МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОІ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи

на тему:

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ АВТЕНТИФІКАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Виконав: студент 6 курсу, групи БСДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми
«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Філін М.Ю.
(прізвище та ініціали)
Керівник Власенко В.О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.

КИЇВ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Г.І. Гайдур
"___" _____ 2020 року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Філін Михайло Юрійович
(прізвище, ім'я, по батькові)

1. Тема роботи: «Технологія забезпечення автентифікації від несанкціонованого доступу в інформаційних системах»
керівник магістерської роботи Власенко В.О., к.т.н.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «13» жовтня 2020 року №230.
2. Строк подання студентом роботи 15 грудня 2020 р.
3. Вихідні дані до роботи:
Системний підхід для здійснення аналізу технології автентифікації, авторизації та адміністрування дій у інформаційній системі;
Дослідити варіанти реалізації методів автентифікації, що використовують паролі та PIN-коди, методів строгої автентифікації, а також методів біометричної автентифікації; розробити типові рекомендації щодо створення апаратно-програмних систем ідентифікації і автентифікації в ІС.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити:
4.1. Аналіз сучасних методів і засобів ідентифікації та автентифікації.
4.2. Застосування методів і засобів ідентифікації та автентифікації в банківських інформаційно-комунікаційних системах
4.3. Шляхи побудови раціональної системи ідентифікації та автентифікації в інформаційно-комунікаційних системах.
5. Перелік графічного матеріалу:

5.1 Типові схеми проведення заходів з ідентифікації/автентифікації.
5.2 Презентація доповіді, виконана в Microsoft PowerPoint.

6. Дата видачі завдання 09 жовтня 2020 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів	Примітка
1	2	3	4
1.	Уточнення постановки завдання	09.10.2020р.	вик.
2.	Аналіз літератури	12.10.2020р	вик.
3.	Обґрунтування вибору рішення	15.10.2020р	вик.
4.	Збір даних	06.11.2020р	вик.
5.	Аналіз сучасних методів і засобів ідентифікації та автентифікації	21.11.2020р	вик.
6.	Застосування методів і засобів ідентифікації та автентифікації в банківських інформаційно-комунікаційних системах	30.11.2020р	вик.
7.	Шляхи побудови раціональної системи ідентифікації та автентифікації в інформаційно-комунікаційних системах	05.12.2020р	вик.
8.	Апробація роботи на науково-методичному семінарі та науково-технічній конференції	09.12.2020р.	вик.
9.	Оформлення та друк пояснювальної записки	15.12.2020р.	вик.
10.	Оформлення презентацій	10.12.2020р.	вик.
11.	Отримання рецензій	22.12.2020р.	вик.
12.	Захист в ДЕК	18.01.2021р.	

Студент _____ Філін М.Ю.
(підпис) (прізвище та ініціали)

Керівник магістерської роботи _____ Власенко В.О.
(підпис) (прізвище та ініціали)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент ФілінМ.Ю. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
на тему: «Технологія забезпечення автентифікації від несанкціонованого доступу в інформаційних системах**».**

Магістерська робота і рецензія додаються.
Директор інституту ННІЗІ _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Філін М.Ю. за період навчання в інституті, на факультеті, у відділенні
(прізвище та ініціали студента)
ННІЗІ з 2019 року до 2021 року повністю виконав 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) _____ Черниш О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент Філін М.Ю. обрав тему роботи, метою якої було дослідити технологію забезпечення автентифікації від несанкціонованого доступу в інформаційних системах В роботі досліджено особливості застосування паролів та PIN-коди, методи строгої автентифікації, а також методів біометричної автентифікації Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Філін М.Ю. показав вміння самостійно розробив рекомендації, щодо застосування різних методів автентифікації Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Філіна Михайла Юрійовича на оцінку **«добре»** та присвоїти йому кваліфікацію 2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів.

Керівник магістерської роботи _____ Власенко В.О.
(підпис)

“____”_____2020 рік

Висновок кафедри про бакалаврську роботу

Магістерська робота розглянута. Студент Філін М.Ю.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії.
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)
_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)
“____”_____2020 рік

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента **Філіна Михайла Юрійовича**

на тему: **«Технологія забезпечення автентифікації від несанкціонованого доступу в інформаційних системах»**

Актуальність:

Позитивні сторони:

1. Зміст роботи відповідає завданню. Студент показав гарний рівень знань і ступінь підготовленості його до майбутньої роботи за фахом.
2. Обґрунтовано проведено дослідження різних методів автентифікації в інформаційних системах.
3. Текст викладено грамотне, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

Висновок: робота заслуговує оцінку "добре", а студент – Філін Михайло Юрійович гідний присвоєння кваліфікації2149.2 професіонал з організації інформаційної безпеки, викладач вищих навчальних закладів

Якість бакалаврської роботи	
виконано на замовлення підприємства	
виконано за тематикою НДР	
виконано з макетом	
має практичну цінність	*

Підпис рецензента

_____ _____
(П.І.Б.)

_____
(посада, науковий ступінь, вчене звання)

РЕФЕРАТ

Текстова частина магістерської роботи: 74 сторінок, 29 рисунків, 4 таблиць, 34 джерела.

Об'єктом дослідження в роботі процес ідентифікації та аутентифікації користувача у системі інформації.

Предметом – методи та моделі ідентифікації та аутентифікації користувачів в захищених інформаційно-комунікаційних системах.

Метою роботи є виявлення особливостей побудови та використання сучасних методів і засобів автентифікації/ідентифікації користувачів ІКС підприємства (організації) для забезпечення їх доступу до роботи в локальних і глобальних мережах.

Для досягнення поставленої мети в роботі: досліджено тенденції розвитку та напрямки впровадження сучасних технологій ідентифікації/автентифікації; розглянуто систему PassWindow як двофакторну некриптографічну технологію ідентифікації/автентифікації; розглянуто протокол Kerberos як провідну технологію ідентифікації/ автентифікації в банківських ІС; розроблено шляхи побудови раціональної системи ідентифікації та автентифікації в інформаційно-комунікаційних системах з використанням стандартів SAML, OpenID Connect та протоколу Kerberos.
В роботі вирішене завдання розробки методичних рекомендацій щодо підвищення надійності ідентифікації/автентифікації користувачів ІКС при роботі в локальних і глобальних мережах, засновані та правильному вибору правил політики безпеки, а також криптографічних методів.

Галузь застосування. Матеріали роботи можуть бути використані при розробці, впровадженні та експлуатації системи безпеки ІТ систем та мереж підприємства (організації).

Ключові слова: АВТЕНТИФІКАЦІЯ, АНАЛІЗ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, КРЕДИТКА КАРТКА, ПАРОЛЬ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ, СТРОГА АВТЕНТИФІКАЦІЯ, СЕРТИФІКАЦІЯ, ЦИФРОВИЙ ПІДПИС, PIN-КОД.

ЗМІСТ

Стор.

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ЕОМ — електронно-обчислювальна машина
ІКС — інформаційно-комунікаційна систем
КЗЗ — комплекс засобів захисту
КС — комп’ютерна система
КСЗІ — комплексна система захисту інформації
НСД — несанкціонований доступ
ПЗ — програмне забезпечення
ПЕОМ — персональна електронна обчислювальна машина
СЗІ — система захисту інформації
СУБД — система управління базами даних
CA — Certificate Authority (цент сертифікації)
DES — Data Encryption Standart (стандарт шифрування даних)
IP — Internet Protocol (міжмережний протокол)
KDC — Key Distribution Center (центр розподілу ключів)
PAP — Password Authentication Protocol (протокол парольної автентифікації)
PIN — Private Identification Number (персональний ідентифікаційний номер)
PKI — Public Key Infrastructure (інфраструктура відкритих ключів)
SSL. — Cecure Sockets Layer (рівень захисщкних сокетів)
SSO — Single Sign-On (система однократної автентифікації)
TCP — Transport Control Protocol (протокол управління передаванням)
VPN — Virtual Private Network (віртуальні приватні мережі)

ВСТУП

Актуальність теми. Інформаційно-комунікаційні системи та мережі – невід'ємна частина сучасного світу, бізнесу, політики, державних і регіональних органів. Головним завданням є забезпечення безпеки інформації, розмежування доступу, авторизація користувача і даних. Найбільш актуальним є питання безпеки інформації для корпоративних організацій і підприємств з розгалуженою структурою (філії, агентства).

Збільшення кількості користувачів, розширення спектру послуг, збільшення потоку передачі даних вимагає складної і точно побудованої системи управління мережею. Інформаційні потоки: електронна пошта, передачі конфіденційних даних, он-лайн спілкування, отримання віддаленого доступу до бази даних головного офісу і т.п. являються об'єктом несанкціонованого доступу з боку зловмисників. Саме тому при адмініструванні таких інформаційних мереж постають певні проблеми, а саме проблема захисту інформаційно-комунікаційних систем, що розуміє під собою стан захищеності властивостей ІР (цілісності, доступності, конфіденційності) системи, що забезпечує нормальний процес функціонування інформаційно-комунікаційних систем та мереж (ІКСМ) з умов гарантованого надання встановленого переліку послуг системи.

Кожний користувач сучасних інформаційно-комунікаційних систем декілька разів на день стикається з процедурами ідентифікації та аутентифікації. Ці процедури виконуються кожний раз, коли користувач вводить пароль для доступу до інформаційної системи, мережі, бази даних або при запуску прикладної програми. В результаті їх виконання оператор або отримує доступ до певних ресурсів інформаційної системи, або ні. Процедура аутентифікації користувача є обов'язковим етапом функціонування будь-якої сучасної інформаційно-комунікаційної системи та **отримує особливу актуальність**.

Мета і завдання дослідження. Мета даної дипломної роботи - виявлення особливостей побудови та використання сучасних методів і засобів ідентифікації/автентифікації користувачів ІКС підприємства (організації) для забезпечення їх доступу до роботи в локальних і глобальних мережах. Для досягнення поставленої мети необхідно вирішити такі завдання:

дослідити тенденції розвитку та напрямки впровадження сучасних технологій ідентифікації/автентифікації; дослідити систему PassWindow як двофакторну некриптографічну технологію

ідентифікації/автентифікації; дослідити протокол Kerberos як провідну технологію ідентифікації/
автентифікації в банківських ІКС;

розробити шляхи побудови раціональної системи ідентифікації та автентифікації в інформаційно-комунікаційних системах з використанням стандартів SAML, OpenID Connect та протоколу Kerberos.

Виходячи з такого, у роботі ***об'єктом дослідження*** є процес ідентифікації та аутентифікації користувача у системі інформації. ***Предметом*** – методи та моделі ідентифікації та аутентифікації користувачів в захищених інформаційнокомунікаційних системах. *Методи дослідження.* Для вирішення означеного вище наукового завдання в роботі використані методи математичного аналізу, теорії інформаційної безпеки, прогнозування та прийняття рішень.

Наукова новизна одержаних результатів. Новими науково-обґрунтованими результатами, які отримані в роботі, є:

алгоритм двофакторної автентифікації повідомлень у банківських системах PassWindow; процедури ідентифікації/автентифікації з використанням стандартів SAML,
OpenID Connect та протоколу Kerberos; процедура багатофакторної ідентифікації/автентифікації на трансакційному ідентифікаційному коді та службі коротких повідомлень.

Практичне значення одержаних результатів. Практичне значення мають:

- характеристики системи ідентифікації/автентифікації;
- основані принципи та засоби забезпечення ідентифікації/автентифікації ;
- рекомендації щодо підвищення ефективності інформаційної безпеки сучасного підприємства.

Матеріали роботи можуть бути використані при розробці, впровадженні та експлуатації системи безпеки ІТ систем та мереж підприємства (організації).

Апробація результатів дипломної роботи. Основні наукові результати дипломної роботи доповідалися та обговорювалися на двох науково-технічних конференціях (НТК),

1 АНАЛІЗ СУЧАСНИХ МЕТОДІВ І ЗАСОБІВ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

У зв’язку з загальним розповсюдженням комп’ютерних технологій все гострішою встає проблема захисту інформації в інформаційно-комунікаційних системах (ІКС). Тому дуже актуальними бачиться теоретичні розробки в області захисту комп’ютерної інформації та практичне їх застосування безпосередньо в певних конкретних комп’ютерних системах. Питання захисту інформації в комп’ютерних системах вирішується для того, щоб ізолювати нормально функціонуючу інформаційну систему від несанкціонованих управляючих дій і доступу сторонніх осіб або програм до комп’ютерних даних, що захищаються. Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури. Управління доступом – ефективний метод захисту інформації, регулюючий використовування ресурсів інформаційної системи, для якої розроблялася концепція інформаційної безпеки (ІБ). Методи і системи захисту інформації, що спираються на управління доступом, включають наступні функції захисту інформації в ІКС:

– ідентифікація користувачів, ресурсів і персоналу системи ІБ;

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

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

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

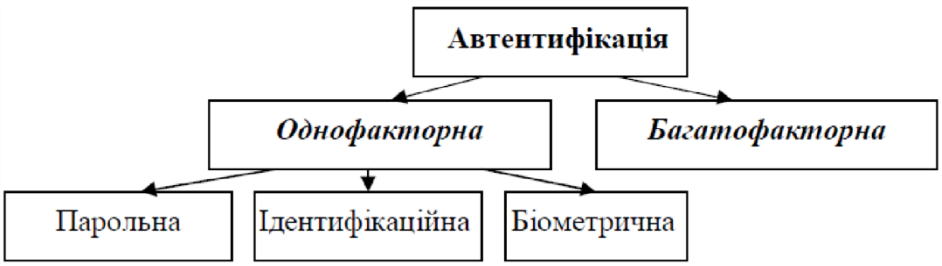
Як бачимо, система ідентифікації і аутентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу (НСД) до будь-якої інформаційно-комунікаційної системи. Під НСД до інформації розумітимемо доступ до інформації, що порушує встановлені правила розмежування доступу і здійснюваний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

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

(повідомити своє ім'я). Ідентифікація – це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). За допомогою аутентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова "аутентифікація" іноді використовують словосполучення "перевірка достовірності". Аутентифікація – це процедура, яка перевіряє, чи має користувач з пред'явленим ідентифікатором право на доступ до ресурсу. Ці процедури (ідентифікація та аутентифікація) нерозривно зв'язані між собою, оскільки спосіб перевірки визначає, яким чином і що користувач повинен пред'явити системі, щоб отримати доступ.

1.1 Огляд технологій ідентифікації/автентифікації користувачів в інформаційно-комунікаційних системах

Сьогодні існує декілька технологій ідентифікації та автентифікаці



користувачів в інформаційно-комунікаційних системах (рис.1.1).

Ідентифікація та автентифікація

Рис.1.1. Система технологій ідентифікації та автентифікації

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

1.1.1 Парольна ідентифікація/автентифікація користувачів в ІКС

Нещодавно парольна ідентифікація/автентифікації була ледве не єдиним способом визначення особистості користувача. І в цьому немає абсолютно нічого дивного. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні. Суть її зводиться до наступного. Кожен зареєстрований користувач якої небудь системи одержує набір персональних реквізитів (звичайно використаються пари логин-пароль). Далі при кожній спробі входу він повинен вказати свою інформацію. Ну а оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особистість та ідентифікує її.

При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте, по сукупності характеристик їх слід визнати найслабкішим засобом перевірки достовірності. Саме слабкий рівень парольного захисту є однією з основних причин уразливості комп'ютерних систем до спроб несанкціонованого доступу. Але поки символьний пароль – найпоширеніший спосіб ідентифікації і аутентифікації користувачів і ще довго їм залишатиметься.

Наступні заходи дозволять значно підвищити надійність парольного захисту:

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

– управління терміном дії паролів, їх періодична зміна;

– обмеження доступу до файлу паролів;

– обмеження кількості невдалих спроб входу в систему;

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

Для детальнішого розгляду принципів побудови парольних систем сформулюємо декілька основних визначень. Ідентифікатор користувача – деяка унікальна кількість інформації, що дозволяє розрізняти індивідуальних користувачів парольної системи (проводити їх ідентифікацію). Часто ідентифікатор також називають ім'ям користувача або ім'ям облікового запису користувача. Пароль користувача – деяка секретна кількість інформації, відома

тільки користувачу і парольній системі, яке може запам'ятати користувачем і пред'явлене для проходження процедури аутентифікації. Одноразовий пароль дає можливість користувачу однократно пройти аутентифікацію. Багаторазовий пароль може бути використаний для перевірки достовірності повторно.

Обліковий запис користувача – сукупність його ідентифікатора і його пароля. База даних користувачів парольної системи містить облікові записи всіх користувачів даної парольної системи. Під парольною системою розумітимемо програмно-апаратний комплекс, що реалізовує системи ідентифікації і аутентифікації користувачів ІКС на основі одноразових (рис.1.2,а) або багаторазових (рис.1.2,б) паролів.

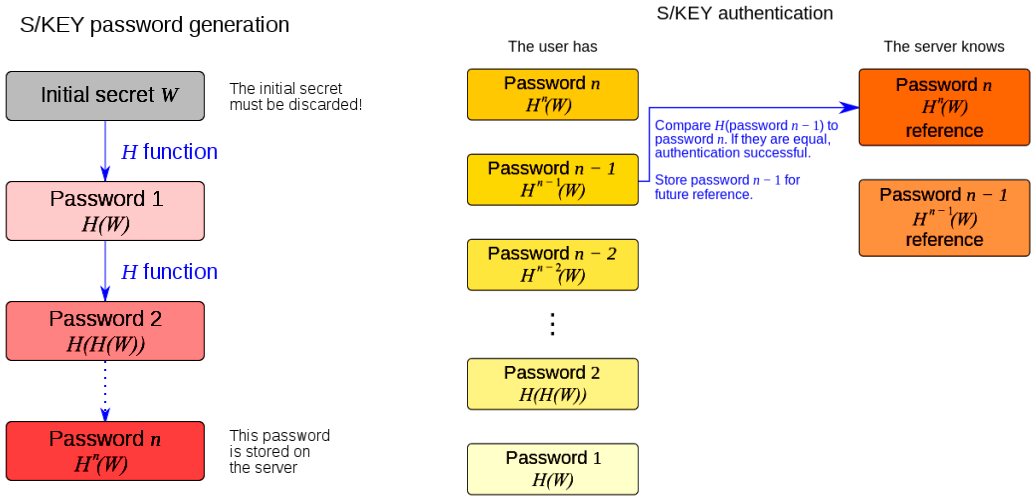


Рис.1.2. Система одноразових (а) та багаторазових (б) паролів

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

– інтерфейс користувача;

– інтерфейс адміністратора;

– модуль сполучення з іншими підсистемами безпеки; – база даних облікових записів.

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

Нижче перераховані типи загроз безпеки парольних систем.

1). Розголошування параметрів облікового запису через:

– підбір в інтерактивному режимі;

– підглядання;

– навмисну передачу пароля його власником іншій особі;

– захват бази даних парольної системи;

– перехоплення переданої по мережі інформації про пароль; – зберігання пароля в доступному місці.

2). Втручання у функціонування компонентів парольної системи через: – впровадження програмних закладок;

– виявлення і використовування помилок, допущених на стадії розробки; – виведення з ладу парольної системи.

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

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

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

– ввести пароль так, що його зможуть побачити сторонні;

– передати пароль іншій особі навмисно або під впливом помилки.

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

Важливим аспектом стійкості парольної системи є спосіб зберігання паролів в базі даних облікових записів. Можливі наступні варіанти зберігання паролів:

– у відкритому виді;

– у вигляді згорток (хешування); – зашифрованими за деяким ключем.

Найбільший інтерес представляють другий і третій способи, які мають ряд особливостей. Хешування (використання незворотної хеш-функції до будь-якої інформації перетворює її на унікальний код) не забезпечує захист від підбору паролів по словнику у разі отримання бази даних зловмисником. При виборі алгоритму хешування, який буде використаний для розрахунку згорток паролів, необхідно гарантувати неспівпадіння значень згорток, отриманих на основі різних паролів користувачів. Крім того, слід передбачити механізм, що забезпечує

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

При шифруванні паролів особливе значення має спосіб генерації і зберігання ключа шифрування бази даних облікових записів. Перерахуємо деякі можливі варіанти: ключ генерується програмно і зберігається в системі, забезпечуючи можливість її автоматичного перезавантаження; ключ генерується програмно і зберігається на зовнішньому носієві, з якого прочитується при кожному запуску; ключ генерується на основі вибраного адміністратором пароля, який вводиться в систему при кожному запуску. У другому випадку необхідно забезпечити неможливість автоматичного перезапуску системи, навіть якщо вона виявляє носій з ключем. Для цього можна зажадати від адміністратора підтверджувати продовження процедури завантаження, наприклад, натисненням клавіші на клавіатурі. Найбільш безпечне зберігання паролів забезпечується при їх хешуванні і подальшому шифруванні отриманих згорток, тобто при комбінації другого і третього способів.

Враховуючи, що користувачі нерідко вибирають недостатньо стійкі паролі, можна зробити висновок, що отримання бази даних облікових записів або перехоплення переданого по мережі значення згортки пароля представляють серйозну загрозу безпеці парольної системи. В більшості випадків аутентифікація відбувається в розподілених системах і пов'язана з передачею по мережі інформації про параметри облікових записів користувачів. Якщо інформація, що передається по мережі в процесі аутентифікації, не захищена належним чином, виникає загроза її перехоплення зловмисником і використання для порушення захисту парольної системи. Відомо, що багато комп'ютерних систем дозволяють перемикати мережевий адаптер в режим прослуховування адресованого іншим одержувачам мережевого трафіку в мережі, заснованій на передачі пакетів даних. Нагадаємо основні види захисту мережевого трафіку: фізичний захист мережі; кінцеве шифрування; шифрування пакетів.

Поширені наступні способи передачі по мережі паролів:

- у відкритому вигляді;
- зашифрованими;
- у вигляді згорток;

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

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

– перехоплення і повторне використання інформації;

– перехоплення і відновлення паролів;

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

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

Схеми аутентифікації "з нульовим знанням" або "з нульовим розголошуванням" вперше з'явилися в середині 80-х – на початку 90-х років. Їх основна ідея полягає в тому, щоб забезпечити можливість одному з пари суб'єктів довести істинність деякого твердження другому, при цьому не повідомляючи йому ніякої інформації про зміст самого твердження. Наприклад, перший суб'єкт (що "доводить") може переконати другого ("перевіряючого"), що знає певний пароль, насправді не передаючи тому жодної інформації про сам пароль. Ця ідея і відбита в терміні "доказ з нульовим розголошуванням". Стосовно парольного захисту це означає, що якщо на місці перевіряючого суб'єкта виявляється зловмисник, він не отримує ніякої інформації про доказуване твердження і, зокрема, про пароль. Загальна схема процедури аутентифікації з нульовим розголошуванням складається з послідовності інформаційних обмінів (ітерацій) між двома учасниками процедури, по завершенню якої перевіряючий із заданою ймовірністю робить правильний висновок про істинність твердження, що перевіряється. Із збільшенням числа ітерацій зростає ймовірність правильного розпізнавання істинності (або помилковості) твердження.

