Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Добровольського Дмитра Михайловича*

академічної групи *125м-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Безпека операцій з платіжними терміналами*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Герасина О. В.			
розділів:				
спеціальний	ас. Мілінчук Ю.А..			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Добровольському Д. М.* **академічної групи** *125м-17-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Безпека операцій з платіжними терміналами*

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.18 № 2025-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *Платіжні термінали*

Предмет досліджень *Проведення операцій з платіжними терміналами*

Мета *Забезпечення безпеки операцій з платіжними терміналами*

Вихідні дані для проведення роботи *Матеріали науково-дослідної переддипломної практики*

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна *Аналіз атак і вразливостей платіжних терміналів, розробка методик безпечного проведення операцій з платіжними терміналами*

Практична цінність ***впровадження розроблених методик безпечного проведення операцій з платіжними терміналами та підвищення рівня освідченності громадян у данному питанні***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

результати роботи повинні відповідати вимогам чинного законодавства України та методичним рекомендаціям до підготовки та захисту дипломної роботи магістрів спеціальності «Кібербезпека»

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Огляд джерел за темою та напрям досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-24.11.18
Виконання економічного розділу	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***полягає у забезпеченні зменшення збитків від атак на платіжні термінали***

Соціальний ефект ***підвищення рівня довіри користувачів до проведення Операцій з платіжними терміналами та підвищенні репутації банків***

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ к.т.н., доц. Герасина О. В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Добровольський Д. М.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: __ с., __ рис., 4 додатки, 11 джерел.

Об’єкт дослідження: Платіжні термінали - банкомати, термінали самообслуговування, POS-термінали.

Мета дипломної роботи: забезпечення безпеки проведення операцій з платіжними терміналами.

У першому розділі дипломної роботи проаналізовано види платіжних терміналів, проаналізовано їх склад, схему роботи, проаналізовано основні види атак.

У спеціальній частині дипломної роботи проаналізовані можливі атаки на платіжні термінали, розроблені методики захисту від данних атак, розроблен ряд вирішення типових проблем у роботі платіжних терміналів, створені методики безпечного проведення операцій з платіжними терміналами.

У економічній частині були розраховані витрати на реалізацію методик, щодо безпечного проведення операцій з платіжними терміналами.

Практична значимість дипломної роботи полягає у впровадженні розроблених методик безпечного проведення операцій з платіжними терміналами для підвищення рівня освідченності громадян у данному питанні та впровадженні методів захисту від типових атак на платіжні термінали.

БЕЗПЕКА ОПЕРАЦІЙ З ПЛАТІЖНИМИ ТЕРМІНАЛАМИ, БАНКОМАТИ, ТЕРМІНАЛИ САМООБСЛУГОВУВАННЯ, POS-ТЕРМІНАЛИ.

РЕФЕРАТ

Пояснительная записка: __ с., __ рис., 4 додаткы, 11 источников.

Объект исследования: Платежные терминалы - банкоматы, терминалы самообслуживания, POS-терминалы.

Цель дипломной работы: обеспечение безопасности проведения операций с платежными терминалами.

В первой главе дипломной работы проанализированы виды платежных терминалов, проанализированый их состав, схема работы, проанализированы основные виды атак.

В специальной части дипломной работы проанализированы возможные атаки на платежные терминалы, разработаны методики защиты от данных атак, разработан ряд решения типичных проблем в работе платежных терминалов, созданные методики безопасного проведения операций с платежными терминалами.

В экономической части были рассчитаны затраты на реализацию методик, по безопасному проведению операций с платежными терминалами.

Практическая значимость дипломной работы заключается во внедрении разработанных методик безопасного проведения операций с платежными терминалами для повышения уровня освидченности граждан в данном вопросе и внедрении методов защиты от типичных атак на платежные терминалы.

БЕЗОПАСНОСТЬ ОПЕРАЦИЙ С ПЛАТЕЖНЫМИ ТЕРМИНАЛАМИ, БАНКОМАТЫ, ТЕРМИНАЛЫ САМООБСЛУЖИВАНИЯ, POS-ТЕРМИНАЛОВ.

ABSTRACT

Explanatory note: __ p., __ pic., 4 annexes, 11 sources.

Object of research: Payment terminals - ATMs, self-service terminals, POS-terminals.

The purpose of the thesis: to ensure the security of transactions with payment terminals.

The first chapter of the thesis analyzes the types of payment terminals, analyzes their composition, scheme of work, analyzes the main types of attacks.

The special part of the thesis analyzes possible attacks on payment terminals, developed methods of protection against these attacks, developed a series of solutions to typical problems in the work of payment terminals, created methods for safe operation of transactions with payment terminals.

In the economic part, costs for the implementation of techniques, for the safe conduct of operations with payment terminals were calculated.

The practical significance of the dissertation is the introduction of developed techniques for the safe conduct of transactions with payment terminals in order to increase the level of citizen's accountability in this matter and the introduction of methods of protection against typical attacks on payment terminals.

SAFETY OF OPERATIONS WITH PAYMENT TERMINALS, BANKS, TERMINALS OF SELF-SERVICE, POS-TERMINALS.

ЗМІСТ

ВСТУП

На даний момент термінали стали невід'ємною частиною життя і широко поширені в усьому світі. Вони служать для виконання різноманітних операцій з грошима для полегшення життя людей. Розробка і реалізація їх на основі інформаційно-довідкових і платіжних систем дозволяє клієнтам компаній або урядових установ отримувати оперативний доступ до інформації, використовуючи найсучасніші досягнення в області інформаційних технологій, а також надавати клієнтам найвищий рівень сервісу без залучення спеціально підготовлених співробітників.

Термінали дозволяють зробити більшість послуг і товарів компаній доступними широкому колу споживачів. Зазвичай термінали розміщують в громадських місцях, в яких потенційні клієнти бувають найчастіше: в банках, магазинах, кінотеатрах, торгових центрах. Платіжні термінали можуть запропонувати різноманітний спектр послуг, що надаються компаніями для своїх клієнтів, при цьому, виключаючи необхідність безпосередньої участі персоналу. В основному термінали поєднують в собі кілька різних функцій, і крім надання інформації дають користувачеві можливість скористатися такими послугами як: оплата комунальних та інших рахунків, грошові перекази, замовлення, та оплату товарів, поповнення мобільного рахунку, видачу готівкових грошей та інше. Для цього вони можуть бути оснащені картрідерами, диспензорами та купюроприймачами.

З моменту появи платіжних терміналів з'являлися різного роду шахраї, метою яких було в простий спосіб отримати грошові кошти які зберігаються в платіжних терміналах або вкрасти їх у користувачів цих терміналів. З кожним роком методів вкрасти особисті дані користувачів, їх грошові кошти, або карткові дані стає все більше. З'являються як нові методи так і вдосконалюються старі. Так як банки в свою чергу формують різноманітні методи і політики безпеки, щоб забезпечити себе і своїх клієнтів безпечним проведенням платіжних операцій. Однак на данні дії з боку банків шахраї

відповідають тим що знаходять нові уразливості в роботі платіжних терміналів або розроблюють та вдосконалюють шахрайські пристрої.

Данне питання з точки зору безпеки здійснення операцій з платіжними терміналами стає все актуальнішим в наш час. Оскільки з кожним роком все більше користувачів переходять на використання безготівкових операцій і з'являються нові способи безготівкового розрахунку. Також як з'являються нові способи оплати, нові системи оплати і нові платіжні термінали - з'являються все нові уразливості за допомогою яких стає можливим вкрасти гроші у користувача. Все частіше в новинах з'являються попередження про новий метод шахраїв за допомогою якого вони змогли вкрасти певну кількість грошових коштів у звичайних клієнтів банку. Повністю уникнути данних проблем неможливо так як розробникам не вдається повністю охопити всі уразливості пристрою або системи яку вони розроблюють та вводть в експлоатацію. Однак незалежно від того чи був повністю правильно створений та введено в експлуатацію пристрій у нього з великою часткою ймовірності будуть присутні уразливості які ставлять під загрозу безпеку проведення операцій з платіжними системами і терміналами.

РОЗДІЛ 1. АНАЛІЗ ПЛАТІЖНИХ ТЕРМІНАЛІВ

1.1 Історія платіжних терміналів

Перші платіжні термінали з'явилися у США в 1975 році, а вже через 4 роки стали впроваджуватися електронні платіжні термінали - EFTPOS. Інформаційні технології в цій сфері, розвиваючись досить швидко й стрімко, стали потужним поштовхом для еволюції і впровадження систем електронних платежів. Створення першого персонального комп'ютера, створення мережі Інтернет, електронний обмін даними а також грошовими переказами - всі ці події які відбувалися позитивно відбіліся на ринку електронної комерції і стали початком появи платіжних терміналів і використання платіжних систем і платіжних технологій.

Ключова подія в сфері платіжного термінального обладнання сталася в 1993 році. У ті роки глава криптографічного відділу CWI, Девід Чаум, анонсував нову технологію для можливості реалізації системи віртуальних грошових коштів. Так з'явилася система eCash, яка є базою і основою для сучасних платіжних систем цифрової готівки, які взяли за основу - принципи дії системи eCash.

Суть системи eCash полягала в тому, що гроші зберігались, фактично, на жорсткому диску персонального комп'ютера, а для управління системою і проведення операцій необхідні було спеціальне програмне забезпечення і підключення до мережі Інтернет. Таким чином в 1994 році була реалізована перша покупка через інтернет з використанням системи eCash. Дана операція відбулася в США.

Через рік була розроблена моновалютна мікропроцесорна картка для дрібних покупок - Proton, а відома сьогодні платіжна система Mondex розробила електронний гаманець. Вже в 1996 році обсяг угод через інтернет досяг величезних показників, що спонукало учасників ринку електронних платежів замислюватися про розробку регламентів і стандартів роботи на

ньому, а також про питання інформаційної безпеки. Незабаром були розроблені і опубліковані єдині вимоги до технології виготовлення Мікропроцессорних карт - EMV і спеціальний протокол для проведення електронних транзакцій SET.

