ВСТУП

Вузькоспеціальна, мало кого інтересуюча ще десять років тому тема електронних транзакцій і електронних грошей за останній час стала актуальною не тільки для бізнесменів, а й звичайних користувачів. Трендові слова "e-business", "e-commerce" знає, напевно, навіть дитина, яка хоч інколи читає комп'ютерну або популярну пресу. Завдання дистанційних транзакцій (переказу грошей на велику відстань) з розряду спеціальних перейшла в повсякденні. Однак велика кількість інформації з цього питання зовсім не сприяє ясності в умах громадян. Як через складність і концептуальної НЕ опрацьованості проблеми електронних розрахунків, так і в силу того, що багато популяризаторів працюють найчастіше за принципом зіпсованого телефону, на побутовому рівні все, звичайно, зрозуміло кожному. Але це до того часу, доки не настане черга практичного використання електронних транзакцій. Ось тоді і випливає нерозуміння того, наскільки використання електронних платежів стає невід’ємною частиною в тих чи інших випадках.

На сьогоднішній день завдання прийому електронних транзакцій стає все більш актуальним для тих, хто має на думці займатися комерцією з використанням мережі.

Основним ньюансом при знайомстві з системами електронних платежів для новачка є різноманіття їх пристроїв і принципів роботи і те, що при однотипності реалізації в їх глибині можуть бути сховані досить різні технологічні та фінансові механізми.

Безупинний розвиток популярності глобальної мережі призвів до виникнення нової хвилі підходів і рішень в найрізноманітніших областях світової економіки. Новій течії піддалися навіть такі

консервативні гіганти, як системи електронних платежів в банках. Це стало повштовхом для розвитку нових систем оплати - систем електронних платежів через Інтернет, головною перевагою яких полягає в тому, що клієнти можуть робити фінансові операції, минаючи виснажливі і іноді технічно важко здійснювані етапи фізичного транспортування платіжного доручення в банк. Банки і банківські установи проявили зацікавленість у впровадженні таких систем, так як вони дозволяють підвищити швидкість обслуговування клієнтів і оптимізувати накладні витрати на здійснення платежів.

В системах електронних платежів циркулюють дані, в тому числі і конфіденційні, які вимагають захисту від перегляду, модифікації та нав'язування невірної інформації. Прийняття відповідних технологій захисту, орієнтованих на мережу, викликає серйозні проблеми в даний час. Причина в тому, що архітектура, ресурси і технології мережі Internet орієнтовані на організацію доступу або збору відкритої інформації. Проте, за останній час з'явилися підходи і рішення, які дають можливість застосуванню стандартних технологій Інтернет в побудові систем захищеної передачі даних через Інтернет.

1 ОСНОВИ БЕЗПЕКИ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

1.1 Традиційна і електронна комерція

Нині у зв'язку із загальною інформатизацією і комп'ютеризацією банківської роботи значення інформаційної безпеки віддалених транзакцій в багато разів підвищилась. В результаті повсемістного поширення електронних транзакцій, пластикових карток, комп'ютерних мереж цілью інформаційних атак стали насамперед грошові кошти як банків, так і їх клієнтів. Виконати спробу обкрадання може будь-який - необхідно тільки комп’ютер, підключений до мережі Інтернет.

Дистанційна банківська транзакція - це певні операції, які супроводжують віддалену взаємодію клієнта і платіжної системи. Як приклади дистанційних транзакцій можна привести оплату товарів на просторах Інтернету, використання банкоматів, розрахунки в точках продажу. Як правило в транзакцію входять запит, виконання завдання і відповідь. Звідси наслідком банківських транзакцій є ці три пункти, гроші передаються по лініях зв'язку, саме тому питання захисту дистанційних банківських транзакцій є актуальним і існує безліч механізмів і засобів їх захисту. В цій області додаються серйозні зусилля, як в практичному, так і в теоретичному плані, впроваждуються останні досягнення спеціалістів, залучаються передові технології.

У загальному вигляді будь-яка економічна діяльність складається з процесу виробництва продукту і комерційної функції, основною метою якої є отримання користі за допомогою реалізації виробленого продукту. Комерційна функція, або просто комерція досить широке поняття, яке не передбачає лише продаж будь-якого продукту і отримання оплати за нього.

Традиційна комерція - це звичайний бізнес-процес, який можна показати у вигляді комерційної транзакції, в яку входять кілька етапів. Насамперед компанія виготовляє нову продукцію, потім виходить з нею на ринок, розповсюджує і

забезпечує гарантійну підтримку. Клієнти визначають свою потребу в будь-якому продукті, знайомляться з інформацією про нього, шукають шляхи покупки, порівнюють можливі варіанти з урахуванням вартості, рівня обслуговування, репутації продавця і лише після цього роблять покупки. Комерційна транзакція включає також перемовини про вартість, форму оплати та сроки доставки продукту, укладання угоди, оплату і виконання замови, фіксацію у вигляді документу факту здійснення правочину. Окрім клієнтів і постачальників учасниками правочину є також платіжні системи, банки та інші фінансові структури, що забезпечують переміщення коштів, а також виствітлюють способи доставки, виконують доставку товару споживачам.

Як клієнтів і постачальників можуть виступати:

• - звичайні громадяни (фіз. особи);

• - організації та підприємства (юр. особи).

По пройденню питаннь з реклами постачальник демонструє клієнту каталог товарів або послуг. Клієнт робить замовлення, де вказує назву і тип товару. На підставі замовлення постачальник надсилає йому пропозицію укласти доровір (оферту).

Оферта може здійснюватися у формі договору або, в спрощеному вигляді- рахунку. Якщо згоду отримано клієнт повертає постачальнику акцепт. Акцепт може бути виконаний у вигляді підписного договору або іншим способом. Оплата продукту, в залежності від можливостей клієнта і продавця, може бути оформлена готівкою або безготівковим способом. Оплата товару повинна бути пов'язана з етапом фізичної доставки товару або послуги клієнту.

Комерційна транзакція закінчується етапом фіксації факту завершення угоди, в процесі даного етапу оформляються такі документи як рахунок-фактура, акт, накладні. У найпростішому випадку, наприклад при роздрібній продажі товарів відносно низької вартості, оферта являє собою рахунок, який передається клієнту поштою, факсом або при особистій зустрічі. Акцепт у цьому випадку оформляється у вигляді оплати виставленого рахунку.

Електронна комерція - це вид комерційної діяльності, де відносини між її учасниками на всіх або деяких її етапах регулюються електронним способом. Таким чином, електронна комерція передбачає взаємодію між партнерами з використанням IT, що серьозно підвищує якість та ефективність бізнес-процесів. До електроннї комерції входять не тільки операції, пов'язані з купівлею-продажем товарів і послуг, а також і операції, спрямовані на стабільне отримання прибутку, утворення попиту на товари і послуги, гарантійну підтримку клієнтів і т.п. Електронна комерція, а саме технологія підтримки зовнішніх бізнес-контактів - це перша з двох стандартних складових електронного бізнесу. Друга частка - це автоматизація внутрішніх діяльностей компанії.

Існує декілька загальновизнаних способів, за якими працює електронна коменція

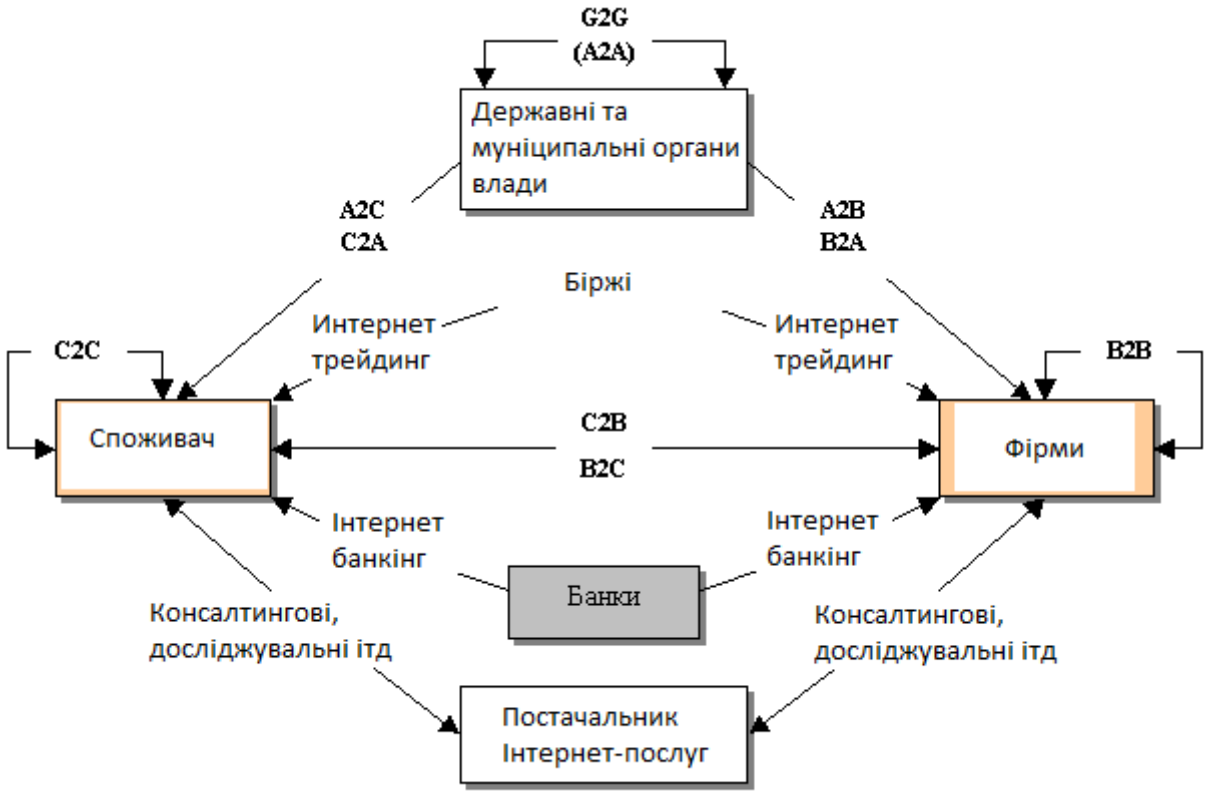

Рис. 1.1 Моделі електронної комерції

До основних способів ведення електронної комерції в Інтернеті відносяться наступні:

• B2C (Business-to-Consumer) ─ фірма─ клієнт ;

• B2B (Business-to-Business) ─ фірма─фірма;

• C2в (Consumer-to-Business) ─ клієнт ─фірма;

• C2C (Consumer-to-Consumer) - клієнт-клієнт;

• B2G або B2A (Business-to-Government, Business-to-Administration) ─ фірма-держава;

• G2B або A2B (Government-to-Business) ─ держава-фірма;

• G2C або A2C (Government-to-Consumer або Administration-to-Consumer) ─ держава-клієнт;

• C2G або C2A (Consumer-to-Government) ─ клієнт-держава;

• G2G або A2A (Government-to-Government) ─ "держава-держава";

• E2E (Exchange-to-Exchange) ─ біржа-біржа;

• інтернет банкінг;

• інтернет-трейдинг;

• інтернет-послуги: послуги дистанційної електронної комерції: системи електронних платежів, доставка продукту; консалтингові послуги; Інтернет страхування.

Схема B2B або бізнес-бізнес

Принцип виконання подібних взаємовідносин дуже простий: фірма торгує з іншою фірмою. B2B - одне з найбільш перспективних і активно розвиваючихся напрямів електронної комерції на сьогодення. Дані Інтернет-платформи роблять можливим значне спросщення проведення операцій на всіх етапах, за допомогою цих методів торгівля стає більш оперативною та прозорою. Найчастіше, в таких випадках представник з боку клієнта має змогу інтерактивно контролювати процес виконання замовлення шляхом доступу до бази даних продавця. Прикладом домовленості B2B - продаж сємплів дизайну сайту задля використання його в подальшому на власному веб-ресурсі. Незаперечно, до цього відносяться і будь-які взаємодії, до яких входять оптові поставки товару або схоже виконання замовлень.

Схема B2C або фірма-клієнт

У даному прикладі підприємство торгує на пряму з клієнтом (не юр. особою, а фізичною). Зазвичай мається на увазі роздрібна торгівля. Клієнту такий спосіб здійснення операції покупки дає можливість спростити та прискорити цю процедуру. Людині не доведеться йти в магазин, щоб зробити свій вибір: досить переглянути інформацію на сайті продавця, вибрати потрібний конфіг і замовити товар з доставкою. Продавцю ж можливості мережі дозволяють більш якісно і оперативніше моніторити попит. Прикладами даного типу торгівлі являються традиційні Інтернет-магазини які спрямовані на певну групу безпосередніх споживачів.

Схема C2C або клієнт-клієнт

Даний приклад електронної комерції здійснюється за допомогою укладення угод між двома клієнтами, жоден з яких не є продавцем в юридичному сенсі слова. Інтернет-плейси для такого типу торгівлі є чимось посереднім між базаром і колонкою оголошень в паперовій газеті. Зазвичай, комерція по схемі C2C виконується на сайтах маркетплейсах, що набули досить серьозної популярності за останні 10 років. Для юзерів даних сайтів основним і найбільш переважним плюсом є значно нижча ціна ніж у офіційних магазинах.

Існує і кілька інших способів електронної комерції, вони не набули такої популярності, але, все ж, застосовуються в деяких небуденних випадках. Йде мова про взаємодію державних структур з споживачами і підприємцями. За останній час стало нормою справити податки, виконати махінації з митницею за допомогою Інтернет мережі. З одного боку це позбавляє клієнтів частини паперової тяганини, а з іншого робота держ.службовців стала набагато простіша.

Зарубіжні стандарти електронної комерції (IOTP, JEPI).

Відкритий торговий протокол Інтернет IOTP (Internet Open Trading Protocol) заводить базу комерції за допомогою Інтернету. IOTP дає можливість обробити випадки, коли продавець стає клієнтом, дає інформацію щодо відстеження доставки товарів і проходження платежів та їх оформлення, також є можливість об’єднати всі ці функції. IOTP підтримує:

• Відомі моделі торгівлі

• Нові моделі торгівлі

• Глобальну сумісність

Протокол створений для звязку між клієнтами, продавцями та банками (фінансові організації). Він спроектований таким чином, щоб контролювати весь процес продажу, забезпечити його універсальність при будь-яких схемах електронних транзакцій. IOTP підтримує такі схеми платежів як MasterCard Credit, Visa Credit, Mondex Cash, Visa Cash, GeldKarte, eCash, CyberCoin, Millicent, Proton і т.п. Кожна схема обмінюється унікальними повідомленнями які не підходять до інших.

Документ який містить у собі схемно-залежні частини протоколу вказує необхідні вимоги в межах яких виконується торгова операція.

Відкритий торговий протокол Інтернет визначає деяке число різних операцій IOTP:

• Купівля. Здійснює пропозицію, оплату і опционно доставку.

