В якості функції перетворення може застосовуватись:

– односпрямована функція;
– асиметричний алгоритм;
– симетричний ключ.

Даний клас механізмів застосовується для автентифікації джерела даних та об’єкту.

Клас 4 (Захищений від розкриття заявленої ІА та атаки типу «повторення» на одного перевіряючого та різних перевіряючих).

Проміжний клас 4a – Механізми з унікальним числом. Даний клас механізмів ідентичний класу 3. Додатково на вхід функції перетворення подається характеристика обраного перевіряючого. Це робиться для додаткового захисту.

Проміжний клас 4b – Механізми із запитом паролю. Даний проміжний клас механізмів гарантує захист від атаки типу «повторення». Реалізується він таким чином. У відповідь на запит автентифікації перевіряючий генерує пред’явнику запит на перевірку пароля у формі елемента даних з унікальним числом. Пред’явник за допомогою деякої функції перевіряє пароль та повертає результуюче значення цієї функції перевіряючому. В якості функції перетворення для механізмів із запитом паролю можуть використовуватись наступні:

– односпрямована функція;
– асиметричний алгоритм;
– симетричний алгоритм;

– не криптографічний алгоритм (наприклад, використання пар одержаних запитів на перевірку пароля).

Даний проміжний клас використовується для автентифікації джерела даних та об’єктів.

Проміжний клас 4c – Спеціалізовані механізми із запитом паролю та шифруванням. Механізм цього класу ґрунтується на трьох обмінах інформацією між пред’явником і перевірником. В якості функції перетворення для даних механізмів можуть бути використані наступні:

– асиметричний алгоритм;

– симетричний алгоритм.

Проміжний клас 4c використовується для автентифікації джерела даних та об’єктів.

Проміжний клас 4d – Механізми з обчисленням відповіді. Механізми з обчисленням відповіді залучають трьох прохідну передачу інформації. При застосуванні механізму із класу 4d забезпечується захист від атаки типу «маскарад». Порушник може обчислити відповідь для деяких запитів, але не для всіх. Чим більше число обмінів виконується, тим менша імовірність такого вгадування.

Всі вище описані механізми можуть застосовуватись для випадків, коли ініціатором автентифікації є перевіряючий. При цьому зміниться кількість обмінів інформацією.

Механізми автентифікації можна класифікувати за методами одержання перевірочної інформації автентифікації наступним чином [6]:

– інтерактивні сертифікати автентифікації;

– автономні сертифікати автентифікації;

– перевірочна ІА, яка надається додатковим шляхом (наприклад, використовуючи захищений канал зв’язку).

Механізм взаємної автентифікації можна отримати за допомогою однопрохідних механізмів. Для цього можна застосовувати класи 1, 2, 3 та 4a. При цьому обміни інформацією можна виконувати в одному з двох напрямків для виконання взаємної автентифікації. Для проміжних класів 4b та 4c однаковий тип механізму можна виконувати в обох напрямках. Тобто, наприклад, перший запит на перевірку може надсилатися разом із запитом на автентифікації. Дані проміжні класи для виконання механізму в обох напрямках обов’язково вимагають

однакового числа обмінів. Проміжний клас 4b може використовуватись разом з механізмами класу 4c. Для реалізації направленої автентифікації у проміжному класі 4d необхідно не менше 3-х обмінів інформацією, у той час як для взаємної автентифікації необхідно хоча б 4-и передавання. В таблиці 1.1 представлена стійкість різних класів до вразливостей.

Таблиця 1.1 – Стійкість класів механізмів автентифікації до вразливостей

Клас / **Уразливості**	0	1	2	3	4a	4b	4c	4d
Розкриття заявленої ІА	+	-	-	-	-	-	-	-
Атака типу повтор на різних перевіряючи	+	+	-	+	-	-	-	-
Атака типу повтор на одного перевіряю чого	+	+	+	-	-	-	-	-
Атака типу підміна, де ініціатор – зловмисник	-	-	-	-	-	-	-	-
Атака типу підміна, в якій зловмисник є відповідачем	+	-	-	-	-	-	-	-

На Україні основними стандартами з автентифікації є ДСТУ ISO/IEC 9798-1:2002 (Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 1. Загальні положення), ДСТУ ISO/IEC 9798-3:2002 (Інформаційні технології. Методи захисту. Автентифікація об’єктів. Частина 3. Механізми, що ґрунтуються на цифровому підписі).

На міжнародному рівні були прийняті наступні стандарти: ISO/IEC 9798-1:2009 (Information technology. Security techniques. Entity authentication. Part 1: General), ISO/IEC 9798-2:2009 (Information Technology. Security Techniques. Entity Authentication. Part 2: Mechanisms Using Symmetric Encipherment Algorithms), ISO/IEC 9798-3:2009 (Information technology. Security techniques. Entity authentication. Part 3: Mechanisms using digital signature), ISO/IEC 9798-4:2009 (Information technology. Security techniques. Entity authentication. Part 4:

Mechanisms using a cryptographic check function), ISO/IEC 9798-5:2009 (Information technology. Security techniques. Entity authentication. Part 5: Mechanisms using zero knowledge techniques), ISO/IEC 9798-6:2009 (Information technology. Security techniques. Entity authentication. Part 6: Mechanisms using manual data transfer).

1.3 Актуальність застосування моделей багатофакторної автентифікації

Використання парольної автентифікації в ІС підприємств та організацій себе вичерпує. Продовжуючи застосовувати цю традиційну методику доступу до власних інформаційних ресурсів, компанії фактично ставлять під загрозу рентабельність і, напевно, саме існування підприємства.

Це твердження має сенс и відноситься, перш за все, до компанії фінансового сектору, а також ряду компаній, що виконують науково-дослідні та дослідно-конструкторські роботи (НДДКР) у високотехнологічних секторах ринку.

Компанія «Trustwave» за результатами власного дослідження, що охоплює ряд компаній у 18 регіонах світу дійшла до висновку що 80% інцидентів у сфері інформаційної безпеки трапляється внаслідок використання слабких паролів. Аналітики присвятили дослідження вразливості елементів у системах інформаційної безпеки, у процесі якого вивчили більше 300 інцидентів, що мали місце у 2011 році. Головний висновок: слабкі паролі користувачів ІС – найбільш вразливе місце, яке використовується зловмисниками, як у великих, так і в малих компаніях.

Слабкий пароль – це погано, але зворотня сторона застосування складних паролів – важкий процес запам’ятовування користувачем. Як наслідок – недбалість їх зберігання у вигляді робочих записів, а в цьому випадку вже не має значення, чи буде пара логін/пароль записана в особистому блокноті співробітника, чи закріплена на моніторі липким листком. Знаючи традицію поводження з такими даними працівників компаній, зловмиснику буде легко отримати ці відомості. Якщо ще врахувати часто застосовану «синхронізацію» паролів для доступу до різноманітних ресурсів. Таким чином два з трьох стовпів ІБ підприємства звалилися.

Деякі зарубіжні компанії, що працюють у сфері аналізу інцидентів в системах безпеки, роблять висновок: несанкціонований доступ до ІзОД щодо фінансової активності підприємства, договорів та графіків здатний призвести не

те, що до втрат, а до розорення . Щорічні втрати від витоків інформації в США оцінюються в мільярдах доларів. Російський галузевий портал «Інформаційна Безпека Банків» в оцінці фінансового збитку від можливих зловживань співробітників посилається на дослідження Асоціації експертів з боротьби з шахрайством (ACFE, США), яка бачить цю суму в розмірі 6 % прибутку банку за рік. За спостереженнями асоціації, втрати при подібних інцидентах, в середньому, досягали $ 100 тис., а в 14,6 % перевищили $ 1 млн. Дослідницька компанія «Javelin Strategy» у своєму щорічному дослідженні, опублікованому в лютому 2012 року, оцінила світовий обсяг шахрайства та витоків даних з організацій за 2011 рік в $ 18 млрд.

Незважаючи на безліч засобів обчислювальної техніки і широкий спектр технологічних рішень, вибір методів автентифікації для компаній, що планують своє майбутнє, невеликий – багатофакторна автентифікація. Однофакторної або парольної автентифікації для безпечної роботи з інформаційними системами в розвиненому бізнесі вже недостатньо [7].

Багатофакторна або розширена автентифікація вже сьогодні застосовується низкою українських компаній у сфері фінансів при створенні сервісів інтернет-банкінгу , мобільного банкінгу, файлообміну і подібних рішень для кінцевих користувачів. Вона заснована на спільному використанні декількох факторів автентифікації (знань, засобів або об'єктів зберігання одній з інформаційних складових легітимної процедури автентифікації), що значно підвищує безпеку використання інформації, щонайменше, з боку користувачів, що підключаються до інформаційних систем по захищеним і незахищеним каналам комунікацій.

Як приклад може послужити процес двофакторної автентифікації користувача, реалізований в даний час низкою українських банків: вхід в особистий кабінет користувача за допомогою мережі інтернет можливий після введення пароля на сторінці, після чого (у разі підтвердженої правомірності), слідує передача одноразового пароля (у вигляді SMS) на мобільний телефон, раніше зареєстрований користувачем.

Аналогічні схеми контролю та управління повноваженнями користувача, його подальших дій у корпоративних чи інших інформаційних системах, можуть бути реалізовані із застосуванням самих різних засобів і методів, вибір яких досить широкий, як за технологічністю, вартістю, виконанню, так і за можливими комбінаціями перерахованих властивостей. Сесія роботи користувача може також контролюватися на предмет відповідності, як IP-адреси останньої успішно

завершеною сесії, так і MAC-адреси відповідного мережного обладнання. Далі можуть йти дії підтвердження або відмови в доступі до інформаційних ресурсів, але довіри до цих двох параметрів контролю бути не може в силу їх технологічної слабкості: IP-адресу можна підмінити, а MAC-адресу просто переписати в ході роботи системи, і навіть без перезавантаження. Проте, як певні контрольні значення ці відомості можуть бути використані.

Наведемо кілька прикладів двофакторної і багатофакторної автентифікації. Методика автентифікації за допомогою SMS заснована на використанні одноразового пароля: перевага такого підходу, в порівнянні з постійним паролем в тому, що цей пароль не можна використовувати повторно. Навіть якщо припустити, що зловмисникові вдалося перехопити дані в процесі інформаційного обміну, він не зможе результативно використовувати вкрадений пароль для отримання доступу до системи. А ось приклад , реалізований із застосуванням біометричних пристроїв і методів автентифікації: використання сканера відбитка пальця, який мається на ряді моделей ноутбуків. При вході в систему користувач повинен пройти процедуру сканування пальця, а потім підтвердити свої повноваження паролем. Успішно завершена автентифікація дасть йому право на використання локальних даних конкретного персонального комп’ютеру (ПК). Проте, регламентом роботи в ІС може бути передбачена окрема процедура автентифікації для доступу до мережевих ресурсів компанії , яка крім введення іншого пароля може включати в себе цілий ряд вимог до подання автентифікатора суб'єкта. Але навіть за такої реалізації, захищеність системи, безсумнівно, посилюється [8]. Аналогічним чином можуть бути використані й інші біометричні автентифікатори.

Як нам вже відомо, будь-який метод автентифікації має свою ймовірність помилки, а точніше так звані помилки першого і другого роду. Нас насамперед цікавить зменшення ймовірності помилки другого роду, тобто проникнення зловмисника в систему під виглядом авторизованого користувача. Для однофакторних моделей автентифікації така ймовірність є точною характеристикою системи, в багатофакторної моделі вона обчислюється з часткових ймовірностей . При побудові схем багатофакторної автентифікації можуть використовуватися механізми з послідовним, паралельним або комбінованим застосуванням факторів. Під послідовним застосуванням факторів будемо розуміти таке їх використання , при якому помилка хоча б по одному з них , тобто отримання несанкціонованого доступу (НСД), призводить до відмови

в доступі. Тобто, послідовна структура багатофакторної автентифікації працездатна, якщо всі її фактори разом забезпечують з певною ймовірністю відмову в НСД. Послідовний механізм факторної автентифікації можна використовувати при побудові схем багатофакторної автентифікації. За таких умов для протидії НСД необхідно, щоб хоча б один фактор не був пройденим успішно. Тобто, послідовна схема автентифікації працездатна, якщо всі її елементи працездатні. Під паралельним використанням факторів автентифікації будемо розуміти таке їх одночасне застосування, при якому НСД відбувається тоді, коли хоча б по одному з них отримано НСД. У теж час, паралельні схеми автентифікації можуть, а по суті повинні, коли їх кілька, застосовуватися послідовно. У цьому випадку необхідно говорити про комбіновані механізми автентифікації. Розглянемо спочатку комбіновані схеми багатофакторної автентифікації з паралельно-послідовним з'єднанням елементів [9]. У цьому випадку можливе використання декількох факторів – наприклад паролів, особистих ключів та біометричних ознак. Структурну схеми реалізації механізму трьохфакторної автентифікації наведено на рисунку 1.3 [9].

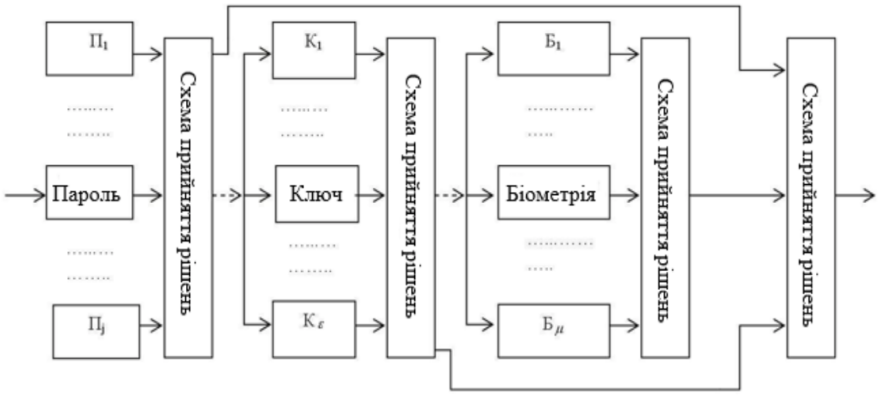

Рисунок 1.3 – Комбінований механізм трьохфакторної автентифікації

Ймовірність НСД для цього механізму визначається за формулою (1.1):

$$P_{НСД} = (1 - \Pi_{i=1}^{j} P_i^n) \cdot (1 - \Pi_{i=1}^{\varepsilon} P_i^k) \cdot (1 - \Pi_{i=1}^{\mu} P_i^\sigma), \qquad (1.1)$$

де P_i^n – ймовірність правильної роботи механізму використання паролю;

P_i^k – ймовірність правильного застосування механізму особистого ключа;

P_i^{σ} – ймовірність правильного застосування механізму біометричної ознаки.

1.4 Захист від несанкціонованого доступу за допомогою багатофакторної моделі

НСД – доступ до інформації, що здійснюється з порушенням правил розмежування доступу. Виділяють наступні методи здійснення НСД в комп'ютерних системах та мережах:

- використання програмних закладок;
- використання апаратних закладок;
- використання вірусних програм;
- крадіжка носіїв інформації, що захищається;
- незаконне копіювання інформації, що захищається;
- перехоплення по технічному каналу витоку інформації;
- НСД до системного програмного забезпечення (ПЗ).

Згідно з документами системи захисту інформації (ТЗІ) (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) за результатом впливу на інформацію та систему її обробки загрози поділяються на такі класи:

- порушення конфіденційності інформації (отримання інформації користувачами або процесами всупереч встановленим правилам доступу);
- порушення цілісності інформації (повне або часткове знищення, викривлення, модифікація, нав'язування хибної інформації);
- порушення доступності інформації (часткова або повна втрата працездатності системи, блокування доступу до інформації);
- втрата спостережливості або керованості системи обробки (порушення процедур ідентифікації та автентифікації користувачів та процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).

Для того щоб забезпечити захист інформації та ресурсів від НСД потрібно як мінімум надавати користувачам послуги спостережливості, конфіденційності, в тому числі прибирати можливість негативного впливу на інформацію, втручання у процес її обробки, порушення працездатності автоматизованої системи (АС).

Тобто, захищати необхідно всі компоненти АС від НСД: апаратуру та обладнання, програми, дані, персонал.

Процес виявлення НСД до інформації та ресурсів засновується на системній класифікації, що здійснюється за наступними критеріями:

– всі загрози НСД поділяються на природні та техногенні. Природні загрози НСД спричиняються стихійними природними явищами та об'єктивними фізичними процесами. Техногенні загрози НСД є наслідком діл рук людини, технічних засобів і систем;

– за походженням техногенні загрози НСД поділяються на випадкові та навмисні. Випадкові загрози НСД спричиняються помилками проектування АС та системи захисту інформації, помилками у програмному забезпеченні, збоями та відмовами апаратури та систем забезпечення, помилками персоналу тощо. Навмисні загрози НСД спричинені діями людей;

– за місцем розміщення джерел загроз НСД відносно АС навмисні загрози НСД поділяються на дистанційні та контактні. До дистанційних відносяться такі загрози як НСД, джерело яких знаходиться за межами підконтрольної території. Контактні загрози НСД здійснюються в межах підконтрольної зони, як правило при проникненні в приміщення, де знаходяться засоби обробки та зберігання інформації.

За типом основного засобу, який використовується для реалізації загрози НСД, всі джерела загроз поділяються на такі групи: людина, апаратура, програма та фізичне середовище. На практиці при спробі НСД задіяні всі або деякі групи. Основним призначенням інформаційної системи є надання користувачам (системи, інформації) послуг в виконанні різних інформаційних завдань (наприклад, бізнес, банк, послуги). При цьому, в процесі їх вирішення ставиться задача мінімізації втрат власників та користувачів.

У захищених інформаційно-телекомунікаційних системах (ІТС) можна виділити чотири типи суб’єктів зображених на рисунку 1.4:

– користувачі К1 та К2, що є джерелами та одержувачами інформації;

– телекомунікаційна система (ТС);

– крипто аналітична система, що представляє собою сукупність порушників або зловмисників;

– арбітр.

