МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

"На правах рукопису"
УДК 681.3.06

«До захисту допущено»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)

“_____” січня 2022 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **МЕТОДИ ТА ЗАСОБИ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНО-ТЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА ВИРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ ЇХ ЕФЕКТИВНОСТІ**

Студент групи СЗДМ-61 Перепелиця Ліна Сергіївна _____

Науковий керівник: к.т.н.,проф. Ахрамович Володимир Миколайович _____

Нормоконтроль: Гребенніков Ассаді Болдхоягович _____

КИЇВ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ Г. В. Шуклін
(підпис)
“___”_____ 2021 р.

ЗАВДАННЯ

на магістерську атестаційну роботу

студенту Перпелиці Ліні Сергіївні

1. **Тема роботи:** «Методи та засоби автентифікації користувачів вінформаційно-текомунікаційних системах та вироблення рекомендацій щодо підвищення їх ефективності»
   Затверджена наказом по університету “___”_____2021 р. № _____
2. **Термін здачі** студентом оформленої роботи “___”_____2021 р.
3. **Об’єкт дослідження:** Процес ідентифікації та аутентифікації користувачів у інформаційно-телекомунікаційних системах.
4. **Предмет дослідження:** Методи ідентифікації та аутентифікації користувачів в інформаційно-телекомунікаційних системах.
5. **Мета дослідження:** Дослідження методів і засобів та їх використання у проведенні ідентифікації/аутентифікації користувачів в інформаційно-телекомунікаційних системах підприємства (організації) для організації їх доступу та роботи в мережах.
6. **Перелік питань, які мають бути розроблені:**
   1. Аналіз сучасних методів і засобів ідентифікації та автентифікації.
   2. Шляхи побудови раціональної системи ідентифікації та автентифікації в інформаційно-комунікаційних системах.
7. **Перелік публікацій:**
8. **Перелік ілюстративного матеріалу:**

   Презентація.

Дата видачі завдання “___”_____ 2021 р.

Науковий керівник _____ В.М. Ахрамович
(підпис)

Завдання прийнято до виконання _____ Л.С. Перепелиця
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерськоїроботи	Строк виконання етапів магістерської роботи	Примітка
1.	Аналіз науково-технічної літератури	07.10.2021р.	Вик.
2.	Системний підхід до аналізу технологій автентифікації ,авторизації та адміністрування дій у інформаційно-комунікаційній системі	15.10.2021р.	Вик.
3.	Дослідити варіанти реалізації методів автентифікації, що використовують паролі та PIN-коди, методів строгої автентифікації, а також методів біометричної автентифікації	30.10.2021р.	Вик.
4.	Розробити типові рекомендації щодо створення апаратно-програмних систем ідентифікації і автентифікації в ІКС	15.11.2021р.	Вик.
5.	Реферат, вступ, висновки.	27.11.2021р.	Вик.
6.	Підготовка презентації до захисту.	13.12.2021р.	Вик.

Студент СЗДМ - 61 Л.С. Перепелиця _____
Науковий керівник к.т.н., проф В.М. Ахрамович _____
Нормоконтроль: А.Б. Гребенніков _____

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Перепелиця Л.С. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Методи та засоби автентифікації користувачів в інформаційно-текомунікаційних системах та вироблення рекомендацій щодо підвищення їх ефективності»».
Магістерська робота і рецензія додаються.
Директор інституту _____ Савченко В.А
(підпис)

Довідка про успішність

Перепелиця Л.С. за період навчання в Навчально-Науковому інституті Телекомунікацій
(прізвище та ініціали студента)
з 2021 року до 2022 року повністю виконала навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.
Секретар інституту, факультету (відділення) _____ ___
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студентка Перепелиця Л.С.обрала тему роботи, методи та засоби автентифікації користувачівв інформаційно-текомунікаційних системах. Перелік використаних джерел свідчить про вміннямагістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Перепелиця Л.С. показала відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконана сумлінно, акуратно та вчасно запланом.

Все це дозволяє оцінити виконану магістерську роботу студента Перепелиці Ліни Сергіївни на оцінку **«відмінно»** та присвоїти йому кваліфікацію 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.
Керівник магістерської роботи_____ Ахрамович В.М.
(підпис)
“___”_____2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Перепелиця Л.С.допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії.
Завідувач кафедри _Системи інформаційного та кібернетичного захисту
(назва)
_____ Шуклін Г.В.
(підпис) (прізвище таініціали)
“_____”_____2021 рік.

РЕФЕРАТ

Магістерська робота присвячена дослідженню сучасних методів проведення аутентифікації користувачів в корпоративних інформаційно-телекомунікаційних системах та вироблення рекомендацій щодо підвищення їх ефективності за допомогою застосування сучасних методів і засобів ідентифікації/аутентифікації. Робота складається зі вступу, 3 розділів, які містять 29 рисунків та 4 таблиці, висновків й списку використаних джерел, що включає 44 найменування. Загальний обсяг роботи становить 80 сторінок, з яких 6 сторінок займають ілюстрації й таблиці на окремих аркушах, а також перелік умовних скорочень і список використаних джерел.

Об'єкт дослідження - процес ідентифікації та аутентифікації користувачів у інформаційно-телекомунікаційних системах.

Предмет дослідження – методи ідентифікації та аутентифікації користувачів в інформаційно-телекомунікаційних системах.

Метою роботи є дослідження методів і засобів та їх використання у проведенні ідентифікації/аутентифікації користувачів в інформаційно-телекомунікаційних системах підприємства (організації) для організації їх доступу та роботи в мережах.

В даній магістерській роботі були досліджені тенденції розвитку, а також напрямки впровадження сучасних технологій ідентифікації/аутентифікації; проаналізовано протокол Kerberos; проаналізовано систему PassWindow ; вироблені шляхи побудови системи ідентифікації та аутентифікації в інформаційно-телекомунікаційних системах з використанням таких стандартів як SAML, OpenID Contect, та протоколу Kerberos.

Результатом стало вирішене завдання дослідження сучасних методів проведення аутентифікації користувачів в корпоративних інформаційно-телекомунікаційних системах та вироблення рекомендацій щодо підвищення їх ефективності за допомогою застосування сучасних методів і засобів ідентифікації/аутентифікації при роботів локальних і глобальних мереж.

Галузь застосування.

Матеріали даної роботи можуть використовуватися при виборі, розробці, впровадженні та експлуатації системи інформаційної безпеки.

ІНФОРМАЦІЙНА БЕЗПЕКА, АУТЕНТИФІКАЦІЯ, АНАЛІЗ, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ПАРОЛЬ, ІДЕНТИФІКАЦІЯ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, СЕРТИФІКАЦІЯ, ЦИФРОВИЙ ПІДПИС.

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЕП	—електронний підпис
ІБ	—інформаційна безпека
ІС	—інформаційна система
ІКС	— інформаційно-текомунікаційна систем
КЗЗ	— комплекс засобів захисту
КС	— комп’ютерна система
КСЗІ	— комплексна система захисту інформації
НСД	— несанкціонований доступ
ПЗ	— програмне забезпечення
СЗІ	— система захисту інформації
СУБД	— система управління базами даних
IP	— Internet Protocol (міжмережний протокол)
KDC	— Key Distribution Center (центр розподілу ключів)
PAP	— Password Authentication Protocol (протокол парольної аутентифікації)
PIN	— Private Identification Number (персональний ідентифікаційний номер)
PKI	— Public Key Infrastructure (інфраструктура відкритих ключів)
SSL.	— Secure Sockets Layer (рівень захищених сокетів)
SSO	— Single Sign-On (система однократної аутентифікації)

TCP — Transport Control Protocol (протокол управління передаванням)

VPN — Virtual Private Network (віртуальні приватні мережі)

ВСТУП

Важливим завданням забезпечення цілісності конфіденційної інформації є захист від НДС до ресурсів інформаційно-телекомунікаційих систем, що веде за собою необхідність утворення надійних та зручних систем контролю доступу.

Ідентифікація – це процедура розпізнання користувача в системі за допомогою заздалегідь визначеного імені чи іншої інформації про нього. Така процедура є початковою в процесі надання доступу до системи та після неї здійснюється аутентифікація та авторизація.

Аутентифікація – це процедура перевірки належності ідентифікатора об'єкту, встановлення чи підтвердження дійсності, а також перевірка чи є об'єкт або суб'єкт, що перевіряється, насправді тим, за кого він себе видає .

Кожний користувач сучасних інформаційно-телекомунікаційних систем по кілька разів на день проходить процедури ідентифікації та аутентифікації. Цей процес виконується кожного разу, коли користувач вводить пароль для доступудо інформаційно-телекомунікаційної системи, мережі чи бази даних або при запуску прикладної програми. Після виконання процесу оператор чи отримує доступ до ресурсів інформаційно- телекомунікаційної системи, чи ні. Тож процедура аутентифікації користувача є обов’язковою для функціонування інформаційно-телекомунікаційної системи та **отримує актуальність**.

Мета і завдання дослідження. Мета даної дипломної роботи-є дослідження методів, особливостей побудови та використання сучасних методів і засобів проведення ідентифікації/аутентифікації користувачів в інформаційно-телекомунікаційних системах підприємства (організації) для організації їх доступу та роботи в локальних і глобальних мережах.

Для досягнення поставленої мети потрібно вирішити наступні завдання:

- дослідити тенденції розвитку та напрямки впровадження сучасних технологій ідентифікації/аутентифікації;
- дослідити протокол Kerberos
- розробити шляхи побудови системи ідентифікації та аутентифікації в

інформаційно-телекомунікаційних системах.

Виходячи з вищеперечисленного , у роботі ***об'єкт дослідження***- процес ідентифікації та аутентифікації користувача у системі інформаційно-телекомунікаційній системі . ***Предметом*** дослідження - методи та моделі ідентифікації та аутентифікації користувачів в захищених ІКС. *Методи дослідження.* Для вирішення наукового завдання в роботі використані методи математичного аналізу, прогнозування та прийняття рішень.

1 АНАЛІЗ СУЧАСНИХ МЕТОДІВ І ЗАСОБІВ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ

У зв'язку з загальним розповсюдженням комп'ютерних технологій все більш актуальною є проблема захисту інформації в інформаційно-комунікаційних системах (ІКС). Тож питання захисту інформації в комп'ютерних системах вирішується для ізоляції нормально функціонуючої інформаційної системи від НДС сторонніх осіб чи програмного забезпечення до комп'ютерних даних, що захищаються. Створення єдиної та централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури. Управління доступом – ефективний метод захисту інформації, котрий регулює використовування ресурсів інформаційної системи, для якої розроблялася концепція ІБ. Методи і системи захисту інформації, що спираються науправління доступом, включають в себе такі функції захисту інформації в ІКС:

- ідентифікація користувачів, ресурсів системи ІБ;
- розпізнання та встановлення достовірності користувача по обліковими даним, що вводяться ;
- допуск до певних умов роботи згідно регламенту, наказаному кожному окремому користувачу, що визначається засобами захисту інформації і є основою інформаційної безпеки більшості типових моделей ІКС;
- протоколювання звертань користувачів до ресурсів, ІБ котрих захищає ресурси від НСД та відстежує некоректну поведінку користувачів системи.

Можна зробити висновок, що система ідентифікації\аутентифікації є одним з важливих елементів інфраструктури захисту від НСД до будь-якої інформаційно-телекомунікаційної системи. Під НСД до інформації маємо на увазі доступ до інформації, котрий порушує заздалегіть встановлені правила розмежування доступу та здійснюваний з використанням штатних засобів обчислювальної техніки або автоматизованих систем.

Потрібно зазначити, що НСД може носити випадковий або навмисний характер.

Таким чином основною задачею систем ідентифікації і аутентифікації є визначення та верифікація необхідного набору повноважень суб'єкта при доступі до інформаційної системи. В свою чергу ідентифікація дозволяєсуб'єкту (користувачу чи процесу, який діє від імені користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я).

Для здійснення довіреної передачі даних чинне законодавство в більшій мірі охоплює лише електронні підписи. На даний момент в Україні немає основ для безпечних, надійних та простих електронних операцій, які включають в себе електронну ідентифікацію, аутентифікацію та підписи. Чинне законодавство потребує значного покращення, розширення, а також прийняття на рівні Європейського союзу (ЄС).

Електронний підпис – це деякі дані в електронній формі, котрі приєднуються чи логічно пов'язуються з іншими електронними даними, і використовуються користувачем в якості підпису.

1.1. Система безпеки доступу до ресурсів. Поняття аутентифікації

«Ідентифікація», «аутентифікація» і «авторизація» - це три взаємопов'я- зані між собою поняття, котрі складають основу системи безпеки. Ідентифікація - це передача ідентичності ІС. Перед автентифікацією заявник зазвичай все одно надає ІС посвідчення (наприклад, логін або адресу електронної пошти), а монітор стверджує посвідчення шляхом автентифікації(наприклад, за допомогою пароля).

Аутентифікація - це процес під час якого проходить підтвердження особи користувача. Користувачі ідентифікуються з використанням різних механізмів аутентифікації. В системі безпеки процес аутентифікації перевіряє інформацію, надану користувачем, за допомогою бази даних [1], [2].

Нарешті, авторизація це надання користувачеві привілегій. Схему доступу до ресурсів показано на Рис. 1.1

Рис. 1.1. Схема доступу до ресурсів

Системи аутентифікації дають відповіді на такі питання як наприклад: «хто є користувачем?» та «чи дійсно користувач являється саме тим, ким він / вона собою являє?». Отже, аутентифікація це один з найбільш важливих способів підвищення довіри, а також безпеки комерційних додатків.

Зв'язок між позивачем та спостерігачем позначений як канал. Канал - це опора спілкування між позивачем та спостерігачем. Такий канал можна розглядати як конфіденційний та достовірний, а також безпечний або небезпечний. Конфіденційний канал є стійким до перехоплення; автентичний канал являється стійким до взлому; безпечний канал є стійким до обох; а незахищений канал не стійкий взагалі.

Загальні базові кроки для проведення аутентифікації:

1. Початковий крок: позивач не аутентифікований;

2. Етап підключення: заявник вимагає від ІС використання функції, що вимагає аутентифікація. В свою чергу ІС просить спостерігача перевірити чи справжній заявник.

3. Крок аутентифікації: заявник вже аутентифікований та відкриває сеанс. Після цього ІС надає користувачеві необхідні функції.

4. Крок відключення: користувач відключається від спостерігача, після

чого стан повертається до початкового кроку. Такий крок може бути ініційований після проходження певного періоду, або дією користувача.

Для ІС можуть використовуватися різні рівні аутентифікації, як наприклад, рівень для адміністраторів системи та рівень для користувачів. У такій системі рівень аутентифікації градуюється за шкалою: рівень 0 призначений для нерозпізнаних користувачів, котрі мають найнижчі права в системі; рівень N призначений для адміністратора, який володіє повними правами; один чи декілька рівнів від 0 до N. Така схема полягає в тому, що для переключення на вищий рівень довіри з боку ІС може бути таке, що знадобитися аутентифікація [3].

Сам процес може полягати на поєднанні одного чи кількох факторів аутентифікації. Визнані фактори для аутентифікації людини:

1. Те, що знає користувач: пароль, PIN-код чи кодова фраза,;
2. Те, що належить користувачеві: телефон, USB-токен, програмний токен, смарт-карта,cookie-файл;
3. Те, що кваліфікує користувача: відбиток пальця, фрагмент ДНК, геометрія обличчя;
4. Те, що може зробити користувач: підпис чи жест;
5. Де знаходиться користувач: геолокація користувача на конкретній момент часу.

Протокол аутентифікації - це так званий тип протоколу комп'ютерного зв'язку чи криптографічного протоколу, котрий був спеціально розроблений для передачі даних аутентифікації між двома об'єктами. [4]

Завдання даного протоколу -вказати точну серію кроків, котрі необхідні для виконання процесу аутентифікації. Він має відповідати основним принципам протоколу:

1. Протокол має включати дві чи більше сторін, кожен, хто приймає участь в протоколі, повинен знати протокол заздалегідь;
2. Всі залучені сторони повинні дотримуватися протоколу;
3. Протокол повинен бути однозначним - кожен крок повинен бути точно визначений;

4. Протокол має бути повним, тобто включати вказану дію для кожної можливої ситуації;

Є безліч різних систем, до яких користувачеві необхідний доступ, і тому протоколи аутентифікації, зазвичай, є відкритими стандартами Тож розглянемо основні протоколи.

Протокол аутентифікації пароля (далі – ПАП). ПАП – є одиним з найстаріших протоколів аутентифікації. Цей протокол ініціалізується тим, що клієнт надсилає пакет із обліковими даними (ім'я користувача та пароль) на початку з'єднання, слід зауважити, що клієнт повторює запит автентифікації аж до тих пір, допоки не буде отримано підтвердження. [5] Такий метод є дуже небезпечнім, тому що облікові дані пересилаються «у відкритому вигляді» , що робить його вкрай вразливим навіть до найпростіших видів атак.

