МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

“ На правах рукопису”
УДК

«До захисту допущено»
Завідувач кафедри СІКЗ
_____ Шуклін Г.В.
“____” _____2020 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 Кібербезпека

на тему: **ПЛАТІЖНІ КАРТКИ**

Студент групи СЗДМ-61 Луценко Михайло Миколайович _____
(підпис)

Науковий керівник: к.т.н., доцент. Ахрамович Володимир Миколайович
_____
(підпис)

Нормоконтроль: _____
(підпис)

Київ – 2020

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
к.т.н. Шуклін Г.В
“__” _____ 2019р.

З А В Д А Н Н Я

на магістерську атестаційну роботу

студенту Луценко Михайлу Миколайовичу

1. Тема роботи: Платіжні картки, керівник Ахрамович Володимир Миколайович, к.т.н., доцент., затверджені наказом вищого навчального закладу від “__” _____ 2019 року №____.

2. Термін здачі студентом оформленої роботи “___” _____ 20__ р.

3. Предмет дослідження: методика захисту платіжних карт.

4. Об’єкт дослідження: процес захисту платіжних карт.

5. Мета роботи: побудова методики оцінки захищеності платіжних карт.

6. Перелік питань, які мають бути розроблені:

1. Розглянути технічні канали захисту платіжних карт.
2. Розглянути безконтактні канали проведення операцій за допомогою платіжних карт.
3. Виконати аналіз роботи карт в банкоматах та платіжних терміналах.
4. Виконати дослідження методів захисту платіжних карт в системах банкомату та терміналу.
5. Розробити основні принципи та рекомендації по захисту платіжних карт.

7. Перелік публікацій:

8. Перелік ілюстративного матеріалу:

1. Презентація виконана на 12 слайдах для подання за допомогою оверхедів (світлопроекторів) та комп’ютерних засобів.

9. Дата видачі завдання “__” вересня 2019 р.

Керівник: Ахрамович Володимир Миколайович _____

Завдання прийняв до виконання: Луценко Михайло Миколайович _____

КАЛЕНДАРНИЙ ПЛАН

№ З\П	Назва етапів магістерської роботи	Строк вико-нання етапів	Примітка
1	**2**	**3**	**4**
1	Уточнення постановки завдання	до.	Виконано
2	Аналіз літератури	до.	Виконано
3	Обґрунтування вибору рішення	до	Виконано
4	Збір даних	до	Виконано
5	Написання першого розділу роботи	до.	Виконано
6	Написання другого розділу роботи	до	Виконано
7	Написання третього розділу роботи	до	Виконано
8	Написання четвертого розділу роботи	до	Виконано
9	Підготовка ілюстративного матеріалу	до	Виконано
10	Отримання рецензій	до	Виконано
11	Захист в ДЕК		

Студент М.М. Луценко

Науковий керівник В.М. Ахрамович

АНОТАЦІЯ

В роботі розглянуто основні технічні канали проведення операцій за допомогою платіжних карт, особливу увагу присвячено безконтактним системам проведення операцій, розглянуто методи і засоби захисту інформації при проведенні операцій по карткам, розглянуто методики захисту персональної інформації клієнтів, що зберігається на картках, проведено дослідження операцій по карткам від надходження запиту до банку, до фактичного списання коштів торгівельною мережею. На основі отриманих даних розроблено основні принципи захисту платіжних карт як в контактних системах звязку так і в безконтактних і зроблено відповідні висновки.

Робота складається зі вступу, чотирьох розділів, що містять 10 рисунків, 1 таблицю, виснову та списку використаних джерел, що містить 35 найменувань. Загальний обсяг роботи становить 90 аркушів.

АННОТАЦИЯ

В работе рассмотрены основные технические каналы проведения операций с помощью платежных карт, особое внимание посвящено бесконтактным системам проведения операций, рассмотрены методы и средства защиты информации при проведении операций по карточкам, рассмотрены методики защиты персональной информации клиентов, сохраняется на карточках, проведено исследование операций по карточкам от поступления запроса в банк, до фактического списания средств торговой сетью. На основе полученных данных разработаны основные принципы защиты платежных карт как в контактных системах связи так и в бесконтактных и сделаны соответствующие выводы.

Работа состоит из введения, четырех глав, содержащих 10 рисунков, 1 таблицу, виснов и списка использованной литературы, содержащий 35 наименований. Общий объем работы составляет 90 листов.

ANNOTATION

The main technical channels of transactions with payment cards are considered in the work, special attention is paid to contactless systems of conducting transactions, methods and means of protection of information during card transactions are considered, methods of protection of personal information of clients are considered, stored on cards, research of operations on cards from the receipt of the request to the bank, before the actual write-off of funds by the trading network. Based on the obtained data, the basic principles of payment card protection were developed both in contact and contactless systems, and the relevant conclusions were drawn.

The work consists of an introduction, four chapters containing 10 figures, 1 table, conclusions and a list of used literature, containing 35 titles. The total amount of work is 90 pages.

РЕФЕРАТ

Магістерська робота присвячена платіжним картам на методам їх захисту. В роботі виконано дослідження загальної нормативно-правової бази в сфері захисту інформації, розглянуто основні методи та принципи проведення операцій за допомогою платіжних карт.

Проведено дослідження наявних методів упередження загроз і засобів захисту платіжних карт. Розглянуто декілька основних методик захисту платіжних карт при роботі з банкоматом та термігалом. Виконано дослідження проведення операцій як в безконтактних системах проведення платежу, так і в звичайних системах.

Як заключення магістрської роботи було розроблено основні рекомендації по захисту платіжних карт.

Робота складається зі вступу, чотирьох розділів, що містять 10 рисунків, 1 таблицю, висновків та списку використаних джерел, що містить 25 найменувань. Загальний обсяг роботи становить 90 аркушів.

Об'єктом дослідження даної роботи є система захисту каналів звя'зку при здійсненні платежів за допомогою платіжних карток. **Предмет дослідження –** методика захисту платіжних карт. Мета роботи – є визначення загроз у технологіях звя'зку, аналіз методів попередження та усунення найбільш ймовірних небезпек при розрахунку картою.

Як результат у роботі виконано На основі отриманих даних розроблено основні принципи захисту платіжних карт як в контактних системах звязку так і в безконтактних і зроблено відповідні висновки.

Галузь застосування: результати досліджень можуть використовуватись в навчальному процесі для підготовки студентів відповідного напряму, в реалізації ліцензованими підприємствами відповідного напряму, а також в розробці нових методик оцінки.

Ключові слова: Інформація, безпека, платіжні картки, безконтактні платіжні карти, технології зв'язку, захист платіжних карток, банкомат, платіжна система, nfc системи.

ВСТУП ……..…….……..…

АНОТАЦІЯ……..

ANNOTATION …….....

РОЗДІЛ 1 ПЛАТІЖНІ СИСТЕМИ ТА КАРТКИ.....…….……...

1.1 Принципи функціонування електронних платіжних систем…...
1.2 Електронні плстикові карти …….....
1.3 Персональний ідентифікаційний номер ….....…
1.4 Типи шахрайства .....…..…….....

РОЗДІЛ 2 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ POS, ТА БАНКОМАТІВ.....

2.1 Системи терміналів (POS)…….....…….
2.2 Забезпечення безпеки банкоматів.....…….……..
2.3 Універсальна електронна платіжна система UEPS.....
2.4 Емісія платіжних карток.……..……..…….....

РОЗДІЛ 3 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ ЧЕРЕЗ МЕРЕЖУ INTERNET ….....……....
3.1 Основні види електронної торгівлі .....……..……....
3.2 Основні методи захисту інформації.....……..…...
3.3 Особливості функціонування протоколу SET ……...…….
3.4 Учасники системи розрахунків і криптографічні засоби захисту транзакцій.....…….....
3.5 Використання сертифікатів .....
3.6 Технологічні рішення для електронної торгівлі …….....

РОЗДІЛ 4 ОХОРОНА ПРАЦІ …….....
ВИСНОВКИ …….
СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ …….
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

EMV CCPS – Близькість платіжної системи навколишнього середовища
UCAF – Універсальний ідентифікаційний код власника картки
AAV – Значення автентифікації власника рахунку
CAVV – Значення підтвердження автентифікації власників картки
ACS – Домен постачальника послуг
RF – Радіо частота
ATM – Банкомат
MQ – Маскарадинг
URI – Уніфікований ідентифікатор ресурсу
FWT – Час очікування кадру
DoS – Відмова в Обслуговуванні
TCP – протокол управління передачею
ISO – Міжнародна асоціація стандартів
CRM – Система Управління Взаємозв'язками з Клієнтами
XML – Розширювана Мова Розмітки
AAUI – Активація програми для користувача інтерфейсу
POS – Торгывельний термінал
API – Інтерфейс програми програмування
FCI – Інформація про керування файлами
HCE – Емуляція держателя карти
PPSE – Близькість системи навколишнього середовища
RFID – Радіочастотна ідентифікація
NFC – Технологія ближнього поля
EMV – Протокол безпеки безконтактних платіжних карток
SEID – Ідентифікатор безпечного елемента

ВСТУП

З кожним роком кількість людей, які користуються банківськими картами, поступово збільшується. Вже не за горами той час, коли карта стане основним платіжним інструментом і практично повністю витіснить готівку з обігу (в цьому більше зацікавлені не самі люди і банки, а держава, так як безготівковий розрахунок легше контролювати). Безготівковий спосіб оплати по карті зручний і має масу переваг, він використовується в багатьох країнах не один десяток років. Але, на жаль, в даному питанні є і зворотна сторона. В першу чергу, це різного роду шахрайство з банківськими картами

Безконтактні платіжні картки - це картки, які використовують радіочастотну ідентифікацію (RFID) для здійснення безпечних платежів. Безконтактна платіжна технологія на кредитних картах, таких як PayPass MasterCard і PayWave Visa, використовує RFID, і дозволяє власникам карток пропускати свої карти перед безконтактними платіжними терміналами для завершення транзакцій.

Всі платіжні картки використовують один і той же протокол спеціальний протокол зв'язку безконтактного зв'язку EMV (EMV CCPS) для зв'язку з пристроями, що активують зв'язок (NFC). Однак EMV CCPS використовується для фізичної зв'язку між терміналом та платіжною картою, і відрізняється від протоколу власних платежів.

Розділ 1
ПЛАТІЖНІ СИСТЕМИ ТА КАРТКИ

1.1. Принципи функціонування електронних платіжних систем.

Електронна платіжна система - Платіжна система (або платіжно-розрахункова система) - це сукупність ресурсів, що використовуються для переказу грошей між фінансовими установами. Банк міжнародних розрахунків (BIS, що розшифровується як Bank for International Payment) визначає платіжну систему як "засіб, за допомогою якого перераховуються кошти між банками".

Пластикова карта - це персоніфікований платіжний інструмент, що дає держателю карти можливість проводити операції безготівково для придбання товарів і послуг, а також отримання готівкових коштів в банківських автоматах і відділеннях банків. Підприємства торгівлі та сервісу та відділення банків, які беруть карту як платіжний інструмент, утворюють *приймальню мережу точок обслуговування* картки.

При створенні платіжної системи однією з основних вирішуваних завдань є вироблення і дотримання загальних правил обслуговування карток, випущених емітентами, що входять в платіжну систему, проведення взаєморозрахунків і платежів. Такого роду правила впливають безпосередньо на технічні аспекти операцій з картами - стандарти систем даних, процедури проведення авторизації, специфікації щодо обладнання та інші, так і фінансові аспекти обслуговування карт - процедури проведення розрахунків з підприємствами що проводять торгівлю і сервіс, вони входять до складу приймальної системи, правила та норми по взаєморозрахункам між банками і т.п.

Ядром платіжної системи,з організаційної точки зору, є асоціація банків, об'єднана договірними зобовязаннями. Крім того, до складу електронної

платіжної системи входять підприємства торгівлі та сервісу, ці підприємства утворюють мережу точок, що здійснюють обслуговування. Для корректного функціонування платіжної системи відіграють дуже важливу роль спеціалізовані організації по здійсненню технічної підтримки по обслуговуванню платіжних карт: процесингові центри, центриналаштування комунікацій, центри що спеціалізуються на технічному прослуховуванні і т.п.

Узагальнена схема функціонування електронної платіжних системи представлена на рис. 1 . Банк, який уклав угоду з платіжною системою і отримав відповідну ліцензію, може виступати в двох якостях - як банк-емітент і як банк-еквайєр. *Банк-емітент* випускає пластикові картки та гарантує виконання фінансових зобов'язань, пов'язаних з використанням цих карток як платіжних засобів. *Банк-еквайєр* обслуговує підприємства торгівлі і сервісу, які приймають до оплати карти як платіжні засоби, а також приймає ці платіжні засоби до переведення в готівку в центральних своїх відділеннях і через банкомати, що йому належать. Основними платіжними функціями, що проводить банк-еквайр є фінансові операції, пов'язані з проведенням розрахунків і платежів точками обслуговування. Технічні атрибути діяльності банку-еквайра (обробка запитів на авторизацію; взаємо розрахунок проведених коштів на розрахункові рахунки торгівельних мереж коштів, що призначені для товарів та послуг, та були проведені через картки; прийом, відсортовування і пересилання документів, які фіксують проведення угод з використанням карт і т.п.) можуть бути делегірувані еквайєром процесингових центрів.

Неавтоматизована процедура прийому платежу з допомогою карти порівняно проста. В першу чергу касир підприємства повинен переконатися в достовірності пластикової карти по ряду ознак. При оплаті підприємство повинно перенести реквізити пластикової картки клієнта на спеціальний чек з допомогою копіювальної машини-імпринтера, занести в чек суму, на яку його було придбано або ока зана послуга, і отримати підпис клієнта. Оформлений подоб ним чином чек називають *сліпом.*

В цілях забезпечення безпеки операцій платіжної системи рекомендується не перевищувати нижні ліміти сум для різних регіонів і видів бізнесу, за якими можна прово дить розрахунки без авторизації. При перевищенні лімітної суми або в разі виникнення сумніву в особистості клієнта перед прийняття має проводити *процедуру авторизації.* При авторизованого зації підприємство фактично отримує доступ до інформації про стан рахунку клієнта і може встановити приналежність кар ти клієнтові і його платіжну спроможність в розмірі суми угоди. Одна копія сліпа залишається на підприємстві, другий передається клієнту, третя доставляється в банк-еквайєр і служить підставою для відшкодування суми платежу підприємству з рахунку клієнта.

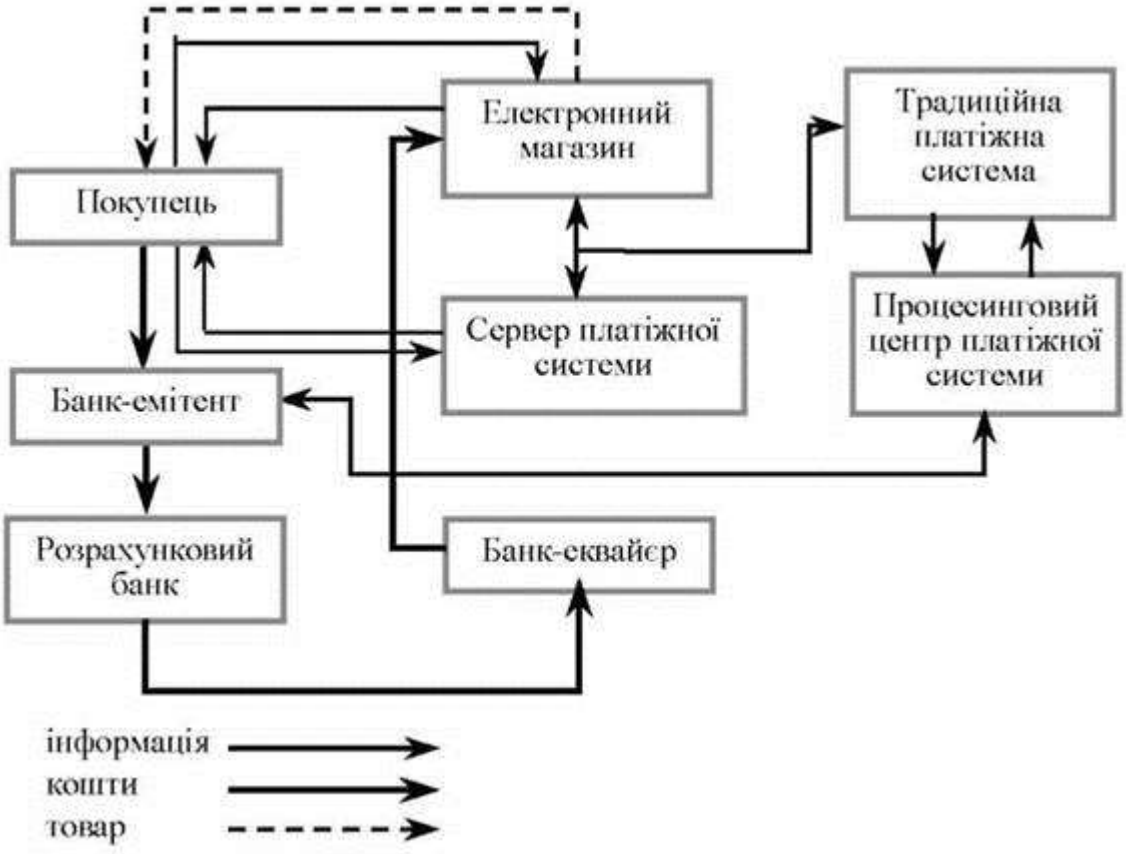


Рис. 1. Узагальнена схема функціонування електронних платіжних систем

В останні роки широку популярність придбали *автоматизовані торгові POS -термінали* (Point-Of-Sale -оплата в точці продажу) і банкомати.

При використанні POS - терміналів немає необхідності в заповненні сліпів. Реквізити та пластикової карти зчитуються з її магнітної смуги на вбудованому в POS -термінал зчитувачі. Клієнт вводить в термінал свій PIN-код (Personal Identification Number - персональний ідентифікаційний номер), відомий тільки йому. Елементи PIN -коду включаються в загальний алгоритм шифрування запису на магнітній смузі і служать електронним підписом власника карти. На клавіатурі POS - терміналу набирається сума угоди .

Якщо угода здійснюється в відділенні банку і в процесі відбувається видача клієнту готівки грошей , крім банківських POS - терміналів може бути використаний *електронний касир - банкомат.* Конструктивно він являє собою автоматизований сейф зі вбудованим POS - терміналом .

Термінал через вбудований модем звертається за авторизованим посиланням в відповідну платіжну систему. При цьому використовуються потужності процесингового центру, послуги якого надаються торговцю банком - еквайром.

Процесинговий центр представляє собою спеціалізовану сервісну організацію, яка забезпечує проведення обробки запитів які надійшли від банків - еквайєрів або особисто з торгівельних мереж та мереж, що проводять обслуговування на авторизацію і технічна обробка протоколів транзакцій - фіксують данні про вироблених за допомогою пластикових карт платежах і видачі готівкових коштів. Зокрема процесінговий центр має базу даних, яку від обслуговує і там тримаються дані про банки – члени, що входять до платіжної системи і власники пластикових банківських карт. Процесинговий центр обробляє та зберігає дані, де вказані ліміти власників карт і виконує запити на проведення авторизації, якщо банк - емітент не має технічних можливостей вести власну базу даних (банк offline). В іншій ситуації (банк online) процесинговий центр проводить пересилку отриманих даних по запиту в банк-емітент карти, верифікація якої щойно проходить. Фактично процесинговий центр займається забезпеченням і пересилкою відповіді до банку, що обслуговую торгівельну мережу – банк еквайєр.

Банком-еквайр, що виконує свої функцій проводить розрахунки з банками-емітентами. Кожен банк, що проводить придбання, банк-еквайер, для здійснення переказу коштів до пунктів обслуговування платежів власників карток банків-емітентів, які включені до Платіжної системи. Тому відповідні кошти повинні бути передані банку-еквайеру банком-емітентом. Більш швидкі розрахунки платежів між торгівельними мережами та емітентами забезпечується наявністю в платіжній системі кореспонденського, розрахункового банку (один, або декілька банків), в якому банки-члени системи відкривають кореспондентські рахунки. На основі протоколів транзакцій, знятих у день транзакції, центр обробки готує та поширює кінцеві дані для розрахунків між учасниками платіжної системи, а кожен формує та розповсюджує безпосередньо до банків-одержувачів стоп листи (переліки карток, операції по яких по різним причинам були скасовані, або призупинені).

