МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра комп'ютерної інженерії та інноваційних технологій

Пояснювальна записка

до кваліфікаційної роботи
другого (магістерського) рівня

на тему **ДОСЛІДЖЕННЯ КРИПТОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ**

Виконав: студент 2 курсу, групи КТК-2.1
спеціальності 125 Кібербезпека

Кравченко І. А.

Керівник Йона Л.Г.

Рецензент Григор'єва Т.І.

Одеса – 2023

ДОВІДКА

кафедри КІ та ІТ про виконану магістерську роботу

студентки 2 курсу ФКПІ та КН групи КТК-2.1

Кравченко Ірини Аркадієвни

на тему Дослідження криптографічних методів захисту інформації в системах банківської безпеки

Висновок нормоконтролера наскрізна зашена до кваліфікаційної роботи виконано з коректними посиланнями ДСТУ. Оформлено згідно вимог внутрішнього положення НТУ

Нормоконтролер к.т.н., доцент _____ В.В. Педан

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

Висновок відповідального за наявність плагіату згідно з сертифікатом ID 1015712723 унікальність роботи підтверджено

Відповідальна особа к.т.н., доцент _____ В.В. Педан

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

Попередня експертиза (захист) магістерської роботи

(бакалаврської роботи чи магістерської роботи)

студ. Кравченко І. А. проведена "12" грудня 2023 р.

(прізвище і.б.)

Висновки Розділи МР відповідають завданню, усі пункти завдання виконано. Текстова та графічна частина роботи виконані згідно вимог до її оформлення. Проаналізовано методи забезпечення конфіденційності та цілісності електронних документів при передачі інформації. Запропоковано удосконалення процесу шифрування за створеним ключем шифрування методом тензорного аналізу. МР відповідає вимогам до КР за заявленою спеціальністю та може бути рекомендована до захисту в ДЕК

Члени комісії _____ к.т.н., доцент Шока І.Г.

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

_____ к.т.н., доцент Педан В.В.

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

_____ вик. каф. КІ та ІТ Швець О.З.

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

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра комп'ютерної інженерії та інноваційних технологій
Освітній ступінь магістр
Галузь знань 12 Інформаційні технології
Спеціальність 125 Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри КТта ІТ
к.т.н., доц. Л.Г.Йона
"25" 09 2023 року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ РОБОТУ

Кравченко Ірини Аркадієвни

1. Тема роботи: Дослідження криптографічних методів захисту інформації в системах банківської безпеки

керівник роботи доцент Йона Л. Г.
затверджені наказом закладу вищої освіти від 25.09.2023р. №1951

2. Строк подання студентом роботи 11.12.2023

3. Вихідні дані до роботи:
Дослідити сучасні методи криптографічного захисту інформації за призначенням.

4. Зміст розрахунково-пояснювальної записки
Розділ 1: Захист інформації у банківських системах.
Розділ 2: Сучасні криптографічні алгоритми захисту електронного документообігу.
Розділ 3: Алгоритми ідентифікації та автентифікації.

5. Перелік графічного матеріалу (з зазначенням обов'язкових креслень)
Слайд 1 – Титульний слайд

Слайд 2 - мета роботи

Слайд 3 – Схема функціонування електронної платіжної системи

Слайд 4 – типи атак на банкывські системи

Слайд 5 – атаки на банківські системи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Завдання видав	Завдання прийняв

7. Дата видачі завдання 26.09.2023

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Вступ	25.09.23 – 04.10.2023	Вик
2	Розділ 1 Захист інформації у банківських системах.	05.10.23 – 11.10.2023	Вик
3	Розділ 2 Сучасні криптографічні алгоритми захисту електронного документообігу	12.10.23 – 25.10.2023	Вик
4	Розділ 3 Алгоритми ідентифікації та автентифікації.	26.10.23 – 04.11.2023	Вик
5	Висновки та рекомендації	05.11.23 – 25.11.2023	Вик
6	Перелік джерел посилання, Додаток А	26.11.23 – 08.12.2023	Вик

Студентка _____ Кравченко І.А.
(підпис)

Керівник роботи _____ _Йона Л.Г
(підпис)

ВІДГУК

на магістерську роботу студентки Кравченко І. А.

на тему: **«Дослідження криптографічних методів захисту інформації в системах банківської безпеки»**

Тема магістерської роботи здобувачки Кравченко І. А. пов'язана з проблемою захисту інформації в банківських системах.

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 справжності користувача та документа за допомогою протоколів автентифікації.

Криптографія вивчає методи захисту інформації, яка передається загальнодоступними каналами. При цьому каналом зв'язку передається вже не сама інформація, а результат її перетворення за допомогою шифрування, що не дозволяє неправочинному користувачеві прочитати її без знання ключа шифрування. Крім того, особливу увагу потребує захист електронного документообігу за допомогою сучасних технологій здійснення електронних транзакцій.

В магістерській роботі Кравченко І.А. надається результат дослідження сучасних криптографічних методів та аналіз систем захисту інформації від неправочинних користувачів. З ціллю підвищення ефективності засобів захисту конфіденційної інформації, пропонується здійснювати шифрування повідомлення за допомогою операцій тензорного аналізу. У магістерській роботі використані авторські матеріали Міжнародної конференції «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2023) за темою «Захист конфіденційної інформації шляхом шифрування на основі тензорних методів».

В процесі виконання магістерської роботи здобувачка Кравченко І.А. показала добру підготовку з питань статистичної теорії зв'язку, знання систем та пристроїв обробки інформації, уміння працювати з літературою.

Рівень підготовки Кравченко І.А. заслуговує оцінки „відмінно".

Вважаю, що здобувач Кравченко І.А. заслуговує присвоєння за заявленою спеціальністю 125 Кібербезпека кваліфікації магістр з кібербезпеки.

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

РЕЦЕНЗІЯ

на магістерську роботу студента Кравченко І. А.

на тему: «Дослідження криптографічних методів захисту інформації в системах банківської безпеки»

У магістерській роботі студентки Кравченко І. А. розглянуто сучасні алгоритми, які використовуються для захисту інформації в банківських системах, зокрема в електронних платіжних системах.

Актуальність питання полягає в тому, що в роботі досліджуються сучасні алгоритми криптографічного захисту інформації за їх призначенням.

Одним із напрямів дослідження є системи електронних платежів і розрахунків. На сьогодні форми електронних платежів швидко розвиваються. Отже, розвиток технологій електронних платежів потребує використання сучасних методів захисту електронних транзакцій в платіжних системах.

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

Проте в роботі є деякі недоліки:

- не достатньо розглянуто аналіз асиметричних алгоритмів шифрування;

- розглянуто замало алгоритмів електронного підпису.

Але вказані недоліки не знижують цінності виконаної роботи.

Магістерська робота відповідає вимогам до випускних кваліфікаційних робіт магістрів та заслуговує оцінки «відмінно».

Здобувач Кравченко І. А. заслуговує присвоєння за заявленою спеціальністю 125 Кібербезпека кваліфікації магістр з кібербезпеки

Рецензент
Доцент кафедри
Інформаційних технологій Григор'єва Т.І.

UNICHECK
by Turnitin

Имя пользователя:
Анна Серединко

ID проверки:
1016024121

Дата проверки:
20.12.2023 16:52:45 EET

Тип проверки:
Doc vs Internet + Library

Дата отчета:
28.12.2023 16:08:41 EET

ID пользователя:
100001433

Название файла: МР Кравченко І.А. (3)

Количество страниц: 58 Количество слов: 9558 Количество символов: 75137 Размер файла: 19.94 MB ID файла: 1015712723

29.7% Совпадения

Наибольшее совпадение: 10.2% с Интернет-источником (http://dspace.onua.edu.ua/bitstream/handle/11300/26277/%d...

24% Источники из Интернета | 541 ..... Страница 60

9.44% Источники из Библиотеки | 43 ..... Страница 63

0% Цитат

Исключение цитат выключено

Исключение списка библиографических ссылок выключено

8.31% Исключений

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

8.2% Исключений из Интернета | 179 ..... Страница 64

0.1% Исключенного текста из Библиотеки | 2 ..... Страница 64

Модификации

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

Замененные символы | 20

РЕФЕРАТ

Текстова частина магістерської роботи: 57 с., 11 рисунків, 1 таблиця, 1 додаток, 16 слайдів, 22 джерел.

АВТЕНТИФІКАЦІЯ, ЕЛЕКТРОННІ ТРАНЗАКЦІЇ, ЕЛЕКТРОННИЙ ПІДПИС, ЗАХИСТ БАНКІВСЬКИХ СИСТЕМ, ЗАХИСТ ДОКУМЕНТООБІГУ, КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, BANKID.

Об'єкт дослідження – банківська система захисту інформації.

Мета роботи – провести аналітичне дослідження сучасних криптографічних методів захисту інформації в банківських системах. Розглянути забезпечення конфіденційності електронних документів при передачі, методи ідентифікації, підтвердження справжності клієнта та даних системою банківського дистанційного обслуговування.

Метод дослідження – аналітичний з використанням комп'ютерних технологій.

У магістерській роботі описані сучасні методи криптографічного захисту документообігу. Розглянута структура банківських систем, види атак на банківські системи та методи їх захисту. Проаналізовані методи забезпечення конфіденційності електронних документів при передачі по відкритим каналам зв'язку та технології захисту електронних транзакцій, методи ідентифікації, методи підтвердження справжності банківських даних при використанні систем дистанційного банківського обслуговування, реалізацію системи BankID та електронного підпису.

ABSTRACT

Text part of the master's thesis: 57 p., 22 figures, 1 table, 1 appendix, 22 sources.

AUTHENTICATION, ELECTRONIC TRANSACTIONS, ELECTRONIC SIGNATURE, PROTECTION OF BANKING SYSTEMS, PROTECTION OF DOCUMENT FLOW, CRYPTOGRAPHIC PROTECTION OF INFORMATION, BANKID.

The object of research is the banking information security system.

Purpose – to conduct an analytical study of modern cryptographic methods of information security in banking systems. To consider ensuring the confidentiality of electronic documents during transmission, methods of identification, authentication of the client and data by the system of distance banking services.

The research method is analytical with the use of computer technologies.

The master's thesis describes modern methods of cryptographic protection of document flow. The structure of banking systems, types of attacks on banking systems and methods of their protection are considered. The methods of ensuring the confidentiality of electronic documents when transmitted over open communication channels and technologies for protecting electronic transactions, identification methods, methods of confirming the authenticity of banking data when using remote banking systems, implementation of the BankID system and electronic signature are analysed.

ЗМІСТ

ВСТУП..... 9

1ЗАХИСТ ІНФОРМАЦІЇ У БАНКІВСЬКИХ СИСТЕМАХ..... 11

1.1 Структура банківських систем..... 11

1.2 Електронна платіжна система..... 11

1.3 Особливості захисту банківських систем.....15

1.3.1 Різновиди атак на банківську систему 16

1.3.2 Методи захисту банківських систем 18

2 СУЧАСНІ КРИПТОГРАФІЧНІ АЛГОРИТМИ ЗАХИСТУ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ.....20

2.1 Види криптографічних алгоритмів 20

2.2 Захист конфіденційної інформації шляхом шифрування 20

2.3 Захист інформації в електронних банківських системах 20

2.4 Підтвердження справжності даних при використанні систем дистанційного банківського обслуговування 25

3 АЛГОРИТМИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ..... 29

3.1 Ідентифікація та автентифікація користувача..... 29

3.2 Автентифікація документів за допомогою електронного підпису..... 35

3.2.1 Алгоритм електронного підпису RSA..... 42

3.2.2 Алгоритм електронного підпису Ель-Гамаля 44

3.3 Система автентифікації BankID..... 45

3.4 Побудова системи автентифікації користувача..... 47

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ..... 52

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ..... 53

Додаток А ПЕРЕЛІК КОПІЙ ДЕМОНСТРАЦІЙНОГО МАТЕРІАЛУ

ВСТУП

Задачі захисту інформації від несанкціонованого доступу та захисту електронного документообігу залежать від стану та розвитку обчислювальної техніки. Нові методи обробки і зберігання інформації, а також сучасні відкриті мережі відкрили безліч можливостей, як для бізнесу, так і для звичайних користувачів у повсякденному житті.

