МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра комп'ютерних наук

Пояснювальна записка

до кваліфікаційної роботи
другого (магістерського) рівня

на тему **ДОСЛІДЖЕННЯ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ**

Виконав: студент 2 курсу, групи ІКК–2.1,
спеціальності 122 Комп'ютерні науки
Перуцький О.В.

Керівник Йона Л. Г.

Рецензент Григор'єва Т. І.

Одеса – 2023

Д О В І Д К А

кафедри КН про виконану магістерську роботу

студента 2 курсу ФКПІ та КН групи ІКК–2.1

Перуцького Олега Валерійовича

на тему Дослідження методів автентифікації користувача в телекомунікаційних системах

Висновок нормоконтролера пасновальна записка до кваліф. роботи викон з незначними порушеннями ДСТУ. Оформлено згідно вимог КПІ

Нормоконтролер викл. каф. ТК 15.12.2023 р. Клімішина Г.В.

(науковий ступінь, вчене звання, посада) (підпис, дата) (і. б. прізвище)

Висновок відповідального на наявність плагіату згідно з сертифікатом ID 1015733224 унікальність роботи підтверджено

Відповідальна особа викл. каф. ТК 15.12.2023 Клімішина ГВ

(науковий ступінь, вчене звання, посада) (підпис, дата) (і. б. прізвище)

Попередня експертиза (захист) магістерської роботи

(бакалаврської роботи чи магістерської роботи)

студ. Перуцького О.В. проведена "15" грудня 2023 р.

(прізвище і.б.)

Висновки Кваліфікаційна робота виконана у повному обсязі. В роботі проведено дослідження методів автентифікації користувача в телекомунікаційних системах. Кваліфікаційна робота відповідає вимогам до випускних кваліфікаційних робіт зі спеціальності 122 Комп'ютерні науки та рекомендована до захисту.

Члени комісії _____ к.т.н., доц. Соловецька І.М.

(підпис) (науковий ступінь, вчене звання, посада, прізвище і. б.)

_____ к.т.н., доц. Рудий О.П.

(підпис) (науковий ступінь, вчене звання, посада, прізвище і. б.)

_____ к.т.н., доц. Розенвассер Д.М.

(підпис) (науковий ступінь, вчене звання, посада, прізвище і. б.)

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра ком'ютерних наук
Освітній ступінь магістр
Галузь знань 12 Інформаційні технології
Спеціальність 122 Комп'ютерні науки

ЗАТВЕРДЖУЮ
Завідувач кафедри КН
к.т.н., доц.
І.М. Соловська
"25" 09 2023 року

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ

Перуцького Олегу Валерійовичу

1. Тема роботи: Дослідження методів автентифікації користувача в телекомунікаційних системах

керівник роботи Йона Лариса Григорівна, к.т.н., доцент каф. КІ та ІТ

затверджені наказом закладу вищої освіти від 25.09.2023 р. № 1959

2. Строк подання студентом роботи 11.12.2023

3. Вихідні дані до роботи Дослідити сучасні алгоритми автентифікації користувача та надати рекомендації щодо підвищення кіберзахисту підприємства

4. Зміст розрахунково–пояснювальної записки

Розділ 1: Огляд методів ідентифікації та автентифікації користувача.

Розділ 2: Метод автентифікації.

Розділ 3: Протоколи автентифікації.

Розділ 4: Застосування методів автентифікації користувача.

5. Перелік графічного матеріалу (зазначенням обов'язкових креслень)

Слайд 2 Мета роботи

Слайд 3 Протоколи автентифікації.

Слайд 4 Фактори автентифікації.

Слайд 5 Біометрична автентифікації.

Слайд 6 Автентифікація з використанням одноразових паролів.

Слайд 7 Методи автентифікації

Слайд 8 Проста автентифікація

Слайд 9 Електронний цифровий підпис

Слайд 10 Рекомендації щодо підвищення кіберзахисту підприємства

Слайд 11 Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1			
2			
3			

7. Дата видачі завдання 25.09.2023

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Вступ	25.09.23 – 30.09.2023	вик
2	Огляд методів ідентифікації та автентифікації користувача	01.10.23 – 15.10.2023	вик
3	Метод автентифікації	16.10.23 – 29.10.2023	вик
4	Протоколи автентифікації	30.10.23 – 05.11.2023	вик
5	Застосування методів автентифікації користувача	06.11.23 – 13.11.2023	вик
6	Висновки та рекомендації	14.11.23 – 30.11.2023	вик
7	Перелік джерел посилань	01.12.23 – 07.12.2023	вик
8	Додаток А	08.12.23 – 11.12.2023	вик

Студент _____ О.В. Перуцький
(підпис)

Керівник роботи _____ Л.Г. Йона
(підпис)

ВІДГУК

на магістерську роботу здобувача Перуцького О. В.

на тему: «Дослідження методів автентифікації користувача в телекомунікаційних системах»

Тема магістерської роботи здобувача Перуцького О. В. є актуальною та пов'язана з проблемою автентифікації користувача. Процес підтвердження справжності користувача необхідний для того, щоби захистити інформаційну систему від неправочинних користувачів та надати можливість працювати з інформацією тільки тому, хто має на це право.

В магістерській роботі надається результат дослідження сучасних криптографічних методів та аналіз систем захисту інформації від неправочинних користувачів. Результати дослідження представлені у тезах доповіді «Дослідження методів автентифікації користувача» на IX Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Гуманітарний і інноваційний ракурс професійної майстерності: пошуки молодих вчених».

Магістерська робота Перуцького О. В. відповідає вимогам до випускних кваліфікаційних робіт магістрів та заслуговує оцінки «добре».

Здобувач Перуцький О. В. заслуговує присвоєння кваліфікації магістр з комп'ютерних наук за заявленою спеціальністю 122 Комп'ютерні науки.

Керівник, к.т.н., доц. кафедри
Комп'ютерної інженерії
та інноваційних технологій Йона Л. Г.

РЕЦЕНЗІЯ

на магістерську роботу здобувача Перуцького О. В.

на тему: «Дослідження методів автентифікації користувача в телекомунікаційних системах»

У магістерській роботі здобувача Перуцького О. В. розглянуто сучасні алгоритми, які використовуються для захисту цілісності інформації та можливості перевірки справжності користувача шляхом проведення процедур ідентифікації та автентифікації.

Актуальність питання полягає в тому, що в роботі досліджуються сучасні алгоритми криптографічного захисту інформації за їх призначенням. Крім того, проведено аналіз щодо методів багатофакторної автентифікації та частоти використання методів автентифікації за певними критеріями.

Текстова частина магістерської роботи викладена послідовно, чітко, технічно та грамотно.

Проте в роботі є деякі недоліки:

- бажано при доведенні результатів аналізу щодо частоти використання методів автентифікації за певними критеріями, дати пояснення відповідності позначень у відсотковому еквіваленті;

- в роботі не достатньо уваги приділено протоколам з використанням комбінованих методів біометричної автентифікації.

Але вказані недоліки не знижують цінності виконаної роботи.

Магістерська робота Перуцького О. В. відповідає вимогам до випускних кваліфікаційних робіт магістрів та заслуговує оцінки «добре».

Здобувач Перуцький О. В. заслуговує присвоєння кваліфікації магістр з комп'ютерних наук за заявленою спеціальністю 122 Комп'ютерні науки.

Рецензент
завідувачка кафедри
Інформаційних технологій,
к.т.н., доцент Т.І.Григор'єва

UNICHECK
by Turnitin

Имя пользователя:
Анна Серединко

ID проверки:
1016039479

Дата проверки:
28.12.2023 10:34:14 EET

Тип проверки:
Doc vs Internet + Library

Дата отчета:
28.12.2023 16:05:00 EET

ID пользователя:
100001433

Название файла: MP_Перуцького_11_12_2023_итог

Количество страниц: 58 Количество слов: 8748 Количество символов: 71946 Размер файла: 12.56 MB ID файла: 1015733224

Обнаружены модификации текста (могут влиять на процент совпадений)

29.9%
Совпадения

Наибольшее совпадение: 16.6% с источником из Библиотеки (ID файла: 1015712723)

13.1% Источники из Интернета | 275 ..... Страница 60

21% Источники из Библиотеки | 45 ..... Страница 61

0% Цитат

Исключение цитат выключено

Исключение списка библиографических ссылок выключено

8.29% Исключений

Некоторые источники исключены автоматически (фильтры исключения: количество найденных слов меньш...

7.85% Исключений из Интернета | 500 ..... Страница 62

0.69% Исключенного текста из Библиотеки | 31 ..... Страница 65

Модификации

Обнаружены модификации текста. Подробная информация доступна в онлайн-отчете.

Замененные символы | 896

Подозрительное форматирование | 2 страницы

РЕФЕРАТ

Текстова частина магістерської роботи: 55 с., 22 рисунки, 2 таблиці, 1 додаток, 6 джерел.

АВТЕНТИФІКАЦІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ЕЛЕКТРОННИЙ ПІДПИС, ІНФОРМАЦІЙНО–КОМУНІКАЦІЙНА СИСТЕМА, ПАРОЛЬ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ, PIN–КОД.

Об'єкт дослідження – методи автентифікації користувача в телекомунікаційних системах.

Мета роботи – дослідити методи автентифікації користувача в телекомунікаційних системах. Визначити принципи побудови системи підтвердження справжності користувача в телекомунікація. Сформулювати рекомендації щодо підвищення кіберзахисту підприємства.

Метод дослідження – моделі автентифікації користувачів в телекомунікаційних системах.

У магістерській роботі вивчається розвиток та напрямок впровадження сучасних методів автентифікації користувача в телекомунікаційних системах. Визначається принципи побудови системи підтвердження справжності користувача в телекомунікаціях. Класифікуються фактори автентифікації користувача. Досліджується частота використання методів автентифікації у системах захисту за певними критеріями. Сформуються рекомендації щодо підвищення кіберзахисту підприємства.

Матеріали роботи можуть бути застосовані при впровадженні та експлуатації системи безпеки IT систем та мереж підприємства (організації, установ).

ABSTRACT

The text part of the master's thesis: 53 pp., 22 images, 2 chart, 1 addition, 6 sources.

AUTHENTICATION, INFORMATION SECURITY, ELECTRONIC SIGNATURE, INFORMATION AND COMMUNICATION SYSTEM, PASSWORD, SOFTWARE, ELECTRONIC DOCUMENT SYSTEM, PIN CODE.

The object of research is methods of user authentication in telecommunication systems.

The purpose of the work is to investigate methods of user authentication in telecommunication systems. Determine the principles of building a user authentication system in telecommunications. Formulate recommendations for improving the enterprise's cyber protection.

Research method – user authentication models in telecommunication systems. The master's work studies the development and direction of implementation of modern methods of user authentication in telecommunication systems. The principles of building a user authentication system in telecommunications are defined. User authentication factors are classified. The frequency of using authentication methods in protection systems according to certain criteria is studied. Recommendations will be made to increase the cyber protection of the enterprise.

The work materials can be applied in the implementation and operation of the security system of IT systems and networks of the enterprise (organization, institution).

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАК

КС – комп'ютерна система

ПЗ – програмне забезпечення

ПЕОМ – персональна електронна обчислювальна машина

СЗІ – система захисту інформації

IP – Internet Protocol (міжмережвий протокол)

PAP – Password Authentication Protocol (протокол парольної автентифікації)

PIN – Private Identification Number (персональний ідентифікаційний номер)

PKI – Public Key Infrastructure (інфраструктура відкритих ключів)

SSO – Single Sign–On (система однократної автентифікації)

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАК

КС – комп’ютерна система

ПЗ – програмне забезпечення

ПЕОМ – персональна електронна обчислювальна машина

СЗІ – система захисту інформації

IP – Internet Protocol (міжмережний протокол)

PAP – Password Authentication Protocol (протокол парольної автентифікації)

PIN – Private Identification Number (персональний ідентифікаційний номер)

PKI – Public Key Infrastructure (інфраструктура відкритих ключів)

SSO – Single Sign–On (система однократної автентифікації)

ВСТУП

З розвиненням інформаційних технологій майже у всіх сферах життя людини, виникає проблема із захистом інформаційних систем. Технічний прогрес в інформаційних технологіях стрімко розвивається, тому і зловмисники, які хочуть заволодіти інформацією, постійно удосконалюють свої знання та вигадують нові способи заволодіння даними.

Під час обробки інформації з pfrhbnbv доступом повинен забезпечуватися її захист від несанкціонованого перегляду, змін, видалення, копіювання, поширення. У разі, коли йдеться про таємну інформзакритим ацію, то вона має передаватися по каналам захищеного зв'язку або здійснюватися за допомогою технічного чи криптографічного захисту інформації.

Спробою захистити інформацію від несанкціонованого доступу так чи інакше вирішувались на протязі всієї історії розвитку людства. Розвиток обчислювальної техніки, нові методи обробки та її зберігання, а також сучасні відкриті мережі відкрили безліч можливостей, як для бізнесу, так і для звичайних користувачів у повсякденному житті.

