Житомирська політехніка	Міністерство освіти і науки України Державний університет «Житомирська політехніка»

ЛЕКЦІЯ №7

КРИПТОГРАФІЧНІ ПРОТОКОЛИ. ПРОТОКОЛИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ. ЕЛЕКТРОННО-ЦИФРОВИЙ ПІДПИС

План лекції:

1. КРИПТОГРАФІЧНІ ПРОТОКОЛИ.
2. ЕЛЕКТРОННІ ПЛАТЕЖІ:
   - ПЛАСТИКОВІ КАРТКИ.
   - СУРОГАТНІ ПЛАТІЖНІ ЗАСОБИ В INTERNET.
   - РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET.
   - ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET.
   - ЦИФРОВІ ГРОШІ.
3. ЕЛЕКТРОННО-ЦИФРОВИЙ ПІДПИС.

ПИТАННЯ №1

КРИПТОГРАФІЧНІ ПРОТОКОЛИ

ЗАВДАННЯ КРИПТОГРАФІЇ:

У класичній Шеннонівській моделі системи секретного зв'язку є два учасники, які повністю довіряють один одному і яким необхідно передавати між собою інформацію, не призначену для третіх осіб. Завдання *забезпечення конфіденційності* (тобто захисту секретної інформації від зовнішнього противника) історично є **першим завданням криптографії**. Воно традиційно вирішується за допомогою криптосистем.

Крім забезпечення конфіденційності, криптографію **часто використовують для вирішення таких завдань**:

- *перевірка автентичності (аутентифікація)* – одержувач повідомлення має мати можливість
- встановити його джерело, а зловмисник не здатний замаскуватися під когось іншого;
- *забезпечення цілісності* – одержувач повідомлення може перевірити, чи не було повідомлення змінено в процесі доставки, а зловмисник не здатний видати неправдиве повідомлення за справжнє;
- *незаперечення авторства* – відправник повідомлення згодом не повинен мати можливість заперечувати надсилання повідомлення;
- *забезпечення невідстежуваності (анонімність)* – відправник повідомлення може виконувати законні дії (наприклад, оплату послуг через Інтернет), не будучи впізнаним (ідентифікованим).

ВІДМІННОСТІ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ ВІД КРИПТОСИСТЕМ

Якщо завдання забезпечення конфіденційності розв'язують за допомогою криптосистем, то для розв'язання інших завдань розробляють криптографічні протоколи. Є й інші **відмінності криптографічних протоколів від класичних криптосистем**, з яких можна виділити такі:

- протоколи можуть бути інтерактивними, тобто передбачати багатораундовий обмін повідомленнями між учасниками;
- у протоколі може бути задіяно більше двох учасників;
- учасники протоколу можуть не довіряти один одному. Тому криптографічні протоколи мають захищати їхніх учасників не тільки від зовнішнього противника, а й від нечесних дій партнерів.

Таким чином, ***протокол*** – сукупність правил, що регламентують послідовність кроків, які здійснюються двома або більшою кількістю сторін для спільного розв'язання певної задачі, а також регламентують формати повідомлень, які пересилаються між учасниками обміну, та дії при виникненні збоїв.

Збої під час обміну повідомленнями можуть виникати внаслідок помилкових, зокрема й навмисно помилкових дій учасників або зміні їхньої послідовності, а також унаслідок пропажі або викривлення повідомлень, які передаються, у передавальному середовищі. На регламентацію дій у разі виникнення збоїв слід звернути особливу увагу, оскільки її часто не беруть до уваги, що може повністю зруйнувати безпеку учасників навіть у стійкому криптографічному протоколі.

Опис протоколу, що виключає неоднозначність сприйняття, називають ***специфікацією протоколу***.

Криптографічні протоколи – порівняно молода галузь математичної криптографії. Перші протоколи з'явилися приблизно наприкінці 70-х р. двадцятого століття. Відтоді ця галузь бурхливо розвивалася, і за останні десятиліття перетворилася на основний об'єкт досліджень у теоретичній криптографії. На даний момент є вже не менше двох десятків різних типів криптографічних протоколів.

КЛАСИФІКАЦІЯ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

ХАРАКТЕРИСТИКА КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Тип протоколу	Коротка характеристика
За практичним застосуванням	
примітивні	Не мають самостійного застосування. Використовуються як своєрідні "будівельні блоки" під час розроблення прикладних протоколів.
прикладні	Розв'язують конкретну прикладну задачу, яка виникає (або може виникнути) на практиці.
За наявністю третьої сторони	
з посередником	Посередник бере участь у протоколі та допомагає його виконати двом сторонам. Сторони можуть не довіряти одна одній, але вони повністю довіряють посереднику.
з арбітром	Посередник вступає в протокол тільки у виняткових випадках – коли між сторонами виникають розбіжності.
самодостатні	Посередник відсутній – чесність сторін гарантується самим протоколом.

