ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ЕЛЕКТРОННИХ ПЛАТІЖНИХ СИСТЕМ З ВИКОРИСТАННЯМ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ»

Виконав студент 6 курсу, групи БСЗМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми«Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Бабич О.В.
(прізвище та ініціали)
Керівник Борсуковський Ю.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
"___"_____ 2021 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Бабичу Олександру Владиславовичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія захисту електронних платіжних систем з використанням криптографічних алгоритмів»

керівник магістерської роботи Борсуковський Юрій Володимирович, доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «___» _____ 2021 року №____.

2. Строк подання студентом магістерської роботи 15.12.2021 р.

3. Вихідні дані до магістерської роботи
1)Основні загрози електронно платіжних систем;
2)Основні протоколи захисту електронно платіжних систем;
3)Інтеграція криптографічних методів захисту
4)документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібн розробити)
1. Актуальність проблеми захисту електронно платіжних систем
2. Функціонування криптографічних методів захисту.
3. Критичні точки стійкості в криптографічних алгоритмах.
4. Варіант топології системи управління захистом кінцевих точок корпоративно інформаційної системи.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.
2. Об’єкт, предмет, мета та наукові завдання дослідження.
3. Актуальність електронно платіжних систем.
4. Аналіз протоколів захисту.
5. Призначення та можливості криптографічних алгоритмів захисту.
6. Міжнародні стандарти захисту.
7. Стійкість алгоритмів шифрування.
8. Надстійкі та проблемні в інтегруванні алгоритми
9. Хешування та шифрування.
10. Висновки за результатами роботи.

6. Дата видачі завдання 27.09.2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконанн етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцеви точок корпоративних інформаційних систем.	27.09.2021 р.	
2.	Аналіз наукової та технічної літератури з питань тем магістерської роботи.	03.10 2021 р.	
3.	Аналіз методів та засобів захисту кінцевих точок.	28.10 2021 р.	
4.	Розроблення варіанту топології системи управлінн захистом кінцевих точок корпоративно інформаційної системи.	07.11.2021 р.	
5.	Розроблення рекомендацій щодо застосуванн технології управління захистом кінцевих точо корпоративної інформаційної системи.	18.11.2021 р.	
6.	Оформлення результатів дослідження. Проходженн плагіату	27.11.2021 р.	
7.	Підготовка доповіді до захисту.	15.12.2021 р.	

Студент Бабич О.В.
(підпис) прізвище та ініціали

Керівник магістерської робот Борсуковський Ю.В.
(підпис) прізвище та ініціали

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Бабич О.В до захисту магістерської роботи
(прізвище та ініціали)

спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія захисту електронних платіжних систем з використанням криптографічних алгоритмів».

Магістерська робота і рецензія додаються.

Директор інституту _____ _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Бабич О.В. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2020 року по 2022 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту _____ Черниш О.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерськоїї роботи

Студент ***Бабич О.В*** обрав тему роботи, метою якої було дослідити зміст технології захисту електронно платіжних систем та розробити варіант створення алгоритму на базі криптостійкого алгоритму. Перелік використаних джерел свідчить про вміння магістром розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Бабич О.В. показав відмінну теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.
Все це дозволяє оцінити виконану магістерську роботу студента Бабича О.В. на оцінку **«добре»** та присвоїти йому кваліфікацію 2149.2 професіонал з організації інформаційної безпеки, викладач закладу вищої освіти.

Керівник магістерської роботи _____ Борсуковський Ю.В.
(підпис) (прізвище та ініціали)
“____” _____ 2021 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Бабич О.В.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії
Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 52 сторінки, 12 рисунків, 13 джерел.

Об'єкт дослідження – процес забезпечення захисту електронно платіжних систем

Предмет дослідження – технологія захисту електронно платіжних систем з використанням криптографічних алгоритмів

Мета роботи – розробити варіант стійкого алгоритму на базі існуючих.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, створення та інтеграція.

В роботі проведено аналіз проблеми забезпечення кібербезпеки електронно платіжних систем та визначено мета розобки варіанту стійкого криптографічного алгоритму на базі існуючих. Проаналізовано існуючі алгоритми шифрування, та протоколи захисту.

Досліджено методи та засоби створення, використання протоколів захисту, концепції електронно платіжних систем та інтеграції криптографічних алгоритмів .

На основі досліджень проведених в роботі розроблено криптографічний алгоритм на базі існуючого та приклад його використання в електронно платіжній системі.

Галузь використання – кібербезпека банківської структури.

ЕЛЕКТРОННО ПЛАТІЖНА СИСТЕМА, КІБЕРБЕЗПЕКА, КРИПТОГРАФІЧНІ АЛГОРИТМИ, ПРОТОКОЛИ ЗАХИСТУ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЕПС –Електронна платіжна система;

ДСТУ – державний стандарт України;

НСД – несанкціонований доступ;

НБУ – національний банк України;

ЕЦП – електронно-цифровий підпис;

ПЗ – програмне забезпечення;

СУБД – система управління базою даних;

АКА – автомат касир;

ІБ – інформаційна безпека;

ЦСК –центр сертифікації ключів.

АСОІБ - автоматизованих систем обробки інформації банків

ОЕД- Обмін електронними даними

ВСТУП

Невід'ємною частиною господарського життя людського суспільства на певному етапі історичного розвитку стають кошти. При цьому розрахунки можуть набувати як готівкової, так і безготівкової форми. Їхня еволюція від простої, примітивної форми (готівкової) до більш доцільної (безготівкової) пройшла багатовіковий шлях. Грошові розрахунки з використанням безготівкових розрахунків набагато вигідніші з усіх поглядів. Це значно прискорюють процес оплати, полегшують його, сприяють зниженню витрат звернення. Швидкий розвиток Інтернету в 90-х роках минулого століття змусив змінити саму сутність грошей, їх форму та призначення.

В останні роки у фінансовому світі досить важливу сходинку зайняли електронні платіжні системи, що пов'язано з активною еволюцією грошей як засобу платежу.

Електронні платіжні системи (ЕПС) – це технологія прямих взаєморозрахунків між учасниками угоди без додаткових умов за допомогою інтернету чи мобільного зв'язку. Через оперативність застосування ЕПС сприяло різкому розвитку електронної комерції. Сьогодні ЕПС – зручний засіб розрахунків з операторами стільникового зв'язку, інтернет-провайдерами, великими магазинами та ін.

На даний момент як ЕПС застосовується кілька основних технологій:

1. Дистанційні фінансові послуги

2. Сервіси мобільних платежів

Мобільний банкінг- сервіс який допомогає в управлінні коштами на банківському рахунку за допомогою SMS-повідомлень, що відправляються на спеціальний номер банку, складених за допомогою типових шаблонів.

Мобільні операторські платежі. Це такий електронний платіжний сервіс операторів мобільного зв'язку, що дозволяє оплачувати товари та послуги за

допомогою мобільного телефону чи інтернет-порталу за допомогою коштів на особовому рахунку чи банківській картці.

При створенні платіжної системи однією з основних розв'язуваних завдань є вироблення та дотримання загальних правил обслуговування карток, випущених емітентами, що входять до платіжних систем, проведення взаєморозрахунків і платежів. Ці правила охоплюють як чисто технічні аспекти операцій з картками - стандарти даних, процедури авторизації, специфікації на обладнання та інші, так і фінансові аспекти обслуговування карт - процедури розрахунків з підприємствами торгівлі та сервісу, що входять до складу приймальної мережі, правила взаєморозрахунків між банками та і т.д.

Завдяки швидкому зростанню та розповсюдженню електронних платіжних систем, постало питання щодо інтеграції методів безпеки в системи розрахункових операцій, з використанням технологій захисту на прикладі криптографічних алгоритмів. Тому тема магістерської роботи є досить актуальною то своєчасно.

1.ДОСЛІДЖЕННЯ ТЕОРЕТИЧНИХ АСПЕКТІВ ЕЛЕКТРОННО-ПЛАТІЖНИХ СИСТЕМ

1.1 Електронно-платіжні системи в сучасному світі

Питання безпеки електронних платіжних систем є складним завданням для фінансового сектора та регуляторів. Існують дві серйозні проблеми – несанкціоновані списання коштів з банківських карток або рахунків юридичних осіб та загальна гарантія збереження платежів, що здійснюються через небанківські системи переказу платежів. Заходи, що вживаються в останні роки, змогли зробити електронні переклади більш безпечними.

Під терміном "електронна платіжна система" (ЕПС) розуміється система розрахунків, при якій платежі проводяться по інтернет-каналах, традиційної обробки платіжних доручень не відбувається.

Під це визначення потрапляють:

- розрахунки за допомогою банківських карток традиційних систем Visa, MasterCard та ін.. Задля повної гарантії захисту транзакцій виникає проблема несанкціонованих списань внаслідок перехоплення трафіку чи отримання номерів карток;
- програми міжбанківських розрахунків електронними каналами зв'язку, у тому числі швидких платежів, що здійснюються банками за номерами телефонів;
- розрахунки через електронні гаманці («Яндекс.Гроші»,»Kiwi», «webmoney»,та інші);
- розрахунки через інфраструктуру мобільних операторів та інші сучасні рішення.

Якщо говорити про захист від несанкціонованих переказів ЕПС загалом, незалежно від рівня кожної конкретної моделі до них діють однакові вимоги.

Серед найбільш уразливих місць:

- інтернет-трафік між учасниками обміну електронними повідомленнями про фінансові трансакції (банками, операторами платіжних гаманців, банкоматами, клієнтами);

• обробка інформації всередині банку або оператора (наприклад, Яндекс.Денег), коли дані можуть бути доступними співробітникам;

• постійна доступність систем платежів для клієнтів, відсутність збоїв у роботі та лінії зв'язку.

Наявність цих уразливостей змушує банки та операторів забезпечувати захист трафіку при пересиланні доступними способами (передача захищеними каналами, шифрування) та розробляти моделі автентифікації відправника та одержувача коштів.

При цьому у роботі банку або оператора платежів виникають проблеми:

• визначення взаємної автентичності учасників трансакції під час встановлення з'єднання;

• забезпечення конфіденційності та справжності платіжних доручень, що надсилаються по інтернету, та інших документів;

• захист процесу надсилання, формування доказів відправлення та отримання документів;

• забезпечення виконання документа (наприклад, постійне перебування залишку на кореспондентському рахунку банку, що дозволяє організувати платіж).

Банк та оператор ЕПС зобов'язані реалізувати механізми захисту клієнтів від несанкціонованих списань грошових коштів, конкретні вимоги до яких визначаються політиками операторів та регламентами НБУ:

• управління доступом клієнта, співробітників оператора та одержувача, створення механізму автентифікації;

• контроль автентичності та цілісності інформації у повідомленні;

• забезпечення конфіденційності відомостей у процесі передачі;

• неможливість відмовитися від авторства доручення на надсилання коштів або повідомлення;

• гарантії доступу до ресурсів та не втрати повідомлення на шляху, його доставки;

• неможливість оператора чи банку відмовитися від виконання доручення на переказ чи платіж;

• збереження даних за дорученнями та повідомленнями.

Для здійснення платежів за допомогою банківських карток міжнародні системи переказів застосовують власні заходи ІБ міжкарткових переказів, що кореспондують з вимогами НБУ. Для інших операторів електронних платежів, що здійснюють понад 6 мільйонів переказів на рік, працює програма сертифікації Qualified Security Assessor (QSA).

В Україні працюють представництва кількох організацій, які мають право на видачу сертифікату, і він буде надано, якщо оператор відповідає наступним вимогам:

• його діяльність відповідає міжнародному стандарту Payment Card Industry Data Security Standard (PCI DSS);

• оператор сервісу платежів отримав сертифікат на відповідність міжнародним вимогам до менеджменту ІБ кредитних організацій у сфері розробки, впровадження та супроводу програмних засобів ISO/IEC 27001:2005;

• оператор працює з використанням електронно-цифрового підпису (ЕЦП);

• шифрування здійснюється дозволеними засобами криптографічного захисту, розробленими організаціями, які мають ліцензії на право провадження діяльності з надання, технічного обслуговування криптографічних засобів.

Стандарт захисту інформації в індустрії платіжних карток PCI DSS був розроблений міжнародними операторами платіжних карток Visa та MasterCard.

1.2 Аналіз основних загроз ЕПС

В Інтернеті існує безліч варіантів шахрайства, що дозволяють зловмисникам спритно обманювати людей, красти особисті дані, а згодом і гроші. В електронно-платіжних системах виділяються наступні:

Розглянемо перелік загроз, що виникають при пересиланні платіжних та інших повідомлень:

- несанкціонований доступ до ресурсів та даних системи (підбір пароля, злом систем захисту та адміністрування, маскарад);

- перехоплення та підміна трафіку (підробка платіжних доручень, атака типу "людина посередині");

- IP-спуфінг (підміна мережевих адрес);

- відмова у обслуговуванні;

- Атака на рівні додатків;

- сканування мереж або мережна розвідка;

- Використання відносин довіри в мережі.

Причини, що призводять до появи подібних уразливостей:

- відсутність гарантії конфіденційності та цілісності переданих даних;

- Недостатній рівень перевірки учасників з'єднання;

- недостатня реалізація чи некоректна розробка політики безпеки;

- відсутність чи недостатній рівень захисту від несанкціонованого доступу (антивіруси, контроль доступу, системи виявлення атак);

- існуючі вразливості операційних систем (ОС), ПЗ, СУБД, веб-систем і мережевих протоколів;

- непрофесійне та слабке адміністрування систем;

- проблеми при побудові міжмережевих фільтрів;

- збої у роботі компонентів системи або їх низька продуктивність;

- уразливості під час управління ключами.

Основні види атак на фінансові повідомлення та фінансові транзакції:

- розкриття вмісту;

- Подання документа від імені іншого учасника;

- несанкціонована модифікація;

- Повтор переданої інформації.

Існує чотири основні форми віддаленого банківського обслуговування клієнтів [5]:

- домашнє (телефонне) обслуговування;

- Розрахунок з автоматичним касовим апаратом (банкоматом);

- Розрахунок у точці продажу;

- фінансовий сервіс із використанням всесвітньої мережі Інтернет.