Після впровадження комп'ютерних мереж доступ до інформації став ще простішим, що в свою чергу робить легкість та швидкість такого доступу значно підвищує загрозу несанкціонованого використання інформації, тому питання надійного захисту авторських прав, прав інтелектуальної власності або конфіденційних даних є надзвичайно актуальними. Величезний обсяг інформації та різноманітних послуг надається через мережу Інтернет, без необхідності безпосередньої зустрічі з людиною, що їх замовляє. Наявність процедур автентифікації та ідентифікації користувачів для обмеження несанкціонованого доступу до баз даних та її об'єктів (апаратні, програмні та інформаційні ресурси) є умовою будь–якої захищеної системи, оскільки всі системи захисту інформації розраховані на роботу з пойменованими суб'єктами і об'єктами інформаційних систем. Спільний алгоритм роботи таких систем полягає в тому, щоб отримати від

суб’єкта (користувача) інформацію, що ідентифікує його особу, підтвердити її відповідність та надати (або не надати) цьому користувачеві можливість роботи з системою.

Мета захисту інформації від несанкціонованого доступу так чи інакше вирішувались на протязі всієї історії людства. Розвиток обчислювальної техніки, нові методи обчислення і зберігання інформації, а також сучасні відкриті мережі відкрили безліч можливостей, як для бізнесу, так і для звичайних користувачів у повсякденному житті.

1 ОГЛЯД МЕТОДІВ ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЇ

1.1 Парольна ідентифікація

Способом визначення особистості користувача стана не так давно парольна ідентифікація. Так як вона сама проста в реалізації та використанні. Парольна ідентифікація. Людина будь якої системи отримає набір особистих реквізитів (але використовується пари логін-пароль). У разі входу користувача до системи вона обов’язково повинна використовувати свою інформацію. А так як вона унікальна то відповідно цього система дозволяє ідентифікувати користувача.

Основною метою парольної ідентифікації, яка була зазначена вище – це дуже легка реалізація та легке застсування. Також, використання парольної ідентифікації не потребує зовнішних затрат: цей процес використовується в усіх програмних продуктах, що на даний час є у продажу. Виходячи з наведеного вище, система захисту інформації є простою та доступною для використання.

Дані перелічемо недоліків, які також присутні для цієї системи. Але їх дуже багато. І самий головний з них це – дуже велика залежність надійності ідентифікації і від самого користувача, а також, від застосованих ним паролів. Цей недолік пов’язаний з тим, що більшість користувачів застосовують прості та ненадійні ключові слова, які легко підбирати. Це пов’язано з тим, що люди використовують дуже короткі паролі, що легко підібрати. Із-за цього спеціалісти з області інформаційної безпеки радять застосовувати паролі, які мають велику кількість символів, до яких входять хаотично словосполучення цифр, букв та різноманітних символів. Але користувачі не бажають запам’ятовувати паролі, які починають записувати до нотатника, або розташовують у доступних місцях. Все це є має великий удар по інформаційній безпеці.

1.2 Апаратна ідентифікація

Принцип ідентифікації ґрунтується на визначенні особи користувача за допомогою об’єкта-ключа, який використовується виключно користувачем. Звичайно, мова йде не прозвичайні ключі, з якими знайомий широкий загал, а про спеціальні електронні ключі. Наразі найбільш поширеними є два типи пристроїв.

На першій картці зібрані всі види карток. Існує дуже багато різних типів, кожен з яких працює за своїм принципом. Наприклад, безконтактні картки (проксіміті-картками) дуже прості у використанні і можуть ідентифікувати користувачів як в комп’ютерних системах, так і в системах контролю доступу до будівель. Смарт-картки вважаються найбільш надійними і схожі на банківські картки, які знайомі багатьом людям. Крім того, існують дешевші, але менш захищені від несанкціонованого доступу картки, такі як магнітні картки та картки зі штрих-кодом.

До інших типів ключів, які можна застосовувати для ідентифікації обладнання, є так звані токени. Вони мають власну захищену пам’ять і під’єднуються безпосередньо до порту комп'ютера(USB,LAN).

Основною перевагою використання апаратної ідентифікації є її висока надійність. Дійсно, токени можуть зберігати ключі в пам'яті, які неможуть бути викрадені хакерами. Крім того, в токенах реалізовані різні механізми безпеки. Крім того, завдяки вбудованому мікропроцесору, електронні ключі можуть не тільки брати участь у процесі ідентифікації користувача, але й виконуватиінші корисні функції. У випадку з апаратною ідентифікацією чи не найсерйознішою небезпекою є можливість викрадення зловмисником токенів у зареєстрованих користувачів. Однак цю проблему можна легко вирішити, використовуючи багатофакторну ідентифікацію (що таке багатофакторна ідентифікація, розглянемо нижче).

Далі обговоримо недоліки апаратної ідентифікації. Один з них – це можливість викрадення електронного ключа, як ми вже згадували. Другий недолік – ціна. Загалом, вартість електронних ключів та програмного забезпечення, яке з ними працює, останнім часом значно знизилася. Тим неменш, експлуатація системи

ідентифікації власності вимагає певних інвестицій. Одже кожному зареєстрованому користувачеві (або принаймні привілейованим користувачам, таким як адміністратори, керівники компаній тощо) має бути наданий персональний токен. Крім того, деякі типи ключів можуть з часом зношуватися або втрачатися. Це означає, що ідентифікація власності вимагає певних операційних затрат.

1.3 Ідентифікація за біометричними ознаками

Ідентифікація – це процес розпізнавання людини за якимось признаком. Біометрична ідентифікація відрізняється тим, що використовуються унікальні властивості людини. Зазвичай процес біометричної ідентифікації проходить одночасно з біометричною автентифікацією. Тому розглядати процес біометричної ідентифікації пропонується разом з процесом автентифікації.

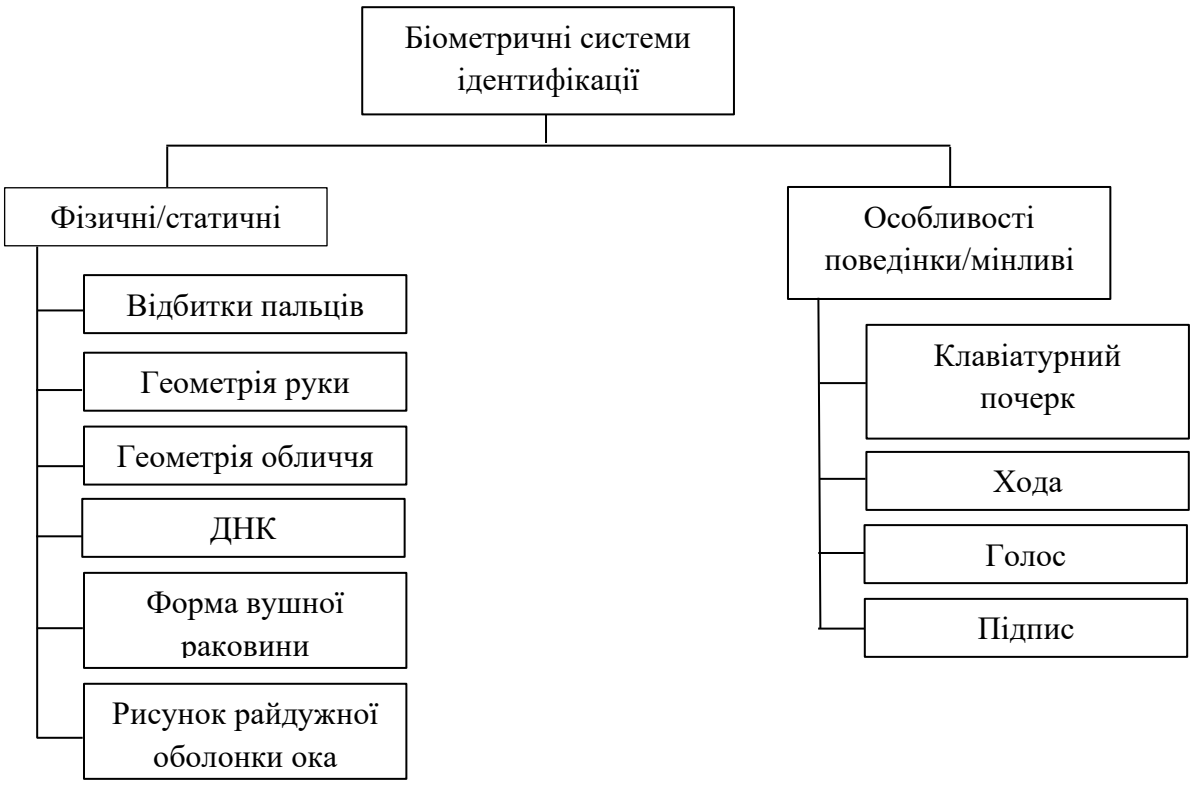


Рисунок 1.1 – Біометрична система ідентифікації

В даному разі основним параметром розпізнавання та підтвердження справжності користувача буде відбуватися на підставі фактору властивості. Біометричні властивості людини можна поділити на два підкласи, а саме: статичні характеристики користувача та динамічні характеристики. Статичні характеристики відрізняються тим, що вони не змінюються впродовж визначеного терміну. Динамічні характеристики інакше називаються мінливими тому, що можуть змінюватися на протязі часу.

2 МЕТОДИ АВТЕНТИФІКАЦІЇ

З розвиненням інформаційних технологій майже у всіх сферах життя людини, виникає проблема із захистом інформаційних систем. Технічний прогрес в інформаційних технологіях стрімко розвивається, тому і зловмисники, які хочуть заволодіти інформацією, постійно удосконалюють свої знання та вигадують нові способи заволодіння даними.

Під час обробки інформації з обмеженим доступом повинен забезпечуватися її захист від несанкціонованого перегляду, змін, видалення, копіювання, поширення. У разі, коли йдеться про таємну інформацію, то вона має передаватися захищеними каналами зв'язку або здійснюватися за допомогою технічного чи криптографічного захисту інформації.

Криптографічні методи захисту інформації характеризуються тим, що в залежності від призначення, для виконання завдання відбувається перетворення інформації на підставі ключової інформації.

До завдань криптографічного захисту інформації входить забезпечення:

– конфіденційності, тобто захисту від витоку інформації (вирішується шифруванням);

– доступності, тобто інформація повинна бути доступна тільки тому користувачеві, для якого вона призначена (вирішується шифруванням);

– цілісності, тобто інформація повинна бути захищена від несанкціонованої модифікації (вирішується електронним цифровим підписом);

– автентифікації, тобто підтвердженням справжності (вирішується електронним цифровим підписом і сертифікатом);

– незаперечності, тобто неможливості відмовитися від вчиненої дії (вирішується електронним цифровим підписом і сертифікатом).

Криптографічний захист інформації реалізується за допомогою програмних, програмно-апаратних та апаратних засобів шляхом перетворення даних з використанням ключової інформації з метою зашифрування та розшифрування

повідомлення, перевірки авторства, справжності користувача, цілісності та доступності інформації.

Існують різні алгоритми криптографічного перетворення інформації. Криптографічні алгоритми можна поділити на 2 класи: симетричні та асиметричні. Алгоритми, які об’єднують обидва класи називаються гібридними.

Симетричні алгоритми характеризуються тим, що шифрування та розшифровування відбувається за допомогою одного спільного секретного ключа шифрування.

Асиметричні алгоритми характеризуються тим, що вони крім секретного ключа мають відкритий (публічний ключ). Тому ці системи називають двоключовими чи системами з відкритим ключем. Несиметричні алгоритми також можуть використовуватися для процесу шифрування, проте лише невеликих повідомлень (через те, що вони дуже повільно працюють).

Частіше асиметричні системи використовуються для автентифікації документів та розподілу ключів.

Наявність процедур ідентифікації та автентифікації користувачів є обов’язковою умовою будь-якої захищеної системи, оскільки всі механізми захисту інформації розраховані на роботу з пойменованими суб'єктами і об'єктами інформаційних систем.

Для правильного тлумачення, необхідно розрізняти такі основні поняття, як ідентифікація, автентифікація та авторизація.

2.1 Метод простої автентифікації

Системи захисту інформації призначені для забезпечення конфіденційності та цілісності електронної інформації, а також для забезпечення суворої автентифікації учасників електронної системи, учасників інформаційної роботи та фахівців організації, які беруть участь у створенні та обробці електронних документів. Дляз абезпечення суворої автентифікації організації використовується система ідентифікації користувачів, яка є основою системи розподілу ключової

інформації. Автентифікація – це процедура перевірки автентичності суб’єкта, який входить у систему та надає свій ідентифікатор.

Автентифікація багатофакторна – автентифікація, яка виконується із використанням механізмів захисту, які бувають двох або більше типів.

Фактор автентифікації – певний вид інформації, що надається користувачем системі при його автентифікації. Виділяють три фактори автентифікації, що використовуються в різних комбінаціях: на основі знання чого–небудь, володіння чимось, на основі біометричних характеристик.

У таблиці 2.1 показано класифікацію факторів автентифікації з прикладами.

Таблиця 2.1 – Класифікація факторів автентифікації.