НАЙПОШИРЕНІШІ КРИПТОГРАФІЧНІ ПРОТОКОЛИ

ПИТАННЯ №2

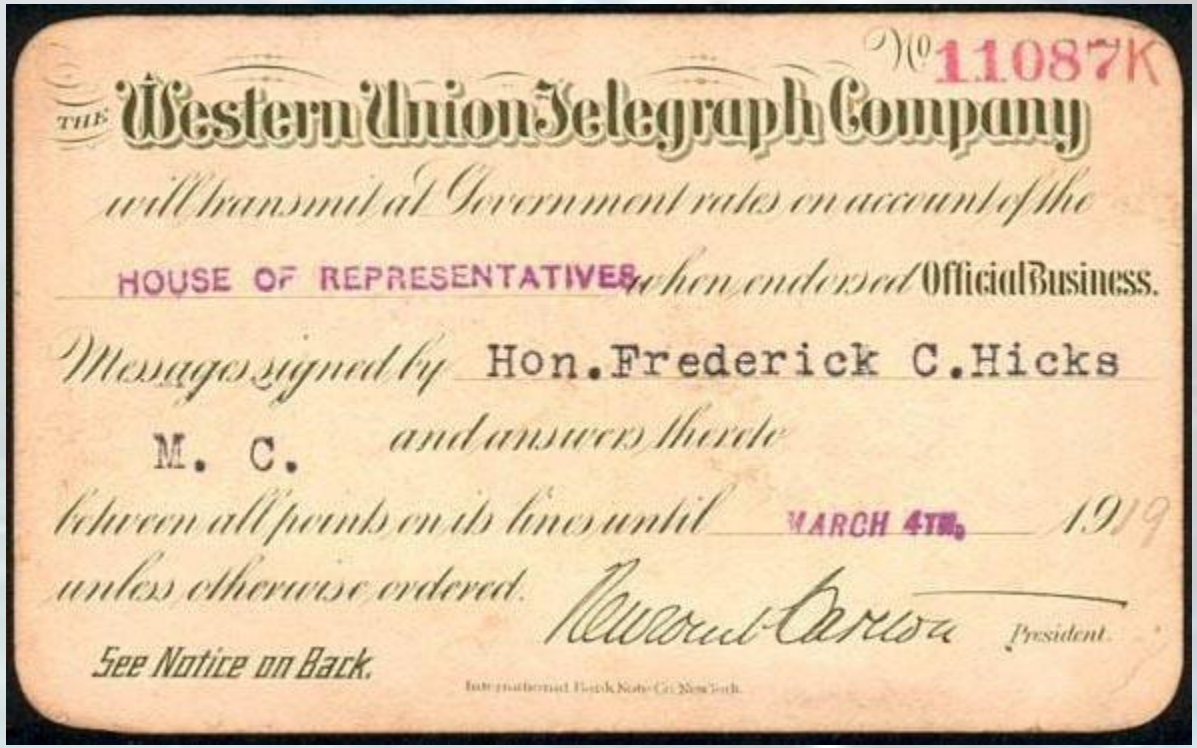
ЕЛЕКТРОННІ ПЛАТЕЖІ

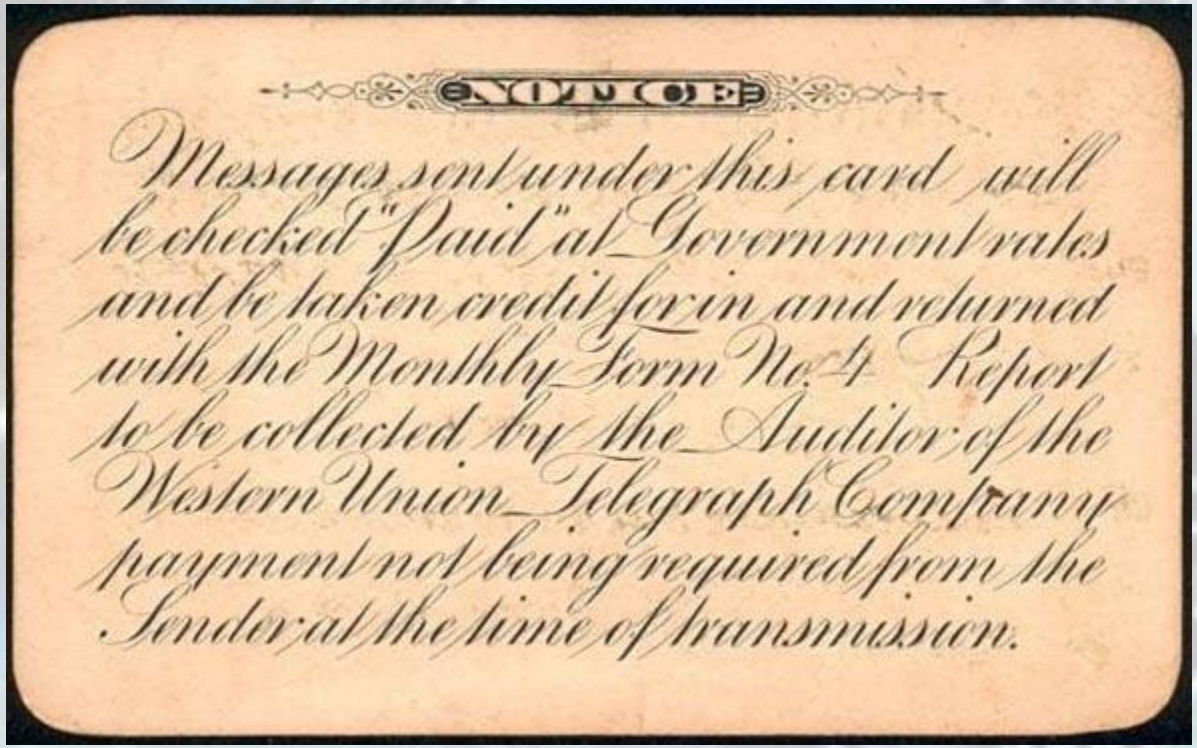
ПЛАСТИКОВІ КАРТКИ

На початку XX ст. альтернативним (до векселів і чеків) інструментом безготівкової форми оплати товарів і послуг стали картки. У 1888 р. Едуард Белламі (Edward Bellamy) у своїй книзі "Озираючись назад" (англ. Looking Backward) уперше вживає термін "кредитна картка", під якою розуміли щось схоже на картку соціального страхування для нарахування дивідендів громадянам від держави. У реальності ж **найперша кредитна картка була випущена General Petroleum Corporation California** (зараз Mobil Oil) у 1914 р. Власник картонної картки отримував значні зручності в обслуговуванні та знижки під час купівлі товару на будь-якій бензоколонці компанії, а компанія – постійних клієнтів і стабільні доходи.

Того ж року аналогічні карти (споживча платіжна карта – англ. customer charge card) випустила компанія Western Union Telegraph Company. Так, один із різновидів таких карток видавали тільки членам уряду США, він давав право відправляти телеграми в кредит за рахунок уряду. На зворотному боці картки є напис на цей рахунок – "Payment not being required from the sender at the time of transmission" ("Оплата під час передачі від відправника не вимагається").

КАРТКА WESTERN UNION ДЛЯ НАДСИЛАННЯ ТЕЛЕГРАМ





ПЛАСТИКОВІ КАРТКИ

Недовговічність картонних карток змусила шукати їм заміну, і через десять років почали з'являтися перші металеві картки з тисненням. Тиснення дало змогу частково автоматизувати процес обслуговування цих карток, оскільки з них можна було робити відбитки та переносити інформацію про власника на видрукувані чеки, що дало змогу вести облік і реєстрацію продажів за кожною з них. У 1928 р. компанія Charga-Plate почала випуск металевих карток, на яких було вказано ім'я та адресу клієнта.

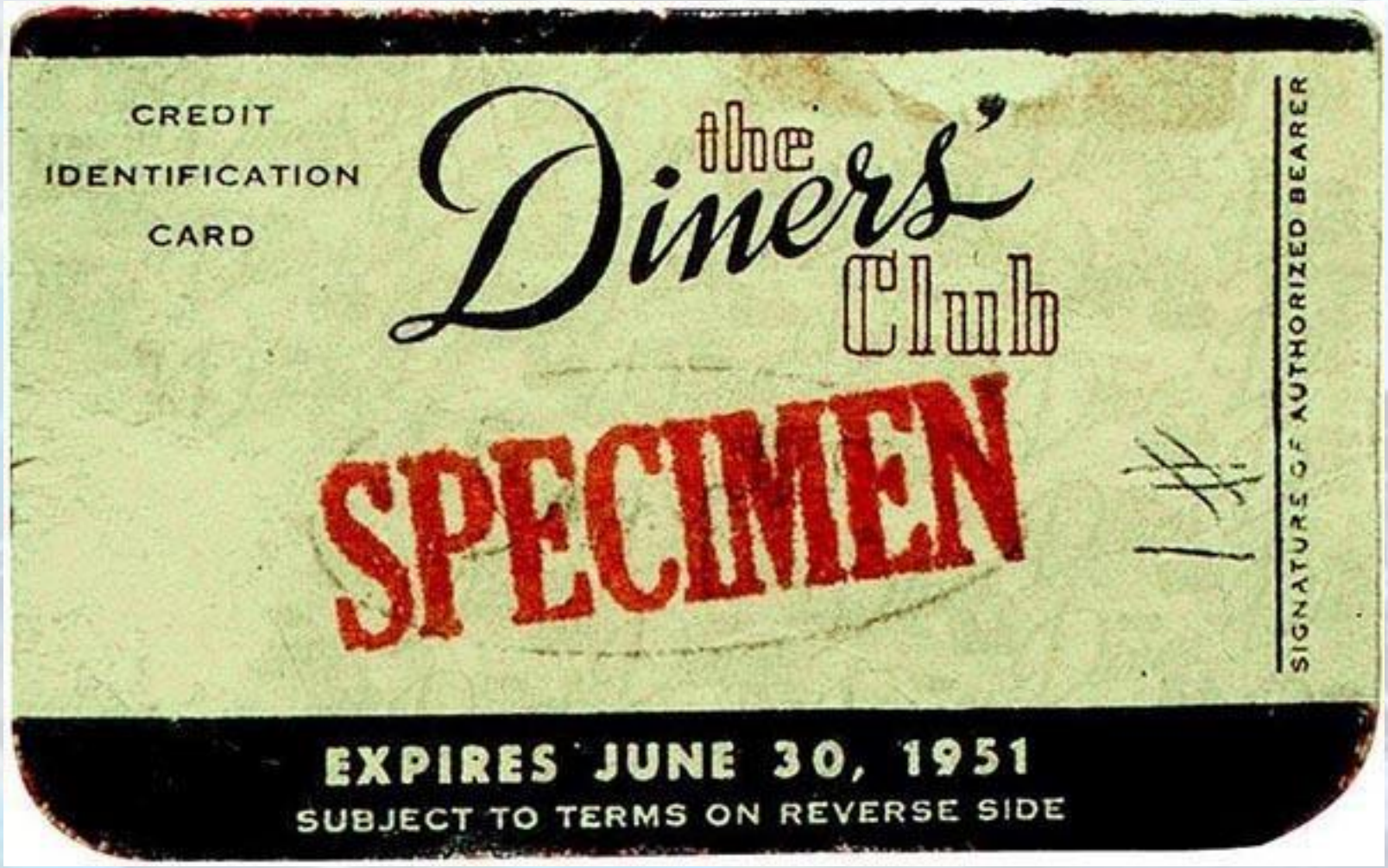
КАРТКА CHARGA-PLATE

ПЛАСТИКОВІ КАРТКИ

Першу банківську картку, на думку багатьох фахівців, придумав Джон С. Біггінс, який був експертом зі споживчого кредитування з Національного банку Флетбуш у Нью-Йорку. Біггінсом, який був експертом зі споживчого кредитування з Національного банку Флетбуш у Нью-Йорку. У 1946 р. він започаткував роботу за кредитною схемою "Charge-it". Ця схема будувалася на розписках клієнтів, якими оплачувалися покупки в магазинах. Після того як покупка відбулася, магазин здавав розписки в банк, і банк оплачував їх з рахунків покупців. У Флетбуші було вперше випробувано класичний ланцюжок розрахунків, який донині використовують у банківському картковому бізнесі.