Протокол аутентифікації запит-рукостискання. Процес автентифікації завжди ініціалізується сервером / хостом та може виконуватися в будь-який час протягом сеансу, навіть неоднократно. Сервер надсилає випадковий рядок (як правило довжиною 128 Б). Клієнт використовує пароль і рядок, отримані в якості параметрів для хеш-функції MD5, після цього відправляє результат разом з ім'ям користувача як звичайний текстт. Сервер використовує ім'я користувача для застосування тієї ж функції і порівнює обчислений і отриманий хеш. Аутентифікація пройшла успішно або ні.

Розширений протокол аутентифікації (далі – РПА). РПА аутентифікація ініціюється сервером. Обмін відбувається наступним чином: автентифікатор відправляє запит на авутентифікацію однорангового вузла; після чого цей вузол відправляє пакет назад у відповідь на дійсний запит; потім аутентифікатор надсилає додатковий пакет запиту, і вузол знову відповідає на запит; таким чином діалог триває до тих пір, аж до поки аутентифікатор не зможе аутентифікувати однорангового вузла (неприйнятні відповіді на один чи декілька запитів), і в цьому випадку реалізація автентифікатора повинна передати повідомлення про помилку РПА; так може бути діалог аутентифікації до тих пір, допоки автентифікатор не зрозуміє, що аутентифікація відбувася успішно, і такому

випадку автентифікатор повинен передати успіх РПА [6].

TACACS, XTACACS і TACACS +. Використовує увтентифікацію на базі IP без шифрування (імена користувачів та паролі передаються як простий текст). У більш свіжої версії XTACACS (Extended TACACS) додані авторизація а також облік. Потім ці два протоколи замінили на TACACS +. TACACS + розділяє компоненти, таким чином це дає відокремити і обробляти їх на окремих серверах TACACS + є власністю Cisco.

Служба віддаленої аутентифікації користувачів з телефонним підключенням (RADIUS). Цей протокол найчастіше використорують інтернет-провайдери. Облікові дані зазвичай засновані на комбінації імені користувача та пароля, для транспорту використовується протокол NAS і UDP. [7]

DIAMETR. Походить від RADIUS, але має безліч покращень, таких як використання більш надійного транспортного протоколу TCP або SCTP та вищий рівень безпеки завдяки TLS. [8]

Kerberos. Централізована мережева система аутентифікації. Це метод перевірки автентичності за замовчуванням в Windows 2000. Сам процес аутентифікації є набагато складнішим аніж в попередніх протоколах. Так Kerberos використовує криптографію з симетричним ключем, а також вимагає довіреної третьої сторони і може використовувати криптографію з відкритим ключем на певних етапах аутентифікації, якщо це потрібно. [9]

1.2. Класифікації аутентифікації

1.2.1. **З точки зору виду методу**

Метою аутентифікації є підтвердження особистості, проте набір методів аутентифікації дуже широкий та може варіюватися по-різному. Розглянемо список декількох поширених методів аутентифікації:

1. Аутентифікація за допомогою паролю;
2. Аутентифікація за допомогою смарт-карти;
3. Біометрична аутентифікація;
4. Аутентифікація за допомогою цифрового сертифікату.

Кожен з наведених методів аутентифікації має своє застосування проте і свої недоліки. Наприклад, такени чи смарт-крти можуть бути викрадені, системи розпізнавання можуть бути взламані. Таким чином можна визначити, що метою аутентифікації являється перевірка ідентичності об'єкта із заданим рівнем довіри. За умови, якщо метод перевірки аутентичності не вважається цілком надійним, надана перевірка також не може вважатися надійною.

1.2.2. **З точки зору кількості методів**

Всього можна виділити є чотири типи аутентифікації з точки зору кількості методів:

1. Однофакторна аутентифікація;
2. Двофакторна аутентифікація;
3. Трьохфакторна аутентифікація;
4. Чотирьохфаторна аутентифікація.

Однофакторна аутентифікація використовує лише один з вищезазначенних методів аутентифікації. В свою чергу багатофакторна аутентифікація - це багаторівнева система безпеки, шо перевіряє особистість. Двофакторна, трьохфакторна та чотирьохфакторна аутентифікації є підмножинами

багатофакторної аутентифікації.

Двофакторна аутентифікація представляю собою двоетапний процес аутентифікації. Такий метод може поєднувати декілька методів в собі, наприклад, ім'я користувача і пароль, а також PIN-код з фізичним або мобільним токеном для додаткової безпеки. Таке поєднання факторів аутентифікації ускладнює доступ потенційного зловмисника і робить атаку більш складною та ресурсозатратною.

Трьохфакторна аутентифікація поєднує в собі такі фактори як «Я знаю», «Я маю», «Я є». Принцип такий як і у двофакторній аутентифікації, «Я знаю» та «Я маю», як правило, включає імена користувачів, паролі та одноразовий токен і додатковий фактор «Я є», котрий використовує біометричні дані, наприклад, як відбитки пальців, для перевірки особи користувача.

Чотирьохфакторна аутентифікація - форма багаторівневої безпеки, яка включає в себе знання, володіння, приналежність, а також місце розташування користувача.

Традиційні імена користувачів і паролі є дуже вразливими для кіберзлодіїв. Проте багатофакторну аутентифікацію останнім часом вважають однією з найбільш ефективних способів підвищення безпеки. Тому що багаторівневість гарантує, що користувачі при запиті доступу є тими, ким вони себе ідентифікують. В такому разі навіть при крадіжці кіберзлочинцями облікового запису, вони будуть змушені перевіряти особистість іншим способом.

1.2.3. **З точки зору рівня безпеки**

Найбільш часті типи аутентифікації відрізняють за рівнем безпеки, який забезпечується об'єднанням чинників з однієї чи декількох нищенаведених категорій факторів аутентифікації:

1. «Сильна» аутентифікація;
2. Неперервна аутентифікація;
3. Електронна аутентифікація.

«Сильна» аутентифікація - аутентифікація, при якій користувач зрівнюється з реальною особою, організацією чи довірителем. Найчастіше «сильну»

автентифікацію ототожнюють з двофакторною, проте це є невірним судженням. Тому що «сильна» аутентифікація не кожного разу може бути багатофакторною. Наприклад, під час дзвінку в банк з метою ідентифікації особи зазвичай запитують номер карти, номер паспорта, і тд. Проте все це є тільки одним фактором - «я знаю» , що означає, що це не багатофакторна аутентифікація , але вона є «сильною». На практиці в таких випадках рекомендують застосовувати багатофакторну автентифікацію.

Безперервна аутентифікація - метод перевірки, котрий спрямований на забезпечення підтвердження користувача та здійснення захисту кібербезпеки Постійно вимірюючи ймовірність того, що деякі користувачі являються тими, за кого вони себе видають, так безперервна аутентифікація перевіряє користувача не тільки один раз, а безперервно напротязі всього сеансу. Безперервна аутентифікація націлена на забезпечення інтелектуальної та безпечної перевірки особистості при цьому без переривання робочого процесу і реалізується вона з використанням машинного навчання та великої кількості чинників, включаючи поведінкові моделі та біометрію.

Традиційні форми перевірки, такі як однофакторна аутентифікація,і двофакторна аутентифікація не пропонують безперервної перевірки ідентифікації особистості. Потреба в нових стратегіях управління ідентифікацією та доступом, таких як безперервна аутентифікація, збільшується в результаті стрімкого розвитку цифрових технологій і кіберзлочинності.

Рішення управління ідентифікацією та доступом з функцією безперервної аутентифікації постійно збирає інформацію про дії користувача та шаблонах поведінки та навчається розуміти нормальну і незвичну поведінку користувача за допомогою зібраних даних. На основі такого аналізу поведінки користувача доступ до системи може бути наданий або буде запрошена додаткова перевірка особи користувача.

Варіанти та невідповідності в поведінці та діях користувача в системі можуть бути виміряні або перевірені безперервно під час сеансу. Крім того, якщо користувач поводить себе невідповідно шаблону, тобто його звичній поведінці або

знаходиться під загрозою, то в такому випадку доступ може бути відкликаний, а сеанс завершиться в той же момент. Деякі методи виявлення змін включають в себе натискання клавіш, дотик (сила натискання пальця) або риси обличчя, такі як положення очей, розмір ока та частота моргання.

Електронна аутентифікація - процес встановлення впевненості в іде- нтифікаційних даних користувача, які були представлені в електронній формі в ІС. Цифрова чи електронна аутентифікації можуть використовуватися як синоніми, коли мається на увазі про процес аутентифікації, що підтверджує особу людини. Під час використання разом з електронним підписом може бути доказом того, чи були модифіковані отримані дані після їхнього підписання початковим відправником. Електронна аутентифікація може знизити ризик крадіжки особистих даних за рахунок підтвердження того, що людина являється тим, за кого вона себе видає, під час виконання транзакцій в Інтернеті.

Є різні методи провдення цифрової аутентифікації, котрі можуть використовуватися для аутентифікації, від пароля до ищих рівнів безпеки, які можуть використовувати багатофакторну автентифікацію. В залежності від рівня безпеки, що використовується, користувачеві може бути потрібно підтвердити свою особистість, наприклад, за допомогою токенів безпеки, контрольних питань, на які заздалегідь була отримана відповідь, або наявності сертифіката стороннього центру сертифікації, що підтверджує його особу.

Існує чотири види схем цифрової аутентифікації: локальна аутентифікація, централізована аутентифікація, глобальна централізована аутентифікація, глобальна аутентифікація і веб-додаток.

Під час використання локальної схеми програма зберігає дані, що стосуються облікового запису користувача. І в свою чергу така інформація зазвичай не передається до інших програмам. Відповідальність за підтримку та запам'ятовування типів. А також кількості облікових даних, що пов’язані зі службою, до котрої він має отримати доступ, лежить виключно на користувачеві. Проте дана схема має високий ризик того, що область зберігання паролів буде скомпрометована.

Використання централізованої схеми дозволяє кожному користувачеві

задіяти одні і ті ж облікові дані для доступу до різних служб. Кожна програма індивідуальна, але повинна мати можливість взаємодії з центральною системою для успішної аутентифікації. Це дозволяє користувачеві отримати доступ до необхідної інформації і закритих ключів, що дозволяють підписувати документи електронним способом.

Використання глобальної централізованої схеми дозволяє користувачеві отримати прямий доступ до служб аутентифікації.

Найбільш безпечна схема - це глобальна централізована аутентифікація і веб-додаток (портал). Вони використовують єдині механізми аутентифікації, що включає мінімум два фактори.

1.3. Проблеми безпеки аутентифікації

Атаки на процес аутентифікації поділяються на три основних групи:

1. Атаки на користувацький інтерфейс;
2. Атаки на базу даних шаблона;
3. Атаки на системні модулі та взаємозв’язки між модулями.

Щодо атак на користувацький інтерфейс,то аутентифікація відіграє дуже важливу роль в безпеці веб-додатків. Під час того, коли користувач вводить своє ім'я для входу та надає пароль для аутентифікації і проходить підтвердження вірності введених даних, додаток призначає системі певні права користувача на основі ідентифікатора, що встановлений наданими обліковими даними.

HTTP може мати декілька різних видів протоколів аутентифікації:

1. Базовий - ім'я користувача / пароль у відкритому вигляді;
2. Дайджест - базовий, але на відміну від першого, паролі зашифровані;
3. На основі форми - налаштовується форма, що використовується для введення облікових даних користувача і обробляється з використанням налаштованої логіки в бекенді.
4. NTLM – це власний протокол аутентифікації компанії Microsoft, котрий реалізований в заголовках HTTP-запиту / відповіді.

5. Negotiate -це новий протокол від Microsoft, котрий дає змогу клієнту і серверу погоджувати будь-який тип аутентифікації, вказаний вище. Також додає Kerberos для клієнтів, які використовують Microsoft IE v5 +.

6. Сертифікати на стороні клієнта. Хоч SSL / TLS використовується не так і часто, проте він має можливість перевірки автентичності цифрового сертифікату, який надаєтьс веб-клієнтом, що, робить його токеном автентифікації.

7. Microsoft Passport - служба єдиного входу (SSI), що керуються компанією Microsoft, яка надає змогу веб-сайтам (так званим «Passport Partners») автентифікувати користувачів через їх членство в службі Passport. Даний механізм використовує той ключ, що і Microsoft та партнерським сайт, для створення файлу cookie, котрий ідентифікує користувача.

Всі вищенаведені протоколи аутентифікації працюють через HTTP (або SSL / TSL) з обліковими даними, що вбудовані прямо в трафік запиту / відповіді.

Цей вид атаки не є технологічною дірою в безпеці ОС або серверного ПЗ. Це шидше залежить від того, як надійно зберігаються паролі та наскільки легко злодію дістатися до сервера.

Якщо зловмисник отримує доступ в систему, підтверджуючи , що він є відомим і чинним користувачем, то отримує доступ туди і на тому рівні, що було призначено цьому користувачу.

В таблиці 1.1 наведено поширені атаки, спрямовані на процес аутентифікації.

Таблиця 1.1

Типи атак на процес аутентифікації

Атака	Опис
Метод грубої сили	Метод взлому пароля за допомогою обробки всіх можливостей, щоб знайти пароль. При атаці цим методом зловмисник: Захоплює форму хешування паролів; Атакує файл хеша в автономному режимі за допомогою зломщика грубої сили.

Словник	Спроба підібрати пароль, перебираючи список слів зі словника. Часто символи і букви верхнього і нижнього регістра замінюються всередині словникової роботи. Атака по словнику працює, тому що користувачі часто використовують ненадійні паролі, котрі легко підібрати.
Аналіз паролів (сніффінг)	Спроба перехоплення паролів, котрі передаються по комп'ютерній мережі. Зазвичай для перехоплння пакетів в мережі використовуються спеціальні програми. Потім зловмисник аналізує отримані пакети, для того щоб визначити, які з них містятьпаролі, а які ні. Шифрування даних, шо передаються, забезпечує кращий захист від цього виду атак.
Спуфінг	Атака використовується для того, щоб приховати справжнє джерело пакетів чи перенаправити трафік в інше місце. Найбільш поширеною формою підміни типового IP-пакета є зміна адреси джерела. Так для вихідного пристрою підміняється справжня адреса, наприклад, сайта чи сервера. Спуфінгові атаки: Використовують в пакетах змінені адреси джерела чи / або призначення; Може включати спуфінг сайту, котрий обманом змушує користувачів розкрити свої облікові дані чи конфіденційну інформацію.

Атака посередника	Використовуються для перехоплення інформації, що передається між двома партнерами по зв'язку. Атаки типу посередника: Зловмисник знаходиться між клієнтом та сервером .Клієнта обманом змушують пройти аутентифікацію і таким чином отримують дані. Обидві сторони на кінцевих точках думають, що вони обмінюються даними один з одним, в той час як зловмисник перехоплює і / або підміняє дані.Потім зловмисник аутентифікується на сервері, використовуючи перехоплені облікові дані. Часто така атака використовується для перехоплення даних кредитних карт, облікових даних онлайн-банку і конфіденційної інформації.
Повторне відтворення	Зловмисник перехоплює трафік і використовує його в інший час, для спроби відтворення аутентифікації.
Злом	Атака під час якої зловмисник краде відкритий і активний сеанс зв'язку у легітимного користувача Зловмисник захоплює сеанс та відключає вихідний пристрій; Стан сеансу TCP / IP регулюється так, щоб зловмисник міг вставляти альтернативні пакети в потік зв'язку. [17]

Заходи протидії атакам на автентифікацію:

1. Використання надійної парольної політики;
2. Збереження історії паролів, для запобігання їх повторноо використання;
3. Використання багатофакторної аутентифікації;
4. Використання строгої системи порядкової нумерації;
5. Аудит кількості невдалих спроб входу в систему;
6. Контролювання мережі та систем на предмет наявності інструментів чи ПЗ для перехоплення і крадіжки паролів;
7. Впровадження блокування облікового запису при введенні великої кількості неправильних паролів за відносно короткий проміжок часу.

Пропозиції щодо посилення паролів:

1. Паролі обов’язково мають містити кілька типів символів: прописні, рядкові, цифри та спеціальні символи;
2. Мінімальна довжина пароля не менше восьми символів для звичайних користувачів і не менше дванадцяти для адміністраторів;
3. Не використовувати частину імені користувача чи електронної пошти;
4. Регулярна зміна паролів кожні 45 днів.

Що стосується атак на бази даних шаблонів, біометричні дані, що зберігаються в базі даних шаблонів, можуть бути змінені або вилучені. Таким чином для захисту біометричного шаблону є різні методи, такі як скасована біометрія та дрібна біометрія . Захист за допомогою скасованої біометрії включає навмисне повторюване спотворення прийнятого біометричного сигналу на основі певного перетворення. Метод дробової біометрії маскує частину біометричних даних перед відправкою.

Атаки на системні модулі пов'язані зі зміною внутрішніх компонентів можуть

здійснюватися в модулях попередньої обробки, вилучення ознак, зіставлення і прийняття рішень. Так шкідливе ПЗ може видавати себе одним з модулів і відправляє вихідні дані, що належать противнику, в наступні модулі, такі як атака троянського коня .

