МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Одарченко Р.С.
“_____”_____2021 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Захищена система електронного документообігу на базі платформи Google Workspace».

Виконавець: _____ Шаповалова А.В.
(підпис)

Керівник: _____ Бахтіяров Д. І.
(підпис)

Нормоконтролер: _____ Бахтіяров Д. І.
(підпис)

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Одарченко Р.С.
“_____”_____2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

Шаповалової Анни Володимирівни
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломної роботи (проекту): «Захищена система електронного документообігу на базі платформи Google Workspace»
затверджена наказом ректора від «06» квітня 2021 р. № 559 / ст
2. Термін виконання роботи: з 17.05.2021 р. по 20.06.2021 р.
3. Вихідні дані до роботи: Огляд основних вимог до ЕЦП; розгляд можливостей використання ЕЦП у ВНЗ; дослідження способів формування ЕЦП та основних криптографічних алгоритмів; створення власного цифрового підпису, підписання та відправка онлайн документа з використанням платформи Google Workspace
4. Зміст пояснювальної записки: Загальні вимоги до електронного цифрового підпису та можливості його застосування у вищих навчальних закладах; особливості формування електронного цифрового підпису; аналіз системи електронного документообігу Google Workspace
5. Перелік обов'язкового графічного (ілюстративного) матеріалу:. Поліпшений процес заповнення відомостей; алгоритм шифрування з використання симетричного шифрування; порядок виконання хешування

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів диплому	17.05.2021-19.05.2021	Виконано
2	Вступ	19.05.2021-20.05.2021	Виконано
3	Загальні вимоги до електронного цифрового підпису та можливості його застосування у вищих навчальних закладах	21.05.2021-25.05.2021	Виконано
4	Особливості формування електронного цифрового підпису	26.05.2021-30.05.2021	Виконано
5	Аналіз системи електронного документообігу Google Workspace	31.05.2021-03.06.2021	Виконано
6	Захищена система електронного документообігу на базі платформи Google Workspace	04.06.2021-08.06.2021	Виконано
7	Усунення недоліків дипломної роботи	09.06.2021-12.06.2021	Виконано

7. Дата видачі завдання: «26» квітня 2021 р.

Керівник дипломної роботи _____ Бахтіяров Д. І.
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Шаповалова А.В.
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Дипломна робота «Захищена система електронного документообігу на базі платформи Google Workspace» містить 62 сторінки, 21 рисунок, 2 таблиці, 23 використаних джерела.

ЕЛЕКТРОНИЙ ДОКУМЕНТООБІГ, ЕЛЕТРОННИЙЦИФРОВИЙ ПІДПИС, ПЛАТФОРМА GOOGLE WORKSPACE, АЛГОРИТМИ ШИФРУВАННЯ, ОСОБИСТИЙ КЛЮЧ.

Об’єкт дослідження – процеси електронного документообігу з використанням додатків Google Workspace.

Предмет дослідження – електронний цифровий підпис, як інструмент для оптимізації електронного документообігу.

Мета дипломної роботи – вивчення та ефективне впровадження електронного цифрового підпису як засобу підтвердження та захисту електронних даних.

Методи дослідження – теоретичний метод, аналітичний огляд, метод порівняння і аналізу.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

AES – Advanced Encryption Standard

DSA – Digital Signature Algorithm

EGSA – El Gamal Signature Algorithm

PIN – Personal Identification Number

RSA – Rivest, Shamir Adleman

SMS – Short Message Service

USB – Universal Serial Bus

АЦСК – акредитований центр сертифікації ключів

ВНЗ – вищий навчальний заклад

ДФС – Державна фіскальна служба

ЕДП – електронні довірчі послуги

ЕП – електронний підпис

ЕЦП – електронний цифровий підпис

ЗС – засвідчувальний центр

КЕП – кваліфіковваний електронний підпис

ПЗ – програмне забезпечення

УЕП – удосконалений електронний підпис

ЦСК – центр сертифікації ключів

ВСТУП

Актуальність теми. Україна йде шляхом цифрової політики та діджіталізації суспільства. Оскільки переважна більшість людей користується різними гаджетами для зберігання, відтворення та передачі інформації, тому постає актуальна потреба в збереженні та безпечному захисті інформації.

Застосування електронного документообігу на сьогодні все ширше розповсюджується на все більше сфер життя. Для забезпечення захищеності документів та для підтвердження унікальності документа найкращим варіантом є використання електронного цифрового підпису.

Електронний цифровий підпис – ефективний засіб контролю та захисту електронного документа від підробки або внесення змін, отриманий в результаті криптографічного перетворення інформації з використанням секретного ключа, що дозволяє ідентифікувати власника ключа підпису і встановити відсутність зміни інформації в електронному документі.

Мета і завдання дослідження.

Мета дипломної роботи полягає в вивченні та ефективному впровадженні електронного цифрового підпису як засобу підтвердження та захисту електронних даних.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Огляд основних вимог до ЕЦП, законодавчих основ, розвитку ЕЦП в Україні.
2. Розгляд можливостей використання ЕЦП у ВНЗ.
3. Дослідження способів формування ЕЦП.
4. Дослідження основних криптографічних алгоритмів, з допомогою яких утворюється ЕЦП.
5. Дослідження та можливості організації електронного документообігу з допомогою платформи Google Workspace.

6. Створення власного цифрового підпису, підписання та відправка онлайн документа з використанням платформи Google Workspace.

Об'єктом дослідження є процеси електронного документообігу з використанням додатків Google Workspace.

Предметом дослідження є електронний цифровий підпис, як інструмент для оптимізації електронного документообігу.

Методи досліджень. Для досягнення поставлених цілей в роботі використано теоретичні методи: аналітичний огляд загальних вимог до ЕЦП, розвиток ЕЦП в Україні, аналіз нормативно-правової бази, наукової літератури, дослідження криптографічних алгоритмів, з допомогою яких утворюється ЕЦП.

Практичне значення отриманих результатів.

Ідея активного впровадження електронного документообігу в усі можливі сфери діяльності створює передумови для покращення якості управління та сприяє утворенню цілісної електронної системи документообігу. Невід'ємною частиною електронного документа є електронний цифровий підпис, що забезпечить цілісність документа та підтвердить особу, що підписала документ. Використання ЕЦП суттєво заощаджує час та витрати, прискорює проведення чисельних операцій, виключає необхідність додаткових зустрічей і переговорів.

Можливості застосування ЕЦП може значно зекономити час при підписанні будь-яких електронних документів, до прикладу, звітів, договорів, наказів, екзаменаційних та залікових відомостей тощо. Електронні підписи не тільки допомагають вузам скоротити кількість роздрукованих документів, які необхідно підписати, а також час, що витрачається на їх обробку, крім того електронні підписи скорочують витрати та є надійно захищеними. Особливо актуальним є використання ЕЦП у вищих навчальних закладах під час дистанційного навчання, оскільки в цей період майже всі документи були переведені в електронний формат.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2021 р.

РОЗДІЛ 1
ЗАГАЛЬНІ ВИМОГИ ДО ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ТА МОЖЛИВОСТІ ЙОГО ЗАСТОСУВАННЯ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

1.1. Нормативно-правові засади впровадження електронного цифрового підпису в Україні

Внаслідок активного розвитку та впровадження сучасних онлайн-сервісів та електронного документообігу виникає потреба в визначеному аналозі цифрового підпису для підтвердження особи. Електронний цифровий підпис (ЕЦП) створений з метою забезпечення автентифікації особи.

У 2003 році Україна прийняла закон «Про електронний цифровий підпис» від 22 травня 2003р. № 852-IV, який запровадив у наше правове поле поняття електронного підпису та електронного цифрового підпису. Цей Закон визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при його використанні. У тому ж році був прийнятий закон «Про електронні документи та електронний документообіг» від 22 травня 2003р. № 851-IV.

Відповідно до статті 1 Закону «Про електронний цифровий підпис» електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа; особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу; відкритий ключ – параметр криптографічного алгоритму перевірки електронного

цифрового підпису, доступний усім суб'єктам відносин у сфері використання електронного цифрового підпису [1].

Цей Закон втратив чинність 7 листопада 2018 року, на підставі закону «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII і визначає правові та організаційні засади надання електронних довірчих послуг, у тому числі транскордонних, права та обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг, порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також правові та організаційні засади здійснення електронної ідентифікації.

Метою цього Закону є врегулювання відносин у сферах надання електронних довірчих послуг та електронної ідентифікації.

Згідно з статтею 22 даного Закону формування та видача кваліфікованого сертифіката відкритого ключа без ідентифікації особи, ідентифікаційні дані якої міститимуться у кваліфікованому сертифікаті відкритого ключа, не допускаються. Ідентифікація фізичної особи, яка звернулася за отриманням послуги формування кваліфікованого сертифіката відкритого ключа, здійснюється за умови її особистої присутності за паспортом громадянина України або за іншими документами, які унеможливлюють виникнення будь-яких сумнівів щодо особи, відповідно до законодавства про Єдиний державний демографічний реєстр та про документи, що посвідчують особу, підтверджують громадянство України чи спеціальний статус особи [2].

Однією з головних переваг впровадження електронного розпізнавання міжнародних стандартів є двостороннє визнання українських та іноземних сертифікатів відкритих ключів, а також електронних підписів. Тобто, засоби електронного розпізнавання особи, що були випущені в Україні, можуть бути використані за кордоном, а в Україні можуть бути визнані засоби, випущені закордоном.

Іншим не менш важливим нововведенням є впровадження взаємодії, тобто забезпечення взаємодії технічних рішень, що використовуються у наданні електронних послуг, та їх здатності взаємодіяти між собою.

До того ж впроваджується Довірчий список, в якому міститься інформація про юридичних та фізичних осіб разом з інформацією про кваліфіковані електронні довірчі послуги, які вони надають.

Відповідно до зазначеного закону електронний підпис може бути трьох категорій:

- простий електронний підпис та печатка – з низьким рівнем довіри;
- удосконалений електронний підпис та печатка – з середнім рівнем довіри;
- кваліфікований електронний підпис та печатка – з високим рівнем довіри.

Простий цифровий підпис

Застосовуючи коди, паролі чи інші засоби, простий цифровий підпис підтверджує факт формування електронного підпису певною особою. Простий цифровий підпис має низький рівень захисту. Він лише дозволяє ідентифікувати автора документа. Простий цифровий підпис не захищає документ від підробки.

Удосконалений електронний підпис (УЕП) – електронний підпис, який відповідає таким додатковим критеріям:

- здійснюється шляхом криптографічного перетворення даних, до яких він підключений, з використанням спеціального обладнання або програмного забезпечення;
- з застосуванням персонального ключа, який пов'язаний з підписувачем і виконує його електронну ідентифікацію;
- будь-яке порушення цілісності даних, пов'язаних з відповідним підписом, обов’язково буде виявлено.

Кваліфікований електронний підпис (КЕП) – вдосконалений електронний підпис, що створюється через кваліфікований інструмент електронного підпису та ґрунтується на кваліфікованому сертифікаті відкритого ключа. КЕП в електронному документі рівнозначно власному підпису, а також мокрий друк на папері.

Окрім електронних підписів, даний закон впроваджує визначення електронної печатки. Електронну печатку можна вдосконалити та кваліфікувати – критерії

подібні до відповідних критеріїв класів підписів. Різниця полягає у тому, що електронним підписом можуть користуватися як юридичні, так і фізичні особи, а електронною печаткою - лише юридичні особи. У функціональному відношенні між електронним підписом та електронною печаткою немає суттєвої різниці.

1.2. Діяльність Акредитованих центрів сертифікації ключів.

Для створення електронного підпису в Україні діють Акредитовані центри сертифікації ключів - (АЦСК), які мають право:

- створювати електронний цифровий підпис та обслуговувати посиленні сертифікати ключів;
- отримувати та перевіряти інформацію, необхідну для реєстрації підписувача та формування посиленого сертифіката ключа, безпосередньо в юридичної або фізичної особи чи її представника.

Акредитований центр сертифікації ключів - це державний орган який надає такі послуги:

- надає захист засобам електронного цифрового підпису;
- допомагає генерації відкритих та закритих ключів;
- надає послуги обслуговування сертифікатів ключів, а саме формування, скасування, зберігання та блокування;
- фіксує час;
- надає актуальну інформацію про чинні та скасовані сертифікати ключів.

Акредитований центр сертифікації ключів має виконувати усі зобов'язання та вимоги, встановлені чинним законодавством для центру сертифікації ключів, та додатково зобов'язаний використовувати для надання послуг електронного цифрового підпису надійні засоби електронного цифрового підпису [3].