• Повернення. Здійснює повернення платежу для покупки, виконаної раніше.

• Обмін цінностями. Включає в себе два платежу, наприклад в разі обміну валют.

• Аутентифікація. Проводить перевірку для організації або приватної особи - чи є вони тим, за кого себе видають.

• Відгук платежу. Здійснює відгук електронного платежу з фінансової установи.

• Депозит. Реалізує депозит коштів у фінансовій установі.

• Запит. Виконує запит стану операції IOTP, яка знаходиться в процесі реалізації, або вже виконана.

• Пінг. Простий запит однієї програми IOTP з метою перевірки, чи функціонує інший додаток IOTP.

JEPI, (Joint Electronic Payment Initiative) - це те, що стоїть між платежами і покупками.

Стандарт Joint Electronic Payment Initiative заснований на трьох протоколах:

1.. SET (Secure Electronic Transactions) - (SET, Безпечні електронні транзакції) - це стандартизований протокол для проведення операцій по кредитній / банківській картці через небезпечні мережі (наприклад Інтернет). SET це не сама платіжна система, а набір правил і протоколів безпеки (цифрових сертифікатів, криптографічних технологій) для аутентифікації здійснюваних транзакцій. Це дозволяє користувачам безпечно використовувати кредитні / банківські карти у відкритій мережі. Однак, SET не знаходила популярності. VISA тепер просуває XML-протокол 3-D Secure.

2. PEP (Protocol Extension Protocol) - протокол, який виконується поверх стандартного HTML на Web-сервері.

3. UPP (Universal Payment Preamble) - протокол переговорів, який визначає відповідну методологію розрахунків для продавця.

1.2 Безпека платіжних систем традиційної комерції

Платіжна система Інтернет - система здійснення розрахунків в процесі купівлі та продажу товарів між безнес організаціями та користувачами Інтернету. Така платіжна система дає можливість перетворити службу по обробці замовлень в повноцінний магазин, що зі сторони клієнта є незаперечним плюсом, бо покупку можна здійснити не відходячи від комп’ютера.

В даній системі електронної комерції платіж є дійсним лише при дотриманні певних умов:

• Дотримання конфіденційності. При здійсненні покупки через Інтернет клієнт хоче, щоб його дані, такі як номер картки, були відомі тільки тим, хто має на це законне право.

• Цілісность інформації. Інформація про покупку ніким не може бути змінена.

• Аутентифікація. Продавець і клієнт мають бути впевнені, що учасники транзакції є тими за кого себе видають.

• Засоби оплати. Клієнт повинен мати можливість оплатити покупку будь-якими доступними способами.

Авторизація. За допомогою цього процесу, система може зрозуміти, чи є у клієнта кошти для виконання транзакції.

• Ризик продавця. Торгуючи на просторах Інтернету, продавець може отримати небажані проблеми у вигляді відмови від товару та недобросовістними клієнтами. Величина ризиків повинна бути урегульована з представником платіжної системи та іншими організаціями, які включені в торгові ланцюжки, за допомогою спец. угод.

• Плата за транзакцію. Конкурентноспроможність – найважливіший фактор, тому ціна за обробку транзакцій повинна бути нижча ніж у конкурентів. Ціна за обробку закладена у вартість.

Всі вище вказані умови мають бути реалізовані в платіжній системі Інтернет. Більш детально це буде обговорюватися під час розгляду конкретних методів платежів, які, по суті, є електронними версіями традиційних платіжних систем. Таким чином, всі платіжні системи можна розділити на

• дебетові (працюють з ел. чеками і цифровою готівкою);

• кредитні (кредитні картки).

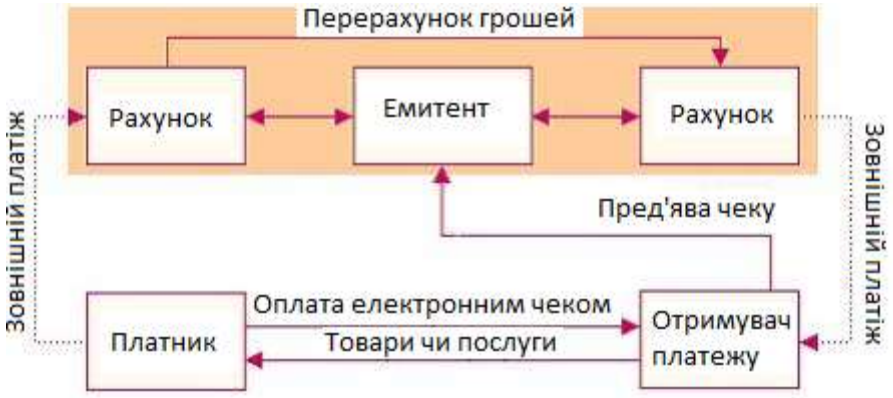

Рис. 1.2 Схема проведення платежу

Дебетові системи.

Побудовані так само як їх оффлайнові прототипи: чекові і звичайні грошові. У схему залучені такі сторони як емітенти і користувачі. Обидві сторони

являються незалежними. Емітент - суб'єкт, керуючий платіжною системою. Він виробляє якісь електронні знаки, що представляють платежі, такі як гроші на банкових рахунках. Користувачі, в свою чергу, мають дві головні функції. Вони виробляють і приймають платежі в Інтернет, використовуючи випущені електронні знаки.

Електронні чеки.

Електронні чеки являються майже тим самим, що і звичайні паперові чеки і є дозволом клієнта для банку, щоб той у свою чергу списав гроші з рахунку. Операція є дійсною при пред'явленні одержувачем чека в банку. Відмінностей від звичайного паперового лише дві. Перша, виписуючи паперовий чек, платник ставить свій справжній підпис (в електронному – електронна), друга чеки випускаються тільки в електронному вигляді.

Проведення платежів проходить в кілька етапів:

1. Клієнт підписує електронний чек електронним підписом і надсилає його продавцю. Задля більшої безпеки, ключ шифрується банком за допомогою відкритого ключа.

2. Електронний чек показується до оплати платіжній системі, здійснюється перевірка ЕЦП.

3. Якщо ЕЦП підтверджено, то товар постачається клієнту а гроші списуються з рахунку.

Нажаль труднощі врвадження в Україні компенсують простоту схеми. Тут чекові схеми поки не набули поширення і немає сертифікаційних центрів.

Кілька слів про сертифікаційних центрах. Електронний підпис використовує схему шифрування за допомогою відкритого ключа, створюється особистий ключ для підпису і відкритий ключ для перевірки. Особистий ключ доступний лише користувачу, а відкритий всім. Найзручнішим способом поширення відкритих ключів - використання сертифікаційних центрів. Щоб користувач не повинен був поширювати свій відкритий ключ, він знаходится у сертифікаційного центру. Крім того, сертифікаційні центри гарантують аутентифікацію, з допомогою якої жоден не зможе згенерувати ключ від імені іншої людини.

Електронні гроші.

В інтернеті можна знайти все, що може знадобитися людині: товари, послуги, спілкування, можливість самовираження, ігри і т.п. Тому потребу в платіжній системі відчули чк продавці так і клієнти.

Завданням будь-якого виду електронних грошей є створення універсального платіжного середовища, що об'єднує клієнтів і продавців товарів і послуг.

Метою електронних коштів є підвищення економічної ефективності інтернету як галузі.

Механізм електронних грошей зроблений таким чином, що дозволяє в області власної квартири робити покупки, укладати угоди, та вести активну комерційну діяльність. Електронні гроші досить схожі на електронні карти, замість піну і карти, у Вас логін та пароль. В будь-який час ви можете перевести гроші в електронного рахунку на банківський, поштовим переказом чи будь-яким іншим способом.

Електронні гроші повністю “імітують” паперові гроші. Також, емітент випускає їх електронні аналоги, які в різних системах називаються по-різному (наприклад, купони). Далі, вони купуються клієнтами, які з їх допомогою виконують транзакції, а потім продавець погашає їх у емітента. При емісії кожна грошова одиниця завіряється електронним друком, яка перевіряється випускаючою структурою перед погашенням.

Одним з величезних плюсів фізичних грошей - їх анонімність, тобто на них не написано, хто і коли їх витрачав. Деякі системи, за аналогією, дозволяють покупцеві отримувати електронну готівку так, щоб не можна було визначити зв'язок між ним і грошима. Це здійснюється за допомогою схеми сліпих підписів.

Варто ще зазначити, що при використанні електронних грошей стає непотрібна аутентифікація, оскільки система працює на випуску грошей в обіг перед їх використанням.

Далі наведена схема платежу із використанням цифрових грошей.

1. Клієнт заздалегідь обмінює паперові гроші на електронні. Зберігання готівки у клієнта може бути здійснено двома способами, що визначається використовуваною системою:

• На хард диску комп'ютера.

• На смарт-картах.

Різні системи використовують безліч схем обміну. Деякі відкривають спец рахунки, на які перераховуються кошти з рахунку клієнта в обмін на електронні знаки. Деякі банки можуть самостійно емітувати електронну готівку. При цьому вона емітується тільки по запиту користувача з наступним її переводом на комп'ютер або картку цього користувача і зняттям грошового еквівалента з його рахунку. При реалізації ж сліпого підпису клієнт сам створює електронні знаки, надсилає їх в банк, де під час введення реальних грошей на рахунок вони завіряються печаткою і надсилаються назад користувачу.

Платіжна система Інтернет - система здійснення розрахунків в процесі купівлі та продажу товарів між безнес організаціями та користувачами Інтернету. Така платіжна система дає можливість перетворити службу по обробці замовлень в повноцінний магазин, що зі сторони клиєнта є незаперечним плюсом, бо покупку можна здійснити не відходячи від комп’ютера.

В даній системі електронної комерції платіж є дійсним лише при дотриманні певних умов:

• Дотримання конфіденційності. При здійсненні покупки через Інтернет клієнт хоче, щоб його дані, такі як номер картки, були відомі тільки тим, хто має на це законне право.

• Цілісность інформації. Інформація про покупку ніким не може бути змінена.

• Аутентифікація. Продавець і клієнт мають бути впевнені, що учасники транзакції є тими за кого себе видають.

• Засоби оплати. Клієнт повинен мати можливість оплатити покупку будь-якими доступними способами.

Авторизація. За допомогою цього процесу, система може зрозуміти, чи є у клієнта кошти для виконання транзакції.

• Ризик продавця. Торгуючи на просторах Інтернету, продавець може отримати небажані проблеми у вигляді відмови від товару та недобросовістними клієнтами. Величина ризиків повинна бути урегульована з представником платіжної системи та іншими організаціями, які включені в торгові ланцюжки, за допомогою спец. угод.

• Плата за транзакцію. Конкурентноспроможність – найважливіший фактор, тому ціна за обробку транзакцій повинна бути нижча ніж у конкурентів. Ціна за обробку закладена у вартість.

Всі вище вказані умови мають бути реалізовані в платіжній системі Інтернет. Більш детально це буде обговорюватися під час розгляду конкретних методів платежів, які, по суті, є електронними версіями традиційних платіжних систем. Таким чином, всі платіжні системи можна розділити на

• дебетові (працюють з ел. чеками і цифровою готівкою);

• кредитні (кредитні картки).

Дебетові системи.

Побудовані так само як їх оффлайнові прототипи: чекові і звичайні грошові. У схему залучені такі сторони як емітенти і користувачі. Обидві сторони являються незалежними. Емітент - суб'єкт, керуючий платіжною системою. Він виробляє якісь електронні знаки, що представляють платежі, такі як гроші на банкових рахунках. Користувачі, в свою чергу, мають дві головні функції. Вони виробляють і приймають платежі в Інтернет, використовуючи випущені електронні знаки.

Електронні чеки.

Електронні чеки являються майже тим самим, що і звичайні паперові чеки і є дозволом клієнта для банку, щоб той у свою чергу списав гроші з рахунку. Операція є дійсною при пред'явленні одержувачем чека в банку. Відмінностей від звичайного паперового лише дві. Перша, виписуючи паперовий чек, платник

ставить свій справжній підпис (в електронному – електронна), друга чеки випускаються тільки в електронному вигляді.

Проведення платежів проходить в кілька етапів:

1. Клієнт підписує електронний чек електронним підписом і надсилає його продавцю. Задля більшої безпеки, ключ шифрується банком за допомогою відкритого ключа.

2. Електронний чек показується до оплати платіжній системі, здійснюється перевірка ЕЦП.

3. Якщо ЕЦП підтверджено, то товар постачається клієнту а гроші списуються з рахунку.

Нажаль труднощі врвадження в Україні компенсують простоту схеми. Тут чекові схеми поки не набули поширення і немає сертифікаційних центрів.

Кілька слів про сертифікаційних центрах. Електронний підпис використовує схему шифрування за допомогою відкритого ключа, створюється особистий ключ для підпису і відкритий ключ для перевірки. Особистий ключ доступний лише користувачу, а відкритий всім. Найзручнішим способом поширення відкритих ключів - використання сертифікаційних центрів. Щоб користувач не повинен був поширювати свій відкритий ключ, він знаходится у сертифікаційного центру. Крім того, сертифікаційні центри гарантують аутентифікацію, з допомогою якої жоден не зможе згенерувати ключ від імені іншої людини.

Електронні гроші.

В інтернеті можна знайти все, що може знадобитися людині: товари, послуги, спілкування, можливість самовираження, ігри і т.п. Тому потребу в платіжній системі відчули чк продавці так і клієнти.

Завданням будь-якого виду електронних грошей є створення універсального платіжного середовища, що об'єднує клієнтів і продавців товарів і послуг.

Метою електронних коштів є підвищення економічної ефективності інтернету як галузі.

Механізм електронних грошей зроблений таким чином, що дозволяє в області власної квартири робити покупки, укладати угоди, та вести активну

комерційну діяльність. Електронні гроші досить схожі на електронні карти, замість піну і карти, у Вас логін та пароль. В будь-який час ви можете перевести гроші в електронного рахунку на банківський, поштовим переказом чи будь-яким іншим способом.

Електронні гроші повністю “імітують” паперові гроші. Також, емітент випускає їх електронні аналоги, які в різних системах називаються по-різному (наприклад, купони). Далі, вони купуються клієнтами, які з їх допомогою виконують транзакції, а потім продавець погашає їх у емітента. При емісії кожна грошова одиниця завіряється електронним друком, яка перевіряється випускаючою структурою перед погашенням.

Одним з величезних плюсів фізичних грошей - їх анонімність, тобто на них не написано, хто і коли їх витрачав. Деякі системи, за аналогією, дозволяють покупцеві отримувати електронну готівку так, щоб не можна було визначити зв'язок між ним і грошима. Це здійснюється за допомогою схеми сліпих підписів.

Варто ще зазначити, що при використанні електронних грошей стає непотрібна аутентифікація, оскільки система працює на випуску грошей в обіг перед їх використанням.