У 1949 р. голова Hamilton Credit Corporation Френк Макнамара домовився з двома своїми приятелями, Альфредом Блумінгдейлом і Ральфом Снайдером, створити компанію, кредитні картки якої брали б до оплати більш ніж в одній торговельній мережі. На ідею створення таких карт Макнамара наштовхнула неналежна до його статусу ситуація, коли, повечерявши у своєму улюбленому ресторані Major's Cabin Grill (Нью-Йорк), він виявив, що забув гаманець удома. У результаті йому довелося телефонувати дружині і просити, щоб вона привезла гроші в ресторан. Таким чином, у 1950 р. з'явилася **перша універсальна платіжна система**, що отримала назву **Diners Club ("Ресторанний (обідній) клуб")**.

КАРТКА DINERS CLUB



ПЛАСТИКОВІ КАРТКИ

Назва Diners Club пояснюється тим, що спочатку кредитні картки Diners Club безплатно роздавали завсідникам 14 нью-йоркських ресторанів, розташованих поблизу від Empire State Building. Картки друкувалися на прямокутнику зі щільного паперу зі списком ресторанів на зворотному боці. Власник картки пред'являв її в ресторані, той передавав копії рахунків у Diners Club, яка раз на місяць виставляла клієнту загальний рахунок. Клієнт розплачувався з Diners Club, а компанія – з ресторанами. До кінця 1950 р. у компанії було близько 20 тисяч клієнтів, а картки приймали у 285 ресторанах. У 1953 р. компанія почала міжнародну діяльність (Великобританія, Канада, Мексика і Куба), ставши першою міжнародною платіжною системою, що працює з кредитними картками, а в 1969 р. її картки першими почали приймати в СРСР.

ПЛАСТИКОВІ КАРТКИ

Першу банківську картку було випущено 1951 р. (банк Franklin National Bank, Нью-Йорк), першу пластикову картку – 1959 р. (American Express), перша пластикова картка з магнітною смугою – у 1970 р. (IBM, American Express і American Airlines), перша смарт-картка – у 1983 р. (France Telecom).

Пластикові картки бувають трьох різновидів:

- кредитні;
- дебетові;
- з дозволеним овердрафтом.

ПЛАСТИКОВІ КАРТКИ

Кредитна картка (лат. credit – "він вірить") – персоніфікований платіжний інструмент, призначений для здійснення операцій (одержання готівки в банкоматах, оплати товарів і послуг), що здійснюються винятково за рахунок грошових коштів, наданих банком клієнту в межах установленого ліміту відповідно до умов кредитного договору. Картка є "персоніфікованою", тому що містить інформацію, що містить номер картки або банківського поточного рахунку, ім'я та прізвище власника, строк придатності картки (дати початку та кінця строку) тощо. Кредитна картка може замінювати споживчі кредити та кредити на невідкладні потреби. Головною перевагою кредитних карток перед кредитами є можливість використання кредиту, не звітуючи перед банком про його цільове використання, та можливість постійного поновлення кредитної лінії після погашення.

ПЛАСТИКОВІ КАРТКИ

Дебетова картка (лат. debet – "він винен") – аналогічна до кредитної, за виключенням того, що розрахунки за нею виконуються винятково грошовими коштами клієнта, наявними на депозитному рахунку, прив'язаному до картки.

Картка з дозволеним овердрафтом – щось середнє між кредитною та дебетовою картками. Овердрафт (англ. overdraft – понад заплановане, перевитрата) – кредитування банком розрахункового рахунку клієнта (у межах встановленого ліміту) для оплати товарів і послуг у разі недостатності або відсутності на розрахунковому рахунку клієнта грошових коштів.

ПЛАСТИКОВІ КАРТКИ

Підприємства торгівлі та сервісу, що приймають картку, а також відділення банків утворюють **платіжну (приймальну) мережу**. Нині пластикові картки є найпоширенішою формою безготівкової оплати. Про популярність пластикових карток свідчить той факт, що в Європі у 2003 р. їх було в обігу 938 на 1 000 жителів, а за кожною з них було в середньому здійснено 38.6 операцій за рік.

Суттєвим недоліком карток із магнітною смугою є те, що її досить легко підробити, а PIN-код, який має бути відомий тільки власнику картки і необхідний для отримання готівки в банкоматах, можна з'ясувати різними способами.

Інший суттєвий недолік – картка під час кожного платежу повністю ідентифікує свого власника. Якщо власник картки використовує її для купівлі квитків на транспорт, то можна відстежити всі його поїздки, що в цивілізованому суспільстві без санкції прокурора неприпустимо. Аналогічним чином, для кожного власника карток можна зібрати інформацію про те, які товари і де він купує, якими послугами користується, які культурно-видовищні заходи відвідує тощо.

Усунути останній недолік покликані так звані ***електронні гаманці*** та ***картки передоплати/картки зі збереженою вартістю*** – картки, що дають змогу зберігати у своїй пам'яті певну "суму" (гроші, хвилини, літри, поїздки), витрачати яку можна без жодної авторизації. Звісно, ця "сума" попередньо має бути "покладена в гаманець". Електронні гаманці також не позбавлені недоліків – як і для звичайного гаманця зі справжніми грошима, якщо його вкрали, то гроші, наявні на поточний момент у гаманці, можна вважати втраченими.

СУРОГАТНІ ПЛАТІЖНІ ЗАСОБИ В INTERNET

На зорі електронних платежів через Інтернет застосовувалися різні типи сурогатів. Ці засоби розрахунків пропонувалися кількома компаніями, найвідоміші з яких First Virtual Holdings і Software Agents. Електронні гроші в таких системах представлялися у вигляді **цифрових купонів** і **жетонів**. Клієнт за готівковий або безготівковий розрахунок купував у "банку" на деяку суму послідовності символів (для них "банк" гарантував ***нетривіальність алгоритму генерації*** та ***унікальність кожного екземпляра***), якими розплачувався з торговцем. Торговець повертав їх у "банк" в обмін на ту саму суму, за вирахуванням комісійних. При цьому на "банку" лежав обов'язок контролю наявності жетона в реєстрі виданих і відсутності в реєстрі тих, що надійшли назад. Під час пересилання жетонів через Internet використовували шифрування з відкритим ключем.