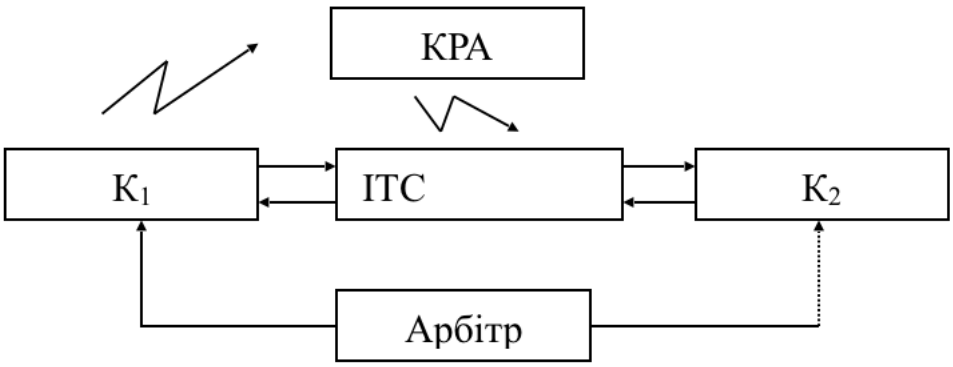

Рисунок 1.4 – Модель захищеної інформаційно-телекомунікаційної системи

Порушник (зловмисник) – навмисно чи не навмисно реалізує погрози з метою нанесення втрат системі та або власникам , користувачам.

Погроза – потенційно існуюча небезпека нанесення втрат в системі, в результаті реалізації деяких дій порушниками та зловмисниками. Існують такі типи загроз:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності;
- порушення спостережливості;
- порушення справжності та неспростовності.

Погрози бувають активні і пасивні.

Пасивна – це така погроза, у результаті реалізації якої не змінюється інформаційний стан системи, але збиток присутній.

Активна – це така погроза, в результаті реалізації якої змінюється стан інформаційної системи та присутні збитки власникам та або користувачам системи.

Порушник – це така особа, яка ненавмисно, внаслідок необізнаності, цілеспрямовано, за злим наміром або без нього, використовуючи різні можливості, методи та засоби здійснила спробу зробити операції, які призвели або можуть призвести до порушення властивостей інформації, що визначаються політикою безпеки.

Модель порушника відображає його практичні та потенційні можливості, апріорні знання, час та місце дії тощо. Під час коли розробляють модель порушника визначаються:

– припущення щодо категорії осіб, до яких може належати порушник;

– припущення щодо мотивів дій порушника (цілей, які він переслідує);

– припущення щодо рівня кваліфікації та обізнаності порушника та його технічної оснащеності (щодо методів та засобів, які використовуються при здійсненні порушень);

– обмеження та припущення для характеру можливих дій порушника (за часом та місцем дії та ін.).

Розберемо модель порушника, припускаючи наявність у системі порушника другого рівня (порушник корпоративного типу, може створити спеціальні технічні засоби, вартість яких може співвідноситьсь з можливими фінансовими втратами , спотворення та знищення інформації, що захищається. В такому разі для розподілу обчислень при проведенні атак можуть бути застосовані локальні обчислювальні мережі).

Припускається, що особи, такі як адміністратори, та співробітники підрозділів з розробки та супроводження програмного забезпечення не відносяться до потенційних порушників. Співробітники служби захисту інформації є висококваліфікованими користувачами, але завдяки своїм функціональним обов’язкам вони мають доступ майже до повного набору інформації, звідси можемо зробити таке припущення, що вони не будуть робити спроб для подолання засобів захисту. Внутрішній порушник не може проводити атаку за межами контрольованої зони (КЗ) та має приховувати свої дії від інших співробітників. У ролі зовнішніх порушників виступають хакери [10].

2 ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ТА ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ

2.1 Криптографічні протоколи автентифікації та види атак на них

Протокол ідентифікації – алгоритм спільних дій двох суб’єктів спрямований на підтверження особистості одного із суб’єктів-учасників протоколу.

Дуже важливими характеристиками криптографічного протоколу є можливість перевірки автентичності (справжності) об’єктів (суб’єктів), які взаємодіють між собою, встановлення автентичності та криптографічна живучість ключів. Тож розглянемо основні поняття та визначення щодо криптографічних протоколів автентифікації.

У найбільш узагальненому вигляді під криптографічним протоколом автентифікації будемо мати на увазі криптографічний протокол встановлення достовірності твердження, що об’єкт (суб’єкт) має очікувані властивості. Як правило, достовірність твердження встановлюється з деякою ймовірністю. Тому має сенс застосувати таке визначення протоколу автентифікації: автентифікація об’єкта (суб’єкта) – це підтвердження із заданою ймовірністю того, що об’єкт (суб’єкт) є тим, за кого він себе видає.

Протокол цифрового підпису – алгоритм дій двох або більше суб’єктів з доведенням того, що певна інформація є цілісною, справжньою та належить одному суб’єктові – учасникові протоколу.

Основні характеристики (параметри) криптопротоколів [11]:

- автентифікація суб’єктів;
- автентифікація ключів;
- вид автентифікації;
- вид автентифікації ключів;
- вид підтвердження ключів;
- новизна ключів;
- управління ключами;
- складність обчислень;
- можливість попередніх обчислень;
- захищеність від раніше переданих повідомлень;
- вимоги до третьої сторони;

– крипто живучість ключів;

– складність криптоаналізу;

– неспростовність;

– число повторень (раундів, обмінів).

При виконанні криптопротоколів необхідно забезпечити якість. На основі цього потрібно зрозуміти наскільки вид протокола задовольняє вимогам та користувачам. Автентифікація ключів може бути явна та неявна. Явна автентифікація ключів, якщо реалізований етап підтвердження ключів.

Управління (контроль) ключами – спроможність абонентів використовувати ключі при необхідності.

Вимоги до третьої сторони:

– поставка загальних параметрів;

– виготовлення сертифікатів.

Криптоживучість ключів – спроможність криптосистеми забезпечувати криптоживучість криптограм.

Неспростовність – гарантії того, що можна довести, що «А» передав повідомлення, а «В» прийняв його та обробив.

У таблиці 2.1 наведено основні криптографічні співвідношення, що стосуються генерування асиметричних пар ключів для ЕЦП [11].

Таблиця 2.1 – Параметри асиметричних пар ключів

Ключі та параметри /Вид КРП ЕЦП	Асиметрична пара (ключі)	Конфіденційний ключ ЕЦП	Відкритий ключ (сертифікат) ЦП	Загальносистемні параметри ЦП	Складність криптоаналізу
Перетворення RSA	(E_i, D_i)	E_i	D_i	$P = NQ$	Субекспоненційна
Перетворення DSA (ГОСТ Р 34.10-94)	(X_i, Y_i)	X_i	$Y_i = g_i^x (mod)P$	P, q, g	Субекспоненційна
Перетворення ДСТУ 4145 - 2002 (ISO/IEC14888-3, ISO/IEC 9796-3)	(d_i, O_i)	d_i	$O_i = d_i G(mod)q$	$a, b, G, n, f(x)(P), h$	Експоненційна
Перетворення зі спарюванням точок ЕК	(d_{iD}, Q_{iD})	$D_i = sQ_{iD}$	$Q_{iD} = H_i(ID)$	G_1, G_2, e, H_1, P, H_2, H_3,F^{2m}, P_p	Міжекспоненційна та субекспоненційна

Усі відомі атаки відносно механізмів автентифікації можна розділити на два основних види [11]:

– атака типу «повтор» (раніше передане повідомлення) – при реалізації якої порушник спочатку записує обмінну ІА, запам’ятовує її, а потім пізніше передає, тобто відтворює;

– атака типу «підміна» – обмін якої при реалізації ІА перехоплюється, підміняється та оперативно знову відтворюється, наприклад, передається перевірнику.

Структуру типів атак на механізми та протоколи автентифікації подано на рисунку 2.1 [11].

Рисунок 2.1 – Класифікація атак на механізми та протоколи автентифікацію

Атака типу «повтор» можлива за умов знання декількома перевірниками перевірочної ІА комітента, наприклад, засобом її перехоплення, запам’ятовування та наступного відтворення. Така атака називається «раніше переданим повідомленням», так як, по суті, при її реалізації відтворюється санкціонована пред’явником ІА. У випадку вдалої реалізації атаки типу «повтор» її іноді називають «маскарад».

Основним моментами захисту проти атаки типу «повтор» є використання запитів, наприклад паролів, маркерів з підписаною ІА тощо. При цьому запити генеруються перевірником, але перевірник не може використовувати один і той самий запит на пароль більш ніж один раз, тому їх джерело повинне ґрунтуватися на різноманітних послідовностях. Для протистояння атаці типу «повтор» можна застосовувати унікальні числа, наприклад, номери передач, випадкові числа, а також робити запити паролів. При цьому унікальні числа генерує пред’явник, а при повторенні унікального числа (чи даних) перевірник від нього відмовляється, тобто воно однаковим перевірником не приймається. Для протистояння атаці

типу «повтор» для різних перевірників, як правило, необхідно використовувати запити паролів. Також для протистояння атаці типу «повтор» для різних перевірників використовується обчислення заявленої ІА, наприклад, будь-яких характеристик, які є унікальними для перевірника, у першу чергу таких, як ім’я, IP-адреса або взагалі будь-які атрибути, що містять перевірочну ІА.

В атаці типу «підміна» порушник виступає в ролі ініціатора автентифікації. Такий вид атак можливий тільки в такому випадку, коли ініціаторами можуть бути як пред’явник, так і перевірник. У процесі реалізації атаки пред’явник і перевірник можуть обмінятися інформацією автентифікації через порушника. При цьому порушник для перевірника є пред’явником, а для пред’явника перевірником. Метою атаки типу «підміна» для порушника «С» є спроба представити себе для перевірника «В» як пред’явника «А». Дії порушника при виконанні атаки можна подати таким чином. Порушник одночасно взаємодіє як з «А», так і з «В». Причому порушник «С» представляється для «А» перевірником «В» і робить запит на його автентифікацію. Далі порушник «С» представляється для «В» пред’явником «А» і робить запит, щоби «В» автентифікував його. У процесі автентифікації пред’явник «А» насправді взаємодіє з порушником «С», який видає себе за перевірника «В», і таким чином порушник «С» отримує деяку інформацію від пред’явника «А», яку потім використовує в процесі автентифікації з перевірником «В». Далі в процесі автентифікації перевірник «В» взаємодіє з порушником «С», який видає себе за пред’явника «А», і таким чином порушник «С» одержує деяку інформацію від перевірника «В», яку потім використовує в процесі автентифікації з пред’явником «А». Далі порушник «С» бере участь в процесі автентифікації з перевірником «В» як уже автентифікованим пред’явником «А».

Для протидії атаці «підміна» необхідно:

– встановити з необхідною ймовірністю ініціатора взаємодії – це завжди або пред’явник, або перевірник;

– обмінна ІА, яка надається пред’явником, повинна розрізнятися залежно від статусу пред’явника щодо ініціювання процесу автентифікації, що дає можливість перевірникові відстежувати факт перехоплення обмінної ІА.

Для того щоб атаки типу «підміна» реалізувалась, у якій порушник є відповідачем, порушнику потрібно перебувати посередині між ініціатором та

відповідачем. Спочатку він перехоплює інформацію автентифікації та відправляє її відповідачу, виконуючи якби то роль ініціатора.

Надалі атака типу «підміна» може виконуватися наступним чином:

– коли порушник очікує моменту, щоб його помилково прийняли за відповідача;

– систематично, тобто коли порушник видає себе за відповідача.

Для захисту від атаки типу «підміна» можна використовувати такі механізми як додаткові послуги, на сам перед такі, як контроль цілісності або забезпечення таємності при додатковому обміні даними. При цьому обмінну ІА можна комбінувати з деякою іншою інформацією, що містить повноваження пред'явника та перевірника, наприклад, забезпечує легітимність частин для вироблення ключа. Зроблений ключ може потім бути застосований як ключ для механізмів забезпечення цілісності й конфіденційності, які засновані на криптографічних перетвореннях, наприклад, особистого ключа ЕЦП; інтеграцію адреси мережі в обмінну ІА (наприклад, у підпис мережевої адреси) у системах з контролем доставки пакетів даних за правильними адресами мереж.

2.2 Захист від несанкціонованого доступу шляхом використання асиметричної криптографії

Є багато алгоритмів асиметричної криптографії. В даній роботі ми розглянемо основні: перетворення в кільцях (алгоритм RSA), перетворення в полі Галуа (DSA), перетворення в групі точок еліптичних кривих, криптоперетворення у кільцях зрізаних поліномів та криптоперетворення зі спарюванням точок еліптичних кривих. Основну увагу при пошуку методів захисту від НСД звертаємо на задачі повного розкриття. Для RSA-перетворення задача повного розкриття в основному зводиться до факторизації модуля перетворення, для перетворення в полі Галуа – до дискретного логарифмування в полі Галуа, для перетворення в групі точок еліптичних кривих – до дискретного логарифмування на еліптичній кривій, для криптоперетворень у кільцях зрізаних поліномів – до розв'язання певних задач в алгебраїчних решітках. Особливу групу складають задачі криптоаналізу криптоперетворень зі спарюванням точок еліптичних кривих тощо. Ці задачі є субекспоненційно або експоненційно складними. Методи факторизації можна поділити такі класи – з експоненційною та субекспоненційною складністю. Та окремо поліноміальний метод Г. Чалмерса.

До експоненційно складних методів належать такі [10]:

– перебирання типу «груба сила» зі складністю $O(N^{1/2})$;

– ρ-Полларда метод зі складністю $O(N^{1/4})$;

– ρ –1 Полларда метод;

– ρ +1 метод Вільямса;

– метод квадратичних форм Шенкса зі складністю $O(N^{1/4})$;

– метод Лемана.

До субекспоненційних методів належать:

– метод Діксона зі складністю $L_N(1/2,2\sqrt{2})$;

– метод безперервних дробів зі складністю $L_N(1/2,\sqrt{2})$;

– метод квадратичного решета зі складністю $L_N(1/2,1)$;

– метод еліптичних кривих зі складністю $L_p(1/2,\sqrt{2})$, де p – найменше просте, яке ділить N;

– метод решета числового поля зі складністю $L_N(1/3,(64/9)^{1/3})$;

– метод спеціального решета числового поля зі складністю $L_N(1/3,(32/9)^{1/3})$.

У таблиці 2.2 наведено формули для розрахунку складності факторизації відповідних методів.

Таблиця 2.2 – Складність факторизації RSA

Назва методу	Складність методу
Перебирання типу груба сила	$O(N^{1/2})$
ρ-Полларда метод	$O(N^{1/4})$
Метод квадратичних форм Шенкса	$O(N^{1/4})$
Метод Діксона	$L_N(1/2,2\sqrt{2})$
Метод безперервних дробів	$L_N(1/2,\sqrt{2})$
Метод квадратичного решета	$L_N(1/2,1)$
Метод еліптичних кривих	$L_p(1/2,\sqrt{2})$
Метод решета числового поля	$L_N(1/3,(64/9)^{1/3})$
Метод спеціального решета числового поля	$L_N(1/3,(32/9)^{1/3})$
Поліноміальний метод Чалмерса	$\ln^m N, 4 < m < 5$

З таблиці робимо висновок, що при застосуванні квадратичного або загального решета числового поля складність факторизації RSA модуля має субекспоненційний характер. При цьому для факторизації модулів, величина яких перевершує 330–350 бітів, краще використовувати метод загального решета числового поля. Підтвердженням висловленого є попередні роботи по криптоаналізу RSA. В той же час, необхідно відзначити, що метод квадратичного решета є набагато простішим у реалізації та розумінні.

2.3 Автентифікація за допомогою Смарт-картки та USB-ключів

Смарт-картка (smart – інтелектуальна, або розумна) – це звичайна пластикова картка з вбудованою мікросхемою. Ступінь «інтелектуальності» мікросхеми є дуже різним – від найпростішого контролера читання/запису даних в електронну пам'ять картки, до мікропроцесора, що має розвинуту систему команд, вбудовану файлову систему і т.п. Смарт-картка має змогу виконувати складні операції по обробці інформації та зберігати її. Звідси і назва – Smart (інтелектуальна) картка. Однак, ця назва є більш «народною». В стандарті ISO/IEC 7816 використовується термін Integrated Circuit Card (ICC) – картка з інтегрованою схемою, щоб охопити всі пристрої, де міститься інтегральна схема.

Смарт-картка була винайдена французом Роланом Морено в середині 70-х років, але тільки в кінці 80-х років технологічні досягнення зробили її достатньо зручною і доступною для практичного використання.

Є декілька видів класифікації смарт-карток (наприклад, за типом мікросхеми, яка в ній вбудована та за функціями, які виконує смарт-картка). Найпростіші типи карток містять тільки пам'ять, більш складніші є мікроелектронні-обчислювальні машини (ЕОМ), які забезпечують великий набір сервісних функцій.

Залежно від типу мікросхеми, вбудованої в картку, розрізняють такі типи смарт-карток:

– картки з програмованим постійним пристроєм для запам'ятовування є найпростішим типом карток. Основне їх застосування – розрахунки за телефонні переговори;

– картки з енергозалежною перепрограмованою пам'яттю надають доступ до перезаписування інформації, що зберігається в них. Основне їх застосування – зберігання індивідуальних даних;

– картки із захищеною перепрограмованою пам'яттю, які забезпечують доступ для читання/запису тільки після вводу спеціального коду. Основне їх застосування – розрахункові картки або зберігання захищених даних;

– багатофункціональні картки містять великий об'єм енергозалежної перепрограмованої пам'яті, спеціальний мікропроцесор і вбудовану операційну систему (ОС), що забезпечує набір сервісних функцій. Ці картки можуть застосовуватися для будь-яких додатків, включаючи розрахунки користувача.

За призначенням можна виділити картки-лічильники, картки пам’яті та мікропроцесорні картки.

Картки-лічильники застосовуються для такого типу розрахунків, коли потрібне віднімання фіксованої суми за кожну платіжну операцію. Такі картки ще називають наперед оплаченими картками.

Найбільшого поширення в світі набули телефонні картки пам'яті, власники таких карток мають змогу зробити певну кількість телефонних дзвінків, оскільки в телефонах-автоматах одиниця часу розмови має фіксовану ціну. Картка застосовується в контактному режимі (мікросхема фізично контактує із зчитуючим пристроєм). При кожному новому контакті число «дозволених дзвінків» у пам'яті картки зменшується на один біт пам'яті. Після того, як ліміт сплачених дзвінків закінчено, картка перестає функціонувати. Аналогічно картки-лічильники застосовуються при оплаті за проїзд, автостоянку, ліфти і т.п.

Картки пам'яті використовуються для збереження інформації. Сама їх назва говорить про те, що мікросхема картки містить тільки такий пристрій, що запам'ятовує. Є два типи таких карток: із захищеною і незахищеною пам'яттю.