Далі наведена схема платежу із використанням цифрових грошей.

1. Клієнт заздалегідь обмінює паперові гроші на електронні. Зберігання готівки у клієнта може бути здійснено двома способами, що визначається використовуваною системою:

• На хард диску комп'ютера.

• На смарт-картах.

Різні системи використовують безліч схем обміну. Деякі відкривають спец рахунки, на які перераховуються кошти з рахунку клієнта в обмін на електронні знаки. Деякі банки можуть самостійно емітувати електронну готівку. При цьому вона емітується тільки по запиту користувача з наступним її переводом на комп'ютер або картку цього користувача і зняттям грошового еквівалента з його рахунку. При реалізації ж сліпого підпису клієнт сам створює електронні знаки,

надсилає їх в банк, де під час введення реальних грошей на рахунок вони завіряються печаткою і надсилаються назад користувачу.

При розрахунках через Інтернет і отриманні готівки через фальшиві банкомати можлива електронна крадіжка грошей з рахунку. Тому слід бути вкрай обережним. Для цього потрібно не використовувати сумнівні платіжні шлюзи, особливо на порнографічних сайтах. У деяких країнах існують фальшиві банкомати, зчитувальні магнітні смуги і коди, після чого гроші йдуть до шахраїв.

Такі банкомати можуть навіть видати готівку. Тому в таких країнах рекомендується користуватися банкоматами при банках і великих торгових центрах. Також не рекомендується говорити номер своєї карти і код CVV2 / CVC2 на зворотному боці (в зв'язку з тим, що цих реквізитів зазвичай досить для здійснення платежів в Інтернет). Замурований в стіну банкомат або банкомат, що знаходиться в будівлі банку - більш надійний спосіб зняття грошей з рахунку.

• При отриманні грошей через банкомат і багатьох терміналах потрібно ввести PIN-код, який зазвичай складається з чотирьох цифр. Рекомендується його запам'ятати і ні в якому разі не зберігати його разом з картою. У незаконного володаря чужої карти є не менше десяти тисяч варіантів, однак після третього неправильного вводу PIN-коду карта зазвичай блокується на добу, а деякі банки-емітенти в таких випадках можуть навіть дати банкомату команду на захоплення карти. Якщо карта VISA, то в цьому випадку карту зазвичай пересилають в банк-емітент, так як банк-еквайєр в цьому випадку отримує винагороду. Якщо це MasterCard, то карта нікуди не пересилається, так як винагороди не передбачено, і зазвичай такі захоплені карти сторонніх банків через деякий час знищуються, якщо не надійде жодної інформації з банку-емітента. Якщо ж зберігати код разом з картою, то зловмиснику не складе ніяких труднощів отримати гроші в будь-якому банкоматі.

• Щоб здійснити оплату в торгових точках код найчастіше вводити не потрібно, однак на зворотному боці картки стоїть підпис власника. При покупці випускається два чека. На одному покупець розписується і залишає продавцю.

Підписи на карті і чеку повинні збігатися. Для безпеки не можна дозволяти продавцеві проводити дії, в результаті яких карта зникає з поля зору її власника.

• При обміні карти в зв'язку із закінченням терміну дії необхідно стежити, щоб здана карта була розрізана банківським працівником як мінімум навпіл. Нову карту необхідно якомога швидше активувати, тобто зробити з неї будь-яку операцію, наприклад, запросити в банкоматі баланс рахунку. При отриманні конверта з PIN-кодом необхідно простежити, щоб він був запечатаний.

1.3 Інфраструктура безпеки електронної комерції

За визначенням CNP-транзакція (Cardholder Not Present) являє собою операцію покупки по пластиковій картці, в момент скоєння якої клієнт не присутній особисто в торговій точці, а повідомляє торговій точці реквізити своєї картки (зазвичай номер карти і її термін придатності), необхідні для проведення авторизації, заочно (листом, по телефону, мережі передачі даних і т. п.).

Зазвичай процес покупки виглядає наступним чином. Клієнт за допомогою персонального комп'ютера (або іншого пристрою), підключеного до мережі Інтернет, вибирає потрібні йому товари в віртуальній вітрині товарів сайту торгової точки. Підтвердивши вибір товарів і згоду з їх вартістю, клієнт повідомляє торговій точці про бажання заплатити за покупку за допомогою пластикової карти.

Далі відбувається діалог між торговою точкою і власником карти, метою якого є отримання реквізитів картки покупця для їх подання в мережу у вигляді стандартного авторизационного запиту. Протягом цього діалогу торгова точка і покупець іноді мають можливість аутентифицировать один одного, що забезпечує безпеку транзакції.

Отримані від клієнта дані про реквізити карти (до речі, торгова точка може і «не бачити» ці дані) торгова точка передає своєму обслуговуючому банку, який на основі цих даних формує і представляє в мережу авторизаційний запит. Починаючи з цього моменту, транзакція обробляється за тими ж правилами, що і

звичайна операція купівлі пластиковою карткою. Авторизаційний запит обслуговуючого банку у вигляді повідомлення в форматі, прийнятому у відповідній платіжній системі, передається банку-емітенту клієнта, який авторизує транзакцію і про результат авторизації повідомляє обслуговуючому банку. Обслуговуючий банк передає торговій точці рішення емітента, яке повідомляється власнику карти. У разі успішного завершення транзакції клієнт отримує електронний чек, що містить адресу торгової точки в Інтернеті, її назва, суму покупки і т. П.

Способи вирішення проблеми безпеки транзакцій в електронній комерції

З першого дня введення електронної комерції стало ясно, що методи ідентифікації власника карти, що застосовуються в звичайних транзакціях, є недостатніми для транзакцій електронного типу.

Дійсно, при здійсненні операції купівлі у фізичному магазині продавець має право розглянути пропоновану для розрахунку пластикову карту на предмет її відповідності вимогам платіжним системам (зокрема перевірити наявність голограми, спеціальних секретних символів, звірити підписи на панелі і торговому чеку і т. П.). Крім того, продавець може зажадати від покупця документ, що засвідчує його особу. Все це робить шахрайство з підробленою карткою досить дорогим підприємством.

У разі транзакції в електронній комерції все, що потрібно від шахрая - знання реквізитів картки. Витрати, пов'язані з виготовленням підробленої фізичної карти, в цьому випадку не потрібно.

У світі пластикових карт із магнітною смугою найнадійнішим способом захисту транзакції від шахрайства є використання PIN-коду для ідентифікації власника картки його банком-емітентом. Секретною інформацією, якою володіє власник карти, є PIN-код. Він являє собою послідовність, що складається з 4-12 цифр, відому тільки власнику картки і його банку-емітенту. PIN-код застосовується завжди при проведенні транзакції підвищеного ризику, наприклад при видачі власнику карти готівки в банкоматах. Видача готівки в банкоматах відбувається без присутності представника обслуговуючого банку (ситуація

схожа на транзакцію електронної комерції). Тому звичайних реквізитів картки для захисту операції «зняття готівки в банкоматі» недостатньо і використовується секретна додаткова інформація - PIN-код.

Більш того, загальна тенденція розвитку платіжних систем - більш активне використання PIN-коду для операцій «покупки» по дебетових картках. Здавалося б, використання подібного ідентифікатора могло б допомогти вирішити проблему безпеки, однак це не так. На жаль, в додатку до електронної комерції цей метод в класичному вигляді непридатний.

Використання PIN-коду має проводитися таким чином, щоб цей секретний параметр на всіх етапах обробки транзакцій залишався зашифрованим (він повинен бути відомий тільки власнику картки і банку-емітенту). У реальному світі це вимога реалізується за рахунок використання в пристроях введення транзакції спеціальних фізичних пристроїв, званих PIN-PAD і містять Hardware Security Module - апаратно-програмні пристрої захисту, що дозволяють зберігати і перетворювати інформацію, що надходить надійним чином. Ці пристрої зберігають спеціальним чином захищений секретний комунікаційний ключ, згенерований обслуговуючим банком даної торгової точки. Коли власник карти вводить значення PIN-коду, воно негайно шифрується комунікаційним ключем і відправляється всередині авторизационного запиту на хост обслуговуючого банку. На хості обслуговуючого банку зашифрований ідентифікаційний код перекодируется всередині Hardware Security Module хоста (хост обслуговуючого банку також має свій пристрій шифрування) в блок, зашифрований на комунікаційному ключі платіжної системи, і передається в мережу для подальшого пред'явлення емітенту. По дорозі до емітента PIN-код буде перетворюватися ще кілька разів, але це не важливо. Важливо інше - для того, щоб слідувати класичною схемою обробки PIN-коду, кожен власник картки повинен зберігати криптограми комунікаційних ключів всіх обслуговуючих банків, що на практиці неможливо.

Класичну схему можна було б реалізувати за допомогою застосування асиметричних алгоритмів шифрування даних PIN-коду власника карти відкритим

ключем торгової точки. Однак для подання PIN-коду в платіжну мережу його необхідно зашифрувати, як це прийнято у всіх платіжних системах, симетричним ключем.

Існує інше, некласична рішення по використанню PIN-коду. Наприклад, можна на комп'ютері власника карти шифрувати PIN-код плюс деякі динамічно мінливі від транзакції до транзакції дані на ключі, відомому тільки емітенту і власнику карти. Такий підхід вимагає рішення задачі розподілу секретних ключів. Це завдання є досить непростим (очевидно, що у кожного власника карти повинен бути свій індивідуальний ключ), і якщо вже вона вирішується, то використовувати її рішення має сенс для інших, більш ефективних у порівнянні з перевіркою PIN-коду методів аутентифікації власника карти.

У той же час ідея перевірки PIN-коду була реалізована для підвищення безпеки транзакцій в електронній комерції по картах, бази даних яких зберігаються на хості процесора STB CARD. У загальних рисах STB CARD реалізує наступну схему. Власники карт, емітенти яких тримають свою базу даних карток на хості STB CARD, можуть отримати додатковий PIN-код, званий PIN2. Цей код є послідовністю з 16 шістнадцяткових цифр, яка роздруковується в PIN-конверті, переданому власнику карти, і обчислюється емітентом за допомогою симетричного алгоритму шифрування, застосованого до номера карти і використовує секретний ключ, відомий тільки емітенту карти.

Далі під час проведення транзакції на одній з торгових точок, що обслуговується банком STB CARD, у власника карти в процесі отримання даних про клієнта запитується інформація по PIN2. Клієнт вводить це значення в яку заповнюють форму і повертає її торговій точці.

Тут слід зауважити, що власник карти в дійсності веде діалог в захищеній SSL-сесії не з торговою точкою, а з віртуальний POS-сервером, через який працює торгова точка.

Повертаючись до схеми STB CARD, відзначимо, що, звичайно ж, в заповненій клієнтом формі PIN2 не міститься, а в дійсності все виглядає наступним чином: торгова точка (точніше, сервер Assist), визначивши, що має

справу з картою банку STB CARD, передає власнику карти форму, яка містить підписаний java-аплет, який реалізує деякий симетричний алгоритм шифрування. При цьому PIN2 грає роль секретного ключа цього алгоритму шифрування, а шіфруемие дані виходять в результаті застосування хеш-функції до номера карти, суму та дату транзакції, а також випадковим числу Nn генерируемому торговою точкою. Таким чином, в заповненій власником карти формі присутній тільки результат шифрування перерахованих вище даних про транзакції на ключі PIN2.

Далі торгова точка формує авторизаційної повідомлення, передане на хост обслуговуючого банку, що містить крім "стандартних" даних транзакції ще результат шифрування і випадкове число Nn.

Емітент карти, отримавши повідомлення торгової точки, за номером картки обчислює значення PIN2, і далі за номером картки, суму та дату транзакції, а також за випадковим числу Nn, обчислює результат шифрування цих даних на ключі PIN2. Якщо отримана величина збігається з аналогічною величиною отриманої з повідомлення торгової точки, верифікації PIN-коди вважається виконаним успішно. В іншому випадку транзакція відкидається.

Таким чином, технологія перевірки PIN-коду, прийнята в системі STB CARD, в дійсності забезпечує не тільки динамічну аутентифікацію клієнта, але ще і гарантує «наскрізну» цілісність деяких даних про транзакції (сума транзакції, номер картки). Під «наскрізний» цілісністю тут розуміється захист від модифікації даних на всьому протязі від їх передачі від клієнта до банку-емітента.

Мінуси даного підходу полягають у наступному:

- для реалізації схеми перевірки значення PIN-коду необхідно, щоб торгова точка вміла формувати відповідну форму з java-апплетом, що відразу звужує сферу застосування схеми у відносно невеликому безлічі торгових точок;

- використання довгого (16 hex цифр) ключа робить його застосування на практиці вкрай незручним для власника карти;

- захист від підставки (форма, яка запитує PIN2, надається клієнтові не торговою точкою, а шахраєм, з цілю дізнатися PIN2) заснована на надійності аутентифікації клієнтом сервера торгової точки, а також на підписуванні аплету

секретним ключем сервера торгової точки. Оскільки порушення обох захистів призводить тільки до появи на екрані монітора власника карти відповідного попередження, супроводжуваного питанням продовжити сесію чи ні, то особливо довіряти цим формам захисту не варто;

- використання хеш-функції в алгоритмах шифрування, як відомо дана функція оборотна;

В результаті проведеного аналізу платіжні системи сформували основні вимоги до схем проведення транзакції в електронній комерції, що забезпечує необхідний рівень її безпеки.

Ці вимоги зводяться до наступного:

- Аутентифікація учасників покупки (покупця, торгової точки і її обслуговуючого банку). Під аутентифікацією покупця (продавця) розуміється процедура, яка доводить (на рівні надійності відомих криптоалгоритмів) факт того, що даний власник карти дійсно є клієнтом деякого емітента-учасника (обслуговуючого банку-учасника) даної платіжної системи. Аутентифікація обслуговуючого банку доводить факт того, що банк є учасником цієї платіжної системи.

- Реквізити платіжної картки (номер картки, термін її дії, CVC2 / CVV2 і т. П.), Що використовується при проведенні транзакції, повинні бути конфіденційними для торгової точки.

- Неможливість відмови від транзакції для всіх учасників транзакції, тобто наявність у всіх учасників незаперечного доказу факту здійснення покупки (замовлення або оплати).

- Гарантування магазину платежу за електронну покупку - наявність у торговельній точки докази того, що замовлення було виконано.

SSL (англ. Secure Sockets Layer - рівень захищених сокетів) - криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером. SSL спочатку розроблений компанією Netscape Communications. Згодом на підставі протоколу SSL 3.0 був розроблений і прийнятий стандарт RFC, що отримав ім'я TLS.

Протокол забезпечує конфіденційність обміну даними між клієнтом і сервером, що використовують TCP / IP, причому для шифрування використовується асиметричний алгоритм з відкритим ключем. При шифруванні з відкритим ключем використовуються два ключа, причому будь-який з них може використовуватися для шифрування повідомлення. Тим самим, якщо використовується один ключ для шифрування, то відповідно для розшифровки потрібно використовувати інший ключ. У такій ситуації можна отримувати захищені повідомлення, публікуючи відкритий ключ, і зберігаючи в таємниці секретний ключ.

