Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Дробота Максима Владиславовича*

академічної групи *125-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Обгрунтування політики безпеки при побудові криптографічних алгоритмів електронно-цифрового підпису*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.-м.н. проф. Кагадій Т.С.			
розділів:				
спеціальний	ас. Олішевський І.Г.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Дроботу Максиму Владиславовичу* **академічної групи** *125-20-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Обгрунтування політики безпеки при побудові криптографічних алгоритмів електронно-цифрового підпису***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Провести дослідження методів захисту інформації електронного цифрового підпису в Україні	15.03.2024
Розділ 2	Розробити політику безпеки електронного цифрового підпису на основі існуючих криптографічних алгоритмів	10.05.2024
Розділ 3	Розрахувати економічну ефективність запровадження розробленої моделі політики безпеки електронного цифрового підпису	11.06.2024

Завдання видано _____ Ілля ОЛІШЕВСЬКИЙ
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Максим ДРОБОТ
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 74 с., 11 рис., 1 табл., 4 додатка, 29 джерел.

Об’єкт дослідження: криптографічні системи захисту інформації електронно-цифрового підпису.

Предмет розробки: політика безпеки інформації електронно-цифрового підпису.

Мета роботи: визначення необхідного рівня захисту інформації електронно-цифрового підпису.

У першому розділі було розглянуто основні методи захисту інформації, зокрема ті, що використовуються в системах електронно-цифрового підпису, наведено приклади первісного застосування електронно-цифрового підпису в Україні, обгрунтовано його застосування нормативно-правовими актами.

У другому розділі було розглянуто основні сфери застосування електронно-цифрового підпису, описано методологію роботи його криптографічних алгоритмів, розроблено модель порушника, модель загроз та політику безпеки інформації.

У третьому розділі було розраховано економічну ефективність впровадження розробки кваліфікаційної роботи на приватні підприємства та урядові структури.

Практична цінність розробки полягає у створенні критеріїв та правил щодо захисту систем електронно-цифрового підпису на приватних підприємствах та урядових структурах.

ПОЛІТИКА БЕЗПЕКИ, ІНФОРМАЦІЙНА БЕЗПЕКА, КРИТЕРІЇ ЗАХИЩЕННОСТІ, ЗАГРОЗИ, ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ.

ABSTRACT

Explanatory note: 74 p., 11 pic., 1 table, 4 app, 23 sources.

Object of research: cryptographic systems of electronic digital signature information protection.

Subject of development: information security policy of electronic digital signature.

Purpose: determination of the necessary level of protection of electronic digital signature information.

In the first chapter, the main methods of information protection, in particular those used in electronic digital signature systems, examples of the initial use of electronic digital signatures in Ukraine were considered, and justified its use by regulatory and legal acts.

In the second chapter, the main areas of application of the electronic digital signature were considered, the methodology of its cryptographic algorithms was described, the offender model, threat model and information security policy were developed.

In the third chapter, the economic efficiency of the implementation of the development of qualification work for private enterprises and government structures was calculated.

The practical value of the development lies in the creation of criteria and rules for the protection of electronic digital signature systems at private enterprises and government structures.

SECURITY POLICY, INFORMATION SECURITY, SECURITY CRITERIA, THREATS, INFORMATION WITH RESTRICTED ACCESS, CRYPTOGRAPHIC PROTECTION OF INFORMATION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ЕЦП – електронно-цифровий підпис;

ЗСУ – Збройні Сили України;

ІКС – інформаційно-комунікаційна система;

ІС – інформаційна система;

КЕП – кваліфікований електронний підпис;

КЗІ – криптографічний захист інформації;

МВС – Міністерство Внутрішніх Справ;

ОР – обчислювальні ресурси;

ПЗ – програмне забезпечення;

СБУ – Служба безпеки України;

СД – схема доповнення;

СЕД – система електронного документообігу.

ЗМІСТ

с.

ВСТУП

Електронний документообіг стає невід'ємною частиною реальності сьогодення. Україна поступово починає відмовлятись від паперової документації, що можна спостерігати в багатьох державних структурах, таких як: Міністерство освіти і науки України, Міністерство оборони України, Міністерство охорони здоров'я України, Центри надання адміністративних послуг тощо.

З приходом ведення електронної документації з'являється проблема підтвердження належності надрукованого документа до конкретного громадянина. Електронний цифровий підпис став на заміну паперовому рукописному підпису, чим вирішив проблему підтвердження належності особи. Наразі він використовується для верифікації правдивості документа, проведення банківських операцій та ідентифікації користувача онлайн-порталу. Актуальною версією ЕЦП на момент публікації роботи є кваліфікований електронний підпис.

Ідентифікація є непростим завданням в умовах необхідності збереження конфіденційності інформації. В процесі створення, передачі, обробки існують великі ризики витоку даних. Для запобігання імовірних загроз КЕП має містити потужні криптографічні алгоритми захисту.

Метою кваліфікаційної роботи є обґрунтування значущості та рівню захищеності криптографічних систем ЕЦП в актуальній версії його застосування в сферах документообігу, онлайн-банкінгу та на порталах державних структур України.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Захищеність інформації є серйозним питанням будь-якої людини в сучасному суспільстві. За результатами щорічного всеукраїнського опитування Київського міжнародного інституту соціології, датованого вереснем 2022 року, 72% респондентів є регулярними користувачами інтернету в часі від 3 годин щоденно. Інфографіку наведено на рисунку 1.1.

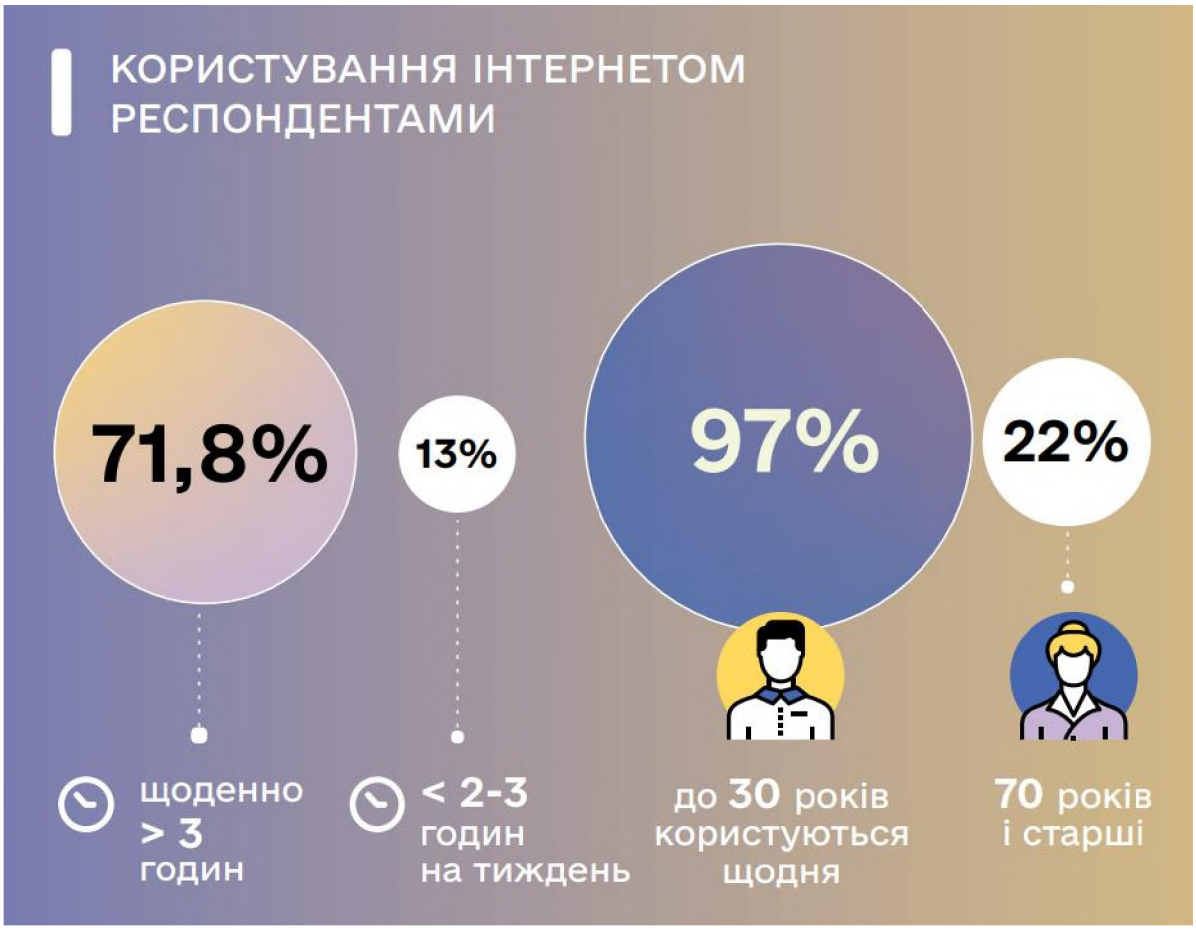

Рисунок 1.1 Користування інтернетом українцями

Серед величезного обсягу інформації, яка постійно потрапляє в мережу та отримується самими користувачами, завжди існують ризику витоку та втрати конфіденційних даних.

1.2 Методи захисту інформації

Існує декілька видів захисту інформації:

1. Фізичний – використовує захисні споруди та обладнання різного типу для запобігання негативного фізичного впливу навколишнього середовища та проникненню осіб без повноважень з метою викрадення, пошкодження, компрометації інформації.

До засобів фізичного захисту відносяться системи сигналізації, протипожежні системи, датчики безперервного контролю приміщення, сейфи тощо.

2. Організаційний – включає в себе впорядкування та організацію плану захисту приміщень та носіїв інформації, обмежуючи і надаючи доступ до інформації з обмеженим доступом.

До організаційних засобів захисту відноситься проектування захисних споруд, планування розміщення обладнання сигналізації, надання повноважень доступу співробітникам до захищеної інформації, створення протоколів взаємодії з інформацією тощо.

3. Правовий – регулювання доступу, необхідного рівня захисту та встановлення покарань за невиконання вимог взаємодії з інформацією Законами України, нормативно-правовими актами, внутрішніми органами управління.

До засобів правового захисту інформації відносяться Закони України відповідного змісту та внутрішні правила компаній, що взаємодіють з інформацією.

4. Морально-етичний – має психологічний вплив за неналежну поведінку в суспільстві, що суперечить морально-етичним стандартам. Супроводжується зниженням авторитету, репутації.

5. Програмний – ПЗ, розроблене для розмежування рівнів доступу до інформації, захисту цілісності інформації та попередження про ймовірні або існуючі інциденти її компрометації.

До засобів програмного захисту інформації належать антивіруси, фаєрволи, СУБД і їм подібні.

6. Криптографічний – набір математичних алгоритмів, які виконують команди шифрування і дешифрування даних, обмежуючи доступ користувачам без необхідних ключів для їх перегляду.

До засобів криптографічного захисту інформації відносяться приватні та публічні ключі, криптосистеми, протоколи обміну даних, ЕЦП тощо.

1.3 Криптографічні методи захисту інформації

Криптографія – це наука, що гарантує безпеку інформації, її цілісність та недоступність для сторонніх осіб з використанням математичних методів.

Найбільш безпечним методом захисту інформації є криптографічний. Високий рівень захисту досягається завдяки тому, що криптографія охороняє конкретно саму інформацію, а не блокує доступ до неї. Це досягається завдяки використанню програм та математичних алгоритмів.

Основні завдання криптографії:

– перегляд інформації має бути можливим лише маючи необхідний ключ;

– за наявності алгоритму, який використовується для шифрування повідомлення, безпека інформації не має знижуватись;

– ключі повинні мати надійний захист;

– унеможливити розшифрування інформації шляхом створення надійних ключів, на підбір яких обчислювальним системам доведеться використати потужності за межами їх можливостей;

– усі дані, що накладаються на інформацію в процесі шифрування, повинні бути надійно приховані;

– навіть за наявності видозміненого ключа, вихідний текст має істотно відрізнятись від оригінального;

– ключі повинні мати складну залежність.

Криптографія використовує два методи шифрування інформації: симетричний та асиметричний.

1.3.1 Симетричний метод шифрування даних

У симетричному методі використовуються два однакових ключі для шифрування та дешифрування інформації або вони мають слабкий рівень залежності (легке обчислення одного ключа з іншого).

Існують два типи симетричного шифрування:

1. Блочний метод.

При блочному шифруванні береться ключ та фрагмент повідомлення. Довжина зашифрованого фрагменту є такою самою, як і довжина вхідного тексту. Після шифрування першого блоку відбувається шифрування наступного, з їх подальшим поєднанням. Так відбувається надалі аж до останнього фрагменту тексту.

Стандартом блочних шифрів є AES (Advanced Encryption Standard). Алгоритм, який використовується в AES, має фіксовану 128-бітну довжину блоку.