Фактор автентифікації					
Знання	Володіння	Властивості			
		Біометричні		За дією	За місцем
		Статичні	Динамічні		
PIN	Ключ	Відбиток пальця, губ	Голос	Жест	Розташування
Кодова фраза	USB- токен	Сітківка, райдужна оболонка ока	Динаміка підпису	Підпис	Позиція на поточний час
Пароль	Смартфон	Геометрія обличчя, долоні	Клавіатурний почерк	Електронний підпис	
	Картка	ДНК	Рух губ		
		Форма черепа, вуха	Хода		
		Зображення вен	Почерк		

Для підвищення точності системи автентифікації зазвичай використовують багатофакторну автентифікацію. Наприклад, для перевірки справжності користувача система може запросити введення паролю та якийсь біометричний параметр людини. При цьому, для підвищення точності біометричної системи враховується значення коефіцієнту помилкового збігу (ймовірність того, що системою невірно відбудеться порівняння вхідного зразка з еталоном, який є у базі даних) та коефіцієнту помилкової розбіжності (ймовірність того, що системою помилково не буде розпізнаний справжній вхідний зразок користувача). Ці коефіцієнти ще можна знайти в літературі під назвою помилка I типу та помилка II типу відповідно, та відображають спроможність системи обмежувати вхід

авторизованим користувачам. Системи з низькою пороговою величиною коефіцієнту помилкового збігу більш захищені, проте системи з низьким порогом коефіцієнту помилкової розбіжності є більш зручними у використанні. Тому при налаштуванні системи автентифікації, необхідно знайти компроміс між безпекою та простотою використання.

Можна проаналізувати методи автентифікації, що найчастіше застосовуються користувачами за такими критеріями, як: зручність, безпека, вартість, актуальність чи можливість використання в наявній інфраструктурі. У таблиці 2.2 показано частоту використання методів автентифікації за певними критеріями.

Таблиця 2.2 – Частота використання методів автентифікації у системах захисту.

Критерії Захисту	Методи автентифікації							
	PIN	Пароль	Картка	Відбиток пальця	Підпис	Сітківка ока	ДНК	ЕП
Безпека	**	**	**	**	**	***	***	***
Зручність	***	***	***	***	**	**	*	**
Актуальність	***	***	***	**	**	**	*	**
Вартість	***	***	***	**	**	**	*	*

* – мало; ** – часто; *** – дуже часто

В процесі пересилання даних для проведення процесу автентифікації, ці дані необхідно шифрувати. Це є необхідною умовою роботи системи для того, щоби зловмисник не зміг скористатися перехопленим повідомленням.

Просту автентифікацію поділяють на два види:

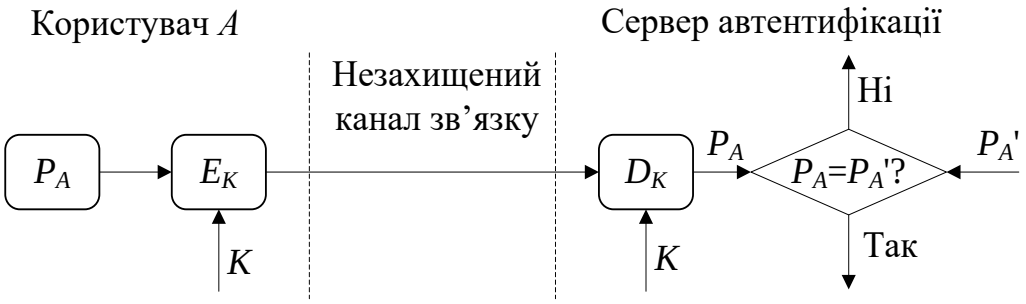
– з використанням паролів;

– з застосуванням односторонньої функції.

На Рис. 2.1 показано схему простої автентифікації користувача, де видно, що перед пересиланням пароля P_A, що надав користувач, відбувається його шифрування секретним ключем K. На приймальній стороні цей пароль

відновлюється шляхом розшифровуванням секретним ключем та порівнюється з еталоном паролю, що зберігається в базі даних системи.

Найпростіший метод автентифікації з використанням пароля заснований на порівнянні наданого користувачем пароля P_A з вихідним значенням P_A', що зберігається на сервері автентифікації. Оскільки пароль повинен зберігатися в таємниці, він повинен шифруватися перед пересиланням по незахищеному каналу. Якщо в результаті порівняння значення P_A і P_A' є однакові, то пароль P_A вважається справжнім, а користувач – законним.



P_A – пароль D – розшифрування

E – зашифровування K – ключ

Рисунок 2.1 – Схема простої автентифікації з використанням пароля

Кращим по безпеці є вид простої автентифікації з застосуванням односторонніх функцій. При перевірці введеного користувачем пароля система обчислює одностороннюю функцію і порівнює результат зі значенням у таблиці паролів для даного користувача. У подібному випадку файл, в якому зберігається таблиця, повинен бути захищений від запису. Застосування односторонніх функцій дозволяє також захищати паролі у разі передачі їх по загальнодоступних каналах.

Схема простої автентифікації з застосуванням односторонньої функції для перевірки пароля показана на Рис. 2.2

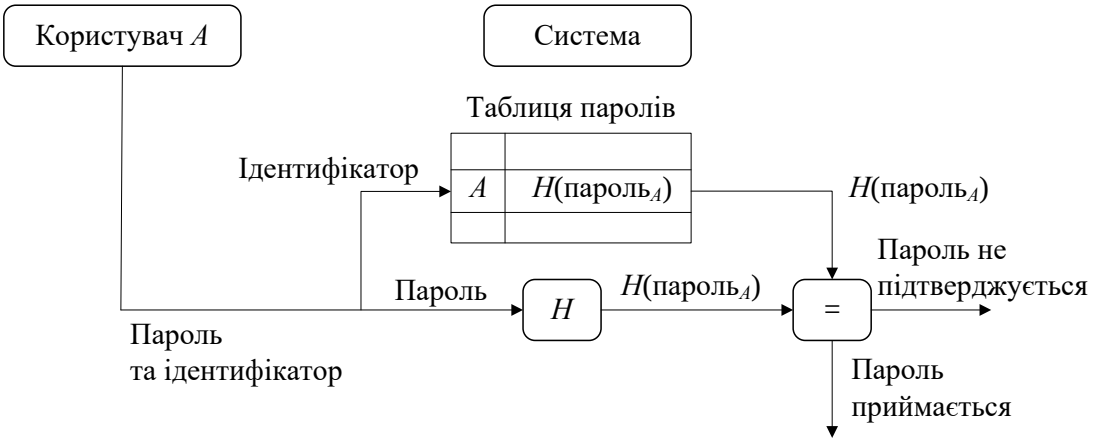


Рисунок 2.2 – Схема простої автентифікації з використанням односторонньої функції для перевірки пароля

У схемі простої автентифікації передача пароля й ідентифікатора користувача може здійснюватися наступними методами:

– в незашифрованому вигляді; це може бути, як з протоколом парольної автентифікації PAP (Password Authentication Protocol) паролі, які передаються по лінії зв’язку у відкритій незахищеній формі;

– в захищеному вигляді; всі передані дані (ім’я та пароль користувача, випадкове число і позначки часу) будуть захищені за допомогою шифрування наприклад, протокол S\Key або однонаправленої функції.

2.2 Автентифікація за допомогою одноразових паролів

Одноразові паролі (One–Time Passwords – OTP) – це динамічна інформація, що генерується пристроєм автентифікації (програмних або апаратних), для генерації одноразових паролів з метою автентифікації клієнтів під час входу в систему, а також для підтвердження платіжних доручень.

OTP-токенгенеруєодноразовіпаролізадопомогоюхеш-функційабокриптографічнихалгоритмів:

– Симетрична криптографія – в цьому випадку користувач і сервера утентифікації використовують один і тойжесекретний ключ;

– Асиметрична криптографія – в цьому випадку закритий ключ зберігається напристрої, а сервер автентифікації використовує відповідний відкритий ключ.

Існують різні комбінації використання даних криптографічних алгоритмів у реалізаціях OTP–токенів. Зазвичай в OTP–токенах застосовується симетрична криптографія. Пристрій кожного користувача містить унікальний персональний особистий ключ, який використовується для зашифровування деяких даних (в залежності від реалізації методу) для генерації OTP. Цей самий ключ зберігається на сервері автентифікації, який виконує автентифікацію даного користувача. Сервер зашифровує ті самі дані і порівнює два результати шифрування: отриманий ним і присланий від клієнта. Якщо результати збігаються, то користувач успішно проходить автентифікацію. OTP–токени, що використовують симетричну криптографію, можуть працювати в асинхронному або синхронному режимі. Відповідно методи, використовувані OTP–токенами, можна поділити на дві групи, що працюють:

В асинхронному режимі;

– метод «запит–відповідь» (challenge–response).

В синхронному режимі;

– метод «тільки відповідь» (response only);

– метод «синхронізація за часом» (time synchronous);

– метод «синхронізація за подією» (event synchronous).

2.3 Біометрична автентифікація

Біометрична автентифікація – методи автентифікації, які засновані на використанні унікальних біологічних характеристик об’єкта. В якості таких характеристик можуть бути використані: відбиток пальця, геометрія обличчя, геометрія руки, сітчатка ока і т.ін.

Біометрія це совокупність автоматизованих методів ідентифікації та/або автентифікації людей на основі їх поведінкових та й фізіологічних характеристик. До їх числа відносяться структура відбитку пальців, сітківка та роговиця очей,

параметри кінцівок та таке інше. До характеристик, що відображають манеру поведінки відносять динаміка ручного підпису, ритм роботи серця, стиль роботи із клавіатурою. Також до них можна віднести аналіз особливостей голосу та розпізнавання мови.

У совокупності робота з біометричними даними побудована з таких етапів. Створюється організація система (банк даних) потенційних користувачів. Це організується на сам перед збором біометричних характеристик користувача. До характеристик відносяться такі вихідні дані, такі як відбиток пальця, роговиці.

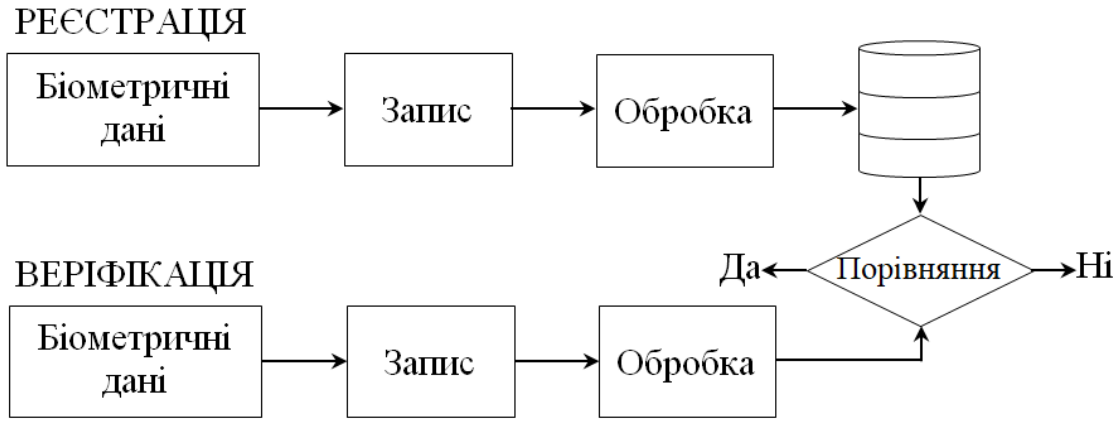


Рисунок 2.3 – Структура роботи біометричної автентифікації

Для ідентифікації та й насамперед автентифікації користувача продовжується обробка, після чото повторюється пошук даних у створеній базі. У разі успішного пошуку даних у базі користувач автентифікується.

Точність біометричної системи вимірюється двома параметрами:

– коефіцієнт помилкового збігу (False Match Rate – FMR), також відомим під назвою помилка типу I або коефіцієнт помилкового прийому (False Accept Rate – FAR). FMR – імовірність, що система невірно порівнює вхідний зразок з невідповідним шаблоном у базі даних;

– коефіцієнт помилкової розбіжності (False Non–Match Rate – FNMR), також відомим під назвою помилка типу II або коефіцієнт помилкового відхилення (False Reject Rate – FRR). FRR – імовірність того, що система не визнає справжність відбитка пальця зареєстрованого в ній користувача.

Обидва коефіцієнти відображають здатність системи надавати обмежений вхід авторизованим користувачам. Системи з низьким значенням FMR більш захищені, а системи з низьким значенням FNMR більш прості у використанні. У загальному випадку для даних систем при завданні порогової величини діє правило: чим нижче FMR, тим вище FNMR. Таким чином, часто безпека і простота використання конкурують між собою.