Ще одним способом підвищення стійкості парольних систем, пов'язаної з передачею паролів по мережі, є застосування одноразових (one - time) паролів. Загальний підхід до застосування одноразових паролів заснований на послідовному використанні хеш-функції для розрахунку чергового одноразового пароля на основі попереднього. На початку користувач одержує впорядкований список одноразових паролів, останній з яких також зберігається в системі

аутентифікації. При кожній реєстрації користувач вводить черговий пароль, а система розраховує його згортку і порівнює з еталоном, що зберігається у системі. У разі співпадіння користувач успішно проходить аутентифікацію, а введений ним пароль зберігається для використання як еталон при наступній реєстрації. Захист від мережевого перехоплення в такій схемі заснований на властивості необоротності хешфункції. Найбільш відомі практичні реалізації схем з одноразовими паролями – це програмний пакет S/KEY. і розроблена на його основі система OPIE.

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

1.1.2 Апаратна ідентифікація/автентифікація користувачів в ІКС

Цей принцип ідентифікації/автентифікації ґрунтується на визначенні особистості користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні. Природно, мова йде не про звичні для більшості людей ключі, а про спеціальні електронні. На даний момент найбільше поширення одержали два типи пристроїв: різноманітні карти (проксіміті-карти, смарт-карти, магнітні карти і т.д.) та так званні токени (token), які підключаються безпосередньо до одного з портів комп'ютера. Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм, зазвичай невеликих розмірів для зручності його носіння з собою. До складу електронних систем ідентифікації і аутентифікації входять (рис.1.3):

Рис.1.3. Токени

1). Переносні токени:

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

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

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

– PIN/синхронні.

Таблиця 1.1

Продукт	Основные преимущества	Основные недостатки
USB-токены	Мобильность — токен можно использовать на любом компьютере, где есть USB-порт. Поддержка большого числа приложений ИТ-безопасности. Очевидная принадлежность токена пользователю	Требуется установка ПО пользователя
Смарт-карты	Высокий уровень безопасности. Компактность. Поддержка большого числа приложений	Требуется установка ПО пользователя. Требуется считывающее устройство
USB-токены со встроенным чипом	Высокий уровень безопасности. Мобильность. Поддержка большого числа приложений. Очевидная принадлежность токена пользователю	Требуется установка ПО пользователя
OTP-токены	Мобильность. Легкость в использовании. Не требуется установка ПО пользователя	Ограниченный круг поддерживаемых приложений Требуется сервер аутентификации. Ограниченное время эксплуатации в связи с использованием батарейки
Гибридные токены	Мобильность. Поддержка большого числа приложений. Не требуется установка ПО пользователя для применения одноразовых паролей (OTP). Очевидная принадлежность токена пользователю	Ограниченное время эксплуатации в связи с использованием батарейки (кроме тех случаев, когда пользователь может заменить батарейку самостоятельно)
Программные токены	Не требуется аппаратное устройство	Секретный ключ слабо защищен. Ограниченный круг поддерживаемых приложений. Требуется сервер аутентификации

2). Різноманітні карти – це пристрої, схожі на переносні аутентифікатори, але складніші по своєму складу. Карти бувають:

– пасивні (карти з пам'яттю); – активні (інтелектуальні карти).

Останні включають CPU, мініатюрну операційну систему, годинник, програми на ROM (readonly memory – пам'ять тільки для читання), буферну пам’ять (RAM) для криптографічних розрахунків, незалежну пам'ять або EEPROM (Electrically Erasable Programmable Read-Only Memory) для зберігання цифрових ключів. За допомогою смарт-карти проводиться розрахунок одноразових паролів і здійснюється взаємодія з пристроєм через картридер. Після введення PIN-кода картридер сам запрошує смарткарту, і подальший процес протікає без участі людини, завдяки чому можна використовувати достатньо довгі

ключі.

Карт досить багато, і працюють вони по різних принципах. Так, наприклад, досить зручні у використанні безконтактні карти (їх ще називають проксіміті-карти), які дозволяють користувачам проходити ідентифікацію як у комп'ютерних системах, так й у системах доступу в приміщення. Найбільш надійними вважаються смарт-карти – аналоги звичних багатьом людям банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-кодом і т.д.Що таке USB-ключ, розглянемо на прикладі eToken від компанії Aladdin Software. eToken – персональний засіб аутентифікації і зберігання даних, що апаратно підтримує роботу з цифровими сертифікатами і електронними цифровими підписами (ЕЦП).

Рис. 1.4. Цифрові підписи

eToken може бути виконаний у вигляді USB-ключа або стандартної смарт-карти. eToken підтримує роботу і інтегрується зі всіма основними системами і додатками, що використовують технології смарт-карт або PKI (Public Key Infrastructure).

Основне призначення:

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

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

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

eToken як засіб аутентифікації підтримується більшістю сучасних операційних систем, бізнес-додатків і продуктів по інформаційній безпеці. Можливості застосування:

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

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

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

– системи електронної торгівлі, «клієнт-банк», «домашній банк»; – захист комп'ютерів;

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

– клієнт-банк, home-банк.

eToken забезпечує: аутентифікацію користувачів за рахунок використання криптографічних методів; безпечне зберігання ключів шифрування і ЕЦП, а також закритих ключів цифрових сертифікатів для доступу до захищених корпоративних мереж і інформаційних ресурсів; мобільність користувача і можливість безпечної роботи з конфіденційними даними в недовіреному середовищі (наприклад, на чужому комп'ютері) за рахунок того, що ключі шифрування і ЕЦП генеруються ключем eToken апаратно і не можуть бути перехоплені; безпечне використання – скористатися ключем eToken може тільки його власник, що знає PIN-код ключа; реалізацію як західних та російських, так і вітчизняних стандартів на шифрування і ЕЦП; зручність роботи – ключ виконаний у вигляді брелока зі світловою індикацією режимів роботи і безпосередньо підключається до USB-портів, якими зараз оснащено 100% комп'ютерів, не вимагає спеціальних зчитувачів, блоків живлення, проводів і т.п.; використання одного ключа для вирішення безлічі різних завдань – входу в комп'ютер, входу в мережу, захисту каналу, шифрування інформації, ЕЦП, безпечного доступу до

захищених розділів Web-сайтів, інформаційних порталів і тому подібне. Безконтактні смарт-карти розділяються на ідентифікатори Proximity і смарт-карти, що базуються на міжнародних стандартах ISO/IEC 15693 і ISO/IEC 14443. У основі більшості пристроїв на базі безконтактних смарт-карт лежить технологія радіочастотної ідентифікації. Основними компонентами безконтактних пристроїв є чип і антена. Ідентифікатори можуть бути як активними (з батареями), так і пасивними (без джерела живлення). Ідентифікатори мають унікальні 32/64 розрядні серійні номери.

Системи ідентифікації на базі Proximity криптографічно не захищені, за винятком спеціальних рекомендованих систем. USB-ключі працюють з USB-портом комп'ютера.

Виготовляються у вигляді брелоків. Кожний ключ має 32/64 розрядний серійний номер.

USB-ключі, представлені на ринку:

- eToken R2, eToken Pro – компанія Aladdin Knowledge Systems;
- iKey10xx, iKey20xx,iKey 3000 – компанія Rainbow Technologies;
- ePass 1000 ePass 2000 – фірма Feitian Technologies; – ruToken – розробка компанії «Актив» і фірми «АНКАД»; – uaToken – компанія ТОВ «Технотрейд».

USB-ключі – це спадкоємці смарт-карт, через це структури USB-ключів і смарт-карт ідентичні.

Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. І дійсно, у пам'яті токенів можуть зберігатися ключі, підібрати які досить складно. Крім того, в них реалізовано чимало різних захисних механізмів, а вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції. Головна небезпека у застосуванні апаратної ідентифікації криється у можливості крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані. Другий мінус розглянутої технології – ціна. Взагалі, останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. Проте, для введення в експлуатацію системи такої ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом де які типи ключів можуть зношуватися, крім того,

вони можуть бути загублені й т.д. Тобто апаратна ідентифікація вимагає деяких експлуатаційних витрат.

1.1.3 Біометрична ідентифікація/автентифікація користувачів в ІКС

Біометрія – це ідентифікація людини по унікальним, властивим тільки їй біологічним ознакам. Тобто, можна сказати, що біометричні технології споконвічно розроблялися для точного встановлення особистості людини. А тому рішення використати їх в області інформаційної безпеки виглядає цілком логічним. Причому даний напрямок розвивається дуже активно. Сьогодні експлуатується вже більше десятка різних біометричних ознак. Причому для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів. Так що користувачам, що вирішили використати біометричну ідентифікацію, є із чого вибрати.

Біометрична ідентифікація/автентифікації – це спосіб ідентифікації особи по окремих специфічних біометричних ознаках, властивих конкретній людині. Сучасний рівень розвитку комп'ютерних технологій дозволив використовувати подібні ознаки як основу для ідентифікації людини і ухвалення рішення про можливість доступу до ресурсів комп’ютерних систем. Серед біометричних механізмів ідентифікації можна виділити такі:

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

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

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

Серед статичних методів в задачах ідентифікації користувача комп’ютерних систем використовуються наступні:

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

Рис.1.5. Пальцевий та долонний дактилоскопічні сканери

2. Ідентифікація по розташуванню вен на долоні. Прилад, який прочитує інформацію в цьому випадку, є інфрачервона камера. В результаті на вході програми при формуванні цифрового коду з'являється малюнок вен на руці людини. Не потребує контакту людини з пристроєм для сканування. Має високі показники надійності і достовірності.

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

4. Ідентифікація по райдужній оболонці ока. Малюнок райдужної оболонки ока – унікальний для кожної людини. В цьому методі важлива не тільки спеціальна камера, але і надійне програмне забезпечення. Адже саме за допомогою програмного забезпечення із зображення виділяється малюнок потрібної нам райдужної оболонки.

Цей метод є одним з найбільш точних серед біометричних методів.

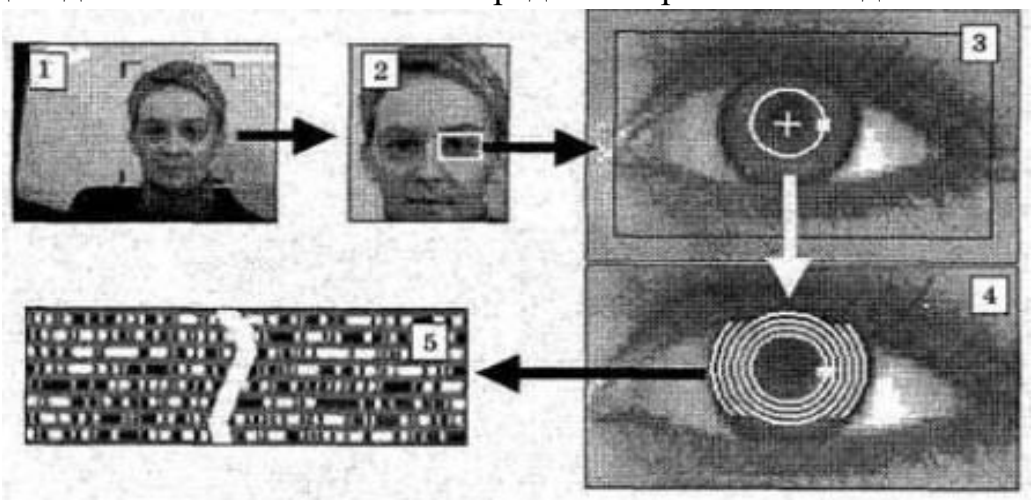
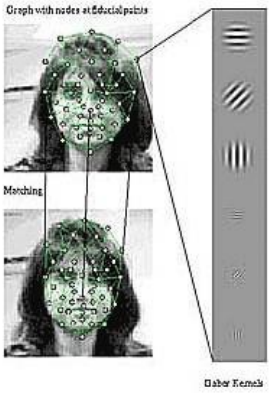


Рис. 1.6. Аутентифікація за райдужною оболонкою ока

5. Ідентифікація за формою кисті руки. Цей метод ґрунтується на розпізнаванні геометричних особливостей кисті руки. Спеціальний сканер формує тривимірний малюнок кисті. При аналізі цього малюнка виконуються вимірювання, за допомогою яких формується відповідний цифровий код.

6. Ідентифікація за формою обличчя.



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

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

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

2. Ідентифікація по почерку. При ідентифікації за даним методом звичайно досліджується підпис людини. Перевіряються такі динамічні характеристики, як: графічні параметри, сила натиску на поверхню, швидкість нанесення підпису. На основі цих характеристиках і будується цифровий код.

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

При всьому теоретичному різноманітті можливих біометричних методів тих, що застосовуються на практиці серед них небагато. Основних методів три – розпізнавання по відбитку пальця, по зображенню особи (двомірному або

тривимірному), по райдужній оболонці та по сітківці ока. На сьогоднішній день всі біометричні технології є імовірнісними і нерідко дана обставина служить основою для критики біометрії.

Важко не погодитися, що біометричні технології надійніші і зручніші за ті засоби захисту, які широко застосовувалися до теперішнього часу. Але, незважаючи на активну діяльність протягом останніх років у напрямку розробки та вдосконалення методів ідентифікації користувачів з метою управління доступом до ресурсів інформаційних систем, надійність та стійкість існуючих систем недостатня для потреб сьогоднішнього дня. Головним достоїнством біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує. Правда, сьогодні вже відомо кілька способів обману дактилоскопічних сканерів. Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або може бути використана фотографія пальця зареєстрованого користувача. Втім, треба зізнатися, що сучасні пристрої значно стійкіші по відношенню до подібної фальсифікації. Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входить до цієї системи, необхідно придбати власний сканер. Звичайно, останнім часом ціни на біометричні пристрої постійно знижуються. Крім того, не дуже давно з'явилися миші й клавіатури з вбудованими дактилоскопічними сканерами.

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

Останнім часом набуває поширення комплексна або багатофакторна ідентифікація.

1.1.5 Багатофакторна ідентифікація/автентифікація користувачів в ІКС

Багатофакторну ідентифікацію/автентифікацію не можна виділити в окремий вид. Тим не менш в таких системах для визначення особи користувача в ІКС застосовується відразу кілька параметрів. Причому комбінуватися ці параметри можуть у довільному порядку. Втім, сьогодні в переважній більшості випадків використовується тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися підбора його пароля зловмисником (без електронного ключа вона працювати не буде), а також крадіжки токена (він не

буде працювати без пароля). Втім, у деяких системах застосовуються максимально надійні процедури ідентифікації. У них одночасно використаються паролі, токени й біометричні характеристики людини.

Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і тим самим підвищує безпеку. На сьогодні існують комбіновані системи наступних типів:

– системи на базі безконтактних смарт-карт і USB-ключів; – системи на базі гібридних смарт-карт; – біоелектронні системи.

Безконтактні смарт-карти і USB-ключі. У корпус брелока USB-ключа вбудовується антена і мікросхема для створення безконтактного інтерфейсу. Це дозволить організувати управління доступом в приміщення і до комп'ютера, використовуючи один ідентифікатор. Дана схема використовування ідентифікатора може виключити ситуацію, коли співробітник, покидаючи робоче місце, залишає USB-ключ в роз'ємі комп'ютера, що дозволить працювати під його ідентифікатором. У разі ж, коли не можна вийти з приміщення, не використовуючи безконтактний ідентифікатор, даної ситуації вдасться уникнути. На сьогодні найбільш поширено два ідентифікатори подібного типу:

– RfiKey – компанія Rainbow Technologies;
– eToken PRO RM – компанія Aladdin Software Security R.D.

eToken RM – USB-ключі і смарт-карти eTokenPRO, доповнені пасивними RFID-мітками. RFID-технологія (Radio Frequency Identification, радіочастотна ідентифікація) є найпопулярнішою на сьогодні технологією безконтактної ідентифікації. Радіочастотне розпізнавання здійснюється за допомогою закріплених за об'єктом так званих RFIDміток, несучих ідентифікаційну і іншу інформацію. З сімейства USB-ключів eToken RFID-міткою може бути доповнений тільки eToken PRO/32K.

Гібридні смарт-карти. Гібридні смарт-карти містять різнорідні чипи. Один чип підтримує контактний інтерфейс, інший – безконтактний. Як і у разі гібридних USBключів, гібридні смарт-карти вирішують дві задачі: доступ в приміщення і доступ до комп'ютера. Додатково на карту можна нанести логотип компанії, фотографію співробітника або магнітну смугу, що робить можливим повністю замінити звичайні пропуски і перейти до єдиного "електронного пропуску". Смарт-карти подібного типу розробляють багато компаній: HID Corporation, Axalto, GemPlus, Indala, Aladdin Knowledge Systems і ін. У Росії компанією Aladdin Software Security R.D. розроблена технологія виробництва

гібридних смарт-карт eToken Pro/SC RM. В них мікросхеми з контактним інтерфейсом eToken Pro вбудовуються в безконтактні смарт-карти. Смарткарти eToken PRO можуть бути доповнені пасивними RFID-мітками виробництва HID/ISOProx II, EM-Marine (частота 125 кГц), Cotag (частота 122/66 кГц), Ангстрем/КИБИ-002 (частота 13,56 Мгц), Mifare і інших компаній. Вибір варіанту комбінування визначає замовник.

Біоелектронні системи (рис.1.7). Як правило, для захисту комп'ютерних систем від несанкціонованого доступу застосовується комбінація з двох систем – біометричної і контактної на базі смарт-карт або USB-ключів. Найчастіше як біометричні системи застосовуються системи розпізнавання відбитків пальців.

Рис.1.7. Багатофакторні біометричні термінали

При збігу відбитку з шаблоном дозволяється доступ. До недоліків такого способу ідентифікації можна віднести можливість використовування муляжу відбитку. Досягти підвищення надійності та точності автоматизованих систем ідентифікації користувачів можна за рахунок об’єднання використання біометричних характеристик разом з класичними способами ідентифікації користувачів (наприклад, парольний захист, PINкод, використання різноманітних карт і т.д.).

Актуальною бачиться проблема розробки і дослідження комплексних систем, що використовують для прийняття рішення доступу до інформаційних систем декілька біометричних характеристик користувача (наприклад, використовувати разом особливості клавіатурного почерку, голосу, динаміки роботи користувача з маніпулятором «миша» або використання відбитків декількох пальців і т.д.). Деякі виробники вже розпочали інтеграцію двох методів розпізнавання обличь, включаючи дво- і тривимірні зображення.

1.2 Міжнародні стандарти по криптографічним протоколам ідентифікації/автентифікації

Основним міжнародним стандартом по криптографічним протоколам аутентифікації є стандарт Міжнародної організації по стандартизації та Міжнародної електротехнічної комісії ISO / IEC 9798 - Information technology – Security techniques -
Entity authentication mechanisms, що складається з п'яти частин (табл.1.2):

ISO / IEC 9798-1 - «General Model»;

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

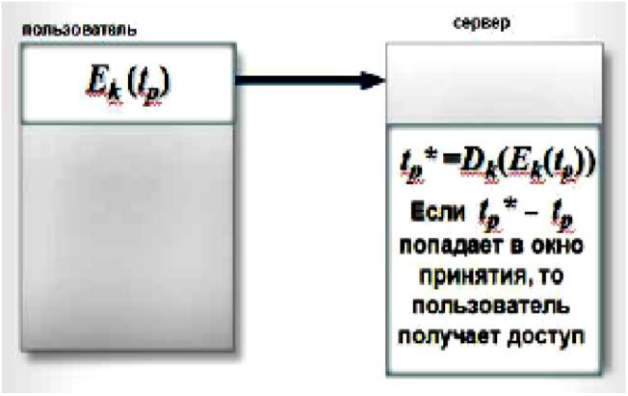
ISO / EEC 9798-3 - «Entity authentication using a public-key algorithm »; ISO / IEC 9798-4 - «Mechanisms using a cryptographic check function»; ISO / IEC 9798-5 - «Mechanisms using zero knowledge techniques».

Таблиця 1.2

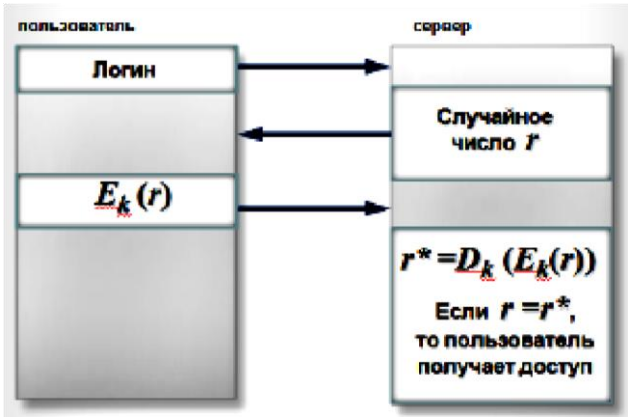
Standard	Title	Status	Abstract
ISO/IEC 9798-1	**Entity authentication** Part 1: General	3rd ed. 2010	*ISO/IEC 9798 specifies several kinds of entity authentication mechanisms that an entity to be authenticated proves its identity by showing its knowledge of a secret.*
-2	Part 2: Mechanisms using symmetric encipherment algorithms	3rd ed. 2008 *Under revision*	
-3	Part 3: Mechanisms using digital signature techniques	2nd ed. 1998 (+Amd1) *Under revision*	
-4	Part 4: Mechanisms using cryptographic check function	2nd ed. 1999	
-5	Part 5: Mechanisms using zero knowledge techniques	3rd ed. 2009	
-6	Part 6: Mechanisms using manual data transfer	2nd ed. 2010	
ISO/IEC 20009-1	**Anonymous entity authentication** Part 1: General	1st ed. 2013	*ISO/IEC 20009 specifies anonymous entity authentication mechanisms in which a verifier makes use of a group signature scheme to authenticate the entity with which it is communicating, without knowing this entity's identity, and which based on blind signatures and weak secrets.*
-2	Part 2: Mechanisms based on signatures using a group public key	1st ed. 2013	
-3	Part 3: Mechanisms based on blind signatures	*Under development*	
-4	Part 4: Mechanisms based on weak secrets	*Under development*	

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

Стандартом ISO / IEC 9798-2 передбачені три способи аутентифікації (зірочками в таблицях позначені необов'язкові компоненти повідомлень):

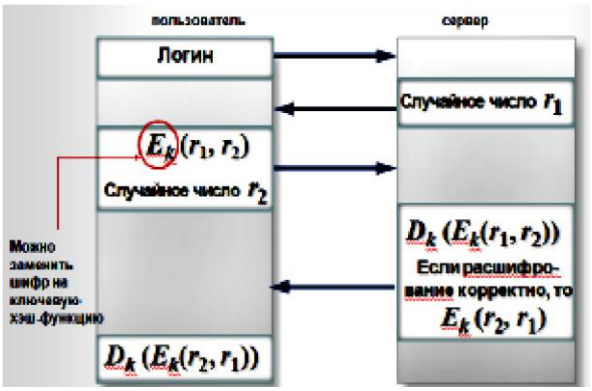


1. Одностороння аутентифікація, заснована на мітці часу. Якщо у претендента і перевіряючого є системний годинник, немає необхідності надсилати запит. претендент відразу може направити повідомлення з включеною в нього міткою часу, а перевіряючий - звірити мітку з показаннями свого годинника.