У картках з незахищеною пам'яттю немає обмежень щодо читання або запису даних. Використовувати такі картки як платіжні дуже небезпечно. Достатньо легально придбати таку картку, скопіювати її пам'ять на диск, а далі після кожної покупки відновлювати її пам'ять копіюванням початкового стану даних з диска. Зрозуміло, що таку операцію може виконати лише кваліфікований програміст, але на практиці ми бачимо, що людей, здатних на це, достатньо.

У картках із захищеною пам'яттю використовується спеціальний механізм для дозволу читання/запису або вилучення інформації. Щоб провести ці операції,

необхідно ввести спеціальний секретний код (а іноді й не один). Як правило, картки із захищеною пам'яттю містять область, куди записуються ідентифікаційні дані. Ці дані не мають можливості бути змінені, що дуже важливо для забезпечення неможливості фальсифікації картки. Картки із захищеною пам'яттю можна використовувати, як платіжний засіб, а також для зберігання конфіденційних даних.

Мікропроцесорні картки схожі на картки пам'яті, але мікросхем містить мікропроцесор (чіп-модуль), який робить такі картки дійсно інтелектуальними. Мікропроцесор – це мікросхема (інтегральна схема, чіп), яка здатна зберігати великий обсяг інформації і виконувати арифметичні та логічні операції. Мікропроцесорні картки, практично є мікрокомп’ютерами зі своїм процесором, оперативною та постійною пам'яттю і навіть операційною системою. Як правило, у такі картки вбудовані криптографічні засоби, які забезпечують шифрування інформації. Мікропроцесори мають такі основні характеристики:

– тактова частота до 5 Мгц;
– об'єм оперативної' пам'яті (ОЗП) до 256 байт (для виконання команд);
– об'єм постійної пам'яті (ПЗП) до 10 Кбайт (для зберігання ОС);
– ємність перезаписуваної енергозалежної пам'яті до 8 Кбайт.

У картку вбудовується спеціалізована операційна система, що забезпечує великий набір сервісних операцій і засобів безпеки. ОС картки підтримує файлову систему, яка передбачає розмежування доступу до інформації. Для інформації, що зберігається в будь-якому записі (файл, група файлів, каталог), можуть встановлюватись такі режими доступу:

– завжди доступна для читання/запису. Цей режим дозволяє читання/запис інформації без знання спеціальних секретних кодів;
– доступна для читання, але вимагає спеціальних повноважень для запису. Цей режим дозволяє вільне читання інформації, але дозволяє запис тільки після вводу спеціального секретного коду;
– спеціальні повноваження для читання/запису. Цей режим дозволяє доступ для читання або запису після пред'явлення спеціального секретного коду, причому коди для читання і запису можуть бути різними;
– недоступна. Цей режим не дозволяє читати або записувати інформацію. Інформація доступна тільки внутрішнім програмам картки. Звичайно цей режим встановлюється для записів, що містять криптографічні ключі.

Смарт-картки використовуються для ідентифікації, автентифікації, авторизації користувачів, зберігання ключової інформації і проведення криптографічних операцій в довіреному середовищі. Смарт-картки знаходять все більше застосування в різних областях, від систем накопичувальних знижок до банківських платіжних карт, студентських квитків, SIM-карт і проїзних квитків, наприклад, на метро, а також для кодування таких відомостей, як, наприклад, історія хвороби. Зараз в багатьох країнах світу широко використовуються та поширюються, так звані, електронні посвідчення особи, наприклад Іспанія використовує, так звані, ID картки, Малайзія картки MyKad тощо. В їх основі лежить електронна картка, яка поєднує у собі багато функцій: ідентифікація особи, водійські права, зберігання інформації щодо стану здоров'я власника картки, електронний гаманець, інтеграція с банкоматами, оплата проїзду, криптографічні функції та ін. За рахунок своєї багатофункціональності смарт-картки набули широкого розповсюдження у світі у найрізноманітніших сферах.

Наша країна не є винятком. На даний момент в Україні впровадили проект «Соціальна картка» – це впровадження автоматизованих обліково-платіжних систем на основі персоніфікованих електронних пластикових карт, так званих «соціальних карт», в містах України. Електронна соціальна картка має змогу виконувати різні функції, зокрема облікову, інформаційну, платіжну та ін. Саме тому сьогодні важливою задачею є аналіз та обґрунтування основних вимог до смарт-карт а також висунення пропозицій щодо побудови такої системи в Україні. Розглянемо життєвий цикл виробництва картки.

1) Розробка вбудованого ПЗ. Усе ПЗ на смарт-картці може розглядатися як вбудоване. Однак, воно може бути розділене на «спеціалізоване ПЗ», ПЗ операційної системи та прикладного ПЗ.

2) ІС розробка. На цій стадії виробляється апаратний засіб для смарт - карт. У більшості випадків ця конструкція не є якоюсь специфічною для системи на смарт - картках, вона для загального призначення, але потім на неї буде встановлено ОС та різне додаткове ПЗ, яке буде визначати її призначення.

3) ІС виробництво. На стадії виробництва відбувається розробка ІС та ПЗ, яке буде зберігатися в ПЗУ (поєднання спеціального ПЗ, операційної системи і, можливо, прикладного ПЗ). Потім ІС виготовляється у формі пластини та випробовується.

4) ІС пакування. Пластини розрізають на окремі мікросхеми та пакують в відсік для вставки в карту.

5) Виробництво картки. ІС поміщається у пластикову карту, і може мати печатку, тиснення, лист з магнітною смугою, та інші процеси обробки.

6) Персоналізація та кастомізація. Перед видачою картка повинна бути підготовлена для її власника. Це означає підготовку початкових конфігурацій: завантажені усі програми, додатки, данні, які є індивідуальні для кожного власника, наприклад, ім’я власника картки та PIN код та інше.

7) Видача картки та її використання. Кожен з етапів життєвого циклу виробництва піднімає питання безпечності кожного з етапів.

У таблиці 2.3 представлені питання безпеки на кожному етапі.

Таблиця 2.3 – Питання безпеки на етапах життєвого циклу смарт-картки

Етап життєвого циклу	Питання безпеки
Розробка вбудованого ПЗ	Випадкове або зловмисне спотворення/модифікація: бібліотеки ПЗ; ОС; програми. Доступ до розробки програмного забезпечення може допомогти зловмисникові розробляти атаки на випущені картки.
ІС розробка	Недоліки або зміни, що можуть призвести до вразливості. Доступ до проектних даних, які можуть бути використані для нападу.
ІС Виробництво	Доступ до зразків у тестовому режимі може призвести до руйнуванню конфіденційності або/та цілісності вмісту ІС. Доступ до/модифікація у тестовому режимі перевірки достовірності даних – у зловмисника є можливість отримати результати та змінити їх. Доступ до/модифікація даних ініціалізації (ключів).
ІС пакування	Доступ до зразків у тестовому режимі.
Виробництво картки	Доступ до зразків в тестовому режимі. Доступ до операційної системи/прикладного ПЗ на початкової стадії, перш ніж всі заходи безпеки будуть застосовані може дозволити зловмиснику прочитати конфіденційні дані, або занести зміни в конфігурацію картки. Доступ до сировини картки може допомогти зловмисникові зробити підробку для використання її у системі.
Персоналізація і кастомізація	Доступ до даних ініціалізації (наприклад, до ключів, кредитних лімітів або інших параметрів схеми). Доступ до особистих даних власника.
Видача картки та її використання	Доступ до даних під час доставки дає повноваження для оновлення параметрів картки (включаючи розблокування). Доступ до оновлень ОС, який може бути використаний для атаки. Створення оновлень для ОС, наприклад, для завантаження шкідливого коду. Диференційний аналіз живлення (DPA) та помилок (DFA). Фізичні атаки на ІС.

Електронний ключ (ЕК) – апаратний засіб, призначений для захисту ПЗ та даних від копіювання, нелегального використання і несанкціонованого розповсюдження. ЕК повинен бути виконаний у вигляді малогабаритного знімного USB-пристрою на двошаровій друкованій платі, яка розмішена у пластиковому корпусі одноразової зборки. На друкованій платі встановлюються електронні компоненти ЕК та USB-з'єднувач.

ЕК повинен виконувати наступні функції:

– управління особистими ключами ЕЦП та протоколу розподілу ключовими даними, що включає:

– прийом та зберігання загальних параметрів для алгоритму ЕЦП та протоколу розподілу ключів;

– генерацію особистого ключа ЕЦП та протоколу розподілу;

– зберігання особистих ключів ЕЦП та протоколу розподілу ключів в зашифрованому вигляді з контролем цілісності;

– знищення особистих ключів ЕЦП та протоколу розподілу ключів;

– формування ЕЦП від даних, що завантажуються з ЕОМ з використанням особистого ключа ЕЦП;

– генерацію сеансових ключів;

– формування спільного секретного ключа за протоколом розподілу ключових даних з використанням власного особистого ключа протоколу розподілу та відкритого ключа отримувача;

– кодування та розшифрування сеансових ключів з використанням сформованого спільного секретного ключа;

– прийом та зберігання двох довгострокових ключових елементів (ДКЕ), що використовуються у алгоритмі генерації випадкових бітових послідовностей та протоколі розподілу ключових даних;

– автентифікацію користувача перед початком роботи;

– управління параметрами автентифікації користувача, що включає встановлення і зміну даних автентифікації користувача;

– прийом, зберігання, надання доступу та знищення довільних даних користувача у ЕК.

ЕК повинен включати наступні функціональні вузли:

– процесор із вбудованими: генератором тактових частот, оперативним запам’ятовуючим пристроєм (ОЗП), постійним запам’ятовуючим пристроєм (ПЗП), контролером шини USB;

– генератор випадкового сигналу (ГВС);

– стабілізатори напруги живлення усіх компонентів ЕК.

Процесор призначений для:

– виконання програм, що реалізують функції ЕК;

– збереження у вбудованому ПЗП особистих ключів, даних автентифікації та довільних даних користувача;

– організації обміну інформацією з ЕОМ через інтерфейс USB.

ГВС призначений для генерації аналогового випадкового сигналу та перетворення його в двійковий, який використовується при формуванні випадкових послідовностей.

Програми ЕК повинні включати:

– внутрішні програмні компоненти ЕК (внутрішні програми);

– системні програмні компоненти;

– програмний комплекс тестування та конфігурування ЕК.

Внутрішні програми ЕК призначені для:

– прийому та зберігання у ПЗП загальних параметрів для алгоритму ЕЦП та протоколу розподілу ключів;

– генерації особистого ключа ЕЦП та протоколу розподілу ключів з використанням алгоритму генерації випадкових бітових послідовностей ЕЦП і вбудованого апаратного ГВС;

– зберігання у ПЗП особистих ключів ЕЦП та протоколу розподілу ключів в зашифрованому вигляді з контролем цілісності;

– знищення з ПЗП особистих ключів ЕЦП та протоколу розподілу ключів;

– формування ЕЦП від даних, що завантажуються з ЕОМ з використанням особистого ключа ЕЦП;

– генерація сеансових ключів;

– формування спільного секретного ключа за протоколом розподілу ключовими даними з використанням особистого ключа протоколу розподілу та відкритого ключа протоколу розподілу отримувача;

– зашифрування та розшифрування сеансових ключів з використанням сформованого спільного секрет-ного ключа;

– прийому та зберігання у ПЗП двох ДКЕ;

– автентифікації користувача перед початком роботи;

– управління параметрами автентифікації користувача;

– прийому, запис та зберігання у ПЗП довільних даних користувача;

– надання доступу та знищення довільних даних користувача з ПЗП.

Системні програмні компоненти призначені для:

– забезпечення коректного розпізнавання ЕК ОС ЕОМ;

– передачу кодів команд та вхідних даних для виконання відповідних внутрішніх програм крипто-графічного модуля, які виконують перетворення вхідних даних у вихідні;

– отримання з ЕК результатів виконання команд та вихідних даних.

Програмний комплекс тестування та конфігурування призначений для:

– перевірки роботоспроможності ЕК;

– конфігурування параметрів ЕК у ОС ЕОМ;

– встановлення або зміни даних автентифікації користувача ЕК шляхом їх завантаження у ЕК;

– форматування ЕК, що включає знищення особистих ключів та довільних даних користувача у ЕК.

До складу ключових даних ЕК повинні входити:

– ДКЕ, що використовуються у алгоритмі генерації випадкових бітових послідовностей та протоколі розподілу ключових даних;

– загальні параметри ЕЦП та протоколу розподілу ключів;

– особистий та відкритий ключі ЕЦП;

– особистий та відкритий ключі протоколу розподілу ключів.

Особисті та відкриті ключі ЕЦП і протоколу розподілу ключів повинні генеруватися в середині ЕК. Після чого особисті ключі повинні зберігатися у внутрішньому ПЗП, а відкриті – передаватися у ЕОМ для подальшого їх розповсюдження.

Захист від НСД до інформації, що обробляється у ЕК, повинен здійснюватися наступним чином:

– використання командного інтерфейсу взаємодії, що виключає прямий доступ до внутрішніх вузлів та програм ЕК;

– зберігання особистих ключів в ПЗП у захищеному вигляді;

– автентифікації користувача до початку роботи з ЕК.

Захист та контроль цілісності особистих ключів у ПЗП повинен здійснюватися на основі пароля захисту. Особисті ключі повинні контролюватися на цілісність шляхом вироблення вставки та захищатися шляхом кодування в режимі простої заміни.

Автентифікація користувача перед початком роботи повинна здійснюватися шляхом передачі у ЕК пароля доступу до ЕК, хешуванням пароля та порівнянням з еталоном, що зберігається у ПЗП. На основі результату порівняння ЕК повинний приймати рішення про успішність автентифікації.

У таблиці 2.4 наведемо характеристики деяких електронних ключів, представлених на ринку.

Таблиця 2.4 – Характеристики електронних ключів

Виріб	Ємність пам’яті, кБ	Розрядність серійного номеру	Алгоритми шифрування
iKey 20xx	8/32	64	DES (ECB и CBC), DESX, 3DES, RC2, RC5, MD5, RSA-1024/2048
eToken R2	16/32/64	32	DESX (ключ 120 бит), MD5
eToken Pro	16/32	32	RSA/1024, DES, 3DES, SHA-1
ePass 1000	8/32	64	MD5, MD5-HMAC
ePass 2000	16/32	64	RSA, DES, 3DES, DSA, MD5, SHA-1
ruToken	8/16/32/64/128	32	ГОСТ 28147-89, RSA, DES, 3DES, RC2, RC4, MD4, MD5, SHA-1
uaToken	8/16/32/64/128	32	ГОСТ 28147-89

2.4 Застосування біометричної автентифікації

За останні два десятиліття біометричні технології зробили великий крок вперед. Багато в чому цьому сприяло поширення мікропроцесорних технологій. Ще в 80-ті роки систему контролю доступу, яка використовує біометричні характеристики людини, можна було побачити лише у фантастичних фільмах. Сьогодні ж використання в СКУД біометричних сканерів практично не

ускладнює систему безпеки, і її вартість для деяких біометричних методів дуже низька. Більш того, близько третини ноутбуків виходить зараз із вбудованою системою зчитування відбитку пальців, а якщо в ноутбуці є відеокамера, на нього можна встановити систему розпізнавання людини за обличчям.

Біометрія (Biometrics) – технологія ідентифікації особи, яка використовує фізіологічні параметри суб'єкта (код ДНК, відбитки пальців, райдужну оболонку ока, зображення обличчя, тембр голосу і т. п.). Біометричні технології активно використовуються в багатьох областях, які пов'язані зі захистом доступу до конфіденційної інформації, до матеріальних цінностей, при перетині державного кордону і т. п.

Стандарти в області біометрії розробляються підкомітетом SC 37 «Біометрія» Технічного комітету ISO/IEC JTC 1 «Інформаційні технології». У роботі підкомітету приймає участь 26 країн, серед яких є і Україна. Ще 10 країн беруть участь у роботі підкомітету як спостерігачі. Підкомітетом «Біометрія» розроблено 39 стандартів [12]. Слід зазначити, що розроблені на даний час стандарти [13] охоплюють такі напрями біометрії:

– біометричний прикладний програмний інтерфейс (БіоППІ) та біометричний графічний інтерфейс користувача;

– специфікація елементів та форматів біометричних даних;

– процедури дій органу реєстрації у сфері біометрії та специфікацію формату провідної організації;

– статистичні та динамічні біометричні параметри: дані та шаблон відбитка пальця, зображення обличчя, радужна оболонка ока, характеристики підпису, спектральні та контурні дані рисунка відбитка пальця, зображення сосудів і геометричні дані силуету кисті;

– експлуатаційні випробування, випробування на відповідність та протоколи випробувань у біометрії;

– біометричні профілі, процедури контролю доступу для працівників аеропортів, біометрична верифікація та ідентифікація особи моряків;

– протоколи взаємодії при використанні біометричного прикладного програмного інтерфейсу;

– фіксація відбитків десяти пальців з використанням біометричного прикладного програмного інтерфейсу.

Під фіксацією мається на увазі процес отримання біометричного зразка від особи, що взаємодіє з біометричною системою для реєстрації або ідентифікації своєї особистості. До біометричного зразка можна віднести не тільки інформацію, яку отримано з сенсора, але і ту, яку отримуємо після обробки. Слід зауважити, що діяльність відповідного міжнародного підкомітету ISO/IEC направлена на стандартизацію усіх областей біометрії. Узагальнена модель взаємозв'язку стандартизованих областей біометрії показана на рисунку 2.2 [13].