Домашнє банківське обслуговування дозволяє клієнтам отримати доступ до банківських та інформаційних послуг, не виходячи з дому.

Переваги цього виду обслуговування:

- для клієнта - велика доступність даних та управління своїми фінансовими справами;

- для банку – зменшення вартості обслуговування.

Введення даних для платежу при голосовому зв'язку (ідентифікатор, номер рахунку, розмір платежу) здійснюється клієнтом або з клавіатури телефону або голосом (що менш надійне з точки зору безпеки, але технічно доступне).

Банківський автомат-касир (АКА, банкомат) - спеціалізований пристрій, призначений для обслуговування клієнта без банківського персоналу. Це найважливіша частина банківської системи, призначена, переважно, видачі готівки. Крім цієї функції АКА може виконувати ряд додаткових, серед яких:

- Перевірка стану рахунку клієнта;

- Зміна параметрів рахунку клієнта;

- Здійснення різних платежів;

- надання інформації про:

а) страховий поліс клієнта;

б) котирування цінних паперів на фондовому ринку;

в) купівлі та продажу акцій;

г) обмінні курси валют тощо.

Системи, що забезпечують розрахунки продавця та покупця у точці продажу, (point-of-sale, POS). В основному всі термінали, підключені до цих систем, розміщені на підприємствах торгівлі. Більшість таких терміналів встановлені в супермаркетах, тому що там відбувається велика кількість покупок протягом дня, а також в інших магазинах та на автозаправних станціях.

Системи POS забезпечують такі послуги:

- перевірку та підтвердження чеків;

- перевірку та обслуговування дебетових та кредитних карток;

- Використання системи електронних розрахунків.

Банки, що фінансують систему розрахунків у точці продажу, таким чином розширюють список своїх клієнтів шляхом надання їм більших зручностей для покупок у магазинах з використанням віддалених пристроїв. Торгівля, у свою чергу, збільшує кількість клієнтів, розширює управління майном, зберігає час клієнтів та зменшує ризик втрати готівки.

Фішинг – витончений спосіб шахрайства, що передбачає крадіжку особистих даних, а саме паролів, банківських рахунків, логінів, номерів пластикових карток. Сутність методу полягає у надсиланні листа по e-mail від імені будь-якої авторитетної організації, наприклад, банківської установи. У тексті співробітники псевдо-організації рекомендують оновити або передати будь-яку інформацію під різним приводом. Особливість фішингу полягає в детальному опрацюванні шахрайської схеми. Для більшої достовірності зловмисники створюють сайти, які точно копіюють інтернет-ресурс підставної організації. Відтак людина не підозрює про обман, потрапляє на «гачок» і втрачає гроші. Щоб уникнути подібних неприємностей, важливо виявляти граничну пильність та навчитися обчислювати підроблені сайти.

Скіммінг - напрямок, що передбачає застосування спеціальних пристроїв, що дозволяють вважати необхідну інформацію з магнітної стрічки пластикової картки. Алгоритм дій виглядає так:

Спочатку зловмисник фіксує скіммер на приймачі банкомату. Особливість цього пристрою полягає в тому, що воно майже не відрізняється від заводського гнізда. В основі приладу лежить спеціальна схема, яка забезпечує зчитування даних. Водночас, до банкомату кріпиться відеокамера, метою якої є фіксація PIN-коду. На останньому етапі шахрай робить копію картки та за допомогою вкраденого коду знімає всі кошти.

Однією з переваг електронних грошей є неможливість їхньої підробки (у класичному розумінні). Їх не можна надрукувати, а після придбати щось із застосуванням підроблених банкнот. Віртуальна валюта має електронно-цифрову форму і використовується тільки в мережі, але це не гарантує стовідсотковий захист, розроблено безліч варіантів шахрайства, що дозволяють обманювати довірливих людей.

Але існує кілька основних способів захисту грошей, що дозволяють зберегти електронні заощадження від зловмисників:

Паролі. Практично кожен користувач глобальної мережі щодня стикається з необхідністю введення спеціальних кодів для входу в особистий кабінет того чи іншого сайту. Схожа система впроваджена і в електронних платіжних сервісах, багато з яких застосовують цей спосіб як основний метод забезпечення безпеки. На практиці може використовуватися не один, а відразу кілька паролів, які бувають стаціонарними або такими, що змінюються. У разі код оновлюється при кожному відвідуванні ресурсу. Нова комбінація надходить на e-mail або мобільний телефон. Контрольний пароль зазвичай вводиться при проведенні будь-якої фінансової операції в мережі. Такий захід дозволяє додатково захистити користувача, який здійснив транзакцію та тимчасово відійшов від комп'ютера. Інша людина вже без вказівки на контрольний код не зможе провести будь-яку фінансову маніпуляцію і скористатися чужими коштами. Розглянута система має широкий попит у багатьох платіжних системах, у тому числі Яндекс.Гроші, Qiwi та інші (називається «Платіжний пароль»). Питання безпеки грошей добре продумане ще в одному сервісі - Вебмані. Тут одного пароля для входу в гаманець недостатньо - потрібна наявність файлу ключів. Застосування PIN-коду як захист характерне і для банківських карток. Він зазвичай складається з чотирьох цифр, які кожен користувач задає індивідуально. Як показала практика, такий спосіб захисту електронних грошей не відрізняється великою надійністю, а сама система безпеки схильна до злому. Якщо ж зловмисник вкрав картку і намагається підібрати пароль, «пластик» блокується після трьох допущених помилок. Але лише пароль не дає достатній рівень надійності, тому його рекомендується поєднувати з іншими способами захисту.

Файли ключів. Розглянутий метод використовується у Вебмані та забезпечує додаткову надійність. Його сутність у тому, що після проходження реєстрації клієнту видається спеціальний файл, у якому містяться ключі від сховища. Для отримання доступу до накопичень, користувач повинен мати під рукою пароль, а також згаданий вище документ. Крім того, у файлу гаманця передбачений свій

захист, що забезпечує безпеку грошей. Тут також необхідно ввести певну комбінацію букв, цифр та символів. Для додаткового захисту особистих заощаджень згаданий вище файл рекомендується зберігати поза жорстким диском комп'ютера, наприклад, на флешці. В іншій ситуації після проникнення в ПК зловмисник отримує всі необхідні дані для злому гаманця.

Набір символів на екрані. Одним із способів захисту від різних хробаків, троянів та вірусів є екранна клавіатура. Така методика застосовується в одній із найпопулярніших систем EasyPay. На відміну від інших ЕПС, введення необхідних символів не з звичайної клавіатури, а через спеціальне зображення на екрані монітора. Така методика захисту має дві сторони. У разі набору пароля інша людина може підглянути інформацію, а потім використовувати її для злому. Якщо ж уважно підійти до цього моменту та виробляти набір, коли сторонні люди відсутні, можна захистити практично всі види електронних грошей від клавіатурних шпигунів. Останні являють собою програми, які проникають у комп'ютер користувача та зчитують спеціальний лог-файл (саме в ньому зберігається інформація про введені через клавіатуру символи). Але існують інші програми, які фіксують, а згодом відтворюють будь-які дії користувача, у тому числі і переміщення мишкою. Отже, приймати рішення про актуальність застосування звичайної або дисплейної клавіатури необхідно індивідуально з урахуванням поточної ситуації.

Спеціальна фраза. Для підвищення рівня захисту своїх коштів кожен користувач повинен придумати одне або кілька слів. Застосування такої методики дозволяє захиститися від фішингу.

Блокування рахунку. До цього кроку доводиться вдаватися у ситуації, коли розглянуті вище способи не спрацювали або можуть забезпечити необхідний рівень захисту. Таке можливо, коли людина випадково втратила пароль, стала жертвою крадіжки даних із ПК або не може знайти пластикову картку. Отже, якщо основні засоби захисту не спрацювали, користувач надсилає SMS на певний номер або здійснює дзвінок з командою блокування електронного рахунку. Цей захід підходить для крайніх випадків, але саме він забезпечує кращий захист електронних грошей у надзвичайній ситуації.

Тому досить важливо вжити деяких заходів, спрямованих на безпеку будь-якої транзакції в мережі. Адже схеми несанкціонованого доступу до чужих віртуальних заощаджень прогресують, а часто онлайн-шахраї випереджають на крок розробників захисних механізмів.

1.2.1 Криптографія як засіб захисту ЕПС

Шифрування – це найбільш широко використовуваний механізм захисту в обчислювальних системах. Кожна електронна платіжна система використовує свої методи, алгоритми шифрування, протоколи передачі для виконання безпечних транзакцій і передачі. Одні системи використовують алгоритм шифрування RSA та протокол передачі HTTPs, інші використовують алгоритм DES та протокол SSL для передачі зашифрованих даних.

Криптографія - засіб, як зберегти інформацію в таємниці, створює захист інформації за допомогою шифрування. Шифрування – це перетворення «відкритого тексту» з метою зробити незрозумілим його сенс. Завдяки перетворенню виходить шифротекст. Процес зворотного перетворення – розшифрування (розшифрування, дешифрація) – відновлення вихідного тексту із шифротексту.

Шифрування використовується для забезпечення захисту паролів, що застосовуються для аутентифікації користувачів, системної інформації, а також інформації, що передається в лініях зв'язку, захисту даних у файлах та базах даних тощо.

Криптографічний алгоритм (шифр або алгоритм шифрування) – це математичні функції, що використовуються для шифрування та розшифрування (використовується дві функції: одна – для

шифрування, інша – для розшифрування).

У сучасній криптографії надійність криптографічного алгоритму забезпечується використанням ключів. Зашифрований текст завжди можна розшифрувати у початковий вигляд, знаючи відповідний ключ. Деякі алгоритми шифрування використовують різні ключі для шифрування та розшифрування.

Під криптосистемою розуміється алгоритм шифрування, а також безліч різноманітних ключів, відкритих та шифрованих текстів.

У загальному випадку порядок роботи системи обміну повідомленнями, секретність інформації в якій забезпечується за допомогою шифрування, можна представити схемою, показаною на рис. 1.1

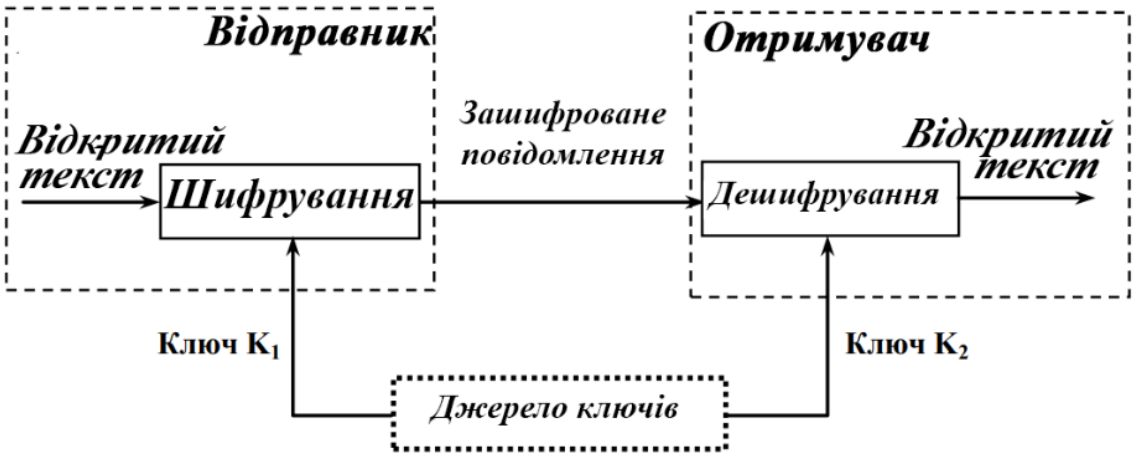

Рис 1.1 Загальна система криптографічного зв'язка

Існує два різновиди алгоритмів шифрування з використанням різних типів ключів: криптосистеми з відкритим ключем та симетричні криптосистеми.

Симетричним називають криптографічний алгоритм, якому ключ, який використовується для шифрування повідомлення, може бути отриманий з ключа розшифрування та навпаки. У більшості симетричних систем використовується лише один ключ, який має зберігатися у секреті. Такі алгоритми називають одноключовими, або алгоритмами із секретним ключем.

Алгоритми шифрування з відкритим ключем ще називають асиметричними алгоритмами шифрування вони влаштовані так, що ключ, який використовується для шифрування, відрізняється від ключа, застосовуваного для розшифрування повідомлення, і ключ розшифрування не може бути за прийнятний час розрахований через ключ шифрування. Тому ключ шифрування не потрібно тримати в таємниці та її називають відкритим. Ключ розшифрування є таємним, або секретним. Симетричну криптосистему можна порівняти із сейфом, а ключ – із комбінацією, що дозволяє відкрити сейф кожному, хто цю комбінацію знає. Алгоритм шифрування з відкритим ключем можна порівняти з поштовою

скринькою: просто опустити в нього пошту зашифрувати повідомлення за допомогою відкритого ключа, але складно повідомлення отримати – це може зробити тільки людина, має спеціальний ключ розшифрувати повідомлення може тільки той, хто знає відповідний таємний ключ.

1.2.2 Використання протоколів захисту в електронно-платіжних системах

Більшість електронних платіжних систем, зокрема інтернет-магазини, використовують у роботі web-браузери. Враховуючи, що SSL вбудований практично у всі відомі web-браузери, забезпечення безпеки даних, що передаються в 99% випадків [11] здійснюється на його основі. Однак слід зазначити такі негативні сторони SSL, які необхідно враховувати при прийнятті рішення про використання цього протоколу при організації захищеного каналу взаємодії між учасниками платіжних електронних транзакцій.

• Відсутність автентифікації покупця. Незважаючи на те, що в протоколі SSL закладено можливість запиту сертифіката покупця, автентифікація покупця є опціональною і, як правило, не здійснюється, що унеможливлює використання SSL при операціях з банківським рахунком.

• Аутентифікація продавця URL. Сертифікат, що надається продавцем, свідчить лише про зв'язок останнього із зазначеною URL-адресою, при цьому немає жодної інформації про взаємодію продавця та банку, що обслуговує зазначену платіжну систему.

• Відкритість реквізитів покупця. Незважаючи на те, що вся інформація, що передається в рамках SSL, є зашифрованою, дані про банківські реквізити покупця потрапляють до продавця у відкритому вигляді.