Процесорний центр також може забезпечити споживання банків-емітентів новими картками, розміщення замовлень на заводах. Що їх виготовляють, та подальшу персоналізацію цих карт. Особливістю проведення продажів та видачі готівкових коштів по пластиковим карткам є те, що ці фінансові операції здійснюються торгівельними мережами (магазинами) та банківськими структурами "в борг", тобто товари і готівкові кошти отримуються клієнтом на руки в той же час, а кошти на їх погашення надходять на розрахунковий рахунок при обслуговуванні підприємств та торгівельних мереж через певний час (як правило декілька днів). Гарантом виконання платіжних зобов'язань, що можуть виникнути в процесі проведення обслуговування пластикових банківських карт, являється банк, що іх випустив, а це банк-емітент. Характер та розмір гарантій, що надає банк-емітент залежить від типу клієнта, якому були надані платіжні повноваження, ці повноваження фіксуються видом картки та типом договору що заключив банк та клієнт, що отримав карту.

За видом розрахунків, виконуваних з допомогою пластикових карт, розрізняють кредитні та дебетові карти.

Кредитні карти є найбільш поширеним видом пластикових карт. До них відносяться карти загальнонаціональних систем США Visa і MasterCard, American Express і ряду інших. Ці карти пред'являють на підприємствах торгівлі і сервісу для оплати товарів і послуг. При оплаті з допомогою кредитних карт банк покупця відкриває йому кредит на суму покупки, а потім через деякий час (зазвичай 25 днів) надсилає рахунок. Покупець повинен повернути сплачений чек (рахунок) назад в банк. Природно, подібну схему банк може запропонувати тільки найбільш заможним і перевіреним з своїх клієнтів, які мають хорошу кредитну історію перед банком або солідні вкладення в банк в вигляді депозитів, цінностей або нерухомості.

Тримач дебетової карти має вносити заздалегідь на свій рахунок в банку-емітенті певну суму. Об’єм цієї суми визначає розмір ліміту коштів, які доступні клієнту. В момент здійснення розрахунків з допомогою цієї карти відповідно до використання зменшується і ліміт. Контроль ліміту виконується при проведенні авторізації, авторизація в момент використання дебетової карти є обов'язковою процедурою. Для встановлення або збільшення ліміту тримачу карти необхідно провести внесення коштів на свій розрахунковий рахунок. Для страхування тимчасового розриву між моментом здійснення платежу і моментом отримання банком відповідної інформації на рахунку клієнта повинен підтримуватися незнижуваний залишок .

Кредитна та дебетова картки можуть бувають НЕ тільки персональними, але і корпоративними банківськими картами. Корпоративні банківські карти надаються компанією своїм співробітникам для проведення оплати до відрядні або інших витрат по службовим потребам. Корпоративні банківські картки компанії обєднані з одним або декількома рахунками в банку цієї компанії. Ці карти можуть мати розподілений або неподілений ліміт. В першій ситуації кожному з держателів корпоративних банківських

карт встановлюється індивідуальні ліміти. В другій ситуації підхід до встановлення лімітів підходить невеликим фінансовим організаціям і не передбачає розмежування ліміту.

В останні роки все більше уваги приділяють електронним платіжним системи, що використовують мікропроцесорні (смарт) карти. Принциповим відмінністю мікропроцесорних карт від всіх інших платіжних карт є те, що вони несуть особисту інформацію про стан рахунку клієнта держателя карти, по суті вони є транзитним рахунком. Всі транзакції відбуваються в режимі off - line в процесі діалогу карта - термінал або карта клієнта - карта торговця.

Така система є майже повністю безпечною завдяки високою мірою захищеності кристала з мікропроцесором і повної дебетової схемою розрахунків. Крім того, хоча карта з мікропроцесором дорожче звичайної, для платіжної системи це дешевше в експлуатації за рахунок того, що в режимі off-line немає навантаження на телекомунікації.

Для забезпечення надійної роботи електронна платіжна система повинна бути надійно захищена.

З точки зору інформаційної безпеки в системах електронних платежів існують такі вразливі місця :

- Пересилання платіжних і інших повідомлень між банком і клієнтом і між банками ;
- Обробка інформації всередині організацій відправника і по лучателя повідомлень ;
- Доступ клієнтів до засобів , акумульованих на рахунках .

Одним з найбільш вразливих місць в системі електронних платежів є пересилання платіжних і інших повідомлень між банками, між банком і банкоматом, між банком і кліентом . Пересилання платіжних і інших повідомлень пов'язана із наступними особливостями :

- Внутрішні системи організацій відправника і одержувача повинні бути пристосовані для відправки і отримання електронних документів і

забезпечувати необхідну захист при їх обробці всередині організації (захист кінцевих систем);

- Взаємодія відправника і одержувача електронного документа здійснюється опосередковано - через канал зв'язку. Ці особливості породжують такі проблеми :
- Взаємне пізнання абонентів (проблема встановлення взаємної справжності):
- Захист електронних документів, переданих по каналах зв'язку (проблеми забезпечення конфіденційності і цілісності документів);
- Захист процесу обміну електронними документами (проблема докази відправлення і доставки документа) ;
- Забезпечення виконання документа (проблема взаємного НЕ довіри між відправником і отримувачем з - за їх приналежності до різних організаціям і взаємної незалежності).

Для забезпечення функцій, що відповідають за захисту інформації на окремих них вузлах системи електронних банківських платежів повинні бути реалізовані наступні механізми захисту :

- Управління доступом на кінцевих системах ;
- Контроль цілісності повідомлення ;
- Забезпечення конфіденційності повідомлення ;
- Взаємна аутентифікація абонентів ;
- Неможливість відмови від авторства повідомлення ;
- Гарантії доставки повідомлення ;
- Неможливість відмови від прийняття мёр по повідомленням ;
- Реєстрація послідовності повідомлень ,
- Контроль цілісності послідовності повідомлень .

Якість рішення зазначених вище проблем в значній мірі визначається раціональним вибором криптографічних засобів при реалізації механізмів захисту.

1.2. Електронні пластикові картки

Пластикова карта має в своїй основі пластину із спеціального пластику стандартних розмірів (85,6 х 53,9 х 0,76 мм), спеціальний пластик виготовлений із стійкої до механічних пошклджень і термічних впливів пластмаси. Основнна функція пластикової банківської карти - забезпечення ідентифікації користувача, що її використовує як суб'єкт що належить платіжній системі. Для цієї цілі на пластикову карту наносять лого типи банку-емітента і платіжної системи, що проводить обслуговування по цій картці, ім'я держателя карти, номер рахунку клієнта, термін дії карти і т.п. Інколи, на карті може бути присутнім фотографій власника та підпис клієнта. Алфавітно-цифрові дані - ім'я та номер рахунку клієнта, все це може бути ембосовано банком, що обслуговує клієнта, т.е . нанесені методом рельєфного шрифту. Це дає можливість при ручний обрабоці карток, що були прийняті до оплати, швидко перенести дані на касовий чек за допомогою спеціального пристрою, що називається імпринтером, проводять процедуру "прокатування" картки (процес аналогічно отримання другого екземпляру при використанні паперу для копіювання).

За принципом дії бувають пасивні та активні пластикові карти. Пасивні пластикові карти всього лише зберігають інформацію на тому чи іншому носії. До них відносяться пластикові карти з магнітною смугою.

На магнітних картках, що використовуються для фінансових операцій, є до трьох треків, відомих як треки 1, 2 і 3. Доріжка 3 практично не використовується основними світовими мережами, такими як VISA, а часто навіть фізично не присутній на картці завдяки більш вузькому магніту смуга. Зчитувачі карт торгових точок майже завжди читають трек 1 або трек 2, а іноді і те й інше, якщо одна доріжка не читається. Мінімальна необхідна інформація про рахунок власника картки для завершення транзакції присутній на обох треках. Доріжка 1 має більш високу щільність бітів (210 біт на дюйм проти

75) - це єдиний трек, який може містити алфавітний текст, а значить, і єдиний доріжка, яка містить ім'я власника картки.

Доріжка 1 записується з кодом, відомим як DEC SIXBIT плюс непарний паритет. Інформація про доріжку 1 на фінансових картках міститься у кількох форматах: A, який зарезервований для власного використання емітента картки B, що описано нижче, CM, які зарезервовані для використання ANSI

Підкомітет X3B10 та NZ, які доступні для використання окремими емітентами карт:

Доріжка 1, формат B:

- Почати дозорну - один символ (як правило, '%')
- Код форматування = "B" - один символ (лише альфа)
- Номер основного рахунку (PAN) - до 19 символів. Зазвичай, але не завжди, відповідає номеру кредитної картки, надрукованому на передній частині картки.
- Сепаратор поля - один символ (загалом '^')
- Ім'я - від двох до 26 символів
- Сепаратор поля - один символ (загалом '^')
- Дата придатності - чотири символи у формі YYMM.
- Службовий код - три символи
- дискреційні дані - можуть містити індикатор ключа підтвердження PIN-коду (PVKI, 1 символ),

Значення підтвердження PIN-коду (PVV, 4 символи), значення підтвердження картки або карта

Код підтвердження (CVV або CVK, 3 символи)

- Кінцевий дозор - один символ (як правило, '?')
- Перевірка поздовжньої надмірності (LRC) - це один символ та символ дійсності розраховано з інших даних на трасі. Більшість пристроїв зчитування не повертають цього значення коли карта перенесена на рівень

презентації, і використовуйте її лише для перевірки введення внутрішньо для читача.

Доріжка 2: Цей формат був розроблений банківською галуззю (ABA). Цей трек написано с 5-бітова схема (4 біти даних + 1 паритет), яка дозволяє отримати шістнадцять можливих символів, що чисел 0-9 плюс шість знаків: <=>? Підбір шести пунктуаційсимволи можуть здатися дивними, але насправді шістнадцять кодів просто відображаються в діапазоні ASCII 0x30 через 0x3f, що визначає десятизначні символи плюс ці шість символів. Формат даних є наступним чином:

- Почати дозорну - один символ (загалом ';')
- Номер основного рахунку (PAN) - до 19 символів. Зазвичай, але не завжди,

відповідає номеру кредитної картки, надрукованому на передній частині картки.

- роздільник - один знак (загалом '=')
- Дата придатності - чотири символи у формі YYMM.
- Службовий код - три цифри. Перша цифра вказує правила обміну, друга

вказує обробку авторизації, а третя визначає коло послуг

- Дискреційні дані - як у трековій
- Кінцевий дозор - один символ (як правило, '?')
- Перевірка поздовжньої надмірності (LRC) - це один символ та символ дійсностірозраховано з інших даних на трасі. Більшість пристроїв зчитування не повертають цього значення коли карта перенесена на рівень презентації, і використовуйте її лише для перевірки введеннявнутрішньо для читача.

Значення службових кодів, поширені у фінансових картках:

Перша цифра

1: Міжнародний обмін ОК

2: Міжнародний обмін, використовуйте IC (чіп), де це можливо

5: Національний обмін тільки за винятком двосторонньої угоди

Сторінка 6

6: Національний обмін тільки за винятком двосторонньої угоди, використовуйте IC (чіп) де

здійсненний

7: Ні обміну, крім двосторонньої угоди (закритий цикл)

9: Тест

Друга цифра

0: Нормально

2: Зверніться до емітента через Інтернет-засоби

4: Зверніться до емітента через Інтернет, за винятком двосторонньої угоди

Третя цифра

0: Ніяких обмежень, PIN-код не потрібно

1: Без обмежень

2: Тільки товари та послуги (без готівки)

3: Тільки банкомат, потрібен PIN-код

4: Тільки готівкою

5: Тільки товари та послуги (без готівки), PIN-код не потрібно

6: Без обмежень, використовуйте PIN-код, де це можливо

7: Тільки товари та послуги (без готівки), використовуйте PIN-код, де це можливо

Усі значення, не прямо вказані вище, зарезервовані для подальшого використання

Примітки:

- Ці полоси можна повністю стерти, якщо наблизити до високої міцності

Неодимові магніти комерційні кодери можуть використовувати '~' для запуску дозорного, ';' для сепаратора.

- Приклад коду: '~ #; дані? '

Інші типи карт

Смарт-карти - це картки нового покоління, що містять мікросхем інтегральної мікросхеми. Картка можуть мати металеві контакти, які фізично з'єднують картку з читачем, при цьому безконтактні карти використовують магнітне поле або радіочастоту (RFID) для зчитування близькості.

Гібридні смарт-карти на додаток до чіпа включають магнітну смужку - це найчастіше знайдені в платіжній картці, так що картки також сумісні з платіжними терміналами, які не включайте зчитувач смарт-карт.

Картки з усіма трьома можливостями: магнітна смуга, чіп смарт-карти та чіп RFID що стає загальним, оскільки для більшої діяльності потрібні такі картки Карти з мікросхемою можна класифікувати по НЕ скільком ознаками .

*Перша ознака - функціональні можливості карти***.** Тут можна виділити Основні типи платыжних банкывських карт:

• карти з лічильником ;

• карти з пам'яттю ;

• карти з мікропроцессором .

Другою ознакою э тип обміну даних із зчитуючим пристроєм:

• карти з технологією контактного зчитування ;

• карти з технологією індукційного зчитування .

Карти з лічильником застосовуються, в багатьох випадках, в тих ситуаціях, коли та чи інша платіжна операція потребує зменшення кількості залишку на рахунку власника карти на певну затверджену суму. Такі карти використовуються та застосовуються в спеціалізованих додатках з функцією передоплати (плата за використання мобільного звязку, оплата товарів і т.п.) Очевидно, що застосування карт із технологією лічильника обмежена і не передбачає великої перспективи.

Карти з пам'яттю є перехідним єтапом між картами з технологією лічильника і картами з мікропроцесором. Карта з пам'яттю - це жорстка карта з лічильником, в якій прий ти заходи, що підвищують її рівень захищеність від стандартних атак зловмисників. У найпростіших карт, що вже існують обсяг пам'яті цих карт може становити від 256 байт до 128 кілобайт. Цей тип пам'яті може бути реалізованих або в вигляді програмованого постійного запомятовуючого пристрою ППЗП (EPROM), що допускає од нократно запис і багаторазове зчитування з цієї карти, або в вигляді електрично перетворювача програмованого постійного пристрою, що запам'ятовує ЕСППЗУ (EEPROM), що допускає багаторазову за пись і багаторазове зчитування.

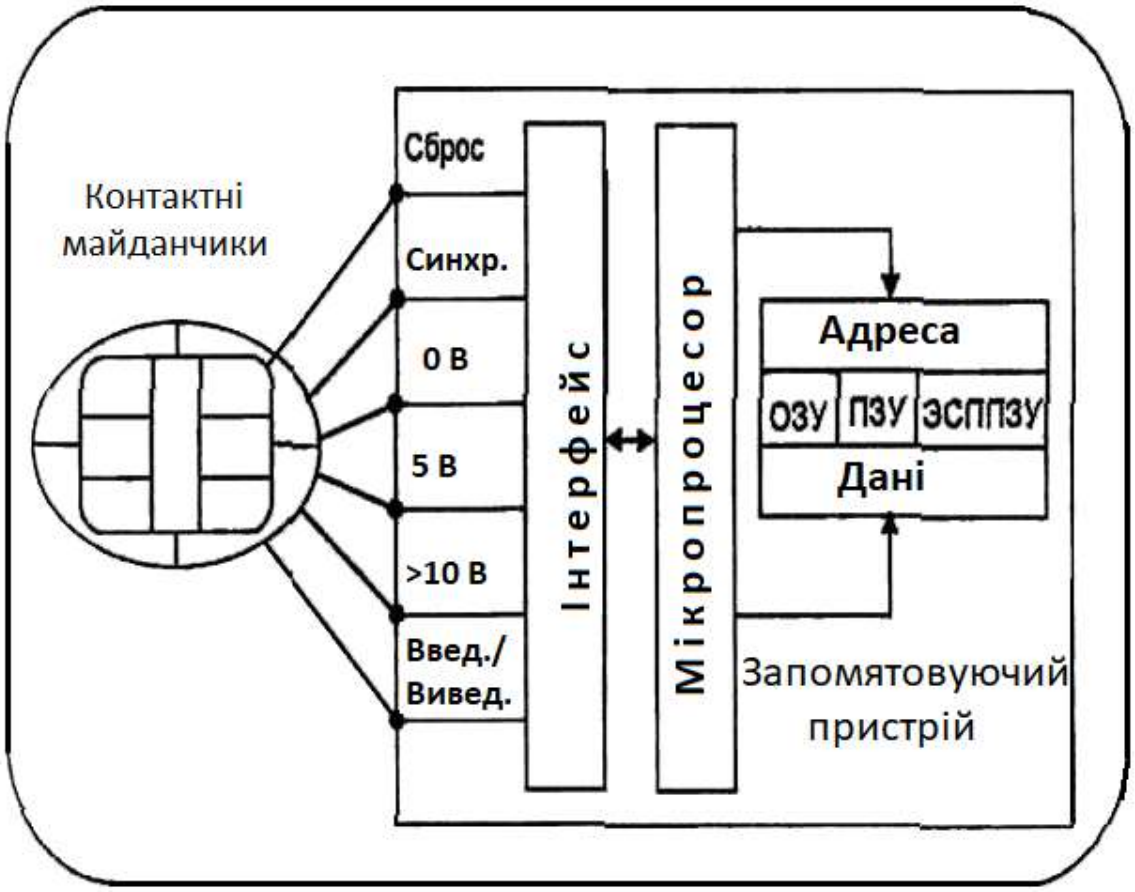
Карти з пам'яттю можна поділити на два типи з НЕ захищеної (полнодоступной) і захищени видом пам'ятті.

У картах першого типу немає ніяких обмежень на читання і запис даних Їх не можна використовувати в якості платіжних, так як фахівець середньої кваліфікації може їх досить просто " зламати ".

Карти другого типу мають область ідентифікаційних даних і одну або кілька прикладних областей. Ідентифік ционная область карт допускає лише одноразову запис при персоналізації і в подальшому доступна лише для зчитування. Доступ до прикладних областей регламентується і здійснюється тільки при виконанні певних операцій, зокрема при введенні секретного PIN -коду.

Рівень захисту карт з пам'яттю вище, ніж у магнітних карт, і вони можуть бути використані в прикладних системах, в яких фінансові ризики, пов'язані з шахрайством, відно сительно невеликі. Як платіжний засіб карти з пам'яттю використовуються для оплати таксофонів загального користування, проїзду в транспорті, в локальних платіжних системах (клубні карти) Карти з пам'яттю застосовуються також в системах допуску в приміщення і доступу до ресурсів комп'ютерних мереж (ідентифікаційної карти). Карти з пам'яттю мають більш низьку вар тість в порівнянні з картами з мікропроцесором

Карти з мікропроцесором називають також інтелекту альних картами або смарт-картами (smart cards). Карти з мікро процесором є по суті мікро-комп'ютери і зі тримають все відповідні основні апаратні компоненти центральний процесор (ЦП), оперативний запам'ятовуючий пристрій (ОЗУ), постійний запам'ятовуючий пристрій (ПЗП) і електронно стираючий програмований ПЗУ (ЕСППЗУ) (мал. 2).



Мал 2 . Архітектура смарт-карти

В даний час в смарт-карти встановлюють компоненти:

• Мікропроцесори з текстовою частотою до 200 МГц ;

• Оперативний ЗП ємністю до 64 Кбайт,

• Постійне ЗП ємністю до 512 Кбайт ;

• Незалежне ЗП ємністю до 32 Кбайт .

У ПЗУ записаний спеціальний набір технічних програм, звичайною операційної системою карти COS (Card Operation System). Операціцна сис-

тема має підтримку файлової системи, що базується в ЕСППЗУ (ємність якого перебуває в діапазоні 8 ... 56 Кбайт, але може досягати і 256 Кбайт) і забезпечувати регламентацію доступу до даними. При цьому частина даних може бути доступна тільки внутрішнім програмам картки.

Смарт - карта забезпечує великий набір функцій :

- розмежування повноважень доступу до внутрішнім ресурсам (завдяки роботі з захищеною файловою системою);
- шифрування даних з застосуванням різних алгоритмів ;
- формування електронної цифрової підписи ;
- ведення ключовий системи ;
- виконання всіх операцій взаємодії власника карти , банку і торговця .