1.4. Висновки до розділу

Ідентифікація, аутентифікація і авторизація - це три взаємопов'язані поняття, які складають основу системи безпеки. Аутентифікація - це процес під час якого відбувається підтвердження особи користувача. Системи аутентифікації дають відповіді на такі питання як: «хто є користувачем?» і «чи дійсно користувач є тим, за кого він себе представляє?».

Класифікація аутентифікації відбувається з точки зору методу (пароль, смарт-карта, сертифікат, біометрія), а також з точки зору кількості використаних методів (однофакторна, двуфакторна, трьохфакторна, чотирьохфакторна) та з точки зору рівня безпеки («сильна», безперервна, електронна).

Атаки на процес аутентифікації поділяються на три основних типи: атаки на користувацький інтерфейс, атаки на базу даних шаблона, атаки на системні модулі та взаємозв’язки між модулями. Найпоширеніші атаки: метод грубої сили, по словнику, сніффінг, спуфінг..

Ні один з методів сам по собі не є цілком безпечним, тому зараз найбільш актуальним є метод багатофакторної аутентифікації.

2 АНАЛІЗ МЕТОДІВ ТА ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ

2.1. Криптографічні протоколи автентифікації

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

Дуже важливими факторами криптографічного протоколу є можливість перевірки автентичності об’єктів\суб’єктів, котрі взаємодіють між собою.

Аутентіфікація об’єкта\суб’єкта – це підтвердження із заданою ймовірністю того, що об’єкт\суб’єкт насправді той, 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;
- управління ключами;
- складність обчислень;
- захищеність від раніше переданих повідомлень;
- вимоги до третьої сторони;
- новизна ключів;
- крипто живучість ключів;
- складність криптоаналізу;
- неспростовність;

- число повторень (раундів, обмінів).

Під час використання криптопротоколів, безпосередньо, необхідно забезпечити якість. Для цього потрібно чітко зрозуміти наскільки вид протокола відповідає вимогам. Аутентифікація ключів буває явною та неявною.

Управління ключами – це спроможність абонентів використовуватиключі 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, щостосуються 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	$Y_i = g_1^X (mod) P$	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})	$D_i = sQ_{iD}$	$Q_{iD} = \mid H_i (ID)$	G_1, G_2, e, H_1, P, H_2, H_3,F^{2m}, P_p	Міжекспоненційна та субекспоненційна

2.2. Система PassWindow як некриптографічна технологія аутентифікації

Некриптографічні алгоритми аутентифікації передбачають використання для підтвердження достовірності користувача не тільки логіна та паролю, а й додаткових засобів (мобільних телефонів, смарт-карт, токенів).

Алгоритм некриптографічної автентифікації наведено на (рис.2.1).

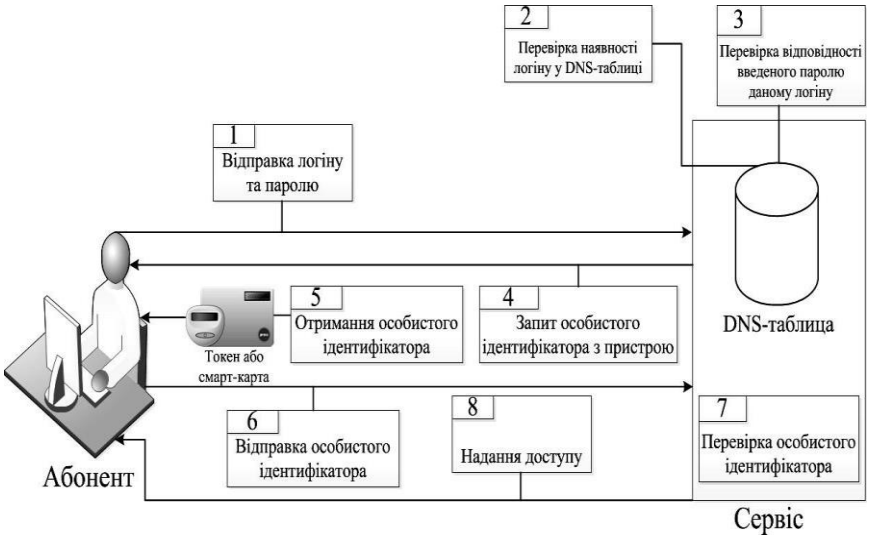


Рис. 2.1. Схема алгоритму некриптографічної автентифікації

Значне місце через систем аутентифікації займає PassWindow, яку застосовують великі банки багатьох країн. Дана система належить до класу двофакторних і некриптографічних систем аутентифікації. Вона основана на тому, що користувач крім того, що знає пароль доступу до певного імені користувача (“логіна”), має інструмент для додаткового отримання ключа доступу. Таким інструментом може бути електронний сертифікат на пристрої користувача або код безпеки, який надсилається на особистий телефон чи в спеціальний застосунок або ж біометричні дані користувача.

Алгоритм PassWindow - алгоритм двофакторної аутентифікації, котрий базується на формуванні унікального ключа. Частина цього ключа друкується на прозорій частині стандартного посвідчення особи у вигляді штрих-коду, який

складається із рисок. Для того щобскласти унікальний ключ доступу, необхідно притиснути картку до екрану монітора, термінала, мобільного телефона чи планшета у виділену область, в якій формується друга частина коду, що також має вигляд штрих-коду з рисками, які змінюються.

Шаблони штрих-коду PassWindow можуть бути під виглядом унікальних статичних зображень послідовності символів або як більш розширена анімаційна версія всього шаблону. Послідовності шаблонів штрих-коду генерує сервер автентифікації і кожен з них є унікальним , таким чином може використовуватися тільки з ключем, до якого вони підходять.

Будь-який буквено-цифровий код можна надійно передати за допомогою PassWindow, але наразі реалізація методу спрямована на передавання коротких рядків випадкових цифр, щоб використаня їх як одноразового паролю у поєднанні з цифрами, що ідентифікують унікальність транзакції перевірки справжності користувача.

Коли користувач підтверджує, що унікальна інформація в межах транзакції , (закодована в штрих-кодах) відповідає бажаній, от він може завершити транзакцію, ввівши відповідний одноразовий пароль.

Основні етапи системи PassWindow подано на (рис.2.3).

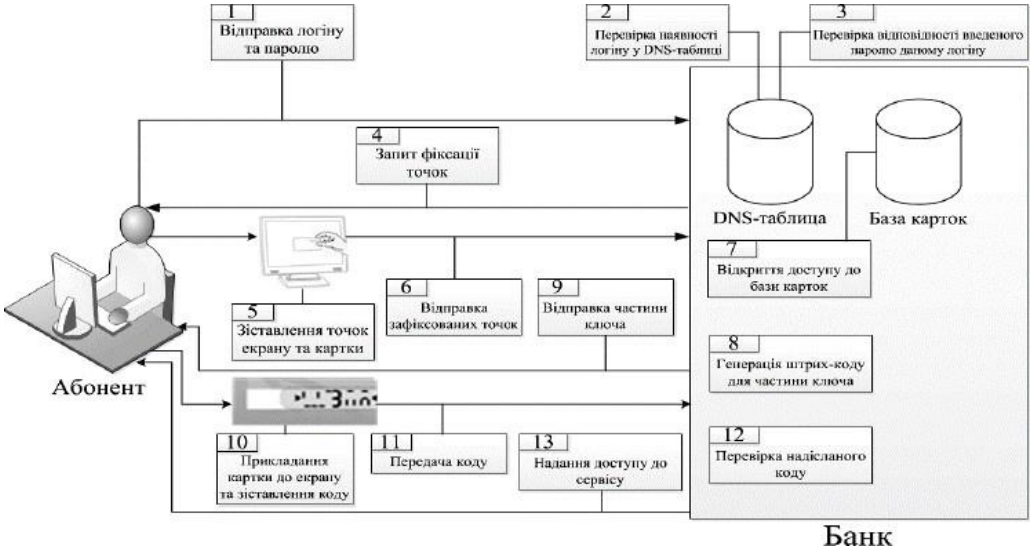


Рис. 2.3. Схема алгоритму подвійної автентифікації PassWindow

Принцип роботи методу автентифікації має такий алгоритм:

1. Абонент проходить ідентифікацію.

2. Проходить перевірка наявності логіну у DNS-таблиці.
3. Перевірка введеного паролю
4. Запит фіксації точок картки.
5. Після прикладання картки користувачем до екрану відбувається фіксація відповідності точок штрих-кодукартки.
6. Зафіксовані точки відправляються до сервісу, де надалі зберігаються.
7. Відкриття доступу до бази карток.
8. Генерація штрих-коду для другої частини ключа
9. Надсилання частини ключа штрих-коду абоненту.
10. Абонент, прикладаючи персональну картку до екрана свого пристрою,формує код (код йде після літери Р).
11. Зіставлений код надсилається до сервісу.
12. Надісланий код перевіряється направильність.
13. В разі успішної аутентифіції надається доступ до сервісу.

2.3. Автентифікація за допомогою смарт-картки та USB-ключів

Смарт-картка– це звичайна пластикова картка з вбудованою в неї мікросхемою. Ступінь складності мікросхеми є дуже різним – від найпростішого контролера читання/запису данихв електронну пам'ять картки, до мікропроцесора, що має розвинуту систему команд та вбудовану файлову систему. Смарт-картка має змогу виконувати складні операції по обробці інформації та зберігати її.

Є декілька класифікацій смарт-карток ,наприклад, за типом мікросхеми, яка в ній вбудована та за функціями, що вона виконує.

Залежно від типу мікросхеми в смарт-картці виділяють:

- смарт-картки з енергозалежною перепрограмованою пам'яттю. Вони надають доступ до перезаписування інформації, що зберігається на них. Основним їх застосуванням є зберігання індивідуальних даних;
- смарт-картки із захищеною перепрограмованою пам'яттю. Вони дають доступ для читання/запису лише після вводу спеціального коду. Основне застосування – розрахункові картки або зберігання захищених даних;
- багатофункціональні смарт-картки мають великий об'єм енергозалежної перепрограмованої пам'яті та спеціальний мікропроцесор і вбудовану (ОС), що забезпечує набір сервісних функцій. Такі смарт-картки можуть застосовуватися для будь-яких застосунків, включаючи розрахунки користувача.

За призначенням вирізняють такі смарт-картки: лічильники, пам’яті, мікропроцесорні.

Картки-лічильники використовуються коли потрібне віднімання фіксованої суми за кожну платіжну операцію

Зазвичай картки- лічильники застосовуються при оплаті за проїзд, автостоянку і т.п.

Картки пам'яті використовуються для збереження інформації. Є два типи таких карток: із захищеною і незахищеною пам'яттю.

У смарт-картках із незахищеною пам'яттю немає обмежень щодо читання\запису даних.

У смарт-картках із захищеною пам'яттю є спеціальний механізм для дозволу читання/запису або вилучення інформації. Щоб провести будь-яку операцію потрібно ввести спеціальний секретний код, а іноді навіть не один. Зазвичай, смарт-картки із захищеною пам'яттю мають область, в котру записуються ідентифікаційні дані. Записані дані не можуть бути змінені, що необхідно для забезпечення неможливості фальсифікації картки. Такі картки можуть використовуватися, як платіжний засіб та для зберігання конфіденційних даних.

Мікропроцесорні картки схожі на картки пам'яті, але містять чіп-модуль, котрий робить такі картки дійсно розумними. Мікропроцесор – це мікросхема чи чіп, котрі можуть зберігати великий обсяг інформації і виконувати арифметичні чи\або логічні операції. Такі картки, по-суті, є мікрокомп’ютерами зі своїм процесором, оперативною та постійною пам'яттю і навіть ОС. Як правило, у такі картки вбудовані криптографічні засоби, що забезпечують також і шифрування інформації.

У картку вбудовується спеціалізована ОС, що надає великий набір сервісних операцій і засобів безпеки. ОС картки підтримує файлову систему, яка передбачає розмежування доступу до інформації, що зберігається на картці

Смарт-картки можуть використовуються для ідентифікації, аутентифікації чи авторизації користувача, зберігання на ній ключової інформації , а також здійснення криптографічних операцій.

Електронний ключ (ЕК) – апаратний засіб, котрий призначається для захисту ПЗ та даних від несанкціонованого копіювання і розповсюдження та нелегального використання. ЕК має вигляд малогабаритного знімного USB-пристрою на двошаровій друкованій платі, котра вбудована в пластиковий корпус. На платі встановлюють електронні компоненти ЕК та USB-з’єднувач.

ЕК має виконувати наступні функції:

- управління особистими ключами ЕЦП та протоколу розподілу ключовими даними, що включає:
- прийняття і зберігання загальних параметрів для алгоритму ЕЦП та протоколу

розподілу ключів;

- генерацію і зберігання особистих ключа ЕЦП та протоколу розподілу в зашифрованому вигляді з контролем цілісності;
- знищення особистих ключів ЕЦП та протоколу розподілу ключів;
- формування ЕЦП для даних, котрі завантажуються з ЕОМ за допомогою використання особистого ключа ЕЦП;
- генерацію сеансових ключів;
- формування спільного секретного ключа
- кодування та розшифрування сеансових ключів за допомогою спільного секретного ключа;
- приймання та зберігання двох довгострокових ключових елементів (ДКЕ), котрі використовуються у алгоритмі генерації випадкових бітових послідовностей;
- аутентифікацію користувача до початку роботи;
- управління параметрами аутентифікації користувача
- приймання, зберігання та надання доступу, а також знищення довільних даних користувача у ЕК.

ЕК має містити наступні функціональні вузли:

- процесор із вбудованими: оперативним запам'ятовуючим пристроєм (ОЗП), постійним запам'ятовуючим пристроєм (ПЗП), генератором тактових частот, 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;

- аутентифікації користувача до початку роботи з ЕК.

Захист та контроль цілісності особистих ключів у ПЗП має здійснюватися на основі захисту пароля. Особисті ключі підлягають контролю на цілісність шляхом вироблення вставки та захищатися за допомогою кодування у режимі простої заміни.

Аутентифікація користувача до початку роботи повинна здійснюватися шляхом передачі у ЕК пароля доступу до ЕК, з хешуваням паролю та порівнянням з еталоном, що зберігається у ПЗП. На основі виданого результату порівняння ЕК має приймати рішення про успішність аутентифікації.

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, цьому дуже сприяло поширення мікропроцесорних технологій. Сьогодні використання в СКУД біометричних сканерів практично не ускладнює систему безпеки, а вартість для деяких біометричних методів не є затратною. Наразі десь близько третини ноутбуків мають вбудованусистему зчитування відбитку пальців, а відеокамера на них дозволяє встановити систему розпізнавання людини за обличчям.

Біометрія– технологія ідентифікації особи, що використовує фізіологічні параметри суб'єкта (відбитки пальців, райдужну оболонку ока, зображення обличчя, тембр голосу і т. п.). Зараз біометричні технології активно використовуються в багатьох областях, що потребують захисту доступу до конфіденційної інформації, матеріальних цінностей, при перетині державного кордону і т. п.

Оскільки біометричні дані є таємними й часто стають об'єктом атак, то вони підлягають захисту, а в середовищах обміну такими даними має використовуватись криптографічний захист.

Основні біометричні характеристики людини (БХЛ), за допомогою яких найчастіше здійснюється її ідентифікація:

- відбитки пальців;
- геометрія долоні, кисті руки або пальця;
- форма і геометрія обличчя;
- форма і будова черепа;
- сітківка ока;
- райдужна оболонка ока;
- ДНК;
- динаміка підпису;
- динаміка клавіатурного набору;

- особливості накреслення рукописного тексту;
- рух губ;
- голос;
- хода.

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

Універсальність – це змога представлення людини однією характеристикою. Унікальність означає, що не має бути двох людей з абсолютно ідентичними характеристиками.

Сталість\перманентність означає, що надана характеристика не повинна змінюватися з часом. Збирання (вимірювальність) – можливість швидко і легко одержати та деталізувати характеристику від індивідуума. Проведемо оцінку 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
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. Перша група використовує статичні

параметри: відбитки пальців, геометрію руки, райдужна оболонка ока і т. п. Друга група- динамічні параметри: відтворення підпису або рукописного ключового слова, тембр голосу і т. п.

У всіх біометричних технологіях можна виділити однакову базову модель. Спочатку створюється первинний реєстраційний шаблон користувача. Шаблон створюється збиранням декількох зразків за допомогою будь-якого біометричного сенсора. Потім із зібраних зразків добуваються характерні для них ознаки й отримані результати з'єднуються згідно певного алгоритму в шаблон. Первинний шаблон зберігається програмою як контрольний і еталонний шаблон.

Отже, при аутентифікувати користувача, з сенсора отримується зразк, обробляється та зіставляється з раніше зареєстрованим контрольним шаблоном. Дану форму біометричної аутентифікації називають верифікацією, потому що проводиться перевірка того, чи являється користувач тим, ким за кого видає себе.