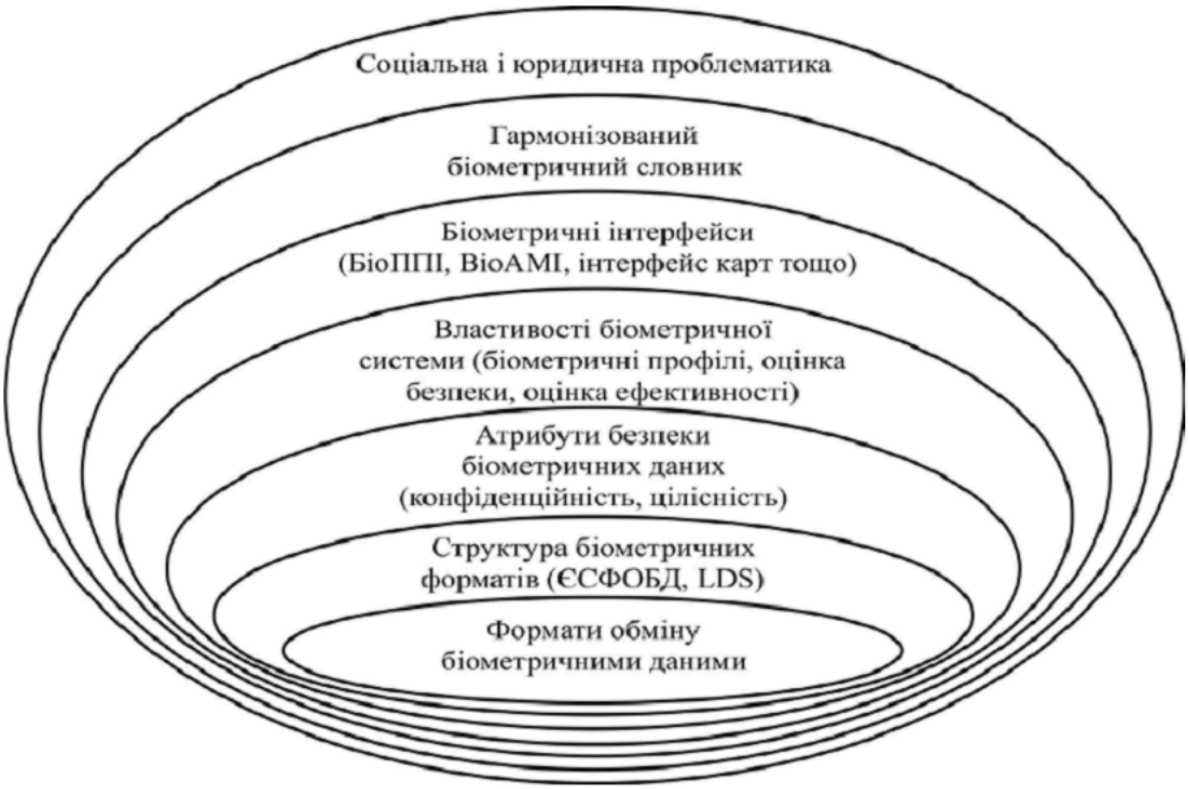

Рисунок 2.2 – Узагальнена модель взаємозв’язку стандартизованих областей біометрії

Біометричні дані, які містять у собі біометричну характеристику особи і відповідають стандартизованим форматам обміну біометричними даними, представляють собою ядро біометричної сумісності. Такі структури біометричних форматів, які визначені в ISO/IEC 19785-1 [14] як єдина система форматів обміну біометричними даними (ЄСФОБД), служать обгорткою навколо біометричних даних.

Оскільки біометричні дані є таємними даними й об'єктом атак, то вони підлягають захисту й в середовищах обміну цими даними має використовуватись

криптографічний захист. Біометричні властивості профілів, оцінки безпеки й ефективності відіграють важливу роль при реалізації біометричних систем різного типу. Біометричні інтерфейси є необхідними засобами для покращення інтеграції і використання різноманітних біометричних компонентів, у тому числі тих, які створені різними виробниками.

Гармонізований словник біометричних термінів, який на даний час знаходиться у постійному розвитку, рекомендується використовувати при створенні та реалізації всіх біометричних технологій. Створення і впровадження прикладних рішень з використанням біометричної верифікації або ідентифікації визначаються соціальними і юридичними вимогами і, відповідно, мають місце в контексті зазначених вимог.

Перелічимо основні біометричні характеристики людини (БХЛ), за допомогою яких здійснюється її ідентифікація:

- відбитки пальців;
- форма і геометрія обличчя;
- форма і будова черепа;
- сітківка ока;
- райдужна оболонка ока;
- геометрія долоні, кисті руки або пальця;
- термографія особи, термографія руки;
- малюнок вен на долоні або пальці руки;
- ДНК; запах тіла;
- форма вуха;
- динаміка підпису;
- динаміка клавіатурного набору;
- голос;
- рух губ;
- хода;
- особливості накреслення рукописного тексту.

Ідеальна характеристика повинна легко збиратись, бути універсальною, унікальною и постійною [15].

Універсальність – можливість представлення людини однією характеристикою. Унікальність означає, що не повинно бути двох осіб з ідентичними характеристиками.

Сталість (перманентність) – характеристика не повинна змінюватися з часом. Збирання (вимірювальність) – можливість швидко і легко одержати та деталізувати характеристику від індивідуума. У ході даної роботи була проведена оцінка зазначених раніше властивостей БХЛ та представлена у таблиці 2.5.

Таблиця 2.5 – Оцінка властивостей біометричних характеристик людини

Характеристика	Універсальність	Унікальність	Сталість	Вимірювальність
Відеообраз обличчя	Висока	Низька	Середня	Висока
Термограма обличчя	Висока	Висока	Низька	Висока
Відбиток пальця	Середня	Висока	Висока	Середня
Геометрія руки	Середня	Середня	Середня	Висока
Райдужна оболонка ока	Висока	Висока	Висока	Середня
Сітківка	Висока	Висока	Середня	Низька
Підпис	Низька	Низька	Низька	Висока
Голос	Середня	Низька	Низька	Середня
Відбиток губ	Висока	Висока	Середня	Низька
Особливості вуха	Середня	Середня	Середня	Середня
Динаміка підпису	Висока	Висока	Низька	Висока
Хода	Висока	Середня	Низька	Низька

Як правило, при класифікації біометричних технологій виділяють дві групи систем за типом біометричних параметрів, що використовуються. Перша група використовує статичні біометричні параметри: відбитки пальців, геометрію руки, зображення обличчя, райдужна оболонка ока і т. п. Друга група використовує динамічні параметри: динаміку відтворення підпису або рукописного ключового слова, тембр голосу і т. п.

Усі біометричні технології характеризуються однаковою базовою моделлю. Спочатку необхідно створити первинний реєстраційний шаблон користувача. Ця операція здійснюється шляхом збору кількох зразків за допомогою будь-якого біометричного сенсора. Далі зі зразків добуваються характерні ознаки й отримані результати об'єднуються згідно певного алгоритму в шаблон. Процес створення даного первинного шаблона називається реєстрацією (або фіксацією). Алгоритми, які використовуються для створення шаблонів, можуть бути запатентовані за бажанням розробника. Первинний шаблон зберігається прикладною програмою як контрольний шаблон. Також можна зберігати цей шаблон за допомогою спеціальних засобів у відповідному модулі архіву біометричного прикладного

програмного інтерфейсу. Отже, кожного разу, коли необхідно автентифікувати користувача, з сенсора отримують зразки (або зразок), обробляють їх для подання в придатній для використання формі та зіставляють із раніше зареєстрованим контрольним шаблоном. Таку форму біометричної автентифікації називають верифікацією, оскільки проводиться перевірка того, чи є користувач тим, ким він себе називає (тобто перевіряється заявлена особистість).

У стандартах термін «біометрична верифікація» визначається як автоматизований процес оцінювання твердження про те, що поданий біометричний зразок (зразки) та вже збережений біометричний шаблон належать одному й тому самому джерелу біометричної інформації. Крім того, біометричні технології використовують іншу форму автентифікації, яка називається ідентифікацією. При ідентифікації користувачу не потрібно заявляти свою особистість. У даному випадку оброблені зразки користувача порівнюються з базою контрольних шаблонів і приймається рішення про те, який з них має найбільший ступінь схожості. Залежно від отриманого результату може бути ухвалене рішення про ідентичність користувача та особи, шаблон якої має найбільший ступінь схожості з урахування порогу ступеня схожості. В біометричних стандартах термін «біометрична ідентифікація» визначається як процес порівняння поданих біометричних даних з усіма шаблонами в базі даних (схема «один до декількох») з метою визначення відповідності та, якщо відповідність визначено, ідентифікації відповідної особи. Можлива архітектурна реалізації вищенаведеної базової моделі зображена на рисунку 2.3 [13].

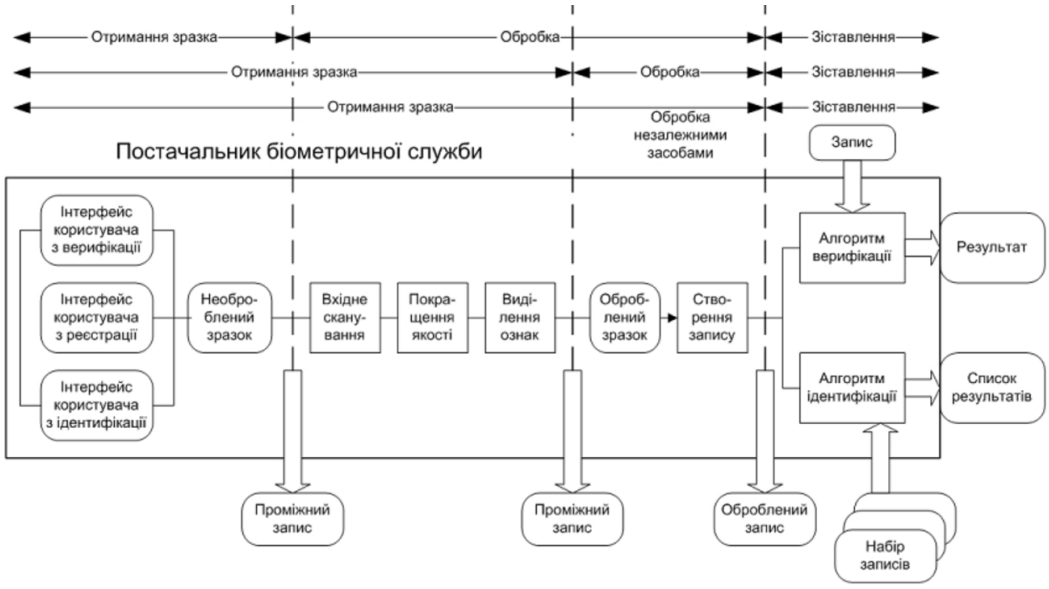

Рисунок 2.3 – Архітектурна реалізація базової моделі біометричної системи

Стадії, зазначені над блоком «Постачальник біометричної служби», відповідають елементарним функціям інтерфейсу верхнього рівня: отримання зразка, обробка та зіставлення. Різні стадії операцій верифікації та ідентифікації показані у блоці, позначеному як «постачальник біометричний служби». Під постачальником біометричної служби розуміється компонент прикладної програми, який здійснює біометричні операції за допомогою певного інтерфейсу або шляхом безпосереднього керування одним або декількома модулями біометричного прикладного програмного інтерфейсу, або з використанням наперед визначених функцій.

Дати визначення та відобразити узагальнену біометричну систему досить складно, оскільки слід врахувати різноманітні біометричні застосування і технології. Але, тим не менш, можливо виділити загальні елементи, які характерні будь-якій біометричній системі. Біометричні зразки здобувають з об'єкта за допомогою сенсорів. Вихідні дані з сенсора передаються на обробку даних, при якій добувають відмінні, але обов'язково повторювані ознаки зразка, і відкидають всі інші дані. Виділені в такий спосіб ознаки можуть бути збережені в базі даних у вигляді «шаблона» або піддані порівнянню з окремим шаблоном, декількома шаблонами або всіма шаблонами, що зберігаються в базі даних.

Метою цього порівняння є визначення ступеня збігу, на підставі якого приймається рішення про визнання особи за результатами зіставлення ознак зразка і шаблонів. Інформаційні потоки в узагальненій біометричній системі та її структурні компоненти подані на рисунку 2.4 [13].

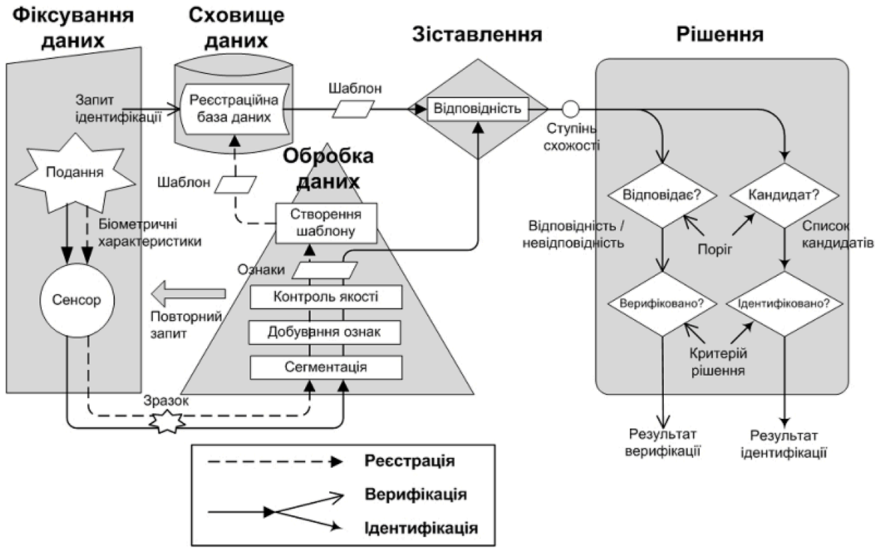

Рисунок 2.4 – Концептуальна схема узагальненої біометричної системи

Система складається з підсистем фіксації даних, обробки сигналів, зберігання, зіставлення й ухвалення рішення. Схема ілюструє процеси реєстрації, верифікації й ідентифікації. Слід зазначити, що елементи, надані в даній концептуальній моделі, можуть бути відсутні або не відповідати безпосередньо фізичним компонентам у реальній біометричній системі.

Підсистема фіксації даних збирає зображення або сигнали біометричних характеристик суб'єкта, які надані біометричному сенсору, та видає це зображення або сигнал у вигляді біометричного зразка.

Підсистема передавання даних (не зображена на схемі, оскільки може бути відсутня в біометричній системі у явному вигляді) забезпечує обмін зразками, ознаками та шаблонами між різними підсистемами.

Ці зразки, ознаки та шаблони можна передавати використовуючи стандартні формати обміну біометричними даними. Біометричний зразок можна ущільнити та/або зашифрувати перед передаванням та розгорнути та/або дешифрувати перед використанням. Також він може бути змінений у процесі передавання через шум у каналах передачі або через втрати в процесі ущільнення та розширення. Рекомендується використовувати криптографічні методи, що захищають автентичність, цілісність та конфіденційність біометричних даних, що передаються та зберігаються.

Підсистема обробки сигналів виділяє відмітні ознаки з біометричного зразка. Це можливо шляхом виділення сигналу біометричних характеристик суб’єкта з отриманого зразка (сегментації), добування ознак та контролю якості, який забезпечуватиме відмітність та повторюваність добутих ознак. Якщо підсистема контролю якості відхилить отриманий зразок (зразки), керування може бути повернуто підсистемі фіксації даних для збору додаткового зразка (зразків).

Можна визначити кілька рівнів обробки біометричних даних, які представлені на рисунку 2.5:

– здобуті дані: необроблені дані отримані з сенсора;

– проміжні дані: дані, оброблені після отримання з сенсора, але у формі непридатній для зіставлення – на такі дані посилаються, як на дані зображень або поведінки;

– оброблені дані: дані у формі придатній для зіставлення – на ці дані посилаються, як на дані ознак.

Рисунок 2.5 – Послідовність обробки біометричних даних

У випадку реєстрації, підсистема обробки сигналів створює шаблон із добутих біометричних ознак.

Підсистема зберігання даних містить реєстраційну базу, яка служить для зберігання шаблонів. Кожний шаблон пов'язаний з певною інформацією про суб’єкт реєстрації. Слід зазначити, що перед збереженням у реєстраційній базі даних, формат шаблонів може бути змінений відповідно до формату обміну біометричними даними. Шаблони можуть бути збережені в пристрої біометричної фіксації, на переносному носії (наприклад, смарт-карті), локально – на персональному комп'ютері або локальному сервері, або в централізованій базі даних.

Підсистема зіставлення даних порівнює біометричні дані з даними одного або декількох шаблонів та передає інформацію про ступінь схожості до підсистеми ухвалення рішень. Ступінь схожості визначає ступінь відповідності ознак шаблонам, з якими проводилося порівнювання. При верифікації один визначений запит суб’єкта реєстрації ініціює один розрахунок ступеня схожості. У випадку ідентифікації декілька або всі шаблони можуть бути порівняні з ознаками, вихідний ступінь схожості буде отриманий для кожного порівняння.

Підсистема ухвалення рішення використовує ступені схожості, створені однією або більше спробами, для надання вихідного рішення щодо запиту верифікації або ідентифікації.

У випадку верифікації, порівняння ознак та шаблону вважається успішним, якщо ступінь схожості перевищує встановлене граничне значення. Підтвердження реєстрації суб’єкта може бути ухвалене у відповідності з правилами прийняття рішень, які можуть вимагати або допускати кілька спроб верифікації.

У випадку ідентифікації зареєстрований шаблон є потенційним кандидатом для суб’єкта, коли ступінь схожості перевищує встановлене граничне значення.

Правила ухвалення рішень можуть дозволити або вимагати декількох спроб перед ухваленням рішення про ідентифікацію.

Підсистема керування (не зображена на схемі) керує у повній мірі правилами, реалізацією і використанням біометричної системи відповідно до узаконених, юрисдикційних і соціальних обмежень та вимог.

Біометрична система може взаємодіяти або не взаємодіяти із зовнішніми прикладними програмами або системами через прикладний програмний інтерфейс, апаратний інтерфейс або інтерфейс протоколів.

2.5 Методи та порівняльний аналіз біометричних систем автентифікації

Унікальні фізіологічні характеристики кожного людського організму складають основу статичних методів біометричної автентифікації. Статичні характеристики людини не змінюються протягом всього життя і є невід'ємними від неї.

Серед статичних методів розрізняють наступні:

- за відбитком пальця;
- за формою долоні;
- за розташуванням вен на лицьовій стороні долоні;
- за сітківкою ока;
- за райдужною оболонкою ока;
- за формою обличчя;
- за термограмою особи;
- за ДНК.

