

СИСТЕМИ БАНКІВСЬКОЇ БЕЗПЕКИ

Л. Г. Йона, О. В. Онацький, О. В. Швець

СИСТЕМИ БАНКІВСЬКОЇ БЕЗПЕКИ

Державний університет інтелектуальних технологій і зв'язку

Кафедра кібербезпеки та технічного захисту інформації

Л. Г. Йона, О. В. Онацький, О. В. Швець

СИСТЕМИ БАНКІВСЬКОЇ БЕЗПЕКИ

**Навчальний посібник
з дисципліни
«Системи банківської безпеки»**

для освітньо-професійної підготовки бакалаврів
з галузі знань 12 «Інформаційні технології»
за спеціальністю 125 «Кібербезпека»

Одеса
2022

Рецензент

Захарченко М.В., д.т.н., професор кафедри кібербезпеки та технічного захисту інформації, державного університету інтелектуальних технологій і зв'язку

Йона Л. Г., Онацький О. В., Швець О. В. Системи банківської безпеки: навч. посіб. Одеса: ДУІТЗ, 2022. – 192 с.

ISBN 978-966-413-696-6

Навчальний посібник призначено для студентів, які вивчають дисципліну “Системи банківської безпеки”. Розглянуто методи захисту електронних транзакцій під час еквайрингу, криптографічні методи та апаратні засоби захисту інформації, зокрема методи автентифікації, електронний підпис над полем цілих чисел і у групі точок еліптичних кривих, атаки на схеми електронного підпису.

Схвалено на засіданні кафедри КБ та ТЗІ. Протокол № 4 від 20.11.2020 р.

Затверджено методичною радою ДУІТЗ. Протокол № 1 від 11.03.2021 р.

ISBN 978-966-413-696-6

© Йона Л.Г., Онацький О.В.,
Швець О.В., 2022

© ДУІТЗ, 2022

ЗМІСТ

ВСТУП	5
1 ЗАХИСТ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМАХ	7
1.1 Електронна платіжна система.....	7
1.2 Правові основи діяльності платіжних систем.....	11
1.3 Засоби забезпечення безпеки платіжних систем.....	13
1.4 Платіжні картки та їх класифікація.....	18
1.5 Стандарт безпеки даних індустрії платіжних карток.....	22
1.6 Ідентифікація та автентифікація користувача.....	25
1.6.1 Персональний ідентифікаційний номер.....	27
1.6.2 Схема виведення PIN з номеру рахунку користувача.....	28
1.6.3 Парольні системи захисту.....	29
1.7 Універсальна електронна платіжна система.....	31
1.8 Національна платіжна система «Простір».....	33
2 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЛАТІЖНИХ ТЕРМІНАЛІВ ПІД ЧАС ЕКВАЙРІНГУ	35
2.1 Захист системи POS.....	35
2.2 Захист процесу еквайрингу в банкоматах.....	39
3 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ	44
3.1 Особливості функціонування протоколу SET.....	44
3.2 Протокол захисту інформації в електронних платіжних системах 3-D Secure.....	61
4 КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ	64
4.1 Загальна класифікація криптографічних перетворень.....	64
4.2 Методи автентифікації.....	68
4.3 Електронний підпис.....	80
4.3.1 Основні поняття та визначення.....	80
4.3.2 Вимоги до системи електронного підпису.....	84
4.3.3 Структура системи електронного підпису України.....	85
4.3.4 Методи побудови схем електронного підпису.....	88
4.3.5 Основні поняття та застосування геш-функцій.....	91
4.4 Алгоритм електронного підпису RSA.....	94

4.5 Електронний підпис GQ	97
4.6 Колективний підпис GQ	100
4.7 Електронний підпис на базі шифру Ель-Гамала.....	102
4.8 Електронний підпис Шнорра	104
4.9 Стандарт цифрового підпису DSS.....	106
4.10 Алгоритм електронного підпису Ніберга-Рюпеля з відновленням повідомлення.....	110
4.11 Криптосистема на еліптичних кривих	113
4.12 Алгоритм електронного підпису ECDSA	129
4.13 Алгоритм електронного підпису ECSS.....	133
4.14 Алгоритм електронного підпису EC-GDSA.....	135
4.15 Алгоритм електронного підпису EC-KCDSA	139
4.16 Стандарт електронного підпису ДСТУ 4145–2002	142
4.17 Класифікація атак на схеми електронного підпису.....	151
4.18 Протокол автентифікації з нульовою передачею знань на еліптичній кривій	152
5 АПАРАТНІ ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.....	156
5.1 Засоби криптографічного захисту інформації	156
5.2 Модуль безпеки МБ-2 НБУ	159
5.3 Електронний ключ “Алмаз-1К”	160
5.4 Електронний ключ “Кристал-1”	162
5.5 Криптомодуль “Тряда-61”	164
5.6 Мережний криптомодуль “Тряда-301”	168
5.7 Апаратний генератор випадкових чисел “Тряда-3”	172
5.8 IP-шифратор.....	173
5.9 Шлюз захисту “Бар’єр-301”	177
5.10 Шлюз мережний “Бар’єр-1ЦСК”	179
ЛІТЕРАТУРА.....	182
Додаток А ПЕРЕЛІК СТАНДАРТІВ ТА ТЕХНІЧНИХ СПЕЦИФІКАЦІЙ	185
Додаток Б НЕЗВЕДЕНІ ПОЛІНОМИ НАД ПОЛЕМ ГАЛУА $GF(2)$	189
Додаток В РЕКОМЕНДОВАНІ ПРИМІТИВНІ МНОГОЧЛЕНИ ЗГІДНО ДСТУ 4145–2002	190

ВСТУП

Впродовж останніх років світова банківська система суттєво змінювалася і ці зміни обумовлені глобалізацією фінансових ринків, розвитком інформаційних технологій, збільшенням пропозицій та розширенням асортименту банківських послуг, впровадженням інноваційних технологій в керуванні банками. Інтенсивне використання глобальної мережі виявило проблеми, які пов'язані з інформаційною безпекою, а саме:

- необхідність захисту інформації, що передається комунікаційними каналами;
- забезпечення тривалого зберігання даних в електронному вигляді;
- запобігання несанкціонованого доступу до інформації;
- проведення процедур автентифікації користувачів та повідомлень;
- забезпечення необхідної швидкодії та надійності системи.

Необхідною умовою побудови та функціонування банківської системи є забезпечення її комплексного захисту.

Стрімкий розвиток банківської системи обумовлюється розширенням різноманітних сучасних банківських послуг. Однією із таких послуг є створення систем електронних платежів і розрахунків. Розвиток технологій електронних платежів потребує використання сучасних методів захисту електронних транзакцій в платіжних системах. На сьогодні у світі є значна кількість різноманітних платіжних систем, в яких побудова, технології функціонування та характерні особливості економіки країн суттєво відрізняються. При цьому, платіжні системи є основним каналом, яким можуть передаватися потрясіння на внутрішніх та міжнародних грошових та інших ринках і провокувати системні кризи, що загрожують стабільності цих ринків. Тому ефективність, оперативність, економічність, надійність, безпека та зручність – це основні вимоги як до платіжної системи окремої країни, так і до світової фінансової системи загалом і тому лише електронні платіжні системи, які використовують найсучасніші досягнення техніки і технологій, можуть задовольнити переліченим вимогам. Саме система електронних міжбанківських переказів забезпечує життєдіяльність банківської системи України та є необхідною умовою для успішного розвитку ринкової економіки нашої держави.

На сьогодні форми електронних платежів швидко розвиваються.

На жаль, шахрайські технології боротьби з методами захисту інформації також постійно удосконалюються та іноді дають змогу збільшити вірогідність шахрайських транзакцій. Тому є необхідність безперервного удосконалення протоколів захисту під час Інтернет-еквайрингу.

Захист віддалених банківських транзакцій є дуже актуальним питанням, тому існує значна кількість методів їх захисту. Одним із найнадійніших засобів захисту інформації є використання криптографічних протоколів. За допомогою криптографічних протоколів вирішуються різноманітні завдання, а саме: захист інформації шляхом шифрування; підтвердження дійсності користувача/документа за допомогою протоколів автентифікації; генерація та розподілення ключів.

1 ЗАХИСТ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМАХ

1.1 Електронна платіжна система

Будь-який вид розрахунків за допомогою мережі Інтернет (оплата послуг, покупка або продаж товару чи інформації), потребує легкого універсального способу, який дозволяв би здійснювати зручні, дешеві, швидкі та безпечні електронні транзакції в режимі реального часу.

Технології здійснення електронних платежів постійно розвиваються, так на сьогодні число людей, що здійснюють покупки через Інтернет, перевищила мільярд. Незважаючи на постійне зростання шахрайства, зручність і швидкість здійснення розрахунків за допомогою мережі Інтернет веде до збільшення користувачів Інтернет-еквайрингу. При цьому важливо виконання двох умов: забезпечення необхідного рівня сервісу і гарантування безпеки для всіх учасників процесу здійснення платежів через мережу Інтернет за допомогою пластикової картки. Все це потребує використання сучасних методів захисту електронних транзакцій.

Розвинення технологій електронних платежів вимагає удосконалення методів забезпечення безпеки електронних платіжних систем. Перш, ніж розпочати розгляд методів захисту електронних платежів, необхідно розібратися з основними поняттями платіжної системи.

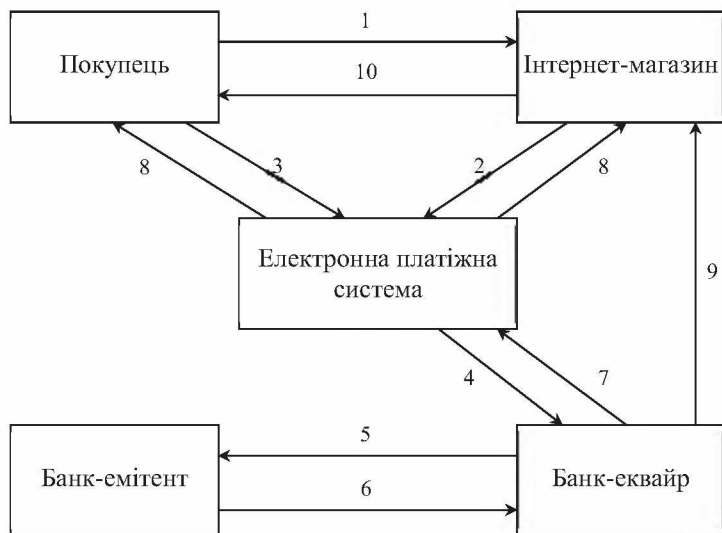
Електронна платіжна система (ЕПС) – це є система, де як платіжний інструмент використовуються пластикові картки.

Платіжна система може здійснювати операції як за допомогою готівки, так і безготівковими засобами. Вона є невід'ємним елементом економічних операцій, що стосуються обміну грошової вартості в обмін на товар, послугу або фінансовий актив. Тому платіжну систему можна надати у вигляді системи механізмів, які служать для переказу грошових коштів між суб'єктами господарювання та для розрахунку за платіжними зобов'язаннями, що виникають між ними.

Існує багато різних електронних платіжних систем, серед них Visa, MasterCard, EasyPay, Portmone, iPay та ін. Проте не можна назвати таку систему, яка б домінувала в різних напрямках, тому готівки та кредитні картки використовуються разом з електронними аналогами. В Україні

найпоширенішими є системи Visa та MasterCard. Корпорації Visa та MasterCard постійно розробляють інноваційні рішення на основі даних і аналітичних висновків, щоб підвищити безпеку і захищеність електронних платежів.

Схема роботи електронної платіжної системи показана на рис. 1.1.



- | | |
|--------------------------------------|-------------------------|
| 1 Запит на оплату товару | 6 Переказ коштів |
| 2 Перенаправлення на сервер платежів | 7 Результат авторизації |
| 3 Введення карткових даних | 8 Результат авторизації |
| 4 Авторизація | 9 Переказ коштів |
| 5 Авторизація | 10 Доставка товару |

Рисунок 1.1 – Схема функціонування електронної платіжної системи

Електронна пластикова картка – це є платіжний інструмент, що дає змогу його власнику виконувати безготівковий платіж за товар чи послугу, а також отримання готівки в банкоматах та банківських установах.

До електронних пластикових карток пред'являються вимоги унікальності і необоротності.

Вимога унікальності означає, що картка повинна містити дані, які дозволяють ідентифікувати (розпізнати) саму картку та її власника. Досягається це за допомогою елементів захисту, що наносяться на картку при

її виготовленні.

Вимога незворотності має на увазі неможливість відновлення первинної інформації, що записана на картку. Для цього вся інформація зберігається на картці в зашифрованому вигляді.

Банк, який уклав угоду з ЕПС і має відповідну ліцензію, може виступати як банк-емітент або банк-еквайр.

Банк-емітент – випускає пластикові картки та гарантує виконання фінансових зобов'язань, пов'язаних з використанням цих карток як платіжний інструмент.

Банк-еквайр – здійснює фінансові операції, пов'язані з виконанням розрахунків і платежів точками обслуговування (підприємствами торгівлі та сервісу, відділеннями банків, що приймають пластикову картку як платіжний інструмент).

До механізмів, які використовуються для переказу коштів між суб'єктами господарювання в процесі розрахунків за платіжними зобов'язаннями, належать також спеціальні установи, що надають платіжні послуги – клірингові установи, розрахункові банки та агенти з розрахунків. Розрахунковий банк забезпечує проведення в платіжній системі взаєморозрахунків між банками еквайрами й емітентами.

Процесинговий центр ЕПС – це організація, яка збирає відомості про ліміти власників карток, обробляє і розсилає підсумкові дані для взаєморозрахунків між банками, а також формує стоп-листи для банків еквайрів і точок обслуговування.

Стоп-лист – це список платіжних карток, за якими заборонено проведення операцій. До стоп-листів заносяться загублені або вкрадені картки, що виключає можливість їх несанкціонованого або злочинного використання. Стоп-лист розсилається в торгові точки банком-еквайром, що їх обслуговує. Залежно від платіжної системи, стоп-лист може бути електронним і паперовим.

Електронні гроші (e-money) – одиниці вартості, які зберігаються на електронному пристрої, приймаються як засіб платежу і є грошовим зобов'язанням особи. Вони записані на рахунках у банківських комп'ютерах і переміщуються по електронних мережах, і не є загальноприйнятим платіжним засобом, вони знаходяться тільки в рамках певної ЕПС і зазвичай носять ту саму назву, що й платіжна система.

Еквайринг (acquiring) – процес здійснення розрахунків з підприємствами, які надають товари чи послуги за операціями, що здійснюються з використанням платіжних банківських карток через POS-термінали, і здійснення операцій по видачі готівки держателям банківських карток, які не є клієнтами кредитної організації. Еквайринг є послугою технологічного, інформаційного обслуговування розрахунків за операціями, що здійснюються з використанням електронних платіжних засобів у платіжній системі.

Інтернет-еквайринг (internet acquiring) – процес здійснення платежів при використанні пластикової картки через мережу Інтернет. При цьому картка має бути такою, щоб її власник мав змогу розраховуватись нею і в звичайних магазинах. Інтернет-еквайринг дозволяє провести розрахунки в Інтернет-магазинах чи сплатити різноманітні послуги (наприклад, сплатити за Інтернет, мобільний зв'язок, комунальні послуги тощо).

Мобільний еквайринг (mobile acquiring) – процес здійснення платежів, який дозволяє заплатити за товар чи послугу в зоні присутності покупця.

Транзакція (transaction) – це банківська операція, що полягає в переказі грошових коштів з одного рахунку на інший чи видачі готівки в банкоматах та банківських установах.

Реконсиляція (reconciliation) – процедура контролю, яка полягає в ідентифікації та перевірці виконання кожного переказу коштів за допомогою показників, визначених платіжною системою.

Кліринг (clearing) – механізм, що включає збирання, сортування, реконсиляцію та проведення взаємозаліку зустрічних вимог учасників платіжної системи, а також обчислення за кожним із них сумарного сальдо за визначений період часу між загальними обсягами вимог та зобов'язань.

Банківська таємниця – відомості щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту. Такими відомостями в державі, зокрема, є: відомості про стан рахунків клієнтів, у тому числі стан кореспондентських рахунків банків у Національному банку; операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; фінансово-економічний стан

клієнтів; системи охорони банку та клієнтів; інформація про організаційно-правову структуру юридичної особи-клієнта, її керівників, напрями діяльності; відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація; інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню; коди, що використовуються банками для захисту інформації. Інформація про банки чи клієнтів, що збирається під час проведення банківського нагляду, також становить банківську таємницю.

1.2 Правові основи діяльності платіжних систем

Для ефективної діяльності платіжної системи необхідні правила, які регулювали б права та обов'язки всіх учасників процесу платежу як у нормальних умовах функціонування платіжної системи, так і у разі якихось порушень такого функціонування. Це набуває особливого значення, коли відбувається перехід від традиційних платіжних систем на основі паперових документів до сучасних електронних платіжних систем, у яких значно важче визначити стан та місцезнаходження конкретного платіжного документа на певний момент. Правила платіжної системи можуть бути викладені в законодавчому або нормативному акті, угоді або разом у цих документах.

Закон може забезпечити стабільність та пріоритет щодо інших правил; нормативний акт надає можливість коригувати правила за необхідності, а угода дозволяє приватному сектору впливати на процес визначення правил. Закон або нормативний акт можуть допускати зміну деяких правил на підставі угоди між сторонами платежу, щоб забезпечити здійснення права на контракт та можливість експерименту. Правила платіжної системи часто розробляються як самостійні документи, що не повинні спиратися на інші документи. Незалежно від джерела походження правил, що регулюють платежі (законів, нормативних актів, домовленостей чи угод), усі вони повинні відповідати критерію справедливості та, в разі потреби, мають узгоджуватись у ході переговорів усіх зацікавлених сторін (банків, Центрального банку й об'єднань споживачів) та оприлюднюватися.

Особливо важливим є опрацювання та запровадження законодавчих актів для сприяння автоматизації обробки платежів з метою підвищення

ефективності платіжної системи. Існують суттєві відмінності між різними країнами щодо правових основ регулювання платіжних систем. Разом із тим, в усіх країнах використовують кілька тотожних або, щонайменше, дуже близьких основоположних принципів. В усіх країнах існує так зване банківське законодавство, основною метою якого є регулювання питань ліцензування банків та нагляду за ними. Крім того, прийнято закони про центральні банки, що визначають сферу відповідальності центрального банку, зокрема, його функції стосовно платіжних операцій. Поряд із вищезазначеними законами існують також конкретні законодавчі акти, що встановлюють правила використання певних фінансових інструментів (наприклад, чеків та переказних векселів) при виконанні платежів. Крім того, методи виконання платіжних операцій визначаються також у загальних законодавчих документах, наприклад, цивільному кодексі чи комерційному кодексі будь-якої конкретної країни.

Деякі інші закони також можуть стосуватися платежів. Чіткі закони про платежі сприяють визначеності щодо платіжного процесу, запобіганню загальних порушень у діяльності, що пов'язана з платежами. При роботі над створенням законів про платежі постає питання: чи має уряд визначати права та обов'язки всіх учасників платежів (включаючи банки-кореспонденти та посередників), чи варто законодавчо дозволити сторонам в окремих платіжних операціях, поряд з їх банківськими установами та розрахунковими палатами, самим домовлятися про свої права й обов'язки? Закон про платежі має врівноважувати інтереси різних учасників платіжної системи. Наприклад, надавачі платіжних послуг, включаючи банки та розрахункові організації, хочуть мати економічно обґрунтовані закони та норми, дотримання яких не пов'язане з великими витратами. Мабуть, і кінцевим користувачам платіжної системи необхідні правила, що не потребують особливих затрат. Проте, деякі кінцеві користувачі можуть бути зацікавлені у відносно дорогих заходах щодо захисту інтересів споживача, які призведуть до великих витрат. Тому необхідний баланс інтересів.

Останнім часом особливого значення набуває законодавче врегулювання питань, пов'язаних із платежами на електронній основі, якого раніше могло не існувати. Якщо електронні платежі не матимуть повноправного юридичного статусу, користувачі платіжної системи наполягатимуть на отриманні паперового повідомлення про переказ, перш ніж відповідний

розрахунок вважатиметься остаточним, що зведе нанівець ефективність електронної системи. Окремі положення та норми виконання платежів в основному викладаються в угодах на основі цивільного права й у загальних правилах, які є узгодженими між сторонами, що домовляються. У зв'язку з цим варто зазначити, що існує лише незначна кількість загальнодіючих принципів. Здебільшого, правила платіжної системи прагнуть відокремити платіжну операцію від комерційної транзакції, що лежить у її основі (наприклад, продажу товару). Обробка платежів здійснюється більш ефективно, якщо всі платіжні транзакції обробляти однаково, незважаючи на конкретну основу. Правила платіжної системи повинні чітко визначати суттєві елементи платежу щодо форми та методів передачі (паперові, електронні, усні тощо). Так, для платежів на паперовій основі часто обумовлені текст та форма відповідних документів, а в електронних системах – формат і реквізити платіжних повідомлень. Існують обмеження щодо умов виконання чи зобов'язання на майбутню дату. Правила системи мають визначати, кому з учасників дозволяється обробляти платежі, хто відповідає за перевірку достовірності транзакцій, щоб запобігти здійсненню шахрайських операцій у рамках системи, а також встановлювати норми відповідальності у випадках, коли такі операції все ж відбулися. В електронних системах перевірка достовірності зазвичай здійснюється автоматично. Мають бути визначені жорсткі умови щодо термінів і методів виконання платіжних інструкцій та здійснення розрахунків.

1.3 Засоби забезпечення безпеки платіжних систем

Політика інформаційної безпеки банківських і платіжних систем сильно відрізняється від аналогічних політик інших компаній. Це пояснюється в першу чергу специфічним характером загроз, а також публічною діяльністю банків. Оскільки для клієнтів робота з банком повинна бути легкою та зручною, то банки змушені робити доступ до рахунків досить простим.

Для забезпечення фізичної та класичної інформаційної безпеки існують вироблені стандартні заходи. У напрямі безпеки автоматизованих систем обробки інформації банку ситуація складніша. Методи та засоби безпеки автоматизованих систем вимагають постійного оновлення та модернізації, оскільки комп'ютерні технології схильні до частих радикальних змін.

Захист банківської інформації – це комплексна задача, яка не може вирішуватися тільки у межах банківських програм. Для ефективної реалізації захисту необхідно спочатку вибрати та налаштувати операційні системи та мережні системні засоби, які підтримують функціонування банківських програм. Необхідно виділити два напрями серед дисциплінарних засобів забезпечення захисту. Перший – користувач системи повинен володіти мінімально достатньою кількістю інформації щодо особливостей побудови системи. Другий – система повинна містити багаторівневі засоби ідентифікації користувачів та контролю їх прав.

Інформаційна безпека означає можливість протистояти спробам нанесення збитків власникам або користувачам системи за різних навмисних або ненавмисних впливів на неї. Система захисту інформації повинна забезпечувати безперервний захист інформації щодо переказу грошей на усіх етапах її формування обробки, передачі та зберігання. Електронні документи, що містять інформацію, яка відноситься до банківської таємниці або є конфіденційною, повинні бути зашифрованими під час передавання їх за допомогою комунікаційних каналів зв'язку. Порядок захисту та використання засобів захисту інформації щодо переказу визначається Законами України “Про платіжні системи та переказ грошей в Україні” [1], “Про захист інформації в інформаційно-комунікаційних системах” [2], “Про захист інформації в автоматизованих системах” [3], “Про електронні комунікації” [4], нормативно-правовими актами Національного банку України (Інструкцією Національного банку України про міжбанківський переказ грошей в Україні в національній валюті, Положення про захист електронних банківських документів з використанням засобів захисту інформації НБУ № 829 від 26.11.2015 р. [5]) та правилами платіжних систем. Відповідно до ст. 1 Закону України “Про захист інформації в автоматизованих системах”: *«Захист інформації – сукупність організаційно-технічних заходів і правових норм для запобігання заподіяння шкоди інтересам власника інформації чи автоматизованої системи та осіб, які користуються інформацією»* [3].

Задача захисту інформації у банківській системі є набагато складнішою, ніж в інших організаціях. Розв'язання такої задачі передбачає планування організаційних, системних заходів, які забезпечують захист. Також необхідно постійно здійснювати комплексний підхід до забезпечення захисту

банківських та платіжних систем. Проте, при плануванні захисту необхідно дотримуватися межі між необхідним рівнем захисту і тим рівнем, коли захист починає заважати нормальній роботі персоналу.

Об'єктами захисту є інформація, що обробляється в автоматизованій системі, права власників автоматизованої системи, права користувача. Захисту підлягає будь-яка інформація в автоматизованій системі, необхідність захисту якої визначається її власником або чинним законодавством.

Автоматизована банківська система (АБС) – автоматизована система банку – комплекс програмно-технічних засобів, спрямований на автоматизацію банківської діяльності. Забезпечує інтеграцію різних підсистем, кожна з яких спрямована на виконання тієї чи іншої сфери діяльності банку.

Система захисту електронних банківських документів – сукупність методів та засобів, що включає апаратно-програмні, програмні засоби захисту, ключову інформацію та систему розподілу ключової інформації, технологічні засоби контролю та організаційні заходи щодо захисту інформації.

Суб'єктами відносин, пов'язаних з обробкою інформації в автоматизованій системі, є:

- власники інформації чи уповноважені ними особи;
- власники автоматизованої системи чи уповноважені ними особи;
- користувачі інформації;
- користувачі автоматизованої системи.

Безпеку платіжних систем можна розглядати як таку, що складається із зовнішньої та внутрішньої.

Зовнішня безпека включає:

- захист від втрати або модифікації системою інформації при стихійних лихах (пожежах, землетрусах та ін.);
- захист системи від проникнення зломисників ззовні з метою викрадення, отримання доступу до інформації або виведення системи з ладу.

Мета внутрішньої безпеки – забезпечення надійної та коректної роботи, цілісності інформації і компонентів (ресурсів) системи. Це передбачає створення надійних і зручних механізмів регламентування діяльності всіх користувачів, а також персоналу, який обслуговує систему, та дотримання

правил доступу до ресурсів системи.

Можна виділити два підходи, які гарантують безпеку інформаційних систем: фрагментарний та комплексний. Фрагментарний підхід орієнтується на протидію чітко визначеним загрозам за певних умов використання системи. Головною позитивною рисою такого підходу є міцний захист щодо конкретної загрози, але основний недолік – локальність дії та відсутність єдиного захищеного середовища для обробки інформації. Тому такий підхід неприйнятний для захисту платіжних систем.

Для створення захисту платіжних систем треба використовувати комплексний підхід, а саме: створення захищеного середовища для обробки платіжної та службової інформації у системі, яке об'єднує різноманітні (правові, організаційні, програмно-технічні) засоби для протидії будь-яким загрозам. До основних засобів захисту інформації можна віднести такі: фізичні, апаратні, програмні, апаратно-програмні засоби, криптографічні та адміністративні методи.

Фізичні засоби захисту – це засоби, необхідні для зовнішнього захисту електронно-обчислювальної машини (ЕОМ), території та об'єктів на базі обчислювальної техніки, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів інформаційних систем та інформації, що захищаються. Спектр сучасних фізичних засобів захисту дуже широкий. Це різного роду замки, які можуть встановлюватись на вході в приміщення та на блоках системи, це системи пожежної сигналізації і т.п. До цієї групи засобів захисту також належать різні засоби екранування робочих приміщень та каналів передачі даних.

Апаратні засоби захисту – це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються у серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку та ін.

Основні функції апаратних засобів захисту:

- заборона несанкціонованого (неавторизованого) зовнішнього доступу віддаленого користувача;

- заборона несанкціонованого (неавторизованого) внутрішнього доступу до баз даних у результаті випадкових чи умисних дій персоналу;

- захист цілісності програмного забезпечення.

Ці функції реалізуються шляхом:

- ідентифікації суб'єктів (користувачів, обслуговуючого персоналу) і об'єктів (ресурсів) системи;
- автентифікації суб'єкта за наданим ним ідентифікатором;
- перевірки повноважень, яка полягає в перевірці дозволу на певні види робіт;
- реєстрації (протоколювання) при звертаннях до заборонених ресурсів;
- реєстрації спроб несанкціонованого доступу.

Програмні засоби захисту необхідні для виконання логічних й інтелектуальних функцій захисту, які вбудовані до складу програмного забезпечення системи.

За допомогою програмних засобів захисту реалізуються наступні задачі забезпечення безпеки:

- контроль завантаження та входу в систему за допомогою системи паролів;
- розмежування і контроль прав доступу до системних ресурсів, терміналів, зовнішніх ресурсів, постійних та тимчасових наборів даних і т.п.;
- захист файлів від вірусів;
- автоматичний контроль за роботою користувачів шляхом протоколювання їхніх дій.

Апаратно-програмні засоби захисту – це засоби, які ґрунтуються на синтезі програмних та апаратних засобів. Вони широко використовуються при автентифікації користувачів АБС. Автентифікація – перевірка ідентифікатора користувача перед допуском його до ресурсів системи.

Апаратно-програмні засоби захисту використовуються також при накладанні електронних підписів відповідальних користувачів. Найбільш поширеним в АБС є використання смарт-карт (smart card), які вміщують паролі та ключі користувачів.

Система захисту інформації повинна забезпечувати:

- цілісність інформації, що передається в платіжній системі, та компонентів платіжної системи;
- конфіденційність інформації під час її обробки, передавання та зберігання в платіжній системі;
- доступність до інформації, тобто можливість постійного та

безперешкодного доступу до компонентів платіжної системи особам, які мають на це право або повноваження, визначені законодавством України, а також встановлені договором;

- неможливість відмови користувача від факту передавання та одержувача від факту прийняття документа.

При побудові політики безпеки платіжної системи використання криптографічного захисту інформації та безпечного розподілу ключів значно посилює безпеку роботи системи.

За принципами використання криптографічний захист може бути вбудованим у платіжну систему або бути додатковим механізмом, який може відключатися.

Необхідно акцентувати увагу на тому, що розробка заходів охорони, технологічних та програмно-апаратних засобів криптографічного захисту здійснюється платіжною організацією відповідної платіжної системи, її членами або іншою установою на їх замовлення.

Криптографічні методи захисту інформації дуже широко використовуються в АБС і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту. Тому криптографічні методи захисту заслуговують окремого розгляду.

1.4 Платіжні картки та їх класифікація

Платіжна картка (payment card) є платіжним інструментом, який дає змогу здійснення безготівкового платежу за товар чи послугу, а також одержання готівки в банкоматах та банківських установах.

До банківських платіжних карток висуваються дві основні вимоги:

- перша вимога означає, що картка повинна бути унікальною, тобто серед усіх карток, які були випущені банком-емітентом, не має бути двох однакових за характеристиками;

- друга вимога означає, що картка повинна мати властивість незворотності, тобто не може бути відновлена первісна інформація на картці.

За принципом дії картки розподіляють на:

- пасивні картки;
- активні картки.

На пасивних картках просто зберігається інформація (зазвичай це карти

з магнітною стрічкою).

Активні пластикові картки характеризуються тим, що в них вбудована електронна мікросхема, що дає змогу розрізняти їх за функціональними можливостями на:

- картки-лічильники;
- картки з пам'яттю;
- картки з мікропроцесором.

Для захисту пасивних пластикових карток від підробки є два основних способи:

1) метод магнітних водяних знаків, який передбачає нанесення на магнітну стрічку, яка розташована на картці, спеціального рисунка;

2) метод “сендвича”, який полягає в тому, що одна стрічка містить ділянки з різними рівнями намагнічення. Сучасні пасивні пластикові картки мають кілька ступенів захисту.

Однією з основних функцій пластикової картки є забезпечення ідентифікації власника картки, який є користувачем платіжної системи.

З цією метою на пластикову картку наносять:

- логотипи банку-емітента;
- логотипи платіжної системи, що обслуговує цю картку;
- іменні дані власника картки;
- номер рахунка власника картки;
- термін дії картки;
- тощо.

Також може бути фотографія власника картки, підпис, голограма, нестандартні шрифти для ембосування (рельєфне тиснення).

За технологічними особливостями розрізняють картки двох видів: з магнітною смугою (стрічкою) та з вбудованою мікросхемою (chipcard – чіп або smart card – смарт-картка чи “інтелектуальна” картка).

Картки з магнітною смугою мають на звороті магнітну стрічку, на якій записані дані, що необхідні для ідентифікації власника картки при її використанні в електронних терміналах.

На магнітну стрічку зазвичай записують дані, які містять:

- банківські реквізити власника картки (ім'я та прізвище, код банківської установи, номер рахунка);
- термін дії картки;

– персональний ідентифікаційний номер.

Персональний ідентифікаційний номер (Personal Identification Number – PIN) передбачається для кредитних і подібних карток (наприклад, SIM-карток); з його допомогою виробляється авторизація власника картки. PIN-код повинен знати тільки власник картки. Зазвичай передбачено обмеження спроб правильного введення PIN-коду (як правило, не більше 3 разів), після чого карта блокується для використання.

Картка з вбудованою мікросхемою (смарт-картка) складається із запам'ятовувальних пристроїв для збереження інформації та процесора, який є складовою комп'ютера і здатний обробляти інформацію, записану в запам'ятовувальних пристроях (рис. 1.2). Обсяг пам'яті картки дозволяє зберігати та використовувати інформацію про її власника, банківський рахунок клієнта, а також кілька сотень останніх операцій, виконаних з використанням картки.

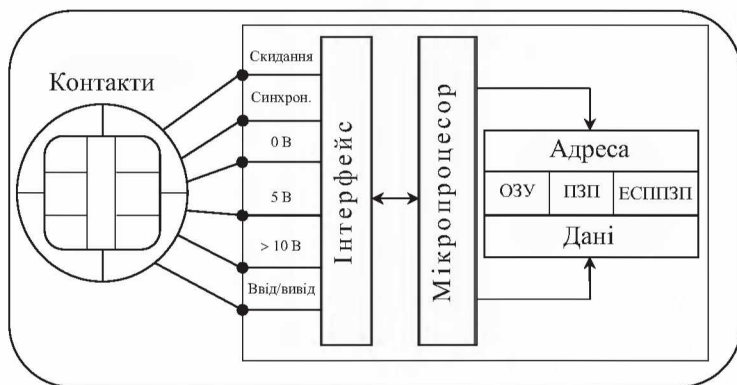


Рисунок 1.2 – Архітектура смарт-картки

Смарт-картку можна використовувати для отримання готівки у банкоматі, для оплати товарів і послуг в організаціях роздрібною торгівлі і побутового обслуговування, для отримання кредиту тощо.

Відомості, що записуються у мікросхемі картки, дають змогу здійснити транзакцію в автономному режимі (off-line), тобто без безпосереднього зв'язку з центральним процесором банківської комп'ютерної системи в момент здійснення транзакції. Оскільки на картці зберігається інформація

про суму коштів, яка є на банківському рахунку, то процедура авторизації тут зайва. При цьому, якщо ліміт перевищений, то транзакція не відбудеться. Якщо ж сума транзакції менша від суми ліміту, то в момент її здійснення сума вільного ліміту буде зменшена. В такому разі на картку здійснюється запис відповідного залишку, який може бути використаний при наступній купівлі. При поповненні рахунку на суму коштів, ліміт поновлюється, про що робиться новий запис у мікросхемі.

Всі платіжні картки, які призначені для розрахунків, можуть поділятися на індивідуальні і корпоративні (бізнес-картки).

Індивідуальні картки банки видають приватним особам: своїм платоспроможним клієнтам, а також іншим особам після аналізу “кредитної історії” останніх і відкриття їм поточного (карткового) рахунку в банку або внесення страхового депозиту.

Корпоративні картки видаються юридичним особам під їх гарантії і забезпечення також після аналізу платоспроможності юридичної особи. Користуватися корпоративними картками можуть співробітники організації, яка отримала картку. Співробітникам відкриваються персональні рахунки, які пов’язані з корпоративним картковим рахунком. При цьому, відповідальність перед банком за корпоративний картковий рахунок несе організація, а не власники індивідуальних корпоративних карток.

Сфера платіжних систем розвивається швидкими темпами. Але далеко не все, що пропонує ринок, є безпечним і зручним продуктом для кінцевого користувача. Безпека здійснення електронних транзакцій залежить в першу чергу від користувача.

Так, можна сформулювати поради щодо забезпечення безпеки здійснення транзакцій в Інтернеті:

- необхідно зберігати платіжну картку в надійному місці (шістнадцяти цифр номера, терміну дії та CVV-коду (Card Verification Value) досить, щоб злоумисники могли нею скористатися для оплати в Інтернеті);

- необхідно зберігати паролі конфіденційними (паролі до платіжної картки повинні бути максимально складними і непередбачуваними та зберігатися окремо від картки);

- треба сплачувати послуги на сайтах, які використовують захищене з’єднання (надійні сайти використовують захищене з’єднання, адреса безпечного ресурсу починається з [https: //...;](https://...)

– необхідно завжди використовувати для покупок тільки особисті пристрої (на сторонніх комп'ютерах, планшетах/телефонах паролі можуть зберегтися, і зловмисник може отримати доступ до вашої карти, крім того, ще треба оновлювати антивірус);

– не можна нікому повідомляти особисту інформацію (індивідуальний ідентифікаційний номер та дату народження, в комплекті з даними картки – знахідка для шахраїв);

– рекомендовано користуватися SMS-підтвердженнями оплат (3-D Secure – функція захисту, яка підключена до більшості банківських карток, дана технологія безпеки знижує ризики несанкціонованих Інтернет-операцій);

– необхідно періодично відстежувати всі здійснені операції та перевіряти рахунки.

Оплата в Інтернеті банківськими картками передбачає обробку даних платіжної картки, що підвищує ризик шахрайства. Система переказу коштів повинна відповідати міжнародним платіжним стандартам безпеки. Так, безпечна платіжна система має бути сертифікована відповідно до стандарту PCI DSS, який захищає персональні дані власника картки та запобігає шахрайству при оплаті.

1.5 Стандарт безпеки даних індустрії платіжних карток

Стандарт безпеки даних індустрії платіжних карток (Payment Card Industry Data Security Standard – PCI DSS) розроблений з метою спрощення впровадження та поширення заходів щодо забезпечення і повсюдного впровадження стандарту безпеки даних про власників карток [6, 7]. PCI DSS розроблений Радою зі стандартів безпеки індустрії платіжних карток (Payment Card Industry Security Standards Council – PCI SSC). Засновниками PCI SSC є міжнародні платіжні системи Visa, MasterCard, American Express, JCB (платіжна система Японії) і Discover.

Стандарт PCI DSS являє собою сукупність вимог щодо забезпечення безпеки даних про власників платіжних карток, які передаються, зберігаються й обробляються в інформаційних інфраструктурах організацій. Вимоги стандарту поширюються на всі компанії, що працюють з міжнародними платіжними системами Visa та MasterCard на території Центральної та Східної Європи, Близького Сходу й Африки. Так,

всеукраїнський сервіс прийому платежів в Інтернеті iPay.ua сертифікований міжнародним стандартом безпеки PCI DSS, тому власники банківських карток можуть бути впевнені, що їхні карткові дані надійно захищені під час здійснення платежів.

Також у стандарті PCI DSS [7] надано таблицю (табл. 1.1), яка ілюструє найбільш часто використовувані елементи даних про власників карток і критичних автентифікаційних даних; дозволено або заборонено їх зберігання та чи повинен бути захищений кожен із цих елементів. Таблиця не є вичерпною, вона демонструє різні типи вимог до кожного елемента.

Таблиця 1.1 – Ілюстрація вимог щодо найбільш часто використовуваних даних

Дані	Елемент даних	Зберігання дозволено	Потрібно захист	Вимога 3.4 PCI DSS
про власників карток	Номер платіжної картки (Primary Account Number – PAN)	так	так	так
	Ім'я власника карти (Cardholder Name)	так	так	ні
	Сервісний код (Service Code)	так	так	ні
	Дата закінчення терміну дії карти (Expiration Date)	так	так	ні
критичні автентифікаційні ¹	Магнітна смуга карти ²	ні	не визначено	не визначено
	CAV2/CVC2/CVV2/CID ³	ні	не визначено	не визначено
	PIN/PIN Block	ні	не визначено	не визначено

¹Критичні автентифікаційні дані не повинні зберігатися після авторизації (навіть у зашифрованому вигляді).

²Повна магнітна смужка картки, її зашифроване надання у чипі й інші види надання.

³CAV (Card Authentication Value) – JCB, CVC (Card Validation Code) – MasterCard, CVV (Card Verification Value) – Visa, CID (Card IDentification number) – American Express.

Вимога 3.4 у стандарті PCI DSS. Привести PAN до нечитабельного вигляду в усіх місцях їх зберігання (включаючи журнали, резервні копії,

знімні цифрові носії), використовуючи для цього будь-який з наступних методів:

- односпрямоване ґешування на основі стійкої криптографії (ґеш-код повинен бути сформований з цілого PAN);
- усічення (ґеш-код не може використовуватися для заміни усіченого сегмента PAN);
- індексні маркери і шифрувальні блокноти (такі блокноти при зберіганні повинні бути захищені);
- стійка криптографія з супутніми процесами і процедурами керування ключами.

Вимога 3.4 застосовується тільки до PAN. Якщо PAN зберігається разом з іншими даними про власників, то відповідно до вимоги 3.4 зберігати у нечитабельному вигляді необхідно тільки PAN. Якщо PAN не зберігається, не обробляється і не передається, то вимоги PCI DSS не застосовуються.

Безпечні платіжні додатки при впровадженні у середовище відповідності стандарту PCI DSS дозволять уникнути порушень безпеки і шахрайських дій, які можуть привести до компрометації повного змісту даних магнітної смуги, перевірочних значень (CAV2, CID, CVC2, CVV2), а також PIN і PIN-блоків.

PCI DSS являє мінімальний набір цілей для контролю, який може бути посилений місцевими, регіональними або галузевими законами і постановами. Також, законодавства або нормативні вимоги можуть вимагати особливого захисту персональної інформації або інших елементів даних (наприклад, імені власника картки), або визначати порядок розкриття організацією інформації про споживачів. Приклади включають закони, які стосуються захисту персональних даних, приватності, крадіжки особистих даних або безпеки інформації. PCI DSS не замінює собою місцеві або регіональні закони, урядові розпорядження або інші законні вимоги.

У стандарті надано приклади випадків, у яких платіжні додатки можуть перешкоджати досягненню відповідності:

- зберігання даних магнітної смуги і/або еквівалентної чіпкової інформації в клієнтській мережі після авторизації;
- додатки, що вимагають від клієнтів відключення різних опцій, необхідних у стандарті PCI DSS, наприклад, антивірусного програмного забезпечення, міжмережевих екранів для належної роботи програми;
- використання розробниками небезпечних методів підключення,

використовуваних для підтримки користувача.

Стандарт PCI DSS застосовується для всіх організацій, залучених в обробку платіжних карт: процесингових центрів, еквайрів, емітентів і постачальників послуг, а також організацій, які зберігають, обробляють або передають дані про власників карток або критичні автентифікаційні дані.

1.6 Ідентифікація та автентифікація користувача

Ідентифікація (identification) – це процес розпізнавання користувача (суб'єкта) за його ідентифікатором, є першим та одним із ключових елементів інфраструктури захисту від несанкціонованого доступу (НСД) до будь-якої інформаційної системи.

Ідентифікація – це надання користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). Процес ідентифікації тісно пов'язаний з процесом автентифікації, другим кроком перевірки користувача.

Автентифікація (authentication) – це процес підтвердження справжності користувача. За допомогою автентифікації інша сторона переконується, що користувач є дійсно тією людиною, за кого вона себе видає. Автентифікація – це процедура, яка перевіряє, чи має користувач з наданим ідентифікатором право на доступ до ресурсу. Ці процедури (ідентифікація та автентифікація) нерозривно зв'язані між собою, оскільки спосіб перевірки визначає, яким чином і що користувач повинен надати системі, щоб отримати доступ. Сьогодні існує декілька способів ідентифікації користувачів.

1) **Парольна ідентифікація.** Суть її зводиться до наступного. Кожен зареєстрований користувач якої-небудь системи одержує набір персональних реквізитів (зазвичай використовуються одночасно логін та пароль), які необхідно довести при кожній спробі входу у систему. Головна перевага паролльної ідентифікації – це простота реалізації та використання.

Головний недолік паролльної системи ідентифікації – величезна залежність надійності ідентифікації від паролів, що обираються.