Біометричні технології застосовують й іншу форму аутентифікації, яку називають ідентифікацією. При проведенні процесу ідентифікації користувачу не потрібно вказувати свою особистість. В цьому процесі оброблені зразки користувача зрівнюються із базою контрольних шаблонів і приймається рішення який з них має найбільший ступінь схожості. В термін «біометрична ідентифікація» - процес порівняння поданих біометричних даних з усіма шаблонами в базі даних для визначення відповідності та в разі, якщовідповідність визначено, ідентифікації відповідної особи. Можлива архітектурна реалізації вищенаведеної базової моделі зображена на рисунку 2.3 [13].

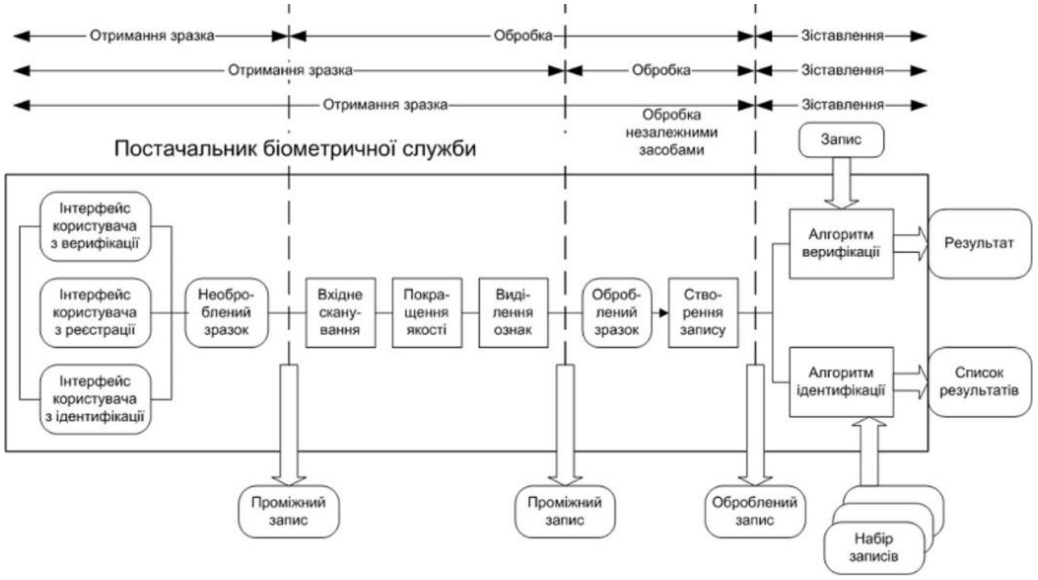


Рисунок 2.3 – Архітектурна реалізація базової моделі біометричної системи

Стадії, котрі позначені над блоком «Постачальник біометричної служби», мають відповідність елементарним функціям інтерфейсу верхнього рівня: отримання зразка, обробка та зіставлення. Стадії операцій верифікації та ідентифікації показані висвітленні у блоці «постачальник біометричний служби». Під постачальником біометричної служби мається на увазі компонент програми, котрий робить біометричні операції за допомогою певного інтерфейсу або шляхом безпосереднього керування модулями біометричного програмного інтерфейсу, або з використанням наперед визначених функцій.

.Інформаційні потоки в узагальненій біометричній системі та її структурні компоненти подані на рисунку 2.4 [13].

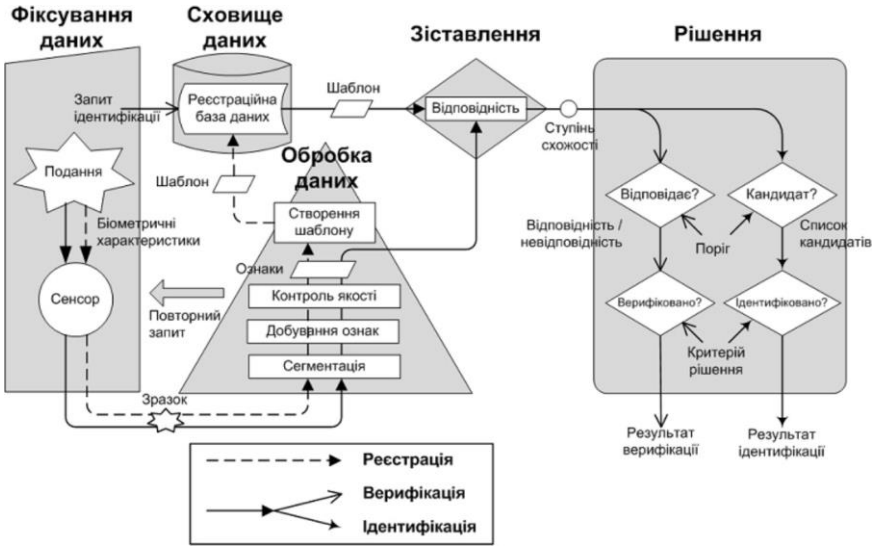


Рисунок 2.4 – Концептуальна схема узагальненої біометричної системи

Система складається таких підсистем: фіксування, обробки і зберігання даних, зіставлення й ухвалення рішення. Вищенаведена схема показує процеси реєстрації, верифікації й ідентифікації. Проте елементи, надані в даній концептуальній моделі, можуть відрізнятися, тобто бути відсутніми чи не відповідати безпосередньо фізичним компонентам у реальній біометричній системі.

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

Зразки, ознаки та шаблони можна передавати з використанням стандартних форматів обміну біометричними даними. Біометричний зразок можна ущільнити та/або зашифрувати перед передачею та розгорнути та/або дешифрувати до використання. Також зразок може бути модифікованих у процесі передавання через сторонній шум у каналах передачі або через втрати в процесі ущільнення та розширення.

Можна визначити кілька рівнів обробки біометричних даних, рис 2.5:

1. здобуті дані: необроблені дані отримані з сенсора;

2. проміжні дані: оброблені дані, але у формі непридатній для зіставлення – на такі дані посилаються, як на дані зображень або поведінки;

3. оброблені дані: дані у формі придатній для зіставлення –дані ознак.

Рисунок 2.5 – Послідовність обробки біометричних даних

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

Підсистема зберігання даних містить реєстраційну базу для зберігання шаблонів. Кожний шаблон містить якусь інформацію про суб'єкт реєстрації. Шаблони можуть зберігатися в пристрої біометричної фіксації, на переносному носії або в централізованій базі даних.

Підсистема зіставлення даних порівнює біометричні дані з шаблонами та передає інформацію про ступінь схожості до підсистеми ухвалення рішень. Ступінь схожості визначає ступінь відповідності ознак шаблонам, з якими вони порівнювалися. При проведенні 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 ухвалення вихідного рішення на запит верифікації або ідентифікації.

При верифікації, порівняння ознак та шаблону вважається успішним, при умові якщо ступінь схожості вищий, ніж встановлене граничне значення.

Підтвердження реєстрації суб'єкта ухвалюється згідно з правилами прийняття рішень, котрі можуть вимагати або допускати декілька спроб проходження верифікації.

При ідентифікації зареєстрований шаблон є потенційним кандидатом для суб'єкта, коли ступінь схожості більший, ніж встановлене граничне значення.

Підсистема керування (не зображена на схемі) керує 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.

помилкових відмов.

На рисунку 2.6 наведена частота використання методів біометричної

автентифікації [23].

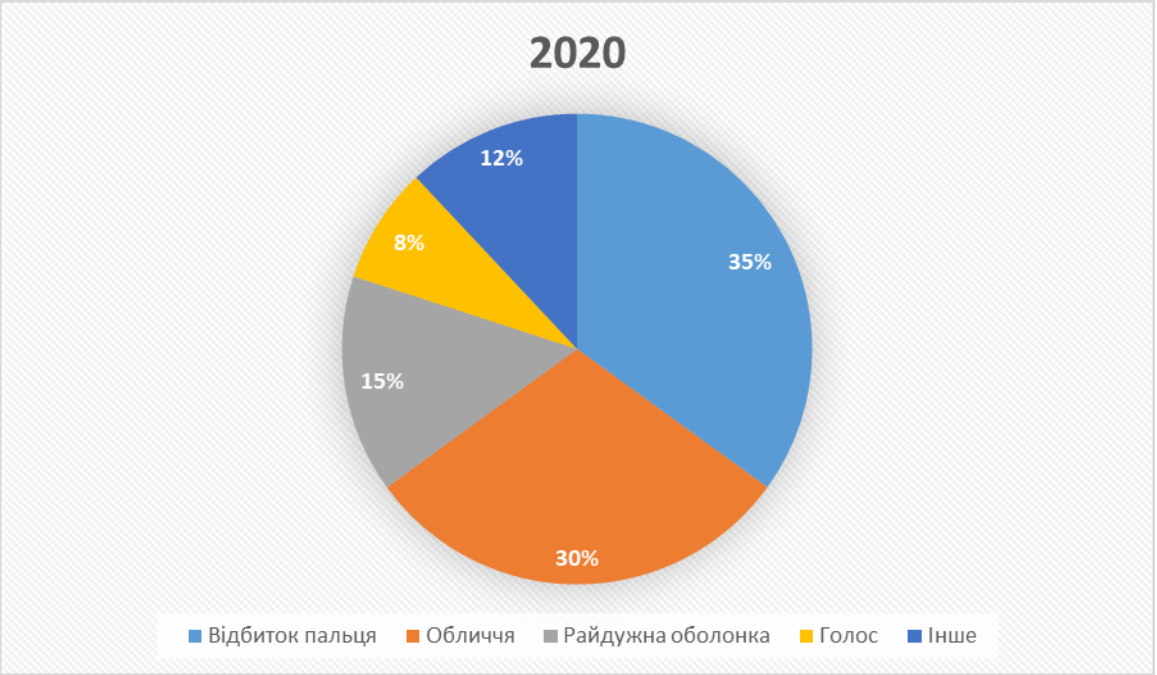


Рис. 2.6. Статистика використання методів біометричної аутентифікації на 2020 р.

На даний момент можна зазначити, що біометричні технології аутентифікації мають дуже великі перспективи розвитку. При використанні систем на основі біометричних методів процедури доступу стають швидшими , безпечнішими та простішими. Проте біометричні технології також мають ряд складнощів і проблем, таких як використання пристроїв біометричної ідентифікації людьми з деякими фізичними вадами, по підготовці професійних кадрів, зменшення вартості пристроїв та інше.

2.5. Протокол Kerberos як провідна технологія ідентифікації/автентифікації

Протокол Kerberos використовують для аутентифікації в системах “клієнт-сервер” й обміну інформацією, призначеною для встановлення захищеного каналу зв'язку між користувачами, що працюють у локальній чи глобальній мережах. Kerberos був розроблений для TCP/IP мереж і побудований на основі довіри учасників протоколу до третього (довіреної) стороні. Служба Kerberos забезпечує надійну аутентифікацію в мережі з наступною авторизацією доступу клієнта (клієнтського додатка) до ресурсів цієї ж мережі. Захищеність установлених сесій Kerberos обумовлюється застосуванням симетричних алгоритмів шифрування.Служба Kerberos розділяє спеціальний секретний ключ з кожним суб'єктом мережі, і знання цього ключа рівносильно доказу дійсності суб'єкта мережі.

Система Kerberos має структуру типу “клієнт-сервер” і складається із клієнтських частин , котрі установлені на всі машини мережі та сервері Kerberos KS. Клієнтами можуть бути користувачі, а також незалежні програми, що виконують такі дії, як доступ до баз даних, доступ до принтерів, одержання привілеїв в адміністратора й т.п.

Kerberos також створює *сеансові ключі* (session key), котрі видаються клієнтові й серверу (або двом клієнтам) і нікому більше. Сеансовий ключ використається для шифрування повідомлень, котрими обмінюються сторони та знищується одразу після завершення сеансу.

У системі Kerberos використаються два типи документів: мандат (ticket) і аутентифікатор (authenticator).

Одержання первісного мандата - виділення мандата Ticket Granting Ticket (TGT), котрий доводить службі TGT дійсність клієнта. TGT зашифровується на секретному ключі TGS та включає ідентифікатори клієнта й сервера, сеансовий ключ пари TGS-клієнт і початковий та кінцевий час дії TGT. Сервер аутентифікації посилає ці два зашифрованихповідомлення клієнтові.

Таким чином клієнт має змогу пройти аутентифікацію в TGS- сервер за

допомогою отриманого мандата TGT протягом усього терміну дії TGT.

Далі клієнт може одержати окремий мандат для кожної потрібної йому послуги. Із цією метою клієнт повинен надіслати запит у службу TGS (ПЗ надсилає запит автоматично, без втручання користувача). Такий запит складається з мандата TGT й аутентифікатора. Аутентифікатор,зашифрований на ключі парного зв'язку клієнта й сервера TGS, містить ідентифікатори клієнта та сервера, випадковий сеансовий ключ та мітку часу. TGS,отримавши запит, розшифровує TGT своїм секретним ключем. Після цього TGS використовує включений в TGT сеансовий ключ, з метою розшифрування аутентифікатора. В кінці проводиться порівняння інформації, котра знаходиться в аутентифікаторі, з інформацією мандата. Якщо все вірно, то TGS дозволяє виконання запиту.

Перевірка міток часу припускає, що годинники всіх комп'ютерів і серверів синхронізовані. В разі коли час, зазначений у запиті, значно відрізняється від поточного моменту, то TGS вважає запит спробою повторення попереднього.

У відповідь на вірний запит, TGS надає клієнтові мандат для доступу до цільового сервера. TGS також створює сеансовий ключ для клієнта й цільового сервера, котрий зашифрований сеансовим ключем, що є загальним для клієнта й TGS. Ці два повідомленнявідправляються клієнтові. Після чого клієнт розшифровує повідомлення й витягує звідти сеансовий ключ.

Запит послуги. Тепер клієнт може підтвердити свою дійсність цільовому серверу. Для успішного здійснення аутентифікації у цільовому сервері клієнт створює аутентифікатор, котрий містить його ім’я, мережеву адресу та мітки часу й зашифрований на сеансовому ключі “клієнт-сервер”, і відправляє його разом з мандатом, зашифрованим на секретному ключі цільового сервера, котрий переданий від служби TGS. Після прийняття даних від клієнта, цільовий сервер здійснює перевірку аутентифікатора. Він розшифровує його своїм секретним ключем й витягає з нього сеансовий ключ . Мандат також перевіряється. Сама процедура перевірки схожа із процедурою “клієнт-TGS”- перевіряється відповідність мережних адрес та тимчасової мітки. Якщо все добре, то сервер упевнений, що клієнт - саме той, за кого він себе видає.

Якщо вимагається взаємна перевірки дійсності, то в такому разі сервер посилає клієнту повідомлення, котре складається з мітки часу, що зашифрована сеансовим ключем. Це дає змогу довести, що сервер знає правильний секретний ключ і в змозі розшифрувати мандат і посвідчення. За необхідності клієнт та сервер мають змогу шифрувати наступні повідомлення загальним ключем. Так як даний ключ відомий лише їм, то вони обоє мають змогу полагатися, що останнє повідомлення, котре зашифроване цим ключем, було відправлено іншою стороною.

Kerberos може бути використаний також і для міждоменної аутентифікації. При доступі клієнта в центр розподілу ключів KDC з метою доступу до сервера з іншого дону, KDC видає клієнтові *мандат переадресації* (refferal ticket) для звеpенення до KDC того домену, у якому знаходиться необхідний користувачеві сервер (рисунок 2.6). На малюнку прийняті наступні позначення

1. Запит для проведення аутентифікації.
2. TGT для KDC.
3. Пред'явлення TGT для KDC.
4. Мандат доступу до сервера.
5. Аутентифікація й обмін даними.

Мандат переадресації - це TGT, котрий зашифрований на ключі парного зв'язку KDCдвох доменів. У такому випадку мандат для доступ до сервера надає користувачеві саме той KDC, де знаходиться запитуваний сервер.

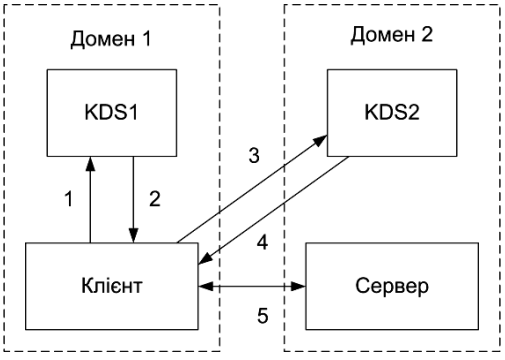


Рис. 0.0. Схема міждоменної аутентифікації через Kerberos

Таким чином доступна аутентифікація з використанням Kerberos також і в мережах з безліччюдоменів. Але для цього необхідно створити якийсь центральний домен, котрий здійснює однозначну переадресацію запитів конкретним KDC.

Kerberos працює в недовіреному програмному середовищу. Неправильна конфігурація середовища може привести до витоку критичної інформації, наприклад вихід усередовище передачі сеансових ключів, що зберігаються на жорсткому диску, або данихвідкритої інформації. Навіть при зберіганні ключів під час сеансу роботи користувача тільки в оперативній пам'яті збій в ОС може привести до того, що ключі мають змогу копіюватися на жорсткий диск. Тому безпека Kerberos залежить від надійності захисту робочої станції, на якій установлений даний протокол.