Автентифікація за відбитком пальця. Розпізнавання відбитків пальців – це один з найпростіших і добре відомих біометричних методів ідентифікації особи. Саме він виявився найбільш практичним щодо реалізації та сприйняття його людьми і саме він використовується вже тривалий час. Відбитки пальців у всіх людей абсолютно різні. Всі люди, що населяють в наш час Землю, мають, притаманні тільки їм одним, певні відбитки пальців. І навіть відбитки пальців всіх попередніх поколінь людей також відмінні від всіх наступних. Правоохоронні органи в усьому світі використовують ідентифікацію за відбитками пальців вже більше ста років, причому до сьогодні не виявлено жодного випадку збігу відбитків пальців у різних людей, включаючи навіть однояйцевих близнят. У силу

цього саме відбитки пальців руки однієї людини вважаються специфічною, притаманною тільки цій людині «особистою карткою», і саме в такій якості ця властивість застосовується в усьому світі. Але така особливість пальців руки людини була виявлена лише до кінця XIX століття. До того часу вони представлялися людям просто набором ліній, нічого не позначають і не володіли якимись особливостями.

Шкіра людини складається з двох шарів, при цьому нижній шар утворює безліч виступів – сосочків (від лат. Papillae – сосочок), у вершині яких є отвори вихідних протоків потових залоз. На основній частині шкіри сосочки (потові залози) розташовуються хаотично і їх важко побачити. У кожному відбитку пальця можна визначити два типи ознак: глобальні; локальні. Глобальні ознаки – це ті ознаки, які можна побачити неозброєним оком. На окремих ділянках шкіри кінцівок, папіляри строго впорядковані в лінії (гребні) і утворюють так звані унікальні папілярні візерунки. Ці візерунки і відображають всю людську індивідуальність. На рисунку 2.6 наведено типи папілярних візерунків [16].

Рисунок 2.6 – Типи папілярних візерунків

Інший тип ознак – локальні. Їх називають минуціями, та вони є унікальні для кожного відбитка ознаки. Минуції визначають пункти зміни структури папілярних ліній (закінчення, роздвоєння, розрив і т.д.), орієнтацію папілярних ліній і координати в цих пунктах. Кожен відбиток містить до 70 минуцій. Область образу чи інакше виділений фрагмент відбитку, в якому локалізовані всі ознаки.

Ядро – це частина, розміщена в середині цілого відбитку або деякої обраної області. Пункт «дельта» – це початкова точка. Місце, в якому відбувається розділення або додавання борозенок папілярних ліній, або також можна вважати дуже коротку борідку. Тип лінії – дві найбільші лінії, які починаються як паралельні, а потім розходяться і огинають всю область цього виду. Лічильник ліній – число ліній на області образу або між ядром і пунктом «дельта».

На рисунку 2.7 відзначені дві лінії та те, що розташоване між ними [16]. Ця частина може виступати в якості області образу, але у більшості своєму, прийнято обирати всю площу відбитка. Практика доказує, що відбитки пальців різних людей можуть мати схожі глобальні ознаки. При цьому, неможливо мати однакові мікровізерунки минуцій. Тому глобальні ознаки використовують для розділення бази даних на класи і на етапі автентифікації. На другому етапі визначення використовують вже локальні ознаки. Зараз в основному для розпізнавання відбитків пальців використовуються стандарти ANSI і ФБР США, у державах СНД – також і російські [17-20]. У них визначено наступні вимоги до образу відбитка: кожен образ представляється у форматі не стисненого TIF; образ повинен мати розширення не нижче 500 dpi; образ повинен бути напівтоновим з 256 рівнями яскравості; максимальний кут повороту відбитка від вертикалі не більше 15 градусів; основні типи минуцій – закінчення і роздвоєння.

Рисунок 2.7 – Локальні типи ознак – минуції

Розглянемо наступні принципи порівняння відбитків за локальними ознаками.

1) Етап 1. Поліпшення якості початкового зображення відбитка. Збільшується різкість кордонів папілярних ліній.

2) Етап 2. Обчислення поля орієнтації папілярних ліній відбитка. Зображення розбивається на квадратні блоки, зі стороною більше 4 пікселів і за градієнтами яскравості обчислюється кут t орієнтації ліній для фрагмента відбитка.

3) Етап 3. Бінаризація зображення відбитка. Приведення до чорно-білого зображення (1 bit) пороговою обробкою.

4) Етап 4. Потоншення ліній зображення відбитка. Потоншення проводиться до тих пір, поки лінії не будуть шириною 1 піксель.

5) Етап 5. Виділення минуцій. Зображення розбивається на блоки 9x9 пікселів. Після цього підраховується число чорних (ненульових) пікселів, що знаходяться навколо центру. Піксель в центрі вважається минуцією, якщо він сам ненульовий, і сусідніх ненульових пікселів один (минуція «закінчення») або два (минуція «роздвоєння»). Координати виявлених минуцій та їх кути орієнтації записуються у вектор: W (p) = [(x1, y1, t1), (x2, y2, t2)...(xp, yp, tp)] (p – число минуцій). При реєстрації користувачів цей вектор вважається еталоном і записується в базу даних. При розпізнаванні вектор визначає поточний відбиток (що цілком логічно).

6) Етап 6. Зіставлення минуцій. Два відбитки одного пальця будуть відрізнятися один від одного поворотом, зсувом, зміною масштабу та / або площею дотику в залежності від того, як користувач прикладає палець до сканера. Тому не можна сказати, чи належить відбиток людині чи ні на підставі простого їхнього порівняння (вектори еталона і поточного відбитка можуть відрізнятися по довжині, містити невідповідні минуції і т.д.). Через це процес зіставлення повинен бути реалізований для кожної минуції окремо.

Етапи порівняння:

- реєстрація даних;
- пошук пар відповідних минуцій;
- оцінка відповідності відбитків;

– при реєстрації визначаються параметри афінних перетворень (кут повороту, масштаб і зрушення), за яких деяка минуція з одного вектора є певною минуції з другого.

Під час пошуку для кожної минуції потрібно перебрати до 30 значень повороту (від -15 градусів до +15), 500 значень зсуву (від -250 пкс до 250 пкс - хоча, звісно, межі вибирають і трохи менше) і 10 значень масштабу (від 0,5 до 1,5 з кроком 0,1). Разом до 150000 кроків для кожної з 70 можливих минуцій. Оцінка відповідності відбитків виконується за формулою (2.1):

$$K = \frac{(D \cdot D \cdot 100\%)}{p \cdot q} \qquad (2.1)$$

де D – кількість минуцій, що збігалися;

p – кількість минуцій еталона;

q – кількість минуцій ідентифікованого відбитка.

У тому випадку, якщо результат є більшим за 65 %, відбитки можна вважати ідентичними (також поріг може бути зміненим завдяки виставлянням іншого рівня пильності).

Після того як автентифікація пройшла, процес можна вважати закінченим. Для ідентифікації необхідно повторити цей процес для всіх відбитків що існують в базі даних (так вибирається користувач, рівень відповідності якого найбільший та результат не менший за поріг 65%). Незважаючи на те, що описаний вище принцип порівняння відбитків забезпечує високий рівень надійності, все ж таки продовжуються пошуки більш досконалих (і швидкісних) методів порівняння.

Представлена технологія є найпоширенішою в порівнянні з іншими методами біометричної автентифікації. Незважаючи на те, що технологія сканування відбитків пальців є дешевою і достатньо точної, вона не настільки однозначна як деякі інші біометричні технології.

Зчитувач відбитків можна ввести в оману, використовуючи, наприклад, латексні протези пальців, які відтворювали б справжній відбиток.

Деякі зчитувачі також можна обдурити, знявши відбитки пальців з будь-якої поверхні за допомогою тюнера до лазерних принтерів, а потім відтворивши це зображення на фотопапері.

Іншим недоліком методу є те, що деякі інваліди зі зрозумілих причин не можуть користуватися такою технологією. Переваги та недоліки даного методу наведені в таблиці 2.6.

Таблиця 2.6 – Переваги та недоліки методу ідентифікації за відбитком пальця

Переваги	Недоліки
1. Компактний зчитувач.	1. Недостатній захист від підробки відбитку пальця.
2. Низька вартість пристрою.	
3. Невеликий процент помилок.	2. Візерунок відбитку пальця легко змінюється подряпинами.
4. Проста процедура сканування відбитку.	

Розглянемо спосіб ідентифікації за візерунком кровоносних судин, розташованих на поверхні очного дна (сітківці). Сітківка розташована глибоко всередині ока, але навіть це не заважає сучасним технологіям. Навпаки слід відзначити, що саме завдяки цій властивості, сітківка – є однією з найбільш стабільних фізіологічних ознак організму.

Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності. Для цього необхідного спрямувати світло через зіницю до кровоносних судин на задній стінці ока. Лазерний промінь м'якого випромінювання можна використовувати в цьому процесі. Вени і артерії, що постачають кров'ю очі, добре видно при підсвічуванні очного дна зовнішнім джерелом світла. Ще в 1935 році Саймон і Голдштейн розкрили унікальність дерева кровоносних судин очного дна для кожного окремого організму [21]. Сканери для сітківки ока набули значного поширення в надсекретних системах контролю доступу, оскільки у них один з найнижчих відсотків відмови доступу зареєстрованих користувачів. Крім того, у системах передбачений захист від муляжу. У даний час широкому поширенню цього методу перешкоджає ряд причин: висока вартість зчитувача; невисока пропускна здатність; психологічний фактор. Невисока пропускна здатність пов'язана з тим, що користувач повинен протягом декількох секунд дивитися в окуляр на зелену крапку. І тим не менше, ці системи удосконалюються і знаходять своє застосування. У США, наприклад, розроблено нову систему перевірки пасажирів, яка заснована на скануванні сітківки ока. Фахівці стверджують, що тепер для перевірки не треба діставати з

кишені гаманець з документами, що достатньо лише пройти перед камерою. Дослідження сітківки ґрунтуються на аналізі більш як 500 характеристик. Після сканування код буде зберігатися в базі даних разом з іншою інформацією про пасажира, і в подальшому ідентифікація особи займатиме лише кілька секунд. Використання подібної системи буде абсолютно добровільною процедурою для пасажирів. Англійська Національна фізична лабораторія (National Physical Laboratory, NPL), за замовленням організації Communications Electronics Security Group, що спеціалізується на електронних засобах захисту систем зв'язку, провела дослідження різних біометричних технологій ідентифікації користувачів. В ході випробувань система розпізнавання користувачів за сітківкою ока не дозволила допуск жодному з більш ніж 2,7 млн. «сторонніх», а серед тих, хто мав права доступу, лише 1,8% були помилково відкинуті системою (проводилися три спроби доступу). Як повідомляється, це був наднизький коефіцієнт помилкових рішень серед перевіряючих систем біометричної ідентифікації. А найбільший відсоток помилок був у системи розпізнавання обличчя – в різних серіях випробувань вона відкинула від 10 до 25 % законних користувачів.

Також унікальним статичним ідентифікатором для кожного індивіду є райдужна оболонка ока. Неповторність малюнка райдужної оболонки обумовлена генотипом особистості. Затверджено, що навіть у близнюків спостерігаються суттєві відмінності райдужної оболонки.

Лікарі використовують малюнок і колір райдужної оболонки для виявлення генетичної схильності до деяких захворювань і також для самої діагностики захворювань. Виявлено, що при ряді захворювань на райдужній оболонці з'являються характерні пігментні плями і зміни кольору. В технічних системах розпізнавання використовуються тільки чорно-білі зображення, що поменшують впливу стану здоров'я на результати ідентифікації людини та служать високою роздільною здатностю. Ідея розпізнавання на основі параметрів райдужної оболонки ока з'явилася ще в 1950-х роках [22].

Джон Даугман, професор Кембриджського університету, винайшов технологію, до складу якої входила система розпізнавання за райдужною оболонкою, що використовується зараз в Nationwide ATM. У той час вчені довели, що не існує двох людей з однаковою райдужною оболонкою ока (більше того, навіть у однієї людини райдужні оболонки очей відрізняються), але програмного забезпечення, здатного виконувати пошук і встановлювати відповідність зразків відсканованого зображення, тоді ще не було. У 1991 році

Даугман почав роботу над алгоритмом розпізнавання параметрів райдужної оболонки ока і в 1994 році отримав патент на цю технологію. З цього моменту її ліцензували вже 22 компанії, в тому числі Sensar, British Telecom і японська OKI. Отримане при скануванні райдужної оболонки ока зображення зазвичай виявляється більш інформативним, ніж оцифроване у випадку сканування відбитків пальців.

Унікальність малюнка райдужної оболонки ока дозволяє випускати фірмам цілий клас досить надійних систем для біометричної ідентифікації особи. Для зчитування візерунка райдужної оболонки ока застосовується дистанційний спосіб зняття біометричної характеристики. Зараз використовуються два основні підходи розпізнавання райдужної оболонки ока, що відрізняються способами представлення образів.

У першому підході райдужна оболонка ока виділяється з зображення очей, у другому – образом є матриця штрих-кодів, відповідна радужці. У першому підході є два своїх способи подання: у вигляді кілець, що відносяться до області райдужної оболонки; у вигляді прямокутника, отриманого шляхом перетворення декартової системи координат в полярну. Спочатку визначається центр зіниці і два радіуси щодо нього – радіус зіниці і радіус зовнішнього краю райдужної оболонки (межі визначаються пороговою обробкою). Межі зіниці та райдужної оболонки не є при цьому круглими. Вони стають такими після додаткового оброблення. Після чого виконується збільшення чіткості образу.

Другий спосіб можна подати у вигляді такого алгоритму: визначення місця розташування, центру і контурів зіниці; визначення радіусів зіниці і зовнішнього краю райдужної оболонки; формування полярної системи координат; перетворення кожного пікселя з декартової системи в полярну.

На останньому етапі може знадобитися інтерполяція зображення, тому що цілочисельні декартові координати не завжди відповідають цілочисельним полярним. У результаті по осі X відкладені кути полярної системи координат, а по осі Y – значення радіуса (радіус зовнішнього кола радужки мінус радіус внутрішнього). Другий підхід, хоч і вимагає великих обчислень на етапі реєстрації, але зручніший тому, що поворот зображення, перетвореного з декартової системи координат в полярну, замінюється циклічним зсувом.

Другий підхід розпізнавання райдужної оболонки ока (одержання матриці штрих-кодів) можна подати наступним чином. Зображення ока виділяється з зображення обличчя, потім на райдужну оболонку накладається спеціальна маска

штрих-кодів. У результаті виходить матриця, отримана шляхом логічного множення маски на райдужну оболонку. Образ-еталон виходить розміром 512 байт. Системи цього класу, використовуючи звичайні відеокамери, захоплюють відео зображення очей на відстані до одного метра від відеокамери, здійснюють автоматичне виділення зіниці та райдужної оболонки. Пропускна здатність таких систем дуже висока. Ймовірність же помилкових спрацьовувань невелика. Крім цього, передбачений захист від муляжу. Вони сприймають лише око живої людини. Ще одна перевага цього методу ідентифікації – висока стійкість. На працездатність системи не впливають окуляри, контактні лінзи та сонячні відблиски.

Перевага сканерів для райдужної оболонки полягає в тому, що вони не вимагають, щоб користувач зосередився на цілі, тому що зразок плям на райдужній оболонці знаходиться на поверхні ока.

Навіть у людей з ослабленим зором, але з неушкодженою райдужною оболонкою, все одно можуть скануватися і кодуватися ідентифікуючі параметри. Навіть якщо є катаракта (ушкодження кришталика ока, яке знаходиться позаду райдужної оболонки), то і вона ніяк не впливає на процес сканування райдужної оболонки. Однак погане фокусування камери, сонячний відблиск та інші труднощі при розпізнаванні приводять до помилок в 1 % випадків. Перспективи поширення цього способу біометричної ідентифікації для організації доступу в комп'ютерних системах дуже великі. Тим більше, що зараз вже існують мультимедійні монітори з вбудованими в корпус відеокамерами. Тому на такий комп'ютер досить встановити необхідне програмне забезпечення і система контролю доступу готова до роботи. Зрозуміло, що і її вартість при цьому буде не дуже високою.

Динамічні методи біометричної автентифікації ґрунтуються на поведінковій (динамічній) характеристиці людини, тобто побудовані на особливостях, характерних для підсвідомих рухів у процесі відтворення якої-небудь дії.

Серед динамічних методів автентифікації розрізняють наступні:

– за рукописним почерком;
– за клавіатурним почерком;
– за голосом.

У сучасному світі все більше проявляється інтерес до мовних технологій, зокрема, до ідентифікації людини за голосом [23]. Це пояснюється, з одного боку,

появою високопродуктивних обчислювальних систем на базі персональних комп'ютерів і апаратних засобів, що дозволяють виробляти введення сигналу в комп'ютер, а, з іншого боку, високою потребою систем автентифікації в різних галузях життєдіяльності людини. Метод ідентифікації людини за голосом існує з того часу, як людина навчилася говорити. Тому переваги і недоліки цього методу відомі всім.

Привабливість даного методу – зручність у застосуванні. Метод перевірки голосу має дві позитивні відмінності від інших біометричних методів: по-перше, це ідеальний спосіб для телекомунікаційних програм; по-друге, більшість сучасних комп'ютерів вже мають необхідне апаратне забезпечення. Основна проблема, пов'язана з цим біометричним підходом – точність ідентифікації. Однак це не є серйозною проблемою з того моменту, як пристрої ідентифікації людини за голосом розрізняють характеристики людської мови.

Голос формується з комбінації фізіологічних і поведінкових чинників. В даний час ідентифікація за голосом використовується для керування доступом до приміщення середнього ступеня безпеки, наприклад, лабораторії та комп'ютерних класів. Ідентифікація за голосом зручний, але в той же час не такий надійний, як інші біометричні методи. Наприклад, людина з застудою або ларингітом може відчувати труднощі при використанні даних систем. Існує також можливість відтворення звукозапису з магнітофона.

Технологія розпізнавання голосу – ймовірно, найбільш практичне рішення для більшості мережевих додатків, у всякому разі, на даний момент.

Системи розпізнавання голосу аналізують характеристики цифрованої мови, в тому числі її тон, висоту і ритм. Незважаючи на те, що залишаються технічні питання, зокрема, на зниження надійності розпізнавання за наявності шумів, це досить економічне рішення, так як мікрофони і звукові картки вже давно отримали прописку в мережі.

Як відомо, джерелом мовного сигналу служить мовоутворюючий тракт, який збуджує звукові хвилі в пружному повітряному середовищі. Сформований мовний сигнал і передається у просторі у вигляді звукових хвиль. Приймач сигналу – це давач звукових коливань. Зазвичай для цих цілей використовують мікрофон – пристрій для перетворення звукових коливань в електричні. Існує велика кількість типів мікрофонів (вугільні, електродинамічні, електростатичні, п'єзоелектричні та ін.).