2. Одностороння аутентифікація з використанням випадкових чисел. В якості запиту перевіряючий посилає випадкове число, згенеровано з допомогою генератора псевдовипадкових чисел. Отримавши запит, претендент обчислює відповідь на нього - зашифровує з допомогою алгоритму симетричного

шифрування отримане випадкове число і (якщо необхідно) ідентифікатор. перевіряючий розшифровує отриманий шифротекст і перевіряє структуру запиту. Якщо вона вірна, він приймає претендента.



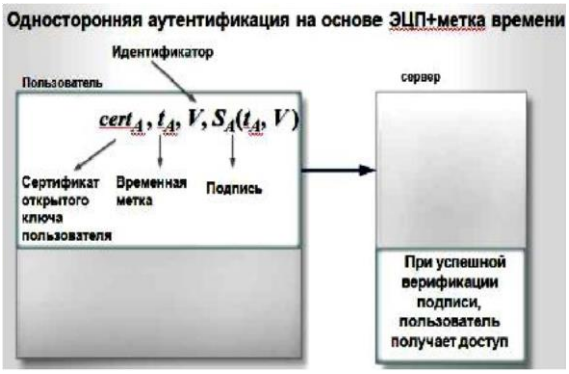
3. Взаємна аутентифікація з використанням випадкових чисел. Відмінність цього протоколу від попереднього в тому, що тут кожен з учасників по черзі виконує ролі перевіряючого і претендента, т. е. вони перевіряють аутентічнсть один одного.

Протокол взаємної аутентифікації - це по суті два протоколи односторонньої

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

Протоколи «запит - відповідь» з використанням асиметричних криптосхем

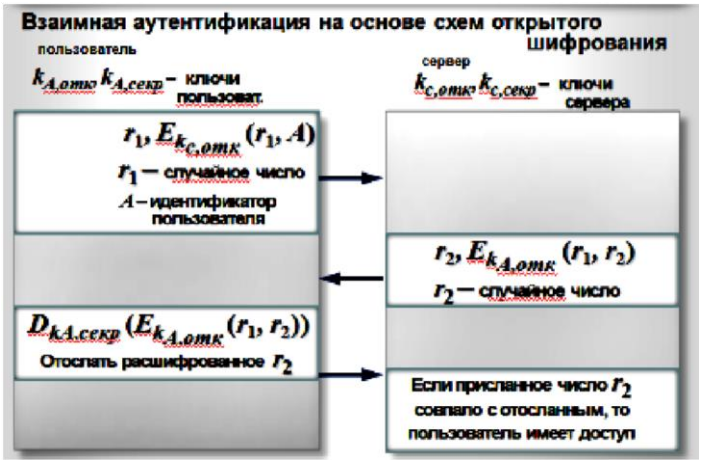
Такі протоколи можна розділити на дві групи: протоколи з використанням ЕЦП і протоколи з використанням схем відкритого шифрування. В стандарті ISO / IEC9798-3 рекомендовані: 1) протоколи з використанням схем цифрового підпису:



В описах протоколів зустрічаються позначення $cert_A$ сертифікатів відкритих ключів цифрового підпису відповідних учасників протоколу, тобто структури даних, містять їх ідентифікатори, відкриті ключі і іншу службову інформацію, завірену цифровим підписом засвідчувального центру. Детальніше метод сертифікації відкритих ключів буде розглянуто пізніше. Протоколи, подібні описаним вище, використовуються також в стандарті Міжнародного телекомунікаційного союзу ITU X.509. У ньому описані протоколи аутентіфікації, суміщені з протоколами обміну ключами.

2) протоколи з використанням схем відкритого шифрування.

Загрози безпеки ІКС можна поділити на мережеві атаки (інформація, яка надходить з віддаленого агента) і локальні атаки, які походять від шкідливих програм, вже встановлених на системі клієнта, наприклад, троянів, руткітів тощо. Часто оцінки безпеки автентифікації зосереджені переважно на мережевих атаках, припускають, що користувальницький термінал (тобто настільний комп'ютер, ноутбук або мобільний пристрій) є захищеною платформою. Проте нерідко зловмисник отримує повний доступ до ПК жертви через приховані процеси зв'язку, які залишилися від шкідливих програм, що використовують невиправлені діри в безпеці ліцензійного програмного забезпечення.



Типовими методами атак на протоколи аутентифікації:

1. Самозванство (impersonation) - один користувач намагається видати себе за іншого.

2. Повторна передача (replay attack) – повторна передача колишніх аутентифікаційних даних будь-яким користувачем.

3. Підміна боку аутентификационного обміну (Interleaving attack) - зловмисник в ході атаки має можливість модифікувати проходить через нього трафік.

4. Відображення передачі (reflection attack) - один з варіантів атаки підміни, коли в рамках даного Сенсу зловмисник пересилає назад перехоплену інформацію.

5. Вимушена затримка (forced delay) – зловмисник перехоплює деяку інформацію і передає її через деякий час.

6. Атака з вибіркою тексту (chosen-text attack) - зловмисник перехоплює трафік і намагається отримати інформацію про довготривалі ключах.

Атаки на протоколи аутентифікації та шляхи їх поводження

Тип атаки	Контрмеры
Повторная передача	Использование протоколов «запрос – ответ», меток времени, случайных чисел, вставка идентифицирующей информации в ответы
Подмена стороны	Связывание всех сообщений в рамках одной сессии протокола (например, используя одноразовый и уникальный идентификатор во всех сообщениях)
Отражение	Использование идентификаторов сторон в передаваемых сообщениях, построение протокола таким образом, чтобы каждое сообщение имело отличную от других форму
Выборка текста	Использование протоколов, обладающих свойством доказательства с нулевым разглашением знания, включение в каждое сообщение случайных чисел
Задержка передачи	Комбинация меток и случайных чисел

Висновки до першого розділу

На основі аналізу загроз інформаційній безпеці та існуючих засобів ідентифікації та аутентифікації користувачів інформаційних систем, можна впевнено сказати, що парольний захист на сьогодні є одним з найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах і системах, так і в мережах світового масштабу. Проте без використовування інших механізмів захисту парольний захист, сам по собі, не є надійним, оскільки не може забезпечити потрібного захисту. Досить розповсюдженими в якості ідентифікаторів є також різноманітні електронні ключі (токени, карти і т.і.). Але слід зауважити, що останнім часом все більшого поширення набувають системи ідентифікації, які використовують біометричні характеристики людини при вирішенні задачі доступу до інформаційних систем.

Таким чином, розглянувши технології апаратної (або електронної), парольної, біометричної ідентифікації та аутентифікації можна зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде саме вживання систем комплексної (або багатофакторної) ідентифікації та аутентифікації, що дозволить уникнути людських помилок, зв'язаних із застосуванням слабких паролів і посилити вимоги до парольної аутентифікації.

Щодо вибору системи ідентифікації безпосередньо в кожній окремій ситуації, користувач повинен: об’єктивно оцінити співвідношення цінності інформації, що захищається, та вартості програмно-апаратного забезпечення ідентифікації/ аутентифікації, яке обираєте (включаючи супровід); оцінити зручність у використанні (контактні, безконтактні) та сприйняття обраного підходу користувачами; визначити потрібний рівень захищеності («що» і від «кого» потрібно захищати). Але безперечною порадою є обов’язкове використання комплексної системи ідентифікації, яка поєднує декілька підходів до вирішення задач доступу до інформаційних ресурсів ІКС.

2 ЗАСТОСУВАННЯ МЕТОДИ ТА ЗАСОБИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

Сучасні системи ідентифікації/автентифікації базуються на пред'явленні користувачем комп'ютера статичної пари ідентифікатор/пароль. Однак такі пари можуть бути скомпрометовані через халатність користувачів або можливості підбору паролів зловмисником. Значні інтервали часу, протягом яких пароль та ідентифікатор залишаються незмінними, дають змогу застосувати різні методи їх перехоплення і підбору. Для того, щоб підвищити захищеність комп'ютерної системи, адміністратори обмежують термін дії паролів, але в типовому випадку цей термін становить тижні та місяці, що цілком достатньо для зловмисника. Радикальним рішенням є застосування двофакторної автентифікації, коли система просить користувача надати їй "те, що ти знаєш" (ім'я і, можливо, якийсь PIN-код), і "те, що у тебе є"– який-небудь апаратний ідентифікатор, що асоціюється з цим користувачем. Останнім часом такі системи автентифікації широко використовують у банківських системах.

2.1 Система PassWindow як двофакторна некриптографічна технологія ідентифікації/автентифікації в банківських ІКС

Особливе місце серед систем ідентифікації/автентифікації займає система автентифікації PassWindow, яку застосовують великі банки Малайзії, Чилі, Туреччини, Індонезії та Австралії. Вона належить до класу двофакторних не криптографічних систем ідентифікації/автентифікації й основана на тому, що користувач крім того, що знає пароль доступу до певного імені користувача ("логіна"), володіє й інструментом для отримання відповідного йому ключа доступу. Останнім може слугувати збережений на комп'ютері електронний сертифікат безпеки або код, який надходить на особистий телефон як СМС з кодом підтвердження, або ж відбиток пальця, знятий електронним пристроєм.

Методи строгої (двофакторної) автентифікації найчастіше використовуються у фінансовій сфері, але в принципі можуть застосовуватися практично в будь-якій області. Основні способи побудови систем двофакторної автентифікації поділяються на:

1. Програмне забезпечення для ідентифікації конкретного ПК. У комп'ютер інсталюється спеціальна програма, що встановлює в ньому

криптографічний маркер. Тоді в процесі автентифікації задіяні два фактори: пароль і маркер, вбудований у ПК. Оскільки маркер постійно є на комп'ютері, користувачеві для входу в систему потрібно буде лише ввести логін і пароль.

2. Біометрія. Використання біометрії як вторинного фактора ідентифікації полягає в ідентифікації фізичних характеристик людини (відбиток пальця, райдужна оболонка ока тощо).

3. Одноразовий електронний mail- або sms-пароль. Використати як вторинний фактор ідентифікації такий пароль можливо, відправивши другий одноразовий пароль на зареєстровану адресу електронної пошти або на мобільний телефон.

4. Токен з одноразовим паролем. Користувачу видається пристрій, що генерує паролі, які постійно змінюються. Саме ці паролі і вводять користувачі на додаток до звичайних паролів під час автентифікації.

5. Контроль ззовні. Цей метод передбачає дзвінок з банку на попередньо зареєстрований телефонний номер. Користувач повинен ввести пароль з телефону, і лише після цього він отримає доступ до системи.

6. Ідентифікація з використанням гаджетів. Таку ідентифікацію здійснюють, помістивши криптографічну мітку на будь-який пристрій користувача (наприклад, на USB-накопичувач, iPad, карту пам'яті тощо). Під час реєстрації користувач повинен під'єднати цей пристрій до ПК.

7. Картка з шаром, який зіскоблюється. Користувачу видається картка з PINкодом, який використовується лише один раз.

Аналіз показав, що в банківських системах, як правило, застосовуються системи двофакторної автентифікації, основані на одноразових e-mail- або sms-паролях та різних типах токенів. Сьогодні кілька компаній пропонують системи двофакторної автентифікації, основані на генерації одноразових паролів (One-Time Password – OTP), серед яких RSA Security, VASCO Data Security і ActivIdentity.

Для реалізації двофакторної автентифікації використовують різні види генераторів OTP. Генератор OTP являє собою автономний портативний електронний прилад, здатний генерувати і відображати на вбудованому ЖК-дисплеї цифрові коди. Для сім'ї пристроїв Digipass компанії VASCO механізм генерації одноразових паролів оснований на криптографічному TripleDES-перетворенні набору даних, що складається з 40 бітів поточного часу і 24-бітового

вектора даних, унікальних для кожного ідентифікатора доступу. Некриптографічні алгоритми автентифікації передбачають використання для підтвердження достовірності абонента не тільки його логіна та паролю, а й додаткових засобів (мобільних телефонів, смарт-карт, токенів). Авторизація за допомогою предметів відбувається тільки за наявності спеціального пристрою, який може зчитувати інформацію з перерахованих ідентифікаторів. Робота системи має такий алгоритм:

1. Користувач надсилає запит на доступ у систему й вводить свій логін та пароль.
2. Сервіс перевіряє наявність логіна у DNS-таблиці.
3. У DNS-таблиці перевіряється відповідність введеного паролю та логіна.
4. Якщо збігаються дані, система надсилає запит користувачеві на введення ідентифікатора із додаткового засобу.
5. Абонент отримує свій унікальний ідентифікатор з пристрою.
6. Абонент надсилає ідентифікатор до системи.
7. Система перевіряє індивідуальний ідентифікатор суб’єкта.__
8. У разі збігу даних із еталонним варіантом автентифікацію визнають вдалою й надають доступ до системи, якщо дані не збігаються – суб’єкт повертається до першого кроку. Алгоритм некриптографічної автентифікації наведено на рис. 2.1.

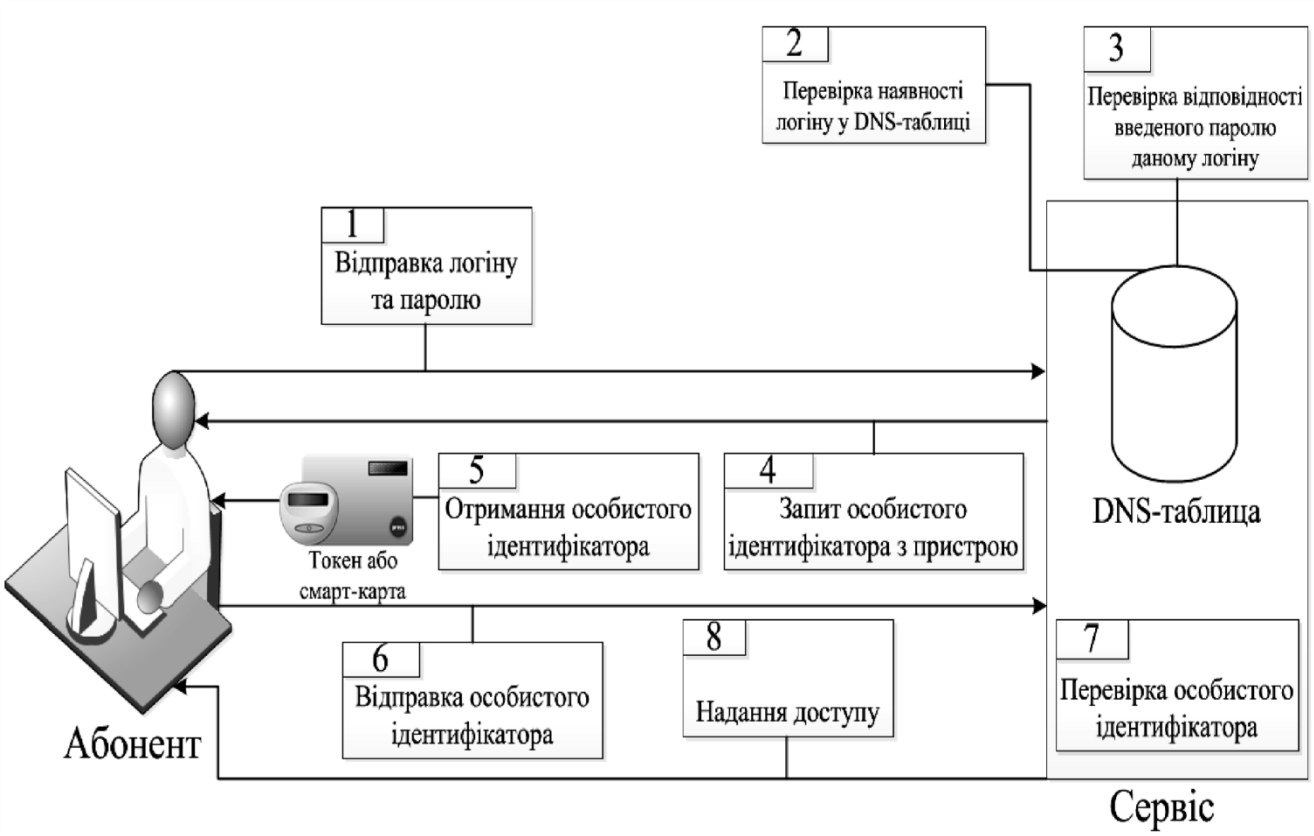


Рис. 2.1. Схема алгоритму некриптографічної автентифікації

Для автентифікації за допомогою біометричного алгоритму суб’єкт повинен пройти сканування однієї чи декількох фізіологічних (відбиток пальців, райдужна оболонка ока, сітківка ока, риси обличчя тощо) або поведінкових характеристик (підпис, клавіатурний почерк, тембр голосу). Цей метод, як правило, використовують на дуже важливих об’єктах та системах зі спеціальним устаткуванням. Робота системи має такий алгоритм:

1. Користувач зчитує біометричні дані за допомогою біометричного давача.

2. Зчитані дані надсилають на сервер, де порівнюють з еталонними даними, які зберігаються у базі даних.

3. У разі збігу даних із еталонним варіантом автентифікація вважається вдалою й надається доступ до системи, якщо ж ні – суб’єкт повертається до першого кроку. Алгоритм парольної автентифікації наведено на рис. 2.2.

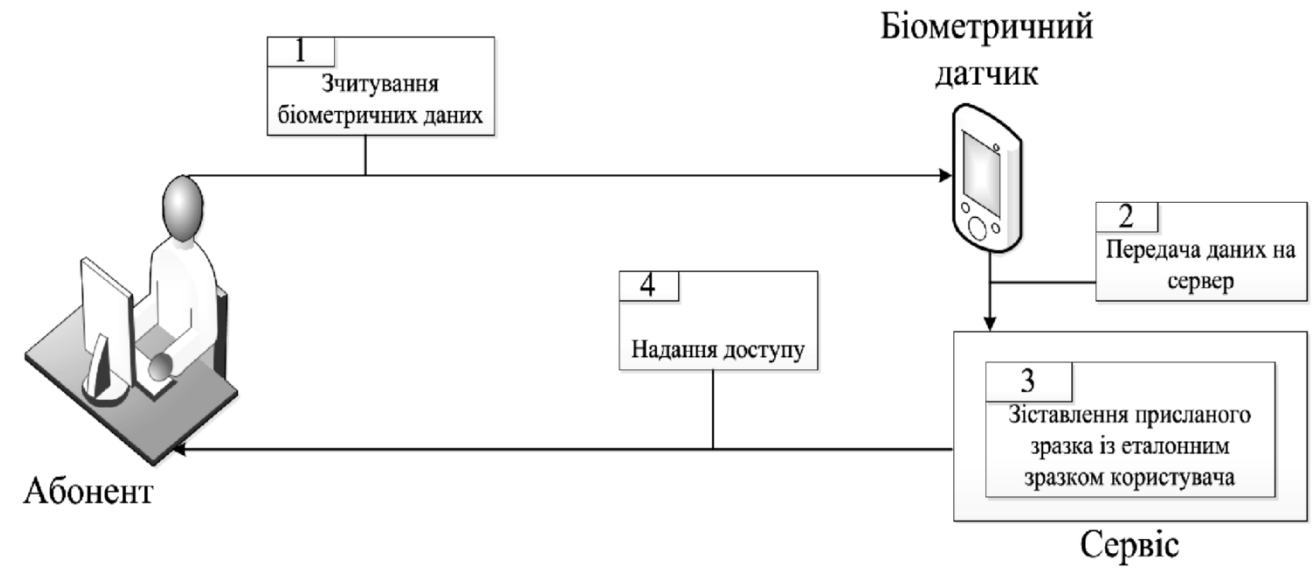


Рис. 2.2. Схема алгоритму біометричної автентифікації

2.1.1 Алгоритм двофакторної автентифікації повідомлень у банківських системах PassWindow

Алгоритм PassWindow - алгоритм двофакторної автентифікації, побудований на формуванні унікального ключа, частина якого надрукована на прозорій частині стандартного посвідчення особи у вигляді штрихкоду, який складається із рисок. Щоб скласти унікальний ключ доступу, треба притиснути свою картку до екрана монітора, термінала, мобільного телефона чи планшета у відповідну область, де формується друга частина коду, що також має вигляд штрихкоду з рисками, які змінюються.

Шаблони штрихкоду PassWindow можуть існувати у вигляді унікальних статичних зображень послідовності символів або у вигляді більш розширеної анімаційної версії всього шаблону. Ці анімовані штрихкоди складаються з послідовності статичних шаблонів, кожний з яких містить закодовані символи або ж нічого не означають і просто динамічно додають ентропію у весь шаблон. Послідовності шаблонів штрихкоду генерує динамічно сервер автентифікації так, що кожен є унікальним (і, отже, є сенс) тільки у разі використання разом з ключем, до якого вони підходять. Будь-яке втручання або підробка шаблону штрихкоду будуть пасивно представлені користувачу у вигляді появи комбінацій в шаблоні, які не відповідають очікуванням, наприклад, випадково розміщені сегменти, які не містять ніяких символів, випадкові цифри, яких бракує, або надлишкові цифри, що з’являються в межах одного шаблону, або проведення перевірки інформації, яка не стосується активної транзакції. Будь-який буквено-цифровий код можна

надійно передати за допомогою методу PassWindow, проте поточна реалізація методу спрямована на передавання коротких рядків випадкових цифр, щоб використати їх як одноразовий пароль у поєднанні з цифрами, які ідентифікують унікальність транзакції перевірки справжності користувача. Як тільки користувач підтверджує, що унікальна інформація в межах транзакції – закодована в штрихкодах – відповідає бажаній, він може завершити транзакцію, ввівши відповідний одноразовий пароль.

Основні етапи системи PassWindow подано на рис. 2.3.