Протокол SSL складається з двох подпротоколов: протокол SSL записи і рукостискання. Протокол SSL записи визначає формат, використовуваний для передачі даних. Протокол SSL включає рукостискання з використанням протоколу SSL записи для обміну серіями повідомлень між сервером і клієнтом під час встановлення першого з'єднання. Для роботи SSL потрібно, щоб на сервері був SSL-сертифікат.

SSL надає канал, який має 3 основних властивості:

• Аутентифікація. Сервер завжди аутентифицирующей, в той час як клієнт аутентифицирующей в залежності від алгоритму.

• Цілісність. Обмін повідомленнями включає в себе перевірку цілісності.

• Приватність каналу. Шифрування використовується після встановлення з'єднання і використовується для всіх наступних повідомлень.

Сертифікат X.509 - стандарт, що визначає формати даних і процедури розподілу відкритих ключів за допомогою сертифікатів з цифровими підписами, які надаються сертифікаційними органами (CA).

Для технології відкритих ключів необхідно, щоб користувач відкритого ключа був впевнений, що цей ключ належить саме тому віддаленого суб'єкту (користувачеві або системі), який буде використовувати засоби шифрування або цифрового підпису. Таку впевненість дають сертифікати відкритих ключів, тобто структури даних, які пов'язують величини відкритих ключів з суб'єктами. Цей зв'язок досягається цифровим підписом довіреної CA під кожним сертифікатом.

Сертифікат має обмежений термін дії, зазначений в його підписаному змісті. Оскільки користувач сертифіката може самостійно перевірити його підпису і терміну дійсності, сертифікати можуть поширюватися через незахищені канали зв'язку і серверні системи, а також зберігатися в кеш-пам'яті незахищених призначених для користувача систем. Зміст сертифіката має бути однаковим в межах всього PKI. В даний час в цій області пропонується загальний стандарт для Інтернет з використанням формату X.509 v3:

- Номер версії
- Серійний номер
- Емітент
- Суб'єкт
- Відкритий ключ суб'єкта (алгоритм, ключ)
- Період дії
- Додаткові (необов'язкові) значення
- Алгоритм підпису сертифіката
- Значення підпису сертифіката

X509-сертифікати зберігаються як правило у вигляді DER (стандартне розширення .cer) або PEM-файлів.

Список відкликання сертифікатів (CRL)

CRL є список відкликаних сертифікатів із зазначенням часу. Він підписується CA і вільно поширюється через загальнодоступний репозиторій. У списку CRL кожен відкликаний сертифікат розпізнається за своїм серійним номером. Коли у якийсь системи виникає необхідність у використанні сертифіката (наприклад, для перевірки цифрового підпису віддаленого користувача), ця система не тільки перевіряє підпис сертифіката і термін його дії, а й переглядає останній з доступних списків CRL, перевіряючи, чи не відкликаний цей сертифікат .

Висновки: Досліджено основи електронної комерції та традиційної електронної комерції. Визначено основні поняття безпеки платіжних систем, та інфраструктури безпеки електронної комерції.

2 БЕЗПЕКА ЕЛЕКТРОННИХ ТРАНЗАКЦІЙ В СИСТЕМАХ B2C І C2C

2.1 Безпека заочних карткових транзакцій

На сьогоднішній день існує три загрози безпеки карткових транзакцій. Перша - підробка карт, друга - крадіжка або втрата карти, і третя - випадки шахрайства при проведенні транзакції, яку здійснюють без пред'явлення платіжної картки. При цьому перші дві причини займають сьогодні в світі 73% всіх випадків карткового шахрайства, тому багато банків ставлять першочерговим завданням боротьбу саме з цими категоріями шахрайства.

Як приклад розглянемо проблему підробки мікропроцесорної карти (Counterfeit).

На сьогоднішній день ринок EMV-карт переважно складається з карт, які використовують статичну аутентифікацію карти (Static Data Au-thentication, або SDA).

На відміну від карт з динамічної аутентифікації (DDA-карт) їх позначають як SDA-карти. На SDA-картці зберігаються підписані емітентом дані, цілісність яких, з його точки зору, є критичною (наприклад, номер картки, порядковий номер власника карти, дата закінчення терміну дії, профіль використання карти і т. П.).

Всі ці дані, включаючи підпис емітента, зберігаються на карті у відкритому вигляді. Сенс статичної аутентифікації полягає в тому, щоб зробити неможливою модифікацію підписуються даних (для чого необхідно знати спеціальний ключ,

який використовується при персоналізації карти і відомий тільки емітенту) і мати захист від персоналізації чипа без авторизації емітента.

Очевидно, що, незважаючи на ці заходи, SDA-карту порівняно легко підробити. Маючи на руках подібний продукт, його фальсифікація обійдеться шахраєві в суму, рівну приблизно 30 дол. При цьому знову виготовлена карта при офлайнових транзакціях успішно пройде процедуру статичної аутентифікації і, більш того, навіть підтвердить правильність будь-якого введеного злочинцем PIN-коду.

Таким чином, можна стверджувати, що застосування мікропроцесорних SDA-карт не вирішує повністю проблему підроблених, а також украдених / втрачених карт. А адже на базі саме цих карт сьогодні емітується не менше 99% EMV-продуктів!

Справа в тому, що перехід на DDA-карти, що забезпечують дійсно високий рівень безпеки, сьогодні досить дорогий. Вартість таких карт приблизно в 2 рази перевищує номінальну вартість SDA-карт і становить близько 2 дол., Що пояснюється необхідністю наявності додаткового криптографічного процесора і 4 Кбайт пам'яті EEPROM.

Крім того, міграція на DDA-карти зажадає від банку і істотних змін в своєму картковому бек-офісі. Зокрема, йому доведеться міняти ПО на машині персоналізації. Останнє обумовлено не тільки зміною даних, що записуються на карту, але і тим, що при переході на карту іншого виробника доведеться міняти набір адміністративних команд, використовуваних для її персоналізації.

В якості пояснення тут слід зазначити, що стандарт EMV НЕ формалізує адміністративні команди, в результаті чого різні виробники карт використовують свої набори таких команд.

Крім того, сьогодні в Росії значна частка емісії доводиться на зарплатні проекти, для яких подібне подорожчання продукту є неприпустимим.

Нарешті, важливо відзначити, що на російському картковому ринку обсяг шахрайства, з точки зору емісії, сьогодні поки що не такий вже й великий - переважна кількість випадків фрода доводиться на еквайринг.

Очевидно, що при такому положенні справ фінансові втрати до останнього часу несли в основному зарубіжні банки. Правда, при зміні відповідальності (EMV liability shift), наміченої міжнародними платіжними системами на 2005 рік, відповідальність за весь цей фрод може перейти на російських еквайєрів.

Тому з цієї точки зору еквайринг мікропроцесорних карт обіцяє нашим банкам набагато більше потенційних стимулів для якнайшвидшої міграції на чіп, ніж емісія EMV-продуктів.

Загальні правила безпеки:

1. Не можна зберігати PIN-код разом з картою. «Ми спеціально видаємо пам'ятки по правильній поведінці власника картки. За останній час ми зіткнулися з ситуаціями, коли у наших клієнтів, які втратили карти, ПІН-код був записаний на самій карті! »- каже Володимир Онуфрієв (« Газпромбанк ») на засіданні круглого столу« Банківські пластикові карти ». До речі, у багатьох випадках це правило поширюється і на номери банківських карт. Візьмемо для прикладу будь-яку міжнародну платіжну систему. Знаючи тільки номер карти і термін закінчення її дії, можна оплачувати покупки в інтернет-магазинах або замовляти будь-які послуги через Глобальну мережу. Таким чином, листок з номером картки (який ми записали для негайних дій в екстрених випадках) краще не носити з собою, а зберігати в надійному місці.

2. Ніколи і нікому не повідомляйте свій PIN-код. Його не має права вимагати у вас ніхто - ні працівники банку, що видав картку, ні обслуговуючий персонал банкомата, ні співробітники магазина. Приклад, зловмисник дізнається телефонний номер і повні прізвище, ім'я та по батькові жертви, а також назва банку-емітента, що випустив його карту. Потім він дзвонить йому і представляється співробітником цієї організації. Знання імені та по батькові людини, а також згадка його банку зазвичай притупляє обережність жертви. Ну а далі шахрай просить співрозмовника негайно повідомити йому номер його карти і PIN-код для доступу до неї. При цьому звучать такі причини, як "комп'ютерний збій банківської системи і необхідність відновлення бази даних", "перемога в лотереї, проведеної нашим банком", і т.п. Деякі йдуть ще далі. Вони

представляються співробітниками служб безпеки і стверджують, що картою людини скористався зловмисник, якого тільки що спіймали. І щоб відшкодувати збитки, понесені власником, необхідний PIN-код. Про те, що відбувається після того, як людина повідомить шахраям секретні дані про свою карту, напевно, розповідати не варто.

Тому досить запам'ятати одну річ. Ніхто і ні за яких обставин не може вимагати від вас номер карти або PIN-код для доступу до неї. Це правило поширюється абсолютно на всіх: на працівників банку, на співробітників правоохоронних органів, на обслуговуючий персонал банкоматів і т. Д. Деякі джерела стверджують, що власник картки може повідомити PIN-код міліціонерам або працівникам прокуратури за рішенням суду. Однак насправді це не так. Співробітники правоохоронних органів, маючи на руках постанову суду, звернуться прямо в банк, звідки зможуть простежити всі операції з даною карткою, а також заблокувати потрібний рахунок.

3. Ніколи не передавайте карту іншої людини. По-перше, під час затримання карти банкоматом він не зможе її отримати назад. Адже навіть в магазині касир може попросити підтвердити особу власника документами або підписом. По-друге, не можна гарантувати, чи буде той, кому ви довірили свою картку, поводитися з нею так само обачно, як і ви. Якщо вам необхідно, наприклад, віддати її родичам, то можете зробити додаткову карту, встановивши на неї ліміт зняття грошей.

4. Залиште свій зразок підпису прямо на карті. Правда, робити це варто тільки в тому випадку, якщо це передбачено договором. Далеко не всі карти припускають нанесення на них підписи власника. Зазвичай це вірно тільки відносно карт міжнародних платіжних систем. Це необхідно для захисту ваших грошей. Припустимо, що карта була вкрадена і зловмисник прийшов з нею в магазин за покупками. Побачивши підпис на карті, касир може вимагати від шахрая розпис, щоб переконатися в його праві розпоряджатися грошима. Правда, у нас це роблять рідко.

Винятком є організації, каси яких не обладнані POS-терміналами. У цьому випадку покупець повинен розписатися на сліпах (чеках), а касир зобов'язаний порівняти цю підпис зі зразком на карті.

5. При втраті картки негайно повідомте про це по телефону. Якщо ви втратили пластикову карту, негайно телефонуйте в банк, який її видав.

6. Періодично перевіряйте історію операцій на вашому картковому рахунку не рідше, ніж раз на місяць. Особливу увагу слід звернути на операції з рахунком після поїздок, в яких ви користувалися своєю карткою. Найкраще підключити сервіс інформування про транзакції по картці через SMS.

2.2 Протокол безпечних електронних транзакцій SET

SET (Security Electronics Transaction). SET заснований на використанні цифрових сертифікатів за стандартом X.509. Протокол виконання захищених транзакцій SET є стандартом, розробленим компаніями MasterCard і VISA при значній участі IBM, GlobeSet та інших партнерів. Він дозволяє покупцям купувати товари через Інтернет, використовуючи найзахищеніший на даний час механізм виконання платежів. SET є відкритим стандартним багатостороннім протоколом для проведення безпечних платежів з використанням пластикових карток в Інтернет. SET забезпечує крос-аутентифікацію рахунку власника картки, продавця і банку продавця для перевірки готовності оплати товару, цілісність і секретність повідомлення, шифрування цінних та вразливих даних. Тому SET можна назвати стандартною технологією або системою протоколів виконання безпечних платежів з використанням пластикових карток через Інтернет.

SET дозволяє споживачам і продавцям підтвердити справжність всіх учасників угоди, яка відбувається в Інтернет, за допомогою криптографії, застосовуючи, в тому числі, і цифрові сертифікати.

Обсяг потенційних продажів в галузі електронної комерції обмежується досягненням необхідного рівня безпеки інформації, який забезпечують разом покупці, продавці і фінансові інститути, стурбовані питаннями забезпечення

безпеки платежів через Інтернет. Як згадувалося раніше, базовими завданнями захисту інформації є забезпечення її доступності, конфіденційності, цілісності та юридичної значимості. SET, на відміну від інших протоколів, дозволяє вирішувати зазначені завдання захисту інформації.

В результаті того, що багато компаній займаються розробкою власного програмного забезпечення для електронної комерції, виникає ще одна проблема. У разі використання цього ПО всі учасники операції повинні мати одні й ті ж додатка, що практично нездійсненно. Отже, необхідний спосіб забезпечення механізму взаємодії між додатками різних розробників.

У зв'язку з перерахованими вище проблемами компанії VISA і MasterCard разом з іншими компаніями, що займаються технічними питаннями (наприклад IBM, яка є ключовим розробником в розвитку протоколу SET), визначили специфікацію і набір протоколів стандарту SET. Ця відкрита специфікація дуже швидко стала де-факто стандартом для електронної комерції. У цій специфікації шифрування інформації забезпечує її конфіденційність. Цифровий підпис і сертифікати забезпечують ідентифікацію та аутентифікацію (перевірку справжності) учасників транзакцій. Цифровий підпис також використовується для забезпечення цілісності даних. Відкритий набір протоколів використовується для забезпечення взаємодії між реалізаціями різних виробників.

SET забезпечує наступні спеціальні вимоги захисту операцій електронної комерції:

• таємність даних оплати і конфіденційність інформації замовлення, переданої разом з даними про оплату;

• збереження цілісності даних платежів; цілісність забезпечується за допомогою цифрового підпису;

• спеціальну криптографію з відкритим ключем для проведення аутентифікації;

• аутентифікацію по кредитній картці, яка забезпечується застосуванням цифрового підпису та сертифікатів власника карток;

• аутентифікацію продавця і його можливості приймати платежі за пластиковими картками із застосуванням цифрового підпису та сертифікатів продавця;

• підтвердження того, що банк продавця є діючою організацією, яка може приймати платежі за пластиковими картками через зв'язок з процесінговою системою; це підтвердження забезпечується за допомогою цифрового підпису та сертифікатів банку продавця;

• готовність оплати транзакцій в результаті аутентифікації сертифіката з відкритим ключем для всіх сторін;

• безпеку передачі даних за допомогою переважного використання криптографії.