2.4 Багатофакторна автентифікації

У багатофакторної автентифікації важливо те, що одним з факторів є пароль, який користувач знає і який дозволяє діяти на основі його волі з виключенням примусу третіх осіб. Цей фактор для зручності зазвичай передається по основному каналу, по якому відбувається комунікація. Другим фактором може бути щось, що належить користувачеві, або біометрична характеристика, така як код, отриманий за допомогою маркера безпеки, або відбиток пальця, знятий через смартфон. Другий фактор завжди має транслюватися по альтернативному каналу, щоб уникнути його захоплення і використання разом з першим фактором. Часто другий фактор надходить по альтернативному каналу (наприклад, код, що відправляється по SMS), але потім повертається назад на основний канал з усіма описаними вище ризиками крадіжки. Наприклад, при автентифікації за технологією ідентифікації відбитків пальців, ім’я користувача записується для реєстрації, а відсканований відбиток заміняє пароль. На сам перед ім’я користувача у цьому випадку буде показником для отримання його облікового запису та здійснення порівняння між шаблоном зчитаного під час реєстрації відбитка і раніше збереженим шаблоном в базі даних для даного імені користувача.

3 ПРОТОКОЛИ АВТЕНТИФІКАЦІЇ

3.1 Електронний цифровий підпис

Електронний цифровий підпис (ЕЦП) або електронний підпис (ЕП), використовується для автентифікації текстів, переданих телекомунікаційними каналами.

Функційно він є аналогом звичайного рукописного підпису й має основні його переваги:

– засвідчує, що підписаний текст виходить від імені користувача, котрий поставив підпис;

– не надає саме цьому користувачеві можливості відмовитися від зобов'язань, пов'язаних з підписаним текстом;

– гарантує цілісність підписаного тексту.

Цифровий підпис являє собою відносно невелику кількість додаткової цифрової інформації, переданої разом з підписуваним текстом.

Система ЕЦП включає дві процедури:

– процедуру формування підпису;

– процедуру перевірки підпису.

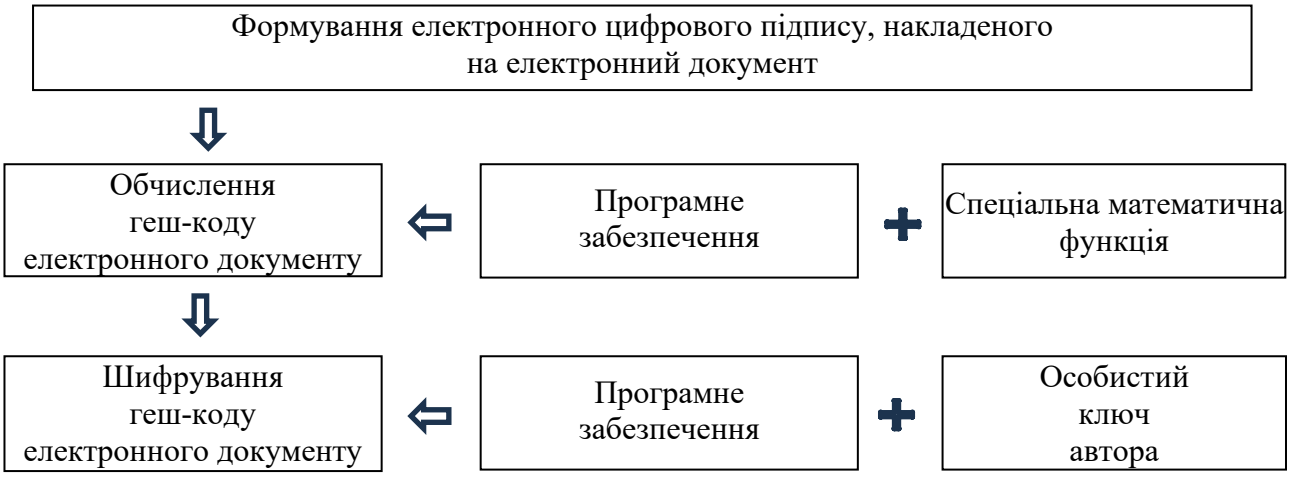


Рисунок 3.1 – Структурна схема побудови ЕП

У процедурі постановки підпису використовується секретний ключ відправляча повідомлення, у процедурі перевірки підпису – відкритий ключ відправляча. При формуванні ЕП відправляч найперш обчислює геш-функцію *h(M)* тексту *M*, який він підписує. Обчислене значення геш-функції *h(M)* являє собою один короткий блок інформації *m*, котра схарактеризовує весь текст *M* у цілому. Потім число *m* зашифровується секретним ключем відправляча. Здобувана при цьому пара чисел являє собою ЕЦП для тексту *M*.

При перевірці ЕП одержувач повідомлення знову обчислює геш-функцію *m = h(M)* прийнятого каналом тексту *M*, після чого за допомогою відкритого ключа відправляча перевіряє, чи відповідає здобутий підпис обчисленому значенню *m* геш-функції.

Засадничим моментом у системі ЕЦП є неможливість підробки ЕП користувача без знання його секретного ключа для підписування. В якості підписуваного документа може бути використано будь-який файл. Підписаний файл утворюється з непідписаного файлу, до якого додається електронний підпис.

Кожний підпис містить таку інформацію:

– дата підпису;

– термін завершення дії ключа даного підпису;

– інформація про особу, котра підписала файл (П.І.Б., посада, коротке найменування фірми);

– ідентифікатор особи, котра поставила підпис;

– власне цифровий підпис.

Процес використання системи ЕП припускає наявність мережі абонентів, які надсилають один одному підписані електронні документи. Для того щоб підписати документ та бути впевненим, що він надійшов до одержувача у незмінному вигляді обирається пара ключів. При цьому в цієї парі один ключ буде відкритий (публічний), а інший – секретний (приватний). При створенні підпису відправник користується секретним ключем, а одержувач перевіряє підпис відкритим ключем.

Відкритий ключ є необхідним інструментом, який дозволяє перевірити чинність електронного документа та автора підпису. Відкритий ключ не дозволяє обчислити

секретного ключа.

Для генерування пари ключів (секретного й відкритого) в алгоритмах ЕП, як і в асиметричних системах шифрування, використовуються різні математичні схеми, ґрунтовані на застосовуванні однонапрямлених функцій. Ці схеми поділяються на дві групи. В підґрунті такого поділу лежать відомі складні обчислювальні завдання:

– факторизація (розкладання на множники) великих цілих чисел;

– дискретне логарифмування.

На сьогоднішній день розвиток інформаційних технологій привів до появи електронного документообігу. Проте використання електронного документообігу, пов’язане зі збереженням документів від несанкціонованого копіювання, модифікації і підробки. Для вирішення проблеми захисту інформації від НСД необхідне використання сучасних засобів і методів захисту.

Особливо актуальними ці проблеми стали з прийняттям у державах на міжнародному рівні, у тому числі в Україні, основоположних законів «Про електронні документи та електронний документообіг» [4], «Про захист інформації в інформаційно-телекомунікаційних системах» [5], «Про електронні довірчі послуги» [6]. На виконання цих законів в Україні створюється інфраструктура відкритих ключів, перш за все для підтримки системи електронного цифрового підпису. При цьому першочерговим завданням в Україні, що вимагає свого вирішення, є надання органам державної влади, місцевого самоврядування, юридичним та фізичним особам послуг із забезпечення цілісності, справжності, неспростовності, а в більшості випадків і конфіденційності інформації та різноманітних даних, що надані в електронному вигляді, електронних документів і повідомлень, програмного забезпечення, що ними використовуються. Крім того, у зв’язку з інтеграцією України у світовий інформаційний простір, орієнтацією на вступ України до Європейського співтовариства, важливим є завдання забезпечення взаємодії органів державної влади, місцевого самоврядування, юридичних і фізичних осіб на світовому рівні, з використанням іноземних і міжнародних інформаційних та інформаційно-комунікаційних систем, різноманітних інформаційних технологій, відкритих систем Інтернету.

Вимоги до системи електронного підпису

У сучасних автоматизованих системах керування, комп'ютерних системах мереж, різних інформаційних і телекомунікаційних системах, інформаційно-телекомунікаційних системах, а також системах електронного документообігу висуваються високі вимоги до забезпечення цілісності, автентичності (справжності), неспростовності та доступності інформації (електронних документів) на всіх етапах їх життєвого циклу. При цьому під інформацією будемо розуміти сукупність усіх даних і програм, що використовуються у системі чи технології, незалежно від їхнього логічного чи фізичного подання. Під інформацією розумітимемо також і повідомлення й електронні документи, що циркулюють у відповідних системах чи технологіях. Електронний підпис, по суті, являє собою додані до інформації дані, обчислені за допомогою криптографічного перетворення інформації, що захищається, і параметри, наявність яких дозволяє упевнитися в цілісності й справжності інформації та її джерела, а також забезпечити захист від підробки з боку отримувача.

На цей час розроблені й застосовуються низка алгоритмів ЕП, що використовують симетричні або асиметричні методи, різний математичний апарат і дозволяють виробляти та перевіряти підписи одним чи багатьма суб'єктами в автономному чи інтерактивному режимах. Надана нижче класифікація дозволяє визначити властивості будь–якого відомого алгоритму цифрового підпису та зробити порівняння його з іншими алгоритмами, а також визначити за низкою критеріїв кращого з них. Класифікація може бути здійснена за такими ознаками та критеріями.

За кількістю учасників:

– одиничний – коли в процесі вироблення ЕП достатньо одного учасника;

– груповий – коли в процесі вироблення ЕП повинно бути більше ніж один учасник.

При цьому груповий підпис може здійснюватися:

– із залученням для здійснення електронного підпису послуги третьої довірчої сторони;

– без залучення третьої довірчої сторони.

За терміном дії ключів:

– ЕП без терміну обмеження дії ключів;

– ЕП з терміном обмеження дії ключів.

За способом перевірки:

– інтерактивні – схеми ЕП, що потребують протокольної взаємодії учасників. При цьому інтерактивні ЕП можуть також бути незаперечними. Незаперечні ЕП – це підписи, що не дають можливості перевірки ЕП без дозволу суб'єкта (об'єкта), що підписує;

– неінтерактивні – схеми ЕП, що не потребують протокольної взаємодії учасників.

За способом вироблення підпису:

– ЕП з відновленням – частина або повне повідомлення може бути відновлене з ЕП;

– ЕП з додатком – ЕП приєднується до повідомлення і в такому вигляді надсилається адресату;

– сліпий ЕП – ЕП, що здійснюється без можливості перегляду змісту повідомлення;

– ЕП за дорученням – який здійснюється довірчим суб'єктом від імені суб'єкта, що довіряє, без надання довірчому суб'єкту таємних ключів суб'єкта, що довіряє;

– ЕП контракту – коли документ (контракт) підписується одночасно двома підписами (сторонами);

– колективний (множинний) підпис (aggregate signature) – дозволяє декільком користувачам підписувати єдиний документ;

– кільцевий підпис (ring signature) – один із механізмів реалізації ЕП, за якого відомо, що повідомлення підписав один із членів списку потенційних підписантів, але не розкриває, хто саме.

3.2 Алгоритм електронного підпису RSA

Технологія застосовування електронного підпису припускає наявність мережі абонентів, які надсилають один одному електронні документи. У цій ситуації для формування електронного підпису кожного абонента використовують окрему пару ключів – K_1 (іноді позначається літерою e) і K_2 (іноді позначається літерою d). Секретний ключ K_2 відомий лише користувачеві, а його ідентифікаційний номер ID і ключ K_1 розміщують у загальнодоступному каталозі для інших абонентів мережі. Це дозволяє будь–якому абонентові мережі перевіряти істинність цифрового підпису документів, одержуваних від її власника. Значення ідентифікаційного номера використовується в певних алгоритмах формування сигнатури.

Найбільш поширеною системою формування ЕП є система, в основі якої лежить алгоритм RSA. Узагальнену схему формування й перевірки електронного підпису RSA показано на Рис.3.2

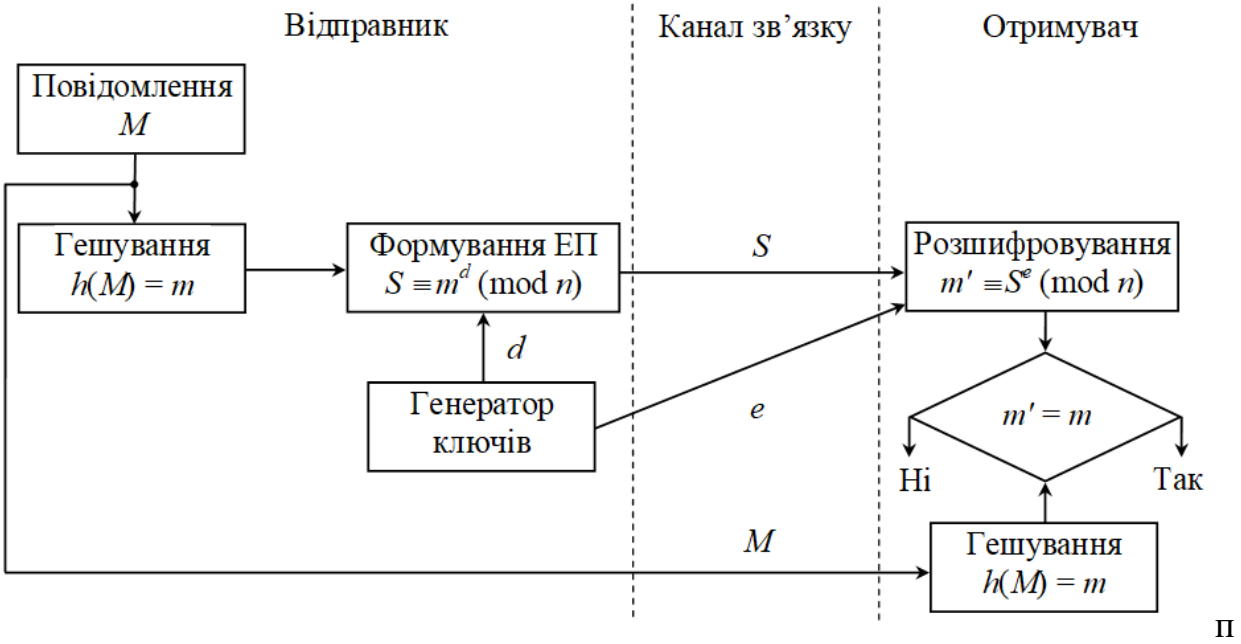


Рисунок 3.2 – Схема електронного підпису RSA

Обираються великі прості числа p і q, обчислюється $n = pq$, функція Ейлера $\varphi(n) = (p - 1)(q - 1)$ і вибирається відкритий ключ e ($e < \varphi(n)$, НОД $(e, \varphi(n)) = 1$).