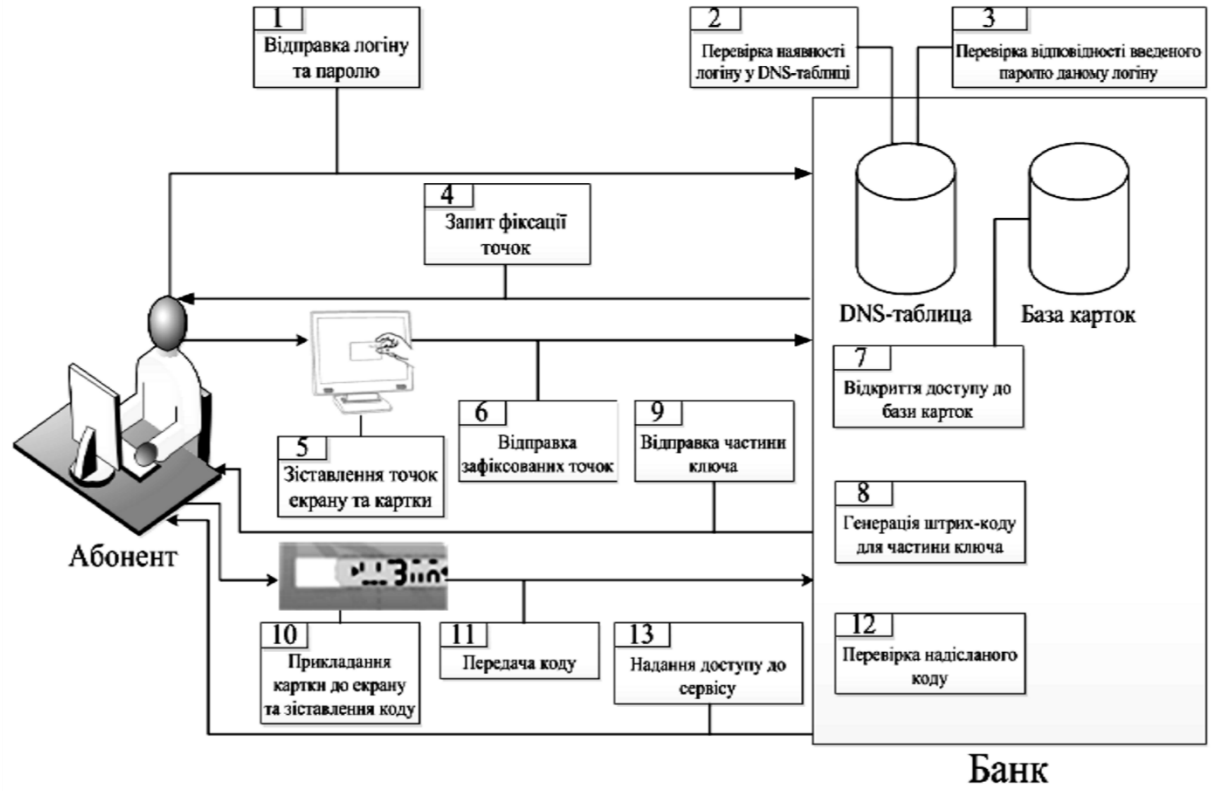


Рис. 2.3. Схема алгоритму подвійної автентифікації PassWindow

Принцип роботи методу автентифікації має такий алгоритм:

1. Абонент ідентифікується у системі.
2. Сервіс перевіряє наявність логіна у DNS-таблиці.
3. У DNS-таблиці перевіряється відповідність введеного паролю та логіна.
4. Якщо ідентифікація пройшла успішно – абоненту надсилають запит фіксації точок картки.
5. Абонент прикладає картку до екрана, після чого відбувається фіксація відповідності точок штрихкоду картки.
6. Зафіксовані точки відправляються до сервісу, де надалі зберігаються.

7. У сервісі відкривається доступ до бази карток.

8. Здійснюється генерація штрихкоду для частини ключа, що надалі дасть змогу формувати код.

9. Сформований штрихкод частини ключа надсилається 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 на правильність.

13. Якщо перевірку успішно пройдено – автентифікація успішна. Абоненту надається доступ до сервісу.

Оцінка безпеки систем двофакторної автентифікації. Аналіз сучасних систем автентифікації показав, що їх безпеку вимірюють, поділивши різницю між вартістю атак і вигодою для того, хто атакує, на вартість захисту від них. Тому дорогі, хоча й безпечніші методи, такі як криптографічні PKI-пристрої з власними захищеними каналами зв'язку, екранів і клавіатур, оцінюються так низько за шкалою безпеки, тоді як банківські системи все ще переважно спираються на найдешевший і, здавалося б, найменш захищений спосіб використання PIN-кодів і паролів. Через загальну вартість і складність розгортання таких пристроїв часто надають перевагу їх використанню, а не криптографічним системам безпеки.

2.1.2 Гіпотетичні атаки на засіб аутентифікації PassWindow

Атаки "посередника" і фішинг (MITM)

Відбуваються, коли зловмисник між клієнтом і сервером і видає себе за обидві сторони, здійснює перехоплення, запис або зміну взаємодії між ними. PassWindow вирішує цю проблему, надаючи пасивну перевірку на рівні транзакцій, щоб переконатися, що користувач знає про справжність транзакції, яку він виконує до введення OTP після завершення цієї транзакції. Отже, PassWindow захищає від шахрайських атак MITM транзакцій і забезпечує автентифікацію в обох напрямах – від користувача до сервера і від сервера до користувача.

Атаки в області соцінженерії.

В "атаках соціальної інженерії" користувача переконують розголосити його особисті дані, і в разі апаратних маркерів – його одноразові паролі. Комбінації

клавіш PassWindow не так легко передаються в усній формі або через друковані символи, тим самим запобігаючи найзручнішим телефонним атакам соціальної інженерії, які використовуються проти електронних апаратних маркерів. Цей метод отримав назву “вішинг”. Ці атаки використовують людину, яка дзвонить користувачу і видає себе за уповноваженого представника обслуговування. Усний запит здійснюється для читання дійсного коду авторизації з пристрою автентифікації жертви, що нібито дає змогу людині, яка дзвонить, виявити, наприклад, “важливу конфіденційну інформацію”.

Малоймовірно, що зловмисник спробує дізнатись комбінацію клавіш PassWindow від клієнта цим способом, тому що важко на словах пояснити візуальні характеристики сегмента PassWindow матриці.

“Людина в браузері”, або хакерське проникнення.

Зловмисник одержує звіти від шкідливих програм, встановлених на комп’ютері жертви, і виявляє, що жертва звертається до сайта фінансової організації, програмне забезпечення змінює дані форми в браузері на такі, щоб інший обсяг коштів передавався на чужий рахунок – зазвичай гібридний. Власник такого рахунка потім передає ці гроші зловмиснику. Перевірка інформації, пов’язаної з операцією, може бути закодована в штрих-коді шаблону PassWindow. Це може запевнити користувача, наприклад, що кошти переводяться на правильний рахунок.

Проста крадіжка.

Єдиним способом для відкриття і копіювання ключового шаблону PassWindow є пряме копіювання карти відразу після її отримання. Цю можливість знижують, вводячи відтінок, який можна роздрукувати поверх шаблону, що ускладнить спроби фотографування і ксерокопіювання. Однак, оскільки PassWindow використовується в стратегії двофакторної автентифікації, простого знання ключового шаблону недостатньо для шахрайської автентифікації без знання логіна або пароля жертви.

Підглядання зі спини.

PassWindow захищений проти “підглядання зі спини”– непомітного спостереження за тим, як користувач вводить свої дані. Оскільки ключ/штрихкод являє собою одноразовий пароль, ті, що підглядають, не можуть скористатись ним. Знову ж, відтінок, надрукований поверх ключового шаблону на картці, робить шаблон невидимим ні для кого, окрім користувача.

Пряма атака на сервер автентифікації PassWindow.

Зловмисник може спробувати безпосередньо атакувати сервер автентифікації PassWindow, щоб порушити цілісність всієї процедури автентифікації PassWindow. Сервер автентифікації PassWindow використовує дуже простий і обмежений протокол зв'язку, і вся обробка автентифікації здійснюється на самому сервері. Його функціональність обмежена створенням даних зображення штрихкоду, отриманням коротких кодів доступу і значення ідентифікаторів користувачів, і, зрештою, видаванням відповіді (так/ні) на запит перевірки автентичності. Крім цього, різні стратегії автентифікації управляють задовільною швидкістю запитів і термінів відповіді. Цей базовий цифровий зв'язок з сервером автентифікації дає невелику можливість зловмиснику безпосередньо зайняти сервер будь-яким ефективним способом, що може привести до успішного доступу. *Аналітична атака на секретний ключ*

Зловмисник може спробувати вивести друковану комбінацію клавіш користувача через аналітичну (наприклад, статистичну або алгебраїчну) атаку. Це можна зробити з використанням складної програми "атака посередника" або шкідливих встановлених локально програм на основі моніторингу, що дасть змогу перехоплювати і штрихкоди PassWindow, і відповідні відповіді користувача. З часом, коли у зловмисника накопичуються ці пари запит/відповідь, він може потенційно отримати деяке уявлення про ключові шаблони PassWindow через аналіз перехоплених даних.

З метою тестування уразливості PassWindow до такого нападу розроблено алгоритм злому, який намагається використовувати ці принципи для виконання зазначеного аналізу. Сам алгоритм використовує техніку "грубої сили". Він починається з генерації всіх комбінацій, в результаті чого цифри, які є результатом, можуть бути поміщені в шаблоні. Наприклад, шестизначний результат у шаблоні з 14 колонок дає такі можливі варіанти (серед інших):

2 - 5 - 7 - 2 - 4 - 3 - - -
2 - 5 - 7 - 2 - 4 - - 3 - -
2 - 5 - 7 - 2 - 4 - - - 3 -
2- - 5- - 7 - 2 - 4 - - 3

Кожна комбінація оцінюється за відомим штрихкодом, щоб розрахувати, може він становити цифру в запиті чи ні. Сегменти можуть або бути присутні, якщо вони необхідні для побудови рішення, або ні, якщо вони мають бути відсутні для нього, або можуть бути невідомими, якщо сегмент далеко від цифри чи накладається на біт штрихкоду. Після окремого набору комбінацій для кожного

перехоплення алгоритм шукає несумісності між комбінаціями. Він бере першу комбінацію першого набору, порівнюючи його, своєю чергою, з кожною комбінацією другого комплекту. Якщо вона несумісна з кожною комбінацією в другій групі, комбінація відкидається.

Перевірка сумісності триває так, що кожна комбінація в кожному наборі порівнюється з комбінаціями кожного іншого набору. Якщо комбінація відкидається, тоді кожний наступний набір необхідно переглянути. Здійснюючи перебір і аналіз достатньої кількості перехоплень, алгоритм здатний вивести ключовий шаблон з достатнім ступенем достовірності. Однак ця атака потребує значної кількості перехоплень зломником: від 20 –30 в разі малих шаблонів (до 4–5 цифр), сотень для великих шаблонів (до 10 цифр), декількох тисяч (до 40 цифр) в разі використання методу в анімаційному режимі підвищеної безпеки. Отже, безпека PassWindow полягає не стільки в складності алгоритму, необхідного для її вирішення, скільки в системній складності вилучення достатньої кількості інформації залежно від цілі атаки. Якщо PassWindow використовується правильно, то висока ймовірність того, що необхідна інформація може бути недоступна навіть для найдосвідченіших хакерів.

Підроблені (ослаблені) штрихкоди.

Зловмисник може спробувати послабити захист PassWindow, змінюючи частоту кадрів зі справжнього (перехопленого) штрихкоду, перш ніж доставити ослаблений (спрощений) штрихкод користувачеві. Цей метод зменшує ентропію штрихкоду, щоб змінити деталі, які могли б спростити аналіз перехоплення запитів / відповідей. Однак явно пошкоджений штрихкод пасивно попереджає користувача про спробу нападу, викликаючи його підозри щодо використання обчислювальної техніки та комунікаційних каналів. Ефективний практичний спосіб моніторингу системи PassWindow. Проведений аналіз загроз системи PassWindow показав, що найефективнішою загрозою є аналітична атака на секретний ключ (штрихкод картки). Для успішної роботи алгоритму потрібно від трьох до п’яти сесій моніторингу (передачі клієнтом ОТР банку).

Алгоритм моніторингу пластикових карток складається з таких кроків:

1. Моніторинг каналу зв’язку та отримання даних за сесіями.
2. Переведення даних у клас індикатора (у вигляді бінарного коду), яким можна оперувати як об’єктом (клас індикатора являє собою масив із семи одиниць/нулів).

3. Перевірка можливості формування “цифр” в кожній позиції картки (цикл за всіма сесіями). Всередині циклу починається цикл за кожною послідовністю – по черзі кожен індикатор представляється “правильним” (вважаємо, що в ньому була цифра). Всередині циклу проводиться перевірка – якщо поточна позиція є “правильною”, тоді створюється варіант, в який записується інвертований індикатор генератора; якщо це “неправильна” позиція, то записується індикатор. Після кожного циклу усередині однієї послідовності йде перетин з варіантами минулої послідовності, тобто N . N (Ni & Nj), якщо всі послідовності в поточній сесії перетнуті – звільняємо їх, тобто кінцеві листи (варіанти) проглядаються і викидаються копії.

4. Перегляд всіх послідовностей у всіх сесіях. Перетин всіх листів між сесіями по черзі (перша сесія з другою, результат їх перетину з третьою сесією і т.д.). Після кожного перетину листа із суміжною сесією – листи “чистяться” від копій.

5. Перетин листів всіх сесій між собою. Цикл за всіма листами – кожен варіант (або лист) перевіряється на вхідних даних – на даних генератора. Якщо він має конфлікт з якимось з індикаторів, то такий лист (варіант) відкидається. У результаті залишиться тільки один варіант, який не має конфліктів ні з однією з послідовностей всіх сесій.

6. Виведення кінцевого варіанта в файл output.txt у форматі бінарного рядка.

Алгоритм моніторингу пластикових карток PASSWINDOW наведено на рис. 2.4.

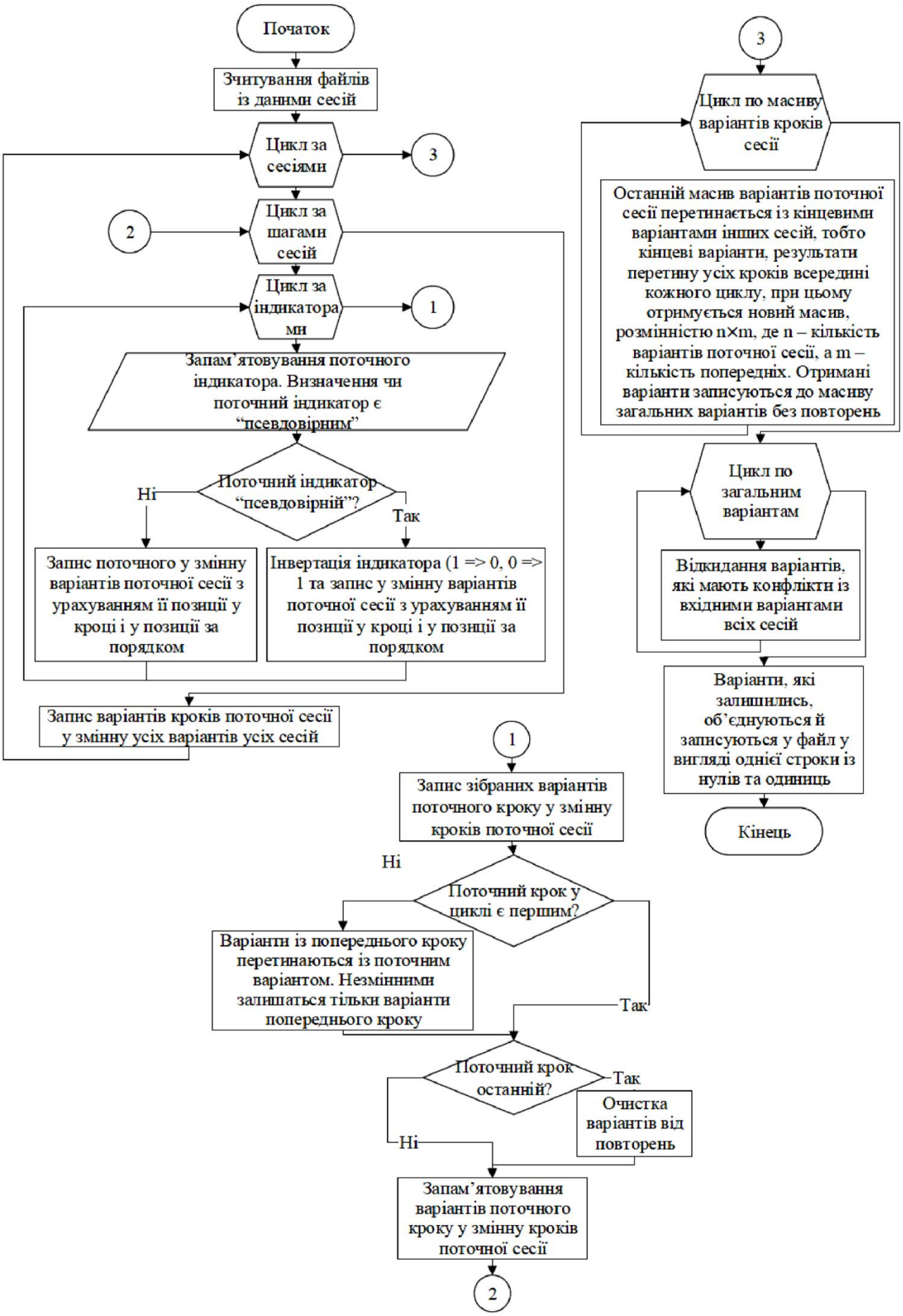


Рис. 2.4. Алгоритм моніторингу пластикових карток PASSWINDOW

2.2 Протокол Kerberos як провідна технологія ідентифікації/автентифікації в банківських ІКС

Протокол Kerberos використається для автентифікації в системах “клієнт-сервер” й обміну ключовою інформацією, призначеною для встановлення захищеного каналу зв'язку між абонентами, що працюють як у локальної, так й у глобальних мережах. Особливий інтерес даний протокол представляє тому, що він убудований як основний протокол автентифікації в операційній системі Microsoft Windows 2000 й UNIX BSD. Kerberos забезпечує автентифікацію в мережах, що не заслуговують довіри, тобто при роботі Kerberos мається на увазі, що зловмисники можуть виконувати наступні дії:

- видавати себе за одну з легітимних сторін мережного з'єднання;
- мати фізичний доступ до одному з комп'ютерів, що беруть участь у з'єднанні; перехоплювати будь-які пакети, модифікувати їх й/або передавати повторно.

Відповідно, забезпечення безпеки в Kerberos побудовано таким чином, щоб нейтралізувати будь-які потенційні проблеми, які можуть виникнути через перерахованих вище дії зловмисників. Kerberos розроблений для мереж TCP/IP і побудований на основі довіри учасників протоколу до третього (довіреної) стороні. Служба Kerberos, що працює в мережі, діє як довірений посередник, забезпечуючи надійну автентифікацію в мережі з наступною авторизацією доступу клієнта (клієнтського додатка) до ресурсів мережі. Захищеність установлених у рамках сесії Kerberos з'єднань обумовлюється застосуванням симетричних алгоритмів шифрування. Служба Kerberos розділяє окремий секретний ключ із кожним суб'єктом мережі, і знання такого секретного ключа рівносильно доказу дійсності суб'єкта мережі.

Основу Kerberos становить протокол автентифікації й розподілу ключів НідхемаШредера (Needham-Schroeder) із третьою довіреною стороною. Розглянемо цю версію протоколу Нідхема-Шредера стосовно до Kerberos. У протоколі Kerberos (версія 5) беруть участь дві взаємодіючі сторони й довірений сервер KS, що виконує роль центра розподілу ключів KDC. Вихідний об'єкт позначається через *A*, а викликуваний (об'єкт призначення) - через *B*. Учасники сеансу *A* й *B* мають унікальні ідентифікатори Id_A й Id_B відповідно. Сторони *A* й *B*, кожна окремо, розділяють свій секретний ключ із сервером *KS* . Нехай сторона *A*

хоче одержати сеансовий ключ для інформаційного обміну зі стороною *B*. Сторона *A* ініціює фазу розподілу ключів, посилаючи по мережі серверу *KS* ідентифікатори Id_A й Id_B:

$$A\square\ RS\ Id$$

$$Id: \quad {}_A, \quad {}_B \quad (2.1)$$

Сервер *KS* генерує повідомлення з тимчасовою оцінкою *T* , терміном дії *L*, випадковим сеансовим ключем *K* й ідентифікатором Id_A. Він шифрує це повідомлення секретним ключем, що розділяє зі стороною *B*.

Потім сервер *KS* бере тимчасову оцінку *T* , термін дії *L*, сеансовый ключ *K* , ідентифікатор Id_B сторони *B* й шифрує все це секретним ключем, що розділяє зі стороною *A*. Обоє ці зашифровані повідомлення він відправляє стороні *A*:

$$KS\ \square A\ E\ T\ L\ Id: \quad {}_A(, ,_B), E\ T\ L\ Id_B(,$$

$$, \quad {}_A) \quad (2.2)$$

Сторона *A* розшифровує перше повідомлення своїм секретним ключем, перевіряє оцінку часу *T* , щоб переконатися, що це повідомлення не є повторенням попередньої процедури розподілу ключів. Потім сторона *A* генерує повідомлення зі своїм ідентифікатором Id_A й оцінкою часу *T* , шифрує його сеансовим ключем *K* і відправляє стороні *B*. Крім того, *A* відправляє для *B* повідомлення від *KS* , зашифроване ключем сторони *B*:

$$A\square B\ E\ Id\ T\ E\ T\ L\ K\ Id: \ {}_K({}_A,), {}_B(,$$

$$, \quad , \quad {}_A) \quad (2.3)$$

Тільки сторона *B* може розшифрувати повідомлення (2.3). Сторона *B* одержує оцінку часу *T* , термін дії *L*, сеансовий ключ *K* й ідентифікатор Id_A. Потім сторона *B* розшифровує сеансовим ключем *K* другу частину повідомлення (2.3). Збіг значень *T* й Id_A у двох частинах повідомлення підтверджують дійсність *A* по відношенню к. *B*

Для взаємного підтвердження дійсності сторона *B* створює повідомлення, що складається з оцінки часу *T* плюс 1, шифрує його ключем *K* і відправляє стороні *A*:

$$B\square A\ E\ T: \ {}_K(\square 1) \quad (2.4)$$

Якщо після розшифрування повідомлення (2.4) сторона *A* одержує

очікуваний результат, вона знає, що на іншому кінці лінії зв'язку перебуває дійсно *B*.

Цей протокол успішно працює за умови, що годинники кожного учасника синхронізовані з годинниками сервера *KS* . Слід зазначити, що в цьому протоколі необхідний обмін із *KS* для одержання сеансового ключа щораз, коли *A* бажає встановити зв'язок с. *B* Протокол забезпечує надійне з'єднання об'єктів *A* і *B* за умови, що жоден із ключів не скомпрометований і сервер *KS* захищений.

Система Kerberos має структуру типу "клієнт-сервер" і складається із клієнтських частин *C*, установлених на всі машини мережі (робітники станції користувачів і сервери), і сервера Kerberos KS, що розташовується на якому-небудь (не обов'язково виділеному) комп'ютері. Клієнтами можуть бути користувачі, а також незалежні програми, що виконують такі дії, як завантаження вилучених файлів, відправлення повідомлень, доступ до баз даних, доступ до принтерів, одержання привілеїв в адміністратора й т.п.

Сервер Kerberos KS можна розділити на дві частини: сервер автентифікації AS (Authentication Server) і сервер служби видачі мандатів TGS (Ticket Granting Service). Фізично дані сервери можуть бути сполучені. Інформаційними ресурсами, необхідними клієнтам З, управляє сервер інформаційних ресурсів RS. Передбачається, що сервери служби Kerberos надійно захищені від фізичного доступу зловмисників.