Ключ, довжиною у 128 біт, виконує наступні операції:

– subBytes() – побайтово обробляє блоки повідомлення, нелінійно замінюючи їх (див. рисунок 1.2);

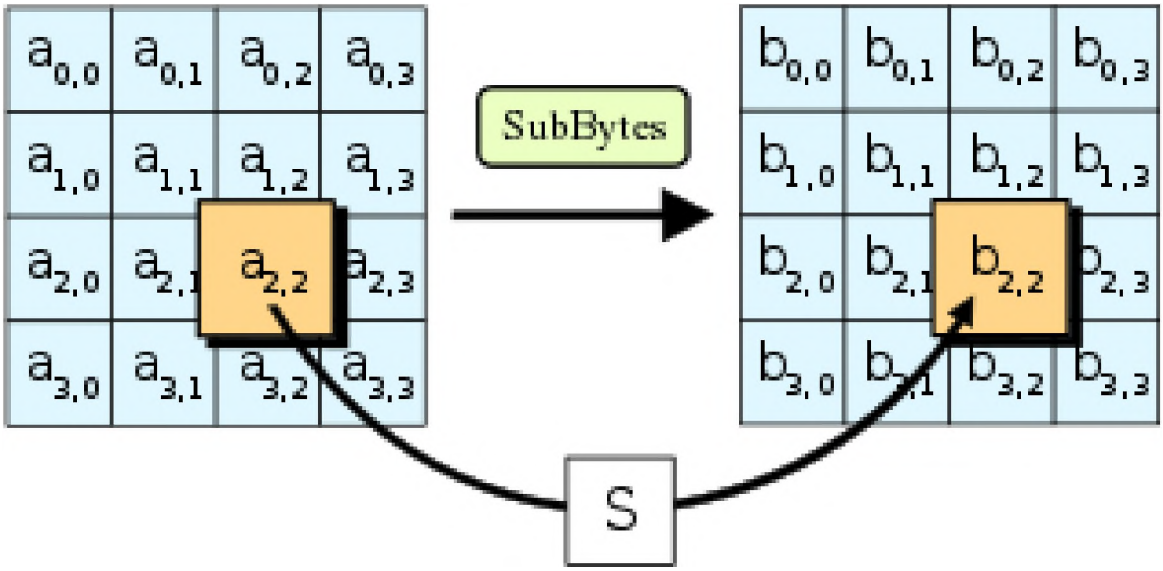

Рисунок 1.2 – Приклад роботи операції subBytes()

– shiftRows() – горизонтально зсуває елементи рядків блоку на x байтів (див. рисунок 1.3);

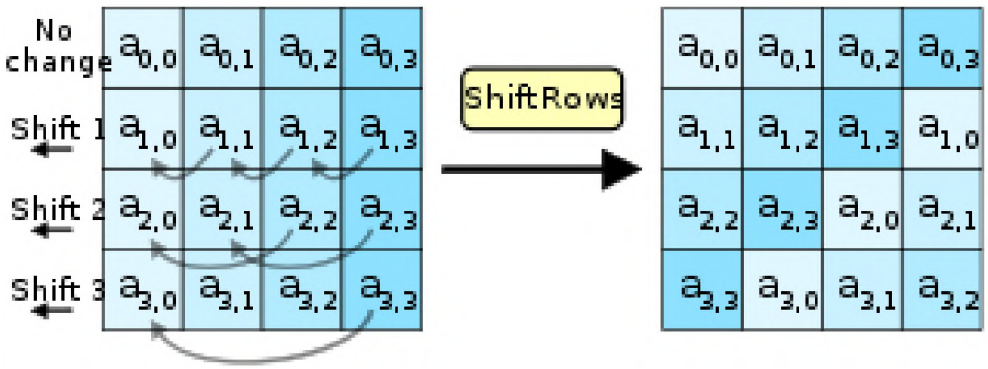

Рисунок 1.3 – Приклад роботи операції shiftRows()

– mixColumns() – замінює байти в колонках, перемножуючи їх на сталу величину (див. рисунок 1.4);

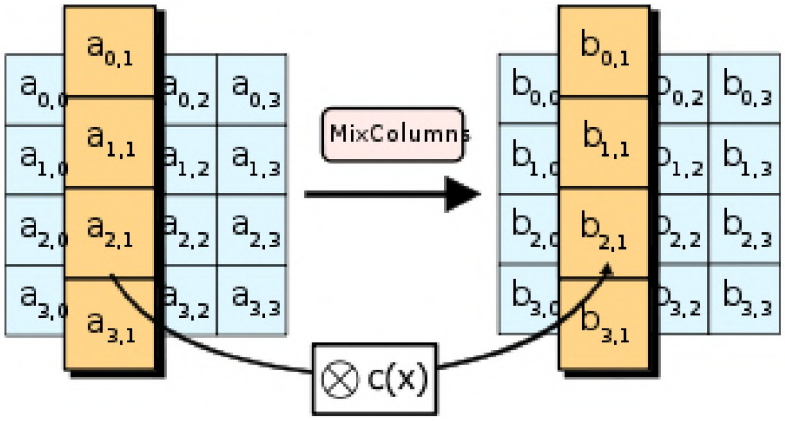

Рисунок 1.4 – Приклад роботи операції mixColumns()

– xorRoundKey() – створює новий зашифрований блок, побайтово виконуючи операцію виняткової диз'юнкції з вхідним блоком та ключем (див. рисунок 1.5).

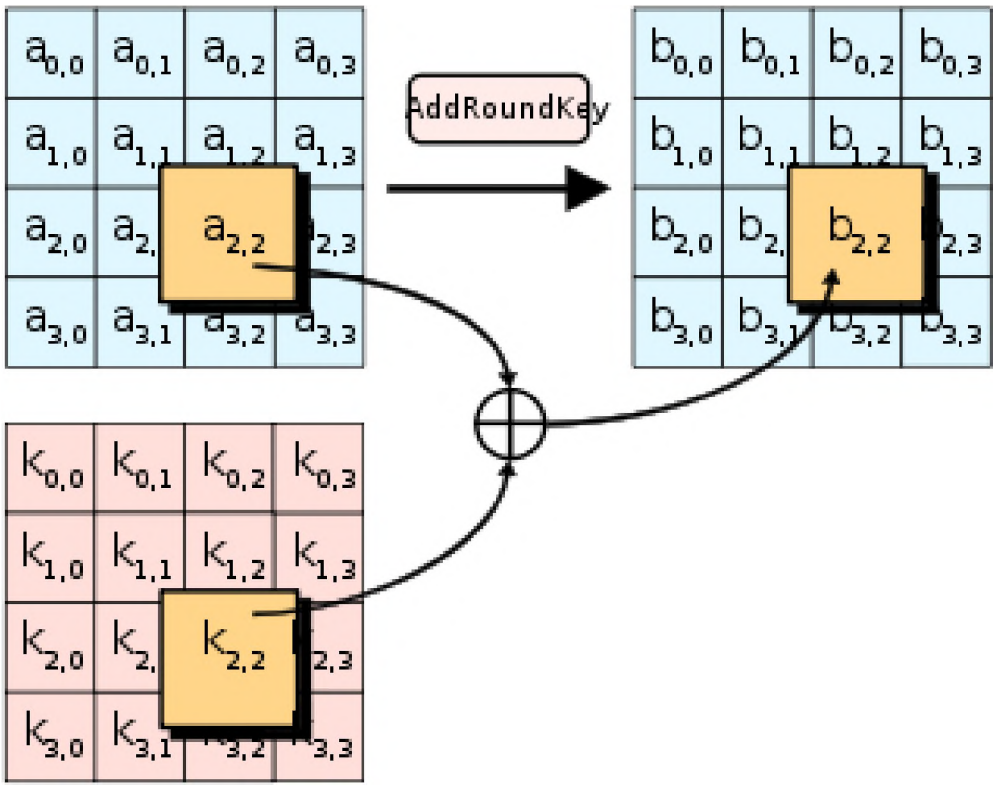

Рисунок 1.5 – Приклад роботи операції xorRoundKey()

Після проходження 10-ти раундів, алгоритм зупиняється і результатом його роботи є зашифроване повідомлення. Важливо відмітити, що операція mixColumns() не виконується в останньому раунді.

2. Потоковий метод.

Потоковий метод використовує просте шифрування XOR (виняткова диз'юнкція) вхідного повідомлення та ключа. Кожен символ даних потоково замінюється іншими байтами, незалежно від інших байтів повідомлення.

Даний метод використовується у таких алгоритмах як RC4, CSS, Salsa20. На відміну від перших двох, що є ненадійними на даний момент часу, алгоритм Salsa20 широко використовується у наші дні.

1.3.2 Асиметричний метод шифрування даних

Асиметричне шифрування – метод шифрування даних, що використовує два різних ключі: публічний і приватний. Незважаючи на те, що публічний ключ

може знаходитись у вільному доступі для використання усіма користувачами мережі інтернет, на безпеку це ніяк не впливає.

Основна мета асиметричного шифрування полягає в тому, щоб користувачі мали змогу обмінюватись зашифрованими повідомленнями, попередньо не домовляючись про безпекові умови.

Яскравим прикладом використання асиметричного шифрування є алгоритм RSA.

RSA – криптографічний алгоритм, що використовує розкладання на множники складних цілих чисел з використанням відкритого ключа. Розробниками цього алгоритму є Rivest, Shamir і Adleman, абревіатурою прізвищ яких і є назва алгоритму.

Принцип алгоритму RSA базується на чотирьох етапах:

- створення ключів;
- надсилання публічного ключа;
- шифрування повідомлення;
- розшифрування повідомлення.

Детальніше про всі етапи буде розглянуто у другому розділі кваліфікаційної роботи.

1.4 ЕЦП в Україні

Електронний підпис – дані в електронному вигляді, що поєднуються з електронними даними, відповідно до яких було застосовано процедуру підписання, з метою ідентифікації належності особи до цих даних.

Електронний цифровий підпис – електронний підпис, що містить певний набір криптографічних алгоритмів, які поєднують дані підписувача із даними, до яких було застосовано процедуру підписання. Особистий та відкритий ключі використовуються для накладання та перевірки підпису відповідно.

У 2011 році 15 лютого було проведено засідання у складі багатьох науковців та представників державних органів на тему: «СЕД в Україні: сучасний

стан та перспективи розвитку». В ході цього обговорення розглядались можливості держави до введення системи електронного документообігу та способи її подальшого розвитку. Таке засідання мало велику значущість для багатьох юридичних та фізичних осіб України. Питання бюрократії та часу, який витрачався на процеси передачі, підтвердження, розгляду паперової документації, суттєво затримувало розвиток бізнесу в країні та взаємодію громадян із урядовими формуваннями.

До розгляду було подану низку питань, зокрема:

- існуючий на даний момент рівень розвитку СЕД в Україні;
- порівняння використання СЕД в інших країнах світу;
- впровадження СЕД на загальнонаціональному рівні;
- збереження конфіденційності інформації при використанні СЕД;
- рівень захищеності ЕЦП.

На момент проведення цього засідання було очевидно зрозуміло, що рівень захисту інформації не є достатньо високим для впровадження СЕД та використання ЕЦП на загальнонаціональному рівні. Водночас, екологічна та бюрократична проблема хвилювала як органи державних структур, так і громадян країни.

З часом Міністерство цифрової трансформації України поставило на меті створити досконалу версію СЕД та ЕЦП таким чином, щоб кожна людина могла користуватись державними послугами не виходячи з дому.

У 2020 році був офіційно запущений мобільний додаток Дія. З моменту його створення усі урядові організації почали підв'язуватись до цього додатку, надаючи можливість взаємодії зі своїми базами даних, а також електронними послугами.

1.5 Нормативно-правова база

У 2018 році набув чинності Закон України «Про електронну ідентифікацію та електронні довірчі послуги». З дати його прийняття електронний цифровий підпис має державне визнання та може бути прирівняним до фізичного підпису.

Кожна фізична та юридична особа, що є громадянином України, може використовувати ЕЦП для наступних цілей:

– ідентифікація особи на веб-порталах та застосунках державних установ;
– підписання електронної документації, засвідчуючи особу підписувача;
– отримання державних електронних послуг;
– підтвердження цілісності та правдивості даних;
– проведення банківських операцій.

Будь-який документ, на який було накладено ЕЦП має юридичну силу. Подання звітності, підписання декларацій, електронних звернень до державних установ, підтвердження особи може бути засвідчено електронним підписом.

Згідно статті 1 пункту 1 Закону України «Про електронну ідентифікацію та електронні довірчі послуги», надавачем електронних довірчих послуг є юридична або фізична особа - підприємець, яка надає хоча б одну кваліфіковану електронну довірчу послугу. Такі особи мають бути внесені до Довірчого списку.

Довірчий список наразі вміщає в собі 22 назви юридичних осіб, до складу яких зокрема входять:

– ПриватБанк;
– Генеральний штаб ЗСУ;
– Військова частина Державної прикордонної служби;
– Дія;
– МВС України;
– Казначейська служба України;
– Податкова служба України;
– «Укрзалізниця»;
– Сервіс «Вчасно»;
– СБУ.

Розрізняються три рівні довіри до засобів електронної ідентифікації: низький, середній та високий.

До низького рівня довіри належить простий ЕЦП. Він може бути виступати як логін та пароль на веб-порталах, підтвердження користувача через електронну пошту або SMS-повідомлення тощо.

До середнього рівня довіри належить удосконалений ЕЦП. Такий підпис може ідентифікувати особу користувача та перевірити дані на їх цілісність.

До високого рівня довіри належить кваліфікований підпис. Він є надійним та може використовуватись для підписання електронних документів.

Кваліфікований електронний підпис (КЕП) має найвищий рівень довіри та є таким, що прирівнюється до фізичного.

Надавачі послуг електронної ідентифікації зобов'язані дотримуватись наступних правил:

– мати засоби електронної ідентифікації відповідно до визначеного рівня довіри;

– захищати персональні дані користувачів, що користуються їх електронними послугами;

– отримувати електронні дані, які містяться у відкритому ключі електронного цифрового підпису з метою ідентифікації особи підписувача;

– захищати дані, що передаються від користувачів електронних послуг;

– проводити постійний контроль та перевірку ризиків зниження рівня безпеки;

– проінформувати відповідні державні органи про інциденти втрати або компрометації персональних даних користувачів, що користуються електронними послугами;

– проінформувати користувачів електронних послуг про інциденти втрати або компрометації персональних даних;

– заблокувати доступ до електронних послуг в разі інциденту втрати або компрометації персональних даних користувачів;

– надавати користувачам електронних послуг повний перелік правил та умов використання їх ресурсів.

Таким чином досягається високий рівень довіри між користувачем та надавачем електронних послуг, оскільки будь-яка взаємодія з персональними даними громадян України регулюється чинним законодавством.

1.6 Висновок

В даному розділі кваліфікаційної роботи було розглянуто основні принципи та засоби захисту інформації в інформаційно-комунікаційних системах. Детально розібрано їх складові, переваги та недоліки, можливості для застосування в системах електронного документообігу.

Більш поглиблено було розібрано принципи, на яких грунтується криптографічний метод захисту інформації. Наведено приклади застосування в існуючих алгоритмах шифрування даних та можливості для їх застосування в електронно-цифровому підписі.

З електронних джерел було узято інформацію про минулий досвід використання електронно-цифрового підпису в Україні. Розписано принципи, на яких базується електронний цифровий підпис, головна мета його використання та проблеми, які він вирішує.

Наведено інформацію з офіційних порталів законодавчої бази про регулювання електронно-цифрового підпису Законом України. Прописано обов’язки та необхідні правила його використання в системі електронного документообігу.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Принцип роботи ЕЦП

Механізм роботи ЕЦП відноситься до симетричного криптографічного методу захисту інформації з відкритим та особистим ключем.

Особистий ключ – створюється шляхом генерації випадкових чисел сервісом, що надає можливість створення особистого електронного цифрового підпису.