2) **Апаратна (або електронна) ідентифікація.** Цей принцип ідентифікації ґрунтується на визначенні особистості користувача по якомусь предмету, електронному ключу, токєну, що перебувають у його персональному користуванні.

На даний момент найбільшого поширення одержали два типи пристроїв: різноманітні картки (смарт-картки, магнітні картки і т.д.) та токени (token), які підключаються безпосередньо до одного із портів комп'ютера.

Головною перевагою застосування апаратної ідентифікації є досить висока надійність. Це обумовлено тим, що в апаратному обладнанні реалізовано чимало різних захисних механізмів, крім того, вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції. Проте недоліком використання апаратної ідентифікації є можливість крадіжки зловмисниками токенів або карток у зареєстрованих користувачів. Крім того, вони можуть бути втрачені, передані іншій особі, дубльовані. Іншим недоліком цієї технології є дорожнеча введення в експлуатацію такої системи ідентифікації.

3) Ідентифікація за біометричними ознаками людини. Цей метод є самим зручним і надійним методом не тільки для розпізнавання користувача, а й для підтвердження його особистості.

Незалежно від типу системи автентифікації в ній завжди присутні п'ять елементів.

Перший елемент – конкретна людина (користувач) або процес, який повинен проходити автентифікацію – суб'єкт доступу.

Другий елемент – розпізнавальний знак, ідентифікатор, який виділяє цього користувача або цей процес серед інших.

Третій елемент – відмінна характеристика (автентифікатор), що підтверджує приналежність ідентифікатора суб'єкту доступу.

Четвертий елемент – власник системи (адміністратор), який несе відповідальність за використання системи, і в розмежуванні авторизованих користувачів та інших покладається на механізм автентифікації.

П'ятий елемент – механізм автентифікації, який дозволяє перевірити присутність відмінної характеристики.

При успішному проходженні автентифікації суб'єкту доступу повинні бути видані деякі права (привілеї). Для цього служить механізм керування доступом. За допомогою цього ж механізму суб'єкт доступу позбувається прав (привілеїв), якщо автентифікація була неуспішною.

Більш детально методи автентифікації описані у 4 розділі цього посібника.

1.6.1 Персональний ідентифікаційний номер

Персональний ідентифікаційний номер використовують для ідентифікації та автентифікації клієнта банку-емітента.

PIN-код має бути відомий тільки власнику картки, який може ввести PIN для підтвердження справжності за допомогою спеціальної клавіатури банкомата чи терміналу. В ході авторизації операції використовується одночасно як пароль доступу власника картки до терміналу (банкомата) і як особистий ключ для цифрового підпису запиту. Для перевірки PIN-коду використовується алгоритм, що реалізується мікропроцесором на картці. Коли картка вводиться у зчитувальний пристрій банкомата чи терміналу, набраний код порівнюється з PIN-кодом, що є записаним на магнітній стрічці. Якщо вони збігаються, то здійснюється операція автентифікації (підтвердження дійсності) користувача та відкривається доступ до комунікаційної мережі для подальшого виконання платежу чи видачі готівки. Якщо вони не збігаються, то справжність користувача не підтверджується і користувач не може користуватися платіжною картою для здійснення транзакції. Користувач може здійснити ще кілька спроб набору PIN-коду (зазвичай 3) і, в разі незбігу кодів, картка заблоковується та вилучається.

PIN-код – це аналог пароля. Довжина PIN має бути до 12 символів (зазвичай – це послідовність від 4 до 8 цифр). Значення PIN зв'язано з атрибутами банківської картки, тому PIN можна назвати аналогом підпису власника картки.

Існують два типи PIN:

- 1) призначений (derived), тобто PIN призначений банком який видав картку;
- 2) призначений випадковий (random), тобто PIN, який був обраний власником картки.

Якщо PIN призначений банком, то він використовує один з двох варіантів генерації PIN.

Перший варіант – PIN генерується криптографічно з номера рахунка власника картки. Тоді номер рахунка клієнта доповнюється нулями або іншою константою до шістнадцятирічних цифр (8 байтів). Потім одержані 8 байтів зашифровуються з використанням таємного ключа за алгоритмом DES (Data Encryption Standard). З одержаного шифртексту (8 байтів), починаючи з

молодших байтів, виділяються послідовності, довжиною по 4 біти. Якщо значення числа, утвореного цими бітами, менше за 10, то одержана цифра включається в PIN, інше значення поки відкладається. Отже, обробляються всі 8 байтів (64 бітів). Якщо в результаті обробки не вдалося одержати необхідну кількість десяткових цифр для PIN-коду, тоді повертаються до відкладених, невикористаних комбінацій і з кожної по черзі віднімається число 10 для отримання наступної цифри PIN-коду.

Перевага такого методу в тому, що не потрібно зберігати PIN в електронній платіжній системі. А недоліком є те, що за необхідності зміни PIN потрібно замінити на нове значення банківський рахунок власника картки, або згенерувати новий ключ.

Другий варіант – банк, обираючи значення PIN, випадковим чином зберігає його у вигляді криптограми. Обрані значення банк передає власникам банківських карт по захищеному каналу зв'язку (це може бути лист, що надається банком особисто в руки користувача чи замовне поштове відправлення). Недоліком є те, що досить складно запам'ятати PIN власнику картки. Доведено, що середньостатистична людина може запам'ятати комбінацію лише з чотирьох цифр. Саме тому, зазвичай, значення PIN дорівнює чотирьом цифрам. Проте, щоб запобігти можливий перебір дозволених комбінацій зловмисником, користувач може здійснити обмежену кількість спроб набору PIN-коду і, в разі неправильного введення коду, платіжну картку буде заблоковано.

1.6.2 Схема виведення PIN з номера рахунка користувача

Схему виведення PIN з номера рахунка користувача показана на рис. 1.3.



Рисунок 1.3 – Схема виведення PIN з номера рахунка користувача

Для більшої зручності використовують значення PIN, що обирається самим клієнтом. При цьому, існує два способи обрання:

- 1) використовують один PIN для різних цілей;
- 2) задавати PIN, як сукупність літер та цифр для зручності запам'ятовування.

При ідентифікації користувача за значенням PIN та кредитної картки використовують два способи перевірки PIN.

Перший спосіб має назву «неалгоритмічний», тобто шляхом порівняння виведеного PIN зі значенням, збереженим у базі даних у зашифрованому вигляді.

Другий спосіб має назву «алгоритмічний», тобто введений клієнтом PIN перетворюється за певним алгоритмом з використанням секретного ключа і потім порівнюється зі значенням PIN, який зберігається у певному вигляді на карті.

Переваги цих способів в тому, що:

- відсутні копії PIN на сервері банку;
- відсутній обмін PIN між банком (чи POS-терміналом) та користувачем.

Це виключає можливість перехоплення PIN злоумисником. Крім того є спрощення роботи системи за рахунок відсутності необхідності дій в режимі on-line (реальному масштабі часу).

1.6.3 Парольні системи захисту

Головна перевага парольної ідентифікації – простота, зручність і звичність. Паролі давно вбудовані в операційні системи та інші сервіси. При правильному використанні, паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки.

Значно підвищити надійність парольного захисту дозволять наступні заходи:

- накладання технічних обмежень: встановлення мінімальної довжини пароля, використання в паролі різних груп символів (пароль повинен містити літери, цифри, знаки пунктуації і т.п.);
- періодична зміна паролів, тобто керування терміном дії паролів;
- обмеження доступу до файла, де зберігаються паролі;
- обмеження кількості невдалих спроб входу у систему;

– використання програмних генераторів паролів (програма, що ґрунтується на визначених правилах, може генерувати тільки благозвучні паролі, що легко запам'ятовуються).

Принципи побудови парольних систем мають деякі особливості.

Ідентифікатор користувача – це інформація, що дозволяє розрізнити індивідуальних користувачів парольної системи (проводити їх ідентифікацію).

Пароль користувача – це конфіденційна інформація, що відома тільки користувачу. Вона також зберігається в базі даних системи для можливості порівняння наданого пароля зі зразком та здійснення проходження процедури автентифікації. Одноразовий пароль дає можливість користувачу одноразово пройти автентифікацію. Багаторазовий пароль може бути використаний неодноразово.

Обліковий запис користувача – це сукупність ідентифікатора та відповідного пароля. База даних системи містить облікові записи всіх користувачів даної парольної системи.

Під парольною системою розуміють програмно-апаратний комплекс, що реалізовує системи ідентифікації та автентифікації користувачів автоматизованих систем на основі одноразових або багаторазових паролів. Як правило, такий комплекс функціонує спільно з підсистемами розмежування доступу і реєстрації подій. В окремих випадках парольна система може виконувати низку додаткових функцій, зокрема генерацію і розподіл короточасних (сеансових) криптографічних ключів.

Основними компонентами парольної системи є:

- інтерфейс користувача;
- інтерфейс адміністратора;
- модуль поєднання з іншими підсистемами безпеки;
- база даних облікових записів.

Парольна система є одним із перших об'єктів атаки при вторгненні зловмисника в захищену систему.

Типи загроз безпеки парольних систем можна надати, по-перше, як *розголошування параметрів облікового запису* через:

- підбір в інтерактивному режимі;
- підглядання;
- навмисну передачу пароля його власником іншій особі;

- захват бази даних парольної системи;
- перехоплення переданої по мережі інформації про пароль;
- зберігання пароля в доступному місці;
- по-друге, як *втручання у функціонування компонентів парольної системи* через:
 - впровадження програмних закладок;
 - виявлення і використання помилок, що допущені на стадії розробки;
 - виведення з ладу парольної системи.

Деякі з перерахованих типів загроз пов'язані з наявністю так званого людського фактора. Важливим аспектом надійності парольної системи є спосіб зберігання паролів у базі даних облікових записів. Для того, щоб злоумисник не мав змоги скористатися паролем користувача, паролі повинні зберігатися у вигляді згорток (утворюються завдяки процесу гешування) чи у вигляді криптограм (утворюються в процесі шифрування за допомогою секретного ключа).

1.7 Універсальна електронна платіжна система

Універсальна електронна платіжна система (Universal Electronic Payment System – UEPS) розроблена французькою компанією NET 1 International та заснована на автономному принципі обслуговування власників карток в торговій точці або банкоматі [8]. За безпосередньої взаємодії двох карток базовим алгоритмом шифрування є алгоритм DES. Оскільки на сьогодні довжина секретного ключа шифрування в даному алгоритмі є занадто мала, підвищити криптостійкість можна за рахунок подвійного зашифровування вихідного тексту. Висока криптостійкість забезпечується використанням подвійного шифрування блока вихідного тексту на ключах 8 байтів (використовується послідовне зашифровування 2 ключами по 64 біта).

Подвійне зашифровування – дворазове шифрування блока відкритого тексту за допомогою двох різних секретних ключів. Спочатку зашифровують блок відкритого тексту M ключем K_1 , тобто шифртекст

$$C_1 = E_{K_1}(M), \quad (1)$$

де $E_{K_1}(M)$ – функція перетворення зашифровування E відкритого тексту M на підставі першого секретного ключа K_1 . А потім отриманий шифртекст C_1 зашифровують ще раз за допомогою другого секретного ключа K_2 . Остаточно, криптограма C_2 є результатом функції перетворення зашифровування E шифртексту C_1 за допомогою другого секретного ключа K_2 :

$$C_2 = E_{K_2}(C_1). \quad (2)$$

Розшифрування D виразу (2) є зворотним процесом, тобто відкритий текст

$$M = D_{K_1}(D_{K_2}(C_2)). \quad (3)$$

Для злому методом повного перебору замість 2^n комбінацій, (де n – кількість біт у блоці вихідного тексту) необхідно перебрати 2^{2n} , де $n = 64$, тобто кількість можливих спроб перебору для знаходження ключа суттєво зростає і дорівнює 2^{128} .

У платіжних системах, що працюють у режимі off-line, значна частина функцій з забезпечення контролю дії від несанкціонованого доступу лягає на мікропроцесорну картку (МПК).

В універсальній системі використовуються три основних типи МПК:

- 1) службові картки персоналу банку;
- 2) торгові картки;
- 3) картки клієнта.

Картки не дозволяють здійснити механічне зчитування інформації шляхом спилювання кристала по прошарках, шляхом сканування електронним мікроскопом, шляхом впливу ультрафіолету. У цьому випадку МПК виходить з ладу. Архітектура самої картки така, що МПК контролює доступ до захищених комірок пам'яті та передає керування програмі UEPS.

Центр емісії виконує наступні функції:

- 1) генерацію головного ключа платіжної системи;
- 2) первинну емісію МПК, тобто привласнення карткам унікальних серійних номерів;

3) занесення на картки громадської ідентифікуючої і контрольної інформації та занесення головного ключа системи на картку;

4) введення довідників учасників, типів карток і кодів валют, що використовують у системі;

5) введення єдиної бази даних за заводськими номерами й унікальним серійним номером картки, які використовуються у системі.

На рис. 1.4 показана спрощена архітектура платіжної системи (скорочення ОП – операційний пункт).

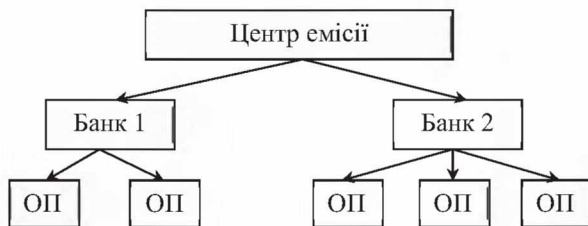


Рисунок 1.4 – Архітектура платіжної системи

Банки-учасники перед початком випуску своїх карток створюють власний набір ключів, який заносять на карту в процесі емісії і використовують при формуванні та обробці фінансових транзакцій.

Операційні пункти – пункти, в яких проводиться обслуговування клієнтів банку, відкритих закритих ключів, видача карток.

У платіжній системі UEPS торговий термінал не зберігає ніякої секретної інформації, а відіграє роль елемента, який забезпечує взаємодію двох захищених електронних інтелектуальних пристроїв. Всі операції здійснюються в діалозі двох карток, при цьому поза карток вся інформація завжди зашифрована на базі сесійних ключів.

1.8 Національна платіжна система «Простір»

«Простір» – державна платіжна система, в якій розрахунки за товари та послуги, одержання готівки та інші операції здійснюються за допомогою електронних платіжних засобів [9].

Національний банк створив платіжну систему НПС «Простір» з дотриманням відкритих міжнародних стандартів.

Національний банк створив державну систему електронних платежів (СЕП) для забезпечення розрахунків банків та їх клієнтів у гривні в межах України. Національний банк є Платіжною організацією та розрахунковим банком СЕП. Учасниками СЕП є Національний банк, банки України та Державна казначейська служба України.

СЕП забезпечує високий рівень безпеки і надійності переказу коштів між банками та обслуговує приблизно 96% міжбанківських платежів в Україні.

СЕП належить до системи валових розрахунків у режимі реального часу (Real-Time Gross Settlement – RTGS).

СЕП дає змогу відправляти платежі в одному з двох режимів: реального часу і файлового. В режимі реального часу кошти потрапляють на рахунок банку-одержувача миттєво; у файловому режимі час проходження платежу від банку-відправника до банку-одержувача у середньому складає 15 хв.

У середньому в день СЕП обробляє 1,6 млн. платежів на суму близько 199 млрд. грн. Проте потенціал СЕП значно більший – запас пропускної спроможності СЕП дозволяє щоденно обробити практично у 10 разів більше документів, ніж теперішні обсяги [9]:

- 97,7 % усіх операцій за картками українських банків-емітентів здійснюються на території України, лише 2,3 % за її межами;

- система «Простір» побудована за міжнародними стандартами EMV (Europay, MasterCard, VISA) та CPA (Common Payment Application), банкоматно-термінальне обладнання є повністю технічно сумісним зі стандартами міжнародних платіжних систем;

- 98 % POS-терміналів та 87 % банкоматів можуть обслуговувати картки «Простір»;

- картками «Простір» можна здійснювати платежі та розрахунки в Інтернеті.

2 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЛАТІЖНИХ ТЕРМІНАЛІВ ПІД ЧАС ЕКВАЙРІНГУ

2.1 Захист системи POS

Платіжний термінал (payment terminal) – електронний пристрій, який зчитує дані з електронної пластикової картки, або зі смартфона з функцією NFS (Near Field Communication – технологія бездротового високочастотного зв'язку малого радіуса дії) та встановленого відповідного програмного забезпечення із внесеними реквізитами платіжної картки. При цьому зв'язок терміналу з банком здійснюється по електронних каналах зв'язку.

POS-термінал (Point Of Sale terminal) – потужна повнофункціональна система, що дає можливість для підключення й адаптації широкого спектра касової периферії. Сучасні POS-термінали мають всі переваги персональних комп'ютерів (ПК), їх функціональне призначення: реєстрація продажів, авторизація карток, програми лояльності, моніторинг касирів.

Використання POS-терміналів дозволяє автоматизувати операції з обслуговування картки та суттєво зменшити час обслуговування. Можливості і комплектація POS-терміналів варіюються в широких межах, однак типовий сучасний термінал обладнаний пристроями читання як карток із магнітною смугою, так і смарт-карток, енергонезалежною пам'яттю, портами для підключення PIN-клавіатури, принтера, з'єднання з комп'ютером або з електронним касовим апаратом.

Крім того, POS-термінал може бути оснащений модемом з можливістю автодозвону. POS-термінал володіє “інтелектуальними” можливостями – його можна програмувати. Все це дозволяє проводити не тільки on-line авторизацію карток із магнітною смугою і смарт-карток, але і використовувати при роботі зі смарт-картками режим off-line з накопиченням протоколів транзакцій, які під час сеансів зв'язку передаються в процесинговий центр. Під час сеансу зв'язку POS-термінал може також приймати і запам'ятовувати інформацію, передану ЕОМ процесингового центру. Подібним чином може здійснюватися перепрограмування POS-терміналів.

Системи POS забезпечують розрахунки продавця і покупця в точці продажу, здійснюють перевірку й обслуговування дебіторських і кредитних

карток покушця безпосередньо в місцях продажу товарів і послуг у рамках системи електронних платежів.

POS-термінали призначені для обробки транзакцій при фінансових розрахунках з використанням пластикових карток із магнітною смугою і смарт-карток. Використання POS-терміналів дозволяє автоматизувати операції з обслуговування цих карток й істотно зменшити час обслуговування.

Сучасний POS-термінал обладнаний:

- пристроями зчитування як з карток із магнітною смугою, так і зі смарт-карток;
- енергонезалежною пам'яттю;
- портами для підключення PIN-клавіатури (клавіатури для набору клієнтом PIN-коду);
- принтера;
- з'єднання з персональним комп'ютером або електронним касовим апаратом.

Під час цих сеансів POS-термінал може також приймати і запам'ятовувати інформацію, передану ЕОМ процесингового центру. В основному це бувають стоп-листи.

Схема функціонування системи POS показана на рис. 2.1.



Рисунок 2.1 – Схема POS-термінала

Процедура розрахунків у POS-терміналі наступна:

- покупець для оплати покупки надає свою дебіторську або кредитну

картку і вводить значення PIN для підтвердження особи;

- продавець, у свою чергу, вводить суму грошей, яку необхідно сплатити за покупку або послуги;

- потім у банк-еквайр (банк продавця) направляється запит на переказ грошей;

- банк-еквайр переадресовує цей запит у банк-емітент для перевірки справжності картки, наданої покупцем;

- якщо ця картка справжня і покупець має право застосовувати її для оплати продуктів і послуг, банк-емітент переводить гроші у банк-еквайр на рахунок продавця;

- після переказу грошей на рахунок продавця банк-еквайр посилає на POS-термінал повідомлення, в якому повідомляє про завершення транзакції;

- після цього продавець видає покупцеві товар і повідомлення.

Перш ніж буде здійснена транзакція, інформація про покупку повинна виконати складний шлях, під час проходження якого можливі спотворення і втрата повідомлень.

Для захисту системи POS слід дотримуватись таких вимог:

- перевірка PIN, введеного покупцем, повинна здійснюватися через систему банку-емітента. При пересиланні по каналах зв'язку значення PIN має бути зашифровано;

- повідомлення, що містять запит на переказ грошей (або підтвердження про переказ), повинні перевірятися на справжність для захисту від внесення змін при проходженні по лініях зв'язку.

Самим уразливим місцем системи POS є її POS-термінали. POS-термінал не захищений від зовнішніх впливів. Загрози для POS-терміналу пов'язані з можливістю розкриття секретного ключа, який знаходиться у POS-терміналі і служить для шифрування інформації, що передається цим терміналом у банк-еквайр. Загроза розкриття ключа терміналу досить реальна, тому що ці термінали встановлюються в таких, місцях, що не охороняються, це магазини, автозаправні станції тощо.

Для захисту від загроз зворотного та прямого трасування застосовують три методи: метод виведеного ключа, метод відкритих ключів, метод ключа транзакції.

Метод виведеного ключа забезпечує зміну ключа при кожній транзакції незалежно від її змісту. Для генерації ключа шифрування використовують

односпрямовану функцію від поточного значення ключа і деякої випадкової величини. Процес генерації ключа являє собою “блукання” по дереву. Схема виведення ключа з урахуванням двійкового надання номера S ключа показана на рис. 2.2

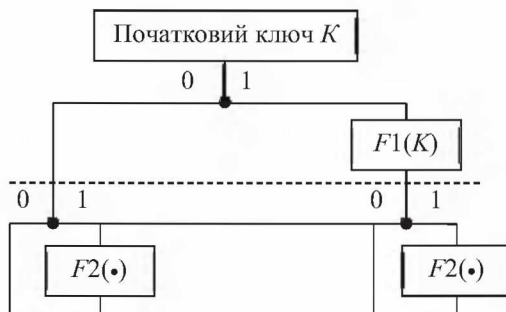


Рисунок 2.2 – Схема виведення ключа з урахуванням двійкового надання номера S ключа

Вершиною дерева є деяке початкове значення ключа K , щоб отримати ключ з номером S , число S надається у двійковій формі і при обчисленні враховується його структура починаючи зі старшого розряду.

Якщо L -й двійковий розряд числа $S = 1$, тоді до поточного значення ключа K застосовується односпрямована функція $FL(K)$, реалізована на основі алгоритму DES, де L – номер двійкового розряду ключа.

Якщо $L = 0$, тоді переходять до розгляду наступного розряду числа S не застосовуючи односпрямовану функцію.

Для необхідної швидкодії, кількість одиниць у числі S має бути менше або дорівнювати 10. Цей метод забезпечує захист тільки від загрози зворотного трасування. Недоліком даного методу є складність реалізації.

Метод відкритих ключів дозволяє забезпечити надійне шифрування переданої інформації і здійснює захист від будь-яких видів трасування. POS-термінал забезпечується секретним ключем для розшифрування повідомлення банку-еквайра. Цей ключ генерується при ініціалізації терміналу. Після генерації секретного ключа термінал посилає пов'язаний з ним відкритий ключ на ПК банку-еквайра. Обмін між учасниками взаємодії виконується за допомогою відкритого ключа кожного з них. Підтвердження справжності учасників здійснюється спеціальним центром реєстрації ключів

з використанням своєї пари відкритого і закритого ключів. Недоліком є досить низька швидкодія.

Метод ключа транзакції дозволяє шифрувати інформацію передану між POS-терміналом і банком-еквайром, при цьому використовується унікальний ключ, який може змінюватись від транзакції до транзакції. Для генерації нового ключа використовуються наступні складові: односпрямована функція від попереднього значення ключа, зміст транзакції, інформація отримана від картки. Цей метод забезпечує захист як від зворотного, так і від прямого трасування. Розкриття одного ключа не дає можливості зловмиснику дізнатися всі попередні і всі наступні транзакції. Недоліком є складність реалізації.

На сьогоднішній день 96% всіх POS-терміналів, підключених до Українського процесингового центру та розміщених в торгових мережах, приймають до оплати безконтактні картки.

Держателі платіжних карток оцінили перевагу і зручність безконтактних платежів, тому кількість оплат безконтактними картками значно зросла і займає понад 20 відсотків від усіх покупок картками в POS-терміналах. Динамічне зростання цих показників сприяє збільшенню кількості POS-терміналів, які приймають безконтактні картки.

2.2 Захист процесу еквайрингу в банкоматах

Банкоматом називають банківський автомат для видачі та інкасування готівки при операціях з пластиковими картками. Банкомат дозволяє власнику картки одержувати інформацію про поточний стан рахунку (в тому числі і роздруківкою на папері), а також проводити операції з перерахування коштів з одного рахунку на інший.

Банкомат забезпечений пристроєм для читання електронної платіжної картки, а також дисплеєм и клавіатурою для інтерактивної взаємодії з власником картки. Банкомат оснащений персональною ЕОМ, яка забезпечує керування банкоматом і здійснює контроль за його станом, що важливо, оскільки банкомат є сховищем готівок. Для забезпечення комунікаційних функцій банкомати оснащуються платами, а іноді і модемами.

Грошові купюри в банкоматі розміщуються в касетах, які знаходяться в спеціальному сейфі. Число касет визначає кількість номіналів купюр, які

видаються банкоматом. Розміри касет можна регулювати, що дозволяє заповнювати банкомат практично будь-якими купорами.

Сучасні банкомати можуть працювати у двох режимах роботи, а саме в автономному режимі (off-line) та в режимі реального часу (on-line).

Більшість моделей банкоматів розраховані на роботу в режимі реального часу з картками з магнітною смугою, однак з'явилися банкомати, що здатні працювати зі смарт-картками в автономному режимі.

Автономний режим роботи (off-line) банкомата характерний тим, що банкомат функціонує незалежно від комп'ютерів банку. Запис інформації про транзакції вводиться на внутрішній магнітний диск і виводиться на вбудований принтер. Перевагами автономного режиму банкомата є його відносна дешевизна і незалежність від якості ліній зв'язку.

Для захисту інформації, що зберігається на картці з магнітною смугою, застосовується її шифрування. Для того щоб банкомати одного і того ж банку сприймали пластикові картки з магнітною смугою, в них повинен бути використаний один ключ для шифрування та розшифрування інформації. Компрометація його хоча б на одному з банкоматів призведе до порушення захисту на всіх банкоматах.

Перевагами використання автономного режиму роботи є дешевизна обладнання та незалежність від якості ліній зв'язку.

Проте недоліком є те, що досить складно обслуговувати такі банкомати, тому що кожен день необхідно оновлювати стоп-листи. Крім того використання одного і того ж ключа шифрування на всіх банкоматах знижує криптостійкість системи.

Режим реального часу (on-line) характерний тим, що банкомат постійно підключений до процесингового центру, тобто обмін інформацією між ним і банкоматом відбувається безперервно. У цьому випадку всі необхідні дані про клієнта, рух коштів і залишки на його рахунку можуть перебувати в процесинговому центрі, усі транзакції по картковому рахунку виконуються ним у реальному масштабі часу.

Реєстрація транзакцій здійснюється безпосередньо на головному комп'ютері банку, а підтвердження про здійснення транзакції може видаватися на екран або на принтер банкомата для отримання роздрукованого чека.

Режим реального часу має низку переваг порівнянно з автономним

режимом:

- дає можливість клієнту не тільки отримати готівкові гроші, а й здійснювати маніпуляції зі своїм рахунком;

- централізована ідентифікація/автентифікація дозволяє істотно підвищити стійкість системи до компрометації ключів шифрування;

- централізована перевірка ідентифікатора користувача уможливорює оперативне оновлення списків заборонених до використання карток, а також введення обмежень на кількість готівки, яку може отримати клієнт протягом одного дня (для захисту від використання украдених карток).

Проте недоліками цього режиму роботи є необхідність наявності надійних каналів зв'язку між банкоматом і банком та можливість аналізу трафіка між банкоматом і головним комп'ютером банку.

При реалізації транзакції банкомат обмінюється з головним комп'ютером банку трьома повідомленнями:

- запит банкомата;
- відповідь банку;
- повідомлення банкомата про платіж.

Запит банкомату містить наступні дані:

- ідентифікатор банкомата;
- номер рахунку й іншу облікову інформацію клієнта;
- серійний номер карти;
- захисний символ;
- зашифрований PIN клієнта;
- кількість необхідних грошей;
- номер транзакції;
- код для всіх даних повідомлення.

Відповідь банку містить такі дані:

- ідентифікатор банкомата;
- код операції, що дозволяє (забороняє) платіж;
- номер транзакції;
- код для всіх даних повідомлення.

Повідомлення банкомата про платіж містить такі дані:

- ідентифікатор банкомату;
- номер транзакції;
- код для всіх даних повідомлення.

У цьому обміні повідомленнями для перевірки цілісності даних використовується код автентифікації повідомлення MAC (Message Authentication Code).

В даний час поширеною формою використання банкомата є створення так званої мережі банкоматів, в якій бере участь кілька банків.

Банки-учасники переслідують наступні цілі:

- зменшення вартості операцій для учасників;
- розподіл витрат і ризиків при впровадженні нових видів послуг між учасниками;

- подолання географічних обмежень для зручності користувача.

Проте при спільному використанні декількома банками мережі банкоматів виникає проблема захисту конфіденційної інформації банків один від одного. Для вирішення цієї проблеми запропоновано схему централізованої перевірки PIN-коду кожним банком у своєму центрі зв'язку з банкоматом. Ускладнюється також система розподілу ключів між усіма учасниками мережі.

На рис. 2.3 показана схема проходження інформації про PIN-код клієнта між банком-емітентом і банком-еквайром.

Якщо клієнт банку 2 (емітент) звертається до банкомату банку 1 (еквайр), то в мережі банкоматів відбуваються наступні дії:

- 1) після процедур ідентифікації та автентифікації (введення картки та значення PIN відповідно) банкомат визначає чи має цей клієнт рахунок у банку 1;

- 2) якщо ні, то транзакція направляється в маршрутизатор, який використовує ідентифікаційний номер банку 2 емітента та надсилає цю транзакцію на сервер банку 2 або проводить перевірку PIN для банку 2;

- 3) якщо перевірка PIN проводиться на сервері банку 2, то там виводиться повна інформація про транзакцію і перевіряється достовірність введеного PIN-коду;

- 4) незалежно від результату, сервер банку 2 пересилає повідомлення про результат перевірки на сервер банку 1.

Вимоги до банку-емітента:

- карти, які випускаються цим банком повинні прийматися всіма банкоматами мережі;

- банк-емітент повинен володіти технічною можливістю перевірки

власних клієнтів.



Рисунок 2.3 – Схема проходження інформації про PIN клієнта між банком-емітентом і банком-еквайром

Вимоги до банку-еквайра:

- у банкоматі цього банку повинна бути реалізована перевірка приналежності транзакцій;
- якщо немає можливості перевірити правильність PIN іншого банку, банк-еквайр повинен передати дані на мережевий маршрутизатор.

Для захисту взаємодії банків один з одним і банкоматами має здійснюватися кінцеве шифрування інформації, яка передається по мережі. З цією метою вся мережа банкоматів поділяється на зони. Для забезпечення безпечної взаємодії серверів банків, у кожній із зон діють свої ключі шифрування.

3 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

3.1 Особливості функціонування протоколу SET

Держателі платіжних карток оцінили зручність платежів та переказів з картки на картку в Інтернеті. Відбувається постійне зростання кількості таких переказів, зокрема частка переказів від загальної кількості фінансових транзакцій за платіжними картками. Слабким місцем мережної інфраструктури є незахищені канали зв'язку, де існує можливість появи неіснуючих платежів, перехоплення та несанкціонованого використання платіжних даних, інших проявів шахрайства та зловживань. Такі випадки траплялися в Інтернеті. Існують два шляхи захисту передачі інформації: ізолювання мережі, яка використовується для обробки платежів, тобто використання приватних мереж, і шифрування даних.

Загально визнано, що асиметричні алгоритми шифрування забезпечують вищий рівень надійності та безпеки. Найбільш поширене шифрування за допомогою відкритих ключів. Для розшифрування використовуються таємні ключі. Кількість можливих комбінацій, придатних для розшифрування зашифрованої за допомогою відкритих ключів інформації, залежить від довжини ключа в бітах. Вживання довгих послідовностей у ролі ключів дозволяє випереджати можливості сучасних комп'ютерів, забезпечуючи надійний захист найважливішої інформації. Донедавна в Інтернеті для захисту інформації найчастіше застосовувалися ключі довжиною 40 бітів. Але ці ключі були легко розкриті. Нині в Інтернеті розповсюджені ключі довжиною 1024 бітів або навіть довші, що робить практично неможливим їх розкриття.

Для того щоб покупець, тобто власник кредитної картки міг без побоювань заплатити за покупку через мережу, необхідно мати надійний механізм захисту передачі електронних платежів. Такий підхід полягає в негайній авторизації і шифруванні інформації в мережі Інтернет з використанням протоколів SSL/TLS і SET.

Протокол SSL (Secure Sockets Layer – рівень захищених сокетів) забезпечує встановлення безпечного з'єднання між клієнтом і сервером.

Протокол TLS (Transport Layer Security – захист на транспортному рівні)

забезпечує можливість автентифікації і безпечної передачі даних.

Протокол SET (Secure Electronic Transaction – безпечні електронні транзакції) передбачає шифрування виключно фінансової інформації.

Протокол SET розроблено з метою захисту транзакцій, здійснюваних у Інтернет за допомогою пластикових платіжних карток. У розробці оригінальних специфікацій SET брали участь багато відомих компаній, включаючи IBM, Microsoft, Netscape, RSA, Verisign.

Протокол SET забезпечує такі три види сервісу:

- 1) створення захищеного комунікаційного каналу, що зв'язує всі сторони, які беруть участь у транзакції;
- 2) забезпечення довіри за допомогою цифрових сертифікатів X.509 v3;
- 3) забезпечення таємності через те, що інформація виявляється доступною тільки учасникам транзакції і тільки тоді і там, де вона необхідна.

Вимоги до протоколу SET, що мають дотримуватися при обробці платежів по кредитних картках у Інтернет й інших подібних мережах:

1) конфіденційність платежу й інформації про замовлення. Необхідно гарантувати власникам пластикових карт, що дана інформація надійно захищена і виявиться доступною тільки тому, кому вона призначена. Конфіденційність до того ж зменшує ризик обману кожного з учасників у здійсненні транзакції сторін чи злочинних дій третьої сторони. Для забезпечення конфіденційності застосовується шифрування;

2) гарантія цілісності всіх переданих даних означає, що в ході передачі інформація, що міститься у повідомленні SET, не перетерпить ніяких змін. Для забезпечення цілісності служить механізм електронного підпису;

3) автентифікація пред'явника кредитної картки як законного власника відповідного рахунка. Механізм, що зв'язує пред'явника кредитної картки з відповідним номером рахунка, має зменшувати імовірність шахрайства і знижувати загальну вартість обробки платежів. Для перевірки того, що пред'явник кредитної картки є законним власником відповідного дійсного рахунка, застосовуються такі засоби, як електронний підпис і сертифікати;

4) автентифікація продавця як особи, що має право приймати транзакції по кредитних картках, за допомогою з'ясування його зв'язку з відповідною фінансовою організацією. Ця вимога доповнює попередню. Власники платіжних карток повинні мати можливість ідентифікувати продавців, яким вони можуть направляти захищені транзакції. У цьому випадку теж

використовуються електронні підписи і сертифікати;

5) гарантоване використання кращих конструктивних рішень і методів захисту для забезпечення найвищого ступеня захисту всіх легальних учасників електронних комерційних транзакцій. Специфікації SET будуються на застосуванні криптографічних алгоритмів і протоколів, що мають високий рівень захищеності і добре в цьому відношенні перевірених;

6) незалежність протоколу від механізмів захисту транспортування даних за відсутності будь-яких обмежень на використання таких механізмів. SET може забезпечувати захист, спираючись безпосередньо і винятково на стек протоколів TCP/IP (Transmission Control Protocol/Internet Protocol – протокол управління передачею/протокол Інтернету). Але при цьому SET ніяк не впливає на роботу інших механізмів захисту, таких як IPSec (IP Security) чи SSL/TLS, і не залежить від них;

7) сприяння і підтримка сумісності між прикладними програмними і мережними продуктами різних постачальників. Протоколи і формати SET не залежать від апаратних платформ, операційних систем і програмного забезпечення, призначеного для роботи в Web.

Головні можливості SET. Щоб відповідати описаним вище вимогам, у протоколі SET реалізовані такі можливості:

1) **конфіденційність інформації.** Інформація про рахунок власника карти і платежу захищається під час пересилання по мережі. Цікава і важлива особливість SET полягає в тому, що продавець при цьому не може з'ясувати номер кредитної картки її власника – ця інформація виявляється доступною тільки тому, хто видав кредитну картку банку. Для забезпечення конфіденційності використовується шифрування за традиційною схемою за допомогою алгоритму DES;

2) **цілісність даних.** Інформація про платіж, що посиляється власником картки продавцю, містить інформацію про замовлення, особисті дані й інструкції зі здійснення платежу. SET гарантує, що зміст відповідних повідомлень не буде змінено на шляху їх проходження. Цілісність даних досягається за допомогою електронних підписів RSA, що використовують геш-коди. Деякі повідомлення захищаються також за допомогою алгоритму HMAC (Hash-based Message Authentication Code – геш-код автентифікації повідомлень), що використовує SHA (Secure Hash Algorithm – безпечний алгоритм гешування). Автентифікація рахунку власника картки SET дає

продавцю можливість перевірити, чи є пред'явник кредитної картки законним користувачем відповідного дійсного рахунка. Для цієї мети у SET передбачене використання цифрових сертифікатів X.509 v3 з підписами RSA;

3) автентифікація продавця. SET дозволяє власнику картки перевірити, чи має продавець відношення до відповідної фінансової організації і право приймати платежі по кредитних картках. Для цієї мети в SET передбачене використання цифрових сертифікатів X.509 v3 з підписами RSA.

На відміну від IPsec і SSL/TLS протокол SET для вирішення кожної конкретної задачі пропонує тільки по одному алгоритму. Це пояснюється тим, що SET є єдиним додатком, що відповідає цілком конкретному набору вимог, тоді як IPsec і SSL/TLS відносяться до універсальних протоколів, призначених для підтримки широкого спектра додатків.

Формат сертифіката відкритого ключа у протоколі SET задовольняє стандарту X.509 v3. Сертифікат містить такі дані:

- версію протоколу X.509 (завжди встановлюється значення, рівне 3);
- серійний номер сертифіката (serial number) – унікальний цілочисловий номер сертифіката, присвоюється центром сертифікації, що видав сертифікат;
- ідентифікатор алгоритму (algorithm identifier) електронного підпису, використовуюваного центром сертифікації для підписування сертифіката;
- ім'я центру (issuer name) сертифікації, генеруючого сертифікат;
- термін початку дії сертифіката;
- термін закінчення дії сертифіката;
- ім'я власника (subject name) сертифіката;
- ідентифікатор алгоритму, в якому буде використовуватися сертифікований ключ;
- значення відкритого ключа, який сертифікується;
- рівень власника сертифіката в протоколі SET, тип сертифіката (сертифікат власника картки, сертифікат торгової точки тощо);
- електронний підпис сертифіката, зроблений з використанням центру сертифікації.

Учасниками транзакцій, що здійснюються за допомогою SET, є такі сторони (рис. 3.1):

- власник платіжної картки (покупець, клієнт). У середовищі електронних платежів індивідуальні і корпоративні споживачі взаємодіють із

продавцями зі своїх персональних комп'ютерів через Інтернет. Власником картки в даному випадку є будь-який зареєстрований власник пластикової платіжної картки (MasterCard, Visa і т.п.), виданої йому деяким уповноваженим емітентом;

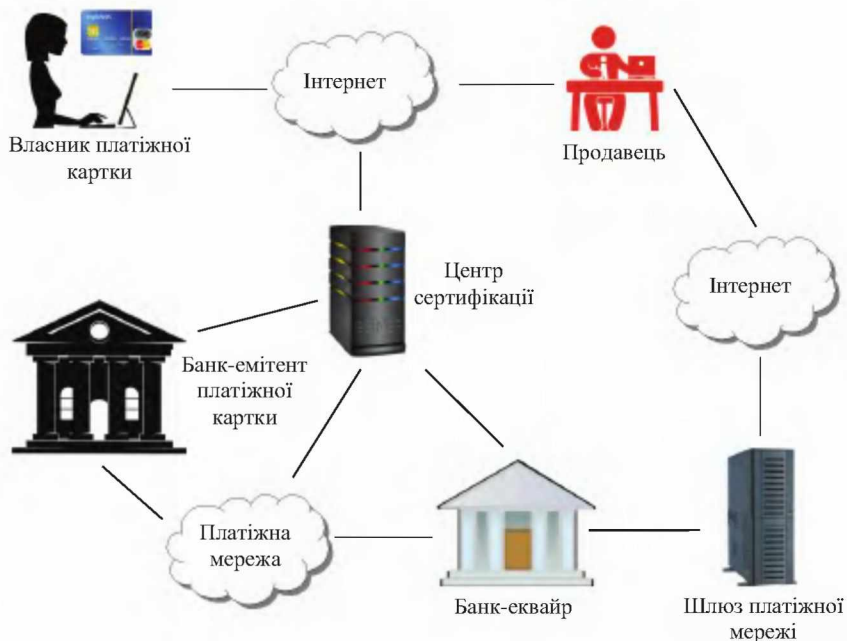


Рисунок 3.1 – Компоненти захищеної системи електронної комерції

– продавець. Продавець є особою, у якої власник картки може придбати товари або послуги. Звичайно такі товари чи послуги пропонуються на продаж на Web-вузлі або по електронній пошті. Продавець, що має право приймати платежі по платіжних картках, повинен мати відповідні відносини з операційним центром;

– емітент платіжної картки. Банк-емітент, що видав платіжну картку відповідній особі (власнику картки). Як правило, відкрити рахунок можна поштою або з'явившись особисто в офіс емітента. Усю відповідальність за оплату заборгованості власника картки за даною картою несе емітент картки;

– банк-еквайр (операційний центр). Фінансова організація, що веде розрахунки з продавцем, який виконує авторизацію платіжних карток і здійснює відповідні платежі. Продавці звичайно готові приймати кредитні картки різних видів, але не хочуть мати справ з великим числом різних банківських асоціацій чи безліччю окремих емітентів платіжних карток. Операційний центр проводить для продавця перевірку того, що рахунок кредитної карти є дійсним, і пропонує покупку щодо вартості не виходить за рамки припустимого кредитного ліміту. Операційний центр також виконує електронний переказ грошових сум на рахунок продавця. Згодом операційний центр отримує за це визначену компенсацію від емітента картки через банківську платіжну мережу;

– шлюз платіжної мережі (payment gateway). Сукупність засобів, контрольованих операційним центром чи уповноваженою їм третьою стороною і використовуваних для обробки платіжних повідомлень продавця. Шлюз платіжної мережі пов'язує SET й існуючі банківські платіжні мережі, виконуючи функції авторизації і передачі платежів. Продавець обмінюється повідомленнями SET зі шлюзом платіжної мережі через Інтернет, а шлюз платіжної мережі зв'язаний безпосередньо чи по внутрішній мережі із системою обробки фінансових документів відповідного операційного центру;

– центр сертифікації (Certification Authority). Об'єкт, якому довіряється видавати сертифікати X.509 v3 відкритих ключів власників карток, продавців і шлюзів платіжної мережі. Успішна робота SET багато в чому залежить від наявності добре організованої інфраструктури сертифікації, доступної для використання у відповідних цілях.