До самого протоколу Kerberos пред'являється ряд додаткових вимог, які докладно описані в RFC-1510. Приведемо тільки основні з них:

- служби Kerberos мають бути захищеними від атак, котрі спрямовані на відмову в обслуговуванні;
- здійснюється синхронізація системного часу всіх учасників системи;
- служби Kerberos мають бути надійно захищені від будь-яких видів несанкціонованого доступу;
- отримані клієнтом мандати, а також секретні ключі мають бути захищені від несанкціонованого доступу.

Невиконання вищезазначених вимог може стати причиною успішної атаки.

На сьогоднішній день протокол Kerberos є широко розповсюдженим засобом автентифікації. Kerberos може бути використаний в сполученні з різними криптографічнимисхемами, включаючи шифрування з відкритим ключем.

2.5. Висновки до другого розділу

Проведений аналіз методів автентифікації показав, що практично всі системи як основу використовують криптографічні алгоритми та схильні до традиційних атак на криптографічні процедури та на основі соціальної інженерії. Особливе місце серед них займає система двофакторної автентифікації PassWindow, основана на використанні штрих-кодів для формування автентифікатора, що ефективніше від інших протистоїть сучасним онлайн-атакам. Запропонований алгоритм моніторингу системи PassWindow дає змогу за 3–5 сесій передачі OTP паролів отримати унікальний штрих-код картки користувача.

Найефективнішим механізмом при цьому використання спеціального коду. Це дає можливість не передавати реквізитів картки через Інтернет безпосередньо продавцеві. Головним є те, що цей код можна змінювати щоразу для нової трансакції, що передбачає як значні затрати для банківської установи, так й створення окремого підрозділу для постійного супроводження та генерування код.

3 ПОБУДОВА СИСТЕМИ АУТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-ТЕКОМУНІКАЦІЙНИХ СИСТЕМІ

Перспективою у розвитку систем ідентифікації та аутентифікації є створення єдиної та комплексної системи (ЄСІА), яка б забезпечувала надійний та санкціонований доступ користувачів. Її основними функціями має бути:

- реєстрація фіз.осіб, підприємств, ІКС;
- забезпечення перевірки користувача при реєстрації;
- ідентифікація і аутентифікація користувачів веб-додатків ІКС;
- підтримка даних в актуальному стані;
- надання контрольованого користувачем доступу до його даних за запитами ІКС.

Архітектура перспективної ЄСІА подана на (рис.3.1).

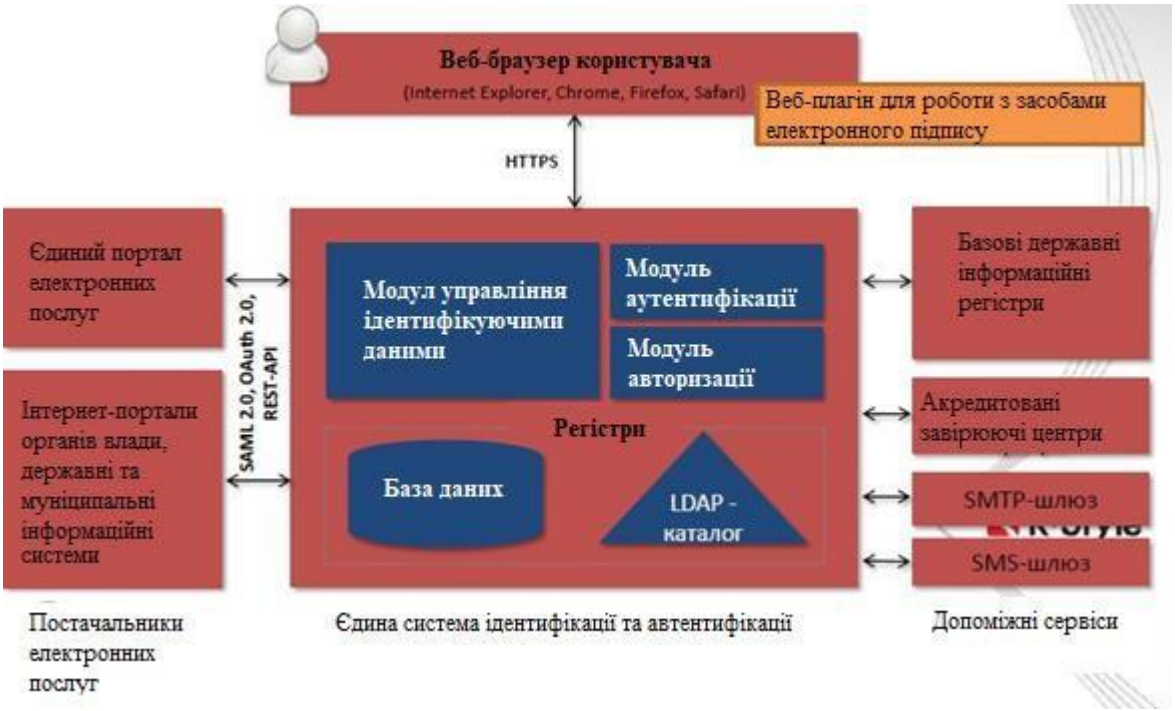


Рис.3.1 Архітектура перспективної ЄСІА

ЄСІА може використовувати додаткові сервіси, наприклад, для верифікації даних користувачів , перевірки сертифікатів ЕЦП та відправки повідомлень.

Користувачі отримують можливість одноразової аутентифікації. Це означає, що пройшовши процедуру аутентифікації в ЄСІА, користувач може протягом одного сеансу роботи увійти в кілька систем, без повторного вводу логіну і паролю.

З метою забезпечення зазначеного функціоналу в ЄСІА доцільно реалізувати два альтернативних механізми, а саме:

- по-перше, механізм, заснований на стандарті SAML версії 2.0 (рис.3.2);

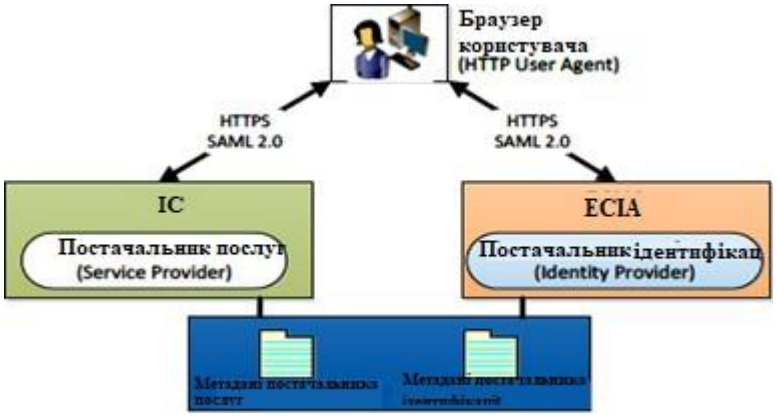


Рис.3.2. Схема взаємодії ІКС з ЄСІА з використанням стандарту SAML V2.0

- по-друге, механізм, заснований на моделі OpenID Connect 1.0 (рис.3.3).

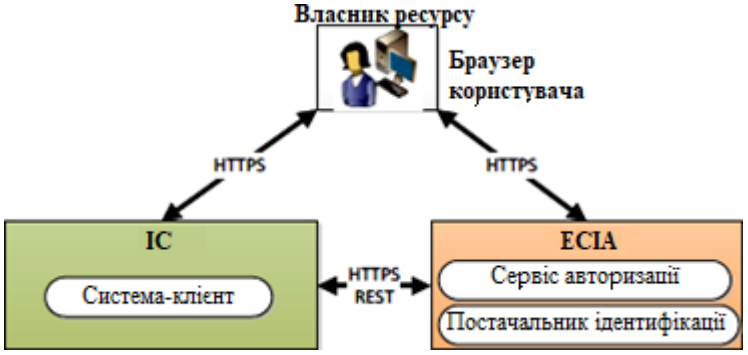


Рис.3.3. Схема взаємодії ІКС з ЄСІА з використанням стандарту OpenID Connect1.0

3.1. Процедура аутентифікації звикористанням стандарту OpenIDConnect

OpenID - відкритий стандарт децентралізованої системи аутентифікації, котрий дає змогу створити єдиний обліковий запис для аутентифікації на безлічі не зв'язаних один з одним інтернет-ресурсів, використовуючи послуги третіх осіб. Базовою функцією OpenID є надання портативного, клієнт-орієнтованого, цифрового ідентифікатора для вільного і децентралізованого використання.

OpenID дає змогу використовувати один обліковий запис зареєстрований у OpenID провайдера, на безлічі інших сайтів. Користувач має змогу обрати, котру саме інформацію надати сайту.

Механізм роботи:

1. кінцевий користувач ініціює процес аутентифікації на інтернет-сервісі. Дляцього він вводить пропонований ідентифікатор в форму входу, представлену на сайті.
2. з ідентифікатора інтернет-сервіс визначає URL кінцевої точки OpenID провайдера, який застосовується кінцевим користувачем. Ідентифікатор може містити тільки Ідентифікатор провайдера і в такому випадку кінцевий користувач вказує свій заявлений ідентифікатор, взаємодіючи з провайдером.
3. Інтернет-сервіс і OpenID провайдер створюють загальний секретний ключдля коду аутентифікації, за його допомогою інтернет-сервіс аутентифікує повідомлення від провайдера без додаткових запитів до нього для перевірки автентичності.
4. у режимі checkid_setup інтернет-сервіс перенаправляє браузер користувачана сайт провайдера для виконання аутентифікації. У режимі checkid_immediate комунікація браузера з провайдером відбувається непомітно для користувача.
5. провайдер перевіряє, авторизованих користувач на сервері і чи хоче він аутентифікуватися на інтернет-сервісі.
6. провайдер перенаправляє браузер користувача назад в інтернет-сервіс, при цьому передаючи сервісу результати аутентифікації.
7. інтернет-сервіс перевіряє справжність інформації, отриманої від провайдера. Якщо на кроці 3 було створено спільний секретний ключ, то перевірка

відбувається за допомогою нього. Якщо ключ не був створений, то в такому разі інтернет-сервіс відправляє провайдеру додатковий запит (check_authentication) У першому випадку інтернет-сервіс називається залежноюстороною без пам'яті (stateless), а в другому - німий (dumb).

8. Після успішної перевірки інтернет-сервіс аутентифікує користувача.

ЄСІА дозволятиме аутентифікувати користувача в якості представника організації. Для цього ІКС повинна:

- запросити у ЄСІА не тільки маркер ідентифікації, а й маркер доступу(на отримання даних користувача);
- з використанням маркера доступу і програмного інтерфейсу ЄСІА, заснованого на REST, отримати інформацію про співробітника організації;

Сценарій з авторизацією користувача:

Система ЄСІА володітиме функціоналом по наданню системі-клієнту інформації, на підставі якої можливе проведення авторизації аутентифікованого користувача. Рішення про авторизацію користувача приймає система, доступ до котрої він намагається отримати. Для отримання авторизаційних даних слід використовувати програмний інтерфейс. У цьому випадку крім маркера ідентифікації система має запросити маркер доступу до потрібних аавторизаційних даних. Отримавши маркер доступу, ІКС зможе отримати дані про користувача і на їх основі прийняти рішення про надання доступу користувачеві до своїх ресурсів. Загальна

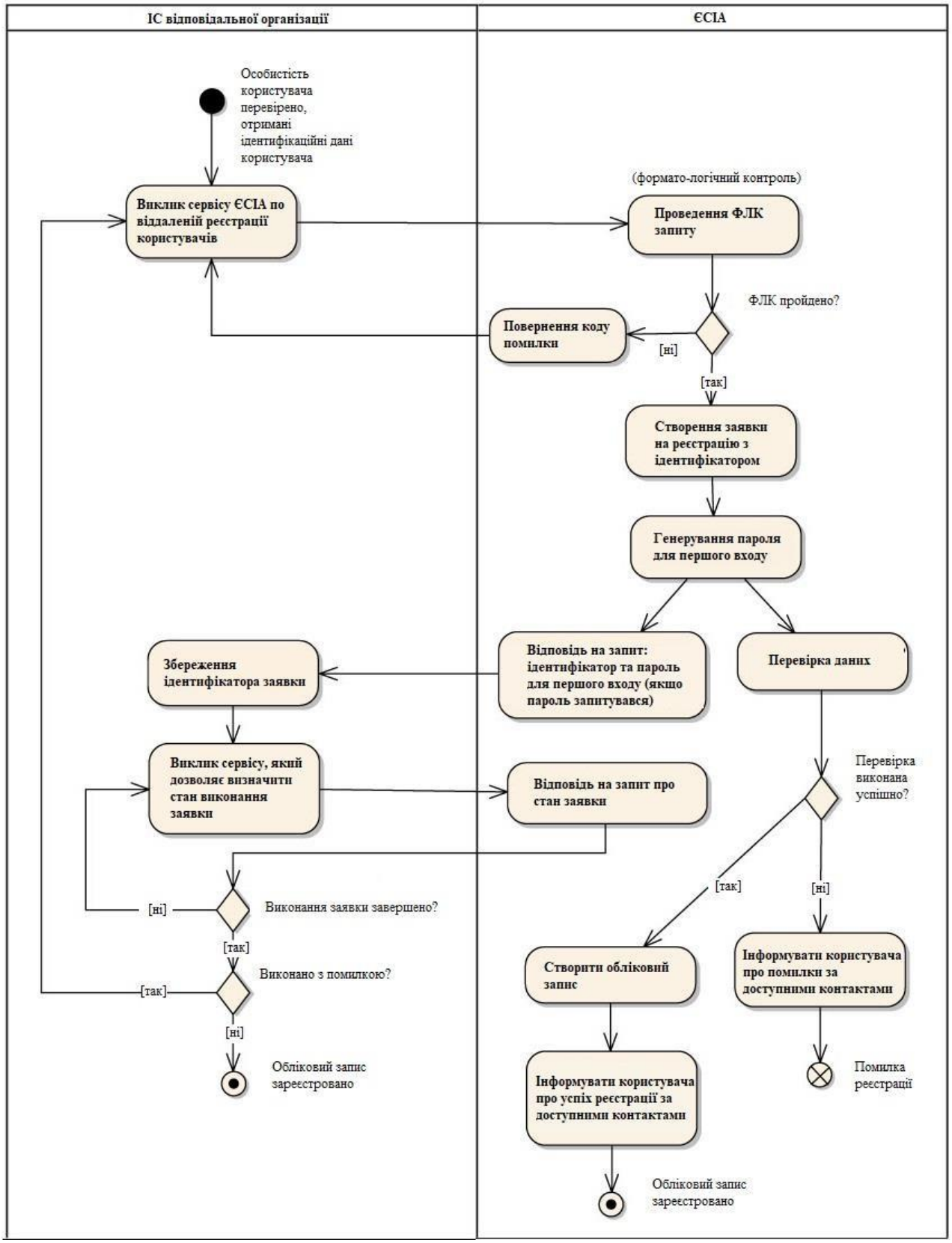


схема реєстрації користувача (рис.3.10).

Рис.3.10. Загальна схема реєстрації користувача

3.2. **Процедура ідентифікації/автентифікації з використанням стандарту SAML**

Security Assertion Markup Language (SAML)- мова розмітки, заснована на мові XML. Відкритий стандарт обміну даними аутентифікації і авторизації між учасниками, зокрема, між постачальником облікових записів (Identity provider) і постачальником сервісу (Service provider)

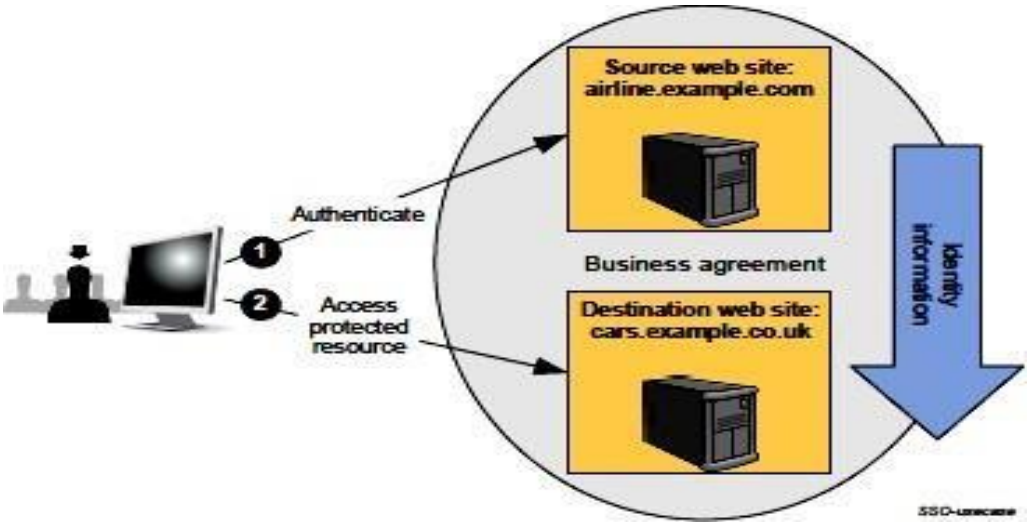


Рис.3.4 Загальний варіант єдиного входу в систему

Стандарт (SAML) визначає структуру на основі XML для опису та обміну інформацією про безпеку між онлайновими діловими партнерами. Одна з важливих проблем, яку намагається вирішити даний стандарт - забезпечення наскрізної аутентифікації(Single Sign-On) при роботі через браузер.