Акредитацію АЦСК виконує Центральний засвідчувальний орган, який відповідає вимогам, встановленим законодавством. Нині акредитованими є 25 центрів сертифікації ключів, що представлені в таблиці 1.1.[4]

Таблиця 1.1

Акредитовані центри сертифікації ключів та засвідчувальні центри

№	Найменування
1	АКЦІОНЕРНЕ ТОВАРИСТВО КОМЕРЦІЙНИЙ БАНК "ПРИВАТБАНК" https://acsk.privatbank.ua
2	Державна прикордонна служби України http://acsk.dpsu.gov.ua/
3	Генеральний штаб Збройних Сил України http://ca.mil.gov.ua
4	Офіс Генерального прокурора https://ca.gp.gov.ua
5	Державна казначейська служба України http://acsk.treasury.gov.ua
6	Державне підприємство "ДІЯ" https://ca.diia.gov.ua
7	Державне підприємство "Українські спеціальні системи" http://csk.uss.gov.ua
8	Інформаційно-довідковий департамент ДПС www.acskidd.gov.ua
9	Міністерство внутрішніх справ України http://ca.mvs.gov.ua
10	Національний банк України http://canbu.bank.gov.ua
11	Публічне акціонерне товариство "Державний ощадний банк https://ca.oschadbank.ua
12	Акціонерне товариство "УкрСиббанк" https://csk.ukrsibbank.com
13	Товариство з обмеженою відповідальністю "Алтерсайн" http://altersign.com.ua
14	Товариство з обмеженою відповідальністю "Арт-мастер" www.masterkey.ua

Закінчення таблиці 1.1

15	Товариство з обмеженою відповідальністю "Інтер-Метл" http://cesaris.itsway.kiev.ua
16	Філія "Головний інформаційно-обчислювальний центр" публічного акціонерного товариства "Українська залізниця" https://csk.uz.gov.ua/
17	Товариство з обмеженою відповідальністю "Центр сертифікації ключів "Україна" www.uakey.com.ua
18	Товариство з обмеженою відповідальністю "Ілайф https://ca.e-life.com.ua/
19	АЦСК ринку електричної енергії https://acsk.oree.com.ua/
20	Український інститут інтелектуальної власності https://ukrpatent.org
21	АКЦІОНЕРНЕ ТОВАРИСТВО "ПЕРШИЙ УКРАЇНСЬКИЙ МІЖНАРОДНИЙ БАНК" https://pki.pumb.ua/
22	Товариство з обмеженою відповідальністю "ДЕПОЗИТ САЙН" https://depositsign.com
23	Засвідчувальний центр Національного банку України https://czo.gov.ua/
24	АТ "КРЕДІ АГРІКОЛЬ БАНК" https://ca.credit-agricole.ua/
25	ПАТ «Альфа-Банк» https://ca.alfabank.kiev.ua/

1.3. Застосування електронного цифрового підпису

Електронний цифровий підпис широко використовується в системах електронного документообігу різного призначення. ЕЦП може бути використаний в якості підпису на електронному документі, оскільки є рівноцінний власному підпису.

Постанова Кабінету Міністрів України «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» № 1452 від 28 жовтня 2004 року визначає вимоги щодо застосування ЕЦП органами державної влади.

Згідно з цим порядком органи державної влади можуть використовувати лише надійно захищені засоби ЕЦП. Також для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа [5].

Органи державної влади не можуть застосовувати електронний цифровий підпис:

- при складанні електронних документів, які не можуть бути оригіналами у випадках, передбачених чинним законодавством;
- при вчиненні правочинів на суму, що перевищує 1 млн. гривень.

Органи державної влади на договірних засадах отримують послуги, пов'язані з електронним цифровим підписом, від акредитованого центру сертифікації ключів. Слід зауважити, що орган державної влади може отримувати такі послуги лише від одного акредитованого центру сертифікації ключів. Використання підписувачами особистих ключів, відповідні відкриті ключі яких засвідчені іншими акредитованими центрами сертифікації ключів, забороняється.

Відповідальність за застосування електронного цифрового підпису несе керівник, якщо інше не встановлено чинним законодавством. Застосування електронного цифрового підпису в установах державної влади забезпечує підрозділ інформаційних технологій, якщо такий відсутній - підрозділ, що виконує подібні функції, або працівник, спеціально визначений наказом керівника цієї установи.

Порядок надання працівникам органів держаної влади права застосування електронного цифрового підпису, ведення обліку, зберігання та знищення їх особистих ключів, а також надання акредитованому центру сертифікації ключів інформації, необхідної для формування, скасування, блокування або поновлення посилених сертифікатів відкритих ключів підписувачів цих установ,

визначається наказом її керівника, якщо інше не встановлено чинним законодавством.

Електронний цифровий підпис підписувач може застосовуватись лише після отримання органом державної влади від акредитованого центру сертифікації ключів посиленого сертифіката його відкритого ключа. У разі звільнення підписувача орган влади звертається до акредитованого центру сертифікації ключів для скасування посиленого сертифіката його відкритого ключа, а особистий ключ знищується методом, що не допускає можливості його відновлення.

Підписувач використовує у процесі виконання своїх функцій лише особистий ключ. Підписувач може мати і використовувати лише один особистий ключ, якому відповідає відкритий ключ з чинним посиленим сертифікатом, отриманим органом державної влади. Це обмеження не стосується електронної печатки. Підписувач несе відповідальність за зберігання особистого ключа. Копіювання особистих ключів або передача їх іншим особам забороняється.

Справжність електронного цифрового підпису, накладеного на електронний документ або інші електронні дані, та цілісність цього документа (даних) перевіряється з дотриманням таких вимог:

- електронний цифровий підпис має бути обов’язково підтверджений з використанням посиленого сертифіката ключа та з допомогою надійно захищених засобів цифрового підпису;
- під час перевірки повинен використовуватися посилений сертифікат ключа, який є чинним в час підписання електронного документа;
- особистий ключ підписувача повинен відповідати відкритому ключу, що зазначений у сертифікаті;
- на час перевірки повинен бути чинним посилений сертифікат відкритого ключа акредитованого центру сертифікації ключів або посилений сертифікат відкритого ключа [6].

ЕЦП широко використовується в таких сферах:

- банківські платіжні системи;
- для здійснення електронної звітності;

- для електронної реєстрації угод;
- митне декларування товарів і послуг;

На сьогоднішній день за допомогою ЕЦП здійснено організування електронного документообігу, подання звітності в електронному вигляді, організація електронного листування, укладення договорів в електронній формі, а також можливість використовувати електронні сервіси ДФС України та послуги інших державних установ і відомств.

15 грудня 2017 року в Україні набрала чинності чергова судова реформа. Відповідно до якої документи переводяться в електронний формат з використанням власного цифрового електронного підпису [7].

З цього можна виділити певні переваги використання ЕЦП:

- поява можливості зашифрувати документ;
- зручність працювати з електронними документами, що мають юридичну силу;
- процедура перевірки ЕЦП реалізується з допомогою комп'ютера, тому вона безпомилкова та дозволяє уникнути людського фактору при перевірці звичайного підпису;
- конфіденційність інформації;
- підписавши документ ЕЦП, він не може бути зміненим чи підробленим;
- ЕЦП фіксує час підписання.

1.4. Можливості застосування ЕЦП у вищих навчальних закладах

У вищих навчальних закладах кожного дня витрачається багато часу на підписання різного роду документів: відомостей, договорів, наказів, звітів тощо. Труднощі полягають в тому, що документ може містити в собі одразу декілька підписів. Зазвичай персони, що підписують документ, перебувають в різних місцях, тоді з'являється необхідність пересилати або переміщувати документ, а це займає багато часу. Вирішенням цієї проблеми може бути застосування електронного цифрового підпису, що зможе значно зекономити час. Особливо актуальним є

використання ЕЦП у вищих навчальних закладах під час дистанційного навчання, оскільки в період дистанційного навчання майже всі документи були переведені в електронний формат.

Прикладом може слугувати заповнення екзаменаційних або залікових відомостей, яке відбувається щонайменше двічі на рік. Як правило, в заповнені відомостей приймають участь викладач, дирекція та директор. Головною ланкою тут є дирекція, що виконує роль посередника між викладачем і директором. Для зручності дирекція підгодовує пусті відомості, оскільки директор має підписувати багато відомостей. Після чого викладач заповнює відомості, далі вони містяться в інформаційній системі університету. До того ж складності додає й те що, директор при підписанні пустих відомостей, не бачить оцінок.

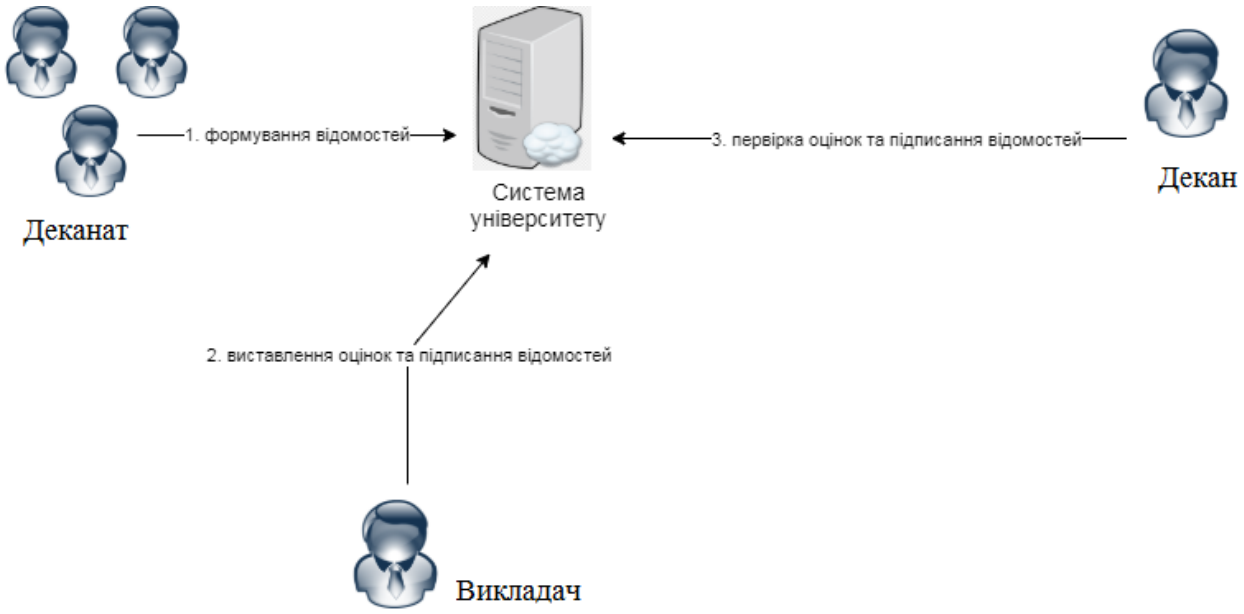

Рис. 1.1. Поліпшений процес заповнення відомостей

Застосування електронного цифрового підпису дає можливість істотно зекономити час для видачі та здачі відомостей. Головна суть ідеї в тому, що саме інформаційна система університету стає посередником між викладачем та директором. Ось як це може виглядати: дирекція записує інформацію про студента в систему, потім створюються електронні відомості, викладач вводить оцінки, і для підтвердження ставить свій цифровий підпис, а директор в свою чергу отримує

сповіщення та також підписує документ із застосуванням ЕЦП. Цей варіант заповнення електронних відомостей може бути використаний під час дистанційного навчання, оскільки всі відомості переводяться в електронний формат, і це зможе скоротити час заповнення та підписання відомостей (рис. 1).

Одними з найбільш поширеними носіями електронних цифрових підписів можна вважати смарт-карти та SIM-карти. Під час застосування SIM-картки підписання здійснюється на смартфоні, а передача даних між смартфоном та сервером здійснюється через мережу. Як правило, цей процес втілюється відповідним представником служби, що надає простий інтерфейс іншим особам для надсилання запиту та отримання результату. Ці інтерфейси зазвичай використовують відкриті технології, які дозволяють легко і швидко запровадити цю послугу на мережевих порталах, включаючи інформаційний портал університету. При застосуванні смарт-картки підписання здійснюється на самій картці через комп'ютер клієнта, що може створити певні труднощі. З міркувань безпеки мережеві технології не дозволяють отримати доступ до комп'ютерних пристроїв клієнта або файлової системи клієнта. Як варіант вирішення може бути використана підписана технологія застосування JAVA або, навпаки, технологія ActiveX. Ці технології дають можливість викликати методи на смарт-карті та в подальшому надіслати дані, що були отримані на сервер університетської інформаційної системи.

Даний варіант, що представлений на рисунку 1 містить в собі підготовку документа та підписи з допомогою ЕЦП, може бути також застосований для покращення документообігу у ВНЗ, до прикладу підписання різного роду документів(звітів, договорів, наказів тощо).

ВИСНОВКИ ДО РОЗДІЛУ 1

У цьому розділі було розглянуто правові засади для впровадження електронного цифрового підпису в Україні. На даний момент чинним законом є Закон України «Про електронні довірчі послуги» від 05.10.2017 р. №2155-VIII. Цей Закон визначає правові та організаційні засади надання електронних довірчих

послуг, а також правові та організаційні засади здійснення електронної ідентифікації. Важливим аспектом цього закону є також визнання українських сертифікатів ключів та цифрових підписів закордоном.

ЕЦП вважаються одним з найбільш захищених методів підписання електронних документів. Цифрові підписи знижують ризик дублювання або зміни самого документа та гарантують, що підписи перевірені, справжні і законні. Функції безпеки, вбудовані в цифрові підписи, гарантують, що документи не були змінені без дозволу.

На сьогодні використання електронного цифрового підпису набирає популярності, активно запроваджується в органах та установах державної влади. Також ЕЦП широко використовується в таких сферах: банківські платіжні системи; для здійснення електронної звітності; для електронної реєстрації угод; митне декларування товарів і послуг. Із кожним роком сфери використання ЕЦП тільки продовжать розширюватися. Особливо застосування ЕЦП є дуже актуальним під час активного переходу на дистанційну роботу та поширення дистанційного навчання, що дає можливість швидко та безпечно підписувати електронні документи.