Основна перевага SET перед багатьма існуючими системами забезпечення інформаційної безпеки полягає в використанні цифрових сертифікатів (стандарт X.509, версія 3), які асоціюють держателя картки, продавця і банк продавця з низкою банківських установ платіжних систем VISA і MasterCard.

SET дозволяє зберегти існуючі відносини між банком, власниками карток та продавцями, та інтегрується з існуючими системами, спираючись на такі якості:

• відкритий, повністю документований стандарт для фінансової індустрії;

• заснований на міжнародних стандартах платіжних систем;

• спирається на існуючі в фінансовій галузі технології та правові механізми.

До речі, спільний проект, реалізований компаніями IBM, Chase Manhattan Bank USA NA, First Data Corporation, GlobeSet, MasterCard і Wal-Mart дозволяє власникам карток Wal-Mart MasterCard, випущених банком Chase, купувати товари на сайті Wal-Mart Online, який є одним з найбільших вузлів електронної комерції США.

Розглянемо більш детально процес взаємодії учасників платіжної операції відповідно до специфікації SET, представлений на малюнку з сайту компанії IBM:

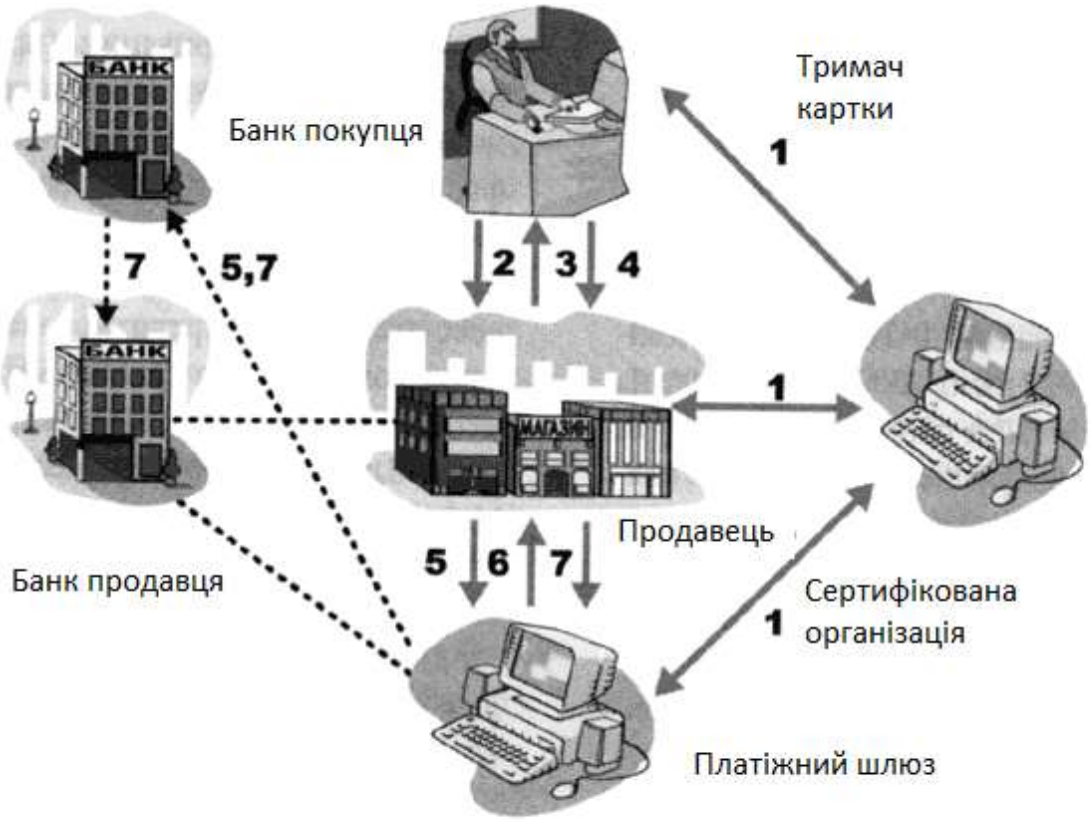

Рис. 2.1 Схема процесу взаємодії учасників платіжної операції відповідно до специфікації SET

На малюнку:

• Власник картки - покупець робить замовлення.

• Банк покупця - фінансова структура, яка випустила кредитну картку для покупця.

• Продавець - електронний магазин, що пропонує товари і послуги.

• Банк продавця - фінансова структура, що займається обслуговуванням операцій продавця.

• Платіжний шлюз - система, контрольована зазвичай банком продавця, яка обробляє запити від продавця і взаємодіє з банком покупця.

• сертифікує організація - довірча структура, яка видає і перевіряє сертифікати.

Взаємовідносини учасників операції показані на малюнку безперервними лініями (взаємодії описані стандартом або протоколом SET) і пунктирними лініями (деякі можливі операції).

Динаміка взаємовідносин та інформаційних потоків відповідно до специфікації стандарту SET включає наступні дії:

1. Учасники запитують і отримують сертифікати від сертифікує організації.

2. Власник пластикової картки переглядає електронний каталог, вибирає товари та посилає замовлення продавцю.

3. Продавець пред'являє свій сертифікат власнику картки в якості посвідчення.

4. Власник картки пред'являє свій сертифікат продавцю.

5. Продавець запитує у платіжного шлюзу виконання операції перевірки. Шлюз звіряє надану інформацію з інформацією банку, що випустив електронну картку.

6. Після перевірки платіжний шлюз повертає результати продавцю.

7. Через деякий час, продавець вимагає у платіжного шлюзу виконати одну або більше фінансових операцій. Шлюз надсилає запит на переказ визначеної суми з банку покупця в банк продавця.

Представлена схема взаємодії підкріплюється в частині інформаційної безпеки специфікацією Chip Electronic Commerce, створеної для використання смарт-карток стандарту EMV в Інтернеті (www.emvco.com). Її розробили Europay, MasterCard і VISA. Поєднання стандарту на мікропроцесор EMV і протоколу SET дає безпрецедентний рівень безпеки на всіх етапах транзакції.

Компанія "Росбизнесконсалтинг» 20 june 2000 р помістила на своєму сайті повідомлення про те, що одна з найбільших світових платіжних систем VISA оприлюднила 19 червня 2000 року свої ініціативи в галузі безпеки електронної комерції. За словами представників системи, ці кроки покликані зробити покупки в Інтернеті безпечніше для покупців і продавців. VISA вважає, що впровадження нових ініціатив дозволить скоротити кількість суперечок щодо транзакцій в Інтернеті на 50%. Ініціатива складається з двох основних частин. Перша частина -

це Програма аутентифікації платежів (Payment Authentication Program), яка розроблена для зниження ризику неавторизованого використання рахунку власника картки і поліпшення сервісу для покупців і продавців в Інтернеті. Друга - це Глобальна програма захисту даних (Global Data Security Program), мета якої - створити стандарти безпеки для підприємств електронної комерції із захисту даних про картки та їх власниках.

Учасники системи розрахунків і криптографічні засоби захисту транзакцій.

Протокол SET змінює спосіб взаємодії учасників системи розрахунків. В даному випадку електронна транзакція починається з власника картки, а не з комерсанта або еквайра.

Комерсант пропонує товар для продажу або надає послуги за плату. Протокол SET дозволяє комерсанту пропонувати електронні взаємодії, які можуть безпечно використовувати власники карток. Еквайєром (одержувачем) є фінансова установа, яка відкриває рахунок комерсанту і обробляє авторизації і платежі по кредитних картках. Еквайєр обробляє повідомлення про платежі, переведених комерсанту за допомогою платіжного міжмережевого інтерфейсу. При цьому протокол SET гарантує, що при взаємодіях, які здійснює власник картки з комерсантом, інформація про рахунок кредитної картки буде залишатися конфіденційною. Фінансові установи створюють асоціації банківських кредитних карток, які захищають і рекламують даний тип картки, створюють і вводять в дію правила використання кредитних карток, а також організують мережі для зв'язку фінансових установ один з одним. Системи кредитних карт утвердилися в значній мірі як платіжний засіб для придбання товарів безпосередньо у продавця. Основна відмінність використання кредитних карт в мережі Internet полягає в тому, що відповідно до стандарту SET для захисту транзакцій електронної торгівлі використовуються процедури шифрування і цифрового підпису. Мережа Internet розрахована на одночасну роботу мільйонів користувачів, тому в комерційних Internet-додатках неможливо використовувати тільки симетричні криптосистеми з секретними ключами (DES, ГОСТ28147-89). У зв'язку з цим застосовуються також асиметричні криптосистеми з відкритими ключами. Шифрування з

використанням відкритих ключів передбачає, що у комерсанта і покупця є по два ключа-один відкритий, який може бути відомий третім особам, а інший-приватний (секретний), відомий тільки одержувачу інформації. Правила SET передбачають початкове шифрування повідомлення з використанням випадковим чином згенерованого симетричного ключа, який, в свою чергу, шифрується відкритим ключем одержувача повідомлення. В результаті утворюється так званий електронний конверт. Одержувач повідомлення розшифровує електронний конверт за допомогою свого приватного (секретного) ключа, щоб отримати симетричний ключ відправника. Далі симетричний ключ відправника використовується для розшифрування надісланого повідомлення.

Цілісність інформації та аутентифікації учасників транзакції гарантується використанням електронного цифрового підпису. Для захисту угод від шахрайства та зловживань організовані спеціальні центри (агентства) сертифікації в Internet, які стежать за тим, щоб кожен учасник електронної комерції отримував би унікальний електронний сертифікат. У цьому сертифікаті за допомогою секретного ключа сертифікації зашифрований відкритий ключ даного учасника комерційної угоди. Сертифікат генерується на певний час, і для його отримання необхідно представити в центр сертифікації документ, що підтверджує особу учасника (для юридичних осіб-их легальну реєстрацію), і потім, маючи "на руках" відкритий ключ центру сертифікації, брати участь в угодах.

Розглянемо приклад шифрування. Комерсант Аліса хоче направити зашифроване повідомлення про товар покупцеві Бобу у відповідь на його запит. Аліса пропускає опис товару через односпрямований алгоритм, щоб отримати унікальне значення, відоме як дайджест повідомлення. Це свого роду цифровий зліпок з опису товару, який згодом буде використаний для перевірки цілісності повідомлення. Потім Аліса шифрує цей дайджест повідомлення особистим (секретним) ключем для підпису, щоб створити цифровий підпис. Після цього Аліса створює довільний симетричний ключ і використовує його для шифрування опису товару, свого підпису і копії свого сертифіката, який містить її відкритий

ключ для підпису. Для того щоб розшифрувати опис товару, Бобу потрібно захищена копія цього довільного симетричного ключа.

Сертифікат Боба, який Аліса повинна була отримати до ініціації безпечної зв'язку з ним, містить копію його відкритого ключа для обміну ключами. Щоб забезпечити безпечну передачу симетричного ключа, Аліса шифрує його, користуючись відкритим ключем Боба для обміну ключами. Зашифрований ключ, який називається цифровим конвертом, направляється Бобу разом із зашифрованим повідомленням. Нарешті, вона відправляє повідомлення Бобу, що складається з наступних компонентів: • симетрично зашифрованого опису товару, підписи і свого сертифіката; • асиметрично зашифрованого симетричного ключа (цифровий конверт). Продовжимо попередній приклад і розглянемо процедуру розшифрування. Боб отримує зашифроване повідомлення від Аліси і перш за все розшифровує цифровий конверт особистим (секретним) ключем для обміну ключами з метою вилучення симетричного ключа. Потім Боб використовує цей симетричний ключ для розшифрування опису товару, підписи Аліси і її сертифіката. Далі Боб розшифровує цифровий підпис Аліси з допомогою її відкритого ключа для підпису, який отримує з її сертифіката. Тим самим він відновлює оригінальний дайджест повідомлення з описом товару. Потім Боб пропускає опис товару через той же односпрямований алгоритм, який використовувався Алісою, і отримує новий дайджест повідомлення з розшифрованих описом товару. Потім Боб порівнює свій дайджест повідомлення з тим дайджестом, який отриманий з цифрового підпису Аліси. Якщо вони в точності збігаються. Боб отримує підтвердження, що зміст повідомлення не змінилося під час передачі і що вона підписана з використанням особистого (таємного) ключа для підпису Аліси. Якщо ж дайджести не збігаються, це означає, що повідомлення або було відправлено з іншого місця, або було змінено після того, як було підписано. В цьому випадку Боб робить певні дії, наприклад повідомляє Алісу або відкидає отримане повідомлення. Протокол SET вводить нове застосування цифрових підписів, а саме-використання подвійних цифрових підписів. В рамках протоколу SET подвійні цифрові підписи використовуються

для зв'язку замовлення, відправленого комерсанту, з платіжними інструкціями, що містять інформацію про рахунок і відправленими банку. Наприклад, покупець Боб хоче направити комерсанту Алісі пропозицію купити одиницю товару і авторизацію своєму банку на перерахування грошей, якщо Аліса прийме його пропозицію. У той же час Боб не хоче, щоб в банку прочитали умови його пропозиції, так само як і не хоче, щоб Аліса прочитала його інформацію про рахунок. Крім того, Боб хоче пов'язати свою пропозицію з перерахуванням так, щоб гроші були перераховані тільки в тому випадку, якщо Аліса прийме його пропозицію. Все вищесказане Боб може виконати за допомогою цифрового підпису під обома повідомленнями за допомогою однієї операції підписування, яка створює подвійну цифровий підпис. Подвійна цифровий підпис створюється шляхом формування дайджесту обох повідомлень, зв'язування двох повідомлень разом, обчислення дайджесту підсумку попередніх операцій і шифрування цього дайджесту особистим ключем для підпису автора. Автор зобов'язаний включити також дайджест іншого повідомлення, з тим щоб одержувач перевірив подвійну підпис. Одержувач будь-якого з цих повідомлень може перевірити його справжність, генеруючи дайджест зі своєї копії повідомлення, пов'язуючи його з дайджестом іншого повідомлення (в порядку, передбаченому відправником) і обчислюючи дайджест для отриманого результату. Якщо новостворений дайджест відповідає розшифрованої подвійний підписи, то одержувач може довіряти справжності повідомлення. Якщо Аліса приймає пропозицію Боба, вона може відправити повідомлення банку, вказавши на свою згоду і включивши дайджест повідомлення з пропозицією Боба. Банк може перевірити справжність авторизації Боба на перерахування і дайджесту повідомлення з пропозицією Боба, наданого Алісою, щоб підтвердити подвійну підпис. Таким чином, банк може перевірити справжність пропозиції на підставі подвійної підписи, але банк не зможе прочитати умови пропозиції.

2.3 Нові протоколи безпеки заочних платежів

Стандарт SPA / USAF від MasterCard International.

Корпорація MasterCard International представила Secure Payment Application (SPA) - нове рішення для забезпечення безпеки кредитних і дебетових платежів між власниками карток, продавцями і фінансовими установами. SPA є останньою новинкою в ряду інтернет-рішень MasterCard в сфері захисту всіх сторін, що беруть участь в онлайнових грошових операціях - власника картки, продавця і емітента картки.