Виникає питання : чому SAML потрібен для обміну інформацією про безпеку. Є декілька драйверів стандарту SAML,включаючи:

по-перше, SSO. Все більше вимагається підтримка веб-SSO. Зазвичай , застосовуються файли cookie для підтримки інформації про стан аутентифікації користувача, таким чином повторна аутентифікація не вимагається коженого разу, коли користувач хоче отримати доступ до системи. Але файли cookie ніколи не передаються між DNS

доменами,так інформація про стан аутентифікації в файлах cookie з одного домену ніколи не доступна іншому домену. Тому необхідна підтримка мультидоменної SSO (MDSSO) - автентифікація через використання власних механізмів для передачі інформації про її стан між доменами. Хоча використання одного продукту постачальника іноді може бути життєздатним в рамках одного підприємства, ділові партнери, як правило, мають неоднорідні середовища, які використовують фірмові протоколи недоцільно для MDSSO. SAML вирішує проблему MDSSO,надаючи стандартну незалежну від постачальника граматику та протокол для передачі інформаціїпро користувача з одого веб-серверу на інший, незалежно від доменів DNS- сервера.

по-друге, *Federated identity*(*корпоративна ідентифікація)*. Застосовується коли Інтернет- служби намагаються створити спільне середовище додатків для їх взаємних користувачів, розуміючи при цьому не тільки синтаксис протоколу і семантику, котрий приймає участь у обміні іформацією та ким являється користувач. Користувачі зазвичай мають окремі локальні ідентифікатори в межах доменів кожного із партнерів, з котрим взаємодіють. Корпоративна ідентифікація (рис.3.5) надає засіб для цих партнерських служб для узгодження та встановлення загального ідентифікатору. Вважають, що користувач має корпоративну ідентифікацію, якщо партнери створили таку угоду про те, як звернутися до користувача. За допомогою такого типу обміну можливо зменшити витрати на управління ідентифікацією, так як різним послугам не потрібно самостійно збирати та обслуговувати дані, пов'язані з ідентифікацією

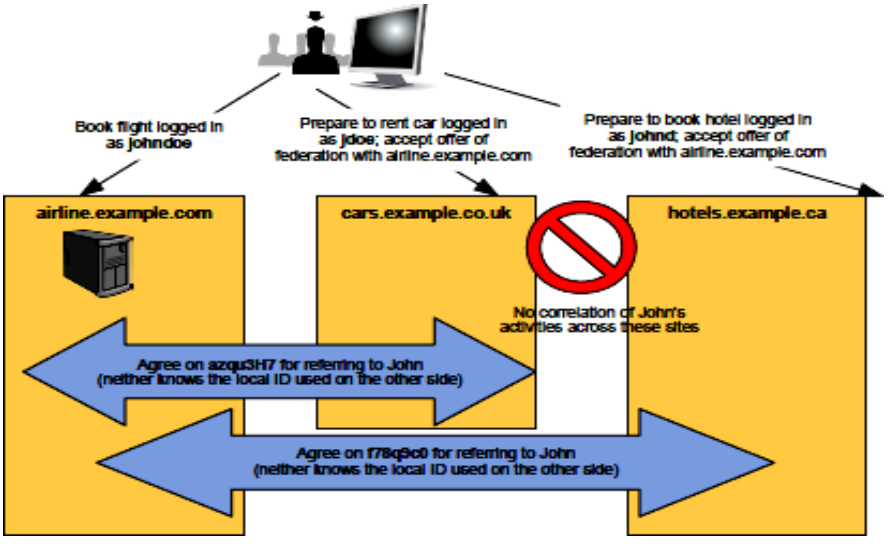


Рис. 3.5 Загальний випадок використання корпоративної ідентифікації

по-третє, Web services and other industry standards. SAML дозволяє використовувати підтвердження безпеки за межами "рідного" контексту протоколу на основі протоколу SAML.

На рисунку 3.6 розкрито основні поняття SAML, а на рисунку 3.7 показано типовий приклад зв'язку компонентів SAML.

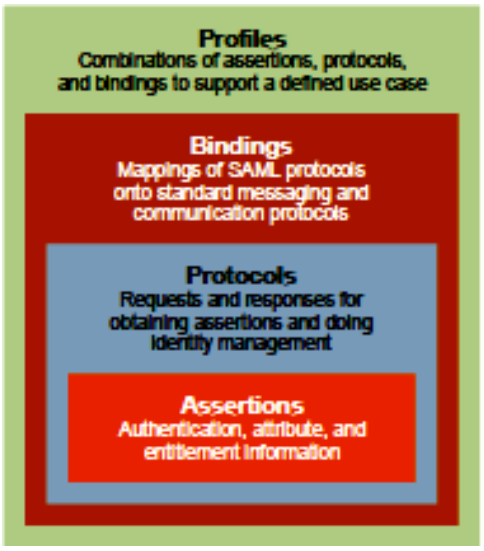
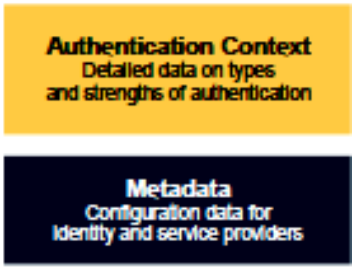


Рис. 3.6 Основні поняття SAML



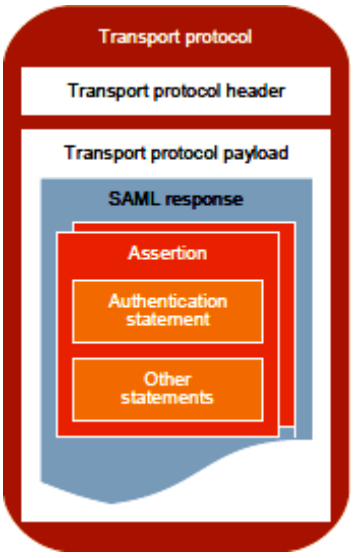


Рис.3.7. Зв'язок компонентів SAML

Базовим сценарієм є сценарій аутентифікації фіз. Особи. Цей сценарій дозволяє отримати відомості про індивідуальний користувача (фізичну особу) в момент аутентифікації і відповідає профілю Web Browser SSO Profile стандарту SAML 2.0. Сценарій має такі кроки:

1. Користувач натискає на сторінці системи постачальника послуг кнопку «Увійти через ЄСІА».

2. Постачальник послуг формує і відправляє в ЄСІА запит на аутентифікаціюі перенаправляє браузер користувача на сторінку аутентифікації ЄСІА.

3. ЄСІА перевіряє, статус аутентифікації користувача. Якщо користувач в ЄСІА не аутентифікувався, то повинен пройтиаутентифікацію одним з доступних способів. В випадку, коли користувач ще не зареєстрований в ЄСІА, то він повиен перейти до процесу реєстрації.

4. Коли користувач аутентифікований, ЄСІА перевіряє, що рівень

достовірності ідентифікації користувача відповідає вимогам системи, які зафіксовані в метаданих.

5. Якщо користувач аутентифікований, ЄСІА передає в систему відповідь на запит аутентифікації, котрий має набір тверджень SAML (SAML Assertions) про користувача.

6. Постачальник послуг приймає рішення про авторизацію користувача наоснові отриманої з ЄСІА інформації.

ЄСІА також дозволятиме аутентифікувати користувача як юридичну особу та/або ОГВ. Якщо включити таку функцію, в метадані постачальника послуг,то ЄСІА у відповіді на запит аутентифікації буде передавати відомості про організацію користувача. Якщо користувач є учасником кількох організацій, то ЄСІА попередньо попросить користувача вказати ім’я організації від імені якої він здійснює аутентифікацію. Якщо система має користувачів з різними ролями, то в процесі аутентифікації користувач матиме можливість зробити вибір ролі, через яку буде працювати.

Після аутентифікації, ЄСІА встановлюватиме призначену для користувача сесію Узагальненупроцедуру ідентифікації/автентифікації за протоколом SAML подано на (рис.3.8).

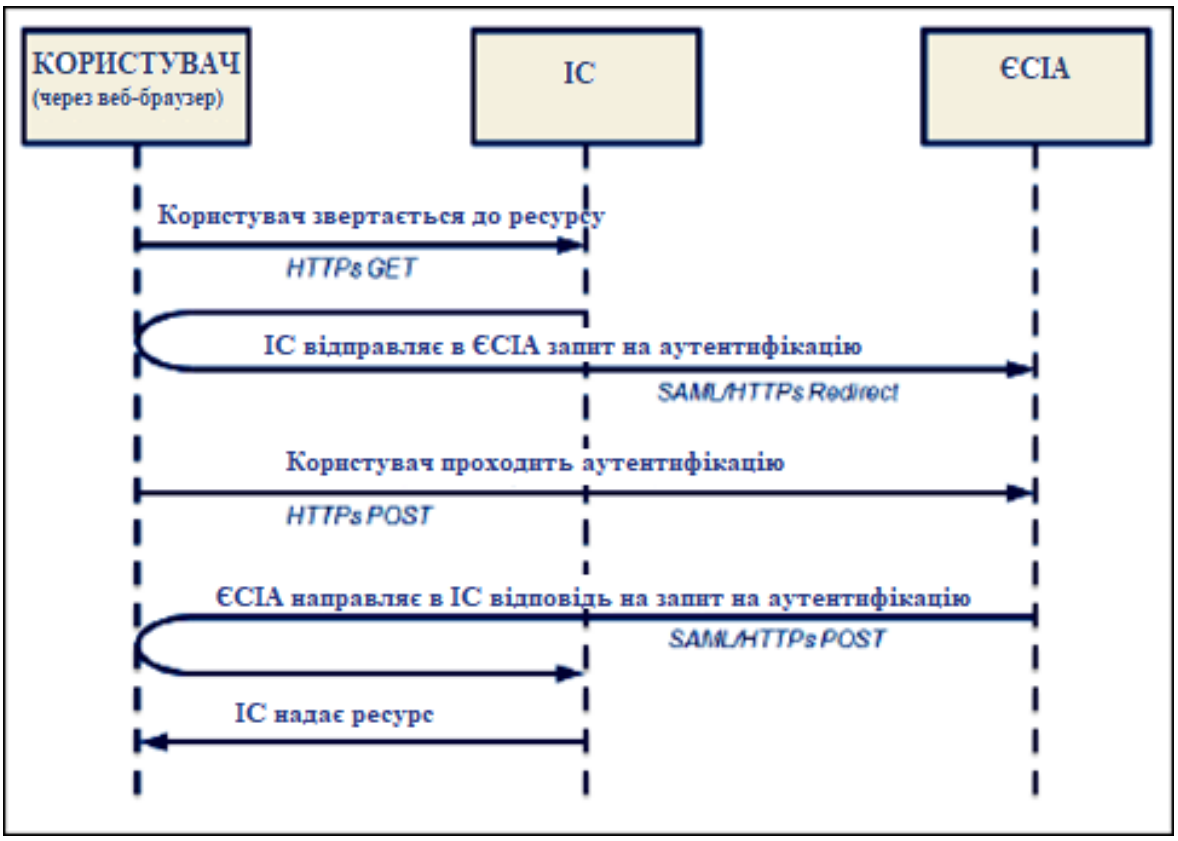


Рис. 3.8 Узагальнена процедура ідентифікації/автентифікації користувачів з використанням протоколу SAML

Система ЄСІА буде володіти функціоналом з надання постачальнику послуг інформації, на підставі котрої можна провести авторизацію аутентифікованого користувача. Рішення про здійснення авторизації користувача приймає система, в кортій користувач проходить авторизацію (Таблиця 3.1).

Таблиця 3.1

Вимоги до авторизації користувачів

Вимоги	Рекомендоване рішення
Знання про користувача для строворення сеансу (ім'я, ідентифікатор). Без необхідності зберігання даних про активність користувача до наступного сеансу.	Предоставляти доступ тільки після отримання з ЄСІА відповіді на запит аутентифікації, що має необхідний набір відомостей про користувача.
Більш детальні знання про користувача (наприклад, ПІБ, e-mail, локація та інше) і довготривало зберігати контекст (налаштування, дії, коментарі).	При першому вході користувача сторювати і реєструвати його ідентифікатор.
Вимагається обмежити набір надаваних функцій в залежності від типу облікового запису, ролі користувача, використаного метода аутентифікації.	При спробі користувача звернутися до функції, для надання якої поточний тип облікового записукористувача, роль користувача або метод аутентифікації єнедостатніми, вивести йому повідомлення з поясненням про наступні дії.

В наступній таблиці наведено рекомендації щодо перевірки відповідності вимогам ІС типу облікового запису та ролі користувача та використаного методу аутентифікації, а також надано рекомендації щодо повідомленням та подальших дій.

Таблиця 3.2

Рекомендації щодо інформування користувача про невідповідність авторизації вимогам системи

Ситуація	Як визначити ситуацію	Що повідомити і запропонувати користувачеві
Користувач з обліковим записом з типом звернення ("неперевірена") спробував звернутися до функцій, що надаються лише стандартним ("перевіреним") і/або "підтвердженим" обліковим записам.	Проаналізувати твердження SAML з ім'ям assurenceLevel або personTrusted	При доступі до функцій, що потребують стандартного (перевіреного) облікового запису: "Для доступу вам необхідно пройти процидуру перевірки своїх даних. Якщо ваші особисті дані тільки-но пройшли перевірку, то вам потрібно ввійти в систему повторно." Посилання на перевірку даних: https://esia-portal.test.dergposlugi.ua/validate При доступі до функцій, що потребують підтвердженого облікового запису: "Для доступу вам необхідно пройти процедуру перевірки своїх даних і підтвердження особистості. Якщо ви тільки-но підтвердили свою особистість, то вам потрібно ввійти всистему повторно." Посилання на перевірку даних: https://esia-portal.test.dergposlugi.ua/validate
Користувач з обліковим записом з типом стандартна (перевірена) спробував звернутися до функцій, надаваним тільки для "підтверджених" облікових записів.	Проаналізувати твердження SAML з ім'ям assurenceLevel	"Для доступу вам необхідно пройти процедуру підтвердження особистості. Якщо ви тільки-но підтвердили свою особистість, то вам потрібно увійти до системи повторно" Посилання на підтвердження особистості: https://esia-portal.test.dergposlugi.ua/confirm

Продовження таблиці 3.2

Рекомендації щодо інформування користувача про невідповідність авторизації вимогам системи

Ситуація	Як визначити ситуацію	Що повідомити і запропонувати користувачеві
Користувач з обліковим записом з роллю фізичного лиця спробував звернутися до функцій, надаваних тільки для ПП/ посадових осіб/ ЮО та інших	Проаналізувати твердження SAML з ім'ям globalRole і orgType	Якщо необхідна роль співробітника ЮО і данний обліковий запис має тип "підтверджено": "Для доступу вам необхідно увійти до системи в якості співробітника юридичного обличчя. Якщо ви є керівником юридичного обличчя, ви також можете зареєструвати обліковий запис юридичного обличчя". Посилання для реєстрації ЮО: https://esa-portal.test.dergposlugi.ua/org Якщо необхідна роль ІП і данний обліковий запис мають тип "підтверджена": "Для доступу вам необхідно увійти в система в якості приватного підприємця. Ви також можете зареєструвати обліковий запис Приватного підприємця." Посилання: https://esa-portal.test.dergposlugi.ua/orgs Якщо необхідна роль посадового обличчя ОДВ і данний обліковий запис має тип " підтверджена" : "Для доступу вам необхідно увійти в систему в якості посадового обличчя органу державної влади." Якщо користувач має спрощений (не перевірений) / стандартний (перевірений) обліковий запис, то необхідно його проінформувати про необхідність підтвердження особистості. Це є необхідною попередньою умовою для можливості отримання користувачем ролі посадового обличчя ЮО, ОДВ або ролі ПП.
Користувач, що аутентифікувався по паролю, спробував отримати доступ до функції, що потребує аутентифікації за електронним підписом.	Проаналізувати твердження SAML з ім'ям authnMethod.	"Для доступу вам необхідно використати засіб кваліфікованого електронного підпису. Якщо у вас є засіб електронного підпису, увійдіть знову, використавши цей засіб." Після цього повідомлення рекомендується розмістити кнопку виклику єдиного закінчення сессії.