Також було розглянуто питання можливості застосування електронного цифрового підпису у ВНЗ. Застосування ЕЦП може значно зекономити час при підписанні будь-яких електронних документів, до прикладу, звітів, договорів, наказів, екзаменаційних та залікових відомостей тощо. Електронні підписи не тільки допомагають вузам скоротити кількість роздрукованих документів, які необхідно підписати, а також час, що витрачається на їх обробку, крім того електронні підписи скорочують витрати.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ДО РОЗДІЛУ 1

1. Закон України «Про електронний цифровий підпис» від 22 травня 2003р. № 852-IV

2. Закон України «Про електронні довірчі послуги» від 05.10.2017 р. №2155-VIII

3. Про затвердження Порядку акредитації центру сертифікації ключів : Постанова Кабінету Міністрів України від 13 липня 2004 р. № 903

4. Електронний реєстр чинних, блокованих та скасованих сертифікатів [Електронний ресурс] – Режим доступу до ресурсу: https://czo.gov.ua/ca-registry

5. Постанова Кабінету Міністрів України «Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності» № 1452 від 28 жовтня 2004 року

6. Система електронного документообігу. Електронний цифровий підпис. [Електронний ресурс] – Режим доступу до ресурсу: http://www.znannya.org/?view=e-government-documents

7. Електронний цифровий підпис: навіщо він та як його отримати [Електронний ресурс] – Режим доступу до ресурсу: https://ckp.in.ua/articles/9544

8. Електронний документообіг та захист інформації: навч. посіб./ О.Б. Кукарін / за заг. ред. д.держ.упр., професора Н.В.Грицяк – К.: НАДУ, 2015 – 84 с.

РОЗДІЛ 2
ОСОБЛИВОСТІ ФОРМУВАННЯ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

2.1. Поняття та призначення електронного цифрового підпису

Електронний цифровий підпис є рівнозначним з власним підписом і має таке призначення:

- аутентифікація особи, яка підписала документ;
- підтвердження того що підписаний документ є цілісним та не був модифікований;
- неможливість відмовитися від документа, що був підписаний.

Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. ЕЦП може бути реалізований з використанням симетричних та асиметричних схем шифрування, а також з допомогою хеш-функцій. Електронний цифровий підпис не може бути визнаний недійсним лише по тій причині, що документ є в електронній формі. При надійному зберіганні особистого ключа, підпис не може бути підробленим. Так само і електронним документ не може бути підроблений, оскільки у випадку здійснення будь-яких змін в документі, це буде миттєво виявлено.

2.2. Поняття особистого та відкритого ключа

Приватний ключ: у приватному ключі той самий ключ (секретний ключ) використовується для шифрування та дешифрування. Цей ключ є симетричним, оскільки єдиним ключем є копіювання або надання спільного доступу іншою стороною для розшифрування тексту шифру. Це швидше, ніж криптографія з відкритим ключем.

Відкритий ключ: у відкритому ключі використовуються два ключі, один ключ використовується для шифрування, а інший – для дешифрування. Один ключ

(відкритий ключ) використовується для шифрування простого тексту для перетворення його в текст шифру, а інший ключ (приватний ключ) використовується приймачем для розшифрування тексту шифру для читання повідомлення.

Таблиця 2.1

Порівняння відкритого та секретного ключа

Секретний ключ	Відкритий ключ
Приватний ключ швидший за відкритий.	Цей ключ повільніший, ніж приватний ключ.
Для шифрування та дешифрування повідомлення використовується один і той же ключ (секретний ключ) та алгоритм.	У криптографії відкритого ключа використовуються два ключі, один ключ використовується для шифрування, а другий - для дешифрування.
У криптографії приватного ключа ключ зберігається як таємниця	У криптографії відкритого ключа один із двох ключів зберігається як таємниця.
Приватний ключ є симетричним, оскільки існує лише один ключ, який називається секретним ключем.	Відкритий ключ є асиметричним, оскільки існує два типи ключів: приватний та відкритий.
У цій криптографії відправник та одержувач повинні використовувати один і той же ключ.	У цій криптографії відправник і одержувач не повинні використовувати один і той же ключ.

Дуже важливим є надійне зберігання особистого ключа, адже є небезпека, що доступ до ключа може отримати стороння особа та підписати документ від іншого імені.

Одним з найпопулярнішим способом збереження особистого ключа є жорсткий диск персонального комп’ютера, але цей метод має свої недоліки:

- захищеність ключа напряму залежить від того наскільки захищений персональний комп’ютер;
- можливість підписувати документ є тільки на тому комп’ютері, де зберігається ключ або в іншому випадку необхідно зберігати особистий ключ на декількох комп’ютерах, які використовуються, що є не дуже зручним.

Нині поширені також такі способи зберігання особистих ключів як смарткарти, USB-брелки, флеш накопичувачі. Найбільш захищеним вважається смарткарта, оскільки доступ до неї здійснюється за допомогою PIN-кода. Якщо ви вводите неправильний пін-код більше трьох разів, сховище блокується, запобігаючи спробам отримати доступ до ключа шляхом відгадування значення пін-коду. Всі ключові операції виконуються в пам'яті сховища, тобто ключ ніколи не залишає його. Таким чином, перехоплення ключа з оперативної пам'яті виключається.

2.3. Симетрична схема

У разі симетричного шифрування один і той же ключ використовується як для шифрування, так і для дешифрування повідомлень. Оскільки весь механізм залежить від збереження загального секрету ключа – це означає, що він повинен бути переданий одержувачу безпечним способом, щоб можна було використовувати його для розшифровки повідомлення.

Алгоритми симетричного шифрування можуть використовувати як блокові, так і потокові шифри. У блокових шифри кілька бітів (порціями) шифруються як єдине ціле. Наприклад, AES використовує розмір блоку 128 біт з опціями для трьох різних довжин ключів – 128, 192 або 256 біт.

Симетричне шифрування страждає від проблем з вичерпанням ключів, і без належного обслуговування ієрархії ключів або ефективної ротації ключів може статися витік інформації, яка потенційно може бути використана зловмисником для відновлення секретного ключа. Незважаючи на те, що при симетричному

шифруванні виникають проблеми з управлінням ключами, це шифрування працює швидше і працює без великих накладних витрат на ресурси мережі. Тому його часто використовують у поєднанні з асиметричним шифруванням.

Ключові висновки по симетричному шифруванні: для шифрування і дешифрування використовується єдиний загальний ключ; він не дуже добре масштабується, тому що секретний ключ не повинен бути втрачений або переданий неавторизованим сторонам, інакше вони можуть прочитати повідомлення.

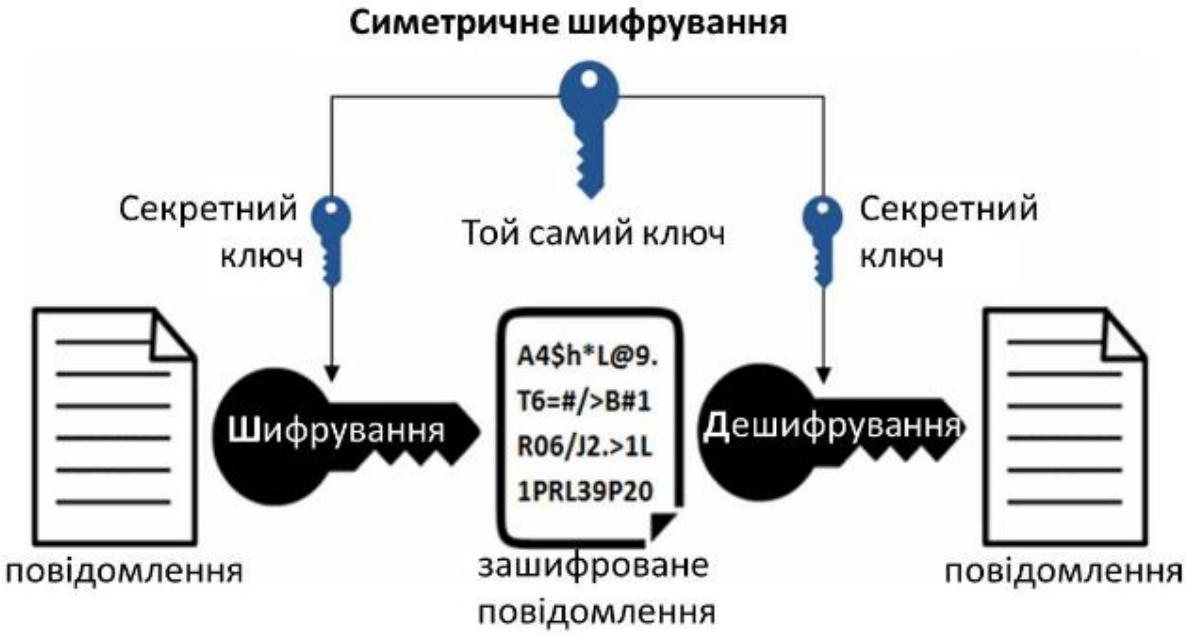

Рис. 2.1. Алгоритм шифрування з використання симетричного шифрування

Симетричні схеми ЕЦП мають такі недоліки: необхідність при передачі інформації, підписувати кожен біт інформації окремо, як наслідок це може призвести до збільшення підпису, в такому випадку підпис може бути більшим за повідомлення, яке передавалось майже удвічі; обрані для підписання документа ключі використовуються лише один раз, оскільки після завершення процесу підписання документа половина особистого ключа розривається.

2.4. Асиметрична схема

Асиметричні схеми ЕЦП відносяться до криптосистем з відкритим ключем. В асиметричних схемах цифрового підпису підписання виконується за допомогою закритого ключа, а перевірка підпису - за допомогою відкритого ключа.

Асиметрична схема цифрового підпису охоплює три процеси:

- генерація ключів. За допомогою алгоритму генерації ключів вибирається особистий ключ із набору можливих приватних ключів і визначається відкритий ключ, що відповідає приватному;
- формування підпису. Підпис визначається для певного електронного документа з використанням закритого ключа;
- перевірка підпису. З використанням відкритого ключа відбувається визначення дійсності підпису для певного документа.

Для прикладу особа відправляє свій відкритий ключ на сервер і запитує певну інформацію. Сервер шифрує інформацію, за допомогою відкритого ключа власника, і відправляє зашифровану інформацію. Клієнт отримує цю інформацію та здійснює її розшифрування. Через те що, це відбувається асиметрично, крім браузера, ніхто не може розшифрувати передану інформацію, навіть тоді коли стороння особа має відкритий ключ.

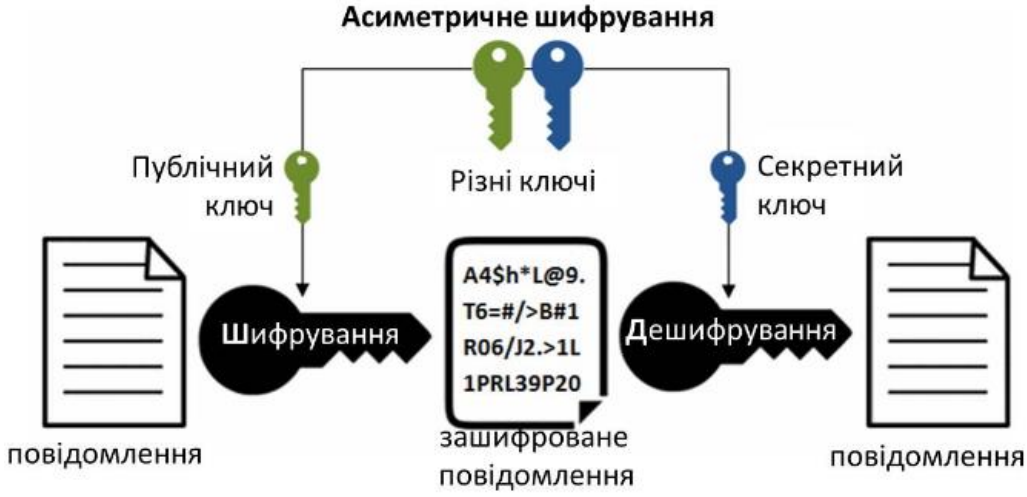

Рис. 2.2. Алгоритм шифрування з використання асиметричного шифрування

Необхідні умови для використання цифрового підпису:

- перевірка підпису здійснюється лише з використанням відкритого ключа, що відповідає приватному
- створення законного цифрового підпису є дуже складним без приватного ключа.

При асиметричному шифруванні закритий ключ передається тільки ініціатору ключа, оскільки необхідно підтримувати його безпеку.

Оскільки асиметричне шифрування – більш складний процес, ніж симетричне, потребується більше часу. Однак цей тип шифрування пропонує вищий рівень безпеки в порівнянні з симетричним шифруванням, оскільки закритий ключ не призначений для спільного використання і зберігається в секреті.

2.5. Алгоритми ЕЦП

Алгоритми ЕЦП поділяються на два великі класи:

1) загальні цифрові підписи, які потрібно пов’язати з підписаним повідомленням.

2) цифрові підписи з відновленням повідомлень, вже містить документ, що підписується: в процесі перевірки підпис обчислюється автоматично і тіло документа.

2.5.1. Алгоритм RSA

Алгоритм RSA - це алгоритм асиметричної криптографії. Асиметричний фактично означає, що він працює з двома різними ключами, тобто з відкритим ключем і закритим ключем. Як випливає з назви, відкритий ключ надається всім, а закритий ключ залишається закритим.

Алгоритм RSA має такі особливості:

- алгоритм RSA – це популярне зведення в ступінь в кінцевому полі цілих чисел, включаючи прості числа;

- цілі числа, які використовуються в цьому методі, досить великі, що ускладнює вирішення;
- у цьому алгоритмі є два набори ключів: закритий ключ і відкритий ключ.