Але в мікрофонах будь-якого типу чутливим елементом є пружна мембрана, за допомогою якої передається коливальний процес під впливом звукових хвиль. Мембрана пов'язана з елементом, який перетворює коливання мембрани в електричний сигнал. З виходу мікрофона сигнал подається на вхід звукової картки персонального комп'ютера. Під час запису звукова картка є аналого-цифровим перетворювачем з широкими можливостями настроювання параметрів оцифрування. Основними параметрами є частота дискретизації та розрядність кодування. Ці параметри визначають якість і розмір вибірки, що отримується в результаті запису. Причому розмір запису і її якість прямо пропорційні, тобто чим вище якість запису, тим більше її розмір.

Щоб забезпечити компроміс між якістю і розміром, скористаємося знаннями про властивості людського голосу при виборі параметрів аналого-цифрового перетворення. На цей момент у нас і за кордоном реалізовані системи автоматичної ідентифікації за голосом, більшість з яких будуються за єдиною концептуальною схемою: здійснюється реєстрація користувача та обчислюється шаблон; вибираються ділянки мовного потоку для подальшого аналізу; здійснюється первинне оброблення сигналу; обчислюються первинні параметри; будується «відбиток» (шаблон) голосу; проводиться порівняння «відбитків» голосів і формується рішення щодо ідентичності голосів або «близькості» голосу до групи голосів.

Підпис – один з класичних способів ідентифікації, що застосовується вже кілька століть в юридичній практиці, банківській справі та торгівлі. Існує два незалежних способи ідентифікації за підписом [23]:

– ідентифікація за зображенням підпису на документі;

– ідентифікація за динамікою підпису, що вводиться в комп'ютер.

У першому способі потрібно порівняти два зображення. З цим краще впорається людина. У другому способі є дані про коливання пера при відтворенні підпису в тривимірному просторі (X, Y – координати і Z – тиск на планшет). З цим може впоратися тільки комп'ютер.

Ідентифікація за клавіатурним почерком – це ідентифікація людини за власним стилем друкування. Система ідентифікації за клавіатурним почерком заснована на фіксованому паролі, але приблизно можуть бути й незалежними від тексту, що набирається, як системи розпізнавання голосу.

Наведемо основні характеристики біометричних технологій:

– FTE (failure to enroll) – помилка зняття характеристики (помилка реєстрації в системі); час розпізнавання;

– стійкість до навколишнього середовища (експлуатаційні якості можуть втрачати стабільність в залежності від оточуючих умов);

– стійкість до підробки (несанкціонованого доступу);

– соціальна прийнятність – згода людей на збір даних;

– точність – будь-яку біометричну систему можна налаштувати на різну пильність;

– вартість.

Крім того, у кожній з реалізацій технології можна виділити також наступні характеристики:

– FRR (false rejection rate) – частота помилок «першого роду» – помилкова відмова;

– FAR (false acceptance rate) – частота помилок «другого роду» – помилковий допуск.

Для користувачів також важливі такі характеристики:

– можливість ідентифікації і автентифікації;

– складність реалізації систем ідентифікації;

– досягнута точність (рівень FRR і FAR);

– можливість безконтактного зчитування;

– розміри файла-еталона (чим більше розмір образу, тим повільніше йде розпізнавання).

В ідеальному варіанті система біометричної автентифікації мала б FAR = 0 і FRR = 0. Однак, такі значення в реальності не досяжні. Значення будь-якої з двох помилок можливо зменшити. Недолік цього у тому, що друге значення зросте. Зазвичай системні параметри налаштовують так, щоб досягти необхідного коефіцієнта помилкових підтверджень, що визначає відповідний коефіцієнт помилкових відмов.

На рисунку 2.8 наведена частота використання методів біометричної автентифікації за даними Acuity Market Intelligence [23].

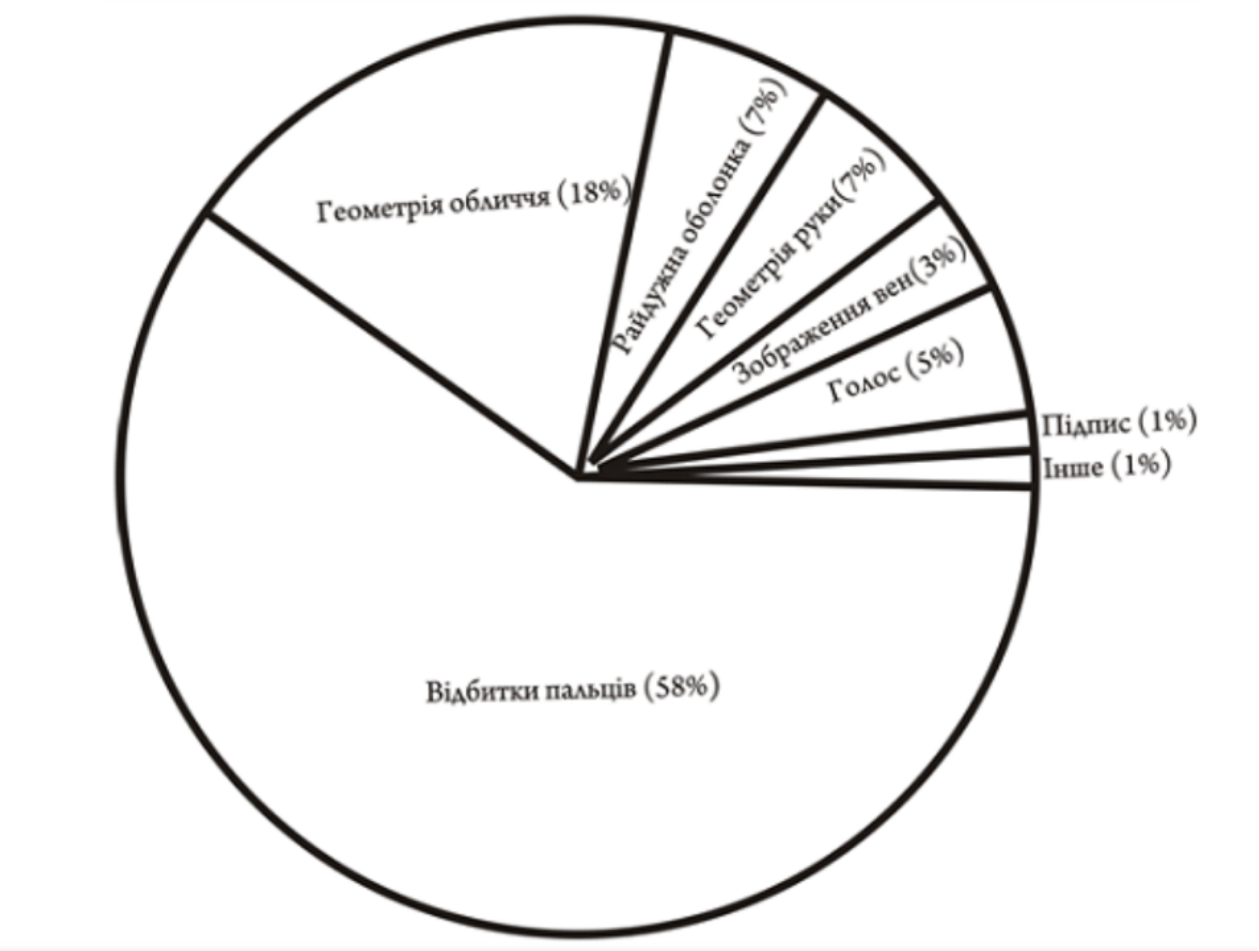

Рисунок 2.8 – Сегментація біометричного ринку по застосовуваним ідентифікаторам

Якщо систему необхідно охарактеризувати одним критерієм, то використовується коефіцієнт рівної ймовірності помилок 1-го і 2-го (EER – Equal Error Rates), який є точкою збігу ймовірностей FRR і FAR. Якісна і надійна система повинна мати низький рівень EER.

Порівняльний аналіз методів біометричної автентифікації проводився на основі помилок першого і другого роду, а також помилки зняття характеристики (FTE).

Порівняння проводилося за наступними біометричними параметрами: відбиток пальця, райдужна оболонка ока, 3-х мірне зображення обличчя, голос. Результати порівнянь наведені в таблиці 2.7.

На основі проведеного аналізу, можна зробити висновок про те, що найбільш точним і найкращим методом біометричної автентифікації є автентифікація за голосом.

Таблиця 2.7 – Порівняння біометричних систем

Характеристика	Відбиток пальця	Голос	Райдужка	Обличчя
Надійність верифікації	96,7-98%	99,14-99,9%	95,4-95,9%	95,9%
FTE	4%	2%	7%	0,1%
FAR	2,5%	0,75%	6%	0,1%
FRR	0,1%	0,75%	0,001%	2,5%
Вартість	100$	400$	500$	1200$

Біометричні технології автентифікації мають великі перспективи розвитку. При використанні систем на основі біометричних методів процедури доступу стають швидше, безпечніше і простіше. Але, незважаючи на величезну кількість переваг, біометричні технології мають ряд складнощів і проблем. Так, необхідно вирішувати питання щодо використання пристроїв біометричної ідентифікації людьми з деякими фізичними вадами, по підготовці професійних кадрів, зменшення вартості пристроїв та інше.

3 РОЗРОБКА ЗАХИЩЕНОГО МЕТОДУ РЕАЛІЗАЦІЇ ДИСТАНЦІЙНОЇ РОБОТИ

3.1 Дистанційна робота, технології та протоколи безпечної реалізації

Типові вимоги роботодавців до працівників вже не діють. На даний момент сформувався запит на активних, мобільних суб'єктів праці, готових до змін робочого процесу і бажаючих змінюватися в професійному плані. Всі ці зміни сприяють появі нового типу працівників, що виконують свої трудові завдання в режимі віддаленого доступу, поза територією звичного робочого місця роботодавця.

Дистанційна зайнятість – форма зайнятості, при якій працівник і роботодавець територіально розподілені, знаходяться поза єдиного офісного простору і взаємодіють один з одним за допомогою інформаційно-комунікаційних технологій. У сучасному світі працювати віддалено можна, як будучи співробітником компанії (перебуваючи в штаті організації), так і не будучи її штатним працівників, виконуючи конкретні завдання або реалізовуючи певні проекти. У першому випадку таку зайнятість правильно називати дистанційній, у другому – інтернет-самозайнятості або інтернет-фрілансом.

Робоче місце фрілансера може бути організовано в будинку, в кафе або в спеціалізованих центрах. На ринку праці фрілансерів саме останні набирають популярність. Вони називаються коворкінг-центрам. В коворкінг-центрах існує вся необхідна інфраструктура для виконання роботи: підключення до мережі Інтернет та електрики, зони харчування та відпочинку, переговорні і безпосередньо самі робочі місця.

Оплата праці фрілансера проводиться за годинної тарифної ставки. Також можливий варіант оплати за завершення поставленого завдання, по закінченню якого-небудь проекту. Самозайняті професіонали виконують роботи за завданнями від різних замовників, яких знаходять самостійно на спеціалізованих інтернет-майданчиках. При цьому і роботодавці здійснюють тут пошук підходящих кандидатів. В ряду міжнародних інтернет-майданчиків фріланс індустрії необхідно відзначити: Upwork, Freelancer, TopTal, тощо. Зокрема, Upwork – одна з найпопулярніших фріланс бірж, де кількість угод та виконаних робіт сягає понад 10 млн в рік. Інтерфейс системи простий і розібратися в ньому

починаючому фрілансеру не складе ніяких труднощів. При реєстрації можливо пройти спеціалізовані тести, що підтверджують знання і навички виконавця.

Неодмінною умовою здійснення віддаленої зайнятості є наявність у дистанційно зайнятого працівника або у фрілансера стаціонарного персонального комп'ютера або мобільного ноутбука. В даний час для здійснення робочого процесу набувають популярності мобільні пристрої: планшети і смартфони. Крім технічних засобів необхідно мати доступ в Інтернет. При виконанні особливо важливих робіт використовуються кілька інтернет-провайдерів для здійснення резервування.

Спеціалізоване програмне забезпечення віддаленого доступу до інформаційних ресурсів роботодавця дозволяє працівнику дистанційно виконувати практично всі поставлені завдання, як якщо б він знаходився в офісі за робочим комп'ютером. У той же час дистанційний наймання і фріланс в визначальною мірою залежать від безперебійно функціонуючої технології. Якщо організація має глобально розподілену команду (по декількох країнах), то у неї можуть виникнути проблеми технічного характеру, наприклад, повільна робота Інтернету в певних регіонах світу. В цьому випадку програми доступу до робочого комп'ютера допомагають дистанційно зв'язати працівника і його роботодавця. Технологія роботи таких програм дозволяє застосовувати їх на низьких швидкостях і неякісних інтернет-з'єднаннях. Часто використовуваними програмними засобами в категорії роботи з віддаленим робочим столом є Microsoft Remote Desktop (RDC), Citrix, Radmin, DameWare, VNC, TeamViewer.

Для вирішення проблеми комунікації між територіально розподіленими суб'єктами праці і для ефективної взаємодії віддаленого персоналу експлуатуються спеціалізовані засоби обміну повідомленнями та відеодзвінки. Їх застосування здатне замінити всі інші раніше використовувані засоби внутрішньокорпоративної комунікації. У ряду найбільш популярних інструментів спілкування можна виділити месенджер від компанії Google – Hangouts. Також можливість зібрати всю команду разом, забезпечити її членам комунікації, не пов'язані з роботою, обговорення останніх новин і особистих проблем забезпечує месенджер Slack. Він дозволяє об'єднати безліч сервісів в режимі «одного вікна» (Google Drive, Google Docs, Twitter, Trello, Google Hangouts, DropBox, Email, соціальні мережі та ін.). Для кожної теми і проекту можливо створити окремий канал. У Slack зручно проводити відео та аудіо конференції, отримувати аналітичну статистику, накопичувати знання для передачі колегам.

Дистанційна робота передбачає, що співробітники, які виконують свої функції поза офісом, позбавляються корпоративної культури. Тому менеджменту компанії необхідно забезпечувати регулярний контакт з працівниками для негайного усунення виникаючих проблем і подбати про те, щоб інструкції і регламенти по процесам для віддаленого персоналу були якомога більш ясними і точними. З зазначеними проблемами можуть допомогти впоратися технології управління талантами (англ. Talent management system, TMS), що дозволяють вирішувати питання навчання і розвитку, досягнення цілей, формування компетенцій, управління ефективністю та кар'єрним ростом працівників. Зокрема, лідерами ринку управління талантами визнані такі програми, як SuccessFactors, Oracle Talent Management Cloud та Webtutor.

З метою вивчення практики віддаленої роботи в вітчизняних організаціях була розроблена анкета та проведено дослідження. У дослідженні взяло участь 14 чоловік. З них кілька місяців працюють віддалено 38,5%; від 1 до 2 років – 7,1%; від 2 до 5 років – 47,2%; більше 5 років працюють 7,2% респондентів. Віддалено працюють в тиждень (приблизно): 1-8 ч – 42,9%; 9-18 ч – 14,3%; 19-27 ч – 14,3%; 28-36 ч – 14,3%; більше 40 ч – 14,3%.

Опитані вказали наступні напрямки діяльності організації, в яких вони працюють, але поза територією організації: інформаційні технології, юриспруденція, дослідження, виробництво і збут засобів індивідуального захисту, банківська сфера, освітня організація, навчання та консультаційні послуги, консалтинг, тренінги, банківська сфера, рекрутери, фахівці з оплати праці та бізнес-тренери.

При організації віддаленої роботи необхідно враховувати аспекти інформаційної безпеки, а саме, захист корпоративної ІС від НСД. Для виконання даної цілі налаштовуються VPN-з'єднання. Розглянемо кілька застосовуваних для цього протоколів: PPTP, L2TP/IPsec, SSTP і OpenVPN.

Специфікація PPTP розроблялася консорціумом, заснованим Microsoft для організації VPN. Тому PPTP довгий час залишався стандартом для корпоративних мереж. З цієї ж причини він використовує протокол шифрування Microsoft Point-to-Point Encryption (MPPE). Специфікація присутня на будь-якій VPN-сумісної платформі і легко налаштовується без додаткового програмного забезпечення. Ще одна перевага PPTP – висока швидкість. Але, PPTP недостатньо безпечний. З моменту включення протоколу до складу Windows 95 OSR2 в кінці дев'яностих, розкрилися кілька вразливостей. Найсерйозніша вразливість – це можливість

неінкапсульована автентифікації MS-CHAP v2. Це дозволило зламати PPTP за два дні. Microsoft спробували це виправити, перейшовши на протокол автентифікації PEAP, але потім самі запропонували використовувати VPN-протоколи L2TP / IPsec або SSTP. Ще один момент – PPTP-підключення легко заблокувати, тому що протокол працює з одним портом номер 1723 і використовує GRE-протокол.

Layer 2 Tunneling Protocol, або L2TP, також представлений практично у всіх сучасних операційних системах і працює з усіма VPN сумісними пристроями. L2TP не вміє шифрувати трафік, тому його часто використовують в зв'язці з IPsec. Однак це призводить до появи негативного ефекту – в L2TP / IPsec відбувається подвійна інкапсуляція даних, що негативно позначається на продуктивності. Також L2TP використовує п'ятисотий UDP-порт, який легко блокується файрволом, якщо ви перебуваєте за NAT. L2TP / IPsec вміє працювати з шифрами 3DES або AES. Перший вразливий для атак типу meet-in-the-middle і sweet32, тому сьогодні мало зустрічається на практиці. При роботі з AES-шифром про великі вразливості невідомо, тому в теорії цей протокол повинен бути безпечний при правильній реалізації. Найбільш серйозна проблема з L2TP / IPsec полягає в тому, що багато VPN-сервісів реалізують його недостатньо добре. Вони використовують pre-shared keys (PSK), які можна завантажити з сайту. PSK потрібні для встановлення з'єднання, тому навіть якщо дані виявляються скомпрометованими, вони залишаються під захистом AES. Але атакуючий може використовувати PSK, щоб видати себе за VPN-сервер і потім підслухати зашифрований трафік (навіть завантажити шкідливий код).