Перші термінали вперше були реалізовані на комп'ютерах, здатних одночасно обслуговувати кілька обчислювальних процесів. Це дозволило більш раціонально розподіляти обчислювальні ресурси між користувачами що стало досить відчутно оскільки перші обчислювальних машини були досить дорогими і потребували постійного сервіісного обслуговування. Перші термінальні системи були алфавітно-цифровими (клавіатура, миша, підключення до мережі), в рамках такої концепції для забезпечення захисту достатньо вирішити традиційні питання безпечної обробки даних (ідентифікація / аутентифікація користувача), а також забезпечити надійну передачу даних від термінального сервера до терміналу. Але прогрес незмінно йде вперед і на зміну старим термінальним системам прийшли нові «тонкі» клієнти, які вимагають комплексного підходу, для організації і їх захисту.

1.2 Класифікація платіжних терміналів

Платіжний термінал - автономний апаратно-програмний пристрій, що дозволяє фізичній особі самостійно виконувати різного роду операції.

Серед платіжних терміналів можна виділити 3 основні типи терміналів за типом проводимих користувачем операцій:

Банкомат - це електронний програмно-технічний пристрій, що здійснює автоматизований прийом і видачу готівкових грошових коштів з використанням банківських карт.

Термінал самообслуговування - це електронний програмно-технічний пристрій, який здійснює різного роду операції і може обробляти як карту так і готівкові кошти.

POS-термінал - це електронний програмно-технічний пристрій для прийому до оплати платіжних карт. POS-термінал може приймати картки з чіпом, магнітною смугою і безконтактні карти, а також інші пристрої, що мають безконтактне сполучення.

1.2.1 Види банкоматів

Серед банкоматів можна виділити певні типи терміналів за методом їх розміщення і функціонування:

1.2.1.1 Вбудовувані банкомати

Даний вид досить поширений. Термінали даного виду найчастіше можна побачити вмонтованим в будівлю або прилавок магазину. Найчастіше він має два блоки - зовнішній і внутрішній. Внутрішній блок вміщує в собі сейф, а зовнішній блок представлений у вигляді козирька який захищає інтерфейс взаємодії з користувачем від погодних умов. Оскільки зовнішня частина терміналу розміщена у відкритих громадських місцях - зовнішній блок має необхідний влагозахист та термостійкість.

Переваги:

Даний термінал вигідно використовувати так як він може працювати цілодобово в не залежності від дня і ночі, також він має захист від різного роду погодних умов.

Недоліки:

Вбудовувані банкомати всупереч їх захищенності від різних погодних умов і температурних змін все ж схильні до них внаслідок тривалої експлуатації без належного технічного обслуговування.

Одним з факторів відмови від розміщення подобного роду терміналів є ряд необхідних монтажних робіт для установки сейфу в приміщенні.

1.2.1.2 Напольні банкомати

Даний вид терміналів найчастіше розміщується всередині різних закритих громадських місць, а саме в приміщеннях банків, магазинах, торгових центрах. Термінал такого типу досить компактний і найчастіше розміщується на ряду з терміналами самообслуговування. Даний термінал може здійснювати видачу готівки в автоматичному режимі.

Переваги:

Даний термінал зазвичай розміщують в місцях з максимальним потоком людей що робить його найбільшвикористовуванним. Також данна модель терміналу більш компактна що дає можливість розміщувати її в місцях з обмеженим обсягом приміщень або невеликих коридорах.

Оскільки даний термінал розміщується в громадських приміщення. Він постійно перебуває під відеоспостереженням й охороною. Що дає більше гарантій на його безпеку

Недоліки:

Дана модель терміналу обмежена часом роботи того приміщення в якому вона розміщенна.

У деяких випадках дана модель розміщується в неопалюваних приміщеннях, що ставить під загрозу працездатність терміналу в холодну або жарку пору так як дана модель не має належного захисту від зовнішніх факторів.

1.2.2 Види терміналів самообслуговування

Серед терміналів самообслуговування можна виділити певні типи терміналів за методом їх розміщення і функціональності:

1.2.2.1 Вуличні платіжні термінали

Даний вид терміналів має ключову особливість у тому, що такий апарат можна розміщувати на вулиці. Так як даний термінал оснащений різноманітним обладнанням та часто піддається різного впливу погодних умов і температурних впливів, то до нього пред'являються жорсткі вимоги в захисті від волог і термостійкості. Оскільки даний термінал розміщений у відкритих громадських місцях, що означає що за ним не ведеться постійного охоронного контролю. Таким чином більший спектр уваги приділено різним захисним антивандальним пристосуванням.

Переваги:

Вуличний платіжний термінал вигідно використовувати так як обладнання може працювати протягом усього дня і ночі, незалежно від погодних умов.

Недоліки:

Вуличні платіжні термінали всупереч їх захищенності від різних погодних умов і температурних змін все ж схильні до них внаслідок тривалої експлуатації без належного технічного обслуговування.

Також захисні "антивандальні системи" в даних терміналах не забезпечують належний захист оскільки на них приділяється недостатньо уваги або ж сама захисна система побудована без урахування різного роду небезпечних чинників й схильна до атак.

1.2.2.2 Напольні платіжні термінали

Найбільш поширений вид платіжних терміналів, який добре зарекомендував себе на ринку. Даний платіжний термінал рекомендовано встановлювати в закритих громадських приміщеннях захищених від впливу погодних умов - супермаркетах, банківських установах, аеропортах, торгових центрах та інших громадських місцях.

Переваги:

Напольні платіжні термінали вигідні у використанні так як це широко поширений вид терміналів який зарекомендував себе на ринку, що означає - він досить надійний.

Напольні платіжний термінали знаходяться в приміщенні що виключає ряд загроз пов'язаних з перебуванням його на вулиці, а також тому що найчастіше в подібних приміщеннях встановлені системи сигналізації або наряд охорони - можна зробити висновок що вони достатньо захищені.

Недоліки:

Напольні платіжні термінали не завжди встановлюють в спеціалізованих для цього місцях. Що викликає ряд проблем пов'язаних з дією на термінал температурних умов. Досить часто приміщення відведені під термінали не оснащені обігрівачами і охолоджувачами повітря що може викликати перебої в роботі платіжного терміналу або втрату його працездатності аж до заміни терміналу.

Напольні термінали менш захищені від вандалізму так як мається на увазі що в місцях де вони розташовані мають знаходится патруль охороні або охоронні датчики. Однак є випадки коли подібні термінали розміщені в не захищенних або недостатньо захищенних приміщеннях, що дає можливість злодіям реалізувати його розтин або вкрасти термінал та перенести його в підготовленне приміщення з подальшим розкриттям сейфу.

1.2.2.3 Навісні платіжні термінали

Менш поширений вид платіжних терміналів, які виділяються своїми невеликими розмірами. Це компактне обладнання яке легко кріпиться на стіні. Подібні термінали раціонально використовувати в місцях з обмеженою територією.

Переваги:

Навісні платіжні термінали є досить компактною моделлю платіжних терміналів що виділяє її серед інших видів.

Недоліки:

Навісні платіжні термінали також як і вуличні термінали поступаються по захисту від вандалізму і схильні до різних погодних факторів, що ставить під питання їх працездатність під впливом температурних факторів.

1.2.2.4 Багатофункціональні платіжні термінали

До останнього часу цей вид терміналів був досить рідкісним, на сьогоднішній день можна відзначити, що багато терміналів оснащуються подібними функціями. Виходячи з назви, данне обладнання може виконувати кілька різних операцій. У багатофункціональному платіжному терміналі можливо не тільки здійснювати оплату за комунальні послуги і послуги зв'язку, а й роздруковувати фотографії, проводити сканування документів, зберігати на термінал різного типу інформацію. Надання користувачам можливості користуватися багатофункціональними терміналоми є послугою, за яку компанія-власник терміналу зазвичай стягує з користувачів плату. Плата може призначатися як відсоток від проведеної суми, часто з обмеженням мінімальної або максимальної суми, або може бути не стягнена з користувача в явному вигляді, а замість цього стягуватися з організації-одержувача платежу.

Переваги:

Багатофункціональні платіжні термінали є багатозадачним комплексом здатним виконувати різноманітні операції що власне і виділяє його серед інших терміналів.

Дані комплекси можуть бути корисні в громадських місцях для задоволення потреб користувачів.

Недоліки:

Багатофункціональність платіжних терміналів частково є і їх мінусом. Так як програмне забезпечення даних терміналів є досить новим і не рідко може вміщати в себе безліч вразливостей пов'язаних з недоробкою і малим терміном експлуатації подібних систем.

1.2.3 Види POS-терміналів

Серед POS-терміналів можна виділити певні типи терміналів за методом їх розміщення і функціональності:

1.2.3.1 Стаціонарні POS-термінали

Стаціонарні термінали працюють від мережі 220 В і не мають вбудованого акумулятора. Найчастіше данні термінали застосовуються в торгових точках, де мобільність не є вирішаючим фактором. Таким чином термінал встановлено на конкретному місці і покупцеві необхідно підійти й оплатити свої покупки.

1.2.3.2 Переносні POS-термінали

Переносні термінали мають вбудований акумулятор й найчастіше використовуютьсяя в місцях, де необхідна мобільність - кафе, ресторани, таксі, служба доставки й інше. Данні термінали також можливо використовувати і як стаціонарні термінали. Для передачі даних у терміналах використовується канал GPRS через сім-карту мобільного оператора зв'язку, Wi-Fi або Bluetooth. У першому випадку мобільність терміналу обмежується рівнем сигналу від мобільної антени зв'язку, у другому і третьому випадках мобільність терміналу обмежується розміщенням точки доступу Wi-Fi або Bluetooth станції.

1.2.4 Узагальнені мінуси більшості терміналів:

Крім недоліків відведених кожному з перерахованих вище терміналів також можна віднести загальні вразливості цих пристроїв.