Ідея RSA заснована на тому, що велике ціле число складно розкласти на множники. Відкритий ключ складається з двох чисел, де одне число є множенням двох великих простих чисел. І закритий ключ також є похідним від тих же двох простих чисел. Тому, якщо хтось може факторизувати велике число, закритий ключ буде скомпрометований. Отже, надійність шифрування повністю залежить від розміру ключа, і якщо ми подвоїмо або потроїмо розмір ключа, надійність шифрування зросте в геометричній прогресії. Ключі RSA зазвичай можуть мати довжину 1024 або 2048 біт, але експерти вважають, що 1024-бітові ключі можуть бути зламані в найближчому майбутньому. Але до сих пір це здається нездійсненним завданням [12].

2.5.2. Алгоритм EGSA

Основна ідея цього алгоритму – неможливість підробки електронного цифрового підпису. Для досягнення такої мети потрібно вирішити більш складну обчислювальну задачу, а не просто розбити велике ціле число. Крім того, розробник Ель Гамаль зміг усунути недоліки алгоритму RSA та запобігти ризикам підробки ЕЦП без визначення секретного ключа.

Для генерації закритого та відкритого ключів потрібно довільно вибрати два простих цілих числа P та G, за умови, що P<G. Відправник та отримувач електронного документа, що був підписаний ЕЦП, застосовують однаково великі та не засекречені числа. Відправник обирає будь-яке число X та визначає:

$$Y = G^X \ mod\ P \tag{2.1}$$

Параметр Y і є відкритим ключем та застосовується для перевірки підпису. Параметр X є секретним ключем та застосовується для підписання документів, це число повинно залишатися в таємниці. Щоб повідомлення M було підписано,

відправнику потрібно здійснити хешування хеш-функцією h в ціле число m та згенерувати рандомне ціле число К. Наступним кроком необхідно визначити параметр:

$$\text{a} = G^{\text{К}} \ mod\ P \tag{2.2}$$

Потім на основі алгоритма Евкліда визначається ціле число b, з допомогою секретного ключа X:

$$m = X \cdot a + K \cdot b\ (mod(P-1)) \tag{2.3}$$

Числа a і b створюють цифровий підпис S = (a, b)

Слід мати на увазі, що при створенні кожного електронного цифрового підпису потрібне нове значення номера К, яке визначається випадковим чином.

Алгоритм EGSA є класичним прикладом того, як повідомлення доставляється у відкритій формі. Відмінності між алгоритмами EGSA та RSA:

- аналогічним ступенем захисту алгоритм EGSA працює на цілих числах, які на 25% коротші за алгоритми RSA. Це зменшує час обчислення в середньому в 2 рази;
- обчислити модуль P легко, потрібно лише переконатися, що число є простим, а число (P - 1) має великий простий коефіцієнт;
- алгоритм EGSA не дозволяє електронних цифрових підписів нових повідомлень без знання секретного ключа;
- підпис EGSA в 1,5 рази більший за підпис RSA.

2.5.3. Алгоритм DSA

Алгоритм DSA є стандартним для цифрового підпису, який заснований на алгебраїчних властивостях завдання дискретного логарифмування і модульного зведення в ступінь і заснований на принципі криптосистем з відкритим ключем.

Алгоритм цифрового підпису не використовує закритий ключ для шифрування даних. Крім того, алгоритм цифрового підпису дійсно використовує відкритий ключ для розшифрування цих даних. Щоб створити цифровий підпис з двома 160-бітними числами, DSA працює за принципом унікальної математичної

функції. Ці два числа складаються з використанням закритого ключа і дайджесту повідомлення.

Оскільки відкритий ключ не використовується для аутентифікації підписи, процес перевірки є складним. Обидва ключі використовуються для захисту даних в спеціальному алгоритмі цифрового підпису для подальшого забезпечення безпеки.

Тепер для створення дайджесту повідомлення використовується хеш-функція. Згенерований дайджест повідомлення разом з алгоритмом DSA дає цифровий підпис. Цей підпис потім вирушає разом з повідомленням. На приймаючій стороні одна і та ж хеш-функція використовується для аутентифікації джерела і даних.

Переваги алгоритму цифрового підпису

- довжина підпису не тільки висока, але і менша в порівнянні з іншими стандартами цифрового підпису;
- швидкість обчислення підпису менше;
- DSA вимагає менше пам'яті для роботи в порівнянні з іншими цифровими стандартами;
- DSA не містить патентів, тому його можна використовувати безкоштовно.

Недоліки алгоритму цифрового підпису

- для аутентифікації потрібно багато часу, оскільки процес перевірки включає складні оператори залишку. На обчислення потрібно багато часу;
- дані в DSA не зашифровані. Ми можемо тільки аутентифікувати дані [13].

2.6. Поняття хеш-функцій

Хеш-функція - це математична функція, яка перетворює числове вхідне значення в інше стисле числове значення. Вхідні дані хеш-функції мають довільну довжину, але вихідні дані завжди мають фіксовану довжину. Значення, що повертаються хеш-функцією, називаються дайджестом повідомлення або просто хеш-значеннями.

Хеш-функції володіють такими основними властивостями:

Детермінізм – алгоритм хешування повинен бути детермінованим, що означає, що він завжди дає результат однакового розміру, незалежно від розміру введення, з якого ви почали. Це означає, що якщо ви виконуєте хешування одного речення, результуючий результат повинен бути того ж розміру, що і при хешуванні всієї книги.

Стійкість до попереднього зображення. Ідея полягає в тому, що сильний алгоритм хешування – це алгоритм, стійкий до попереднього зображення, що означає, що неможливо змінити значення хеш-функції для відновлення початкового вхідного повідомлення з відкритим текстом. Отже, концепція хеш є незворотною, односторонньої функцією.

Опір зіткнення – зіткнення відбувається при зіткненні двох об'єктів. Що ж, ця концепція перенесена в криптографію з хеш-значеннями. Якщо дві унікальні вибірки вхідних даних призводять до однакових вихідних даних, це називається конфліктом. Це погана новина і означає, що алгоритм, який ви використовуєте для хешування даних, не працює і, отже, небезпечний. По суті, проблема полягає в тому, що хтось може створити шкідливий файл зі штучним значенням хеш-функції, який відповідає справжньому (безпечному) файлу, і видати його за справжній, тому що підпис буде збігатися. Алгоритм хешування – це той, який стійкий до цих колізій.

Ефект лавини – це означає, що будь-яка зміна, внесена у вхід, незалежно від того, наскільки вона незначна, призведе до значної зміни виходу. По суті, невелика зміна (наприклад, додавання коми) перетворюється в сніжний ком або в щось набагато більше, звідси і термін «лавинний ефект».

Швидкість хешування – алгоритми хешування повинні працювати з розумною швидкістю. У багатьох ситуаціях алгоритми хешування повинні швидко обчислювати хеш-значення; це вважається ідеальною властивістю криптографічної хеш-функції. Однак ця властивість є трохи суб'єктивною. Річ у тім, швидше не завжди краще, тому що швидкість повинна залежати від того, як буде використовуватися алгоритм хешування. Іноді вам потрібен більш швидкий алгоритм хешування, а в інших випадках краще використовувати більш повільний,

для виконання якого потрібно більше часу. Перший краще підходить для підключення до веб-сайтів, а другий – для хешування паролів.

Загалом хеш-функції здатні забезпечити цілісність даних, захистити від несанкціонованих модифікацій, забезпечити захист для збережених паролів та дозволяє працювати з різними швидкостями та для різних цілей.

При виконанні хешування повідомлення, ви берете рядок даних будь-якого розміру в якості введення, проганяєте її через математичний алгоритм, який призводить до генерації виведення фіксованої довжини.

У деяких методах хешування вхідні дані розбиваються на більш дрібні блоки рівного розміру. Якщо в будь-якому з блоків недостатньо даних для того, щоб він був однакового розміру, то для його заповнення можна використовувати відступи (одиниці і нулі). Потім ці окремі блоки даних обробляються алгоритмом хешування і в результаті видається хеш-значення. Процес виглядає приблизно так:

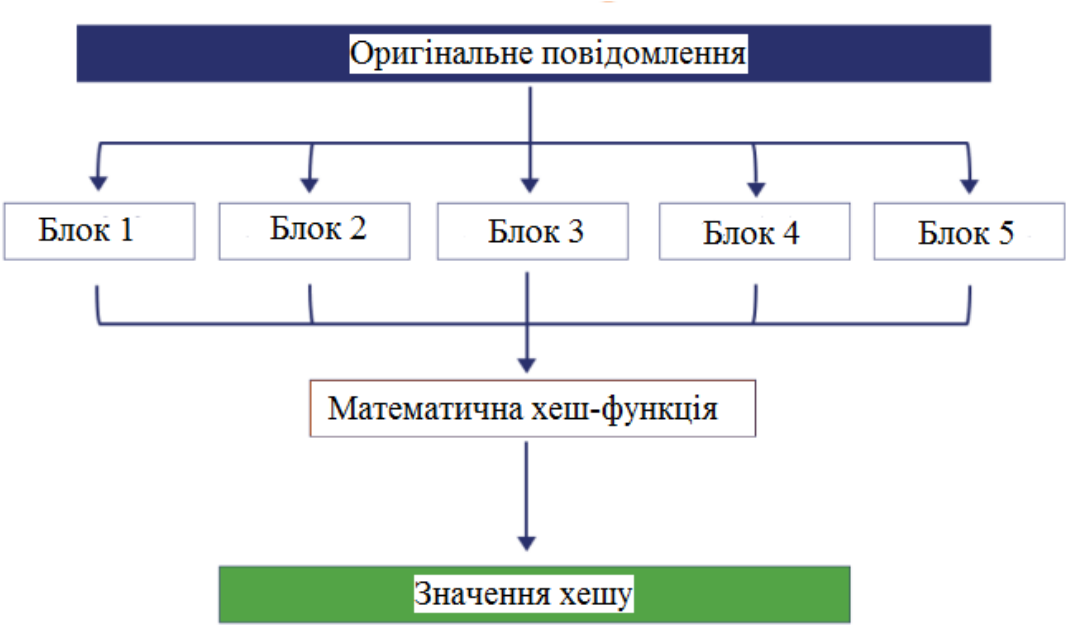

Рис. 2.3. Порядок виконання хешування

Кожен блок здійснює хешування індивідуально, всі блоки взаємопов'язані. Хеш-значення першого блоку даних вважається вхідним значенням і додається до другого блоку даних. Таким же чином хешуються вихідні дані другого блоку об'єднуються з третім блоком, а об'єднане вхідне значення знову хешується. І так

далі і так далі, цикл триває до тих пір, поки ви не отримаєте фінальний результат, який являє собою сукупне значення всіх задіяних блоків.

Це означає, що якщо дані будь-якого блоку підроблені, його хеш-значення зміниться. І оскільки його хеш-значення подається в якості вхідних даних в наступні блоки, все хеш-значення змінюються. Таким чином можна виявити навіть незначну зміну вхідних даних, оскільки воно змінює все значення хеш-функції [14].

ВИСНОВКИ ДО РОЗДІЛУ 2

У цьому розділі розглянуто процес формування електронного підпису, основне призначення, основні схеми та алгоритми на базі яких формується, поняття ключів та хеш-функцій. Електронний цифровий підпис прирівнюється до власного і має таке призначення: аутентифікація особи, що підписала документ; підтвердження того що підписаний документ є цілісним та не був модифікований; неможливість відмовитися від вже підписаного документа.

Найбільш застосованими є асиметричні схеми з використанням відкритого ключа, що охоплюють три процеси: генерація пари ключів, що дає змогу обрати приватний ключ та обчислити відповідний відкритий; формування підпису, що обчислюється за допомогою закритого ключа; перевірка підпису, що здійснюється за допомогою відкритого ключа.

Широко застосовуються і хеш-функції, які здатні забезпечити цілісність даних, захистити від несанкціонованих модифікацій, забезпечити захист для збережених паролів та дозволяють працювати з різними швидкостями та для різних цілей.

Серед алгоритмів цифрового підпису можна виділити RSA алгоритм, який вважають безпечним та надійним для користувачів завдяки використанню складної математики. Алгоритм RSA складно зламати, оскільки він включає факторизацію простих чисел, які важко розкласти на множники. Більш того, алгоритм RSA використовує відкритий ключ для шифрування даних, і цей ключ відомий всім, тому поділитися відкритим ключем легко.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ДО РОЗДІЛУ 2

9. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.

10. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2002 – 816 с.

11. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб, пособие для студ. высш. учеб, завед. — М.: Академия, 2005. — 256 с.

12. RSA Algorithm in Cryptography [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/rsa-algorithm-cryptography/

13. Digital signature algorithm [Електронний ресурс] – Режим доступу до ресурсу: https://www.educba.com/digital-signature-algorithm/

14. Cryptography hash functions [Електронний ресурс] – Режим доступу до ресурсу: https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

РОЗДІЛ 3

АНАЛІЗ СИСТЕМИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ GOOGLE WORKSPACE

3.1. Поняття платформи Google Workspace

Google Workspace – це набір інструментів, створений для підвищення продуктивності та співпраці програмного забезпечення та продуктів, розроблений корпорацією Google. Google Workspace включає в себе для спільної роботи (Docs, Sheets, Slides, Forms та Sites), для спілкування (Gmail, Meet, Chat та Calendar), для сховища (Drive) та забезпечує адміністративну панель для управління користувачами та службами.(рис. 3.1).