SPA є схему забезпечення безпеки, яка використовує переваги інфраструктури Universal Cardholder Authentication Field (UCAF) корпорації MasterCard. UCAF це система передачі даних, здатна, зіставивши дані банку-емітента картки та інформацію, відому онлайн-продавцю, гарантувати, що угода здійснюється реальним власником картки. В системі USAF існує 23-байтное поле, закрите шифром від торгової точки і еквайрера. Воно передається від власника картки до емітента через торгову точку і еквайрера, які не мають доступу до шифру. Емітент проводить авторизацію. Таким чином, торгова точка з мінімальними вдосконаленнями отримує гарантію оплати, що є одним з ключових моментів в електронній торгівлі. При цьому, інфраструктура UCAF підтримує транзакції як з кредитними картами MasterCard, так і з дебетовими картами Maestro. Слід зауважити, що USAF підтримує безліч додатків для ідентифікації та захисту емітента, включаючи SPA, смарт-карти і багато іншого. Поєднання UCAF і SPA дозволяє засвідчити особу власника рахунку, генерує і передає підтвердження, що, угода авторизована законним власником, і створює основу для гарантії платежу електронним торговим підприємствам.

Принцип дії Технологія SPA аналогічна електронного чеку, виписуються від імені власника рахунку. Система передбачає використання Покупцем цифрового гаманця - e-wallet (SPA-сумісного гаманця). Для цього Покупець повинен завантажити спеціальне програмне забезпечення з сайту MasterCard.

Кожен раз, коли зареєстрований власник рахунку здійснює операцію, система генерує її специфічний атрибут - "показник посвідчення власника рахунку" (Accountholder Authentication Value, AAV), що представляє собою 32-значний код, який містить інформацію описують саме цю угоду (інформація про власника рахунку і проводиться транзакції, включаючи найменування товару та суму платежу). Таким чином, унікальне значення цієї змінної, мінливий з кожною транзакцією, дозволяє ідентифікувати власника картки, фактично пов'язуючи власника рахунку з угодою, яка мала місце по відношенню до певного торговому підприємству на певну суму. Збіг значення цієї змінної, мінливого з кожною наступною транзакцією, буде підтверджувати легітимність використання карти для запитуючої сторони.

Переваги технології SPA (Secure Payment Application):

SPA не вимагає великих фінансових витрат, оскільки інтегрується у вже існуючі системи захисту. Ця система надає продавцеві еквівалент підпису власника картки, підтверджуючи, що емітент уже перевірив власника картки ще до завершення платіжної операції.

SPA забезпечує ідентифікацію власника картки.

SPA ніяк не впливає на тривалість часу, необхідного для здійснення онлайнових покупок або для підтвердження платежу.

Рис. 2.2 Схема виконання онлайнових покупок

SPA не вимагає використання інфраструктури відкритого ключа (PKI), що значно спрощує використання цього додатка усіма сторонами.

SPA дає Інтернет-Магазину повну гарантію аутентифікації Покупця (власника карти) і спеціальне підтвердження того, що платіж був здійснений з його згоди.

Відповідальність за шахрайські транзакції, не санкціоновані власником картки, знімається з онлайнової торгової точки і компанії, що здійснює еквайринг.

SPA підтримує застосування різних пристроїв доступу в Інтернет для здійснення транзакцій (наприклад, транзакції з мобільного телефону)

недоліки:

Основним недоліком технології можна вважати, більш складну реалізацію системи SPA, ніж, наприклад, технології 3D-Secure від Visa International

Так же недоліком є те, що користувачеві доводиться попередньо завантажувати додаткове додаток, з web-сторінки банківської установи.

3-D Secure (протокол трьох доменів).

Архітектура 3-D Secure

Віза розробила протокол 3-D Secure (так званий протокол трьох доменів), щоб збільшити ефективність онлайнових транзакцій і прискорити зростання електронної комерції.

Розвиток і впровадження цього протоколу має принести вигоду всім учасникам онлайнової транзакції, надавши банкам-емітентам можливість аутентифицировать власників карток під час онлайнової покупки. Це підвищить надійність і безпеку транзакцій і зменшить можливість шахрайського використання кредитних карт в Інтернеті - якщо покупки будуть відбуватися з використанням технології 3D-secure.

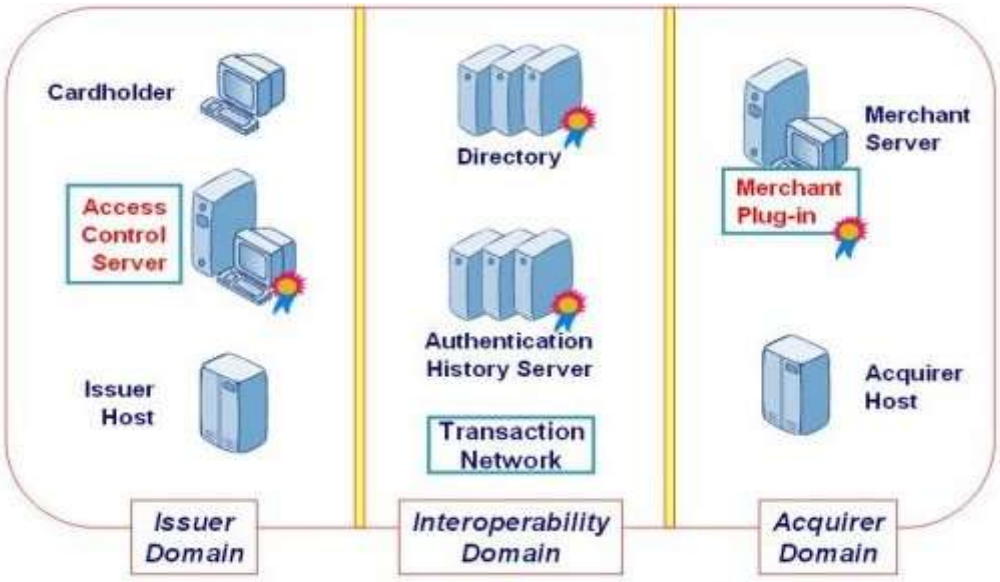

Рис. 2.3 Архітектура 3-D Secure

Переваги даного протоколу полягають у наступному:

- використання 3-D Secure зменшує можливі втрати грошей всіма учасниками транзакції, оскільки істотно зменшує кількість чарджбеков, ініційованих держателями карток через те, що карта була використана шахраями. - Щоб використовувати протокол, клієнтам не обов'язково купувати нове апаратне або програмне забезпечення - Протокол може бути розширений і доповнений банком-емітентом, щоб найкращим чином відповідати вимогам клієнтів без необхідності банкам-еквайрам і Мерчант вводити доповнення до протоколу зі свого боку. - Протокол може використовуватися на таких перспективних для розвитку електронної комерції платформах, як мобільні телефони, кишенькові комп'ютери, цифрові телевізори. - Він заснований на широко застосовуються технічних стандартах, що підтримуються міжнародними організаціями. - Надає можливість ведення (і доступу до) централізованого архіву аутентифікації, який буде корисний для прийняття рішення щодо спірних транзакцій.

Архітектура 3-D Secure:

Віза розробила модель трьох доменів як основу нових рішень для платіжних систем. Основна ідея моделі в тому, що весь процес аутентифікації, що забезпечує безпеку транзакцій, розбивається на три домену (або іншими словами області):

Issuer Domain (Домен емітента) - його призначення в тому, що обслуговуючий банк виробляє аутентифікацію своєї торгової точки на основі

правил і методів, встановлених самим обслуговуючим банком (т. Е. В цьому випадку вся відповідальність за аутентифікацію лягати на обслуговуючий банк торгової точки);

Acquirer Domain (Домен еквайра) - його призначення в тому, щоб визначити правила і процедури обміну інформацією між доменами емітента та еквайра, що гарантують цим доменів взаємну аутентифікацію один одного.

Власник карти знаходиться в домені емітента, а торгове підприємство (Мерчант) знаходиться в домені еквайра, які в свою чергу взаємодіють між собою через домен Interoperability (Міжопераційний).

Сервер контролю доступу (Access control server - ACS) Сервер контролю доступу виконує дві функції:

1. Перевірка можливості 3-D Secure аутентифікації для номера карти 2. Аутентифікація власника карти для конкретної транзакції або забезпечення підтвердження спроби аутентифікації в разі, якщо аутентифікація недоступна (неможлива). Хоча ці функції і описані, як здійснюються одиночним логічним ACS, фізичних серверів, що забезпечують реалізацію функцій ACS, може бути багато. Наприклад кожен з цих серверів «обслуговує» певний діапазон номерів карт.

Сервер історії аутентифікації Даний сервер знаходиться під управлінням Віза. Його основні функції такі: - отримати повідомлення від сервера контролю доступу для кожної спроби аутентифікації (незалежно від успішності спроби) - зберігає отримані записи

Копія даних, що зберігаються сервером історії аутентифікації, може бути передана еквайрам і емітентам для вирішення спірних питань.

VisaNet

Щодо аутентифікації платежів VisaNet виконує свою традиційну роль: - Отримує запити на авторизацію від еквайра - Пересилає їх емітенту - Пересилає відповіді емітента до еквайра - Надає еквайрам і емітентам інші сервіси (кліринг, установка і т п).

Як працює аутентифікація платежу.

Рис. 2.4 Схема аутефекації платежу

Власник карти робить покупку. Коли власник кредитної картки має намір зробити покупку, він або повинен надати інформацію про свій рахунок (карті), або використовує спеціальне програмне забезпечення (наприклад, цифровий гаманець), щоб це зробити. Коли власник карти підтверджує своє бажання зробити покупку, запускається плагін сервера мерчанта (ПСМ) Merchant Server Plug-in (MPI). Програма ПСМ може перебувати на сайті інтернет-магазину, у еквайра або у процесингового центру третьої сторони.

Запит до Віза директор

ПСМ посилає повідомлення до сервера Віза директор, щоб визначити, чи можливо провести аутентифікацію для даної кредитної картки. Якщо ПСМ отримує відповідь, що власник картки зареєструвався попередньо (заявка на можливість участі в 3-D Secure відправляється власником картки банку-емітенту) і можливо провести аутентифікацію, відповідь було надіслане до ПСМ буде містити інструкції, як зв'язатися з сервером контролю доступу відповідного емітента. Якщо номер рахунку клієнта знаходиться за межами інтервалу, в якому розташовані номери допущених до 3-D Secure карт, сервер Віза директор повертає транзакцію до сервера мерчанта через ПСМ, після чого мерчант може відправляти стандартний запит на авторизацію.

Аутентифікація власника карти

ПСМ надсилає запит на аутентифікацію до сервера контролю доступу. Зазвичай ця відсилання проводиться за допомогою броузера покупця. Сервер контролю доступу виробляє аутентифікацію - шляхом виведення на комп'ютер покупця діалогового вікна, в яке необхідно ввести пароль, або використовує інший метод аутентифікації за типом кредитної картки (наприклад, в разі чіп-карти) Сервер контролю доступу формує відповідь і запевняє його цифровим підписом, потім повертає його до ПСМ.

2.4 Безпека транзакцій з використанням електронних грошей

Термін «електронні гроші» є відносно новим і часто застосовується до широкого спектру платіжних інструментів, які засновані на інноваційних технічних рішеннях. Наслідком цього є відсутність єдиного, визнаного в світі визначення електронних грошей, яке б однозначно визначало їх економічну і правову сутність.

Електронним грошам властиво внутрішнє протиріччя - з одного боку вони є засобом платежу, з іншого - зобов'язанням емітента, яке повинно бути виконано в традиційних неелектронних грошах. Такий парадокс можна пояснити за допомогою історичної аналогії: свого часу банкноти теж розглядалися, як зобов'язання, яке підлягає оплаті монетами або дорогоцінними металами. Очевидно, що з плином часу, електронні гроші будуть однією з різновидів форми грошей (монети, банкноти, безготівкові гроші та електронні гроші). Так само очевидно, що в майбутньому центробанки будуть виробляти емісію електронних грошей, так само як зараз карбують монету і друкують банкноти.

Поширеним помилкою є ототожнення електронних грошей з безготівковими грошима.

Електронні гроші, будучи неперсоніфікованим платіжним продуктом, можуть мати окреме звернення, відмінне від банківського обігу грошей, проте можуть і звертатися в т.ч. і в державних або банківських платіжних системах. Як правило, обіг електронних грошей відбувається за допомогою комп'ютерних

мереж, Інтернету, платіжних карт, електронних гаманців і пристроїв, що працюють з платіжними картами (банкомати, POS-термінали, платіжні кіоски і т. Д.). Також, використовуються і інші платіжні інструменти різної форми: браслети, брелоки, блоки мобільних телефонів і т. Д., В яких є спеціальний платіжний чіп.

Електронні гроші зазвичай поділяють на два типи: на базі смарт-карт (англ. Card-based) і на базі мереж (англ. Network-based). І перша, і друга група поділяються на анонімні (неперсоніфіковані) системи, в яких дозволяється проводити операції без ідентифікації користувача і не анонімні (персоніфіковані) системи, що вимагають обов'язкової ідентифікації користувача.

Слід також розрізняти електронні фіатние гроші і електронні нефіатние гроші. Електронні фіатние гроші обов'язково виражені в одній з державних валют і є різновидом грошових одиниць платіжної системи однієї з держав. Держава законами зобов'язує всіх громадян приймати до оплати фіатние гроші. Відповідно, емісія, обіг та погашення електронних фіатних грошей відбувається за правилами національних законодавств, центробанків або інших державних регуляторів. Електронні нефіатние гроші - є електронними одиницями вартості недержавних платіжних систем. Відповідно, емісія, обіг та погашення (обмін на фіатние гроші) електронних нефіатних грошей, відбуваються за правилами недержавних платіжних систем. Ступінь контролю і регулювання державними органами таких платіжних систем в різних країнах сильно відрізняються. Часто недержавні платіжні системи прив'язують свої електронні нефіатние гроші до курсів світових валют, проте держави ніяк не забезпечують надійність і реальну цінність таких вартісних одиниць. Електронні нефіатние гроші є різновидом кредитних грошей.

Однією з поширених помилок є віднесення до електронних грошей сучасних засобів доступу до банківського рахунку, а саме, традиційних банківських платіжних карт (як мікропроцесорних, так і з магнітною смугою), а також інтернет-банкінгу. У системах, які здійснюють розрахунки електронними грошима, банківські рахунки використовуються тільки при введенні і виведенні грошей з системи. При цьому використовується консолідований банківський рахунок емітента електронних грошей, а не карткові або поточні рахунки

користувачів. При емісії електронних грошей традиційні гроші зараховуються на консолідований банківський рахунок емітента. При пред'явленні електронних грошей для погашення традиційні гроші списуються з консолідованого банківського рахунку емітента.