Ця послідовність чисел завжди є і має бути унікальною, що не повторюється в жодному із випадків генерації інших користувачів електронної ідентифікації та послуг.

Довжина електронного цифрового підпису складає 264 біти.

Підпис не може бути поширений, скопійований або перенесений на інші носії інформації. Це технічно неможливо і є необхідним з погляду безпеки інформації та збереження конфіденційності персональних даних. Тобто особистий ключ електронного підпису існує тільки в єдиному екземплярі власника.

Відкритий ключ – обчислюється з особистого ключа власника електронного цифрового підпису. У зворотному порядку так не працює. Особистий ключ ніяким чином не може бути обчислений або викритий з відкритого. Відкритий та особистий ключі можуть взаємодіяти з документами або сервісами ідентифікації лише в парі.

Сертифікат відкритого ключа – документ в електронному вигляді, який накладається на електронні дані і підтверджує належність відкритого ключа конкретній фізичній або юридичній особі, що застосувала процедуру підписання.

Цифровий сертифікат містить:

- серійний номер;
- найменування алгоритму цифрового підпису;
- прізвище, ім’я, по-батькові власника сертифіката;
- термін дії;

– найменування юридичної особи, що видала сертифікат;

– найменування центру сертифікації;

– електронний підпис центру сертифікації;

– відкритий ключ власника;

– окремі позначки ідентифікації алгоритму, на підставі якого було згенеровано відкритий ключ власника.

Візуальний вид алгоритму наведений на рисунку 2.1.

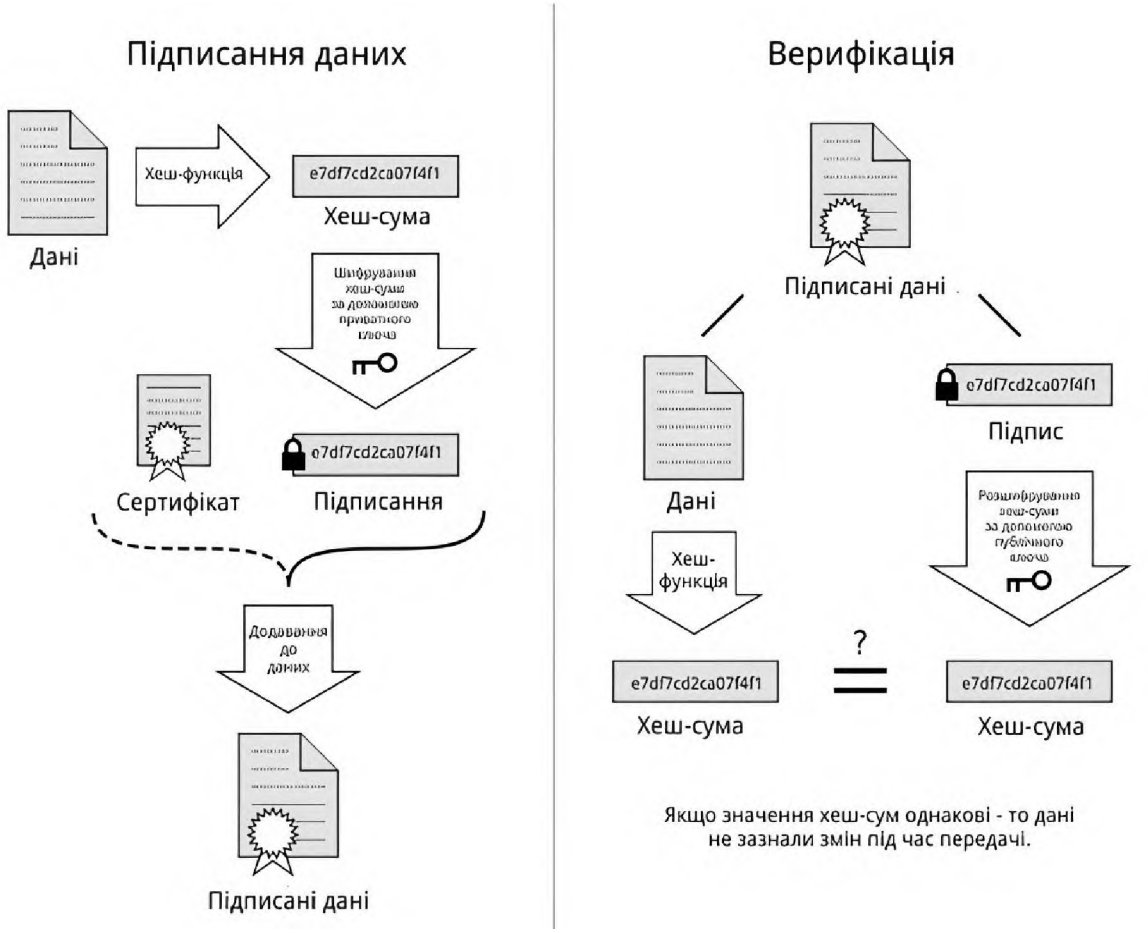

Рисунок 2.1 – Візуальна послідовність роботи ЕЦП

2.2 Криптографічні алгоритми ЕЦП

Реалізація алгоритмів шифрування на даний момент можлива у чотирьох видах представлення криптографічних систем:

– RSA;

– ElGamal;

– DSA;

– ECDSA.

Кожен з цих алгоритмів шифрування підтримує взаємодію і застосування до електронного цифрового підпису. Але в кожного з них є свої недоліки, які детальніше треба розглядати.

2.2.1 Підпис алгоритмом RSA

RSA – найперший алгоритм, що поєднав у собі можливості шифрування та цифрового підпису. Такий алгоритм мав досвід застосування в Україні в криптосистемі електронного цифрового підпису.

Процес генерації ключів:

1. Генератор випадкових або псевдовипадкових чисел створює два прості числа p і q. Довжина кожного числа не має перебільшувати 512 біт з метою пришвидшення подальшого їх обчислення та запобігання виникнення можливих помилок. За стандартом слід використовувати саме 512-бітні значення.

2. Обчислюється добуток n цих двох простих чисел:

$$n = pq \tag{2.1}$$

3. Застосовується функція Ейлера від добутку простих чисел:

$$\varphi(n) = (p-1)(q-1) \tag{2.2}$$

4. Випадковим або псевдовипадковим чином обирається число таке, що $1 < e < \varphi(n)$ і НСД$(e, \varphi(n)) = 1$.

5. За розширеним алгоритмом Евкліда знаходиться число d з рівняння:

$$d \equiv e^{-1} (\mathrm{mod}\, \varphi(n)) \tag{2.3}$$

Пара чисел n і e утворює відкритий ключ, а число d – особистий. Особливо важливим після розрахунку даних для генерації пари ключів видалити початкові числа p і q та не зберігати їх ні на жодному носії інформації, оскільки за наявності первісних чисел секретний ключ може бути розкритий.

Надалі наступає черга обчислення цифрового підпису за формулою 2.4:

$$c = m^d \pmod n \tag{2.4}$$

де c – цифровий підпис,

m – хеш-сума $0 \leq m < n$, створена з повідомлення узгодженою СД,

d – особистий ключ підписувача.

Для перевірки дійсності ключа має виконуватись рівність:

$$m' = c^e \pmod n \tag{2.5}$$

де m’ – хеш-сума зашифрованого повідомлення,

e – відкритий ключ підписувача.

Якщо хеш-сума m дорівнює хеш-сумі m’ – підпис дійсний, в іншому випадку – ні. У такий спосіб закритий ключ підписувача залишається невідомим, а відкритий ключ може бути застосований для підтвердження його приналежності до цифрового підпису.

Особливо важливим елементом в алгоритмі RSA є доповнення повідомлень за узгодженими оборотними протоколами, по типу OAEP. Ігнорування використання схем доповнень може призвести до таких наслідків, як:

– якщо m буде приймати значення 0 або 1, зашифровані тексти також будуть відповідати значенням 0, 1 відповідно при довільних значеннях e і n;

– якщо значення e буде занадто малим, то є ризик відновлення початкового повідомлення з зашифрованого повідомлення. Така ситуація може скластись у випадку 2.6.

$$m^e < n \Rightarrow c = m^e (\mathrm{mod}\, n) = m^e \Rightarrow m = \sqrt[e]{c} \tag{2.6}$$

2.2.2 Підпис алгоритмом ElGamal.

Тахер Ель-Гамаль у 1985 році удосконалив алгоритм Діффі-Геллмана. Результатом його роботи була утворена схема, придатна для шифрування та цифрового підпису.

ElGamal алгоритм виграє у RSA тим, що він не був запатентований Тахером, а отже розробникам не доведеться сплачувати за ліцензії при використанні його розробки.

Генерація ключів:

1. Генерація випадкового або псевдовипадкового простого числа, довжиною p бітів.
2. Вибирається один випадковий елемент g з поля Z_p.
3. Вибирається одне ціле випадкове число x, з урахуванням нерівностей $1 < x < p - 1$.
4. Обчислюється рівняння:

$$y = g^x (\mathrm{mod}\, p) \tag{2.7}$$

Результатом обчислень є відкритий (p, g, y) та приватний ключ (x).

Процедура підписання:

1. Отримуємо хеш-суму m з повідомлення M.
2. Вибираємо випадкове або псевдовипадкове число з діапазону $1 < k < < p – 1$ таке, що НСД(k, p-1) = 1.
3. Обчислюється рівняння:

$$r = g^k \pmod p \tag{2.8}$$

4. Обчислюється рівняння з використанням особистого ключа x:

$$s \equiv (m - xr)k^{-1} \pmod{p-1} \tag{2.9}$$

Пара чисел r і s вважається підписом повідомлення M.

Процедура перевірки підпису:

1. Виконується перевірка двох умов:
   - $0 < r < p$;
   - $0 < s < p - 1$.

Якщо хоча б одна нерівність видає результат False – підпис несправжній.

2. Обчислюється хеш-сума m з повідомлення M.
3. Перевіряється відповідність з рівності, маючи дані про відкритий ключ p, g, y:

$$y^r r^s \equiv g^m \pmod p \tag{2.10}$$

Якщо ця рівність виконується, то підпис є справжнім.

2.2.3 Підпис алгоритмом DSA

Digital Signature Algorithm (DSA) – криптографічний алгоритм, побудований на принципі асинхронної криптографії з відкритим ключем, але може використовуватись лише при створенні електронних цифрових підписів.

Схему алгоритму DSA наведено на рисунку 2.2.

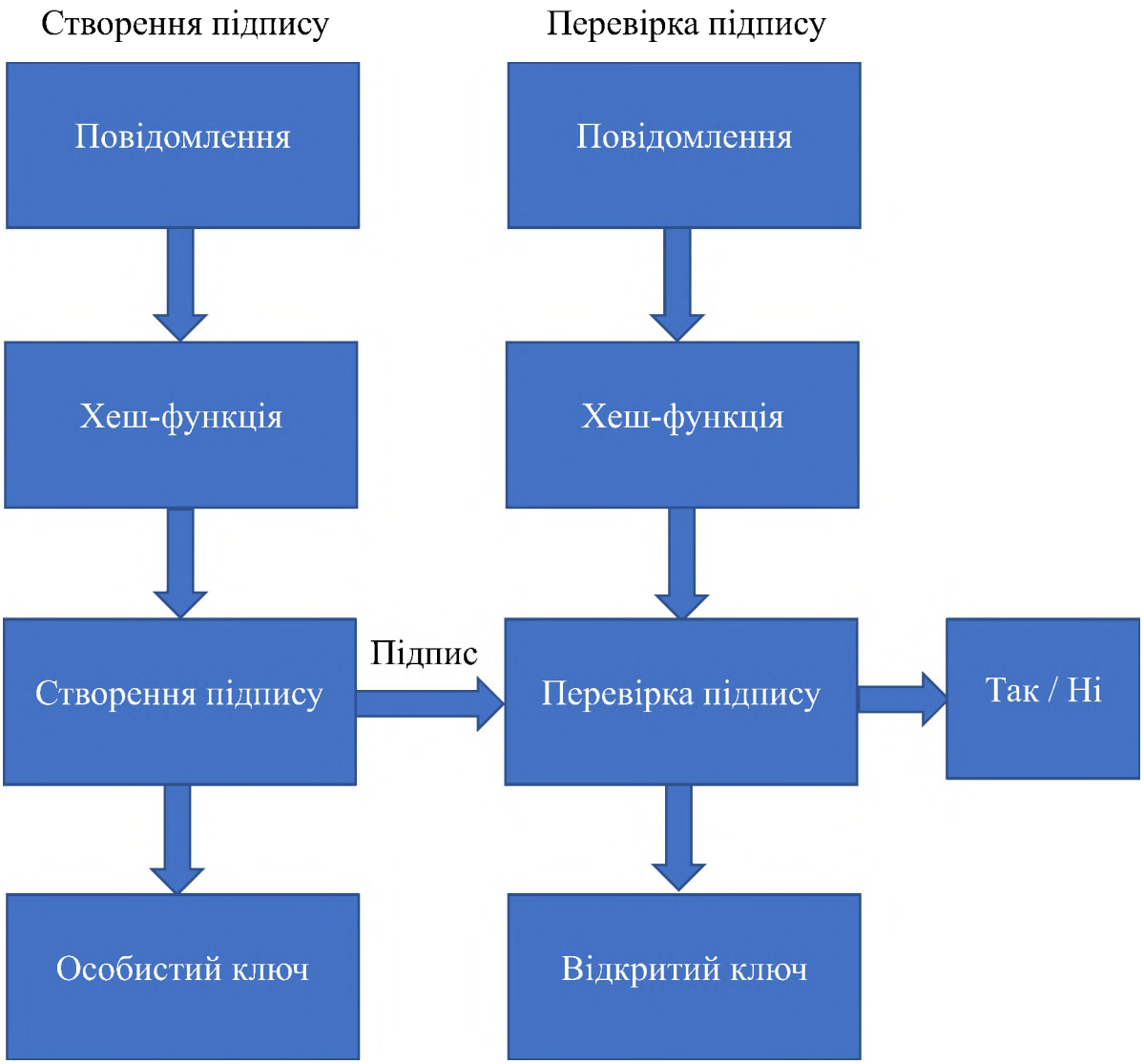

Рисунок 2.2 – Схема роботи алгоритму DSA

Генерація ключів в такому алгоритмі має дві фази. Перший етап є вибором параметрів алгоритму, які можуть бути спільними для різних користувачів системи, тоді як другий етап обчислює одну пару ключів для одного користувача.