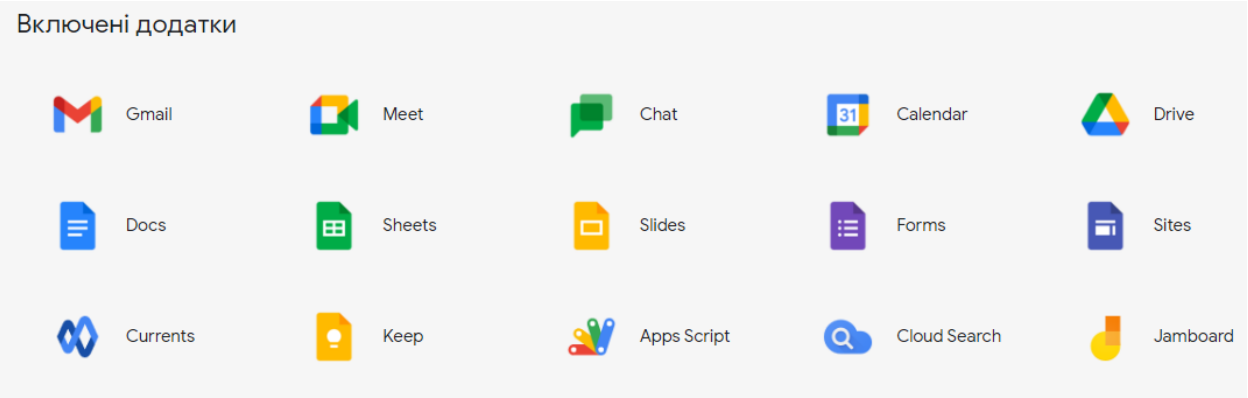

Рис. 3.1. Додатки, що входять до Google workspace

Google Workspace добре підходить для:

- Малого та середнього бізнесу, що хочуть використовувати набір інструментів програм, де їх команди можуть легко співпрацювати та обмінюватися файлами, а адміністратори можуть контролювати доступ та налаштування безпеки.
- Самозайняті або фрілансери, які шукають доступне рішення електронної пошти та інструменти підвищення продуктивності та хочуть мати можливість легко ділитися роботою з клієнтами та партнерами.

- Школи та навчальні заклади, що прагнуть налагодити співпрацю між викладачами та учнями (існує безкоштовна версія Google Workspace for Education).
- Некомерційні організації, які хочуть скористатися безкоштовною некомерційною версією Google Workspace.
- Всі, хто віддає перевагу працювати в хмарі, а не використовувати настільні рішення та локальне сховище.

3.2. Основні продукти системи Google Workspace

Gmail - це веб-служба електронної пошти, запущена у вигляді обмеженої бета-версії 1 квітня 2004 року. Проте вже у лютому 2016 року в усьому світі було задіяно понад 1 мільярд активних користувачів-споживачів, і вона стала популярною завдяки наданню користувачам великого обсягу дискового простору.

Платні функції Gmail включають в себе: можливість налаштувати електронну пошту з своїм доменним ім’ям (@ yourcompany.com), необмежену кількість групових адрес електронної пошти, гарантований час безвідмовної роботи 99,9%, удвічі більше особистого Gmail, відсутність реклами, цілодобову підтримку, синхронізацію Google Workspace для Microsoft Outlook і багато іншого.

Google Документи, Таблиці та Презентації: використовуються ці додатки для створення динамічних документів, щоб створювати і редагувати текстові документи, електронні таблиці або презентації прямо у веб-браузері. Ці програми допомагають оптимізувати командне співробітництво за рахунок простого обміну документами, редагування в реальному часі, коментарів, створення декількох авторів, перевірки версій, вбудованого чату і автоматичного збереження.

Google Диск: можливість зберігати всі свої документи і файли в цьому централізованому хмарному сховищі. Всім об'єктам можна легко поділитися власними посиланнями і налаштуваннями дозволів, і їх можна знайти в лічені секунди завдяки розширеній функції пошуку Google Workspace. Google Workspace також є джерелом ще однієї найбільшої переваги Google Workspace – необмеженого обсягу даних.

Cloud Search: розширює свої можливості пошуку за допомогою цього інструменту пошуку для всього підприємства. Можна відстежувати будь-які файли, що зберігаються, в додатках Gmail, G Drive і Calendar.

Календар Google: можна з легкістю планувати внутрішні і зовнішні зустрічі за допомогою вбудованого додатка-календаря Google. Календар Google, який легко підключається безпосередньо до Gmail, дає вам доступ до цілого ряду корисних функцій Google Workspace, таких як створення декількох календарів, нагадування по електронній пошті для зборів (поряд з інформацією про дорожню обстановку в реальному часі) і інтеграція календаря з конференц-залами, щоб запобігти обмін інформацією про доступність.

Google Hangouts / Meet: підтримуйте зв'язок з колегами та клієнтами, використовуючи ці альтернативи Google та Zoom. Обидві програми для відеоконференцзв'язку повністю інтегровані з програмами Google Workspace і можуть бути доступні будь-кому, хто має посилання, що дозволяє проводити високоякісні віртуальні зустрічі, будь то зустрічі один на один або групові. Google Meet може прийняти до 250 учасників по телефону і підтримує 100 000 глядачів для прямої трансляції заходу.

Chat: користувачі можуть обмінюватися повідомленнями в інших додатках Google, а також мати свої власні чати.

Sites: користувачі можуть створювати свої власні веб-сайти за допомогою платформи Google.

Apps scripts: ця функція пропонує дизайн програми, який розробники можуть додавати в деякі з існуючих додатків пакета.

Cloud Search: користувачі можуть шукати дані в хмарному сховищі Google.

Keep: користувачі можуть створювати списки справ, замітки і нагадування, щоб тримати себе і своїх товаришів по команді в курсі.

Currents: ця комунікаційна платформа допомагає командам залишатися на зв'язку за допомогою повідомлень, зображень, відео та розмов.

Forms: користувачі можуть створювати опитування та анкети для отримання інформації та прийняття рішень на основі даних.

3.3. Безпека системи Google Workspace

Ще одна з основних причин використання Google Workspace полягає в тому, що платформа докладає всіх зусиль для забезпечення безпеки вашої інформації. Google застосовує суворі провідні в галузі протоколи безпеки як для фізичних центрів обробки даних, так і для операцій, розміщених в хмарі.

Деякі з цих заходів включають:

- двоетапна перевірка: якщо хтось входить в систему з нерозпізнанаого пристрою, користувачеві облікового запису негайно відправляється текстове повідомлення з кодом підтвердження, щоб забезпечити додатковий рівень безпеки. Введення двоетапної аутентифікації підвищує рівень безпеки вашого облікового запису Google. Також Google, розробив ключ безпеки – реальний фізичний ключ, який використовується для доступу до вашого профілю облікового запису Google. Він відправляє зашифрований підпис, а не код, і гарантує, що ваш логін не буде піддано фішингу. А використання цього ключа економить час – коли необхідно підтвердити свій обліковий запис Google в браузері Chrome, індикатор ключа буде блимати. Просто торкніться його, і підпис відправиться автоматично. Цей електронний ключ може зберігатися в USB-слоті або мати велику знімну модель на вашій зв'язці ключів або в вашому гаманці. Таким чином ключ завжди буде знаходитись поряд, і ним можна скористатися в будь-який зручний момент [16].

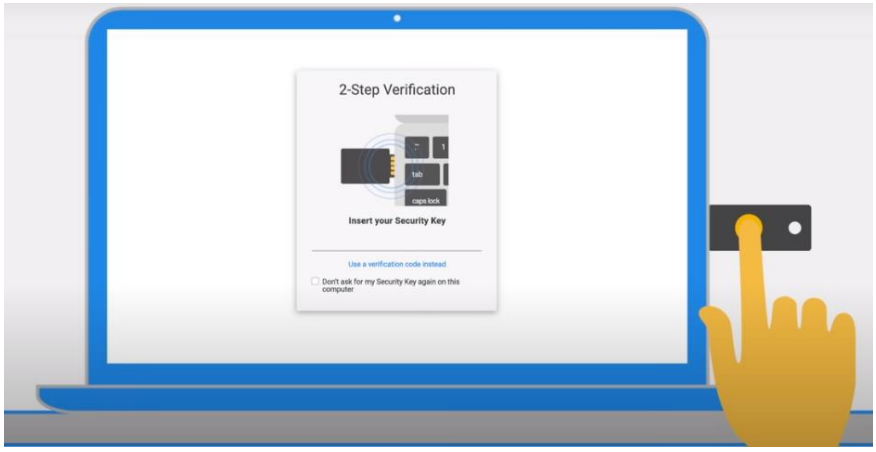

Рис.3.2. Процес проходження аутентифікації з допомогою ключа

- сучасна безпека: лазерне виявлення і біометрія – заходи безпеки, які використовуються для захисту фізичних центрів обробки даних Google.
- досконала пряма секретність: весь контент, який переміщається між серверами Google і серверами інших компаній, зашифрований. Наприклад, кожен електронний лист, який ви відправляєте або отримуєте, на 100% зашифровано, тому його можна безпечно відкрити. Адміністратори також можуть встановлювати індивідуальні правила шифрування для певного контенту.
- виявлення II моніторингу входу в систему: у випадку будь-якої підозрілої активності, Google негайно повідомить адміністраторів, якщо виявить новий вхід в систему або незвичну поведінку.

Google Workspace захищає дані найбезпечнішим способом. Він проходить аудит і відповідає найвищим стандартам безпеки в галузі. Його функції безпеки дозволяють створювати гнучкі і масштабовані робочі простори незалежно від використовуваного браузера або пристрою.

У той же час функції безпеки Google Workspace допомагають досягти поставлених цілей, захищаючи важливі дані. Крім того, надійні функції безпеки Google Workspace полегшують безпечне спілкування і надають адміністраторам підвищений контроль і прозорість для своїх організацій. Інформація зі звітів про захист даних також може допомогти адміністраторам виявляти конфіденційні матеріали, дозволяючи їм приймати більш обґрунтовані рішення про те, як найкраще захистити дані організації.

Підвищена обізнаність адміністраторів про безпеку даних дозволяє їм приймати обгрунтовані рішення щодо захисту. Таким чином, компанії, що використовують Google Workspace, можуть бути впевнені, що їх інформація в безпеці – це вимога стає все більш важливою, оскільки витік даних і інші загрози кібербезпеки стають все більш поширеними [17].

3.4. Використання Google Workspace для навчання

Google Workspace for Education Fundamentals – це колекція інструментів та послуг Google, розроблених спеціально для навчальних закладів та організацій домашнього навчання. Розроблений для ефективної співпраці, простоти викладання та безпеки всіх залучених. Існують різні варіанти Google Workspace for Education Fundamentals:

Google Workspace for Education Fundamentals – засоби навчання та викладання, такі як Classroom, Google Meet, Google Docs, Google Forms та Google Chat.

Google Classroom – це інструмент для спільної роботи викладачів і студентів, який допомагає організувати і спростити роботу в класі. Всього декількома клацаннями миші ви можете створити клас, додати своїх учнів і створити завдання або оголошення. Ви зможете бачити, хто виконав завдання, хто ще працює над ним, і виставляти оцінки, коли воно буде виконано. Ви також можете миттєво пропонувати студентам зворотний зв'язок і бачити їхні запитання або коментарі до їх завдань.

Google Workspace for Education Standard (з квітня 2021) – ті самі інструменти, що й Google Workspace for Education Fundamentals, але з додатковими функціями безпеки та адміністрування.

Teaching and Learning Upgrade (з квітня 2021 р.) додає вдосконалення відео, доповнення до Класу та інші функції та інструменти до Google Workspace for Education Fundamentals або Google Workspace for Education Standard.

Google Workspace for Education Plus – усі освітні стандарти та функції оновлення викладання та навчання, а також додаткові функції для деяких служб, таких як відстеження учасників у Google Meet.

Google Workspace for Education Fundamentals безкоштовно надаються навчальним закладам, які відповідають певній кваліфікації. Google Workspace for Education Standard, Teaching and Learning Upgrade та Google Workspace for Education Plus пропонуються з платною підпискою [18].

Нова модель зберігання надасть університетам базовий рівень 100 ТБ уніфікованого хмарного сховища, яким користуються всі ваші користувачі – цього більш ніж достатньо для зберігання понад 100 мільйонів документів, 8 мільйонів презентацій або 400 000 годин відео. Ця політика набуде чинності у всіх виданнях Google Workspace for Education для існуючих клієнтів у липні 2022 року і поширюватиметься на нових клієнтів, які зареєструються в 2022 році [19].

3.5. Переваги та недоліки використання системи Google Workspace

Після дослідження платформи Google Workspace можна виділити певні переваги та недоліки її використання.

До переваг можна віднести:

Зручність. Наявність всіх офісних інструментів в одному місці – це величезна цінність. З Google Workspace перемикання між електронною поштою, документами, календарями і чатом стає безпроблемним, що дозволяє заощадити неймовірну кількість часу і зусиль.

Простота використання. Продукти Google Workspace прості і легко адаптуються. Наприклад, документи і таблиці пропонують урізані, але функціональні можливості знайомих інструментів, таких як Microsoft Word і Excel. Інші інструменти, включаючи консоль адміністратора, також прості в навігації і інтуїтивно зрозумілі у використанні.

Спільна робота і спільне використання. Одна із сильних сторін Google Workspace – це те, наскільки легко спрощує співпрацю між членами команди. Кілька членів команди можуть працювати над одним і тим же документом одночасно, а файли можна швидко спільно використовувати між різними користувачами.

Все працює в хмарі: Google дійсно був засновником концепції роботи в хмарі (і в кінцевому підсумку змусив конкурентів, таких як Microsoft, зробити те ж саме). Всі додатки Google Workspace запускаються з веб-браузерів, що означає відсутність програмного забезпечення для завантаження, а зміни в документах автоматично зберігаються і вносяться в режимі реального часу.

Набір додатків. Як ми бачимо, набір інструментів для підвищення продуктивності і спільної роботи в Google Workspace вражає і покриває переважну більшість потреб.