З появою глобальних комп’ютерних мереж доступ до інформації став дуже простим. В той же час легкість та швидкість такого доступу значно підвищує загрозу несанкціонованого використання інформації, тому питання надійного захисту авторських прав, прав інтелектуальної власності або конфіденційних даних є надзвичайно актуальними. Особливо це стосується банківських систем, зокрема захисту інформації при здійсненні електронного документообігу та електронних транзакцій. Величезний обсяг інформації та різноманітних послуг надається через мережу Інтернет, без необхідності безпосередньої зустрічі з людиною, що їх замовляє. Наявність процедур ідентифікації та автентифікації користувачів для обмеження доступу незаконних суб'єктів (користувачі, процеси) інформаційних систем до її об'єктів (апаратні, програмні та інформаційні ресурси) є обов'язковою умовою будь-якої захищеної системи, оскільки всі механізми захисту інформації розраховані на роботу з пойменованими суб'єктами і об'єктами інформаційних систем. Алгоритм роботи таких систем полягає в тому, щоб отримати від користувача таку інформацію, яка дозволила би перевірити справжність особи, а потім надати (або не надати) цьому користувачеві допуск до системи для можливості подальшої роботи.

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

1 ЗАХИСТ ІНФОРМАЦІЇ У БАНКІВСЬКИХ СИСТЕМАХ

1.1 Структура банківських систем

Впродовж останніх років світова банківська система суттєво змінювалася і ці зміни обумовлені розвитком інформаційних технологій, збільшенням пропозицій банківських послуг, впровадженням інноваційних технологій в керуванні банками.

Структуру банку визначають зовнішні вимоги та особливості його роботи.

До зовнішніх умов відносяться [1]:

- вказівки власників банку;
- цілі створення даної конкретної організації;
- її місце в фінансово-економічній системі країни або регіону.

Серед внутрішніх аспектів роботи банку особливо важливими є:

- основні напрямки діяльності: кредитування, залучення коштів у внески, розрахункові та обмінні операції;
- масштаб діяльності банку: один або кілька близьких міст, представництва в регіонах країни, міжнародні структури;
- найважливіші категорії клієнтів банку: приватні особи, виробничі або торгові підприємства, окремі галузі і ін.

Єдиного підходу, шаблону для банківської структури не зустрічається, але є деякі загальні принципи.

Можна виділити кілька підходів до побудови внутрішнього середовища банку:

- виходячи з напрямків діяльності, основних функцій;
- орієнтуючись на головних зовнішніх споживачів банківського продукту;
- поєднуючи в собі два перші варіанти, згідно конкретної ситуації.

В спектрі банківських операцій зручно поєднувати роботу з приватними особами у відділі роздрібних операцій, а сервісними організаціями – у відділі корпоративного бізнесу.

Внутрішня система комерційного банка може бути представлена так:

- Вище керівництво банком призначає виконавчі органи і контролює їх діяльність.

- Правління банку на чолі з головою - елемент поточного, оперативного управління. У його підпорядкуванні знаходяться керівники всіх інших підрозділів.

- Управління роздрібного бізнесу. Відділи, які обслуговують приватних осіб: кредитування, валютно-обмінні операції, прийом вкладів, операції з банківськими картами.

- Управління корпоративного бізнесу виконує роботу з організаціями. Кредитування, залучення коштів, виробництво платежів та інших розрахунків, залучення коштів організацій на депозити.

- Управління безпеки і контролю. Відділи з такими завданнями можуть входити до складу двох наведених вище управлінь або мати єдине керівництво. Часто контроль, внутрішню і зовнішню безпеку поділяють між декількома окремими управліннями.

- Управління міжбанківських комунікацій. Такий підрозділ можна вважати за необхідне на сучасному етапі консолідації банківської системи. Для роботи з банками-партнерами, конкурентами та всіма іншими кредитними установами створюється особливе управління, або ці функції залишаються у віданні керівництва банку.

- Бухгалтерія. Структура обов'язкова для будь-якого господарюючого суб'єкта, і завжди має єдине керівництво.

- Управління операцій на фондовому ринку. В розпорядженні банків, на різних умовах, виявляються цінні папери багатьох підприємств і держав. Для звернення з цими активами банки можуть формувати спеціальні служби.

- Юридичне управління. Існує у всіх банках, має в своїй назві вказівку на спеціалізацію і єдине керівництво.

- Управління розвитку. Сюди відносяться елементи системи пов'язані з пошуком нових ринків, клієнтів, напрямків і способів доходу. Відділи розвитку

створюються при різних управліннях або об'єднуються в єдину службу при тісній взаємодії з іншими підрозділами.

- Піар і реклама. Ці напрямки можуть виділятися в окремі банківські структури, можуть об'єднуватися з управлінням розвитку, або підкорятися підрозділам, орієнтованим на певних клієнтів.
- Управління інформаційних технологій. По міру комп'ютеризації систем обробки інформації та розвитком віддаленого управління, подібні служби стали обов'язковою частиною будь-якої банківської структури. Вони взаємодіють з усіма відділами, але зазвичай складають єдину систему.
- Регіональні підрозділи. Такі елементи притаманні великим банкам. Система управління в них варіюється за кількома критеріями. Іноді регіональні підрозділи дублюють в своєму складі всі перераховані вище управління і служби, іноді займаються тільки деякі напрямки, наприклад – роботу з фізичними особами.
- Галузеві управління. Створюються не завжди, але можуть бути необхідні банкам, які мають особливі інтереси в певних галузях або масового споживача в одній сфері діяльності: сільському господарстві, міжнародної торгівлі, енергетиці та ін.

На сьогодні форми електронних платежів швидко розвиваються. Однією із послуг є створення систем електронних платежів і розрахунків. Розвиток технологій електронних платежів потребує використання сучасних методів захисту електронних транзакцій в платіжних системах.

1.2 Електронна платіжна система

Електронною платіжною системою (ЕПС) є система, де платіжним інструментом використовують пластикові картки.

Платіжна система може здійснювати операції як за допомогою готівки, так і безготівковими засобами. Існує багато різних електронних платіжних систем, серед них Visa, MasterCard, EasyPay, Portmone, iPay та ін.

Проте не можна обрати таку домінуючу систему в різних напрямах, тому готівки та платіжні карткивикористовуються разом з електронними аналогами. В Україні частіше використовуються системи Visa та MasterCard.

Платіжна картка – це є інструмент, що дає змогу його власнику виконувати безготівкову оплату платіж товару чи отримання готівки в банкоматах.

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.

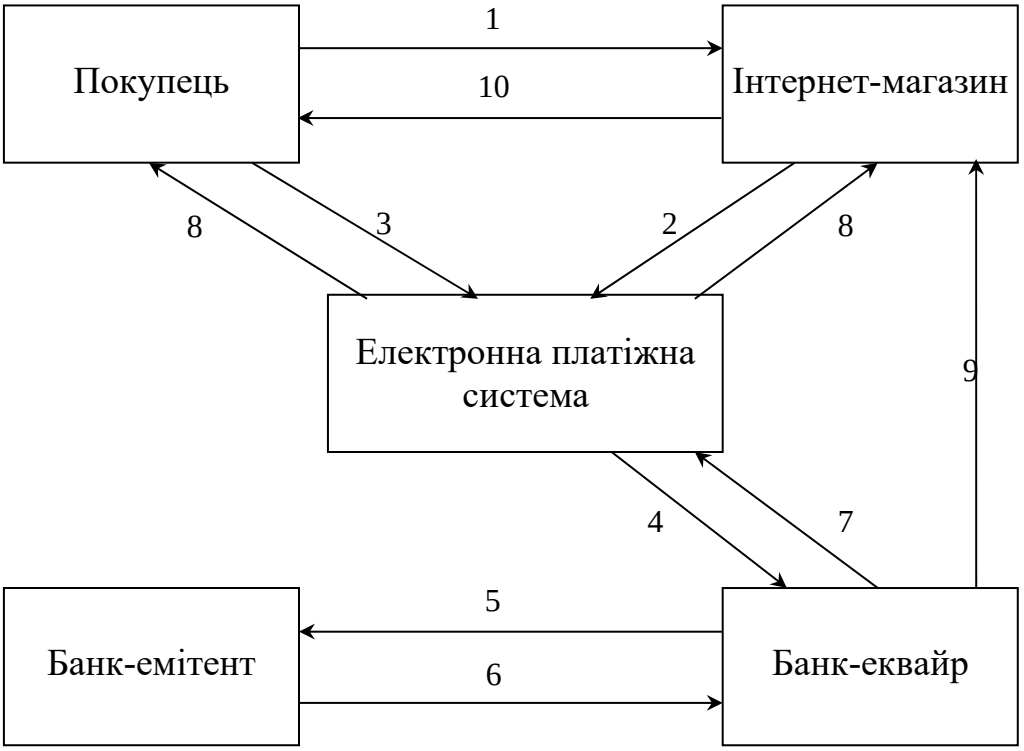
Банк-еквайр – здійснює фінансові операції, пов'язані з виконанням розрахунків і платежів точками обслуговування (підприємствами торгівлі та сервісу, відділеннями банків, що приймають пластикову картку як платіжнийінструмент).

Розрахунковий банк забезпечує проведення в платіжній системі взаєморозрахунків між банками еквайрами й емітентами.

Транзакція – це здійснення безготівкових операцій між рахунками чи видачі готівки в банкоматах.

Інтернет-еквайринг – процес здійснення оплати платіжною карткою системою дистанційного банківського обслуговування

Схема роботи ЕПС показана на рис. 1.1 [2].



1- Запит на оплату товару
2- Перенаправлення на сервер платежів
3- Введення даних платіжної картки
4,5 – Процедура авторизації
6,9 – Переказ коштів
7,8 – Результат процедури авторизації
10 – Видача товару чи послуги

Рисунок 1.1 – Схема роботи електронної платіжної системи.

1.3 Особливості захисту банківських систем

Інтенсивне використання глобальної мережі виявило проблеми, які пов’язані з інформаційною безпекою, а саме:

– необхідність захисту інформації, що передається каналами зв’язку;

– 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.

Захист інформації в банках являє собою складну проблему, яка має специфічні особливості, які не притаманні іншим системам.

Можна сформулювати основні вимоги до банківської системи:

1) технічне оснащення банку має бути на найвищому рівні;
2) персонал банку повинен постійно проходити навчання та підвищення кваліфікації щодо правил поведінки для мінімізації загроз витоку інформації.

Рисунок 1.2 - Внутрішні джерела загроз банківській системи

1.3.1 Різновиди атак на банківську систему

Великі банки сьогодні приділяють багато уваги захисту периметра своєї мережі, тому організувати атаку на сервери або веб-додатки складно. Найпоширенішим та найефективнішим методом проникнення в інфраструктуру банку є фішингові електронні листи на адресу співробітників банку, які надсилаються як на ділові адреси, так і на особисті.

Ще одним варіантом початкового розповсюдження шкідливого програмного забезпечення є хакерство сторонніх компаній шляхом зараження сайтів, які часто відвідують банківські службовці.

Типи атак на банківськи системи :

- Фішинг;
- Скімінг;
- Кардинг;
- Віруси та шкідливі програми;
- DDoS-атаки;
- Злам рахунків;
- Шахрайські дії;
- Соціальна інженерія;
- Тощо

Якщо злочинці отримають доступ до локальної мережі банку, для подальшого розвитку атаки їм потрібно отримати права адміністратора системи.

Етапи атаки на банківські системи:

- Розвідка та підготовка;
- Проникнення у внутрішню мережу;
- Розвиток атаки і закріплення в мережі;
- Компрометація банківських систем і розкрадання грошей;
- Приховування слідів.

Після закріплення в мережі зловмисники мають знати, на яких вузлах знаходяться банківські системи та як отримати до них доступ.

Найпоширеніші вразливості:

- використання застарілих версій програмного забезпечення;
- множинні помилки конфігурації;
- використання простих паролів;
- відсутність багатофакторної автентифікації для доступу до систем.

Злочинці можуть тривалий час залишатися в інфраструктурі банку, залишаючись непоміченими, збираючи інформацію про інфраструктуру та процеси.

Крадіжку грошей можна запобігти, якщо вчасно виявити факт втручання.

Основними способами розкрадань є:

- переказ коштів на підставні рахунки через системи міжбанківських платежів;
- переказ грошових коштів на криптовалютні гаманці;
- управління банківськими картами і рахунками;
- управління процесом видачі готівки в банкоматах.