Недолік – ідентифікація власника жетонів.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

Розрахунок пластиковими картками в Інтернеті є одним з найпоширеніших способів здійснення онлайн-платежів. Цей метод надзвичайно зручний, безпечний і доступний для користувачів у всьому світі. Ось, як він працює:

1. **Вибір товарів або послуг**: Спочатку ви переглядаєте або вибираєте товари або послуги в інтернет-магазині, на веб-сайті або в додатку. Після того, як ви виберете те, що хочете придбати, ви переходите до етапу оплати.
2. **Вибір способу оплати**: Під час оформлення замовлення ви обираєте спосіб оплати, який зазвичай включає оплату пластиковою карткою. Ви можете ввести дані своєї карти в онлайн-форму або використати попередньо збережену інформацію про карту, якщо це можливо.
3. **Введення даних карти**: Вам потрібно ввести наступну інформацію з вашої карти:
   - Номер картки: Це унікальний 16-значний номер на передній стороні карти.
   - Термін дії: Дату закінчення терміну дії вашої карти.
   - CVV (Card Verification Value) або CVC (Card Verification Code): Трьохзначний (або чотиризначний) код, який зазвичай знаходиться на зворотній стороні карти.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

4. **Авторизація**: Після введення даних карти система зв'язується з банком, який видав вашу карту, для отримання авторизації на оплату. Банк перевіряє, чи є достатньо коштів на рахунку та чи відповідають введені дані валідній картці.
5. **Підтвердження оплати**: Якщо операція пройшла успішно, ви отримуєте підтвердження оплати, яке може бути надіслане вам на пошту або виведене на веб-сайті. Ви також можете отримати підтвердження оплати від вашого банку через SMS або інший спосіб сповіщення.
6. **Завершення замовлення**: Після успішної оплати ви можете завершити процес замовлення і отримати свій товар або послугу.

Цей спосіб розрахунку є дуже популярним завдяки своїй зручності та широкому поширенню пластикових карт. Важливо слідкувати за безпекою та уникати введення інформації про карту на сумнівних або ненадійних веб-сайтах. По можливості необхідно використовувати картки з технологією EMV (що включає чіп), оскільки вони забезпечують додатковий рівень безпеки.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

У 1994 р. була заснована компанія **CyberCash**, яка першою запропонувала технологію, що дає змогу використовувати пластикові картки для розрахунків у Мережі. Пропоноване цією компанією програмне забезпечення використовує шифрування з відкритим ключем для конфіденційного передавання даних про пластикову картку від покупця до торговця. При цьому всі реальні розрахунки і платежі здійснюються засобами процесингових компаній без використання Internet. За CyberCash пішли й інші, а кульмінацією цього процесу стала угода про спільну діяльність із надання розрахункових послуг в Internet, укладена 9 січня 1995 р. між MasterCard і виробником комунікаційного програмного забезпечення Netscape.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

Розглянемо **порядок оплати товарів і послуг за допомогою платіжної системи CyberCash**. Попередньо покупець повинен завантажити загальнодоступне програмне забезпечення CyberCash Vallet через Інтернет – програму, що встановлює з'єднання між покупцем, продавцем та їхніми банками.

1. Вибравши товар, покупець натискає на кнопку CyberCash "PAY" панелі продавця.
2. Продавець надсилає покупцеві рахунок, який містить інформацію про покупку, що відображається на екрані дисплея покупця.
3. Покупець додає або обирає зі списку номер кредитної картки, що використовується для оплати, і вказує додаткові відомості.
4. Уся ця інформація забезпечується електронним підписом покупця, що реалізується за допомогою програми CyberCash, шифрується і передається продавцю разом із хеш-кодом рахунку.
5. При отриманні цього повідомлення, продавець додає до нього інформацію для авторизації банком, яка шифрується, забезпечується електронним підписом продавця і пересилається серверу CyberCash.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

6. Сервер CyberCash переадресує відповідну інформацію в банк, супроводжуючи її запитом на здійснення платежу на користь продавця, включаючи його авторизацію.
7. Банк дешифрує та обробляє отриману інформацію, після чого здійснює відповідну операцію з кредитною карткою.
8. Відгук банку передається серверу CyberCash, який надсилає продавцю електронну квитанцію, частину якої продавець переадресує покупцеві.

Для генерації ЕЦП використовується RSA, повідомлення шифруються DES, хеш-коди обчислюються за алгоритмом MD5.

Недолік – ідентифікація власника пластикової картки.

Процесингова компанія – :

1) фірма, що координує розрізнені процеси;

2) компанія, що координує розрахунки за кредитними картками між емітентом картки (банком, що випустив картку), еквайрером (банком, що здійснює розрахунки з торгівлею), торговельною фірмою і користувачем кредитної картки.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

Сучасні системи електронних платежів є невід'ємною частиною сучасного світу, де електроніка і цифрові технології відіграють ключову роль в повсякденному житті. Ці системи зробили електронні трансакції легшими, швидшими та більш безпечними, роблячи їх доступними для всіх. Давайте розглянемо деякі з найбільш важливих та популярних систем електронних платежів, які існують сьогодні:

- **PayPal**: PayPal є однією з найбільш відомих і поширених систем електронних платежів. Вона дозволяє користувачам надсилати та отримувати гроші через інтернет, пов'язуючи свій банківський рахунок або кредитну картку з обліковим записом PayPal.
- **Apple Pay і Google Pay**: Ці мобільні платіжні системи дозволяють користувачам здійснювати покупки через свої смартфони. Вони базуються на технології NFC (Near Field Communication) і дозволяють проводити контактні та безконтактні оплати.
- **Stripe**: Stripe є платіжною системою, спеціалізованою на онлайн-бізнесі. Вона надає інструменти для обробки кредитних карток та інших методів оплати в інтернет-магазинах та додатках.
- **Venmo**: Venmo є популярною серед молоді системою електронних платежів у Сполучених Штатах. Вона дозволяє користувачам надсилати гроші один одному та ділитися рахунками через мобільний додаток.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

- **Bitcoin та криптовалюти**: Криптовалюти, такі як Bitcoin, представляють собою цифрові активи, які можна використовувати для електронних платежів. Вони базуються на технології блокчейн і надають можливість швидких та глобальних транзакцій без посередників.
- **SWIFT і SEPA**: SWIFT (Society for Worldwide Interbank Financial Telecommunication) і SEPA (Single Euro Payments Area) - це системи для міжнародних банківських переказів. SWIFT використовується глобально, а SEPA спеціалізується на платежах в єврозоні.
- **AliPay і WeChat Pay**: Ці китайські платіжні системи дуже популярні в Китаї та надають можливість здійснювати платежі через мобільні додатки.
- **Payoneer**: Payoneer спеціалізується на глобальних бізнес-платежах та переказах грошей між різними країнами та валютами.

Ці системи змінюють спосіб, яким ми взаємодіємо з грошима та здійснюємо фінансові транзакції. Вони надають більше можливостей, комфорту та безпеки. Однак важливо пам'ятати про захист особистих даних та бути обережними при користуванні цими системами, особливо під час онлайн-платежів.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

Україна має велику кількість систем та платіжних сервісів, які дозволяють користувачам та підприємцям розраховуватися пластиковими картками в Інтернеті. Тут наведено деякі з найпоширеніших систем та платіжних сервісів для розрахунків пластиковими картками в Україні:

- **ПриватБанк**: ПриватБанк є найбільшим банком в Україні і надає рішення для онлайн-платежів через пластикові карти. Вони також надають послуги мерчант-аккаунтів для бізнесів.
- **Ощадбанк**: Ощадбанк також підтримує онлайн-платежі через пластикові карти, і це один з найбільших банків в Україні.
- **MonoBank**: MonoBank – це онлайн-банк, який надає можливість відкривати віртуальні картки та використовувати їх для онлайн-платежів. Вони також надають додаток для мобільних пристроїв.
- **WayForPay**: WayForPay – це платіжний сервіс, який дозволяє бізнесам приймати платежі пластиковими картками в Україні та інших країнах.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

- **LiqPay**: LiqPay – це платіжний сервіс, який надає можливість обробки онлайн-платежів та використання пластикових карток для оплати.
- **Platon**: Platon – це платіжний сервіс, який надає послуги обробки платежів для бізнесів та користувачів.
- **Portmone**: Portmone – це платіжний сервіс, який дозволяє споживачам та бізнесам робити платежі за допомогою пластикових карток через їх платформу.
- **PayU**: PayU – це міжнародний платіжний сервіс, який працює в Україні та надає послуги для обробки платежів в Інтернеті.