Необмежене хмарне сховище: користувачі отримують необмежене сховище. Крім того, файли, створені в Google документах, таблицях, презентаціях і т. д., не витрачаються за межами вашого сховища.

Доступна безкоштовна версія: багато інструментів (Gmail, Документи, Диск і т. д.) доступні для безкоштовного використання (для особистих облікових записів) з деякими обмеженнями на сховище і адресою електронної пошти @ gmail.com. Однак при реєстрації в Google Workspace ви отримуєте безкоштовну 14-денну пробну версію, щоб налаштувати професійний адрес електронної пошти та випробувати додаткові функції, такі як консоль адміністратора.

Інтеграції: Google Workspace має величезну, постійно зростаючу кількість інтеграцій з усіма видами інструментів, які ви можете використовувати (веб-розробка, творчість, бухгалтерський облік та фінанси, академічні науки і т. д). Це дозволяє Google Workspace легко інтегруватися в будь-які існуючі процеси.

Недоліки:

Дана платформа не така просунута, як Microsoft Office: порівнюючи Документи, Таблиці та Презентації з настільними версіями Word, Excel і Powerpoint, ви виявите, що вони не так просунуті. Їм не вистачає гнучкості форматування і функціональності, які є в інструментах Microsoft, що може бути обмежуючим для деяких.

Необхідний доступ в Інтернет: Google Workspace повністю заснований на хмарі, а це означає, що вам потрібне підключення до Інтернету, щоб мати можливість використовувати його у великій кількості. При цьому доступні деякі автономні функції (наприклад, можливість редагувати документи в автономному режимі і синхронізувати зміни, коли ви знову в мережі).

Сумісність з Microsoft. Хоча Документи, Таблиці та Презентації здебільшого підтримують формати Microsoft, іноді можуть виникати проблеми з відображенням /

перетворенням певних елементів, що не ідеально, якщо ви продовжуєте багато працювати з інструментами Microsoft Office.

Безпека: розміщення даних в хмарі завжди представляє більш високий ризик безпеки в порівнянні з локальним розміщенням даних, хоча Google Workspace дозволяє реалізувати такі заходи, як двоетапна перевірка, щоб мінімізувати ризик.
Проблеми з декількома обліковими записами: якщо у вас є кілька облікових записів в Google (наприклад, професійний і особистий обліковий запис), вам може бути трохи незручно переключатися між обліковими записами і входити в систему майже кожен раз. Було б непогано, якби Google Workspace завжди розпізнавав останній використаний вами логін при переході між додатками.

ВИСНОВКИ ДО РОЗДІЛУ 3

В цьому розділі було розглянуто систему електронного документообігу Google Workspace, що являє собою набір інструментів, створених для підвищення продуктивності та співпраці програмного забезпечення та продуктів, розроблений корпорацією Google. Google Workspace включає в себе для спільної роботи (Docs, Sheets, Slides, Forms та Sites), для спілкування (Gmail, Meet, Chat та Calendar), для сховища (Drive) та забезпечує адміністративну панель для управління користувачами та службами.

Одна з основних причин використання Google Workspace полягає в тому, що платформа докладає всіх зусиль для забезпечення безпеки вашої інформації. Google застосовує суворі провідні в галузі протоколи безпеки як для фізичних центрів обробки даних, так і для операцій, розміщених в хмарі. Google Workspace захищає дані найбезпечнішим способом. Проходить аудит і відповідає найвищим стандартам безпеки в галузі. Функції безпеки дозволяють створювати гнучкі і масштабовані робочі простори незалежно від використовуваного браузера або пристрою.

При роботі з Google Workspace можна виділити певні переваги використання: зручність, а саме наявність всіх офісних інструментів в одному місці. З Google Workspace перемикання між електронною поштою, документами, календарями і

чатом стає безпроблемним, що дозволяє заощадити неймовірну кількість часу і зусиль. Простота використання: продукти Google Workspace прості і легко адаптуються. Наприклад, документи і таблиці мають подібні функціональні можливості знайомих інструментів, таких як Microsoft Word і Excel. Користувачі отримують необмежене сховище. Багато інструментів (Gmail, Документи, Диск і т. Д.) доступні для безкоштовного використання. Google Workspace має величезну, постійно зростаючу кількість інтеграцій з усіма видами інструментів. Проте є й певні недоліки: Google Workspace повністю заснований на хмарі, а це означає, що потрібне підключення до Інтернету, щоб мати можливість користуватися даною системою. Таким чином, дана платформа є дуже простою та зручною у використанні, і може бути використана для роботи чи навчання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ДО РОЗДІЛУ 3

15. Products Google Workspace [Електронний ресурс] – Режим доступу до ресурсу: https://workspace.google.com/intl/en_uk/features/

16. The key for working smarter, faster and more securely [Електронний ресурс] – Режим доступу до ресурсу: https://workspace.google.com/learn-more/key_for_working_smarter_faster_and_more_securely.html

17. A short guide to Google Workspace security [Електронний ресурс] – Режим доступу до ресурсу: https://www.sherweb.com/blog/g-suite/google-workspace-security/

18. Google Workspace for education overview [Електронний ресурс] – Режим доступу до ресурсу: https://support.google.com/a/answer/7370133/google-workspace-for-education-overview?hl=en

19. More options for learning with Google Workspace for education [Електронний ресурс] – Режим доступу до ресурсу: https://blog.google/outreach-initiatives/education/google-workspace-for-education/

РОЗДІЛ 4
ЗАХИЩЕНА СИСТЕМА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ НА БАЗІ ПЛАТФОРМИ GOOGLE WORKSPACE

4.1. Створення власного електронного цифрового підпису

Створення власного підпису буде відбуватися онлайн за допомогою сервісу Приват24. Для цього необхідно авторизуватися в додатку, в послугах обрати бізнес та натиснути завантажити сертифікат.

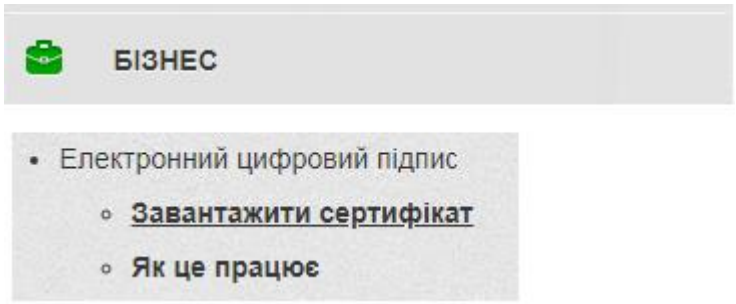

Рис. 4.1. Вікно входу для завантаження сертифікату в Приват24

Далі необхідно перевірити правильність введених особистих даних

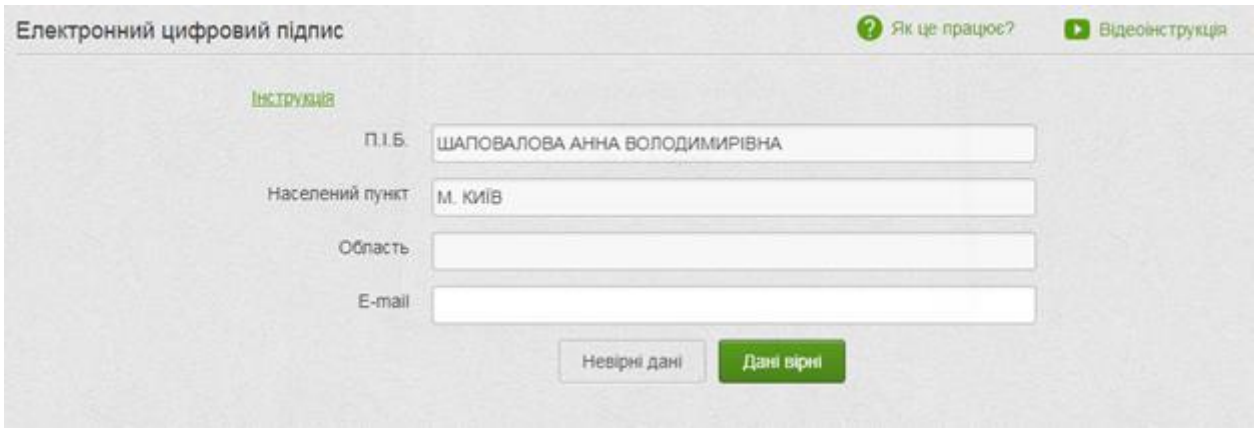

Рис. 4.2. Вікно заповнення особистих даних при створенні ЕЦП

Наступним кроком необхідно придумати пароль, який повинен бути мінімум 8 символів, містити в собі символи латинського алфавіту та цифри. Пароль повинен бути дуже надійним.

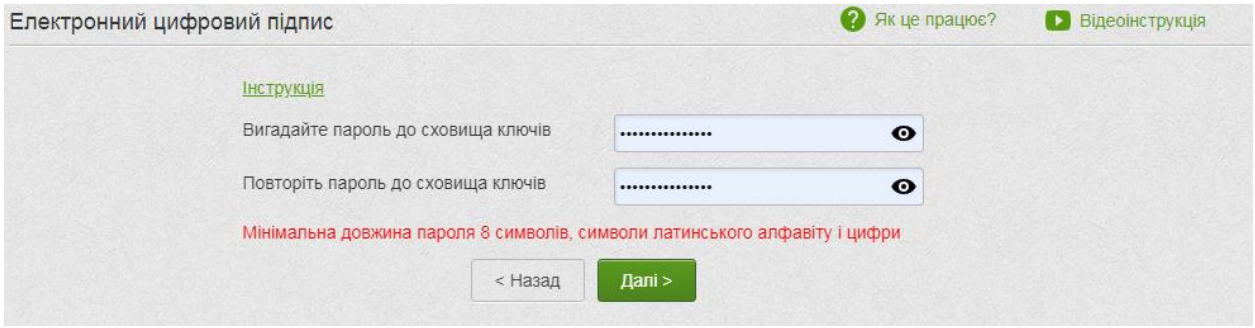

Рис. 4.3. Вікно створення пароля

Після цього потрібно ввести код з SMS, що був надісланий на вказаний номер телефону та ознайомитися з умовами та правилами надання банківських послуг і після цього натиснути галочку про згоду.

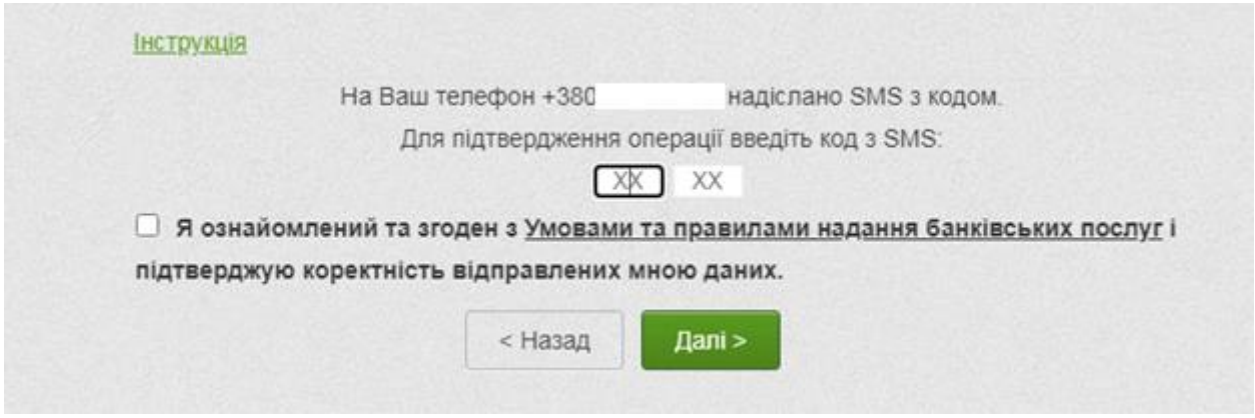

Рис. 4.4. Вікно для введення коду для підтвердження операції

Потім з’явиться інформація про успішність створення сертифікату разом з серійним номером та терміном дії сертифікат.

Рис. 4.5. Вікно про успішне отримання сертифікату ключа

Файл з ключем ЕЦП завантажується на комп’ютер та має такий вигляд:

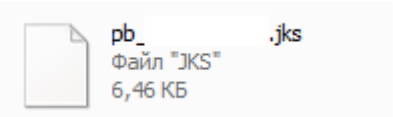

Рис. 4.6. Вигляд файлу з ключем ЕЦП

4.2. Робота з Google Docs та їх застосування.

Google Docs - це текстовий редактор Google на базі браузера, дозволяє створювати, редагувати і обмінюватися документами в Інтернеті, а також отримувати до них доступ з будь-якого комп'ютера, підключеного до Інтернету. Google неймовірно спростив обмін документами на різних платформах і спільну роботу над ними в режимі реального часу з вікна браузера. Ви можете використовувати Google Docs так само, як і документи Word: створювати нові документи, використовувати шаблони Google Docs, ділитися документами із іншими та співпрацювати в режимі реального часу. Не потрібно пам'ятати про збереження документа Google, тому що Google автоматично зберігає ваші документи на вашому Google Диску, і ви не побачите кнопки «Зберегти». Також є можливість переглядати та редагувати документи в автономному режимі, без підключення до Інтернету, увімкнувши в налаштуваннях офлайн доступ. Будь-які внесені вами зміни будуть синхронізовані після повторного підключення до Інтернету [20].