З метою ускладнення розслідування інциденту злочинці вживають заходів щодо знищення слідів перебування в системі. Незважаючи на те, що зловмисники переходять на використання сценаріїв, що працюють в оперативній пам'яті, система залишається ознаками їх присутності: записи в журналах подій, зміни в реєстрі та інші підказки. Зашифровані дані в більшості випадків відновити не вдається, тоді банк зазнає збитків, спричинених вимушеним простоєм бізнес-процесів, що може бути значно більшим збитком ніж від крадіжки коштів.

1.1.1 Методи захисту банківських систем

Електронна платіжна система крім інших видів захисту має використовувати криптографічний, який повинен відповідати стандартним вимогам: криптостійкі алгоритми, захист від імітації, стійкі до компромісів ключові системи та інші. Проте, платіжна система має низку специфічних особливостей, які пред'являють додаткові вимоги до засобів криптографічного захисту як технічно, так і організаційно. При цьому необхідно пам’ятати про використання лише сертифікованих криптографічних систем.

Систему інформаційної безпеки зазвичай ділять на дві частини: захист периметра обчислювальної мережі організації і захист внутрішніх хостів.

Захист периметра мережі:

- Міжмережеве екранування
- Системи виявлення та запобігання атак (IDS/IPS)
- Контроль поштового та web-трафіку
- Антивірусні засоби на поштовому та проксі-сервері і ряді інших

пристроїв

Захист внутрішніх хостів:

- Антивірусні засоби
- Персональні МСЕ
- Хостові модулі систем IDS/IPS
- Хостові модулі DLP-систем
- Засоби контролю периферійних пристроїв

2 СУЧАСНІ КРИПТОГРАФІЧНІ АЛГОРИТМИ ЗАХИСТУ

ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

2.1 Види криптографічних алгоритмів

Криптографічним захистом інформації є перетворення початкової інформації за допомогою спеціальних даних (а саме ключових даних) для шифрування та відновлення повідомлення чи підтвердження його справжності.

У класичних методах криптографії використовується тільки одна одиниця секретної інформації – ключ, знання якого дозволяє відправникові зашифрувати інформацію, а одержувачеві – розшифрувати її. Крім того, пара ключів в несиметричних криптосистемах застосовується для процедури автентифікації. Наприклад, для формування цифрового підпису, тобто підписання документу відправником, застосовується секретний ключ, а перевірка підпису здійснюється одержувачем за допомогою відкритого ключа. Саме операції розшифровування та постановки підпису нездійсненні без знання секретного ключа. Використання криптографії дає можливість бути впевненим у конфіденційності, цілісності, справжності інформації, захисті авторського права тощо.

2.2 Захист конфіденційної інформації шляхом шифрування

У сучасному світі інформаційних технологій, при обміні документами по незахищених каналах зв’язку, користувачі можуть зіткнутися з проблемою витоку інформації чи її модифікування. Зловмисники можуть завдати істотних збитків банківським та комерційним структурам, державним підприємствам та організаціям, а також приватним особам, які використовують електронний документообіг. Для того, щоб вирішити цю проблему, необхідно забезпечити захист інформації, що міститься в документі та провести процедуру встановлення автентичності автора і самого документа.

Комплекс процесів та технологічних рішень, які допомагають здійснити захист даних та запобігання несанкціонованому доступу до системи, входять до складу понять, що визначають кібербезпеку, яка є одним із найважливіших елементів національної і інформаційної безпеки [4,5].

Застосування тензорних методів в технічних напрямках, в тому числі, в телекомунікаціях [8,9], отримані результати виводять дослідження на новий рівень, який не вдавалося отримати, використовуючи методи, що застосовувалися раніше. Використання тензорного аналізу запропоновано для дослідження

характеристик якості мережі масового обслуговування, яка складається з систем масового обслуговування M/M/1 [6]. Обґрунтовано доцільність тензорного методу, що дозволяє отримувати ефективні рішення оцінки характеристик якості при одночасному аналізі мережі та мережі масового обслуговування різної структури та розмірів функціональних характеристик [6,7].

Тензорні методи дозволяють розв’язувати різні мережеві завдання, прогнозувати стан мережі на певному проміжку часу з урахуванням топології мережі та особливості функціонування використовуваних протоколів. Показано можливість спільного математичного моделювання структурних властивостей та функціональних характеристик телекомунікаційних систем за допомогою спеціального способу завдання системи координат та властивості інваріантності тензора, де інваріантом є значення трафіку у кожний конкретний момент часу.

В [10] розглянуто тензорну модель телекомунікаційної мережі, яку представлено в базисі міжполюсних шляхів і внутрішніх вузлових пар. Перевагою використання саме тензорної моделі є забезпечення якості обслуговування за показниками пропускної здатності, середньої міжкінцевої затримки та ймовірності втрат пакетів.

Для дослідження якісних характеристик функціонування мережі MVNO/LTE запропоновано тензорний метод декомпозиції архітектури мережі з метою отримання оптимальної конфігурації з’єднання базових станцій e-NodeB за критеріями максимальної пропускної здатності та заданих параметрів затримки [7].

Забезпечити захист основних властивостей інформації, а саме конфіденційності, цілісності та доступності, можна шляхом використання криптографічних алгоритмів. Якщо йдеться про забезпечення конфіденційності, тобто захисту від витоку інформації, то це вирішується шляхом шифрування відкритого повідомлення. Зашифроване повідомлення у вигляді криптограми передається одержувачеві по незахищеному каналу. При цьому, для зашифровування та розшифрування повідомлення, необхідно знати ключ шифрування (правило перетворення).

В залежності від обраного алгоритму шифрування, операції зашифровування та розшифрування можуть виконуватися по-різному. Так, якщо

використовувати симетричний алгоритм шифрування, то процедури зашифровування та розшифровування виконуватимуться одним спільним секретним ключем.

В разі використання асиметричного алгоритму, процес шифрування буде виконуватися двома різними ключами. Тобто зашифровування тексту буде здійснюватися відправником за допомогою відкритого ключа, а процес відновлення повідомлення з криптограми – за допомогою іншого секретного ключа одержувача. Ця пара ключів обирається за певним законом [13].

Проте, для процесу шифрування частіше обирають саме симетричні системи зі спільним секретним ключем. Цей вибір пояснюється швидкістю шифрування (асиметричні системи працюють повільніше).

Для підвищення ефективності засобів захисту конфіденційної інформації пропонується здійснювати шифрування повідомлення тензорними методами [14,15].

Розглянемо початковий вихідний текст, наприклад, у вигляді тензора четвертої валентності T_{ijk}^{h} n – мірного простору, $h,i,j,k=\overline{1,n}$. Якщо здійснити алгебраїчне додавання з числовим коефіцієнтом 0,5 після операцій симетрування і альтернування по двох коваріантних індексах, то компоненти вихідного тензора не зміняться [14]:

$$T_{ijk}^{h}=0{,}5(T_{(ij)k}^{h}+T_{[ij]k}^{h}), \qquad (1)$$

де формулою $T_{(ij)k}^{h}=T_{ijk}^{h}+T_{jik}^{h}$ задається операція симетрування по двох індексах і та j; $T_{[ij]k}^{h}=T_{ijk}^{h}-T_{jik}^{h}$ – операція альтернування по індексах і та j.

Перетворення (1) може виступати в якості ключа шифрування. В результаті операцій симетрування і альтернування по двох індексах із вихідного тензора T_{ijk}^{h} ми отримаємо два тензори $T_{(ij)k}^{h}$ і $T_{[ij]k}^{h}$, які можно зберігати або відправляти. Тобто в процесі шифрування із одного тензора ми отримали два тензори. Потім за допомогою формули (1) можна здійснити розшифрування. Оскільки розглянуті операції симетрування і альтернування є дуже простими, то всі обчислення не потрибують затрати великих ресурсів. Тому процеси шифрування

і розшифрування є простими і достатньо швидкими, тобто є ефективними[16]. На Рис.2.1 показано процес створення ключа шифрування.

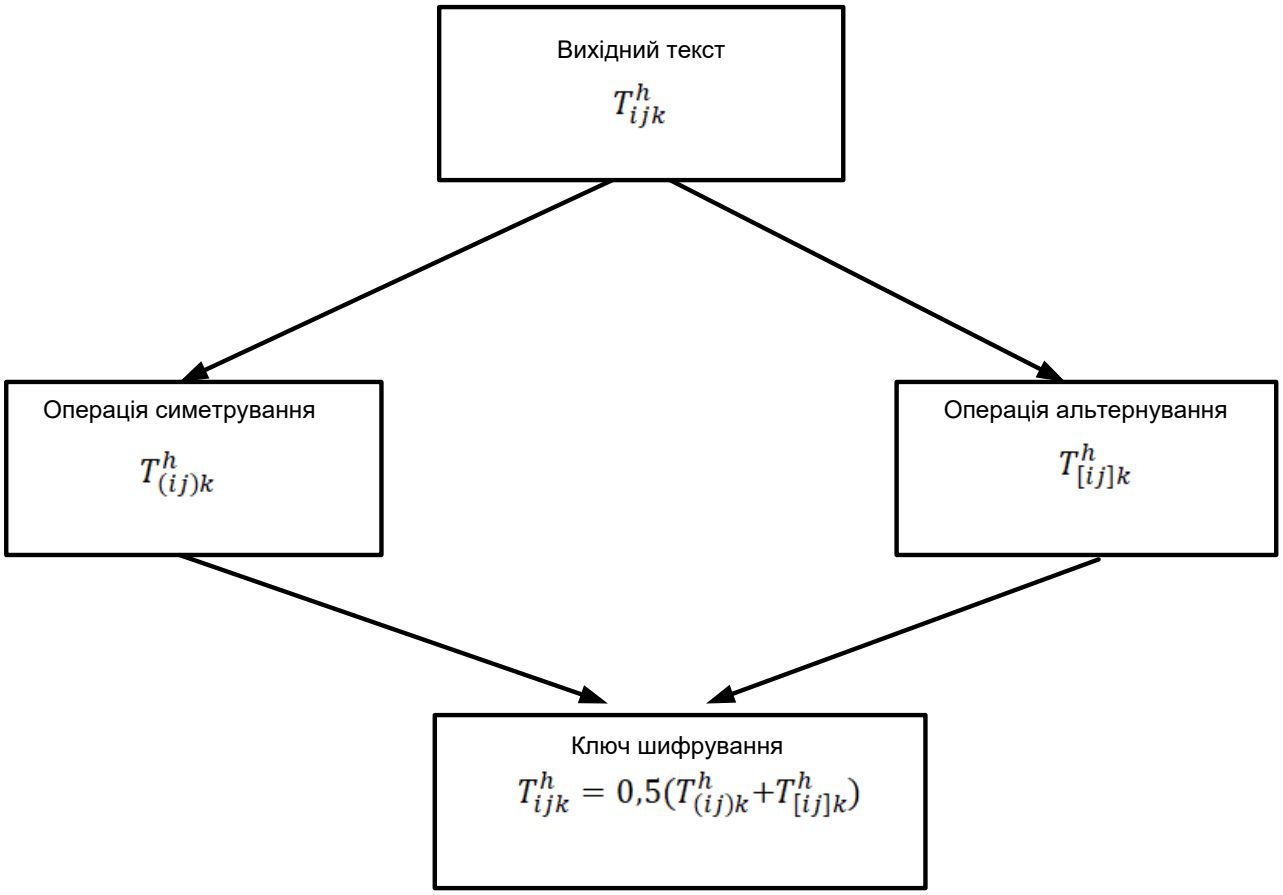


Рисунок 2.1 - Процес створення ключа шифрування

Таким чином, можна зробити висновки, що за результатом виконання операцій тензорного аналізу, можна отримати можливість зашифровування повідомлень та розшифровування криптограм. При цьому відбувається підвищення швидкодії процесу забезпечення захисту конфіденційної інформації при здійсненні документообігу.

2.3 Захист інформації в електронних банківських системах

Захист систем дистанційного банківського обслуговування є актуальним питанням й існує значна кількість методів їх захисту. Проте одним із найнадійніших засобів захисту інформації є використання криптографічних протоколів. За допомогою криптографічних протоколів вирішуються різноманітні завдання, а саме: захист інформації шляхом шифрування; підтвердження справжності користувача та документа за допомогою

протоколів автентифікації; розподілення ключів.

Основний недолік симетричного шифрування – необхідність передавати ключі "з рук в руки". Недолік цей дуже серйозний, оскільки робить неможливим використання симетричного шифрування в системах з необмеженою кількістю учасників. Однак в іншому симетричне шифрування має одні переваги, які добре видно на фоні серйозних недоліків шифрування асиметричного.