• Експортні обмеження протоколу. Незважаючи на те, що в 1999 р. Державний Департамент США ухвалив рішення про зняття експортних обмежень, деякі браузери підтримують протокол SSL з експортними обмеженнями, що стосуються довжини ключів для алгоритмів шифрування інформації, що істотно знижує захищеність даних, що передаються.

Як було показано в попередньому розділі, одним з основних недоліків протоколу SSL з точки зору можливості його використання в платіжних системах із застосуванням пластикових карток є система сертифікації, що не дозволяє автентифікувати покупця, а також автентифікує продавця виключно URL. Крім цього для здійснення платежів покупцю необхідно надсилати продавцю свої платіжні реквізити, що дозволяло недобросовісному продавцю здійснити шахрайство стосовно покупця.Для усунення зазначених недоліків VISA International спільно з MasterCard був розроблений протокол SET - Secure Electronic Transaction, орієнтований на платіжні системи з використанням пластикових карток.

Протокол SET крім чотирьох сутностей, характерних для будь-якої платіжної системи – покупця, продавця, банку-емітента та банку-еквайєра, вводить дві нові – центр сертифікації (ЦС, CA – Certificate Authority) та платіжний шлюз (Payment Gateway) рис 1.2

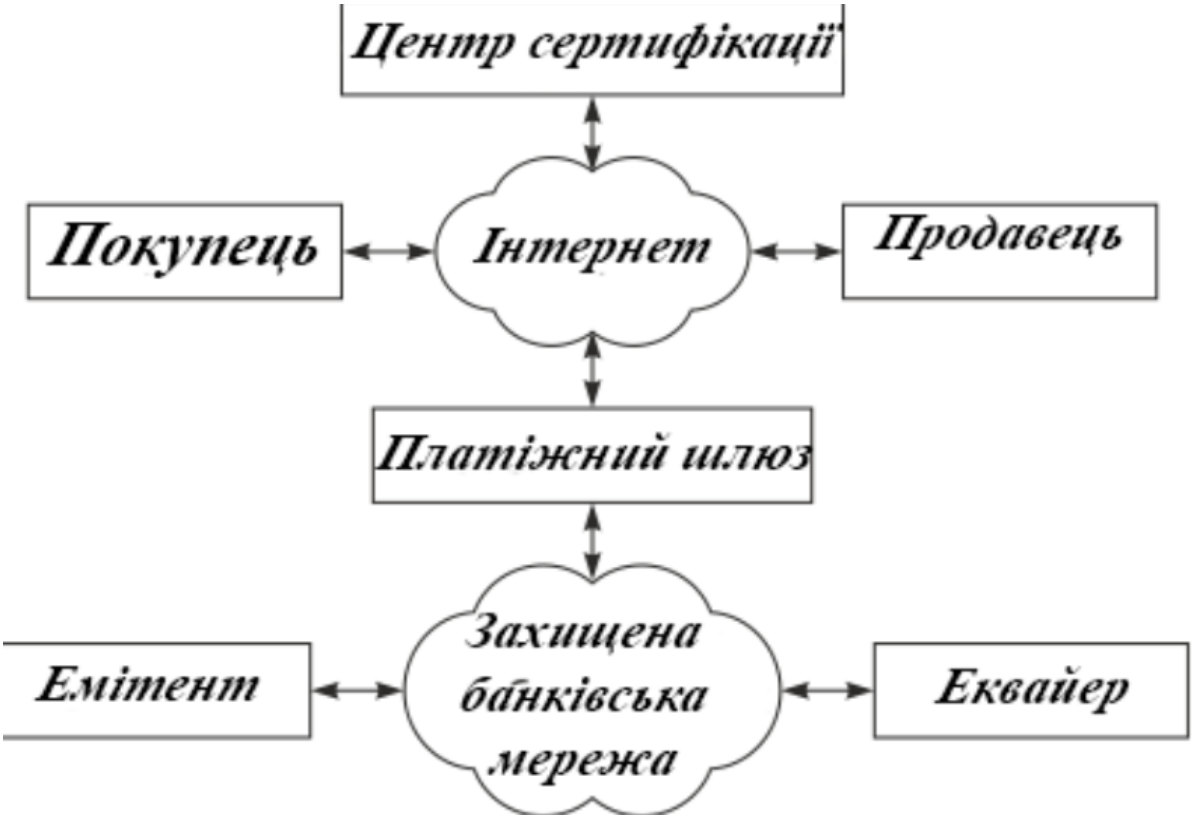

Рис. 1.2 Взаємодія учасників платіжної транзакції за допомогою протоколу SET

Функція центрів сертифікації полягає у формуванні, розповсюдженні, підтримці та анулюванні сертифікатів; платіжний шлюз забезпечує підтримку

сертифікатів та взаємодію з платіжною системою.Перед початком транзакції покупець, продавець та платіжний шлюз мають отримати сертифікати, щоб бути автентифікованими у системі. Всі дані передаються відкритими каналами зв'язку в зашифрованому вигляді, при цьому безпосереднього зчитування інформації з пластикової картки не відбувається - власник картки аутентифікує себе за допомогою відповідного сертифіката. Взаємодія емітента та еквайєра здійснюється за допомогою захищеної міжбанківської мережі

Процес захищеної взаємодії двох абонентів за допомогою криптографічних перетворень показано на рис. 1.3 .

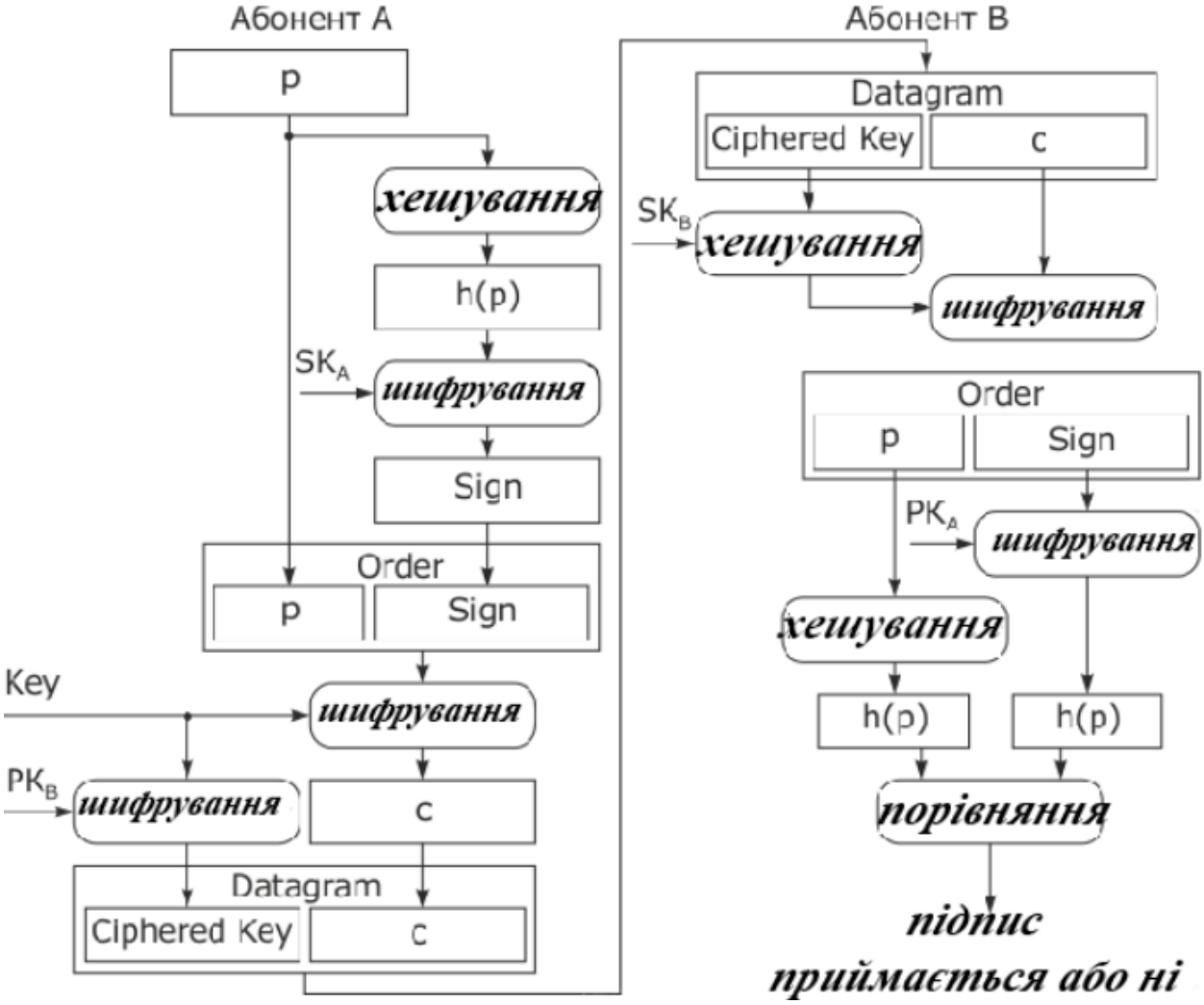

Рис 1.2 Криптографічні перетворення на прикладі двох абонентів

Абонент *A* формує повідомлення *p* потім хешує його та зашифровує на своєму секретному ключі SK_A отримуючи цим підпис повідомлення Sign.

Об'єднавши оригінал повідомлення та підпис, абонент *A* отримує повідомлення Order, яке шифрує на сеансовому ключі Key, згенерованому випадковим чином. Отримане повідомлення *C* є однією з частин повідомлення Datagram, що надсилається. Другою частиною Datagram є Ciphered Key – сеансовий ключ, зашифрований на відкритому ключі PK_B абонента *B*

Повідомлення Datagram передається на транспортний рівень і надсилається абоненту *B*. Отримавши вказане повідомлення, абонент *B* витягує з нього зашифрований сеансовий ключ Ciphered Key та розшифровує його на своєму секретному ключіSK_B. Потім абонент *B* витягує з Datagram фрагмент *C* і розшифровує за допомогою сеансового ключа, отримуючи цим повідомлення Order. Далі слідує перевірка підпису абонента *A* шляхом розшифрування sign з використаннямPK_A відкритого ключа абонента A та порівняння отриманого хеш-образу *h (p)* з хеш-образом повідомлення *p*.

Протокол SET підтримує чотири криптографічні алгоритми:

- *RSA - для формування та перевірки електронного цифрового підпису переданого повідомлення, а також для зашифрування та подальшого розшифрування сеансового ключа;*
- *DES - для зашифрування та подальшого розшифрування інструкцій продавцю та платіжному шлюзу з прикріпленим подвійним цифровим підписом;*
- *SHA-для хешування інформації;*
- *HMAC-SHA-1 — щоб створити код автентифікації повідомлення.*

1.3 Загальні вимоги до захисту інформції в платіжних системах

Система захисту інформації в платіжній системі забезпечує захист інформації щодо переказу коштів на всіх етапах її формування, оброблення, передавання та зберігання відповідно до вимог законодавства України. Організація яка виступає в якості платника встановлює організаційні, технічні та технологічні вимоги щодо захисту інформації в платіжній системі та для суб’єктів переказу коштів. Корстувачі платіжної системи повинні слідувати вимогам щодо захисту

інформації, які встановлені законодавством України та цими правилами. Про порушення щодо вимог інформаційної безпеки в платіжній системі учасники платіжної системи зобов’язані повідомляти Платіжну організацію. У випадках наявності ознак вчинення злочину учасники також зобов’язані повідомляти про такі порушення правоохоронні органи. Головною метою впровадження у платіжній системі організаційних заходів та технічних засобів захисту інформації є:

- захист інформації щодо електронних документів на переказ вид несанкціонованого доступу, спотворення чи знищення;
- унеможливлення здійснення протиправних дій щодо інформації та інформаційних систем обслуговуючим персоналом.

Головними об'єктами захисту в системі є:

- електронні документи на переказ та їх архіви;
- інформаційні повідомлення між платіжною організацією, розрахунковим банком, операторами послуг платіжної інфраструктури, учасниками платіжної системи та іншими суб'єктами переказу коштів;
- інформація з обмеженим доступом, що зберігається в базах даних платіжної системи та резервних копій;
- інформація про платників та отримувачів переказів;
- засоби обробки та захисту інформації (програмно-технічні та криптографічні);
- серверне та мережеве обладнання задіяне для переказу коштів;
- криптографічні ключі, паролі та інша конфіденційна інформація, яка використовується для авторизації програмно-технічними засобами та користувачами.

Користувачі ЕПС зобов’язані мати в своїй структурі посади працівників які будуть відповідальні за управління інформаційною безпекою та адміністрування засобів захисту інформації.

Задля протидії та запобіганню порушень з боку інформаційної безпеки в платіжній системі. Організація виконує такі міри:

- виявлення джерела загрози безпеці інформації кібербезпеці та аналіз потенційних можливостей внутрішніх та зовнішніх порушників;
- оцінка можливих уразливостей інформаційних систем, а також програмно-апаратних засобів захисту інформації, комутаційного та мережевого обладнання;
- досліджує можливі способи порушення безпеки інформації;
- аналізує та оцінює можливі наслідки від виникнення загроз ІБ, порушення деяких властивостей інформації(цілісність, доступність, конфіденційність), а також системи захисту у інформації в цілому.

Завдяки таким заходам, платіжна організація повинна сформувати зміни до вимог ІБ та КБ користувачів платіжної системи.

З ціллю забезпечення безпеки інформації та зниження ризикам ІБ в платіжній системі, організація платіжної системи, користувачі платіжної системи, спеціаліст надання послуг платіжної інфраструктури виконує такі криптографічні заходи :

- використання лише сертифікованих засобів криптографічного захисту для інформації, вимога щодо захисту якої встановлена законом;
- застосування удосконаленого або кваліфікованого ЕЦП на електронних документах на переказ;
- адміністрування розподілом прав доступу користувачів до інформаційних систем, аудит засобів доступу до них, ідентифікація виконання дій учасниками, а також протоколювання цих дій;
- відповідність парольним політикам;
- керування генерацією, обліком та поширенням ключової інформації;
- використання лише захищених каналів та протоколів під час передачі інформації;
- використання засобів захисту баз даних;

- здійснення антивірусного захисту на серверах, та робочих комп’ютерах персоналу
- аудит, контролювання мережевого трафіку з метою виявлення злочинних дій і спроб виконати НСД до програмно-апаратних компонентів;
- фільтрування та обмеження мережевого трафіку, протоколами, портами;
- створення бекапів, резервне копіювання системних компонентів

Висновки до першого розділу

Проаналізовано поняття електронні платіжні системи. Зазначено, що це технологія або ж сервіс, що являє собою сукупність методів, домовленостей і підтехнологій, що дозволяє проводити розрахунки між контрагентами мереж передачі даних.