Деякі карти забезпечують режим " самоблокировки " (неможливість подальшої роботи з нею) при спробі несанк ціонірованного доступу. Смарт - карти дозволяють істотно спростити процедуру ідентифікації клієнта. Для перевірки PIN - коду застосовується алгоритм , реалізований мікропроцесором на карті. Це дозволяє відмовитися від роботи POS - терміналу і бан Комата в режимі реального часу і централізованої перевірки PIN. Зазначені вище особливості роблять смарт-карту високо захищеним платіжним інструментом, який може бути ис користування мож в фінансових додатках, що пред'являють підвищена шенние вимоги до захисту інформації. Саме тому мик ропроцессорние смарт - карти розглядаються в даний час як найбільш перспективний вид пластикових карт .

За принципом взаємодії зі зчитує устройст вом розрізняють карти двох типів:

- карти з контактним зчитуванням ;
- карти з безконтактним зчитуванням .

Карта з контактним зчитуванням має на своїй по поверхні 8 ... 10 контактних пластин. Розміщення контактних пластин, їх кількість і призначення висновків різні у різних виробників і природно, що зчитувачі для карт даного типу розрізняються між собою.

В останні роки почали широко застосовуватися карти з безконтактним зчитуванням. У них обмін даними між картою і зчитує пристроєм проводиться індукційним спо собом. Очевидно , що такі карти надійніше і довговічніше.

Персоналізація та авторизація карт - важливий етап підготовки! Використання пластикових карток.

Персоналізація картки здійснюється при видачі картки клієнту. При цьому на картці записуються дані, що дозволяє ідентифікувати карту та її власника, а також підвищити купівельну здатність картки при прийнятті її на оплату чи видачі готівки.

Для авторизації вони розуміють процес затвердження матеріалів про продаж або видачі готівки на картці. Для авторизації сервісний пункт звертається із запитом до платіжної системи про підтвердження ДЖЕНІ авторитетом власника картки та його візових віз FINANCIAL. Технологія авторизації залежить від типу картки, схеми платіжної системи та технічного обладнання пункту обслуговування.

Історично початковим способом персоналізації карток було тиснення.

Тиснення - це процес тиснення даних на пластичній основі картки. Як правило, на картках банків-емітентів викарбувано такі дані:

• номер картки;

• дайте штепсельну вилку та закінчується термін дії;

• прізвище та ім'я власника.

Деякі платіжні системи, наприклад Visa, що вимагають тиснення двох спеціальних символів, однозначно визначають право власності банку-емітента на платіжну систему. Ембоссери (пристрої для тиснення рельєфу на карті) створюють обмежене коло віробників. У ряді західних країн законодавство забороняє вільний продаж тиснення. СПЕЦІАЛЬНІ символи, які підтверджують, що картка належить до тієї чи іншої платіжної системи, доставляються власникові тиснення лише з дозволу керівного органу платіжної системи. Рельєфна картка може слугувати платіжним засобом під час відбиття

візитів - пристрою для прокатки штор (чек), що підтверджує ідеальну платіжну операцію.

Персоналізація карт включає магнітну смугу, що кодує шкури або програмування мікросхеми.

Кодування магнітної смуги здійснюється, як правило, на тому ж обладнанні, що і тиснення. При цьому частина інформації про картку, яка містить номер картки та період її дії, як на магнітній смузі, так і на рельєфі. Однак бувають ситуації, коли після первинного кодування необхідно додатково вводити інформацію на магнітні доріжки. У цьому випадку використовуються спеціальні пристрої з функцією «читати - писати». Це можливо, зокрема, коли PIN-код для використання картки НЕ генерується спеціальною програмою, але може бути обраний клієнтом на власний розсуд.

Програмування мікросхеми НЕ особливо вимагає цих технологічних прийомів, але в них є деякі організації Onni Features. Зокрема, для підвищення безпеки та включення можна натрапити на програмні операції різних областей мікросхеми і географічно розділені та окреслені правами іноземців, які приймаються в цьому процесі.

Зазвичай ця процедура поділяється на три етапи:

- Активація картки розпочинається на першому робочому місці (введення її в дію)
- на іншому робочому місці циркулюють операції, пов'язані із безпекою;
- На третьому робочому місці персональна картка персоналізована.

Традиційно процес авторизації здійснюється або "вручну", коли продавець або касир передає запит по телефону оператору (авторизація голосу), або автоматично, коли карта розміщена в POS-терміналі, дані зчитуються з картка, касир вводить суму платежу, а власник картки зі спеціальною клавіатурою - секретний PIN-код. Після цього термінал здійснює авторизацію або шляхом встановлення зв’язку з базою даних Платіжної системи (он-лайн режим), або шляхом здійснення додаткового обміну цим самою карткою (авторизація в режимі офлайн). Що стосується зняття готівки, процес має подіб-

ний характер, з єдиною особливістю, що гроші в автоматичному режимі видаються спеціальним розширенням - банкоматом, який дає право на авторизацію. Щоб захистити картки від підробки та надалі несанкціоновано! Застосування Використовуйте різні методи та заходи. Наприклад, щоб персоналізувати картки, чорно-білі або кольорові фотографії власника картки термодруком можуть бути зафарбовані на пластиковій основі. На будь-якій картці завжди є спеціальна смужка із зразками підпису власника картки. Для захисту картки як такої різні платіжні спільноти використовують СПЕЦІАЛЬНІ об'ємні зображення на передній і задній сторонах картки (голограми).

1.3. Персональний ідентифікаційний номер.

Випробуваним і вірним способом ідентифікації власника банківської карти є використання секретного персонального PIN-коду. Значення PIN-коду має бути тільки від власника карти. Довжина ПІН-коду повинна бути досить високою, щоб ймовірність вгадати зловмисника з правильним значенням за допомогою повної атаки була досить мала. З іншого боку, довжина PIN-коду повинна бути досить короткою, щоб власники карт могли запам'ятати його значення. Рекомендована довжина ПІН-коду становить 4 ... 8 десяткових цифр, але може досягати 12.

Припустимо, що PIN-код складається з чотирьох цифр, і тоді противник, який намагається зіставити PIN-код з банківською картою, стикається з проблемою вибору одного з десяти тисяч варіантів. Якщо кількість спроб введення невірного значення PIN-коду обмежена п'ятьма на карту в день, у цього противника є шанс на успіх менше 1: 2000. Але на наступний день противник може спробувати знову, і його шанси зростуть до 1: 1000. Кожен наступний день збільшує ймовірність успіху проти псевдоніма. Тому багато банків накладають абсолютне обмеження на кількість невірних спроб введення ПІН-коду на карту, щоб виключити атаку будь-якого роду. Якщо ліміт перевищено, ця карта вважається невірною і обрана.

Значення ПІН-коду однозначно пов'язане з відповідними атрибутами банківської карти, тому ПІН-код можна інтерпретувати як підпис власника картки. Щоб ініціювати транзакцію, власник карти за допомогою POS-терміналу вставляє свою картку в спеціальний слот зчитувача і вводить свій ПІН-код за допомогою спеціальної термінальній клавіатури. Якщо введене значення ПІН-коду і номер рахунку клієнта, записані на магнітній смузі карти, збігаються, то ініціюється транзакція.

Захист персонального PIN-коду вашої банківської карти має вирішальне значення для безпеки всієї платіжної системи. Банківські картки можуть бути втрачені, вкрадені або підроблені. У таких випадках єдиною контрзаходом проти несанкціонованого доступу залишається секретне значення PIN-коду. Ось чому відкритий PIN-код повинен бути відомий тільки законному власникові картки. Він ніколи не зберігається і не передається через систему електронних платежів. Очевидно, що значення PIN-коду має зберігатися в секреті протягом усього терміну дії карти.

Метод ПІН-коду робить істотний вплив на безпеку системи електронних платежів. Як правило, персональні ідентифікаційні номери можуть генеруватися як банком, так і власниками карт. Зокрема, клієнт розрізняє два типу PIN-коду:

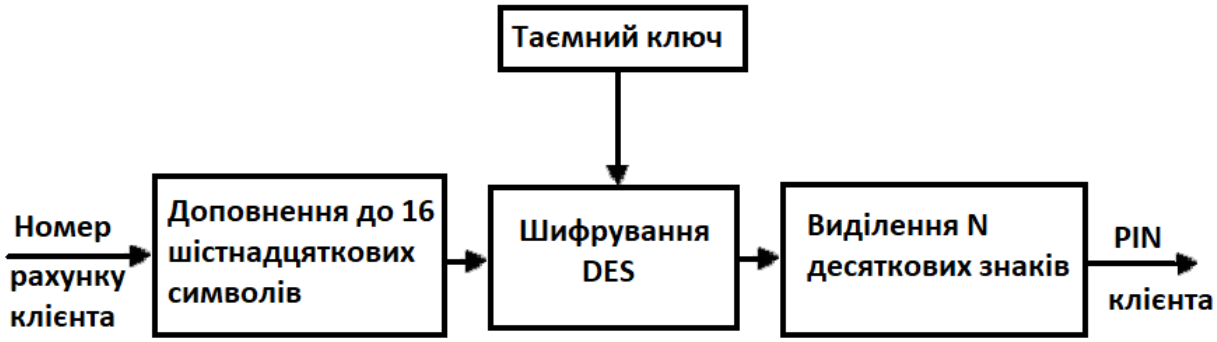
• ПІН-код, присвоєний йому банком-емітентом карти;

• PIN-код, обраний власником карти самостійно.

Якщо ПІН призначається банком, банк зазвичай використовує одну з двох опцій для процедур генерації ПІН.

У першому варіанті ПІН-код генерується криптографически з номера рахунку власника картки. Процес генерації ПІН-коду за номером рахунку показаний на рис. 3. Спочатку номер рахунку клієнта доповнюється нулями або інший константою до 16 шістнадцяткових цифр (8 байтів). Потім отримані 8 байтів шифруються DES з використанням секретного ключа. З отриманого зашифрованого тексту довжиною 8 байт відокремлюються 4-бітові блоки, починаючи з молодшого байта. Якщо число, сформований цими бітами, ме-

нше 10, результуюча цифра включається в СІН, в іншому випадку це значення НЕ використовується. Всі 64 біта (8 байтів) обробляються таким чином. Якщо в результаті неможливо отримати відразу необхідну кількість десяткових цифр, то вони перетворюються в невикористовувані 4 довічних блоку, з яких віднімають10.



Мал. 3 . Схема виведення PIN з номера рахунку клієнта

Очевидно, перевага цієї процедури полягає в тому, що значення ПІН-НЕ потрібно зберігати всередині електронних платіжних систем. Недоліком такого підходу є те, що якщо вам потрібно змінити PIN-код, вам потрібно вибрати або новий обліковий запис клієнта, або новий криптографічний ключ. Банки вважають за краще плавити так, що номер рахунку клієнта втрачається. З іншого боку, оскільки всі PIN-коди обчислюють один криптографічний ключ, зміна одного PIN-коду при збереженні облікового запису клієнта неминуче тягне за собою зміну всіх персональних ідентифікаційних номерів

В іншому варіанті здійснення банк вибирає значення PIN-коду vaping, зберігаючи значення цього PIN-коду у формі відповідної криптограми. Банк передає вибрані значення ПІН власникам карток за допомогою захищеного каналу

Використання PIN-коду, побачення з банком, незручно для клієнта навіть із кліпом його довжини. Зберігати такий PIN-код в пам'яті важко, і тому власник картки може десь записати його. Головне, НЕ писати PIN-код безперервно на карту, або, будь ласка, чи якесь інше видне місце. Інакше завдання зла людини сильно впаде.

Для більшої зручності клієнта Використовуйте значення PIN-коду, що його замовляє Клієнт. Цей спосіб визначення значення PIN дозволяє клієнту:

• використання одного і того ж PIN-коду для різних цілей;

• встановіть PIN-код як комбінацію літер та цифр (для зручності запам'ятовування).

Коли Клієнт вибирає PIN-код, він повинен бути повідомлений банку. PIN-код може бути переданий до банку замовлень поштою або надісланий через захищений термінал, розташований в офісі банку, який негайно шифрується. Якщо банк не обійде використання обраного Клієнтом ПІН-коду, виконайте наступні дії. Шкірна цифра PIN-кодів, обраних Клієнтом, є модулем 10 (без переказів) з відповідною цифрою PIN-коду, зняття банком з рахунку клієнта. Отримання десяткового номера називається “Shift”. Це зміщення зберігається на карті клієнта. Оскільки PIN-код PIN випадковий, визначити Клієнт не можна за його «зміщенням».

Основна вимога безпеки полягає в тому, щоб значення PIN-коду запам'яталося власнику картки, а невинні зберігалися в будь-якій читається формі. Але люди недосконалі і дуже часто забувають свої значення PIN. Тому банки заздалегідь затоплюються, щоб підготувати СПЕЦІАЛЬНІ процедури для такої справи. Банк може реалізувати один із наступних підходів. Перша заснована на відновленні клієнта PIN-коду, який забув клієнт, та відправці його власнику картки. В іншому підході нове значення PIN просто генерується.

Під час ідентифікації клієнта за допомогою PIN-коду та перед представленням картки існують два основні способи підтвердження PIN-коду. неальгоритмічні та алгоритмічні.

Неалгоритмічний метод підтвердження PIN НЕ вимагає спеціальних алгоритмів для змін трансформації. Перевірка PIN-коду здійснюється шляхом безпосереднього порівняння PIN-коду, введеного клієнтом, зі значеннями, що зберігаються в базі даних. Зазвичай база даних із значеннями PIN-кодів

КЛІЄНТІв шифрується за допомогою методу шифрування Шифрування, щоб захистити її від ускладнення процесу порівняння.

Алгоритмічно метод перевірки PIN-коду полягає в тому, що Клієнт буде робити записи PIN за певним алгоритмом, використовуючи секретний ключ, а потім порівнювати їх зі значенням PIN-коду, яке зберігається в певній формі на транспортному засобі. Переваги цього методу перевірки:

- Відсутність копії ПІН-коду на хост-комп'ютері, включаючи його розголошення працівниками банку;
- Відсутність передачі PIN-коду між банкоматами або POS-терміналом та основним комп'ютером банку і не дозволяє йому перехопити зловмисника або накласти результат порівняння;
- Спрощення роботи над створенням системного програмного забезпечення, оскільки в реальному часі більше немає необхідності в діях.

1.4 Типи шахрайства

Шахрайство з додатками:

Цей вид шахрайства відбувається, коли хтось фальсифікує додаток для отримання кредитної картки. Шахрайство з застосуванням досконалим трьома способами:

Непередбачуване посвідчення особи, де особа незаконно отримує особисту інформацію іншої людини і відкриває рахунки в його або її ім'я, використовуючи частково законну інформацію.

Фінансове шахрайство, де індивідуум надає неправдиві інформація про його або її фінансове становище для придбання кредиту. Not-received items (NRI), додатково звані поштовими перехоплення відбуваються після того, як карта була викарбувано з поштової перш ніж він досягне мети свого власника.

Втрачені, або вкрадені карти:

Картка загублена, або вкрадена після того, як законний власник рахунку отримав карту і втратив її, або хтось краде карту. цей вид шахрайства по суті

є найкращим шлях для шахрая, щоб заволодіти альтернативними кредитні карти без інвестицій в технології. це також можливо, найжорсткіший вид античного шахрайства з кредитними картами.

Захоплення аккаунта:

Цей тип шахрайства трапляється, коли шахрай незаконно отримує данні про персональну інформацію клієнтів. шахрай приймає контроль (захоплення) законної облікового запису або надаючи клієнтам no або номер карти. шахрай потім зв'язується з емітентом карти, маскуючи реальному власнику карти, попросити, щоб пошта була перенаправлено на новий адреса. Особа, яка вчинила картку звітів про шахрайство, втратило і просить відправити заміну. Підроблені та фальшиві картки: Створення підроблених карт разом з втраченими / вкраденими картками представляють найбільшу загрозу при шахрайстві з кредитними картами. Шахраї постійно знаходять нові і додаткові інноваційні способи щоб робити фальшиві картки. ряд методів використовуються для створення помилкових і підроблених карт.

1. Видалення магнітної смуги: шахрай може існуючу карту, яка була незаконно отримана шляхом металева смуга з потужним електромагнітом. Шахрай потім заштовхує деталі на картці, щоб вони відповідали деталям законної карти, яку вони перевиготовили, наприклад, від викраденого до кидка. як тільки шахрай почне використовувати карти, касир може пронести картку через багато разів, перш ніж усвідомити, що металева смуга не працює. Потім касир переходить до ручного введіть дані карти в термінал. Це манера шахрайства має високий ризик, оскільки касир буде уважно переглядаючи карту, щоб прочитати цифри. Підроблені карти, як і деякі традиційні способи шахрайства кредитної картки, перетворення в неконкурентну техніку незаконного накопичення коштів або товарів.

2. Створення підробленої карти: шахрай буде виробляти фальшиву картку

з нуля, використовуючи складні машини. Це може бути перш за все загальне різноманітність шахрайства, хоча для підроблених карток необхідно багато

зусиль і талантів. сучасні карти кілька заходів безпеки, призначених для його створення дуже клопітно для шахраїв створення підробок хорошої якості. Голограми вводяться в більшості кредитних карт і дуже складно підробити. Тиснення голограм на самій карті - ще одна проблема для шахраїв карт.

3. Зміна даних карти: шахрай буде змінювати данні карти або повторного її тиснення - шляхом застосування тепла і тиску до карти, що була виготовлена законним емітентом, або шляхом їх повторного кодування з використанням комп'ютерного програмного забезпечення, яке кодує дані магнітної смуги на карту.

4. Скіммінг: більшість випадків фальсифікації шахрайства пов'язані з skimming методом, де реальні дані картки через магнітну смугу електронно виведена на іншу. Скіммінг швидко зростає, тому що найпопулярніший вид шахрайство з кредитними картами. Співробітниками компаній встановлено, що шахраї несуть кишенькові пристрої для скіммінгу, пристрій зчитування магнітної смуги на батарейках, при цьому вони зчитують карт клієнта, щоб отримати карту клієнта. Шахрай робить це, поки клієнт ждетдля того, щоб транзакція була дійсною через термінал карти.Скіммінг відбувається невідомо власнику карти і такстрашно клопітно, а то й неможливо відстежити. Вальтернатівние випадки, деталі, отримані скіммірованіем, іспользуютсясовершать шахрайські транзакції, не пов'язані з картою, посредствоммошеннікі. Часто власник карти не знає про шахрайство до моменту, коли в заяві з'являється перелік покупок, які вони не створили.

5. Білий пластик: білий пластик може бути розміром з карточкуіз пластика будь-якого кольору, який шахрай створює і кодіруетс законним знанням магнітної смуги для незаконних угод. Однак ця карта виглядає як ключ камери містить законні знання магнітної смуги, які

шахраї будуть використовувати на POS-терміналах, які не потребують перевірки данних або перевірки карти.

Пов'язані з торговцями шахрайства ініціюються або власниками

торгового підприємства або їх робочих. види шахрайства, ініційоване торговцями:

Торгівельна змова:

Цей тип шахрайства відбувається після того, як власники торговців і / або їх працівники змовляються здійснювати шахрайство, використовуючи свої

рахунки клієнта і особисті дані. власників і / або їх

працівники передають інформацію про клієнтів шахраям.

Триангуляція:

Шахрай в цьому виді шахрайства діє з Інтернет Веб сайту, продукт пропонується за значно зниженими ставками і також відправляються до оплати. Нечесний сайт, на перший погляд, є законним аукціоном або традиційним сайтом продажів. Клієнт, в той час як вводить дані замовлення, в той час надає інформацію, таку як ім'я, адреса і діючі дані кредитної картки на сайт. коли шахраї отримують ці деталі, вони замовляють продукт з законного веб-сайту

використовуючи подробиці про оплату кредитною карткою. Потім шахрай йде на покупку іншого товару з використанням номерів кредитних карт

клієнт. Цей метод призначений для створення початкової плутанини, а також безчесні інтернет компанії таким чином будуть діяти досить довго, щоб накопичити величезну кількість продуктів, придбаних за допомогою браковані номера кредитних карт.

Інтернет надав чудову основу для шахраїв щоб здійснювати шахрайство з кредитними картами в простій формі. Нещодавно шахраї почали діяти в дійсно на міжнародному рівні. З розширенням транскордонних або «глобальних» соціальних, економічних і політичних областях, мережа стала новим світовим ринком, захоплення клієнтів з більшості країн світу. самі часто використовувані методи в веб-шахрайстві:

1. Клонування веб-сайтів:

клонування веб-сайтів - це якщо шахраї клонують повний сайт або просто сторінки, з яких ви можете розмістити замовлення. У Клієнтів немає причин повірити не обробляючи компанію, яку їм потрібно було отримати товарів або послуг, тому що сторінки, які вони перегляд ідентичний перегляду реального веб-сайта.клонірованний або підроблений веб-сайт може отримати ці дані і відправити клієнту квитанцію про транзакції через електронну як і оригінальна компанія. Споживач нічого не сумнівається, в той час як шахраї мають всі подробиці і зробити шахрайство з кредитними картами.