Протягом дії сесії користувач має увійти в одну або кілька інших систем, підключених до ЄСІА без додаткової аутентифікації. В разі необхідності в одночасному завершенні сесії у всіх системах використовується відповідний сценарій. Єдине завершення сесії здійснюється відповідно до профілю Single Logout стандарту SAML. Користувач ініціює процес при натисканні кнопки «Вихід» в системі постачальника послуг, котрий реалізував указаний сценарій.Інформаційна система не повинна самостійно ініціювати єдине завершення сесії.

Сценарій включає наступні кроки:

1. Користувач натискає кнопку «Вихід» всистемі.
2. Система формує і направляє в ЄСІА запит на завершення сесії - <LogoutRequest>.
3. ЄСІА визначає інших учасників сесії. Решта учасників сесії - це все системи,в які користувач увійшов через ЄСІА протягом поточної сесії. Якщо інші учасникиіснують, ЕСІА відправляє запит <LogoutRequest> кожному зних.
4. Система, що отримала <LogoutRequest>, завершує на своєму боці активнусесію користувача. Потімформує і відправляє в ЄСІА відповідь про те, що сесія завершена - <LogoutResponse>.
5. Коли всі інші учасники коректно завершили свої сесії, ЄСІА формує і відправляє відповідь <LogoutResponse> системі, яка ініціювала процедуру завершеннясесії. Якщо хтось із постачальників послуг не зміг завершити сесію, ЄСІА відображає користувачеві веб-сторінку, яка інформує про те, що процедура не може бути коректно завершена та необхідно перезапустити браузер.
6. Система, яка ініціювала процедуру завершення сесії, обробляє отриманий від ЄСІА відповідь. Наприклад, перенаправляє користувача на веб-сторінку завершення сесії

3.3. Процедура ідентифікації/автентифікації з використанням стандартуKerberos

Ще одним методом аутентифікації, на котрий слід звернути уагу- протокол Kerberos.. Ця система передбачає відсутність ключа між сервером продавця та покупця, а також присутні нові зв'язки між сервером продавця та PGS TGS у Kerberos, (рис.3.11).

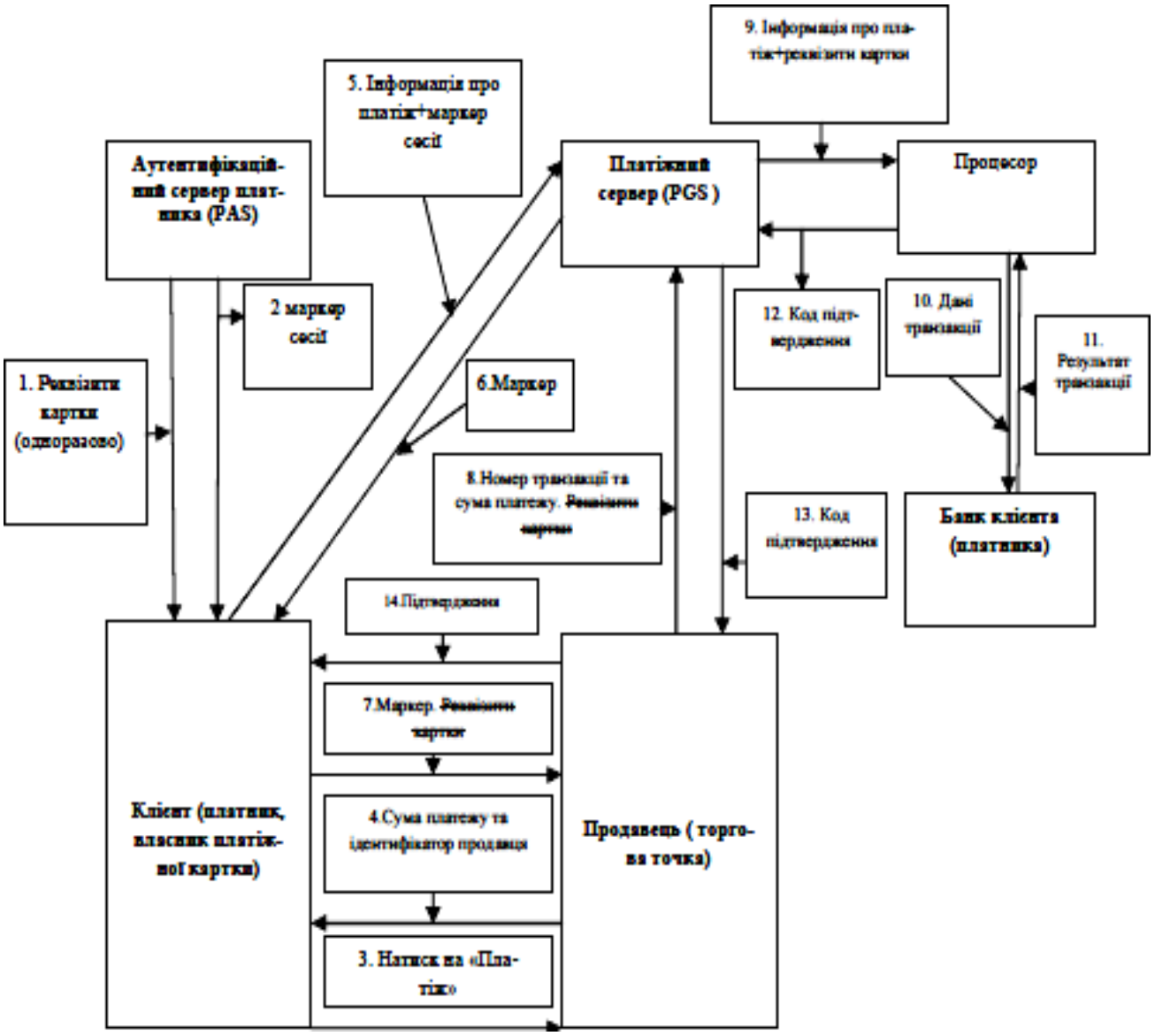


Рис. 3.11. Схема реалізації інтернет-транзакції на основі протоколу автентифікації Kerberos

Наприклад, у схемі інтернет-транзакції , клієнт зв’язується ізторговою точкою, а торгова точка у свою чергу – із платіжним шлюзом. У нашому жвипадку, із схеми на рис. 3.10, видно, що платіжний сервер (PGS), який замінив платіжний шлюз, зв’язується, як з покупцем, так і з продавцем, на відміну від існуючої системи Kerberos. В обміні ключами також вартує дещо змінити, а саме між покупцем іпродавцем (рис. 3.12).

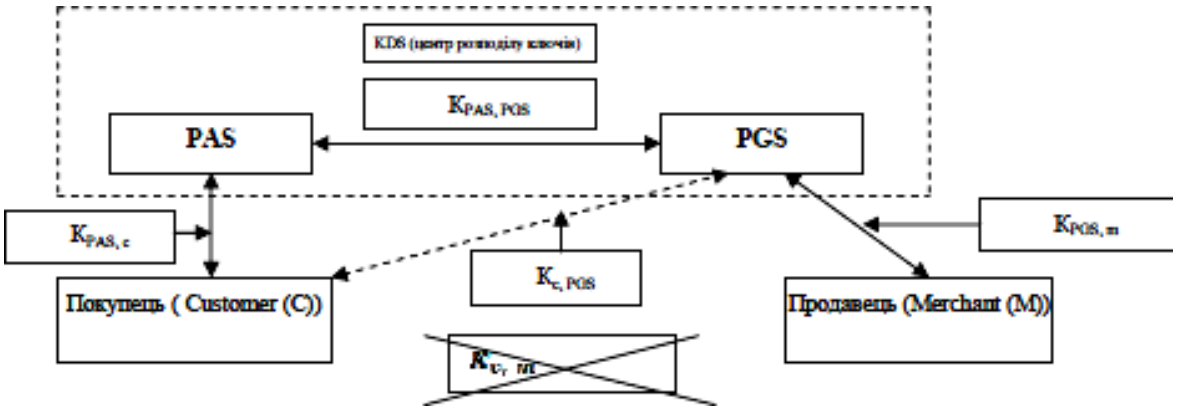


Рис.3.12. Процес обміну ключами в протоколі автентифікації Kerberos

Також, у вище запропонованій системі використовуються два маркери - маркер сеансу та маркер платежу, котрий має інформацію пропокупця, продавця та суму платежу.

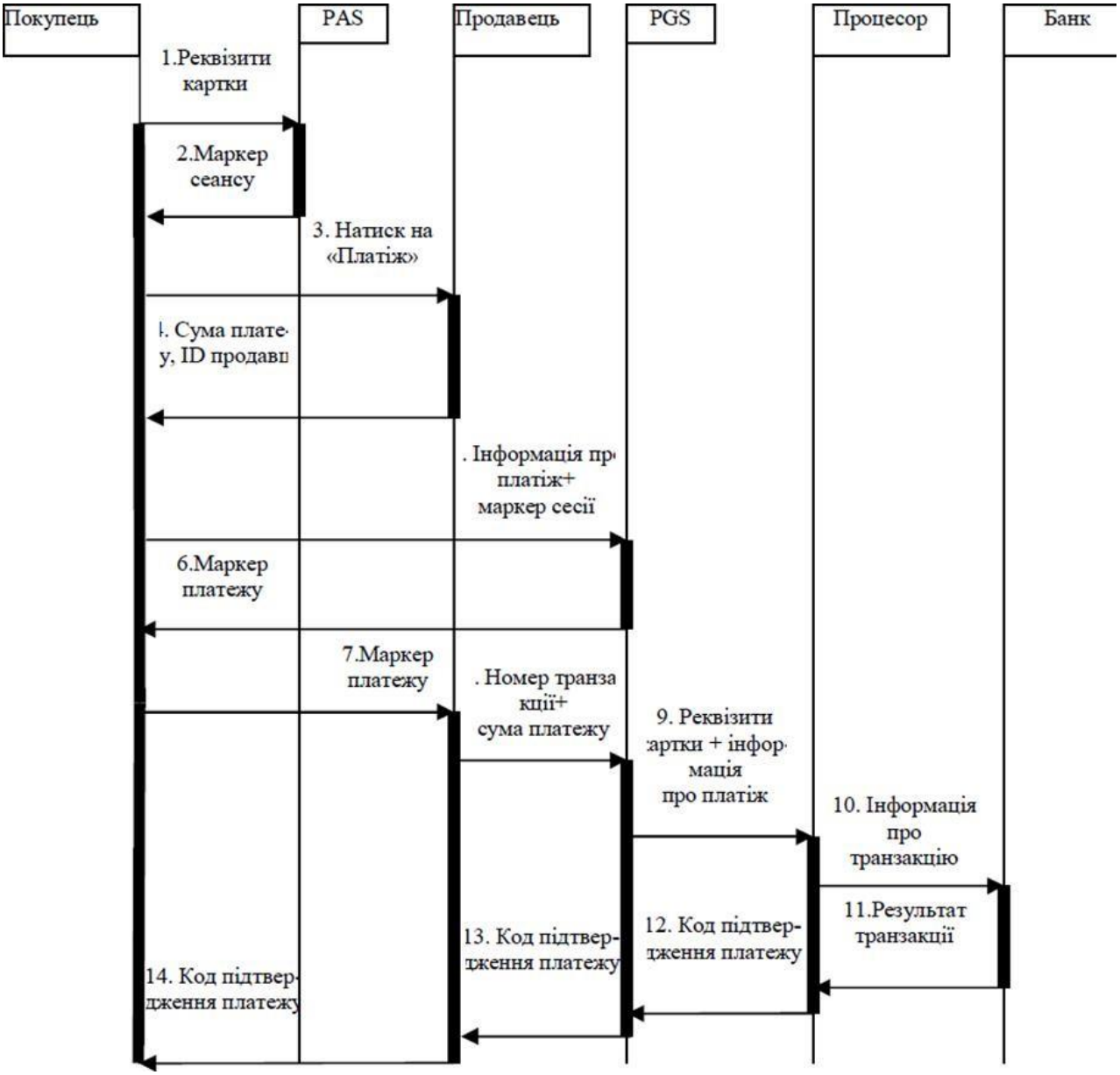


Рис. 3.13. Покрокова діаграма здійснення інтернет-транзакцій в протоколіKerberos

Як можна помітити з (рис.3.13), платіжний сервер (PGS), котрий замінив платіжний шлюз, зв’язується з покупцем та з продавцем. При цьому (рис.2.9) спочатку покупець надсилає до аутентифікаційного серверу реквізити своєї картки і отримує натомість маркер сесії. Після цього користувач надає інформацію про платіж (сума платежу, назва продавця) разом із маркером сесії платіжному серверу (PGS) та отримує від нього маркер платежу. Потім покупець відсилає продавцю цей маркер платежу. І торгова точка надсилає номер транзакції платіжному сервера. Отримавши номер транзакції, PGS робить обробку платежу.

Очевидною перевагою для вищенаведеного варіанту з використанням протоколу Kerberos є відсутність безпосередньої передачі реквізитів картки від покупця до продавця під час інтернет-платежу. Таким чином можна зменшити кількість шахрайських дій, що пов’язані з перехопленням реквізитів картки. У схемі протоколу продавцю передаються маркери платежу, а не інформація по картці. В цьому випадку ні продавець, ні зловмисник, який зламує базу даних, не можуть несанкціоновано отримати реквізити картки.

Запропоноване удосконалення може бути застосоване до існуючого протоколу шляхом модифікації потоку даних, тобто замість надсилання реквізитів картки безпосередньо продавцю, до платіжного сервера надходить маркер.

3.4Процедура багатофакторної ідентифікації/автентифікації на трансакційному ідентифікаційному коді та службі коротких повідомлень

Багатофакторна аутентифікаційна система базується на трансакційному ідентифікаційному коді (TIC) та на службі короткихповідомлень (SMS) для створення додаткового рівня безпеки, котрий відсутній при традиційній аутентифікації. Цей код схожий на одноразовий пароль (OTP), але забезпечує більшнадійну аутентифікації. TIC засвідчує, що поточна трансакція була ініційована саме тим, яка є істинним власником рахунку (банківської картки), а не зловмисником. TIC-коди володіють певними властивостями: створюються банком псевдо-випадково згенерованими кодами; можуть являти собою складну послідовність цифр або буквено-цифрових символів; кожна трансакція вимагає унікального коду для автентифікації, тобто кожен код використовується лише один раз. Механізм генерації кодів є суворо. Банк зберігає номер телефону клієнта, щоб згодом надіслати SMS для підтвердження транзакції. Багофакторна аутентифікація використовується для перевірки покупця та транзакції відповідно до наступних кроків:

1. Базова автентифікація: вхід на веб-сервер користувача з використанням призначений йому веб-ім’я та паролю для базової автентифікації;
2. TIC-автентифікація: Після успішної стандартної аутентифікації користувача, веб сервер запросить ввести TIC (друга автентифікація).
3. SMS-підтвердження: Після успішної TIC-аутентифікації, третьою аутентифікацією є SMS-підтвердження. Користувач отримує SMS із деталями транзакції, які необхідні для ідентифікації та розпізнавання ініціатора транзакції.

Механізм багатофакторної автентифікації передбачає наступні кроки :

1. клієнт отримує логін та пароль у своєму банку при відкритті рахунку абомаючи рахунок у цьому банку;
2. покупець входить на веб-сервер свого банку через GPRS-з’єднання,

використовуючи свій логін та пароль. Ця перша автентифікації призначена для ідентифікації покупця веб-сервером;

3. після успішної першої автентифікації покупець отримає опцію, щоб розпочати транзакцію із вхідним повідомленням та ідентифікатором сесії;

4. покупець обирає спосіб оплати (кредитна картка, дебетна картка, електронний переказ). У випадку розрахунку карткою протокол вимагає дійсні реквізити платіжногозасобу;

5. покупець вводить деталіплатежу;

6. клієнт не може здійснити транзакцію без TIC. Треба мати на увазі, що TICи захищені паролем на мобільному телефоні, і цей пароль перед використанням в

транзакції буде дешифрований за допомогою одного із TIC шифрів.

7. уся сукупність трансакційних записів разом з TIC буде далі зашифрована та передана серверу дляобробки.
8. автентифікаційний сервер банку розшифровує отриману інформацію про транзакцію та витягує звідти TIC. Сервер перевіряє отриманий від покупця код, порівнюючи його із кодом, збереженим разом із інформацією про рахунок клієнта, атакож який був обраний із списку кодів бази даних сервера. Якщо обидва коди співпали,використаний код автоматично знищується із бази даних. Якщо ж коди не співпали, тоді автентифікаційний сервер скасовує будь-які подальші транзакції клієнта та надсилаєповідомлення про помилку.
9. якщо TIC автентифікація є успішною, тоді авторизаційний сервер генеруєтекст повідомлення (SMS) та надсилає його до SMS шлюзу/ адаптера для передачі через стільникову мережу. Стільникова мережа використовує SMSC як основний пристрій мережі для передачі SMS на стільниковий телефон користувача.
10. покупець підтверджує ініційовану трансакцію за допомогою SMS із текстом

«ТАК» або скасовує обираючи текст повідомлення «НІ» (рис. 3.14).