Перший недолік асиметричних алгоритмів шифрування – це мала швидкість виконання операцій зашифровування і розшифровування, зумовлена тим, що для виконання обчислень необхідно мати велику ємність ресурсів. Другий недолік – "теоретичний", тобто математично криптостійкість алгоритмів асиметричного шифрування не доказана. Це пов’язано перш за все з задачею дискретного логарифму – поки ще не доведено, що її розв’язання за припустимий час неможливе. Зайві труднощі завдає і необхідність захисту відкритих ключів від підміни – підмінивши відкритий ключ легального користувача, зловмисник зможе забезпечити зашифровування повідомлення на своєму відкритому ключі і потім легко розшифрувати його власним секретним ключем.

Враховуючи всі переваги, можна зробити висновок, що найбільш придатними для захисту інформації шляхом шифрування при передаванні мережами загального користування є симетричні алгоритми. Це обумовлено тим, що вони мають високу швидкість шифрування та забезпечують відповідну криптографічну стійкість.

Щодо переваг асиметричних алгоритмів, то по-перше – це їх зручність, нема необхідності держати ключі шифрування у таємниці. При використанні асиметричних алгоритмів застосовують відкритий ключ для зашифрування та/чи перевірки справжності документу. А для розшифровування документу та/чи при необхідності підтвердити справжність документу використовують секретний(приватний) ключ. Проте основними напрямками використання асиметричних алгоритмів є саме автентифікація документу та розподіл ключів.

Для захисту електронних транзакцій використовуються сучасні криптопротоколи різного призначення: шифрування, розподілення ключів, гешування та автентифікації [17].

Для комплексного рішення всіляких проблем платіжними системами Visa і MasterCard було створено набір протоколів, що відомі як стандарт SET (Secure Electronic Transactions) «Безпечні електронні транзакції». У цьому протоколі для захисту транзакцій при здійсненні електронних платежів використовуються дві процедури: по-перше, шифрування та по-друге, автентифікація за допомогою цифрового підпису. Протокол гарантує, що при взаємодії власника пластикової карти і продавця, інформація про рахунок кредитної карти залишатиметься конфіденційною (використовується подвійний цифровий підпис) [18-21] . Перевагою протоколу SET можна відзначити посилення безпеки, включаючи можливість автентифікації всіх учасників транзакції. Проте недоліками протоколу SET є технологічна складність, велика вартість впровадження цієї технології і дорожнеча у використанні.

Протокол TLS забезпечує можливість повторного підключення без додаткової автентифікації і узгодження ключів сеансу. Протокол може забезпечити узгодження допустимих криптографічних алгоритмів: генерування ключів (DH); шифрування (RC2, RC4, IDEA, DES, 3-DES, AES, Blowfish); цифрового підпису та автентифікації (DSS, RSA); гешування (SHA-1, MD5).

З метою підвищення рівня безпеки електронних платежів, корпорація VISA розробила протокол 3-DSecure і запропонувала клієнтам послугу Verified by Visa (VbV). Послуги, що ґрунтуються на підставі цього протоколу також були прийняті компаніями MasterCardпід назвою Master Card Secure Code (MCC) і JCB International як J/Secure.

Протокол 3-D Secure на відміну від протоколу SET, дешевше в реалізації, зручніший у використанні і додає ще один крок автентифікації користувача. В протоколі 3-D Secure, до банківської інформації додається додатковий запит на підтвердження справжності платіжної картки (зазвичай

це одноразовий пароль підтвердження, що надсилається банком в SMS - повідомленні на телефон клієнта).

2.4 Підтвердження справжності даних при використанні систем дистанційного банківського обслуговування

У середовищі електронних платежів індивідуальні і корпоративні споживачі взаємодіють із продавцями зі своїх персональних комп'ютерів через Інтернет. Учасники транзакцій, що здійснюються за допомогою протоколу SET [2]:

– покупець (клієнт), що є будь-який зареєстрований власник пластикової платіжної картки (MasterCard, Visa, тощо), виданої йому банком емітентом;

– продавець, що є особою, у якої власник картки може придбати товари або послуги та повинен мати відповідні відносини з операційним центром;

– емітент платіжної картки. Банк-емітент, що видав платіжну картку відповідній особі (власнику картки). Усю відповідальність за оплату заборгованості власника картки за даною карткою несе емітент картки;

– банк-еквайр веде розрахунки з продавцем, який виконує авторизацію платіжних карток і здійснює відповідні платежі.;

– шлюз платіжної мережі (payment gateway). пов'язує SET й існуючі банківські платіжні мережі, виконуючи функції авторизації і передачі платежів;

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

Приведемо алгоритм, що відбувається під час транзакції:

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

2) Покупець після процедури перевірки особистості отримує цифровий сертифікат, підписаний банком. Цей сертифікат засвідчує відкритий ключ 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, один з них використовуватиметься для електронного підпису, а другий – для обміну ключами. Продавцю також буде потрібна копія сертифіката відкритого ключа шлюзу платіжної мережі;

4) Покупець розміщує замовлення. обирає список товарів та відправляє продавцю. Продавець у відповідь висилає бланк замовлення з зазначеними в ньому списком обраних товарів, цінами, загальною вартістю замовлення і номером замовлення;

5) Відбувається перевірка продавця. Разом із бланком замовлення продавець висилає копію свого сертифіката для можливості підтвердження справжності продавця;

6) Покупець відправляє замовлення, що підтверджує покупку товарів за замовленням. Платіжна інформація у зашифрованому виді містить необхідні дані кредитної картки. Сертифікат покупця дозволяє продавцю виконати верифікацію покупця;

7) Продавець відправляє запрос для перевірки платіжноспроможності покупця;

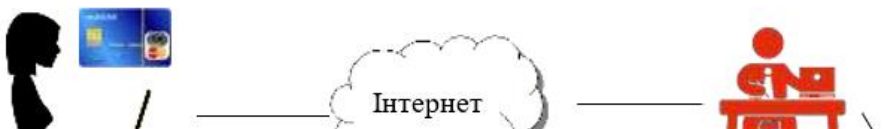
8) Продавець відправляє покупцю підтвердження замовлення;

9) Продавець організовує доставку товарів або виконання послуг покупцю;

10) Продавець запитує отримання платежу.

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

На Рис.2.2 представлено протокол захищеної системи електронної комерції.



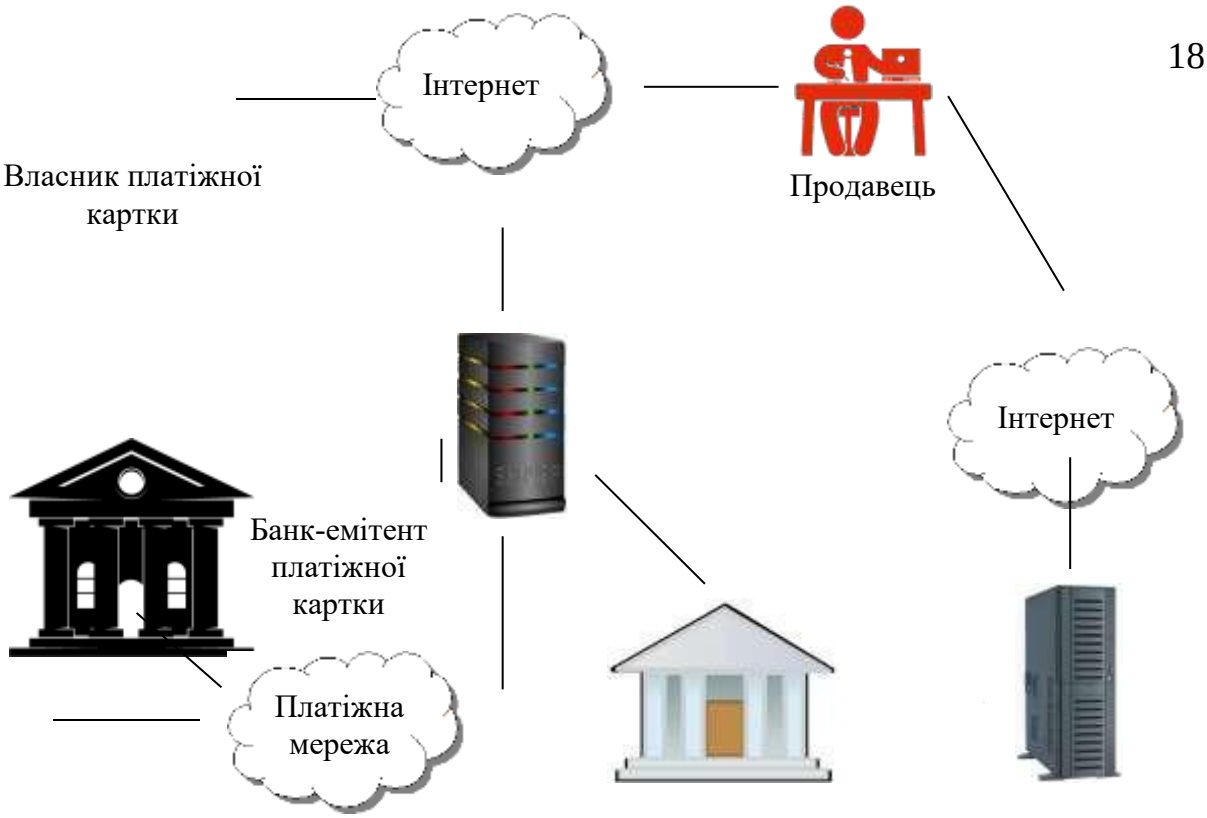


Рисунок 2.2 – Протокол захищеної системи електронної комерції.

3 АЛГОРИТМИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

3.1 Ідентифікація та автентифікація користувача

Інформаційні системи (ІС) різного масштабу стали невід'ємною частиною базової інфраструктури держави, бізнесу, громадянського суспільства. Дедалі більше інформації, що захищається, переноситься в ІС. Сучасні інформаційні технології не тільки забезпечують нові можливості ведення бізнесу, державної та суспільної діяльності, а й створюють значні потреби у забезпеченні безпеки захисту інформації.

Основними процедурами реєстрації користувачів в ІС є процедура ідентифікації і автентифікації. Перший крок – ідентифікація. На ній відбувається розпізнавання інформації про користувача, наприклад, логін та пароль. Другий крок – автентифікація. Це процес перевірки інформації про користувача. Іншими словами, це означає що необхідно переконатися, що користувачі дійсно є тими, за кого себе видають. Методами автентифікації користувача можуть бути паролі, біометричні методи, смарт-картки, сертифікати тощо. Несанкціоноване отримання зловмисником доступу до ІС пов'язане насамперед із порушенням процедури автентифікації.

Процес автентифікації користувача комп'ютером можна поділити на два етапи. Підготовчий – виконується під час реєстрації користувача у системі. Саме тоді користувач запитує зразок автентифікаційної інформації, наприклад, пароль або контрольний відбиток пальця, який буде розглядатися системою як еталон при автентифікації. Штатний –зразок автентифікаційної інформації запитується в користувача знову і порівнюється з еталоном, що зберігається в системі. Якщо зразок схожий з еталоном із заданою точністю, тоді користувач вважається впізнаним, інакше користувач буде вважатися чужим, результатом чого буде, скажімо, відмова у доступі на комп'ютер.

У будь-якому випадку функція обчислення еталона з автентифікаційної інформації повинна бути односпрямованою, тобто легко розраховуватися, але бути проблемою при спробі обчислення у зворотному напрямку.

Відомо, що багато зловживань інформацією інформаційної системи здійснюються внутрішніми користувачами, партнерами та постачальниками

послуг, які мають прямий доступ до системи. Більшість з них, – це випадки несанкціонованого отримання прав та привілеїв, крадіжки та передачі облікової інформації користувачів інформаційної системи, що стає можливим через недосконаліть технологій розмежування доступу та автентифікації користувачів. У зв'язку з цим, розробка нових методів забезпечення безпеки, а також вдосконалення вже існуючих є одними з найбільш пріоритетних напрямків розвитку систем безпеки.

В цілому автентифікація за рівнем інформаційної безпеки ділиться на три категорії:

– статична автентифікація (наприклад,постійні паролі);
– стійка автентифікація (динамічні дані);
– постійна автентифікація (генерація підписів для кожного біта інформації).