Розміщення платіжних терміналів в безлюдних місцях або в місцях де не ведеться відеофіксація - ставить під загрозу не тільки вчинення користувачами платіжних операцій, але і дає можливість встановити різного роду шахрайські

пристрої здатні зчитувати і зберігати інформацію про особисті дані користувачів. Також розміщуючи платіжний термінал в подібних місцях компанія ставить під загрозу й готівкові кошти які зберігаються у терміналі.

Розміщення терміналів в неналежно обладнаних місцях або несвоєчасне технічне обслуговування терміналів. Термінали які спочатку розроблялися для експлуатації в громадських місцях поза приміщенням мають значний захист від різного роду погодних умов. Однак велика кількість даних терміналів проходять несвоєчасне обслуговування або зовсім його не проходять. Що ставить питання безпеки проведених з ними операцій. Так як в зв'язку з відмовою різного роду обладнання у таких терміналах з'являються уразливості.

Погано організований антивандальний захист. Сейф багатьох платіжних терміналів знаходиться всередині корпусу. Відповідно подібні термінали уразливі до методу грубої сили. Такі платіжні термінали стає можливим перевезти у зручне для зловмисника місце і розкрити.

1.3 Принципова схема пристрою терміналу

Основні складові платіжних терміналів:

Комп'ютерний відсік - являє собою металевий каркас у середині терміналу в якому передбачено місце для розміщення різного роду пристроїв і їх об'єднання в єдину систему.

Укладальник купюр - спеціальний пристрій який проводить розподіл купюр по касетах в залежності від номіналу купюри і її стану.

Валідатор купюр - спеціальний пристрій влаштований по типу сканера який зчитує певну інформацію з купюри і визначає номінал купюри і її оригінальність.

Діспенсер - специальний пристрій розташований під екраном банкомату який проводить видачу готівкових коштів користувачеві.

Сейф терміналу - в ньому зберігаються касети з грошима і касета вибракування. Являє собою, як правило, сейф з ключем і поворотним колесом.

Касета - спеціальний відсік який є сховищем прийнятих купюр і у який відбувається розподіл купюр щодо їх номіналу, також в кожному терміналі є касета браку у яку відправляються купюри які термінал не зміг правильно розпізнати або вони з тих чи інших причин не відповідали встановленим параметрам.

Принтер - спеціалізований пристрій який знаходиться у терміналі і виконує функцію друку чеків. Відповідно до закону кожен термінал повинен бути обладнаний фіскальним реєстратором, який реєструє всі платежі в буфері. Цей пристрій в обов'язковому порядку повинен видавати чеки на суму обрану та підтверженну користувачем, знімати щоденний звіт про оброблені платежі за день і відправляти цей звіт власнику терміналу, і зберігати копії цих даних для податкової служби.

GSM модем - спеціальний пристрій який служить для здійснення підключення до мережі і необхіден для здійснення зв'язку між терміналом і спеціальним сервером між якими проходить обмін інформацією - розрахунковому центром .

Електромеханічний замок - спеціальний пристрій який необхідний для включення/виключення живлення платіжного терміналу і служить для зовнішнього включення/вимикання терміналу. Він може застосовуватися як для швидкого виконання зазначених операцій, так і для організації системи безпеки в якості додаткового інструменту. Електричний замок потрібен для відкриття/закриття автомата, а також для авторизації персони для доступу до адміністративних функцій терміналу. Прописування в системі ключів відбувається через адміністративний інтерфейс терміналу.

1.4 Типи термінальних клієнтів:

1. Сучасні персонально обчислювальні машини. У якості термінального клієнта виступає сучасна персональна електронно-обчислювальна машина, яка є повнофункціональним набором прикладного програмного забезпечення.

Функція роботі користувача з термінальним сервером є однією з функцій, які виконуються на цій персональній електронно-обчислювальній машині;

2. Застарілі персонально обчислювальні машини. У ролі термінального клієнта виступають застарілі персональні електронно-обчислювальні машини, на яких сучасні операційні системи працюють занадто повільно або не запускаються, однак власники даних машин їх не утилізують. Як правило, такі комп'ютери мають жорсткий диск, до них можна підключити дисковод, CD ROM привід, також є кілька PCI-роз'ємів. Однак в якості терміналів данні комп'ютери досить функціональні - необхідно запустити ОС (MS DOS або Windows 98), налаштувати підключення до мережі та запустити ПО термінального клієнта;

3. Спеціалізовані термінальні клієнти. Даний вид термінальних клієнтів представляють собою спеціалізовані комп'ютери, які спочатку розроблялися для роботи в якості тонких термінальних клієнтів. Вони мають певний обмежений набір інтерфейсів для підключення периферійних пристроїв і найчастіше функціонують під управлінням ОС Linux або Windows CE.

1.5 Технологія процесів в терміналах

Після того як термінал оплати був встановлений, його підключили до мережі електроживлення і інтернету, він вводиться в експлуатацію. Але перш, ніж він зможе почати прийом платежів, необхідно відкрити особовий рахунок у організатора платіжної системи і внести будь-яку суму на рахунок, в межах якої доведеться оперувати грошима клієнтів терміналу. Авансовий платіж є залогом, такої сумми готівки, яку оплачує клієнт.

Коли платник здійснює оплату за допомогою терміналу, інформація про здійснений через термінал платіж поступає до організатора платіжної системи. З рахунку власника терміналу відбувається автоматичне зняття суми проведеного платежу і перерахування її на рахунок одержувача.

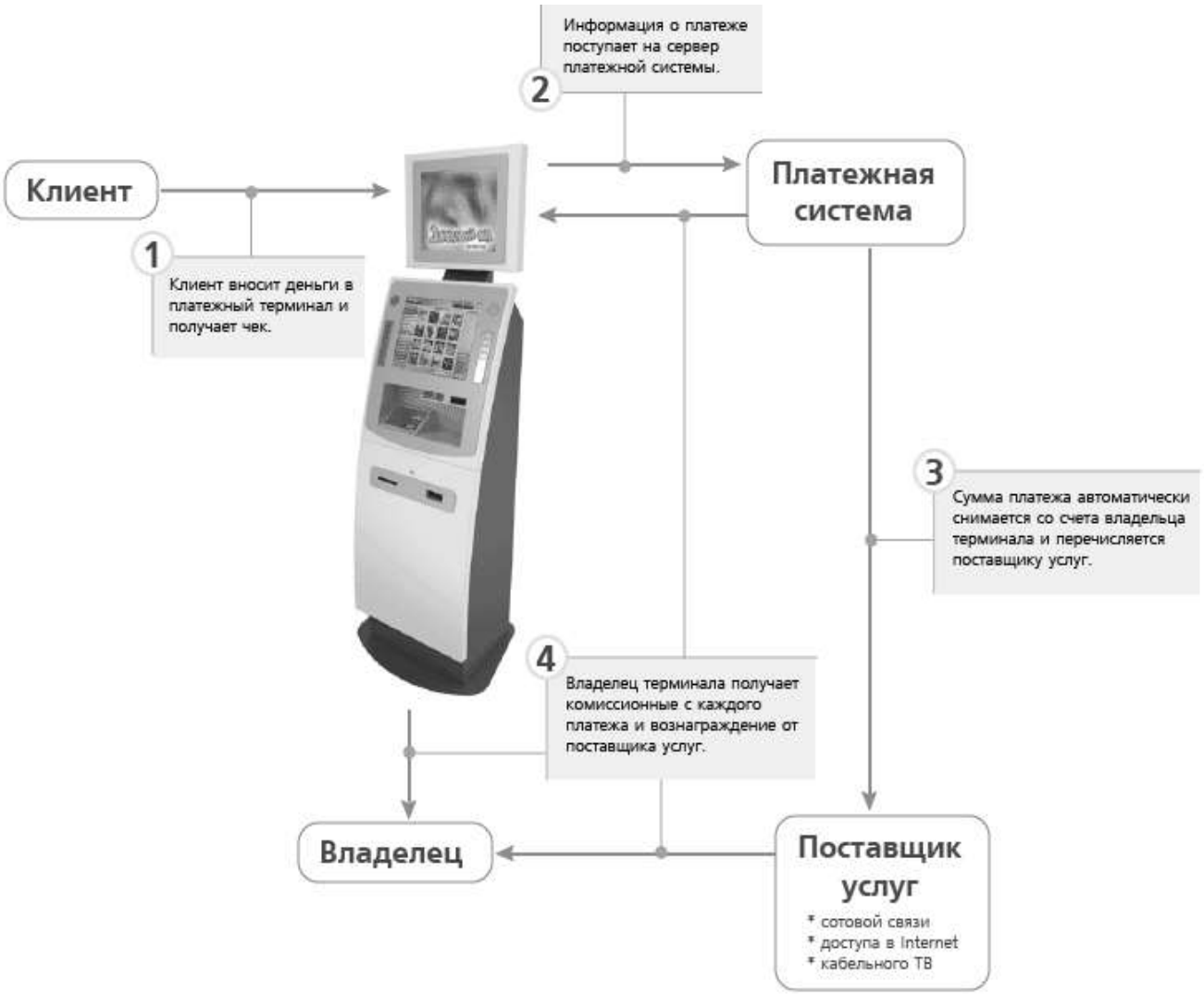

Рисунок 1.1 - Схема роботи терміналу

Принцип роботи терміналу оплати полягає в наступному:

1. Платник за допомогою графічного інтерфейсу встановленого в терміналі програмного забезпечення вибирає послугу, яку хоче оплатити.

2. У купюроприймач вставляються купюри, які піддаються перевірці на оригінальність і визначається їх номінал. Спеціально для цих цілей у терміналі встановлено валідатор купюр, який працює в автоматичному режимі і виконує цю функцію.

3. Після надходження в термінал оплати грошових коштів інформація про це за допомогою вбудованого модему передається в розрахунковий центр

платіжної системи. Таким чином, фізичні кошти стають віртуальною валютою.

4. Розрахунковий центр обробляє отриману з термінала оплати інформацію і направляє її у банк, в якому у даного платника відкритий рахунок.

5. З банківського рахунку проводиться списання грошових коштів в такому ж обсязі як і було внесено платником в термінал оплати.