Розглянуто основні загрози електронно платіжних систем, положення щодо використання криптографічних засобів безпеки та насамперед протоколи безпеки.

Встановлено проблеми захисту електронних платіжних систем, а також вимоги щодо надання можливості протидії кіберінцидентам.

2 АНАЛІЗ ОСНОВНИХ ПРОБЛЕМ ЗАХИСТУ ЕПС

2.1 Основні засоби та методи захисту ЕПС

Стратегія інформаційної безпеки платіжних систем дуже відрізняється від аналогічних стратегій інших компаній та організацій. Це зумовлено специфічним характером загроз, а також публічною діяльністю банків, які змушені робити доступ до рахунків досить легким для зручності для клієнтів.

Звичайна компанія будує свою інформаційну безпеку, виходячи лише з вузького кола потенційних загроз — головним чином захист інформації від конкурентів. Така інформація цікава лише вузькому колу зацікавлених осіб, і організацій.

Розглянемо фактори, які має враховувати інформаційна безпека банку [3].

Інформація, що зберігається і обробляється в банківських системах, являє собою реальні гроші. З інформації комп'ютера можуть проводитися виплати, відкриватися кредити, переказуватися значні суми. Цілком зрозуміло, що незаконне маніпулювання з такою інформацією може призвести до серйозних збитків. Ця особливість різко розширює коло злочинців, які робили замах саме на банки (на відміну від, наприклад, промислових компаній, внутрішня інформація яких мало кому цікава).

Інформація у банківських системах зачіпає інтереси великої кількості людей та організацій – клієнтів банку. Як правило, вона конфіденційна, і банк відповідає за забезпечення необхідного ступеня таємності перед своїми клієнтами. Звичайно, клієнти вправі очікувати, що банк повинен дбати про їхні інтереси, інакше він ризикує своєю репутацією з усіма наслідками, що звідси випливають.

Конкурентоспроможність банку залежить від того, наскільки клієнту зручно працювати з банком, а також наскільки широкий спектр послуг, включаючи послуги, пов'язані з віддаленим доступом. Тому клієнт повинен мати можливість швидко та без стомлюючих процедур розпоряджатися своїми грошима. Але така

легкість доступу до грошей підвищує ймовірність злочинного проникнення у банківські системи. Інформаційна безпека банку (на відміну більшості компаній) має забезпечувати високу надійність роботи комп'ютерних систем навіть у разі позаштатних ситуацій, оскільки банк відповідає за власні кошти, а й за гроші клієнтів.

Банк зберігає важливу інформацію про своїх клієнтів, що розширює коло потенційних зловмисників, зацікавлених у крадіжці чи псуванні такої інформації.

Злочини у банківській сфері також мають особливості [3].

Багато злочинів, скоєних у фінансовій сфері, залишаються невідомими для широкої публіки у зв'язку з тим, що керівники банків не хочуть турбувати своїх акціонерів, бояться піддати свою організацію новим атакам, побоюються зіпсувати свою репутацію надійного сховища коштів і, як наслідок, втратити клієнтів.

Успішні комп'ютерні злочини, зазвичай, вимагають великої кількості банківських операцій. Проте великі суми можуть пересилатися лише за кілька транзакцій.

Комп'ютерні злочини не завжди є високотехнологічними. Достатньо підробки даних, зміни параметрів середовища автоматизованих систем обробки інформації банків (АСОІБ) тощо, а ці дії доступні обслуговуючому персоналу. Специфічною рисою захисту банківських систем є спеціальна форма обміну електронними даними - електронних платежів, без яких жоден сучасний банк неспроможна існувати.

Обмін електронними даними (ОЕД) це міжкомп'ютерний обмін діловими, комерційними, фінансовими електронними документами. Наприклад, замовленнями, платіжними інструкціями, контрактними пропозиціями, накладними, квитанціями.

ОЕД забезпечує оперативну взаємодію торгових партнерів (клієнтів, постачальників, торгових посередників та інших.) всіх етапах підготовки торгової угоди, укладання договору та реалізації поставки. На етапі оплати договору та переказу коштів ОЕД може призводити до електронного обміну

фінансовими документами. У цьому створюється ефективне середовище для торгово-платіжних операцій [8]:

- можливе ознайомлення торгових партнерів з пропозиціями товарів та послуг, вибір необхідного товару/послуги, уточнення комерційних умов (вартості та строків поставки, торгових знижок, гарантійних та сервісних зобов'язань) у реальному масштабі часу;

З технічного погляду проблеми захисту віддалених транзакцій вирішуються за допомогою кількох механізмів, які відповідають за забезпечення адекватної безпеки електронних банківських систем. Робота більшості цих механізмів забезпечується службами мережі з розширеним набором послуг (Value-Added Network, VAN). Служби, що реалізують обмін електронними документами, повинні виконувати такі функції:

- забезпечити захист від випадкових та умисних помилок

- забезпечити адаптацію до частих змін кількості користувачів, типів обладнання, способів доступу, обсягів трафіку, топології

- підтримувати різні типи апаратного та програмного забезпечення, що поставляється різними виробниками

- здійснювати управління та підтримку мережі для забезпечення безперервності роботи та швидкої діагностики порушень

- реалізовувати повний спектр прикладних завдань ОЕД, включаючи електронну пошту

- реалізовувати максимально можливу кількість вимог партнерів

- включати служби резервного копіювання та відновлення після аварій.

У системах обміну електронними документами мають бути реалізовані такі механізми, що забезпечують реалізацію функцій захисту на окремих вузлах системи та на рівні протоколів високого рівня [4]:

- рівноправна аутентифікація абонентів;

- неможливість відмови від авторства повідомлення/прийому повідомлення;

- Контроль цілісності повідомлення;

- Забезпечення конфіденційності повідомлення;

- Управління доступом на кінцевих системах;

- гарантії доставки повідомлення;

- неможливість відмовитися від вжиття заходів щодо повідомлення;

- Реєстрація послідовності повідомлень;

- Контроль цілісності послідовності повідомлень;

- Забезпечення конфіденційності потоку повідомлень.

2.1.1 Обмін даними за допомогою SSL

Процес обміну даними з допомогою протоколу SSL представлений на рис. 2.1.

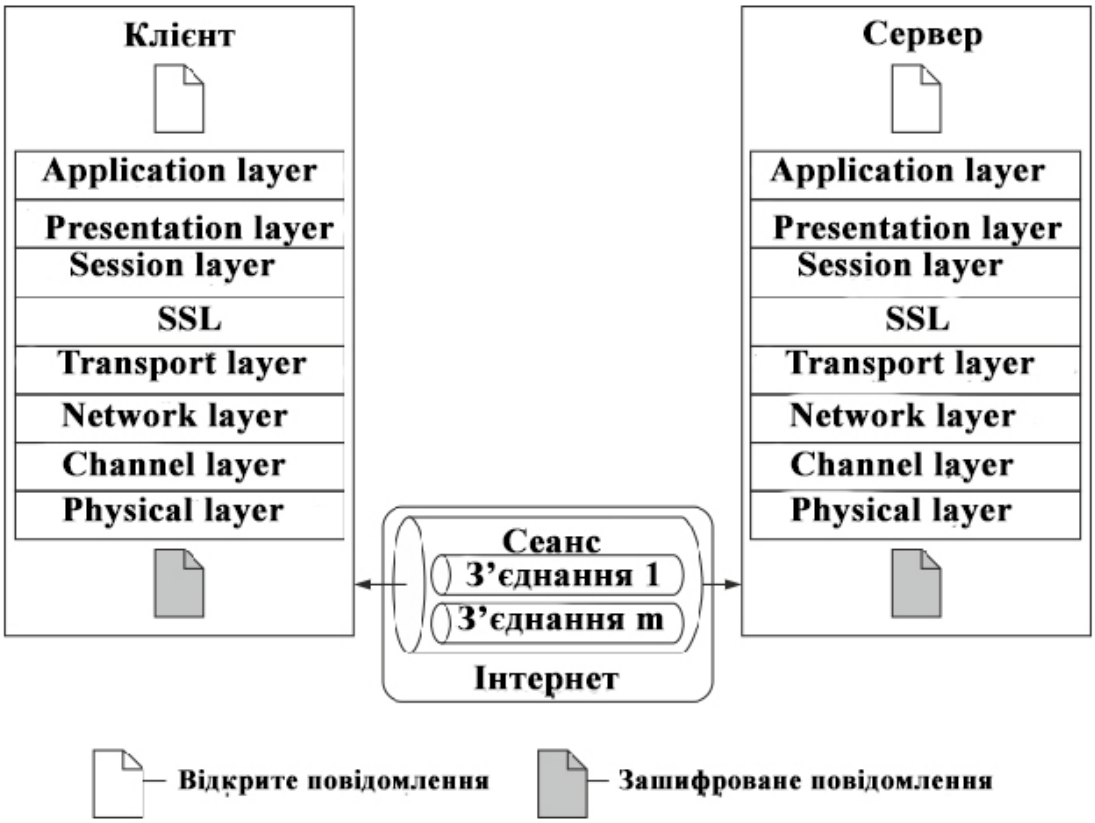

Рис 2.1 Взаємодія клієнта та сервера за допомогою SSL

Щоразу, коли клієнт під'єднується до сервера, починається сеанс SSL. У межах кожного сеансу можливо кілька з'єднань. Якщо клієнт під'єднується до іншого сервера, новий сеанс починається без поточного розриву. При поверненні до першого сервера користувач може відновити з'єднання за допомогою раніше встановлених параметрів або створити нове з'єднання. Для запобігання атакам

SSL передбачає обмеження часу дії сеансу (як правило, 24 годинами), після якого сеанс припиняється, і для подальшого спілкування з сервером необхідно створити новий сеанс.

Сеанс SSL характеризується такими значеннями.

• Ідентифікатор сеансу (Session_ID) – випадкове число, що генерується на стороні клієнта та дозволяє повернутися до вже встановленого сеансу.

• Сертифікати вузла (Client_Certificate та Server_Certificate) – сертифікат учасника інформаційної взаємодії відповідно до стандарту [12]• Метод стиснення - алгоритм стиснення даних, що передаються. алгоритми, що підтримуються, вказані в RFC 3749 [13.].

• Специфікація шифру - визначає параметри криптоалгоритмів:

о для обміну ключами та перевірки їх справжності: криптосистема з відкритим ключем RSA, протокол вироблення загального секретного ключа Діффі-Хеллмана (Diffie-Hellman), DSA (Digital Signature Algorithm), Fortezza.

о для симетричного шифрування: RC2, RC4, DES, 3DES, IDEA, AES;

о для хешування: SHA, MD5.

• Секретний ключ сеансу (Master_Secret) - секретний ключ, що розділяється клієнтом і сервером.

• Прапорець відновлення - параметр, який визначає можливість збереження вибраних параметрів для нового з'єднання в межах поточного сеансу.

• З'єднання SSL характеризується такими значеннями.

• Випадкові числа (Client_Random та Server_Random), які застосовуються при виробленні спільного секретного ключа.

• Ключі для шифрування/розшифрування інформації (Client_Write_Secret = Server_Read_Secret та Server_Write_Secret = Client_Read_Secret).

• Ключі для підпису повідомлень (секретні Server_MAC_Write_Secret та Client_MAC_Write_Secret).

• Вектори ініціалізації (Server_IV та Client_IV) - синхропосилання для блокових алгоритмів шифрування.

• Два послідовні числа для сервера та клієнта, що запобігають атакам перехоплення та повтору повідомлення.

SSL включає чотири протоколи, які представлені на рис. 2.2:

• Handshake;

• Record;

• Alert;

• CCS (Change Cipher Specification).

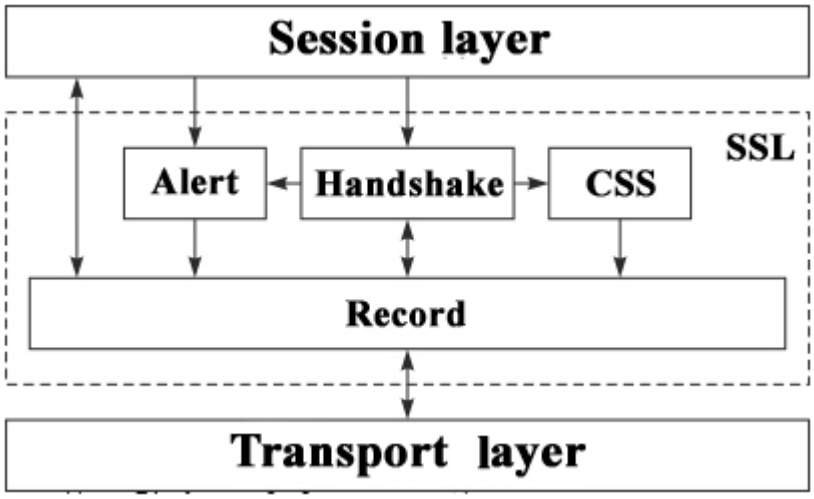

Рис.2.2 Протоколи SSL

Handshake. Цей протокол призначений для взаємної автентифікації клієнта та сервера, встановлення сеансу або з'єднання.

Установка сеансу схематично представлена на рис. 10.3 зазвичай ініціалізується клієнтом за допомогою повідомлення ClientHello (іноді ініціатором виступає сервер, посилаючи повідомлення HelloRequest, що символізує про те, що сервер готовий до процедури Handshake), в якому клієнт передає наступні параметри:

• версія SSL, яка підтримується клієнтом;

• ідентифікатор сеансу - значення, за яким можна відновити сеанс;

• довільне число Client_Random;

• список алгоритмів стиснення, шифрування та хешування інформації, що підтримуються клієнтом.