Опишемо послідовність подій, що відбуваються під час транзакції, а потім зупинимося докладніше на деяких криптографічних деталях даного процесу:

1) покупець відкриває рахунок. Покупець відкриває рахунок кредитної картки (наприклад, MasterCard чи Visa) у банку, що здійснює електронні платежі і підтримує SET;

2) покупець отримує сертифікат. Після встановленої процедури перевірки особистості покупець отримує цифровий сертифікат X.509 v3, підписаний банком. Цей сертифікат засвідчує відкритий ключ RSA покупця і термін дії цього ключа. Він також установлює гарантовану банком відповідність між парою ключів покупця і його кредитною карткою;

3) продавець отримує свої сертифікати. Продавець, що збирається приймати оплату за платіжною карткою визначеного типу, повинен отримати два сертифікати двох своїх відкритих ключів: один із них використовуватиметься для електронного підпису, а інший – для обміну ключами. Продавцю також буде потрібна копія сертифіката відкритого ключа шлюзу платіжної мережі;

4) покупець розміщує замовлення. Цей процес може припускати, що покупець спочатку повинний відвідати Web-вузол продавця, щоб вибрати придатний товар і визначити ціну. Після цього покупець відправляє продавцю список потрібних йому товарів, а продавець у відповідь висилає бланк замовлення з зазначеними в ньому списком обраних товарів, цінами, загальною вартістю замовлення і номером замовлення;

5) перевірка продавця. Разом із бланком замовлення продавець висилає копію свого сертифіката, щоб покупець мав можливість переконатися в тому, що він дійсно має справу з дійсним продавцем;

6) замовлення і платіж відправляються продавцю. Покупець відправляє замовлення і платіжну інформацію продавцю, додаючи до них свій сертифікат. Замовлення підтверджує покупку товарів, зазначених у бланку замовлення. Платіжна інформація містить необхідні дані кредитної картки. Платіжна інформація зашифровується таким чином, щоб продавець не зміг її прочитати. Сертифікат покупця дозволяє продавцю виконати верифікацію покупця;

7) продавець запитує авторизацію платежу. Продавець відправляє платіжну інформацію шлюзу платіжної мережі з запитом підтвердження того, що доступний покупцю кредит достатній для здійснення даного платежу;

8) продавець підтверджує замовлення. Продавець відправляє покупцю підтвердження замовлення;

9) продавець доставляє товари або надає послуги. Продавець організовує доставку товарів або виконання послуг покупцю;

10) продавець запитує отримання платежу. Цей запит відправляється шлюзу платіжної мережі, що обробляє всі платіжні доручення.

Протокол SET використовує подвійний підпис (dual signature). Мета подвійного підпису така сама, як і стандартного електронного підпису: гарантувати автентифікацію і цілісність даних.

Клієнт пов'язує два повідомлення, які призначені для двох різних одержувачів. У цьому випадку, клієнт хоче послати інформацію про замовлення (Order Information – OI) продавцю і платіжну інформацію (Payment Information – PI) банку. Продавцеві не потрібно знати номер кредитної картки клієнта, і банку не потрібно знати деталі замовлення клієнта. Посилання необхідне, щоб клієнт зміг довести, що платіж призначено для цього замовлення. При цьому потрібно поєднати ці зведення так, щоб їх можна було використовувати при виникненні конфлікту.

Клієнт відправляє продавцю два підписаних повідомлення – OI (замовлення) і PI (платіж), а продавець пересилає повідомлення PI у банк. Якщо продавець одержує від покупця якесь інше замовлення, то продавець зможе заявити, що дане повідомлення PI оплачує нове, а не старе повідомлення OI. Зв'язування виключає таку можливість.

На рис. 3.2 показана схема використання подвійного підпису.

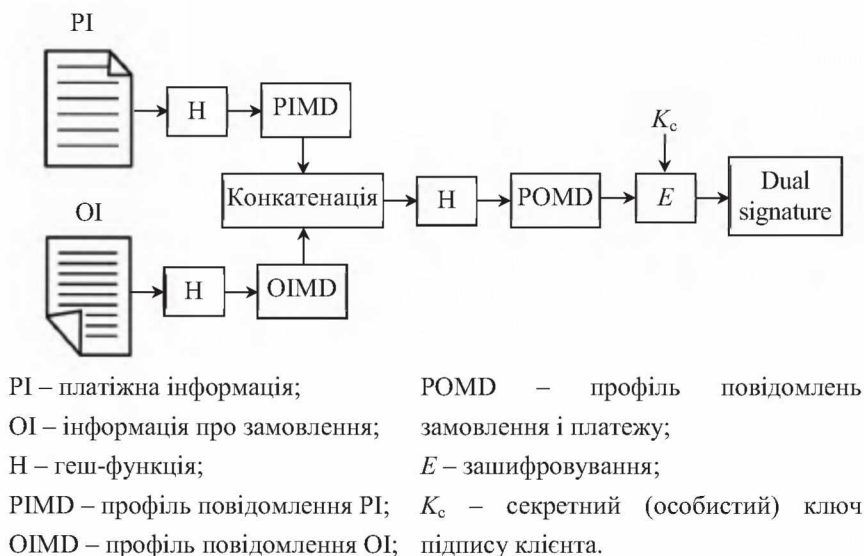


Рисунок 3.2 – Створення подвійного підпису

Спочатку клієнт використовуючи алгоритм гешування для повідомлень PI і OI. Два отриманих геш-коди зв'язуються операцією конкатенації, і для результату зв'язування теж обчислюється геш-код. Нарешті, клієнт зашифрує підсумковий геш-код з використанням свого секретного ключа

K_c електронного підпису, у результаті отримуючи подвійний підпис. Уся процедура формально може бути записана в такому вигляді:

$$DS = E_{K_c} \left[H(H(PI) \| H(OI)) \right],$$

де K_c – особистий ключ електронного підпису клієнта.

Тепер припустимо, що продавець має подвійний підпис DS, повідомлення OI і профіль повідомлення PIMD. Крім того, у продавця є відкритий ключ клієнта, що був витягнутий із сертифіката клієнта. У таких умовах продавець може обчислити два значення:

$$H(PIMD \| H(OI)) \text{ та } D_{K_a} [DS],$$

де K_a – відкритий ключ електронного підпису клієнта.

Якщо обидва значення виявляються рівними, продавець вважає, що підпис перевірений. Точно так само, маючи DS, PI, профіль повідомлення OIMD і відкритий ключ клієнта, банк може обчислити

$$H(H(PI) \| OIMD) \text{ та } D_{K_a} [DS].$$

І знову, якщо ці значення виявляються рівними, банк вважає, що підпис клієнта перевірений. Підводячи підсумок, можна сказати, що:

- продавець отримує повідомлення OI і виконує перевірку підпису клієнта;
- банк отримує повідомлення PI і виконує перевірку підпису клієнта;
- повідомлення OI і PI виявляються зв'язаними, і покупець може довести їх зв'язок.

Типи транзакцій, підтримувані SET, перераховані в табл. 3.1.

Таблиця 3.1 – Типи транзакцій SET

Типи транзакцій	Опис
1	2
Cardholder registration (реєстрація власника карти)	Власники платіжних карт мають зареєструватися в центрі сертифікації, щоб мати можливість відправляти повідомлення SET продавцям

Продовження таблиці 3.1

1	2
Merchant registration (реєстрація продавця)	Продавці повинні зареєструватися в центрі сертифікації, щоб мати можливість обмінюватися повідомленнями SET з покупцями і шлюзами платіжної мережі
Purchase request (вимога на закупівлю)	Повідомлення, що відправляється покупцем продавцю, що містить ОІ для продавця і РІ для банку
Payment authorization (дозвіл на оплату)	Послідовність повідомлень, якими обмінюється продавець зі шлюзом платіжної мережі для авторизації відповідного платежу з рахунку відповідної кредитної картки
Payment capture (одержання платежу)	Дозволяє продавцю запросити отримання відповідного платежу в шлюзу платіжної мережі
Certificate inquiry and status (запит сертифіката і його статусу)	Якщо центр сертифікації не може швидко обробити запит на одержання сертифіката, у відповідь покупцю чи продавцю відправляється повідомлення про те, що запитуючій стороні потрібно звернутися за відповіддю на запит повторно пізніше. Власник платіжної картки або покупець посилає повідомлення Certificate Inquiry для того, щоб з'ясувати стан процесу обробки його запиту сертифіката й отримати сертифікат, якщо запит був удоволений
Purchase inquiry (запит на постачання)	Дозволяє власнику платіжної карти перевірити стан процесу обробки замовлення після отримання відповіді на повідомлення про розміщення замовлення. Зверніть увагу на те, що це повідомлення містить інформацію не про недопоставлені товари, а тільки про авторизацію, проводку платежів і з'ясування кредитних можливостей
Authorization reversal (відкликання запиту авторизації)	Дозволяє продавцю змінити раніше зроблені запити на дозвіл здійснити платіж. Якщо замовлення не може бути виконане взагалі, продавець відкликає всі дані відповідного запиту. Якщо ж замовлення не може бути виконане частково (наприклад, коли постачання частини товарів відкладається), продавець відкликає частину підлягаючої авторизації суми
Capture reversal (відкликання запиту на здійснення платежу)	Дозволяє продавцю виправити помилки в запитах на здійснення платежу, наприклад, якщо помилково службовцем була введена неправильна сума
Batch administration (пакедне адміністрування)	Дозволяє продавцю обмінюватися інформацією зі шлюзом платіжної мережі з питань, що стосуються груп платежів
Credit reversal (відкликання запиту на кредит)	Дозволяє продавцю змінити параметри раніше запитаного кредиту

Закінчення таблиці 3.1

1	2
Credit (кредит)	Дозволяє продавцю відкрити кредит у відношенні рахунка власника платіжної картки, наприклад, при поверненні товару покупцем чи ушкодженні товару в процесі доставки. Зверніть увагу на те, що ініціатором повідомлення Credit завжди є продавець, а не власник платіжної картки. Весь обмін даними між власником платіжної картки і продавцем, у результаті якого відкривається кредит, відбувається за рамками протоколу SET
Payment gateway certificate request (запит сертифіката шлюзу платіжної мережі)	Дозволяє продавцю запросити сертифікат шлюзу платіжної мережі й одержати копії поточних сертифікатів ключів обміну і електронного підпису
Error message (повідомлення про помилку)	Говорить про те, що сторона, яка відповідає, відмовила в прийомі повідомлення через неправильний формат останнього, або тому, що не вдалося виконати верифікацію вмісту повідомлення

Обробка платежів у протоколі SET. Розглянемо докладно такі типи транзакцій:

- вимога на закупівлю (Purchase Request);
- дозвіл на оплату (Payment Authorization);
- отримання платежу (Payment Capture).

Вимога на закупівлю (Purchase Request). До того як почати обмін даними вимоги на закупівлю (Purchase Request), власник платіжної картки повинен завершити перегляд списку доступних товарів, вибрати потрібні й оформити замовлення. Даний попередній етап закінчується відправленням продавцем бланка замовлення покупцю. Усі ці попередні операції не зв'язані з SET.

Обмін даними вимоги на закупівлю складаються з чотирьох повідомлень:

- ініціюючий запит (Initiate Request);
- відповідь на ініціюючий запит (Initiate Response);
- вимога на закупівлю (Purchase Request);
- відповідь на вимогу на закупівлю (Purchase Response).

Щоб власник платіжної картки мав можливість відправляти

повідомлення SET продавцю, необхідно одержати копії сертифіката продавця і сертифіката шлюзу платіжної мережі. Запити на отримання цих сертифікатів містяться в повідомленні Initiate Request, що покупець відправляє продавцю. Це повідомлення містить інформацію про тип кредитної картки, використовуваної покупцем, ідентифікатор, призначений покупцем даній парі повідомлень “запит-відповідь”, і значення оказії, покликане гарантувати оригінальність повідомлення.

Продавець генерує відповідь і підписує її своїм особистим ключем електронного підпису. Відповідь має включати значення оказії покупця, інше значення оказії, що покупець повинен буде повернути в наступному повідомленні, а також ідентифікатор даної транзакції. Крім підписаної відповіді, повідомлення Initiate Response містить сертифікат підпису продавця і сертифікат шлюзу платіжної мережі для обміну ключами.

Власник платіжної картки перевіряє дійсність сертифікатів продавця і шлюзу платіжної мережі шляхом перевірки підписів відповідних центрів сертифікації, а потім створює повідомлення OI і PI. В обох цих повідомленнях міститься ідентифікатор транзакції, згенерований продавцем. Повідомлення OI безпосередньо не включає таких даних замовлення, як кількість чи ціна товарів, а містить посилання на замовлення, створене у процесі обміну повідомленнями між продавцем і покупцем на етапі узгодження ще до першого повідомлення SET. Потім власник платіжної картки готує повідомлення Purchase Request (рис. 3.3). Для цього власник платіжної картки генерує одноразовий ключ K_S для схеми симетричного шифрування. Це повідомлення складається з наступних блоків інформації.

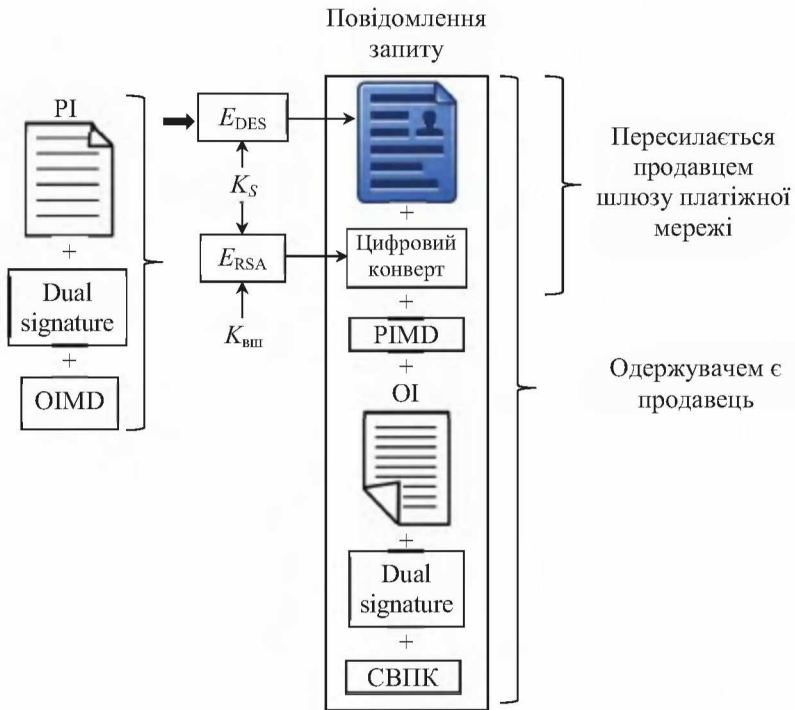
1) **Інформація про платіж.** Пересилається продавцем шлюзу платіжної мережі і містить такі дані:

- дані PI;
- подвійний підпис, обчислений для сукупності PI і OI та підписаний з використанням секретного ключа підпису покупця;
- профіль повідомлення OIMD;
- цифровий конверт.

Значення профілю повідомлення OIMD необхідно для того, щоб шлюз платіжної мережі міг перевірити подвійний підпис. Усі зазначені елементи зашифровуються за допомогою K_S .

Цифровий конверт формується шляхом зашифрування за допомогою

відкритого ключа шлюзу $K_{\text{вп}}$ платіжної мережі, призначеного для обміну ключами. Цей елемент називається **цифровим конвертом**, оскільки для того, щоб отримати можливість прочитати елементи, цей конверт необхідно відкрити (тобто розшифрувати). Значення K_S залишається продавцю невідомим. Тому продавець не зможе прочитати нічого з усієї цієї стосовної до платежу інформації.



PI – платіжна інформація;

OI – інформація про замовлення;

PIMD – профіль повідомлення PI;

OIMD – профіль повідомлення OI;

E – зашифрування RSA для
асиметричної та DES для
симетричної схеми;

K_S – тимчасовий ключ симетричної
схеми шифрування;

$K_{\text{вп}}$ – відкритий ключ шлюзу
платіжної мережі для обміну
ключами;

СВПК – сертифікат власника
платіжної картки.

Рисунок 3.3 – Структура повідомлення Purchase Request,
що відправляється власником платіжної картки

2) **Інформація про замовлення.** Ця інформація потрібна продавцю і містить такі дані:

- дані ОІ;
- подвійний підпис, обчислений для сукупності РІ і ОІ та підписаний з використанням секретного ключа підпису покупця;
- профіль повідомлення РІМД.

Значення РІМД необхідно для того, щоб продавець міг перевірити подвійний підпис. Зазначимо, що дані ОІ відправляються у відкритому вигляді.

3) **Сертифікат власника платіжної картки.** Містить сертифікат відкритого ключа електронного підпису власника платіжної картки. Цей сертифікат необхідний як продавцю, так і шлюзу платіжної мережі.

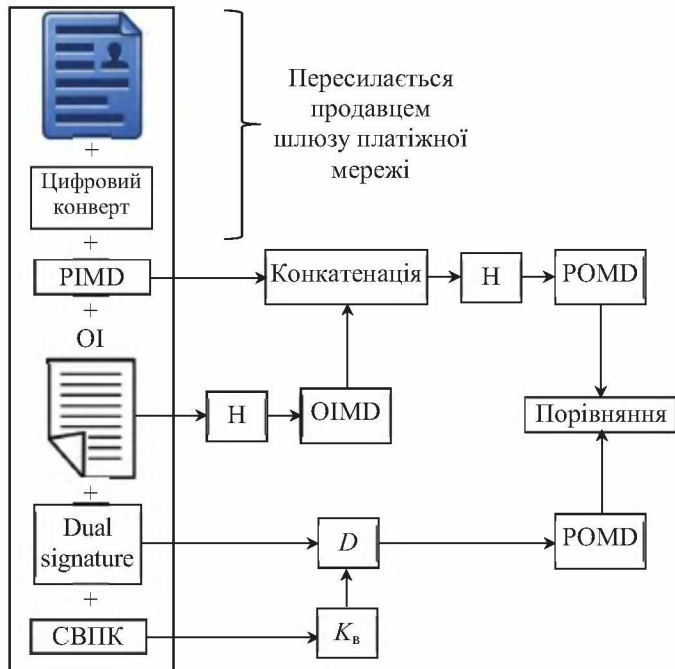
Після одержання повідомлення Purchase Request продавець виконує такі дії (рис. 3.4):

- перевіряє сертифікати власника платіжної картки за допомогою підписів центрів, що містяться в них, сертифікації;
- перевіряє подвійний підпис за допомогою відкритого ключа електронного підпису власника платіжної картки. Це дозволяє переконатися в тому, що замовлення не було змінено під час пересилання і було підписане власником платіжної картки;
- обробляє замовлення і пересилає платіжну інформацію шлюзу платіжної мережі для авторизації платежу (відповідний процес буде описаний нижче);
- відправляє повідомлення Purchase Response власнику платіжної картки.

Повідомлення Purchase Response містить блок відповіді, що підтверджує замовлення і посилається на відповідний номер транзакції. Цей блок підписується продавцем за допомогою його секретного ключа електронного підпису. Після цього блок разом з підписом, а також сертифікат підпису продавця відправляються власнику платіжної картки.

Коли програмне забезпечення, установлене на комп'ютері власника платіжної картки, одержує повідомлення Purchase Response, воно перевіряє спочатку сертифікат продавця, а потім підпис блока відповіді.

Повідомлення
запиту



OI – інформація про замовлення;
 OIMD – профіль повідомлення OI;
 H – геш-функція;
 POMD – профіль повідомлень
 замовлення і платежу;

D – розшифрування RSA;
 K_v – відкритий ключ підпису
 покупця;
 СВІПК – сертифікат власника
 платіжної картки.

Рисунок 3.4 – Схема обробки повідомлення Purchase Request продавцем

Дозвіл на оплату (Payment Authorization). Під час обробки замовлення, що надійшло від власника платіжної картки, продавець виконує авторизацію транзакції (одержання дозволу на оплату) за допомогою шлюзу платіжної мережі. Таке одержання дозволу на оплату (авторизація платежу) означає санкціонування транзакції емітентом платіжної картки. Авторизація дає продавцю гарантію того, що він одержує плату за проданий товар, і тому продавець може виконати доставку товарів чи послуг покупцю. Обмін даними для одержання дозволу на оплату формується з двох повідомлень:

- запит дозволу на оплату (Authorization Request);
- відповідь на запит дозволу на оплату (Authorization Response).

Повідомлення Authorization Request складається з таких блоків інформації.

1) **Інформація про платіж.** Ця інформація була одержана від покупця і містить такі дані:

- дані PI;
- подвійний підпис, обчислений для сукупності PI і OI і підписана з використанням особистого ключа підпису покупця;
- профіль повідомлення OIMD;
- цифровий конверт.

2) **Інформація авторизації.** Ця інформація генерується продавцем і містить такі дані:

- блок авторизації, що включає ідентифікатор транзакції, підписаний особистим ключем електронного підпису продавця і зашифрований тимчасовим ключем схеми симетричного шифрування, що генерується продавцем;
- цифровий конверт, сформований шляхом зашифрування тимчасового ключа за допомогою відкритого ключа шлюзу платіжної мережі, призначеного для обміну ключами.

3) **Сертифікати.** Продавець включає у повідомлення сертифікат електронного підпису власника платіжної картки (служить для перевірки подвійного підпису), сертифікат ключа свого електронного підпису (дозволяє перевірити підпис продавця) і сертифікат свого ключа для обміну ключами (необхідний для відповіді шлюзу платіжної мережі).

Маючи ці дані, шлюз платіжної мережі виконує такі дії:

- перевіряє всі сертифікати;
- розшифровує цифровий конверт блока даної авторизації, щоб одержати ключ для схеми симетричного шифрування, а потім розшифровує блок даних авторизації;
- перевіряє підпис продавця для блока даних авторизації;
- розшифровує цифровий конверт блока платіжної інформації, щоб одержати ключ для схеми симетричного шифрування, а потім розшифровує блок платіжної інформації;
- перевіряє подвійний підпис блоку платіжної інформації;

– перевіряє збіг ідентифікатора транзакції, одержаного від продавця, з ідентифікатором, включеним до складу даних PI, що надійшли (через продавця) від власника платіжної картки;

– запитує й отримує дозвіл на оплату в емітента платіжної картки.

Маючи дозвіл на оплату в емітента платіжної картки, платіжний шлюз повертає продавцю повідомлення Authorization Response. Це повідомлення складається з таких блоків інформації.

1) **Інформація авторизації**. Включає блок авторизації, підписаний особистим ключем електронного підпису шлюзу платіжної мережі і шифрований згенерованим шлюзом платіжної мережі одноразовим ключем для схеми симетричного шифрування. Крім того, включає цифровий конверт, що містить цей одноразовий ключ, зашифрований за допомогою відкритого ключа продавця, використовуваного для обміну ключами.

2) **Інформація мандата на отримання платежу** (capture token). Ця інформація буде використана для здійснення платежу згодом. Даний блок має ту ж форму, що і попередній, тобто містить підписаний і зашифрований мандат з цифровим конвертом. Цей мандат не обробляється продавцем, а має бути просто повернутий їм у тому же вигляді шлюзу платіжної мережі в запиті на оплату.

3) **Сертифікат**. Сертифікат електронного підпису шлюзу платіжної мережі.

Маючи підтвердження авторизації платежу від шлюзу платіжної мережі, продавець може виконати доставку товарів чи послуг покупцю.

Одержання платежу (Payment Capture). Щоб отримати плату за товари чи послуги, продавець звертається до шлюзу платіжної мережі з ініціативою виконання транзакції одержання платежу, що складається з двох повідомлень:

– повідомлення запиту на одержання оплати (Capture Request);

– повідомлення відповіді на запит на одержання оплати (Capture Response).

Для повідомлення Capture Request (запит на оплату) продавець генерує, підписує і зашифровує блок даних запиту на оплату, що включає суму платежу й ідентифікатор транзакції. Дане повідомлення має також включати раніше одержаний (у повідомленні Authorization Response) зашифрований мандат на одержання платежу для даної транзакції і, крім того, сертифікати

ключів продавця для електронного підпису й обміну ключами.

Маючи це повідомлення, шлюз платіжної мережі розшифровує і перевіряє блок даних запиту на оплату, а також розшифровує і перевіряє блок мандата на одержання платежу. Потім перевіряється відповідність між даними цих двох блоків. Після цього шлюз платіжної мережі створює розрахунковий запит, що відсилається емітенту платіжної картки по закритій платіжній мережі. У результаті цього запиту кошти перераховуються на рахунок продавця.

Потім шлюз за допомогою повідомлення Capture Response (відповіді на запит на оплату) сповіщає продавця про перерахування коштів. Повідомлення містить підписаний і зашифрований шлюзом блок даних відповіді на запит на оплату. Крім того, це повідомлення містить сертифікат електронного підпису шлюзу платіжної мережі. Програмне забезпечення, установлене на комп'ютері продавця, маючи дане повідомлення, зберігає його для використання в програмах обліку й узгодження коштів, що надходять від операційного центру.

3.2 Протокол захисту інформації в електронних платіжних системах 3-D Secure

3-D Secure (Three-Domain Secure) є торговою маркою корпорації віза, розроблена з метою безпеки електронних платежів. Протокол дозволяє додати процесу авторизації перевірку справжності в режимі реального часу. Це автентифікація заснована на застосуванні трьох доменів (рис. 3.5):

- 1) домен еквайра (acquirer domain) (продавця і банку в який перераховуються гроші). Домен відповідає за конкретний запит і вірний шлях перенаправлення власника картки;
- 2) домен емітента (issuer domain) (власника карти і банку, який видав цю картку). Домен відповідає за надання істинної інформації про клієнта;
- 3) домен сумісності (interoperability domain) (надає платіжній системі протокол 3-D). Домен відповідає за збереження даних.

При здійсненні платежу картою банку, який підтримує протокол 3-D Secure до необхідної інформації додається додатковий запит (зазвичай це одноразовий пароль, який надсилається у SMS на мобільний телефон клієнта банку); або деякі банки використовують систему постійних паролів,

одержуваних при реєстрації і при здійсненні кожної електронної транзакції, вводить саме цей пароль, але він є менш надійним.

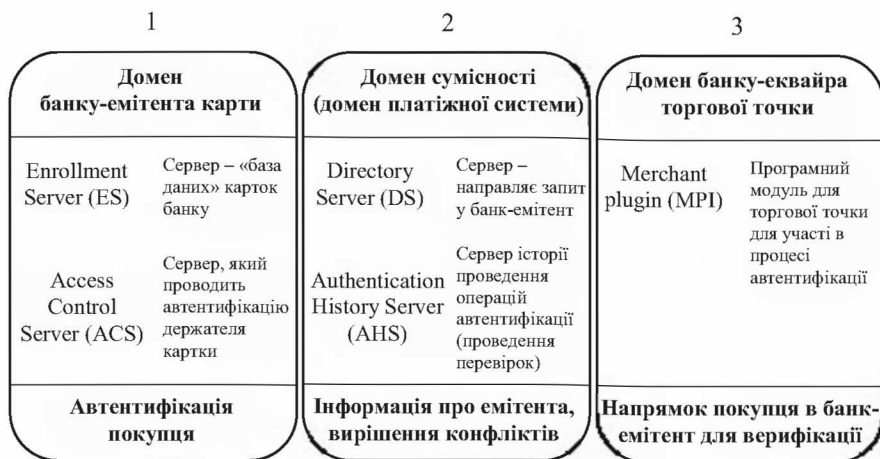


Рисунок 3.5 – Структура трьох доменів протоколу 3-D Secure

Структурна схема протоколу 3-D Secure показана на рис. 3.6. Власник банківської картки (клієнт) формує замовлення (покупку) на сторінці Інтернет-магазину та ініціює процес платежу за картою (1). Інтернет-магазин, використовуючи MPI (Merchant Plugin), пересилає спеціальний авторизаційний запит на DS (Directory Server). DS перевіряє номер картки на підтримку 3-D Secure технології (2). Після відповіді від DS про те, що даний власник картки може здійснювати платіж за технологією 3-D Secure, для запиту підтверджує пароля, модуль MPI відправляє запит на сервер банку-емітента (3). Власник картки вводить пароль на веб-сторінки ACS (Access Control Server) банку-емітента (4). ACS відправляє авторизаційну відповідь на MPI і одночасно зберігає дані про результат проведення автентифікації на сервері платіжної системи AHS (Authentication History Server), на якому зберігаються дані про всі транзакції проведені за технологією 3D-Secure. Згодом ці дані можуть використовуватися при вирішенні претензій клієнтів і при проведенні арбітражу спірних операцій (5). MPI обробляє відповідь ACS і в разі позитивної відповіді банку-емітента відправляє авторизаційний запит на сервер банку-еквайра (6). Далі через платіжну систему авторизаційний запит відправляється в банк-емітент картки.

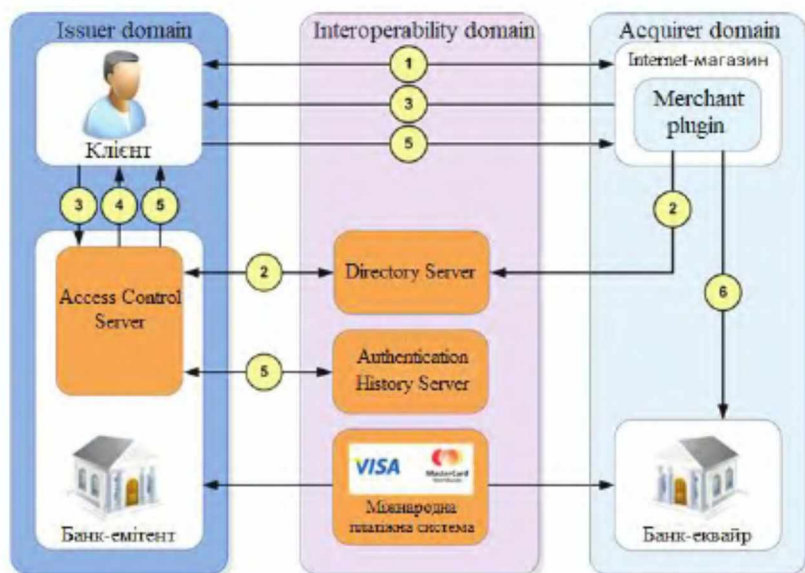


Рисунок 3.6 – Структурна схема протоколу 3-D Secure

4 КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

4.1 Загальна класифікація криптографічних перетворень

Криптографічні системи за типом алгоритму шифрування поділяються на дві великі групи: симетричні і асиметричні.

Якщо для зашифрування і розшифрування інформації використовується один ключ, то такі алгоритми називається **симетричними** або **криптосистемами з секретним ключем** (рис. 4.1).



Рисунок 4.1 – Структурна схема криптосистеми з секретним ключем

В **асиметричних криптосистемах** або **криптосистемах з відкритим ключем** використовується два різних ключі – один використовується для зашифрування, який називається відкритим (K_1), інший – для розшифрування, який називається секретним або особистим (K_2) (рис. 4.2).

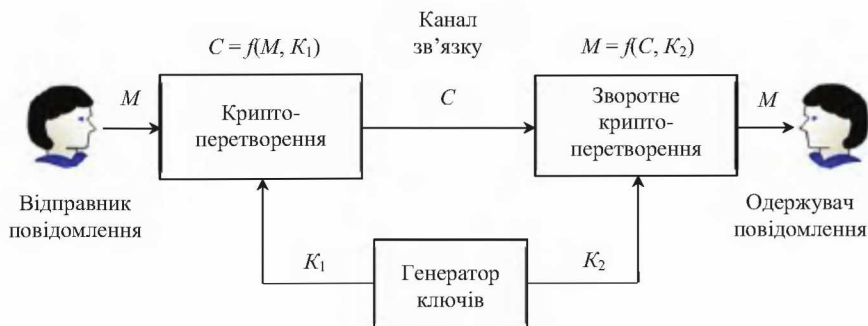


Рисунок 4.2 – Структурна схема криптосистеми з відкритим ключем

Особливостями криптоперетворень в асиметричних криптосистемах є:

- пряме криптографічне перетворення виконується з використанням відкритого ключа $K_v (K_1)$;
- зворотнє криптографічне перетворення виконується з використанням секретного (особистого) ключа $K_c (K_2)$;
- ключова пара (K_v, K_c) має бути випадковою та вибиратись із повної множини дозволених для використання ключових пар, причому $K_v \neq K_c$.

Гібридними називають криптосистеми, що поєднують обидва типи криптографічних систем, як правило, текст повідомлення зашифровується з використанням симетричної криптосистеми, а секретний ключ зашифровується з використанням асиметричної криптосистеми (рис. 4.3).

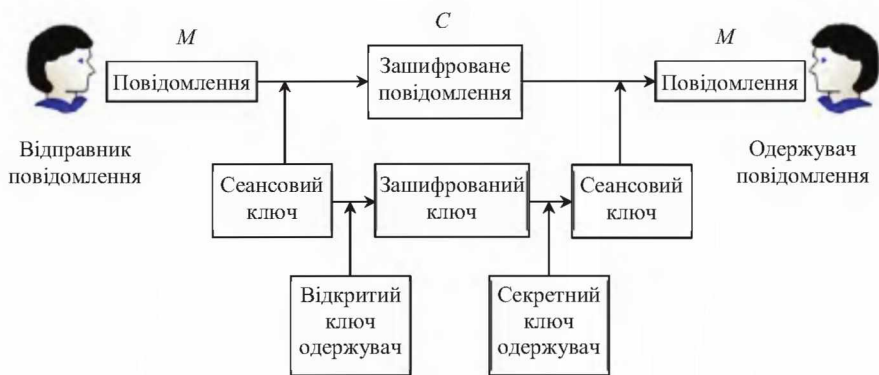


Рисунок 4.3 – Структурна схема гібридної криптосистеми

Симетричні криптоперетворення, у свою чергу, поділяються на **блокові шифри** та **поточкові шифри**. Функції ґешування (ґеш-функції) також можна віднести до симетричних криптографічних перетворень, оскільки в ключових функціях ґешування використовуються симетричні криптографічні перетворення та ключі.

У **блокових шифрах** символи відкритого тексту поділяються на блоки фіксованої довжини з подальшим зашифровуванням кожного блока окремо. При цьому однаковим зашифрованим блокам буде відповідати однаковий шифртекст.

У **поточних шифрах** кожен символ відкритого тексту зашифровується незалежно від інших і розшифровується таким самим чином.

До елементарних криптографічних перетворень (шифрів) належать:

- гамування, тобто складання символів інформації M (повідомлення) з ключем K чи гамою шифрування I , за відповідним модулем;
- перетворення типу “підстановка” символів повідомлення M , згідно з ключем $K(I)$;
- перетворення типу “перестановка” символів повідомлення згідно з ключем $K(I)$;
- зсув бітів, символів, слів згідно з ключем $K(I)$ тощо;
- афінні перетворення бітів, символів, слів згідно з ключем $K(I)$ тощо;
- аналітичні перетворення згідно з правилами, формулами, залежностями згідно з ключем $K(I)$ тощо.

Асиметричні криптографічні перетворення використовуються при здійсненні направленного шифрування, за деяких умов – при виконанні електронного підпису, а також реалізації механізмів генерування ключів.

Класифікація та призначення криптографічних перетворень показано на рис. 4.4 [10].

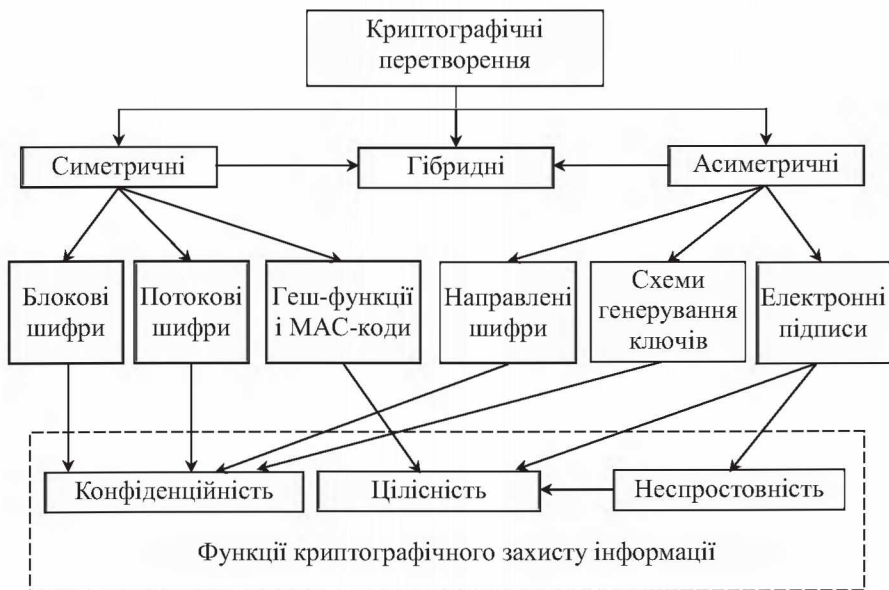


Рисунок 4.4 – Класифікація та призначення криптографічних перетворень

Класифікація криптосистем за стійкістю [10]. Залежно від складності задачі криптоаналізу, шифри за криптографічною стійкістю можна поділити на чотири класи:

1) *безумовно стійкі або теоретично недешифровані* – криптосистеми, відносно яких криптоаналітик ніколи не зможе виконати криптоаналіз як практично, так і теоретично.

Безумовно стійкими або теоретично недешифрованими є криптосистеми (шифри), у яких при виконанні вимог щодо вибору параметрів та керування ключами, згідно з сучасними поглядами, забезпечується умова: $t_6 \rightarrow \infty$, де t_6 – безпечний час;

2) *обчислювально стійкі* – такі криптосистеми, відносно яких можна виконати криптоаналіз, але при вибраних у шифрі параметрах і ключах на нинішньому етапі розвитку криптоаналізу для розв’язання задачі криптоаналізу в допустимі часові значення доступних ресурсів недостатньо.

Обчислювально стійкими є криптосистеми (шифри), щодо яких складність криптоаналізу оцінюється як експоненційно складна і значення безпечного часу набагато більше $t_{ц}$ – часу цінності інформації: $t_6 \gg t_{ц}$;

3) *ймовірно стійкі* – криптосистеми, доведення стійкості щодо яких зводиться до розв’язання математичної задачі, складність розв’язання якої не доведено.

Ймовірно стійкі – криптосистеми (шифри), щодо яких складність криптоаналізу оцінюється як експоненційно або субекспоненційно складна, складність розв’язання яких не доведена і значення безпечного часу набагато більше часу цінності інформації: $t_6 \gg t_{ц}$;

4) *обчислювально нестійкі* – у таких шифрах складність криптоаналізу на межі можливостей криптоаналітика, або при проектуванні в них вимушено чи через некомпетентність закладені слабкості.

Обчислювально нестійкі – криптосистеми (шифри), у яких складність криптоаналізу на межі можливостей криптоаналітика, або у які при проектуванні вимушено чи через некомпетентність закладені слабкості, а значення безпечного часу одного порядку або менше часу цінності інформації: $t_6 \leq t_{ц}$.

Дана класифікація дозволяє практично оцінити й порівняти криптосистеми та криптоперетворення.

4.2 Методи автентифікації

Система захисту інформації банку створена для забезпечення конфіденційності та цілісності електронної інформації, а також суворої автентифікації учасників систем електронних платежів, учасників інформаційних задач і фахівців організацій, які беруть участь у підготовці й обробленні електронних документів. Для здійснення суворої автентифікації організації застосовується система ідентифікації користувачів, яка є основою системи розподілу ключової інформації.

Автентифікація (authentication) – це процедура перевірки автентичності суб'єкта, який входить у систему та надає свій ідентифікатор.

Автентифікація багатofакторна (multifactor authentication) – автентифікація, яка здійснюється за допомогою захищених механізмів двох або більше типів. Наприклад, застосування для автентифікації паролем разом із токеном або автентифікації біометричної разом із паролем.

Фактор автентифікації (factor authentication) – певний вид інформації, що надається суб'єктом системі при його автентифікації. Виділяють три фактори автентифікації (табл. 4.1), що використовуються в різних комбінаціях: на основі знання чого-небудь, володіння чимось, на основі біометричних характеристик [11].

Таблиця 4.1 – Фактори автентифікації

Фактори автентифікації	Класифікація типів факторів автентифікації NCSC-TG-017 ¹	Приклади факторів автентифікації
На основі знання чого-небудь	Type 1: Authentication by Knowledge	Пароль PIN-код
На основі володіння чимось	Type 2: Authentication by Ownership	Фізичний ключ Пластикова картка ОТР-токен
На основі біометричних характеристик	Type 3: Authentication by Characteristic	Відбиток пальця Рисунок сітківки ока Голос

¹NCSC-TG-017 (National Computer Security Center) – документ “A Guide to Understanding Identification and Authentication in Trusted Systems” [11]

В інформаційних технологіях використовуються такі методи автентифікації:

- одностороння (одностороння) автентифікація, коли клієнт системи для доступу до інформації доводить свою автентичність;
- двобічна (взаємна) автентифікація, коли, крім клієнта, свою автентичність повинна підтверджувати і система (наприклад, банк);
- трибічна автентифікація, коли використовується так звана нотаріальна служба автентифікації для підтвердження достовірності кожного з партнерів в обміні інформацією.

Основним міжнародним стандартом з автентифікації є стандарт Міжнародної організації зі стандартизації та Міжнародної електротехнічної комісії ISO/IEC 9798 – Information technology – Security techniques – Entity authentication, що складається з шести частин [12]:

- ISO/IEC 9798-1:2010 Part 1: General;
- ISO/IEC 9798-2:2019 Part 2: Mechanisms using authenticated encryption;
- ISO/IEC 9798-3:2019 Part 3: Mechanisms using digital signature techniques;
- ISO/IEC 9798-4:1999 Part 4: Mechanisms using a cryptographic check function;
- ISO/IEC 9798-5:2009 Part 5: Mechanisms using zero-knowledge techniques;
- ISO/IEC 9798-6:2010 Part 6: Mechanisms using manual data transfer.

На основі стандартів ISO/IEC 9798, ДСТУ ISO/IEC 9798, ДСТУ ISO/IEC 20009-4:2018 можна побудувати загальну схему класифікації протоколів автентифікації, яка показана на рис. 4.5.

Проста автентифікація (simple authentication). Загалом просту автентифікацію розділяють на два види:

- 1) з використанням паролів (рис. 4.6);
- 2) з використанням односторонньої функції (рис. 4.7).

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



Рисунок 4.5 – Загальна схема класифікації протоколів автентифікації

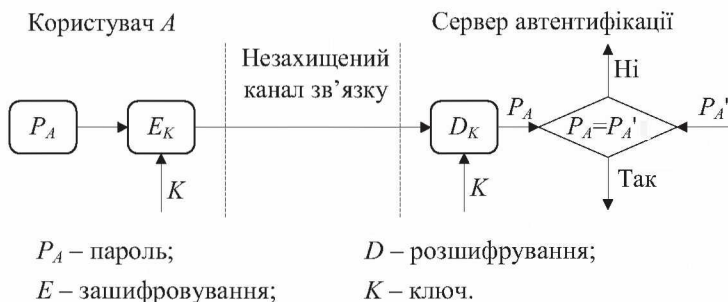


Рисунок 4.6 – Схема простої автентифікації з використанням пароля

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

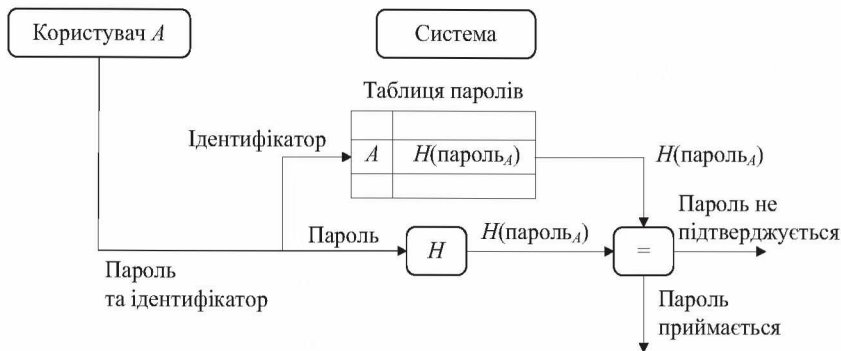


Рисунок 4.7 – Схема простої автентифікації з використанням односторонньої функції для перевірки пароля

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

- а) в незашифрованому вигляді; наприклад, згідно з протоколом паролльної автентифікації PAP (Password Authentication Protocol) паролі передаються по лінії зв'язку у відкритій незахищеній формі;
- б) в захищеному вигляді; всі передані дані (ім'я та пароль користувача, випадкове число і позначки часу) захищені за допомогою шифрування наприклад, протокол S\Key або однонаправленої функції.

Автентифікація з використанням одноразових паролів. Одноразові паролі (One-Time Passwords – OTP) – динамічна інформація, що генерується для одиничного використання за допомогою автентифікаційних пристроїв (програмних або апаратних), використовується для генерації одноразових паролів з метою автентифікації клієнтів під час входу в систему, а також для підтвердження платіжних доручень.

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

- симетрична криптографія – в цьому випадку користувач і сервер автентифікації використовують один і той самий секретний ключ;
- асиметрична криптографія – в цьому випадку в пристрої зберігається секретний ключ, а сервер автентифікації використовує відповідний відкритий ключ.

Існують різні комбінації використання даних криптографічних

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

- 1) в асинхронному режимі;
 - метод “запит-відповідь” (challenge-response);
- 2) в синхронному режимі;
 - метод “тільки відповідь” (response only);
 - метод “синхронізація за часом” (time synchronous);
 - метод “синхронізація за подією” (event synchronous).