Врешті, обчислюється секретний ключ d, взаємно обернене з e ($ed \equiv 1 \bmod \varphi(n)$). У відкритому каталозі розміщують значення (e, n), а секретний ключ d зберігається у автора документа.

Припустимо, що відправник хоче підписати повідомлення M перед його надсиланням. При цьому передбачається, що сам текст документа шифрувати не потрібно. Спочатку повідомлення M гешується за допомогою геш–функції h в ціле число m:

$$h(M) = m. \tag{3.1}$$

Потім відправник зашифровує m секретним ключем d:

$$S \equiv m^d \pmod{n}. \tag{3.2}$$

Пара чисел (M, S) передається адресатові як електронний документ M, підписаний електронним підписом S.

Адресат, отримавши підписаний документ (M, S), обчислює значення m за двома різними способами. По–перше, він відновлює геш–значення m', застосовуючи криптографічне перетворення підпису S з використанням відкритого ключа e:

$$m' \equiv S^e \pmod{n}. \tag{3.3}$$

По–друге, одержувач відшукує результат гешування одержаного повідомлення M за допомогою такої самої геш–функції h:

$$h(M) = m. \tag{3.4}$$

Якщо обидва значення збігаються $m' = m$, тобто дотримується рівність

$$S^e \pmod{n} = h(M), \tag{3.5}$$

то одержувач визнає пару (M, S) за справжнє значення документа.

Доказ коректності підпису RSA

$$\begin{aligned} S^e(\mathrm{mod}\ n) &\equiv m^{ed}\ (\mathrm{mod}\ n) \equiv \\ &\equiv (m^{k\,(p-1)(q-1)+1})\ \mathrm{mod}\ (pq) \equiv \\ &\equiv (mm^{k\,(p-1)(q-1)})\ \mathrm{mod}\ (pq) \equiv m = h(M). \end{aligned} \tag{3.6}$$

В якості геш–функції у схемі підпису RSA використовують функції сімейства MD.

3.3Стандарт цифрового підпису ДСТУ 4145–2002

ДСТУ 4145–2002 встановлює механізм створення цифрового підпису, який базується на властивостях груп точок еліптичних кривих над полями $GF(2^m)$. Загальні параметри підпису можуть бути ідентичними для довільної кількості користувачів цифрового підпису [7].

В ДСТУ 4145–2002 використовуються наступні перетворювання даних:

1) Перетворювання елемента основного поля на ціле число.

Установимо алгоритм перетворювання елемента основного поля $x \in GF(2^m)$ на ціле число a.

Вхідні дані алгоритму: елемент основного поля $x \in GF(2^m)$, $x = (x_{m-1}, ..., x_0)$, порядок базової точки еліптичної кривої n.

Результат виконання алгоритму – ціле число $a = (a_{L-1}, ..., a_0)$, яке задовольняє умові $L = L(a) < L(n)$.

Алгоритм перетворювання елемента основного поля на ціле число:

– якщо елемент x основного поля дорівнює 0, то $a \leftarrow 0$ $L = L(a) \leftarrow 1$, кінець алгоритму;

– обчислюємо ціле число $k = L(n) - 1$;

– приймаємо $a_i = x_i$ для $i = 0, ..., k - 1$ і знаходимо j, що дорівнює найбільшому індексові i, за якого $a_i = 1$. Якщо такого індексу немає, то приймаємо $a \leftarrow 0$ і

завершуємо виконування алгоритму;

– двійковий рядок (a_j, ..., a_0) довжини $L = L(a) = j + 1$ зображує ціле число a, яке є результатом виконання алгоритму.

2) Перетворювання геш–коду на елемент основного поля**.**

Установлюємо алгоритм перетворювання результату обчислення функції гешування (h_{L_H-1}, ..., h_0) на елемент основного поля $x \in GF(2^m)$,

$$x = (x_{m-1}, ..., x_0). \tag{3.7}$$

Вхідні дані алгоритму: геш–код (h_{L_H-1}, ..., h_0).

Результат виконання алгоритму – елемент основного поля $x \in GF(2^m)$, $x = (x_{m-1}, ..., x_0)$.

Алгоритм перетворювання результату обчислення функції гешування на елемент основного поля:

– обчислюємо ціле число $k = \min(m, L_H)$;

– приймаємо $x_i = h_i$ для $i = 0, ..., k - 1$;

– якщо $k < m$, то приймаємо $x_i = 0$ для $i = 0, ..., m - 1$;

– двійковий рядок (x_{m-1}, ..., x_0) зображує елемент x основного поля, який є результатом виконання алгоритму.

3) Перетворювання пари цілих чисел на цифровий підпис.

Установлюємо алгоритм перетворювання пари цілих чисел (r, s), які задовольняють умовам $0 < r < n$, $0 < s < n$, на цифровий підпис $D = (D_{L_D-1}, ..., D_0)$.

Вхідні дані алгоритму*:* пара цілих чисел (r, s) у двійковому зображенні:

$$r = (r_{L(r)-1}, ..., r_0); s = (s_{L(s)-1}, ..., s_0); 0 < r < n; 0 < s < n, \tag{3.8}$$

довжина цифрового підпису L_D: $L_D \geq 2L(n)$, L_D є кратне до 16.

Результат виконання алгоритму – цифровий підпис $D = (D_{L_D-1}, ..., D_0)$ довжини L_D.

Алгоритм перетворювання пари цілих чисел на цифровий підпис:

– приймаємо $l = L_D/2$;

– утворюємо двійковий рядок R за правилом:

– приймаємо $R_i = r_i$ для $i = 0, ..., L(r) – 1$,

– приймаємо $R_i = 0$ для $i = L(r), ..., l – 1$;

– утворюємо двійковий рядок S за правилом:

– приймаємо $S_i = s_i$ для $i = 0, ..., L(s) – 1$,

– приймаємо $S_i = 0$ для $i = L(s), ..., l – 1$;

– рядок D є конкатенація двох рядків $S \| R$;

– двійковий рядок $D = (D_{L_D-1}, ..., D_0)$ довжини L_D є результат виконання алгоритму.

4) Перетворювання двійкового рядка на пару цілих чисел.

Установлюємо алгоритм перетворювання двійкового рядка D парної довжини L_D на пару цілих чисел $r = (r_{L(r)-1}, ..., r_0)$; $s = (s_{L(s)-1}, ..., s_0)$.

Вхідні дані алгоритму: двійковий рядок $D = (D_{L_D-1}, ..., D_0)$ парної довжини L_D.

Результат виконання алгоритму – пара цілих чисел $r = (r_{L(r)-1}, ..., r_0)$ та $s = (s_{L(s)-1}, ..., s_0)$.

Алгоритм перетворювання двійкового рядка на пару цілих чисел:

крок 1, обчислюємо ціле число $l = L_D/2$;

крок 2, приймаємо $r_i = D_i$ для $i = 0, ..., l – 1$;

крок 3, визначаємо j як найбільше i, $i = 0, ..., l – 1$, для якого $r_i = 1$;

крок 4, якщо такого індексу немає, то $r \leftarrow 0$, $j = 0$ і переходимо до кроку 6 ;

крок 5, двійковий рядок $(r_{L(r)-1}, ..., r_0)$, $L(r) = j + 1$ зображує ціле число r;

крок 6, приймаємо $s_i = D_{i+l}$ для $i = 0, ..., l – 1$;

крок 7, визначаємо індекс j як найбільше i, $i = 0, ..., l – 1$, для якого $s_i = 1$;

крок 8, якщо такого індексу немає, то $s \leftarrow 0$, $j = 0$ і переходять до кроку 10;

крок 9, двійковий рядок $(s_{L(s)-1}, ..., s_0)$; $L(s) = j + 1$,зображує ціле число s;

крок 10, пара цілих чисел r та s є результатом виконання алгоритму.

Перевірення цифрового підпису. Перевіримо цифровий підпис, обчислений вище. При перевіренні цифрового підпису використовують ті самі загальні параметри: обчислений вище відкритий ключ та геш–функцію без додаткових вказівок ($iH = 1$, $L_H = 256$, iH не передається).

Якщо $r = \tilde{r}$, то підпис є справжній.

4 ЗАСТОСУВАННЯ МЕТОДІВ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА

Сучасні системи автентифікації базуються на процесі підтвердження особи користувача ідентифікатор/пароль. Автентифікація дає відповіді на питання: «хто є користувачем?» і «чи дійсно користувач є тим, ким він / вона собою являє?».

Рішенням для подолання проблеми не захищеності комп'ютерної системи є застосування багатофакторної автентифікації, коли системапросить користувача надати їй:

– що знає користувач: пароль, кодова фраза, PIN-код, дівоче прізвище матері;

– що належить користувачеві: USB-токен, телефон, смарт-карта, програмний токен, cookie-файл навігатора;

– що кваліфікує користувача: відбиток пальця, фрагмент ДНК, зразок голосу, геометрія руки;

– може зробити користувач: підпис (електронний цифровий підпис), жест;

– знаходиться користувач: поточне місце розташування / позиція, інформація на поточний час.

4.1 Види атак на засоби автентифікації

Стійкість схеми електронного підпису залежить від стійкості використовуваних криптоалгоритмів та геш-функцій і визначається стосовно пари загроза–атака.

На схеми електронного підпису впливіають дуже велика кількість атак:

– атака на основі відомого відкритого ключа (key-only attack) – найслабша з атак, практично завжди доступна для зловмисника;

– атака на основі відомих підписаних повідомлень (known-message attack) – у розпорядженні зловмисника є певне (поліноміальне від k) число пар (M, S), де M – певне повідомлення, а S – припустимий підпис для нього, при цьому зловмисник не може впливати на вибір M;

– проста атака з вибором підписаних повідомлень (generic chosen-message attack) – зловмисник має можливість обрати певну кількість підписаних повідомлень, при цьому відкритий ключ він отримує після такого вибору;

– спрямована атака з вибором повідомлень (directed chosen-message attack) – обираючи підписані повідомлення, зловмисник знає відкритий ключ;

– адаптивна атака з вибором повідомлень (adaptive chosen-message attack) – зловмисник знає відкритий ключ; вибір кожного наступного підписаного повідомлення він може робити на основі знання припустимого підпису попереднього обраного повідомлення.

Кожна атака спрямована на досягнення певної мети. Можна відокремити такі різновиди загроз для схем електронного підпису (у порядку зростання потужності):

– екзистенційна підробка (existential forgery) – створення зловмисником підпису для якого-небудь, можливо безглуздого, повідомлення m', яке відрізняється від перехопленого;

– селективна підробка (selective forgery) – створення підпису для обраного повідомлення;

– універсальна підробка (universal forgery) – знаходження ефективного алгоритму формування підпису, функціонально еквівалентного до S;

– повне розкриття (total break) – обчислення секретного ключа, можливо відмінного від k^{secret}, який відповідає відкритому ключу k^{public}, що надає можливість формувати підписи для будь-яких повідомлень.

Найбільш надійними є схеми, стійкі проти найслабкішої із загроз на базі найпотужнішої з атак, тобто проти екзистенційної підробки на базі атаки з вибором підписаних повідомлень. Справедливе є твердження: схеми електронного підпису, стійкі проти екзистенційної підробки на базі атаки з вибором підписаних повідомлень, існують тоді й тільки тоді, коли існують односторонні функції.