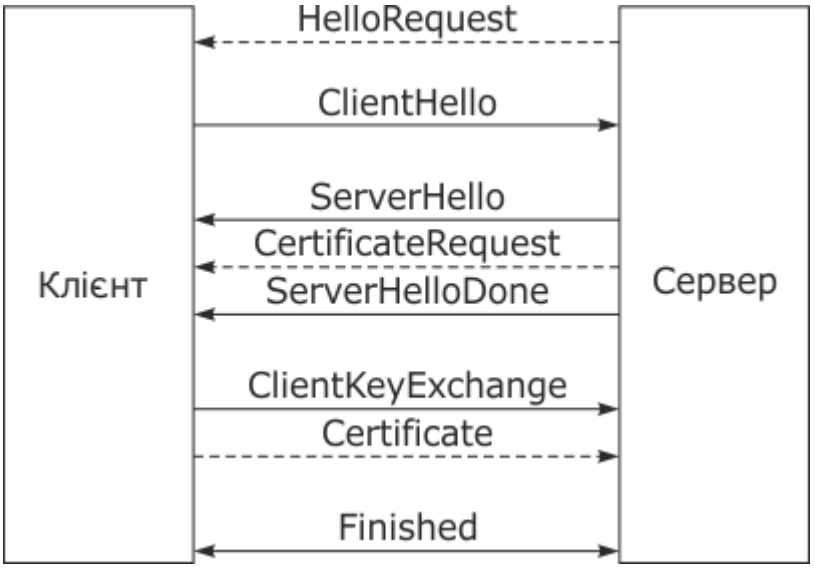

Рис.2.3 Процес встановлення нового сеансу в Handshake

У відповідь на це повідомлення сервер надсилає повідомлення ServerHello, що містить такі параметри:

• версія SSL, яку підтримує сервер;

• випадкове число Server_Random;

• список алгоритмів стиснення, шифрування та хешування інформації, які будуть використовуватись при реалізації сеансу або з'єднань.

Окрім цього повідомлення, сервер надсилає свій сертифікат. У разі, якщо використовувані алгоритми вимагають сертифіката клієнта, сервер надсилає клієнту запит на сертифікат - CertificateRequest. Потім сервер надсилає клієнту повідомлення ServerHelloDone, яке символізує закінчення передачі повідомлення ServerHello.

Якщо клієнт не підтримує алгоритми, запропоновані сервером, або не надіслав свій сертифікат у відповідь на відповідний запит, установка сеансу переривається. Інакше клієнт перевіряє сертифікат сервера, генерує Pre_Master_Secret, зашифровує його на відкритому ключі сервера, отриманому із сертифіката останнього, і надсилає отримане значення у повідомленні ClientKeyExchange. Сервер розшифровує отримане повідомлення за допомогою свого секретного ключа та отримує Pre_Master_Secret. Таким чином, обидві сторони (клієнт і сервер) мають три значення - Server_Random, Client_Random і

Pre_Master_Secret і можуть виробити Master_Secret за схемою, представленою на рис. 2.4.

Рис.2.4 Розробка Master_Secret на початку сеансу

Після цього обидві сторони посилають повідомлення Finished, що являє собою зашифровані на секретному ключі Master_Secret параметри сеансу і символізує завершення процесу установки нового сеансу.

Рис 2.5 Створення нового з'єднання Handshake.

Вона починається з надсилання клієнтом повідомлення ClientHello, в якому міститься ідентифікатор сеансу та згенероване випадкове число Client_Random. Сервер шукає отриманий ідентифікатор таблиці поточних сеансів. Якщо цей ідентифікатор відсутній, це означає, що сеанс минув або не було встановлено. І тут запит клієнта відхиляється. Якщо ж ідентифікатор існує, то з'єднання може використовувати алгоритми стиснення, шифрування та хешування, визначені для сеансу, якщо встановлений відповідний прапор. Інакше здійснюється вибір алгоритмів за аналогією із встановленням нового сеансу.

У відповідь на повідомлення ClientHello сервер надсилає повідомлення ServerHello, яке містить Server_Random. Знаючи Server_Random, Client_Random

і Master_Secret, клієнт і сервер можуть виробити значення, що характеризують поточне з'єднання рис. 2.6.

Рис.2.6 Створення параметрів з'єднання

Завершується встановлення з'єднання посилкою клієнтом та сервером повідомлень ChangeCipherSpec, що підтверджують прийняття обома сторонами алгоритмів стиснення, шифрування та хешування інформації та повідомлень Finished, що символізують закінчення процесу встановлення нового з'єднання.

Record. Цей протокол призначений для перетворення даних, що передаються сеансовим рівнем транспортного та назад. Перетворення даних відбувається за схемою, наведеною на рис. 2.7.

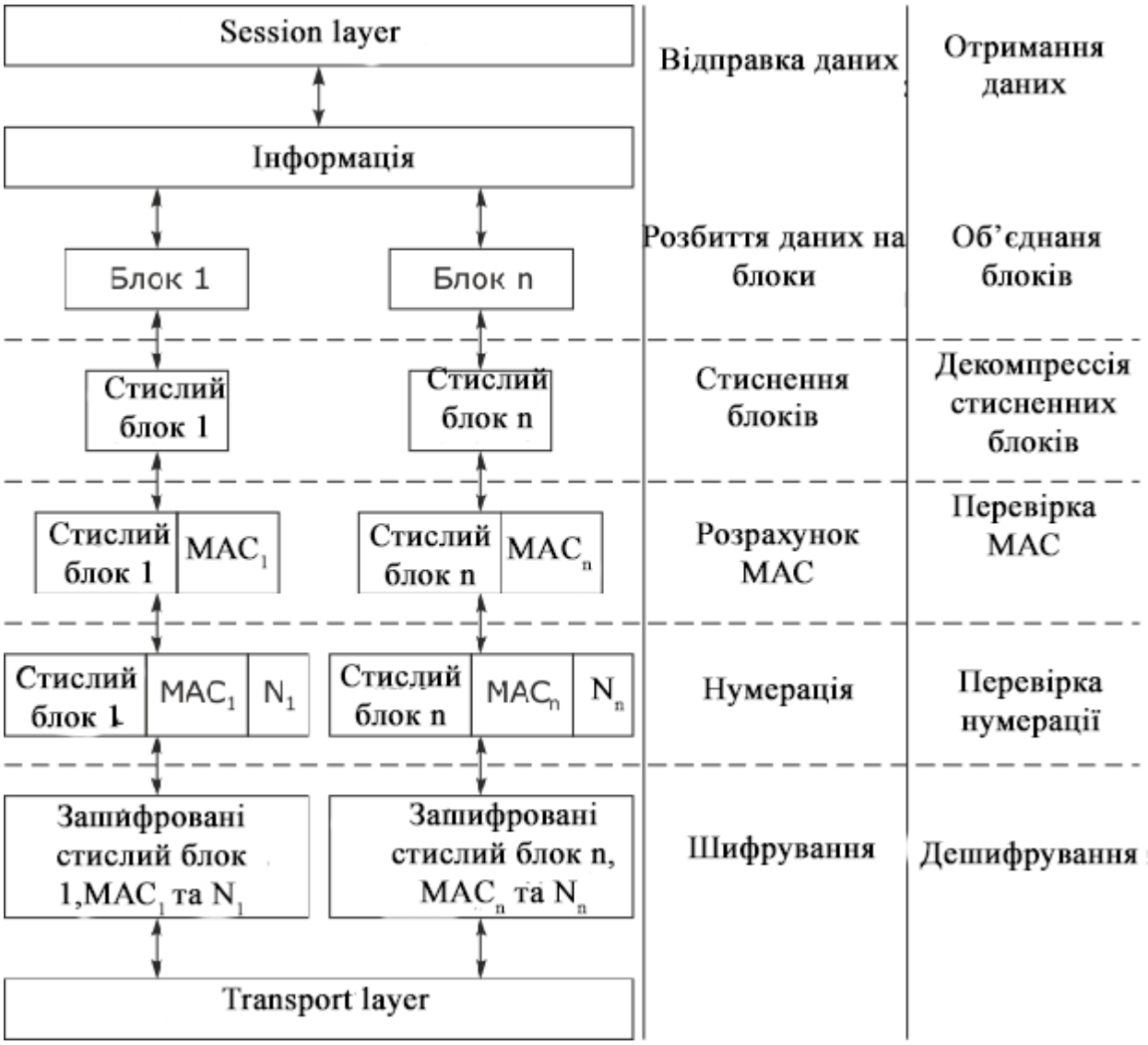

Рис 2.8 Обробка інформації в протоколі Record

Інформація, що передається відправником, розбивається на блоки розміром не більше 2^14 + 2048 байт кожен. Потім кожен блок стискається за допомогою вибраного алгоритму стиснення. Після цього обчислюється MAC кожного блоку та прикріплюється до останнього. Отримані фрагменти послідовно нумеруються для запобігання атакам, зашифровуються за допомогою вибраного алгоритму і передаються на транспортний рівень. Отримувач розшифровує отримані фрагменти, перевіряє послідовність їх номерів і цілісність повідомлень. Потім фрагменти розпаковуються та об'єднуються в єдине повідомлення.

2.1.2 Удосконалений аналог SET

Так само як і SSL, SET є надбудовою над транспортним рівнем, проте, на відміну від SSL, шифрує не всі дані, що надаються транспортним рівнем, а лише ті, що належать до платіжних транзакцій. Решта даних, що передаються транспортному рівню, проходять без змін рис. 2.9.

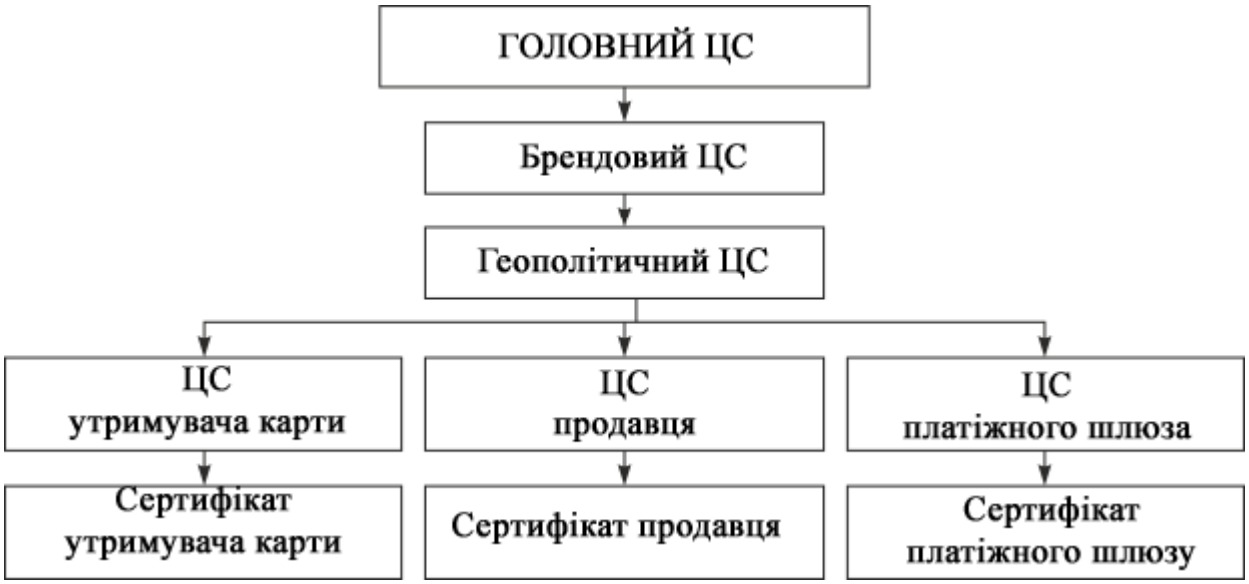

Рис 2.9 Система сертифікації протоколу SET

Головний центр сертифікації (RCA – Root CA) виконує наступні функції:

формування сертифікатів для брендових ЦС;

• створення сертифікатів для власних відкритих ключів;

• формування та розсилка списку відкликаних сертифікатів (CRL – Certificate Revocation List) для брендових ЦС.

Брендові центри сертифікації (BCA – Brand CA) є ЦС платіжних систем. За аналогією з головним ЦС вони формують сертифікати для ЦС нижчого рівня і допомагають розсилати CRL. Геополітичні центри сертифікації (GCA - Geo-Political CA) призначені для спрощення процедури взаємодії брендового ЦС та географічно розподілених центрів сертифікації власників карток, а саме:

• ЦС власника картки (CCA – Cardholder CA);

• ЦС продавця (MCA – Merchant CA);

• ЦС платіжного шлюзу (PCA – Payment Gate CA).

Центри сертифікації власників карток займаються формуванням, поширенням, підтримкою та анулюванням сертифікатів. Сертифікат є електронним документом, що засвідчує справжність зазначеного в ньому відкритого ключа. Відповідно до стандарту X.509.3 (ISO/IEC 9594-8 [EMV ICC Specification for Payment Systems.]) сертифікат має певні поля, представлені в таблиці 2.1

Таблиця 2.1. Основні поля сертифіката

Поле	**Опис**
Version	Версія протоколу X.509 (дорівнює 3)
Serial Number	Унікальний серійний номер сертифіката
Algorithm Identifier	Алгоритм, використаний для підпису сертифіката
Issuer Name	Ім’я ЦС, що випустив сертифікат
Validity.NotBefore	Дата початку дії сертифіката
Validity.NotAfter	Дата закінчення дії сертифіката
Subject Name	Ім’я власника сертифікату
Algorithm	Алгоритм, завдяки якому сформовано новий ключ
Subject Public Key Info	Значення відкритого ключа який сертифікують
Signature	Підпис

Крім зазначених полів у сертифікаті присутні значення, необхідні застосування перелічених у сертифікаті алгоритмів.

У протоколі SET передбачено чотири типи ключів, які використовуються учасниками платіжних транзакцій:

• ключ для підпису повідомлення (Digital Signature Key);

• ключ для шифрування даних (Data Encipherment Key);

• ключ для підпису сертифіката (Certificate Signature Key);

• ключ для підпису списку відкликаних сертифікатів (CRL Signature Key).