Суворо автентифікація (strong authentication) – автентифікація, де для отримання доступу до інформації необхідно надати більше одного доказу механізму автентифікації.

У протоколах суворої автентифікації можуть бути використані асиметричні алгоритми з відкритими ключами, симетричні алгоритми, геш-функції, електронний підпис. У цьому випадку сторона, що доводить, може продемонструвати знання секретного ключа одним із наступних способів:

- 1) розшифрувати запит, зашифрований на відкритому ключі;
- 2) поставити свій підпис на запиті (на основі електронного підпису).

Нижче надамо класифікацію двох груп протоколів, які рекомендовані у стандарті ISO/IEC 9798-3 [11]:

- 1) протоколи з використанням схем відкритого шифрування:
 - а) одностороння автентифікація:

$$B \rightarrow A: h(r), B, E_{K_A}(r, B);$$

$$A \rightarrow B: r,$$

де $h()$ – геш-функція; r – випадкове число; E_{K_A} – алгоритм асиметричного шифрування з відкритим ключем K_A абонента A .

Абонент B (сервер) вибирає випадкове число r й обчислює значення геш-функції $h(r)$, далі обчислює значення $E_{K_A}(r, B)$. Абонент B відправляє повідомлення абоненту A . Абонент A розшифровує E_{K_A} (секретним ключем абонента A) й отримує значення r' та B' , а також обчислює $h(r')$. Після цього відбувається низка порівнянь, які доводять, що $h(r') = h(r)$ і, що отриманий ідентифікатор $B = B'$ дійсно вказує на абонента B . У випадку успішного проведення порівняння абонент A посилає значення r абоненту B . Отримавши його, абонент B перевіряє, чи це дійсно те значення, яке він відправив у першому повідомленні;

б) взаємна автентифікація:

$$A \rightarrow B: E_{K_B}(r_1, A);$$

$$B \rightarrow A: E_{K_A}(r_1, r_2);$$

$$B \rightarrow A: r_2,$$

де E_{K_B} – алгоритм асиметричного шифрування з відкритим ключем K_B учасника B ; r_1 – випадкове число, яке генерує учасник A ; r_2 – випадкове число, яке генерує учасник B ;

2) протоколи з використанням електронного підпису:

а) одностороння автентифікація з позначками часу:

$$A \rightarrow B: certA, t_A, B, S_A(t_A, B),$$

де $certA$ – сертифікат відкритого ключа абонента A ; t_A – позначка часу, яку генерує абонент A ; S_A – підпис, який генерує абонент A .

б) одностороння автентифікація з використанням випадкових чисел:

$$B \rightarrow A: r_B;$$

$$A \rightarrow B: certA, r_A, B, S_A(r_A, r_B, B),$$

де r_A, r_B – випадкові числа, які генерують абоненти A та B відповідно.

в) взаємна автентифікація з випадковими числами:

$$B \rightarrow A: r_B;$$

$$A \rightarrow B: \text{cert}_A, r_A, B, S_A(r_A, r_B, B);$$

$$B \rightarrow A: \text{cert}_B, A, S_B(r_A, r_B, A),$$

де cert_B – сертифікат відкритого ключа абонента B ; S_B – підпис, який генерує абонент B .

Протоколи, подібні описаним вище, використовуються також у стандарті Міжнародного телекомунікаційного союзу ITU (International Telecommunication Union) X.509. У ньому описуються протоколи автентифікації, які поєднуються із протоколами обміну ключами.

Протоколи автентифікації з нульовим передаванням знань. Один з істотних недоліків протоколів простої автентифікації полягає в тому, що після того, як абонент A , що доводить, передасть перевіряючому B свій пароль, перевіряючий може, використовуючи даний пароль, видати себе за A . Протоколи суворої автентифікації ліквідують цей недолік, але існує інша проблема. Річ у тому, що абонент A , відповідаючи на запити абонента B , зобов'язаний продемонструвати знання секретного ключа; при цьому передана інформація не може бути прямо використана абонентом B . Проте деяка її частина допоможе абоненту B отримати додаткову інформацію про секрет абонента A . Наприклад, абонент B може так сформулювати запити, щоб передані відповіді аналізувалися з метою витягання із них додаткової інформації про секрет.

Для вирішення описаних проблем застосовують протоколи доказу знання, які володіють додатковою властивістю нульового розголошення секрету – доказ з нульовим розголошенням (zero-knowledge proof – ZKP).

Протоколи з нульовою передачею знань характеризуються трьома властивостями:

1) повнота (completeness) – означає, що при виконанні чесними учасниками протокол вирішує ту задачу, для якої він створений;

2) коректність (soundness) – здатність протистояти загрозам з боку порушника, який не володіє необхідною секретною інформацією, але намагається виконати протокол від імені учасника A , який за визначенням повинен володіти такою інформацією;

3) нульове розголошення (zero-knowledge) – таке виконання протоколу, що ніяка інформація про учасника, що доводить певне твердження, крім факту його істинності, не може бути одержана нечесним перевіряючим з переданих повідомлень під час сеансу зв'язку.

Протоколи доказу виконують у вигляді послідовності незалежних циклів (раундів), кожен з яких складається з трьох кроків певного виду:

1. $A \rightarrow B: \gamma$ (заявка – witness);
2. $A \leftarrow B: x$ (запит – challenge);
3. $A \rightarrow B: y$ (відповідь – response).

Після виконання кожного циклу сторона, що перевіряє, приймає рішення про справжність доказу. Значне поширення для автентифікації одержали криптографічні протоколи доказу з нульовим розголошенням знань на базі асиметричного шифрування, відомими з яких є: Fiat-Shamir, Schnorr, Okamoto, Guillou-Quisquater, Brickell-McCurley, Feige-Fiat-Shamir.

Протокол Шнорра (Schnorr). Нехай p – просте число; q – простий дільник числа $p - 1$; α – елемент поля Z_p порядку q . В якості секретного ключа абонент A обирає число k в інтервалі $1 < k < q - 1$, в якості відкритого ключа

$$Y_a \equiv \alpha^{-k} \pmod{n}.$$

Нехай $cert_A$ – сертифікат відкритого ключа абонента A .

Протокол має вигляд:

1. $A \rightarrow B: cert_A, \gamma \equiv \alpha^r \pmod{p}$;
2. $B \rightarrow A: x$;
3. $A \rightarrow B: y \equiv (r + kx) \pmod{q}$.

Тепер, якщо виконано рівність $\gamma \equiv \alpha^y Y_a^x \pmod{p}$, то перевіряючий (абонента B) приймає доказ; якщо рівність не виконано, то – відкидає. Повнота протоколу випливає з рівності

$$\alpha^y Y_a^x \pmod{p} \equiv \alpha^{r+kx} (\alpha^{-k})^x \pmod{p} \equiv \alpha^r \pmod{p} = \gamma.$$

Протокол Шнорра показано на рис. 4.8.

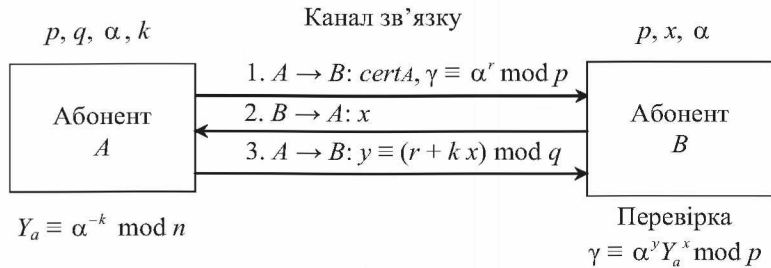


Рисунок 4.8 – Протокол Шнорра

Приклад протоколу Шнорра. Нехай $p = 48731$; $q = 443$; $\alpha = 11444$; $k = 357$; $r = 274$; $x = 129$. Розрахуємо відкритий ключ

$$Y_a \equiv 11444^{-357} \bmod 48731 \equiv 29420^{357} \bmod 48731 \equiv 7355.$$

Протокол:

1. $A \rightarrow B: \text{cert}A, \gamma \equiv 11444^{274} \bmod 48731 \equiv 37123$;
2. $B \rightarrow A: x = 129$;
3. $A \rightarrow B: y \equiv (274 + 357 \cdot 129) \bmod 443 \equiv 255$.

Абонент B перевіряє:

$$11444^{255} \cdot 7355^{129} \bmod 48731 \equiv 26233 \cdot 10575 \bmod 48731 \equiv 37123 = \gamma.$$

Абонент B приймає доказ оскільки рівність виконано.

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

Біометрія являє собою сукупність автоматизованих методів ідентифікації й/або автентифікації людей на основі їх фізіологічних і

поведінкових характеристик. До числа фізіологічних характеристик відносяться особливості відбитків пальців, сітківки й роговиці очей, геометрія руки й особи й т.п. До поведінкових характеристик відносяться динаміка підпису (ручний), ритм роботи серця, стиль роботи із клавіатурою. На стику фізіології й поведінки перебувають аналіз особливостей голосу й розпізнавання мови.

У загальному вигляді робота з біометричними даними організована в такий спосіб (рис. 4.9). Спочатку створюється й підтримується база даних характеристик потенційних користувачів. Для цього біометричні характеристики користувача знімаються, обробляються і результат обробки (біометричний шаблон) заноситься в базу даних (вихідні дані, такі як результат сканування пальця або роговиці, звичайно не зберігаються).

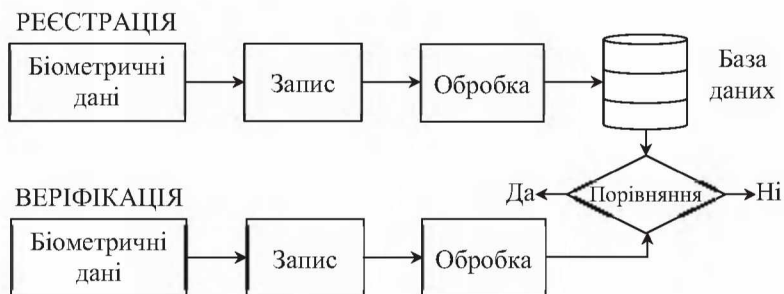


Рисунок 4.9 – Структура роботи біометричної автентифікації

Надалі для ідентифікації (й одночасно автентифікації) користувача процес зняття й обробки повторюється, після чого виробляється пошук у базі даних шаблонів. У випадку успішного пошуку особистість користувача і її дійсність вважаються встановленими. Для автентифікації досить зробити порівняння з одним біометричним шаблоном, обраним на основі попередньо уведених даних.

Звичайно біометрію застосовують разом з іншими ідентифікаторами, такими, наприклад, як паспорт, інтелектуальні карти. Іноді біометрична автентифікація є лише першим рубіжем захисту й слугує для активізації інтелектуальних карт, що зберігають криптографічні секрети; у такому випадку біометричний шаблон зберігається на тій самій карті. Для захисту біометричної інформації в Україні застосовується стандарт:

– ДСТУ ISO/IEC 24745:2015 «Інформаційні технології. Методи захисту. Захист біометричної інформації» (ISO/IEC 24745:2011, IDT);

– ДСТУ ISO/IEC 19784-1:2019 «Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 1. Специфікація біометричного прикладного програмного інтерфейсу» (ISO/IEC 19784-1:2018, IDT);

– ДСТУ ISO/IEC 19784-2:2012 «Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 2. Інтерфейс постачальника функції біометричного архіву» (ISO/IEC 19784-2:2007/Cor 1:2011, IDT);

– ДСТУ ISO/IEC 19784-4:2019 «Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 4. Інтерфейс постачальника функції біометричного сенсора» (ISO/IEC 19784-4:2011, IDT);

– ДСТУ ISO/IEC 19785-1:2017 «Інформаційні технології. Загальна структура форматів обміну біометричними даними. Частина 1. Специфікація елементів даних» (ISO/IEC 19785-1:2015, IDT);

– ДСТУ ISO/IEC 19785-2:2012 «Інформаційні технології. Загальна структура форматів обміну біометричними даними. Частина 2. Процедури роботи реєстраційного органу у сфері біометрії» (ISO/IEC 19785-2:2006, IDT);

– ДСТУ ISO/IEC 19785-3:2019 «Інформаційні технології. Загальна структура форматів обміну біометричними даними. Частина 3. Специфікація формату провідної організації» (ISO/IEC 19785-3:2015, IDT);

– ДСТУ ISO/IEC 19785-4:2017 «Інформаційні технології. Загальна структура форматів обміну біометричними даними. Частина 4. Специфікація формату блоку захисту інформації» (ISO/IEC 19785-4:2010, IDT).

Автентифікація за відбитками пальців. Ця біометрична технологія, цілком імовірно, в майбутньому використовуватиметься найширше. Переваги засобів доступу по відбитку пальця – простота використання, зручність і надійність. Весь процес ідентифікації здійснюється досить швидко і не вимагає особливих зусиль від користувачів. Вірогідність помилки при ідентифікації користувача набагато менша порівняно з іншими біометричними методами.

Використання геометрії руки. Переваги ідентифікації за геометрією долоні порівняно з автентифікацією по відбитку пальця в питаннях надійності, хоча пристрій для прочитування відбитків долонь займає більше місця. Найбільш досконалий пристрій, Handkey, сканує як внутрішню, так і бічну сторону руки.

Автентифікація за райдужною оболонкою ока. Перевага сканування райдужної оболонки полягає в тому, що зразок плям на оболонці знаходиться на поверхні ока, і від користувача не вимагається спеціальних зусиль. Фактично відеозображення ока може бути відскановане на відстані метра, що робить можливим використання таких сканерів у банкоматах. Ідентифікуючі параметри можуть скануватися і кодуватися, зокрема, й у людей з ослабленим зором, але непошкодженою райдужною оболонкою.

Автентифікація за сітківкою ока. Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, направленою через зіницю до кровоносних судин на задній стінці ока. Сканери для сітківки ока набули значного поширення в надсекретних системах контролю доступу, оскільки ці засоби автентифікації характеризуються одним з найнижчих відсотків відмови в доступі зареєстрованим користувачам і майже нульовим відсотком помилкового доступу.

Автентифікація за рисами особи (за геометрією особи) – один із напрямів, що швидко розвиваються, в біометричній індустрії. Розвиток цього напрямку пов'язаний зі швидким зростанням мультимедійних відеотехнологій. Проте більшість розробників поки зазнають труднощі в досягненні високого рівня виконання таких пристроїв.

Точність біометричної системи вимірюється двома параметрами:

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

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

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

4.3 Електронний підпис

4.3.1 Основні поняття та визначення

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

Одним із поширених у світі засобів такого захисту електронних документів від копіювання, модифікації і підробки є **електронний цифровий підпис** або **електронний підпис** (ЕП), який за допомогою спеціального програмного забезпечення підтверджує справжність інформації документа, його реквізитів і факту підписання конкретною особою. Програма електронного документообігу з використанням ЕП на сьогодні активно впроваджується в державних установах і органах державної влади, що істотно розширює можливості застосування ЕП і розвиток електронного документообігу в Україні.

Особливо актуальними ці проблеми стали з прийняттям у державах на міжнародному рівні, у тому числі в Україні, основоположних законів “Про електронні документи та електронний документообіг” [13], “Про електронні довірчі послуги” [14], “Про захист інформації в інформаційно-комунікаційних системах” [2]. На виконання цих законів в Україні створюється інфраструктура відкритих ключів, перш за все для підтримки системи електронного підпису. При цьому першочерговим завданням в Україні, що вимагає свого вирішення, є надання органам державної влади, місцевого самоврядування, юридичним та фізичним особам послуг із забезпечення цілісності, справжності, неспростовності, а в більшості випадків і конфіденційності інформації та різноманітних даних, що надані в електронному вигляді, електронних документів і повідомлень, програмного забезпечення, що ними використовуються. Крім того, у зв'язку з інтеграцією України у світовий інформаційний простір, орієнтацією на вступ України до Європейського співтовариства, важливим є завдання забезпечення взаємодії органів державної влади, місцевого самоврядування, юридичних і фізичних

осіб на світовому рівні, з використанням іноземних і міжнародних інформаційних та інформаційно-комунікаційних систем, різноманітних інформаційних технологій, відкритих систем Інтернету.

Особлива увага на міжнародному рівні приділяється проблемам стандартизації. Прийняті та вже знайшли широке застосування базових стандартів, рекомендації на моделі та системи електронного підпису:

- ISO/IEC 9796-3 «Information technology. Security techniques. Digital signature schemes giving message recovery. Part 3: Discrete logarithm based mechanisms»;

- ISO/IEC 14888-3:2018 «Information technology. Security techniques. Digital signatures with appendix. Part 3: Discrete logarithm based mechanisms»;

- ISO/IEC 15946-1:2016 «Information technology. Security techniques. Cryptographic techniques based on elliptic curves»;

- ISO/IEC 9594-8:2020 «Information technology. Open systems interconnection. Part 8: The Directory: Public-key and attribute certificate frameworks»;

- ITU-T X.509 «Information technology. Open Systems Interconnection. The Directory: Public-key and attribute certificate frameworks».

В Україні також уведено в дію та застосовується власні стандарти та гармонізовані:

- ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка»;

- ДСТУ 7564-2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування»;

- ДСТУ 7624-2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення»;

- ДСТУ ISO/IEC 14888-1:2015 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 1. Загальні положення» (ISO/IEC 14888-1:2008, IDT);

- ДСТУ ISO/IEC 14888-2:2015 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел» (ISO/IEC 14888-2:2008, IDT);

- ДСТУ ISO/IEC 14888-3:2019 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми на основі

дискретного логарифмування» (ISO/IEC 14888-3:2018, IDT);

– ДСТУ ISO/IEC 9796-2:2015 «Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел» (ISO/IEC 9796-2:2010, IDT);

– ДСТУ ISO/IEC 9796-3:2015 «Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі» (ISO/IEC 9796-3:2006, IDT);

– ДСТУ ETSI TR 102 272:2015 «Електронні підписи та інфраструктура (ESI). ASN.1 формат політики підпису» (ETSI TR 102 272:2003, IDT);

– ДСТУ ETSI TS 102 176-1:2017 «Електронні підписи та інфраструктури (ESI). Алгоритми та параметри безпечних електронних підписів. Частина 1. Геш-функції й асиметричні алгоритми» (ETSI TS 102 176-1:2011, IDT);

– ДСТУ ISO/IEC 15946-1:2019 «Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 1. Загальні положення» (ISO/IEC 15946-1:2016, IDT);

– ДСТУ ISO/IEC 9594-8:2014 «Інформаційні технології. Взаємозв'язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів» (ISO/IEC 9594-8:2014, IDT).

Закон України “Про електронні довірчі послуги” [14] визначає правові та організаційні засади надання електронних довірчих послуг, 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. Закон України “Про електронні довірчі послуги” закріплює основні поняття та визначення [14].

Електронна послуга – будь-яка послуга, що надається через інформаційно-комунікаційну систему.

Електронна довірча послуга – послуга, яка надається для забезпечення електронної взаємодії двох або більше суб'єктів, які довіряють надавачу електронних довірчих послуг щодо надання такої послуги.

Електронна ідентифікація – процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи.

Засіб електронної ідентифікації – носій інформації, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг.

Електронні дані – будь-яка інформація в електронній формі.

Електронний підпис – електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис.

Кваліфікований електронний підпис – удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа.

Кваліфікована електронна печатка – удосконалена електронна печатка, яка створюється з використанням засобу кваліфікованої електронної печатки і базується на кваліфікованому сертифікаті електронної печатки.

Засіб кваліфікованого електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які реалізують криптографічні алгоритми генерації пар ключів та/або створення кваліфікованого електронного підпису чи печатки, та/або перевірки кваліфікованого електронного підпису чи печатки, та/або зберігання особистого ключа кваліфікованого електронного підпису чи печатки.

Засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа.

Електронна позначка часу – електронні дані, які пов'язують інші електронні дані з конкретним моментом часу для засвідчення наявності цих електронних даних на цей момент часу.

Засіб електронного підпису чи печатки – апаратно-програмний або апаратний пристрій чи програмне забезпечення, які використовуються для створення та/або перевірки електронного підпису чи печатки.

Кваліфікований сертифікат відкритого ключа – сертифікат відкритого ключа, який видається кваліфікованим надавачем електронних довірчих послуг, засвідчувальним центром або центральним засвідчувальним органом.

Інтероперабельність – технологічна сумісність технічних рішень, що використовуються під час надання електронних послуг, та їх здатність взаємодіяти між собою.

4.3.2 Вимоги до системи електронного підпису

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

Електронний підпис повинен володіти наступними властивостями:

а) повинна бути можливість перевірити автора, дату і час створення підпису;

б) повинна бути можливість ідентифікувати вміст під час створення підпису;

в) підпис повинен бути перевірений третьою стороною для вирішення спорів.

Таким чином, функція електронного підпису включає функцію автентифікації/ ідентифікації.

На підставі цих властивостей можна сформулювати наступні вимоги до електронного підпису:

а) підпис повинен бути двійковим зразком, який залежить від повідомлення, що підписується;

б) підпис повинен використовувати деяку унікальну інформацію відправника для запобігання підробки або відмови;

в) створювати електронний підпис має бути відносно легко;

г) повинно бути обчислювально неможливо підробити електронний підпис як створенням нового повідомлення для існуючого електронного

підпису, так і створенням помилкового електронного підпису для деякого повідомлення;

д) електронний підпис має бути досить компактним і не займати багато пам'яті.

4.3.3 Структура системи електронного підпису України

Систему ЕП в Україні прийнято будувати за ієрархічним принципом. На рис. 4.10 наведено узагальнену схему інформаційної структури відкритих ключів України [15]. Основними структурними елементами системи ЕП України є центральний засвідчувальний орган, засвідчувальні центри центральних органів виконавчої влади, акредитовані центри сертифікації ключів, центри сертифікації ключів (ЦСК), відокремлені пункти реєстрації ключів, заявники – юридичні та фізичні особи (користувачі), контролюючий орган.

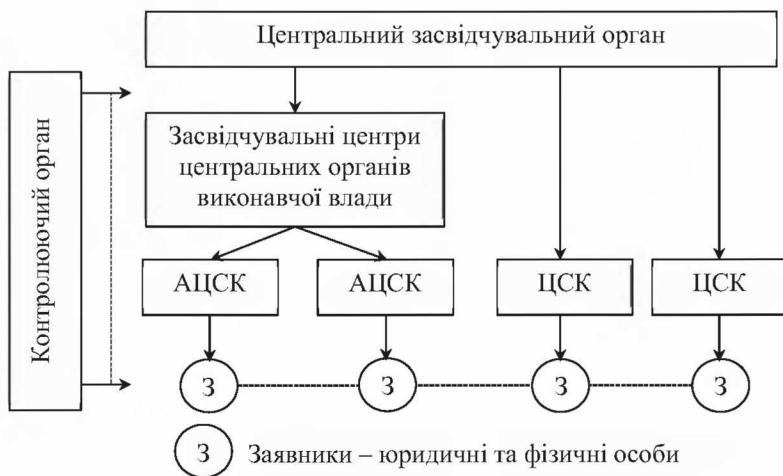


Рисунок 4.10 – Узагальнена схема структури відкритих ключів України

Центральний засвідчувальний орган (ЦЗО) у національній системі ЕП України є головним центром сертифікації відкритих ключів, основними завданнями якого є обслуговування посилених сертифікатів ключів центрів в Україні, акредитація центрів сертифікації ключів та засвідчувальних центрів

відповідно до законодавства України. ЦЗО відповідно до покладених на нього завдань щодо внутрішньодержавної системи ЕП:

- здійснює акредитацію центрів, видачу, переоформлення й анулювання відповідних свідоцтв;
- формує і видає центрам сертифікати ключів;
- проводить реєстрацію центрів;
- блокує, скасовує та поновлює сертифікати ключів центрів;
- веде реєстр суб'єктів, які надають послуги, пов'язані з електронним підписом;
- веде електронні реєстри сертифікатів ключів центрів, у тому числі блокованих і скасованих;
- зберігає сертифікати ключів центрів;
- забезпечує цілодобово доступ до сертифікатів ключів центрів та їх електронних реєстрів через загальнодоступні комунікаційні мережі;
- приймає на зберігання сертифікати ключів, їх реєстри та документовану інформацію, яка підлягає обов'язковій передачі від центрів до ЦЗО в разі припинення їх діяльності;
- розглядає заяви і скарги щодо неналежного функціонування центрів та подає відповідні пропозиції контролюючому органу;
- повідомляє контролюючий орган про обставини, які перешкоджають діяльності ЦЗО.

Акредитований центр сертифікації ключів (АЦСК) здійснює свою діяльність у сфері електронного документообігу, застосування ЕП органами державної влади, органами місцевого самоврядування, підприємствами, установами й організаціями усіх форм власності, іншими суб'єктами господарської діяльності та фізичними особами.

Перелік послуг ЕП, що надаються центром:

- обслуговування сертифікатів відкритих ключів абонентів;
- реєстрацію абонентів;
- надання абонентам засобів ЕП та шифрування даних, засобів генерації особистих і відкритих ключів;
- сертифікацію відкритих ключів абонентів;
- розповсюдження сертифікатів;
- керування статусом сертифікатів та розповсюдження інформації про статус сертифікатів;

– надання послуг фіксування часу.

Порядок застосування ЕП органами державної влади, органами місцевого самоврядування, підприємствами, установами й організаціями державної форми власності визначається Кабінетом Міністрів України. Порядок застосування ЕП у банківській діяльності визначається Національним банком України.

Відокремлені пункти реєстрації заявників є відособленими підрозділами без правового статусу юридичної особи, що реалізують функції центру з реєстрації абонентів та їх подальшого обслуговування на відповідній території. Відокремлені пункти уповноважені укладати договори про надання послуг ЕП. Безпосереднє керування відокремленими пунктами здійснюється центром сертифікації ключів.

Користувачі (абоненти) ЕП. Абонент має право:

- своєчасно отримувати якісні послуги ЕП;
- одержувати сертифікат центру;
- одержувати список відкликаних сертифікатів, сформований центром;
- застосовувати сертифікат центру для перевірки справжності ЕП сертифікатів, сформованих центром;
- застосовувати список відкликаних сертифікатів, сформований центром, для перевірки статусу власного сертифіката та сертифікатів інших абонентів;
- сформувати відкриті й особисті ключі на своєму робочому місці з використанням надійного способу ЕП;
- ознайомитись з інформацією щодо діяльності центру та надання послуг ЕП;
- вимагати скасування, блокування або поновлення свого сертифіката ключа.

Контролюючий орган. Функції контролюючого органу здійснює спеціально уповноважений центральний орган виконавчої влади у сфері криптографічного захисту інформації – Державна служба спеціального зв'язку та захисту інформації України.

Контролюючий орган перевіряє дотримання закону центрального засвідчувального органа, засвідчувального центру центральних органів виконавчої влади, акредитованих центрів сертифікації ключів та центрів сертифікації ключів.

4.3.4 Методи побудови схем електронного підпису

Існує декілька методів побудови схем ЕП [16], а саме:

а) шифрування електронного документа (ЕД) на основі симетричних алгоритмів. Така схема передбачає наявність у системі третьої особи (арбітра), що користується довірою учасників обміну підписаними у подібний спосіб електронними документами. Взаємодія користувачів даної системи здійснюється за таким алгоритмом:

- учасник A зашифровує повідомлення на власному секретному ключі k_A , зміст якого узгоджено з арбітром, потім зашифроване повідомлення передається арбітрові із зазначенням адресата даного повідомлення (інформація, що ідентифікує адресата, передається також у зашифрованому вигляді);

- арбітр розшифровує отримане повідомлення на ключі k_A , проводить необхідні перевірки і потім зашифровує на секретному ключі k_B учасника B . Далі зашифроване повідомлення надсилається учасникові B разом з інформацією про те, що воно надійшло від учасника A ;

- учасник B розшифровує це повідомлення й переконується в тому, що відправником є учасник A .

За авторизацію документа у наданій схемі вважатиметься сам факт зашифрування ЕД секретним ключем і передавання зашифрованого ЕД арбітра. Основною перевагою цієї схеми є наявність третьої сторони, що виключає будь-які суперечні питання між учасниками інформаційного обміну, тобто в даному разі не потрібно додаткової системи арбітражу ЕП. Недоліком схеми є наявність третьої сторони і використання симетричних алгоритмів шифрування;

б) шифрування ЕД з використанням асиметричних алгоритмів шифрування. Фактом підписання документа в такій схемі є зашифрування документа на секретному ключі його відправника. Ця схема теж використовується дуже рідко внаслідок того, що довжина ЕД може виявитися критичною. Застосування асиметричних алгоритмів для зашифрування повідомлень великої довжини є неефективне з точки зору швидкісних характеристик. У цьому разі не потрібно наявності третьої сторони, хоча вона може виступати в ролі сертифікаційного органу відкритих ключів користувачів;

в) розвитком попередньої ідеї стала найбільш розповсюджена схема ЕП, а саме: зашифрування остаточного результату опрацювання ЕД геш-функцією за допомогою асиметричного алгоритму. Структурну схему такого варіанта побудови ЕП показано на рис. 4.11.

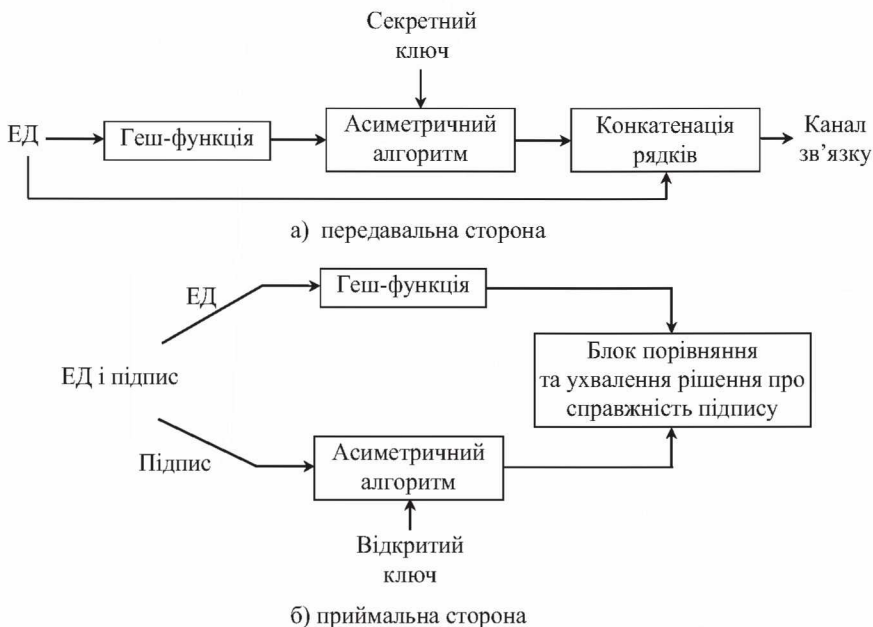


Рисунок 4.11 – Структурна схема побудови ЕП

Генерування підпису відбувається в такий спосіб:

а) учасник *A* обчислює геш-код від ЕД. Отриманий геш-код проходить процедуру перетворення з використанням власного секретного ключа, після чого отримане значення (що і є ЕП) разом з ЕД надсилається учасникові *B*;

б) учасник *B* повинен отримати ЕД з ЕП та сертифікований відкритий ключ користувача *A*, а потім провести розшифрування на ньому ЕП, сам ЕД підлягає операції гешування, після чого результати порівнюються і, якщо вони збігаються, ЕП визнається за справжній, в іншому разі – за помилковий.

Стійкість даного типу ЕП базується на стійкості асиметричних алгоритмів шифрування і застосовуваних геш-функцій.

Взагалі підписаний ЕД виглядає як пара, що складається з бінарних рядків (M, S), де M становить собою ЕД, а S – підпис, розв'язок рівняння

$$E_k(S) = M,$$

де E_k є функцією з секретом.

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

За кількістю учасників:

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

б) груповий – коли в процесі вироблення ЕП повинно бути більше ніж один учасник. При цьому груповий підпис може здійснюватись:

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

– без залучення третьої довірчої сторони.

За терміном дії ключів:

а) ЕП без терміну обмеження дії ключів;

б) ЕП з терміном обмеження дії ключів.

За способом перевірки:

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

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

За способом вироблення підпису:

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

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

в) сліпий ЕП (blind signature) – ЕП, що здійснюється без можливості

перегляду змісту повідомлення;

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

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

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

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

За математичною задачею, на якій засновується стійкість ЕП:

а) на складності задачі розкладання на співмножники (факторизації) великого числа – модуля перетворення;

б) на складності розв'язання задачі дискретного логарифма в полях Галуа;

в) на складності розв'язання задачі дискретного логарифма в групі точок еліптичної кривої;

г) на складності розв'язання задачі дискретного логарифма в групі точок гіпереліптичної кривої;

д) на складності знаходження найкоротшого вектора в заданій числовій решітці (наприклад, Nth-degree TRuncated polynomial ring Signature algorithm або NTRUSign).

4.3.5 Основні поняття та застосування геш-функції

Невід'ємною частиною ЕП є використання геш-функцій.

Геш-функцією (hash function) називається перетворення h , яка перетворює інформаційну послідовність M довільної довжини на послідовність фіксованої довжини $h(M)$, називану **геш-кодом**. Окрім того, геш-функції широко застосовуються і для вирішення багатьох інших питань, пов'язаних із забезпеченням захисту потоків даних, наприклад для гешування паролів користувачів з метою подальшого їхнього шифрування та зберігання у базі даних. Функція гешування може служити як криптографічна контрольна сума – код виявлення змін (Manipulation

Detection Code – MDC) або для перевірки цілісності повідомлення (Message Integrity Check – MIC).

Однією з найважливіших характеристик геш-функцій, що зумовили їхнє широке впровадження у практику, виявилася здатність одержувати з відкритого тексту великої довжини геш-код набагато меншою довжиною, що в певних випадках дозволяє дуже ефективно скоротити мережний трафік. Застосовування геш-функцій надає можливість усувати надлишковість відкритого тексту, що при подальшому криптографічному перетворенні геш-коду відкритого тексту позитивно позначається на криптографічних властивостях зашифрованого повідомлення.

Всі існуючі функції гешування можна поділити на два великих класи:

- 1) безключові геш-функції, що залежать тільки від повідомлення;
- 2) геш-функції із секретним ключем, що залежать як від повідомлення, так і від секретного ключа.

Існує три методи побудови геш-функцій:

- 1) на базі певної складно обчислюваної математичної задачі;
- 2) на базі алгоритмів блокового шифрування;
- 3) розроблення з нуля.

Кожен із зазначених методів має власні переваги й недоліки, однак, найбільш поширеними сьогодні є останні два. Це пов'язано з тим, що при побудові геш-функцій з нуля, виникає можливість враховувати таку їхню властивість, як ефективна програмна реалізація. Широке застосовування геш-функцій, побудованих на базі алгоритмів блокового шифрування, є наслідком ретельного опрацювання питання стійкості багатьох з існуючих алгоритмів.

По використовуваних внутрішніх перетвореннях функції гешування можна поділити на:

- функції, що використовують бітові логічні перетворення, різні зрушення і, як правило, є багатоцикловими;
- функції, що використовують блокові симетричні шифри;
- функції, що використовують перетворення в групах, полях і кільцях з цілочисловими чи поліноміальним базисом;
- функції, що використовують матричні перетворення.

До геш-функцій ставляться такі вимоги:

- результат роботи геш-функцій має залежати від усіх двійкових символів вихідного повідомлення, а також від їхнього взаємного

розташування;

- геш-функція має бути стійкою в розумінні звертання;
- геш-функція має бути стійкою в розумінні виявлення колізій.

Область використання геш-функцій:

- захист паролів при їхньому передаванні та зберіганні;
- формування контрольних кодів MDC;
- отримання стисненого зразка повідомлення перед формуванням електронного підпису;
- оперативний контроль перебігу програм.

Визначальними вимогами до функцій гешування є їхня стійкість до пошуку першого прообразу, другого прообразу, а також стійкість до колізій.

Стійкість до пошуку першого прообразу – відсутність ефективного поліноміального алгоритму обчислення зворотної функції, тобто не можна відновити повідомлення M за відомою його геш-функцією $h(M)$, за реальний час (незворотність). Це властивість еквівалентна тому, що геш-функція є односторонньою функцією.

Стійкість до пошуку другого прообразу (колізій першого роду) – обчислювально неможливо, знаючи повідомлення M та його геш-функцію $h(M)$, знайти таке інше повідомлення $M' \neq M$, для якого виконувалася б умова $h(M) = h(M')$.

Стійкість до колізій (колізій другого роду) – неможливість побудування двох повідомлень, для яких вироблялося б однакове значення геш-функції, тобто для заданої геш-функції h обчислювально неможливо знайти два повідомлення M і M' , $M' \neq M$, для яких виконувалася б умова $h(M) = h(M')$.

Найбільш відомі алгоритми отримання геш-образів повідомлень – MD2, MD4, MD5, MD6, SHA-1, SHA-2, SHA-3 (Кеccak), RIPEMD, TIGER, HAVAL, Whirlpool, Tiger.

В Україні також уведено в дію та застосовуються власні стандарти, які гармонізовані з міжнародними документами:

- ДСТУ 7564-2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування»;
- ДСТУ ISO/IEC 10118-2:2015 «Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції, що використовують n -бітний

блоковий шифр» (ISO/IEC 10118-2:2010; Cor 1:2011, IDT);

– ДСТУ ISO/IEC 10118-4:2015 «Інформаційні технології. Методи захисту. Геш-функції. Частина 4. Геш-функції, що використовують модульну арифметику» (ISO/IEC 10118-4:1998; Cor 1:2014; Amd 1:2014, IDT).

4.4 Алгоритм електронного підпису RSA

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

Найбільш поширеною системою формування ЕП є система, в основі якої лежить алгоритм RSA. Узагальнену схему формування й перевірки електронного підпису RSA [16] показано на рис. 4.12.

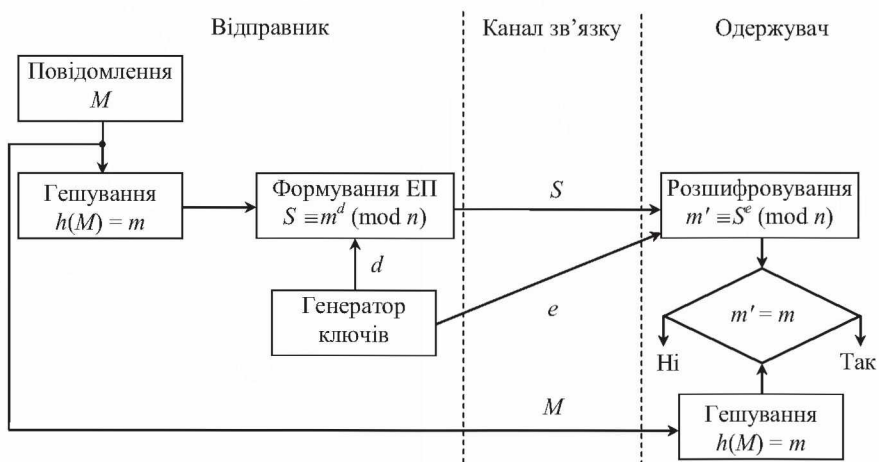


Рисунок 4.12 – Схема електронного підпису RSA

Обираються великі прості числа p і q , обчислюється $n = pq$, функція Ейлера $\varphi(n) = (p - 1)(q - 1)$ і вибирається відкритий ключ e ($e < \varphi(n)$, $\text{НОД}(e, \varphi(n)) = 1$). Врешті, обчислюється секретний ключ d , взаємно обернене з e ($ed \equiv 1 \pmod{\varphi(n)}$). У відкритому каталозі розміщують значення (e, n) , а секретний ключ d зберігається у автора документа.

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

$$h(M) = m.$$

Потім відправник зашифровує m секретним ключем d :

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

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

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

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

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

$$h(M) = m.$$

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

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

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

Доказ коректності підпису RSA

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

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

Приклад електронного підпису RSA. Нехай $p = 31$ і $q = 73$, тоді

$$\begin{aligned} n &= 31 \cdot 73 = 2263; \\ \varphi(2263) &= (31 - 1)(73 - 1) = 2160. \end{aligned}$$

Нехай задано відкритий ключ $e = 59$ і секретний ключ $d = 659$. У відкритому каталозі розміщують значення $(59, 2263)$.

Відправник хоче підписати повідомлення M , для якого значення геш-функції дорівнює $h(M) = 273$.

У цьому разі відправник обчислює

$$S \equiv 273^{659} \pmod{2263} \equiv 2082$$

і формує підписане повідомлення $(M, 2082)$.

Одержувач, маючи підписане повідомлення, обчислює значення геш-функції $h(M) = 273$ та

$$m' \equiv 2082^{59} \pmod{2263} \equiv 273.$$

Значення $m' = h(M) = 273$ збіглися, тобто підпис є справжній.

Електронний підпис RSA є вразливий щодо так званої мультиплікативної атаки. Інакше кажучи, алгоритм підпису RSA дозволяє криптоаналітику без знання секретного ключа d сформулювати підписи під тими документами, в яких результат ґешування можна обчислити як добуток результатів ґешування вже підписаних документів.

4.5 Електронний підпис GQ

Безпека електронного підпису GQ (Guillou-Qisquater) заснована на складності добування квадратного кореня за модулем великого складеного числа за заданим модулем n .

Обираються великі прості числа p і q , обчислюється $n = pq$, функція Ейлера $\varphi(n) = (p-1)(q-1)$ і обирається ціле число e , для якого $\text{НОД}(e, \varphi(n)) = 1$ і $e < \varphi(n)$. Обираються атрибут J відправника – ціле число $1 < J < n$, для якого $\text{НОД}(J, n) = 1$. Параметр J і особистий ключ k відправника взаємопов'язані виразом

$$Jk^e \equiv 1 \pmod{n},$$

де $k \in Z_n$.

Знаходимо особистий ключ k за наступним алгоритмом:

- обчислюємо $J^{-1} \pmod{n}$;
- обчислюємо $t_1 \equiv e^{-1} \pmod{p-1}$ і $t_2 \equiv e^{-1} \pmod{q-1}$;
- обчислюємо $x_1 \equiv \left(J^{-1}\right)^{t_1} \pmod{p}$ і $x_2 \equiv \left(J^{-1}\right)^{t_2} \pmod{q}$;
- знаходимо k , що таке одночасно $k \equiv x_1 \pmod{p}$ і $k \equiv x_2 \pmod{q}$.

Параметри (n, e, J) вільно публікуються, а особистий ключ k відправника зберігається у автора документа.

Для того, щоб підписати повідомлення M користувач виконує наступні дії:

- обирає випадкове число α , яке $1 < \alpha < n-1$ і обчислює параметр x

$$x \equiv \alpha^e \pmod{n};$$

– об'єднує повідомлення M і x та гешує результат для отримання першого параметра підпису r ($1 < r < e-1$):

$$r = h(M \| x) \text{ або } r \equiv [h(M \| x)] \pmod{e}, \text{ якщо } r > e;$$

- обчислює другий параметр підпису s :

$$s \equiv (\alpha k') \bmod n.$$

Підписом повідомлення M є пара чисел (r, s) , які передаються одержувачу разом з атрибутом J відправника.

Перевірка підпису. Нехай прийнято повідомлення M і його значення (r, s) та J . Одержувач обчислює параметр u

$$u \equiv (s^e J^r) \bmod n$$

та перевіряє рівність результату r' з параметром підпису r

$$r' = h(M \parallel u) = r.$$

Якщо рівність виконується, то підпис є справжній.

Схема електронного підпису GQ показана на рис. 4.13.

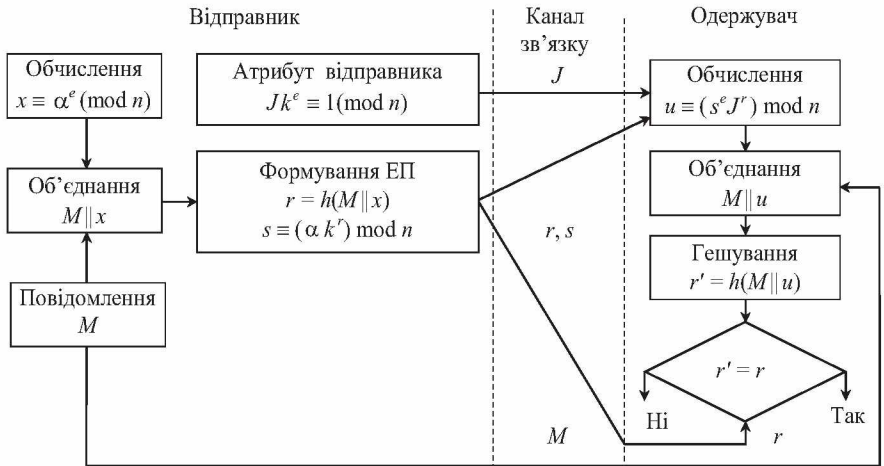


Рисунок 4.13 – Схема електронного підпису GQ

Доказ коректності підпису GQ

$$u \equiv (s^e J^r) \bmod n \equiv [(\alpha k')^e (k^{-e})^r] \bmod n \equiv \alpha^e \bmod n = x.$$

Приклад електронного підпису GQ. Нехай $p = 113$ і $q = 599$, тоді

$$n = 113 \cdot 599 = 67687;$$
$$\varphi(67687) = (113 - 1)(599 - 1) = 66976.$$

Нехай відкритий ключ $e = 311$ і атрибут відправника $J = 100$. Перевірка умов: $311 < 66976$ і $100 < 67687$; НОД $(311, 66976) = 1$ і НОД $(100, 67687) = 1$.