На даний час багато дослідників розробляють нові методи автентифікації пристроїв. Завдання полягає у розробці методів розпізнавання, які б надавали однозначну інформацію про результат перевірки.

Перше, з чим має справу як користувач, так і зловмисник, при доступі до будь-якого сервісу – це автентифікація. Саме ця дія дозволяє визначити, що користувач, який звертається за інформацією або бажає здійснити якісь дії – той, за кого він себе видає. Тому метою автентифікації є максимальне унеможливлення використання чужих облікових даних.

Автентифікація користувача – це метод, який запобігає доступу неавторизованих користувачів до конфіденційної інформації.

Існує три фактори автентифікації, на які можна розділити різні типи автентифікації:

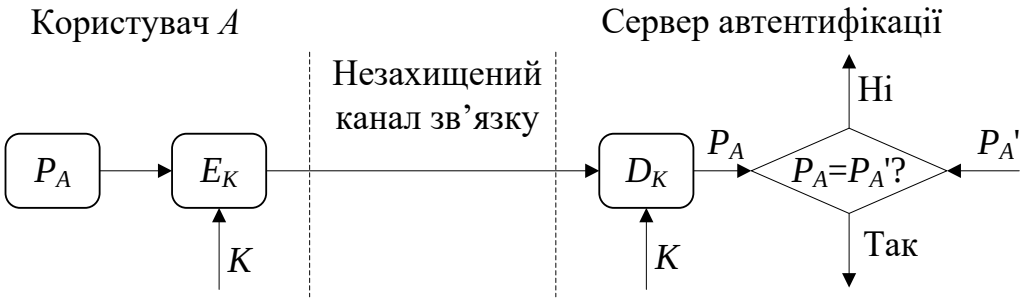
– фактор знань: те, що людині відомо, наприклад пароль або відповідь на таємне запитання;
– фактор володіння: те, що людина демонструє, тобто фізичний об’єкт, як мобільний телефон або маркер безпеки;
– фактор властивості: деякі фізичні властивості, наприклад, біометрична характеристика або модель поведінки.

Методи простої автентифікації поділяють на два види [2]:

– з використанням паролів;
– з використанням односторонньої функції

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

Схема простої автентифікації з використанням пароля показана на Рис. 3.1



P_A – пароль користувача А;
E – функція зашифровування;
D – функція розшифрування;
K – ключ шифрування

Рисунок 3.1 – Схема простої автентифікації з використанням пароля

Проте, безпечнішим 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 телекомунікаційних каналах.

Схема простої автентифікації з використанням односторонньої функції для перевірки пароля показана на Рис. 3.2

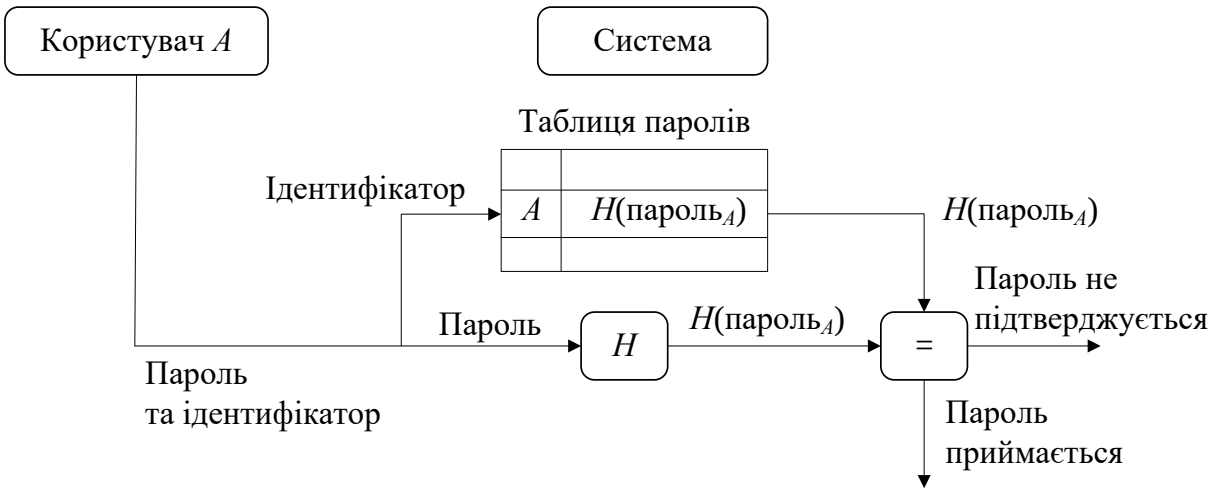


Рисунок 3.2 – Схема простої автентифікації з використанням односторонньої функції для перевірки пароля

Автентифікація з використанням одноразових паролів (One-Time Passwords – OTP) – динамічна інформація, що генерується для одиничного використання за допомогою пристроїв автентифікації (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.

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 співпадають, то користувач проходить автентифікацію. Методи, що

застосовані в OTP-токенах, можна розрізняти за режимами роботи:

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).

Методи біометричної автентифікації засновані на використанні унікальних біологічних характеристик суб'єкта. В якості таких характеристик можуть бути використані: відбиток пальця, геометрія обличчя, геометрія руки, сітчатка ока, хода, голос, ДНК, тощо.

Для захисту біометричної інформації застосовується стандарт ДСТУ ISO/IEC 24745:2015 «Інформаційні технології. Методи захисту. Захист біометричної інформації».

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.

Багатофакторна автентифікація характеризується тим, що порівняння з еталоном відбувається не за одним критерієм відповідності, за кількома.

У багатофакторної автентифікації важливо те, що одним з факторів є

пароль, який користувач знає і який дозволяє діяти на основі його волі з виключенням примусу третіх осіб. Цей фактор для зручності зазвичай передається по основному каналу, по якому відбувається комунікація.

Другим фактором може бути щось, що належить користувачеві, або біометрична характеристика, така як код, отриманий за допомогою маркера безпеки, або відбиток пальця, знятий через смартфон. Другий фактор завжди має транслюватися по альтернативному каналу, щоб уникнути його захоплення і використання разом з першим фактором. Часто другий фактор надходить по альтернативному каналу (наприклад, код, що відправляється по SMS), але потім повертається назад на основний канал з усіма описаними вище ризиками крадіжки.

Наприклад, при автентифікації за технологією ідентифікації відбитків пальців, ім'я користувача вводиться для реєстрації, а відбиток пальця заміняє пароль. У цьому випадку ім'я користувача є покажчиком для одержання його облікового запису і перевірки відповідності між шаблоном зчитаного під час реєстрації відбитка і раніше збереженим шаблоном в базі даних для даного імені користувача.

Багатофакторна автентифікація є методом перевірки справжності користувача за кількома параметрами.

До категорій таких доказів відносять види автентифікації:

– фактор знання - інформація, яку знає користувач (пароль, пін-код)

– фактор володіння - річ, якою володіє користувач (електронна карта, токен, флеш-пам'ять);

– фактор властивості- біометрична характеристика людини (контур обличчя, відбитки пальців, райдужна оболонка очей, капілярні візерунки, послідовність ДНК тощо).

У таблиці 3.1 показано фактори автентифікації.

Таблиця 3.1 – Фактори автентифікації

Фактори автентифікації	Приклади факторів автентифікації
Фактор знання	Пароль PIN-код

Фактор володіння	Фізичний ключ Пластикова картка OTP-токен
Фактор властивості	На основі біометричних характеристик : Відбиток пальця Рисунок сітківки ока Голос тощо

Біометричні системи доступу є дуже зручними для користувачів. На відміну від паролів і носіїв інформації, які можуть бути втрачені, вкрадені, скопійовані, біометричні системи доступу засновані на людських параметрах, які завжди знаходяться разом з ними, і проблеми їх збереження не виникає. Втратити їх майже неможливо. Також неможлива передача ідентифікатора третім особам.

3.2 Автентифікація документів за допомогою електронного підпису

Стрімкий розвиток інформаційних технологій привів до появи електронного документообігу, що пов’язане зі збереженням документів від несанкціонованого копіювання, модифікації і підробки. Для вирішення проблеми захисту інформації від несанкціонованого доступу необхідно застосовувати сучасні засоби та методи захисту електронної системи.

Одним із поширених у світі засобів такого захисту електронних документів від копіювання, модифікації і підробки є електронний підпис, який за допомогою спеціального програмного забезпечення підтверджує справжність інформації документа, його реквізитів і факту підписання конкретною особою.

Електронний підпис (ЕП), використовується для автентифікації текстів, передаваних телекомунікаційними каналами .

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

- засвідчує, що підписаний текст виходить від імені користувача, який підписав документ;

- не надає можливості автору відмовитися від зобов'язань, пов'язаних з підписаним текстом;
- гарантує цілісність підписаного тексту.

Електронний підпис являє собою невелику кількість додаткової цифрової інформації, що передається разом з відкритим текстом [2].

Система ЕП включає дві процедури:

1 підписання документу відправником;

2 перевірка підпису під документом одержувачем.

У процедурі формування підпису використовується секретний ключ відправника повідомлення, у процедурі перевірки підпису – відкритий ключ відправника.

При формуванні ЕП відправник обчислює геш-функцію $h(M)$ тексту M, який він підписує. Обчислене значення геш-функції $h(M)$ являє собою один короткий блок інформації m, що характеризує весь текст M у цілому. Потім число m зашифровується секретним ключем відправника. Знайдена при цьому пара чисел є ЕП для відкритого тексту M.

При перевірці ЕП одержувач також обчислює геш-функцію $m = h(M)$ тексту M, що надіслав відправник. Потім публічним ключем відправника одержувач обчислює значення m геш-функції, відновлене з підпису, що був переданий відправником. У разі збігу обчислених значень двох гешів на боці одержувача, приймається рішення, що підпис справжній, отже і повідомлення є справжнім.

Засадничим моментом у системі ЕП є те, що не можливо підпис користувача сформувати без знання його секретного ключа для створення підпису. Підписаний документ утворюється з початкового відкритого тексту, до якого додається сформований електронний підпис.

Кожний підпис містить таку інформацію:

- дата підпису;
- термін завершення дії ключів даного підпису;
- інформація про особу, котра підписала файл (П.І.Б., посада та назва фірми);
- ідентифікатор особи, що поставила підпис;
- власне цифровий підпис.

Технологія застосовування системи ЕП припускає наявність мережі абонентів, які надсилають один одному підписані електронні документи. Для кожного абонента генерується пара ключів: секретний і відкритий. Секретний ключ зберігається абонентом у таємниці й використовується ним задля формування ЕП. Відкритий ключ є відомий всім іншим користувачам і призначений для перевірки ЕП одержувачем підписаного електронного

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

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

- факторизація (розкладання на множники) великих цілих чисел;
- дискретне логарифмування.

До системи електронного підпису сформульовані деякі вимоги.

Так, у сучасних автоматизованих системах керування, комп'ютерних системах мереж, різних інформаційних і телекомунікаційних системах, інформаційно-телекомунікаційних системах, а також системах електронного документообігу висуваються високі вимоги до забезпечення цілісності, автентичності (справжності), неспростовності та доступності інформації (електронних документів) на всіх етапах їх життєвого циклу. При цьому під інформацією будемо розуміти сукупність усіх даних і програм, що використовуються у системі чи технології, незалежно від їхнього логічного чи фізичного подання. Під інформацією розумітимемо також і повідомлення й електронні документи, що циркулюють у відповідних системах чи технологіях.

Можна заявити, що функція електронного підпису містить функцію автентифікації/ ідентифікації.

Можна сформулювати наступні вимоги до електронного підпису:

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

б) підпис має застосовувати унікальну інформацію відправника для запобігання модифікації;

в) формування електронного підпису має бути простим;

г) повинно бути неможливо підробити електронний підпис шляхом обчислень, як створенням нового повідомлення для існуючого електронного підпису, так і створенням помилкового електронного підпису для деякого повідомлення;

д) електронний підпис має не займати багато пам'яті.

Розглянемо деякі методи побудови схем електронного підпису:

а) шифрування електронного документа (ЕД) на основі симетричних алгоритмів;

б) шифрування ЕД з використовуванням асиметричних алгоритмів шифрування.

в) зашифровування остаточного результату опрацювання електронного документу геш-функцією за допомогою асиметричного алгоритму. Структурну схему такого варіанта побудови ЕП показано на Рис.3.3.