2. Помилкові сайти продавця: ці сайти зазвичай надають клієнту особливо низька вартість надання послуг. сайт запитує повну кредитну карту клієнта деталі, такі як ім'я та адреса в обмін на доступ до зміст сайту. Більшість з цих сайтів заявляють, що є безкоштовними,

однак потрібно дійсний номер майстер-карти для перевірки

люди віку. Ці сайти створені для накопичення як декількох кількість кредитних карт. Сайти ніколи не спісиваетотдельних осіб за надані ними послуги. Сайти як правило, є частиною більш великої злочинної мережі, яка або використовує маленький відбиток який він збирає, щоб підняти доходи або продає справжні дані кредитної картки дрібним мошеннікам.3. Генератори кредитних карт: генератори номерів кредитних карт комп'ютерні програми, які генерують дійсні номери кредитних карти дати закінчення. Ці генератори працюють, генеруючи спіскіномеров кредитної картки рахунків з одного облікового запису числа. Ці роботи шляхом неправильного перекладу математичного Luhn алгоритм, який використовують емітенти карт для отримання альтернативної діючої карти число спроб. Генератори дозволяють користувачам незаконно згенерованими кількома цифрами, тому що це дозволив користувач.

Розділ 2
ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СИСТЕМ POS, ТА БАНКОМАТІВ.

2.1 Системи терміналів (POS).

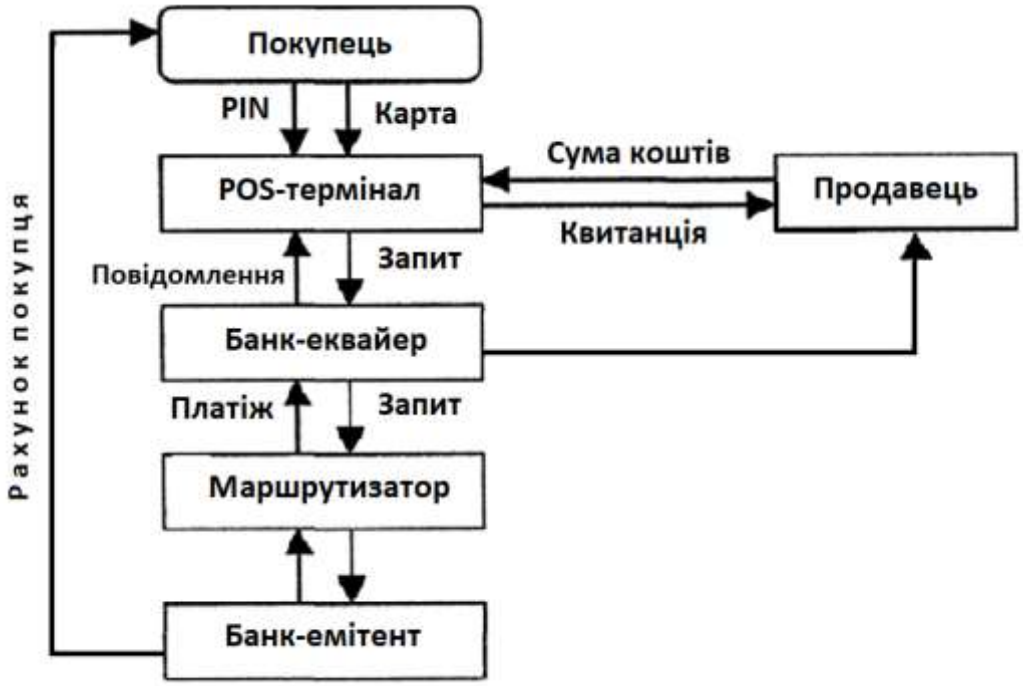
Системи торгівельних мереж POS (Point - Of - Sale), ці системи забезпечують розрахунки між продавцем і покупцем в точці продажу, термінали отримали широке розповсюдження у всіх країнах світу і, на самперед, в США. Системи торгівельних розрахунків POS здійснюють перевірку достовірності і обслуговування як дебетових так і кредитних карт клієнта в місцях продажу товарів і послуг. Не відходячи від каси в рамках банківської системи електронних платежів. POS - термінали, що входять до цих систем, розміщуються на різних підприємствах, що займаються торгівлею в магазинах, супермаркетах, на заправних станціях і т.п.

POS - термінали призначені для обробки запитів по транзакціям при фінансових розрахунках з використанням банківських платіжних карток, що мають як магнітну смугу так і смарт – карт, з мікропроцесором. Встановлення POS – терміналівв торгівельні мережі дозволяє автоматизувати операції по обслуговуванню клієнтів з платіжними картами і суттєво зменшити час обслуговування клієнтів. Можливості і комплектація POS - терміналів варіюються в широких межах, однак типовий сучасний POS - термінал оснащений устройст вами зчитування як з карт з магнітною смугою, так і зі смарт-

карт; незалежній пам'яттю; портами для підключення PIN - клавіатури (клавіатури для набору клієнтом PIN - коду); принтера; з'єднання з персональним комп'ютером або електронним касовим апаратом .

Зазвичай POS-термінал також був обладнаний модемом з можливим автоматичним повторним набором. POS - термінал використовує "розумні" функції - його можна запрограмувати. Такий мовний асемблер використовується як мовне програмування, а також діалекти мов C та BASIC. Все це дозволяє здійснювати авторизаційну картку з магнітною смужкою, вона перебуває в режимі реального чаю для мене (онлайн) і використовується зі смартфоном - карткою режиму офлайн (офлайн) з накопиченням протоколів транзакцій. Ці протоколи транзакцій передаються до звітного центру протягом години сеансів зв'язку. Під час POS-сеансів термінал також може бути відомий і зберігати дані, передані EMM, що містяться в центрі. В основному це стоп-листів.

POS позиція - термінали, які використовуються в комплекті та на високому рівні, можуть бути з'єднані між собою в доларових доларах, коли НЕ залишилося півтора-двох доларів. Ми порівнюємо розміри та вагу POS-терміналів з аналогією інших апаратних апаратних пристроїв.



Мал. 4. Схема функціонування системи POS

Схема системи POS показана на рис. 4. Покупець представляє свою дебетову або кредитну карту для оплати покупки та вводить PIN-код для підтвердження своєї особи. Продавець, у свою чергу, вводить суму грошей, яку потрібно заплатити за покупку чи послугу. Потім запит на переказ коштів надсилається банку-покупцю (банку продавця). Банк-набувач направляє цей запит банку-емітенту для перевірки справжності картки, поданої покупцем. Якщо ця картка реальна і покупець має право використовувати її для оплати товарів і послуг, банк-емітент перераховує гроші банку-покупцю на рахунок продавця. Після переказу грошей на рахунок продавця банк-одержувач отримує повідомлення в POS-терміналі, щоб повідомити вас про завершення транзакції. Після цього продавець віддає покупцеві товари та повідомлення.

Слід звернути увагу на складний шлях, який повинна пройти інформація про покупку до завершення транзакції. Під час проходження цим шляхом спостерігаються спотворення та втрата повідомлень.

Для захисту POS-системи слід дотримуватися та дотримуватися таких вимог:

- Перевірка PIN-коду, введеного покупцем, повинна здійснюватися банківською системою-емітентом. При пересиланні по каналах зв'язку значення PIN-коду повинно бути зашифровано.
- Повідомлення, що містять запит на переказ грошей (або під підтвердженням переказу), повинні перевіряти справжність, щоб захистити від заміни та модифікації при проходженні через лінії зв'язку та процесори обробки.

Найбільш вразливою точкою POS-системи є її POS-термінали. На відміну від банкоматів, в цьому випадку спочатку передбачається, що POS-термінал НЕ захищений від зовнішніх впливів. Загрози для POS - терміналу пов'язані з можливістю розкриття секретного ключа, який знаходиться в POS - терміналі і використовується для шифрування інформації, що передається цим терміналом банку - покупцю. Загроза розкрити ключ терміналу досить реальна, оскільки ці термінали встановлюються в місцях, які не захищені, наприклад магазини, АЗС тощо.

Потенційні загрози через розкриття ключових даних отримали такі назви.

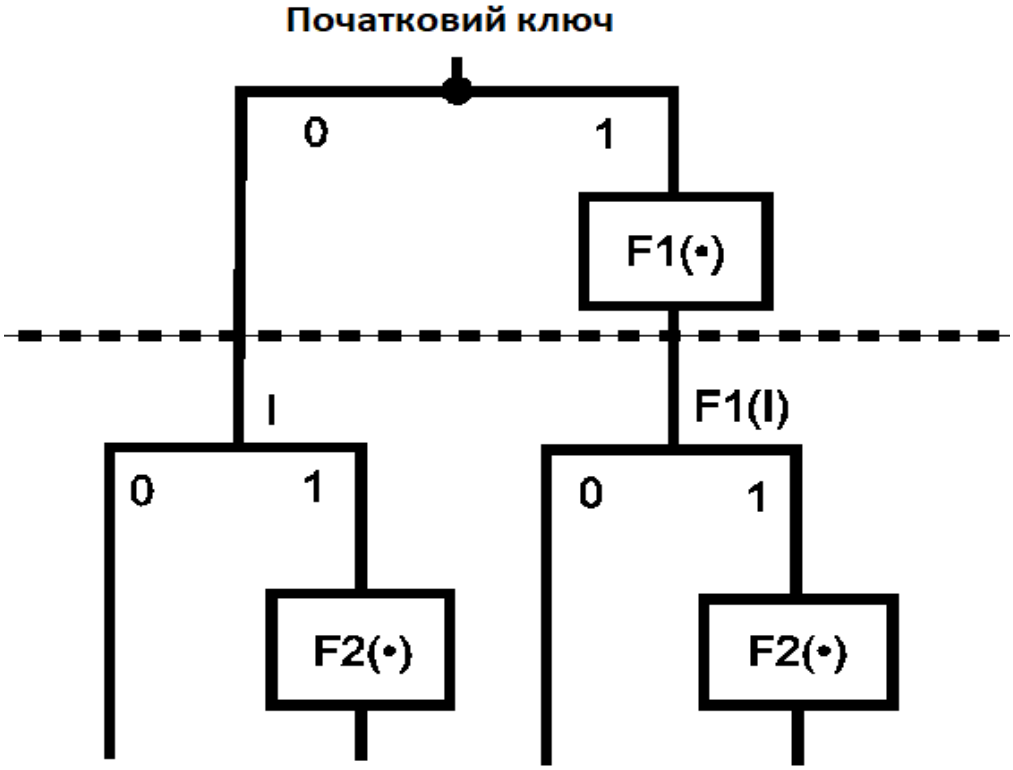
- "Зворотний слід". Суть цієї загрози полягає в тому, що якщо зловмисник отримає ключ шифрування, він може спробувати відновити значення PIN-коду, використовуване в попередніх транзакціях.
- «Прямий слід». Суть цієї загрози полягає в тому, що якщо зловмисник отримає ключ шифрування, він спробує відновити значення PIN-коду, яке буде використано в наступних транзакціях.

Захищено від загрози зворотного та прямолінійного відстеження:

- Метод похідного ключа;
- Метод транзакційного ключа;
- Метод відкритого ключа.

Суть перших двох методів полягає в тому, що вони забезпечують модифікацію ключа шифрування переданих даних для кожної транзакції.

Метод виведення ключа забезпечує ключову зміну для кожної транзакції, незалежно від її змісту. Для генерації ключа шифрування використовується однонаправлена функція поточного значення ключа та деякої випадкової змінної. Процес отримання (виведення) ключа для шифрування наступної транзакції - це добре відоме «блукання» по дереву (рис. 5).



Мал. 5 . Схема виведення ключа з урахуванням довічного уявлення номера S ключа

Вершиною дерева рис. 5 є деякий початкове значення ключа I. Щоб отримати ключ з номером S , число S представляють в двійковій формі. Потім при обчисленні значення ключа враховується структура двійкового подання числа S , починаючи з старшого розряду. Якщо L - й двійковий розряд числа S дорівнює 1, то до поточного значення ключа К застосовується одне спрямована функція FL (K), де L - номер розглянутого д воічного розряду . В іншому випадку переходять до рассмотре нию наступного розряду числа S, НЕ застосовуючи однонаправлені ної функції. Остання реалізована на основі алгоритму DES. Для отримання достатнього швидкодії кількість одиниць в

двійковому представленні числа S зазвичай обмежується - їх повинно бути НЕ більш 10. Цей метод забезпечує захист тільки від загрози "зворотнього трасування".

Метод ключа транзакції дозволяє зашифрувати інформацію, передану між POS - терміналами та банком-одержувачем, використовуючи унікальний ключ, який може змінюватись від транзакції до транзакції. Для створення нового ключа транзакції використовуються такі компоненти:

• однонаправлена функція значення попереднього ключа;

• зміст угоди;

• Інформація, отримана з картки.

Також передбачається, що попередня транзакція була успішною. Метод ключа транзакції забезпечує захист як від „зворотного відстеження”, так і від „відстеження вперед”. Розкриття єдиного ключа не дозволяє зловмисникові розкрити всі попередні та всі наступні транзакції. Недоліком цієї схеми є складність її реалізації.

Метод відкритого ключа дозволяє надійно захистити себе від будь-якого виду відстеження та забезпечити надійне шифрування переданої інформації. У цьому випадку POS-терміналу надається секретний ключ для розшифровки повідомлень банку - покупця. Цей ключ генерується під час ініціалізації терміналу. Після генерування секретного ключа термінал надсилає пов'язаний відкритий ключ на комп'ютер банку - набувача. Обмін між учасниками взаємодії здійснюється за допомогою відкритого ключа кожного з них. Під автентифікацію учасників здійснюється спеціальним центром реєстрації ключів за допомогою власної пари відкритих та приватних ключів. Недоліком цього способу є його відносно низька швидкість.

2.2 Забезпечення безпеки банкоматів.

Касовий апарат - це банкомат для видачі та збору готівки під час операцій із пластиковими картками. Крім того, банкомат дозволяє власнику картки

отримувати інформацію про поточний стан рахунку (включаючи виписку на папері), а також проводити операції з переказу коштів з одного рахунку на інший

Банкомат оснащений зчитувачем карт, а також дисплеєм та клавіатурою для інтерактивної взаємодії з власником картки. Банкомат оснащений персональним комп'ютером, який забезпечує управління банкоматом та його управління. Останнє є дуже важливим, оскільки банкомат є сховищем готівки. Для забезпечення функцій зв'язку банкомати оснащені платами X.25, а іноді і модемами.

Банкноти в банкоматі розміщуються в касетах, які знаходяться в спеціальному сейфі. Кількість касет визначає кількість номіналів, виданих банкоматами. Розміри касет регулюються, що дозволяє заряджати банкомат практично будь-якою банкнотою.

Банкомати - це стаціонарні пристрої великих габаритних розмірів і ваги. Орієнтовні розміри: висота 1,5 ... 1,8 м, ширина і глибина - близько 1 м, вага - близько тонни. Більше того, для запобігання можливих крадіжок їх монтують ретельно. Банкомати розміщують як у охоронюваних приміщеннях, так і не на вулиці.

Сьогодні більшість моделей банкоматів розроблені для роботи в режимі реального часу (в режимі он-лайн) з картками з магнітною смугою, однак з'явилися банкомати, це спосіб роботи зі смарт-картами в режимі офлайн (офлайн).

Офлайн (офлайн) режим роботи банкомата характеризується тим, що банкомат працює незалежно від комп'ютерів банку. Інформація про транзакцію записується на внутрішній магнітний диск і виводиться на вбудований принтер. Перевагами автономного режиму банкомату є його відносно низька вартість та незалежність від якості ліній зв'язку. Це дуже важливо для країн з поганим обслуговуванням телефону. У той же час низька вартість установки безпосередньо визначає високу вартість експлуатації таких банкоматів. Для того, щоб оновити «чорні списки» (списки зупинок) втрачених карт, вам пот-

рібно ходити та обслуговувати такі банкомати хоча б раз на день спеціально призначеній особі. З великою кількістю таких пристроїв таке обслуговування важко.

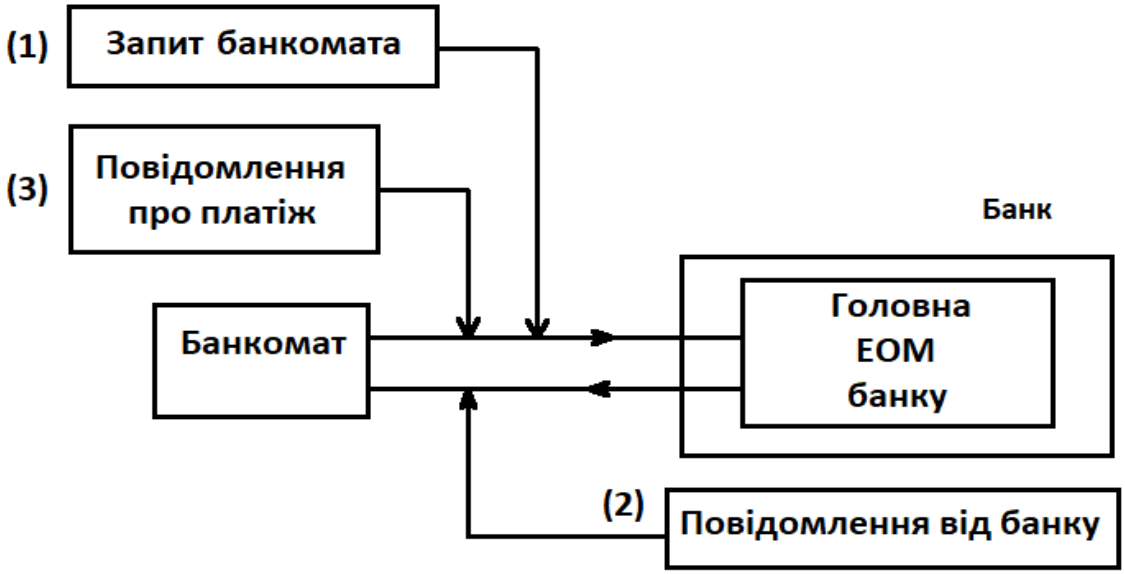
Труднощі виникають і при ідентифікації (автентифікації) клієнта. Для захисту інформації, що зберігається на картці за допомогою магнітної смуги, використовується її шифрування. Для того, щоб банкомати одного банку прийняли пластикові картки з магнітною смужкою, вони повинні використовувати один ключ для шифрування (дешифрування). Порушення його принаймні в одному з банкоматів призведе до порушення захисту на всіх банкоматах

Режим в режимі реального часу (он-лайн) характеризується тим, що банкомат повинен бути підключений безпосередньо або через телефонну мережу до основного комп'ютера банку. У цьому випадку реєстрація транзакцій здійснюється безпосередньо на головному комп’ютері банку, хоча підтвердження транзакції видається принтеру банкомату. Коли операція реалізована, банкомат обмінюється трьома повідомленнями з головним комп'ютером банку (рис. 6)

1) запит на банкомат;

2) у відповідь повідомлення банку;

3) повідомлення банку про платежі.



Мал 6. Схема обміну повідомленнями між банкоматом і головною ЕОМ банку при ідентифікації та платежі

Запит про банкомат включає такі дані:

- ідентифікатор банкоматів;
- номер рахунку та інші дані клієнта;
- Номер картки,
- символ безпеки;
- Зашифрований PIN-код клієнта;
- необхідна кількість грошей;
- номер транзакції;
- Код підтвердження всіх даних повідомлень.

У відповідь повідомлення банку включає такі дані.

- ідентифікатор банкоматів,
- Код транзакції, дозволяє (забороняє) оплату,
- номер транзакції;
- Код підтвердження всіх даних повідомлень.

У цьому повідомленні для перевірки цілісності даних використовується код автентифікації повідомлення (MAC).