4.2 Рекомендації щодо підвищення кіберзахисту підприємства

Для забезпечення основних властивостей інформації, яка має певну цінність

і є важливою для її власника, існує багато правових документів. Використовувалося досить дороге технічне обладнання, запроваджувались суворо регламентовані організаційні заходи, але все це не давало повної гарантії очікуваних результатів. Для цього існує багато причин, які можна розділити на три групи:

– ігнорування системного підходу до методів захисту інформації;

– відсутність механізмів повного та достовірного підтвердження якості захисту інформації;

– недоліки регулювання безпеки інформаційного простору;

– відсутня система управління та управління інформаційною безпекою.

Під поняттям інформаційної безпеки ми будемо розуміти стан захисту життєво важливих інтересів людей, суспільства і країни, що дозволяє запобігти шкоди через:

– неповноту, несвоєчасність та недостовірність використаної інформації;

– вплив негативної інформації;

– негативні наслідки використання інформаційних технологій;

– несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації.

Для вирішення проблеми інформаційної безпеки необхідно уточнити та сформулювати цілі та завдання інформаційної безпеки.

Чітко розуміти той факт, що чим конкретніша мета, чим краще набір обмежень і якість ресурсів, тим більше шансів на досягнення бажаного результату. Якщо мета захисту інформації носить простий характер, її реалізація цілком можлива і не потребує використання значних ресурсів. Проте, чим вищі вимоги до системи захисту інформації, тим складніше і складніше буде реалізувати завдання.

При цьому кожен окремий елемент відносно невеликий за вагою, але створює більш надійну і міцну систему в комплексі. В такій системі необхідно підкреслити не властивості кожного окремого елемента, а їх взаємодію. Саме з цієї причини система набуває специфічних властивостей, яких немає у цих елементів.

Для створення надійної системи захисту інформації в сучасних інформаційно–комунікаційних системах і мережах насамперед необхідно

визначити деякі можливі загрози інформаційним ресурсам.

Тільки комплексний підхід до інформаційної безпеки може бути успішним. Для захисту інтересів суб'єктів інформації в сучасній ІСУ необхідно поєднувати заходи на таких рівнях:

– законодавчого (нормативно–правовий);

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

– процедурного (заходи безпеки, орієнтовані на людей).

4.3 Побудова системи автентифікації користувача в телекомунікаціях

При розробці систем та автентифікації перспективним є створення єдиної (інтегрованої) системи (ЄСІА), яка, наприклад, забезпечить користувачам безпечний доступ до загальнодоступних інформаційних ресурсів. Основною функцією системи має бути:

– реєстрація комунікаційно-інформаційних порталів - систем, осіб, організацій, установ;

– перевірка ідентичності особи при реєстрації;

– ідентифікація та автентифікація користувачів у національному веб-додатку ІКС;

– актуальна підтримка даних користувачів, організацій, установ.

Забезпечує безпечний та контрольований доступ до даних користувача за запитом ІКС. Перспективна архітектура ЄСІА на рис.4.1.

У системі ЄСІА додатковими послугами може бути використання персональних даних користувача для перевірки, перевірки сертифікатів електронного підпису та надсилання повідомлень. Наступні користувачі братимуть участь у ЄСІА:

– особи з рахунками в індивідуальному реєстрі ЄСІА;

– індивідуальний підприємець (фізична особа);

– юридичні особи (фізичні особи, пов'язані з обліковими записами юридичних осіб

ЄСІА);

– посадові особи місцевих та національних адміністрацій, підприємств, організацій, установ.

Усі учасники мають можливість виконати одноразову автентифікацію. Після завершення процесу автентифікації в системі ЄСІА користувачі можуть входити в кілька систем, програм, порталів протягом одного сеансу без необхідності повторно вводити логіни та паролі.

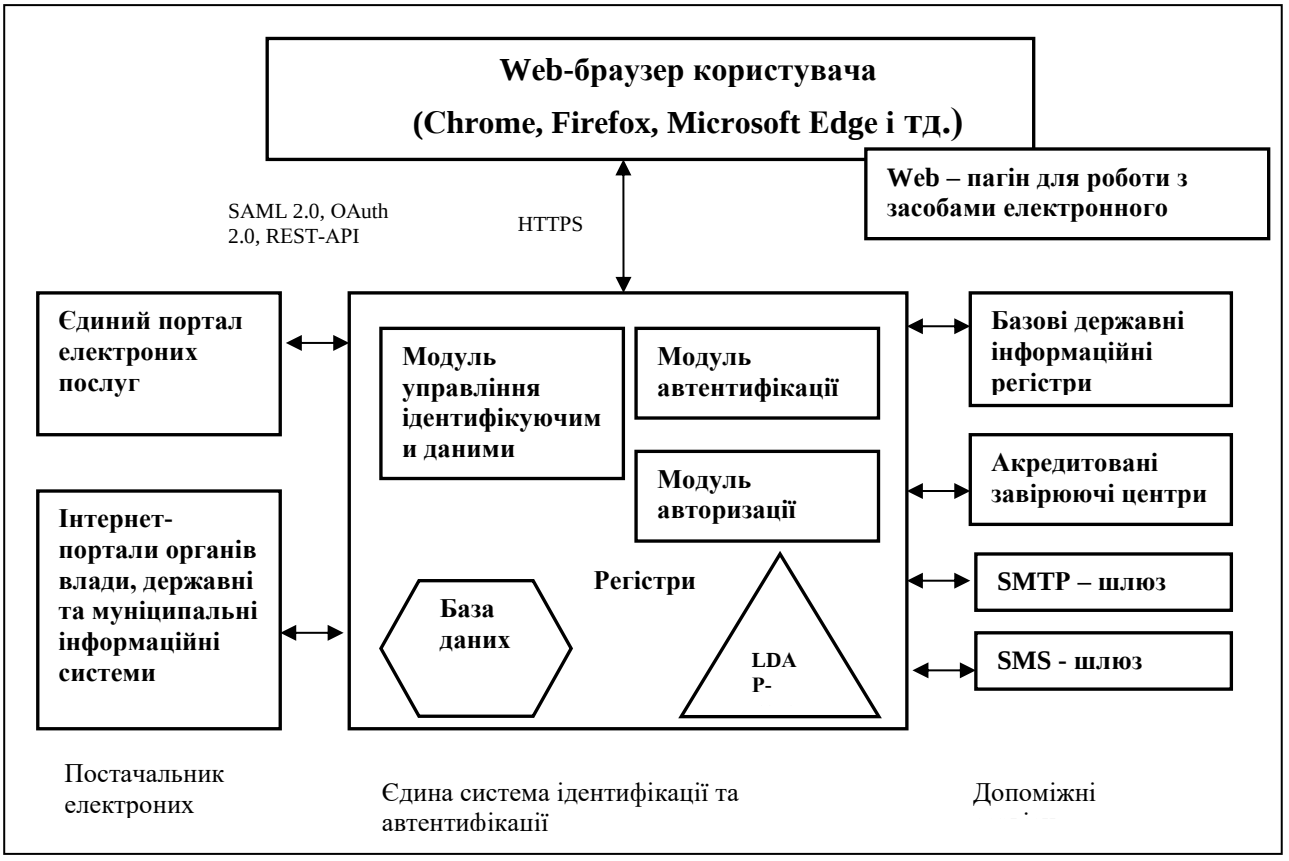


Рисунок 4.1 – Архітектура перспективної ЄСІА

Для забезпечення функціонування в системі ЄСІА необхідно запровадити два механізми, а саме:

– механізм на основі стандарту SAML версії 2.0 Рис.4.2;

– протокол встановлює взаємодію таких сторін:

– власники ресурсів - ядра, які можуть надавати доступ до захищених ресурсів (наприклад, окремі особи, заявники);

– клієнтські системи - програми, що запитують доступ до захищених ресурсів від імені їх власників;

–сервер авторизації — служба, яка генерує маркери ідентифікації для

клієнтських систем, автентифікацію для отримання дозволу від власників ресурсів і маркери доступу для надання доступу до даних;

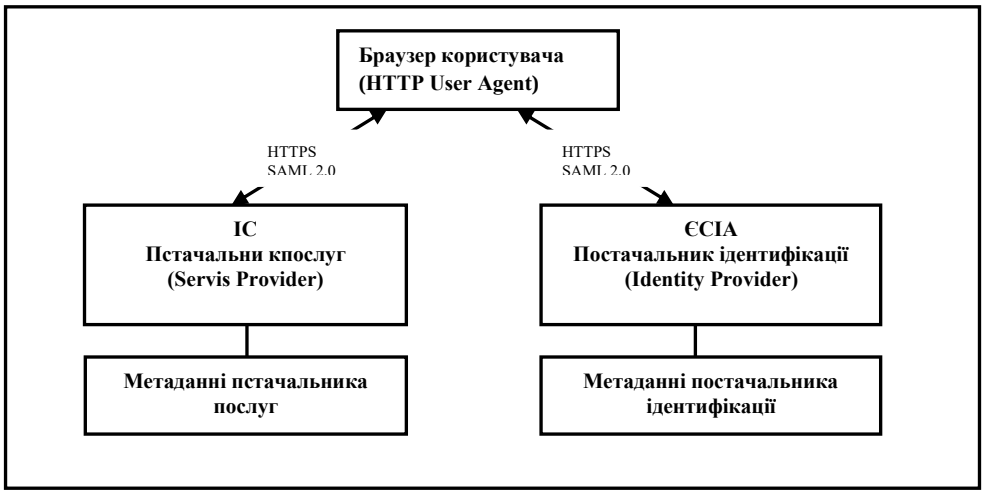


Рисунок 4.2 – Схема взаємодії між ІКС та системою ЄСІА з стандартом SAML V2.0

–сервер ресурсів – служба, яка надає доступ до ресурсів, захищених шляхом перевірки маркерів ідентифікації, автентифікації та маркерів доступу, таких як облікові дані користувача.

Механізм на основі моделі OpenID Connect 1.0 Рис.4.3.

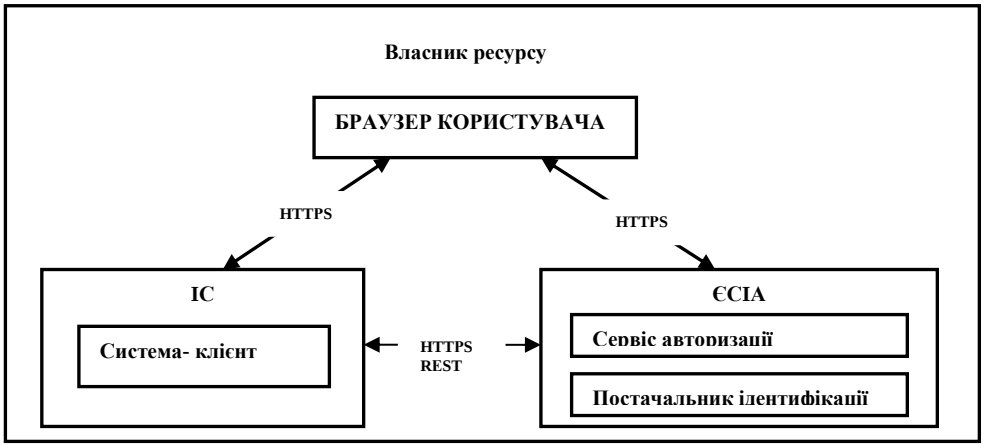


Рисунок 4.3 – Сценарії взаємодії ICS із системами ЄСІА за стандартом OpenID Connect 1.0

Автентифікація з використанням стандартуSAML

SAML або Security Assertion Markup Language - мова розмітки на основі XML, розширена до XHTML, RSS, Atom. Використовується для обміну даними

автентифікації та авторизації між учасниками, особливо між постачальниками ідентифікації та постачальниками послуг. SAML — це продукт OASIS, розроблений Радою безпеки технічних служб. Цей стандарт був розроблений у 2001 році. Останнє серйозне оновлення SAML було випущено в 2005 році, але розширення протоколу постійно випускалися за допомогою інших стандартів.

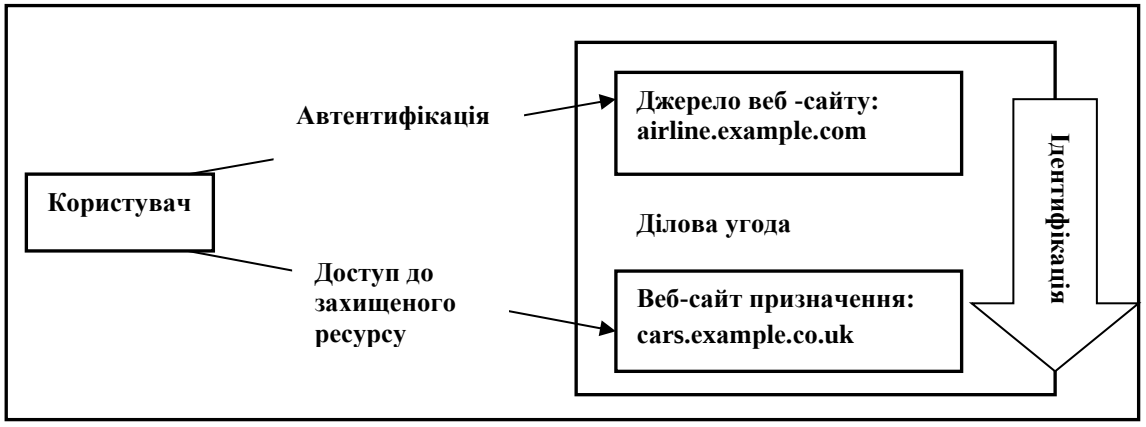


Рисунок 4.4 – Стандартний єдиний вхід

Цей стандарт (SAML) визначає структуру на основі XML для опису та обміну захищеною інформацією між онлайн-діловими партнерами. Важливою проблемою, яку вирішує SAML, є забезпечення однофакторної автентифікації (єдиного входу) під час роботи через веб-браузер. Це відображається у формі тверджень, що передаються через стандарт SAML, що додаткам і додаткам, що працюють у мережі домену, можна довіряти. Цей стандарт OASIS SAML визначає точний синтаксис і правила для запиту, створення, спілкування та використання цих операторів SAML.