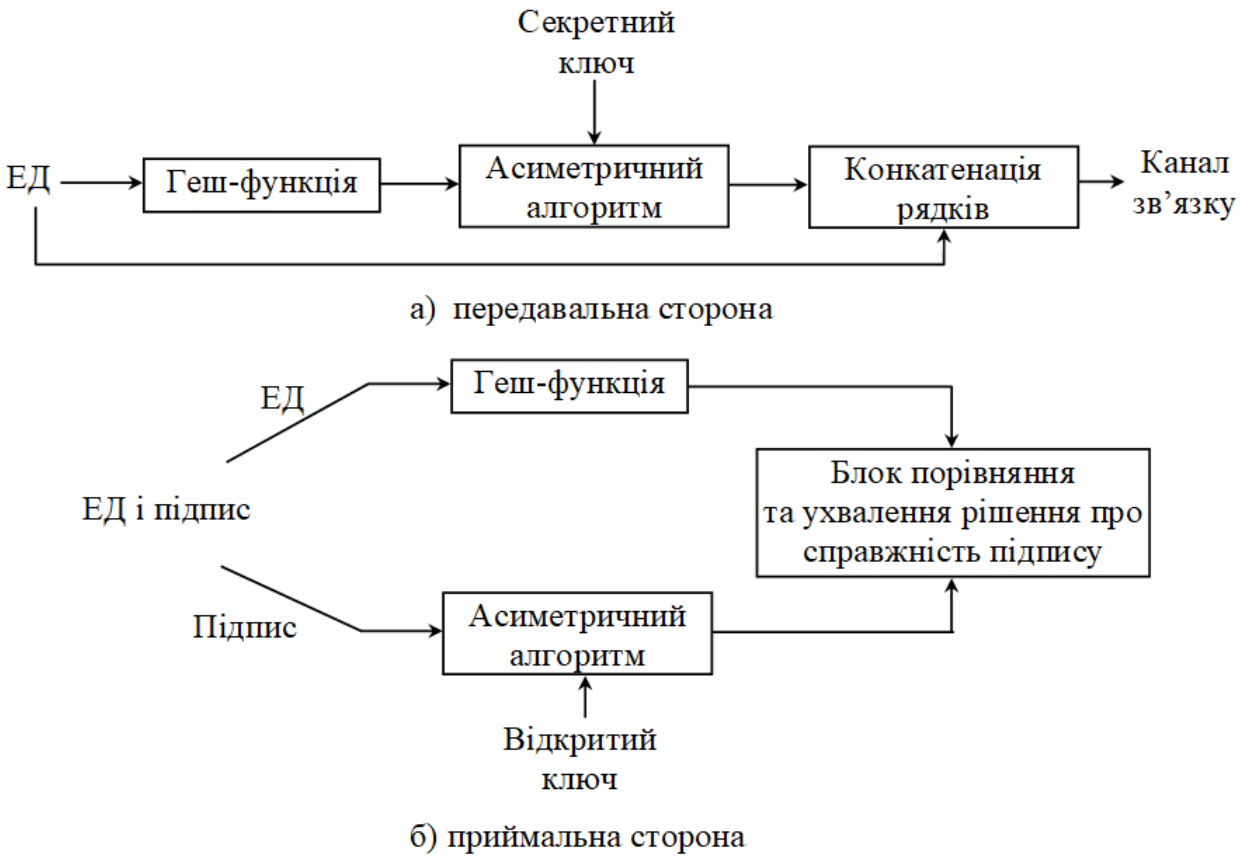


Рисунок 3.3 – Структурна схема побудови ЕП

Генерування підпису відбувається в такий спосіб:

а) відправник повідомлення обчислює геш від відкритого електронного

документа. Отриманий геш перетворюється секретним ключем, після чого отримане значення підпису разом з текстом надсилається одержувачеві;

б) одержувач повідомлення повинен відновити текст з підпису та сертифікований відкритий ключ відправника, а потім провести розшифровування на ньому ЕП, сам документ опрацьовується операцією гешування, після чого результати порівнюються і, якщо вони збігаються, ЕП визнається справжнім.

Стійкість електронного підпису обумовлена криптостійкістю асиметричних алгоритмів шифрування і застосовуванням геш-функцій.

Електронний документ, що підписаний, 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. Надана класифікація дозволяє визначити властивості будь-якого алгоритму цифрового підпису та порівняти його з іншими алгоритмами. 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 – 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, NTRU Signature Algorithm або NTRUSign).

Невід’ємною частиною алгоритму електронного підпису є

використовування геш-функцій. При цьому, в алгоритмі ЕП використовується стандартизована геш-функція, яка обчислюється окремо.

Геш-функцією перетворює інформаційну послідовність M довільної довжини на послідовність фіксованої довжини $h(M)$, називану геш-кодом. Функція гешування може служити як криптографічна контрольна сума – код виявлення змін (Manipulation Detection Code – MDC) або для перевірки цілісності повідомлення (Message Integrity Check – MIC).

Всі існуючі функції гешування можна представити як 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.

Основні три методи побудови геш-функцій:

– на базі певної складно обчислюваної математичної задачі;

– на базі алгоритмів блокового шифрування;

– розроблення з самого початку.

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 алгоритми шифрування;

– функції, що застосовують перетворення в групах, полях і кільцях з цілочисловим базисом;

– функції, що базуються на матричні перетворення.

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 $h(M) = h(M')$.

1.2.1 Алгоритм електронного підпису RSA

Найбільш відомою системою електронного підпису є система, в основі якої лежить алгоритм RSA. Узагальнену схему формування й перевірки електронного підпису RSA показано на Рис.3.4 [22].

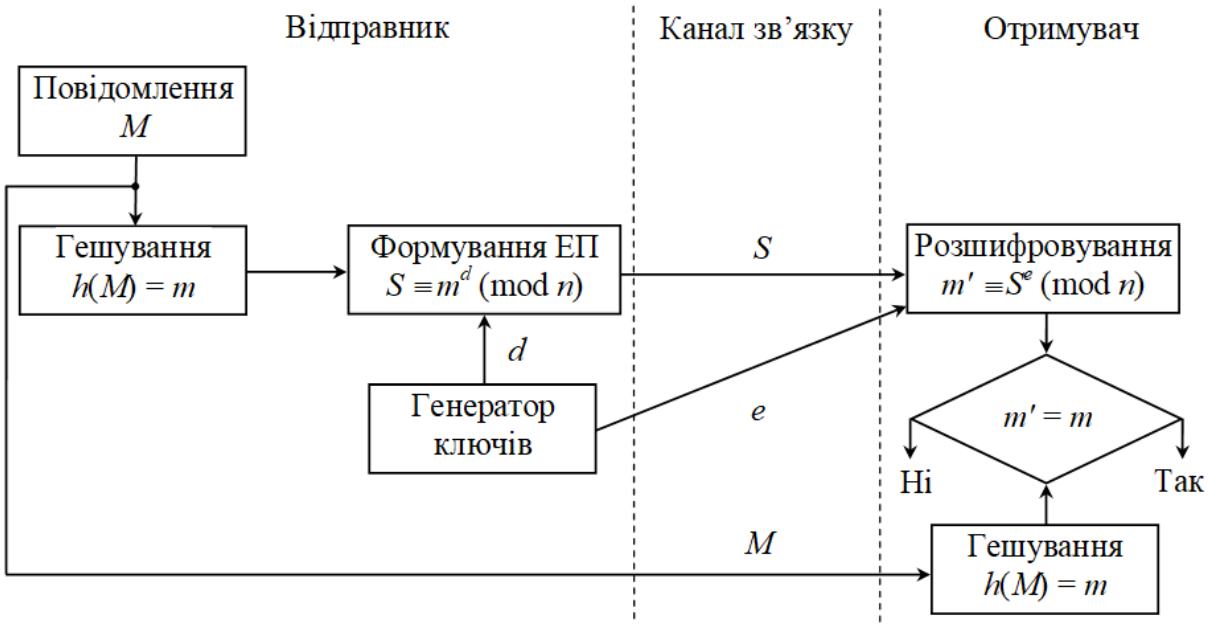


Рисунок 3.4 – Схема електронного підпису RSA

За алгоритмом ЕП RSA по-перше, обираються великі прості числа p і q, обчислюється модуль $n = pq$, функціяЕйлера $\varphi(n) = (p - 1)(q - 1)$ і вибирається відкритий ключ e (за умови $e < \varphi(n)$, НОД $(e, \varphi(n)) = 1$). Врешті, обчислюється секретне число d, взаємно обернене з e ($ed \equiv 1 \bmod \varphi(n)$). У відкритому каталозі розміщують значення(e, n), а секретний ключ d зберігається у автора документа.

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

$$h(M) = m.$$

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.

1.2.2 Алгоритм електронного підпису Ель Гамаля

Алгоритм електронного підпису Ель Гамаля не має тих недоліків, що є в алгоритмі ЕП RSA. Крім цього, сучасні алгоритми ЕП на еліптичних

кривих побудовані на підґрунті саме алгоритму електронного підпису Ель Гамаля.

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;$1 < k < p - 1$; НОД $(k, p - 1) = 1$ й обчислює

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

Число Y відправник подає в якості відкритого ключа. Узагальнену схему формування й перевірки електронного підпису Ель Гамаля показано на Рис.3.5.

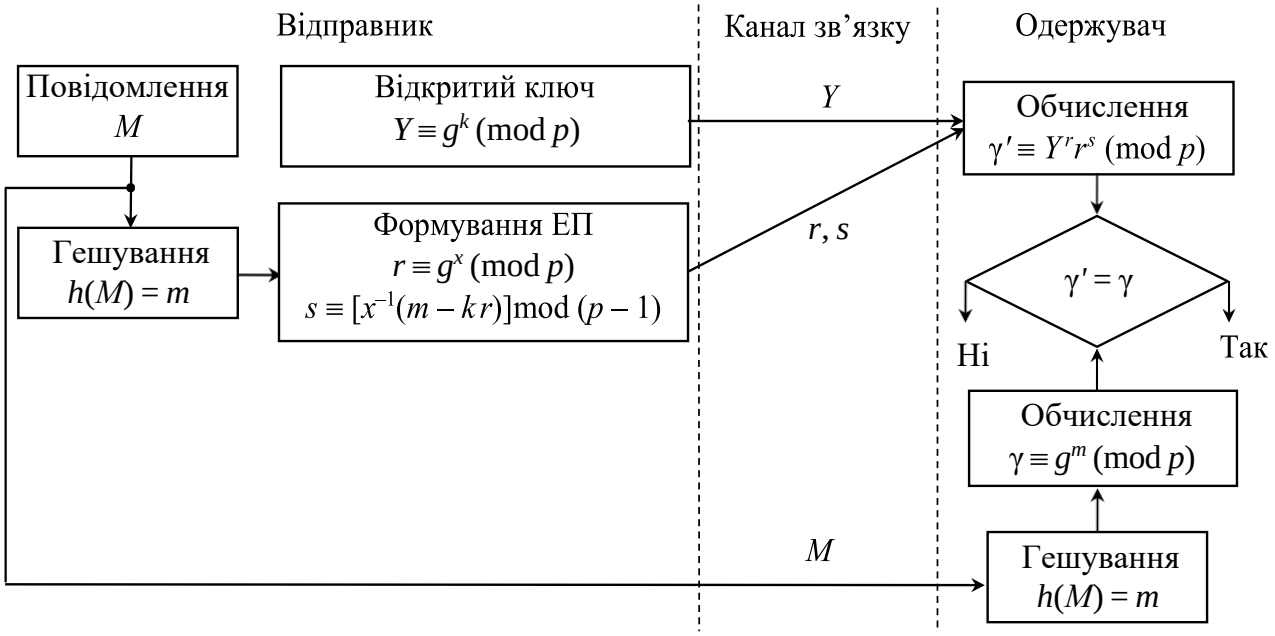


Рисунок 3.5 – Схема електронного підпису Ель-Гамаля

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:

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

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

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

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

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

Якщо рівність виконується, то підпис є справжній.

3.3 Система автентифікації BankID

З набранням чинності новим Законом про фінансовий моніторинг фінансові установи (банки та фінансові компанії) отримали право проводити віддалену ідентифікацію клієнтів, отже банки без фізичного контакту з клієнтом можуть відкривати рахунки, випускати віртуальну банківську карту або видавати фізичну платіжну карту.