Мережні служби, що вимагають перевірки дійсності, і клієнти, які хочуть використати ці служби, реєструють в Kerberos свої секретні ключі. Kerberos зберігає базу даних про клієнтів й їхні секретні ключі. Наявність у цій базі даних секретних ключів кожного користувача й ресурсів мережі, що підтримують даний протокол, дозволяє створювати зашифровані повідомлення, що направляють клієнтові або серверу; успішне расшифрування цих повідомлень й є гарантією проходження автентифікації всіма учасниками протоколу.

Kerberos також створює *сеансові ключі* (session key), які видаються клієнтові й серверу (або двом клієнтам) і нікому більше. Сеансовий ключ використається для шифрування повідомлень, якими обмінюються дві сторони, і знищується після закінчення сеансу.

Область дії системи Kerberos поширюється на ту ділянку мережі, всі користувачі якого зареєстровані під своїми іменами й паролями в базі даних сервера Kerberos.

Загалом процес ідентифікації й автентифікації користувача в системі

Kerberos версії 5 можна описати в такий спосіб (рис. 2.5). Клієнт І3, бажаючи одержати доступ до ресурсу мережі, направляє запит серверу автентифікації AS. Сервер AS ідентифікує користувача за допомогою його імені й пароля й висилає клієнтові мандат на доступ до сервера служби виділення мандатів TGS (Ticket-Granting Service).

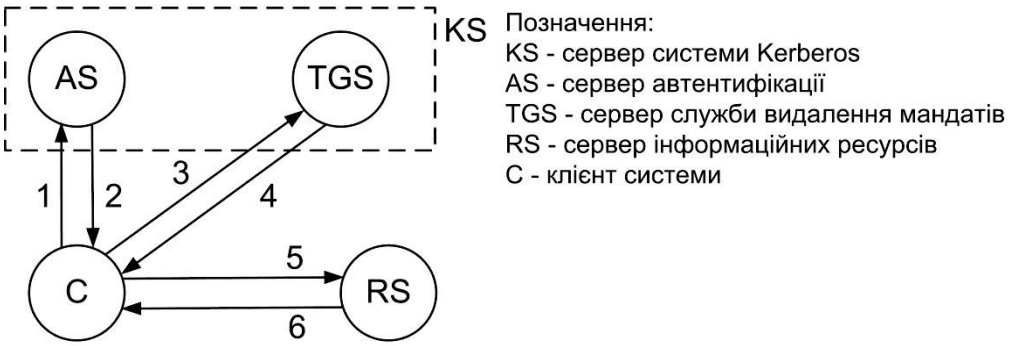


Рисунок 2.5. Схема роботи протоколу Kerberos

Для використання конкретного цільового сервера інформаційних ресурсів *RS* клієнт *Із* запитує в TGS мандат на звертання до цільового сервера *RS*. Якщо все в порядку, TGS дозволяє використання необхідних ресурсів мережі й посилає відповідний мандат клієнтові С. Основні кроки роботи системи Kerberos (рисунок 2.7):

1. *C□AS* - запит клієнта *C* к серверу *AS* на дозвіл звернутися до служби TGS.
2. *AS C□* - дозвіл (мандат) від сервера *AS* клієнтові *3і* звернутися до служби TGS.
3. *C TGS□* - запит клієнта *C* к службі *TGS* на одержання допуску (мандата) до сервера ресурсів *RS*.
4. *TGS C□* - дозвіл (мандат) від служби *TGS* клієнтові *Із* для звертання до сервера ресурсів *RS*.
5. *C RS□* - запит інформаційного ресурсу (послуги) у сервера *RS*.
6. *RS C□* - підтвердження дійсності сервера *RS* і надання інформаційного ресурсу (послуги) клієнтові *C*.

Дана модель взаємодії клієнта із серверами може функціонувати тільки за умови забезпечення конфіденційності й цілісності переданої керуючої інформації. Без строгого забезпечення інформаційної безпеки клієнт Із не може відправляти серверам AS, TGS й RS свої запити й одержувати дозволи на доступ до

обслуговування в мережі.

Щоб уникнути можливості перехоплення й несанкціонованого використання інформації, Kerberos застосовує при передачі будь-якої керуючої інформації в мережі систему багаторазового шифрування з використанням комплексу секретних ключів (секретний ключ клієнта, секретний ключ сервера, секретні сеансові ключі пари клієнтсервер). Kerberos може використати різні симетричні алгоритми шифрування й хешфункції, однак обов'язковими для підтримки встановлені алгоритми Triple DES й MD5.

У системі Kerberos використаються два типи вірчих документів: мандат (ticket) і автентифікатор (authenticator). *Мандат* використається для безпечної передачі серверу ідентифікаційних даних клієнта, якому виданий цей мандат. У ньому також утримується інформація, що сервер може використати для перевірки того, що клієнт, що використає мандат, - це саме та особа, якій даний мандат був виданий. *Автентифікатор* - це додатковий атрибут, пропонований разом з мандатом. Надалі в цьому розділі буде застосовуватися система позначень, використовувана в документах Kerberos: *c* - клієнт; *s* - сервер; *a* - мережна адреса клієнта; *v* - початок і закінчення часу дії мандата; *t* - мітка часу; K_x - секретний ключ x; $K_{x,в}$ - сеансовий ключ для *x* и *в*; $\{m\}\ K_x$ - повідомлення т, шифроване секретним ключем K_x суб'єкта x; $T_{x,в}$ - мандат x на використання в; $Ax_{,в}$ - аутентифікатор x для в.

Мандат Kerberos має наступну форму: $T_{c\,s,} \square s\ c\ a\ v\ R\ K,\{\ ,\ ,\ ,\ _{c\,s,}\}_s$.

Мандат надається одному клієнтові для доступу до строго певного сервера й на строго певний час. Він містить ім'я клієнта, його мережна адреса, початковий і кінцевий час дії клієнта й сеансовий ключ $K_{s\,c,}$, зашифровані на секретному ключі K_s сервера.

Якщо клієнт одержав мандат, він може використати його для доступу до сервера протягом проміжку часу, відведеного для даного мандата. Клієнт не може розшифрувати мандат (він не знає секретного ключа K_s сервера), але він може пред'явити його серверу в зашифрованій формі. Ніхто з, що підслухують у мережі не зможе прочитати або змінити мандат при передачі його по мережі.

Автентифікатор Kerberos має форму: $A_{C\,S,} \square s\ c\ a\ v\ K,\{\ ,\ ,\ ,_{R\,S,})K_S$.

Автентифікатор створюється клієнтом щораз, коли той хоче одержати доступ до цільового сервера. Автентифікатор містить ім'я клієнта, мітку часу й сеансовий ключ, зашифровані на сеансовому ключі $K_{C\,S,}$ загальному для клієнта й

сервера.

На відміну від мандата, автентифікатор використається тільки один раз. Однак клієнт може генерувати автентифікатори в міру потреби (йому відомий загальний секретний ключ $K_{C\,S,}$). Використання автентифікатора переслідує дві мети. По-перше, автентифікатор містить деякий відкритий текст, зашифрований сеансовим ключем. Це доводить, що клієнтові відомий ключ. По-друге, зашифрований відкритий текст включає мітку часу. Ця мітка часу не дозволяє зловмисникові, що перехопив даний автентифікатор і мандат, використати їх через деякий час для успішного проходження процедури автентифікації.

В Kerberos версії 5 використається п'ять типів повідомлень (див. рис.2.7):

1. Клієнт-Kerberos: *c tgs,* .
2. Kerberos-клієнт: $\{K_{c\,tgs,}\}K\ T_c\{\ _{c\,tgs,}\}K_{tgs}$.
3. Клієнт-TGS: $\{A_{c\,s,}\}K_{c\,tgs,}\{T_{c\,tgs,}\}K_{tgs\,s,}$.
4. TGS-клієнт: $\{K_{c\,s,}\}K_{c\,tgs,}\{T_{c\,s,}\}K_s$.
5. Клієнт-сервер: $\{A\ K\ T\ K_{c\,s,}\}\ _{c\,s,}\{\ _{c\,s,}\}\ _s$.

Розглянемо використання цих повідомлень докладніше.

Одержання первісного мандата. У клієнта є частина інформації, що доводить його особистість, - його пароль. Зрозуміло, що не слід змушувати клієнта передавати пароль по мережі. Протокол Kerberos мінімізує ймовірність компрометації пароля, але при цьому не дозволяє користувачеві правильно ідентифікувати себе, якщо він не знає пароля. Клієнт посилає на сервер автентифікації Kerberos повідомлення, що містить його ім'я й ім'я його сервера TGS (може бути кілька серверів TGS). На практиці користувач найчастіше просто вводить своє ім'я - і програма входу в систему надсилає запит. Сервер автентифікації Kerberos шукає дані про клієнта у своїй базі даних. Якщо інформація про клієнта є в базі даних, Kerberos генерує сеансовий ключ $K_{c\,tgs,}$, що буде використатися для обміну даними між клієнтом й TGS. Kerberos шифрує цей сеансовий ключ секретним ключем клієнта K_c. Потім він створює для клієнта мандат на виділення мандата TGT (Ticket Granting Ticket), що доводить службі TGS дійсність клієнта. TGT зашифровується на секретному ключі TGS і містить ідентифікатори клієнта й сервера, сеансовий ключ пари TGS-клієнт, а також початковий і кінцевий час дії TGT. Сервер автентифікації посилає ці два зашифрованих повідомлення клієнтові.

Тепер клієнт приймає дані повідомлення, розшифровує перше повідомлення своїм секретним ключем K_c й одержує сеансовий ключ $K_{c\ tgs,}$. Секретний ключ є

односпрямованою хеш-функцією клієнтського пароля, тому в законного користувача не буде ніяких проблем. Зловмисник не знає правильного пароля й, отже, не може розшифрувати відповідь сервера автентифікації. Тому зловмисник не може одержати мандат або сеансовий ключ.

Клієнт зберігає мандат TGT і сеансовий ключ, стираючи пароль і хеш-значення. Ця інформація знищується для зменшення ймовірності компрометації. Якщо зловмисник спробує скопіювати вміст пам'ять клієнта, він одержить тільки TGT і сеансовий ключ. Ці дані важливі, але тільки на час життя TGT Коли термін дії TGT мине, ці відомості стануть безглуздими. Тепер клієнт має можливість пройти автентифікацію в TGS-сервера за допомогою отриманого мандата TGT протягом усього терміну дії TGT, зазначеного в ньому.

Одержання серверних мандатів Далі клієнт може одержати окремий мандат для кожної потрібної йому послуги. Із цією метою клієнт повинен надіслати запит у службу TGS (на практиці програмне забезпечення надсилає запит автоматично, тобто невидимо для користувача). Цей запит складається з мандата TGT й автентифікатора. Автентифікатор, зашифрований на ключі парного зв'язку клієнта й сервера TGS, містить ідентифікатори клієнта й сервера, що вимагається йому,, випадковий сеансовий ключ і мітку часу. TGS, одержавши запит, розшифровує TGT своїм секретним ключем. Потім TGS використає включений в TGT сеансовий ключ, щоб розшифрувати автентифікатор. У завершення проводиться порівняння інформації, що втримується в автентифікаторі, з інформацією мандата. Точніше, мережна адреса клієнта у квитку звіряється з мережною адресою, зазначеною в запиті, а також рівняється мітка часу з поточним часом. Якщо все збігається, TGS дозволяє виконання запиту.

Перевірка міток часу припускає, що годинники всіх комп'ютерів синхронізовані, принаймні, з точністю до декількох хвилин. Якщо час, зазначений у запиті, значно відрізняється від сучасний момент, TGS уважає такий запит спробою повторення попереднього запиту. Служба TGS повинна також відслідковувати правильність термінів дії автентифікаторів, тому що послуги сервера можуть запитуватися кілька разів послідовно з одним мандатом, але різними автентифікаторами. Інший запит з тим же мандатом і вже використаною

міткою часу автентифікатора буде відкинутий.

У відповідь на вірний запит TGS надає клієнтові мандат для доступу до цільового сервера. TGS також створює сеансовий ключ для клієнта й цільового сервера, зашифрований сеансовим ключем, загальним для клієнта й TGS. Обоє ці повідомлення відправляються клієнтові. Клієнт розшифровує повідомлення й витягає сеансовий ключ.

Запит послуги. Тепер клієнт може довести свою дійсність цільовому серверу. Для успішного проходження автентифікації в цільового сервера клієнт створює автентифікатор, що складається з його імені, мережної адреси й мітки часу й зашифрований на сеансовому ключі "клієнт-сервер", і відправляє його разом з мандатом, зашифрованим на секретному ключі цільового сервера, що був переданий від служби TGS. Прийнявши дані від клієнта, цільовий сервер проводить перевірку автентифікатора. Він розшифровує його за допомогою свого секретного ключа й витягає з нього сеансовий ключ "клієнт-сервер". Мандат також піддається перевірці. Процедура перевірки схожа із процедурою, проведеної у випадку сесії "клієнт-TGS", тобто перевіряється відповідність мережних адрес і тимчасової мітки. Якщо все в порядку, то сервер упевнений, що клієнт - саме той, за кого він себе видає.

Якщо додаток вимагає взаємної перевірки дійсності, сервер посилає клієнтові повідомлення, що складається з мітки часу, зашифрованої сеансовим ключем. Це доводить, що серверу відомі правильний секретний ключ і він може розшифрувати мандат і посвідчення. При необхідності клієнт і сервер можуть шифрувати подальші повідомлення загальним ключем. Тому що цей ключ відомий тільки їм, вони обоє можуть бути впевнені, що останнє повідомлення, зашифроване цим ключем, відправлено іншою стороною. На практиці вся ця складна процедура автентифікації виконується автоматично й не доставляє клієнтові яких-небудь значних незручностей.

Особливості міждоменної автентифікації. Kerberos може використатися й для міждоменної автентифікації. У випадку обігу клієнта в центр розподілу ключів KDC для доступу до сервера, що перебуває в іншому домені, KDC видає клієнтові *мандат переадресації* (refferal ticket) для звертання до KDC того домену, у якому перебуває необхідний сервер (рисунок 2.6). На малюнку прийняті наступні позначення

1. Запит на автентифікацію.
2. TGT для KDC.

3. Пред'явлення TGT для KDC.
4. Мандат доступу до сервера.
5. Автентифікація й обмін даними.

Мандат переадресації являє собою TGT, зашифрований на ключі парного зв'язку KDC двох доменов. У цьому випадку мандат на доступ до сервера надає клієнтові той KDC, у веденні якого перебуває запитуваний сервер.

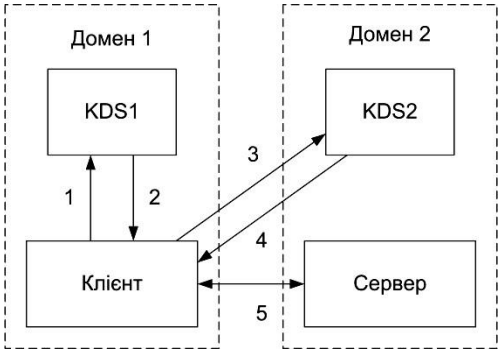


Рис. 2.6. Схема між доменної автентифікації в протоколі Kerberos

Теоретично можливе використання Kerberos для автентифікації в мережах з безліччю доменів. Однак у цьому випадку (у зв'язку з кількістю обігів, що зростають пропорційно кількості доменів) прийде створити якийсь центральний домен, що здійснює однозначну переадресацію запитів конкретним KDC.

Безпека Kerberos. Хоча протокол Kerberos одержав широке поширення серед користувачів і піддавався численним доробкам, у результаті чого з'явилася його п'ята версія, у деяких випадках і він може стати об'єктом успішної атаки порушника.

Насамперед варто пам'ятати, що Kerberos, як і будь-який інший програмний засіб криптографічного захисту, працює в недовереному програмному середовищу. Недокументовані можливості або неправильна конфігурація даного середовища може привести до того, що відбудеться витік критичної інформації, наприклад вихід у середовище передачі сеансових ключів, що зберігаються на жорсткому диску, або даних відкритої інформації. Навіть у випадку зберігання ключів на час сеансу роботи користувача тільки в оперативній пам'яті збій в ОС може привести до того, що ключі будуть скопійовані на жорсткий диск. При використанні на робочій станції із установленим ПЗ Kerberos багатокористувальницького режиму або при відсутності контролю доступу до робочої станції створюється потенційна можливість внесення закладень-програм-закладок або модифікації криптографічного ПЗ. Тому безпека Kerberos багато в чому 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 повинні бути захищені від атак, спрямованих на відмову в обслуговуванні;
- необхідна синхронізація системного часу всіх учасників системи, оскільки мітки часу беруть участь у процесі автентифікації;
- Kerberos не захищає від атак підбором пароля. Проблема в тім, що зберігається в KDC ключ користувача є результатом переробки його пароля за допомогою хэш-функции. У випадку слабкого пароля можливий його підбор;
- служби Kerberos повинні бути надійно захищені від всіх видів

несанкціонованого доступу;

- отримані клієнтом мандати, а також секретні ключі повинні бути захищені від несанкціонованого доступу.

Невиконання зазначених вимог може стати причиною успішної атаки.

На сьогоднішній день протокол Kerberos є широко розповсюдженим засобом автентифікації. Kerberos може використатися в сполученні з різними криптографічними схемами, включаючи шифрування з відкритим ключем. Як приклад можна привести схему організації інтернет-транзакції, коли клієнт на основі системи Kerberos зв’язується із торговою точкою, а торгова точка у свою чергу – із платіжним шлюзом.

Висновки до другого розділу

Проведений аналіз методів автентифікації показав, що практично всі системи як основу використовують криптографічні алгоритми (таблиці) і схильні як до традиційних атак на криптографічні процедури, так і до атак на основі соціальної інженерії, і не в повному обсязі забезпечують безпеку їх використання в банківських системах. Особливе місце серед них займає система двофакторної автентифікації PassWindow, основана на використанні штрихкодів 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 штрихкод картки

користувача, що практично призводить до руйнування безпеки банківської системи.

Найефективнішим механізмом при цьому використання спеціального коду, який генерує, наприклад, банк покупця. 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 ШЛЯХИ ПОБУДОВИ РАЦІОНАЛЬНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Перспективою у розвитку систем ідентифікації таавтентифікації є створення єдиної (комплексної) системи (ЄСІА), яка б забезпечувалв санкціонований доступ користувачів, наприклад, до державних інформаційних ресурсів. Її основними функціями має бути:

реєстрація фіз.осіб, організацій, інформаційно-комунікаційних систем; забезпечення перевірки особистості при реєстрації;

ідентифікація і аутентифікація користувачів веб-додатків державних ІКС; підтримка даних користувача і організації в актуальному стані; надання контрольованого користувачем доступу до його даних за запитами ІКС. Архітектура перспективної ЄСІА подана на рис.3.1.

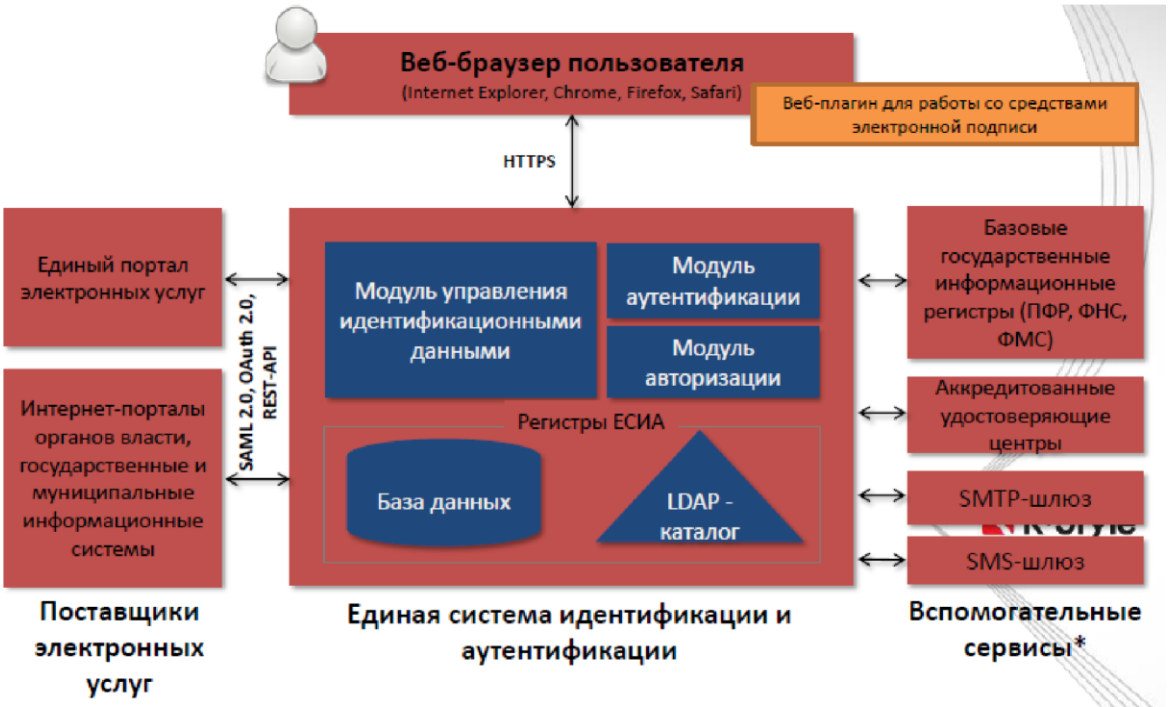


Рис.3.1 Архітектура перспективної ЄСІА

Додаткові сервіси ЕСІА використовуватиме для верифікації особистих даних користувачів, перевірки сертифікатів електронного підпису та відправки повідомлень.

Як користувачі в ЄСІА прийматимуть участь: фізичні особи, які мають

обліковий запис в реєстр фізичних осіб ЄСІА; індивідуальні підприємці (фізичні особи);

юридичні особи (фізичні особи, приєднані до облікових записів юросіб ЄСІА); посадові особи підприємств та організацій.