Знаходимо особистий ключ k :

– обчислюємо $100^{-1} \pmod{67687} \equiv 52119$;

– обчислюємо $t_1 \equiv 311^{-1} \pmod{112} \equiv 103$ і $t_2 \equiv 311^{-1} \pmod{598} \equiv 25$;

– обчислюємо $x_1 \equiv 52119^{103} \pmod{113} \equiv 91$ і $x_2 \equiv 52119^{25} \pmod{599} \equiv 80$;

– знаходимо $k = 65970$ з порівнянь $k \equiv 91 \pmod{113}$ і $k \equiv 80 \pmod{599}$ (вирішуємо систему порівнянь згідно з Китайською теоремою про залишки).

Формування підпису. Нехай $\alpha = 2000$, обчислюємо параметр x :

$$x \equiv 2000^{311} \pmod{67687} \equiv 7758.$$

Припустимо, що конкатенація повідомлень $M = 1000$ і $x = 7758$ дає результат $M \parallel x = 10007758$. Також припустимо, що гешування цього значення дає дайджест $h(10007758) = 250$. Це означає, що перший параметр підпису $r = 250$. Розраховуємо другий параметр підпису s :

$$s \equiv (2000 \cdot 65970^{250}) \pmod{67687} \equiv 8808.$$

Формується підписане повідомлення у вигляді $(1000, 250, 8808, 100)$, які передаються одержувачеві.

Перевірка підпису. Одержувач обчислює параметр u та перевіряє рівність результату $r' = r$

$$u \equiv (8808^{311} \cdot 100^{250}) \pmod{67687} \equiv 7758;$$
$$r' = h(1000 \parallel 7758) = h(10007758) = 250 = r.$$

Одержувач робить висновок, що підпис є справжній.

4.6 Колективний підпис GQ

Схема електронного підпису GQ може бути перероблена на випадок, коли кілька абонентів хочуть підписати один і той самий документ M . Нехай абоненти A і B підписують повідомлення M , але в процесі підписання може бути залучено будь-яку кількість абонентів.

Абоненти A і B мають унікальні значення:

- J_A атрибут абонента A ($1 < J_A < n$, $\text{НОД}(J_A, n) = 1$);
- J_B атрибут абонента B ($1 < J_B < n$, $\text{НОД}(J_B, n) = 1$);
- k_A особистий ключ абонента A ($k_A \in Z_n$);
- k_B особистий ключ абонента B ($k_B \in Z_n$);
- α_A вибирає випадкове число абонента A ($1 < \alpha_A < n - 1$);
- α_B вибирає випадкове число абонента B ($1 < \alpha_B < n - 1$).

Значення (n, e) є загальними для схеми колективного підпису.

Колективний підпис повідомлення M :

- абонент A обчислює $x_A \equiv \alpha_A^e \pmod{n}$ і значення x_A посилає B ;
- абонент B обчислює $x_B \equiv \alpha_B^e \pmod{n}$ і значення x_B посилає A ;
- абоненти A і B обчислюють $x \equiv (x_A x_B) \pmod{n}$;
- об'єднує повідомлення M і x та гешує результат $r = h(M \| x)$;
- абонент A обчислює $s_A \equiv (\alpha_A k_A^r) \pmod{n}$ і значення s_A посилає B ;
- абонент B обчислює $s_B \equiv (\alpha_B k_B^r) \pmod{n}$ і значення s_B посилає A ;
- абоненти A і B обчислюють $s \equiv (s_A s_B) \pmod{n}$.

Колективний підпис складається з повідомлення M , значень (r, s) і атрибутів обох абонентів: J_A, J_B .

Перевірка підпису. Одержувач обчислює параметри:

- обчислює $J \equiv (J_A J_B) \pmod{n}$;
- обчислює $u \equiv (s^e J^r) \pmod{n}$;
- перевіряє рівність $r' = h(M \| u) = r$, якщо рівність виконується, то колективний підпис є справжній.

Доказ коректності колективного підпису GQ

$$\begin{aligned} u &\equiv (s^e J^r) \pmod{n} \equiv [(\alpha_A k_A^r \alpha_B k_B^r)^e (k_A^{-e} k_B^{-e})^r] \pmod{n} \equiv \\ &\equiv (\alpha_A^e k_A^{re} \alpha_B^{re} k_B^{re} k_A^{-er} k_B^{-er}) \pmod{n} \equiv (\alpha_A^e \alpha_B^e) \pmod{n} \equiv (x_A x_B) \pmod{n} \equiv x. \end{aligned}$$

Схема колективного підпису GQ показана на рис. 4.14.

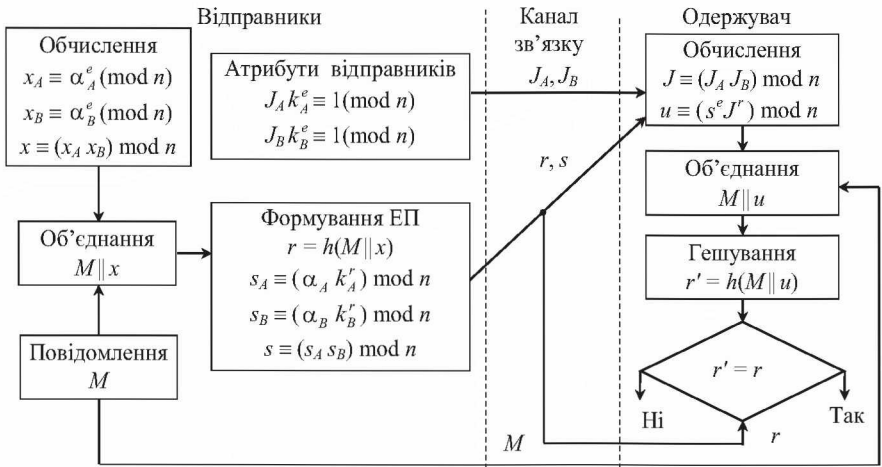


Рисунок 4.14 – Схема колективного електронного підпису GQ

Приклад колективного підпису GQ. Нехай $p = 113$; $q = 599$; $n = 67687$; $\phi(67687) = 66976$; $e = 311$; $M = 1000$; $J_A = 200$; $\alpha_A = 2000$; $J_B = 500$; $\alpha_B = 5000$.

Розрахували особисті ключі абонентів $k_A = 12014$ і $k_B = 26394$ (дивись попередній приклад).

Розрахунок колективного підпису:

$$\begin{aligned}
 x_A &\equiv 2000^{311} \bmod 67687 \equiv 7758; \quad x_B \equiv 5000^{311} \bmod 67687 \equiv 12912; \\
 x &\equiv (7758 \cdot 12912) \bmod 67687 \equiv 62223; \\
 r &= h(1000 \parallel 62223) = h(100062223) = 300; \\
 s_A &\equiv (2000 \cdot 12014^{300}) \bmod 67687 \equiv 50030; \quad s_B \equiv (5000 \cdot 26394^{300}) \bmod 67687 \equiv 32463; \\
 s &\equiv (50030 \cdot 32463) \bmod 67687 \equiv 42012.
 \end{aligned}$$

Параметри колективного підпису $(300, 42012)$, а також $M = 1000$; $J_A = 200$; $J_B = 500$ передаються одержувачеві. Перевірка підпису:

$$\begin{aligned}
 J &\equiv (200 \cdot 500) \bmod 67687 \equiv 32313; \\
 u &\equiv (42012^{311} \cdot 32313^{300}) \bmod 67687 \equiv 62223; \\
 r' &= h(1000 \parallel 62223) = h(100062223) = 300 = r - \text{підпис є справжній.}
 \end{aligned}$$

4.7 Електронний підпис на базі шифру Ель-Гамалія

Нехай відправник збирається підписати документ M . Він обирає велике просте число p і число g (первісний корінь p). Ці числа передаються або зберігаються у відкритому вигляді і можуть бути спільними для цілої групи користувачів. Відправник обирає випадкове число k – особистий ключ; $1 < k < p - 1$; $\text{НОД}(k, p - 1) = 1$ й обчислює

$$Y \equiv g^k \pmod{p}.$$

Число Y відправник подає в якості відкритого ключа.

Опишемо послідовність дій для побудови підпису (рис. 4.15).

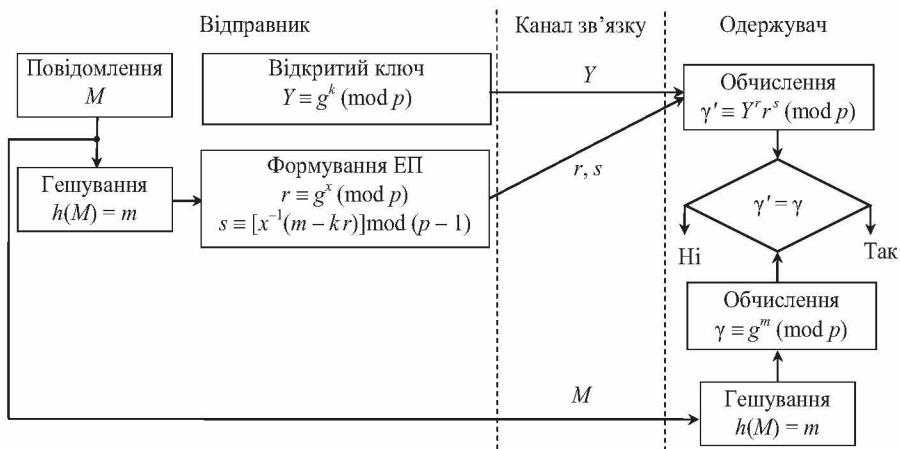


Рисунок 4.15 – Схема електронного підпису Ель-Гамалія

Спочатку обчислюється значення геш-функції $h(M) = m$ й обирається випадкове число x таке, що $x < p - 1$ та взаємно просте з $p - 1$, й обчислюються числа:

$$r \equiv g^x \pmod{p};$$

$$s \equiv [x^{-1}(m - kr)] \pmod{p - 1}.$$

Підписом документа M є пара чисел (r, s) які передається одержувачу.

Одержувач насамперед обчислює значення геш-функції $h(M) = m$ і потім перевіряє підпис, використовуючи рівність

$$(Y^r r^s) \bmod p = g^m \bmod p).$$

Якщо рівність виконується, то підпис є справжній.

Доказ коректності підпису Ель-Гамала

$$\begin{aligned} (Y^r r^s) \bmod p &\equiv (g^{rk} g^{sx}) \bmod p \equiv g^{rk+sx} \bmod p \equiv \\ &\equiv g^{rk+x(m-kr)x^{-1}+(p-1)m} \bmod p \equiv g^{m+(p-1)m} \bmod p \equiv \\ &\equiv (g^m g^{(p-1)m}) \bmod p \equiv g^m \bmod p). \end{aligned}$$

Приклад електронного підпису Ель-Гамала. Нехай $p = 97$; $g = 223$; $k = 43$; $h(M) = 83$; $x = 71$. Відправник обчислює відкритий ключ

$$Y \equiv 223^{43} \bmod 97 \equiv 90.$$

Переходить до обчислення підпису:

$$\begin{aligned} r &\equiv 223^{71} \bmod 97 \equiv 26; \\ s &\equiv [71^{-1}(83 - 43 \cdot 26)] \bmod (97 - 1) \equiv (23 \cdot 21) \bmod 96 \equiv 3. \end{aligned}$$

Формується підписане повідомлення у вигляді $(M, 26, 3)$, яке передається одержувачеві. Одержувач перевіряє справжність підпису. Спочатку він обчислює значення геш-функції $h(M) = 83$, а потім

$$\begin{aligned} (90^{26} \cdot 26^3) \bmod 97 &\equiv (86 \cdot 19) \bmod 97 \equiv 82; \\ 223^{83} \bmod 97 &\equiv 82. \end{aligned}$$

Одержувач робить висновок, що підпис є справжній.

Головною перевагою схеми електронного підпису Ель-Гамала є можливість виробляти підписи для великого числа повідомлень з використанням тільки одного секретного ключа. Щоб зловмисникові підробити підпис, йому потрібно вирішити складні математичні завдання зі

знаходження дискретного логарифма в полі Z_p . Випадкове число x має відразу після обчислення підпису знищуватися, тому якщо, зловмисник знає випадкове число x і сам підпис, то він може знайти особистий ключ.

4.8 Електронний підпис Шнорра

Обирається просте число p довжиною 1024 бітів і q простий дільник числа $(p - 1)$, яке має той самий розмір, що і геш-код, створений геш-функцією h (довжину параметра q прийнято обирати рівною 160 бітам). Вибирається число α – елемент поля Z_p порядку q , відмінне від 1, таке, що $\alpha^q \equiv 1 \pmod{p}$. Параметри (p, q, α) вільно публікуюються. Користувач обирає особистий ключ k , який повинен бути менше q й обчислює відкритий ключ (на базі секретного ключа)

$$Y \equiv \alpha^{-k} \pmod{p}.$$

Для того, щоб підписати повідомлення M користувач виконує наступні дії:

– вибирає випадкове число r , яке $r < q$ й обчислює параметр x

$$x \equiv \alpha^r \pmod{p};$$

– об'єднує повідомлення M і x та гешує результат для одержання першого параметра підпису S_1 :

$$S_1 = h(M \| x);$$

– обчислює другий параметр підпису S_2 :

$$S_2 \equiv (r + kS_1) \pmod{q}.$$

Підписом повідомлення M є пара чисел (S_1, S_2) , які передаються одержувачу.

Перевірка підпису. Нехай прийнято повідомлення M і його значення S_1 та S_2 . Одержувач обчислює параметр x

$$x \equiv (Y^{S_1} \alpha^{S_2}) \bmod p$$

та перевіряє рівність результат (конкатенація M і x) геш-функції h зі параметром підпису S_1

$$h(M \| x) = S_1.$$

Якщо рівність виконується, то підпис є справжній.

Доказ коректності підпису Шнорра

$$\begin{aligned} x &\equiv (Y^{S_1} \alpha^{S_2}) \bmod p \equiv (\alpha^{-kS_1} \alpha^{r+kS_1}) \bmod p \equiv \\ &\equiv \alpha^{-kS_1+r+kS_1} \bmod p \equiv \alpha^r \bmod p = x. \end{aligned}$$

Схема електронного підпису Шнорра показана на рис. 4.16.

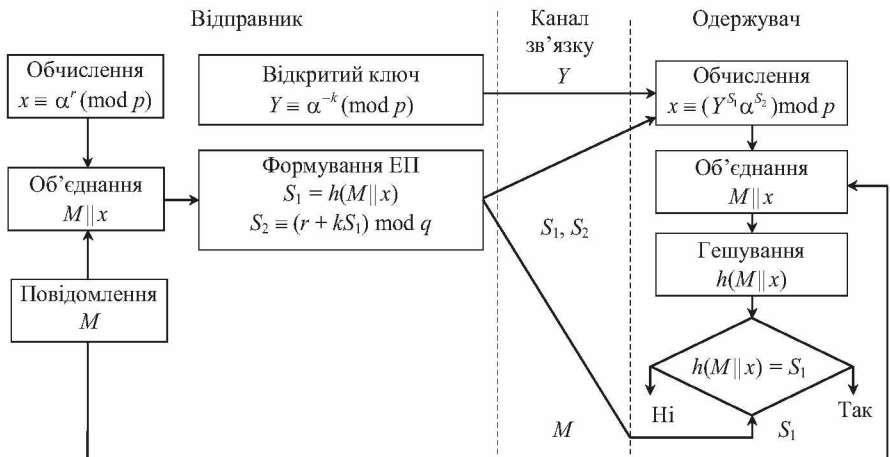


Рисунок 4.16 – Схема електронного підпису Шнорра

Приклад електронного підпису Шнорра. Нехай $p = 1811$; $q = 181$; $\alpha = 85$; $M = 100$; $r = 104$; $k = 167$. Відправник обчислює відкритий ключ

$$Y \equiv 85^{-167} \pmod{1811} \equiv 1044^{167} \pmod{1811} \equiv 1641.$$

Потім переходить до обчислення підпису. Розрахунок параметра x

$$x \equiv 85^{104} \pmod{1811} \equiv 256.$$

Припустимо, що конкатенація повідомлень $M=100$ і $x=256$ дає результат $M\|x = 100256$. Також припустимо, що гешування цього значення дає дайджест $h(100256) = 365$. Це означає, що перший параметр підпису $S_1 = 365$. Розрахуємо другий параметр підпису S_2 :

$$S_2 \equiv (104 + 167 \cdot 356) \pmod{181} \equiv 7.$$

Формується підписане повідомлення у вигляді $(M, 365, 7)$, яке передається одержувачеві. Одержувач обчислює параметр x

$$x \equiv (1641^{365} \cdot 85^7) \pmod{1811} \equiv (1428 \cdot 127) \pmod{1811} \equiv 256.$$

Далі одержувач перевіряє рівність результатів $h(M\|x) = S_1$. Конкатенація повідомлень $M=100$ і $x=256$ дає результат 100256 , а гешування $h(100256) = 365$.

$$h(100256) = 365 = S_1.$$

Одержувач робить висновок, що підпис є справжній.

4.9 Стандарт цифрового підпису DSS

Національний інститут стандартів і технологій США опублікував федеральний стандарт опрацювання інформації FIPS PUB 186, відомий також як DSS (Digital Signature Standard – стандарт цифрового підпису) [17]. Стандарт DSS базується на алгоритмі гешування SHA і становить нову технологію використання цифрового підпису – алгоритм DSA (Digital Signature Algorithm – алгоритм цифрового підпису). Алгоритм DSA є

“класичним” прикладом схеми ЕП на базі використання геш-функції та асиметричного алгоритму шифрування. Стандарт DSS було запропоновано 1991 року, а його відкоригована версія – 1993 року, у відповідь на що виникли сумніви щодо безпеки відповідної схеми. 1996 року в ньому відбулися незначні корективи.

У даному стандарті підпис становить собою два надвеликих цілих числа, одержані у відповідності з процедурами і параметрами, окреслених у DSS. Стійкість системи в цілому ґрунтується на складності знаходження дискретних логарифмів у кінцевих полях.

У стандарті DSS використовується алгоритм, призначений забезпечити лише функцію цифрового підпису. На відміну від RSA, даний алгоритм не може бути використано для шифрування чи обміну ключами.

Алгоритм цифрового підпису DSA створено з урахуванням складнощів обчислення дискретних логарифмів і спирається на схеми, запропоновані Ель-Гамалем та Шнорром. В алгоритмі використовуються три параметри, які є відкритими і передбачаються відомими групі користувачів.

Обирається просте число p довжиною між бітами 512...1024 і $q - 160$ -бітовий простий дільник числа $(p - 1)$. Нарешті обирається число g форми

$$g \equiv h^{(p-1)/q} \pmod{p},$$

де h є цілим числом між 1 та $(p - 1)$, з тим обмеженням, що g має бути більше за 1.

Параметри p , q і g публікуються для всіх користувачів системи ЕД з ЕП. Знаючи ці числа, кожен користувач обирає особистий ключ та генерує відкритий ключ. Особистий ключ k повинен бути числом від 1 до $(q - 1)$ й обиратися у випадковий чи псевдовипадковий спосіб (тримається у секреті). Відкритий ключ обчислюється на базі особистого ключа $Y \equiv g^k \pmod{p}$.

Створення підпису (алгоритм DSA схематично надано в табл. 4.1). Для генерації ЕП користувач обчислює дві величини r і s , які є функціями компонентів відкритого ключа (p, q, g) , особистого ключа користувача k , геш-коду повідомлення $h(M)$ (спочатку рекомендували геш-функцію SHA-1 пізніше SHA-2) і певного цілого числа x , яке має обиратися у випадковий чи псевдовипадковий спосіб і бути єдиним для кожного виконання підпису.

Таблиця 4.1 – Алгоритм цифрового підпису DSA

<i>Глобальні компоненти відкритого ключа:</i>¹ p – просте число, $2^{L-1} < p < 2^L$, де $512 \leq L \leq 1024$ і L кратне до 64, тобто має довжину між бітами 512...1024 з кроком 64 біти; q – простий дільник $(p - 1)$, де $2^{159} < q < 2^{160}$, тобто довжиною 160 бітів; $g \equiv h^{(p-1)/q} \pmod{p}$, де h є яким завгодно цілим числом таким, що $1 < h < (p - 1)$ і $h^{(p-1)/q} \pmod{p} > 1$.
<i>Особистий ключ користувача</i> k – випадкове чи псевдовипадкове число, $0 < k < q$.
<i>Відкритий ключ користувача</i> $Y \equiv g^k \pmod{p}$.
<i>Секретний номер повідомлення користувача</i> x – випадкове чи псевдовипадкове число, $0 < x < q$.
<i>Створення підпису:</i> $r \equiv (g^x \pmod{p}) \pmod{q}$; $s \equiv [x^{-1}(h(M) + kr)] \pmod{q}$; якщо $r = 0$ або $s = 0$, обираємо інший x. <i>Підпис:</i> (r, s)
<i>Перевірка підпису:</i> $u_1 \equiv (h(M)s^{-1}) \pmod{q}$; $u_2 \equiv (rs^{-1}) \pmod{q}$; $v \equiv [(g^{u_1} Y^{u_2}) \pmod{p}] \pmod{q}$. <i>Перевірка рівності:</i> $v = r$
¹У першій версії стандарту DSS рекомендована функція SHA-1 і, відповідно, бітова довжина 160 бітів. Зараз SHA-1 вже не є достатньо безпечним, тому рекомендують геш-функцію SHA-2. У стандарті вказані наступні можливі пари розмірності (в бітах) чисел p, q: (1024, 160), (2048, 224), (2048, 256), (3072, 256).

Значення r та s є ЕП повідомлення M і передаються разом з ним відкритими каналами зв'язку.

Перевірка підпису. Нехай прийнято повідомлення M і його ЕП з параметрами (r, s) . Одержувач перевіряє виконання умов $0 < r < q$ та $0 < s < q$; якщо хоча б одну з них порушено, підпис скасовується. Потім обчислюється величина v :

$$v \equiv [(g^{u_1} Y^{u_2}) \bmod p] \bmod q.$$

Якщо ця величина відповідає компоненту r підпису, то підпис підтверджується. Слід звернути увагу на те, що перевірка наприкінці здійснюється зі значенням r , яке не залежить від повідомлення.

Доказ коректності підпису DSA

$$\begin{aligned} r &\equiv (g^x \bmod p) \bmod q \equiv (g^{\lceil s^{-1}(h(M) + kr) \rceil} \bmod p) \bmod q \equiv \\ &\equiv (g^{(s^{-1} h(M)) \bmod q} g^{(s^{-1} kr) \bmod q} \bmod p) \bmod q \equiv \\ &\equiv (g^{(s^{-1} h(M)) \bmod q} Y^{(s^{-1} r) \bmod q} \bmod p) \bmod q \equiv [(g^{u_1} Y^{u_2}) \bmod p] \bmod q = v. \end{aligned}$$

Схему алгоритму цифрового підпису DSA показано на рис. 4.17.

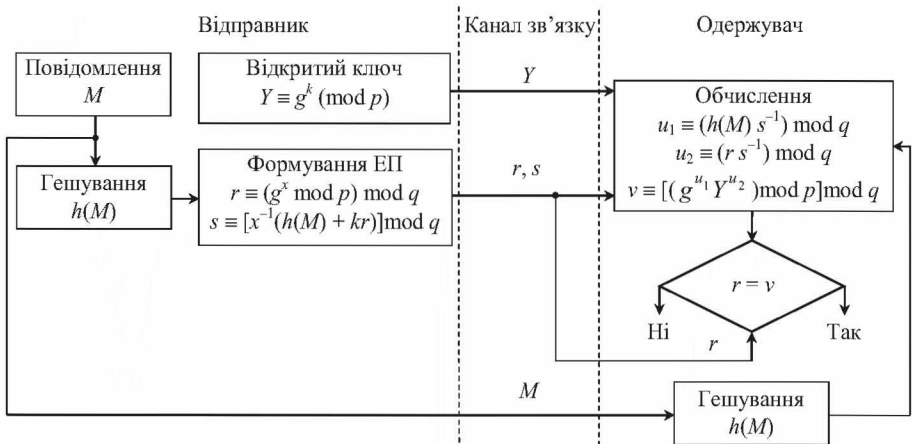


Рисунок 4.17 – Алгоритм цифрового підпису DSA

Приклад електронного підпису DSA. Нехай $p = 1511$; $q = 151$; $g = 1024$; $k = 113$; $x = 97$; $h(M) = 100$. Відправник обчислює відкритий ключ

$$Y \equiv 1024^{113} \pmod{1511} \equiv 1467.$$

Переходить до обчислення підпису. Розрахунок параметрів r, s :

$$r \equiv [1024^{97} (\bmod 1511)] \bmod 151 \equiv 1020 (\bmod 151) \equiv 114;$$

$$s \equiv [97^{-1}(100 + 113 \cdot 114)] \bmod 151 \equiv (137 \cdot 147) \bmod 151 \equiv 56.$$

Формується підписане повідомлення у вигляді $(M, 114, 56)$, яке передається одержувачеві. Одержувач обчислює параметри:

$$u_1 \equiv (100 \cdot 56^{-1}) \bmod 151 \equiv 142;$$

$$u_2 \equiv (114 \cdot 56^{-1}) \bmod 151 \equiv 29;$$

$$v \equiv [(1024^{142} \cdot 1467^{29}) \bmod 1511] \bmod 151 \equiv$$

$$\equiv 1020 (\bmod 151) \equiv 114.$$

Далі одержувач перевіряє рівність результатів $v = r = 114$ – підпис є справжній.

4.10 Алгоритм електронного підпису Ніберга-Рюпеля з відновленням повідомлення

Підпис Ніберга-Рюпеля (Nyberg-Rueppel) – схема електронного підпису з відновленням повідомлення заснована на завданні дискретного логарифмування в кінцевому полі. Схема підпису з відновленням повідомлення має на увазі процедуру, коли повідомлення відновлюється після перевірки підпису, для цього використовують відкриту функцію надмірності F , яка є легко оборотною.

Обирається відкрита функція надмірності F , яка перетворює повідомлення M в дані, які потім підписуються (функція F повинна бути легко оборотною, наприклад $F(M) = M + 2^n \cdot M$).

Обирається просте число p і q – простий дільник числа $(p - 1)$, число α – елемент поля Z_p порядку q , відмінне від 1, таке, що $\alpha^q \equiv 1 \bmod p$.

Параметри p , q і α публікуються для всіх користувачів системи ЕП. Особистий ключ k повинен бути числом від 1 до $(q - 1)$ й обиратися у випадковий чи псевдовипадковий спосіб (тримається у секреті). Відкритий ключ Y обчислюється на базі особистого ключа k

$$Y \equiv \alpha^k (\bmod p).$$

Для того, щоб підписати повідомлення M користувач виконує наступні дії:

- обчислює $F(M) = m$;
- обирає випадкове число z , яке $1 < z < q - 1$ і обчислює параметр x

$$x \equiv \alpha^{-z} \pmod{p};$$

- обчислює перший параметр підпису r

$$r \equiv (mx) \pmod{p};$$

- обчислює другий параметр підпису s

$$s \equiv (rk + z) \pmod{q}.$$

Підписом повідомлення M є пара чисел (r, s) які передається одержувачеві.

Перевірка підпису. Нехай прийнято повідомлення M і його ЕП з параметрами (r, s) . Одержувач перевіряє виконання умов $0 < r < p$ та $0 < s < q$, якщо хоча б одну з них порушено, підпис скасовується. Потім обчислюється величина v і m' :

$$\begin{aligned} v &\equiv (\alpha^s Y^{-r}) \pmod{p}; \\ m' &\equiv (vr) \pmod{p}. \end{aligned}$$

Одержувач виконує зворотнє перетворення $F^{-1}(m') = M'$ та перевіряє рівність $M' = M$, якщо рівність виконується, то підпис є справжній.

Доказ коректності підпису Ніберга-Рюпеля

$$\begin{aligned} v &\equiv (\alpha^s Y^{-r}) \pmod{p} \equiv (\alpha^{rk+z} \alpha^{-kr}) \pmod{p} \equiv \\ &\equiv (\alpha^{rk+z-kr}) \pmod{p} \equiv \alpha^z \pmod{p}; \\ m' &\equiv (vr) \pmod{p} \equiv (vmx) \pmod{p} \equiv (\alpha^z m \alpha^{-z}) \pmod{p} \equiv m. \end{aligned}$$

Схему електронного підпису Ніберга-Рюпеля показано на рис. 4.18.

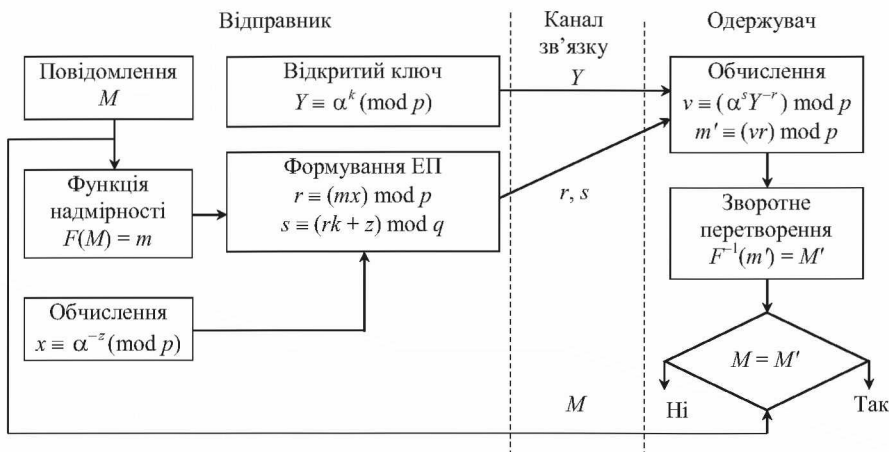


Рисунок 4.18 – Схема електронного підпису Ніберга-Рюпеля

Приклад електронного підпису Ніберга-Рюпеля. Нехай $p = 2111$; $q = 211$; $\alpha = 1384$; $z = 201$; $M = 50$; $k = 176$.

Відправник обчислює Y , m і x :

$$\begin{aligned}
 Y &\equiv 1384^{176} \pmod{2111} \equiv 729; \\
 m &= F(50) = 50 + 2^5 \cdot 50 = 1650; \\
 x &\equiv 1384^{-201} \pmod{2111} \equiv 569.
 \end{aligned}$$

Переходить до обчислення підпису. Розрахунок параметрів r і s :

$$\begin{aligned}
 r &\equiv (1650 \cdot 569) \pmod{2111} \equiv 1566; \\
 s &\equiv (176 \cdot 1566 + 201) \pmod{211} \equiv 40.
 \end{aligned}$$

Формується підписане повідомлення $M = 50$ у вигляді $(1566, 40)$, яке передається одержувачеві. Одержувач перевіряє виконання умов $0 < 1566 < 2111$ та $0 < 40 < 211$ – умови виконані. Потім обчислюються величини v і m' :

$$\begin{aligned}
 v &\equiv (1384^{40} \cdot 729^{-1566}) \pmod{2111} \equiv (1538 \cdot 638) \pmod{2111} \equiv 1740; \\
 m' &\equiv (1740 \cdot 1566) \pmod{2111} \equiv 1650.
 \end{aligned}$$

Одержувач виконує зворотнє перетворення

$$M' = F^{-1}(1650) = 1650 : 33 = 50$$

та перевіряє рівність $M' = M = 50$ – підпис є справжній.

4.11 Криптосистема на еліптичних кривих

Криптосистеми на еліптичних кривих (Elliptic Curve Cryptography – ECC) [10, 15, 16, 18 ... 23] належать до класу криптосистем з відкритим ключем. Їхня безпека базується здебільшого на складності розв’язування задачі дискретного логарифмування у групі точок еліптичної кривої (Elliptic Curve Discrete Logarithm Problem – ECDLP) над кінцевим полем. Цим зумовлено їхню потужну криптостійкість порівняно з іншими алгоритмами. Рішення проблеми ECDLP є більш складним, ніж вирішення проблеми дискретного логарифмування (Discrete Logarithm Problem – DLP).

Існують стійкі криптоалгоритми на еліптичних кривих, базовані на труднощах розкладання великих цілих чисел, коли еліптична крива задається над кінцевим кільцем за складеним модулем, але вони зустрічаються дуже рідко. Проте слід зауважити, що криптостійкість є відносним поняттям, пов’язаним з поняттям найоптимальнішого відомого алгоритму злому системи.

Еліптичні криві (Elliptic Curve – EC) – математичний об’єкт, який може бути визначено над яким завгодно полем. У криптографії зазвичай використовуються кінцеві поля. Для точок на еліптичній кривій вводиться операція складання, яка відіграє ту саму роль, що й операція множення у криптосистемах RSA та Ель-Гамала.

Іншою перевагою криптосистем на еліптичних кривих є висока швидкість опрацювання інформації. Але й тут не все так просто. Зрозуміло, що, маючи потужну криптостійкість, криптосистеми на еліптичних кривих дозволяють використовувати ключ меншої довжини. Проте прийнятна для роботи в мережах, швидкість обчислень досягається лише при використанні спеціалізованих обчислювачів (це цілком природно для криптосистем з відкритим ключем) та полів спеціальних характеристик.

Криптосистеми на еліптичних кривих, як й інші криптосистеми з відкритим ключем, недоцільно застосовувати для шифрування великих обсягів даних. Проте їх можна ефективно використовувати для систем електронного підпису та ключового обміну. З 1998 року використання еліптичних кривих для розв'язування криптографічних задач, таких як електронний підпис, було закріплено у стандартах США ANSI X9.62, FIPS 186-2 [24] та інших.

В Україні ухвалений стандарт цифрового підпису ДСТУ 4145–2002 [25], який базується на еліптичних кривих, а також:

- ДСТУ ISO/IEC 15946-1:2019 «Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 1. Загальні положення» (ISO/IEC 15946-1:2016, IDT);

- ДСТУ 9041:2020 «Інформаційні технології. Криптографічний захист інформації. Алгоритм шифрування коротких повідомлень, що ґрунтується на скручених еліптичних кривих Едвардса»;

- ДСТУ ISO/IEC 15946-5:2019 «Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих» (ISO/IEC 15946-5:2017, IDT).

Зазначимо, що безпека таких систем електронного підпису спирається не лише на стійкість алгоритму на еліптичних кривих, але й на стійкість використовуваної геш-функції.

Численні дослідження свідчать [15, 20, 21, 26], що криптосистеми на підставі еліптичних кривих перевершують інші системи з відкритим ключем за двома важливими параметрами:

- 1) мірою захищеності з розрахунку на кожен біт ключа;
- 2) за швидкодією програмної й апаратної реалізації.

Це пояснюється тим, що для обчислення обернених функцій на еліптичних кривих відомі лише алгоритми з експоненційним зростанням трудомісткості, тоді як для звичайних систем запропоновано субекспоненційні методи. Як наслідок, той рівень стійкості, який досягається, скажімо, в RSA при використанні 1024-бітових модулів, у системах на еліптичних кривих зреалізовується при розмірі модуля 163 бітів, що забезпечує простішу як програмну, так і апаратну реалізацію, а також можливість застосування більш коротких ключів (див. табл. 4.2 [26] згідно з NIST – National Institute of Standards and Technology).

Таблиця 4.2 – Розмір ключів для ECC і RSA згідно з NIST

ECC key, Bits	RSA key, Bits	Key ratio
163	1024	1 : 6
256	3072	1 : 12
384	7680	1 : 20
512	15360	1 : 30

У криптосистем на еліптичних кривих запропоновано використовувати криптоперетворення, що базуються на перетвореннях у групі точок еліптичних кривих над полями $GF(p)$, $GF(2^m)$, $GF(p^m)$.

У **криптосистемах на ЕС простого поля $GF(p)$** використовується рівняння

$$y^2 \equiv x^3 + ax + b \pmod{p},$$

де $a, b \in GF(p)$; $4a^3 + 27b^2 \pmod{p} \neq 0$; $p > 3$ – просте. Група $E(GF(p))$ складається з усіх точок (x, y) ; $x, y \in GF(p)$, які задовольняють рівнянню, і нескінченно віддаленої точки O (рис. 4.19):

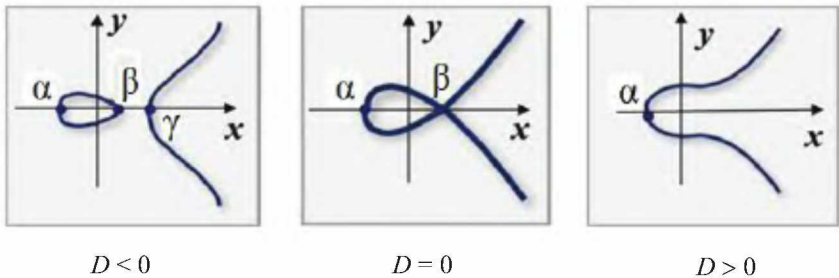


Рисунок 4.19 – Графіки еліптичної кривої за різних значень дискримінанта

$$D \equiv [-16(4a^3 + 27b^2)] \pmod{p}$$

- якщо $D < 0$, то рівняння має три різних дійсних кореня α , β , γ ;
- якщо $D = 0$, то рівняння має корені α , β . У цьому випадку еліптична крива сингулярна;
- якщо $D > 0$, то рівняння має один дійсний корінь α і два комплексних.

Таким чином, якщо характеристика поля $p \neq 2$ і $p \neq 3$, то крива $y^2 \equiv x^3 + ax + b \pmod{p}$ (називається формою Вейєрштрасса), буде несингулярна за умови, що дискримінант $D \equiv [-16(4a^3 + 27b^2)] \pmod{p} \neq 0$.

Множина $E_p(a, b)$ складається з усіх точок (x, y) , $x \geq 0$, $p > y$, які задовольняють рівнянню $y^2 \equiv x^3 + ax + b \pmod{p}$, й точки в нескінченності O . Кількість точок в $E_p(a, b)$, що належать еліптичній кривій, називаються **порядком кривої** $\#E_p(a, b)$ або $|E_p(a, b)|$. **Порядком точки** $P \in E$ називається таке мінімальне ціле позитивне число n , що $nP = O$. Ця величина має важливе значення для криптографічних додатків еліптичних кривих. **Рангом еліптичної кривої** $E_p(a, b)$ називається мінімальне число раціональних точок нескінченного порядку. Точне число точок еліптичної кривої $E_p(a, b)$ обчислити досить важко, проте теорема Хассе про еліптичні криві дає наступну оцінку [20, 21],

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}.$$

Якщо точка P має порядок, то:

- множина $\{O, P, 2P, \dots, (n-1)P\}$ – утворює циклічну підгрупу в $E_p(a, b)$;
 - порядок будь-якої точки є дільником загального числа точок еліптичної кривої, тобто порядку групи точок еліптичної кривої;
 - при $n = |E_p(a, b)|$, точка є утворюючим елементом (генератором) групи.
- При відповідному виборі параметрів a і b (задовольняють умовам $4a^3 + 27b^2 \pmod{p} \neq 0$) число точок на кривій може дорівнювати простому числу і тоді будь-яка точка кривої, крім O , буде породжувати всю групу.

Порядок $\#E_p(a, b)$ еліптичної кривої можна надати у вигляді

$$\#E_p(a, b) = p + 1 - t,$$

де параметр t може приймати як позитивні, так і негативні значення або бути рівним нулю і називається **слідом Фробеніуса** для $E_p(a, b)$.

Важливим параметром еліптичної кривої є інваріант $J(E)$

$$J(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Інваріант $J(E)$ не змінюється при лінійних перетвореннях еліптичної кривої. По відомому інваріанту можна визначити коефіцієнти a, b еліптичної кривої.

Якщо дві криві мають однаковий інваріант, то вони є *ізоморфними кривими*.

Визначену над точками з $E(GF(p))$ операцію додавання алгебраїчно може бути описано в такий спосіб:

$$1) P + O = O + P = P;$$

2) якщо $P = (x, y)$, тоді $P + (x, -y) = O$. Точка $(x, -y)$ є від'ємним значенням точки P і позначається $-P$. Зазначимо, що $(x, -y)$ лежить на еліптичній кривій і належить до $E_p(a, b)$;

3) якщо $P = (x_1, y_1)$ і $Q = (x_2, y_2)$, то $P + Q = (x_3, y_3)$ визначається згідно з правилами:

$$\begin{aligned} x_3 &\equiv (\lambda^2 - x_1 - x_2) \bmod p; \\ y_3 &\equiv [\lambda (x_1 - x_3) - y_1] \bmod p, \end{aligned}$$

де λ – кутовий коефіцієнт визначається

$$\lambda \equiv \begin{cases} \left(\frac{y_2 - y_1}{x_2 - x_1} \right) \bmod p, & P \neq Q; \\ \left(\frac{3x_1^2 + a}{2y_1} \right) \bmod p, & P = Q. \end{cases}$$

Число λ – кутовий коефіцієнт січної, проведеної через точки $P = (x_1, y_1)$ та $Q = (x_2, y_2)$. За $P = Q$ січна перетворюється на дотичну, чим і пояснюється наявність двох формул для обчислення λ .

Графічне представлення складання точок та подвоєння точки еліптичної кривої подано на рис. 4.20, 4.21.

Сума точок $P + Q$ – це точка R , зворотна третьої точки перетину кривої й прямої (див. рис. 4.20). Якщо $P = Q$, то $P + Q = P + P = 2P$ – подвоєння точка. Точка $2P$ – це точка R , зворотна точки перетину кривої та дотичної в точці P (див. рис. 4.21).

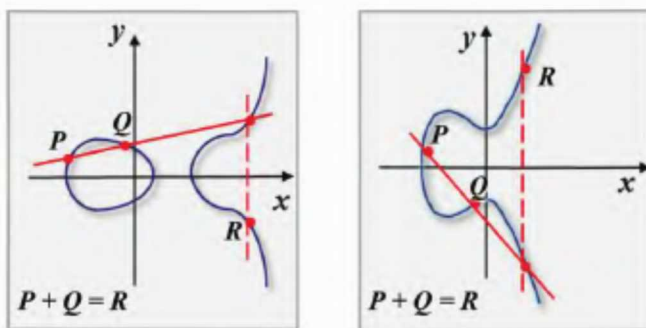


Рисунок 4.20 – Показано графічне складання точок еліптичної кривої

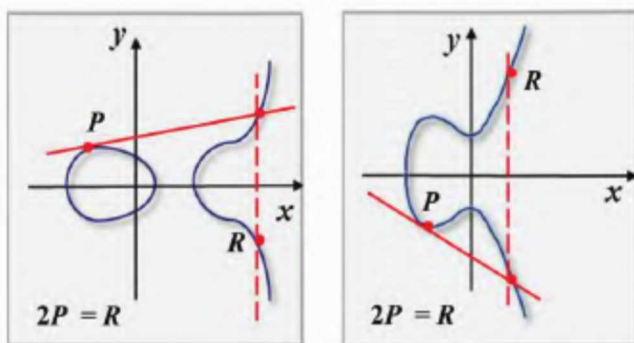


Рисунок 4.21 – Показано графічне подвоєння точки еліптичної кривої

Для того, щоб знайти точки на еліптичній кривій $y^2 \equiv x^3 + ax + b \pmod{p}$, необхідно:

- для кожного значення $1 \leq x \leq p - 1$ обчислити $y^2 \equiv x^3 + ax + b \pmod{p}$;
- для всіх значень y^2 з'ясувати, чи будуть вони квадратично вираховувані або невраховувані за модулем p ;
- якщо y^2 квадратично вираховувані, то знайти корені y_1 і y_2 . Точки (x, y_1) і (x, y_2) лежать на кривій $E_p(a, b)$;
- якщо y^2 квадратично невраховувані, точок з такою абсцисою на кривій немає.