Так само як і SSL, SET є надбудовою над транспортним рівнем, проте, на відміну від SSL, шифрує не всі дані, що надаються транспортним рівнем, а лише ті, що належать до платіжних транзакцій. Решта даних, що передаються транспортному рівню, проходять без змін рис. 2.10.

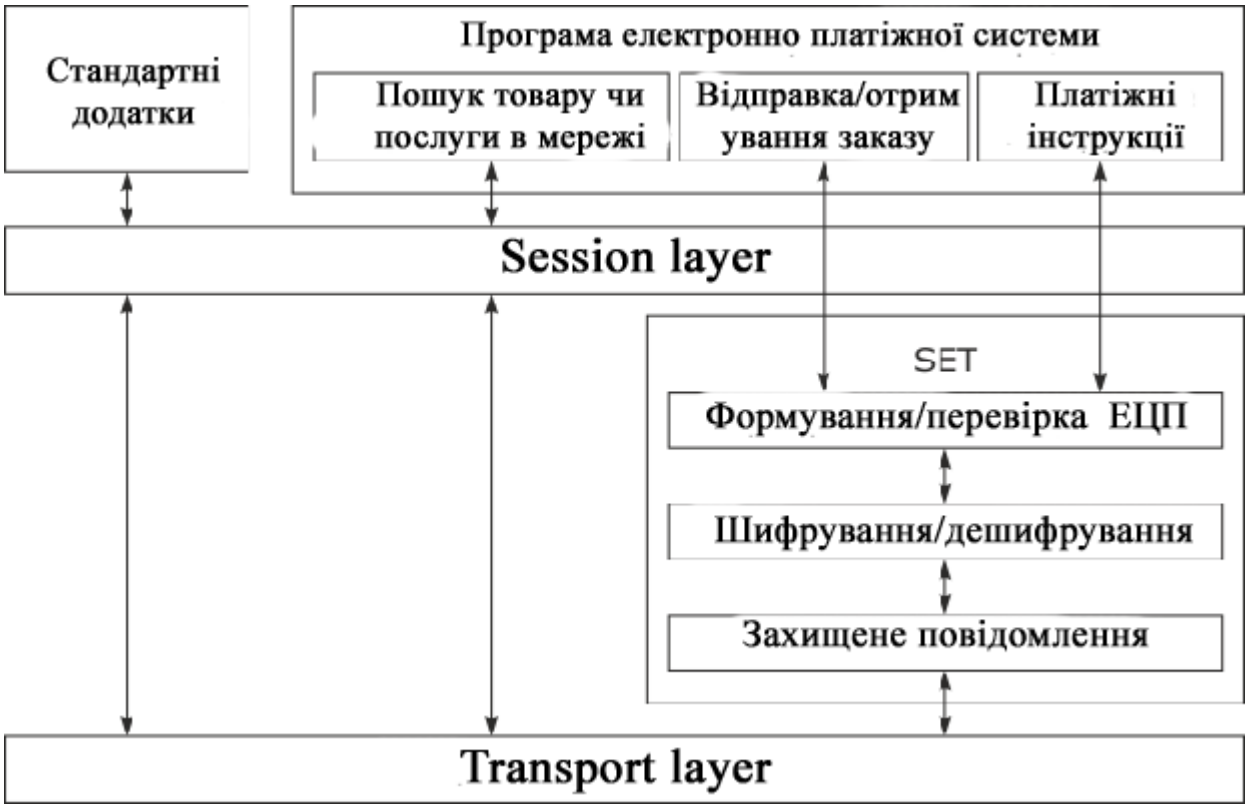

Рис. 2.10 Структура протоколу SET

Для здійснення подібної взаємодії використовується спеціальна програма електронної комерції, на яку покладаються такі функції:

• пошук товарів та послуг в Інтернеті;

• узгодження параметрів замовлення (ціна, термін доставки);

• формування замовлення;

• підготовка та передача параметрів, необхідних SET для організації захищеної взаємодії учасників платіжної транзакції.

Як було зазначено раніше, протокол SET розроблявся у тому, щоб виключити передачу платіжних реквізитів у відкритому вигляді продавцю. Проте будь-яке замовлення передбачає передачу інструкцій як продавцю, і банку. При цьому обидві інструкції мають бути підписані єдиним підписом для виключення конфліктних ситуацій. Вирішення даної задачі представлено в SET у вигляді механізму подвійного електронного підпису.

При транзакції покупець *C* формує два повідомлення:

• m_1- опис замовлення для продавця C, який містить усі необхідні дані для відвантаження товару або надання послуги;

• m_2- інструкції платіжного шлюзу G, які містять у тому числі платіжні реквізити покупця.

Зміст повідомлення m_2 не повинен бути доступний продавцю, m_1 зміст, в принципі, не обов'язково для платіжного шлюзу. При цьому покупець зацікавлений у тому, щоб платіжні інструкції були виконані лише після того, як із умовами замовлення буде згоден продавець.

Для досягнення поставленого завдання покупець формує повідомлення m_3, що є об'єднанням хеш-образів повідомлень m_1 і m_2 :

$m_3 = h(m_1) \,||\, h(m_2)$ Потім покупець застосовує хеш-функцію до повідомлення m_3 та зашифровує результат на своєму секретному ключі SK_C, отримуючи тим самим подвійний електронний підпис: $DoubleSign = SK_C\{h(m_3)\}$. Після цього клієнт формує повідомлення:

$Order_C = m_1 \,||\, h(m_2) \,||\, PK_G\{m_2 \,||\, h(m_2)\} \,||\, SoubleSign,$ що складається з інструкції продавцю, оригіналу та хеш-образу інструкції платіжного шлюзу, зашифрованих на відкритому ключі платіжного шлюзу, та подвійного електронного підпису. Дане повідомлення покупець надсилає продавцю. Продавець, отримавши вказане повідомлення, перевіряє підпис покупця. Для цього він витягає із повідомлення с m_1 та $h(m_2)$ та обчислює значення $m'_3 = h(m_1) \,||\, h(m_2)$. Потім продавець h'_3 обчислює та порівнює його зі значенням $h(m_3)$, яке він отримує з DoubleSign, зашифрувавши останнє на відкритому ключі покупця PK_C :

$h(m_3) = PK_C\{DoubleSign\}$. У разі збігу $h(m_3)$ та h'_3 продавець переконується в цілісності повідомлення і за згодою з умовами угоди витягує дані, що призначаються йому m_1 та $h(m_2)$з $Order_C$ формуючи цим повідомлення $Order_M = h(m_1) \,||\, PK_G\{m_2 \,||\, h(m_2)\} \,||\, DoubleSign,$ яке надсилає платіжному шлюзу.

Отримавши це повідомлення, платіжний шлюз витягує з нього фрагмент $PK_G\{m_2||h(m_2)\}$, розшифровує його на своєму секретному ключі SK_G та отримує платіжні інструкції :

$$m_2 \;||\; h\left(m_2\right) = SK_G\left\{PK_G\left\{m_2 \;||\; h\left(m_2\right)\right\}\right\}.$$

Після цього шлюз витягує з отриманого від продавця повідомлення $h(m_1)$ яке він отримує з DoubleSign, зашифрувавши останнє на відкритому ключі покупця PK_C :

$h\left(m_3\right) = PK_C\left\{DoubleSign\right\}$. Збіг $h(m_3)$ і m'''_3 означає, що, по-перше , платіжні інструкції підписані дійсно покупцем, а по-друге, що продавець погоджується з умовами угоди.

Переконавшись у коректності підпису, шлюз здійснює вказані йому платіжні інструкції.

2.2 Концепції віддалених електронних платежів

Суть концепції віддалених електронних платежів полягає в тому, що повідомлення, що пересилаються по лініях зв'язку, належним чином оформлені і передані, є підставою для виконання однієї або декількох банківських операцій. Жодних паперових документів для виконання цих операцій у принципі не потрібно (хоча вони можуть бути видані). Іншими словами, повідомлення, що пересилається по лініях зв'язку, несе інформацію про те, що відправник виконав деякі операції над своїм рахунком, зокрема над кореспондентським рахунком банку-одержувача (в ролі якого може виступати клірінговий центр), і що одержувач повинен виконати визначені в повідомленні операції. На підставі такого повідомлення можна переслати або отримати гроші, відкрити кредит, сплатити покупку чи послугу та виконати будь-яку іншу банківську операцію. Такі повідомлення називаються електронними грошима, а виконання банківських операцій виходячи з посилки чи отримання таких повідомлень - електронними платежами. Звичайно, весь процес здійснення електронних

платежів потребує надійного захисту. Інакше банк та його клієнтів очікують на серйозні неприємності. Електронні платежі застосовуються при міжбанківських, торгових та персональних розрахунках.

Пересилання грошей за допомогою системи електронних платежів включає наступні етапи (залежно від конкретних умов та самої системи порядок може змінюватися):

- певний рахунок у системі першого банку зменшується на потрібну суму;

- кореспондентський рахунок другого банку у першому збільшується на ту саму суму;

- від першого банку другому надсилається повідомлення, що містить інформацію про виконувані дії (ідентифікатори рахунків, сума, дата, умови тощо); при цьому повідомлення, що пересилається, має бути відповідним чином захищене від підробки: зашифроване, забезпечене цифровим підписом і контрольними полями і т.д.;

- з кореспондентського рахунку першого банку у другому списується потрібна сума;

- певний рахунок у другому банку збільшується на потрібну суму;

- другий банк надсилає першому повідомлення про проведені коригування рахунку; це повідомлення також має бути захищене від підробки у спосіб, аналогічний захисту платіжного повідомлення;

- протокол обміну фіксується в обох абонентів і, можливо, у третьої особи (у центрі управління мережею) для запобігання конфліктам.

На шляху передачі повідомлень можуть бути посередники - клірингові центри, банки-посередники передачі інформації тощо. Основна складність таких розрахунків – впевненість у своєму партнері, тобто кожен з абонентів має бути впевненим, що його кореспондент виконає всі необхідні дії.

Для визначення загальних проблем захисту віддалених транзакцій можна виділити три основні етапи:

- підготовка документа до надсилання;

- Передача документа по каналу зв'язку;

- прийом документа та його зворотне перетворення.

З погляду захисту у системах віддалених платежів існують такі вразливі місця [9]:

- пересилання платіжних та інших повідомлень між банками або між банком та клієнтом

- обробка інформації всередині організацій відправника та одержувача;

- доступ клієнта до коштів, а кумульованим на рахунку.

При надсиланні платіжних та інших повідомлень виникають такі проблеми:

- внутрішні системи організацій одержувача та відправника повинні бути пристосовані до отримання/надсилання електронних документів та забезпечувати необхідний захист при їх обробці всередині організації (захист кінцевих систем);

- взаємодія одержувача та відправника документа здійснюється опосередковано – через канал зв'язку. Це породжує такі види проблем як взаємне розпізнавання абонентів (проблема встановлення аутентифікації під час встановлення з'єднання), захисту документів, що передаються каналами зв'язку (забезпечення цілісності та конфіденційності документів), захисту самого процесу обміну документами (проблема доказу відправлення/доставки документа);

- у випадку відправник і одержувач документа належать до різних організаціям і друг від друга незалежні. Цей факт породжує проблему недовіри - чи буде вжито необхідних заходів щодо цього документа (забезпечення виконання документа).

Повнота вирішення проблем захисту обміну електронними документами залежить від правильного вибору системи шифрування. Система шифрування (або криптосистема) є сукупністю алгоритмів шифрування і методів поширення ключів. Правильний вибір системи шифрування допомагає:

- приховати зміст документа від сторонніх осіб (забезпечення конфіденційності документа) шляхом шифрування його;

- забезпечити спільне використання документа групою користувачів системи обміну електронних документів шляхом криптографічного поділу інформації та

відповідного протоколу розподілу ключів. При цьому для осіб, які не входять до групи, документ недоступний;

- своєчасно виявити спотворення, підробку документа (забезпечення цілісності документа) шляхом запровадження криптографічної контрольної ознаки;

- упевнитися в тому, що абонент, з яким відбувається взаємодія в мережі, є тим, за кого він себе видає (аутентифікація абонента/джерела даних).

Слід зазначити, що при захисті систем обміну електронними даними велику роль відіграє не так шифрування документа, як забезпечення його цілісності та аутентифікація абонентів (джерела даних) під час проведення сеансу зв'язку. Тому механізми шифрування таких системах грають зазвичай допоміжну роль.

У загальнодоступних мережах поширені хакерські напади. Це висококваліфіковані спеціалісти, які спрямованою дією можуть виводити з ладу на тривалий час сервери АБС (DoS-атака) або проникати в їх системи безпеки. Майже всі згадані небезпеки здатний продати хакер-одинак або об'єднана група. Хакер може бути як у ролі зовнішнього джерела загрози, і у ролі внутрішнього (співробітник організації).

Для запобігання проникненню в систему безпеки використовуються такі засоби захисту:

- Шифрування вмісту документа;

- Контроль авторства документа;

- Контроль цілісності документа;

- нумерація документів;

- ведення сесій лише на рівні захисту информации;

- динамічна автентифікація;

- Забезпечення безпеки секретних ключів;

- надійна процедура перевірки клієнта під час реєстрації у прикладній системі;

- Використання електронного сертифіката клієнта;

- Створення захищеного з'єднання клієнта з сервером.

Також необхідно застосовувати комплекс технічних засобів захисту інтернет-сервісів:

- брандмауер (міжмережевий екран) - програмна та/або апаратна реалізація
- системи виявлення атак на мережевому рівні;
- антивірусні засоби;
- захищені ОС, що забезпечують рівень В2 та класифікації захисту комп'ютерних систем та додаткові засоби контролю цілісності програм та даних;
- Захист на рівні додатків: протоколи безпеки, шифрування, ЕЦП, цифрові сертифікати, системи контролю цілісності;
- Захист засобами системи управління БД;
- захист компонентів програмного забезпечення, що передаються по мережі;
- моніторинг безпеки та виявлення спроб вторгнення, адаптивний захист мереж, активний аудит дій користувачів;
- обманні системи;
- Коректне управління політикою безпеки.