6. Списані грошові кошти спрямовуються до кінцевого одержувача платежу - тієї організації, послуги якої були сплачені особою, яка внесла гроші в термінал.

У термінал відправляється інформація про надходження грошових коштів на рахунок одержувача, після чого платнику видається чек, який служить підтвердженням здійснення оплати.

За винятком першого, на виконання всіх етапів потрібно лічені секунди, оскільки всі етапи проходять в повністю автоматичному режимі.

Розміщення купюр в банкоматах. В середині у звичайного банкомату знаходиться від 10 000 - 15 000 банкнот. Вони розкладені по 4 - 6 касет, в кожній з яких - купюри свого номіналу. Заміну касет можна порівняти з картриджами у принтері: модуль виймається незалежно від того, скільки там залишилося банкнот - інкасаторам не дозволяється знати цю інформацію з метою безпеки, а на місце вийнятого - вставляється інший модуль у напрямку вказівної стрілкі, що вказує, яким боком і як необхідно його вставляти.

Інкасація - достатньо дорога і досить ризикована з точки зору безпеки процедура, в зв'язку з цим будь яке обслуговування банкомату обходиться досить дорого. Таким чином логічно що банк прагне до зменшення кількості інкасацій. Виходить що завданням банку є класична задача розподілу ресурсів: з одного боку, у банкоматі завжди повинні бути гроші для клієнтів, з іншого - банк хоче, щоб перед інкасацією з касети виходила остання купюра.

На рисунку 1.2. зображено розташування касет всередині банкомату.

Рисунок 1.2. - Розміщення касет в банкоматах

В даний час робота з великими обсягами готівкових коштів є необхідною практично скрізь: в касових центрах, інкасаторських компаніях, на транспорті, використовуваному для перевезення готівки.

Сучасні касети для готівки і банкомати все частіше захищаються від атак криміналітету інтелектуальними системами безпеки, що запобігають

несанкціонованому доступу до готівки в терміналах банківського самообслуговування. Дані системи передбачають гарантоване превентивне спецфарбування банкнот, що робить безглуздими спроби їх розкрадання за неможливістю подальшого використання

Інтервал відповіді для кожної операції, після дії клієнта повинен бути не більше 30 секунд. Це є вимогою міжнародних платіжних систем. Клієнт вставив карту - можна задуматися на 29 секунд і дати відповідь. Вибрав пункт меню знову можна подумати і так далі. Раніше, коли зв'язок був не особливо швидким це був важливий момент.

Банкомат видає не більше 40 купюр за один раз. Пов'язано це з самим механізмом подачі. На рисунку 1.5.3. показаний зовнішній вигляд касети.

Рисунок 1.3. - Зовнішній вигляд касети

У банкоматі як правило 4-6 касет з купюрами. У касету розміщується ~2.5 тисячі банкнот. Кожна касета налаштована на конкретну банкноту. Тому, навіть якщо при інкасації АТМ переплутати касети місцями - все одно чіп в касеті - не дасть видавати звідти грошей. Зворотний бік медалі - якщо в касету завантажити не ті банкноти - то АТМ почне видавати купюри іншого номіналу. Що швидше за все обернеться нестачею.

Склеєні банкноти, банкноти, які не подобаються з тих чи інших причин банкомату, а також гроші, які клієнт не виняв з щілини видачі - відкидаються в касету вибракування. За розмірами вона менша в два рази стандартної.

Вилучення карт і невірні коди. Поведінка у разі виявлення забороненої карти повністю налаштовується - банкомат може як захопити її, так і залишити у тракті. Теж саме відноситься до видачі карти до чи після грошей, спочатку або у кінці роботи, при відключенні електрики у данному разі банкомат повинен бути оснащений безперебойним пристроєм підтримання єнергії. Яку операцію провести у наслідок неправильного введення ПІН-код, введений помилкового ПІН-код, коли обнуляється лічильник невірних ПІН-код, чи потрібене захоплення карти усі ці операції вирішує хост. Якщо хост не проінструктує банкомат захопити карту, він її не захопить, навіть якщо вона фальшива, вкрадена або втрачена.

Засоби адміністрування служб терміналів. На додаток до стандартних засобів адміністрування служб терміналів в кожну з операційних систем сімейства Windows Server 2003 включені наступні засоби, розширення засобів і команди адміністрування з'єднань, комп'ютерів і користувачів.

1. Групові політики служб терміналів

2. Диспетчер служб терміналів.

3. Налаштування служб терміналів

4. Оснащення ММС «Дистанційні робочі столи»

5. Розширення оснасток «Active Directory - користувачі і комп'ютери» і «Локальні користувачі та групи»

6. Ліцензування сервера терміналів.

7. Лічильники системного монітора

8. Додаткові поля диспетчера задач

9. Підтримка розрахованого на багато користувачів режиму в компоненті «Установка і видалення програм»

10. Команди

11. Групові політики служб терміналів

Групові політики служб терміналів служать для настройки окремих серверів або груп серверів терміналів і призначення політик користувачів або груп користувачів сервера терміналів.

1 Диспетчер служб терміналів

2 Диспетчер служб терміналів служить для управління і спостереження за користувачами, сеансами і процесами з будь-якого сервера мережі, на якому запущені служби терміналів. Він використовується для:

1. Відображення відомостей про сервер, сеанси, користувачів і процесів;

2. Підключення і відключення від сеансів;

3. Спостереження за сеансами;

4. Завершення сеансів;

5. Відправлення повідомлення користувачам;

6. Здійснення виходу користувачів з сеансу;

7. Завершення процесів.

Налаштування служб терміналів

Під час встановлення операційної системи сімейства Windows Server 2003 налаштовується підключення для протоколу віддаленого робочого столу-Remote Desktop Protocol. Завдяки такому типу з'єднання зв'язок, який клієнти використовують для входу в сеанс на сервері для підключень адміністрування віддаленого робочого стола або сервера терміналів. Після завершення установки можна використовувати оснастку «Налаштування служб терміналів» для можливості змінити властивості підключення на локальному комп'ютері або створення нового підключення.

Оснащення «Налаштування служб терміналів» використовується для наступних операцій:

1. Створити ім'я підключення;

2. Встановлення типу підключення;

3. Встановлення транспорту підключення і властивостей транспорту;

4. Встановити максимально допустимої кількість сеансів;

5. Включення або відключення входу в систему через підключення;

6. Встановлення часу очікування підключення;

7. Зміна рівню шифрування;

8. Відключення розірваних підключень;

9. Включення або відключення віддаленого управління сеансом;

10. Включення або відключення можливості автоматичного входу в систему;

11. Вказання програми для запуску при вході користувача в систему;

12. Перевизначення параметра профілю користувача для фонового малюнка;

13. Встановлення дозволу для підключень;

14. Встановлення зіставлення пристроїв клієнта і параметрів підключення.

15. Оснащення ММС «Дистанційні робочі столи»

16. Оснащення ММС

«Дистанційні робочі столи» дозволяє створювати підключення до декількох серверів терміналів, налаштовувати їх на запуск окремих програм під час з'єднання і перемикатися між підключеннями служб терміналів, вибираючи підключення в дереві консолі. Спеціальна версія клієнта служб терміналів відображає робочий стіл обраного комп'ютера в області відомостей ММС.

1. Розширення оснасток «Active Directory - користувачі і комп'ютери» і «Локальні користувачі та групи»

2. Розширення оснасток «Active Directory - користувачі і комп'ютери» і «Локальні користувачі та групи» дозволяють управляти можливостями служб

терміналів для кожного користувача. Для управління цими можливостями можна також використовувати групові політики служб терміналів, хоча в цьому випадку задані параметри можуть бути перевизначені.

Розширення служб терміналів дозволяє:

1. Задати шлях до профілю кожного користувача служб терміналів;
2. Включити або відключити вхід в систему;
3. Встановити обмеження тривалості сеансу;
4. Встановити відключення або скидання розірваного підключення;
5. Включити або відключити віддалене управління;
6. Вказати програми для запуску при вході користувача в систему;
7. Встановити з'єднання дисків і принтерів клієнтів при вході в систему.

Ліцензування сервера терміналів. Ліцензування сервера терміналів застосовується для реєстрації та відстеження ліцензій клієнтів служб терміналів.

Якщо засіб «Ліцензування сервера терміналів" не буде встановлено, сервер терміналів припинить прийом підключень клієнтів без ліцензії через 120 днів від дати першого входу клієнта.

Лічильники системного монітора. Служби терміналів розширюють можливості системного монітора шляхом додавання об'єктів «Користувач» і «Сеанс», а також їх лічильників Ці об'єкти і лічильники можна використовувати для спостереження за ресурсами, які використовує користувач або сеанс. Також служби терміналів додають лічильники для об'єктів «Процес» і «Система».

Додаткові поля диспетчера задач. Служби терміналів надають диспетчеру задач два додаткових поля: ідентифікатор користувача і користувач для спостереження за процесами і завершенням кожного з них у всіх сенсах.

Підтримка розрахованого на багато користувачів режиму в компоненті «Установка і видалення програм»

1.6 Модель порушника функціонування терміналу

Модель порушника. Типологія порушників відповідно підготовленості до подолання системи охорони.

Тип порушника характеризує його ставлення до захищенного об'єкта і його можливості щодо подолання системи охорони.

Категорія відображає соціальне становище порушника. Умовно до категорії "спеціаліст" можна віднести людей, які професійно займаються даним видом діяльності і мають спеціальну підготовку. Вони можуть діяти в інтересах держави або переслідувати особисті цілі. До категорії "аматор" відносяться найманці або люди, які гостро потребують грошові засоби й обдумано вчиняють протиправні дії.

До категорії "дилетант" можна віднести хуліганів, наркоманів, алкоголіків, які проводять проникнення без попередньої підготовки. Вони переслідують, як правило, корисливі цілі. "Співробітник" - це людина, що працює безпосередньо на об'єкті захисту, його мета - збагачення.

Підготовленість порушника характеризується рядом параметрів, основними з яких є психологічні особливості особистості, фізичний стан, технічна оснащеність і рівень обізнаності про об'єкт і системі охорони. Ці характеристики знаходяться у взаємодії, підсилюючи або послаблюючи один одного.