Ці системи та платіжні сервіси дозволяють користувачам та бізнесам в Україні легко та безпечно розраховуватися пластиковими картками в Інтернеті. Вибір конкретної системи залежить від потреби бізнесу, обсягу операцій та інших факторів. Будь ласка, звертайте увагу на комісії та умови обслуговування при виборі платіжної системи для вашого бізнесу або особистого використання.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

Забезпечення безпеки платежів пластиковими картками в Інтернеті є критично важливим завданням, оскільки цей метод оплати може стати предметом атак і зловмисного використання. **Деякі основні методи та рекомендації для забезпечення безпеки платежів з використанням пластикових карток в Інтернеті:**

- **SSL-захист**: Переконайтеся, що веб-сайти та платіжні системи, які ви використовуєте для розрахунків, використовують SSL (Secure Sockets Layer) або TLS (Transport Layer Security) шифрування для захисту передачі даних. Це забезпечує конфіденційність інформації, яка передається між вами та веб-сайтом.
- **Перевірка адреси**: Переконайтеся, що веб-сайт, на якому ви вводите дані картки, має правильну адресу. Не вводьте дані картки на сайтах, які не мають "https://" у посиланні або не виглядають достовірно.
- **Сильні паролі**: Встановіть сильні паролі для облікових записів, пов'язаних із вашими картками або платіжними системами. Використовуйте комбінації великих і малих літер, цифр і спецсимволів. Не використовуйте очевидні паролі, такі як "123456" або "password."
- **Використання двофакторної аутентифікації (2FA)**: Ввімкніть двофакторну аутентифікацію для своїх облікових записів на платіжних системах і банківських веб-сайтах. Це додасть додатковий рівень безпеки, оскільки для входу потрібно буде ввести код, який ви отримуєте на мобільний пристрій.
- **Не зберігайте дані картки**: Не зберігайте дані картки на веб-сайтах або в онлайн-сервісах, якщо це не є необхідністю. Більшість платіжних систем пропонують опцію одноразових платежів без зберігання інформації про картку.

РОЗРАХУНКИ ПЛАСТИКОВИМИ КАРТКАМИ В INTERNET

- **Моніторинг транзакцій**: Регулярно перевіряйте витрати та транзакції на своїх картках. Якщо ви помічаєте незвичні або непідтверджені операції, негайно повідомте банк або платіжну систему.
- **Антивірус та анти-malware софт**: Встановіть і оновлюйте антивірусне та анти-malware програмне забезпечення на своєму комп'ютері та мобільних пристроях для захисту від зловмисних програм.
- **Фішинговий фільтр**: Використовуйте фільтри для електронної пошти та браузера для виявлення підозрілих повідомлень та веб-сайтів.
- **Будьте уважні**: Будьте обережні і не вводьте інформацію про картку на публічних або ненадійних комп'ютерах або мережах Wi-Fi.
- **Сповіщення і моніторинг**: Налаштуйте сповіщення від свого банку або платіжної системи, щоб отримувати повідомлення про кожній транзакції, що відбувається на вашій картці.

Забезпечення безпеки платежів пластиковими картками в Інтернеті вимагає уважності та обережності. Дотримуючись цих рекомендацій та використовуючи безпечні методи оплати, ви зможете зменшити ризики шахрайства та незаконного використання вашої інформації.

ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET

Електронний гаманець (іноді називається криптогаманцем) – це програмне або апаратне засіб для зберігання, управління і використання криптовалют і цифрових активів. Електронні гаманці грають важливу роль в екосистемі криптовалют та дозволяють користувачам зберігати, відправляти і отримувати різні види криптовалют. **Ось деякі ключові аспекти електронних гаманців**:

- **Зберігання криптовалют**: Електронні гаманці дозволяють користувачам зберігати приватні ключі, які необхідні для доступу до їх криптовалютних активів. Ці приватні ключі зашифровуються і зберігаються в гаманці, забезпечуючи безпеку зберігання.
- **Відправлення та отримання криптовалют**: Користувачі можуть використовувати гаманці для відправлення криптовалют і отримання їх від інших користувачів або послуг.
- **Спостереження за балансом**: Електронні гаманці надають можливість перевіряти баланс криптовалютних активів та історію транзакцій.
- **Множина підтримуваних активів**: Багато електронних гаманців підтримують не тільки біткоін, але і різні альткоїни та токени, такі як Ethereum, Ripple, Litecoin і багато інших.

ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET

- **Апаратні гаманці**: Окрім програмних гаманців, існують апаратні гаманці, які є фізичними пристроями для зберігання криптовалют. Вони зазвичай вважаються більш безпечними, оскільки приватні ключі залишаються офлайн.
- **Безпека і приватність**: Електронні гаманці надають різні рівні безпеки та приватності. Деякі гаманці дозволяють користувачам повний контроль над їхніми приватними ключами, тоді як інші можуть надавати додаткові функції, такі як двофакторна аутентифікація та шифрування.
- **Резервне копіювання і відновлення**: Більшість гаманців дозволяють користувачам створювати резервні копії своїх приватних ключів, щоб вони могли бути відновлені в разі втрати гаманця або комп'ютера.
- **Аплікації для мобільних пристроїв**: Багато електронних гаманців також мають мобільні додатки для зручного використання на смартфонах та планшетах.
- **Децентралізовані гаманці**: Деякі гаманці дозволяють користувачам зберігати приватні ключі та керувати своїми криптовалютними активами без посередництва сторонніх служб.

ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET

Розглянемо платіжну систему з використанням електронних гаманців на прикладі першої такої системи в Інтернеті – Webmoney (1998 р.).

1. Користувач завантажує з сайту додаток для Windows, мобільного телефону або браузерну версію.
2. Користувач через програму реєструється (ПІБ, дата народження, адреса, e-mail, номер мобільного телефону) і йому присвоюється 12-значний ідентифікатор (WMID) і висилається файл-ключ, на доступ до якого користувач призначає пароль. Обмін інформацією виконується через SSL.
3. Кожен користувач може отримати як посвідчення своєї особи перед іншими користувачами системи WM-атестат (у тому числі й анонімний). Перевірити атестат будь-якого користувача системи можна в центрі атестації WMT.
4. Користувач заводить електронні гаманці, кожен з яких призначений для розрахунків у строго певній валюті. Поповнити гаманець можна кількома способами: банківським переказом зі свого розрахункового рахунка, готівкою через каси комерційних банків і Ощадбанку, через платіжні термінали й автомати з приймання готівки, за допомогою куплених WM-карток тощо.
5. Користувач може переказувати гроші з одного гаманця в інший (як свій, так і іншого користувача системи Webmoney), але в межах однієї валюти і з урахуванням комісії, що стягується.

ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET

6. Перерахувати в готівку гроші з електронного гаманця можна через відкритий рахунок у банку, спеціалізовані системи, атестовані пункти обміну тощо.
7. Під час оплати товарів і послуг покупець повідомляє продавцю свій WMID і номер гаманця, для яких продавець виставляє рахунок. Отримавши в WM-програмі рахунок, покупець підтверджує оплату або відмовляється від неї.
8. Спрощена процедура оплати без виписки рахунку (наприклад, за ігри, програми, фільми) можлива безпосередньо на сайті продавця через сервіс WM Merchant. У цьому випадку вся процедура оплати займає лічені секунди. Покупець формує на сайті своє замовлення, після чого його перенаправляють на сайт, де він авторизуєтесь за допомогою WM-програми і підтверджує своє бажання оплатити зазначену суму на користь вказаного WMID (продавця). Там же покупець вибирає свій гаманець, з якого здійснює платіж.

Для процедур автентифікації, шифрування, перевірки цілісності тощо використовують алгоритми і протоколи RSA, RC5, MD4, MD5 і SSL.

Недолік – ідентифікація покупця.

SSL – криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером на базі асиметричного шифрування.

RC5 – блоковий шифр, винайдений Р.Рівестом.

ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET

Деякі валютні активи та ключові аспекти сучасних електронних гаманців:

- **«Холодні» та «гарячі» гаманці**: Існують два основних типи електронних гаманців. «Гарячі» гаманці (Hot Wallets) доступні в мережі та підключені до Інтернету, що полегшує швидкий доступ до активів, але може бути менш безпечними. «Холодні» гаманці (Cold Wallets) фізично відокремлені від Інтернету і зазвичай використовуються для зберігання великих сум криптовалют, оскільки вони забезпечують більший рівень безпеки.
- **Мультивалютність**: Багато сучасних гаманців підтримують не тільки одну криптовалюту, але кілька різних активів. Це дозволяє користувачам зберігати та управляти різними видами криптовалют в одному гаманці.
- **Безпека**: Забезпечення безпеки – це один з найважливіших аспектів при виборі електронного гаманця. Сучасні гаманці надають різні заходи безпеки, включаючи двофакторну аутентифікацію (2FA), використання паролів та приватних ключів для захисту ваших активів.
- **Додаткові функції**: Багато гаманців мають додаткові функції, такі як можливість купівлі криптовалюти, інтеграція з біржами, конвертація активів, аналітика та інші корисні інструменти.
- **Мобільні гаманці**: Мобільні гаманці доступні для смартфонів і планшетів, що робить їх дуже зручними для щоденного використання. Користувачі можуть здійснювати оплати та перекази прямо зі свого мобільного пристрою.
- **Хмарні гаманці**: Деякі гаманці пропонують можливість зберігання криптовалют у хмарних сховищах. Це зручно для резервного копіювання та доступу до активів з різних пристроїв.
- **Анонімність**: Деякі гаманці надають можливість здійснювати анонімні транзакції, що цінується користувачами, які цінують приватність.

ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET

На сьогоднішній день існує багато сучасних електронних гаманців, які використовуються користувачами по всьому світу для зберігання та управління криптовалютами та цифровими активами.

Ось деякі з найпопулярніших та широко використовуваних електронних гаманців:

- **Coinbase**: Coinbase – це один з найбільших та найпопулярніших електронних гаманців та обмінників криптовалют в світі. Він дозволяє користувачам зберігати, купувати та продавати різні криптовалюти, такі як Bitcoin, Ethereum, Litecoin і інші.
- **Blockchain.info**: Blockchain.info – це онлайн-гаманець, який надає доступ до гаманця Bitcoin та Ethereum. Він є досить популярним серед користувачів криптовалют і має додаткові функції, такі як діаграми та статистика.
- **Exodus**: Exodus – це гаманець для криптовалют, який надає можливість зберігати більшість популярних криптовалют, включаючи Bitcoin, Ethereum, Ripple і багато інших. Він також має красивий інтерфейс і візуальний портфель.
- **Electrum**: Electrum – це легкий гаманець для Bitcoin, який спеціалізується на безпеці та швидкості. Він доступний для декількох платформ і дозволяє користувачам зберігати свої приватні ключі локально.

ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET

- **Trezor**: Trezor – це приклад апаратного гаманця, який надає максимальний рівень безпеки для зберігання криптовалют. Він виготовляється як фізичний пристрій, що забезпечує ізольоване зберігання приватних ключів.
- **Ledger**: Як і Trezor, Ledger є апаратним гаманцем, який забезпечує безпеку зберігання криптовалют та приватних ключів. Він має декілька моделей, включаючи Ledger Nano S та Ledger Nano X.
- **Atomic Wallet**: Atomic Wallet – це гаманець і обмінник, який підтримує багато криптовалют і дозволяє користувачам виконувати обмін між різними криптовалютами прямо з гаманця.
- **Trust Wallet**: Trust Wallet – це гаманець для мобільних пристроїв, розроблений для зберігання та керування Ethereum і токенами, які співпрацюють з Ethereum.
- **MyEtherWallet (MEW)**: MEW – це онлайн-гаманець, який спеціалізується на Ethereum і дозволяє користувачам зберігати Ether і ERC-20 токени.
- **Coinomi**: Coinomi – це мобільний гаманець, який підтримує багато різних криптовалют та токенів і надає зручний спосіб для зберігання криптовалют.

ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET

В Україні користувачі також мають доступ до багатьох сучасних електронних гаманців для зберігання та управління криптовалютами та цифровими активами. **Ось деякі електронні гаманці, які є популярними в Україні:**

- **MonoBank**: MonoBank – це український онлайн-банк, який надає можливість відкрити віртуальний банківський рахунок та гаманець для зберігання та управління гривневими та криптовалютними активами.
- **Platon**: Platon – це український платіжний гейт, який дозволяє користувачам обробляти платежі та використовувати гаманець для зберігання Bitcoin та інших криптовалют.
- **Trustee Wallet**: Trustee Wallet – це український мобільний гаманець для криптовалют, який дозволяє користувачам зберігати, відправляти та отримувати різні криптовалюти.
- **Hotmine Wallet**: Hotmine Wallet – це гаманець, розроблений українською компанією Hotmine, який дозволяє користувачам зберігати Bitcoin та інші криптовалюти.
- **Lykke Wallet**: Lykke – це гаманець, який надає можливість зберігати криптовалюти та токени. Він також має власну біржу для торгівлі криптовалютами.
- **Paytomat Wallet**: Paytomat Wallet – це український гаманець, який спеціалізується на криптовалютах, призначений для використання у ресторанах, кафе та інших закладах, де приймаються криптовалютні платежі.
- **Guarda Wallet**: Guarda Wallet – це мультикриптовалютний гаманець, який підтримує багато різних криптовалют і токенів. Він доступний на різних платформах, включаючи мобільні пристрої та веб-версію.

ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET

Забезпечення безпеки електронних гаманців є надзвичайно важливим завданням, оскільки криптовалюти та цифрові активи є цінними та цільовими для атак зловмисників. **Ось кілька важливих заходів та рекомендацій для забезпечення безпеки електронного гаманця:**

- **Вибір надійного гаманця**: Почніть з вибору надійного електронного гаманця. Дослідіть різні гаманці та виберіть той, який надає високий рівень безпеки та підтримує ваші криптовалюти.
- **Зберігання приватного ключа в безпечному місці**: Приватний ключ - це ключовий елемент для доступу до ваших цифрових активів. Зберігайте його в безпечному місці, відійдіть від публічного доступу та забезпечте його зашифроване зберігання.
- **Резервне копіювання приватних ключів**: Завжди робіть резервну копію свого приватного ключа. Це дозволить вам відновити доступ до активів у разі втрати чи знищення гаманця.
- **Використовуйте апаратні гаманці**: Апаратні гаманці є надійними фізичними пристроями, які ізолюють ваші приватні ключі від Інтернету і зловмисників. Розгляньте можливість використання апаратного гаманця для великих сум криптовалют.

ЕЛЕКТРОННІ ГАМАНЦІ В INTERNET

- **Оновлення гаманця**: Переконайтеся, що ви використовуєте останню версію вашого гаманця, оскільки вони можуть містити покращені заходи безпеки.
- **Використання двофакторної аутентифікації (2FA)**: Ввімкніть 2FA для доступу до вашого гаманця. Це додасть додатковий рівень безпеки, оскільки потрібно буде ввести одноразовий код для входу.
- **Обережність в мережі**: Уникайте відвідування підозрілих веб-сайтів і не вводьте свої дані з доступом до гаманця на них. Уникайте публічних Wi-Fi мереж і відмовляйтеся від спам-повідомлень та фішингових атак.
- **Не діліться приватними ключами або мнемонічними фразами**: Ніколи не надавайте свій приватний ключ, мнемонічну фразу чи іншу конфіденційну інформацію іншим особам.
- **Регулярно слідкуйте за аккаунтом**: Перевіряйте баланс та історію транзакцій свого гаманця, щоб вчасно виявляти незвичайні операції.
- **Оперативно оновлюйте паролі та PIN-коди**: Регулярно змінюйте паролі та PIN-коди для вашого гаманця і інших облікових записів.

Забезпечення безпеки електронного гаманця вимагає обережності та відповідальності. Дотримуючись цих заходів безпеки, ви зменшуєте ризик втрати криптовалют і незаконного доступу до них.

ЦИФРОВІ ГРОШІ

Переваги і, насамперед, недоліки різних форм безготівкової оплати привели відомого голландського математика Девіда Чома (англ. David Chaum) у 1980-х рр. до ідеї застосування цифрових грошей, які володіють властивістю невідстежуваності. У 1994 р. очолювана ним компанія DigiCash представила технологію мережевих електронних грошей "ecash".

Цифрові гроші – числа, використані як грошові знаки. Оскільки число як таке представляється послідовністю бітів, яка може існувати в необмеженій кількості копій, які не відрізняються одна від одної, очевидно, ключову роль у будь-якій технології забезпечення цифрових платежів відіграє запобігання копіювання "банкнот" та їхнього повторного використання.