Режим у режимі реального часу має ряд переваг перед режимом офлайн. Це дає можливість клієнту не лише отримувати готівку, але й маніпулювати своїм рахунком. Централізоване ідентифікація / автентифікація може значно підвищити стійкість системи до компромісу ключів шифрування. Централізована автентифікація ідентифікатора користувача дозволяє швидко оновлювати перелік карт, які заборонено використовувати, а також запровадити обмеження на суму грошових коштів, які клієнт може отримати протягом одного дня (для захисту від використання викрадених карт).

Однак цей режим можливий лише при наявності надійних каналів зв'язку між банкоматами та банком , що робить його до вільно дорогим. Крім того, наявність каналу зв'язку породжує і інші загрози безпеки по порівнянні з автономним режимом роботи. Це - аналіз трафіку між банкоматом і головним кому п'ютер і імітація роботи головного комп'ютера комп'ютером зловмисника. При аналізі трафіку можна отримати інфор -мацію про рахунках, сумах, умовах платежів і т.п. При імітації роботи головного комп'ютера банку комп'ютер зловмисника може видавати позитивний відповідь на запит банкомату по результатах ідентифікації / аутентифікації

Мережі банкоматів є в даний час розповсюдження странения формою експлуатації банкоматів , в якій що беруть ють кілька банків.

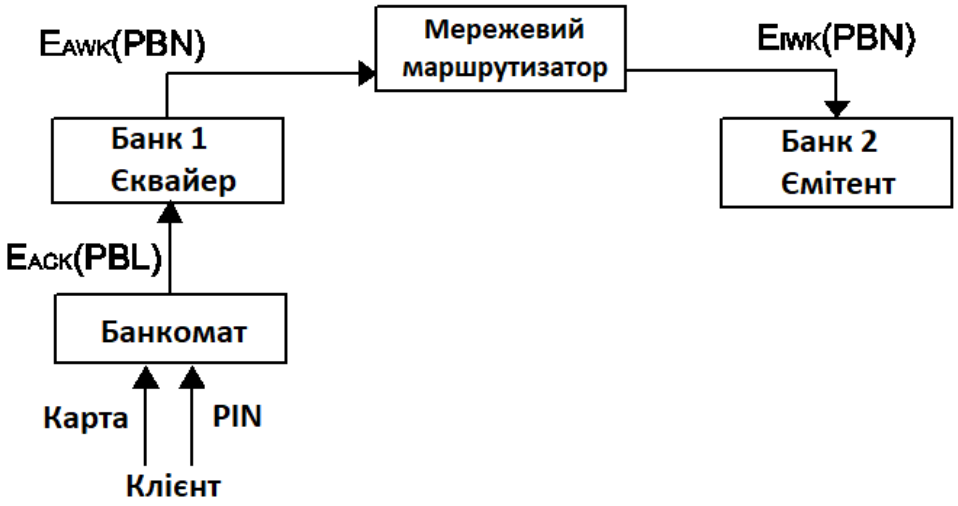
Банки - учасники такої мережі переслідують такі цілі :

- Зменшення вартості операцій для учасників ,
- Поділ витрат і ризику при впровадженні нових видів послуг між учасниками,
- Подолання географічних обмежень і відповідно підвищення суб'єктивної цінності послуг для споживачів

При спільному використанні декількома банками мережі банкоматів виникає серйозна проблема - захист конфіденціальної інформації банків один від одного (ключі шифрування і т.п.) Для вирішення цієї проблеми запропоновано схема центру лізованной перевірки PIN кожним банком в своєму

центрі зв'язку з банкоматами. Ускладнюється також система розподілу ключів між усіма учасниками мережі.

Розглянемо схему проходження інформації про PIN клиента між банкоматом, банком-еквайром (якому належить банкомат) і банком-емітентом (який випустив карту клієнта) (мал. 7).



Мал.7 Схема проходження інформації про PIN клієнта між банкоматом, банком - еквайром і банком - емітентом.

Нехай клієнт Банку2 (Емітента) звернувся до банкомату Банку1 (еквайєр). *При цьому в мережі банкоматів відбуваються наступні дії.*

1. Зчитує пристрій банкомату зчитує інформацію, записану на банківській карті , пред'явленої клиен тому, і потім банкомат визначає , має чи цей клієнт рахунок в Банку 1 - еквайєр.

2. Якщо клієнт НЕ має рахунки в Банку 1, транзакція на спрямовується в мережевий маршрутизатор , який , використовуючи іден тіфікаціонний номер Банку 2 - Емітента BIN (Bank Identification Number), направляє цю транзакцію на головний комп'ютер Банку 2 або виробляє перевірку PIN для Банку 2 .

3. Якщо перевірка PIN проводиться на головному комп'ютері Банку 2, то цей комп'ютер отримує повну інформацію про транзакції і перевіряє достовірність PIN .

4. Незалежно від результату перевірки комп'ютер Банку2 пересилає повідомлення з цим результатом через мережевий березня шрутізатор комп'ютера Банку 1.

Як слід з прикладу, до банку - емітенту пред'являються такі вимоги :

- Випускаємі ним карти повинні сприйматися всіма банкоматами мережі;
- Банк - емітент повинен володіти технологією перевірки pin своїх клієнтів .

До банку - еквайєру пред'являються інші вимоги :

- В банкоматі або головному комп'ютері банку повинна бути реа лізованних перевірка приналежності транзакції ;
- Якщо немає можливості перевірити правильність чужого pin, банк-еквайєр повинен передати дані про транзакції на мережевий маршрутизатор .

Для захисту взаємодії комп'ютерів банків один з одним і з банкоматами має застосовуватися кінцеве (абонентське) шифрування інформації , переданої по лініях зв'язку . Зазвичай використовується наступний підхід : вся мережа банкоматів розбивається на зони, і в кожної з них використовується свій глав ний зональний керуючий ключ ZCMK (Zone Control Master Key). Ключ ZCMK призначений для шифрування ключів при про мене між мережним маршрутизатором і головним комп'ютером банку . Ключ ZCMK індивідуальний для всіх учасників мережі . Зазвичай він генерується випадковим чином маршрутизатором і передається неелектронним способом в банк. Розкриття ключа ZCMK призведе до розкриття всіх PIN , які передаються між маршрутизатором і головним комп'ютером банку

Для шифрування інформації , що надходить від головного комп'ютера банку - емітента на маршрутизатор, використовується ра бочій ключ емітента IWK (Issuer Working Key). Його повідомляє головному комп'ютеру банку - емітента маршрутизатор в зашифрованому на унікальному ZCMK вигляді. Ключ IWK може змінюватися по запиту користувача в процесі роботи .

Аналогічний по призначенню ключ для обміну між банком - еквайром і маршрутизатором називається робочим ключем еквайра AWK (Acquirer Working Key). Для шифрування інформа ції при передачі від банкомату до головного комп'ютера банку - еквайра використовується зв'язковий ключ еквайра АСК (Acquirer Communication Key).

При розгляді функціонування системи захисту введені такі позначення :

EY (X) - шифрування повідомлення X по алгоритму DES з використанням ключа Y ;

DY (X) - розшифрування повідомлення X по алгоритму DES з використанням ключа Y ;

PBL (PIN Block Local) - локальний блок PIN, отриманий з введенного клієнтом PIN, доповненого до восьми символів, і представлений у внутрішньому форматі банкомату ;

PBN (PIN Block Network) - мережевий блок PIN, отриманий з вве денного клієнтом PIN , доповненого до восьми символів, і представлений в вигляді, що готовий для передачі в мережі.

Повернемося до розгляду схеми на мал. 7.

1. Клієнт пред'явив банкомату Банку 1 банківську карту і ввів з клавіатури свій PIN . Банкомат формує PBL , шифру ет його з використанням АСК , т.п. обчислює криптограму Еаск(PBL), і відправляє її на головний комп'ютер Банку1.

2. На головному комп'ютері Банку 1 блок PBL розшифрують вивалісь і перетворюється в блок PBN , потім блок PBN шифру ється з використанням AWK і відсилається в Мережевий маршрутизатор. Процес перетворення

$$E_{ACK}(PBL) \rightarrow E_{AWK}(PBN)$$

називають трансляцією блоку PIN з ключа АСК на ключ AWK . Основне призначення цього процесу - зміна ключа шифрування .

3. Якщо PIN перевіряється на мережевому маршрутизаторі, після отримання криптограми EAWK(PBN) проводиться її рас шифрування, а потім виділення PIN з допомогою перетворень

$$D_{AWK}(E_{AWK}(PBN)) = PBN \rightarrow PIN.$$

Якщо PIN перевіряється Банком 2, прийнята криптограма транслюється з ключа AWK на ключ IWK (обидва ключа зберігаються на мережевому маршрутизаторі):

$$E_{AWK}(PBN) \rightarrow E_{IWK}(PBN).$$

Потім криптограма EIWK(PBN) відправляється в Банк 2.

4. Поступила в Банк2 криптограма EIWK(PBN) перетвориться в залежності від використовуваного способу перевірки або в відкритий PIN :

$$D_{IWK}(E_{IWK}(PBN)) = PBN \rightarrow PIN,$$

або в PIN в формі блоку PBL , зашифрованого на ключі бази даних DBK:

$$E_{IWK}(PBN) \rightarrow E_{DBK}(PBL$$

5. Після будь-якого з цих перетворень здійснюється пошук прийнятого PIN в базі даних існуючих PIN .

6. В результаті виконаної перевірки введений клиен тому PIN або приймається, або відхиляється. Поза залежності від результату перевірки головний комп'ютер Банку 2 пересилає зі спілкування з результатом через Мережевий маршрутизатор на компью тер Банку 1, а той сповіщає банкомат про результати вирішення .

Розглянута схема забезпечення безпеки взаємо дії комп'ютерів в мережі базується на симетричному алго ритмі шифрування DES . Тому на поширення ключа ZCMK накладаються жорсткі обмеження . Застосування асиметричний ної системи шифрування з відкритим ключем дозволяє неяк до спростити ключову систему і відповідно взаємодія між банкоматами та головними комп'ютерами банків .

У неподільні мережі банкоматів досить вико вать на всіх банкоматах однаковий відкритий ключ , а на головному комп'ютері банку - закритий ключ. Це дозволяє шифрувати запит і підтверджує повідомлення з банку, так як забезпе ня конфіденційності відповідного повідомлення необов'язково.

Проблема захисту запиту від активних атак (зміни або введення помилкового запиту) може бути вирішена в разі нерозподіленої мережі використанням пароля для ідентифікації банкоматів.

2.3. Електронна платіжна система UEPS

Особливо важливими є питання забезпечення безпеки функціонування електронної платіжної системи та контролю доступу до фінансової інформації. Враховуючи недостатню розвиненість ліній зв'язку, найбільш перспективні платіжні системи, засновані на автономному принципі (офлайн) обслуговування власників карток у торговій точці або банкоматі. Універсальна електронна платіжна система UEPS (Universal Electronic Payment System) відповідає визначеним вимогам і характеризується високим рівнем безпеки, що підтверджується результатами авторитетних міжнародних експертиз. Ось чому побудова електронної платіжної системи Ощадбанку за допомогою мікропроцесорних карток у Ощадбанку базується на технології UEPS. Концепція та технологія платіжної системи UEPS була розроблена французькою компанією NET 1 International.

Основним технологічним принципом UEPS є здійснення всіх фінансових операцій поза межами прямої взаємодії двох смарт-карт. Основним алгоритмом шифрування інформації є алгоритм DES. Висока криптографічна міцність забезпечується використанням подвійного шифрування на клавішах довжиною 8 байт.

У системах офлайн-платежів більшість функцій щодо забезпечення контролю за діями та захисту від шахрайства покладається на мікропроцесорну карту - основний елемент UEPS. UEPS використовує три основні типи мікропроцесорних карт:

- службові картки персоналу банку;
- торгові картки;

• Картки клієнтів.

Всі карти містять 8-бітний мікропроцесор.

Представляємо технічні характеристики клієнтської картки системи UEPS.

• Процесор: SOS - Томпсон, 8 біт, система інструкцій Motorola 6805.

• Операційна система: багатозадачний чіп операційної системи MCOS (Multitasking Chip Operation System).

• ОЗУ: 160 байт.

• ПЗУ: 6 Кбайт.

• EEPROM: 2 Кбайт (16 Кбіт).

Конструкція та архітектура процесора не дозволяють механічно зчитувати інформацію шляхом викрадення кришталю крадіжкою, сканування за допомогою електронного мікроскопа, впливу ультрафіолетового світла тощо. При спробі виконання таких операцій мікропроцесор повністю виходить з ладу. Сама архітектура мікропроцесорної карти така, що процесор керує доступом до захищених областей пам'яті, передаючи управління на спеціальний додаток UEPS. Вся інформація передається зовні на карту в зашифрованому вигляді і розшифровується прикладною програмою всередині карти за допомогою ключів, що зберігаються в захищених місцях пам'яті. Так само зашифровується інформація, яка залишає картку.

Банківські ключі ніколи не залишають картку у відкритому вигляді.

Склад та архітектура платіжної системи. Основним рівнем єдиної платіжної системи є емісійний центр (рис. 8), який виконує такі функції:

• генерація загального (системоутворюючого) ключа платіжної системи;

• первинний випуск мікропроцесорних карт - присвоєння унікальних серійних номерів USN карт, запис на загальносистемні картки ідентифікує та контролює інформацію, записуючи на картки загальний ключ системи;

• ведення каталогів учасників розрахунків, реєстрація нових учасників (банків - емітентів та набувачів) у системі;

• ведення каталогів типів карток та кодів валют, що використовуються в системі;

• Ведення єдиної бази даних із серійними номерами та USN - номерами карт, що циркулюють у системі.

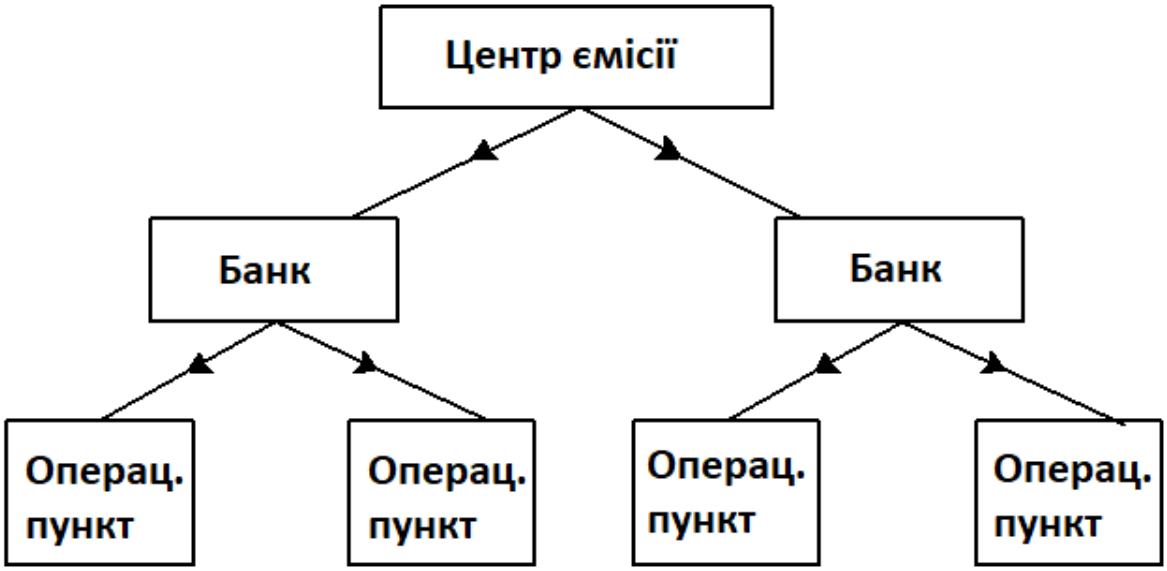


Рис 8. Архітектура платіжної системи

Другий рівень платіжної системи - це банки-учасниці. Банк, що бере участь у платіжній системі, - це фінансова установа, яка бере участь у розрахунках за допомогою мікропроцесорних карток та несе повну фінансову відповідальність за операції, здійснені виданими нею картками. Кожен з банків-учасників, перш ніж розпочати випуск своїх карток (клієнт та торги), створює власний набір ключів емітента чи набувача, які вводяться у картки під час процесу випуску та використовуються при формуванні та обробці фінансових операцій. Перелік технічного обладнання банку-учасниці має ряд машин для циалізованих робочих місць (AWP) для виконавців: адміністратор, охорона, бухгалтер.

Третій рівень ієрархії в платіжній системі - це операційні пункти. Операційні пункти відносяться до структури підрозділу банку учасника, в якому здійснюється обслуговування клієнтів Банку - відкриття / закриття рахунків

на картках, видача карток та здійснення кредитних та дебетових операцій. Карткова система банку-учасниці повинна включати принаймні схему розповсюдження та використання ключів та окремих паролів суб'єктів системи UEPS. Розподіл ключів та паролів на картках банку, продавця та клієнта показано в табл. 9.

Таблиця 9.

Розподіл ключів і паролів по картам банку , торговця і клієнта

Карта банку	Карта торговця	Карта клієнта	Найменування
P_0	P_0	P_0	Майстер-ключ
P1-PIN B	P1-PIN M	P1-PIN 1	паролі P1
P2-RFU	P2-RFU	P2-PIN 2	паролі P2
P3	P3	P3	паролі P3
P4	P4	P4	паролі P4
P5	P5	P5	паролі P5
P6	P6	P6	паролі P6
P7	P7	P7	системоутворюючий ключ P7
KI1, KI2	-	KI1, KI2	Ключі клієнтських карток
-	KA1, KA2	-	Ключі торгових карток
SK	SK	SK	Сесійна (сеансовий) ключ обміну

Дамо пояснення до табл . 9.

Майстер-ключ P 0 забезпечує генеральний доступ до карті. Призначається і відомий тільки центру емісії.

Група паролів P 1:

PIN B - пароль операціоніста банку.

PIN M - пароль касира магазину.

PIN 1 - пароль на зарахування коштів на карту. Призначається і відомий тільки власнику карти. Змінюється власником в off - line терміналі.

Група паролів P 2:

RFU - резервний пароль.

PIN 2 - пароль для списання коштів з картки. Призначається та відоме лише власнику картки. Змінює власника в автономному терміналі. (PIN-коди 1 та PIN 2 паролі можуть бути однаковими на вимогу власника картки.)

Групи паролів РЖД та Р4 є резервними.

Пароль R 5 бере участь разом з R 7 у формуванні ключів сеансу (сесії). Спільний для всіх банків, які беруть участь у єдиній системі розрахунків. Призначається емісійним центром.

Пароль Р6 забезпечує доступ до ключів для запису Klx, Kah. Призначається банком-учасником.

Р6-RFU - резервний пароль.

Системний ключ Р7 бере участь у формуванні ключів сеансу. Є загальне для всіх банків - учасників єдиної платіжної системи. Призначається емісійним центром.

Ключі клієнтських карт KI, KI 2 подаються при зарахуванні коштів на карту. Брати участь у шифруванні записів транзакцій. Призначається банком-учасником.

Ключі торгових карток KA 1, KA 2 подаються при зборі картки продавця. Брати участь у шифруванні записів транзакцій. Призначається банком-емітентом.

Сеанс (сеанс) обмінного ключа SK генерується в пам'яті карт в результаті діалогу карти з карткою і використовується для шифрування всіх потоків інформації між картками під час сеансу зв'язку. Картка, унікальна для кожного сеансу спілкування.

Цикл платіжних транзакцій. У циклі платіжних транзакцій беруть участь три сторони:

• фінансова установа (банк-член);

• власник карт;

• торгово-сервісна компанія, банкомат.

Життєвий цикл платіжної транзакції можна розділити на три етапи.

На першому етапі власник картки має можливість отримати електронну готівку на свою карту в розмірі НЕ довузівського залишку на його особистий рахунок (або банк може позичити клієнту). Цю операцію може виконувати як оператор банку, так і в режимі самообслуговування. Він проводиться на банківському терміналі самообслуговування або на робочому місці оператора банку в он-лайн режимі з автоматизованою системою банку, оскільки доступ до інформації про стан карт - необхідний рахунок клієнта, на підставі якого фінансова операція здійснюється. Тому такі операції можуть відбуватися в будь-якому місці, де існує он-лайн зв'язок із базою даних карткових рахунків клієнтів банку.

Для виконання цієї операції клієнту необхідно надати PIN-код 1, щоб поповнити картку зі свого банківського рахунку.