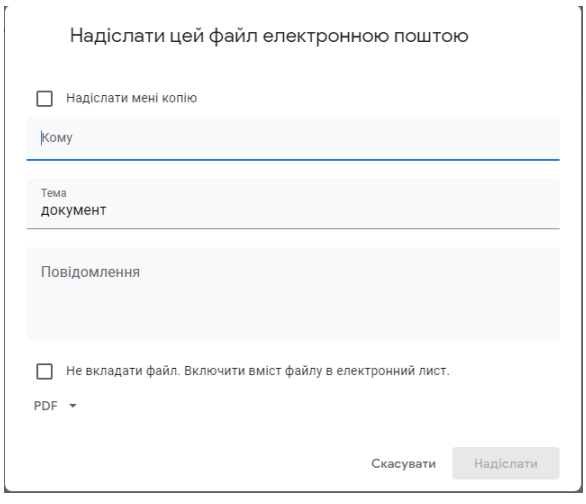

Рис. 4.7. Надсилання документа на електронну пошту

Є можливість відправити файл на електронну адресу. Однак замість того, щоб відправляти документ по електронній пошті, краще поділитися ним. Тому, що спільне використання дозволяє всім бачити і працювати з однією і тією ж версією документа. Таким чином можна уникнути створення копій або дублювання вашої роботи. Одержувачу не потрібен обліковий запис Google для перегляду або редагування документа. Є можливість відкрити спільний доступ для інших користувачів, вказавши їхню електронну адресу, або натиснути кнопку копіювати посилання, тоді посилання збережеться в буфері обміну, і ним можна буде поділитися з іншими користувачами, надавши їм таким чином доступ до документа (рис 4.8).

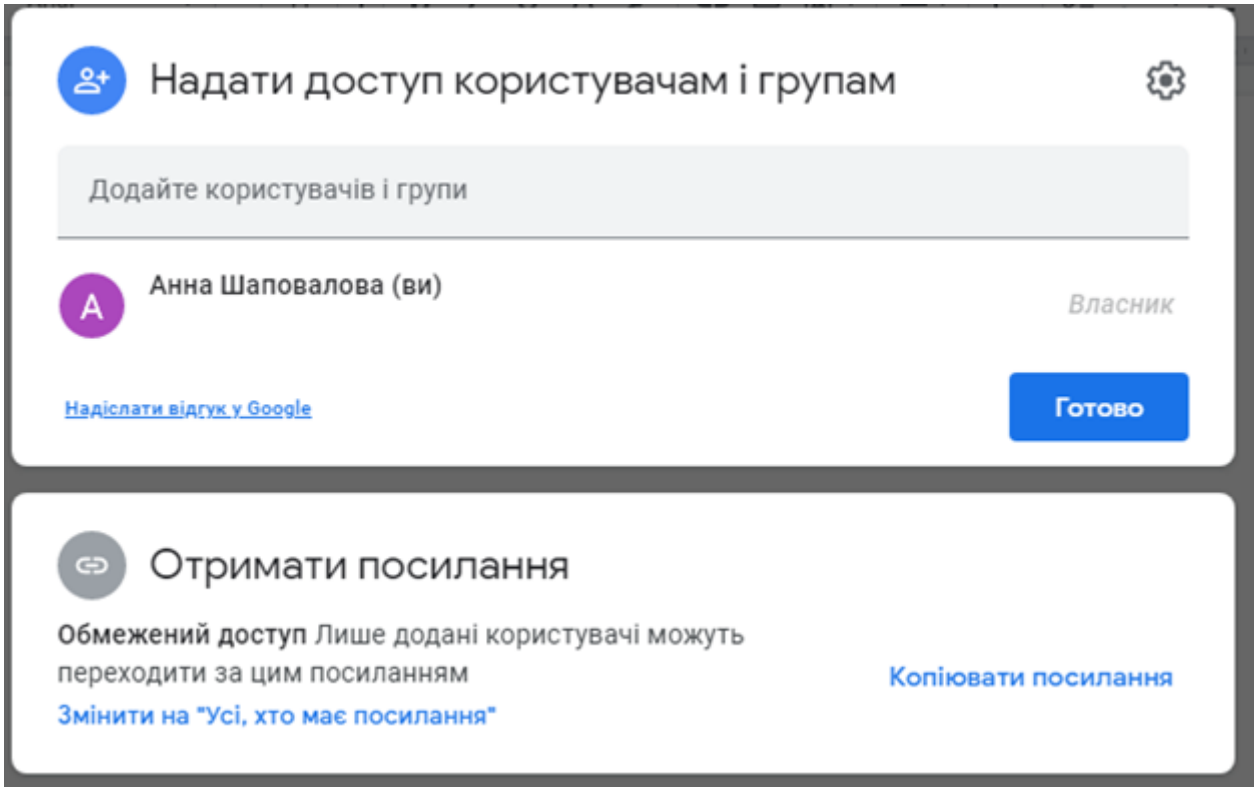

Рис. 4.8. Надання спільного доступу для інших користувачів

Переваги на недоліки використання Google Docs:

Безоплатний доступ до сервісу: для користування Google Docs, не має необхідності купувати ліцензію. Всі інструменти сервісу є у вільному доступі. Необхідно просто створити свій аккаунт в Google та увійти до документів на будь-якому пристрої.

Автоматичне збереження. Великою перевагою в Google Документах є також й те що не має необхідності постійно зберігати будь-які зміни в роботі з документами, адже це робиться автоматично. Також є можливість переглядати та редагувати документи, без підключення до Інтернету, при цьому зміни зроблені за це час будуть збережені одразу після підключення до мережі.

Простий обмін інформацією та простота підключення. Документи Google працюють у веб-браузері – немає необхідності встановлювати Документи на свій комп'ютер. Запуск Документів через Інтернет дає можливість працювати на будь-якому підключеному до Інтернету комп'ютері, або мобільному пристрої, але це є обмеженням: якщо ви втратите з'єднання з Інтернетом, ви втратите доступ до програми. Більше не потрібно копіювати файли та передавати документи через електронну пошту, адже тепер є можливість увімкнути доступ за посиланням.

Спільна робота з документами. Існує лише одна копія файлу, і користувачі одночасно «діляться» цією однією копією в реальному часі, і всі присутні користувачі можуть одночасно змінювати, оновлювати та вводити дані.

Голосове введення. Є можливість надиктувати текст. Google Документи можуть сприймати мову. Просто підключіть гарнітуру, виберіть в інструментах «Голосове введення», наговоріть текст і внесіть необхідні зміни.

Історія редагування. Усі модифікації документа автоматично відстежуються з часом та інформацією про редактор. Також великою перевагою є те, що ви можете бачити, хто вносив зміни в документ, коли вони вносили зміни, і ви навіть можете повернутися до попередньої версії до внесення змін.

Інтеграція. Документи підтримують подібні зв'язки з іншими програмами Google, Таблицями та Презентаціями, але для більш просунутих програм Office, таких як Publisher, Access або Visio, немає аналогів Google. Документи також не можуть зв'язуватись безпосередньо з вашими даними Outlook, щоб об'єднати пошту або прочитати інформацію у вашому календарі.

Сервіс залежить від інтернету. Ви можете редагувати файли, налаштувавши офлайн-доступ, при відсутності підключення немає можливості поділитися файлом .

Ще один недолік - прив'язка до вашого Google-аккаунту. При втраті до нього доступ немає можливості відновити дані.

4.3. Підписання електронного документа за допомогою створеного ЕЦП

Одним з головних законів, що встановлює основні засади електронного документообігу та використання електронних документів був Закон України «Про електронні документи та електронний документообіг», що втратив свою чинність на підставі Закону № 2155, що був розглянутий раніше. Згідно цього Закону для ідентифікації автора електронного документа може використовуватися електронний підпис. Накладанням електронного підпису завершується створення електронного документа [21].

Для підписання документа необхідно зайти на офіційний сайт Центрального засвідчувального центру. Вибираю кваліфікованого надавача електронних послуг, прикріпляю файл з ключем та вводжу пароль.

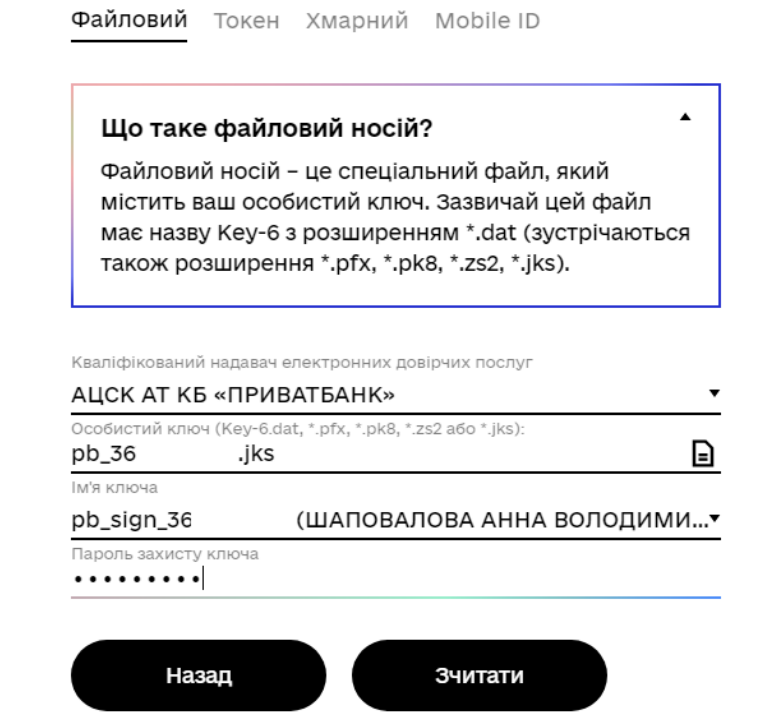

Рис. 4.9. Перший крок підписання документа

На наступному кроці після зчитання сертифіката ключа необхідно перевірити правильність даних.

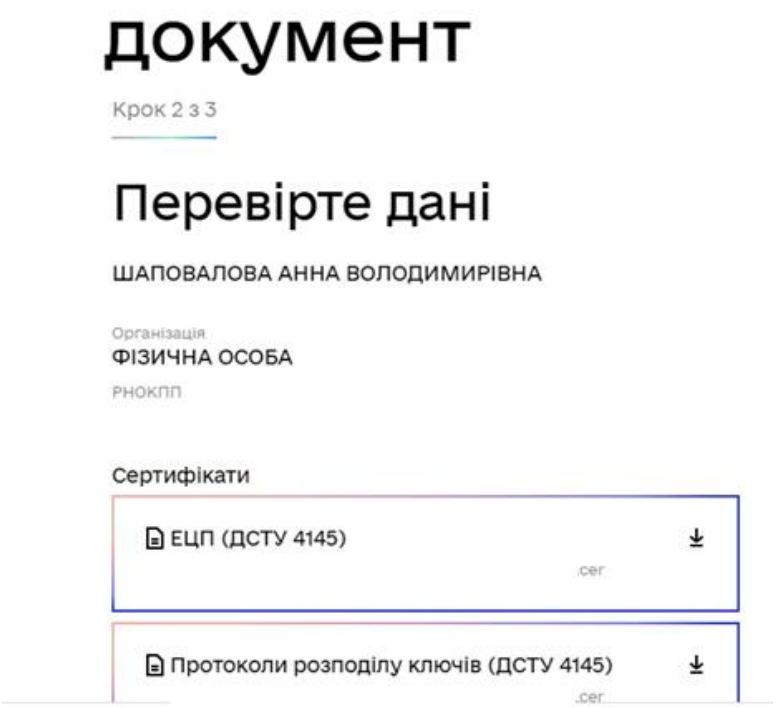

Рис. 4.10. Перевірка правильності введених даних

Рис. 4.11. Завантаження файлу для підпису та обрання формату

Далі необхідно обрати формат підпису та завантажити файл для підпису. У моєму випадку це буде файл з дипломною роботою.

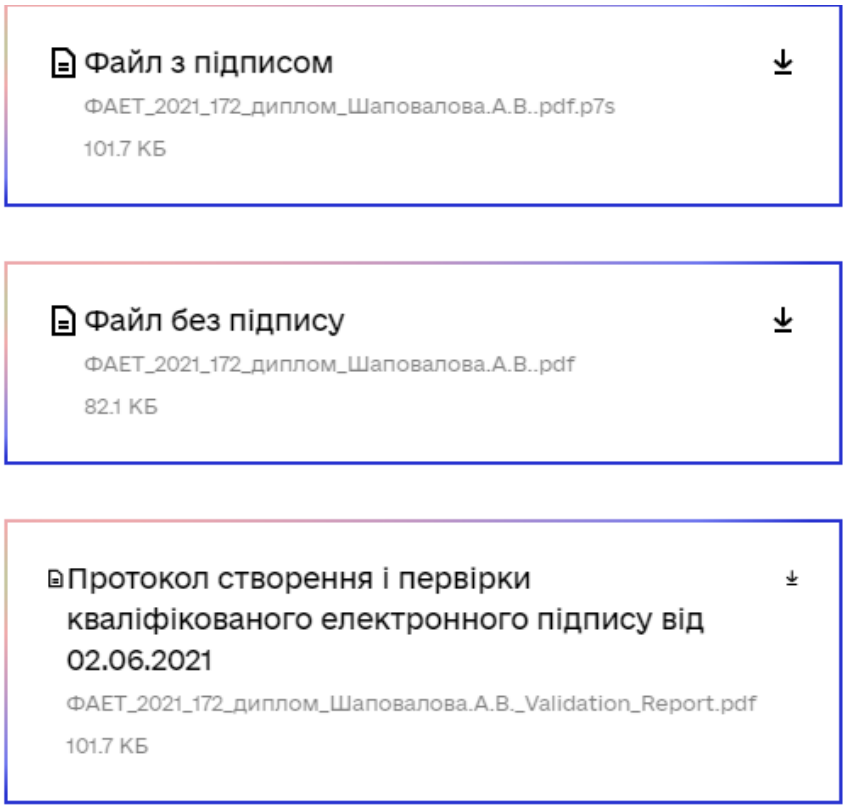

Рис. 4.12. Завершення підписання документа та завантаження його на комп’ютер

Після підписання з’являється вікно з підписаним файлом, який необхідно завантажити собі на комп’ютер.