У протоколі електронного платежу задіяні три учасники, яких будемо називати: банк, покупець (клієнт) і продавець. Покупець і продавець, мають рахунок у банку, а покупець бажає заплатити продавцю за товар або послугу. Далі розглянемо основні моменти взаємодії банку, покупця і продавця.

ЦИФРОВІ ГРОШІ

Етап 1. Переказ грошей з фіатної форми (гроші, номінальна вартість яких встановлюється, забезпечується і гарантується державою за допомогою її авторитету і влади) в цифрову (генерація цифрових грошей).

№ п/п	Опис операції	Приклад
1	Під час сеансу зв'язку клієнт і банк (точніше, їхні програми-представники) аутентифікують один одного.	
2	Клієнт генерує унікальний номер "монети" **m**.	m = 3
3	Вибирає випадкове число r і відсилає повідомлення **m'** = (r^e * m) mod n, де **e** і **n** - відкритий ключ банку. Крім цього клієнт повідомляє банку, яким має бути номінал цієї монети.	r = 5 m' = (5^5 * 3) mod 91 = 2
4	Банк завіряє "монету" **s'** = $(m')^{di}$ mod n і надсилає **s'** клієнту. У цьому виразі **di** - закритий ключ банку, що відповідає запитаному номіналу "монети".	s' = 2^{29} mod 91 = 32
5	Банк зменшує фіатний рахунок клієнта на номінал "монети".	
6	Клієнт обчислює цифровий підпис банку **s** для вихідного номера "монети" **m,** виходячи з рівняння (s * r) mod n = s' або s = (s' * r^{-1}) mod n, де r^{-1} - обернене число за модулем n.	s = 61 [(s * 5) mod 91 = 32] або r^{-1} = 73 [(5 * 73) mod 91 = 1] s = (32 * 73) mod 91 = 61

ЦИФРОВІ ГРОШІ

У цій схемі $\mathbf{r^e}$ – **"закриваючий множник"** (англ. blinding factor). Завдяки застосуванню цього множника банк не знає номер "монети", що підписується, але залишає клієнту цифровий підпис для "монети" з цим номером. Використання "закриваючого множника" і становить основу **"сліпого (затемненого) підпису"**, запропонованого Чомом. Завдяки використанню цього підпису банк не в змозі встановити клієнта, який здійснює оплату цією монетою, але водночас зберігає можливість стежити за одноразовим використанням кожної "монети".

"Відкритий підпис": $s = m^{di} \bmod n = 3^{29} \bmod 91 = 61$.

Підпис **s**, отриманий у результаті відкритого підписання повідомлення **m** і сліпого підписання повідомлення **m'**, ідентичний.

ЦИФРОВІ ГРОШІ

Етап 2. Платіж.

1. Для оплати товарів або послуг покупець передає продавцю номер "монети" m і цифровий підпис до неї **s**.
2. Продавець пересилає цю інформацію в банк або на свій страх і ризик залишає її в себе, щоб потім переслати.
3. Банк перевіряє свій підпис під "монетою" і факт її використання вперше. Якщо "монета" проходить перевірки, то продавцю повідомляють номінал монети, а номер "монети" заносять до реєстру використаних.
4. Продавець вважає оплату здійсненою, при цьому може дати покупцеві здачу готівкою.
5. Банк перераховує суму, еквівалентну номіналу "монети", на рахунок продавця.

Слід наголосити на одному важливому моменті – покупець не може бути ідентифікований навіть за умови змови продавця з банком.

Етап 3. Поповнення рахунку за рахунок цифрових грошей.

Клієнт зв'язується з банком і відправляє йому отриману "монету" (**m** і **s**), закривши її відкритим ключем банку. Банк перевіряє, чи не була вона вже використана, заносить номер у регістр використаних і зараховує відповідну суму на рахунок клієнта.

Незважаючи на всі переваги цифрових грошей, зазначимо все ж таки один недолік. Оскільки "монети" (**m** і **s**) до використання необхідно десь зберігати (на цифровому носії), то існує ймовірність їх крадіжки.

ПИТАННЯ №3

ЕЛЕКТРОННО-ЦИФРОВИЙ ПІДПИС

ЕЛЕКТРОННО-ЦИФРОВИЙ ПІДПИС

Відповідно до ст. 5 Закону України «Про електронні документи та електронний документообіг» ***Електронний документ (ЕД)*** – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язков реквізити документа, зокрема електронний цифровий підпис.

Ст.1 Закону України «Про електронний цифровий підпис» було визначено:

Електронний підпис (ЕП) – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних.

Електронний цифровий підпис (ЕЦП) – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його **цілісність** та **ідентифікувати підписувача**. ЕЦП **накладається за допомогою особистого ключа** та **перевіряється за допомогою відкритого ключа**.

Особистий ключ (ОК) – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Відкритий ключ (ВК) – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису.

Засвідчення чинності відкритого ключа здійснювалося шляхом формування ***сертифіката відкритого ключа*** – документа, що видавався центром сертифікації ключів.

ЕЛЕКТРОННО-ЦИФРОВИЙ ПІДПИС

Сертифікат відкритого ключа – документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в **електронній формі** або у **формі документа на папері** та використовуватися для ідентифікації особи підписувча.

Процес електронного цифрового підпису виглядав таким чином:

1. Підписувач генерує пару ключів – особистий та публічний. Особистий ключ залишається у відправника і зберігається в таємниці. Відкритий ключ передається одержувачу.
2. Підписувач за допомогою свого закритого ключа здійснює криптографічне перетворення документу, формуючи електронний цифровий підпис.
3. Одержувач, отримавши документ, проводить криптографічне перетворення документу з використанням публічного ключа.
4. Без наявності відкритого ключа одержувач не лише не міг переконатися у приналежності інформації її відправнику, а й прочитати зашифрований документ.

НОВИЙ ЗАКОН

7 листопада 2018 року набув чинності **Закон України «Про електронні довірчі послуги»**. З цієї дати втратив чинність Закон України «Про електронний цифровий підпис».

Одним із важливих нововведень закону про електронні довірчі послуги є те, що він запроваджує поняття ***«кваліфікований електронний підпис»***, яке замінило поняття «електронного цифрового підпису».

Згідно з Законом України «Про довірчі послуги» (далі Закон) електронний підпис може бути трьох категорій:

- електронний підпис
- удосконалений електронний підпис
- кваліфікований електронний підпис

ВИЗНАЧЕННЯ ЗГІДНО НОВОГО ЗАКОНУ

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

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

- він зроблений шляхом криптографічного перетворення даних, з якими пов'язаний, за допомогою спеціального обладнання або програмного забезпечення;
- при цьому застосовувався особистий ключ, який однозначно пов'язаний з підписувачем і дає змогу його електронної ідентифікації;
- якщо відбувається втручання в цілісність даних, скріплених таким підписом, таке втручання стає таким, що його можна виявити.

Кваліфікований електронний підпис (КЕП) – це такий підпис, що відповідає всім критеріям для УЕП і, додатково, таким критеріям:

- обладнання та/або програмне забезпечення, якими він здійснюється, підлягають додатковим вимогам;
- він базується на кваліфікованому сертифікаті відкритого ключа.

ВИЗНАЧЕННЯ ЗГІДНО НОВОГО ЗАКОНУ

Особистий ключ (ОК) – параметр алгоритму асиметричного криптографічного перетворення, який використовується як унікальні електронні дані для створення електронного підпису чи печатки, доступний тільки підписувачу чи створювачу електронної печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів.

Відкритий ключ (ВК) – параметр алгоритму асиметричного криптографічного перетворення, який використовується як електронні дані для перевірки електронного підпису чи печатки, а також у цілях, визначених стандартами для кваліфікованих сертифікатів відкритих ключів.