Генерація параметрів:

1. Вибір затвердженої хеш-функції H.
2. Вибір простого числа q довжиною N бітів таким, що співпадає з довжиною значень хеш-функції. Якщо довжина хеш-функції більша, тільки крайній біт з лівої сторони хеш-функції буде сприйматись алгоритмом.
3. Вибір простого числа p довжиною L бітів таким, що вираз (p – 1) кратний числу q.
4. Обрати випадкове ціле число h з множини значень (2, p – 2).

5. Обчислити рівняння:

$$g = h^{\frac{(p-1)}{q}} \pmod{p} \tag{2.11}$$

Не допускається значення числа g = 1. У такому випадку слід обрати інше число h. Зазвичай, h = 2 задовольняє усім вимогам.

Особистий ключ є числом x з множини значень (1, q – 1).

Публічний ключ y розраховується за формулою:

$$y = g^{x} \pmod{p} \tag{2.12}$$

Як було зазначено вище, одним із параметрів генерації є хеш-функція. Існує стандарт NIST 800-90A, що визначає наступні пари значень L і N:

- L = 1024; N = 160;
- L = 2048; N = 224;
- L = 2048; N = 256;
- L = 3072; N = 256.

Цей стандарт також надає рекомендації щодо використання хеш-функцій сімейства SHA-2. Його попередник SHA-1 на даний момент часу вважається недостатньо безпечним.

Процес підпису повідомлення M:

1. Обрати випадкове число k з множини значень (1, q – 1).
2. Обчислити рівняння:

$$r = (g^{k} \pmod{p}) \bmod q \tag{2.13}$$

У випадку r = 0 варто переобрати число k і провести розрахунок наново.

3. Обчислити рівняння:

$$s = (k^{-1}(H(M) + xr)) \bmod q \tag{2.14}$$

У випадку s = 0 варто переобрати число k і провести розрахунки наново.

Цифровим підписом вважається пара значень r і s.

Складними операціями для обчислення є піднесення до степеня за модулем, для яких існують швидкі алгоритми, обчислення хешу, де складність залежить від обраного алгоритму хешування і розміру вхідного повідомлення, і знаходження оберненого елемента, використовуючи, наприклад, розширений алгоритм Евкліда або малу теорему Ферма.

Процес перевірки підпису повідомлення M:

1. Переконатися, що задовольняються нерівності $0 < r < q$ і $0 < s < q$.
2. Обчислити рівняння:

$$w = s^{-1} (\bmod q) \tag{2.15}$$

3. Обчислити рівняння:

$$u_1 = H(M) \cdot w (\bmod q) \tag{2.16}$$

4. Обчислити рівняння:

$$u_2 = r \cdot w (\bmod q) \tag{2.17}$$

5. Обчислити рівняння:

$$v = (g^{u_1} y^{u_2} (\bmod p)) \bmod q \tag{2.18}$$

Якщо виконується рівність v = r, то тільки тоді підпис є дійсним.

При використанні алгоритму DSA ентропія, секретність та унікальність випадкового значення сигнатури k є критичними. Це настільки важливо, що порушення будь-якої з цих трьох вимог може розкрити зловмиснику весь приватний ключ. Подвійне використання значення числа k (навіть при збереженні його в секретності), використання передбачуваних значень або витік навіть декількох бітів значення k в кожній з декількох сигнатур, теоретично може бути достатнім для відновлення повного значення особистого ключа x.

Можна вирішити цю проблему виводячи k з особистого ключа та хешу повідомлення. Це буде гарантувати, що k завжди буде унікальним для кожного нового хешованого повідомлення H(M) і непередбачуваним для зловмисників, що не знають значення приватного ключа x.

2.2.4 Підпис алгоритмом ECDSA

Elliptic Curve Digital Signature Algorithm (ECDSA) – алгоритм цифрового підпису з відкритим ключем, що за своєю будовою подібний до алгоритму DSA, але визначений в групі точок еліптичної кривої.

Бітовий розмір закритого ключа в алгоритмі ECDSA приблизно вдвічі перевищує рівень безпеки в бітах. Досягається це завдяки еліптичному методу криптографії.

Створення параметрів алгоритму:

1. Вибрати хеш-функцію H.
2. Вибрати велике просте число q, що буде визначати порядок однієї з циклічних підгруп групи точок еліптичної кривої.
3. Позначити характеристики кінцевого простого поля координат F_p простим числом p.

Генерація ключової пари:

1. Визначити еліптичну криву E над полем F_p, що кратне числу q.
2. Визначити точку P на еліптичній кривій $E(F_p)$ (див. рисунок 2.3).

3. Обрати випадкове або псевдовипадкове ціле число x з множини значень (1, q – 1).

4. Обчислити рівняння:

$$Q = xP \tag{2.19}$$

Закритим ключем є набір значень (x, E, P, q), а відкритим ключем – (Q, E, P, q).

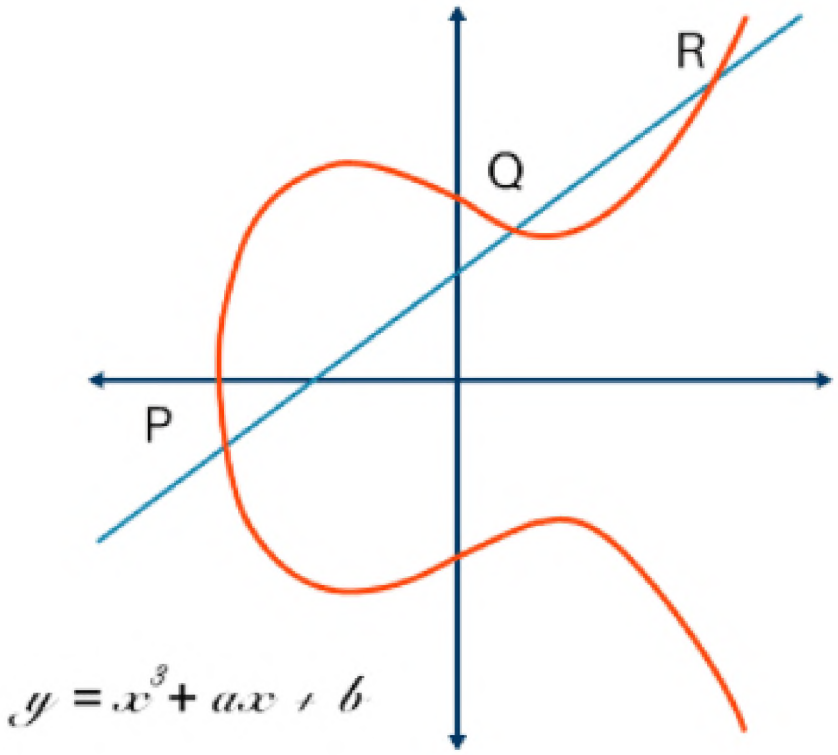

Рисунок 2.3 – Еліптична крива

Створення цифрового підпису:

1. Обчислити хеш-функцію (наприклад, SHA-2) повідомлення H(m). Якщо бітовий розмір числа q перевищує бітовий розмір хеш-функції H(m), то

враховуватись буде значення хеш-функції включно до крайнього лівого біта розміру q.

2. Обрати випадкове або псевдовипадкове ціле число k з множини значень (1, q – 1).

3. Обчислити точку кривої:

$$kP = (x_1, y_1) \tag{2.20}$$

4. Обчислити рівняння:

$$r = x_1 (\mathrm{mod}\, q) \tag{2.21}$$

Якщо r = 0, треба переобрати число k.

5. Обчислити рівняння:

$$s = k^{-1}(H(m) + rx) \mathrm{mod}\, q \tag{2.22}$$

Якщо s = 0, треба переобрати число k.

Цифровим підписом вважається пара значень r і s.

Перевірка цифрового підпису:

1. Якщо значення чисел r і s цілі і лежать у множині значень (1, q – 1), то можна продовжувати перевірку підпису. В іншому випадку підпис вважається недійсним.

2. Обчислити рівняння:

$$u_1 = H(m)s^{-1} (\mathrm{mod}\, q) \tag{2.23}$$

3. Обчислити рівняння:

$$u_2 = rs^{-1} (\mathrm{mod}\, q) \tag{2.24}$$

4. Визначити точку еліптичної кривої:

$$u_1 P + u_2 Q = (x_1, y_1) \tag{2.25}$$

5. Обчислити рівняння:

$$v = x_1 (\mathrm{mod}\, q) \tag{2.26}$$

Якщо v = r, то підпис є дійсним, у будь-якому іншому випадку – підпис не є справжнім.

При рівні безпеки 80 біт (це означає, що зловмиснику потрібно максимум близько 2^{80} операцій для пошуку закритого ключа) – розмір закритого ключа ECDSA становитиме 160 біт. З іншого боку, розмір сигнатури однаковий як для DSA, так і для ECDSA: приблизно 4t бітів, де t є показником степеня у формулі 2^t, тобто близько 320 біт для рівня безпеки 80 біт, що еквівалентно 2^{80} операціям.

2.3 Порівняння алгоритмів ЕЦП

У цьому підрозділі кваліфікаційної роботи буде наведено порівняльну таблицю алгоритмів, що застосовуються при створенні електронних підписів: RSA, ElGamal, DSA і ECDSA.

Таблиця 2.1 – Порівняльна характеристика криптографічних алгоритмів

Назва алгоритму	RSA	ElGamal	DSA	ECDSA
Максимальна довжина L_k публічного ключа, біт	4096	4096	3072	570
Хеш-функції	MD, SHA	MD, SHA	SHA	SHA
Довжина підпису, біт	$L_k * 2$	$L_k * 2$	$F_p * 4$	$F_p * 4$
Відновлення повідомлення	Існує	Не існує	Не існує	Не існує
Швидкість підпису за мінімального розміру ключа, мс	1.48	0.42	0.45	2.88
Швидкість перевірки за мінімального розміру ключа, мс	0.07	0.52	1.18	8.53

Очевидно, що у кожного алгоритму є свої плюси та недоліки. Але будь-який алгоритм потребує детального криптоаналізу для остаточного вирішення ефективності їх застосування.

2.4 Цифровий сертифікат типу PGP

PGP – алгоритм, що використовується для шифрування даних та накладання цифрових підписів на електронні файли. Зазвичай PGP-ключі використовують RSA для їх генерації.

Алгоритм PGP є гібридною криптосистемою. Він поєднує в собі обидва види шифрування – симетричний та асиметричний.

Шифрування даних методом PGP виконується наступним чином:

1. Стискання даних.

Стискання інформації заощаджує місце на фізичному носії інформації, зменшує час передачі по мережі, а також підвищує безпеку. Стиск істотно зменшує ознаки відкритого тексту в зашифрованих даних, що призводить до зменшення ризиків відновлення повної інформації із зашифрованого файлу.

2. Створення сеансового ключа.

Сеансовий ключ це одноразовий симетричний ключ, що використовуватиметься лише для поточної процедури підписання. Такий ключ представляє собою псевдовипадкове число. Тобто генератор випадкових чисел бере дані з довільних рухів комп'ютерної миші та клавіатури користувача. Звідси і походить назва «псевдовипадковий». Числа ніби і мають джерело походження, але все-одно були вибрані у довільному порядку.

3. Шифрування даних сеансовим ключем.

4. Шифрування сеансового ключа відкритим ключем одержувача.

5. Прикріплення зашифрованого сеансового ключа до зашифрованих даних.

Для розшифрування надісланого повідомлення, PGP виконує дії у зворотному порядку. Особистий ключ одержувача «витягує» зашифрований сеансовий ключ із зашифрованого повідомлення, яким потім відновлюється зашифрований текст.

Візуальний алгоритм роботи сертифікату типу PGP наведено на рисунку 2.4.

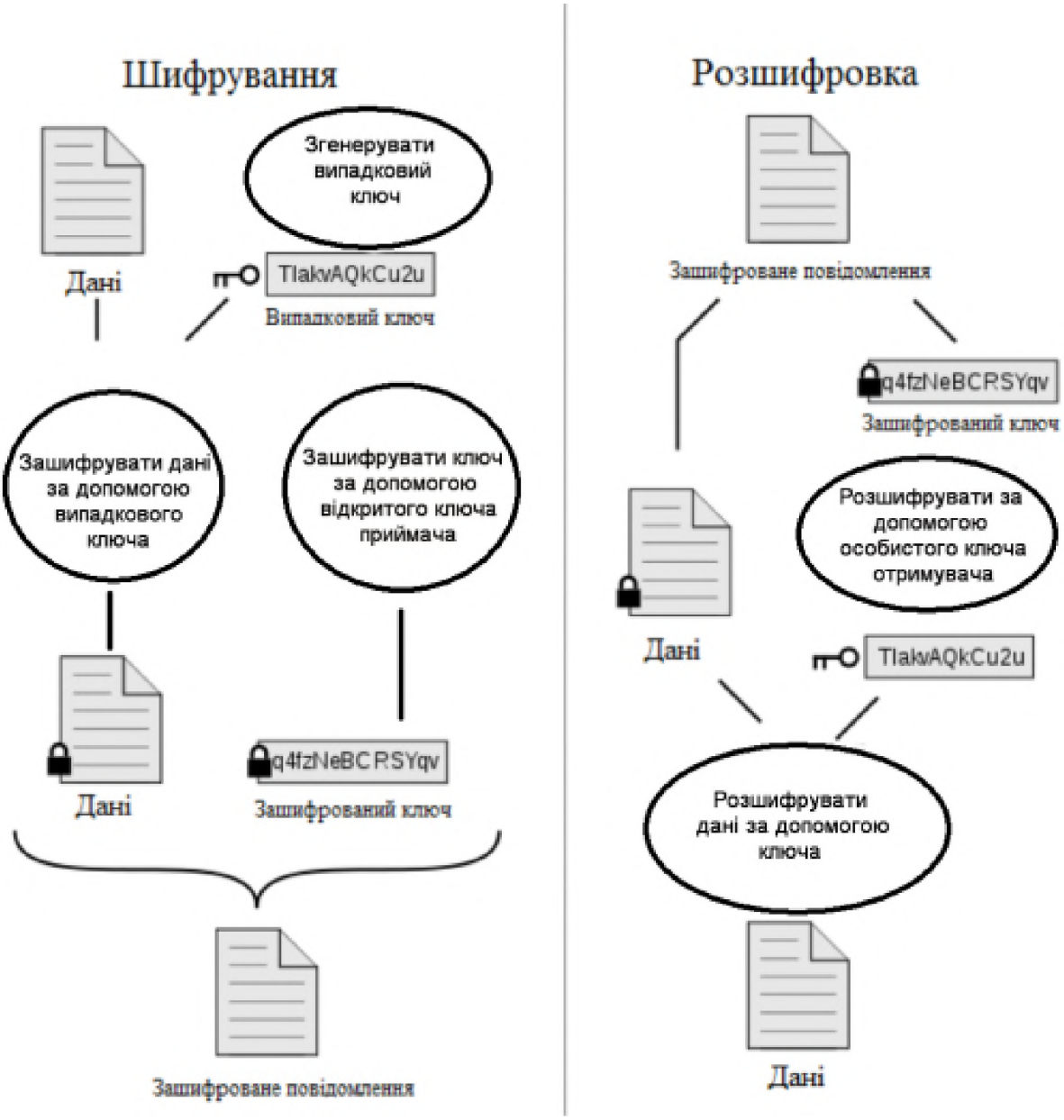

Рисунок 2.4 – Представлення роботи алгоритму PGP

З одного боку PGP шифрування є ефективним, оскільки використовує симетричні та публічні ключі одночасно, що в багато разів швидше за шифрування лише з відкритим ключем. Але великим недоліком такого методу є відсутність центрів сертифікації (англ. CA – certification authority). Тобто будь-яка третя особа може затвердити належність ключів обом сторонам. Це дуже негативно впливає на безпеку підписання документів, адже цифровий підпис має

на меті максимізувати безпекові відносини між суб'єктами систем електронного документообігу та надавачів електронних послуг.