Типологія порушників за характером поведінки. В цілому особу порушника можна визначити як особистість людини, яка йде на вчинення злочину внаслідок властивих йому психологічних особливостей, антигромадських поглядів, негативного ставлення до моральних цінностей і внаслідок вибору суспільно небезпечного шляху для задоволення своїх потреб або невияву необхідної активності в запобіганні негативного результату.

Специфічна сутність особистості порушника полягає в особливостях його психічного складу, які висловлюють собою внутрішні передумови антисоціальної поведінки. Суспільна небезпека висловлюється потенційною

особистості до злочинної поведінки, яка розуміється як внутрішня можливість здійснення за певних умов злочинних дій.

Можна виділити дві групи порушників, що відрізняються характером поведінки при вчиненні протиправних дій на об'єкті, - обережні і необережні.

Обережні порушники характеризуються:

1. Низьким рівнем тривожності;

2. Виявляється товариськість, прагнуть до встановлення міжособистісних контактів;

3. Соціально адаптовані;

Необережні порушники:

1. Характеризуються високим рівнем тривожності;

2. Проявляють невпевненість в собі, схильність до хвилювань при стресі, надлишковий самоконтроль, дезорганізовані поведінку;

3. Реалізують емоційну, а не раціональну поведінку, спокійні реакції на загрози в екстремальній ситуації;

4. Створюють в максимальному ступені аварійні ситуації в стані алкогольного сп'яніння під час керування транспортним засобом.

1.7 Види атак на платіжні термінали

Під атакою на платіжний термінал мається на увазі набір дій шахрая, яким піддається термінал і які спрямовані на крадіжку готівкових грошових коштів з терміналу або на попередню крадіжку карткових даних для подальшої крадіжки грошей або шантажу.

Всі атаки умовно можуть бути розділені на два типи:

Атаки, спрямовані на крадіжку карткових даних;

1. Скімінг - встановлення різного роду накладного обладнання - рідера, відеокамери, накладної клавіатури, шкідливого програмного забезпечення з метою фіксації карткових даних користувачів для подальшої крадіжки грошових коштів.

2. Кард-тріппінг - перехоплення банківської карт и користувача. Для цього в карт рідері банкомату розміщується пристрій, який заважає виходу карти після завершення операції.

3. Фальшиві термінали - термінали переобладнані шахраями з метою отримання карткових даних користувачів для подальшої крадіжки грошових коштів з рахунків жертв.

Атаки, спрямовані на крадіжку грошових коштів.

1. Фізичні напади на банкомати - крадіжка банкоматів, злом сейфів;

2. Кеш-тріппінг - встановлення спеціальної накладки у вікні видачі готівки. Така накладка затримує купюри і не видає їх власникові за результатами операції. Далі шахраї знімають накладку разом з розташованими на ній грошовими коштами;

3. Помилки у роботі терміналу - підключення до системного блоку банкомату з метою викликати помилку для передачі команди диспензору на видачу готівки

1.7.1 Скіммінг

Скіммінг є однією з найбільш поширених атак на платіжні термінали. Скіммінговій атаці піддаються як банкомати так і термінали самообслуговування. При скіммінгу зловмисники прагнуть скопіювати дані з картки користувача платіжного терміналу і для цього встановлюють в отвір для прийому карт спеціальне записуюче обладнання, також записують на камеру або встановлюють спеціальні підроблені накладки на клавіатуру щоб зафіксувати ПІН-код користувача. Здобуті дані потім використовуються шахраями для створення карт-дублікатів і надалі через підставних осіб або своїми силами злочинці німають кошти з карти жертв.

Скіммінгове обладнання можна розділити на 2 типи за способом розміщення на платіжному терміналі:

1. Зовнішні скіммінговие накладки. Скіммінговие накладки найбільш дешевий вид скіммінгових обладнання так як дані пристрої не вимагають дорогих компонентів. Серед скімінгове накладок можна виділити накладки на клавіатуру і картрідер.

Клавіатурна накладка фіксує які вводяться значення ПІН-коду і записує їх на вбудовану пам'ять або в більш інноваційному і дорогому варіанті передає їх по мережі wi-fi або технології bluetooth.

Накладний картрідер зчитує магнітну смугу карти і записує дані про неї на пам'ять скіммера або в більш інноваційному і дорогому варіанті передає їх по мережі wi-fi або технології bluetooth.

2. Внутрішнє скіммінгове обладнання. Досить рідкісний і дорогий тип скіммінгових пристроїв так як складається з дорогих компонентів і вміщує в собі ряд необхідних функцій для віддаленої передачі шахраям інформаці про користувача за допомогою технологій wi-fi, bluetooth або передає дані через карту мобільного оператора використовуючи мобільний інтернет. Скіммінгове обладнання може підключається всередині терміналу не тільки до портів клавіатури і картрідера але також може бути підключено на пряму до комп'ютерного відсіку терміналу що робить можливим крадіжку особистої інформації користувачів терміналу в тривалий проміжок часу.

У випадку терміналів самообслуговування розміщення скіммера всередині терміналу дає можливість шахраям красти особисті дані користувачів крім їх грошових коштів і карткових даних.

Скіммінгове обладнання також може бути розміщенно в будь-яких місцях де потенційна жертва може скористатися своєю банківською карткою. Таким

чином приміщення банку для входу в яке потрібно провести карткою через картоприймач для відкриття електронного замка також стає небезпечним.

1.7.2 Кеш-траппінг

Даний вид шахрайства також називається "Лівантская петля". Частою мішенню даного виду атак з боку зловмисників ставали банкомати. Для реалізації даного методу в найпростішому варіанті необхідно досить небагато - невеликий фрагмент фотоплівки певної довжини. Метою шахраїв в даному методі є захоплення банківської карти користувача платіжного терміналу. Введений пароль шахраї записують за допомогою відеокамери або візуально підглядають під час проведених операцій користувачем. Після того як власник банківської карти йде, без можливості забрати карту, шахраї забирають карту жертви й переводять у готівку усі грошові кошти в іншому банкоматі.

1.7.3 Фальшиві термінали

У зв'язку з здешевленням вартості покупки термінального обладнання стає можливим масова купівля великої кількості терміналів їх незаконне введення в експлуатацію, а також їх удосконалення з метою отримання карткових даних або інших можливих особистих даних користувачів.

Найбільш часто метою шахраїв стають платіжні термінали для здійснення продажів - POS-термінали так як в зв'язку з появою нових технології дані термінали стають дешевшими, також фальшивими можуть бути і термінали самообслуговування.

Фальшиві POS-термінали майже не помітні на перший погляд від своєї оригінальної версії. У деяких випадках підробка практично полность повторює оригінальну модель.

Фальшиві POS-термінали найчастіше можуть знаходиться в ресторанах або продуктових магазинах так як користувач під час оплати убільшості випадків не звертає уваги на те через якийсь термінал він робить транзакцію.

Фальшиві термінал самообслуговування також можуть знаходитись в людних місцях поруч з оригінальними платіжними терміналами інших компаній або банків.

1.7.4 Фізичний напад на банкомати

Одним із способів крадіжки грошових коштів з платіжних терміналів є проникнення всередину апарату і отримання доступу до сховища банкнот шляхом механічного злому корпусу пристрою або відкривання запірних пристроїв. Платіжні термінали привабливі для злочинців тим, що при наявності в обороті досить великих сум грошових коштів, вони не є достатньо укріпленими об'єктами, не кріпляться на спеціальних фундаментах і будівельних конструкціях будівель, які мають більш слабкий, ніж в банківських сейфах, конструктивний захист.

На рисунку 1.4. представлений зовнішній вигляд терміналу, зламаного з метою отримання грошових коштів

Рисунок 1.4. - Зламаний термінал

Зазвичай апарати з прийому платежів зламують за допомогою механічних інструментів. Розкривають корпус апарату або вирізують замки за допомогою дискової пилки, тим самим отримуючи доступ до купюроприймач і контейнеру з банкнотами. Найчастіше такі напади відбуваються на термінали, встановлені поза будівлями або в неохоронюваних приміщеннях. Поширеним способом грабіжки є зняття корпусу зі штатного місця і вивіз його в затишне місце для подальшого розкриття. Дуже часто термінали зламують або ушкоджують з чисто хуліганськими намірами.

На рисунку 1.5. зображений термінал пошкоджений з хуліганськими намірами.

Рисунок 1.5. - Спалений термінал

На рисунку 1.6. зображено термінал зламаний всередині не охороняємого приміщення.

Рисунок 1.6. - Термінал, зламаний всередині будівлі

1.7.5 Кеш-траппінг

Кеш-траппінг - це вид шахрайства, за якого зловмисники розміщують спеціальну планку з клейкою стрічкою в отворі для видачі готівки в банкоматі. У момент видачі купюр банкомат піднімає захисну металеву планку і виштовхує гроші. Однак, якщо на банкоматі встановлено кеш-траппінговий пристрій що представляє собою планку зі стрічкою скотча, то банкноти приклеюються до стрічки, а встановлена шахраями планка не пропускає їх з банкомату.

В результаті, клієнт не може отримати свої гроші, і прочекавши біля банкомату якийсь час з надією отримати свої кошти, користувач залишає місце вважаючи що в роботі терміналу стався збій. Після того як користувач залишає місце з терміналом, приходить шахрай який встановив кеш-траппінгоий пристрій і отримує гроші користувача.

Також одним з варіантів кеш-треппинга є розміщення клейкої стрічки всередині планки видачі готівкових коштів. В ході даного методу кеш-траппінгу під час видачі готівки користувач отримує не всю суму - так як частина купюр приклеюється до клейкої стрічки. Шахраї в свою чергу після того як користувач залишає термінал - забирають решту сумми.

Ознаки кеш-треппинга:

1. Банкомат відобразив на екрані повідомлення про видачу готівки, але не видав грошові кошти - в даному випадку також може з'явиться повідомлення на екрані, про те що клієнт забув гроші в банкоматі, однак повідомлення про помилку в роботі банкомату на дисплеї не з'являлося.