Крім того, клієнт може здійснювати платіжні операції за суми, що не перевищують залишок електронних коштів на своєму автомобілі в будь-якому місці, де встановлено обладнання для обслуговування мікропроцесорних карток стандарту UEPS. Торговий термінал в режимі офлайн, банкомат та ін. Слід зазначити, що реальні гроші, отримані клієнтом на карту, розташовані протягом усього циклу банківських платіжних операцій на окремому рахунку.

На другому етапі клієнт здійснює платіжну операцію в точці продажу. Ця операція відбувається в режимі офлайн без запиту про надання дозволу власника картки, оскільки вся необхідна інформація, включаючи секретну частину, знаходиться на автомобілі клієнта, а картка - електронний гаманець.

Технічно ця операція виконується наступним чином. Мікропроцесорна картка продавця встановлюється в торговому терміналі, і клієнт, вставивши свою картку в зчитувач пристрою торгового терміналу, списує суму покупки зі своєї картки на картку продавця, тоді як залишок на картці клієнта зменшується на сума транзакції, і залишок на картці візового продавця розташується на аналогічну суму. Крім того, картка продавця та картка покупця містять повну інформацію про транзакцію: дату / час, суму транзакції, іден-

тифікатор компанії Patel та магазин з інформацією про банк та номер рахунку власника.

Щоб виконати транзакцію, покупець повинен ввести свій PIN-код 2 для витрачання коштів зі своєї картки. Клієнт та продавець отримують додатково копії інформації про трансакцію (чек покупця, журнал і зберігання льону). Усі транзакції також дублюються в пам'яті торгового терміналу в зашифрованому вигляді. Відображаються найменування магазину, дата / час операції, номер картки клієнта, сума транзакції, а також кодований рядок з інформацією про завершену транзакцію (щоб можна було відновити інформацію про завершену транзакцію). на паперовому чеку.

На третьому етапі купець, зібравши протягом дня на торговій картці перелік усіх операцій, здійснених під час торгової сесії з детальним описом кожної, передає (збирає) цю інформацію з картки продавця в систему розрахунків банку. . Ця операція може бути здійснена автоматично, через модемне телефонне з'єднання або фізично, після пред'явлення картки продавця в будь-якому найближчому відділенні банку або в пункті збору, але в будь-якому випадку зашифрований перелік транзакцій передається саме з картки продавця, і НЕ з пам'яті торгового терміналу. Після завершення сеансу "колекція" картка продавця буде видалена для роботи в наступному сеансі, і зміни до гарячого списку передаються на нього, про що картка продавця повідомляє торговий термінал на початку наступного робочого дня (нова торгова сесія).

На наступному етапі банк, отримавши інформацію про здійснені транзакції, перераховує суму за всі завершені операції цього магазину на рахунок торгової організації.

Торгові термінали. торгові установи та банківські каси оснащені терміналами EFT-10 із програмним забезпеченням UEPS. У терміналі є два зчитувачі для мікропроцесорних карт. В одному зчитувачі на початку робочого дня встановлюється торгова картка, в іншому - картка клієнта при оплаті покупки. При базовій доставці термінів готівковий EFT-10 також має

зчитувач карт з магнітною смужкою та вбудований модем, що дозволяє організувати на одному пристрої сервіс та пластикові картки з магнітною смужкою.

Торговий термінал, який постійно перебуває поза контролем банку, є одним з найбільш вразливих елементів платіжної системи з точки зору безпеки. Він може під Вергалом здійснити спробу зломи (несанкціонованого доступу) злочинними структурами. Тому неприпустимо довіряти торговому терміналу секретну інформацію, критичну з точки зору функцій платіжної системи, тобто банківські ключі та паролі, алгоритми шифрування, списки фінансових операцій тощо.

У платіжній системі UEPS торговий термінал НЕ зберігає секретної інформації, а відіграє лише роль елемента, що забезпечує взаємодію інтерфейсу між двома захищеними ними смарт-пристроями: картками клієнтів та картками торговців. Усі платіжні операції здійснюються лише в діалозі двох карток. Більше того, поза картками вся інформація завжди шифрується на основі клавіш сеансу.

Формування ключів сеансу. Діалог картки клієнта та продавця в торговому терміналі ґрунтується на ключах сесії.

Клієнтська картка, використовуючи внутрішній датчик випадкових чисел, виробляє випадкове число на початку кожного нового сеансу взаємодії з торговою карткою, зашифровує це число на системних клавішах Р 7, Р 5 і звітує про торгову карту.

Картка продавця, що має однакові системні клавіші Р 7, Р 5, розшифровує отриману інформацію і отримує те саме число в розшифрованому вигляді. Використовуючи цей номер у поєднанні з іншими ключами та даними, спільними для обох карток, картки клієнта та продавця, ви одночасно розробляєте сеансовий ключ, ідентичний для обох карт та унікальний для кожного сеансу зв'язку між картками клієнта та продавця.

Клавіша сеансу є лише в пам'яті обох карт, і вони ніколи не залишаються. На основі цього ключа сесії всі потоки інформації між картками шиф-

руються, де спроби перехоплення повідомлень у торговому терміналі робляться марними.

2.4 Емісія платіжних карток.

Усі банки, що беруть участь у єдиній платіжній системі, що використовують картки UEPS, отримують картки, оснащені індивідуальним логотипом (банку-емітента) та стандартизованим програмним забезпеченням.

Процедура видачі карток складається з трьох етапів:

• призначення центром видачі системних ключів;

• призначення банком-учасниками банківських ключів та паролів;

• персоналізація картки клієнта банком-учасником.

З них перші два етапи є таємними і проводяться з дотриманням відповідних заходів безпеки в спеціально обладнаних приміщеннях. Третій етап, пов'язаний з прямою персоналізацією картки, не є класифікованим і виконується звичайним оператором банку в операційній залі в присутності клієнта.

Система видачі карток, розповсюдження та призначення ключів організована таким чином, щоб зберегти унікальні права та обов'язки кожного банку щодо володіння секретною інформацією про свої банківські фінансові ключі.

Процес видачі карток реалізується наступним чином. Емісійний центр отримує в обігу три типи карток - банківські, торгові та клієнтські. Усі картки спочатку відформатовані та завантажені відповідним програмним забезпеченням UEPS. Доступ до всіх карток закривається транспортним ключем RO - транспортом (унікальним для кожного розіграшу), який постачальник надає уповноваженому банку.

Перший етап випуску (секретний етап) виконується в центрі випуску після отримання кожного нового тиражу карток із забезпеченням спеціаль-

них заходів безпеки адміністратором системи безпеки. Представляючи картки РО - транспорт, центр емісії записує на всі картки свого секретного майстра - ключ РО, системні клавіші Р7, Р5 та встановлює унікальну USN у банківській системі для кожної картки.

Другий етап випуску (таємний етап) виконується в банку-учасниці після отримання кожного нового обігу карток із забезпеченням адміністратором системи безпеки спеціальних заходів безпеки. Для банківських та торгових карток встановлюються відповідні паролі Р 1 та Р 6. Представляючи паролі Р 6 на картках банку та торговця, встановлюються паролі KI і KI 2 для банківських карток та KA1 і KA2 для торгових карток. 3 Банк також вносить на картки додаткову інформацію (коди валют, інформацію про магазин тощо).

Третій етап випуску - персоналізація картки - це таємна операція, що виконується в присутності клієнта оператором банку, і НЕ вимагає додаткових заходів безпеки.

Процес персоналізації картки клієнта можливий лише в діалозі з карткою оператора банку. Оператор, подаючи PIN-код PIN B на банківську карту, вводить інформацію про власника на картці клієнта (повне ім’я, банківські реквізити, термін дії картки тощо). Банківська картка передає банківські ключі KI та KI 2 в зашифрованому вигляді на карту клієнта і записує номер картки оператора, що брав участь у персоналізації, на карту клієнта. Банківські ключі KI та KI 2 передаються на картку клієнта з банківської картки, зашифрованої на основі сесійних ключів.

Клієнт вводить паролі PIN1 та PIN2 на карту зі своєї окремої клавіатури.

Картка оператора банку контролює доступ оператора до системи, перевіряючи його особистий пароль PIN B. Крім того, незалежно від бажання оператора, щоразу, коли нова картка персоналізується, номер картки оператора, який видав картку клієнту, завжди зберігається в мікропроцесорі цієї картки. Тому ви завжди можете встановити, який оператор і коли видав цю карту. Слід зазначити, що оператор банку НЕ отримує інформацію про PIN 1

та паролі клієнта PIN 2 для кредитування та дебетування. Ці паролі клієнта НЕ зберігаються в системі, вони значущі для клієнта, відомі лише картці та її власнику і можуть бути змінені клієнтом самостійно в будь-якій точці в режимі офлайн.

Таким чином, без дозволу власника картки, вираженого в повідомленні цієї картки з правильним паролем, ніхто інший, включаючи оператора банку, не може здійснювати фінансові операції з карткою клієнта.

Диференціація відповідальності між банками - учасниками загальної платіжної системи. У системі UEPS лише банк-учасник має право та технічну можливість доступу до інформації на картках, виданих банком. Навіть виробники та постачальники, що володіють усіма технічними засобами, знаннями форматів даних та повідомлень у системі, папками вихідних програм, розташуванням та призначенням усіх ключів та паролів, НЕ можуть отримати доступ до секретної фінансової інформації на картках, не знаючи банківських ключів та PASS .

Система UEPS передбачає чіткий поділ ключів та розмежування обов'язків між банками, які беруть участь у єдиній платіжній системі. Кожен банк, який бере участь у платіжній системі, має свої банківські ключі та паролі, які беруть участь у шифруванні фінансової інформації та відомі лише йому. Ці ключі та паролі унікальні для кожного банку. Таким чином, забезпечення заходів безпеки зводиться до забезпечення надійного зберігання ключів кожним банком, який бере участь у системі. Втрата ключів будь-яким банком-учасником може призвести до можливості несанкціонованого доступу лише до фінансової інформації, що стосується цього банку, і НЕ створюватиме ризик фінансових втрат для інших банків-емітентів, членів єдиної платіжної системи.

Лише одна пара ключів є загальною для всіх банків, які беруть участь у єдиній платіжній системі; це системні ключі P7, P5, які визначають належність певної картки даної платіжної системи. Ці системні ключі беруть участь лише у виробництві сеансового ключа на картках під час операцій у торговій

точці, не несуть відповідальності за шифрування будь-якої іншої інформації на картках клієнта чи продавця.

Подвійне шифрування записів транзакцій на ключах банку - покупця та банку-емітента.

Запис про кожну платіжну операцію вводиться на картку продавця і має складну структуру. Частина інформації залишається незашифрованою (дата операції, банківські реквізити покупця), частина інформації шифрується на ключах банку - покупця КА1 та КА2 (сума, номер картки USN покупця, номер транзакції на торговій картці) та ін.) та частина інформації про ключі банку-емітента в КІ1 та КІ2 (сума, USN, PAN, номер транзакції у списку на картці клієнта тощо).

Торговець в кінці торгової сесії збирає перелік платіжних операцій у своєму банку - набувача. Цей банк є набувачем, представляючи свої ключі КА 1 і КА 2, розшифровує свою частину платіжної операції і визначає клієнта іншого банку, коли і на яку суму здійснив покупку в своєму магазині. Отримавши інформацію про банківські реквізити покупця із запису транзакцій, банк-покупець генерує електронний платіжне повідомлення для банку-емітента, частиною якого є зашифроване свідоцтво банку-емітента.

Банк-емітент, отримавши повідомлення про оплату, розшифровує другу частину трансакції, представляючи свої банківські ключі КІ 1 і КІ 2. Якщо розшифрована інформація повністю відповідає платіжному повідомленню (насамперед, сума транзакції та власник картки реквізити, щоб завершити покупку), це повідомлення про оплату підтверджується та оплачується, інакше воно відхиляється. Це виключає можливість фальсифікації повідомлень у міжбанківських розрахунках.

Коли банки створюють загальний обробний центр, банки можуть залишати за собою право контролювати міжбанківські операції взаємного обліку. Крім того, кожен банк залишає за собою виключне право володіти, призначати та обертати банківські ключі КІ 1, КІ 2, КА 1, КА 2. Моніторинг потоку транзакцій у платіжній системі. Для забезпечення контролю за безпекою та

вирішення спорів у платіжній системі необхідна ефективна схема організації унікальної нумерації та обліку платіжних операцій. У системі кожна платіжна операція ідентифікується складом таких елементів:

• унікальний серійний номер картки клієнта в системі;

• номер транзакції відповідно до переліку операцій на картці клієнта;

• унікальний серійний номер картки магазину в системі;

• номер транзакції відповідно до переліку операцій на карті магазину;

• порядковий номер колекції картки магазину.

Реалізована схема дозволяє однозначно відстежувати транзакцію через усі елементи системи:

Банк - Клієнт - Магазин - Банк.

Розділ 3

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ ЧЕРЕЗ МЕРЕЖУ INTERNET

Кілька десяткыв років тому Інтернет використовувався в основному лише для обміну електронних поштових повідомленнь та для надсилання файлів. Однак в останні роки сучасні інформаційні технології перетворили Інтернет на розвинену інфраструктуру, яка охоплює всі основні інформаційні центри, світові бібліотеки, бази даних науково-правової інформації, багато державних і комерційних організацій, бірж та банків. Будь-яка організація може поширювати інформацію по всьому світу, створивши інформаційну точку підписки в мережі WWW.

Все більше значення набуває електронна торгівля. Число покупок по банківським картам буде рости по мірі созда ня систем замовлень в оперативному режимі Internet. Сьогодні Internet розглядаэться як величезний інформаційний ринок, що охоплює майже все населення планети Земля. Користування відкритої комп'ютерної мережею Internet змінює спосіб доступу до інформації про придбання, пропозиції та оплаті послуг, покупці товарів і розрахунках. Місця здійснення угод поступово переміщуються від традиційних ринків до більш комфортним для споживача- в будинок або офіс. Саме тому компанії що розробляють і створюють програмні комплекси і апаратних засоби торгові і фінансові та банківські організації активно розвивають та впроваджують різноманітні види і методи ведення комерційної діяльності в електронної системі торгівлі - Internet, проявляючи належну турботу про забезпечення її Безпеки.

3.1 Основні види електронної торгівлі

Термін "електронна комерція" означає надання товарів та платних послуг через глобальні інформаційні мережі. Розглянемо найпоширеніші типи електронної комерції сьогодні.

• Традиційною послугою в галузі електронної комерції є продаж інформації, наприклад, передплата на бази даних, що працюють в режимі он-лайн. Цей вид послуг вже поширився по всьому світу.

• Концепція електронних магазинів останнім часом стає все більш популярною за кордоном. Зазвичай електронний магазин - це веб-сайт, який має оперативний каталог товарів, віртуальну «кошик» для покупця, до якої збираються товари, а також платіжні засоби - шляхом надання номера кредитної картки через Інтернет або по телефону . Каталоги товарів в Інтернеті можуть бути оновлені в міру зміни пропозицій товарів або відображення сезонних подій стимулювання попиту. Відправлення товарів покупцям здійснюється поштою або, у випадку жменьки електронних товарів (наприклад, програмне забезпечення), електронною поштою або безпосередньо через веб-сайт через Інтернет.

• Починає розвиватися новий вид електронної комерції - електронні банки. Серед основних переваг електронних банків можна виділити відносно низьку вартість організації такого банку (НЕ потрібно орендувати престижні будівлі, НЕ потрібні сховища тощо) та широке коло клієнтів (практично будь-який користувач Інтернету може стати потенційним клієнтом електронного банку). Тому електронний банк може надавати клієнтам більш вигідні відсотки, ніж звичайний банк, а також більш широкий спектр банківських послуг за меншу плату. Природно, власні системи захисту електронного банку та захист електронної інформації, наприклад, спеціальні картки - генератори випадкових паролів, синхронізуються з паролем на банківському сервері (це дозволяє створювати унікальний пароль щоразу, коли клієнт звертається до банківського сервера) . Інший, менш дорогий підхід пов'язаний із використанням особистих смарт-карт; вони також дозволяють створювати сеансові ключі.

Певна затримка розвитку електронної комерції була пов'язана з відсутністю надійної системи безпеки. Поки платіжна інформація передається через відкриті мережі з або без мінімальних мінімальних запобіжних заходів. Це сприятливо для автоматизованого шахрайства (наприклад, використання фільтрів для всіх повідомлень, що проходять через мережу з метою вилучення номерів рахунків кредитних карток із потоку даних), а також заради балування, що характерно для деяких хакерів.

3.2 Основні методи захисту інформації.

Традиційний і перевірений метод електронної комерції, який бере свій початок від звичайної торгівлі каталогами, - це оплата товарів і послуг кредитною карткою по телефону. У цьому випадку покупець замовляє на Вебсервері перелік товарів, які він хотів би придбати, а потім спілкується з номером телефону своєї кредитної картки продавцем продавця комерційної компанії. Тоді відбувається звичайна авторизація картки, а гроші списуються з рахунку покупця лише на момент відправлення товару поштою або кур’єром.

Для того, щоб покупець - власник кредитної картки міг без побоювань оплатити покупку через мережу, необхідно мати більш надійний, добре розроблений механізм захисту переказу електронних платежів. Такий принципово новий підхід передбачає негайну авторизацію та шифрування фінансової інформації в Інтернеті за допомогою схем SSL та SET.

Протокол SSL (Secure Socket Layer) забезпечує шифрування даних на рівні зв'язку даних.

Протокол захищених електронних транзакцій SET (Secure Electronic Transaction), розроблений Visa та MasterCard, шифрує виключно фінансову інформацію. Протягом півроку було обговорено протокол SET у цілому світу. Основна вимога, яка була йому пред'явлена, - забезпечення повної безпеки та конфіденційності угод. На сьогоднішній день технічні характеристи-

ки протоколу, що забезпечують безпеку, визнані мінімальними. Впровадження цього протоколу у нинішніх власників пластикових карт можливість використання комп'ютерних мереж у фінансових операціях, не побоюючись подальшої долі їхніх платіжних засобів.

Стандарт SET обіцяє значно збільшити продажі кредитних карток через Інтернет. Загальна сума, коли кістка потенційних покупців - власників карток Visa та MasterCard у всьому світі - перевищує 700 мільйонів людей. Забезпечення безпеки електронних транзакцій для такого пулу покупців може призвести до помітних змін, передбачено знижує вартість транзакцій для банків та комапаній що займаються процесингом компаній.

3.3 Особливості функціонування протоколу SET

Для забезпечення повної безпеки та конфіденційності транзакцій протокол SET повинен забезпечити виконання наступних умов.

1. Абсолютна конфіденційність інформації. Власники карток повинні бути впевнені, що їх платіжна інформація захищена та доступна лише вказаному одержувачу. Це неодмінна умова розвитку електронної комерції.

2. Повне зберігання даних. Учасники електронної комерції повинні забезпечити, щоб зміст повідомлення залишався незмінним при передачі від відправника адресату. "Власники картки надсилають повідомлення продавцям, що містять інформацію про замовлення, особисті дані та платіжні інструкції. Якщо хоча б один із компонентів зміниться під час передачі, ця транзакція НЕ буде оброблена належним чином. Тому, щоб уникнути помилок, протокол SET повинен забезпечити збереження та незмінність відправлених повідомлень Одним із таких засобів є використання цифрових підписів.

3. Аутентифікація (автентифікація) облікового запису власника картки. Використання цифрових підписів та засвідчених катів власника картки га-

рантує автентифікацію рахунку власника картки та підтвердження того, що власник картки є законним користувачем цього номера рахунку.

4. Власник картки повинен бути впевнений, що торговець дійсно має право здійснювати фінансові операції з фінансовою установою. Використання цифрових підписів та сертифікатів торговця гарантує власнику картки, безпечно вести електронні торги.

3.4 Учасники системи розрахунків і криптографічні засоби захисту транзакцій.

Протокол SET змінює спосіб взаємодії учасників системи розрахунків. У цьому випадку електронна транзакція починається з власника картки, а НЕ з продавця чи набувача.

Торговець пропонує товари для продажу або надані товари та послуги за певну плату. Протокол SET дозволяє продавцю пропонувати електронні взаємодії, якими власники карток можуть безпечно користуватися.

Еквайр (одержувач) - це фінансова установа, яка відкриває рахунок у продавця та обробляє авторизовані кредити та платежі за допомогою кредитної картки. Покупець обробляє платіжні повідомлення, надіслані продавцю за допомогою шлюзу платежів. У той же час протокол SET гарантує, що під час взаємодії, проведеної власником картки з продавцем, інформація про рахунок на кредитній картці залишатиметься конфіденційною.