Secure Socket Tunneling Protocol, або SSTP, – це VPN-протокол, який розробляла компанія Microsoft. Він ґрунтується на SSL і вперше запущений в Windows Vista SP1. Сьогодні протокол доступний для таких ОС, як RouterOS, Linux, SEIL і Mac OS X, однак основне застосування він все одно знаходить на платформі Windows. Сам SSTP не має криптографічного функціоналу за винятком криптографічного зв'язування, що захищає від атаки MITM. Шифрування даних виконує SSL. Тісна інтеграція з Windows спрощує роботу з протоколом і підвищує його стабільність на цій платформі. Однак SSTP використовує SSL 3.0, який вразливий для атаки POODLE, що в теорії позначається на захищеності VPN-протоколу.

OpenVPN – це відкритий проект, який використовує бібліотеку Open SSL, TLS і ряд інших технологій. Сьогодні він є індустріальним стандартом в комерційних VPN-сервісах і реалізується на будь-якій платформі за допомогою

стороннього ПО. Серед достоїнств OpenVPN виділяється можливість його настройки. Його можна налаштувати для роботи на будь-якому порті. Це дозволяє пересилати трафік наприклад через порт 443, щоб замаскувати його під HTTPS, що ускладнює блокування. Ще одна перевага протоколу – бібліотека OpenSSL. Вона підтримує багато криптоалгоритмів – це 3DES, CAST-128, Camelia, AES і Blowfish.

Останні два найчастіше використовуються на практиці. Також плюсом OpenVPN можна вважати регулярні аудити. Остання проведена перевірка не виявила вразливостей, що впливають на безпеку даних користувачів. Раніше були знайдені кілька вразливостей, що дають зловмисникам можливість проводити DDoS-атаки, але розробники вирішили ці проблемі в новій версії OpenVPN. OpenVPN вважається одним з найнадійніших VPN-протоколів наявних сьогодні і широко підтримується VPN-індустрією.

3.2 Налаштування доступу до корпоративної сеті з використання технології OpenVPN

Розглянемо найчастіший сценарій використання VPN-з'єднання для віддаленого підключення співробітників до робочого місця в офісі за допомогою RDP-з'єднання. На рисунку 3.1 представлена схема використання OpenVPN в корпоративній мережі.

OpenVPN дозволяє створити захищену віртуальну мережу між декількома машинами. Для забезпечення безпеки використовуються наступні механізми:

- автентифікація учасників з'єднання;
- цілісність за рахунок механізму HMAC;
- конфіденційність за рахунок шифрування з'єднання.

Учасники з'єднання після успішної автентифікації виробляють сесійний ключ, який використовується для шифрування пакетів. Для шифрування переданих даних використовується протокол SSL / TLS. Криптографічні операції виконують бібліотеки OpenSSL.

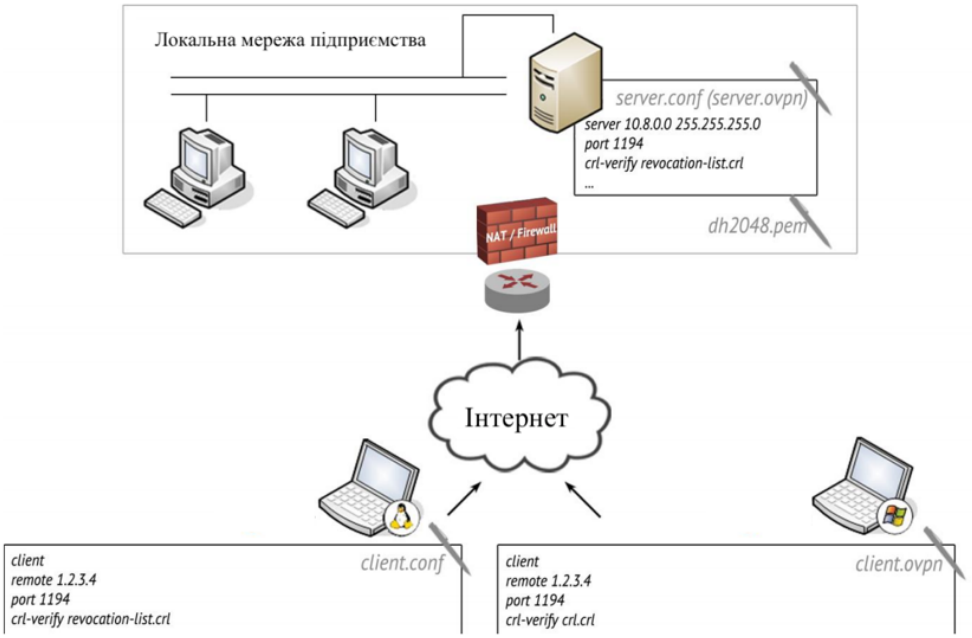

Рисунок 3.1 – Корпоративна мережа з використання OpenVPN

OpenVPN пропонує три методи автентифікації:

– автентифікація симетричним ключем;

– автентифікація за логіном і паролем;

– автентифікація за сертифікатами X.509.

Найбільш ефективним і надійним методом автентифікації є використання сертифікатів стандарту X.509.

Використання сертифікатів дозволяє успішно захистити з'єднання від атак типу MITM.

При ініціалізації з'єднання відбувається обмін сертифікатами, на цьому етапі перевіряються:

– підписані чи сертифікати сторін довіреною кореневих сертифікатом (вказаним у файлі конфігурації сервера і клієнта);

– чи дійсні сертифікати сторін (чи не минув термін дії сертифіката);

– чи не були сертифікати сторін відкликані (опціонально);

– вірний чи тип сертифіката використовують боку (опціонально).

У разі успішної автентифікації сторони переходять до генерації сесійного ключа і встановлення з'єднання.

Для комплексного розуміння технології всі компоненти мережі OpenVPN представлені у таблиці 3.1.

Таблиця 3.1 – Компоненти мережі OpenVPN

Компонент	Опис
Засвідчуючий центр CA	Видає сертифікати на вимогу вузлів мережі VPN, підписані сертифікатом засвідчуючого центру. Надає вузлам мережі VPN свій власний сертифікат для перевірки засвідчуючого боку. Управляє списком відкликаних сертифікатів CRL.
Сервер OpenVPN	ПО сервера OpenVPN створює тунель всередині незахищеної мережі, наприклад, Інтернету. Цей тунель забезпечує безпечний зашифрований трафік між вузлами – учасниками обміну даними в мережі OpenVPN.
Клієнт OpenVPN	ПО клієнта OpenVPN встановлюється на всі вузли, яким необхідний захищений канал передачі даний з сервером OpenVPN. При відповідному налаштуванні сервера OpenVPN можлива захищена передача даних між клієнтами OpenVPN, а не тільки між клієнтами і сервером OpenVPN.
Сертифікати (публічні ключі) X.509	Сертифікати X.509 є публічними ключами, завіреними засвідчуючим центром CA. Вони використовуються для шифрування даних. Факт запевнення сертифікату засвідчуючим центром CA дозволяє ідентифікувати сторону, яка транслює зашифровані дані. Файл запиту на сертифікат створюється на вузлах мережі, потім він переноситься на вузол, що засвідчує, і там підписується. Створений в результаті підписаний сертифікат переноситься назад на запитав його вузол мережі OpenVPN.
Приватні ключі	Приватні ключі секретні. Вони повинні створюватися і зберігатися на кожному вузлі мережі OpenVPN, призначені для розшифрування даних і ніколи не повинні передаватися по мережі. Приватні ключі створюються на вузлах мережі OpenVPN одночасно з файлом запиту на отримання сертифіката.
Список відкликання сертифікатів CRL	Містить список сертифікатів, які втратили довіру. Він створюється і редагується на вузлі, що засвідчує, CA. Щоб відключити вузол від мережі, досить занести його сертифікат в список CRL. Після створення і кожного зміни список CRL переноситься на сервери OpenVPN.
Файл Діффі-Хелмана	Використовується, щоб в разі викрадення ключів виключити розшифрування трафіку, записаного ще до цього викрадення. Створюється на сервері OpenVPN.
Статичний ключ HMAC	Служить для перевірки справжності переданої інформації. Забезпечує захист від DoS-атак і флуду. Створюється на сервері OpenVPN.

Тепер, розуміючи теоретичну основу розглядаємої технології, можна приступати до практичного налаштування. Спочатку необхідно створити та налагодити роботу засвідчуючого центру CA.

Всі операції по створенню ключів і сертифікатів можна виконати за допомогою утиліти openssl. Однак простіше скористатися спеціально створеною для цього програмою Easy-RSA, яка використовує openssl для виконання дій з ключами і сертифікатами. Раніше утиліта Easy-RSA поставлялася разом з OpenVPN, але тепер це окремий проект. Тож, необхідно створити користувача з ім'ям та перейти в домашній каталог, де завантажити дистрибутив програми утилітою wget. Після завантаження треба розпакувати архів master.zip. Команди, які для цього використовуються представлені на рисунку 3.2.

```
# adduser ca
# su ca
$ cd
$ wget https://github.com/OpenVPN/easy-rsa/archive/master.zip
$ unzip master.zip
```

Рисунок 3.2 – Завантаження утиліти Easy-RSA

У таблиці 3.2 перераховані файли і каталоги, що входять в дистрибутив Easy-RSA.

Таблиця 3.2 – Компоненти дистрибутиву Easy-RSA

Файл або каталог	Опис
COPYING	Інформація про ліцензію
ChangeLog	Журнал змін
Licensing	Каталог з файлом тексту ліцензії
README	Коротка інформація про програму Easy-RSA
README.quickstart.md	Короткий посібник по роботі з Easy-RSA
Build	Скрипт для створення дистрибутива
Distro	Цей каталог містить файли для Windows
Doc	Документація Easy-RSA
easyrsa3	Каталог з програмою Easy-RSA
release-keys	Ключ GPG Key ID для підпису дистрибутива

Для того щоб створити інфраструктуру публічних ключів (Public Key Infrastructure, PKI) та засвідчуючий центр CA необхідно виконати команди на рисунку 3.3.

```
$ cd /home/ca/easy-rsa-master/easyrsa3
$ ./easyrsa init-pki
$ ./easyrsa build-ca
```

Рисунок 3.3 – Створення інфраструктури ключів та центру сертифікації

У відповідь на цю команду необхідно ввести пароль та ім'я Common Name. Пароль буде захищати приватний ключ засвідчувального центру, створений в форматі PEM (Privacy Enhancement for Internet Electronic Mail). Цей пароль потрібно буде вводити кожного разу, коли треба підписувати в засвідчувальному центрі сертифікати для серверів і клієнтів OpenVPN. Команда build-ca створить два файли, представлені на рисунку 3.4. Файл ca.key є приватним ключем центру CA, він секретний, і його не можна переносити на інші вузли мережі. Файл сертифіката ca.crt, навпаки, відкритий, і він буде потрібен на вузлах серверів і клієнтів OpenVPN.

```
/home/ca/easy-rsa-master/easyrsa3/pki/private/ca.key
/home/ca/easy-rsa-master/easyrsa3/pki/ca.crt
```

Рисунок 3.4 – Ключ та сертифікат центру сертифікації

Для співробітників які звільняються необхідно заблокувати доступ в мережу VPN компанії. Спеціально для цієї мети в OpenVPN передбачений список відкликання сертифікатів CRL. Для створення списку треба виконати команди представлені на рисунку 3.5. Список відкликання сертифікатів буде створений в файлі /home/ca/easy-rsa-master/easyrsa3/pki/crl.pem.

```
$ cd /home/ca/easy-rsa-master/easyrsa3
$ ./easyrsa gen-crl
```

Рисунок 3.5 – Створення списку відкликання сертифікатів

Якщо потрібно заблокувати виданий раніше сертифікат, треба ввести команду на рисунку 3.6.

```
$ ./easyrsa revoke name_of_user
```

Рисунок 3.6 – Блокування сертифікату

У таблиці 3.3 приведено короткий опис файлів і каталогів PKI, створених на стороні засвідчуючого центу CA.

Таблиця 3.3 – Компоненти дистрибутиву Easy-RSA

Файл або каталог	Опис
ca.crt	Сертифікат засвідчую чого центу CA, що не секретний
crl.pem	Список відкликання сертифікатів CRL
Issued	Каталог з сертифікатами, створеними засвідчуючим центром, не секретні
Private	Каталог з секретними приватними ключами
Reqs	Каталог запитів на сертифікати, які не секретний

Після того, як всі необхідні налаштування для центра CA виконані необхідно перейти до налаштування сервера OpenVPN. Процес створення сервера OpenVPN включає в себе завантаження пакета openvpn, підготовку файлів конфігурації, ключів і сертифікатів.

Після встановлення пакета сервера OpenVPN необхідно підготувати файли конфігурації openssl.cnf і server.conf. Перший з цих файлів визначає конфігурацію OpenSSL та представлений на рисунку 3.7. Другий файл визначає конфігурацію сервера OpenVPN та представлений на рисунку 3.8.

```
[ ca ]
default_ca = CA_default
[ CA_default ]
dir = /etc/openvpn
crl_dir = $dir
database = $dir/index.txt
new_certs_dir = $dir
certificate = $dir/ca.crt
serial = $dir
crl = $dir/crl.pem
private_key = $dir/server.key
RANDFILE = $dir/.rand
default_days = 3650
default_crl_days = 365
default_md = md5
unique_subject = yes
policy = policy_any
x509_extensions = user_extensions
[ policy_any ]
organizationName = match
organizationalUnitName = optional
commonName = supplied
[ req ]
default_bits = 2048
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
x509_extensions = CA_extensions
[ req_distinguished_name ]
organizationName = Organization Name (must match CA)
organizationName_default = Company
organizationalUnitName = Location Name
commonName = Common User or Org Name
commonName_max = 64
[ user_extensions ]
basicConstraints = CA:FALSE
[ CA_extensions ]
basicConstraints = CA:TRUE
default_days = 3650
[ server ]
basicConstraints = CA:FALSE
nsCertType = server
```

Рисунок 3.7 – Файл конфігурації OpenSSL (openssl.cnf)

```
port 1194
proto udp
dev tun
user openvpn
group openvpn
cd /etc/openvpn
persist-key
persist-tun
tls-server
tls-timeout 120
dh /etc/openvpn/dh.pem
ca /etc/openvpn/ca.crt
cert /etc/openvpn/vpn-server.crt
key /etc/openvpn/server.key
crl-verify /etc/openvpn/crl.pem
tls-auth /etc/openvpn/ta.key 0
server 10.15.0.0 255.255.255.0
client-config-dir /etc/openvpn/ccd
client-to-client
topology subnet
max-clients 5
push "dhcp-option DNS 10.15.0.1"
route 10.15.0.0 255.255.255.0
comp-lzo
keepalive 10 120
status /var/log/openvpn/openvpn-status.log 1
status-version 3
log-append /var/log/openvpn/openvpn-server.log
verb 3
mute 20
```

Рисунок 3.8 – Файл конфігурації сервера OpenVPN (server.conf)

Крім openssl.cnf і openvpn.conf в каталозі / etc / openvpn / також потрібні файли, перераховані в таблиці 3.4.

Таблиця 3.4 – Файли серверної частини OpenVPN

Файл	Опис
dh.pem	Файл Діффі-Хелмана для захисту трафіку від розшифровки
ca.crt	Сертифікат засвідчуючого центру CA
Server.crt	Сертифікат сервера OpenVPN
Server.key	Приватний ключ сервера OpenVPN, секретний
crl.pem	Список відкликання сертифікатів CRL
ta.key	Ключ HMAC для додаткового захисту від DoS-атак і флуду

Перш за все необхідно створити приватний ключ і файл запиту на сертифікат для сервера OpenVPN, а також отримати по створеному запиту в засвідчувальному центрі CA підписаний сертифікат. В результаті з'являться файли server.crt і server.key. Щоб створити для сервера OpenVPN запит на сертифікат і приватний ключ, потрібно встановити на сервер OpenVPN програму Easy-RSA, аналогічно тому, як це було зроблено для засвідчувального центру CA.

Сервер OpenVPN не буде відігравати роль центра, що засвідчує, тому після ініціалізації PKI не треба створювати CA командою build-ca. Інфраструктура PKI буде створена в каталозі / home / vpnoperator / easy-rsa-master / easyrsa3 / pki. На рисунку 3.9 представлена команда для отримання запиту на сертифікат і приватний ключ сервера OpenVPN. Цією командою буде створений файл запиту server.req і приватний ключ server.key.

```
$ ./easyrsa gen-req server
```

Рисунок 3.9 – Запит сертифікату та приватного ключа сервера OpenVPN

Тепер необхідно змонтувати USB флеш-диск на хості, що засвідчує CA, та імпортувати від імені користувача запит в PKI і підписати запит на отримання сертифіката завдяки командам представленім на рисунку 3.10. Результат роботи команд представлений на рисунку 3.11.

```
$ cd /home/ca/easy-rsa-master/easyrsa3
$ ./easyrsa import-req /mnt/flash/server.req vpn-server
./easyrsa sign-req server vpn-server
```

Рисунок 3.10 – Команди для підписання запиту на стороні центру сертифікації

```
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request has not been cryptographically verifie
d. Please be sure it came from a trusted source or that you have verified the request checksum with the sender.
Request subject, to be signed as a server certificate for 3650 days:

subject=
    commonName                = server
Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from /home/ca/easy-rsa-master/easyrsa3/openssl-1.0.cnf
Enter pass phrase for /home/ca/easy-rsa-master/easyrsa3/pki/private/ca.key:******
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'server'
Certificate is to be certified until Jun 26 15:48:25 2024 GMT (3650 days)
Write out database with 1 new entries
Data Base Updated
Certificate created at: /home/ca/easy-rsa-master/easyrsa3/pki/issued/vpn-server.crt
```

Рисунок 3.11 –Процес підписання запиту на стороні центру сертифікації

Коли сертифікат отриман та знаходиться на сервері засвідчувального центру у файлі home / ca / easy-rsa-master / easyrsa3 / pki / issued / vpn-server.crt, його необхідно передати на сервер OpenVPN.

Для створення ключа Діффі-Хелмана треба запустити команди представлені на рисунку 3.12.

```
$ cd /home/vpnoperator/easy-rsa-master/easyrsa3
$ ./easyrsa gen-dh
```

Рисунок 3.12 – Створення ключа Діффі-Хелмана

Для створення ключа HMAC використовується команда openvpn з опціями --genkey і –secret, представлена на рисунку 3.13.

```
# cd /etc/openvpn
# openvpn --genkey --secret ta.key
```

Рисунок 3.13 – Створення ключа HMAC

Отже, ми отримали з засвідчувального центру підписаний сертифікат сервера OpenVPN, сертифікат самого засвідчувального центру CA, список

відкликання сертифікатів, створили файл Діффі-Хелмана і ключ HMAC, тому тепер переходимо до налаштування клієнту OpenVPN.