Приклад. Знайти всі точки на еліптичній кривій $E_7(2, 6)$.

Задано $p = 7$; $a = 2$; $b = 6$; $y^2 \equiv x^3 + 2x + 6 \pmod{7}$.

Розрахунки надано в табл. 4.3.

Таблиця 4.3 – Розрахунок точок на еліптичній кривій $E_7(2, 6)$

x	1	2	3	4	5	6
y^2	2	4	4	1	1	3
Символи Лежандра	1	1	1	1	1	-1
Квадратні корені y_1, y_2	4, 3	2, 5	2, 5	1, 6	1, 6	—

Еліптична крива $E_7(2, 6)$ складається з точки O , а також знайдених точок $(1, 4); (1, 3); (2, 2); (2, 5); (3, 2); (3, 5); (4, 1); (4, 6); (5, 1); (5, 6)$ (рис. 4.22).

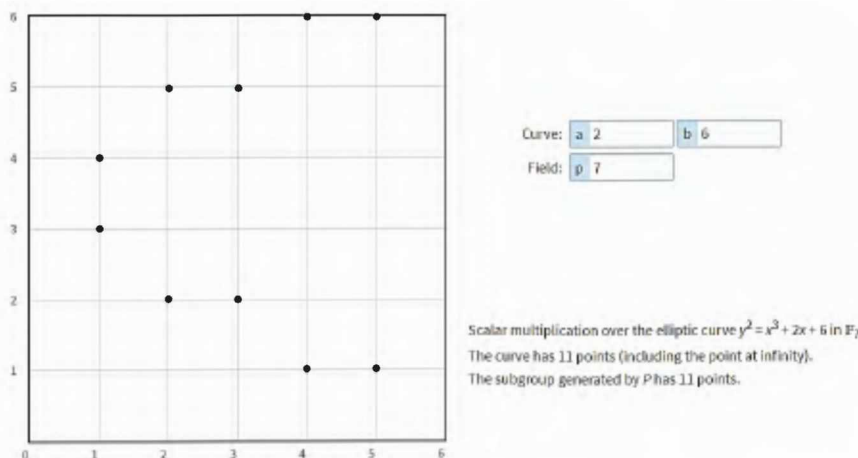


Рисунок 4.22 – Точки на еліптичній кривій $E_7(2, 6)$

Приклад. Знайти $P + Q$; $2P$ і $2P - Q$ для еліптичної кривої $E_{23}(1, 1)$, де $P = (3, 10)$ і $Q = (9, 7)$.

Знаходимо $P + Q = (3, 10) + (9, 7) = (x_3, y_3)$, тоді

$$\lambda \equiv \left(\frac{7 - 10}{9 - 3} \right) \bmod 23 \equiv -\frac{1}{2} \bmod 23 \equiv 11;$$

$$x_3 \equiv (11^2 - 3 - 9) \bmod 23 \equiv 17;$$

$$y_3 \equiv [11(3 - 17) - 10] \bmod 23 \equiv 20.$$

Отже, $P + Q = (3, 10) + (9, 7) = (17, 20)$ (рис. 4.23).

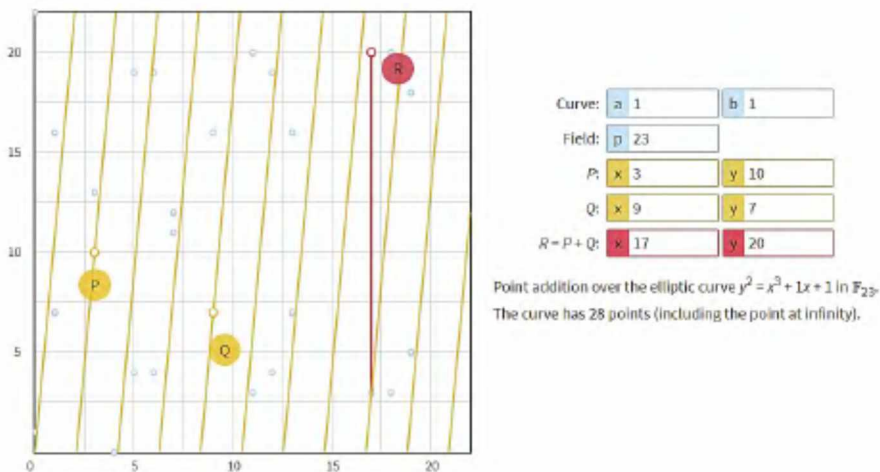


Рисунок 4.23 – Сума точок $P + Q$ на еліптичній кривій $E_{23}(1, 1)$

Знаходимо $2P = 2(3, 10) = (3, 10) + (3, 10) = (x_3, y_3)$, тоді

$$\lambda \equiv \left(\frac{3 \cdot 3^2 + 1}{2 \cdot 10} \right) \bmod 23 \equiv \frac{1}{4} (\bmod 23) \equiv 6;$$

$$x_3 \equiv (6^2 - 2 \cdot 3) \bmod 23 \equiv 7;$$

$$y_3 \equiv [6(3 - 7) - 10] \bmod 23 \equiv 12.$$

Отже, $2P = 2(3, 10) = (7, 12)$ (рис. 4.24).

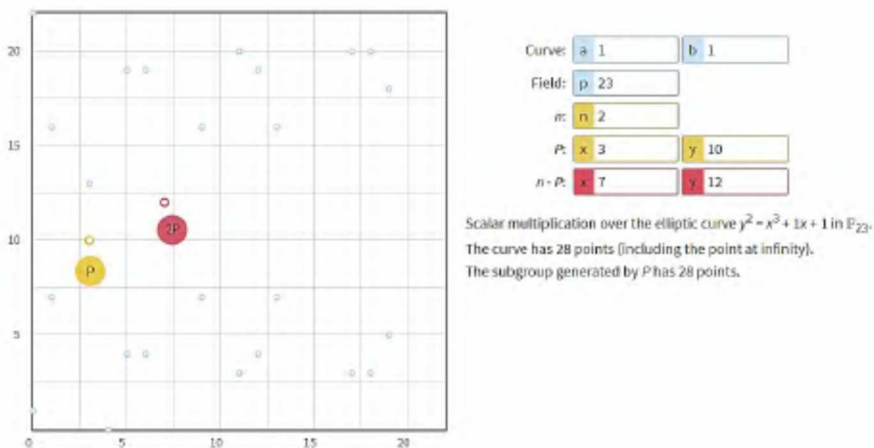


Рисунок 4.24 – Подвоєння точки P на еліптичній кривій $E_{23}(1, 1)$

Знаходимо $2P - Q = (7, 12) - (9, 7) = (7, 12) + (9, 16) = (x_3, y_3)$, тоді

$$\lambda \equiv \left(\frac{16 - 12}{9 - 7} \right) \bmod 23 \equiv 2;$$

$$x_3 \equiv (2^2 - 7 - 9) \bmod 23 \equiv 11;$$

$$y_3 \equiv [2(7 - 11) - 12] \bmod 23 \equiv 3.$$

Отже, $2P - Q = (7, 12) - (9, 7) = (11, 3)$ (рис. 4.25).

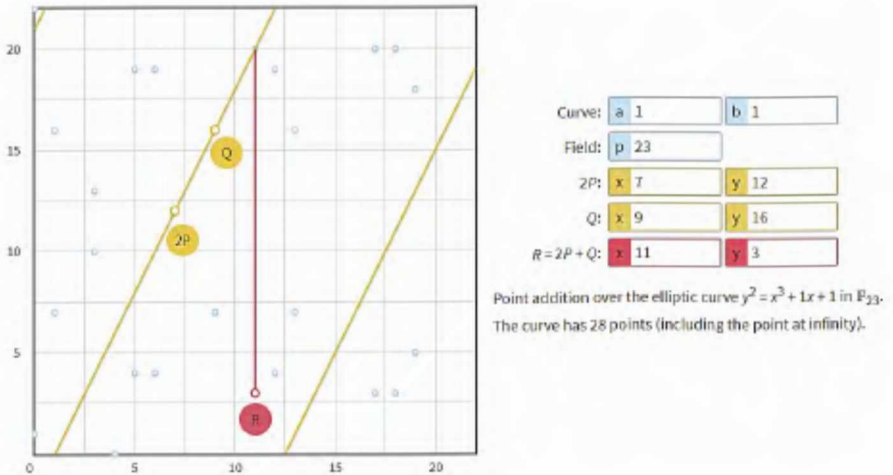


Рисунок 4.25 – Результат розрахунку $2P - Q = 2P + Q$ на кривій $E_{23}(1, 1)$

Приклад. Знайти $13P$ у групі на еліптичній кривій $E_{23}(1, 6)$, де $P = (1, 10)$.

Розрахунок:

$$13_{10} = 1101_2 \Rightarrow 13P = 8P + 4P + P;$$

$$2P = 2(1, 10) = (1, 10) + (1, 10) = (10, 2);$$

$$4P = 4(1, 10) = 2(10, 2) = (10, 2) + (10, 2) = (9, 10);$$

$$8P = 8(1, 10) = 2(9, 10) = (9, 10) + (9, 10) = (14, 21);$$

$$13P = 8P + 4P + P = (14, 21) + (9, 10) + (1, 10) = (14, 2).$$

$$\text{Отже, } 13P = 13(1, 10) = (14, 2).$$

Приклад. Знайти порядок точки $P = (9, 4)$ у групі на еліптичній кривій $E_{11}(6, 3)$, тобто необхідно знайти найменше число n для якого $nP = O$.

Розрахунок точок:

$$\begin{aligned}
2P &= 2(9, 4) = (9, 4) + (9, 4) = (7, 6); \\
3P &= 3(9, 4) = 2(9, 4) + (9, 4) = (7, 6) + (9, 4) = (7, 5); \\
4P &= 4(9, 4) = 2(9, 4) + 2(9, 4) = (7, 6) + (7, 6) = (9, 7); \\
5P &= 5(9, 4) = 4(9, 4) + (9, 4) = (9, 7) + (9, 4) = O.
\end{aligned}$$

Отже, порядок точки $P = (9, 4)$ дорівнює $n = 5$.

Реалізації криптоалгоритмів на базі еліптичних кривих будуються аналогічно алгоритмам у простих кінцевих полях. Фактично операції зведення у степінь і множення за великим модулем, що визначає стійкість шифру, замінюється на скалярний добуток точки еліптичної кривої (табл. 4.4).

Таблиця 4.4 – Принципи побудови криптоалгоритмів у простих кінцевих полях та на базі еліптичних кривих

Терміни і поняття	Криптосистема над простим кінцевим полем	Криптосистема на еліптичній кривій над кінцевим полем
Група	Z_p або Z_n	$E(GF(p))$
Елементи групи	цілі числа $\{1, 2, \dots, (p-1)\}$ або числа $\{1, 2, \dots, (n-1)\}$	точки $P = (x, y)$ на кривій та точка O
Групова операція	множення за модулем p або n	складання точок
Позначення	елементи q, g	точки P, Q
	зворотний елемент g^{-1}	зворотна точка $-P$
	ділення $q/g = q \cdot g^{-1}$	вираховування точок $P - Q$
	зведення у степінь g^x	скалярний добуток xP
Проблема дискретного логарифмування	$g \in Z_p$; $F(x) \equiv g^x \pmod{p}$; знайти x	$P \in E(GF(p))$; $Q = xP$; знайти x

Для використання еліптичної криптографії учасники алгоритму (протоколу) повинні узгодити всі параметри, що визначають еліптичну криву. Генерація еліптичної кривої складається з наступних кроків:

- генерація характеристики поля Галуа;
- генерація коефіцієнтів еліптичної кривої;

- обчислення порядку групи точок еліптичної кривої;
- генерація базової точки;
- визначення порядку базової точки еліптичної кривої.

У криптосистемах над розширеним полем $GF(2^m)$ рівняння ЕС має вигляд (несуперсингулярна крива):

$$y^2 + xy \equiv (x^3 + ax^2 + b) \pmod{f(x), 2},$$

де x, y – точки ЕС, $x, y \in E(GF(2^m))$; a, b – коефіцієнти ЕС; $b \neq (0 \pmod{f(x)}, 2)$; $f(x)$ – незведений поліном над полем $GF(2)$ вигляду

$$f(x) = x^m + h_1 x^{m-1} + h_2 x^{m-2} + \dots + h_{m-1} x^1 + h_m,$$

причому $h_i \in GF(2)$.

Значення x, y, a, b являють собою m -бітні вектори в поліноміальному чи нормальному базисах, зокрема, у поліноміальному базисі x, y, a, b є поліномами не вище m -степеня. При цьому всі операції виконуються за модулем $f(x)$.

Значення порядку n групи точок еліптичної кривої над полем Галуа $GF(2^m)$ має верхню і нижню межі (теорема Хассе) [20, 21]

$$2^m + 1 - 2\sqrt{2^m} \leq n \leq 2^m + 1 + 2\sqrt{2^m}.$$

Відомо два подання груп точок ЕС (два базиси) – афінний і проєктивний.

Афінний базис. Визначимо над точками з $E(GF(2^m))$ операцію складання. Нехай відомі координати двох точок $P = (x_1, y_1)$ і $Q = (x_2, y_2)$, то сума $P + Q = (x_3, y_3)$ визначається згідно з правилами:

$$\begin{aligned} x_3 &\equiv (\lambda^2 + \lambda + x_1 + x_2 + a) \pmod{f(x), 2}; \\ y_3 &\equiv [\lambda(x_1 + x_3) + x_3 + y_1] \pmod{f(x), 2}, \end{aligned}$$

$$\text{де } \lambda \equiv \frac{y_1 + y_2}{x_1 + x_2} \pmod{f(x), 2}.$$

Точка, що подвоєна $2P = P + P = (x_3, y_3)$, визначається згідно з правилами:

$$\begin{aligned}x_3 &\equiv (\lambda^2 + \lambda + a) \bmod (f(x), 2); \\y_3 &\equiv [x_1^2 + (\lambda + 1)x_3] \bmod (f(x), 2),\end{aligned}$$

де $\lambda \equiv x_1 + \frac{y_1}{x_1} \bmod (f(x), 2)$.

Усі параметри є поліномами не вище m -степеня, а $f(x)$ – примітивний поліном над полем $GF(2)$ (додаток Б).

Приклад. Знайти $2P$ і $4P + Q$ для еліптичної кривої над розширеним полем $GF(2^3)$

$$y^2 + xy \equiv (x^3 + x^2 + 10) \bmod (f(x) = x^3 + x + 1, 2),$$

де $P = (10, 100) = (x, x^2)$ і $Q = (10, 110) = (x, x^2 + x)$.

Знаходимо $2P = P + P = (10, 100) + (10, 100) = (x_3, y_3)$, тоді

$$\begin{aligned}\lambda &\equiv \left(x + \frac{x^2}{x} \right) \bmod (f(x), 2) \equiv 0; \\x_3 &\equiv (0^2 + 0 + 1) \bmod (f(x), 2) \equiv 1; \\y_3 &\equiv (x^2 + 1) \bmod (f(x), 2) \equiv x^2 + 1.\end{aligned}$$

Отже, $2P = (x, x^2) + (x, x^2) = (1, x^2 + 1) = (1, 101)$.

Знаходимо $4P = 2P + 2P = (1, 101) + (1, 101) = (x_3, y_3)$, тоді

$$\begin{aligned}\lambda &\equiv (1 + x^2 + 1) \bmod (f(x), 2) \equiv x^2; \\x_3 &\equiv [(x^2)^2 + x^2 + 1] \bmod (f(x), 2) \equiv x + 1; \\y_3 &\equiv [1 + (x^2 + 1)(x + 1)] \bmod (f(x), 2) \equiv x^2 + 1.\end{aligned}$$

Отже, $4P = (1, x^2 + 1) + (1, x^2 + 1) = (x + 1, x^2 + 1) = (11, 101)$.

Знаходимо $4P + Q = (11, 101) + (10, 110) = (x_3, y_3)$, тоді

$$\lambda \equiv \left(\frac{x^2 + 1 + x^2 + x}{x + 1 + x} \right) \bmod (f(x), 2) \equiv x + 1;$$

$$x_3 \equiv [(x+1)^2 + x + 1 + x + 1 + x + 1] \bmod (f(x), 2) \equiv x^2 + x;$$

$$y_3 \equiv [(x+1)(x+1+x^2+x) + x^2 + x + x^2 + 1] \bmod (f(x), 2) \equiv x^2 + x + 1.$$

Отже, $4P + Q = (x+1, x^2+1) + (x, x^2+x) = (x^2+x, x^2+x+1) = (110, 111)$.

Приклад. Знайти порядок точки $P = (10, 10101)$ для еліптичної кривої над розширенням полем $GF(2^5)$ (додаток Б)

$$y^2 + xy \equiv (x^3 + x^2 + 100) \bmod (f(x) = x^5 + x^3 + 1, 2),$$

тобто необхідно знайти найменше число n для якого $nP = O$.

По теоремі Хассе оцінка порядку n групи точок еліптичної кривої над полем $GF(2^5)$ дорівнює:

$$2^5 + 1 - 2\sqrt{2^5} \leq n \leq 2^5 + 1 + 2\sqrt{2^5};$$

$$21,68 \leq n \leq 44,31.$$

Розрахунок точок.

$$\text{Знаходимо } 2P = 2(10, 10101) = 2(x, x^4 + x^2 + 1)$$

$$\lambda \equiv \left[x + \frac{x^4 + x^2 + 1}{x} \right] \bmod (f(x), 2) \equiv x^4 + x^3 + x^2;$$

$$x_3 \equiv [(x^4 + x^3 + x^2)^2 + x^4 + x^3 + x^2 + 1] \bmod (f(x), 2) \equiv x^2 + 1;$$

$$y_3 \equiv [x^2 + (x^4 + x^3 + x^2 + 1)(x^2 + 1)] \bmod (f(x), 2) \equiv x^4 + x^2 + x.$$

Отже, $2P = (x^2 + 1, x^4 + x^2 + x) = (101, 10110)$. Аналогічним чином знаходимо інші точки:

$3P = (1110, 1);$	$4P = (1011, 101);$	$5P = (10110, 1001);$
$6P = (11111, 10);$	$7P = (11110, 10);$	$8P = (1001, 10010);$
$9P = (10010, 110);$	$10P = (11101, 11);$	$11P = (10000, 10000);$
$12P = (1, 11101);$	$13P = (0, 10);$	$14P = (1, 11100);$
$15P = (10000, 0);$	$16P = (11101, 11110);$	$17P = (10010, 10101);$
$18P = (1001, 11011);$	$19P = (11110, 11100);$	$20P = (11111, 11101);$
$21P = (10110, 11111);$	$22P = (1011, 1110);$	$23P = (1110, 1111);$
$24P = (101, 10110);$	$25P = (10, 10111);$	$26P = O.$

Отже, порядок точки $P = (10, 10101)$ дорівнює $n = 26$, тобто $26P = 26(10, 10101) = O$.

Афінний базис вимагає велику обчислювальну складність (реально використовують криві зі значенням $m \geq 163$ та вище)

$$Q = dG \bmod (f(x), 2),$$

де $G = (x_G, y_G)$ – базова точка; d – секретний (особистий) ключ, $d \in (1, n - 1)$; n – порядок базової точки G , причому

$$nG \bmod (f(x), 2) = O.$$

У цьому випадку для зменшення складності чи підвищення швидкості використовується проєктивний базис.

Проективний базис. Перехід з афінного подання в проєктивне з координатами кривої X, Y, Z здійснюється таким чином:

$$x = \frac{X}{Z^2}; y = \frac{Y}{Z^3};$$

$$\frac{Y^2}{Z^6} + \frac{X}{Z^2} \cdot \frac{Y}{Z^3} \equiv \frac{X^3}{Z^6} + \frac{aX^2}{Z^4} + b(\bmod (f(x), 2)), Z \neq 0.$$

Після спрощення одержуємо вираз ЕС над полем $GF(2^m)$ у проєктивному базисі

$$Y^2 + XYZ \equiv X^3 + aX^2Z^2 + bZ^6 \pmod{(f(x), 2)}.$$

Коли ЕС задається в афінних координатах, а точка R – у проєктивних координатах, то справедливі твердження:

1) якщо $P = (x_P, y_P)$ є афінною точкою ЕС, то $R = (x_P, y_P, 1_{GF})$ є відповідною точкою в проєктивних координатах;

2) якщо $R = (X, Y, Z)$ $Z \neq 0_{GF}$, то $P = (X/Z, Y/Z)$ є відповідною афінною точкою ЕС;

3) існує тільки одне рішення $(O_{GF}, 1_{GF}, O_{GF})$ – ця точка відповідає O .

У проєктивних координатах груповий закон на еліптичній кривій формулюється таким чином:

1) точка $(O_{GF}, 1_{GF}, O_{GF})$ є одиничним елементом O щодо операції $+$;

2) якщо $R = (X, Y, Z) \neq (O_{GF}, 1_{GF}, O_{GF})$ є точкою на ЕС, заданою в проєктивних координатах, то $R = (X, X + Y, Z)$.

Нехай $R_1 = (X_1, Y_1, Z_1)$ та $R_2 = (X_2, Y_2, Z_2)$ є дві точки на ЕС – такі, що $R_1 \neq R_2$ і $R_1, R_2 \neq (O_{GF}, 1_{GF}, O_{GF})$, тоді суму цих точок як точку $R_3 = (X_3, Y_3, Z_3)$ можна обчислити за допомогою таких формул:

$$X_3 = su; \quad Y_3 = t(u + s^2 X_1 Z_2) + s^3 Y_1 Z_2 + su; \quad Z_3 = s^3 Z_1 Z_2,$$

$$\text{де } s = X_2 Z_1 + X_1 Z_2; \quad t = Y_2 Z_1 + Y_1 Z_2; \quad u = (t^2 + ts + as^2) Z_1 Z_2 + s^3.$$

Нехай $R = (X, Y, Z) \neq (O_{GF}, 1_{GF}, O_{GF})$ є точка на ЕС, тоді її подвоєння $2R = (X_3, Y_3, Z_3)$ можуть бути обчислені за допомогою таких формул:

$$X_3 = st; \quad Y_3 = t(s + YZ + X^2) + sX^4; \quad Z_3 = s^3,$$

$$\text{де } s = XZ; \quad t = bZ^4 + X^4.$$

Основною особливістю використання проєктивних координат є те, що в цьому базисі не виконується операція ділення за модулем, яка зводиться до знаходження зворотного елемента.

Є готові рекомендації по вибору еліптичних кривих, що забезпечують високий рівень безпеки та ефективність програмної реалізації. Так, американський інститут стандартів і технологій NIST рекомендує до використання 15 еліптичних кривих.

Федеральний стандарт обробки інформації FIPS 186 (Federal Information Processing Standards) рекомендує до використання 10 кінцевих полів, зокрема (див. табл. 4.5) [17, 24]:

– поля $GF(p)$, де просте число p має довжину 192, 224, 256, 384, 521 бітів;

– поля $GF(2^m)$, де $m = 163, 233, 283, 409$ або 571.

Причому для кожного кінцевого поля рекомендується конкретна еліптична крива (по дві для полів $GF(2^m)$) і генеруюча точка. Значення параметра $a = -3$ для рекомендованих еліптичних кривих над полем $GF(p)$.

Таблиця 4.5 – Параметри кривих над полем $GF(p)$ рекомендованих FIPS

$P-192: p = 2^{192} - 2^{64} - 1; a = -3;$ $b = 0x\ 64210519\ E59C80E7\ 0FA7E9AB\ 72243049\ FEB8DEEC\ C146B9B1;$ $n = 0x\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ 99DEF836\ 146BC9B1\ B4D22831.$
$P-224: p = 2^{224} - 2^{96} + 1; a = -3;$ $b = 0x\ B4050A86\ 0C04B3AB\ F5413256\ 5044D0D7\ D7BFD8BA\ 270B3943\ 2355FFB4;$ $n = 0x\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFF16A2\ E0B8F03E\ 13DD2945\ 5C5C2A3D.$
$P-256: p = 2^{256} - 2^{244} + 2^{192} + 2^{96} - 1; a = -3;$ $b = 0x\ 5AC635D8\ AA3A93E7\ B3EBBD55\ 769886BC\ 651D06B0\ CC53B0F6\ 3BCE3C3E\ 27D2604B;$ $n = 0x\ FFFFFFFF\ 00000000\ FFFFFFFF\ FFFFFFFF\ BCE6FAAD\ A7179E84\ F3B9CAC2\ FC632551.$
$P-384: p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1; a = -3;$ $b = 0x\ B3312FA7\ E23EE7E4\ 988E056B\ E3F82D19\ 181D9C6E\ FE814112\ 0314088F\ 5013875A\ C656398D\ 8A2ED19D\ 2A85C8ED\ D3EC2AEF;$ $n = 0x\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF\ C7634D81\ F4372DDF\ 581A0DB2\ 4880A77A\ ECEC196A\ CCC52973.$
$P-521: p = 2^{521} - 1; a = -3;$ $b = 0x\ 051\ 953EB961\ 8E1C9A1F\ 929A21A0\ B68540EE\ A2DA725B\ 99B315F3\ B8B48991\ 8EF109E1\ 56193951\ EC7E937B\ 1652C0BD\ 3BB1BF07\ 3573DF88\ 3D2C34F1\ EF451FD4\ 6B503F00;$ $n = 68647976601306097149819007990813932172694353001433054093944634591855431\ 83397655394245057746333217197532963996371363321113864768612440380340372808\ 892707005449.$

Український стандарт цифрового підпису ДСТУ 4145–2002 ґрунтується на властивостях груп точок на еліптичних кривих над полями $GF(2^m)$. Якщо використовують оптимальний нормальний базис, то основне поле треба обирати з-посеред полів $GF(2^m)$, степені яких надано в табл. 4.6 [25].

Таблиця 4.6 – Припустимі основні поля з оптимальним нормальним базисом

Степінь поля m	173	179	191	233	239	251	281
Степінь поля m	293	359	419	431	443	491	509

Для реалізації стандарту ДСТУ 4145–2002 рекомендується використовувати еліптичні криві, які надані в табл. 4.7 [25].

Алгоритм формування підпису під повідомленням M :

- 1) повідомлення M гешується за допомогою геш-функції $h(M)$;
- 2) обираємо випадкове число $k \in (1, n - 1)$;
- 3) обчислюємо $kP = (x_1, y_1)$ та $r \equiv x_1 \pmod{n}$. Якщо $r \neq 0$, переходимо до кроку 4, в противному разі – повертаємося до кроку 2;
- 4) обчислюємо $s \equiv [k^{-1}(h(M) + dr)] \pmod{n}$. Якщо $s \neq 0$, переходимо до кроку 5, в противному разі – повертаємося до кроку 2;
- 5) підписом під повідомленням M є пара цілих чисел (r, s) .

Алгоритм перевірки підпису:

- 1) якщо r і s – цілі числа, належать до інтервалу $(1, n - 1)$, переходимо до кроку 2, в противному разі – підпис анулюється;
- 2) обчислюємо геш-функцію $h(M)$;
- 3) обчислюємо $u_1 \equiv h(M)s^{-1} \pmod{n}$ та $u_2 \equiv (rs^{-1}) \pmod{n}$;
- 4) обчислюємо $u_1P + u_2Q = (x_0, y_0)$ та $v \equiv x_0 \pmod{n}$;
- 5) підпис є справжній за $v = r$.

Доказ коректності підпису ECDSA

$$\begin{aligned} u_1P + u_2Q &= u_1P + u_2dP = (h(M) + dr)s^{-1}P = \\ &= (h(M) + dr)(h(M) + dr)^{-1}kP = kP. \end{aligned}$$

Схему алгоритму цифрового підпису ECDSA показано на рис. 4.26.

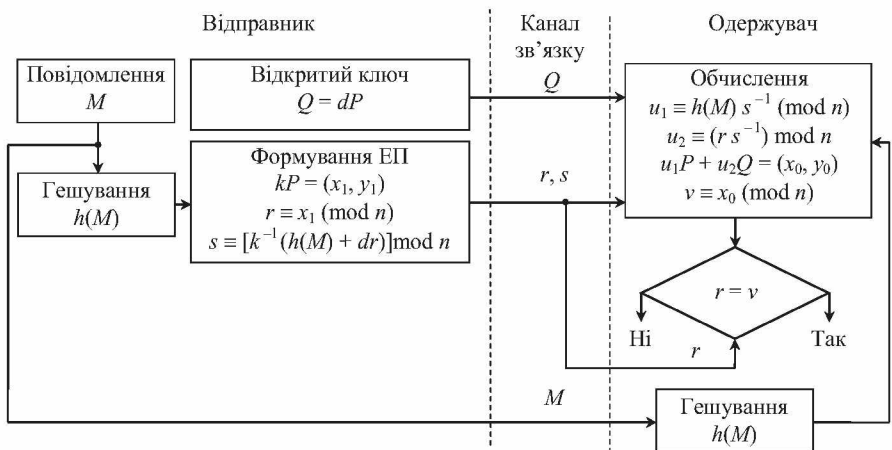


Рисунок 4.26 – Алгоритм цифрового підпису ECDSA

Приклад електронного підпису ECDSA. Нехай $E_{149}(-3, 6)$, що відповідає кривій $y^2 = x^3 - 3 + 6$; $p = 149$; $n = 167$; $P = (50, 21)$; $h(M) = 100$; $d = 13$; $k = 23$.

Розрахунок відкритого ключа

$$Q = 13(50, 21) = (49, 29).$$

Розглянемо детальніше розрахунок одержаного результату.

$$13_{10} = 1101_2 \Rightarrow 13P = 8P + 4P + P.$$

1) Розраховуємо $2P = 2(50, 21) = (50, 21) + (50, 21)$:

$$\lambda = \left(\frac{3 \cdot 50^2 - 3}{2 \cdot 21} \right) \bmod 149 = \frac{59}{2} (\bmod 149) = 104;$$

$$x_3 = (104^2 - 50 - 50) \bmod 149 = 137;$$

$$y_3 = [104(50 - 137) - 21] \bmod 149 = -129 \bmod 149 = 20.$$

Таким чином, $2P = (50, 21) + (50, 21) = (137, 20)$.

2) Розраховуємо $4P = 4(50, 21) = 2(137, 20) = (137, 20) + (137, 20)$:

$$\lambda = \left(\frac{3 \cdot 137^2 - 3}{2 \cdot 20} \right) \bmod 149 = \frac{35}{5} (\bmod 149) = 7;$$

$$x_3 = (7^2 - 2 \cdot 137) \bmod 149 = -76 \bmod 149 = 73;$$

$$y_3 = [7(137 - 73) - 20] \bmod 149 = 130.$$

Таким чином, $4P = (137, 20) + (137, 20) = (73, 130)$.

3) Розраховуємо $8P = 8(50, 21) = 2(73, 130) = (73, 130) + (73, 130)$:

$$\lambda = \left(\frac{3 \cdot 73^2 - 3}{2 \cdot 130} \right) \bmod 149 = \frac{122}{65} (\bmod 149) = 144;$$

$$x_3 = (144^2 - 2 \cdot 73) \bmod 149 = 28;$$

$$y_3 = [144(73 - 28) - 130] \bmod 149 = 92.$$

Таким чином, $8P = (73, 130) + (73, 130) = (28, 92)$.

4) Розраховуємо $12P = 8P + 4P = (28, 92) + (73, 130)$:

$$\lambda \equiv \left(\frac{130 - 92}{73 - 28} \right) \bmod 149 \equiv \frac{38}{45} \pmod{149} \equiv 77;$$

$$x_3 \equiv (77^2 - 28 - 73) \bmod 149 \equiv 17;$$

$$y_3 \equiv [77(28 - 17) - 92] \bmod 149 \equiv 10.$$

Таким чином, $12P = (28, 92) + (73, 130) = (17, 10)$.

5) Розраховуємо $13P = 12P + P = (17, 10) + (50, 21)$:

$$\lambda \equiv \left(\frac{21 - 10}{50 - 17} \right) \bmod 149 \equiv \frac{1}{3} \pmod{149} \equiv 50;$$

$$x_3 \equiv (50^2 - 17 - 50) \bmod 149 \equiv 49;$$

$$y_3 \equiv [50(17 - 49) - 10] \bmod 149 \equiv -120 \bmod 149 \equiv 29.$$

Таким чином, $13P = (17, 10) + (50, 21) = (49, 29)$.

Особистий ключ є $d = 13$, відкритий ключ $Q = (49, 29)$.

Формування підпису під повідомленням M :

$$23(50, 21) = (55, 140) \text{ та } r \equiv 55 \pmod{167} \equiv 55;$$

$$s \equiv [23^{-1}(100 + 13 \cdot 55)] \bmod 167 \equiv 79.$$

Підписом під повідомленням M є пара цілих чисел $(55, 79)$.

Перевірка підпису. Числа $(55, 79)$ – цілі числа, що належать до інтервалу $(1, 166)$.

Обчислюємо u_1 та u_2 :

$$u_1 \equiv (100 \cdot 79^{-1}) \bmod 167 \equiv 52;$$

$$u_2 \equiv (55 \cdot 79^{-1}) \bmod 167 \equiv 62.$$

Знаходимо параметр v :

$$52(50, 21) + 62(49, 29) = (42, 141) + (59, 83) = (55, 140);$$

$$v \equiv 55 \pmod{167} \equiv 55 = r - \text{підпис є справжній}.$$

Реалізація атаки повторного використання числа k ЕП ECDSA.

Однією з відомих атак на ЕП ECDSA є атака при повторному використанні випадкового числа k . У цьому випадку відправник для двох різних повідомлень M_1 і M_2 (з відповідними геш-кодами $h(M_1)$ і $h(M_2)$) при формуванні підпису повторно використовує одне значення числа k . Повторне використання k дозволяє зловмисникові визначити особистий ключ відправника та реалізувати загрозу “повне розкриття”. Тому зміна випадкового числа k зі знищенням попереднього є необхідною умовою безпеки для кожного користувача ЕП ECDSA.

Нехай $h(M_1)$ і $h(M_2)$ геш-функції повідомлень M_1 і M_2 , підписом під повідомленням M_1 є пара цілих чисел (r, s_1) , підписом під повідомленням M_2 – (r, s_2) . Зловмисник розраховує k , а потім особистий ключ d :

$$k \equiv \left(\frac{h(M_1) - h(M_2)}{s_1 - s_2} \right) \bmod n;$$
$$d \equiv \left[r^{-1} \left(\frac{h(M_1)s_2 - h(M_2)s_1}{s_1 - s_2} \right) \right] \bmod n.$$

Приклад атаки. Нехай $E_{149}(-3, 6)$; $p = 149$; $n = 167$; $h(M_1) = 100$; $h(M_2) = 200$; підпис повідомлення M_1 є $(55, 79)$; підпис повідомлення M_2 є $(55, 18)$. Зловмисник розраховує особистий ключ d :

$$d \equiv \left[55^{-1} \left(\frac{100 \cdot 18 - 200 \cdot 79}{79 - 18} \right) \right] \bmod 167 \equiv \frac{125}{61} (\bmod 167) \equiv 13.$$

4.13 Алгоритм електронного підпису ECSS

ECSS (Elliptic Curve Signature Scheme) – система з відкритим ключем для створення ЕП у групі точок еліптичної кривої.

Алгоритм генерування ключів:

- 1) обираємо еліптичну криву $E_p(a, b)$;
- 2) обираємо точку $P \in E_p(a, b)$ порядку n ;
- 3) обираємо довільне число $d \in (1, n - 1)$;
- 4) обчислюємо $Q = dP$;

5) особистим ключем оголошуємо d , відкриті значення – $E_p(a, b)$, P , n , Q .

Алгоритм формування підпису під повідомленням M :

1) повідомлення M гешується за допомогою геш-функції $h(M)$;

2) обираємо випадкове число $k \in (1, n - 1)$;

3) обчислюємо $R = kP = (x_1, y_1)$;

4) обчислюємо $r \equiv [(h(M) + x_1)] \bmod n$. Якщо $r \neq 0$, переходимо до кроку 5, в противному разі – повертаємося до кроку 2;

5) обчислюємо $s \equiv (k - dr) \bmod n$. Якщо $s \neq 0$, переходимо до кроку 6, в противному разі – повертаємося до кроку 2;

6) підписом під повідомленням M є пара цілих чисел (r, s) .

Алгоритм перевірки підпису:

1) якщо r і s – цілі числа, належать до інтервалу $(1, n - 1)$, переходимо до кроку 2, в противному разі – підпис анулюється;

2) обчислюємо геш-функцію $h(M)$;

3) обчислюємо $R' = sP + rQ = (x_1, y_1)$;

4) обчислюємо $r' \equiv [(h(M) + x_1)] \bmod n$;

5) підпис є справжній за $r' = r$.

Схему алгоритму ЕП ECSS показано на рис. 4.27.

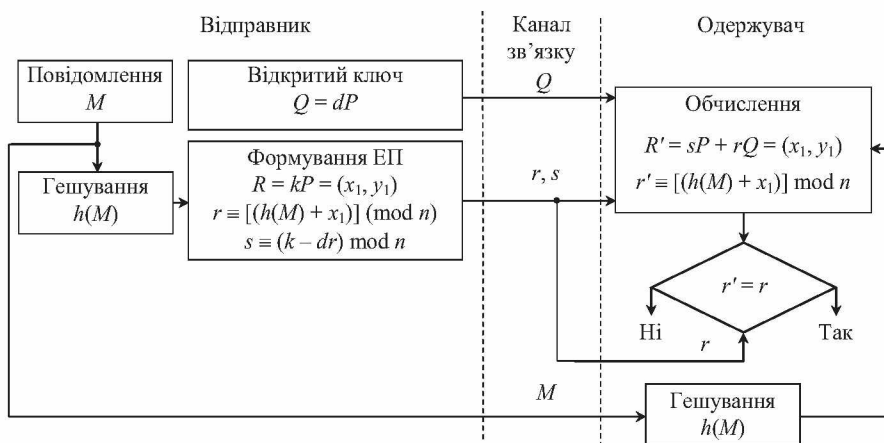


Рисунок 4.27 – Схема електронного підпису ECSS

Доказ коректності підпису ECSS

$$\begin{aligned} R' &= sP + rQ = sP + rdP = (k - dr)P + rdP = \\ &= kP - drP + rdP = kP = R. \end{aligned}$$

Робимо висновок, що як при формуванні, так і при верифікації підпису в ECSS не потрібно обчислювати зворотний елемент поля. Це, звичайно, підвищує продуктивність обчислень і зменшує час цих процедур.

Приклад електронного підпису ECSS. Нехай $E_{3061}(-3, 35)$, що відповідає кривій $y^2 = x^3 - 3x + 35$; $p = 3061$; $n = 3037$; $P = (225, 2)$; $d = 137$; $h(M) = 2000$; $k = 211$.

Розрахунок відкритого ключа

$$Q = 137(225, 2) = (2218, 146).$$

Формування підпису під повідомленням M:

$$\begin{aligned} R &= 211(225, 2) = (1285, 488); \\ r &\equiv (2000 + 1285) \bmod 3037 \equiv 248; \\ s &\equiv (211 - 137 \cdot 248) \bmod 3037 \equiv 2679. \end{aligned}$$

Підписом під повідомленням M є пара цілих чисел $(248, 2679)$.

Перевірка підпису. Числа $r = 248$ і $s = 2679$ – цілі числа, що належать до інтервалу $(1, 3036)$.

Обчислюємо R' і r' :

$$\begin{aligned} R' &= 2679(225, 2) + 248(2218, 146) = \\ &= (1156, 1503) + (533, 488) = (1285, 488); \\ r' &\equiv (2000 + 1285) \bmod 3037 \equiv 248. \end{aligned}$$

Підпис є справжній, оскільки $r' = r = 248$.

4.14 Алгоритм електронного підпису EC-GDSA

EC-GDSA (Elliptic Curve ElGamal Digital Signature Algorithm) – система з відкритим ключем для створення ЕП у групі точок еліптичної кривої на основі схеми Ель-Гамаля.

Алгоритм генерування ключів:

- 1) обираємо еліптичну криву $E_p(a, b)$;
- 2) обираємо точку $G \in E_p(a, b)$ порядку n ;
- 3) обираємо довільне число $d \in (1, n - 1)$;
- 4) обчислюємо $Q = d^{-1}G$;
- 5) особистий ключ – d^{-1} , відкриті значення – $E_p(a, b)$, G , n , Q .

Алгоритм формування підпису під повідомленням M :

- 1) повідомлення M гешується за допомогою геш-функції $h(M)$;
- 2) обираємо випадкове число $k \in (1, n - 1)$;
- 3) обчислюємо $R = kG = (x_R, y_R)$ та $r \equiv x_R \pmod{n}$. Якщо $r \neq 0$, переходимо до кроку 4, в противному разі – повертаємося до кроку 2;
- 4) обчислюємо $s \equiv [(kr - h(M))d] \pmod{n}$. Якщо $s \neq 0$, переходимо до кроку 5, в противному разі – повертаємося до кроку 2;
- 5) підписом під повідомленням M є пара цілих чисел (r, s) .

Алгоритм перевірки підпису:

- 1) якщо r і s – цілі числа, належать до інтервалу $(1, n - 1)$, переходимо до кроку 2, в противному разі – підпис анулюється;
- 2) обчислюємо геш-функцію $h(M)$;
- 3) обчислюємо $u_1 \equiv h(M)r^{-1} \pmod{n}$ та $u_2 \equiv (r^{-1}s) \pmod{n}$;
- 4) обчислюємо $R' = u_1G + u_2Q = (x_R', y_R')$ та $r' \equiv x_R' \pmod{n}$;
- 5) підпис є справжній за $r' = r$.

Схему алгоритму ЕП EC-GDSA показано на рис. 4.28.

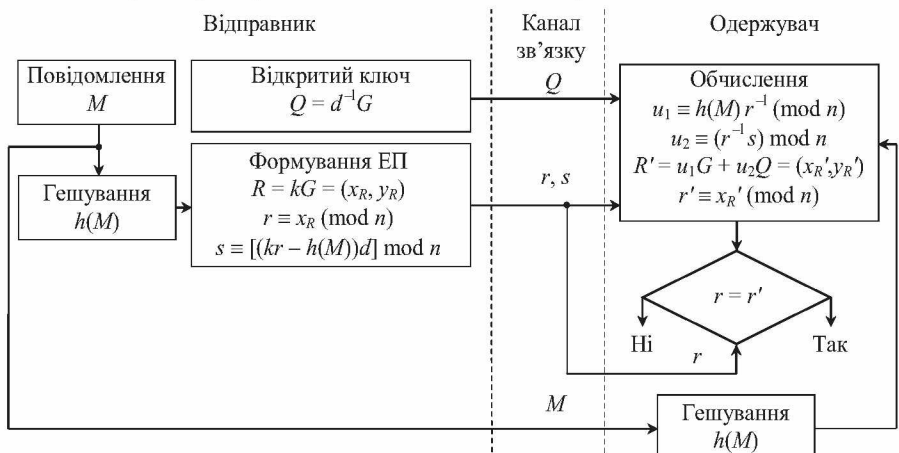


Рисунок 4.28 – Схема електронного підпису EC-GDSA

Доказ коректності підпису EC-GDSA

$$\begin{aligned} R' &= u_1 G + u_2 Q = [h(M) r^{-1}] G + [r^{-1} s d^{-1}] G = \\ &= [h(M) r^{-1}] G + [r^{-1} (kr - (h(M)d) d^{-1})] G = \\ &= [h(M) r^{-1}] G + kG - [h(M) r^{-1}] G = kG = R. \end{aligned}$$

Приклад електронного підпису EC-GDSA. Нехай $E_{1009}(-3, 63)$, що відповідає кривій $y^2 = x^3 - 3 + 63$; $p = 1009$; $n = 967$; $G = (211, 75)$; $h(M) = 500$; $k = 311$; $d = 137$.

Розрахунок відкритого ключа

$$Q = 137^{-1}(211, 75) = (143, 366).$$

Формування підпису під повідомленням M :

$$\begin{aligned} R &= 311(211, 75) = (807, 900); \\ r &\equiv 807 \bmod 967 \equiv 807; \\ s &\equiv [(311 \cdot 807 - 500)137] \bmod 967 \equiv 387. \end{aligned}$$

Підписом під повідомленням M є пара цілих чисел $(807, 387)$.

Перевірка підпису. Числа $r = 807$ і $s = 387$ – цілі числа, що належать до інтервалу $(1, 966)$.