Ще однією типовою помилкою є віднесення до електронних грошей передплачених одноцільових карт, таких як: подарункова карта, паливна карта, телефонна карта і т. Д. Використання такого платіжного інструменту не означає здійснення нового платежу. Реальний платіж здійснюється в момент покупки або поповнення такої карти. Її використання не породжує нових грошових потоків і є простим обміном інформації про спожиті товари або послуги.

Анонімність електронних грошей

Електронні гроші можуть бути анонімними і персоніфікованими. За своєю природою електронні гроші ближче до анонімних готівці, ніж до персоніфікованих безготівковим. Наявність або відсутність анонімності забезпечується правилами і механізмами обігу електронних грошей в певній платіжній системі.

Більшість державних регуляторів, а також державні і недержавні платіжні системи, різними способами намагаються стимулювати персоніфікацію користувачів електронних грошей і операції з ними. Наприклад, для електронних грошей на базі мереж, платіжні системи обмежують розмір електронного гаманця для анонімного користувача, збільшуючи ліміти персоніфікованим користувачам системи. Для електронних грошей на базі карт обмежують максимальну суму в гаманці і вводять персоналізовані механізми поповнення.

Криптографічний захист

Використання криптографії для реалізації електронних грошей запропонував Девід Чом (англ. David Chaum). Їм також запропоновано кілька протоколів шифрування і електронного підпису. Він використовував алгоритм конфіденційного зв'язку для досягнення приховування зв'язків між транзакціями вилучення та внесення грошей. Суть ідеї Чома полягала в так званій системі «сліпий» цифрового підпису (англ. Blind signature), коли підписує інформацію

бачить її лише в частині йому необхідної, але своєю цифровим підписом завіряє справжність всієї інформації: емітент бачить гідність купюр і може запевнити їх справжність, але не знає їх серійних номерів, які знає тільки власник грошей.

При цьому можна строго довести, що такий «сліпий» підписом гарантується справжність всього вмісту купюри з тією ж надійністю, що і звичайної цифровим підписом, яка стала за останні роки одним з найпопулярніших засобів підтвердження автентичності електронних документів. Основою служить метод RSA-шифрування.

2.5 Безпека платіжних смарт-карт і електронних гаманців

EMV (Europay, MasterCard і VISA) - міжнародний стандарт для операцій по банківських картах з чіпом. Цей стандарт розроблений спільними зусиллями компаніями Europay, MasterCard і Visa, щоб підвищити рівень безпеки фінансових операцій.

Основна відмінність для користувача карти стандарту EMV, це вимога введення пін-коду при проведенні будь-якого платежу через термінал (наприклад, в магазинах, ресторанах).

Стандарт EMV визначає фізичне, електронне та інформаційну взаємодію між банківською картою і платіжним терміналом для фінансових операцій. Існують стандарти, засновані на ISO / IEC 7816 для контактних карт, і стандарти ISO / IEC 14443 для безконтактних карт.

Перший стандарт для платіжних карт був створений у Франції в 1989 році і називався Carte Bancaire B0 'стандарт. Також стандарт Geldkarte в Німеччині передував EMV. EMV повністю сумісний з цими двома стандартами. Франція перевела всі карти випускаються на території країни на стандарт EMV.

Найбільш поширені варіації стандарту EMV:

• VSDC - VISA;

• MChip - MasterCard;

• AEIPS - American Express;

• J Smart - JCB.

У травні 2010 року було заявлено, що United Nations Federal Credit Union в Нью-Йорку випустити першу карту стандарту EMV в США.

Особливості та переваги EMV

Основні переваги - підвищений рівень безпеки транзакцій і можливість більш точного контролю транзакцій в «оффлайн». Одна з цілей EMV - підвищити функціональність карт (наприклад, платіжна карта з електронним проїзним). Підвищений рівень безпеки забезпечується за рахунок відходу від візуального контролю (перевірка продавцем голограми, підписи, звірка імені з посвідченням особи) до використання ПІН коду і криптографічних алгоритмів, таких як DES, Triple-DES, RSA і SHA для аутентифікації карти. Час проведення транзакції можна порівняти з онлайновими транзакціями.

Новий рівень безпеки дозволив перенести відповідальність за втрачені кошти в результаті шахрайства з власника карти на банки і платіжні системи.

Протокол COPS призначений для обміну інформацією про політику між серверами політики (Policy Decision Point або PDP) і їх клієнтами (Policy Enforcement Points або PEP). Прикладом клієнта політики є RSVP-маршрутизатор, який повинен реалізовувати управління доступом, що базується на певній політиці [RSVP]. Ми припускаємо, що існує, принаймні, один сервер, який визначає політику в кожному з доменів. Базова модель взаємодії між сервером політики і клієнтом сумісна з документом з управління доступом [WRK]. Характеристики протоколу COPS містять такі моменти (RFC-2748):

1. Протокол використовує модель клієнт-сервер, де PEP посилає запити, здійснює актуалізацію даних, відправляє повідомлення про ліквідацію віддаленим PDP, а PDP повертає відгуки-рішення вузлів PEP.

2. Протокол використовує TCP для надійного обміну повідомленнями між клієнтами і сервером. Отже, не потрібно ніякого додаткового механізму для забезпечення надійної взаємодії між сервером і клієнтами.

3. Протокол є розширюваним і може працювати з будь-якою специфічною інформацією клієнтів без модифікації самого протоколу COPS. Протокол був створений для загального адміністрування, конфігурації і реалізації політики.

4. COPS надає безпеку на рівні повідомлень для цілей аутентифікації, захисту відгуку і цілісності повідомлення. COPS може також використовувати для мети безпеки існуючі протоколи, такі як IPSEC або TLS для здійснення аутентифікації і безпечного каналу між PEP і PDP.

5. COPS є протокол станів. (1) Стан запит / рішення є загальним для системи клієнт-сервер. (2) Стан різних подій (пар запит / рішення) можуть асоціюватися. Під пунктом (1) мається на увазі, що запити клієнта PEP встановлюються або запам'ятовуються віддаленим PDP до тих пір, поки вони не будуть анульовані PEP. У той же час, для заданого стану запиту рішення віддаленого PDP можуть генеруватися асинхронно. Під пунктом (2) мається на увазі, що сервер може реагувати на нові запити по-різному в залежності від надійшли раніше запитів / рішень.

6. Крім того, COPS є протоколом станів, так як він дозволяє серверу конфігурувати клієнта, а потім анулювати цей стан, якщо воно більш не потрібно.

Висновки: Досліджено електронні транзакції в системах B2C та C2C. Визначено поняття заочних платежів та протоколу безпечних карткових транзакцій.

3 ПЛАТІЖНІ СИСТЕМИ УКРАЇНИ

3.1 Електронні платіжні системи інтернету

Електронні платіжні системи - це технологія, що дозволяє проводити розрахунки безпосередньо між контрагентами. В даному випадку відсутня необхідність переказу грошей з одного рахунку на інший у банку чи іншої фінансової установи. Платнику не потрібно вказувати відомості про себе (при оплаті послуг або купівлі товару, що не потребує доставки, наприклад, PIN - коду). На даний момент розрахунки через електронні платіжні системи актуальні відносно операторів стільникового зв'язку, продавців PIN - кодів, інтернет - провайдерів, телефонних компаній і невеликого числа великих магазинів, які торгують матеріальними цінностями.

Web Money Transfer. За допомогою цієї системи можна:

Проводити розрахунки з іншими користувачами, оплачувати товари і послуги в мережі;

Обговорювати з партнерами умови торговельних угод за допомогою голосового сервісу, відеоконференції, захищеної WM - пошти;

Отримувати і видавати позики в титульних знаках (в тому числі колективно);

Автоматизувати управління бюджетом вашої спільної діяльності або мережевого підприємства;

Оплачувати послуги мобільних операторів, провайдерів інтернет і ТВ, оплачувати підписку на ЗМІ;

Створювати власні цифрові чеки для оплати товарів і послуг в інтернет - магазинах і моментальних розрахунків поза мережею;

Проводити обмін електронних валют за вигідним курсом;

Поширювати програмні продукти і електронні книги в захищеному від копіювання форматі;

Проводити розрахунки по електронній пошті, використовувати мобільний телефон як гаманець.

Ця облікова система забезпечує проведення розрахунків в реальному часі за допомогою облікових одиниць - титульних знаків Web Money (WM). Управління рухом титульних знаків здійснюється користувачами за допомогою клієнтської програми WM Keeper.

При переказі коштів використовуються однотипні гаманці, обмін різних титульних знаків проводиться в обмінних сервісах.

Власником і адміністратором системи, що забезпечує її організаційну і технологічну цілісність, є компанія WM Transfer Ltd., яка є розробником, власником і адміністратором системи WebMoney Transfer.

Для того щоб стати учасником системи WebMoney Transfer досить встановити на своєму комп'ютері клієнтську програму WM Keeper і зареєструватися в системі, отримавши при цьому WM ідентифікатор і прийнявши угоди системи. Процес реєстрації також передбачає введення персональних даних і підтвердження їх достовірності за допомогою клієнтської програми WM Keeper.

В системі реалізована програма WM атестації. Кожен користувач має WM атестат - цифрове свідоцтво, складене на підставі наданих їм персональних даних.

Кожен учасник системи має певний бізнес-рівень (BUSINESS LEVEL). BL - це публічна інтегральна характеристика рівня ділової активності власника WM ідентифікатора, яка обчислюється на основі даних про тривалість активного використання WebMoney Transfer; кількості кореспондентів, з якими у користувача були трансакції; обсязі проведених трансакцій, наявності претензій або позитивних відгуків на адресу користувача. Значення BL воможно побачити в діалозі програми WM Keeper при роботі з конкретним контрагентом, а також на сторінках сервісів системи.

Яндекс. Гроші. Яндекс. Гроші - електронна платіжна система, яка реалізує ідею електронних грошей. Забезпечує проведення фінансових розрахунків між учасниками системи (особами, які відкрили рахунки в системі) в режимі реального часу. Валюта розрахунків - російський рубль. Призначена для

забезпечення функціонування систем електронної комерції. Система надає можливість працювати через веб-інтерфейс або з використанням програми-гаманця, що встановлюється на комп'ютер користувача (ця можливість доступна тільки користувачам Windows). Головний офіс компанії знаходиться в Москві, додатковий офіс в Санкт-Петербурзі. Генеральним директором компанії є Євгенія Завалішина.

В системі використовується два типи рахунку: Яндекс. Гаманець і Інтернет. Гаманець. Перший - рахунок, доступ до якого здійснюється за допомогою web інтерфейсу. Другий - рахунок, доступ до якого здійснюється за допомогою спеціальної програми «Інтернет. Гаманець ». Програма безкоштовна, працює під управлінням ОС Windows.

Користувач вносить будь-яким з можливих в системі способів грошові кошти на свій рахунок. У момент оплати товару або послуги система відсилає на рахунок магазину електронні гроші з рахунку користувача. Отримавши електронні гроші від користувача, магазин пред'являє їх в процесинговий центр для підтвердження можливості їх використання (достовірності). Перевіривши, що гроші раніше не використовувалися і є справжніми, процесинговий центр підтверджує їхню платоспроможність магазину і висилає «квитанцію» покупцеві. Одночасно проводиться списання коштів з рахунку користувача в процесинговому центрі і їх зарахування на рахунок магазину. Отримавши підтвердження справжності та платіжності електронних грошей, магазин відсилає квитанцію про оплату на гаманець користувача і виробляє здійснення послуги або надання товару.

Всі ці процедури проводяться практично миттєво і непомітно для користувача.

За допомогою Яндекс. Грошей можна робити покупки в інтернет-магазинах, оплачувати послуги зв'язку і ЖКГ, робити внески в благодійні фонди, розраховуватися за бензин на АЗС. Але не всі користувачі системи звертають увагу на те, що не можна використовувати Яндекс. Гроші для будь-якої комерційної діяльності. Служба безпеки Яндекс. Грошей має право без пояснення

причин і без попередження заблокувати гаманець, що часто є несподіванкою для користувачів системи, яким пропонується провести процедуру «ідентифікації» підтверджує особу користувача і включає письмове пояснення куди і на що вони витрачають свої Яндекс. Гроші.

PayPal. PayPal (англ. «Приятель, що допомагає розплатитися») - найбільша в світі дебетова електронна платіжна система. В даний час PayPal працює в 190 країнах і має більше 164 мільйонів зареєстрованих користувачів. PayPal працює з 18 національними валютами.

Платежі здійснюються через захищене з'єднання після введення e-mail і пароля, вказаних після підтвердження аккаунта. У поняття аккаунт входить адреса, по якому будуть доставлятися покупки. Користувачі PayPal можуть переказувати гроші один одному.

Підтвердження облікового запису включає в себе процедуру зняття грошей з карти користувача із зазначенням коду, який необхідно повідомити PayPal, що підтверджує ідентичність власника карти, що має доступ до історії платежів, особистості, що вводить пароль і інші дані в систему Paypal.

Використання системи PayPal здійснюється на безкоштовній основі: реєстрація в системі безкоштовна, за відправлення грошових коштів комісія з користувача не знімається, за винятком привілейованих статусів (Premier і Business). Комісія стягується з одержувача платежу, розмір комісії залежить від місця розташування країни користувача і статусу.

Інтернет. Гроші. Українська платіжна система Інтернет. Гроші є небанківською системою розрахунків. З точки зору користувача (продавця або покупця), система Інтернет. Гроші - це сукупність електронних гаманців, кожен з яких представляє собою захищену клієнтську програму, що дозволяє переводити і отримувати електронну готівку з інших гаманців, зберігати її в інтернет - банку, виводити з системи на банківські рахунки або в інші платіжні системи. Платіжна система Інтернет. Гроші заснована на технології PayCash.

Використання платіжної системи Інтернет. Гроші дозволяє:

- оплатити мобільний телефон;

- оплатити доступ в інтернет;
- здійснювати покупки в інтернет - магазинах;
- скористатися розширеними можливостями для азартних людей;
- приймати платежі (стягується комісія).

3.2 Проблеми платіжних систем України. Шляхи вдосконалення платіжних систем України

Збільшення кількості терміналів не "підніме» вітчизняний ринок пластикових карт. В кінці минулого року банківські лобісти спільно з представниками українського ринку платіжних систем в черговий раз намагалися реанімувати ідею тотальної терміналізації торгових точок країни. Правда, вже на якісно іншому рівні - не у вигляді проекту відповідного закону (три версії якого були проігноровані ВР), а у вигляді проекту урядової постанови. Даний документ знову піднімає питання добровільно-примусового оснащення платіжними терміналами кожного більш-менш великого магазину, автозаправки чи ресторану в кожному більш-менш густонаселеному пункті. Правда, тепер акцент зміщується з «добровільного» на «примусове»: у проекті прописано чіткий механізм контролю над дотриманням прописаної норми. Схоже, криза завдала відчутного удару по ринку банківського пластику, раз популярність безготівкових розрахунків знову хочуть «впровадити в народ» штучним шляхом. Втім, особливої ефективності від цього механізму (завдання реалізації якого перейшла «у спадок» до нового Кабміну) експерти не бачать: надто вже багато спірних питань може виникнути у всіх учасників процесу «пластикової оплати».