Дистанційна ідентифікація - це підтвердження особи суб'єкта без його фізичної присутності, тобто на відстані за допомогою Інтернету та різних електронних систем. Цей метод перевірки дозволяє легко користуватися послугами, надійно оцифровувати персональну інформацію, різні процеси та збільшувати швидкість обслуговування.

Сьогодні в Україні існує кілька способів дистанційної ідентифікації, а саме: BankID (система НБУ), цивільний електронний паспорт (Card-ID), мобільна ідентифікація (Mobile-ID), електронний цифровий підпис, виданий уповноваженими установами. Система BankID базується на досвіді країн, які вже успішно впровадили цей метод ідентифікації - Швеції, Фінляндії, Естонії, Латвії, Канади та інших.

Віддалене відкриття банківського рахунку можуть здійснити:

- клієнти, які зареєструвались на державному порталі "Акція". Банк отримуватиме дані клієнтів та копії документів (паспорт, посвідчення водія, свідоцтво про реєстрацію автомобіля тощо) через захищені канали;

- клієнти, які раніше відкривали рахунки в інших банках, підключених до системи BankID Національного банку України.

Для клієнтів, які не зареєстровані на порталі "Action" або ніколи не відкривали банківський рахунок, перевірку можна здійснити в онлайн-чаті з менеджером банку.

Видаючи позики, фінансові компанії активно реалізовують можливість ідентифікації клієнта за допомогою програми «Дія», що економить час позичальника та підвищує довіру до нього з боку компанії.

Основна мета створення BankID в Україні – забезпечення надійної та зручної ідентифікації користувача для надання адміністративних та банківських послуг через інтернет на спеціальних порталах [23].

BankID вирішує проблему ідентифікації користувача через Інтернет: щоб надати, наприклад, довідку про нарахування заробітної плати, послуга повинна спочатку переконатися, що інформація запитується цією особою. Якщо громадянин обирає ідентифікацію через BankID, він вводить логін та пароль свого Інтернет-банкінгу, проходить другий етап авторизації (наприклад, введення одноразового пароля через SMS) і тим самим підтверджує свою особу.

Вхід за допомогою BankID дуже схожий на досить популярну кнопку "Увійти через Facebook" або "Увійти через Google" на сторінках реєстрації та працює на основі протоколу OAuth 2.0.

Для того, щоб замовити сертифікат, внести дані до реєстру тощо, достатньо бути клієнтом банку, підключеного до системи BankID.

В даний час до системи BankID підключено 36 банків, серед яких: УкрСибБанк, Райффайзен Банк Аваль, ПриватБанк, Альфа-Банк, Універсальний Банк, Ощадбанк.

Окрім банків, підключена система BankID [24]:

- 56 комерційних абонентів - постачальників послуг (зокрема: lifecell, Укргазбанк);
- 10 некомерційних абонентів - постачальників послуг (зокрема: Харківський центр обробки даних, Полтавська обласна рада, Міністерство

цифрової трансформації України, Міністерство економічного розвитку і торгівлі України).

Можна також пройти автентифікацію за допомогою системи BankID за допомогою смартфона Android. Якщо у користувача є ID-картка (пластиковий паспорт), у смартфоні має бути чіп NFC.

Список сервісів, які підтримують використання сервісу BankID: Міністерство Юстиції України, Єдиний державний портал адміністративних послуг, Портал державних послуг, Електронні петиції до Кабінету Міністрів України, Єдина система міських петицій, Онлайн-система «Громадський бюджет», Державне агентство з питань електронного урядування України, Громадський проект «Бюджет міських ініціатив», Госгеокадастр України, Платформа громадських ініціатив «Мій Голос», а також Львівська міська рада, Портал електронних сервісів міста Харкова і Портал електронних сервісів міста Києва.

Логіка системи базується на організації онлайн-запитів від сервісних порталів до банківської системи певного банку через єдиний шлюз, який є центральним вузлом системи BankID, та передачі адресних даних у підписаному та зашифрованому вигляді. Усі запити проходять виключно через центральний вузол BankID і лише після натискання кнопки клієнтом.

Дані, які банком можуть бути передані порталу, такі:

- прізвище ім'я по батькові;
- дата народження;
- серія та номер паспорта;
- ідентифікаційний номер (ІПН);
- скан-копії паспорта та ІПН;
- адреса реєстрації;
- номер телефону;
- email-адреса.

Ідентифікація через BankID практично не відрізняється від перевірки документів у банках за особистої присутності. При відкритті рахунку українські банки записують і зберігають клієнтські дані – ПІБ, скановані копії паспорта та ІПН, адреса реєстрації і т.д. Це стверджується стандартами реєстрації і зберігання клієнтських даних і контролюється державою в особі

Національного Банку України. Доступ до клієнтських даних при використанні BankID захищається так само надійно, як доступ до грошових коштів через інтернет-банк.

3.4 Побудова системи автентифікації користувача

Сучасні системи автентифікації базуються на процесі підтвердження особи користувача ідентифікатор/пароль. Однак ідентифікатор/пароль можуть бути скомпрометовані користувачем або зловмисником. Значні інтервали часу, протягом яких пароль та ідентифікаторзалишаються незмінними, дають змогу застосувати різні методи їх перехоплення і підбору. Для того, щоб підвищити захищеність комп'ютерної системи, адміністратори обмежують термін дії паролів, але зазвичай цей термін становить тижні та місяці, що цілком достатньо для зловмисника.

Багатофакторна автентифікація в системі базується на трансакційному ідентифікаційному коді (TIC (Transaction Identification CODE)) та на службі короткихповідомлень (SMS(Short Message Service)), який створює додатковий рівень безпеки відсутній при традиційній автентифікації за типом ім'я користувача / пароль.Код має схожість з одноразовим паролем (OTP (One Time Password)). Він забезпечує більшнадійну автентифікацію та використовується лише один раз. TIC підтверджує, що поточна транзакція була ініційована саме тією особою, а не зловмисником, яка є істинним власником рахунку (банківської картки).

TIC-коди мають певні властивості, а саме:

- створюються банком покупця;
- 32 бітними або 64 бітними псевдовипадково згенерованими кодами;
- являють собою складну послідовність цифр або комбінацію цифрових і буквено-цифрових символів;
- кожна транзакція потребує унікального коду для автентифікації, кожен код використовується лише один раз. Механізм генерації кодів передбачає обмежений доступ до них та є суворо конфіденційним, лише уповноваженим на це працівником фінансової установи. Банк за номером телефону клієнта надсилає SMS для підтвердження транзакції. Мережа

стільникового зв`язку використовує окремий канал для передачі і прийому SMS. Тому багатофакторна автентифікація використовується для перевірки покупця та транзакції відповідно до наступних кроків:

1) Первинна автентифікація: Клієнт спочатку входить на веб-сервер, використовуючи веб-ім'я та пароль, призначені йому для базової автентифікації;

2) TIC-автентифікація: Після успішної автентифікації покупця за допомогою його веб-імені та пароля, веб-сервер затребує ввести TIC (друга автентифікація).Покупець розшифровує та вводить TIC, щоб перевірити його справжність на сервері автентифікації та однозначно ідентифікувати транзакцію

3) SMS-підтвердження: Після TIC-автентифікації, наступною автентифікацією являється SMS-підтвердження. Покупець отримує SMS із деталями транзакції, які необхідні для ідентифікації та підтвердження ініціатора транзакції. За допомогою SMS покупець надсилає відповідь підтвердження транзакції («ТАК») або скасовуєїї («НІ»).

Багатофактрна автентифікація передбачає наступні кроки :

1) клієнт отримує логін та пароль у своєму банку при відкритті рахунку або вже має відкритий рахунок в фінансовій установі;

2) клієнт входить на веб-сервер свого банку через GPRS-з'єднання, використовуючи свій логін та пароль. Перша автентифікації призначена для ідентифікації покупця веб-сервером;

3) після успішної першої автентифікації клієнт отримає опцію, щоб розпочати транзакцію із вхідним повідомленням та ідентифікатором сесії;

4) клієнт обирає спосіб оплати (кредитна картка, дебетна картка, електронний переказ). У випадку розрахунку карткою протокол вимагає дійсність реквізиту платежу;

5) клієнт вводить деталі платежу;

6) клієнт не може здійснити транзакцію без TIC. Маємо на увазі, що TIC захищені паролем на мобільному телефоні, і цей пароль перед використанням в транзакції буде розшифрований за допомогою одного із TIC шифрів.

7) усі транзакційні запити разом з TIC будуть далі зашифровані та передані

серверу для обробки.

8) автентифікаційний сервер фінансової установи розшифровує отриману інформацію протранзакцію та інформацію про ТІС.

Сервер перевіряє отриманий від клієнта код, порівнює його із кодом збереженим разом із інформацією про рахунок клієнта, який був відтворений із списку кодів бази даних сервера. Коли обидва коди співпадають,використаний код автоматично знищується із бази даних серверу. Якщо ж коди не співпадають, сервер автентифікації скасовує подальші транзакції клієнта та надсилає йому на телефон повідомлення про помилку.

9) При успішності проходження автентифікації ТІС, авторизаційний сервер генеруєтекст повідомлення (SMS) та відправляє його до SMS шлюзу/ адаптера для подальшої передачі через стільникову мережу. Мережа стільникового зв`язку використовує SMSC, як основний пристрій мережі для передачі SMS на мобільний телефон клієнта.

10) Ініційовану транзакцію клієнт підтверджує за допомогою SMS із текстом. «ТАК» або скасовує обираючи текст «НІ»

Алгоритм багатофакторної автентифікації показано на Рис. 3.6 [22]

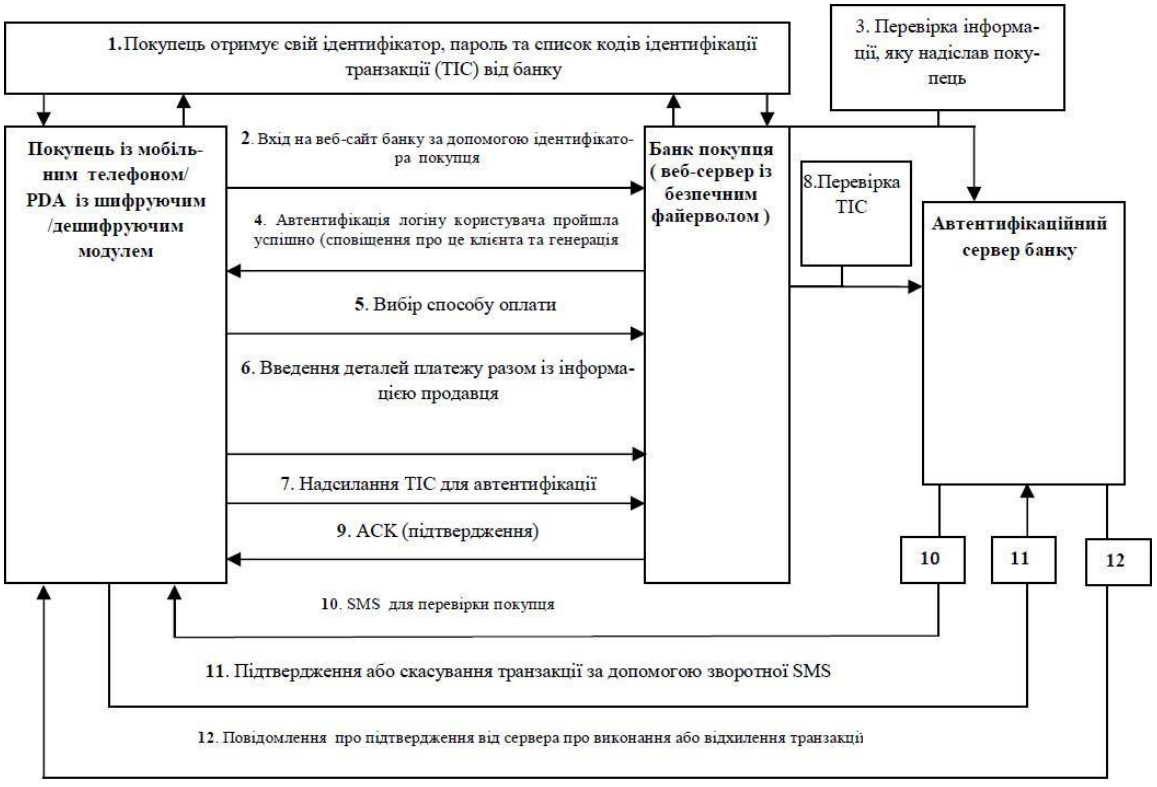


Рисунок 3.6 – Протокол багатофакторної автентифікації

Найбільш уразливими даними у зазначеному протоколі ТІС є коди, які зберігаютьсяна мобільному телефоні, тому вони перебувають у пристроях клієнта у зашифрованому форматі, та захищені паролем, що показано на Рис.3.7.