Один PGP сертифікат може містити в собі безліч підписів від третіх осіб, що засвідчують ідентифікацію ключів відповідним особам, виступаючи замість центрів сертифікації. Така побудова довірчих відносин називається «мережею довіри».

2.5 Цифровий сертифікат типу X.509

Найбільш розповсюдженим форматом цифрових сертифікатів є сертифікат типу X.509. Він завірений стандартом Міжнародної Спілки Електрозв'язку (ITU), що дає визнання цього сертифіката в усіх країнах світу.

X.509 визначає стандарти:

- сертифікатів відкритого ключа;
- атрибутів;
- перевірки методів, якими було проведено сертифікацію;
- списків сертифікатів, що були відкликані.

Сертифікація документів за стандартом X.509 виконується наступним чином:

1. Особа, якій необхідно виконати процедуру цифрового підпису, генерує пару ключів (особистий і публічний);
2. Особа, що виконує запит на підписання сертифікату, звертається до центру сертифікації;
3. Запит на видання сертифікату підписується особистим ключем власника цифрового підпису за допомогою одного з трьох визначених протоколів: CSR, SCEP, CMP. Надалі особистий ключ зберігається в таємниці;
4. Протокол, яким було виконано запит до центру сертифікації, отримує інформацію про ідентифікацію заявника, його публічний ключ і унікальне ім'я;
5. За допомогою відкритого ключа заявника виконується перевірка приналежності особистого ключа до заяви сертифікації відповідним реєстраційним органом.

6. Центр сертифікації видає сертифікат, прив'язавши відкритий ключ до унікального ім'я заявника.

Структура сертифіката X.509 виглядає наступним чином:

Сертифікат:
- Номер версії:
- Серійний номер:
- ID алгоритму підписання:
- Ім'я видавця:
- Термін дії:
  - Не до:
  - Не після:
- Ім'я особи:
- Інформація про відкритий ключ особи:
  - Алгоритм відкритого ключа:
  - Відкритий ключ особи:
- Унікальний ідентифікатор видавця:
- Унікальний ідентифікатор особи:
- Додатково:
  - …

Алгоритм підпису сертифіката:

Підпис сертифіката:

X.509 дозволяє створювати ланцюги сертифікатів (див. рисунок 2.5). У такий спосіб центри сертифікації можуть видавати списки сертифікатів, підтверджуючи приналежність відкритого ключа від першого сертифіката до передостаннього. Вони послідовно підписують особистими ключами відповідність відкритого ключа попереднього сертифіката до центру, яким він був виданий. Останній сертифікат у ланцюжку є «самопідписаним», оскільки має найвищий ступінь довіри.

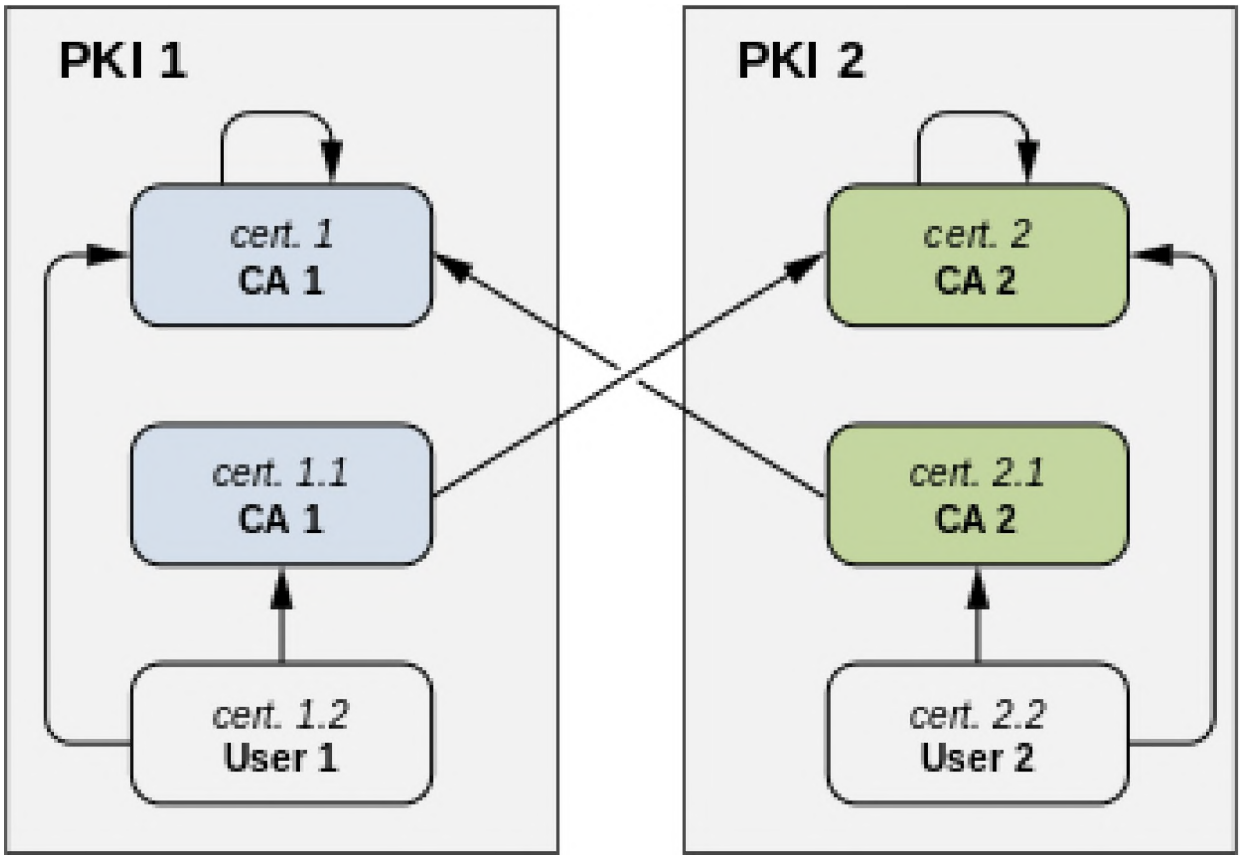

Рисунок 2.5 – Перехресна сертифікація

Для того, щоб сертифікати користувача, що існують в PKI 2 (див. рис. 7), були довіреними PKI 1, CA1 генерує сертифікат cert2.1, що містить відкритий ключ CA2. Тепер і cert2, і cert2.1 мають однаковий відкритий ключ, тому існує два коректні ланцюжки для User 2: cert2.2 → cert2 та cert2.2 → cert2.1 → cert1.

Окрім переваг сертифікатів X.509, вони містять також і слабкі місця:

– можливість використання центрів сертифікації зі списку відкликаних сертифікатів;

– відсутність розгляду кореневих сертифікатів;

– відкликання останнього сертифіката в ланцюжку сертифікатів не перевіряється;

– заяви на перевірку ідентифікаторів, атрибутів та правила надсилаються в одному контейнері, що негативно впливає на конфіденційність даних суб'єктів;

– технічно неможливо центрам сертифікації обмежити інші, підпорядковані їм центри сертифікації у видачі сертифікатів поза доступним

простором імен та атрибутів. У такому випадку X.509 не зможе їх розпізнавати та підтримувати;

– створення ланцюгів сертифікації та процеси перехресної сертифікації є складними та дорогими з точки зору часу їх обробки;

– видача сертифікатів з розширеною перевіркою не перешкоджає видачі сертифікатів з нижчою перевіркою;

– складність унікальних імен.

2.6 Модель порушника

У інформаційній системі, що може взаємодіяти з конфіденційною інформацією, інформацією з обмеженим доступом, інформацією, що вважається державною таємницею, завжди необхідно розробляти модель потенційного порушника.

Мета моделювання полягає у створенні профілю потенційного порушника, що має намір ознайомлення, викрадення, підробки, знищення або редагування захищеної інформації, яка циркулює в ІС або ІКС.

Ця модель може бути надана фахівцям з інформаційної безпеки для подальшого моделювання імовірних загроз та вразливостей інформаційної системи, визначенню ресурсів, необхідних для їх запобігання та розробці комплексу заходів безпеки.

Ця модель являє собою визначення імовірних дій порушника, враховуючи його тип, існуючі повноваження доступу до інформації, час та місце подій. У ході розробці моделі будуть надані відповіді на наступні питання:

– хто є порушником;

– мета порушника;

– доступ порушника до інформації;

– засоби та методи, якими буде користуватись порушник;

– доступність до інформації системи захисту та принципу її роботи.

Інформація, що може бути у доступі порушника:

1. Криптографічні дані.

2. Застосовані аспекти крипто-алгоритмів, такі як тип сертифікатів, хеш-функцій, алгоритмів ЕЦП.

3. Застосовані ОР, що є в доступі порушника.

Атаки порушника можна розділити на два підвиди: пасивні або активні.

При пасивних атаках порушник може діяти наступним чином:

1. Перехоплювати та аналізувати дані, які виконувались в процесі роботи криптографічних алгоритмів, наприклад спроба обчислення сеансового або закритого ключа з перехопленим відкритим ключем підписувача.

2. Робити спроби розв'язання математичних завдань з метою розкриття конфіденційних даних або інформації з обмеженим доступом по відношенню до сеансового або закритого ключа, або обох ключів одночасно.

При активних атаках порушник може діяти подібно криптографічним алгоритмам, додаючи додаткові біти, надсилаючи несправжні повідомлення та/або підписи.

Додаткові імовірні можливості та повноваження порушника відносно до ІС ЕЦП:

– порушник має певний рівень доступу до каналів передачі інформації між особою, що підписує та центром верифікації електронного цифрового підпису;

– можливість запису даних, що надсилаються під час виконання криптографічних алгоритмів електронного цифрового підпису;

– можливість модифікації даних криптографічного алгоритму;

– можливості видалення даних;

– неодноразове використання даних криптографічних алгоритмів;

– можливість несанкціонованої ініціалізації етапів роботи криптографічних алгоритмів, такі як вимкнення, перезапуск, повторення певних дій тощо.

Кожен порушник може перебувати у різних умовах доступу до інформації, тож варто розділити їх на дві категорії:

1. Зовнішній порушник.

Зовнішній порушник може мати лише дані, що перебувають у вільному доступі, такими як публічними ключами, оригінал підписаного повідомлення, електронний цифровий підпис підписувача, загальні параметри системи.

2. Внутрішній порушник.

Внутрішній порушник може мати доступ (постійний або тимчасовий) до сеансових та/або закритих ключів, значень хеш-функцій та інших прихованих даних.

До розгляду подано чотири рівні можливостей порушника в умовах різного доступу до інформації та їх мотивами:

1. Перший рівень – порушник ненавмисним чином отримує доступ до інформації.

2. Другий рівень – порушник має обмежені ресурси для створення та обчислення методів і засобів атак на КЗІ, використовуючи широкий спектр програмного забезпечення та електронно-обчислювального обладнання.

3. Третій рівень – порушник використовує засоби технічного впливу корпоративного рівня на КЗІ, що прирівняні до фінансових збитків в тому випадку, що інформацію було відредаговано, викрадено або знищено. Можуть використовуватись можливості локальних обчислювальних систем.

4. Четвертий рівень – порушник володіє науково-технічними ресурсами, що еквівалентні науково-технічним ресурсам спецслужб розвинених держав.

В основі навмисного впровадження криптоаналізу в більшості випадків є корисливі мотиви. Мотиваційна модель зловмисників зображує поведінку зловмисників в умовах вигоди і витрат, які вони отримують в результаті аналізу. Визначення стратегії напряму залежить від бажання порушника отримати максимальний прибуток та завдати максимальних збитків. Також варто враховувати таку модель поведінки, в умовах якої порушник має на меті лише завдати максимальних збитків, керуючись власними моральними мотивами. Отже, найбільш раціональною варто вважати поведінку, коли порушник співвідносить свої витрати із користю, яку він отримає.

При аналізі криптографічних алгоритмів варто враховувати наступні умови:

– при компрометації закритих ключів електронного цифрового підпису, подальші спроби виконання протоколів мають ризик підробки;

– якщо в системі застосовуються як закриті, так і сеансові ключі, то викрадення перших ніяк не вплине на розкриття сеансових, застосованих раніше.

Варто позначити і границі можливостей порушника. За умов, що криптографічні алгоритми є цілком безпечними, зловмисник ніяким чином не зможе вгадати або дістати оригінальне значення особистого ключа підписувача та не матиме доступу навіть до приблизних його даних. Без особистого ключа порушник не зможе зробити копію електронного цифрового підпису та робити нові підписи без його використання. Знаючи лише відкритий ключ криптографічного алгоритму порушник не зможе викрити особистий ключ підписувача.

2.7 Модель загроз

Моделювання загроз являє собою виявлення потенційних загроз, вразливостей або відсутності точних гарантій того, що система є цілком безпечною для використання і взаємодії для будь-якої ІС або ІКС.