Ввести «пластик» в активне використання в Україні намагаються вже давно. «Спроби впровадження масових безготівкових розрахунків почалися з жовтня 2004 року, коли до Закону України« Про платіжні системи »був включений пункт 14.7 щодо обов'язкового прийому платіжних карток. Для деталізації даного положення Кабінет міністрів своєю постановою №377 з 29.03.2006 року затвердив Умови переведення підприємців, які ведуть господарську діяльність у сфері

торгівлі, громадського харчування та послуг, на обов'язкове приймання спеціальних платіжних засобів в оплату за продані товари (надані послуги).

За даними Української міжбанківської асоціації членів платіжних систем (ЕМА), за п'ять років, які пройшли з моменту прийняття вищезазначених норм, українські банки встановили за власний рахунок в мережах українських торговців близько 90 тис. POS терміналів (стан на 1 січня 2010 року), в той час як ще в 2006 році таких було менше 30 тис. тобто ефект, звичайно, є. Але не настільки значний, як того хотілося б емітентам «пластика». Згідно обліку податкової адміністрації, в нашій країні є понад 400 тис. Організацій, що працюють в сфері торгівлі та послуг, з яких лише 5-7% на даний момент надають українцям можливість розплачуватися карткою. «На жаль, в постанові №377, що діє до сих пір, відсутній механізм регулювання контролю його виконання. Якщо для нас було очевидно, що наявність норми передбачає зобов'язання її виконувати, то для торгових мереж цього виявилося недостатньо. Щоб покласти край сумнівам торговців, в 2006-2008 роках послідовно були розроблені три проекти змін до Закону «Про платіжні системи», покликані більш чітко врегулювати це питання. На жаль, жоден з них не був підтриманий ВР ».

Тому в ЕМА вирішили піти іншим шляхом і, звернувшись в Мінекономіки, отримали підтримку в просуванні проекту урядової постанови «Питання переведення торговців на здійснення розрахунків за продані товари (надані послуги) з використанням спеціальних платіжних засобів». Проект є, по суті, «переспівом» останнього законопроекту ЕМА №1463, де також пропонувалося розпалити в торговців бажання встановлювати POS термінали за допомогою встановлення жорсткої системи контролю та штрафних санкцій.

Аналогічна позиція була закладена і в законопроекті №1463, відхиленому депутатами в червні минулого року. Однак в документах є і відмінності: «У проекті закону норми прив'язувалися до класифікації: різні категорії торговців, з різним оборотом і торговою площею в різні терміни повинні були б забезпечити установку терміналів на підприємствах роздрібної торгівлі. У нинішньому проекті

ідеологія дещо інша. Так, норма Закону «Про платіжні системи» говорить, що підприємство, яке має РРО, має забезпечити прийом платіжних карт. На виконання цього закону в проекті чітко зазначено, що POS терміналами повинні бути обладнані абсолютно всі торгові точки, які проводять розрахунки за допомогою касових апаратів. Внесено виключення, на яких наполягали в Мінфіні і ДПАУ, такі як підприємства торгівлі закритого типу або закладу, які організовують харчування студентів, учнів та викладачів, працівників промислових підприємств. Для суб'єктів малого підприємництва на прохання Ради підприємців робиться відстрочка на півтора року. Крім того, від обов'язкового прийняття спеціальних платіжних засобів звільняються суб'єкти господарювання в населених пунктах з чисельністю населення менше 25 тис., Куди банківська індустрія поки, на жаль, так і не змогла прийти ».

Крім низького інтересу споживачів, перепоною на шляху до популяризації карткових розрахунків в нашій державі є відсутність на те бажання самих суб'єктів господарювання. «Прогресивний підприємець, який прийняв рішення оптимізувати свій бізнес за рахунок впровадження системи карткового розрахунку, відразу ж стикається з низкою вагомих перешкод, які змушують його переглянути свої наміри. Серед таких перешкод - розмір комісійної винагороди, яке вимагають банки за послуги еквайрингу, тобто власне організації розрахунків за допомогою платіжних карток на підприємствах торгівлі та послуг. В даному контексті розробники нібито і спробували вирішити цю проблему, сформулювавши в проекті рекомендацію банкам встановлювати комісійну винагороду на рівні не вище 2% суми проданих товарів (послуг), однак питання, чи врахують комерційні банки таке побажання, залишається під великим сумнівом. Як показує практика, сьогодні банки вимагають за свої послуги комісію на рівні 3,5% і вище. Таким чином, цілком зрозумілою стає позиція підприємця, якому куди дешевше оплачувати послуги інкасації, ніж послуги хоч і зручного, але комерційно невигідного еквайрингу ».

І хоча в проекті рекомендується розглянути питання про можливість встановлення такого обладнання за рахунок власних коштів банків, логічно

припустити, що таку рекомендацію враховуватимуть далеко не всі банки. Особливо в світлі норми про те, що кількість платіжних терміналів у приміщеннях, де здійснюється продаж товарів або надання послуг за допомогою РРО, повинна становити не менше 50% кількості РРО.

В цілому ж, на переконання експертів, тотальна терміналізація навряд чи істотно поліпшить ситуацію на ринку пластикових карт України, який за час кризи впав до рівня 2006 року. За даними НБУ, кількість активних платіжних карт (за якими була здійснена хоча б одна видаткова операція) за останні 12 місяців скоротилося на 25% (з 38,6 млн. До 29,1 млн.). «У зв'язку з кризою було оптимізовано все, що можна було оптимізувати. З одного боку, розорилося певна кількість підприємств, і, відповідно, зарплатні картки їх працівників були закриті. Також в першому півріччі минулого року в зв'язку з ростом невиплат по кредитах практично було припинено кредитування і установка овердрафтів у всіх банках. З іншого боку, банки нарешті перестали, як в соцзмаганні, показувати роздуті цифри карткової статистики і відкрили реальні дані по використовуваних картах. Зараз це справжні цифри того, що є на ринку.

Шахрайство з платіжними картами в Україні виникло тоді ж, коли і сам ринок платіжних карт, - на початку 90 х років. І розвивалося разом з ринком. В кінці 90 х шахраї підробляли карти, перехоплюючи дані (реквізити карткового рахунку, PIN код), що прямують з банкомату або POS терміналу в процесинговий центр шляхом приєднання до кабелю. Через таку незахищеность каналів передачі даних вітчизняних банків міжнародні платіжні асоціації навіть рекомендували іноземцям не розраховуватися картками і не користуватися банкоматами в Україні. Два роки тому банки ускладнили завдання хакерам, звернувшись до більш просунутих методів шифровки переданої інформації.

Тоді шахраї стали шукати інші способи отримання інформації про картки. Скіммінг (копіювання даних з магнітної смуги карти і виготовлення її дубліката) став здійснюватися за допомогою спеціальних насадок (скімерів) на клавіатуру банкомату і конвертів, що вставляються в роз'єм для карти. Ці пристрої зчитують інформацію з магнітної смуги карт, а також фіксують PIN код.

Шахраї намагаються спростити собі життя, отримавши не тільки дані про картковий рахунок, а й PIN код, і тому все частіше вдаються до установки скімерів на банкомати. Вітчизняні викрадачі використовують і фішинг - розсилання листів, що пропонують відвідати web сторінку банку або віртуального магазину з тим, щоб уточнити дані про рахунок або придбати товари або послуги, наприклад, маркетингові дослідження або бази даних. Нещодавно клієнти українських банків повелися на пропозицію шахраїв заробити за допомогою Інтернету. Їхні картки згодом були використані в інтернет-магазинах для покупки ваучерів поповнення рахунків мобільного зв'язку. Аферисти неодноразово розсилали листи абонентам послуги інтернет-банкінгу Приватбанку. Клієнти банку одержували електронні листи нібито від служби безпеки банку з проханням терміново пройти авторизацію, слідуючи за доданою посиланням. При цьому назва шахрайського сайту майже повністю повторювало адресу порталу інтернет-банкінгу «Приват24». Проблеми управління ризиками платіжних систем розкриваються в декількох монографіях, розділах підручником, присвячених банківській справі, статтях і центральних журналах, збірниках наукових праць, тезах доповідей на наукових конференціях.

Так, в фундаментальній праці Дж.Ф. Синки, мл. обговорюються питання розвитку платіжних систем, в тому числі технологічних нововведень в банках, в системі платежів і обробки інформації, поширення електронних банківських систем і автоматизованих клірингових палат. Автор пильну увагу приділяє ролі технологій в банківській справі («в умовах дерегулювання технологія стає зброєю перемоги в конкуренції»), при цьому акцентуючи увагу на тому, що банківська галузь не є піонером в області освоєння нових технологій, і основними причинами цього є «паперу і люди ». Розглядаючи процес впровадження інновацій в банківській справі і розвитку в зв'язку з цим платіжних систем, автор зазначає, що «ефективно використовуються електронні системи платежів здійснюють миттєву верифікацію і переказ коштів, скорочуючи дорогий паперовий вал, який породжується урахуванням операцій». Проводиться аналіз переваг і витрат електронних систем платежів, в рамках якого відзначаються такі

аспекти, як «конфіденційність, забезпечення права власності, вплив на конкуренцію, зниження монополізму, вплив на грошову політику, розвиток і спільне використання систем».

У той же час позначена проблема управління ризиками, що виникають при функціонуванні електронних систем платежів: відзначається, що для гладкого функціонування механізму платежів найважливіше значення має впевненість в отриманні коштів, оскільки в багатьох транзакціях учасники буквально нічого не знають про кредитоспроможність іншого боку. Будь-який збій в системі розрахунків веде до хаосу, а великі платіжні системи є джерелом величезного глобального ризику. Взаємозв'язок фінансових інститутів за допомогою клірингових і розрахункових центрів призводить до виникнення операційних, кредитних і ліквідних ризиків, до в останні роки спостерігається їх значне зростання. При цьому питання, пов'язані з управлінням ризиками електронних платіжних систем, в тому числі з розробкою методів оцінки і зниження операційних ризиків, в роботі не розглядаються.

Разом з тим, з огляду на тенденції збільшення електронного обміну інформацією між банками, в тому числі і на міжнародному рівні, в монографії, на наш погляд, недостатньо уваги приділено що виникають у зв'язку з цим ризиками і способам управління ними. Так, операційний ризик розглядається тільки в рамках класифікації ризиків, що виникають в діяльності банків, і автором обговорюється єдиний спосіб мінімізації даного ризику - «управління якістю - здатність першокласних керуючих вирішувати виникаючі проблеми до того, як вони стануть серйозними проблемами для банку». При цьому не підлягають розгляду етапи управління ризиками платіжних систем, не пропонуються способи їх ідентифікації та оцінки.

3.3 Шляхи вирішення проблем платіжних систем в Україні

Законами встановлено загальний порядок і режим платіжних відносин, також терміни проведення платіжних операцій і відповідальність за невиконання

зазначених приписів. Детально, тобто питання практичного застосування зазначених норм, описані в підзаконних, відомчих нормативних актах. У підсумку ми отримуємо діючу платіжну систему. На практиці вона показала свою працездатність. Для існування платіжної системи необхідно виконання деяких зовнішніх умов, тобто економічний зміст, яким повинні виступати: розрахункові інструменти (попросту кажучи досить одного - коштів), виконання суб'єктами розрахункових відносин обов'язкових приписів щодо здійснення розрахунків, дотримання платіжної дисципліни. Достатність перерахованих вище факторів гарантує існування безкризовий платіжної системи.

Сформована криза змусила всіх підійти до вирішення спільними зусиллями. Підприємства не перестали відвантажувати продукцію, спрямовану на виконання державного замовлення, інші не перестали виконувати неоплачувані замовлення, треті не перестали постачати міста електро- та теплоенергією. Держава та органи державної влади на місцях підійшли до питання виконання своїх зобов'язань з точки зору рівності у взаєминах. Якщо ще в січні місяці питання про залік взаємних зобов'язань сприймалися як неприйнятна альтернатива посилення фіскальної політики, то травень місяць приніс свої плоди. Розширилося коло заліку взаємних зобов'язань.

Методи боротьби з неплатежами якими користуються на рівні суб'єктів держави, великих підприємств, дрібних підприємств - це не більше ніж спроба вирішити проблему для самого себе, комплексного вирішення немає, та й не може бути. Проблему неплатежів має вирішувати уряд, і тільки воно. Чому така винятковість - очевидно. Криза платіжної системи проблема загальнодержавна, серед причин кризи питання є прерогативою Вищої виконавчої влади.

Як заходів по стабілізації платіжного клімату пропонується: формування необхідного обсягу розрахункових інструментів (на початкових етапах не гроші-сурогати. Сурогати є безінфляційним інструментом. Грошова емісія призведе до інфляції, т. К. Великий недолік коштів в економіці. Відволікання частини коштів з фінансового ринку); посилення контролю за обігом готівкової маси; відповідальність за порушення платіжної дисципліни.

Висновки до третього розділу:

Розглянуто електронні платіжні системи інтернету такі як Web Money, Яндекс Money, iMoney і PayPal.

Висвітлено проблеми платіжних систем України та запропоновано шляхи їх вдосконалення.

ВИСНОВКИ

У магістреській роботі отримано такі науково-практичні результати: проаналізовано основи безпеки електронної комерції, безкека електронних транзакцій в системах B2C та C2C. Визначено нові протоколи безпеки заочних платежів, та розглянуто проблеми та шляхи їх вирішення у платіжних системах України;

Електронні гроші з кожним днем стали захоплювати нашу повсякденну реальність, з якою, як мінімум, вже необхідно рахуватися. Звісно, ніхто в найближчі років п'ятдесят (напевно) не відмінить звичайні гроші. Але не вміти справлятися з електронними грошима і упускати ті можливості, які вони з собою несуть, - значить добровільно зводити навколо себе «залізну завісу», який з такою працею розсуваються за останні півтора десятка років. Багато великих фірм пропонують оплату своїх послуг і товарів через електронні розрахунки. Споживачеві ж це значно економить час.

Безкоштовне програмне забезпечення для відкриття свого електронного гаманця і для всієї роботи з грошима максимально адаптовано для масових комп'ютерів, і після невеликої практики не викликає у пересічного користувача ніяких проблем. Наш час - час комп'ютерів, Інтернет та електронної комерції. Люди, що володіють знаннями в цих областях і відповідними засобами, домагаються колосальних успіхів. Електронні гроші - гроші, які отримують все більш широке поширення з кожним днем, що відкривають все більше можливостей для людини, що має доступ в Мережу.

Так само розглянули інфраструктури безпеки і технологічні методи зниження ризиків в системах електронної комерції.