Клієнт вводить локальний пароль чим відкриває список кодів ТІС і обирає код з цього списку, щоб розпочати транзакцію. Вибір будь-якого коду автоматично розшифровує його та виводить на екран клієнта. Це призводить до переміщення обраного коду із списку у середовище клієнта. Локальнийпароль є ключем розшифрування ТІС коду та є відомий лише йому.

Рисунок 3.7 – Захист ТІС коду в середовищі клієнта

Цей пароль невідомий нікому, навіть серверу банківської установи. Код може бути змінений у будь-який момент за бажанням клієнта.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1 Структура банка [електронний ресурс]. Режим доступу: https://myfin.by/wiki/term/struktura-banka

2 Йона Л.Г., Онацький О.В., Швець О.В. Системи банківської безпеки: Навч.посібник. - Одеса: ДУІТЗ. 2022. 191с.

3 Йона Л.Г., Кюне О.О. Аналіз діючих протоколів криптографічного захисту електронних транзакцій, Цифрові технології, № 1, вип.22, -с.96-102, 2017

4 Kivalov S. Detection and prediction of DDoS cyber attacks using spline functions/ S. Kivalov, I. Strelkovskaya // IEEE TCSET 2022, 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET) – 2022.

5 Горлинський В. Кібербезпека як складова інформаційної безпеки України / Віктор Горлинський, Борис Горлинський // Information Technology and Security. – 2019. – Vol. 7, Iss. 2 (13). – P. 136-148.

6 Tensor method of traffic management problems solving with service quality network parameters maintenance [Text] / I.V. Strelkovskaya, I.N. Solovskaya // Eastern-European Journal of Enterprise Technologies. – 2011. – V. 5, № 3(53) – P. 37-42.

7 Strelkovskaya I.V. Tensor model of multiservice network with different classes of traffic service/ I.V. Strelkovskaya, I.N. Solovskaya// Radioelectron.Commun.Syst – 2013. – 56, 296–303. https://doi.org/10.3103/S0735272713060058.
8 Поповський В. В. Основи теорії телекомунікаційних систем: підручник. – Харків: ХНУРЕ, 2018. – 368с.
9 Стрелковская И.В. Тензорные сплайны в задачах восстановления дискретизированных случайных процессов и полей [Текст] / И.В. Стрелковская, Т.И. Григорьева // Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков: ХНУРЭ, 2007. – Вып. 151. – С. 65-69.
10 Лемешко О. В. Дослідження вдосконаленої тензорної моделі маршрутизації в телекомунікаційній мережі, представленої в базисі міжполюсних шляхів і внутрішніх вузлових пар/ О. В. Лемешко, М. О. Євдокименко // Проблеми телекомунікацій. - 2020. – 1(26). – С. 3-22.
11 Григор'єва Т.І., Йона Л.Г., Мазур Г.Д. , Кравченко І.А. Захист конфіденційної інформації шляхом шифрування на основі тензорних методів. Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2023): матеріали конф.,17-20 липня 2023 р.: тези – Одеса: МГУ, 2023. – С.
12 Стрелковская И.В. Сплайн-матрицы в процедуре рекурсивной оценки состояний сетевых элементов и их режимов [Текст] / Стрелковская И.В., Григорьева Т.И. // Комп'ютерні технології друкарства: Збірник наукових праць. – Львів, 2011. – №25. – С. 84-92
13 Hellman M.E. The Mathematics of Public-Key Cryptography / August 1979 Scientific American, INC, 1979. P. 146-157.
14 Разумова М. А., Хотяїнцев В. М. Основи векторного і тензорного аналізу. — К. : ВПЦ «Київський університет», 2011. – 216 с.
15 De Souza Sánchez Filho E. Tensor Calculus for Engineers and Physicists. — Springer, 2016. – 374 p.
16 Білинський Й. Й. Електронні системи: навчальний посібник / Й. Й. Білинський, К. В. Огороднік, М. Й. Юкиш. – Вінниця: ВНТУ, 2011. – 208 с.
17 Йона О. О. Специфічні чинники активізації загроз економічній безпеці господарюючих суб'єктів [Текст] / О. О. Йона // Технологічний аудит та резерви виробництва. – 2012. –№ 4/6 (8). – С. 31-32. – Режим доступу: http://journals.uran.ua/tarp/article/view/5645
18 Йона О. О. Огляд та систематизація типових моделей загроз безпеці персональних даних, які обробляються в спеціальних інформаційних системах підприємств [Текст]/ О. О. Йона // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2012. – № 8(179), Ч. 1. – С. 110-117.
19 Захарченко М.В. О.В. Онацький, Л.Г. Йона, Т.М. Шинкарчук. Асиметричні методи шифрування в телекомунікаціях. –Криптографічні методи захисту інформації в телекомунікаційних системах тамережах: модуль 2 з дисципліни "Захист інформації в телекомунікаційних системах та мережах": навч. посіб. / Одеса: ОНАЗ ім. О. С. Попова, 2011. – 184 с
20 BankID – что это такое и как работает [електронний ресурс]. Режим доступу: https://ain.ua/2018/11/15/kak-rabotaet-bankid/

21 BankID НБУ [електронний ресурс]. Режим доступу: https://bank.gov.ua/ua/bank-id-nbu

22 Laput G., Yang C., Xiao R., Sample A., Harrison C. (2015). Em-sense: Touch recognition of uninstrumented, electrical and electromechanical objects. 28th Annual ACM Symposium on User Interface Software Technology, UIST. New York. P. 157–166 [in English].

Додаток А ПЕРЕЛІК КОПІЙ ДЕМОНСТРАЦІЙНОГО МАТЕРІАЛУ

Слайд 1

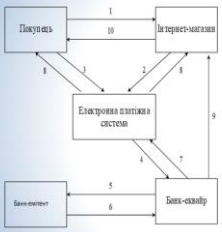
Слайд 2

Слайд 3

- Дослідити сучасні криптографічні методи захисту інформації, що використовуються в банківських системах
- Проаналізувати структуру банківських систем
- Дослідити типи атак та методи захисту від них
- Проаналізувати методи забезпечення конфіденційності та цілісності електронних документів при передачі інформації та удосконалити процес шифрування за створеним ключем шифрування.
- Дослідити методи ідентифікації, підтвердження справжності клієнта та даних системою банківського дистанційного обслуговування.

МЕТА РОБОТИ

Слайд 4



Слайд № 3 Схема функціонування електронної платіжної системи

- **1** Запит на оплату товару;
- **2** Перенаправлення на сервер платежів;
- **3** Введення даних платіжної картки;
- **4,5** Процедура авторизації;
- **6,9** Переказ коштів;
- **7,8** Результат процедури авторизації;
- **10** Видача товару чи послуги

Слайд 5

Слайд № 4 ТИПИ АТАК НА БАНКІВСЬКІ СИСТЕМИ

- Фішинг
- Скімінг
- Кардинг

- Віруси та шкідливі програми
- DDoS-атаки
- Злам рахунків
- Шахрайські дії
- Соціальна інженерія

Слайд 6

Слайд № 5 АТАКИ НА БАНКІВСЬКІ СИСТЕМИ

ЕТАПИ

- Розвідка та підготовка
- Проникнення у внутрішню мережу
- Розвиток атаки і закріплення в мережі
- Компрометація банківських систем і розкрадання грошей
- Приховування слідів злочину

Слайд 7

Слайд № 7 МЕТОДИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

ФІЗИЧНІ МЕТОДИ

- Паспорт
- Біометричні дані
- Підпис
- Персональне ідентифікаційне число

ДИСТАНЦІЙНІ МЕТОДИ

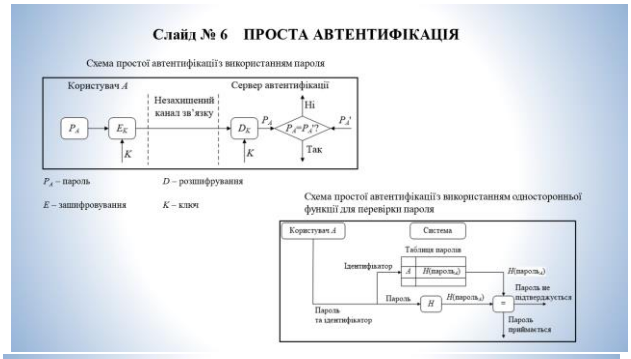
- Електронний банкінг
- Мобільні додатки
- Електронні сертифікати
- Відеоідентифікація
- Багатофакторна автентифікація
- BankID
- Електронний підпис

Слайд 8

Слайд №8 БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЇ

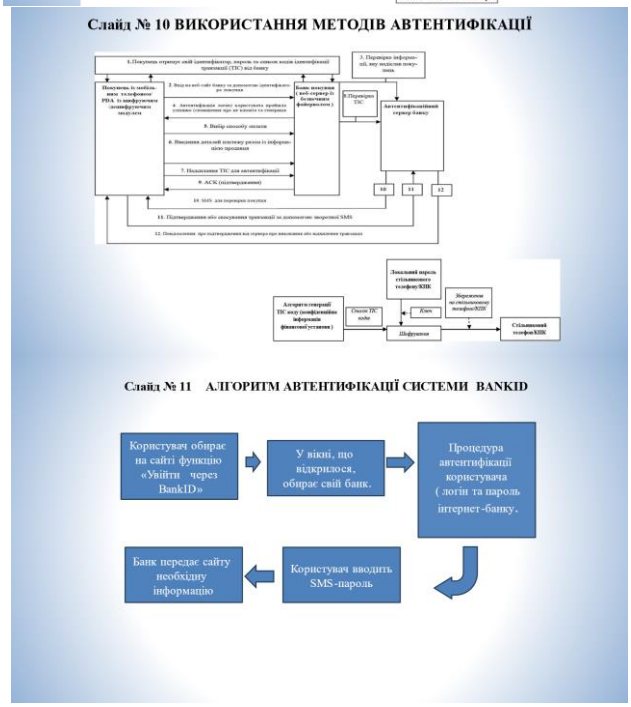
Фактори автентифікації	Приклади факторів автентифікації
Фактор знання	Пароль, Кодова фраза (дівоче прізвище матері), PIN-код
Фактор володіння	Фізичний ключ, USB-токен, Смарт-карта, Смартфон
Фактор властивості	***На основі біометричних характеристик :*** Відбиток пальця, Геометрія руки, Рисунок сітківки ока, Голос ***На основі того, що може зробити користувач:*** Підпис (електронний цифровий підпис), Жест ***На основі того, де знаходиться користувач:*** Поточне місце розташування / позиція, інформація на поточний час; тощо

Слайд 9



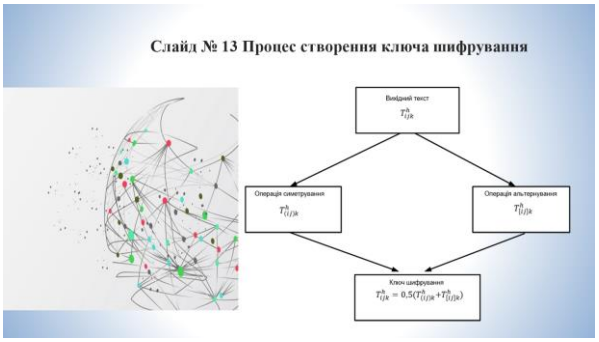
Слайд 10

Слайд 11



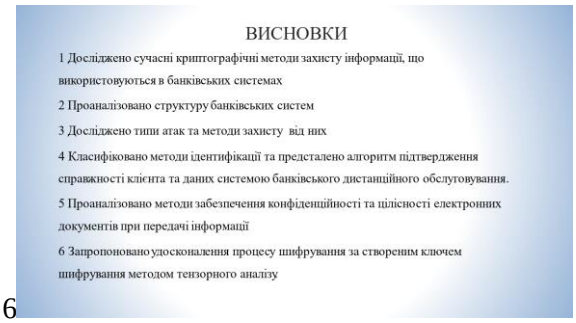
Слайд 12

Слайд 13



Слайд 14

Слайд 15



Слайд 16