Для проведення безпечних банківських транзакцій мають виконуватись:

- аутентифікація документа під час його створення;
- Захист документа при його передачі;
- аутентифікація документа при обробці, зберіганні та виконанні;

2.3 Типи криптографічних алгоритмів

В даний час існує два типи криптографічних алгоритмів: класичні, або симетричні алгоритми, засновані на використанні закритих, секретних ключів, коли і зашифрування, і розшифрування виробляються на тому самому ключі, і алгоритми з відкритим ключем, в яких використовуються один відкритий один закритий ключ, тобто. ці криптоопераціі виробляються різних ключах (ці алгоритми називаються також асиметричними).

Симетричні криптосистеми прийнято підрозділяти на потокові та блокові системи. Поточні системи зашифрують окремі символи відкритого повідомлення. А блокові системи проводять зашифрування блоків фіксованої довжини, складених із поспіль символів повідомлення.

Найстаріша форма шифрування з використанням ключа — симетричне шифрування, або шифрування із секретним ключем. При шифруванні за такою схемою відправник і одержувач володіють одним і тим самим ключем, за допомогою якого і той, і інший можуть зашифровувати та розшифровувати інформацію.

Схемам симетричного шифрування притаманні проблеми з автентичністю, оскільки особистість відправника або одержувача листа гарантувати неможливо. Якщо двоє володіють одним і тим же ключем, кожен з них може написати та зашифрувати дані, а потім заявити, що це зробив інший.

Така невизначеність не дозволяє реалізувати принцип неможливості відмови. Проблему зречення авторства дозволяє вирішити криптографія з відкритим ключем, що використовує асиметричні алгоритми шифрування.

Асиметричні криптосистеми, як правило, є блоковими. При використанні їх можна легко організувати передачу конфіденційної інформації в мережі з великою кількістю користувачів. Справді, щоб надіслати повідомлення, відправник відкрито зв'язується з одержувачем, який або передає свій ключ відправнику, або поміщає його на загальнодоступний сервер. Відправник зашифровує повідомлення на відкритому ключі одержувача та надсилає його одержувачу. При цьому ніхто, крім одержувача, що володіє ключем розшифрування, не зможе ознайомитися зі змістом інформації, що передається. В результаті така система шифрування із загальнодоступним ключем дозволяє істотно скоротити обсяг секретної ключової інформації, що зберігається кожним абонентом.

Відкритий ключ не потрібно зберігати в таємниці. Необхідно лише забезпечити його автентичність, що, як правило, зробити легше, ніж забезпечити розсилку та збереження секретних ключів.

Асиметричні системи шифрування забезпечують значно менші швидкості шифрування, ніж симетричні, внаслідок чого вони зазвичай використовуються не стільки для шифрування повідомлень, скільки для шифрування ключів, що пересилаються між кореспондентами, які потім використовуються в симетричних системах. Шифрування послань відкритим ключем принципово не

дуже відрізняється від симетричного шифрування з використанням секретного ключа, але все ж таки має ряд переваг. Наприклад, відкрита частина ключової пари може вільно поширюватися без побоювань, що це завадить використати особистий ключ.

Для того щоб гарантувати надійний захист інформації, до систем з відкритим ключем пред'являються дві важливі та очевидні вимоги:

• перетворення вихідного тексту має бути незворотнім та виключати його відновлення на основі відкритого ключа;

• визначення закритого ключа на основі відкритого також має бути неможливим на сучасному технологічному рівні. При цьому бажана точна нижня оцінка складності (кількості операцій) розкриття шифру.

Прикладами асиметричних систем шифрування є найпоширеніша у час система шифрування з відкритим ключем система RSA і шифрсистема Эль-Гамаля.

Обидві системи ґрунтуються на складних математичних перетвореннях. Складність знаходження секретного ключа системи RSA визначається складністю розкладання чисел на прості множники. Криптографічна стійкість системи Ель-Гамаля заснована на складності проблеми логарифмування у мультиплікативній групі кінцевого простого поля.

Вибір криптографічного алгоритму і режиму його використання залежить від особливостей інформації, що передається (її цінності, обсягу, способу подання, необхідної швидкості передачі і т. д.), перешкоди захищеності використовуваного каналу зв'язку і можливостей власників із захисту своєї інформації (вартість застосовуваних технічних пристроїв, зручність використання, надійність функціонування і т.п.).

Наявність надійного криптографічного алгоритму і правильний вибір режиму ще не гарантують власнику захищеність інформації, що передається. Важливу роль відіграє правильність їхнього використання. Оскільки навіть найстійкіші шифри при неправильному використанні істотно втрачають свої якості, то конфіденційність інформації, що передається, багато в чому залежить від того, які помилки допускає її власник при використанні криптографічного

захисту. А те, що всі користувачі припускаються помилок, - неминуче і є непорушним і важливим (для криптоаналітика) фактом, оскільки будь-які криптографічні засоби, хоч би якими вони були зручними та прозорими, завжди заважають користувачам у роботі, а різні тонкощі відомі лише криптоаналітикам і, як правило, незрозумілі користувачам цих засобів. Понад те, як суб'єктів взаємодії можуть виступати як люди, а й різні процеси, здійснюють обробку інформації в автоматизованої системі без участі людини. Тому захищеність інформації в системі істотно залежить від того, наскільки правильно там реалізована криптографічна підсистема, яка відповідає за виконання криптографічних функцій. Одна наявність такої підсистеми ще нічого не гарантує.

Підкреслимо різницю між термінами «розшифрування» та «дешифрування». При розшифруванні чинний ключ вважається відомим, у той час як при дешифруванні ключ невідомий. Тим самим розшифрування має здійснюватися так само просто, як і зашифрування; дешифрування є значно складнішим завданням. Саме в цьому полягає сенс шифрування.

Для різних шифрів завдання дешифрування має різну складність. Рівень складності цього завдання і визначає головну властивість шифру — здатність протистояти спробам противника заволодіти інформацією, що захищається. У зв'язку з цим говорять про криптографічну стійкість шифру, розрізняючи стійкіші і менш стійкі шифри. Методи розкриття шифрів розробляє наука, що має назву криптоаналіз. З цієї причини вважати захист надійним без проведення детального криптоаналізу не можна.

Завдання проведення криптографічного аналізу сучасних криптосистем та отримання об'єктивного уявлення про їхню якість є серйозною науковою проблемою. У всіх провідних країнах існують школи спеціалістів-криптографів. Постійно розробляють нові оригінальні методи криптографічного аналізу. Додаткові можливості розкриття криптосистем надає використання високопродуктивної обчислювальної техніки. Тому розробити якісну криптографічну систему нефахівцю в даний час є нереальним. Слід підкреслити,

що йдеться саме про розробку криптографічних рішень, а не про їхню реалізацію в конкретних засобах захисту інформації.

Прикладом, що підтверджує це положення, є порядок розробки та затвердження нового стандарту шифрування AES. Алгоритм вибирався на конкурсній основі, і 5 кращих претендентів протягом тривалого часу аналізувалися широким колом фахівців з різних країн.

Єдиний спосіб уникнути помилок при виборі криптографічних алгоритмів - це тільки сертифіковані криптографічні рішення.

Висновки до другого розділу

Зазначено та проаналізовано, що електронно-платіжні системи посідають невід'ємну частину нашого життя. Питання інформаційної безпеки цих систем посідає досить значне місце в сфері інформаційно-комунікаційних систем.

Розглянуто основні методи та засоби захисту ЕПС, стандарти що використовуються, протоколи захисту передачі даних. Основні функції захисту та методи протидії хакерським атакам.

Виокремлено основні концепції віддалених електронних платежів, та зазначено вразливі сторони інформаційної безпеки електронно-платіжних систем

3. ІНТЕГРАЦІЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ В ЕЛЕКТРОННІ ПЛАТІЖНІ СИСТЕМИ ЯК МЕТОД ЗАХИСТУ

3.1 Вимоги до стійкості криптографічних алгоритмів в ЕПС

На сьогоднішній день існує велика кількість симетричних криптосистем, що забезпечують достатній захист інформації. Найвідомішими серед них є такі алгоритми шифрування як DES, DESX, Triple DES, IDEA, AES та інші. В деяких з них були знайдені вразливості, що дають можливість провести успішний криптоаналіз, інші ж до цих пір умовно вважаються незламними. Проте, не дивлячись на це, серйозною загрозою для подібних алгоритмів є стрімкий розвиток комп'ютерних технологій та, як наслідок, швидке зростання практичної швидкості обчислювальної потужності [1, 2, 3].

Яскравим прикладом цього є алгоритм DES: в часи його розробки довжина ключа в 56 біт здавалася цілком достатньою, а атака повним перебором ключів здавалась абсолютно не практичною. Проте лише за кілька десятиліть дана атака стала можливою практично в домашніх умовах, з використанням обчислювальних потужностей, доступних рядовому користувачу [3, 4]. Подібно до цього, з появою нових технологій, одною з яких, теоретично,може бути квантовий комп'ютер, який за прогнозами може обігнати найкращі з існуючих комп'ютерів в мільйон раз, за швидкістю обчислень, існуючі симетричні алгоритми та класичний підхід до криптографії в цілому може виявитись під загрозою [3]. Одним з варіантів уникнення даної загрози, на нашу думку, може бути створення нелінійних алгоритмів шифрування, що додатково ускладнять криптографічний аналіз даних шифрів.

Практично будь-яка криптосистема будується на основі простоти одностороннього перетворення: маючи ключ можна легко та швидко перетворити (зашифрувати) повідомлення та, у випадку симетричних криптосистем, на основі того ж самого ключа можна провести зворотне перетворення (дешифрування) шифрованого повідомлення. При цьому перед криптоаналітиком, у якого немає даного ключа, а є лише шифроване

повідомлення, стоїть значно важче завдання, оскільки існує непрактична кількість способів якими це повідомлення можна розшифрувати, при цьому існує лише один, в результаті якого можливо отримати початкове повідомлення [5-8].

В сучасній криптографії, в цілому, існує два напрямки симетричних криптосистем: потокові та блочні. Сучасні блокові криптосистеми з симетричними ключами шифровують n-бітові блоки вхідних даних, або розшифровують n-бітовий блок зашифрованих даних. Алгоритми шифрування або дешифрування використовують k-бітовий ключ. В той час потокові алгоритми шифрування, як правило, орієнтовані на роботу в реальному часі.

Вони працюють із малими частинками інформації: з бітами, або байтами, що дозволяє виконувати шифрування, або дешифрування потокових даних [2, 4, 9].

Відповідно до принципу Керкхоффса, якого дотримуються більшість криптологів, стійкість криптосистеми не повинна залежати від принципу шифрування, а повинна базуватися виключно на її ключах [2, 10]. При тому що даний принцип не є деякою істиною в останній інстанції, оскільки існує багато прикладів того як відсутність інформації про принцип шифрування серйозно ускладнювала криптоаналіз, вказаний підхід все ж є одним з головних безпечних вимог до сучасних алгоритмів шифрування, адже криптосистема, що пройшла відповідну перевірку буде гарантовано стійкою в незалежності від контексту її використання [10].

Поєднання криптографічного алгоритму, стійкість якого була доведена за принципом Керкхоффса, з стеганографічними інструментами, різноманітними прийомами заплутування та обфускації, що додатково ускладнять роботу криптоаналітика, в комплексну систему захисту дозволять гарантувати надійний захист важливих даних.

Основні вимоги до сучасної криптосистеми, що може претендувати на надійність та криптостійкість в умовах стрімкого розвитку технологій та постійному нарощуванні обчислювальної потужності комп’ютерів.Головна криптостійкість алгоритму повинна базуватися на складності обчислень, необхідних для криптоатаки: дана складність повинна бути суттєво вищою як за поточний рівень обчислювальної потужності комп’ютерної техніки,

так і за цей показник в майбутньому, з урахуванням згаданого зростання.

Складність обчислень повинна підкріплюватись великим розміром ключа,а середній прогнозований час, затрачений на реалізацію атаки повинен бути абсолютно не практичним. Блочна структура шифрування дозволить забезпечити додаткову криптостійкість, оскільки вона створює залежність одного блоку від іншого, що вимусить криптоаналітика підходити до аналізу шифротексту комплексно,досліджуючи все повідомлення в цілому.

Завданням роботи є створення алгоритму шифрування інформації, який відповідав би сучасним стандартам безпеки, забезпечував високу швидкодію роботи та був легким в модернізації, з можливістю широкого практичного застосування, зокрема стеганографічного. Проектування алгоритму з заявленими характеристиками дозволить забезпечити високий рівень захисту важливих даних та відповідає актуальній тенденції забезпечення цифрової безпеки та захисту конфіденційних даних.

3.2 Функції хешування

Функції, використовувані у процесі вироблення коду аутентифікації повідомлення, отримали назву хеш-функцій.

Хеш-функції – це функції, призначені для «стиснення» довільного повідомлення або набору даних, записаного зазвичай у двійковому алфавіті, деяку бітову комбінацію фіксованої довжини (згортку). Основною вимогою до таких хеш-функцій є рівномірність розподілу їх значень за випадкового вибору значень аргументів.

Хеш-функція, що служить для вироблення коду аутентифікації повідомлення, повинна дозволяти не тільки виявити випадкові помилки в наборах даних, що виникають при їх зберіганні та передачі, а й сигналізувати про активні атаки зловмисника здійснити нав'язування помилкової інформації.

Функція є хеш-функцією, якщо вона задовольняє наступним умовам:

• вихідний текст може бути довільною довжиною;

• саме значення функції має фіксовану довжину;

• значення функції легко обчислюється будь-якого аргумента;

• відновити аргумент за значенням з обчислювальної точки зору практично неможливо;

функція однозначна.

Для того, щоб зловмисник не зміг самостійно обчислити контрольне значення згортки і тим самим здійснити успішну імітацію або заміну даних, хеш-функція повинна залежати від секретного, невідомого зловмисник, параметра - ключа користувача. Цей ключ повинен бути відомий передавальної та перевіряючої сторонам. Такі хеш-функції називатимемо ключовими. Ключові хеш-функції застосовуються в системах з симетричними ключами і дають можливість без додаткових засобів гарантувати як правильність джерела даних, так і цілісність даних у системах з користувачами, що довіряють один одному.