Мета моделювання полягає у наданні систематичного аналізу експертам з кібербезпеки відомостей про необхідні додаткові рівні контролю та/або захисту, враховуючи модель потенційного порушника, ймовірні методи атаки та дані, якими порушник може заволодіти в разі невиконання наданих рекомендацій.

Порушник може здійснювати різні типи загроз, які можна поділити за наступною класифікацією:

– Атака, що базується на доступі до публічного ключа;

Така атака може відбутись у будь-який момент часу, оскільки доступ до публічного ключа не є захищеним і може передаватись третім особам для верифікації електронного підпису. При атаці даної класифікації вважається, що порушник ознайомлений із відомостями про загальносистемні параметри.

– Атака, що базується на інформації про раніше підписані повідомлення;

Така атака враховує, що порушнику, додатково до відомостей з атаки на базі відкритого ключа, відоме число з пари «повідомлення-підпис» раніше підписаних повідомлень. Порушник не може застосовувати інші повідомлення того ж самого цифрового підпису для аналізу.

– Проста атака, що базується на інформації про раніше підписані повідомлення одним і тим самим ЕЦП;

Така атака враховує, що порушнику, додатково до відомостей з атаки, яка базується на інформації про раніше підписані повідомлення, відомо декілька чисел пари «повідомлення-підпис» за умови одного і того ж самого параметру «підпис». Отже порушник може обирати різні параметри «повідомлення» для аналізу.

– Спрямована атака, що базується на інформації про раніше підписані повідомлення одним і тим самим ЕЦП;

Така атака враховує, що порушник, враховуючи відомості з простої атаки, що базується на інформації про раніше підписані повідомлення одним і тим самим ЕЦП, на свій розсуд може обирати публічні ключі для підписаних повідомлень.

– Адаптивна атака, що базується на інформації про раніше підписані повідомлення одним і тим самим ЕЦП.

Така атака враховує, що порушник, враховуючи відомості зі спрямованої атаки, яка базується на інформації про раніше підписані повідомлення одним і тим самим ЕЦП, може обирати публічний ключ і повідомлення з підписом. Обирати наступне повідомлення можливе на основі знань про ймовірний підпис попереднього.

Для криптографічних алгоритмів, що застосовуються у процесі підпису повідомлення із застосуванням ЕЦП, існують наступні види загроз цілісності інформації:

– Підробка екзистенційного виду;

Атака полягає у підробці порушником цифрового підпису на випадкове повідомлення, що було надане підписувачем.

– Підробка вибіркового виду;

Атака полягає у підробці порушником цифрового підпису на заздалегідь визначене повідомлення, що було надане підписувачем.

– Підробка універсального виду;

Атака полягає у визначенні порушником алгоритму створення цифрового підпису, що за своїм походженням може бути прирівняний до оригінального ЕЦП, з або без використання закритого ключа.

– Тотальне розкриття.

Атака полягає у визначенні порушником усіх можливих даних про цифровий підпис підписувача, включаючи закритий ключ, що відповідає публічному ключу. Надалі у розпорядженні порушника є можливості накладання скомпрометованого цифрового підпису на будь-які інші повідомлення, публікуючи їх від ім'я жертви.

Порушник має на меті досягнення певних цілей, зокрема скомпрометувати ІС. Компрометація даних може досягти визначення закритого ключа підписувача або підробку підписаних повідомлень.

Застосувавши певні зусилля, порушник також може досягти компрометації даних про застосовані у процесі формування підпису криптографічні алгоритми, визначивши увесь принцип роботи системи. Для того, щоб порушнику досягти такої мети, йому потрібно розраховувати та передбачати великий обсяг математичних обчислень, які є важкими для прорахунку. Якщо порушник не здатний до здійснення такої роботи, імовірність досягнення його мети може вважатись мінімальною.

Відповідно до зазначених типів атак, варто класифікувати їх за складністю криптоаналізу цифрового підпису.

У випадку коли порушник зміг здійснити атаку типу «тотального розкриття», необхідним для нього є і вміння здійснювати інші види атак із додатковою складністю.

Так само вважається і для атаки типу «універсальної підробки». Якщо порушник вдалось її здійснити, то для нього є необхідним і вміння здійснювати інші види атак із додатковою складністю.

У випадку, якщо порушник зміг здійснити атаку типу «вибіркової підробки», то для нього є необхідним вміння здійснювати атаки не важче, ніж із додатковою складністю.

На рисунку 2.6 зображено модель, яка визначає необхідні для порушника знання здійснення наведених типів підробки.

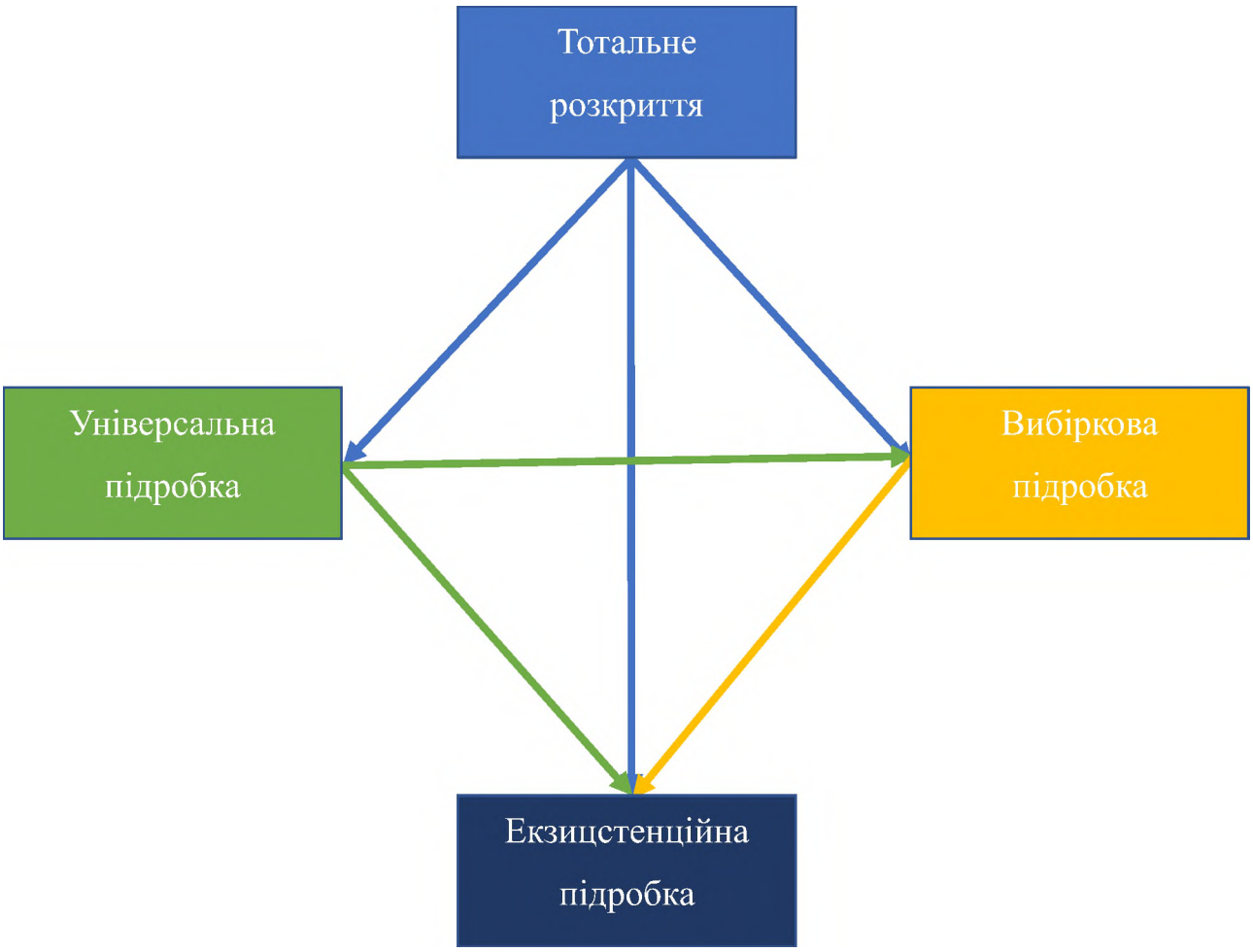

Рисунок 2.6 – Модель атак на алгоритми ЕЦП

Зв’язки на моделі атак відображають реальні можливості порушниках у випадках, коли він є спроможним на виконання тієї чи іншої атаки. Отже порушник, що здійснює атаку типу «вибіркової підробки» не обов’язково буде спроможним здійснити атаку «універсальної підробки», але має бути

спроможним здійснювати атаку типу «екзистенційної підробки», оскільки в іншому випадку це не вважається можливим за недостатності необхідного рівня знань та/або технічних засобів.

Варто розглянути модель, у якій дії порушника існують в умовах взаємодії підписувача і отримувача. Така модель є узагальненою і включає в себе критичні умови взаємодії, оскільки будь-яка зі сторін може виступати порушником. У такий спосіб не можна враховувати довірчі відносини між двома суб'єктами даної моделі і основне завдання захисту лежить лише на криптографічній стійкості алгоритмів застосованого електронного цифрового підпису.

Суб'єкти моделі:

– Підписувач;

– Отримувач;

– Порушник.

Загрози, що надходять від підписувача:

1. Підписувач не передає повідомлення в мережу у відповідь на запит цього повідомлення.

2. Підписувач робить вигляд, що передає повідомлення в мережу у відповідь на запит цього повідомлення.

3. Підписувач підробляє час, в який було надіслано повідомлення отримувачу.

4. Підписувач підробляє повідомлення і надсилає в мережу інформацію, відмінну від тієї, що запитувалась.

Загрози, що надходять від отримувача:

1. Отримувач створює довільне повідомлення та видає його за таке, що було надіслане від підписувача.

2. Отримувач підробляє час, в який було отримане повідомлення від підписувача.

3. Отримувач відхиляє запит на отримання електронного повідомлення від підписувача.

Загрози, що надходять від порушника:

1. Порушник імітує помилковість повідомлення, що було надіслано отримувачу від підписувача у процесі передачі інформації.

2. Порушник модифікує оригінальне повідомлення, що було надіслано отримувачу від підписувача у процесі передачі інформації.

3. Порушник повторно надсилає повідомлення отримувачу, яке до цього вже було отримане ним від підписувача.

Ця модель може існувати і за умов додаткового суб'єкта як випадковий оракул.

Випадковий оракул – ідеалізована хеш-функція, яка виробляє випадкову відповідь на кожен новий запит, рівномірно розподілену по діапазону значень з умовою, що якщо один і той самий запит надходить двічі, то відповідь має бути однаковою. Іншими словами, випадковий оракул це математична функція, що відображає кожен можливий запит у фіксовану випадкову відповідь із заздалегідь існуючої області відповідей.

Випадковий оракул має три властивості: детермінованість, ефективність і забезпечення рівномірного розподілу отриманих значень.

За існування випадкового оракула у вищенаведеній моделі загроз, кожен суб'єкт має доступ до нього. У стандартному процесі створення цифрового підпису порушник не має доступу до оракула, а всі інші можуть із ним взаємодіяти використовуючи класичні бітові рядки. На вхід завжди надходить один бітовий рядок, який виступає аргументом, а на вихід інший, що представляє вихідне число.

2.8 Політика безпеки

Розробка політики безпеки для електронного цифрового підпису є необхідною при його використанні в межах приватних підприємств, державних установ тощо.

Оскільки електронний цифровий підпис взаємодіє із конфіденційною інформацією громадян та ідентифікує особу за її даними, ці дані повинні бути надійно захищеними як технічно, так і з боку правових відносин.

Загальні відомості:

1. Організації та урядові установи не можуть використовувати електронний цифровий підпис для підпису неоригінальних електронних документів неоригінального походження.

2. Організації та урядові установи можуть отримувати послуги електронного цифрового підпису лише від кваліфікованих центрів сертифікації.

3. Обмін інформацією між кваліфікованими центрами сертифікації і організаціями та урядовими установами може здійснюватися лише через електронну мережу.

Організаційна структура:

1. За організацію використання електронного цифрового підпису несе відповідальність керівник організації та урядової установи у випадках не встановлених законодавством.

2. Використання та управління системою електронного цифрового підпису в організаціях та державних установах повинен забезпечувати відділ інформаційних технологій.

3. Відділ інформаційних технологій організації та урядової установи має призначити керівника відділу, адміністратора системи обробки персональних даних, адміністратора системи моніторингу та залучати фахівців з інформаційної безпеки для періодичної перевірки загальноприйнятих умов використання електронного цифрового підпису.

Керівник відділу інформаційних технологій має здійснювати контроль роботи працівників свого відділу, видавати накази про вдосконалення системи безпеки та залучати фахівців з інформаційної безпеки.

Адміністратор системи обробки персональних даних має дотримуватись правил взаємодії з персональними даними, встановлених законодавством, здійснювати контроль достовірності надання персональних даних користувачами, надавати рекомендації про вдосконалення системи безпеки.

Адміністратор системи моніторингу має здійснювати постійний контроль за станом системи безпеки електронного підпису, своєчасно реагувати на можливі кіберінциденти пов'язані з порушенням безпеки, надавати рекомендації про вдосконалення системи безпеки.

4. Відділ інформаційної безпеки має щоденно надавати звітність про стан системи безпеки електронного цифрового підпису.

5. Співробітники відділу інформаційної безпеки повинні проходити щорічну зовнішню сертифікацію для підтвердження своєї кваліфікації з інформаційної безпеки.

6. Співробітники відділу інформаційної безпеки повинні періодично проходити навчання на підвищення своєї кваліфікації.

7. Відділ з інформаційної безпеки має розробити політику конфіденційності даних з якими взаємодіє електронний цифровий підпис.

8. Відділ з інформаційної безпеки повинен мати чітко встановлену ієрархію повноважень доступу до системи безпеки електронного цифрового підпису.

Використання та управління ключами:

1. Генерація криптографічних ключів має здійснюватися згідно встановлених міжнародних стандартів використання криптографічних алгоритмів на апаратних засобах з кваліфікованим рівнем захисту.

2. Приватні ключі повинні зберігатися на апаратних засобах з кваліфікованим рівнем захисту.

3. Публічні ключі повинні надаватися лише відповідним кваліфікованим центрам сертифікації.

4. Доступ до приватних ключів має бути обмежений для співробітників інших відділів організації та співробітників без повноважень на такий доступ, використовуючи системи автентифікації.