Чому для обміну інформацією безпеки потрібен стандарт SAML? Це включає:

– перше, Single Sign-On (одноразовий підпис). На протязі багатьох років при здійснені продажу різноманітних продуктів, які потребують підтримки Web SSO покладаються на файли cookie для підтримки інформації про стан автентифікації користувача. Це дозволяє не повторювати автентифікацію кожного разу, коли веб-користувач хоче отримати доступ до системи. Однак, оскільки файли cookie ніколи не передаються між доменами DNS, інформація про стан автентифікації в файлі cookie з одного домену ніколи не може використовуватися для іншого домену. Таким чином, ці продукти зазвичай підтримують багатодоменну автентифікацію SSO (MDSSO) за допомогою власних механізмів для передачі інформації про їхній стан між доменами. Хоча іноді можливо використовувати пропозицію від одного постачальника в межах одного підприємства, бізнес-партнери часто мають гетерогенні середовища, які використовують власні протоколи, які непрактичні для MDSSO. SAML вирішує

проблему MDSSO, надаючи стандартний, незалежний від виробника синтаксис і протокол для передачі інформації користувача з одного веб-сервера на інший, незалежно від домену сервера DNS.;

– друге, Federated identity (корпоративна ідентифікація). Використовується, коли Інтернет-сервіси намагаються створити загальне прикладне середовище для своїх спільних користувачів, не тільки щоб зрозуміти синтаксис протоколу та семантику, що бере участь в обміні інформацією, а й - хто є користувачі. Зазвичай користувачі мають окремі локальні ідентифікатори в домені безпеки кожного партнера, з яким вони взаємодіють. Фірмовий стиль надає цим партнерським службам інструмент для координації та встановлення загального ідентифікатора. Коли партнер укладає таку угоду про контакт з користувачем, вважається, що користувач має фірмовий стиль. З адміністративної точки зору, цей тип обміну допомагає зменшити витрати на керування ідентифікацією, оскільки різним службам не потрібно самостійно збирати та підтримувати дані, пов'язані з автентифікацією (наприклад, паролі, облікові дані). Крім того, адміністраторам цих служб зазвичай не потрібно вручну налаштовувати та підтримувати спільні ідентифікатори;

– третє, Web services and other industry standards. SAML дозволяє використовувати безпечну автентифікацію для вашого формату поза «рідним» контекстом протоколу SAML. Ця модульність виявилася корисною для інших видів роботи в таких областях, як Служби авторизації (IETF, OASIS), Identity Frameworks, Web Services (OASIS, Liberty Alliance).

Технічний комітет OASIS WS-Security визначає профіль для використання SAML, як частину маркера безпеки WS-Security, який можна використовувати, наприклад, для ввімкнення обміну повідомленнями SOAP для веб-сервісів. Зокрема, використання SAML забезпечує перевагу в тому, що надає стандартний метод обміну інформацією, включаючи атрибути, які нелегко транспортувати за допомогою іншого формату маркерів WS-Security.

Основні поняття SAML розкрито на рис. 4.5.

Базові сценарії – це сценарії, коли особи (наприклад, заявники) автентифікуються. Цей скрипт дозволяє отримати інформацію про одного користувача (особу) під час автентифікації та профіль SSO, сумісний із SAML 2.0. Програма включає в себе наступні кроки:

1. Користувач натискає кнопку на системній сторінці постачальника послуг "Увійти за допомогою ЄСІА".

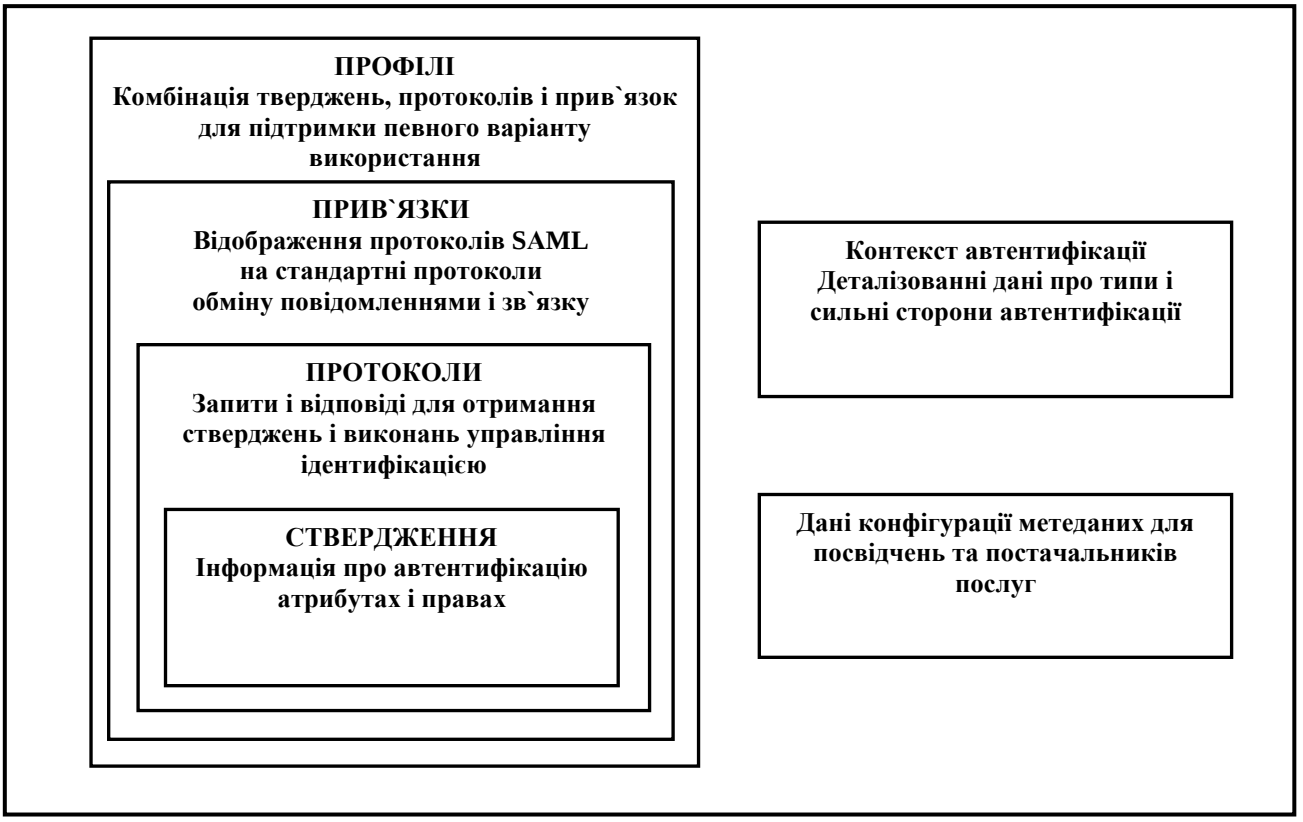


Рисунок 4.5 – Основні поняття SAML та компонентів SAML

Типовий приклад підключення компонентів SAML показаний на рис. 4.6.

Рисунок 4.6– Зв'язок компонентів SAML

2. Постачальник послуг генерує запит на автентифікацію та надсилає його до ЄСІА, перенаправляючи браузер користувача на сторінку автентифікації ЄСІА.

3. ЄСІА перевіряє статус автентифікації користувача. Якщо користувач не автентифікований в ЄСІА, він повинен пройти автентифікацію одним із доступних способів, щоб продовжити процес. Якщо користувач ще не зареєстрований у ЄСІА, він може продовжити процес реєстрації.

4. Під час автентифікації користувача ЄСІА перевіряє, чи відповідає рівень автентифікації користувача системним вимогам, і записує це в метадані.

5. Коли користувач успішно автентифікований, ЄСІА надсилає системі відповідь на запит автентифікації, що містить набір тверджень SAML щодо користувача.

6. Постачальник послуг визначає авторизацію Користувача на основі інформації, отриманої від ЄСІА. ЄСІА також дозволить вам автентифікувати користувачів як: юридичних осіб та/або представників ОГС. Ця функція необхідна для систем, які включають співробітників організації, наприклад, заявників або співробітників ОГС. Якщо ця можливість включена в метадані постачальника послуг, ЄСІА надасть інформацію про організацію користувача у відповідь на запити автентифікації. Якщо користувач є членом кількох організацій, ЄСІА спочатку запитає користувача, від імені якого він автентифікується. Якщо система підтримує роботу користувачів з різними ролями, то під час автентифікації користувач зможе вибрати роль, яку він буде працювати в цій ІКС. Щоб переконатися, що автентифікований співробітник має необхідні дозволи, вам слід скористатися функціоналом системної групи та перевірити, чи вона має необхідні дозволи – рекомендується відповідний оператор SAML.

Після автентифікації користувача ЄСІА встановлює сеанс користувача, який триває 3 години. Факт початку сеансу записується в файлі cookie, який зберігається на комп’ютері користувача. Система може налаштувати «локальний» сеанс користувача. Наприкінці «локального» сеансу система має надіслати новий запит на автентифікацію до ЄСІА.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Автентифікація – це фактично процес перевірки ідентичності суб’єкта. У принципі суб’єктом може бути не тільки людина, а й програмний процес. На закінчення можна сказати, що за допомогою інформації, що зберігається в різних формах, особу можна автентифікувати. Наприклад, це можуть бути: паролі, персональні номери, ключі, мережеві адреси комп’ютерів у мережі; смарт–карти, електронні ключі; зовнішній вигляд користувача, голос, малюнок райдужної оболонки, відбитки пальців та інші біометричні дані.

Автентифікація дозволяє розрізняти доступ до загальнодоступної інформації з достатньою надійністю. Проте існують проблеми із забезпеченням цілісності та надійності інформатизації. Користувач повинен переконатися, що він має доступ до інформації з надійних джерел і що ця інформація не була змінена без відповідних санкцій.

Пошук збігів один з одним (через властивість) називається перевіркою. Цей метод швидкий і вимагає мінімальних вимог до обчислювальної потужності комп’ютера. Пошук "один до багатьох" називається ідентифікацією. Реалізація таких алгоритмів часто не тільки складна, але й дорога. Наприклад, Windows потребує двох об’єктів для автентифікації: імені користувача та пароля. Якщо для автентифікації використовується технологія розпізнавання відбитків пальців, необхідно ввести ім’я для реєстрації, і відбиток пальця замінить пароль. У цьому випадку ім’я користувача є вказівником для отримання його облікового запису та перевірки «взаємної» відповідності між шаблоном, прочитаним під час реєстрації відбитків пальців, і шаблоном, раніше збереженим для цього імені користувача. Крім того, шаблон відбитка пальця, введений під час процесу реєстрації, повинен відповідати всьому набору збережених шаблонів. При виборі методу автентифікації має сенс враховувати кілька основних факторів: цінність інформації; вартість програмно–апаратної автентифікації; продуктивність системи; ставлення користувачів до використовуваного методу автентифікації; деталі

(призначення) захищеного інформаційного комплексу. Очевидно, що вартість, а отже, якість і надійність інструменту перевірки повинні бути пропорційні важливості інформації. Також підвищення продуктивності комплексу часто супроводжується підвищенням ціни.

Основними завданнями безпеки комп'ютерної системи є автентифікація, контроль доступу, аудит, а також забезпечення конфіденційності, доступності та цілісності даних. Сучасні функції безпеки засновані на криптографічних методах, таких як алгоритми секретних і відкритих ключів, гібридні криптосистеми, цифрові підписи та сертифікати. Автентифікація дозволяє переконатися, що користувачі є тими, за кого себе видають, і можуть бути допущені до системи. Паролі часто використовуються для автентифікації користувачів. Сучасні методи автентифікації дозволяють уникнути передачі паролів через незашифровані канали зв'язку. Контроль доступу (авторизація) дозволяє визначити дії, які можуть виконувати авторизовані користувачі над різними об'єктами системи. Авторизація досягається на основі визначення списків контролю доступу, пов'язаних з об'єктами в системі, і визначення списків можливостей, пов'язаних з окремими користувачами. Можна стверджувати, що побудова комплексної системи інформаційної безпеки вимагає глобального підходу до всіх аспектів проблеми. Поступове впровадження інформаційної безпеки на правовому, організаційному, інженерному, апаратному та програмному рівнях дасть змогу створити цілісну систему забезпечення надійної інформаційної безпеки. Дослідження та побудова моделей загроз дозволить виявити слабкі місця в системах та усунути їх. Тому проблема захисту інформації в сучасних інформаційно–комунікаційних системах і мережах потребує комплексного підходу до вирішення проблеми інформаційної безпеки.