Обчислюємо u_1 і u_2 :

$$\begin{aligned} u_1 &\equiv (500 \cdot 807^{-1}) \bmod 967 \equiv 843; \\ u_2 &\equiv (807^{-1} \cdot 387) \bmod 967 \equiv 608. \end{aligned}$$

Обчислюємо R' і r' :

$$\begin{aligned} R' &= 843(211, 75) + 608(143, 366) = (949, 13) + (695, 540) = (807, 900); \\ r' &\equiv 807 \bmod 967 \equiv 807. \end{aligned}$$

Підпис є справжній, оскільки $r' = r = 807$.

Приклад електронного підпису EC-GDSA над розширеним полем.

Нехай задано: несуперсингулярна еліптична крива над розширеним полем $GF(2^7)$ (додаток Б)

$$y^2 + xy \equiv (x^3 + x^2 + 100) \bmod (f(x) = x^7 + x^6 + 1, 2);$$

$n = 67$; $G = (111000, 111)$; $k = 29$; $d = 50$; $h(M) = 37$ (100101₂ – молодші розряди геш-функції | $n - 1 = 6$).

Розрахунок відкритого ключа

$$Q = 50^{-1}(111000, 111) = (1000, 1011101).$$

Формування підпису під повідомленням M:

$$\begin{aligned} R &= 29(111000, 111) = (1011101, 11); \\ x_R &= x^6 + x^4 + x^3 + x^2 + 1 \rightarrow 11011101_2 = 93_{10}; \\ r &\equiv 93 \bmod 67 \equiv 26; \\ s &\equiv [(29 \cdot 26 - 37)50] \bmod 67 \equiv 5. \end{aligned}$$

Підписом під повідомленням M є пара цілих чисел $(26, 5)$.

Перевірка підпису. Числа $r = 26$ і $s = 5$ – цілі числа, що належать до інтервалу $(1, 66)$. Обчислюємо геш-функцію $h(M) = 37$.

Обчислюємо u_1 і u_2 :

$$\begin{aligned} u_1 &\equiv (37 \cdot 26^{-1}) \bmod 67 \equiv 4; \\ u_2 &\equiv (26^{-1} \cdot 5) \bmod 67 \equiv 44. \end{aligned}$$

Обчислюємо R' і r' :

$$\begin{aligned} R' &= 4(111000, 111) + 44(1000, 1011101) = \\ &= (1000, 1010101) + (100000, 1011100) = (1011101, 11); \\ x_{R'} &= x^6 + x^4 + x^3 + x^2 + 1 \rightarrow 11011101_2 = 93_{10}; \\ r' &\equiv 93 \bmod 67 \equiv 26. \end{aligned}$$

Підпис є справжній, оскільки $r' = r = 26$.

4.15 Алгоритм електронного підпису EC-KCDSA

Алгоритм EC-KCDSA (Elliptic Curve Korean Certificate-based Digital Signature Algorithm) розроблений командою KISA (Korea Internet & Security Agency) та вважається одним із найбільш надійних криптографічних алгоритмів ЕП, він також реалізований у національному стандарті ДСТУ ISO/IEC 14888-3:2019. В алгоритмі EC-KCDSA реалізується механізм вироблення ЕП з додатком (доповненням).

Алгоритм генерування ключів:

- 1) обираємо еліптичну криву $E_p(a, b)$;
- 2) обираємо точку $G \in E_p(a, b)$ порядку n ;
- 3) обираємо довільне число $d \in (1, n - 1)$;
- 4) обчислюємо $Q = d^{-1}G$;
- 5) особистий ключ – d^{-1} , відкриті значення – $E_p(a, b)$, G , n , Q та Z (Cert Data) дані сертифіката користувача (підписувача), що містить ідентифікатор користувача, відкритий ключ Q й інші дані.

Алгоритм формування підпису під повідомленням M :

- 1) обираємо випадкове число $k \in (1, n - 1)$;
- 2) обчислюємо $R = kG = (x_R, y_R)$ та $r = h(R) = h(x_R \| y_R)$;
- 3) обчислюємо $s \equiv [(k - r \oplus h(Z \| M))d] \bmod n$. Якщо $s \neq 0$, переходимо до кроку 4, в противному разі – повертаємося до кроку 1;
- 4) підписом під повідомленням M є пара цілих чисел (r, s) .

Алгоритм перевірки підпису:

- 1) спочатку перевіряємо дійсність сертифіката підписувача Z (Cert Data);
- 2) перевіряємо розмірність r і s , $0 < s < n$, $0 < r < 2^n$, якщо так, переходимо до кроку 3, в противному разі – підпис анулюється;
- 3) обчислюємо $e = r \oplus h(Z \| M)$;
- 4) обчислюємо $R' = eG + sQ$ та $r' = h(R') = h(x_{R'} \| y_{R'})$;
- 5) підпис є справжній за $r' = r$.

Доказ коректності підпису EC-KCDSA

$$\begin{aligned} R' &= eG + sQ = [r \oplus h(Z \| M)]G + [(k - r \oplus h(Z \| M))d]Q = \\ &= [r \oplus h(Z \| M)]G + [(k - r \oplus h(Z \| M))d]d^{-1}G = \\ &= [r \oplus h(Z \| M)]G + kG - [r \oplus h(Z \| M)]G = kG = R. \end{aligned}$$

Схему алгоритму ЕП EC-KCDSA показано на рис. 4.29.

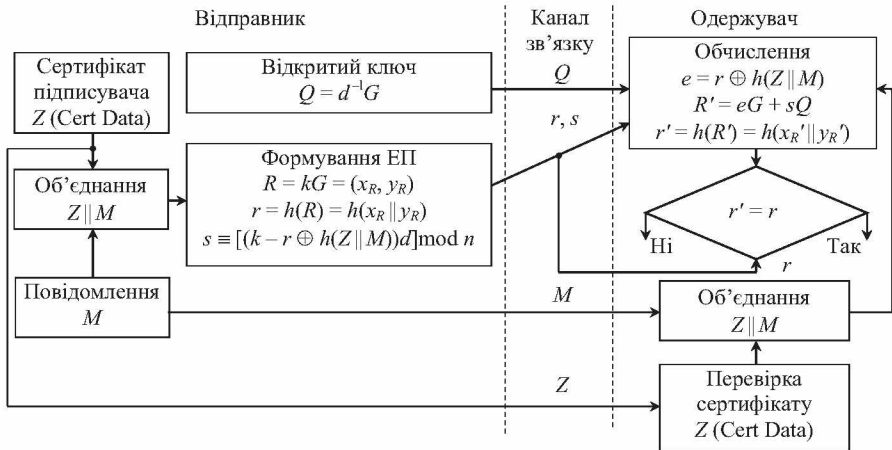


Рисунок 4.29 – Схема електронного підпису EC-KCDSA

Приклад електронного підпису EC-KCDSA. Нехай $E_{31991}(-3, 130)$, що відповідає кривій $y^2 = x^3 - 3x + 130$; $p = 31991$; $n = 31859$; $G = (8484, 3)$; $h(Z || M) = 15432$; $k = 1559$; $d = 2017$.

Розрахунок відкритого ключа

$$Q = 2017^{-1}(8484, 3) = (10515, 21390).$$

Формування підпису під повідомленням M :

$$R = 1559(8484, 3) = (31331, 16854).$$

Конкатенація значень $x_R = 31331$ і $y_R = 16854$ дає результат $x_R || y_R = 3133116854$. Припустимо, що гешування цього значення дає дайджест $h(3133116854) = 16380$, тоді:

$$\begin{aligned} r &= h(3133116854) = 16380; \\ s &= [(1559 - 16380 \oplus 15432)2017] \bmod 31859 \equiv 21745. \end{aligned}$$

Підписом під повідомленням M є пара цілих чисел $(16380, 21745)$.

Перевірка підпису. Обчислюємо R' і r' :

$$\begin{aligned}e &= 16380 \oplus 15432 = 948; \\R' &= 21745(10515, 21390) + 948(8484, 3) = \\&= (18977, 18600) + (5430, 11177) = (31331, 16854); \\r' &\equiv h(3133116854) = 16380.\end{aligned}$$

Підпис є справжній, оскільки $r' = r = 16380$.

Приклад електронного підпису EC-KCDSA над розширеним полем.

Нехай задано: суперсингулярна еліптична крива над розширеним полем $GF(2^{11})$ (додаток Б)

$$y^2 + y \equiv (x^3 + 11x + 100) \bmod (f(x) = x^{11} + x^2 + x + 1, 2);$$

$n = 2113$; $G = (1001000, 10)$; $k = 978$; $d = 1207$; $h(Z \| M) = 2000$ (11111010000₂ – молодші розряди геш-функції | $n - 1 = 11$).

Розрахунок відкритого ключа

$$Q = 1207^{-1}(1001000, 10) = (11011100101, 11010000000).$$

Формування підпису під повідомленням M :

$$R = 978(1001000, 10) = (10111100, 11100110010).$$

Конкатенація значень $x_R = 10111100$ і $y_R = 11100110010$ дає результат $x_R \| y_R = 1011110011100110010$. Гешування цього значення дає дайджест $h(1011110011100110010) = 1985$ (обираємо одинадцять молодших розрядів геш-функції), тоді:

$$\begin{aligned}r &= h(1011110011100110010) = 1985; \\s &\equiv [(978 - 1985 \oplus 2000)1207] \bmod 2113 \equiv 2003.\end{aligned}$$

Підписом під повідомленням M є пара цілих чисел (1985, 2003).

Перевірка підпису. Обчислюємо R' і r' :

$$e = 1985 \oplus 2000 = 17;$$

$$\begin{aligned} R' &= 17(1001000, 10) + 2003(11011100101, 11010000000) = \\ &= (1110100, 1010001100) + (110101111, 10011100) = (10111100, 11100110010); \\ r' &\equiv h(1011110011100110010) = 1985. \end{aligned}$$

Підпис є справжній, оскільки $r' = r = 1985$.

Доведено, що алгоритм ЕП ЕС-KCDSA захищений від таких типів атак, як: “повне розкриття”, на основі підписаних даних, “екзистенційна піддробка”, “селективна піддробка”. Така захищеність забезпечується, в тому числі, за рахунок обов’язкового використання колізійно-стійких функцій гешування.

4.16 Стандарт електронного підпису ДСТУ 4145–2002

ДСТУ 4145–2002 [25] встановлює механізм створення цифрового підпису, який ґрунтується на властивостях груп точок еліптичних кривих над полями $GF(2^m)$. Загальні параметри підпису можуть бути однаковими для довільної кількості користувачів цифрового підпису.

В ДСТУ 4145–2002 використовуються наступні перетворювання даних:

1) *Перетворювання елемента основного поля на ціле число.*

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

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

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

Алгоритм перетворювання елемента основного поля на ціле число:

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

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

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

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

2) Перетворювання геш-коду на елемент основного поля.

Установлюємо алгоритм перетворювання результату обчислення функції гешування $(h_{L_H-1}, \dots, h_0)$ на елемент основного поля $x \in GF(2^m)$, $x = (x_{m-1}, \dots, x_0)$.

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

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

Алгоритм перетворювання результату обчислення функції гешування на елемент основного поля:

- обчислюємо ціле число $k = \min(m, L_H)$;
- приймаємо $x_i = h_i$ для $i = 0, \dots, k-1$;
- якщо $k < m$, то приймаємо $x_i = 0$ для $i = 0, \dots, m-1$;
- двійковий рядок $(x_{m-1}, \dots, x_0)$ зображує елемент x основного поля, який є результатом виконання алгоритму.

3) Перетворювання пари цілих чисел на цифровий підпис.

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

Вхідні дані алгоритму: пара цілих чисел (r, s) у двійковому зображенні: $r = (r_{L(r)-1}, \dots, r_0)$; $s = (s_{L(s)-1}, \dots, s_0)$; $0 < r < n$; $0 < s < n$, довжина цифрового підпису L_D : $L_D \geq 2L(n)$, L_D є кратне до 16.

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

Алгоритм перетворювання пари цілих чисел на цифровий підпис:

- приймаємо $l = L_D/2$;
- утворюємо двійковий рядок R за правилом:
 - приймаємо $R_i = r_i$ для $i = 0, \dots, L(r) - 1$,
 - приймаємо $R_i = 0$ для $i = L(r), \dots, l - 1$;
- утворюємо двійковий рядок S за правилом:
 - приймаємо $S_i = s_i$ для $i = 0, \dots, L(s) - 1$,
 - приймаємо $S_i = 0$ для $i = L(s), \dots, l - 1$;
- рядок D є конкатенація двох рядків $S \parallel R$;
- двійковий рядок $D = (D_{L_D-1}, \dots, D_0)$ довжини L_D є результат виконання

алгоритму.

4) Перетворювання двійкового рядка на пару цілих чисел.

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

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

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

Алгоритм перетворювання двійкового рядка на пару цілих чисел:

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

крок 2, приймаємо $r_i = D_i$ для $i = 0, \dots, l-1$;

крок 3, визначаємо j як найбільше i , $i = 0, \dots, l-1$, для якого $r_i = 1$;

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

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

крок 6, приймаємо $s_i = D_{i+l}$ для $i = 0, \dots, l-1$;

крок 7, визначаємо індекс j як найбільше i , $i = 0, \dots, l-1$, для якого $s_i = 1$;

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

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

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

Приклади обчислень цифрового підпису в поліноміальному базисі.

Вибір загальних параметрів. За основне поле використовуємо кінцеве поле $GF(2^{163})$. Елементи цього поля зображують у поліноміальному базисі, що відповідає примітивному многочленові $X^{163} + X^7 + X^6 + X^3 + 1$ (додаток В).

Використовується еліптична крива над полем $GF(2^{163})$ (табл. 4.7):

$$y^2 + xy = x^3 + x^2 + 5FF6108462A2DC8210AB403925E638A19C1455D21.$$

Порядок цієї еліптичної кривої ділиться на просте число

$$n = 40000000000000000000000002BEC12BE2262D39BCF14D,$$

яке є порядком базової точки (табл. 4.7).

Обчислення базової точки еліптичної кривої здійснюють у такий спосіб. Обчислюємо випадкову точку еліптичної кривої

$$P = (x_P, y_P) = (72D867F93A93AC27DF9FF01AFFE74885C8C540420, \\ 0224A9C3947852B97C5599D5F4AB81122ADC3FD9B).$$

Оскільки $nP = O$, то точка P – базова точка еліптичної кривої.

За особистий ключ цифрового підпису візьмемо ціле число

$$d = 183F60FDF7951FF47D67193F8D073790C1C9B5A3E.$$

Обчислюємо відкритий ключ цифрового підпису, що відповідає обраному особистому ключу:

$$Q = -dP = (x_Q, y_Q) = (057DE7FDE023FF929CB6AC785CE4B79CF64ABDC2DA, \\ 3E85444324BCF06AD85ABF6AD7B5F34770532B9AA).$$

Нехай використовується довжина цифрового підпису $L_D = 512$.

Припустимо, що функцію гешування обрано згідно з ГОСТ 34.311–95 ($iH = 1$) і її використовують без додаткових вказівок. У цьому разі $L_H = 256$. Без додаткових вказівок приймемо також, що iH не передається.

Обчислення цифрового підпису. Обчислюємо геш-функцію за повідомленням T . Нехай результат гешування буде

$$H(T) = 09C9C44277910C9AAEE486883A2EB95B7180166DD \\ F73532EEB76EDA EF52247FF.$$

Перетворення цього рядка на елемент основного поля полягає у відокремленні з цього рядка $\min(m, L_H) = 163$ молодших розрядів. Унаслідок перетворення знайдемо елемент основного поля

$$h = 03A2EB95B7180166DDF73532EEB76EDA EF52247FF.$$

Нехай ціле число

$$e = 1025\text{E}40\text{BD}97\text{DB}012\text{B}7\text{A}1\text{D}79\text{DE}8\text{E}12932\text{D}247\text{F}61\text{C}6.$$

Обчислюємо точку eP :

$$eP = (x_{eP}, y_{eP}) = (42\text{A}7\text{D}756\text{D}70\text{E}1\text{C}9\text{B}\text{A}62\text{D}2\text{C}\text{B}43707\text{C}35204\text{E}\text{F}3\text{C}67\text{C}, \\ 5310\text{A}\text{E}5\text{E}560464\text{A}95\text{D}\text{C}80286\text{F}17\text{E}\text{B}762\text{E}\text{C}544\text{B}15\text{B}).$$

Тоді F_e дорівнює координаті x_{eP} цієї точки

$$F_e = 42\text{A}7\text{D}756\text{D}70\text{E}1\text{C}9\text{B}\text{A}62\text{D}2\text{C}\text{B}43707\text{C}35204\text{E}\text{F}3\text{C}67\text{C}.$$

Обчислюємо добуток елементів основного поля

$$y = hF_e = 274\text{E}\text{A}2\text{C}0\text{C}\text{A}\text{A}014\text{A}0\text{D}80\text{A}424\text{F}59\text{A}\text{D}\text{E}7\text{A}93068\text{D}08\text{A}7.$$

Перетворюємо елемент основного поля y на ціле число r

$$r = 274\text{E}\text{A}2\text{C}0\text{C}\text{A}\text{A}014\text{A}0\text{D}80\text{A}424\text{F}59\text{A}\text{D}\text{E}7\text{A}93068\text{D}08\text{A}7.$$

Обчислюємо ціле число

$$s \equiv (e + dr) \bmod n \equiv 2100\text{D}86957331832\text{B}8\text{E}8\text{C}230\text{F}5\text{B}\text{D}6\text{A}332\text{B}3615\text{A}\text{C}\text{A}.$$

Перетворюємо пару цілих чисел (r, s) на цифровий підпис D :

$$D = 000000000000000000000000274\text{E}\text{A}2\text{C}0\text{C}\text{A}\text{A}014\text{A}0\text{D}80\text{A}424\text{F}59\text{A}\text{D}\text{E}7\text{A}93068\text{D}08\text{A}7; \\ 0000000000000000000000002100\text{D}86957331832\text{B}8\text{E}8\text{C}230\text{F}5\text{B}\text{D}6\text{A}332\text{B}3615\text{A}\text{C}\text{A}.$$

Підписане повідомлення довжини $L = L_T + L_D$ має форму $T \parallel D$.

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

Перевіряємо цифровий підпис:

$D = 0000000000000000000000000000000000274EA2C0CAA014A0D80A424F59ADE7A93068D08A7;$
 $00000000000000000000000000000000002100D86957331832B8E8C230F5BD6A332B3615ACA.$

Перевіримо довжину цифрового підпису: $L_D = 512$, тобто чи є це число кратне до 16 і більше за подвійну довжину двійкового зображення порядку базової точки n .

Обчислюємо $L_T = L - L_D$. Вважаємо, що підписаний текст прийнято без спотворень, тому $L_T > 0$.

Обчислюємо $H(T)$. Підписаний текст прийнято без спотворень, тому результат обчислення функції гешування є, як і при обчисленні цифрового підпису,

$H(T) = 09C9C44277910C9AAEE486883A2EB95B7180166DD$
 $F73532EEB76EDAEF52247FF.$

Перетворюємо результат обчислення функції гешування на елемент основного поля:

$h = 03A2EB95B7180166DDF73532EEB76EDAEF52247FF.$

Перетворюємо цифровий підпис на пару цілих чисел (r, s) :

$r = 274EA2C0CAA014A0D80A424F59ADE7A93068D08A7;$
 $s = 2100D86957331832B8E8C230F5BD6A332B3615ACA.$

Переконаємося, що $0 < r < n$ та $0 < s < n$.

Обчислюємо точку еліптичної кривої

$R = sP + rQ = (x_R, y_R) = (42A7D756D70E1C9BA62D2CB43707C35204EF3C67C,$
 $5310AE5E560464A95DC80286F17EB762EC544B15B).$

Обчислюємо елемент основного поля

Припустимо, що довжина цифрового підпису дорівнює найменшому припустимому значенню $L_D = 352$.

Обчислення цифрового підпису. Обчислюємо $H(T)$ і перетворюємо результат обчислення на елемент основного поля h . Внаслідок перетворення одержуємо елемент основного поля

$$h = 0137187EA862117EF1484289470ECAC802C5A651FDA8.$$

Нехай ціле число

$$e = 70516411E5D9886B8486ECE54A30E9403D103B95F90.$$

Обчислюємо точку eP :

$$eP = (x_{eP}, y_{eP}) = (028886EA28A7C2951FA6473EB3EBC861D3EDB1FBB031, \\ 19059E90F7C7725079CFFE312A389B265140F5BDA493).$$

Тоді F_e дорівнює координаті x_{eP} цієї точки

$$F_e = 028886EA28A7C2951FA6473EB3EBC861D3EDB1FBB031.$$

Обчислюємо добуток елементів основного поля

$$y = hF_e = 0477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A.$$

Перетворюємо елемент основного поля y на ціле число r

$$r = 477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A.$$

Обчислюємо ціле число

$$s \equiv (e + dr) \bmod n \equiv 472EA56AE478F95F1EC9F628FF43857E168B50FB819.$$

Перетворюємо пару цілих чисел (r, s) на цифровий підпис D :

$D = 0477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A;$
 $0472EA56AE478F95F1EC9F628FF43857E168B50FB819.$

Підписане повідомлення довжини $L = 8 + L_T + L_D$ має вигляд $iH \parallel T \parallel D$, де iH – двійковий рядок вигляду 00000001.

Перевірка цифрового підпису. Перевіряємо цифровий підпис, обчислений вище. При перевірці цифрового підпису використовуємо ті самі загальні параметри, обчислений вище відкритий ключ та геш-функцію без додаткових вказівок ($iH = 1$; $L_H = 256$; iH передається).

Перевіряємо цифровий підпис

$D = 0477ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A;$
 $0472EA56AE478F95F1EC9F628FF43857E168B50FB819.$

Без додаткових вказівок, перші 8 бітів повідомлення задають iH . Перевіряємо, чи геш-функція з номером 00000001 є діюча на даний час, і визначаємо відповідну довжину геш-коду $L_H = 256$.

Перевіряємо довжину цифрового підпису: $L_D = 352$, тобто чи є це число кратне до 16 і більше за подвоєну довжину двійкового зображення порядку базової точки n .

Обчислюємо $L_T = L - L_D - L(iH)$. Вважаємо, що підписаний текст прийнято без спотворень, тому $L_T > 0$.

Обчислюємо $H(T)$. Підписаний текст прийнято без спотворень, тому результат обчислення функції гешування є, як і при обчисленні цифрового підпису

$H(T) = 2A681ECE118389B27A108137187EA862117EF1484289$
 $470ECAC802C5A651FDA8.$

Перетворюємо результат обчислення на елемент h основного поля

$h = 0137187EA862117EF1484289470ECAC802C5A651FDA8.$

Перетворюємо цифровий підпис на пару цілих чисел (r, s)

$$r = 477\text{ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A};$$

$$s = 472\text{EA56AE478F95F1EC9F628FF43857E168B50FB819}.$$

Переконуємося, що $0 < r < n$ та $0 < s < n$.

Обчислюємо точку еліптичної кривої

$$R = sP + rQ = (x_R, y_R) = (028886\text{EA28A7C2951FA6473EB3EBC861D3EDB1FBB031}, \\ 19059\text{E90F7C7725079CFFE312A389B265140F5BDA49}).$$

Обчислюємо елемент основного поля

$$y = hx_R = 0477\text{ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A}.$$

Перетворюємо елемент основного поля y на ціле число $\tilde{r}$

$$\tilde{r} = 477\text{ECC260F390FB6D0AE4AE3B7A78120F8EC458EF9A}.$$

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

4.17 Класифікація атак на схеми електронного підпису

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

Надамо класифікацію атак на схеми електронного підпису:

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

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

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

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

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

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

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

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

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

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

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

4.18 Протокол автентифікації з нульовою передачею знань на еліптичній кривій

Модифікація протоколу автентифікації Окамото [27]. Нехай $E_p(a, b)$ – еліптична крива, відома учасникам інформаційного процесу; G і Q – попередньо узгоджені точки еліптичної кривої; $n = \#E_p(a, b)$ – порядок ЕС.

Абонент A вибирає секретні числа k_1 і k_2 ($1 < k_1, k_2 < n$) та обчислює відкритий ключ $Y = k_1G + k_2Q$, які передає абоненту B у вигляді *certA* – сертифікат відкритого ключа абонента A :

1. Абонент A обирає випадкові числа r_1 і r_2 ($1 < r_1, r_2 < n - 1$) та надсилає абоненту B число γ

$$A \rightarrow B: cert_A, \gamma = r_1 G + r_2 Q.$$

2. Абонент B відповідає випадковим запитом x

$$A \leftarrow B: x.$$

3. Абонент A надсилає абоненту B значення y_1 і y_2

$$\begin{aligned} A \rightarrow B: y_1 &\equiv (r_1 + k_1 x) \bmod n, \\ y_2 &\equiv (r_2 + k_2 x) \bmod n. \end{aligned}$$

Абонент B перевіряє рівність

$$y_1 G + y_2 Q - xY = \gamma.$$

Схему протоколу автентифікації Окамото на еліптичній кривій показано на рис. 4.30.

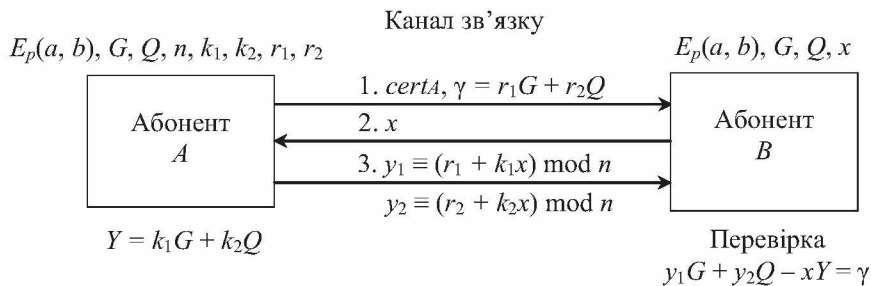


Рисунок 4.30 – Протокол автентифікації Окамото на еліптичній кривій

Повнота протоколу впливає з рівності

$$\begin{aligned} y_1 G + y_2 Q - xY &= (r_1 + k_1 x)G + (r_2 + k_2 x)Q - x(k_1 G + k_2 Q) = \\ &= r_1 G + k_1 xG + r_2 Q + k_2 xQ - xk_1 G - xk_2 Q = r_1 G + r_2 Q = \gamma. \end{aligned}$$

Приклад протоколу Окамото на еліптичній кривій. Нехай $E_{10007}(-3, 7)$; $G = (476, 997)$; $Q = (640, 761)$; $n = 10193$.

Користувач A обирає секретні числа $k_1 = 1293$ і $k_2 = 7911$; випадкові числа $r_1 = 9321$ і $r_2 = 785$ та обчислює відкритий ключ

$$Y = 1293(476, 997) + 7911(640, 761) = \\ = (8082, 8514) + (5022, 9323) = (339, 7167).$$

Протокол:

1. $A \rightarrow B$: $cert_A, \gamma = 9321(476, 997) + 785(640, 761) = (5832, 6370) + (7056, 9304) = (6199, 6142)$;
2. $A \leftarrow B$: $x = 6163$;
3. $A \rightarrow B$: $y_1 \equiv (9321 + 1293 \cdot 6163) \bmod 10193 \equiv 7154$;
 $y_2 \equiv (785 + 7911 \cdot 6163) \bmod 10193 \equiv 3159$.

Абонент B виконує перевірку

$$7154(476, 997) + 3159(640, 761) - 6163(339, 7167) = \\ = (6571, 7075) + (4308, 6078) - (8166, 7701) = (6199, 6142) = \gamma.$$

Абонент B приймає доказ оскільки рівність виконано.

Приклад протоколу Окамото на еліптичній кривій над розширеним полем. Нехай задано: несуперсингулярна еліптична крива над розширеним полем $GF(2^7)$ (додаток Б)

$$y^2 + xy \equiv (x^3 + x^2 + 1001) \bmod (f(x) = x^7 + x^3 + 1, 2);$$

$n = 126$; $G = (1100010, 100111)$; $Q = (111101, 1100001)$.

Користувач A обирає секретні числа $k_1 = 120$ і $k_2 = 79$, випадкові числа $r_1 = 93$ і $r_2 = 85$ та обчислює відкритий ключ

$$Y = 120(1100010, 100111) + 79(111101, 1100001) = \\ = (1011011, 1000101) + (1111111, 10100) = (110111, 1000).$$

Протокол:

1. $A \rightarrow B: cert_A, \gamma = 93(1100010, 100111) + 85(111101, 1100001) =$
 $= (111100, 1011011) + (1001111, 110100) = (10110, 1100011);$
2. $A \leftarrow B: x = 100;$
3. $A \rightarrow B: y_1 \equiv (93 + 120 \cdot 100) \bmod 126 \equiv 123;$
 $y_2 \equiv (85 + 79 \cdot 100) \bmod 126 \equiv 47.$

Абонент B виконує перевірку

$$\begin{aligned} & 123(1100010, 100111) + 47(111101, 1100001) - 100(110111, 1000) = \\ & = (1101100, 110) + (1111111, 1101011) - (11011, 10011) = \\ & = (111110, 100) + (11011, 1000) = (10110, 1100011) = \gamma. \end{aligned}$$

Абонент B приймає доказ оскільки рівність виконано.

5 АПАРАТНІ ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

5.1 Засоби криптографічного захисту інформації

Засіб криптографічного захисту інформації (КЗІ) – програмний, апаратно-програмний та апаратний засіб, призначений для криптографічного захисту інформації [28].

Залежно від способу реалізації розрізняють такі *типи засобів КЗІ* [28]:

- апаратні засоби, алгоритм функціонування (у тому числі криптографічні функції) яких реалізовано в оптичних, механічних, електронних або інших спеціалізованих пристроях та не може бути змінено без зміни цих пристроїв;

- апаратно-програмні засоби, алгоритм функціонування (або окремі функції, у тому числі криптографічні) яких реалізовано у їх спеціально для цього використаних апаратних компонентах (програмованих логічних інтегральних схемах, контролерах) і заміна алгоритму функціонування (або окремих функцій, у тому числі криптографічних) яких можлива виробником цих засобів без зміни апаратних компонентів;

- програмні засоби, алгоритм функціонування (у тому числі криптографічні функції) яких реалізовано програмним забезпеченням, що працює під управлінням операційної системи обчислювальних або комунікаційних пристроїв загального призначення і може бути змінено розробником цього програмного забезпечення, при цьому для роботи засобу не потрібні додаткові спеціально застосовані апаратні компоненти.

Залежно від виконання встановлюються такі *види засобів КЗІ* [28]:

- вид А – засоби, які на конструктивному, алгоритмічному та програмному рівнях є єдиними виробами, що функціонують (експлуатуються) відокремлено від будь-яких інших технічних засобів;

- вид Б – засоби, які на конструктивному, алгоритмічному та програмному рівнях є єдиними виробами та призначені для використання у складі комплексів оброблення та передавання інформації;

- вид В – криптографічні модулі, які не використовуються (не експлуатуються) окремо, а застосовуються як складові частини при побудові засобів КЗІ видів А та Б.

Засоби виду Б поділяються на:

- підвид Б1 – вироби, які встановлюються в розрив каналу електронних комунікацій та/або розділяють потоки захищеної інформації та інформації, що підлягає захисту, а також вироби, що забезпечують відокремлення оброблення захищеної інформації та інформації, що підлягає захисту, в обчислювальній системі;

- підвид Б2 – апаратні, апаратно-програмні або програмні вироби, які підключаються до інших засобів та виконують функції криптографічних перетворень у взаємодії з ними або під їх управлінням;

Залежно від призначення встановлюються такі *категорії засобів КЗІ* [28]:

- засоби шифрування інформації (засоби категорії “Ш”);

- засоби, призначені для виготовлення ключових даних або ключових документів (незалежно від виду носія ключової інформації) та управління ключовими даними, що використовуються в засобах КЗІ (засоби категорії “К”);

- засоби, що реалізують криптоперетворення та/або механізми імітозахисту та призначені для забезпечення захисту (підтвердження) хоча б однієї з таких властивостей інформації: справжності (авторства), цілісності, неспростовності, дати створення (засоби категорії “П”);

- засоби захисту інформації від НСД (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми (засоби категорії “Р”);

- засоби (засоби, об’єднані в комплекси), спеціально призначені для розроблення, дослідження, виробництва та випробувань засобів КЗІ, у тому числі програмування та/або запису в їх апаратні компоненти (програмовані логічні інтегральні схеми, контролери), перевірки та контролю правильності реалізації в засобах КЗІ криптографічних функцій (засоби категорії “З”).

Залежно від вірогідних умов експлуатації засобів КЗІ та відповідно до цінності інформації, що захищається, визначаються *чотири рівні можливостей порушника* [28]:

- нульовий рівень – ненавмисне порушення конфіденційності, цілісності та підтвердження авторства інформації;

- перший рівень – порушник має обмежені кошти та самостійно створює засоби, розробляє методи атак на засоби КЗІ, а також інформаційно-комунікаційні системи із застосуванням поширених програмних засобів та електронно-обчислювальної техніки;

– другий рівень – порушник корпоративного типу має змогу створення спеціальних технічних засобів, вартість яких співвідноситься з можливими фінансовими збитками, що виникатимуть від порушення конфіденційності, цілісності та підтвердження авторства інформації, зокрема при втраті, спотворенні та знищенні інформації, що захищається. У цьому разі для розподілу обчислень при проведенні атак можуть застосовуватися локальні обчислювальні мережі;

– третій рівень – порушник має науково-технічний ресурс, який прирівнюється до науково-технічного ресурсу спеціальної служби економічно розвинутої держави.

З урахуванням установленого рівня можливостей порушника обирається необхідний *клас засобів КЗІ* [28]:

– клас А1 – відповідає вимогам забезпечення стійкості криптоперетворення в умовах, коли можливості порушника обмежені лише сучасним станом науки і техніки (захист від порушника третього рівня);

– клас Б1 – відповідає вимогам забезпечення стійкості криптоперетворення в умовах недокументованих можливостей у прикладному програмному забезпеченні (захист від порушника другого рівня);

– клас Б2 – відповідає вимогам забезпечення стійкості криптоперетворення в умовах здійснення порушником навмисного зовнішнього впливу (захист від порушника другого рівня);

– клас В1 – відповідає вимогам забезпечення стійкості криптоперетворення в умовах несанкціонованих дій з боку легального користувача системи (захист від порушника першого рівня);

– клас В2 – відповідає вимогам забезпечення стійкості криптоперетворення в умовах помилкових дій обслуговувального персоналу та відмов технічних засобів (захист від порушника першого та нульового рівнів);

– клас В3 – відповідає вимогам забезпечення стійкості криптоперетворення за рахунок стійкості криптоалгоритму та правильної його реалізації в засобі КЗІ (захист від порушника нульового рівня).

Класи засобів КЗІ наведено в порядку зменшення вимог таким чином, що рівень, наведений вище, передбачає виконання вимог усіх наведених нижче класів.

5.2 Модуль безпеки МБ-2 НБУ

Модуль безпеки МБ-2 НБУ (ІТ Модуль безпеки МБ-2 НБУ) (рис. 5.1) призначений для роботи у складі програмно-апаратних комплексів банків, їх філій та відділень, які є учасниками Національної системи масових електронних платежів і виконує наступні функції [29]:

- генерація ключової інформації для алгоритмів DES та TDEA (Triple Data Encryption Algorithm);
- зберігання ключової інформації;
- проведення криптографічних операцій за алгоритмами DES та TDEA, одержання кодів автентичності MAC, на основі вказаних криптографічних алгоритмів;
- зберігання лімітів, лічильників та накопичувачів;
- генерація псевдовипадкових чисел;
- захист програмного забезпечення ЕОМ та операційних систем (ОС) від НСД.



Рисунок 5.1 – Модуль безпеки МБ-2 НБУ

Конструкція та технічні характеристики засобу. Модуль безпеки МБ-2 НБУ виконаний у вигляді плати розширення ЕОМ, призначеної для встановлення у з'єднувач системної шини PCI Express x1 (одне стандартне посадкове місце). Виріб має захисний металевий корпус з відсіком для батарей резервного електроживлення. Габаритні розміри виробу з урахуванням з'єднувача та кронштейну 181x127x20 мм. Маса виробу не більше 0,7 кг.

Модуль має систему захисту від несанкціонованого доступу (розкриття корпусу, свердління, пиляння, фрезерування, хімічне травлення тощо) до внутрішніх елементів, яка є активною у незалежності від зовнішнього електроживлення та здійснить видалення ключової інформації, яка зберігається у виробі, при виявленні такої спроби.

Модуль має два інтерфейсних з'єднувача:

- ламельний, для встановлення виробу у слот PCI Express з одним або більше каналом системної плати EOM;

- розетка USB типу A для підключення зчитувача смарт-карток або електронного ключа.

Швидкість виконання криптографічних перетворень за алгоритмами DES – 32 МБіт/с (внутрішня – 150 МБіт/с) та TDEA – 20 МБіт/с (внутрішня – 50 МБіт/с) [29].

5.3 Електронний ключ “Алмаз-1К”

Електронний ключ “Алмаз-1К” (рис. 5.2) призначений для реалізації криптографічних перетворень у складі апаратно-програмних засобів і комплексів КЗІ, що реалізовані на основі EOM [29].



Рисунок 5.2 – Електронний ключ “Алмаз-1К”

Електронний ключ “Алмаз-1К” Bluetooth (рис. 5.3) являє собою малогабаритний електронний пристрій, виконаний у вигляді пластикового брелку [29]. Електронні компоненти виробу (у тому числі тримач батареї електроживлення) встановлені на друковану плату, яка фіксується у корпусі брелку. Кришка брелку фіксується пластиковими зачіпками. Електронний ключ “Алмаз-1К” Bluetooth призначений для роботи зі смарт-пристроями (телефонами, планшетами), портативними ПК (ноутбуками) або інші пристрої (EOM), які підтримують бездротовий інтерфейс Bluetooth 4.0 (та вище) BLE (Bluetooth Low Energy).



Рисунок 5.3 – Електронний ключ “Алмаз-1К” Bluetooth

Електронні ключі “Алмаз-1К” та “Алмаз-1К” Bluetooth виконус наступні функції [29]:

- автентифікацію оператора ЕОМ при доступі до ключа;
- генерацію особистих та відкритих ключів для алгоритму ЕП;
- генерацію особистих та відкритих ключів для протоколу розподілу ключів;
- генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора;
- зберігання особистих ключів у внутрішній пам’яті та захист їх від НСД;
- формування і перевірку ЕП;
- обчислення геш-функції;
- розподіл ключових даних на основі асиметричного протоколу розподілу;
- зберігання довільних даних у внутрішній пам’яті та захист їх від НСД;
- контроль цілісності і працездатності вбудованого програмного забезпечення.

Конструкція та технічні характеристики засобу. Електронний ключ “Алмаз-1К” виконаний у вигляді малогабаритного знімного USB-пристрою, який має програмний інтерфейс CCID (Circuit Card Interface Device). Конструктивно електронний ключ виконаний на двошаровій друкованій платі, яка залита компаундом, що формує захисний шар та встановлена в пластмасовий чи металевий корпус, що формує зовнішній вигляд засобу. На друкованій платі встановлюються електронні компоненти та USB-з’єднувач

типу A-plug (виделка).

Електронні ключі “Алмаз-1К” та “Алмаз-1К” Bluetooth реалізують наступні криптографічні алгоритми та протоколи:

- шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни та режим вироблення імітовставки);
- ЕП за ДСТУ 4145-2002 (всі довжини ключів передбачені стандартом);
- гешування за ГОСТ 34.311-95;
- протокол розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої (довжина ключа до 571 біту).

Швидкість формування ЕП електронного ключа “Алмаз-1К” за ДСТУ 4145-2002, поле $m = 257 - 0,3$ с. Швидкість формування спільного секрету Діффі-Гелмана в групі точок еліптичної кривої, поле $m = 571 - 2,1$ с [29].

Швидкість формування ЕП електронного ключа “Алмаз-1К” Bluetooth за ДСТУ 4145-2002, поле $m = 257 - 0,7$ с. Швидкість формування спільного секрету Діффі-Гелмана в групі точок еліптичної кривої, поле $m = 571 - 3,5$ с [29].

Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливає доступ до особистих ключів з боку апаратного-програмного середовища.

Особисті ключі генеруються, зберігаються та використовуються тільки усередині електронного ключа, та жодним способом не потрапляють за його межі. Зберігання особистих ключів та інших ключових даних здійснюється у внутрішньому постійному запам'ятовуючому пристрої (ПЗП) електронного ключа.

5.4 Електронний ключ “Кристал-1”

Електронний ключ “Кристал-1” (рис. 5.4) призначений для реалізацій криптографічних перетворень у складі апаратно-програмних засобів і комплексів КЗІ, що реалізовані на основі ЕОМ [15, 29].

Електронний ключ “Кристал-1” виконує наступні функції [29]:

- автентифікацію оператора ЕОМ при доступі до ключа;
- генерацію особистих та відкритих ключів для алгоритму ЕП;
- генерацію особистих та відкритих ключів для протоколу розподілу ключів;



Рисунок 5.4 – Електронний ключ “Кристал-1”

- генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора;
- зберігання особистих ключів у внутрішній пам’яті та захист їх від НСД;
- формування і перевірку ЕП;
- обчислення геш-функції;
- розподіл ключових даних на основі асиметричного протоколу розподілу;
- зберігання довільних даних у внутрішній пам’яті та захист їх від НСД;
- зберігання файлів у вбудованому електронному flash-диску та їх шифрування;
- контроль цілісності і працездатності вбудованого програмного забезпечення.

Конструкція та технічні характеристики засобу. Електронний ключ виконаний у вигляді малогабаритного знімного USB-пристрою, який може мати програмний CCID-інтерфейс та електронний flash-диск (протокол USB Mass Storage). Конструктивно електронний ключ виконаний на двошаровій друкованій платі, яка залита компаундом, що формує захисний шар та встановлена в пластмасовий чи металевий корпус, що формує зовнішній вигляд засобу. На друкованій платі встановлюються електронні компоненти та USB-з’єднувач типу A-plug (виделка).

Електронний ключ “Кристал-1” реалізує наступні криптографічні алгоритми та протоколи:

- шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни та режим вироблення імітовставки);
- ЕП за ДСТУ 4145-2002 (всі довжини ключів передбачені стандартом);

- гешування за ГОСТ 34.311-95;
- протокол розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої (довжина ключа до 571 біту).

Швидкість формування ЕП за ДСТУ 4145-2002, поле $m = 257 - 0,1$ с.
Швидкість формування спільного секрету Діффі-Гелмана в групі точок еліптичної кривої, поле $m = 571 - 0,8$ с [29].

Вбудований електронний flash-диск може бути об'ємом 4, 8, 16 чи 32 ГБ. Швидкість запису та зчитування диску з шифруванням за ДСТУ ГОСТ 28147:2009 – 0,5 Мбайт/с [29]. Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливорює доступ до особистих ключів з боку апаратного-програмного середовища. Особисті ключі генеруються, зберігаються та використовуються тільки усередині електронного ключа, та жодним способом не потрапляють за його межі. Зберігання особистих ключів та інших ключових даних здійснюється у внутрішньому ПЗП електронного ключа.

5.5 Криптомодуль “Тряда-61”

Криптомодуль “Тряда-61” – апаратний засіб КЗІ виду Б, підвиду Б2, категорії “П” та “Ш”, класу Б1 [29].

Криптомодуль “Тряда-61” призначений для апаратної реалізації криптографічних перетворень у складі апаратно-програмних засобів і комплексів КЗІ, що реалізовані на основі ЕОМ [29].

Криптомодуль виконує наступні функції:

- автентифікацію оператора ЕОМ при доступі до модуля;
- генерацію особистих та відкритих ключів для алгоритму ЕП;
- генерацію особистих та відкритих ключів для протоколу розподілу ключів;
- генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора;
- зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД;
- формування і перевірки ЕП;
- обчислення геш-функції;
- розподіл ключових даних на основі асиметричного протоколу

розподілу;

- зберігання довільних даних у внутрішній пам'яті та захист їх від НСД;
- резервне копіювання ключів на зовнішні носії (електронні ключі) та відновлення ключів з носіїв;
- контроль цілісності і працездатності вбудованого програмного забезпечення.

Конструкція та технічні характеристики криптомодуля “Грядя-61” (рис. 5.5, 5.6).