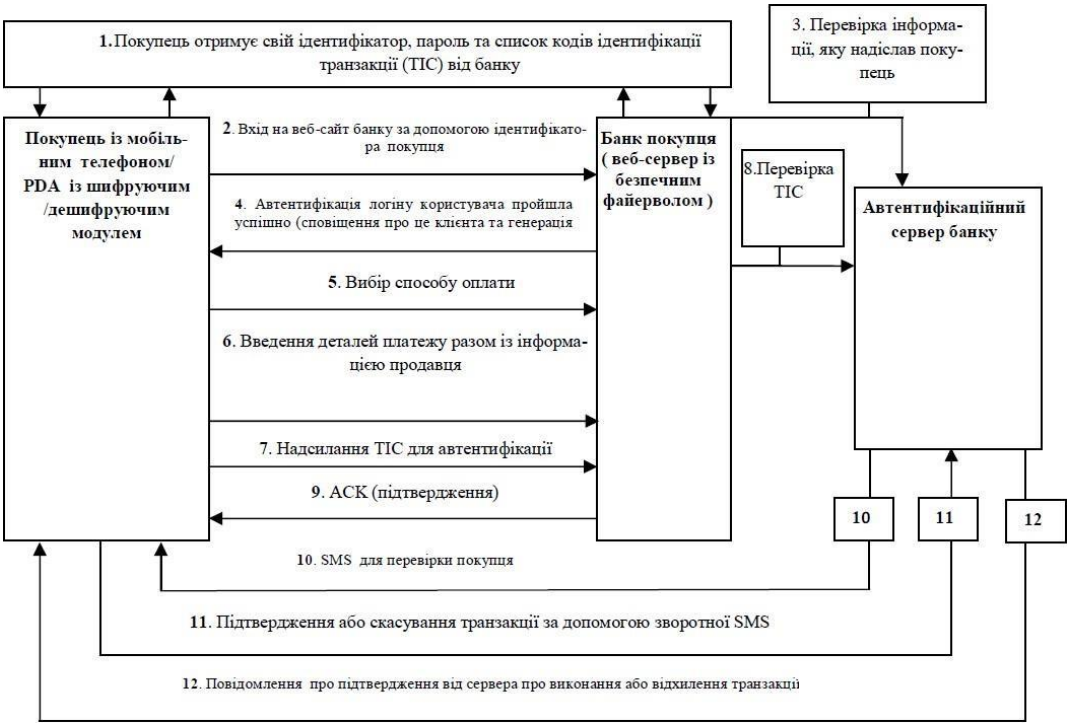


Рис. 3.14. Потік даних у протоколі багатофакторної ідентифікації/автентифікації

У вищеописаному протоколі ТІС коди є найбільш уразливими даними, які зберігаютьсяна стільниковому телефоні /КПК. Саме тому вони перебувають у цих пристроях покупця у зашифрованому форматі, а також захищені паролем, як це зображено на(рис.3.15). Покупець вводить локальний пароль для відкриття списку ТІС кодів і обираєбудь-який код з цього списку, щоб розпочати трансакцію. Цей вибір коду автоматичнорозшифровує його та автоматично виводить на екран користувача. Це також призводить до переміщення обраного коду із списку у середовище клієнта. Локальнийпароль є ключем розшифрування ТІС коду та є відомий лише клієнту.

Рис. 3.15.Захист ТІС коду в середовищі покупця

Навіть серверу фінансової установи є невідомий цей пароль. Код може бути змінений у будь-який момент за бажанням користувача

3.5. Рекомендації щодо підвищення ефективності інформаційної безпеки сучасного підприємства

Для забезпечення основних властивостей інформації, яка становить певну цінність і є важливою, існує цілий ряд нормативно-правових документів. Використовується досить дороге технічне обладнання, впроваджуються системі захисту, однак це не може гарантувати повний захист. Цьому є ряд причин, котрий можна розділити на три групи:

- нехтування системного підходу до методів захисту інформації;
- відсутність механізмів повного і достовірного підтвердження якості захисту інформації;
- недоліки нормативно-правового забезпечення ІБ;
- відсутня система менеджменту та управління ІБ.

Для вирішення проблеми забезпечення ІБ, необхідно чітко визначені та зформулюванні цілі та задачі захисту інформації. В разі коли ціль захисту інформації по нескладна, то її реалізація цілком можлива і не вимагає великих затрат і ресурсів . Але чим вищі вимоги, тим важча і складніша реалізація поставленої задачі.

В даному випадку кожен окремий елемент порівняно втрачає свою вагу, але в комплексі створює значно надійнішу й потужнішу систему. У таких системах необхідно акцентувати увагу не на властивості кожного окремого елемента, а на їх взаємодії. За допомогою цього система набуває специфічних властивостей, котрі не притаманні жодному з даних елементів.

Базові напрями організації захисту інформації ІКС (рис.3.16)

Для побудови надійної СЗІ в сучасних ІКС та мережах потрібно спочатку визначити можливі загрози для інформаційних ресурсів.

В ІБ успіх може принести тільки комплексний підхід. Для захисту інтересів суб'єктів інформаційних в сучасних ІКС необхідно поєднувати заходи наступних рівнів:

- законодавчого ;
- адміністративного;
- процедурного;
- програмно-технічного.

Основними властивостями інформації є цілісність, конфіденційність і доступність. Порушення однієї з цих властивостей може спричинити численні зміни, чи навіть повну втрату цінної інформації.

Саме модель можливих загроз може допомогти впоратись із цією проблемою. Якщо звернути увагу на необхідність та варіанти створення ІБ, можна побудувати своєрідну «піраміду» КСЗІ в ІКС та мережах. Нормативно-правовий захист інформації являється фундаментом побудови всієї ІБ підприємства, організації, установи.

Правовий елемент інформаційного захисту складають законодавчі засоби захисту інформації, які є множиною нормативно-правових актів, котрі діють у певній державі і забезпечують юридичну підтримку для розв'язання задач захисту інформації.В Україні Основним Законом є Конституція.

Рис. 3.16. «Піраміда» організації системи захисту інформації в сучасних ІКС

Для створення правового захисту організації потрібноорганізувати юридично закріплені правові взаємовідносини між державою та підприємством, щодо правомірності використання ІБ, між підприємством та персоналом щодо обов'язковості дотримання порядку захисту інформаційних ресурсів. Організаційний захист інформації – регламентація виробничоїдіяльності та взаємовідносин виконавців

на нормативно-правовій основі.

На даному етапі побудови СЗІ необхідно організувати регламентований режим та охорону приміщення в якому знаходиться інформація. Провести організаційні роботи із співробітниками, використовувати методи їх аутентифікації та ідентифікації, створити обмеження щодо доступу. Особливо важливим моментом є детальний аналіз всіх можливих загроз, а також проведення систематичного контролю і оцінки цих.

Інженерно-технічний захист також невід'ємна части побудови КСЗІ, тому що саме він може попередитинесанкціонований доступ до інформаційних ресурсів та запобігти витоку інформації технічними каналами зв'язку в ІКС.

Основними задачами цієї ланки інформаційної безпеки є:

- попередження проникнення зловмисника до інформації з метою її видалення, модифікації чи викрадення;
- запобігання витоку інформації різними технічними каналами.
- Апаратний захист інформації розуміє під собою наявність апаратного забезпечення До апаратних засобів захисту інформації відносяться різні електронні, електронно - механічні та електронно-оптичні прилади. В наш час є широкий спектр таких приладів, але найбільшого використання набули такі як:
- спеціальні регістри для збереження реквізитів
- пристрої для зчитування індивідуальних характеристик людини(біометрії) з метою її ідентифікації;
- схеми переривання передачі інформації на лінії зв'язку для перевірки адреси видачі даних;
- пристрої для шифрування інформації

Програмний захист інформації - це совокувність ПЗ, для проведення ідентифікації користувачів, контролю доступу, шифрування інформації, знищення тимчасових файлів та інше. Використання ПЗ захисту інформації має цілий ряд переваг - універсальність,надійність, простота у використанні та можливість модифікації.

3.6. Висновки до третього розділу

Аутентифікація - це процес перевірки індивідуальності суб'єкта, котрим може бути не тільки людина, а також і програмний процес. Підсумовуючи, можна визначити, що аутентифікація можлива за допомогою інформації, котра може зберігається в різній формі. Наприклад, це може бути: пароль, особистий номер, цифровий сертифікат, смарт-карта, електронний ключ, відбитки пальців і інші біометричні характеристикикористувача.

Аутентифікація дозволяє розмежувати права доступу доінформації, котра можу бути в загальному користуванні. Проте існує проблема забезпечення цілісності і вірогідності інформатизації. Користувач повинен бути цілком впевнений,що отримує доступ до інформації з джерела, якому може довіряти і що дана інформація не модифікувалася несанкціоновано.

При виборі способу аутентифікації потрібно враховувати такі фактори як: цінність інформації; вартість, продуктивність системи, специфіку інформаційного комплексу, що захищається.Вартість, якість і надійність засобів аутентифікації мають бути пропорційними важливості інформації. Окрім того, підвищення продуктивності комплексу та найдійності, зазвичай, супроводжується його дорожчанням (хоча і не завжди).

ВИСНОВКИ

Згідно проаналізованої інформації, основними завданнями забезпечення ІБ комп'ютерних систем є забезпечення конфіденційності, доступності та цілісності даних, аутентифікація, керування доступом. Сучасні засоби підтримки безпеки ґрунтуються на різних технологіях і аспектах таких як: криптографічних, із секретним і відкритим ключами, гібридні криптосистеми, цифрові підписи і сертифікати. Аутентифікація надає змогу підтвердити,що користувач являється тим, за кого себе представляє. Зазвичай, для підтвердження особи користувача використовують паролі. Сучасні методи аутентифікації дають можливість уникнути передавання пароля у незашифрованому вигляді. Авторизація визначає дії, які авторизований користувач має змогу виконувати з об'єктами у системі. Авторизація реалізована на основі визначення списків контролю доступу, пов'язаних ізоб'єктами у системі, а також списків можливостей, пов'язаних із окремими користувачами. Необхідно зазначити, що створення КСЗІ потребує глобального підходу до кожного із аспектів даного питання. Тільки поетапне виконання правового, організаційного, інженерно-технічного, апаратного та програмного рівнів побудови ІБ може дати можливість створення цілісної системі для забезпечення надійної інформаційної безпеки. Побудова моделі загрози дасть можливість виявити слабкі місця у системі та оперативно усунути їх. Проблеми захисту інформації в сучасних ІКС та мережах потребують комплексного підходу у вирішенні питання ІБ.

Одним із найперспективніших напрямів розвитку систем аутентифікації є розвиток біометричних систем. Основну увагу в розвитку таких систем можна звернути на вдосконалення апаратно-програмних засобів, котрі могли б дозволили досягти зменшеннярівня помилок першого та другого роду, а також були б захищені від спуфінгу.

Переважна більшість систем аутентифікації в майбутньому, скоріше за все, будуть побудовані за комбінованимтипом аутентифікації з використанням декількох методів для кращого захисту.

Також частину систем аутентифікації на основі символьного пароля буде

замінено на системи на основі графічного пароля, як більш захищені. Проте це може викликати певені незручності при введення такого паролю, що обмежить його застосування в найпростіших системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ахрамович. В.М. Ідентифікація й аутентифікація, керування доступом. Сучасний захист інформації. К. ДУТ:-2016 .-№4.- с. 47-51
2. H.Abie,"semanticscholar".URL:https://pdfs.semanticscholar.org/3733/2607f7a7ac8284c514845957fd00583e5614.pdf (дата звернення: 25.09.2020).
3. A Review on Authentication Methods. URL: https://hal.archives- ouvertes.fr/hal-00912435/PDF/A_Review_on_Authentication_Methods.pdf (датазвернення: 25.09.2020).
4. Authentication protocol.URL:https://en.wikipedia.org/wiki/Authentication_protocol (дата звернення:25.09.2020).
5. Vanek T.. "Autentizacní telekomunikacních a datových sítích". CVUTPrague. 4 March 2016.
6. Extensible Authentication Protocol.URL:https://doubleoctopus.com/security-wiki/protocol/extensible-authentication- protocol/ (дата звернення: 25.09.2020).
7. AAA protocols.URL: http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-1/user/guide/acsuserguide/rad_tac_phase.html (дата звернення: 26.09.2020).
8. Liu J. Introduction to Diameter. www.ibm.com. IBM. 24 Januar 2006.
9. Sarah Al-Shareeda. Authentication Technologies for Cloud Compu- ting, IoT and Big Data. 2019. URL: https://digital- library.theiet.org/content/books/10.1049/pbse009e_ch3 (дата звернення: 27.09.2020).
10. Закон України 2155-VIII «Про електронні довірчі послуги» від 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2155-19/ed20171005#n9 (дата звернення: 27.09.2020).
11. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації вкомп’ютерних системах від несанкціонованого доступу» URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=5A88E6FEAB902185A2100ECC92151B59?showHidden=1&art_id=101853&cat_id=89734&ctime=1344501024406 (дата звернення: 28.09.2020).
12. Authentication. URL:

13. https://www.acunetix.com/websitesecurity/authentication/ (дата звернення: 28.09.2020).
14. Authentication attacks and countermeasures. URL: https://sites.google.com/a/pccare.vn/it/security-pages/authentication-attacks-and-countermeasures (дата звернення: 28.09.2020).
15. WAP Authentication. URL: https://www.ibm.com/support/knowledgecenter/en/SSB2MG_4.6.0/com.ibm.ips.doc/concepts/wap_authentication.htm (дата звернення: 29.09.2020).
16. Electronic signature authentication. URL: https://www.docusign.com/esignature/electronic-signature-authentication/ (дата звернення: 29.09.2020).
17. Anonymous identification with cancelable biometrics. URL: https://ieeexplore.ieee.org/document/5297678 (дата звернення: 29.09.2020).
18. Fractional biometrics: Safeguarding privacy in biometric applications.URL:https://www.researchgate.net/publication/220066921_Fractional_biometrics_Safeg uarding_privacy_in_biometric_applications (дата звернення: 29.09.2020).
19. Fake iris detection using structured light.URL: https://www.researchgate.net/publication/261153461_Fake_iris_detection_using_structured_light (дата звернення: 29.09.2020).
20. The Power of Personality The Comparative Validity of Personality Traits, Socioeconomic Status, and Cognitive Ability for Predicting Important Life Outcomes. URL:
21. https://www.researchgate.net/publication/237822262_The_Power_of_Personality_The_Comparative_Validity_of_Personality_Traits_Socioeconomic_Status_and_Cognitive_Ability_for_Predicting_Important_Life_Outcomes (дата звернення: 29.09.2020).
22. 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.
23. ISO/IEC 19785-1:2015 Information technology — Common BiometricExchange Formats Framework — Part 1: Data element specification [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.iso.org/ru/standard/66179.html.

24. 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.
25. 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.
26. ГОСТ Р ИСО/МЭК 19794-2-2005 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 2. Данные изображения отпечатка пальца»
27. ГОСТ Р ИСО/МЭК 19794-4-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 4. Данные изображения отпечатка пальцев».
28. ГОСТ Р ИСО/МЭК 19794-5-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица».
29. ГОСТ Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза».
30. Jain A. Introduction to Biometrics [Text] /A. Jain, A. Ross.// Handbook of Biometrics. Springer. – 2008. – p. 1–22.
31. Крахмалев А. К. Средства и системы контроля и управления доступом / А. К. Крахмалев. – М.: НИЦ «Охрана» ГУВО МВД России, 2003. –85 с.
32. Татарченко Н. В. Биометрическая идентификация в интегрированных системах безопасности/ Н. В. Татарченко, С. В. Тимошенко. – М.: Специальная техника, 2002. – 125 с.
33. Горбенко І.Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія./ І.Д. Горбенко, Ю.І. Горбенко –Харків: «Форт», 2010. – 608 с.
34. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія./ І.Д. Горбенко, Ю.І. Горбенко – Харків: «Форт», 2012.
35. Богуш В.М., Юдін О.К. Інформаційна безпека держави. - К.: «МК-Прес»,2005.- 432с.
36. Почерцов Г.Г. Информационные войны. Основы военно- коммуникативных исследований. - М.:. Рефл-бук, К.: Ваклер, 2000. - 576с.

37. Расторгуев СП. Информационная война. - М.: Радио и связь, 1999. -416с.

38. Расторгуев СП. Философия информационной войны. - М: Московский психолого-социальный институт, 2003. -486с.

39. Соснін О.В., Шименський Л.Є Про правові основи удосконалення системидержавного управління інформаційними ресурсами. Політологічний вісник. 36. наук,праць, №10. - К.: Т-во «Знання України», 2002. - с.212-219

40. Баранов А.А. Концептуальные вопросы информационной безопасности Украины

41. // Безопасность информации. - 1995, №2. - с.4-10

42. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. -СпБ.: БХВ - Петербург, 2003. -688с.

43. П. Браіловський М.М., Головень СМ. та інші. - Технічний захист інформації на об'єктах інформаційної діяльності/ За ред. Проф. В.О. Хорошка. -К.:ДУІКТ, 2007.

44. Петренко СА., Курбатов В.А. Политики информационной безопасности.