Одним з перспективних напрямків розвитку систем автентифікації є розробка біометричних систем. Основні зусилля в цьому напрямку спрямовані на розробку та вдосконалення апаратного та програмного забезпечення для значного зниження рівня помилок типу 1 і типу 2 та запобігання загрозам підробки. Масове виробництво такої системи значно знизило б її вартість.

Більшість майбутніх систем автентифікації будуть побудовані на

комбінованому типі – використовуючи два або більше методів автентифікації одночасно (зв’яжіться

Захищені паролем токени з вбудованими чіпами безконтактної автентифікації, токени з вбудованими засобами біометричної автентифікації тощо).

Розвиток токенів може здійснюватися за такими напрямками: мініатюризація, розробка та вдосконалення безконтактних інтерфейсів (безпека інформаційних каналів, мінімізація споживання енергії), подовження терміну служби, імплантація в організм людини.

Найближчим часом деякі системи автентифікації, засновані на символьних паролях, будуть замінені на системи, засновані на графічних паролях, оскільки це більш безпечно. Однак деякі незручності введення графічного пароля обмежують його використання в найпростіших системах

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Асиметричні методи шифрування в телекомунікаціях. Модуль 2 Криптографічні методи захисту інформації в телекомунікаційних системах та мережах/М.В. Захарченко, О.В. Онацький, Л.Г.Йона, Т.М. Шинкарчук// Навч.посібн.– Рекомендовано МОН молоді та спорту України, – ОНАЗ ім. О.С.Попова, – 2011, – 184с.
2. Системи банківської безпеки / Л.Г. Йона, О.В. Онацький, О.В. Швець// Навчальний посібник,– 2021, –58с.
3. Криптографическая защита электронного документооборота./ Л.Г. Йона, Е.О.Йона, В.С.Терешко / /Збірник наукових праць «Цифрові технології», – 2013, № 13, – С.142–146.
4. Закон України № 851–IV від 01.08.2021р. « Про електронні документи та електронний документообіг» [Електронний ресурс] – Режим доступу: https: //zakon.rada.gov.ua/ laws/show.
5. Закон України № 2121–III від 07.12.2020р. «Про банки і банківську діяльність» [Електронний ресурс] – Режим доступу: https: //zakon.rada. gov.ua/ laws/show.
6. Закон України № 2155–VIII від 01.08.2021р. « Про електронні довірчі послуги» [Електронний ресурс] – Режим доступу: https: //zakon.rada.gov.ua/ laws/show. ДСТУ 4145–2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка» [Електронний ресурс] – Режим доступу: https: //zakon.rada. gov.ua/ laws/show.;

ДОДАТОК А

ПЕРЕЛІК КОПІЙ ДЕМОНСТРАЦІЙНОГО МАТЕРІАЛУ

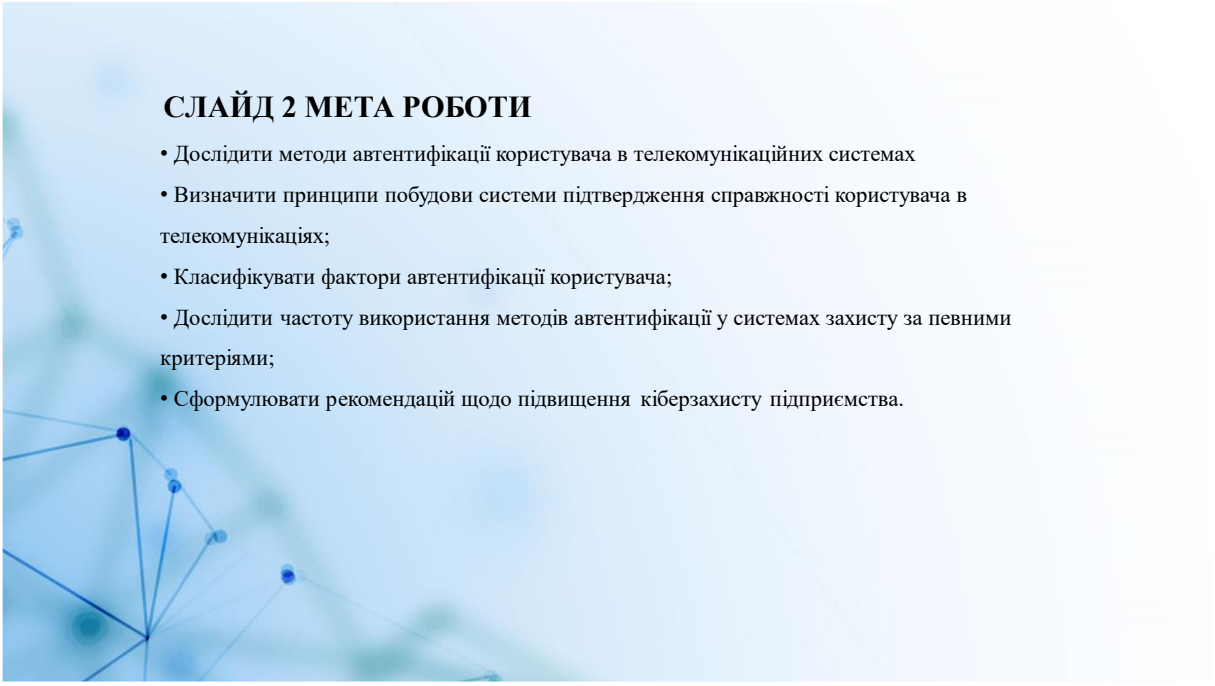


Рисунок А.1 – Рисунок А.1 – Мета роботи

Рисунок А.2 – Протоколи автентифікації

СЛАЙД 4 ФАКТОРИ АВТЕНТИФІКАЦІЇ

ФАКТОРИ АВТЕНТИФІКАЦІЇ					
ЗНАННЯ	ВОЛОДІННЯ	ВЛАСТИВОСТІ			
		Біометричні		За дією	За місцем
		Статичні	Динамічні		
PIN	Ключ	Відбиток пальця, губ	Голос	Жест	Розташування
Кодова фраза	USB- токен	Сітківка ока	Хода	Підпис	Позиція на поточний час
Пароль	Смартфон	Геометрія обличчя, долоні	Клавіатурний почерк	Електронний підпис	
	Картка	ДНК	Рух губ		
		Форма черепа, вуха	Динаміка підпису		
		Зображення вен	Почерк		
		Райдужна оболонка ока			

Рисунок А.3 – Фактори автентифікації

СЛАЙД 5 БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ

БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ– метод, який заснований на використанні унікальних біологічних характеристик людини.

В якості таких характеристик можуть бути використані: відбиток пальця чи губ, геометрія обличчя чи руки, сітківка чи райдужна оболонка ока, хода, голос, підпис, тощо .

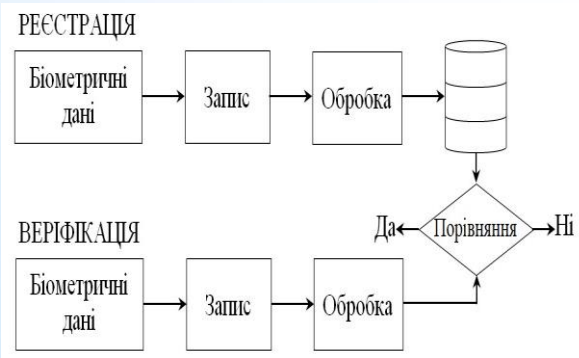


Рисунок А.4 – Біаметрична автентифікації

СЛАЙД 6 АВТЕНТИФІКАЦІЯ З ВИКОРИСТАННЯМ ОДНОРАЗОВИХ ПАРОЛІВ

АВТЕНТИФІКАЦІЯ З ВИКОРИСТАННЯМ ОДНОРАЗОВИХ ПАРОЛІВ (One-Time Passwords – OTP) – метод автентифікації для генерації одноразових паролів з метою автентифікації клієнтів під час входу в систему, а також для підтвердження платіжних доручень, який заснований на генерації динамічної інформації для одиничного використання.

Для генерації одноразових паролів OTP-токени використовують геш-функції або криптографічні алгоритми:

– симетрична криптографія – в цьому випадку користувач і сервер автентифікації використовують один і той самий секретний ключ;

– асиметрична криптографія – в цьому випадку в пристрої зберігається секретний ключ, а сервер автентифікації використовує відповідний відкритий ключ.

Рисунок А.5 – Автентифікація з використанням одноразових паролей

СЛАЙД 7 МЕТОДИ АВТЕНТИФІКАЦІЯ

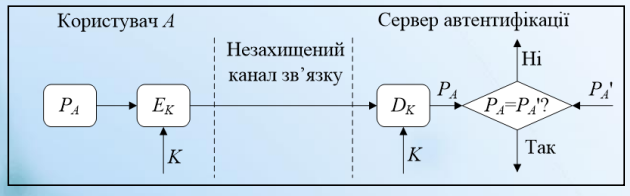
КРИТЕРІЇ ЗАХИСТУ	МЕТОДИ АВТЕНТИФІКАЦІЇ							
	PIN	Пароль	Картка	Відбиток пальця	Підпис	Сітківка ока	ДНК	ЕП
Безпека	**	**	**	**	**	***	***	***
Зручність	***	***	***	***	**	**	*	**
Актуальність	***	***	***	**	**	**	*	**
Вартість	***	***	***	**	**	**	*	*

* - мало
** - часто
*** - дуже часто

Рисунок А.6 – Автентифікація з використанням одноразових паролей

СЛАЙД 8 ПРОСТА АВТЕНТИФІКАЦІЯ

Схема простої автентифікації з використанням пароля



P_A – пароль

D – розшифрування

E – зашифровування

K – ключ

Схема простої автентифікації з використанням односторонньої функції для перевірки пароля

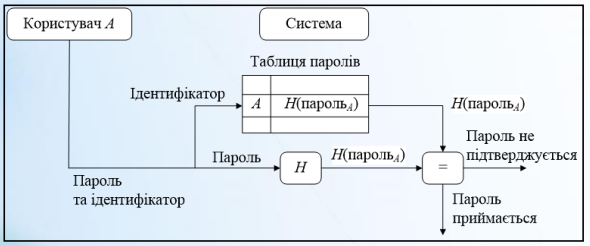


Рисунок А.7 – Проста автентифікація

СЛАЙД 9 ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС

Електронний цифровий підпис (ЕЦП) або електронний підпис (ЕП), використовується для автентифікації текстів, які передають по телекомунікаційних каналах.

ЕЦП є аналогом звичайного рукописного підпису й має основні його переваги:

- засвідчує, що підписаний текст виходить від імені користувача, котрий поставив підпис;
- не надає саме цьому користувачеві можливості відмовитися від зобов'язань, пов'язаних з підписаним текстом;
- гарантує цілісність підписаного тексту.

Цифровий підпис являє собою відносно невелику кількість додаткової цифрової інформації, яка передається разом з підписуваним текстом .

Система ЕЦП включає дві процедури:

1 процедуру формування підпису;

2 процедуру перевірки підпису.

Рисунок А.8 – Електронний цифровий підпис

СЛАЙД 10 РЕКОМЕНДАЦІЇ ЩОДО ПІДВИЩЕННЯ КІБЕРЗАХИСТУ ПІДПРИЄМСТВА.

Для вирішення проблеми інформаційної безпеки необхідно уточнити та сформулювати цілі та завдання інформаційної безпеки підприємства.
Діяльність із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п’яти функцій кібербезпеки:

- **ідентифікація ризиків;**
- **кіберзахист;**
- **виявлення кіберінцидентів;**
- **реагування;**
- **відновлення поточного стану кібербезпеки.**

Відповідно до підпункту 1 частини другої та пункту 3 частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України», абзацу другого частини першої статті 3, пунктів 85, 86 і 88 частини першої статті 14 Закону України «Про Державну службу спеціального зв’язку та захисту інформації України», абзацу другого підпункту 1 пункту 3 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністр ів України від 3 вересня 2014 року № 411, та Загальних вимог до кіберзахистуоб’єктів критичної інфраструктури,затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, з метою підвищення рівня кіберзахисту критичної інформаційної інфраструктури.

Рисунок А.9 – Рекомендації щодо підвищення кіберзахисту підприємства

СЛАЙД 11 ВИСНОВКИ

- Досліджено методи автентифікації користувача.
- Розглянуто класифікацію методів автентифікації.
- Запропоновано використання методів автентифікації в телекомунікаційних системах та вимоги до налаштування, запитів, коментарів.
- Класифіковано фактори автентифікації користувача;
- Досліджено частоту використання методів автентифікації у системах захисту за певними критеріями;
- Сформульовано р екомендацій щодо підвищення кіберзахисту підприємства.

Рисунок А.10 – Висновки