5. Забороняється передача та надсилання приватних ключів електронного цифрового підпису.

6. Приватні ключі мають зберігатись у зашифрованому вигляді та мати алгоритми розшифрування лише для випадків застосування електронного цифрового підпису. При застосуванні електронного підпису приватний ключ повинен надсилатись до криптографічних примітивів по закритих каналах.

7. Резервне копіювання приватних та публічних ключів має періодично здійснюватися і зберігатися на зашифрованих носіях інформації. Забороняється зберігання приватних і публічних ключів на одному носії інформації.

8. Доступ до резервних копій має бути обмежений для співробітників інших відділів організації та співробітників без повноважень на такий доступ, використовуючи системи автентифікації.

9. У випадках компрометації приватних ключів, електронні цифрові підписи, пов'язані із цими ключами, мають бути негайно анульовані. Надання інформації стосовно таких інцидентів керівництву організації є обов'язковим.

10. Приватні та публічні ключі повинні періодично змінювати місце зберігання для запобігання можливих атак та інцидентів компрометації.

11. Мають бути встановлені процедури безпечного знищення приватних та публічних ключів.

Забезпечення безпеки системи ЕЦП:

1. Мають бути встановлені механізми контролю доступу до систем електронного цифрового підпису з мультифакторною автентифікацією співробітників організації.

2. Мають бути встановлені чіткі повноважень доступу до систем електронного цифрового підпису.

3. Обов'язкове ведення постійного запису дій в системі електронного цифрового підпису та спроб отримання доступу до цієї системи.

4. Контроль за цілісністю систем електронного цифрового підпису повинен здійснюватися вповноваженими особами організації.

5. Забезпечити системам електронного цифрового підпису надійний фізичний захист на серверному обладнанні, апаратних модулях безпеки тощо.

6. Запровадити методи і засоби захисту у випадку спроб компрометації даних про систему електронного цифрового підпису та успішних атаках на систему.

7. Запровадити методи і засоби відновлення системи електронного цифрового підпису у випадках успішних атак на систему, що призвело до її непрацездатності.

8. Обмежити доступ до приміщень, встановити систему сигналізації у приміщеннях з серверним обладнанням, апаратними модулями безпеки, фізичними носіями інформації про систему електронного цифрового підпису особам без відповідних на це повноважень.

9. Запровадити системи автономного моніторингу та виявлення вразливостей системи електронного цифрового підпису.

10. Проводити постійні тести на вразливості системи електронного цифрового підпису.

11. Використовувати лише ліцензоване програмне забезпечення у системах електронного цифрового підпису.

12. Проводити регулярне оновлення програмного забезпечення у системах електронного цифрового підпису.

13. Проводити періодичне резервне копіювання даних та конфігурацій системи електронного цифрового підпису на зашифрованих фізичних носіях інформації.

Управління інцидентами та реагування:

1. Розробити модель порушника та модель загроз із урахуванням усіх можливих інцидентів несанкціонованого доступу до системи електронного цифрового підпису.

2. Запровадження системи постійного моніторингу за станом безпеки системи електронного цифрового підпису.

3. Вести постійний запис стану безпеки системи електронного цифрового підпису.

4. Розробити чіткий план реагування на помилковість, компрометацію, спроби отримання доступу до системи електронного цифрового підпису.

5. Проводити аналіз минулих інцидентів, що призвели до порушення стабільного функціонування системи електронного цифрового підпису.

6. Проводити оповіщення співробітників, клієнтів та відповідних державних установ про інциденти порушення стабільного функціонування системи електронного цифрового підпису.

7. Зберігати докази про інциденти порушення стабільного функціонування системи електронного цифрового підпису.

8. Проводити періодичні опитування співробітників із доступом до системи електронного цифрового підпису щодо їх дій у випадках інцидентів порушення стабільного функціонування системи.

Відповідальність та санкції:

1. Розробити правила та процедури, що визначатимуть відповідальність кожного співробітника із доступом до системи електронного цифрового підпису.

2. Проводити постійний контроль за дотриманням встановлених правил співробітниками із доступом до системи електронного цифрового підпису.

3. Проводити тестування співробітників із доступом до системи електронного цифрового підпису щодо обізнаності про правила взаємодії із системою.

4. Запровадити дисциплінарні стягнення за невиконання встановлених вимог взаємодії із системою електронного цифрового підпису.

5. Запровадити юридичну відповідальність за невиконання встановлених вимог взаємодії із системою електронного цифрового підпису.

6. Запровадити фінансові стягнення за невиконання встановлених вимог взаємодії із системою електронного підпису, псування організаційних матеріальних активів.

7. Зберігати докази про невиконання встановлених вимог взаємодії із системою електронного цифрового підпису.

Оновлення політики безпеки:

1. Встановити графік перегляду політики безпеки електронного цифрового підпису.

2. Проводити адаптацію політики безпеки під існуючі ризики загроз та актуальні системи електронного цифрового підпису.

3. Проводити інформування співробітників стосовно змін політики безпеки електронного цифрового підпису.

2.9 Висновок

У поточному розділі кваліфікаційної роботи було розглянуто основні сфери застосування електронного цифрового підпису в межах організацій та державних установ. На сьогоднішній день люди активно користуються електронними послугами та цифровими підписами. Зокрема, цифровий підпис знайшов своє призначення у системах електронного документообігу, чим значно пришвидшив бюрократичні процедури фізичних та юридичних осіб.

Також було детально розібрано криптографічні алгоритми та цифрові сертифікати, які використовуються у системах електронного цифрового підпису. Математичними формулами було зображено їх криптографічну стійкість та проаналізовано можливі ризики витоку інформації з їх примітивів.

Модель порушника та модель загроз показали імовірні можливості для криптоаналітиків до аналізу даних, які можуть бути доступними у різних умовах. Хоча цифровий підпис і надалі продовжує розвиватися, його використання на сьогоднішній день цілком можна вважати безпечним.

Розроблено політику безпеки для організацій та державних установ, що може бути впроваджена до використання систем електронного цифрового підпису. Надані рекомендації із заходів безпеки допоможуть керівникам установ організувати безпечні умови його застосування.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Економічна ефективність розробки політики безпеки

Для впровадження процесу розробки і подальшого його застосування в системі ІКС потрібно розрахувати фінансові витрати на етапах її створення, щоб зрозуміти доцільність розробки в рамках економічного розгляду поставленого питання. У економічній моделі варто враховувати витрати капітального вкладення і поточні.

Капітальні витрати здійснюються на етапах розробки політики безпеки, а поточні будуть реалізовуватись у процесі майбутнього функціонування системи. Також буде враховуватись підтримка технічної частини, базуючись на конкретних платформах її розташування.

Економічні розрахунки в даному розділі покажуть ефективність використання розробки кваліфікаційної роботи та подальшого впровадження системи у сфері електронних цифрових підписів.

3.2 Розрахунок капітальних витрат

На першому етапі створення економічної моделі потрібно визначити трудомісткість розробки політики безпеки та розрахувати витрати на її розробку. Трудомісткість розробки політики безпеки розраховується за наступною формулою:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д} \qquad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки, год;

$t_{в}$ – тривалість розробки політики безпеки, год;

$t_{а}$ – тривалість аналізу ризиків, год;

$t_{вз}$ – тривалість визначення вимог до засобів захисту, год;

$t_{озб}$ – тривалість вибору основних рішень із забезпечення безпеки, год;

$t_{овр}$ – тривалість виконання відновлювальних робіт і забезпечення

безпеки, год;

$t_д$ – тривалість оформлення документів політики безпеки, год.

За розрахунками (3.2) визначено трудомісткість розробки політики безпеки:

$$t = 3 + 18 + 42 + 12 + 24 + 8 + 8 = 115 \text{ год} \quad (3.2)$$

Надалі будуть розраховані витрати на створення політики безпеки за формулою (3.3):

$$K_{рп} = З_{зп} + З_{мч} \quad (3.3)$$

де $З_{зп}$ – заробітна плата фахівця з інформаційної безпеки, грн.;

$З_{мч}$ – вартість витрат машинного часу на розробку, грн..

Заробітна плата фахівця з інформаційної безпеки розраховується за формулою (3.4):

$$З_{зп} = З_{іб} \cdot t \quad (3.4)$$

де $З_{іб}$ – середньогодинна заробітна плата фахівця з інформаційної безпеки, грн./год;

t – тривалість розробки політики безпеки, год.

За наступними розрахунками вирахувано заробітну плату фахівця з інформаційної безпеки:

$$З_{зп} = 125 \cdot 115 = 14375 \text{ грн.} \quad (3.5)$$

Вартість витрат машинного часу на розробку політики безпеки розраховується за формулою (3.6):

$$З_{мч} = С_{мч} \cdot t \tag{3.6}$$

де $С_{мч}$ – вартість однієї години роботи ПК, грн./год;

t – трудомісткість розробки політики безпеки на ПК, год.

Вартість однієї години машинного часу ПК розраховується за формулою (3.7):

$$С_{мч} = Р \cdot С_{е} + \frac{Ф_{зал} \cdot Н_{а}}{F_{р}} + \frac{К_{лпз} \cdot Н_{апз}}{F_{р}} \tag{3.7}$$

де Р – потужність ПК, кВт/год;

$С_{е}$ – тариф на електроенергію, грн./кВт·год;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_{а}$ – річна норма амортизації ПК, частка одиниці;

$Н_{апз}$ – річна норма амортизації ліцензійного ПЗ, частка одиниці;

$К_{лпз}$ – вартість ліцензійного ПЗ, грн.;

$F_{р}$ – річний фонд робочого часу.

За наступними розрахунками визначено вартість однієї години машинного часу ПК:

$$\begin{aligned} С_{мч} &= 0{,}041 \cdot 4{,}32 + \frac{7200 \cdot 0{,}2}{1920} + \frac{2000 \cdot 0{,}1}{1920} = \\ &= 0{,}17712 + 0{,}75 + 0{,}104 = 1{,}03 \text{ грн.} \end{aligned} \tag{3.8}$$

За наступними розрахунками визначено вартість витрат машинного часу на розробку політики безпеки:

$$З_{мч} = 1{,}03 \cdot 115 = 118{,}45 \text{ грн.} \quad (3.9)$$

За наступними розрахунками визначено витрати на створення політики безпеки:

$$К_{рп} = 14375 + 118{,}45 = 14493{,}45 \text{ грн.} \quad (3.10)$$

Капітальні витрати на створення та застосування політики інформаційної безпеки розраховуються за формулою (3.11):

$$К = К_{пр} + К_{зпз} + К_{рп} + К_{то} + К_{навч} + К_{н} \quad (3.11)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки із залученням зовнішніх консультантів, грн.;

$К_{зпз}$ – вартість закупівель програмного забезпечення, грн.;

$К_{пз}$ – вартість розробки політики безпеки, грн.;

$К_{то}$ – вартість закупівлі технічного обладнання, грн.;

$К_{навч}$ – вартість навчання фахівців з інформаційної безпеки, грн.;

$К_{н}$ – вартість роботи зі встановлення обладнання та налагодження системи, грн..

За наступними розрахунками визначено капітальні витрати на створення та застосування політики інформаційної безпеки:

$$К = 120000 + 2000 + 14494 + 30000 + 0 + 1400 = 167894 \text{ грн.} \quad (3.12)$$

Отже, капітальні витрати на створення та застосування політики інформаційної безпеки становлять приблизно 168 тис. грн.

3.2 Визначення поточних витрат

Поточні витрати – витрати, що йдуть на використання (експлуатацію) обслуговування технічного обладнання, а також заробітну плату персоналу за постійний контроль його стану, за визначений період часу.

Річні поточні витрати на експлуатацію системи інформаційної безпеки розраховуються за формулою (3.13):

$$C = C_в + C_к + C_{ак} \tag{3.13}$$

де $C_в$ – витрати на відновлення й модернізацію системи інформаційної безпеки, грн.;

$C_к$ – витрати на керування системою інформаційної безпеки, грн.;

$C_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки, грн.;

Витрати на керування системою інформаційної безпеки розраховуються за формулою (3.14):

$$C_к = C_н + C_а + C_з + C_{єв} + C_{ел} + C_о + C_{тос} \tag{3.14}$$

де $C_н$ – витрати на навчання адміністративного персоналу й кінцевих користувачів, грн.;

$C_а$ – річний фонд амортизаційних відрахувань, грн.;

$C_з$ – річний фонд заробітної плати інженерно-технічного персоналу, грн.;

$C_{єв}$ – державний єдиний внесок на соціальне страхування, грн.;

$C_{ел}$ – вартість електроенергії, грн.;

$С_о$ – витрати на залучення сторонніх організацій, грн.;

$С_{тос}$ – витрати на технічне й організаційне адміністрування, грн..

Річний фонд заробітної плати інженерно-технічного персоналу розраховується за формулою (3.15):

$$С_з = З_{осн} + З_{дод} \quad (3.15)$$

де $З_{осн}$ – основна заробітна плата, грн./рік;

$З_{дод}$ – додаткова заробітна плата, грн./рік.

За наступними розрахунками визначено річний фонд заробітної плати інженерно-технічного персоналу:

$$С_з = 204000 + 20400 = 224400 \text{ грн.} \quad (3.16)$$

Вартість електроенергії, що споживається апаратурою системи безпеки розраховується за формулою (3.17):

$$С_{ел} = Р \cdot F_р \cdot Ц_е \quad (3.17)$$

де Р – потужність обладнання інформаційної безпеки, кВт/год;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки, год;

$Ц_е$ – тариф на електроенергію, грн./кВт·год.

За наступними розрахунками визначено вартість електроенергії, що споживається апаратурою системи безпеки:

$$C_{ел} = 2 \cdot 8760 \cdot 4{,}32 = 75686{,}4 \text{ грн.} \quad (3.18)$$

За наступними розрахунками визначено витрати на керування системою інформаційної безпеки:

$$C_к = 18000 + 10000 + 224400 + 26400 + \\ + 75686 + 80000 + 5037 = 439523 \text{ грн.} \quad (3.19)$$

За наступними розрахунками визначено річні поточні витрати на експлуатацію системи інформаційної безпеки:

$$C = 114660 + 439523 + 200655 = 754838 \text{ грн.} \quad (3.20)$$

Отже, річні поточні витрати на експлуатацію системи інформаційної безпеки становлять 754 тис. грн.