2. Банкомат видав клієнту гроші не в повному розмірі, повідомлення на екрані про недостачу готівкових коштів не відображалося.

1.7.6 Збій в роботі банкомату

Transaction Reversal Fraud - шахрайство, пов'язане зі зняттям готівки в банкоматі. У процесі даного типу шахрайства зловмисник відправляє запит на видачу готівки по карті і одночасно цілеспрямовано заважає банкомату виконати стандартний алгоритм з видачі грошей. Банкомат не може коректно завершити операцію з видачі та приймає ситуацію за збій, про який в банк - процесинговий центр, надходить відповідна інформація про необхідність проведення операції reversal. Тобто відбувається маніпулювання картковим рахунком. Потім злочинець примусово забирає запитувану суму з банкомату, застосовуючи спеціальний механічний пристрій.

1.8 Висновки

У данному розділі було проведено аналіз платіжних терміналів й сформовано основні проблеми безпеки. Таким чином було проведено класифікацію платіжних терміналів відповідно їх типу та методу розміщення, проведен розбір основних пристроїв платіжних терміналів, наведено схему порядку обробки операці платіжними терміналами, сформовано модель порушника. Також було проаналізовано типові атакаи на платіжни термінали й проведено їх класифікацію. Проблеми пов'язані з роботою платіжних терміналов потребують розробки методик захисту від типових атак, ряду типових рекомендацій вирішення основних помилок у роботі терміналів, а також розробку методик безпечного проведення операцій з платіжними терміналами, так як на данний момент користувачі платіжних терміналів не мають достатної обізнанності у данному вопросі, що ставить під загрозу більшость проводимих операцій з платіжними терміналами.

РОЗДІЛ 2.АНАЛІЗ ПРОБЛЕМ ПЛАТІЖНИХ ТЕРМІНАЛІВ ТА РОЗРОБКА ЗАХОДІВ БЕЗПЕКИ

2.1 Розробка контрзаходів

В ході роботи були представлені різні атаки на платіжні термінали. У більшості випадків пов'язаних з атаками на термінали оплати не вдається виявити шахраїв так як термінали оплати встановлюють в приміщеннях без належного охоронного обладнання або зовсім його відсутності.

Встановлені відеокамери мають погану якість відеозйомки, вони підключені до терміналу і починають запис тільки в той момент коли починається робота з терміналом. Дані на таких камерах в більшості випадків не зберігаються більше 10 днів.

Таким чином на данний момент одним з ключових факторів боротьби з установкою шкідливого програмного забезпечення і пристроїв які порушують безпеку платіжних термінал в першу чергу є система комплексного захисту.

Комплексна система активного захисту терміналів опллати, а саме банкоматів і терміналів самообслуговування забезпечує виконання таких функцій:

1. Захист від зовнішнього і внутрішнього вибуху.

2. Захист від внутрішнього вибуху шляхом подачі вибухонебезпечної газоподібної суміші.

3. Захист від зовнішнього механічного та високотемпературного впливу, демонтажу, зриву.

4. Запобігання руйнування приміщень та територій на місці установки банкоматів, сейфів і банківських пристроїв самообслуговування.

5. Своєчасна передача сигналу тривоги на централізований охоронний пульт.

6. Звукове та світлове оповіщення при спробі здійснення крадіжки або злому банкоматів, сейфів і банківських пристроїв самообслуговування.

Одним з найбільш інноваційних рішень даної системи є подсистема активного захисту туманом.

Дана система предназначена для перешкоджання, створення труднощів і блокування злочинних дій зловмисників, спрямованих на незаконне заволодіння майном в разі несанкціонованого проникнення в об'єкт, що охороняється - де розташовується платіжний термінал.

При надходженні команди від охоронного сповіщувача приміщення протягом короткого часу заповнюється щільним білим туманом, що генерується на основі водного розчину - пропіленглюколю. Склад повністю сертифікований, не залишає слідів на майні, не залишає запаху і абсолютно безпечний для людей, тварин, і техніки. Ефектом застосування такої системи є неможливість розглядати будь що на відстані 0.5 м від очей.

Також через 20 секунд після спрацювання генератора туману включається потужний світловий стробоскоп. Як наслідок - повна втрата орієнтації і відсутність можливості здійснювати подальші злочинні дії .

1. Злочинець проник в приміщення - спрацьовує охоронна сигналізація.

Генератор туману починає виробляти туман. На рисунку 2.1. зображено стан приміщення через 5 секунд з моменту спрацьовування системи.

Рисунок 2.1. Через 5 секунд.

2. За лічені секунди генератор туману заповнює простір приміщення туманом. Сильно ускладнюється видимість. На рисунку 2.2. зображено стан приміщення через 12 секунд з моменту спрацьовування системи.

Рисунок 2.2. Через 12 секунд.

3. Видимість пропадає і значно знижується здатність орієнтації в просторі - туман блокує подальші дії злочинця, перешкоджаючи розкрадання майна. На рисунку 2.3. зображено стан приміщення через 20 секунд з моменту спрацьовування системи.

Рисунок 2.3. Через 20 секунд.

Пісистема захисту від вибуху газом

Призначена для запобігання злому платіжних терміналів, а саме банкоматів і терміналів самообслуговування шляхом подачі всередину вибухонебезпечного газоподібної суміші.

Підсистема забезпечує:

1. Раннє виявлення довибухонебезпечних концентрацій горючих газів в захищуваному об'ємі;

2. Формування тривожного сповіщення на централізований пульт охорони і светозвуковой сповіщувач;

3. Протидію вибуху газо-повітряної суміші шляхом створення всередині об'єкту, що охороняється вибухобезпечного середовища за допомогою спеціальної речовини-флегматизатора;

Порядок формування повідомлень:

1. Тривога

2. Розтин

3. Недостатньо речовини-флегматизатора

4. Неісправність головного живлення

5. Неісправность резервного живлення.

Підсистема захисту від зовнішнього і внутрішнього вибуху

Призначена для запобігання взлому платіжних терміналів, а саме банкоматів і терміналів самообслуговування шляхом захисту від впливу внутрішнього або зовнішнього вибуху практично будь-якої вибухової речовини, а також механічного та високотемпературного впливу.

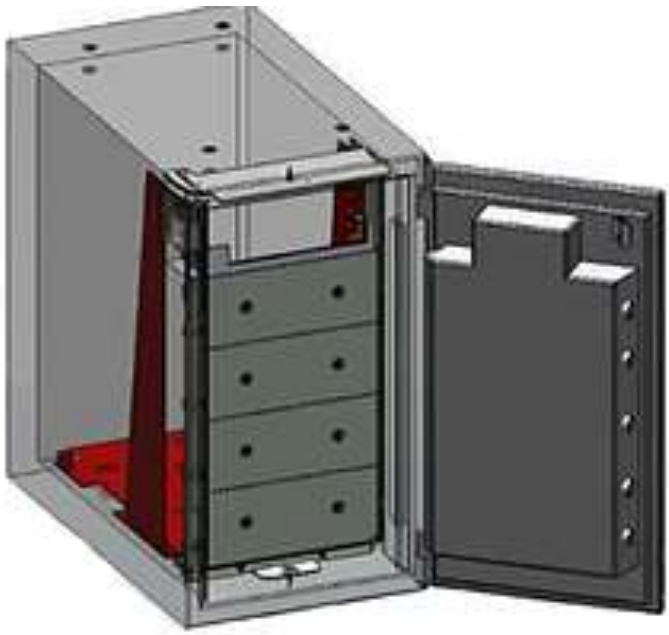

Рисунок 2.4. Схематичний вигляд сейфу з касетами

Основу підсистеми утворює адаптивний сталевий каркас, який утворює бронекапсула, з окремими електронно-керованими дверима на кожну касету з купюрами.

Рисунок 2.5. Зовнішній вигляд захисту касет

Каркас здатний витримати тиск вибухової хвилі в межах 15 бар.

Крім того він може тривалий час успішно протистояти механічному і термічному впливу за допомогою свердла, бура, газової горілки або інших підручних засобів шахраїв.

Підсистема фізичного захисту від демонтажу

Призначена для захисту платіжних терміналів, а саме банкоматів і терміналів самообслуговування від крадіжки шляхом демонтажу. Унікальна система кріплення дозволяє успішно протистояти впливу на банкомат з силою до 350 Кn.

Рисунок 2.6. Підсистема захисту від демонтажу

Система підходить як для поодиноко встановлюються банкоматів і терміналів напольного кріплення, так і для вмонтованих в стіну банкоматів висотою установки до 500 мм.

Рисунок 2.7.

Данна комплексна систему захисту активно може протистояти тягової силі тракторів і вантажівок які часто стають підручними засобами шахраїв під час атак на платіжні термінали.

2.2 Методики протидії типовим атакам

В ході роботи було проаналізовано і проведена класифікація найбільш поширених типів атак на платіжні термінал. Далі ми детально розглянемо розроблені методики щодо захисту до кожної з найбільш поширених типів атак на платіжні термінали.

2.2.1 Скіммінг

Скіммінгова атака на банкомат передбачає установку скіммінгового обладнання для зчитування даних користувача. Відповідно скіммінгове обладнання на картрідері чи клавіатурі у біллшості випадків візуально помітне.

Скіммінговим атакам в більшості випадків схильні банкомати і термінали самообслуговування. Також скіммінгове обладнання може бути встановлено в місця де необхідно зчитувати карту користувача - прикладом може бути двері оснащена електронним замком який відмикає при проводі карти через картрідер.

На рииусунку 2.8. можна бачити скіммінгових накладку на клавіатуру банкомату

Рисунок 2.8. - Накладку на клавіатуру

На рисунку 2.9. можна бачити скіммінгову накладку на карт рідер банкомату

Рисунок 2.9. - Накладка на карт рідер

Методики захисту терміналів оплати від скіммінгових обладнання:

1. Дієвим шляхом боротьби з даним видом атаки є розміщення на зовнішній частині або на екрані банкомату, терміналу попередження. У попередженні має бути розміщена фотографія встановленого в банкоматі або терміналі клавіатури і картрідера, а також ряду рекомендацій в яких описано як варто перевірити дані пристрої в платіжному терміналі.