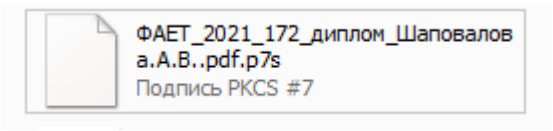

Рис. 4.13 Вигляд підписаного документа

Після підписання та завантаження документа відправлено на перевірку до керівника дипломної роботи через сервіс Google Classroom.

Також на офіційному сайті Центрального засвідчувального центру є можливість перевірити підпис та чи не було внесено змін в підписаний документ.

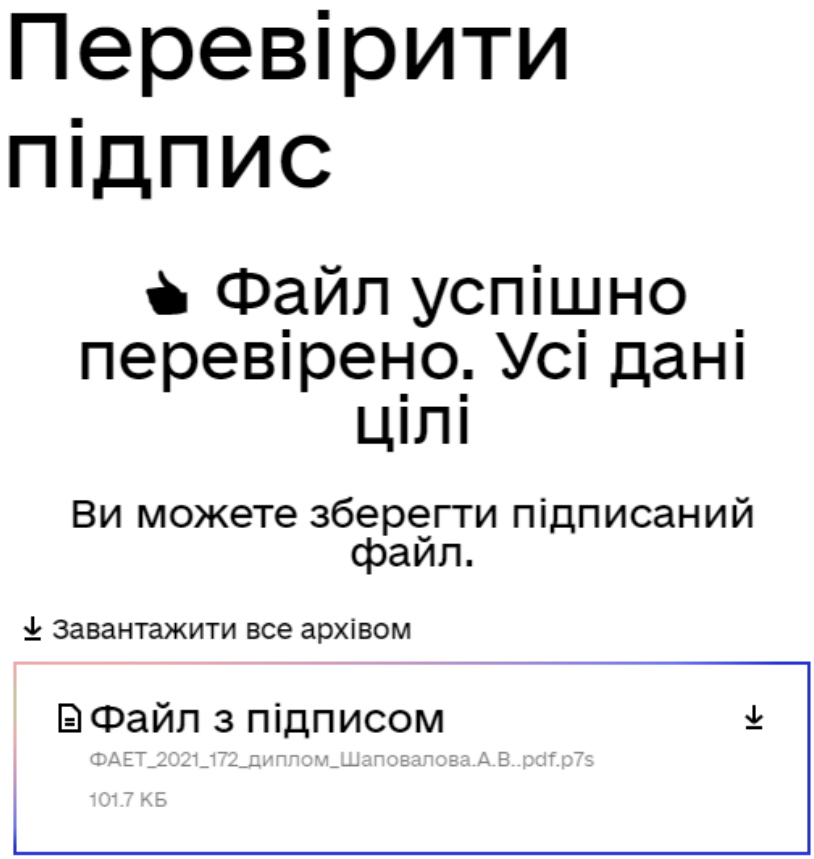

Рис. 4.14. Перевірка підпису

Таким чином, можна легко, швидко, а ще головне безпечно підписувати та перевіряти будь-які електронні документи.

Також існують можливості підписання електронного документа безпосередньо в Google Docs, але підписати документ можливо лише за допомогою електронного підпису. Можливі варіанти підписання документа: 1 спосіб – це застосування інструмента для малювання в Google Docs, за допомогою якого можна власноруч намалювати власний підпис, або завантажити вже готовий підпис. Інший варіант встановити надбудову DocuSign. З допомогою цієї надбудови можна підписувати та надсилати документи на підпис через Google Docs. Крім того, є можливість підписувати та відпавляти прямо з електронної пошти Gmail. Також можна використовувати DocuSign eSignature прямо з Документів для швидкого доступу, та завантажувати в DocuSign для збору підписів, а потім зберігати їх у папці на Диску [22].

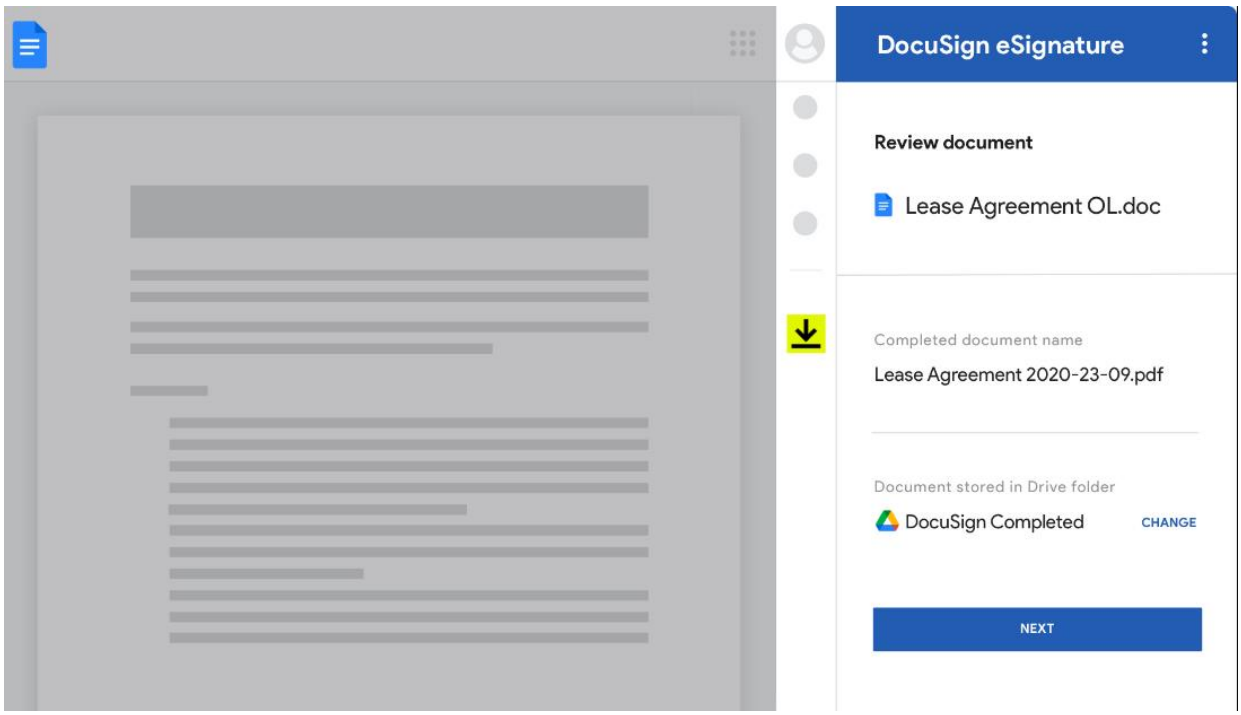

Рис. 4.15. Вигляд надбудови DocuSign для підписання документів

Було б чудово, якби існувала можливість підписувати документи в Google Docs використовуючи власний електронний цифровий підпис, але поки такої можливості не існує.

4.4. Можливості підписання електронних документів через портал Дія

Наразі існує можливість підписувати електронні документи через портал Дія на їх офіційному сайті. За допомогою цієї послуги кожен громадянин може отримати практично будь-яку цифрову і не лише послугу в державних органах, або ж підписати документ використовуючи електронний підпис. Ця процедура є швидкою, безкоштовною та не потребує реєстрації на сайті. Документ з електронним цифровим підписом залишається в браузері користувача й не передається на портал, що свідчить про збереження переданої інформації в конфіденційності. Цей сервіс гарантує більшу безпеку, ніж особисте підписання документу. Оскільки, у випадку накладання підпису можна достовірно ідентифікувати особу, яка підписала документ. Також існує можливість накладання двох підписів на електронний документ.

Отримати цифровий підпис та підписати документ також можливо через додаток Дія на своєму сматрфоні. Для створення підпису необхідно в меню обрати Дія.Підпис та натиснути створити, після пройти перевірку через PhotoID. Програма прирівняє фото обличчя з фото, що міститься в Демографічному реєстрі та у випадку успішної ідентифікації сформує підпис. Ця послуга є безкоштовною та дуже захищеною. Для того щоб підписати документ необхідно: вибрати документ, який потрібно підписати, натиснути на кнопку підписати, підтвердити особу найбільш зручним способом, ввести пароль і все, документ підписано. Також є можливість підписати документ через QR-код. Для цього потрібно відкрити сканер у себе в Дії, навести на QR-код, який компанія розміщує у себе, потім, зробивши скан цього QR-кода, на смартфоні користувача в Дії з'явиться запит на надання копії е-документа. Після підтвердження, користувач за допомогою Дія. Підпис підписує документи та зі свого мобільного пристрою відправляє дані на електронну пошту компанії [23].

З часом портал Дія має на меті інтегруватися з кабінетом водія та кабінетом на порталі пенсійного фонду, банками та страховими компаніями та мобільними операторами. Що зможе суттєво спростити процес надання та отримання державних послуг. На жаль, для цього додатки платформи Google Workspace не підходять, оскільки не мають можливості підписувати електронні документи, безпосередньо в додатках, використовуючи ЕЦП, без додаткового застосування інших додатків або доповнень.

ВИСНОВКИ ДО РОЗДІЛУ 4

В цьому розділі було розглянуто роботу з Google документами, можливості їх застосування. Google Docs редактор Google на базі браузера, дозволяє створювати, редагувати і обмінюватися документами в Інтернеті, а також отримувати до них доступ з будь-якого комп'ютера, підключеного до Інтернету. Можна виділити певні переваги: безоплатний доступ до сервісу; автоматичне збереження; простий обмін

файлами; можливість колективної роботи з документами; голосове введення; безмежний доступ до всіх змін.

Також було проведено практичну частину роботи. Створено власний електронний цифровий підпис за допомогою кваліфікованого надавача електронних довірчих послуг АЦСК АТ КБ "ПРИВАТБАНК" в онлайн сервісі Приват24.Після отримання підпису, було здійснено підписання електронного документа та відправки його керівнику. Ще було досліджено можливості підписання електронних документів в Google Docs. Можливі варіанти підписання: використання інструмента малювання або завантаження електронного підпису з комп’ютера, а також спосіб встановлення надбудови DocuSign, що дозволить підписувати документи через Google Docs, з можливістю потім зберегти цей підпис на Диску.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ДО РОЗДІЛУ 4

20. What is Google Docs and how to use it [Електронний ресурс] – Режим доступу до ресурсу: https://www.makeuseof.com/tag/google-docs-faq/

21. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003р. № 851-IV.

22. DocuSign eSignature for Google [Електронний ресурс] – Режим доступу до ресурсу: https://www.docusign.com/solutions/google

23. Державні послуги онлайн. Дія [Електронний ресурс] – Режим доступу до ресурсу: https://diia.gov.ua/

ВИСНОВКИ

Електронний цифровий підпис – це невід'ємна частина електронного документообігу, що здійснює захист від підробки документу, а також для підтвердження достовірності інформації, викладеної у ньому. Тому ЕЦП останнім часом все більше впроваджується в різних сферах діяльності.

У першому розділі було розглянуто правові аспекти та засади для впровадження електронного цифрового підпису в Україні, а також правові та організаційні засади здійснення електронної ідентифікації, головні умови та вимоги до його застосування.

Також було розглянуто питання можливості застосування електронного цифрового підпису у ВНЗ. Застосування ЕЦП може значно зекономити час при підписанні будь-яких електронних документів, до прикладу, звітів, договорів, наказів, екзаменаційних та залікових відомостей тощо. Електронні підписи не тільки допомагають вузам скоротити кількість роздрукованих документів, які необхідно підписати, а також час, що витрачається на їх обробку, крім того електронні підписи скорочують витрати.

У другому розділі розглянуто процес формування електронного підпису, основне призначення, приведені основні схеми та алгоритми на базі яких формується підпис,також розлянуло поняття ключів та хеш-функцій.

В третьому розділі було розглянуто систему електронного документообігу Google Workspace, що являє собою набір інструментів, створених для підвищення продуктивності та співпраці програмного забезпечення та продуктів, розроблений корпорацією Google. Google Workspace включає в себе для спільної роботи (Docs, Sheets, Slides, Forms та Sites), для спілкування (Gmail, Meet, Chat та Calendar), для сховища (Drive) та забезпечує адміністративну панель для управління користувачами та службами.

В четвертому розділі було розглянуто роботу з Google документами, можливості їх застосування. Google Docs редактор Google на базі браузера, дозволяє

створювати, редагувати і обмінюватися документами в Інтернеті, а також отримувати до них доступ з будь-якого комп'ютера, підключеного до Інтернету. Також було проведено практичну частину роботи. Створено власний електронний цифровий підпис за допомогою кваліфікованого надавача електронних довірчих послуг АЦСК АТ КБ "ПРИВАТБАНК" в онлайн сервісі Приват24.Після отримання підпису, було здійснено підписання електронного документа та відправки його керівнику. Ще було досліджено можливості підписання електронних документів в Google Docs. Можливі варіанти підписання: використання інструмента малювання або завантаження електронного підпису з комп’ютера, а також спосіб встановлення надбудови DocuSign, що дозволить підписувати документи через Google Docs, з можливістю потім зберегти цей підпис на Диску.