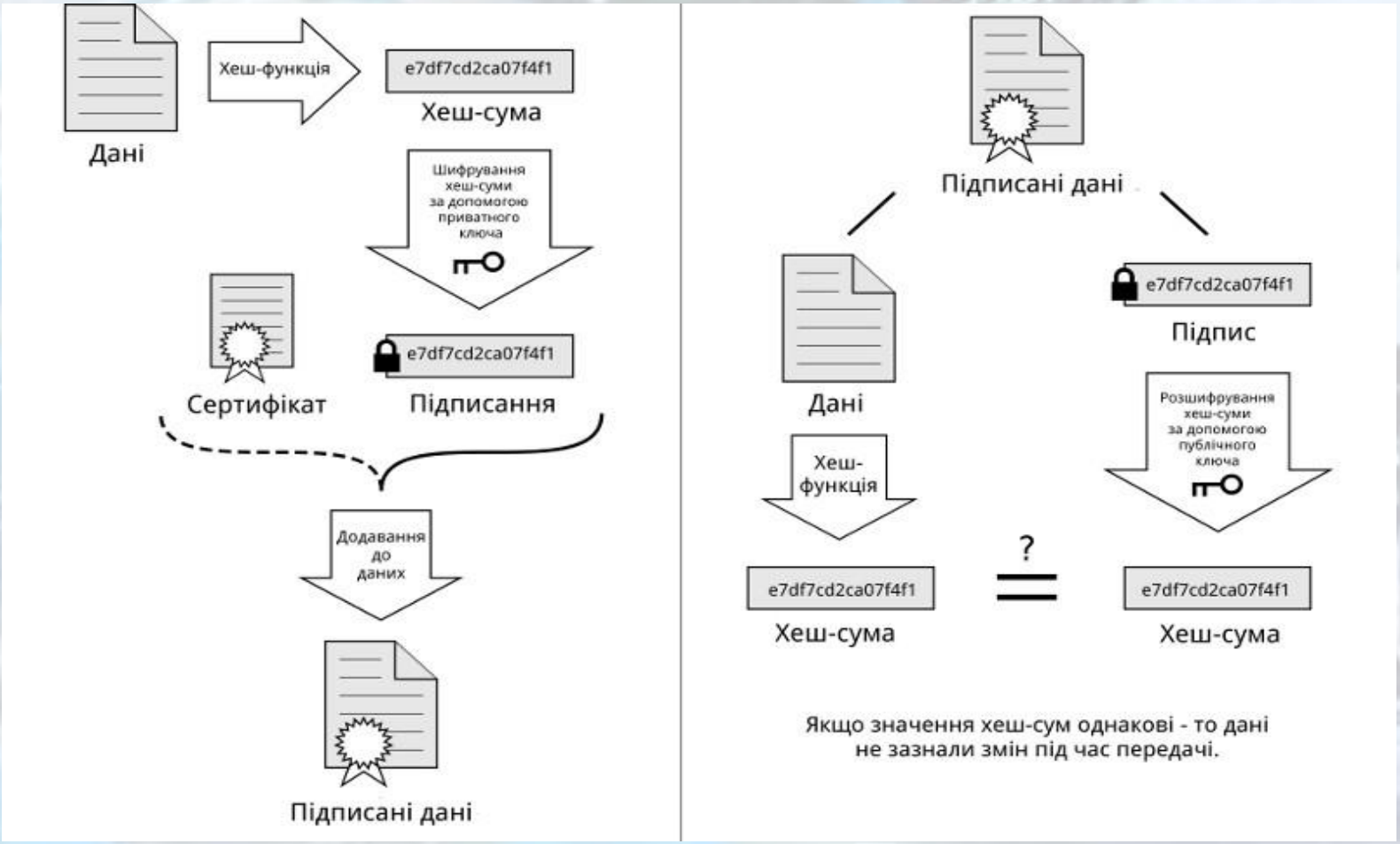
Пара ключів – особистий та відповідний йому відкритий ключі, що є взаємопов’язаними параметрами алгоритму асиметричного криптографічного перетворення.

Сертифікат відкритого ключа – електронний документ, який засвідчує належність відкритого ключа фізичній або юридичній особі, підтверджує її ідентифікаційні дані та/або надає можливість здійснити автентифікацію веб-сайту.

ПІДПИСАННЯ ДАНИХ ТА ВЕРИФІКАЦІЯ

Криптографічний захист електронних підписів заснований на шифруванні, яке передбачає використання пари "відкритий ключ – особистий ключ".

Підписувач



Кореспондент

Підписання даних **Верифікація**

ПІДПИСАННЯ ДАНИХ ТА ВЕРИФІКАЦІЯ

Відкритий ключ (ВК) доступний для кореспондентів і для підписувача, а **особистий ключ (ОК)** має перебувати тільки в підписувача.

При цьому **пара ключів створюється таким чином**, що присвоїти документу електронний підпис можна тільки за допомогою особистого ключа, але перевірити підпис можна за допомогою відкритого ключа, що відповідає особистому ключу.

Кореспондент, отримавши документ ***з удосконаленим електронним підписом***, може, у загальному випадку, покладатися на те, що це присвоєння було зроблено власником особистого ключа.

Однак використання пари ключів не вирішує питання ідентифікації підписувача.

Кореспондент бачить, що документу присвоєно конкретний підпис, але він не завжди може бути впевнений у тому, що:

- особистий ключ не було перехоплено
- відкритий ключ із самого початку не було створено зловмисником з метою видачі себе за підписувача.

ПІДПИСАННЯ ДАНИХ ТА ВЕРИФІКАЦІЯ

Щоб мінімізувати цей ризик, у схему вводиться третя сторона, яка перевіряє особу підписувача й, упевнившись, що дані відкритого ключа відповідають особистим даним підписувача, видає ***сертифікат*** – спеціальний набір даних, асоційований із відкритим ключем, що засвідчується.

Тепер кореспондент, одержавши підписаний документ, який пов'язаний не тільки з відкритим ключем, а і з сертифікатом, може покладатися й на те, що особа, яка застосувала електронний підпис, є тим, чий це підпис.

При цьому якщо третя сторона – засвідчувач внесена до спеціального **Довірчого списку**, то сертифікат, що видається нею, є **кваліфікованим сертифікатом**, і сама вона має **статус кваліфікованого надавача електронних довірчих послуг**.

СПРОЩЕНИЙ ОПИС КЛАСІВ ЕП

Отже, спрощено, класи електронних підписів можна описати таким чином:

- **Електронний підпис** – це будь-яка електронна форма даних, що використовується підписувачем як підпис, не обов'язково захищений. Приклад такого підпису – скан-зображення власноручного підпису, яке прикладається до текстового файла й конвертується у формат pdf.
- **Удосконалений електронний підпис** – це підпис, сформований з використанням засобів криптографії, але при цьому не обов'язково з використанням сертифіката, а якщо й з використанням, то не обов'язково, щоб сертифікат був кваліфікованим. Прикладом існуючого протоколу є рішення, засновані на стандарті OpenPGP.
- **Кваліфікований електронний підпис** – має бути заснований на криптографії, і відкритий ключ має бути підтверджений сертифікатом, і сам сертифікат повинен бути кваліфікованим.

СПРОЩЕНИЙ ОПИС КЛАСІВ ЕП

Крім електронного підпису, Закон запроваджує поняття й ***електронної печатки***. Електронна печатка також може бути **удосконаленою** та **кваліфікованою** – критерії цих класів аналогічні відповідним критеріям класів підписів.

Відмінність полягає в тому, що електронним підписом може користуватися як юридична, так і фізична особа, а електронною печаткою – тільки юридична.

Закон передбачає, що ***електронний підпис чи печатка не можуть бути визнані недійсними й позбавлені можливості розглядатися як доказ у судових справах виключно на тій підставі, що вони мають електронний вигляд чи не відповідають вимогам до кваліфікованого електронного підпису або печатки***.

Тобто відсутність кваліфікації не робить документ, що підписаний простим електронним підписом, автоматично недійсним, але **ступінь довіри до нього може бути низька**.

Кваліфікований електронний підпис, навпаки, **має презумпцію автентичності**. Але ця презумпція не означає незаперечність (навіть автентичність ручного підпису може бути оскаржена). **Удосконалений підпис займає середню позицію**.

ДЯКУЮ ЗА УВАГУ!