2. Також одним з методів захисту від скіммінгового обладнання буде розробка і установка нового покоління антіскіммінгових картридеров і клавіатур. В даному випадку однією з рекомендованих практик є встановлення прозорих картридеров і спеціальних стікерів підтверджуючих що на данний вид обладнання не було нічого встановлено.

3. Одним з найбільш дієвих засобів боротьби зі скіммінгу є приховування ПІН-коду. Для цього необхідно закривати клавіатуру банкомату рукою, сумкою, гаманцем, кепкою і іншими підручними речами під час введення ПІН. Не отримавши ПІН, злочинці не зможуть отримати і доступ до карти-дублікату. З боку банків хорошим варіантом буде розміщення спеціальних повідомлень про приховання клавіатури, а також розміщення спеціалізованих планок для приховування клавіатури від чужих очей або відеокамер встановлених зловмисниками.

4. Дієвою рекомендацією в боротьбі зі скіммінгу також послужить перевірка банкомату на наявність встановленої відеокамери. Дані пристрої можуть мати дуже маленький розмір і візуально бути важко помітними. Але розміщення повідомлень на екрані терміналу про можливе місцезнаходження даних пристроїв підвищить шанси їх помітити.

5. Однією з дієвих методик в цьому ключі буде розміщення повідомлень про винагороду за знайдене скіммінгових обладнання на платіжному терміналі. В даному випадку можлива зміна відносини до операцій з платіжними терміналами і підвищення рівня обережності і зацікавленості користувачів до даної ситуації.

Боротьба з даним методом атак на платіжні термінали змушує шахраїв придумувати нові методи і нові вдосконалені версії скіммінгових обладнання однак це робить створення даного обладнання більш тривалим і дорогим процесом. Що в свою чергу викличе зменшення кількість реалізацій даного виду атак. Найбільш корисним результатом в спробах боротьби банків з даної загрозою є поінформованість і зацікавленість користувача платіжного терміналу в цілості належних йому грошових коштів і збереження його особистої інформації.

2.2.2 Карт траппінг

Метод атаки на платіжні термінали грунтується на крадіжці банківської картки шляхом її утримання в картрідер або навмисної його поломки. Оскільки даний метод за часту використовує підручні засоби, розміщена всередині слота плівка від фотокамери в більшості випадків візуально помітна. Даного виду атаці піддаються найчастіше банкомати так як вони зберігають в картоприймач прийняту карту, однак даного виду атаці також схильні до термінали самообслуговування. На рисунку 2.10. зображенно один з варіантів реалізації карт траппінгу.

Рисунок 2.10. Кард-трапінговий засіб

Методики захисту терміналів оплати від карт-траппінгу:

1. Розміщення повідомлень на екрані платіжного терміналу з метою щоб користувач перевірив картрідер на предмет сторонніх предметів які можуть стирчати з нього або бути візуально помітні всередині. А також як вести себе в разі якщо термінал не видає карту назад.

2. Розробка і створення картридеров які в разі тривалого перебування стороннього предмета запускали сигналізацію і викликали охоронну службу.

3. Так як жертвами подібного роду атак є термінали які знаходяться в недостатньо охоронюваних приміщення. Одним із способів запобігання подібних атак буде установка систем відеоспостереження за терміналом, а також оснащення приміщень в яких розміщений платіжний термінал комплексними сигналізаціями.

Даний метод атак не є достатньо поширеним так як охоплює малу кількість карт користувачів і необхідна постійна участь одного з шахраїв або підставної особи, який буде забирати залишену користувачем в картрідері карту. Однак обізнаність користувачів платіжних терміналів в даному питанні зменшить ймовірність реалізації подібних атак.

2.2.3 Фальшиві термінали

Фальшиві термінали це удосконалення шахраями модель платіжного терміналу яка може зберігати або передавати особисті дані користувача для подальших шахрайський дій - створення карт дублікатів та крадіжки грошових коштів жертв. Найбільш схильні до даної операції POS-термінали так як вони більш доступні і мобільні.

Рисунок 2.11. Оригінальний та фальшивий POS-термінали

Методики захисту від фальшивих терміналів оплати:

1. На даний момент одним з найбільш доступних методів захисту від підміни є забезпечення фізичного контролю над встановленим терміналом перевірка спеціальних наклейок безпеки, перевірка серійного номера терміналу.

2. Розробка і впровадження більш надійної технології аутентифікації терміналу обслуговуючим банком - формування терміналом криптограми транзакції для її перевірки обслуговуючим банком. Криптограма терміналу є деяким аналогом використовуваного сьогодні для онлайнових транзакцій методу забезпечення цілісності повідомлень, що циркулюють між терміналом і хостом обслуговуючого банку.

3. Надійним рішенням проблеми фальшивих терміналів є процедура взаємної аутентифікації карти і терміналу на початку виконання транзакції. Дана процедура змогла б забезпечити безпеку користувачів від можливої

загрози роботи з фальшивим терміналом оплати. Дана процедура не передбачена поточним стандартом і вимагає розробку нового стандарту взаємодії карти і терміналу.

2.2.4 Фізичний напад на банкомати

Метод грубої сили є одним з найбільш дієвих методів щодо отримання грошових коштів з термінального обладнання. Цілями даного методу атаки на платіжні термінали найбільш часто стають термінали самообслуговування так як мають досить примітивну антивандальний захист, невеликі банкомати також стають мішенью шахраїв які крадуть гроші цим методом.

Методики захисту від фізичного нападу на термінали оплати:

1. Корпус терміналу необхідно надійно закріплювати в місцях установки даного обладнання.

2. Місце де буде розміщений термінал оплати необхідно розташовуватися в приміщеннях з цілодобовою охороною та обладнаним відео спостереженням і сигналізацією.

3. Необхідно встановлювати і правильно налаштовувати сигналізаційне пристрій всередині корпусу терміналу. Цей пристрій називається сторожовий таймер і розташовується в комп'ютерному відсіку. Він призначений для контролю стану комп'ютера, формування сигналу на його перезапуск, збору даних про стан датчиків, комутації силового навантаження.

Налаштування сторожового таймера здійснюється з адміністративного інтерфейсу програмного забезпечення терміналу. Залежно від моделі сторожового таймера і програмного забезпечення сервера, цей пристрій може контролювати навіть рівень нахилу апарату, таким чином в разі спроби його впустити пристрій негайно відправить тривожний сигнал на сервер, або відправить sms на мобільний телефон відповідальних осіб.

4. Одним з ключових чинників в запобіганні крадіжок платіжних терміналів є розміщення GPS маячка, який буде сповіщати власника

термінального обладнання про переміщення даного пристрою і допоможе знайти шахраїв які вкрали платіжний термінал. Розміщення GPS маячка є досить дорогою операцією однак розміщуючи термінал в небезпечних місцях робить цю процедуру необхідної.

2.2.5 Кеш траппінг

Вид атаки на банкомати при якому злочинці розміщують на диспензорі, пристрої для видачі готівковий коштів, спеціальну планку яка затримує купюри в банкоматі після чого їх вилучає зловмисник.

Даний метод атаки на платіжні термінали базується на тому що клієнт не отримавши готівкові кошти які видаються терміналом покине місце з терміналом після чого зловмисник зможе їх забрати.

Рисунок 2.12.

Одним з ключових чинників в даній ситуації є проінформованість користувача про дії які необхідно вжити в ситуації виникнення даної помилки Таким чином розміщення на екрані інформаційних повідомлень під час обробки операції зі зняття готівки - стане вирішальним фактором який попередить появу данної ситуації.

Методики захисту від кеш-траппінгових атак на термінали оплати:

1. Швидка та оперативна реакція на зафіксовані випадки кеш-траппінгу. Установка відеоспостереження за банкоматом в якому була зафіксована дана атака.

2. Розміщення на всі банкомати спеціальних анти кеш-траппінгових планок, які запобігають встановленню кеш-траппінгового обладнання.

3. Розміщення спеціального повідомлення під час знімання готівки, в якому описаний алгоритм дій у разі, якщо користувач не отримав грошові кошти.

2.2.6. Збій в роботі платіжного терміналу

Суть даного методу полягає в передачі певної команди діспензору банкомату що викликає видачу готівкових коштів банкоматів. Даний вид атаки реалізується тільки на банкомати.

Рішення даної проблеми є не таким простим в порівнянні з іншими типами атак. Для вирішення даного завдання необхідний комплексний підхід. Оскільки безпосередньо підключитися до банкомати і перехопити зв'язок з хостом є важкореалізовуваної атакою. Оскільки банками було вжито заходів щодо вдосконалення каналів зв'язку, а також поліпшенню алгоритмів шифрування так як дані атаки вже були реалізовані раніше. Данний метод проникнення став більш витонченим і спрямований на внутрішню мережу банку.

Методики рішення атаки спрямованої на збій банкоматів:

1. Розробка і встановлення комплексних систем захисту всередині банку.

2. Розробка і відладження порядку обробки інформації.

3. Постійні заходи з проведення навчання обслуговуючого персоналу і співробітників банку.

4. Перевірки всіх корпоративних листів і розробка особливої політики банку яка запобігає потрапляю інформації із зовні.

2.3 Основні помилки при роботі з платіжними терміналами

Під час роботи з терміналів оплати часто виникають помилки які заважають нормальному функціонуванню терміналу. Дані помилки в більшості випадків є типовими для даного виду пристроїв. Грунтуючись на ряді вдалих рішень конкретних проблем можна розробити рекомендоване рішення для виправлення даних помилок. Дані рішення будуть рекомендовані обслуговуючому персоналу термінального обладнання як довідковий матеріал по вирішенню найбільш поширених помилок.

Платіжні термінали це комплексна система складається з набору певних компонентів з якими з великою ймовірністю можуть відбуватися збої.