3.3 Оцінка ймовірних збитків від атак на системі інформаційної безпеки

При застосуванні заходів і засобів з інформаційної безпеки потрібно враховувати і можливі збитки, що можуть бути спричинені ймовірними атаками на системи захисту. Величину, що характеризує такі збитки, називають відверненими втратами. Вона відображає частину прибутку, яку була втрачена.

3.3.1 Оцінювання величини збитку

Упущена вигода від простою атакованого вузла або сегмента системи безпеки розраховується за формулою (3.21):

$$U = П_п + П_в + V \quad (3.21)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента системи безпеки, грн.;

$П_в$ – вартість відновлення працездатності вузла або сегмента системи безпеки, грн.;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента системи безпеки, грн..

Втрати робочого часу та простої співробітників атакованого вузла або сегмента системи безпеки розраховуються за формулою (3.22):

$$П_п = \frac{\sum З_с}{F} \cdot t_п \qquad (3.22)$$

де $З_с$ – втрати на заробітні плати співробітників, грн.;

$t_п$ – час простою, год;

F – місячний фонд робочого часу, год.

За наступними розрахунками визначено втрати робочого часу та простої співробітників атакованого вузла або сегмента системи безпеки:

$$П_п = \frac{23000}{176} \cdot 72 = 9409{,}1 \text{ грн.} \qquad (3.23)$$

Витрати на відновлення працездатності вузла або сегмента системи безпеки розраховуються за формулою (3.24):

$$П_в = П_{ви} + П_{пв} + П_{зч} \qquad (3.24)$$

де $П_{ви}$ – витрати на повторне введення інформації, грн.;

$П_{ви}$ – витрати на відновлення вузла або сегмента системи безпеки, грн.;

$П_{ви}$ – вартість заміни устаткування або запасних частин, грн..

Витрати на повторне введення інформації розраховуються за формулою (3.25):

$$П_{ви} = \frac{\sum З_с}{F} \cdot t_{ви} \qquad (3.25)$$

де $З_с$ – заробітна плата співробітників, що займаються відновленням інформації атакованого вузла або сегмента системи безпеки, грн.;

$t_{ви}$ – час на відновлення інформації атакованого вузла або сегмента системи безпеки, грн..

За наступними розрахунками визначено витрати на повторне введення інформації:

$$П_{ви} = \frac{13800}{176} \cdot 168 = 13172{,}8 \text{ грн.} \qquad (3.26)$$

Витрати на відновлення вузла або сегмента системи безпеки розраховуються за формулою (3.27):

$$П_{пв} = \frac{\sum З_о}{F} \cdot t_в \qquad (3.27)$$

де $З_о$ – середньогодинна заробітна плата співробітників обслуговуючого персоналу, грн.;

$t_в$ – час відновлення після атаки, год.

За наступними розрахунками визначено витрати на відновлення вузла або сегмента системи безпеки:

$$П_{пв} = \frac{1130}{176} \cdot 72 = 462{,}3 \text{ грн.} \quad (3.28)$$

За наступними розрахунками визначено витрати на відновлення працездатності вузла або сегмента системи безпеки:

$$П_в = 13172{,}8 + 462{,}3 + 0 = 13635{,}1 \text{ грн.} \quad (3.29)$$

Втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента системи безпеки розраховуються за формулою (3.30):

$$V = \frac{O}{F_г} \cdot t_{заг} \quad (3.30)$$

де О – середньогодинний обсяг прибутку, грн.;

$F_г$ – річний фонд часу роботи організації, год;

$t_{заг}$ – загальний час простою атакованого вузла або сегмента системи безпеки, год.

За наступними розрахунками визначено втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента системи безпеки:

$$V = \frac{41624}{2080} \cdot 168 = 3361{,}9 \text{ грн.} \quad (3.31)$$

За наступними розрахунками визначено упущену вигоду від простою атакованого вузла або сегмента системи безпеки:

$$U = 9409,1 + 13635,1 + 3361,9 = 26406,1 \text{ грн.} \quad (3.32)$$

Загальний збиток від атаки на вузол або сегмент системи безпеки розраховується за формулою (3.33):

$$B = \sum_i \sum_n U \quad (3.33)$$

де i – число атакованих вузлів або сегментів корпоративної мережі, одиниці;

n – середнє число атак на рік, одиниці;

За наступними розрахунками визначено загальний збиток від атаки на вузол або сегмент системи безпеки:

$$B = 6 \cdot 16 \cdot 26406,1 = 2534985,6 \text{ грн.} \quad (3.34)$$

3.3.2 Загальний ефект від впровадження системи безпеки

Загальний ефект від впровадження системи безпеки розраховується за формулою (3.35):

$$E = B \cdot R - C \quad (3.35)$$

де B – загальний збиток від атаки на вузол або сегмент системи безпеки, тис. грн.;

R – очікувана ймовірність атаки на вузол або сегмент системи безпеки,

частка одиниці.;

С – щорічні витрати на експлуатацію системи безпеки, тис. грн..

За наступними розрахунками визначено загальний ефект від впровадження системи безпеки:

$$E = 2534985,6 \cdot 0,35 - 754838 = 132406,96 \text{ грн.} \quad (3.36)$$

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінювання економічної ефективності системи безпеки інформації здійснюється на основі показників:

- коефіцієнту повернення інвестицій;
- терміну окупності капітальних інвестицій.

Коефіцієнт повернення інвестицій розраховується за формулою (3.37):

$$ROSI = \frac{E}{K} \quad (3.37)$$

де Е – загальний ефект від впровадження системи безпеки, тис. грн.;

К – капітальні витрати на створення та застосування системи безпеки, тис. грн..

За наступними розрахунками визначено капітальні витрати на створення та застосування системи безпеки:

$$ROSI = \frac{132406,96}{167894} = 0,78 \text{ часток одиниць} \quad (3.38)$$

Термін окупності капітальних інвестицій розраховується за формулою (3.39):

$$T_o = \frac{1}{ROSI} \tag{3.39}$$

За наступними розрахунками визначено термін окупності капітальних інвестицій:

$$T_o = \frac{1}{0,78} = 1,28 \text{ років} \tag{3.40}$$

Отже, окупність розробленої системи безпеки складає 1,28 років, а саме 16 місяців.

3.5 Висновок

Ефективність розробленої моделі політики безпеки є ефективною відносно до фінансових інвестицій, що доведено розрахунками економічних показників. Це доводить доцільність використання об'єкту розробки для підприємств, державних установ, фізичних та юридичних осіб.

Капітальні витрати на створення та застосування політики інформаційної безпеки електронного цифрового підпису становлять близько ста шістдесяти дев'яти тисяч гривень.

Річні поточні витрати на експлуатацію системи інформаційної безпеки становлять близько семисот п'ятдесяти чотирьох тисяч гривень.

Термін окупності капітальних інвестицій становить 16 місяців.

Наведені економічні розрахунки можуть мати відхилення від реальних умов застосування системи безпеки електронного цифрового підпису, на що впливають умови її застосування в межах конкретних підприємств та організацій.

ВИСНОВКИ

На сьогоднішній день електронний цифровий підпис має широке застосування у сферах надання електронних послуг та системах електронного документообігу. Постійний розвиток криптографічної стійкості дає можливості для майбутнього викорінення паперової документації, що знайде позитивний вплив на екологію, витрати часу та універсальності.

Нажаль, суспільство ще не готове сприймати такі досягнення розвитку інформаційних технологій та цілком довіритись цифровим даним. Авжеж, кожна інформація може піддатись компрометації та викраденню зловмисників, але це стосується як цифрового, так і реального світу.

Описані в кваліфікаційній роботі дослідження допоможуть керівникам установ та їх клієнтам більш детально поринути у принципи роботи систем електронного цифрового підпису та зрозуміти ефективність їх використання у повсякденному житті. Не дивлячись на те, що послугами ЕЦП людство може користуватись і зараз, це все ж таки залишається майбутнім.

Над алгоритмами цифрового підпису ще потрібно багато працювати, проводити постійні тести, аналізувати ризики та економічну ефективність використання. Те, що можна затверджувати точно – цифровий підпис є найефективнішою моделлю ідентифікації.

Розроблена в кваліфікаційній роботі політика безпека регулює правила відносин між спеціалістами з інформаційної безпеки та системою електронного цифрового підпису. Збереження конфіденційності персональних даних – основний критерій безпеки, на якому базується ЕЦП.

ПЕРЕЛІК ПОСИЛАНЬ

1. НІСД: стаття «Круглий стіл «СЕД в УКРАЇНІ: сучасний стан та перспективи розвитку», 2011. URL: https://niss.gov.ua/news/novini-nisd/krugliy-stil-sed-v-ukraini-suchasniy-stan-ta-perspektivi-rozvitku

2. Мінгальова Ю.І. Електронний цифровий підпис як головний елемент електронного документообігу, 2013. URL: http://eprints.zu.edu.ua/13979/1/Mingaleva1.pdf

3. Вікіпедія. Вільна енциклопедія: Криптографія. URL: https://uk.wikipedia.org/wiki/Криптографія

4. Аналітичний звіт «Думки і погляди населення України щодо державних електронних послуг», 2023. URL: https://www.undp.org/uk/ukraine/publications/analitychnyy-zvit-dumky-i-pohlyady-naselennya-ukrayiny-shchodo-derzhavnykh-elektronnykh-posluh

5. УЖНУ: Лекція. Технології захисту інформації. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186

6. Вікіпедія. Вільна енциклопедія: Шифрування з симетричними ключами. URL: https://uk.wikipedia.org/wiki/Шифрування_з_симетричними_ключами

7. Classmill: 11 клас Інформатика: Криптографічні методи захисту інформації. Контроль цілісності програмних та інформаційних ресурсів, 2020. URL: https://classmill.com/659/112/m/xnb7A

8. Альбрехт Й.О. Система аутентифікації на базі еліптичних кривих з використанням векторних операцій, 2018. URL: https://ela.kpi.ua/handle/123456789/25522

9. Вікіпедія. Вільна енциклопедія: Advanced Encryption Standard. URL: https://uk.wikipedia.org/wiki/Advanced_Encryption_Standard

10. Гринюк С., Поліщук М. Використання технології шифрування інформації для безпечної передачі в мережі, 2020. URL: https://doi.org/10.36910/6775-2524-0560-2020-39-21

11. Вікіпедія. Вільна енциклопедія: Потоковий шифр. URL:

https://uk.wikipedia.org/wiki/Потоковий_шифр

12. Вікіпедія. Вільна енциклопедія: Асиметричні алгоритми шифрування. URL: https://uk.wikipedia.org/wiki/Асиметричні_алгоритми_шифрування

13. Кушнір В.П. Розробка методів ключового хешування з використанням арифметики еліптичних кривих, 2021. URL: http://elartu.tntu.edu.ua/handle/lib/35549 (дата звернення: 30.06.2024).

14. Вікіпедія. Вільна енциклопедія: RSA. URL: https://uk.wikipedia.org/wiki/RSA

15. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» №45, 2017. URL: https://zakon.rada.gov.ua/laws/show/2155-19

16. Міністерство цифрової трансформації. Центральний засвідчувальний орган. Електронний реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів. URL: https://czo.gov.ua/ca-registry?

17. ZEN: Електронний цифровий підпис (ЕЦП): що це та як створити. URL: https://www.zen.com/uk/blog/business-uk/electronic-digital-signature/

18. Вікіпедія. Вільна енциклопедія: Електронний цифровий підпис. URL: https://uk.wikipedia.org/wiki/Електронний_цифровий_підпис

19. Плотніков В.М., Борцова Ю.В. Алгоритмізація шифрування цифрого підпису, 2020. URL: https://doi.org/10.15673/atbp.v12i1.1703

20. Вікіпедія. Вільна енциклопедія: Цифровий сертифікат. URL: https://uk.wikipedia.org/wiki/Цифровий_сертифікат

21. Плотніков В.М., Борцова Ю.В. Захист даних засобом цифрового підпису, 2020. URL: https://doi.org/10.15673/atbp.v11i4.1599

22. Вікіпедія. Вільна енциклопедія: PGP. URL: https://uk.wikipedia.org/wiki/PGP

23. Wikipedia. The Free Encyclopedia: X.509. URL: https://en.wikipedia.org/wiki/X.509 - Structure_of_a_certificate

24. Полуніна О.О. ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС (ЕЦП) В IT-ENTERPRISE, 2020. URL: https://doi.org/10.32837/chc.v0i34.172

25. Wikipedia. The Free Encyclopedia: ElGamal signature scheme. URL:

https://en.wikipedia.org/wiki/ElGamal_signature_scheme

26. NIST 800-90A. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

27. Вікіпедія. Вільна енциклопедія: Elliptic Curve Digital Signature Algorithm. URL: https://uk.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm

28. Полехіна Ю.М., Тимофєєв Д.С. Модель порушника. Мета та принципи розробки, м. Дніпро. URL: https://www.rusnauka.com/11_EISN_2010/Informatica/63866.doc.htm

29. Пілова Д.П. НТУ«ДП». Методичні вказівки до виконання економічної частини дипломного проекту, м. Дніпро, 2019.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	11	
6	А4	2 Розділ	34	
7	А4	3 Розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

ДроботМВ_125-20-1_ПЗ.docx

ДроботМВ_125-20-1_ПЗ.pdf

ДроботМВ_125-20-1_ПЗ.pdf.asice

ДроботМВ_125-20-1_Пр.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку б. («»).

Керівник розділу _____ Дар'я ПІЛОВА

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Обгрунтування політики безпеки при побудові криптографічних алгоритмів електронно-цифрового підпису
студента групи 125-20-1
Дробота Максима Владиславовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 74 сторінках та містить 11 рисунка, 1 таблиці, 29 джерел та 4 додатка.

Метою даної кваліфікаційної роботи є розробка політики безпеки інформації інформаційно-комунікаційної системи електронно-цифрового підпису.

У загальній частині проведені дослідження методів захисту інформації електронно-цифрового підпису в Україні.

У спеціальній частині була розроблена модель порушника, модель загроз та політика безпеки електронного цифрового підпису на основі існуючих криптографічних алгоритмів.

У економічній частині було розраховано економічну ефективність запровадження розробленої політики безпеки електронного цифрового підпису.

Практична цінність розробки полягає у створенні критеріїв та правил щодо захисту систем електронно-цифрового підпису на приватних підприємствах та урядових структурах.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою, відповідає вимогам положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка». Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник роботи,
ас. Олішевський І.Г.