Користувачі отримують можливість одноразової аутентифікації. Це означає, що пройшовши процедуру аутентифікації в ЄСІА, користувач може протягом одного сеансу роботи увійти в кілька систем, і при цьому повторно вводити логін і пароль не буде потрібно. 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);

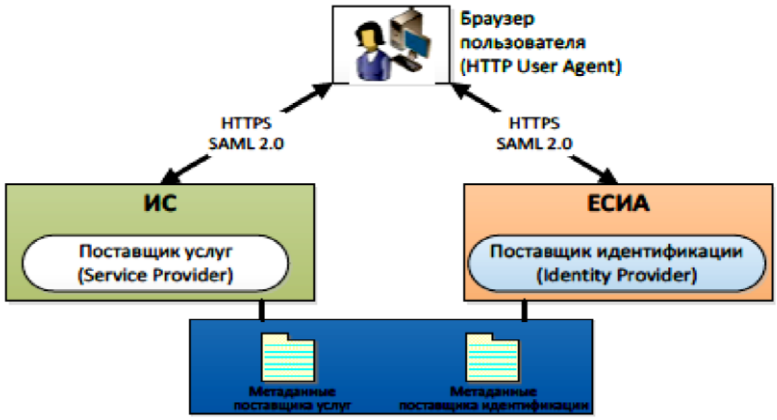


Рис.3.2. Схема взаємодіїІКС з ЄСІА з використанням стандарту SAML V2.0

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

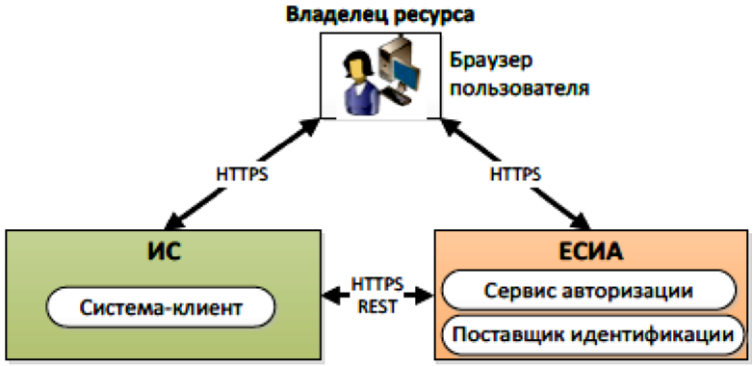


Рис.3.3. Схема взаємодіїІКС з ЄСІА з використанням стандарту OpenID Connect 1.0

Протокол визначає взаємодію наступних сторін:

власник ресурсу (resource owner) - сутність, яка може надати доступ до захищається ресурсу (наприклад, фізична особа, заявник); система-клієнт (client) - додаток, яке запитує доступ до ресурсу, який захищається від імені його власника; сервіс авторизації (authorization server) - сервіс, який випускає для системи-клієнта маркери ідентифікації з дозволами від власника ресурсу, а також маркери доступу, що дозволяють отримувати доступ до даних; постачальник ресурсу

(resource server) - сервіс, що забезпечує доступ до до ресурсу, який захищається на основі перевірки маркерів ідентифікації та маркерів доступу (наприклад, по ідентифікаційним даними користувача).

3.1 Процедура ідентифікації/автентифікації з використанням стандарту SAML

SAML або англ. Security Assertion Markup Language (укр. мова розмітки декларації безпеки) - мова розмітки, заснована на мові XML. Відкритий стандарт обміну даними аутентифікації і авторизації між учасниками, зокрема, між постачальником облікових записів (англ. Identity provider) і постачальником сервісу (англ. Service provider). SAML - продукт OASIS, розроблений Технічним комітетом безпеки сервісів. SAML створений в 2001 році. Останнє значне оновлення SAML було опубліковано в 2005 році, але розширення протоколу постійно випускалися через додаткові, опціональні стандарти.

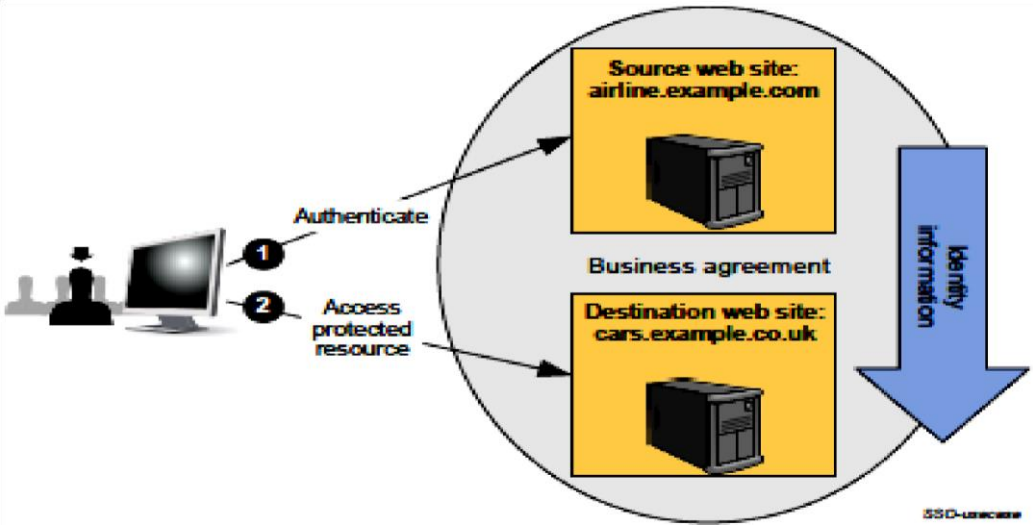


Рис.3.4 Загальний варіант єдиного входу в систему

Стандарт (SAML) визначає структуру на основі XML для опису та обміну інформацією про безпеку між онлайновими діловими партнерами. Однією з важливих проблем, яку намагається вирішити SAML, є забезпечення наскрізної аутентифікації (Single Sign-On, англ. Single Sign On) при роботі через Web-браузер. Це виражається у формі переносних тверджень SAML, що додаткам, які працюють через безпеку мережі домену можуть довіряти. Стандарт OASIS SAML визначає точний синтаксис та правила запиту, створення, спілкування та використання цих тверджень SAML.

Чому SAML потрібен для обміну інформацією про безпеку?

Є декілька драйверів стандарту SAML, включаючи:

по-перше, *Single Sign-On (одноразовий підпис)*. Протягом багатьох років,

різні продукти були продані з вимогою надання підтримка веб-SSO. Ці продукти, як правило, покладаються на файли cookie для підтримки інформації про стан автентифікації користувача, так що повторна автентифікація не вимагається кожен раз, коли веб-користувач хоче отримати доступ до системи. Однак, оскільки файли cookie ніколи не передаються між DNS доменами, то інформація про стан автентифікації в файлах cookie з одного домену ніколи не доступна іншому домену. Тому ці продукти зазвичай підтримують багатодоменну SSO (MDSSO) автентифікацію через використання власних механізмів для передачі інформації про її стан між доменами. Хоча використання одного продукту постачальника іноді може бути життєздатним в рамках одного підприємство, 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 інформації про 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, що бере участь у обміні інформацією, а й – хто є користувачем. Користувачі часто мають окремі локальні ідентифікатори в межах доменів безпеки кожного партнера, з яким вони взаємодіють. Корпоративна ідентифікація (рис.3.5) надає засіб для цих партнерських служб з метою узгодження та встановлення загального ідентифікатору. Вважається, що користувач має корпоративну ідентифікацію, коли партнери створили таку угоду про те, як звернутися до користувача. З адміністративної точки зору цей тип обміну може допомогти зменшити витрати на управління ідентифікацією, оскільки різним послугам не потрібно самостійно збирати та обслуговувати дані, пов'язані з ідентифікацією (наприклад, паролі, ідентифікаційні атрибути). Крім того, адміністраторам цих служб зазвичай не потрібно вручну встановлювати та підтримувати спільні ідентифікатори;

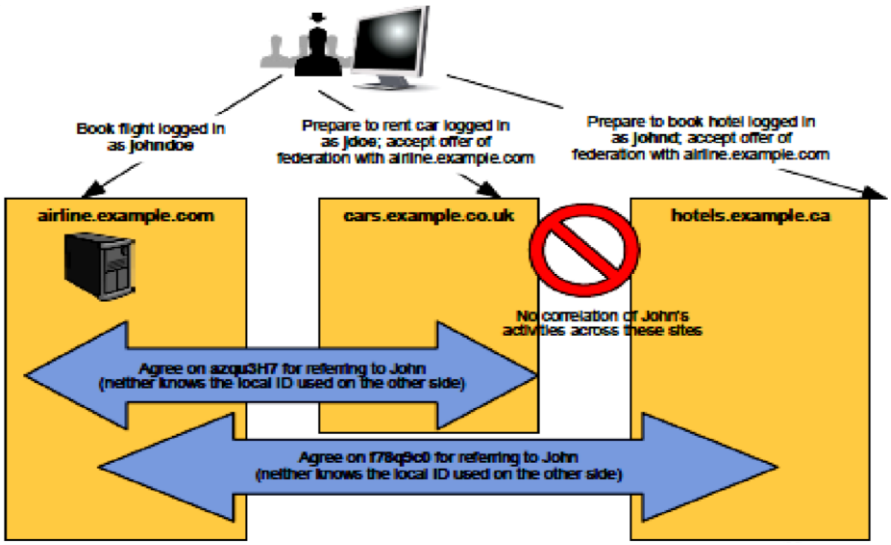


Рис. 3.5 Загальний випадок використання корпоративної ідентифікації

по-третє, *Web services and other industry standards*. SAML дозволяє використовувати для свого формату підтвердження безпеки за межами "рідного" контексту протоколу на основі протоколу SAML. Ця модульність виявилася корисною для інших зусиль галузі, спрямованій на надання послуг з надання авторизації (IETF, OASIS), ідентифікаційних рамок, веб-служб (OASIS, Liberty Alliance) та ін. Технічний комітет OASIS WS-Security визначив профіль для того, щоб використовувати SAML в рамках токену безпеки WS-Security, який може використовуватися, наприклад, для забезпечення обміну повідомленнями SOAP вебсервісів. Зокрема, перевага запропонована використанням SAML полягає в тому, що він забезпечує стандартний підхід до обміну інформацією, включаючи атрибути, які нелегко передавати за допомогою іншого WS-Security токен формату.

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

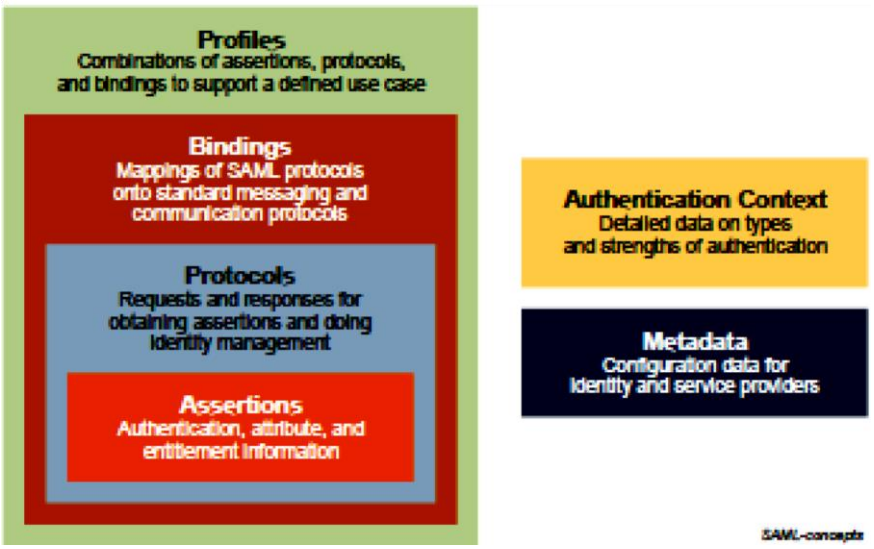


Рис. 3.6 Основні поняття SAML

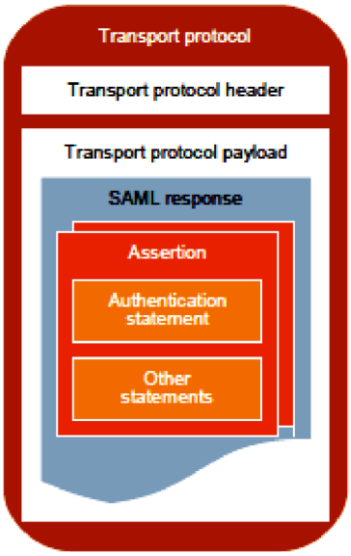


Рис.3.7. Зв'язок компонентів SAML

Базовим сценарієм є сценарій аутентифікації фізичної особи (наприклад, заявника). 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 включає наступні кроки:

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

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

3. ЄСІА перевіряє, статус аутентифікації користувача. Якщо користувач в ЄСІА НЕ аутентифікований, то для продовження процесу він повинен пройти аутентифікацію одним з доступних способів. Якщо користувач ще не зареєстрований в ЄСІА, то він може перейти до процесу реєстрації.

4. Коли користувач аутентифікований, ЄСІА перевіряє, що рівень достовірності ідентифікації користувача відповідає вимогам системи, які зафіксовані в метаданих.

5. Коли користувач успішно аутентифікований, ЄСІА передає в систему відповідь на запит аутентифікації, який містить набір тверджень SAML (SAML Assertions) про користувача.

6. Постачальник послуг приймає рішення про авторизацію користувача на основі отриманої з ЕСІА інформації.

ЄСІА також дозволятиме аутентифікувати користувача в якості представника: юридичної особи та/або ОГВ. Ця функція затребувана системами, серед користувачів яких є співробітники організацій, наприклад, виступаючі як заявники послуг або як посадові особи ОГВ. Якщо включити цю функцію в метаданих 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 ту з них, від імені якої він здійснює аутентифікацію. Якщо система підтримує роботу користувачів з різними ролями, то в процесі аутентифікації користувач матиме можливість зробити вибір ролі, в якій він буде працювати в даній ІКС. Для перевірки наявності у аутентифицированного співробітника необхідних повноважень слід використовувати функціонал системних груп, а для перевірки наявності у неї необхідних повноважень - рекомендується використовувати відповідне SAML-твердження.

Як тільки користувач пройшов аутентифікацію, ЄСІА встановлюватиме призначену для користувача сесію, тривалість якої становить 3 години. Факт початку сесії записується в файлі cookie, який зберігається на комп'ютері користувача. Система може встановити для користувача свою «локальну» сесію. При завершенні «локальної» сесії система повинна спрямовувати в ЄСІА новий запит на аутентифікацію.

Узагальнену процедуру ідентифікації/автентифікації користувачів з використанням протоколу SAML подано на рис.3.8.

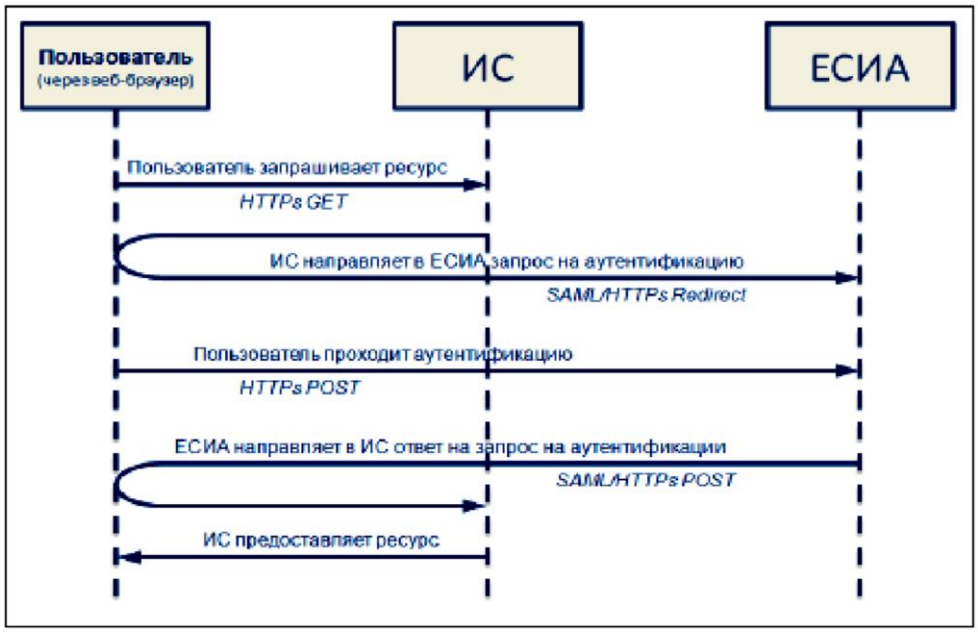


Рис. 3.8 Узагальнена процедура ідентифікації/автентифікації користувачів з використанням протоколу SAML

Сценарій з авторизацією користувача

Система ЄСІА володітиме функціоналом з надання постачальнику послуг інформації, на підставі якої можливе проведення авторизації аутентифицированного користувача. Рішення про авторизацію користувача приймає система, в яку користувач авторизується (Таблиця 3.1).

Таблиця 3.1 - Вимоги до авторизації користувачів

Требования	Рекомендуемое решение
Требуется знать что-то о пользователе для одного сеанса работы (например, имя, которым подписывать комментарии пользователя). Нет необходимости хранить данные об активности пользователя до следующего сеанса.	Давать доступ после получения из ЕСИА ответа на запрос аутентификации содержащего требуемый набор сведений о пользователе.
Требуется знать что-то о пользователе (например, ФИО, email и др.) и длительно хранить пользовательский контекст (настройки, заявки, комментарии).	Давать доступ после получения из ЕСИА ответа на запрос аутентификации содержащего требуемый набор сведений о пользователе. При первом входе пользователя регистрировать его идентификатор
	пользователя (userid). В дальнейшем хранить пользовательский контекст в привязке к этому идентификатору.
Требуется ограничить набор предоставляемых функций в зависимости от типа учетной записи, роли пользователя, использованного метода аутентификации.	Давать доступ после получения из ЕСИА ответа на запрос аутентификации содержащего требуемый набор сведений о пользователе. При попытке пользователя обратиться к функции, для предоставления которой текущие тип учетной записи пользователя, роль пользователя или метод аутентификации являются недостаточными, вывести ему сообщение с пояснениями по дальнейшим действиям. Рекомендуемые сообщения для различных ситуаций приведены в таблице 2. В главе 4.1.1 приведены сведения про типы учетных записей пользователей и роли пользователей.

В наступній таблиці наведено рекомендації по перевірці відповідності вимогам інформаційної системи типу облікового запису користувача, ролі користувача і використаного методу аутентифікації, а також надано рекомендації щодо повідомленнями, які варто надати користувачам в разі невідповідності їх вимогам системи та наведено рекомендації щодо подальших дій.

Таблиця 3.2

Рекомендації щодо інформування користувача про невідповідність авторизації вимогам системи

Ситуация	Как определить ситуацию	Что сообщить и предложить пользователю
Пользователь с учетной записью с типом упрощенная («непроверенная») попытался обратиться к функциям, предоставляемым только для стандартных («проверенных») и/или «подтвержденных» учетных записей.	Проанализировать утверждение SAML с именем assuranceLevel или personTrusted (см. таблицу 5)	При доступе к функциям, требующим стандартной (проверенной) учетной записи: «Для доступа вам необходимо пройти процедуру проверки своих данных. Если ваши личные данные только что прошли проверку, то вам нужно войти в систему повторно.» Ссылка на проверку данных: https://esia-portal1.test.gosuslugi.ru/validate При доступе к функциям, требующим подтвержденной учетной записи: «Для доступа вам необходимо пройти процедуру проверки своих данных и подтверждения личности. Если вы только что подтвердили свою личность, то вам нужно войти в систему повторно.» Ссылка на проверку данных: https://esia-portal1.test.gosuslugi.ru/validate
Пользователь с учетной записью с типом стандартная (проверенная) попытался обратиться к функциям, предоставляемым только для «подтвержденных» учетных записей.	Проанализировать утверждение SAML с именем assuranceLevel (см. таблицу 5)	«Для доступа вам необходимо пройти процедуру подтверждения личности. Если вы только что подтвердили свою личность, то вам нужно войти в систему повторно.» Ссылка на подтверждение личности: https://esia-portal1.test.gosuslugi.ru/confirm
Пользователь с учетной записью с ролью физического лица попытался обратиться к функциям, предоставляемым только для	Проанализировать утверждение SAML с именем globalRole и orgType (см. таблицу 5)	Если необходима роль сотрудника ЮЛ и текущая учетная запись имеет тип «подтверждена»: «Для доступа вам необходимо

ИП / должностных лиц ЮЛ / должностных лиц ОГВ.		войти в систему в качестве сотрудника юридического лица. Если вы являетесь руководителем юридического лица, вы также можете зарегистрировать учетную запись юридического лица» Ссылка для регистрации ЮЛ: https://esia-portal1.test.gosuslugi.ru/org Если необходима роль ИП и текущая учетная запись имеет тип «подтверждена»: «Для доступа вам необходимо войти в систему в качестве индивидуального предпринимателя. Вы также можете зарегистрировать учетную запись индивидуального предпринимателя.» Ссылка: https://esia-portal1.test.gosuslugi.ru/orgs Если необходима роль должностного лица ОГВ и текущая учетная запись имеет тип «подтверждена»: «Для доступа вам необходимо войти в систему в качестве должностного лица органа государственной власти.» Если пользователь имеет упрощенную (непроверенную) /
		стандартную (проверенную) учетную запись, то необходимо его проинформировать о необходимости подтверждения личности. Это является необходимым предварительным условием для возможности получения пользователем роли должностного лица ЮЛ, ОГВ или роли ИП.
Пользователь, аутентифицировавшийся по паролю, попытался получить доступ к функции, требующей аутентификации по электронной подписи	Проанализировать утверждение SAML с именем authnMethod (см. таблицу 5)	«Для доступа вам необходимо использовать средство квалифицированной электронной подписи. Если у вас имеется средство электронной подписи, войдите заново, использовав это средство.» После этого сообщения рекомендуется разместить кнопку вызова единого завершения сессии.

Протягом дії сесії користувач може без повторної аутентифікації увійти в одну або кілька інших систем, підключених до ЄСІА. При виникненні необхідності в одночасному завершенні сесії у всіх системах використовується відповідний сценарій. Єдине завершення сесії необхідно, наприклад, при зміні даних аутентифицированного користувача - в цьому випадку для отримання інформаційними системами в твердженнях SAML оновлених даних користувач повинен здійснити вихід і повторну аутентифікацію в ІКС. Єдине завершення сесії виконується відповідно до профілю Single Logout стандарту SAML. Процес ініціюється користувачем при натисканні кнопки «Вихід» в системі постачальника послуг, який реалізував вказаний сценарій.

Інформаційна система не повинна самостійно ініціювати єдине завершення сесії.

Сценарій включає наступні кроки:

1. Користувач натискає кнопку «Вихід» в системі.
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 учасники існують, ЕСІА відправляє запит <LogoutRequest> кожному з них.
4. Система, що отримала <LogoutRequest>, завершує на своєму боці активну сесію користувача (або перевіряє, що сесія до цього моменту вже неактивна). Потім формує 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 завершення сесії. Якщо якийсь із постачальників послуг не зміг завершити сесію, ЄСІА відображає користувачеві веб-сторінку, що інформує його про те, що процедура не може бути коректно завершена і що користувачеві необхідно перезапустити браузер.
6. Система, яка ініціювала процедуру завершення сесії, обробляє отриманий від ЄСІА відповідь. Наприклад, перенаправляє користувача на веб-сторінку завершення сесії.

3.2 Процедура ідентифікації/автентифікації з використанням стандарту OpenID Connect

OpenID - відкритий стандарт децентралізованої системи аутентифікації, що надає користувачеві можливість створити єдину обліковий запис для аутентифікації на безлічі не пов'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.

Стандарт описує процес комунікації інтернет-ресурсів (Relying Parties), що вимагають аутентифікації, і провайдерів OpenID (OpenID Providers). Існує кілька OpenID провайдерів, які надають хостинг OpenID URL, Аутентифікацію OpenID використовують в тому числі Google, Yahoo !, AOL, LiveJournal, MySpace, IBM, Steam і Orange. Розширення стандарту (the OpenID Attribute Exchange) полегшує передачу даних користувача, таких як ім'я або підлогу, від OpenID провайдера до інтернетресурсу. Поточна версія стандарту, OpenID Connect 1.0, вийшла в лютому 2014 року і була оновленав листопаді 2014 року.