Фінансові установи створюють асоціації банківських кредитних карток, які захищають та рекламують цей тип карт, створюють та застосовують правила користування кредитними картками та організовують мережі для з'єднання фінансових установ між собою.

Системи кредитних карток значною мірою зарекомендували себе як платіжний засіб придбання товарів безпосередньо у продавця. Основна відмінність використання кредитних карток в Інтернеті полягає в тому, що

відповідно до стандарту SET шифрування та процедури цифрового підпису використовуються для захисту електронних комерційних операцій.

Мережа Інтернет розрахована на одночасну роботу мільйонів користувачів, тому в комерційних Інтернет-додатках неможливо використовувати лише симетричні криптосистеми із секретними ключами (DES, ГОСТ 28147-89). У зв'язку з цим використовуються також асиметричні криптосистеми відкритого ключа. Шифрування за допомогою відкритих ключів означає, що у продавця та покупця є два ключі: один - це державний, який може бути відомий третім особам, а другий - приватний (секретний), відомий лише тілу.

Правила SET передбачають початкове шифрування повідомлення за допомогою випадково генерованого симетричного ключа, який, у свою чергу, шифрується відкритим ключем одержувача повідомлення. Результат - так званий електронний конверт. Одержувач повідомлення розшифровує електронний конверт за допомогою свого приватного (секретного) ключа для отримання симетричного ключа відправника. Далі симетричний ключ відправника використовується для розшифровки надісланого повідомлення. Цілісність інформації та автентифікація учасників угоди гарантується за допомогою електронного цифрового підпису.

Для захисту транзакцій від шахрайства та зловживань були створені спеціальні центри (агенції) Інтернет-сертифікації, які забезпечують, щоб кожен учасник електронної комерції отримав унікальний електронний сертифікат. У цьому сертифікаті за допомогою секретного ключа сертифікації зашифрований відкритий ключ цього учасника комерційної угоди. Сертифікат формується протягом певного часу, і для його отримання необхідно представити довідку про посвідчення особи учасника сертифікаційного центру (для юридичних осіб - їх юридичну реєстрацію), а потім, маючи відкритий ключ сертифікаційний центр з боку, беруть участь в операціях.

Розглянемо приклад шифрування. Торгова Аліса хоче надіслати зашифроване повідомлення про товар покупцеві Бобу у відповідь на його запит. Аліса передає опис продукту за допомогою однонаправленого алгоритму для

отримання унікальних знань, відомих як дайджест повідомлень. Це своєрідне цифрове враження від опису продукту, яке згодом буде використано для перевірки цілісності повідомлення. Потім Аліса шифрує цей дайджест повідомлень приватним (секретним) ключем підпису, щоб створити цифровий підпис.

Після цього Аліса створює довільний симетричний ключ і використовує його для шифрування опису продукту, її підпису та копії сертифіката, який містить її відкритий ключ для підписання. Щоб розшифрувати опис продукту, Боб потребує захищеної копії цього довільного симетричного ключа.

Сертифікат Боба, який Аліса повинна була отримати при започаткуванні безпечного зв'язку з ним, містить копію його ключа обміну відкритими ключами. Щоб забезпечити безпечну передачу симетричного ключа, Аліса шифрує його, використовуючи відкритий ключ Боба для обміну ключами. Зашифрований ключ, який називається цифровим конвертом, надсилається Бобу разом із зашифрованим повідомленням.

Нарешті, вона надсилає повідомлення Бобу, що складається з таких компонентів:

• симетрично зашифрований опис товару, підпис та ваш сертифікат;

• асиметрично зашифрований симетричний ключ (цифровий конверт).

Продовжуємо попередній приклад і розглядаємо процедуру дешифрування.

Боб отримує від Аліси зашифроване повідомлення і чекає, коли він розшифрує цифровий конверт своїм особистим (секретним) ключем для обміну ключами, щоб дістати симетричний ключ. Потім Боб використовує цей симетричний ключ, щоб розшифрувати опис продукту, підпис Аліси та її сертифікат. Потім Боб розшифровує цифровий підпис Аліси, використовуючи її відкритий ключ для підпису, який він отримує від її сертифіката. Таким чином, він відновлює оригінальний дайджест повідомлення з описом товару. Потім Боб передає опис продукту через той самий однонаправлений алго-

ритм, який використовувала Аліса, і отримує новий дайджест повідомлень із розшифрованого опису продукту.

Потім Боб порівнює свій дайджест повідомлень з даними, отриманими з цифрового підпису Аліси. Якщо вони точно збігаються, Боб отримує підтвердження того, що повідомлення НЕ змінилося в передачі зі змісту і що воно підписане за допомогою приватного ключа Аліси. Якщо дайджести НЕ відповідають, це означає, що повідомлення або було надіслано з іншого місця, або було змінено після його підписання. У цьому випадку Боб вживає певних дій, наприклад, повідомляє Алісі або відхиляє отримане повідомлення.

Протокол SET запроваджує нове застосування цифрових підписів цього, а саме використання подвійних цифрових підписів. У рамках протоколу SET використовуються подвійні цифрові підписи для повідомлення замовлення, надісланого торговцю, з платіжними структурами, що містять інформацію про рахунок і надсилаються в банк.

Наприклад, покупець Боб хоче надіслати комерсантці Алісі пропозицію придбати одиницю товару та уповноважити її банк перерахувати гроші, якщо Аліса прийме його пропозицію. У той же час Боб НЕ хоче, щоб банк читав умови його пропозиції так само, як він НЕ хоче, щоб Аліса читала інформацію про його рахунок. Крім того, Боб хоче зв’язати його пропозицію з переказом, щоб гроші переказали лише в тому випадку, якщо Аліса прийме його пропозицію.

Боб може здійснити все вищезазначене шляхом цифрового підписання обох повідомлень однією операцією підпису, що створює подвійний цифровий підпис. Подвійний цифровий підпис створюється шляхом формування дайджесту обох повідомлень, що з'єднує два повідомлення разом, обчислення дайджесту результатів попередніх операцій та шифрування цього дайджеста за допомогою операції особистого підпису, яка створює подвійний цифровий підпис. Подвійний цифровий підпис створюється шляхом формування дайджесту обох повідомлень, що з'єднує два повідомлення разом, обчислення

дайвінгу результату попередніх операцій та шифрування цього ключа для підпису автора. Автор також повинен включити дайджест іншого повідомлення, щоб одержувач перевірив подвійний підпис.

Одержувач будь-якого з цих повідомлень може перевірити його справжність, генеруючи дайджест із своєї копії повідомлення, пов'язуючи його з дайджестом іншого повідомлення (у порядку, наданому відправником) та обчислюючи дайджест для результату. Якщо новоствореному дайджесту відповідає подвійне розшифрування підпису, то одержувач може довіряти цілісності повідомлення.

Якщо Аліса приймає пропозицію Боба, вона може надіслати повідомлення банку, вказавши свою згоду і включивши дайджест повідомлення з пропозицією Боба. Банк може перевірити справжність дозволу Боба на передачу та датчик зв’язку за пропозицією Боба, наданою Алісою, щоб підтвердити подвійний підпис. Таким чином, банк може перевірити справжність пропозиції на підставі подвійного підпису, але банк не зможе прочитати умови пропозиції.

3.5 Використання сертифікатів.

Альтернативою безпечної передачі ключів є використання довіреної третьої сторони - органу з сертифікації (сертифікаційного агентства) - для підтвердження того, що відкритий ключ належить власнику картки.

Орган із сертифікації створює повідомлення, що містить ім'я власника картки та його відкритий ключ після того, як власник картки представив докази ідентифікації (посвідчення водія або паспорт). Це повідомлення називається сертифікатом. Сертифікат надається підписом центру сертифікації та містить інформацію про ідентифікацію власника, а також копію одного з відкритих ключів власника.

Учасники протоколу SET мають дві пари ключів і мають два сертифікати. Обидва сертифікати створюються та підписуються одночасно органом із сертифікації.

Сертифікати власників карт функціонують як електронний еквівалент кредитних карт. Вони цифрово підписуються фінансовою установою, тому їх не може змінювати третя сторона. Ці сертифікати містять номер рахунку та термін дії, шифруються за допомогою однонаправленого алгоритму хешування. Якщо номер рахунку та дата закінчення терміну дії відомі, то зв’язок із сертифікатом можна підтвердити, однак цю інформацію неможливо отримати, вивчаючи цей сертифікат. Відповідно до протоколу SET, власник картки надає інформацію про обліковий запис до шлюзу платежів, де здійснюється це з'єднання.

Сертифікат видається власнику картки лише з дозволу фінансової установи - емітента картки. Просивши сертифікат, власник картки вказує намір використовувати електронні торги. Ці сертифікати передаються торговцям разом із запитами на покупку та за зашифрованими інструкціями про оплату. Коли продавець отримає свідоцтво про право власності на карту, він може не сумніватися, що номер рахунку підтверджено фінансовою установою.

Сертифікати торговців - це електронний аналог картини компанії, яка відображається у вікні електронного магазину. Ці сертифікати цифровим чином підписуються фінансовою установою продавця і, отже, НЕ підлягають зміні третьою стороною. Сертифікати служать гарантією того, що продавець має дійсну угоду з набувачем.

Торговець повинен мати принаймні одну пару сертифікатів для участі в операційному середовищі SET, але один торговець може мати багато пар сертифікатів для кожного виду кредитної картки, який він приймає для оплати.

Сертифікати на шлюз платежів видаються набувачем або їх розробниками для систем, які обробляють авторизацію та отримують повідомлення. Ключ шифрування для певного інтерфейсу, який власник картки отримує від

цього сертифіката, використовується для захисту інформації про обліковий запис власника картки. Сертифікати платіжного інтерфейсу видаються набувачеві оператором карт певного типу.

Сертифікати набувача видаються набувачем, щоб він міг приймати та обробляти запити сертифікатів, ініційовані торговцями. Покупці отримують сертифікацію від кожної асоціації кредитних карток.

Сертифікати емітента необхідні емітентам для того, щоб користуватися послугами центру сертифікації, який може приймати та обробляти запити на сертифікати безпосередньо від власників карток через державні та приватні мережі. Емітенти отримують сертифікати від асоціації кредитних карток.

Сертифікати SET перевіряються в ієрархії довіри (рис. 9.9). Кожен сертифікат асоціюється з сертифікатом підпису об'єкта, який надав йому цифровий підпис. Дотримуючись «дерева довіри» до відомої довіреної сторони, ви можете бути впевнені, що сертифікат дійсний. Наприклад, сертифікат власника картки асоціюється з сертифікатом емітента (або асоціації від імені емітента), який, у свою чергу, асоціюється з кореневим ключем через сертифікат асоціації.

Відкритий ключ для кореневого підпису відомий усім про програмне забезпечення SET і може використовуватися для перевірки кожного з сертифікатів. Кореневий ключ буде поширюватися в сертифікаті з автоматичним підписом. Цей сертифікат кореневого ключа буде доступний постачальникам програмного забезпечення для включення до їх програмних засобів.

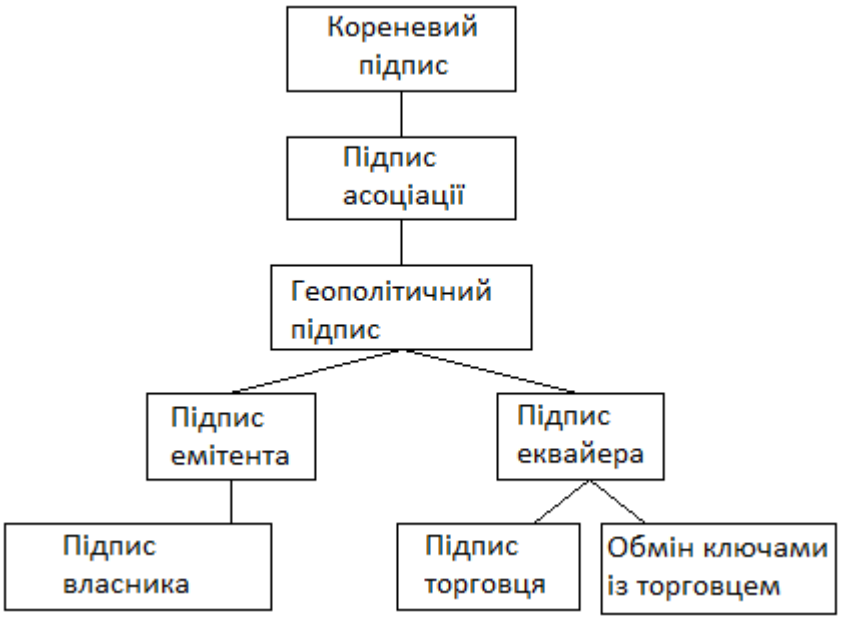


Рис. 9. Ієрархічне дерево довіри

Протокол SET визначає безліч протоколів транзакцій, які використовують криптографічні засоби для без запасних ведення електронної комерції. Серед цих протоколів транзакцій - реєстрація власника картки, реєстрація кому мерсанта, запит про покупку, авторизація платежу, отримання платежа.

Нові досягнення в області безпеки використання кредитних карток, реалізовані в стандарті SET, здатні задовольнити самих недовірливих клієнтів електронних пла тіжних систем, оскільки усуваються всі їх побоювання шляхом впровадження засобів шифрування для скремблювання кредитної картки в такому порядку, щоб її могли читати тільки продавець і покупець.

Системи такого типу мають ряд переваг.

- Гроші клієнта знаходяться під надійним наглядом б анка. Якщо клієнт втратить картку, то його рахунок все одно пов'язаний з його ім'ям. В відміну від систем з використанням готівки у банку є можливість перевірити залишок на рахунку клієнта, тому гроші клієнта НЕ втрачаються.
- Відпадає необхідність в відкритті нового рахунку . У банку для обробки транзакцій даного типу клієнт може продовжувати користуватися

чинним рахунком і кредитної карткою . Цей фактор має велике значення на початкових стадіях електронної торгівлі в WWW мережі Internet.

Однак є і недолік, причому істотний - від присутність конфіденційності. На відміну від транзакцій з електронною готівкою, які є анонімними, в транзакціях з кредитними картами ім'я клієнта жорстко пов'язано зі рахунком.

3.6 Технологічні рішення для електронної торгівлі.

В даний час найбільше поширення в світі отримали два типи програмно - апаратних рішення, запропоновані компаніями Microsoft, Netscape, VeriFone і Ingenico. Всі ці рішення передбачають використання дотримуюся певного набору програмних компонентів :

- Клієнтський комп'ютер , який має доступ до Internet і Web - brouser ;
- Сервер мережі електронної торгівлі, на якому ведеться журнал товарів і приймаються електронні зашифровані запити клієнтів на покупку тих чи інших товарів;
- Засіб для забезпечення взаємної конвертації протоколів Internet і стандартних протоколів авторизації (ISO 8583 і ін.).

Розглянемо реалізацію даної схеми на прикладі про дуктів Microsoft (Merchant Server) і VeriFone (vPOS і vGate). Про програмним забезпечення vPOS встановлюється на робочій станції клієнта і здійснює підтримку протоколу SET, шифрування і аутентифікацію інформації, отримання необхідних сертифіковані катів і ін .

Microsoft Merchant Server крім зазначених вище функцій ведення каталогу і прийому запитів клієнтів здійснює зв'язок з іншим продуктом VeriFone - vGate . Програмне забезпечення vGate, отримуючи запити в форматі SET, розшифровує їх і конвертує в формат ISO 8583. Таким чином, стає віз можна здійснювати платежі в мережі Internet з використанням звичайних кредитних карт. Слід зазначити, що описані вище рішення є по суті адапта-

цією технологій кредитних карт, існую щих ще з 60 х років, до сучасним електронним технологіям.

Альтернативний шлях - впровадження концепції " чисто " елек тронних грошей , концепції DigiCash і CyberCash . Електронні гроші представляють собою спеціальну послідовність електронних деномінацій і електронних підписів , підготовлений них банками . Системи , подібні DigiCash , CyberCash і NetCash, дозволяють клієнтам вносити реальні гроші на банківський рахунок, після чого використовувати цю готівку в електронній формі для придбання різних товарів через Internet . Клієнт банку за водить віртуальний електронний " гаманець ", помістивши в нього визна поділену суму грошей. Клієнти системи DigiCash в якості ек вівалента будь дрібної монети отримують 64 бітовий номер , до торий потім переводиться на жорсткий диск конкретного користувача . Подальша оплата товарів і послуг здійснює ся перерахуванням відповідної бітової інформації . Клієнт може перераховувати цю електронну готівку продавцям в Internet (якщо даний продавець згоден з такою формою оплати). Потім продавець повертає електронну готівку банку в про мен на справжні гроші .

До переваг систем такого типу відносяться :

- Конфіденційність (рух електронної готівки нель зя простежити ; банк НЕ пов'язує номери з яким - або кін конкретним особою , тому НЕ може розкрити інкогніто пла тельщіка);
- Гарантована безпека для банків (будь- покупець може витратити тільки ту суму , яку він має на рахунку).

Недоліком транзакцій описаного типу є те, що електронні гроші нічим НЕ гарантовані. Наприклад, якщо ж стки диск комп'ютера виходить з ладу, або розоряється електронний банк, або хакери розшифровують номери електронної готівки, у всіх цих випадках немає ніякого способу повернути втрачену клієнтом готівку. Оскільки банк НЕ пов'язує гроші з ім'ям клієнта , він НЕ може компенсувати втрати клієнта.

Іншим технологічним рішенням є система платежів з використанням смарт - карт Mondex , яку нещодавно придбала компанія MasterCard . В відміну від традиційних пла тіжних систем система на основі смарт - карт Mondex передбачає емісію електронних грошей, які поміщаються на смарт - карту і можуть листуватися на інші смарт - карти, зніматися з карти в пункtах продажу і т. д. Ще одним відмінністю системи Mondex від інших платіжних систем типу "електронний гаманець" є анонімність платежів. Однак слід мати в виду, що у багатьох країнах законодавчо заборонені анонімні платежі на великі суми.

В системі Mondex вирішені і проблеми конвертації валюти. У кожної з країн, що приєдналися до цього проекту, плани руется організувати спеціальний банк, який буде емітує вать електронну готівку. При перекладі коштів з однієї ва люті в іншу в системі організується спеціальна транзакція між електронними банками двох країн. Перерахунок здійснюва ляется по офіційному курсу, а потім на карту клієнта поміщені ється діюча сума в іншій валюті.

РОЗДІЛ 4.
ОХОРОНИ ПРАЦІ

1. Основні поняття терміни та визначення у галузі охорони праці

Однією зі специфічних форм людської діяльності є трудова діяльність, під якою розуміється не лише праця в класичному її розумінні, а будь-яка діяльність (наукова, творча, художня, надання послуг тощо), якщо вона здійснюється в рамках трудового законодавства.

Важкість та напруженість праці є одними з головних характеристик трудового процесу.

Під час виконання людиною трудових обов‘язків на неї діє сукупність фізичних, хімічних, біологічних та соціальних чинників. Ці чинники звуться виробничим середовищем.

Сукупність чинників трудового процесу і виробничого середовища, які впливають на здоров‘я і працездатність людини під час виконування нею трудових обов‘язків складають умови праці.

Під безпекою розуміється стан захищеності особи та суспільства від ризику зазнати шкоди.

Реальне виробництво супроводжується шкідливими та небезпечними чинниками (факторами) і має певний виробничий ризик. Виробничий ризик – це ймовірність ушкодження здоров‘я працівника під час виконання ним трудових обов‘язків, що зумовлена ступенем шкідливості та/або небезпечності умов праці та науково-технічним станом виробництва.

Поділення несприятливих чинників виробничого середовища на шкідливі та небезпечні зумовлене різним характером їх дії на людський організм, тим, що вони потребують різних заходів та засобів для боротьби з ними та профілактики викликаних ними ушкоджень, а також рядом причин організаційного характеру. В той же час між шкідливими та небезпечними виробничими факторами інколи важко провести чітку межу. Один і той же чинник може ви-

кликати травму і профзахворювання (наприклад, високий рівень іонізуючого або теплового випромінювання може викликати опік або навіть призвести до миттєвої смерті, а довготривала дія порівняно невисокого рівня цих же факторів – до хвороби; пилинка, що потрапила в око, спричиняє травму, а пил, що осідає в легенях, – захворювання, що зветься пневмоконіоз). Через це всі несприятливі виробничі чинники часто розглядаються як єдине поняття – небезпечний та шкідливий виробничий фактор (НШВФ).