Процедура установки клієнта OpenVPN аналогічна процедурі установки сервера OpenVPN. Основні відмінності в файлах конфігурації.

Файли конфігурації, ключі та сертифікати повинні знаходиться в каталозі / etc / openvpn. Файл openssl.cnf, що визначає конфігурацію OpenSSL, використовуйте такий самий, як і для сервера OpenVPN. Файл client.conf для клієнта OpenVPN ж представлений на рисунку 3.14.

```
dev tun
proto udp
remote 192.168.0.54 1194
client
resolv-retry infinite
ca "/etc/openvpn/ca.crt"
cert "/etc/openvpn/developer1.crt"
key "/etc/openvpn/client.key"
tls-auth "/etc/openvpn/ta.key" 1
remote-cert-tls server
persist-key
persist-tun
comp-lzo
verb 3
status /var/log/openvpn/openvpn-status.log 1
status-version 3
log-append /var/log/openvpn/openvpn-client.log
```

Рисунок 3.14 – Файл client.conf для клієнта OpenVPN

Після створення інфраструктури публічних ключів PKI потрібно створити запит на сертифікат і приватний ключ робочої станції користувача, використовуючи команду на рисунку 3.15.

```
$ ./easyrsa gen-req client
```

Рисунок 3.15 – Запит на сертифікат і приватний ключ від клієнта OpenVPN

Тепер потрібно перенести створений запит сертифіката /home/developer1/easy-rsa-master/easyrsa3/pki/reqs/client.req на хост засвідчуючого

центру і записати в файл /home/ca/client.req. Для того щоб підписати запит від клієнта OpenVPN використовується команда на рисунку 3.16.

```
$ ./easyrsa sign-req client developer1
```

Рисунок 3.16 – Підписаннях запиту від клієнта OpenVPN

Після введення підтвердження і пароля приватного ключа CA буде створений сертифікат /home/ca/easy-rsa-master/easyrsa3/pki/issued/developer1.crt.

Тепер файл developer1.crt треба записати разом з файлами ca.crt і ta.key та перенести їх на хост клієнта OpenVPN. Після цього можна запускати роботу OpenVPN на хості клієнта та перевірити з'єднання командою ping.

Завдяки даному методу можливо побудувати достатньо захищеній зв'язок між корпоративною мережею та співробітником, який працює дистанційно. Але, треба звернути увагу, що в цьому методу є незручності, а саме неможливість самостійного налаштування клієнта OpenVPN для співробітника, який не володіє достатніми технічними знаннями. Також, зберігання секретного ключа на незахищеному хості співробітника може призвести до його компрометації. Зазначені проблеми можна вирішити завдяки використанню USB-токенів разом з технологію OpenVPN.

3.3 Застосування USB-токенів у поєднанні з технологією OpenVPN

В попередньому розділі була представлена схема налаштування OpenVPN, в якій користувачі зберігають сертифікат і закритий ключ у файлі формату PKCS # 12 (файл з розширенням .pfx в Windows і .p12 в Linux або MacOS). В цьому випадку доступ до закритого ключа захищений паролем. Для підвищення рівня безпеки та зручності користувачів сертифікати клієнта можуть бути записані на USB-ключ ESMART Token.

Можна виділити наступні переваги зберігання сертифіката користувача на USB-токені, а не у вигляді файлів .pfx:

– всі криптографічні операції з закритим ключем виконуються безпосередньо на USB-ключі ESMART Token, закритий ключ з токена не розгорнеться;

– застосовується двофакторна автентифікація: користувач встановлює з'єднання, пред'являючи сертифікат на USB-ключі ESMART Token і вводить ПІН-код;

– ПІН-код карти захищена від злому методом перебору, кількість спроб задається при ініціалізації токену;

– після вилучення токену в системі залишається тільки сертифікат відкритого ключа, який не є секретним;

– додатково на USB-ключі може зберігатися кореневий сертифікат корпоративного центру сертифікації;

– додатково на USB-ключі може зберігатися призначений для користувача файл конфігурації OpenVPN в текстовому вигляді (в тому числі в захищеному режимі, коли доступ до даних з'являється тільки після пред'явлення ПІН-коду). Схематична робота представлена на рисунку 3.17 та всі необхідні налаштування для комплексної роботи наведені далі у розділі.

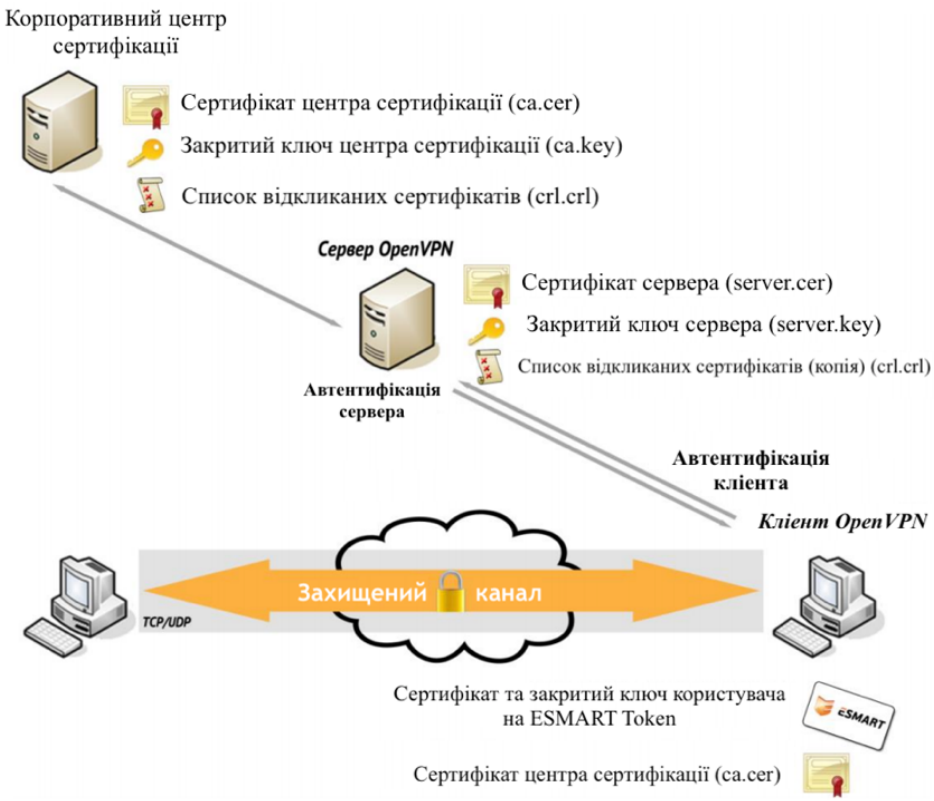

Рисунок 3.17 – Схема мережі з використання OpenVPN та ESMART Token

Всі необхідні команди для налаштування токену перед його використанням приведені в таблиці 3.5.

Таблиця 3.5 – Команди для налаштування ESMART Token

Опис	Команда
Встановлення бібліотеки PKCS#11	rpm -ivh isbc-pkcs11-x.x.x-x.i586.rpm
Ініціалізація токену під Linux	pkcs11-tool --module /usr/lib/libisbc_pkcs11_main.so --init-token --label EsmartToken
Створення ключової пари RSA 1024	pkcs11-tool --module isbc_pkcs11_main.dll --keypairgen --key-type rsa:1024 --login --id 1024 --label myrsakey
Підключення модулю isbc_pkcs11_main.dll	engine -t dynamic -pre SO_PATH:engine_pkcs11 -pre ID:pkcs11 -pre LIST_ADD:1 -pre LOAD -pre MODULE_PATH:isbc_pkcs11_main.dll -pre VERBOSE
Створення запиту на сертифікат	req -engine pkcs11 -new -key slot_1-id_1024 -keyform engine -out cert.csr

Тепер коли запит на сертифікат створено треба підписати його в засвідчуючому центрі CA та записати вже підписаний сертифікат на карту, використовуючи команду на рисунку 3.18.

```
pkcs11-tool --module isbc_pkcs11_main.dll -w cert.cer -y cert –login --id 1024 --label certificate
```

Рисунок 3.18 – Запис підписаного сертифікату на ESMART Token

При використанні ESMART Token також необхідно додати зміни до конфігураційного файлу клієнта, які представлені на рисунку 3.19.

```
dev tun
proto udp
remote 192.168.0.54 1194
client
resolv-retry infinite
ca "/etc/openvpn/ca.crt"
pkcs11-providers /usr/lib/libisbc_pkcs11_main.so
pkcs11-id 'ISBC/ESMART\%20Token/205A406291CB/test/653961313964656 52D39653130 2D653332362D63265312D6166323138646135366 13538'
tls-auth "/etc/openvpn/ta.key" 1
remote-cert-tls server
persist-key
persist-tun
comp-lzo
verb 3
status /var/log/openvpn/openvpn-status.log 1
status-version 3
log-append /var/log/openvpn/openvpn-client.log
```

Рисунок 3.19 – Файл client.conf для клієнта з ESMART Token

При підготовці клієнта потрібні текстовий файл конфігурації та файл кореневого сертифіката. Обидва файли можна також записати на ESMART Token. У цьому випадку все необхідне для встановлення з'єднання буде зберігатися на одному носії. Встановити OpenVPN можна буде зі сховищ. Для роботи з

сертифікатами та даними треба встановити безкоштовний графічний додаток ESMART PKI Client представлений на рисунку 3.20.

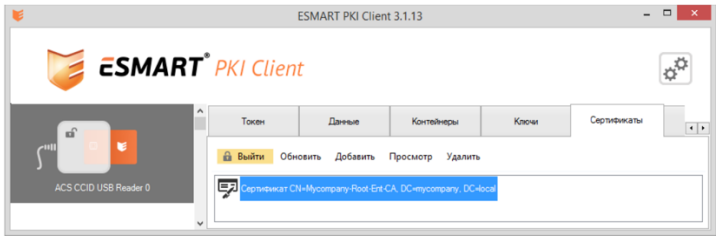

Рисунок 3.20 – Додаток ESMART PKI Client

Для запису файлів на ESMART Token необхідно авторизуватися на токені з допомогою PIN-коду та у вкладці «Значение» створити новий блок і в поле «Значення» скопіювати вміст файлу кореневого сертифіката в кодуванні Base64. Якщо при додаванні блоку відзначити опцію Захищені, блоки будуть видні тільки після авторизації на карті. На рисунку 3.21 зображено блок даних з файлом конфігурації.

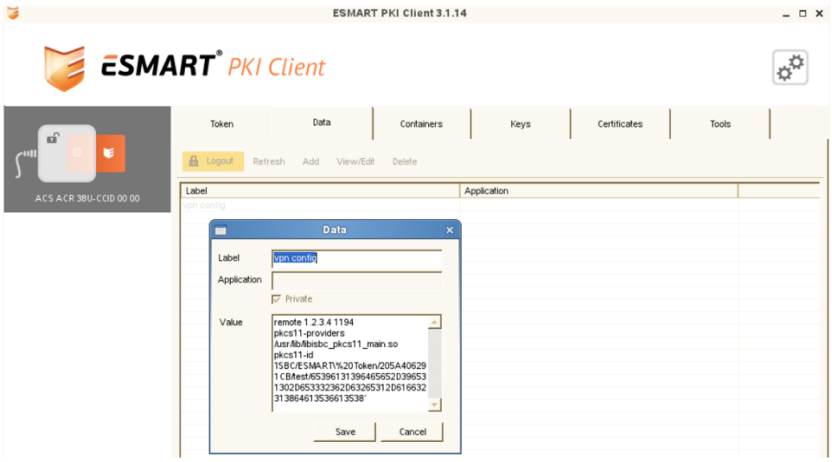

Рисунок 3.21 – Блок даних з файлом конфігурації

Таким чином, ESMART Token повністю готовий для використання співробітником, який працює за межами офісу, але потребую захищеного доступу до інформаційної системи компанії.

Повертаючись до теми роботи, можна зазначити, що в представленій схемі використовується двофакторний метод автентифікації:

– автентифікація з USB-токеном, який належіть;
– автентифікація за паролем, який знаєш.

Система є достатнього захищеною, але все таки існує ймовірність, що токен можуть викрасти та вгадавши пароль виконати несанкціоноване проникнення до мережі. Тому, в компаніях, де питання безпеки дуже важливе з точки зору цінності інформації, я пропоную розробити нову модель токенів з сканером відбитку пальця власника. Модель токену, яку я пропоную використовувати у майбутньому представлена на рисунку 3.22.

Рисунок 3.22 – Модель токену з сканером відбитку пальця

З використанням біометрики безпечність токена значно зростає, бо навіть якщо зловмиснику вдасться викрасти токен, то використати його буде неможливо без відбитка пальця власника його USB-ключа.

ВИСНОВКИ

Завдання на атестаційну роботу виконано. У ході виконання роботи було виявлено, що в якості основних факторів автентифікації можна використовувати: властивість, якою володіє суб'єкт; знання, тобто інформацію, яку знає суб'єкт; володіння – сутність, яку має суб'єкт. При побудові механізмів багатофакторної автентифікації можуть використовуватися окремі механізми, об'єднані послідовно, паралельно або комбіновано. У роботі запропоновано математичну модель механізму трьохфакторної автентифікації та оцінено ймовірність здійснення НСД. Дана модель може бути поширена на довільний розмір простору автентифікації і носить загальний характер.

Також було проаналізовано найпоширеніші методи автентифікації за трьома сутностями. Розглянуто біометричні методи, використання носіїв автентифікаційної інформації, застосування асиметричної криптографії для. При багатофакторній автентифікації значення ймовірності НСД залежить від ймовірностей НСД для кожного з факторів, для отримання оцінки яких необхідно обґрунтувати і конкретизувати метод здійснення атаки для кожного з факторів і визначити для кожного з методів можливість реалізації, можливі похибки і т.п.

У практичній частині роботи було налагоджено захищений метод доступу до корпоративної мережі компанії співробітниками, які працюють дистанційно. Для цього була використана технологія OpenVPN з найбільш ефективним і надійним методом автентифікації з використання сертифікатів стандарту X.509, що дозволяє введення двофакторної автентифікація: користувач встановлює з'єднання, пред'являючи сертифікат на USB-ключі ESMART Token і вводить ПІН-код. Також, на базі проаналізованого матеріалу стосовно вразливостей методів автентифікації та існуючих методів біометричної автентифікації, було запропоновано новий вид токену зі сканером відбитка пальця, враховуючи існуючі вразливості парольної автентифікації.

Окремі результати атестаційної роботи опубліковані у [7-9].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Proposal for a regulation of the European parliament and of the council on electronic identification and trust services for electronic transactions in the internal market: COM (2012) 11 final. – European Commission 04.06.2012. – Brussels: European Commission, 2012. – 119 p.

2. Закон України «Про електронні довірчі послуги» від 14.01.2020 № 440- IX [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2155-19/.

3. Галатенко В.А. Основы информационной безопасности / В. А.Галатенко. – М.: Интернет Университет Информационных Технологий, 2006. – 208 с.

4. Барабанова М.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях/ М.И. Барабанова, В.И. Кияев – СПб.: СПбГУЭФ, 2010. – 267 с.

5. Поповський В. В. Основи криптографічного захисту інформації в телекомунікаційних системах. Навчальний посібник. Частина 1 / В. В. Поповський, А. В. Персіков. – Харків: СМИТ, 2010. – 352 с.

6. Кавуненко Я. О. Оптимізація застосування комплексного методу захисту інформації від витоку по каналам побічних електромагнітних випромінювань / Я. О. Кавуненко. // Харків, ХНУРЕ, Матеріали XXII міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». Том 4. – 2018. – С. 124 – 125.

7. Кавуненко Я. О. Исследование и обоснование выбора методов многофакторной аутентификации / Я. О. Кавуненко, Н. В. Подоляка // Харків, ХНЕУ імені Семена Кузнеця, Матеріали Міжнародної науково-практичної конференції «Інформаційна безпека та інформаційні технології»: тези доповідей, 24-25 квітня 2019 р. – 2019. – С. 11.

8. Кавуненко Я. О. Аналіз криптографічних систем і перспектива використання протоколів у групах КОС / Я. О. Кавуненко. // Харків, ХНУРЕ, Матеріали XXIV міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». – у друці (рік виходу – 2020).

9. Подоляка Н. В. Комплексний підхід при виборі методології оцінки ризиків серверної кімнати як об'єкту підвищеного ризику компанії /

Н. В. Подоляка, Я. О. Кавуненко. // Харків, ХНУРЕ, Матеріали XXIV міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». – у друці (рік виходу – 2020).

10. International Organization for Standardization [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: http://www.iso.org.

11. Романов В. Биометрическая идентификация личности: современное состояние и перспективы развития в Украине / В. Романов, И. Галелюка, П. Клочан. // Электронные компоненты и системы. – 2010. – №5. – С. 16–20.

12. ISO/IEC 19785-1:2015 Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.iso.org/ru/standard/66179.html.

13. Брюхомицкий Ю. А. Тестирование биометрических систем контроля доступа [Електронний ресурс] / Ю. А. Брюхомицкий, М. Н. Казарин. – 2006. – Режим доступу до ресурсу: https://cyberleninka.ru/article/n/testirovanie-biometricheskih-sistem-kontrolya-dostupa/viewer.

14. Гинце А. Новые технологии в СКУД [Електронний ресурс] / А. Гинце // Системы безопасности. – 2005. – Режим доступу до ресурсу: https://www.aktivsb.ru/statii/novye_tekhnologii_v_skud.html.

15. ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца»

16. ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальцев».

17. ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица».

18. ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза».

19. Jain A. Introduction to Biometrics [Text] /A. Jain, A. Ross.// Handbook of Biometrics. Springer. – 2008. – p. 1–22.

20. Крахмалев А. К. Средства и системы контроля и управления доступом / А. К. Крахмалев. – М.: НИЦ «Охрана» ГУВО МВД России, 2003. – 85 с.

21. Татарченко Н. В. Биометрическая идентификация в интегрированных системах безопасности/ Н. В. Татарченко, С. В. Тимошенко. – М.: Специальная техника, 2002. – 125 с.

22. Горбенко І.Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія./ І.Д. Горбенко, Ю.І. Горбенко – Харків: «Форт», 2010. – 608 с.

23. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія./ І.Д. Горбенко, Ю.І. Горбенко – Харків: «Форт», 2012. – 880 с.