На сайті, наприклад, example.com знаходиться форма входу з єдиним полем введення для OpenID ідентифікатора. Найчастіше поруч з таким полем розташовується логотип OpenID. Для того, щоб авторизуватися на даному сайті за допомогою свого ідентифікатора, наприклад, pupkin.openid-provider.org, зареєстрованого у OpenID провайдера openid-provider.org, користувачеві необхідно ввести свій ідентифікатор в пропоновану на сайті форму входу. Після цього сайт example.com перенаправляє користувача на сайт провайдера. Сайт провайдера запитує у користувача підтвердження, чи дійсно користувач бажає надати інформацію про свого облікового запису. Якщо користувач погоджується, то сайт провайдера перенаправляє користувача назад на сайт залежною боку. При зворотному перенаправлення провайдер передасть інформацію про користувача залежною стороні. OpenID провайдером.

OpenID дозволяє користувачеві використовувати один обліковий запис, зареєстровану у OpenID провайдера, на безлічі інших сайтів. Користувач може вибрати, яку інформацію надати сайту. Обмін інформацією профілю або іншими відомостями, які не описані у специфікації OpenID, може бути реалізований поверх протоколу OpenID, з допомогою додаткових видів обслуговування. Для цього передбачено офіційно підтримуваний протоколом OpenID механізм

розширення протоколу. Існує можливість делегування OpenID. Це означає, що власник якогось доменного імені може використовувати його як синонім (аліаса) до вже існуючого OpenID-ідентифікатором, отриманого у будь-якого провайдера OpenID. Для цього необхідно на сторінку, яка використовується в якості делегата додати кілька мета-тегів.

Система OpenID - децентралізована система. Це означає, що немає будь-якої центральної служби або організації, яка дозволяла б використання системи або реєструвала б запитують аутентифікацію OpenID інтернет-ресурси або провайдерів OpenID. Кінцевий користувач може вільно вибирати, якого провайдера OpenID використовувати, і зберігати Ідентифікатор в разі зміни провайдера OpenID.

Стандарт не вимагає JavaScript або сучасних браузерів, проте схема аутентифікації добре сумісна з підходом AJAX. Це означає, що кінцевий користувач може проходити аутентифікацію на сайті, не покидаючи поточну сторінку. В цьому випадку комунікація інтернет-ресурсу з OpenID провайдером буде проходити у фоновому режимі. OpenID-аутентифікація використовує тільки стандартні HTTP (S) запити і відповіді, тому стандарт не вимагає від користувача установки додаткового програмного забезпечення. Для роботи OpenID не потрібно використовувати cookie або будь-які інші механізми управління сесією. Різні розширення можуть спростити використання OpenID, але не є обов'язковими для використання стандарту.

Механізм роботи:

1) кінцевий користувач ініціює процес аутентифікації на інтернет-сервісі. Для цього він вводить пропонований ідентифікатор в форму входу, представлену на сайті.

2) з висунутого ідентифікатора інтернет-сервіс визначає URL кінцевої точки OpenID провайдера, який використовується кінцевим користувачем. пропонований ідентифікатор може містити тільки Ідентифікатор провайдера. У цьому випадку кінцевий користувач вказує свій заявлений ідентифікатор, взаємодіючи з провайдером.

3) Інтернет-сервіс і OpenID провайдер створюють загальний секретний ключ для коду аутентифікації повідомлення по протоколу Діффі-Хеллмана. За допомогою коду аутентифікації повідомлення інтернет-сервіс аутентифікує

повідомлення від провайдера без додаткових запитів до нього для перевірки автентичності.

4) у режимі checkid_setup інтернет-сервіс перенаправляє браузер користувача на сайт провайдера для подальшої аутентифікації. У режимі checkid_immediate комунікація браузера з провайдером відбувається непомітно для користувача.

5) провайдер перевіряє, авторизовані користувач на сервері і чи хоче він аутентифицироваться на інтернет-сервісі. Специфікація OpenID не описує процес аутентифікації користувача на стороні провайдера.

6) провайдер перенаправляє браузер користувача назад в інтернет-сервіс, передаючи сервісу результат аутентифікації.

7) інтернет-сервіс перевіряє справжність інформації, отриманої від провайдера, включаючи повернутий URL, інформацію про користувача, одноразову мітку (nonce) і підпис повідомлення. Якщо на кроці 3 було створено спільний секретний ключ, то перевірка відбувається за допомогою нього. Якщо ключ створений не був, то інтернет-сервіс відправляє провайдеру додатковий запит (check_authentication) для перевірки автентичності. У першому випадку інтернет-сервіс називається залежною стороною без пам'яті (stateless), а в другому - німий (dumb).

8) у разі успішної перевірки інтернет-сервіс аутентифікує користувача.

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

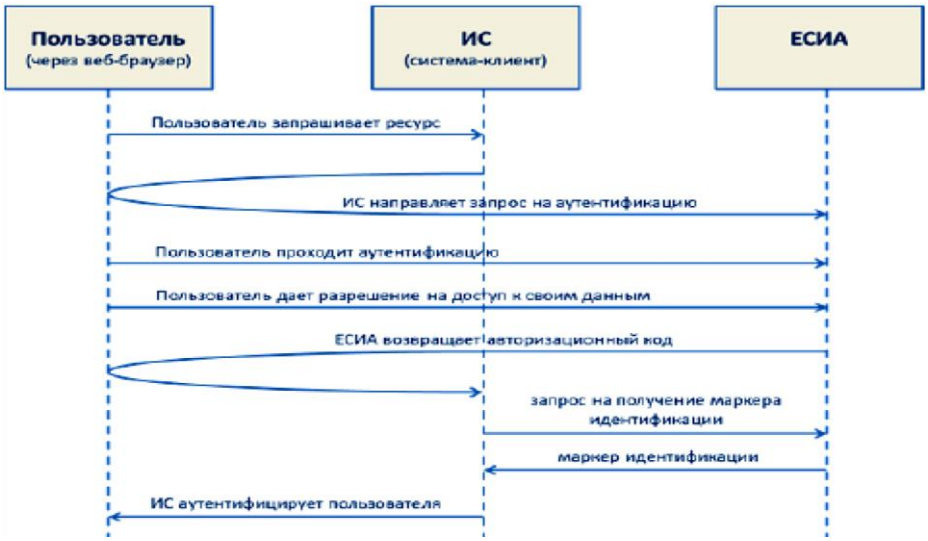


Рис. 3.9 Процедура ідентифікації/автентифікації користувачів з використанням протоколу OpenID Connect

запросити у ЕСІА не тільки маркер ідентифікації, а й маркер доступу (на отримання даних користувача); з використанням маркера доступу і програмного інтерфейсу ЕСІА, заснованого на REST, отримати інформацію про те, співробітником яких організацій є користувач; запросити у користувача, від імені якої організації він буде працювати в даній ІС (якщо користувач є співробітником декількох організацій).

При необхідності ІКС також може перевіряти, чи включений користувач в необхідні системні групи юридичної особи, чи є він керівником організації.

Сценарій з установкою локальної сесії

Як тільки користувач пройшов аутентифікацію, ЄСІА встановлює призначену для користувача сесію, тривалість якої становить 3 години. Факт початку сесії записується в файлі cookie, який зберігається на комп'ютері користувача. Система може встановити для користувача свою «локальну» сесію. При завершенні «локальної» сесії система повинна спрямовувати в ЄСІА новий запит на аутентифікацію.

Сценарій з авторизацією користувача

Система ЄСІА володітиме функціоналом по наданню системі-клієнту інформації, на підставі якої можливе проведення авторизації аутентифицированного користувача. Рішення про авторизацію користувача приймає система, в яку користувач авторизується. Для отримання авторизаційних даних слід використовувати програмний інтерфейс, заснований на архітектурному стилі . У цьому випадку крім маркера ідентифікації система повинна також запросити маркер доступу до потрібних авторизаційним даними. 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 подана на рис.3.10.

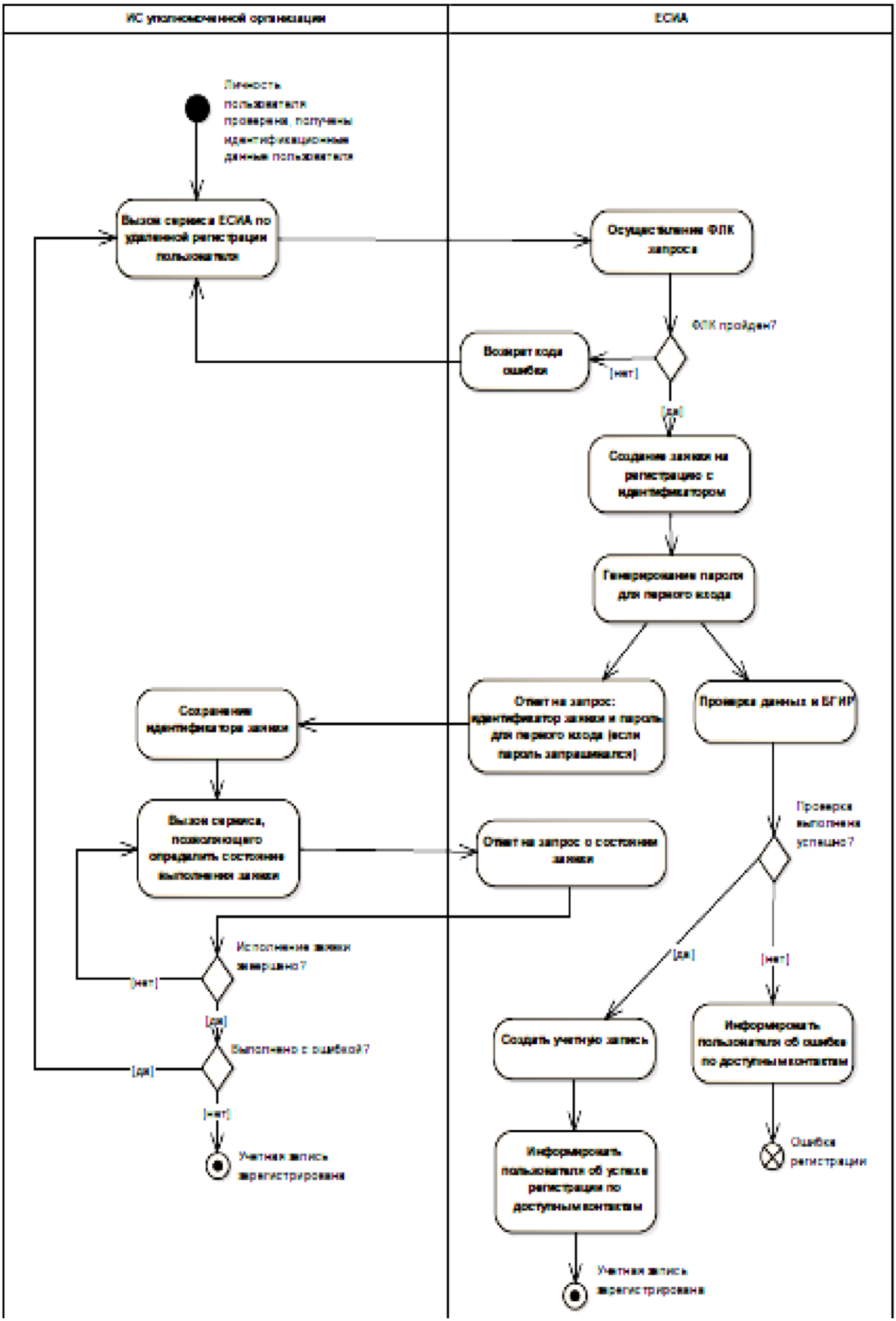


Рис.3.10. Загальна схема реєстрації користувача

3.3 Процедура ідентифікації/автентифікації з використанням стандарту Kerberos

Ще одним методом автентифікації, який, на нашу думку вартий уваги, є протокол Kerberos. Основним недоліком даного протоколу є безпосередня передача реквізитів картки від покупця до продавця. Враховуючи це, можна запропонувати удосконалену систему автентифікації на основі 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)

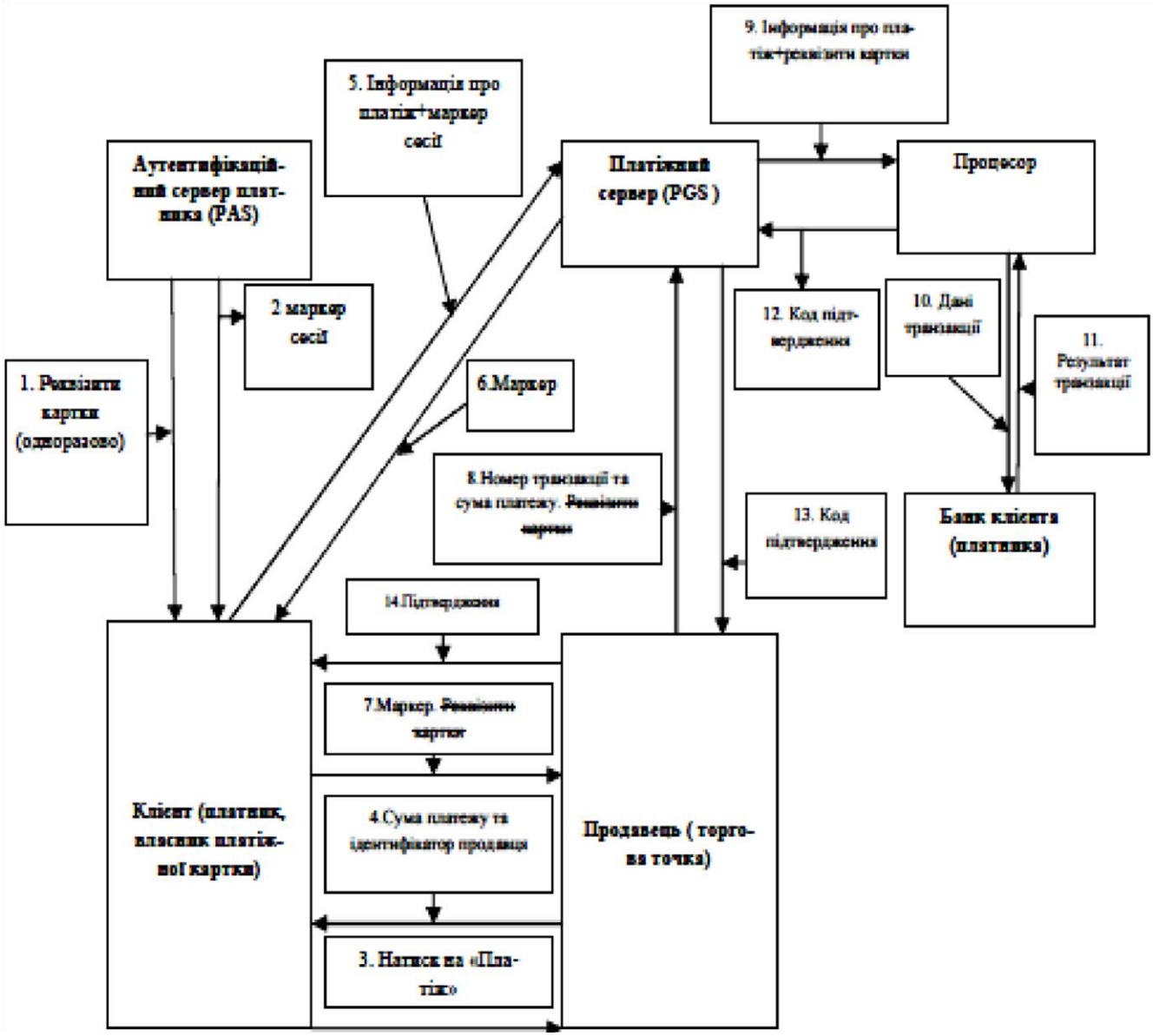


Рис. 3.11. Схема реалізації інтернет-транзакції на основі протоколу автентифікації Kerberos

Наприклад, у схемі інтернет-транзакції на основі системи Kerberos клієнт зв'язується із торговою точкою, а торгова точка у свою чергу – із платіжним шлюзом. У нашому ж випадку, 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 і продавцем (рис. 3.12).

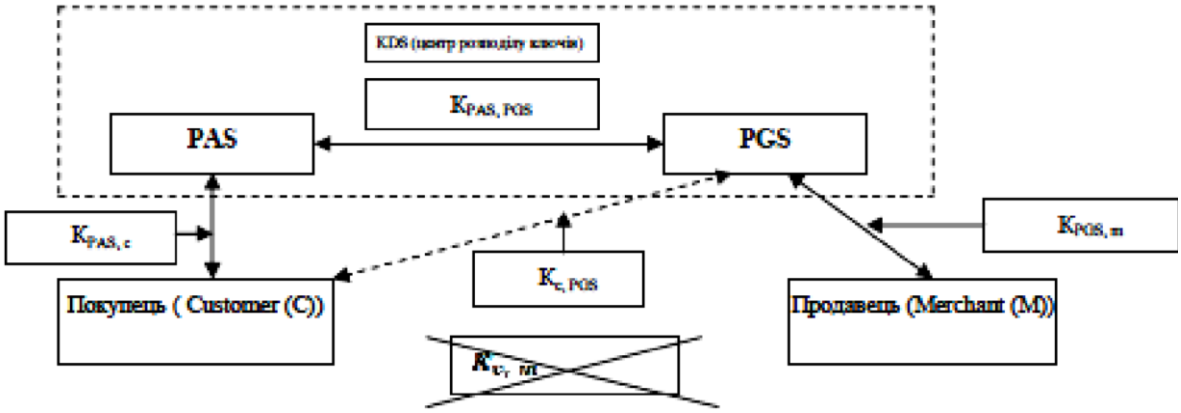


Рис.3.12. Процес обміну ключами в протоколі автентифікації Kerberos

Також, у вище запропонованій системі використовуються два маркери – маркер сеансу (присутній у системі Kerberos) та маркер платежу, який містить інформацію про покупця, продавця та суму платежу.

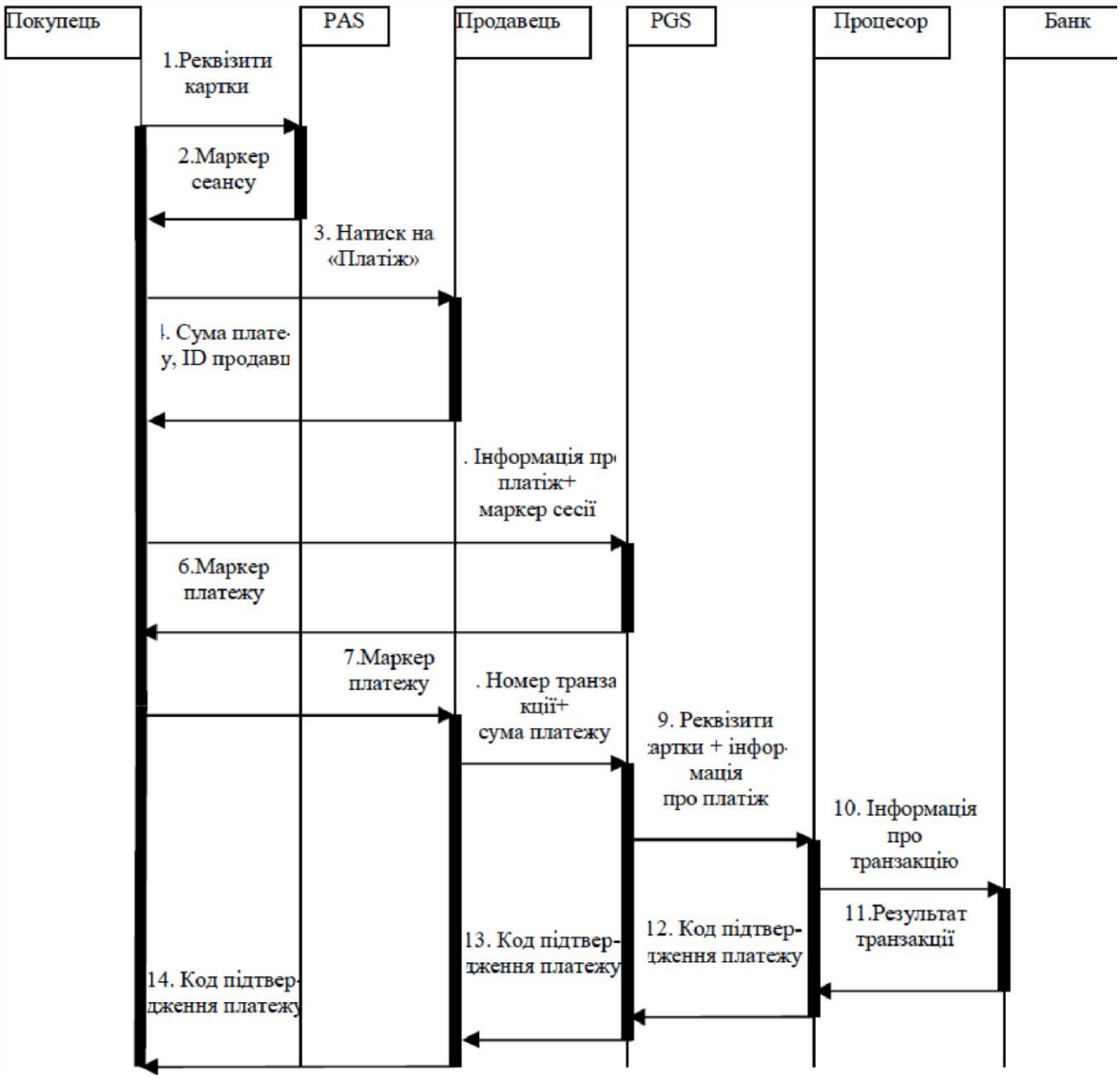


Рис. 3.13. Покрокова діаграма здійснення інтернет-транзакцій в протоколі Kerberos

Як видно з рис. 3.13, платіжний сервер (PGS), який замінив платіжний шлюз, зв'язується, як з покупцем, так і з продавцем, на відміну від існуючої системи Kerberos. При цьому (рис.2.9) спочатку покупець надсилає до аутентифікаційного серверу реквізити своєї картки і отримує натомість маркер сесії. Після цього клієнт надає інформацію про платіж (сума платежу, назва продавця) разом із маркером сесії платіжному серверу (PGS) та отримує від нього маркер платежу. Далі покупець надсилає продавцю цей маркер платежу. Згодом торгова точка надсилає номер транзакції платіжному сервера. Отримавши номер транзакції, PGS здійснює обробку платежу.

Очевидною перевагою запропонованого варіанту протоколу Kerberos є відсутність безпосередньої передачі реквізитів картки від покупця до продавця під час інтернет-платежу. У такий спосіб можна зменшити кількість шахрайств, пов'язаних із перехопленням реквізитів картки. У запропонованій схемі протоколу продавцю передаються маркери платежу замість інформації по картці.