За своїм походженням та природою дії НШВФ можна поділити на 5 груп: фізичні, хімічні, біологічні, психофізіологічні та соціальні.

Один і той же НШВФ за природою своєї дії може належати водночас до різних груп.

Однією з причин появи НШВФ є небезпечні речовини.

Безпека праці – такий стан умов праці, при яких виключена дія на працюючого небезпечних та шкідливих виробничих факторів.

Виходячи з того, що в житті, а тим більше у виробничому процесі, абсолютної безпеки не існує, нерозумно було б вимагати від реального виробництва повного викорінення травматизму, виключення можливості будь-якого захворювання. Але реальним і розумним є ставити питання про зведення до мінімуму впливу об'єктивно існуючих виробничих небезпек. Цю задачу вирішує охорона праці – система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини в процесі трудової діяльності.

Структурно до модулю „Охорона праці” входять наступні складові частини:

- правові та організаційні основи;
- фізіологія, гігієна праці та виробнича санітарія;
- виробнича безпека;
- пожежна безпека на виробництві.

Правові та організаційні основи охорони праці являють собою комплекс взаємозв’язаних законів та нормативно-правових актів, соціально-

економічних та організаційних заходів, спрямованих на правильну і безпечну організацію праці, забезпечення працюючих засобами захисту, компенсацію за важку роботу та роботу в шкідливих умовах, навченість працівників безпечному веденню робіт, регламентацію відповідальності та відшкодування працюючим шкоди в разі ушкодження їх здоров‘я.

Фізіологія, гігієна праці та виробнича санітарія - комплекс організаційних, гігієнічних і санітарно-технічних заходів та засобів, спрямованих на запобігання або зменшення дії на працюючих шкідливих виробничих факторів.

Виробнича безпека – безпека від нещасних випадків та аварій на виробничих об‘єктах і від їх наслідків.

Пожежна безпека на виробництві - комплекс заходів та засобів, спрямованих на запобігання запалювань, пожеж та вибухів у виробничому середовищі, а також на зменшення негативної дії небезпечних та шкідливих факторів, які утворюються в разі їх виникнення.

2. Законодавство України у галузі охорони праці

Законодавство України про охорону праці являє собою систему взаємозв'язаних нормативно-правових актів, що регулюють відносини у галузі реалізації державної політики щодо правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. Воно складається з Закону України «Про охорону праці», Кодексу законів про працю України, Закону України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності" та прийнятих відповідно до них нормативно-правових актів.

Базується законодавство України про охорону праці на конституційному праві всіх громадян України на належні, безпечні і здорові умови праці, гарантовані статтею 43 Конституції України.

Інші статті Конституції встановлюють право громадян на соціальний захист, що включає право забезпечення їх у разі повної, часткової або тимчасової втрати працездатності (ст. 46); охорону здоров'я, медичну допомогу та медичне страхування (ст. 49); право знати свої права та обов'язки (ст. 57) та інші загальні права громадян, в тому числі, право на охорону праці.

Основоположним документом в галузі охорони праці є Закон України «Про охорону праці», який визначає основні положення щодо реалізації конституційного права працівників на охорону їх життя і здоров'я у процесі трудової діяльності, на належні, безпечні і здорові умови праці, регулює за участю відповідних державних органів відносини між роботодавцем і працівником з питань безпеки, гігієни праці та виробничого середовища і встановлює єдиний порядок організації охорони праці в Україні. Інші нормативні акти мають відповідати не тільки Конституції та іншим законам України, але, насамперед, цьому Законові.

Відповідно до Конституції України, Закону України «Про охорону праці» та Основ законодавства України про загальнообов'язкове державне соціальне страхування у 1999 р. було прийнято Закон України «Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності». Цей закон визначає правову основу, економічний механізм та організаційну структуру загальнообов'язкового державного соціального страхування громадян від нещасного випадку на виробництві та професійного захворювання, які призвели до втрати працездатності або загибелі застрахованих на виробництві.

До основних законодавчих актів про охорону праці слід віднести також "Основи законодавства України про охорону здоров'я", що регулюють суспільні відносини в цій галузі з метою забезпечення гармонічного розвитку

фізичних і духовних сил, високої працездатності і довголітнього активного життя громадян, усунення чинників, які шкідливо впливають на їхнє здоров‘я, попередження і зниження захворюваності, інвалідності та смертності, поліпшення спадкоємності. “Основи законодавства України про охорону здоров‘я” передбачають встановлення єдиних санітарно-гігієнічних вимог до організації виробничих та інших процесів, пов‘язаних з діяльністю людей, а також до якості машин, устаткування, будинків та таких об‘єктів, що можуть шкідливо впливати на здоров‘я людей (ст. 28); вимагають проведення обов‘язкових медичних оглядів осіб певних категорій, в тому числі працівників, зайнятих на роботах із шкідливими та небезпечними умовами праці (ст. 31); закладають правові основи медико-соціальної експертизи втрати працездатності (ст. 69).

Крім вищезазначених законів, правові відносини у сфері охорони праці регулюють інші національні законодавчі акти, міжнародні договори та угоди, до яких Україна приєдналася в установленому порядку, підзаконні нормативні акти: Укази і розпорядження Президента України, рішення Уряду України, нормативні акти міністерств та інших центральних органів державної влади. На сьогодні кілька десятків міжнародних нормативних актів та договорів, до яких приєдналася Україна, а також більше сотні національних законів України безпосередньо стосуються або мають точки перетину із сферою охорони праці. Майже 200 підзаконних нормативних актів прийнято у відповідності з Законом “Про охорону праці” для регулювання окремих питань охорони праці. Всі ці документи створюють єдине правове поле охорони праці в країні.

3. Нормативно-правова база охорони праці

Конкретні вимоги охорони праці до виробничого середовища, обладнання, устаткування, порядку ведення робіт, засобів захисту працюючих, порядку навчання працюючих тощо регламентуються відповідними нормативно-

правовими актами, які розробляються у відповідності з законодавством про охорону праці і становлять нормативно-технічну базу охорони праці.

Нормативно-правовий акт – це офіційний документ компетентного органу державної влади, яким встановлюються загальнообов‘язкові правила (норми). Законом України “Про охорону праці” визначено, що нормативно-правові акти з охорони праці (НПАОП)- це правила, норми, регламенти, положення, стандарти, інструкції та інші документи, обов'язкові для виконання.

Стандарти, технічні умови та інші документи на засоби праці і технологічні процеси повинні включати вимоги щодо охорони праці і погоджуватися з органами державного нагляду за охороною праці.

Серед нормативно-правових актів з охорони праці важливе місце посідають державні стандарти України (ДСТУ) та відповідні нормативні акти (правила, норми, інструкції тощо) у тому числі і колишнього Радянського Союзу, які є чинними в Україні на даний час.

Починаючи з 1972 р. в СРСР була розроблена і впроваджена в дію Система стандартів безпеки праці, а її стандарти складали окрему – 12-у групу Єдиної Державної Системи стандартів СРСР, яка мала назву “Система стандартов безопасности труда” (ССБТ). Відповідно до Угоди про співробітництво в галузі охорони праці, укладеної керівниками урядів держав СНД у грудні 1994 року, ця система продовжує розвиватись та удосконалюватись на міждержавному рівні, а її стандарти надалі визнаються Україною як міждержавні стандарти за узгодженим переліком. Ці стандарти внесені до Державного реєстру окремою групою під рубрикою «Міждержавні стандарти системи стандартів безпеки праці».

Нормативні акти з охорони праці підприємств

Власники підприємств, установ, організацій або уповноважені ними органи розробляють на основі нормативно-правових актів і затверджують власні но-

рмативні акти з охорони праці, що діють в межах даного підприємства, установи, організації. Нормативні акти підприємства конкретизують вимоги нормативно-правових актів і не можуть містити вимоги з охорони праці менші або слабкіші ніж ті, що містяться в державних нормах.

До основних нормативних актів підприємства належать:

- Положення про систему управління охороною праці на підприємстві.
- Положення про службу охорони праці підприємства.
- Положення про комісію з питань охорони праці підприємства.
- Положення про навчання, інструктаж і перевірку знань працівників з питань охорони праці.
- Наказ про порядок атестації робочих місць щодо 'їх відповідності нормативних актів про охорону праці.
- Інструкції з охорони праці для працюючих за професіями і видами робіт.
- Інструкції про порядок зварювання і проведення інших вогневих робіт на підприємстві.
- Загальнооб'єктові та цехові інструкції про заходи пожежної безпеки.
- Перелік робіт з підвищеною небезпекою.
- Перелік посадових осіб підприємства, які зобов'язані проходити попередню і періодичну перевірку знань з охорони праці.
- Наказ про порядок забезпечення працівників підприємства спецодягом, спецвзуттям та іншими засобами індивідуального захисту.

Відповідальність за порушення законодавства про охорону праці

Закон України “Про охорону праці” передбачає, що за порушення законів та інших нормативно-правових актів про охорону праці, створення перешкод у діяльності посадових осіб органів державного нагляду за охороною праці, а також представників профспілок, їх організацій та об'єднань винні

особи притягаються до дисциплінарної, адміністративної, матеріальної та кримінальної відповідальності.

Дисциплінарна відповідальність полягає в тому, що на винного працівника накладається дисциплінарне стягнення. Ст. 147 КЗпПУ встановлює два види дисциплінарного стягнення: догана та звільнення з роботи. Законами, уставами та положеннями про дисципліну, які діють в деяких галузях (транспорт, гірничодобувна промисловість тощо), можуть бути передбачені для окремих категорій працівників інші дисциплінарні стягнення.

Адміністративна відповідальність настає за будь-які посягання на загальні умови праці. Відповідно до ст. 41 Кодексу України про адміністративні правопорушення порушення вимог законів та нормативно-правових актів з охорони праці тягне за собою адміністративну відповідальність у вигляді накладання штрафу на працівників та, зокрема, посадових осіб підприємств, установ, організацій, а також громадян - власників підприємств чи уповноважених ними осіб.

Матеріальна відповідальність робітників і службовців регламентується КЗпПУ та іншими нормативними актами, які торкаються цієї відповідальності у трудових відносинах.

Загальними підставами накладення матеріальної відповідальності на працівника є

- наявність прямої дійсної шкоди,
- провина працівника (у формі наміру чи необережності),
- протиправні дії (бездіяльність) працівника,
- наявність причинного зв'язку між винуватим та протиправними діями (бездіяльністю) працівника та заподіяною шкодою.

На працівника може бути накладена відповідальність лише при наявності всіх перелічених умов; відсутність хоча б однієї з них виключає матеріальну відповідальність працівника.

Притягнення працівника до кримінальної, адміністративної і дисциплінарної відповідальності за дії, якими нанесена шкода, не звільнює його від матеріальної відповідальності.

При наявності в діях працівника, яким порушені правила охорони праці, ознак кримінального злочину, на нього може бути покладена повна матеріальна відповідальність, а при відсутності таких ознак на нього покладається відповідальність в межах його середнього місячного заробітку.

Кримінальна відповідальність за порушення правил охорони праці передбачена ст.ст. 271 – 275 КК України, що об‘єднані в розділ Х “Злочини проти безпеки виробництва”.

Кримінальна відповідальність настає не за будь-яке порушення, а за порушення вимог законів та інших нормативно-правових актів про охорону праці, якщо це порушення створило загрозу загибелі людей чи настання інших тяжких наслідків або заподіяло шкоду здоров'ю потерпілого чи спричинило загибель людей або інші тяжкі наслідки.

Порушення вимог законодавчих та інших нормативно-правових актів, передбачених вищезазначеними статтями КК України, карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на строк до п‘яти років, або позбавленням волі на строк до дванадцяти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

ВИСНОВОК

В ході даної магістерської роботи було визначено схему роботи, вразливі місця, слабкості та засоби захисту систем виявлення вторгнень. Була досліджена модель системи яка охоплює значну область в корпоративній мережі та надає надійний захист як від внутрішніх аномалій так і від зовнішніх атак. Використовуючи здобуті данні мною було винесено декілька висновків.

Системи, які направлені на захист інформації як відкритої, так і з обмеженим доступом, повинні складатися з програмних та апаратних засобів, які забезпечують аналіз, моніторинг, контроль інформаційно-телекомунікаційної системи. До таких засобів відноситься: міжмережеві екрани, антивірусні системи, системи виявлення та запобігання вторгнень, різновидні сенсори та датчики, інші спеціалізовані рішення.

Для існуючих ІТС є багато підходів до побудови комплексного захисту, його необхідно обирати в залежності від розміру ІТС. Для невеликих ІТС – достатньо буде обмежитись налаштуванням міжмережевого екрану та антивірусної системи, для середніх і великих, наприклад, хостинг провайдер – необхідно застосувати більш суттєві механізми захисту, такі як: системи виявлення та запобігання вторгнень.

Також не слід забувати про фахівцій та спеціалістів які розгортають, налаштовують та керують системою виявлення вторгнень. Як би власнику не хотілося якомога швидше встановити всю систему, це треба робити не тороплячись та поступово. Сама система відслідковування подій не складна та

досить проста в використанні та встановленні, але сама важка частина в IDS системах – це аналіз та розпізнавання самих втручань та аномалій, оскільки те що для людини виглядає звичайно – система може розпізнати як напад. Проблема визначення атак стоїть перед фахівцями і досі та постійно буде повертатися тому як злодії не стоять на місці та все більше покращюють свої підходи або маскування.

ВИСНОВОК

В ході даної бакалаврської роботи було проаналізовано відомі загрози вторгнення при проведенні операцій по платіжним картам, проведено аналіз найбільш поширених та наведено ряд методів попередження та усунення таких небезпек, розглянуто схеми проведення операцій по платіжним терміналам, банкоматам та принципів їх захисту.

Використовуючи здобуті данні мною було зроблено декілька висновків.

Актуальність проблеми захисту платіжних карток від викрадення коштів, або використання у несанкціонованних платіжних операціях зростає з кожним роком. Особливо це актуально при використанні платіжних карток з безконтактними технологіями зв'язку. Разом із ускладненням технологій звязку та інформаційних технологій постійно зростає витонченність шахрайських схем, тому виключно необхідний постійний аналіз таких випадків несанкціонованного вторгнення, атак зловмисників та виявлених вразливостей безконтактних засобів платежу, ідентифікації, доступу, керування, тощо.

Разом із необхідністю боротьби з атаками зловмисників особливого значення на сьогоднішній день набувають засоби попередження та профілактики.

Таким засобам, їх аналізу та застосуванню і була присвячена ця робота.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ахрамович В.М., Сіренко О.О. Підвищення ефективності криптографічного захисту інформації у локальній мережі об’єкта інформаційної діяльності за допомогою комплексу користувача ЦСК «ІІТ Користувач ЦСК-1».
2. Ахрамович В.М., Амелькін С.В. Системи захисту інформації приватного підприємства. Організація служби захисту інформації приватного підприємства.
3. Ахрамович В.М., Чегренець В.М. Управління ризиками інформаційної безпеки комерційного банку, 2019.
4. Mattord, Verma; "Principles of Information Security." / Verma Mattord, 300p, 2008
5. Sen, Sevil; "Power-Aware Intrusion Detection in Mobile Ad Hoc Networks" / Sevil Sen, John E. Clark, Juan Tapaidor, York , 2006 Access: http://wwwusers.cs.york.ac.uk/~jac/PublishedPapers/AdhocNetsFinal.pdf
6. Anderson, Ross; Security Engineering: A Guide to Building Dependable Distributed Systems./ Ross Anderson, New York: pp. 387–388., 2007
7. Mazzariello, C., Bifulco, R., Canonico, R.: Integrating a network IDS into an open source computing environment. In: Sixth International Conference on Information Assurance and Security (IAS), pp. 265–270. IEEE Publisher, Atlanta, GA (2010)
8. B. Schneier and A. Shostack. Breaking up is hard to do. Modeling security threats for smart cards. In First USENIX Symposium on Smart Cards, USENIX Press, October 1999.
9. U.S. government smart card handbook. Office of Governmentwide Policy, General Services Administration, February 2004.
10. Howard Gobioff, Sean Smith, J. Doug Tygar, and Bennet Yee. Smart cards in hostile environments. In Proc. Workshop on Electronic Commerce, 1996.

11. Anderson, Ross; Security Engineering: Radio frequency devices. FCC Part 15, New York: pp. 387–388., 2001
12. Klaus Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley & Sons, 2003.
13. T. W. H. Fockens. NEDAP - system model for inductive ID systems. NEDAP R&D, Groenlo, The Netherlands, October 2000.
14. Conference of Postal and Telecommunications Administrations (CEPT), Feb ruary 1999.
15. Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. RFID Systems and Security and Privacy Implications. In Workshop on Cryptographic Hardware and Embedded Systems (CHES), LNCS 2523, pages 454 of 470. Springer-Verlag, 2002.
16. Stephen A. Weis. Security and Privacy in Radio-Frequency Identification Devices. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, May 2003.
17. Smart Card Alliance. Конфіденційність та захищені системи ідентифікації: роль смарт-карт як технології, що забезпечує конфіденційність, February 2003. [Електронний ресурс]. – Режим доступу: http://www.smartcardalliance.org/
18. Smart Card Alliance. Press releases, 2003.2004. [Електронний ресурс]. – Режим доступу http://www.smartcardalliance.org/about_alliance/alliance_press.cfm.
19. Relating to the use of short range devices (SRD). CEPT 70-03, October 2004. [Електронний ресурс]. – Режим доступу: http://www.ero.dk/documentation/docs/doc98/official/pdf/REC7003E.PDF .
20. Nokia launches mobile RFID kit, 19 March 2004. [Електронний ресурс]. – Режим доступу: http://www.computerweekly.com/Article129304.htm .
21. Near _eld communication (NFC). ECMA/TC32-TG19/2004/28; ECMA/GA/2004/67, June 2004. [Електронний ресурс]. – Режим доступу: http://www.ecma- international.org .

22. Creating a Complete Model of an Intrusion Detection System effective on the LAN [Електронний ресурс]. – Режим доступу: https://thesai.org/Downloads/Volume3No5/Paper_23-Creating_a_Complete_Model_of_an_Intrusion_Detection_System_effective_on_the_LAN.pdf
23. An Overview of Intrusion Detection Systems [Електронний ресурс]. – Режим доступу: http://www.idt.mdh.se/kurser/ct3340/ht09/ADMINISTRATION/IRCSE09-submissions/ircse09_submission_18.pdf
24. Security technology: Where's the smart money? The Economist, pages 69.70, 7 February 2002
25. Tests reveal e-passport security _aw, 30 August 2004 [Електронний ресурс]. – Режим доступу: http://www.eetimes.com/sys/showArticle.pdf
26. Intrusion Detection Systems [Електронний ресурс]. – Режим доступу: http://www.uni-wuerzburg.de/fileadmin/10030200/IDS.pdf
27. EUROSMART. The voice of the smart card industry. [Електронний ресурс]. – Режим доступу: http://www.eurosmart.com/http://www.europe-smartcard.pdf
28. Guardian Unlimited. The magic of touch, 15 July 2004. [Електронний ресурс]. – Режим доступу: http://ena.lp.edu.ua/bitstream/ntb/1/16-98-104.pdf
29. Common criteria for information technology security evaluation. ISO/IEC 15408; CCIMB-99-031, CCIMB-99-032, CCIMB-99-033, August 1999.
30. A. Shukla. Feasibility study into the measurement of man-made noise. Radiocommunications Agency (DERA), UK Ministry of Defence, AY 3952, March 2001.
31. Mattord, Verma; "Principles of Information Security." / Verma Mattord, 300p, 2008 . [Електронний ресурс]. – Режим доступу: http://www.ti-rfid.com .
32. Mazzariello, C., Bifulco, R., Canonico, R.: Integrating a network IDS into an open source computing environment. In: Sixth International Conference

on Information Assurance and Security (IAS), pp. 265–270. IEEE Publisher, Atlanta, GA (2010)

33. Bakshi, A., Yogesh, B.: Securing cloud from DDOS Attacks using Intrusion detection system in virtual machine. In: Second International Conference on Communication Software and Networks, IEEE Computer Society, pp. 260–264 (2010)
34. HF antenna cookbook. Technical Application Report 11-08-26-001, Texas Instruments, January 2004. [Електронний ресурс]: http://www.ti-rfid.com.
35. Технология NFC - связь на близких расстоянии [Электронный ресурс]. - Режим доступа: http://www.russianelectronics.ru

ДОДАТОК А - ПРЕЗЕНТАЦІЯ