Поряд із ключовими хеш-функціями в деяких випадках застосовуються і безключові хеш-функції. Вони дозволяють за допомогою додаткових засобів (наприклад, шифрування, використання захищеного каналу або цифрового підпису) гарантувати цілісність даних. Ці хеш-функції можуть застосовуватися в системах як з користувачами, що довіряють, так і не довіряють один одному.

Ключові функції застосовуються в ситуаціях, коли сторони довіряють одна одній і можуть мати загальний секретний ключ. Зазвичай у цих умовах не потрібно, щоб система забезпечувала захист у разі відмови одержувача від факту отримання повідомлення або його заміни. Тому від ключових хеш-функцій потрібно, щоб складність підбору повідомлення з правильним значенням згортки і складність підбору для заданого повідомлення з відомим значенням згортки іншого повідомлення з правильним значенням згортки була досить високою. При цьому не потрібно, щоб виконувалася властивість стійкості до колізій.

Від безключових хеш-функцій зазвичай потрібно, щоб вони забезпечували високу складність знаходження повідомлення з заданим значенням згортки, пари повідомлень з однаковими значеннями згортки і другого повідомлення з тим же значенням згортки для заданого повідомлення з відомим значенням згортки.

3.3 Надстійкий алгоритм RSA

RSA зазвичай включає три етапи: генерацію ключа, розшифрування та шифрування.RSA — це конфіденційність і секретність, аутентифікація, цілісність і невідмовність [26], тому що вони доводять, що RSA є чудовою криптосистемою з відкритим ключем безпеки. Алгоритм RSA має багато переваг, а саме має швидке шифрування та процеси перевірки; пропонує високий рівень безпеки; і підтримує конфіденційність даних, невідмовність і надійність даних [7,8]. Підхід представлений у цій дослідницькій роботі вимагає високого рівня безпеки, якого можна ефективно досягти і за допомогою криптографічного алгоритму RSA.

Для генерації ключів шифрування та дешифрування, потрібно:

P та Q обидва значення, P ≠, Q

$$\emptyset = (p-1)\,(q-1)\,1$$

$$1 < e < \emptyset$$

$$\gcd(e, \emptyset) = 1$$

$$\text{Public Key} = \{e, n\}$$

$$\text{Private Key} = \{d, n\}$$

Шифрування відкритого тексту:

$M < n$

Шифрований текст: $C = Me \bmod n$

Розшифрування:

Шифрований текст: $M = Cd \bmod n$

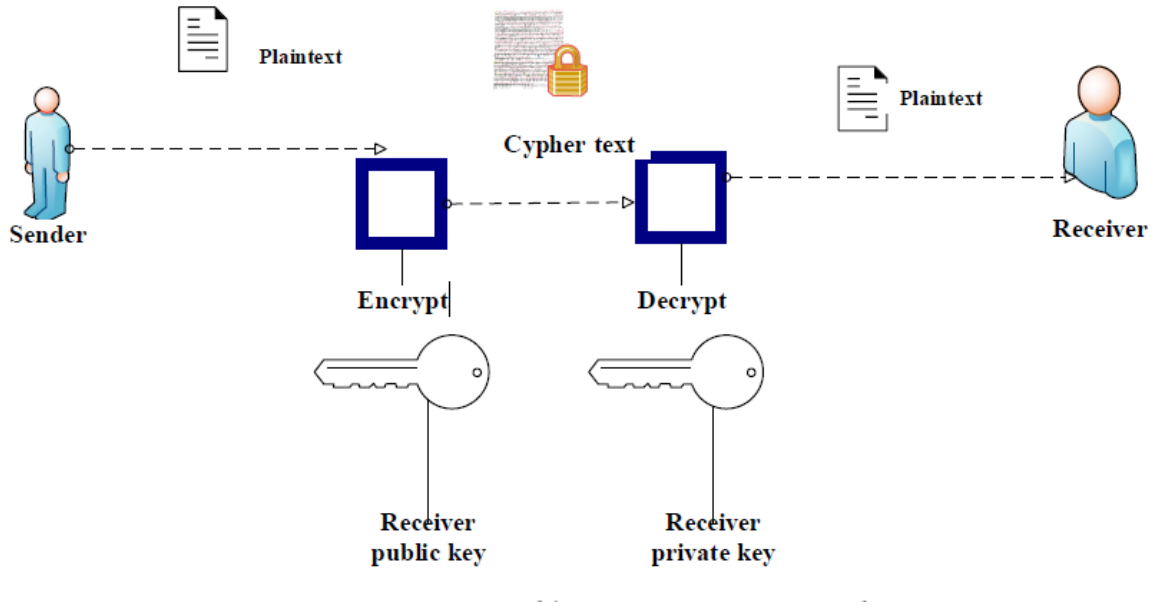

Рис.3.1 Як працює криптосистема з відкритим ключем RSA.

Безпека є ключовою проблемою та життєво важливою проблемою для успіху електронної комерції. У попередній роботі безпечний було запропоновано електронний платіжний шлюз для електронної комерції. У цій статті ми пропонуємо безпечний протокол в електронній комерції для підвищення безпеки процесу електронної комерції, що також може покращити безпеку існуюча робота. Цікаво, що запропонована система не вимагає від клієнта введення його/її особи на веб-сайті продавця, навіть якщо клієнт може приховати свою особистість і зробити тимчасовий ідентифікатор для обробки запиту на послугу. Запропонована система складається з п'яти об'єктів: клієнт (C), продавець (M), платіжний шлюз (PG), банк користувача (B) і банк продавця. Виконують вони наступним чином. Кожна юридична особа, тобто клієнт, продавець, банки-користувачі та торговий банк, реєструється в платіжному шлюзі, щоб створити свій секретний ключ у шлюзі. Секретні ключові елементи необхідні для безпечного спілкування. Крім того, користувач і продавець також створюють секретний ключ між собою. Клієнт розглядає продавця і запитує продукт, тепер з його/її тимчасову особу, створену на веб-сайті продавця, і продавець надсилає запит до платіжний шлюз. Запропонована модель системи електронних платежів представлена на рис 3.2

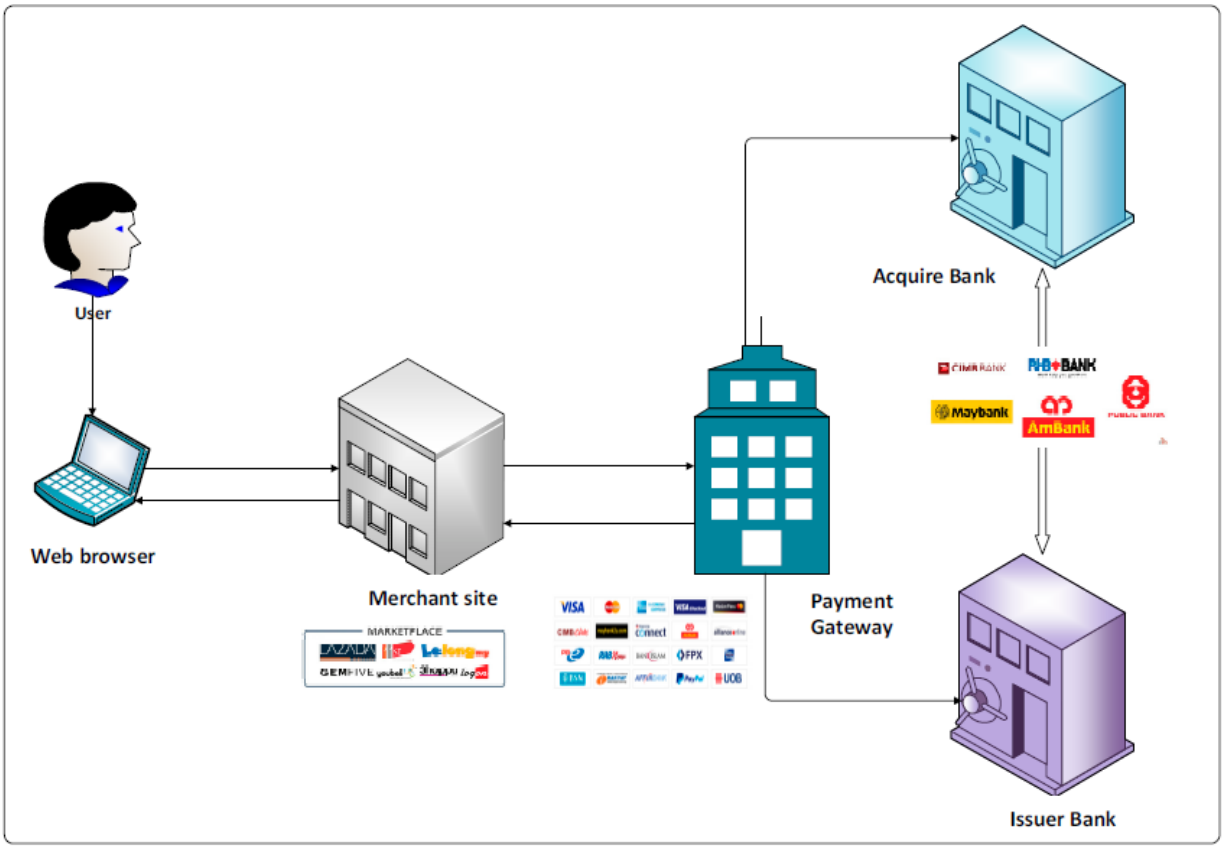

Рис 3.2 Запропонована модель системи електронних платежів

Шлюз виконує кілька кроків перевірки та пересилає петицію зареєстрованому клієнту банк. Одночасно платіжний шлюз пересилає деякі зашифровані повідомлення на сервер. Після отримання запиту на віднімання кількості, банк користувача аутентифікує його та переносить його до шлюзу транзакцій і підтверджує шлюз відрахування, після чого надсилає аутентифіковані дані до платіжного шлюзу. Платіжний шлюз обчислює необхідний результат, а також пересилає його до банку, де банк фіксує різні версії та відповіді на суму, які є прийнятними після перевірки. Користувач ініціює транзакцію, відправивши поштою свою короткострокову ідентичність сервера. Майте на увазі, що пара відкритих ключів продовжу акредитуватися через центр сертифікації.

Висновки до третього розділу

Дослідження технологію захисту електронних платіжних систем, та зазначено, що вона повинна складатися з засобів криптографічного захисту та планів конкретної платіжної системи. Неможливо створити незламний алгоритм шифрування, з часом кожен алгоритм стане застарілим, лише питання часу, та обчислювальної потужності обчислювальної машини.

Розроблено узагальнений сценарій інтеграції надстійкого криптографічного алгоритму на даний час на прикладі RSA який базується на обчислювальній складності завдання факторизації великих цілих чисел.

Моделювання показало, що при деяких сценаріях атаки на криптографічний алгоритм необхідне використання багаторівневих засобів захисту, а саме (багаторівневі рівні автентифікації, одноразові засоби ідентифікації сеансу, та ін.)

.

ВИСНОВКИ

чому В магістерській роботі отримано наступні наукові та науково-практичні результати: Проналізовано основні поняття електронно платіжних систем, з’ясовано головні сфери використання в інформаційних системах. Визначено, що більша частина всіх методів і алгоритмів використовує за основу алгоритм DES. Кожен криптографічний алгоритм має бути криптостійким та відповідати стандартам що зазначені для конкретної електронно платіжної системи

Зазначено, що з точки зору безпеки, асиметричне шифрування, безперечно, краще, оскільки воно забезпечує аутентифікацію. Однак продуктивність є аспектом, який не можна ігнорувати, тому симетричне шифрування завжди буде необхідно. Один ключ використовується для шифрування та дешифрування даних.

Досліджено що від принципу роботи платіжної системи та моделі загроз залежить і засоби захисту. Реалізація рекомендованих регулятором заходів безпеки має призвести до підвищення захищеності електронних платежів, зниження кількості несанкціонованих фінансових трансакцій та списань із банківських карток. Безпека коштів громадян повністю залежить від готовності банків та операторів виконувати вимоги регуляторів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Miva. The History of Ecommerce: How Did It All Begin?—Miva Blog. Available online: https://www.miva.com/blog/the-history-of-ecommerce-how-did it-all-begin/ (accessed on 16 June 2020).

2. Alam, S.S.; Ali, M.H.; Omar, N.A.; Hussain, W.M.H.W. Customer satisfaction in online shopping in growing markets: An empirical study. Int. J. Asian Bus. Inf. Manag. 2020, 11, 78–91.

3. Noor Ardiansah, M.; Chariri, A.; Rahardja, S.; Udin, U. The eect of electronic payments security on e-commerce consumer perception: An extended model of technology acceptance. Manag. Sci. Lett. 2020, 10,73–81.

4. Soare, C.A. Internet Banking Two-Factor Authentication using Smartphones.J. Mob. Embed. Distrib. Syst. 2012, 4, 12–18.

5. Закон України “Про електронні документи та електронний документообіг” 121

6. Закон України “Про електронний цифровий підпис” 127

7. Приклади обчислення цифрового підпису згідно* ДСТУ 4145–2002

8. Захарченко Н. В. и др. Развитие криптографии и ее место в современном обществе. Ч. 1. Классические методы шифрования: Учеб. пособие /

9. Н. В. Захарченко, Л. Г. Йона, Ю. В. Щербина, А. В. Онацкий – Одесса: ОНАС им. А. С. Попова, 2003. – 95 с.

10. Кисель В. А., Захарченко Н. В. Основы криптографии: Учеб. пособие.– Одесса: УГАС им. А. С. Попова, 1997. – 48 с.

11. Защита информации в системах телекоммуникации: Учеб. пособие.

Под ред. В. Л. Банкета. – Одесса: УГАС им. А. С. Попова, 1997. – 96 с.

12. Горохов С. М., Йона Л. Г., Онацький О. В. Сучасні криптографічні системи: Навч. посібник / Під. ред. М. В. Захарченка, – Одеса: ОНАЗ

ім. О. С. Попова, 2007. – 152 с.

11. Digital cellular telecommunications system Vocabulary for 3GPP Specifications(3GPP TR 21.905 version 14.1.1 Release 14) 40-45

12. ISO/IEC 9594-8:2017 21-25

13. Integrated Circuit Card Specifications for Payment Systems 176