І, таким чином, ні продавець, ні зловмисник, який зламує базу даних, не мають можливості нелегально отримати реквізити картки. Варто такожзазначити, що маркер криптографічно безпечний і дійсний лише для конкретного продавця, тож отримання його через прослуховування каналів нічого не дає зловмиснику.

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

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

Багатофакторна автентифікаційна система базується на трансакційному ідентифікаційному коді (TIC (Transaction Identification CODE)) та на службі коротких повідомлень (SMS(Short Message Service)) для створення додаткового рівня безпеки, який відсутній при традиційній автентифікації за типом ім’я користувача / пароль. Цей код схожий на одноразовий пароль (OTP (One Time Password)), але забезпечує більш надійну автентифікації, а також використовується лише один раз. TIC засвідчує, що поточна трансакція була ініційована саме тією особою, а не зловмисником, яка є істинним власником рахунку (банківської картки). TIC-коди володіють певними властивостями, а саме: створюються банком покупця; 32 бітними або 64 бітними псевдо-випадково згенерованими кодами; можуть являти собою складну послідовність цифр або комбінацію цифрових і буквено-цифрових символів; кожна трансакція вимагає унікального коду для автентифікації, тобто кожен код використовується лише один раз. Механізм генерації кодів є суворо конфіденційним та передбачає обмежений доступ до них та лише уповноважених на це працівників фінансової установи. Банк зберігає номер телефону клієнта, щоб згодом надіслати SMS для підтвердження транзакції. Стільникова мережа використовує окремий канал для передачі і прийому SMS. Отже, багатофакторна автентифікація використовується для перевірки покупця та транзакції відповідно до наступних кроків:

1) Базова автентифікація: Спочатку покупець здійснює вхід на веб-сервер, використовуючи призначений йому веб-ім’я та пароль для базової автентифікації;

2) ТІС-автентифікація: Після успішної автентифікації покупця за допомогою його веб-імені та пароля, веб сервер зажадає ввести ТІС (друга автентифікація). Далі покупець розшифровує та вводить ТІС для доведення своєї справжності автентифікаційному серверу та однозначної ідентифікації транзакції;

3) SMS-підтвердження: Після успішної ТІС-автентифікації, третьою автентифікацією являється SMS-підтвердження. Покупець отримує SMS із деталями транзакції, які необхідні для ідентифікації та розпізнавання ініціатора транзакції. За допомогою SMS покупець надсилає підтвердження транзакції («ТАК») або скасовує її («НІ»).

Механізм багатофактрної автентифікації передбачає наступні кроки :

1) клієнт отримує логін та пароль у своєму банку при відкритті рахунку або маючи 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 платіжного засобу;

5) покупець вводить деталі платежу;

6) клієнт не може здійснити транзакцію без ТІС. Треба мати на увазі, що ТІСи захищені паролем на мобільному телефоні, і цей пароль перед використанням в трансакції буде дешифрований з допомогою одного із ТІС шифрів.

7) уся сукупність трансакційних записів разом з ТІС буде далі зашифрована та передана серверу для обробки.

8) автентифікаційний сервер банку розшифровує отриману інформацію про транзакцію та витягує звідти ТІС. Сервер перевіряє отриманий від покупця код, порівнюючи його із кодом, збереженим разом із інформацією про рахунок клієнта, а також 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 надсилає повідомлення про помилку.

9) якщо TIC автентифікація є успішною, тоді авторизаційний сервер генерує текст 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).

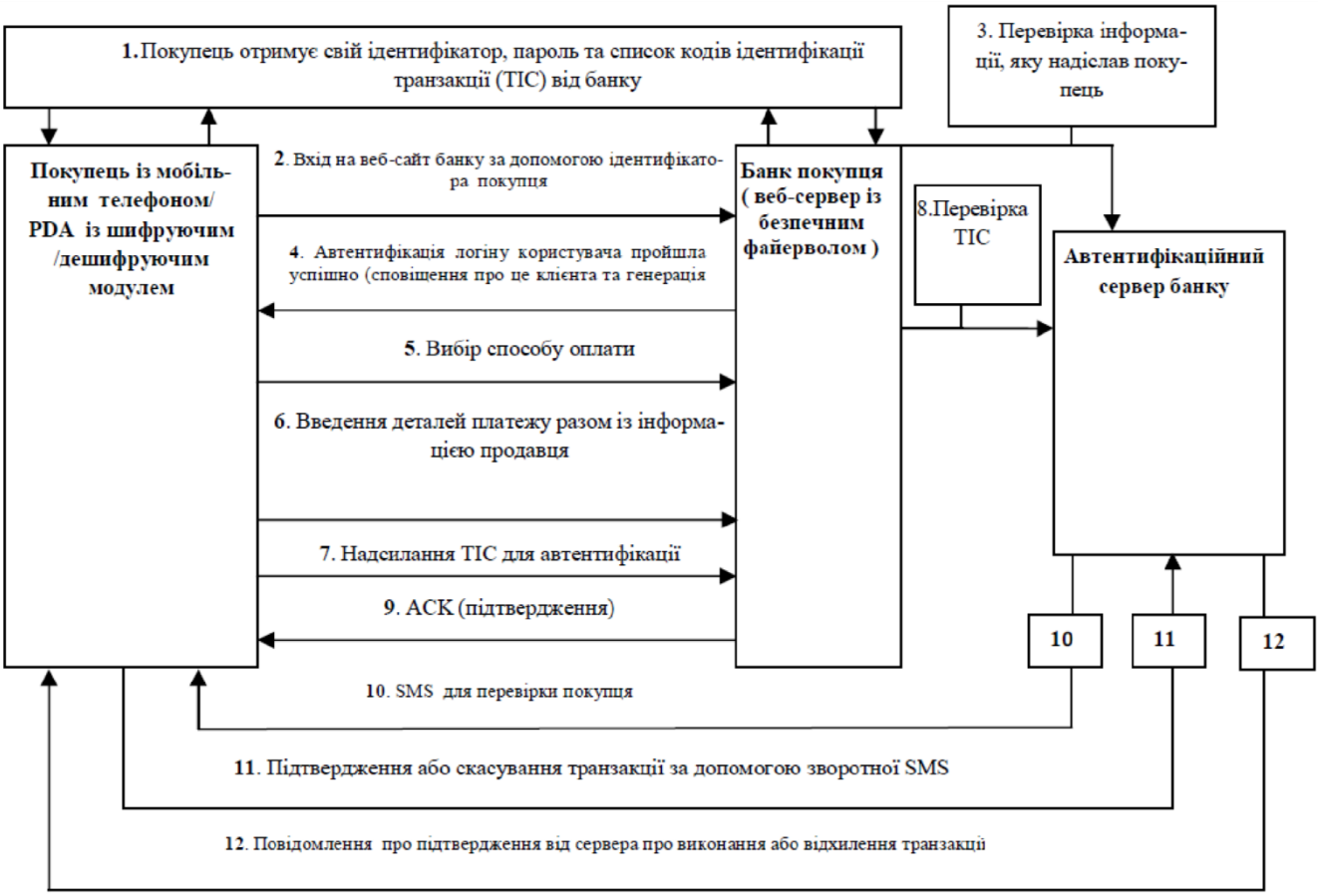


Рис. 3.14. Потік даних у протоколі багатофакторної ідентифікації/автентифікації

У вищеописаному протоколі TIC коди є найбільш уразливими даними, які зберігаються на 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 TIC кодів і обирає будь-який код з цього списку, щоб розпочати трансакцію. Цей вибір коду автоматично розшифровує його та автоматично виводить на екран користувача. Це також призводить до переміщення обраного коду із списку у середовище клієнта.

Локальний пароль є ключем розшифрування ТІС коду та є відомий лише клієнту.

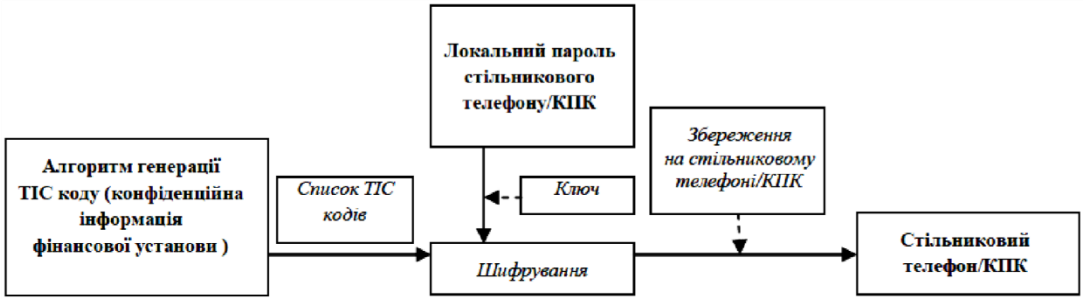


Рис. 3.15.Захист ТІС коду в середовищі покупця

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 для її власника, існує цілий ряд нормативно-правових документів. Використовується досить дороге технічне обладнання, запроваджуються строго регламентовані організаційні заходи, однак все це не може гарантувати у повній мірі бажаний результат. Цьому є певний ряд причин, які 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 інформаційної

безпеки; відсутня система менеджменту та управління

інформаційною безпекою.

Під поняттям інформаційної безпеки будемо розуміти стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Для вирішення проблеми забезпечення інформаційної безпеки, необхідно чітко визначити та сформулювати цілі та задачі захисту інформації. Крім того,

потрібно ясно розуміти те, що чим конкретніше вони сформульовані, чим краще визначений комплекс обмежень та якість ресурсів, тим вірогідніше отримання бажаного результату. Якщо ціль захисту інформації по своєму характеру нескладна, то її реалізація цілком можлива і не вимагає використання серйозних ресурсів. Проте, чим більші вимоги ставляться до системи захисту інформації, 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. Найперше у таких системах потрібно робити акцент не на властивості кожного окремого елемента, а на їх взаємодії. Саме завдяки цьому система набуває таких специфічних властивостей, які не притаманні жодному з даних елементів.

Базові напрями організації захисту інформації ІКС (рис.3.16)

Для побудови надійної системи захисту інформації в сучасних інформаційнокомунікаційних системах та мережах потрібно спочатку визначити ряд можливих загроз для інформаційних ресурсів.

У справі забезпечення інформаційної безпеки успіх може принести тільки комплексний підхід. Для захисту інтересів суб'єктів інформаційних в сучасних ІКС необхідно поєднувати заходи наступних рівнів:

законодавчого (нормативно-правовий);

адміністративного (організаційного, накази та інші дії керівництва організацій, пов'язаних з інформаційними системами, що захищаються);

процедурного (заходи безпеки, орієнтовані на людей); програмно-технічного (інженерно-технічний, апаратний, програмний).

Законодавчий рівень є найважливішим для забезпечення інформаційної безпеки. Більшість людей не здійснюють протиправних дій не тому, що це технічно неможливо, а тому, що це засуджується і/або карається суспільством, тому, що так поступати не прийнято. Основними властивостями інформації є цілісність, конфіденційність і доступність. Порушення однієї з них може спричинити численні зміни, чи навіть цілковиту втрату цінної інформації. Саме модель можливих загроз, допоможе впоратись із цією проблемою. Беручи до уваги всю необхідність та варіанти створення інформаційної безпеки, можна побудувати своєрідну «піраміду» комплексної системи захисту інформації в інформаційно-комунікаційних системах та мережах. Нормативно-правовий захист інформації являється таким собі фундаментом побудови всієї інформаційної безпеки підприємства, організації, установи. Як відомо, право – це

сукупність установлених чи санкціонованих державою загальнообов’язкових правил поведінки (норм), дотримання яких забезпечується методами державного впливу. Правовий елемент інформаційного захисту складають законодавчі засоби захисту інформації, які є множиною нормативно-правових актів (конвенції, закони, укази, постанови, нормативні документи тощо), що діють у певній державі і забезпечують юридичну підтримку для розв’язання задач захисту інформації. В Україні Основним Законом являється Конституція.

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

Для створення правового захисту підприємства, організації, установи, необхідно організувати юридично закріплені правові взаємовідносини між державою та підприємством, щодо правомірності використання інформаційної безпеки, між підприємством та персоналом щодо обов’язковості дотримання порядку захисту інформаційних ресурсів. Організаційний захист інформації – регламентація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі.

На даному етапі побудови системи захисту потрібно 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. Невід'ємною частиною є організація роботи з документами та документованою інформацією. Обов'язкове використання технічних заходів, таких як передавачі, приймачі, сканери, відеокамери, шумогенератори та техніка перехоплення. Особливо важливим моментом є детальний аналіз всіх можливих загроз, а також організація з проведення систематичного контролю.

Інженерно-технічний захист інформації виступає невід'ємною частиною побудови комплексної системи захисту інформації, адже саме він дозволяє попередити несанкціонований доступ до інформаційних ресурсів, запобігти витоку інформації технічними каналами зв'язку.

Основними задачами цієї ланки інформаційної безпеки є: попередження проникнення зловмисника до інформації з метою її знищення, змінення чи викрадення; захист носіїв інформації від їх знищення в результаті різного впливу; запобігання витоку інформації різними технічними каналами.

Апаратний захист інформації розуміє під собою наявність апаратного забезпечення, яке в певній мірі гарантує ступінь захищеності важливих даних. До апаратних засобів захисту інформації відносяться різні електронні, електронномеханічні та електронно-оптичні прилади. В наш час існує широкий спектр таких приладів, але найбільшого використання набули такі:

спеціальні регістри для збереження реквізитів захисту: паролів, кодів ідентифікації, грифів або рівнів секретності; пристрої для вимірювання індивідуальних характеристик людини (голоси, відбитки) з метою його ідентифікації; схеми переривання передачі інформації в лінії зв'язку з метою періодичної перевірки адреси видачі даних; пристрої для шифрування інформації (криптографічні методи).

Програмний захист інформації – складає сукупність програмного забезпечення, для ідентифікації користувачів, контролю доступу, шифрування інформації, знищення тимчасових файлів, тестового контролю системи захисту та інше. Використання програмних засобів захисту інформації має цілий ряд переваг – універсальність, гнучкість, надійність, простота у використанні то можливість модифікації.

Висновки до третього розділу

Аутентифікація - це фактично процес перевірки індивідуальності суб'єкта, яким, у принципі, може бути не тільки людина, але і програмний процес. Узагальнюючи, можна сказати, що аутентифікація індивідів можлива за допомогою інформації, яка зберігається в різній формі. Наприклад, це може бути: пароль, особистий номер, криптографічний ключ, мережева адреса комп'ютера в мережі; смарт-карта, електронний ключ; зовнішність, голос, малюнок райдужної обо-лонки ока, відбитки пальців і інші біометричні характеристики користувача.

Аутентифікація дозволяє обґрунтовано і вірогідно розмежувати права

доступу до інформації, яка знаходиться в загальному користуванні. Однак виникає проблема забезпечення цілісності і вірогідності інформатизації. Користувач має бути впевненим, що одержує доступ до інформації з джерела, що заслуговує довіри, і що дана інформація не моди-фікувалася без відповідних санкцій.

Пошук відповідності методом «один до одного» (за одним атрибутом) називається верифі-кацією. Такий метод відрізняється високою швидкістю і висуває мінімальні вимоги до об-числювальної потужності комп'ютера. Пошук методом «один до багатьох» нази-вається ідентифікацією. Реалізувати подібний ал-горитм зазвичай не тільки складно, але й дорого. Наприклад, в операційних системах Windows для аутентифікапії вимагаються два об'єкти - ім'я користувача і пароль. При аутентифікації за технологією ідентифікації відбитків пальців ім'я вводиться для реєстрації, а відбиток пальця за-міняє пароль. У цьому випадку ім'я користувача є покажчиком для одержання його обліко-вого запису і перевірки відповідності «один до одного» між шаблоном зчитаного під час реєстрації відбитка і раніше збереженим шаблоном для даного імені користувача. За іншого способу введений під час реєстрації шаблон відбитка пальця необхідно зіставити з усім набором збережених шаблонів.

У виборі способу аутентифікації має сенс враховувати кілька основних факторів: цінність інформації; вартість програмно-апаратного забезпечення аутентифікації; продуктивність системи; відношення користувачів до застосовуваних методів аутентифікації; специфіку (призначення) інформаційного комплексу, що захищається. Очевидно, що вартість, а отже, якість і надійність засобів аутентифікації мають бути пропорційними важливості інформації. Окрім того, підвищення продуктивності комплексу, як правило, супроводжується його дорожчанням (хоча і не завжди).

ВИСНОВКИ

Основними завданнями забезпечення безпеки комп'ютерних систем є аутентифікація, керування доступом, аудит, забезпечення конфіденційності, доступності та цілісності даних. Сучасні засоби підтримки безпеки ґрунтуються на таких криптографічних технологіях, як алгоритми із секретним і відкритим ключами, гібридні крип-тосистеми, цифрові підписи і сертифікати. Аутентифікація дає змогу впевнитися, що користувач є тим, за кого себе видає, і може бути допущений у систему. Для підтвердження особи користувача звичайно використовують пароль. Сучасні технології аутентифікації дають змогу уникнути передавання пароля каналом зв'язку у незашифрованому вигляді. Керування доступом (авторизація) дає змогу визначити дії, які авторизова¬ний користувач може виконувати із різними об'єктами у системі. Авторизація реалізована на основі визначення списків контролю доступу, пов'язаних із об'єктами у системі, а також списків можливостей, пов'язаних із окремими користувачами. Можна сказати, що створення комплексної системи захисту інформації потребує глобального підходу до всіх аспектів цього питання. Саме поетапне виконання правового, організаційного, інженерно-технічного, апаратного та програмного рівнів побудови інформаційної безпеки дасть можливість створити цілісну систему для забезпечення надійної безпеки інформації. Вивчення та побудова моделі загрози дасть можливість виявити слабкі місця у системі та усунути їх. Отже, проблеми захисту інформації в сучасних інформаційно-комунікаційних системах та мережах потребують комплексного підходу у вирішенні питання інформаційної безпеки.

1. Перспективним напрямком розвитку систем аутентифікації є розвиток біометричних систем. Основні зусилля в цьому напрямку спрямовані на розвиток і вдосконалення апаратно-програмних засобів, які дозволили б досягти одночасного і значного зменшення рівня помилок першого та другого роду, а також були захищені від спуфінг-загроз. Масовий випуск таких систем дозволить значно зменшити їх вартість.

2. Більшість систем аутентифікації майбутнього будуть побудовані за комбінованим типом – з одночасним використанням двох і більше методів аутентифікації (контактні токени із вбудованими чипами безконтактної аутентифікації та захищені pin-кодом, токени із вбудованими засобами біометричної аутентифікації тощо).

3. Розвиток токенів можливий за наступними напрямками: мініатюризація, розвиток і вдосконалення безконтактних інтерфейсів (захищеність інформаційного каналу, мінімізація енерговитрат), збільшення строку служби, вживлення в організм людини.

4. У найближчому майбутньому частину систем аутентифікації на основі символьного пароля буде замінено на системи на основі графічного пароля, як більш захищені. Проте певна незручність введення графічного пароля обмежить його застосування в найпростіших системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
2. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99 р. № 22.
3. НД ТЗІ 1.1-004-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.99 р. № 22.
4. Про електронні документи та електронний документообіг: закон України від 22 травня 2003 р. № 851-IV // Урядовий кур'єр — 2003. — №119 – 2 липня. – С. 1– 6.
5. Про електронний цифровий підпис: закон України від 22 травня 2003 р. № 851-IV // Урядовий кур'єр — 2003. — №119 – 2 липня. – С. 1– 6.
6. Анин Б. Защита компьютерной информации. — СПб.: БХВ-Петербург, 2000. — 384 с.
7. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV,2009. – 608 с., іл.
8. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО «ТИД «ДС», 2004. – 992 с.
9. Дронь М.М., Малайчук В.П., Петренко О.М. Основи теорії захисту інформації: Навч. посібник. – Д.: Вид-во Дніпропетр. ун-ту, 2001. – 312 с.
10. Конахович Г.Ф., Корченко О.Г., Юдін О.К., Захист інформації в мережах передачі даних: Підручник. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с., іл.
11. Сарбуков А. Аутентификация В Компьютерных Системах / А. Сарбуков А. Грушо // Системы безопасности. – 2003. - №5 (53). – С. 25-29.
12. Чепиков О. Особенности применения Двухфактор-Ной аутентификации / О. Чепиков // Информационная безопасность. – 2005. – №3. – С.35-41.

13. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008. – 544 С.
14. Шрамко В. Н. Защита компьютеров: электронные Системы идентификации и аутентификации / В. Н. Шрамко // PCWeek/RE. – 2004. - №12.
15. ImagiPass 1.1. – Режим доступу: Www. atlantis-Wordprocessor. com /en/imagipass.
16. BioAPI – Режим доступу: Www. bioapi. org.
17. Новые системы паролей. Http://windows2008. At.Ua.
18. Системы идентификации Режим доступу: Http://acoder. org
19. Графический пароль не даёт смотрящему украсть себя. – Режим доступу: Http://www. membrana. ru.
20. Задонский А. Ю. Вопросы аутентификации в современных информационных системах. – Режим доступу: Http://www. compserv. ru.
21. Азаров Д. Особливості механізму вчинення злочинів у сфері комп'ютерної інформації // Юридична Україна. – 2004. – № 7 (19). – С. 64 – 68
22. Баранов А.А., Брыжко В.М., Базанов Ю.К. Защита персональних данных. ОАО «КП ОТИ». К.,1998. – 128 с.
23. Мастяниця Й.І., Соснін О.В., Шиманський Л.Є. Захист інформаційних ресурсів України: проблеми і шляхи їх розв'язання. - К.: Національний інститут стратегічних досліджень, 2000. - 98 с.
24. Василюк В.Я., Климчук СО. Інформаційна безпека держави : Курс лекцій. - К.: КНТ, Видавничий дім «Скіф», 2008. - 136с,
25. Баранов О.А. Інформаційне право України: Стан, проблеми, перспективи. -К.: Видавничий дім «СофтПрес», 2005. - 316с.
26. Богуш В.М., Юдін О.К. Інформаційна безпека держави. - К.: «МК-Прес», 2005.432с.
27. Почерцов Г.Г. Информационные войны. Основы военно-коммуникативных исследований. - М.:. Рефл-бук, К.: Ваклер, 2000. - 576с.
28. Расторгуев СП. Информационная война. - М.: Радио и связь, 1999. -416с.
29. Расторгуев СП. Философия информационной войны. - М: Московский психологосоциальный институт, 2003. - 486с.
30. Соснін О.В., Шименський Л.Є Про правові основи удосконалення системи державного управління інформаційними ресурсами. Політологічний вісник. 36. наук, праць, №10. - К.: Т-во «Знання України», 2002. - с.212-219

31. Баранов А.А. Концептуальные вопросы информационной безопасности Украины // Безопасность информации. - 1995, №2. - с.4-10
32. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. - СпБ.: БХВ - Петербург, 2003. - 688с.
33. 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. - 178с.
34. Петренко СА., Курбатов В.А. Политики информационной безопасности.