Рисунок 5.5 – Криптомодуль “Грядя-61” у пластмасовому корпусі



Рисунок 5.6 – Криптомодуль “Грядя-61” у металевому корпусі

Криптомодуль виконаний у вигляді малогабаритного USB-пристрою, що під'єднується до ЕОМ за допомогою кабелю. Виріб у пластмасовому корпусі має незнімний USB-кабель (рис. 5.5), а виріб у металевому корпусі (рис. 5.6) під'єднується до ЕОМ за допомогою знімного USB-кабелю. Конструктивно криптичний модуль виконаний на двошаровій друкованій платі, яка встановлена у пластиковий чи металевий корпус та залита компаундом, що формує

захисний шар. На друкованій платі встановлюються електронні компоненти криптомодуля. До друкованої плати виробу у пластмасовому корпусі нерозбірно під'єднаний USB-кабель, а виріб у металевому корпусі має miniUSB-розетку типу B для під'єднання знімного USB-кабелю.

Криптомодуль реалізує наступні криптографічні алгоритми та протоколи:

- шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни та режим вироблення імітовставки);
- ЕП за ДСТУ 4145-2002 (всі довжини ключів передбачені стандартом);
- гешування за ГОСТ 34.311-95;
- протокол розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої (довжина ключа до 571 біту).

Швидкість формування ЕП за ДСТУ 4145-2002, поле $m = 257 - 0,1$ с. Швидкість формування спільного секрету Діффі-Гелмана в групі точок еліптичної кривої, поле $m = 571 - 0,8$ с [29].

Апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливає доступ до особистих ключів з боку апаратного-програмного середовища.

Особисті ключі генеруються, зберігаються та використовуються тільки усередині криптомодуля, та жодним способом не потрапляють за його межі. Зберігання особистих ключів та інших ключових даних здійснюється у внутрішньому ПЗП криптомодуля.

Програми криптомодуля включають [15]:

- внутрішні програмні компоненти криптомодуля (внутрішні програми);
- системні програмні компоненти (драйвери або модулі ядра ОС Microsoft Windows та Linux/UNIX);
- програмний комплекс тестування та конфігурування криптомодуля (модуль, що виконується для ОС Microsoft Windows та ОС Linux/UNIX).

Внутрішні програми криптомодуля призначені для [15]:

- прийому та зберігання у ПЗП загальних параметрів для алгоритму ЕП згідно з ДСТУ 4145-2002 та протоколу розподілу ключів;
- генерації особистого ключа ЕП та протоколу розподілу ключів з використанням алгоритму генерації випадкових бітових послідовностей згідно з ДСТУ 4145-2002 і вбудованого апаратного генератора випадкового сигналу (ГВС);

- зберігання у ПЗП особистих ключів ЕП та протоколу розподілу ключів в зашифрованому вигляді з контролем цілісності;
 - нищення з ПЗП особистих ключів ЕП та протоколу розподілу ключів;
 - формування ЕП від даних, що завантажуються з ЕОМ, за алгоритмом згідно з ДСТУ 4145-2002 з використанням особистого ключа ЕП;
 - генерації ключів сеансу для ГОСТ 28147-89;
 - формування спільного секретного ключа за протоколом розподілу ключових даних з використанням власного особистого ключа протоколу розподілу та відкритого ключа протоколу розподілу отримувача;
 - зашифровування та розшифрування ключів сеансу для ГОСТ 28147-89 з використанням сформованого спільного секретного ключа за алгоритмом згідно з ГОСТ 28147-89 (режим простої заміни);
 - автентифікації користувача перед початком роботи шляхом гешування пароля доступу до криптомодуля за алгоритмом згідно з ГОСТ 34.311-95 та порівнянням з еталоном, що зберігається у ПЗП;
 - управління параметрами автентифікації користувача;
 - прийому, запису та зберігання у ПЗП довільних даних користувача;
 - надання доступу та знищення довільних даних користувача з ПЗП.
- Системні програмні компоненти призначені для [15]:
- забезпечення коректного розпізнавання криптомодуля ОС ЕОМ;
 - передачі кодів команд та вхідних даних для виконання відповідних внутрішніх програм криптографічного модуля, які виконують перетворення вхідних даних на вихідні;
 - отримання з криптомодуля результатів виконання команд і вихідних даних.

Програмний комплекс тестування та конфігурування призначений для [15]:

- перевірки роботоздатності криптомодуля;
- конфігурування параметрів криптомодуля в ОС ЕОМ;
- встановлення або зміни даних автентифікації користувача шляхом їх завантаження в криптомодуль;
- форматування криптомодуля, що включає знищення особистих ключів і довільних даних користувача та встановлення даних автентифікації.

5.6 Мережний криптомодуль “Грядя-301”

Криптомодуль мережний “Грядя-301” (рис. 5.7), “Грядя-301” високопродуктивний (рис. 5.8), “Грядя-301” міні (рис. 5.9), “Грядя-301” мікро (рис. 5.10) – апаратні засоби КЗІ виду Б, підвиду Б2, категорії “П” та “Ш”, класу Б1 [29].



Рисунок 5.7 – Криптомодуль мережний “Грядя-301”



Рисунок 5.8 – Криптомодуль мережний “Грядя-301” високопродуктивний



Рисунок 5.9 – Криптомодуль мережний “Грядя-301” міні



Рисунок 5.10 – Криптомодуль мережний “Трояда-301” мікро

Вироби виконує наступні функції [29]:

- автентифікацію ЕОМ при доступі до модуля;
- генерацію особистих та відкритих ключів для алгоритму ЕП;
- генерацію особистих та відкритих ключів для протоколу розподілу ключів;
- генерацію ключів для алгоритму шифрування та генерацію випадкових послідовностей на основі апаратного генератора;
- зберігання особистих ключів у внутрішній пам’яті та захист їх від НСД;
- формування і перевірку ЕП;
- обчислення геш-функції;
- розподіл ключових даних на основі асиметричного протоколу;
- зберігання довільних даних у внутрішній пам’яті та захист їх від НСД;
- резервне копіювання ключів на зовнішні носії (електронні ключі) та відновлення ключів з носіїв;
- контроль цілісності і працездатності вбудованого програмного забезпечення.

Мережний криптомодуль “Трояда-301” (рис. 5.7) виконаний у вигляді окремого мережного вузла. Конструктивно мережний криптомодуль являє собою системну платформу у металевому корпусі висотою 1U та призначену для встановлення в 19-ти дюймову стійку. Засіб має 2 мережних інтерфейси Ethernet 10/100/1000.

Конструктивно мережний криптомодуль “Трояда-301” (рис. 5.8) високопродуктивний являє собою подовжену системну платформу у металевому корпусі висотою 1U та призначену для встановлення в 19-ти

двоїмому стійку. Виріб має 2 мережних інтерфейси Ethernet 10/100/1000 та 2 мережних інтерфейси SFP+ (1000/10000). Інтерфейси можуть бути налаштовані в режимі агрегації.

Мережний криптомодуль “Грядя-301” міні (рис. 5.9) виконаний у вигляді окремого мережного вузла та являє собою системну платформу у металевому корпусі висотою 2U та може встановлюватись в 19-ти двоїмому стійку за допомогою полиці. Засіб має 2 мережних інтерфейси Ethernet 10/100/1000.

Мережний криптомодуль “Грядя-301” мікро (рис. 5.10) також виконаний у вигляді окремого малогабаритного мережного пристрою та являє собою мініатюрну системну платформу у металевому корпусі і має 2 мережних інтерфейси: Ethernet 10/100 та USB (RNDIS – Remote Network Driver Interface Specification). Засіб має розетку RJ-45 для підключення до мережі за допомогою мережного кабелю та miniUSB-розетку типу B для під’єднання до ЕОМ за допомогою знімного USB-кабелю.

Мережний криптомодуль “Грядя-301” реалізує наступні криптографічні алгоритми та протоколи:

- шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни, режим гамування та режим вироблення імітовставки);
- ЕП за ДСТУ 4145-2002 (всі довжини ключів передбачені стандартом – поля 163, 167, 173, 179, 191, 233, 257, 307, 367, 431), RSA за PKCS#1 (IETF RFC 3447) та ECDSA за ДСТУ ISO/IEC 14888-3:2014;
- гешування за ГОСТ 34.311-95;
- протоколи розподілу ключів за ДСТУ ISO/IEC 11770-3:2015 та RSA за PKCS#1 (IETF RFC 3447).

Мережний криптомодуль “Грядя-301”.

Швидкість формування ЕП за ДСТУ 4145-2002, поле $m = 257$: час формування ЕП – 0,64 мс, кількість формувань ЕП – 1560 формувань/с. Швидкість формування спільного секрету за ДСТУ ISO/IEC 15946-3, поле $m = 431$: час формування спільного секрету – 5,12 мс, кількість формувань спільного секрету (державного): 196 формувань/с.

Швидкість формування ЕП за RSA, 2048 біт (SHA-256): час формування ЕП – 18 мс, кількість формувань ЕП – 55 формувань/с. Швидкість формування ЕП за ECDSA, NIST P-256 (secp256r1), 256 біт: час формування ЕП – 1,3 мс, кількість формувань ЕП – 770 формувань/с.

Швидкодія протоколу розподілу ключів за RSA: час розшифрування даних – 18 мс, кількість розшифрувань даних – 55 розшифрувань/с. Швидкодія протоколу розподілу ключів за ECDH: час формування спільного секрету – 21 мс, кількість формувань спільного секрету – 47 формувань/с.

Кількість ключів – 12 288 (зберігання наборів ключів ЕП та протоколів розподілу).

Мережний криптомодуль “Грядя-301” високопродуктивний.

Швидкість формування ЕП за ДСТУ 4145-2002, поле $m = 257$: час формування ЕП – 0,14 мс, кількість формувань ЕП – 6900 формувань/с. Швидкість формування спільного секрету за ДСТУ ISO/IEC 15946, поле $m = 431$: час формування спільного секрету – 1,15 мс, кількість формувань спільного секрету (державного): 875 формувань/с.

Швидкість формування ЕП за RSA, 2048 біт (SHA-256): час формування ЕП – 4,5 мс, кількість формувань ЕП – 225 формувань/с. Швидкість формування ЕП за ECDSA, NIST P-256 (secp256r1), 256 біт: час формування ЕП – 0,32 мс, кількість формувань ЕП – 3100 формувань/с.

Швидкодія протоколу розподілу ключів за RSA: час розшифрування даних – 4,5 мс, кількість розшифрувань даних – 220 розшифрувань/с. Швидкодія протоколу розподілу ключів за ECDH: час формування спільного секрету – 5,12 мс, кількість формувань спільного секрету – 196 формувань/с.

Кількість ключів – 4 194 304 (зберігання наборів ключів ЕП та протоколів розподілу).

Мережний криптомодуль “Грядя-301” мікро.

Швидкість формування ЕП за ДСТУ 4145-2002, поле $m = 257$: час формування ЕП – 8 мс, кількість формувань ЕП – 125 формувань/с. Швидкість формування спільного секрету за ДСТУ ISO/IEC 15946-3, поле $m = 431$: час формування спільного секрету – 74 мс, кількість формувань спільного секрету (державного) – 14 формувань/с.

Швидкість формування ЕП за RSA, 2048 біт (SHA-256): час формування ЕП – 132 мс, кількість формувань ЕП – 8 формувань/с. Швидкість формування ЕП за ECDSA, NIST P-256 (secp256r1), 256 біт: час формування ЕП – 10 мс, кількість формувань ЕП – 100 формувань/с.

Швидкодія протоколу розподілу ключів за RSA: час розшифрування даних – 132 мс, кількість розшифрувань даних – 8 розшифрувань/с.

Швидкодія протоколу розподілу ключів за ECDH: час формування спільного секрету – 160 мс, кількість формувань спільного секрету – 7 формувань/с. Кількість ключів – 384 (зберігання наборів ключів ЕП та протоколів розподілу).

Мережний криптомодуль "Грядя-301" міні.

Швидкість формування ЕП за ДСТУ 4145-2002, поле $m = 257$: час формування ЕП – 2,18 мс, кількість формувань ЕП – 460 формувань/с. Швидкість формування спільного секрету за ДСТУ ISO/IEC 15946-3, поле $m = 431$: час формування спільного секрету – 19,5 мс, кількість формувань спільного секрету – 53 формувань/с.

Швидкість формування ЕП за RSA, 2048 біт (SHA-256): час формування ЕП – 70 мс, кількість формувань ЕП – 15 формувань/с. Швидкість формування ЕП за ECDSA, NIST P-256 (secp256r1), 256 біт: час формування ЕП – 4,3 мс, кількість формувань ЕП – 230 формувань/с.

Швидкодія протоколу розподілу ключів за RSA: час розшифрування даних – 70 мс, кількість розшифрувань даних – 15 розшифрувань/с. Швидкодія протоколу розподілу ключів за ECDH: час формування спільного секрету – 75 мс, кількість формувань спільного секрету – 14 формувань/с.

Кількість ключів – 1536 (зберігання наборів ключів ЕП та протоколів розподілу).

5.7 Апаратний генератор випадкових чисел "Грядя-3"

Апаратний генератор випадкових чисел "Грядя-3" (рис. 5.11) – апаратний засіб КЗІ виду Б, категорії "К", класу Б1 та призначений для апаратної генерації послідовностей випадкових чисел на основі фізичних датчиків шуму у складі апаратно-програмних засобів та комплексів КЗІ, що реалізовані на основі ЕОМ. Область застосування: апаратно-програмні засоби та комплекси КЗІ типу "К", "Ш", "П" та "Р" [29].

Пристрій виконаний у конструктиві плати розширення ЕОМ для встановлення у слот (одне стандартне посадкове місце) системної шини PCI-32 (32 біта, 33 МГц). Пристрій складається з двох незалежних блоків, які функціонують (здійснюють генерацію випадкових бітів) паралельно. Швидкість генерації випадкових бітів з кожного з блоків – 16 Мбіт/с, а з двох блоків одночасно – 32 Мбіт/с.



Рисунок 5.11 – Апаратний генератор випадкових чисел “Гряда-3”

5.8 IP-шифратор

IP-шифратори “Канал-201” мікро (рис. 5.12), **“Канал-201”** (рис. 5.13), **“Канал-301”** (рис. 5.14), **“Канал-401”** (рис. 5.15) – апаратні засоби КЗІ виду Б, категорії “Ш”, класу Б1 [29].

IP-шифратори виконують наступні функції [29]:

- шифрування та контроль цілісності IP-пакетів;
- інкапсуляцію IP-пакетів та їх маршрутизацію між мережними інтерфейсами;

- прийом та введення в дію ключових даних;

- встановлення захищених з’єднань з іншими IP-шифраторами.

IP-шифратори реалізують наступні криптографічні алгоритми та протоколи [29]:

- шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни, режим гамування та режим вироблення імітовставки);

- ЕП за ДСТУ 4145-2002 (всі довжини ключів передбачені стандартом);

- генування за ГОСТ 34.311-95;

- протокол розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої (довжина ключа до 571 біту).



Рисунок 5.12 – ІП-шифратор “Канал-201” мікро
(швидкість шифрування – 40 Мбіт/с)



Рисунок 5.13 – ІП-шифратор “Канал-201”
(швидкість шифрування – 125 Мбіт/с)



Рисунок 5.14 – ІП-шифратор “Канал-301”
(швидкість шифрування – 1 Гбіт/с)



Рисунок 5.15 – ІР-шифратор “Канал-401”

Швидкість шифрування ІР-шифратора “Канал-401” – 1 Гбіт/с при використанні мережних інтерфейсів Ethernet 10/100/1000 та 5 Гбіт/с при використанні мережних інтерфейсів SFP+.

ІР-шифратор “CryptoIP-459” (рис. 5.16) забезпечує крізне шифрування ІР-трафіку, який передається між захищеними локально обчислювальними мережами через ІР-мережу загального користування [30]. “CryptoIP-459” є основою для створення віртуальних приватних мереж (VPN – Virtual Private Network) з шифруванням інформації. На базі пристроїв “CryptoIP-459” можуть бути побудовані криптографічні системи: з відкритими ключами і підтримкою архітектури PKI (Public Key Infrastructure – інфраструктура відкритих ключів) та з відкритими ключами і ручним розподілом сертифікатів абонентів [30].



Рисунок 5.16 – ІР-шифратор “CryptoIP-459”

У пристрої “CryptoIP-459” реалізуються алгоритми криптографічного захисту інформації [30]:

- шифрування за ДСТУ ГОСТ 28147:2009;
- гешування за ГОСТ 34.311-95;
- ЕП за ДСТУ 4145-2002;
- формування сеансового ключа за ДСТУ ISO/IEC 11770-3:2015.

Пристрій підтримує:

- два інтерфейси 10/100Base-T(TX) для підключення до глобальної мережі (рис. 5.16);

- два інтерфейси 10/100Base-T(TX) для підключення до локальної мережі (рис. 5.16);

- USB 2.0 для підключення до ПК локальне управління.

ІР-шифратор “Хортиця” на базі апаратних платформ Cisco UCS E-Series призначений для [31]:

- криптографічного захисту інформації з обмеженим доступом (крім інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом;

- наскрізного шифрування ІР-трафіку, що передається між захищеними локально-обчислювальними мережами через ІР-мережу загального користування.

ІР-шифратор «Хортиця»:

- виконаний на базі апаратних модулів (SM/NCE) виробництва Cisco, що функціонують спільно з маршрутизаторами з інтегрованими сервісами Cisco ISR серії 4000, а саме 4321 (або 4331, 4351, 4431, 4451, 4461), які виконують функції каналотворення та маршрутизації ІР-трафіку згідно функціонального призначення, визначеного виробником цього обладнання;

- використовує інтерфейси маршрутизатора Cisco ISR для підключення до обладнання транспортної мережі (WAN – Wide Area Network), а власні інтерфейси модуля – для підключення до абонентів мережі (LAN – Local Area Network) захищеного зв’язку;

- придатний для побудови VPN поверх будь-яких (але зв’язаних) ІРv4-сетей. Інформація в рамках VPN передається у тунельному режимі;

- кількість тунелів для криптографічної системи з відкритими ключами і підтримкою архітектури PKI може досягати кількох тисяч;

- маршрутизатор із встановленим ІР-шифратором може продовжувати виконувати свої інші функції згідно функціонального призначення.

Криптографічні алгоритми, що реалізуються у ІР-шифратора “Хортиця”:

- шифрування за ДСТУ 7624:2014 “Калина-128/256”, AES-256, ДСТУ ГОСТ 28147:2009;

- гешування за ДСТУ 7564:2014 “Купина-256”, SHA-256, ГОСТ 34311:95;

- ЕП за ДСТУ 4145-2002;

– формування сеансового ключа по схемі Діффі-Гелмана згідно ДСТУ ISO/IEC 11770-3:2015, RFC 2631 (ДСТУ 7624:2014, AES-256), ДСТУ ГОСТ 28147:2009.

У IP-шифратора “Хортиця” реалізована можливість одночасного використання усіх заявлених алгоритмів шифрування у одній захищеній мережі для усіх видів криптографічних систем.

5.9 Шлюз захисту “Бар’єр-301”

Шлюз захисту “Бар’єр-301” (рис. 5.17) – апаратний засіб КЗІ виду Б, категорії “Ш” та “Р”, класу Б1 [29]. Область застосування пристрою – інформаційно-комунікаційні системи, які призначені для обробки конфіденційної інформації, що не є власністю держави.



Рисунок 5.17 – Шлюз захисту “Бар’єр-301” (швидкість шифрування – 250 Мбіт/с, кількість автентифікації клієнтів – 100 автентифікації/с)

Шлюз захисту “Бар’єр-301” виконує наступні функції [29]:

- автентифікацію клієнтів захисту при підключенні до сервера;
- встановлення захищеного TCP-з’єднання з клієнтом в разі успішної автентифікації;
- встановлення відкритого TCP-з’єднання з сервером;
- прийом та розшифрування даних TCP-з’єднання від клієнта та передачі їх на сервер;
- прийом та зашифровування даних TCP-з’єднання від сервера та передачі їх клієнту;
- приймання та передачу управляючої (технологічної) інформації;

– прийом та введення в дію ключових даних.

Шлюз захисту реалізує наступні криптографічні алгоритми та протоколи [29]:

- шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни, режим гамування та режим вироблення імітовставки);
- ЕП за ДСТУ 4145-2002 (всі довжини ключів передбачені стандартом);
- гешування за ГОСТ 34.311-95;
- протокол розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої (довжина ключа до 571 біту).

Шлюз захисту “Бар’єр-301” мікро та міні показано на рис. 5.18, 5.19.



Рисунок 5.18 – Шлюз захисту “Бар’єр-301” мікро (швидкість шифрування – 40 Мбіт/с, кількість автентифікації клієнтів – 10 автентифікації/с)



Рисунок 5.19 – Шлюз захисту “Бар’єр-301” міні (швидкість шифрування – 125 Мбіт/с, кількість автентифікації клієнтів – 50 автентифікації/с)

5.10 Шлюз мережний “Бар’єр-1ЦСК”

Шлюз мережний “Бар’єр-1ЦСК” (рис. 5.20) призначений для [29]:

- попередження витоку інформації, що обробляється у закритому сегменті інформаційно-комунікаційної системи (мережі), у підключений до нього відкритий сегмент, в якому розміщений ЦСК;
- захисту пристрою від НСД;
- моніторингу роботи пристрою.



Рисунок 5.20 – Шлюз мережний “Бар’єр-1ЦСК”

Шлюз мережний “Бар’єр-1ЦСК” має 2 мережних інтерфейси Ethernet 10/100/1000. Один мережний інтерфейс пристрою призначений для підключення до відкритого сегменту мережі (рис. 5.20), в якому розміщений ЦСК, а другий – для підключення до закритого сегменту мережі (рис. 5.20), в якому знаходяться користувачі ЦСК. У закритому сегменті може оброблятися відкрита інформація та службова інформація.

Виключення можливості витоку інформації забезпечується шляхом:

- приймання OSCP-запитів (Online Certificate Status Protocol – протокол визначення статусу сертифіката) (запитів на пошук та перевірку статусу сертифікатів) через інтерфейс закритого сегмента та відправка переформованих запитів до ЦСК через інтерфейс відкритого сегмента;

- приймання через інтерфейс відкритого сегмента та передача через інтерфейс закритого сегмента OCSP-відповідей;

- приймання TSP-запитів (Time Stamp Protocol – протокол отримання позначок часу) (запитів на формування позначок часу) через інтерфейс закритого сегмента та відправка переформованих запитів до ЦСК через інтерфейс відкритого сегмента;

- приймання через інтерфейс відкритого сегмента та передача через інтерфейс закритого сегмента TSP-відповідей із позначками часу;

- приймання CMP-запитів (Certificate Management Protocol – протокол управління обслуговуванням сертифікатів) (запитів на отримання сертифікатів) через інтерфейс закритого сегмента та відправка переформованого запиту до ЦСК через інтерфейс відкритого сегмента;

- приймання через інтерфейс відкритого сегмента та передача через інтерфейс закритого сегмента CMP-відповідей, які містять ланцюжок сертифікатів;

- приймання через інтерфейс закритого сегменту даних віддаленого управління з попередньою автентифікацією адміністратора та шифрування управляючої інформації;

- ведення журналу аудиту.

Захист пристрою від НСД забезпечується шляхом [29]:

- безперервного контролю цілісності корпусу;

- блокування передачі інформації та знищення внутрішнього програмного забезпечення у разі виявлення спроби НСД;

- ведення журналів аудиту подій управління і стану функціонування пристрою (проходження інформації тощо);

- автентифікації адміністратора при доступі до функцій налаштування роботи пристрою (управління) та шифрування управляючої інформації під час віддаленої передачі.

Пристрій підтримує синхронізацію часу за протоколом NTP (Network Time Protocol – мережевий протокол часу) та може працювати в режимі NTP-клієнта (синхронізація часу від NTP-сервера у відкритому сегменті), NTP-сервера (для синхронізації часу на засобах користувачів у закритому сегменті) та одночасно NTP-клієнта і сервера. Управління пристроєм здійснюється віддалено з ЕОМ адміністратора через мережу після виконання протоколу автентифікації за паролем та з подальшим шифруванням

управляючої інформації при передачі.

Швидкість передачі OCSP-, TSP та CMP-запитів – не менше 250 Мбіт/с
із кількістю одночасних підключень – не менше 2500.

ЛІТЕРАТУРА

- 1 Закон України “Про платіжні системи та переказ грошей в Україні”. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2346-14#Text>
- 2 Закон України “Про захист інформації в інформаційно-комунікаційних системах”. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text>
- 3 Про внесення змін до Закону України “Про захист інформації в автоматизованих системах”. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2594-15#Text>
- 4 Закон України “Про електронні комунікації”. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/main/1089-20#Text>
- 5 Постанова правління НБУ “Про затвердження нормативно-правових актів з питань інформаційної безпеки” 26.11.2015 № 829. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/v0829500-15#n10>
- 6 PCI DSS. [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/PCI_DSS
- 7 Стандарт безопасности данных индустрии платежных карт. [Електронний ресурс]. – Режим доступу: https://ru.pcisecuritystandards.org/_onelink_/pcisecurity/en2ru/minisite/en/docs/PCI_DSS_v3_2_RU-RU_Final.pdf
- 8 THE U.E.P.S. TECHNOLOGY. [Електронний ресурс]. – Режим доступу: <http://www.net1.com/key-products/the-ueps-technology/>
- 9 ПРОСТІР (платіжна система). [Електронний ресурс]. – Режим доступу: [https://uk.wikipedia.org/wiki/ПРОСТІР_\(платіжна_система\)](https://uk.wikipedia.org/wiki/ПРОСТІР_(платіжна_система))
- 10 Горбенко І.Д. Прикладна криптологія. Теорія. Практика: монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Видавництво «Форт», 2012. – 880 с.
- 11 NCSC-TG-017. [Електронний ресурс]. – Режим доступу: <https://web.archive.org/web/20160303225728/http://ftp.fas.org/irp/nsa/rainbow/tg017.htm>
- 12 ISO/IEC 9798. [Електронний ресурс]. – Режим доступу: <https://www.iso.org/standards.html>
- 13 Закон України “Про електронні документи та електронний документообіг”. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/851-15#Text>

14 Закон України “Про електронні довірчі послуги”. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>

15 Горбенко Ю.І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія / Ю.І. Горбенко, І.Д. Горбенко. – Харків: Видавництво «Форт», 2010. – 608 с.

16 Захарченко М.В. Асиметричні методи шифрування в телекомунікаціях. – Криптографічні методи захисту інформації в телекомунікаційних системах та мережах: модуль 2 з дисципліни “Захист інформації в телекомунікаційних системах та мережах”: навч. посіб. / М.В. Захарченко, О.В. Онацький, Л.Г. Йона, Т.М. Шинкарчук. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 184 с.

17 FIPS PUB 186-4. [Електронний ресурс]. – Режим доступу: <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>

18 Peter Stavrulakis. Handbook of Information and Communication Security /Peter Stavrulakis, Mark Stamp // – Berlin: Springer-Verlag. – 2010. – 863 p.

19 Болотов А.А. Алгоритмические основы эллиптической криптографии / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.: Мэй, 2000. – 100 с.

20 Ростовцев А.Г. Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко. – М.: Профессионал, 2005. – 490 с.

21 Hankerson D. Guide to Elliptic Curve Cryptography / D. Hankerson, A. Menezes, S. Vanstone. – Springer-Verlag, 2004. – 358 p.

22 Болотов А.А. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. – М.: КомКнига, 2006. – 328 с.

23 Menezes A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 1996. – 816 p.

24 FIPS 186-2. [Електронний ресурс]. – Режим доступу: <https://csrc.nist.gov/csrc/media/publications/fips/186/2/archive/2000-01-27/documents/fips186-2.pdf>

25 ДСТУ 4145–2002. [Електронний ресурс]. – Режим доступу: <https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798>

26 An Elliptic Curve Cryptography (ECC) Primer why ECC is the next generation of public key cryptography The Certicom ‘Catch the Curve’ White Paper Series June 2004. – 24 p.

27 Онацький А.В. Анализ модификаций протоколов Шнорра и Окамото

на эллиптических кривых / А. В. Онацкий. // Восточно-Европейский журнал передовых технологий. – 2013. – № 6/9 (66) – С. 14-18.

28 Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0862-07#Text>

29 АТ “ІІТ”. Засоби та комплекси. [Електронний ресурс]. – Режим доступу: <https://iit.com.ua/products>

30 CryptoIP-459. [Електронний ресурс]. – Режим доступу: <https://avtor.ua/products/CryptoIP/CryptoIP-459>

31 ІР-шифратор “Хортиця”. [Електронний ресурс]. – Режим доступу: <https://avtor.ua/products/CryptoIP/Khortytsia>

Додаток А

ПЕРЕЛІК СТАНДАРТІВ ТА ТЕХНІЧНИХ СПЕЦИФІКАЦІЙ

У додатку А наводиться перелік стандартів та технічних специфікацій дозволених Адміністрацією державної служби спеціального зв'язку та захисту інформації (наказ № 687 від 27.10.2020 р.) України для реалізації в засобах криптографічного захисту інформації.

1. Стандарти, що визначають вимоги до **блокових шифрів** (block ciphers):

– ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення»;

– ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри»;

– ДСТУ ГОСТ 28147:2009 «Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования» (дата скасування 01.01.2022 р.);

– ДСТУ ISO/IEC 10116:2019 (ISO/IEC 10116:2017, IDT) «Інформаційні технології. Методи захисту. Режим роботи *n*-бітних блокових шифрів».

2. Стандарти, що визначають вимоги до **потоків шифрів** (stream ciphers):

– ДСТУ 8845:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення»;

– ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потоків шифри».

3. Стандарти, що визначають вимоги до **асиметричних криптографічних алгоритмів та методів** (asymmetric algorithms and techniques):

– ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння»;

– ДСТУ ISO/IEC 9796-2:2015 (ISO/IEC 9796-2:2010, IDT) «Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують

відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел»;

– ДСТУ ISO/IEC 9796-3:2015 (ISO/IEC 9796-3:2006, IDT) «Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі»;

– ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел»;

– ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні»;

– ДСТУ ISO/IEC 15946-5:2019 (ISO/IEC 15946-5:2017) «Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих»;

– ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри».

4. Стандарт, що визначає вимоги до *кодів автентифікації повідомлень* (message authentication codes):

– ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, IDT) «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми, що використовують спеціалізовану геш-функцію».

5. Стандарти, що визначають вимоги до *геш-функцій* (hash functions)

– ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування»;

– ДСТУ ISO/IEC 10118-2:2015 (ISO/IEC 10118-2:2010; Cor 1:2011, IDT) «Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш-функції, що використовують n -бітний блоковий шифр»;

– ДСТУ ISO/IEC 10118-3:2005 (ISO/IEC 10118-3:2004; Cor 1:2011, IDT) «Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції» (чинність змін до національних стандартів з 01 січня 2022 року);

– ДСТУ ISO/IEC 10118-4:2015 (ISO/IEC 10118-4:1998; Cor 1:2014; Amd 1:2014, IDT) «Інформаційні технології. Методи захисту. Геш-функції.

Частина 4. Геш-функції, що використовують модульну арифметику».

6. Стандарти, що визначають вимоги до **автентифікації сутності** (entity authentication):

– ДСТУ ISO/IEC 9798-1:2015 (ISO/IEC 9798-1:2010, IDT) «Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 1. Загальні положення»;

– ДСТУ ISO/IEC 9798-2:2021 (ISO/IEC 9798-2:2019, IDT) «Інформаційні технології. Методи безпеки ІТ. Автентифікація об'єктів. Частина 2. Механізми, що використовують автентифіковане шифрування» (на заміну ДСТУ ISO/IEC 9798-2:2015);

– ДСТУ ISO/IEC 9798-3:2021 (ISO/IEC 9798-3:2019, IDT) «Інформаційні технології. Методи безпеки ІТ. Автентифікація об'єктів. Частина 3. Механізми з використанням методу цифрового підпису» (на заміну ДСТУ ISO/IEC 9798-3:2002);

– ДСТУ ISO/IEC 9798-4:2015 (ISO/IEC 9798-4:1999; Cor 1:2009; Cor 2:2012, IDT) «Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 4. Методи, що використовують криптографічну перевіро́чну функцію»;

– ДСТУ ISO/IEC 9798-5:2015 (ISO/IEC 9798-5:2009, IDT) «Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 5. Механізми, що використовують методи нульової обізнаності»;

– ДСТУ ISO/IEC 9798-6:2015 (ISO/IEC 9798-6:2010, IDT) «Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 6. Механізми, що використовують ручне передавання даних».

7. Стандарти, що визначають вимоги до **управління ключами** (key management):

– ДСТУ ISO/IEC 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів»;

– ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів»;

– ДСТУ ISO/IEC 11770-4:2015 (ISO/IEC 11770-4:2008; Cor 1:2009, IDT) «Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми, засновані на нестійких секретах»;

– ДСТУ ISO/IEC 11770-6:2018 (ISO/IEC 11770-6:2016, IDT)
«Інформаційні технології. Методи захисту. Керування ключами. Частина 6.
Утворення ключів»;

– ДСТУ ISO/IEC 11770-5:2015 (ISO/IEC 11770-5:2008, IDT)
«Інформаційні технології. Методи захисту. Керування ключами. Частина 5.
Керування груповими ключами».

8. Стандарти, що визначають вимоги до *випадкової генерації біт*
(random bit generation):

– ДСТУ ISO/IEC 18031:2015 (ISO/IEC 18031:2011; Cor 1:2014, IDT)
«Інформаційні технології. Методи захисту. Генерування випадкових бітів».

9. Стандарти, що визначають вимоги до *методів встановлення
чутливих параметрів безпеки* (sensitive security parameter establishment
methods):

– ДСТУ ISO/IEC 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT)
«Інформаційні технології. Методи захисту. Керування ключами. Частина 2.
Механізми з використанням симетричних методів»;

– ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT)
«Інформаційні технології. Методи захисту. Керування ключами. Частина 3.
Механізми з використанням асиметричних методів».

10. Стандарти та технічні специфікації, що визначають вимоги до
форматів криптографічних повідомлень:

– RFC 5652 «Cryptographic Message Syntax (CMS)» з використання
криптографічних алгоритмів згідно з RFC 3370 «Cryptographic Message
Syntax (CMS) Algorithms» або Технічних специфікацій до RFC 5652.

Додаток Б

НЕЗВЕДЕНІ ПОЛІНОМИ НАД ПОЛЕМ ГАЛУА $GF(2)$

Таблиця Б1 – Незведені поліноми над полем Галуа $GF(2)$

№	Сте- пінь m	Подання поліному	№	Сте- пінь m	Подання поліному
1	1	$x + 1$	32		$x^{31} + x^3 + 1$
2	3	$x^3 + x + 1$	33	31	$x^{31} + x^6 + 1$
3		$x^3 + x^2 + 1$	34		$x^{31} + x^7 + 1$
4		$x^5 + x^2 + 1$	35	37	$x^{37} + x^6 + x^4 + x + 1$
5	5	$x^5 + x^3 + 1$	36	41	$x^{41} + x^3 + 1$
6		$x^5 + x^3 + x^2 + x + 1$	37		$x^{41} + x^{20} + 1$
7		$x^5 + x^4 + x^2 + x + 1$	38	43	$x^{43} + x^6 + x^4 + x^3 + 1$
8		$x^5 + x^4 + x^3 + x + 1$	39	47	$x^{47} + x^5 + 1$
9		$x^5 + x^4 + x^3 + x^2 + 1$	40		$x^{47} + x^{14} + 1$
10	7	$x^7 + x + 1$	41		$x^{47} + x^{20} + 1$
11		$x^7 + x^3 + 1$	42		$x^{47} + x^{21} + 1$
12		$x^7 + x^3 + x^2 + x + 1$	43	53	$x^{53} + x^6 + x^2 + x + 1$
13		$x^7 + x^4 + 1$	44	61	$x^{61} + x^5 + x^2 + x + 1$
14		$x^7 + x^4 + x^3 + x^2 + 1$	45	63	$x^{63} + x + 1$
15		$x^7 + x^5 + x^2 + x + 1$	46		$x^{63} + x^5 + 1$
16		$x^7 + x^5 + x^3 + x + 1$	47		$x^{63} + x^{11} + 1$
17		$x^7 + x^5 + x^4 + x^3 + 1$	48		$x^{63} + x^{28} + 1$
18		$x^7 + x^6 + 1$	49		$x^{63} + x^{31} + 1$
19		$x^7 + x^6 + x^3 + x + 1$	50	67	$x^{67} + x^5 + x^2 + x + 1$
20		$x^7 + x^6 + x^4 + x + 1$	51	71	$x^{71} + x^6 + 1$
21		$x^7 + x^6 + x^4 + x^2 + 1$	52		$x^{71} + x^9 + 1$
22		$x^7 + x^6 + x^5 + x^2 + 1$	53		$x^{71} + x^{18} + 1$
23		$x^7 + x^6 + x^5 + x^4 + 1$	54		$x^{71} + x^{20} + 1$
24	11	$x^{11} + x^2 + 1$	55		$x^{71} + x^{35} + 1$
25	13	$x^{13} + x^4 + x^3 + x + 1$	56	73	$x^{73} + x^{25} + 1$
26	17	$x^{17} + x^3 + 1$	57		$x^{73} + x^{28} + 1$
27		$x^{17} + x^5 + 1$	58		$x^{73} + x^{31} + 1$
28	19	$x^{19} + x^5 + x^2 + x + 1$	59	79	$x^{79} + x^9 + 1$
29	23	$x^{23} + x^5 + 1$	60		$x^{79} + x^{19} + 1$
30		$x^{23} + x^9 + 1$	61	83	$x^{83} + x^7 + x^4 + x^2 + 1$
31	29	$x^{29} + x^2 + 1$	62	89	$x^{89} + x^{38} + 1$

Додаток В

РЕКОМЕНДОВАНІ ПРИМІТИВНІ МНОГОЧЛЕНИ ЗГІДНО ДСТУ 4145–2002

Згідно ДСТУ 4145–2002 дозволено задавати основне поле поліноміальним або оптимальним нормальним базисом. Якщо використовують поліноміальний базис, то основне поле треба обирати з-посеред полів $GF(2^m)$, степені яких подано у табл. В.1. Поліноміальний базис задають примітивними тричленами чи примітивними п'ятичленами.

Таблиця В.1 – Припустимі основні поля з поліноміальним базисом і рекомендовані примітивні многочлени

№	Степінь поля m	Примітивний многочлен	№	Степінь поля m	Примітивний многочлен
1	163	$x^{163} + x^7 + x^6 + x^3 + 1$	31	337	$x^{337} + x^{10} + x^6 + x + 1$
2	167	$x^{167} + x^6 + 1$	32	347	$x^{347} + x^{17} + x^6 + x + 1$
3	173	$x^{173} + x^{10} + x^2 + x + 1$	33	349	$x^{349} + x^6 + x^5 + x^2 + 1$
4	179	$x^{179} + x^4 + x^2 + x + 1$	34	353	$x^{353} + x^{26} + x^7 + x^3 + 1$
5	181	$x^{181} + x^7 + x^6 + x + 1$	35	359	$x^{359} + x^{18} + x^4 + x^2 + 1$
6	191	$x^{191} + x^9 + 1$	36	367	$x^{367} + x^{21} + 1$
7	193	$x^{193} + x^{15} + 1$	37	373	$x^{373} + x^9 + x^6 + x + 1$
8	197	$x^{197} + x^{21} + x^2 + x + 1$	38	379	$x^{379} + x^{17} + x^6 + x + 1$
9	199	$x^{199} + x^{11} + x^2 + x + 1$	39	383	$x^{383} + x^9 + x^5 + x + 1$
10	211	$x^{211} + x^{12} + x^6 + x + 1$	40	389	$x^{389} + x^{17} + x^{10} + x + 1$
11	223	$x^{223} + x^{12} + x^2 + x + 1$	41	397	$x^{397} + x^{22} + x^3 + x + 1$
12	227	$x^{227} + x^{21} + x^2 + x + 1$	42	401	$x^{401} + x^{29} + x^4 + x + 1$
13	229	$x^{229} + x^{21} + x^2 + x + 1$	43	409	$x^{409} + x^{15} + x^6 + x + 1$
14	233	$x^{233} + x^9 + x^4 + x + 1$	44	419	$x^{419} + x^{21} + x^{14} + x + 1$
15	239	$x^{239} + x^{15} + x^2 + x + 1$	45	421	$x^{421} + x^7 + x^4 + x + 1$
16	241	$x^{241} + x^{15} + x^4 + x + 1$	46	431	$x^{431} + x^6 + x^3 + x + 1$
17	251	$x^{251} + x^{14} + x^4 + x + 1$	47	433	$x^{433} + x^{15} + x^5 + x + 1$
18	257	$x^{257} + x^{12} + 1$	48	439	$x^{439} + x^8 + x^3 + x^2 + 1$
19	263	$x^{263} + x^{27} + x^2 + x + 1$	49	443	$x^{443} + x^{28} + x^3 + x + 1$
20	269	$x^{269} + x^7 + x^6 + x + 1$	50	449	$x^{449} + x^{25} + x^5 + x^3 + 1$
21	271	$x^{271} + x^{16} + x^3 + x + 1$	51	457	$x^{457} + x^{16} + 1$
22	277	$x^{277} + x^{23} + x^3 + x^2 + 1$	52	461	$x^{461} + x^{23} + x^4 + x + 1$
23	281	$x^{281} + x^9 + x^4 + x + 1$	53	463	$x^{463} + x^{24} + x^6 + x + 1$
24	283	$x^{283} + x^{26} + x^9 + x + 1$	54	467	$x^{467} + x^{28} + x^3 + x + 1$
25	293	$x^{293} + x^{11} + x^6 + x + 1$	55	479	$x^{479} + x^{25} + x^6 + x + 1$
26	307	$x^{307} + x^8 + x^4 + x^2 + 1$	56	487	$x^{487} + x^{15} + x^2 + x + 1$
27	311	$x^{311} + x^{29} + x^4 + x + 1$	57	491	$x^{491} + x^{17} + x^6 + x^2 + 1$
28	313	$x^{313} + x^7 + x^3 + x + 1$	58	499	$x^{499} + x^{29} + x^6 + x^2 + 1$
29	317	$x^{317} + x^9 + x^5 + x^2 + 1$	59	503	$x^{503} + x^3 + 1$
30	331	$x^{331} + x^{12} + x^5 + x^2 + 1$	60	509	$x^{509} + x^{23} + x^3 + x^2 + 1$

Навчальне видання

Лариса Григорівна ЙОНА
Олексій Віталійович ОНАЦЬКИЙ
Оксана Володимирівна ШВЕЦЬ

СИСТЕМИ БАНКІВСЬКОЇ БЕЗПЕКИ

Навчальний посібник

Редактор *Кодрул Л.А.*

ДЛЯ НОТАТОК



Йона Лариса Григорівна

Кандидат технічних наук, доцент кафедри кібербезпеки та технічного захисту інформації державного університету інтелектуальних технологій і зв'язку.

У 1988 році закінчила Одеський електротехнічний інститут зв'язку ім. О.С. Попова за фахом інженер автоматичного електрозв'язку.

З 1991 по 1994 рік навчалась на очному відділенні та закінчила повний курс аспірантської підготовки Одеського електротехнічного інституту зв'язку ім. О.С. Попова за спеціальністю 05.12.02 – Телекомунікаційні системи та управління ними. У 1996 році захистила дисертацію на здобуття вченого ступеня кандидата технічних наук.

Автор понад 35 науково-методичних праць з напрямку комунікацій та інформаційної безпеки.



Онацький Олексій Віталійович

Кандидат технічних наук, доцент кафедри кібербезпеки та технічного захисту інформації державного університету інтелектуальних технологій і зв'язку.

В 1995 році закінчив Одеський державний політехнічний інститут за фахом радіотехніка.

З 1995 по 1998 рік навчався в аспірантурі Української державної академії зв'язку ім. О.С. Попова за спеціальністю 05.12.13 – Радіотехнічні пристрої та засоби телекомунікацій. У 1999 році захистив кандидатську дисертацію.

Автор понад 80 науково-методичних праць з проблем комунікацій та інформаційної безпеки.



Шведь Оксана Володимирівна

Старший викладач кафедри кібербезпеки та технічного захисту інформації державного університету інтелектуальних технологій і зв'язку.

У 2007 році закінчила Одеську національну академію зв'язку ім. О.С. Попова за спеціальністю «Телекомунікаційні системи та мережі».

З 2009 по 2012 рік навчалась в аспірантурі Одеської національної академії зв'язку ім. О.С. Попова за спеціальністю 05.12.13 – Радіотехнічні пристрої та засоби телекомунікацій.

Автор 13 наукових робіт і 4 робіт навчально-методичного напрямку.