Рішення типових помилок було розмежовано за джерелом виникнення даної помилки:

2.3.1 Купюроприймач

1. Помилка в роботі купюроприймача. У більшості випадків після перезавантаження платіжного терміналу виникає помилка на купюроприймачі або він не проходить тест. На екрані з'являється повідомлення, що необхідно

поставити відео. Іноді помилка виникає через деякий час після завантаження і декількох операцій клієнтів.

Дана проблема зазвичай виникає, коли є несправним джерело безперебійного живлення або він некоректно налаштований. Проблема також може виникнути в разі якщо не відключена функція переходу в режим очікування або в сплячий режим. Також необхідно перевірити справність відеокарти, якщо вона вбудована в материнську плату, необхідно протестувати встановивши зовнішню відеокарту. Також необхідно перевірити всі кабелі, особливо, які підходять до купюроприймача, чи не торкаються ніжки кабелю купюроприймача.

2. Купюроприймач перестав приймати нові купюри. У більшості випадків на купюроприймачі встановлена стара версія прошивки, яка не підтримує прийом нових купюр. Необхідно оновити її за допомогою зовнішнього носія до останньої версії прошивки для подальшої нормальної роботи платіжного терміналу.

3. Купюроприемник приймає грошові купюри, але не відображає їх на екрані терміналу. Є кілька можливих варіантів вирішення проблеми: в першому випадку купюроприймач можна протестувати поклавши купюру більшого номіналу, або ймовірно купюроприймач знаходиться в сервісному режимі що унеможливлює відображення грошових коштів на екрані. Рішенням даної проблеми буде перемикання купюроприймача в нормальний режим.

4. Купюропрймач видає купюри назад. Є кілька причин виникнення даної несправності: невідповідність купюроприймача і стекеру в данному випадку необхідно підігнулися стопори, на яких фіксується стекер.

2.3.2 Сенсорні панелі, монітори

1. Master Touch не реагує на дотики. Індикатор постійно горить, якщо екран відключити від контролера, індикатор починає моргати. Дана проблема виникає, якщо термінал недостатньо або неправильно заземлений, необхідно

заземлити корпус терміналу. Також необхідно почистити екран, перевірити контролер. Поставити Master Touch з робочого терміналу. Перебрати дроти, можливо в якомусь місці не є постійного контакту. Так само цілком можливо, що не вистачає потужності комп'ютера, однак дана ситуація виникає рідко. Найчастіше з такими проблемами стикаються, коли вийшов з ладу контролер. Також контролер може не коректно визначається в системі, необхідно перевірити, щоб тип контролера збігався з тим, що визначено в системі. Спробуйте замінити контролер.

2. Tuochscreen погано реагує в середині екрану на натискання. Проблема може вирішувати одним із таких способів: профілактикою мониторной збірки в плані очищення від бруду і пилу, ослабленням гайки яке притягує екран, повторна калібрування. Якщо термінал вже працював якийсь час, можливо, що з-під акустичного скотча виліз клей і потрапив на єкран. Дану проблему можливо вирішити за допомогою леза від маленького канцелярського ножа, прикладається паралельно склу та проводиться кінчиком під акустичним скотчем. Замість леза також можливо використовувати щіточку з жорсткою щетиною.

3. Touchscreen починає працювати тільки після відкриття дверцят терміналу. У данній ситуації необхідно встановити додаткове охолодження на контролер, так як при відкритті дверцят температура падає, і, відповідно, Touchscreen приходить в робочий стан. Також необхідно провести повну чистку монітору, це може бути одна з основних причин перегріву.

4. Лампа підсвічування на моніторі часто виходить з ладу. Дана проблема часто виникає у вуличних терміналів, на екран яких потрапляють прямі сонячні промені. Необхідно також перевірити блок живлення, на предмет вздуття конденсаторів, перевірити блок безперебійного живлення або підключити монітор повз нього. У деяких матрицях проводка, яка йде до ламп, прикрита фольгою. Фольга замикає, через це на інверторі спрацьовує захист.

5. Через деякий час роботи терміналу, при натискання на сенсорну панель, відгук відбувається в іншій частині екрана. Часто ця проблема виникає

через неправильне заземлення контролера, що викликає в свою чергу через порушення електромагнітної статики. Іноді допомагає повторне калібрування екрану, а також профілактичні роботи в плані очистки екрану від бруду і вологи.

6. Комп'ютер працює, індикатор на моніторі світиться, після завантаження монітор працює, приблизно, хвилину і гасне. Іноді відбувається мерехтіння. Ця проблема може виникнути, коли пробиває конденсатори на блоці живлення або згорає одна з ламп. Заміна в даному випадку ламп економічно неефективна, тому краще купити новий монітор. Якщо їх міняти, то треба міняти відразу усі лампи. Але перш, ніж ставити діагноз про вихід з ладу монітора, необхідно перевірити всі дроти які підходять до монітора, а також поставити монітор з робочого терміналу.

2.3.3 Принтери

Проблеми з підключенням - одна з найбільш частих ситуацій. Перевірити чи підключений принтер в електромережу. Якщо так - перевірити справність кабелю і портів. Якщо несправний кабель - необхідно замінити його, а якщо порт, то переключити принтер в інший порт.

1. Принтер викидає чеки. Причин може бути декілька:

Некоректно працюють драйвера. Необхідно їх перевстановити, або налаштувати роботу операційної системи безпосередньо з принтерів без посередництва драйверів.

Вийшли з ладу одна або кілька шестерень. Необхідно замінити зламані шестерні на нові.

Для вирішенняможе бути необхідним змінити операційну систему.

2. Термінал не може виявити підключений за допомогою LPT порту принтер. Для вирішення цієї проблеми необхідно відрегулювати регулятор ширини паперу. Спочатку він встановлений на найширшу - 112 мм ширину.

3. У моніторингу принтер інформує про те, що папір зім'ят. Насправді ж принтер не протягає крізь себе папір. Причиною цієї несправності є знос роликів, через якого чек довго виходить. Через те, що чек довго виходить, клієнт не чекаючи його виходу смикає; відбувається зминання. Щоб усунути цю неполадку, необхідно зробити довжину чека в 30 або 32 рядки.

2.3.4 Модем

1. Модем відмовляє в доступі одному оператору, але працює з іншим.

Причиною даної проблеми є не налаштоване GPRS на сім-карті, або помилка в його налаштуваннях. Також існує ймовірність помилки в рядку ініціалізації, зайвий пробіл або навпаки, десь не поставлений.

2. Модем з'єднується з інтернетом, але в диспетчер не висвічується оператор і рівень сигалу. У данній ситуації допоможе зміна номера COM-порту (через диспетчер пристроїв - порт - параметри порту - додатково). Після цього необхідно буде переставити драйвера на новий номер COM-порту.

3. Модем не працює, але сім карту визначає. Причиною даної неполадки є некоректний кабель, для опитування модему досить трьохпровідного кабелю, а для його нормальної роботи необхідні усі 9. Необхідно перевірити даний факт і поставити необхідний кабель.

4. Модем починає встановлювати зв'язок - але з'єднання не встановлюється.

При появі даної помилки необхідно спробувати кілька варіантів видалити з'єднання і створити його спочатку.

5. Зв'язок зависає при реєстрації персонального комп'ютеру в мережі. Помилка знаходиться в рядку ініціалізації, необхідно перевірити ще раз, на місці чи усі коми правильно розставленні і правильність введених символів. Також необхідно уважно оглянути антену, можливо, вона несправна і тому трапляються збої зв'язку.

2.3.5 Програмне забезпечення

1. На Cardmaster Standart не працює звук при натисканні клавіш на тачскрін. Рішення даної проблеми може бути в: відсутні звукових файли в папці зі звуками або проблема з динаміком.

2. Після набору номера виникає помилка і додаток закривається. Рішення проблеми, криється в проблемі з прошивками в програмному забезпеченні. Повторна установка програмного забезпечення повинна допомогти вирішити дану проблему.

3. Працює термінал, в інтернеті перевіряє номера, видає чеки, а платежі не проходять. Необхідно перезавантажити платіжний термінал.

4. Не запускається операційна система. «Синій екран смерті». Для вирішення даної проблеми: необхідно перевстановити операційну систему, або відновити завантажувальний сектор жорсткого диска.

2.4 Рекомендації щодо безпечного виконання операцій з платіжними терміналами

В ході проведеної роботи і аналізу можливих атак на платіжні термінали були розроблені загальні методики поведінки користувачів в тих чи інших ситуація пов'язаних із здійсненням операцій з платіжними терміналами.

Для кожного виду платіжних терміналів можна визначити ряд послідовних дій які в свою чергу підвищать безпеку зберегти грошові кошти користувачів.

2.4.1 Банкомати.

Даний вид платіжних терміналів найбільш піддається атакам, що робить його найбільш небезпечним. Платіжний термінал цього виду найбільш схильний до таких атак як: скімінг, кеш-траппінг, кард-траппінг. Більшість цих атак можна запобігти при правильному поводженні з банкоматом.

1 Етап. Загальні рекомендації по вибору банкомату:

Необхідно вибирати банкомат в найбільш людних громадських місцях.

Банкомат повинен знаходиться в приміщенні, що охороняється. Гарним вибором буде торговий центр або відділення банку.

Не варто проводити зняття грошових коштів в день отримання заробітної плати.

Візуально обраний банкомат повинен бути в гарному стані без явно видимих слідів ушкоджень на корпусі або пристроях терміналу.

2 Етап. Загальні рекомендації по перевірці банкомату

На банкоматі повинен бути розміщений логотип банку або організації яка встановила термінал - наклейки безпеки, а також серійного номера даного терміналу і контактні номери гарячої лінії на які необхідно телефонувати в разі будь-якої помилки в роботі терміналу.

В першу чергу необхідно візуально оглянути платіжний термінал на ряд виступів, чи не випирає з нього щость стороннє або наявність великих стиків на робочій поверхні.

Варто оглянути картоприймач - місце куди вставляється карта. Чи не стирчить звідти будь-який фрагмент чогось. Також візуально потрібно виявити чи не випирає дана деталь з корпусу банкомату. На картоприймач розташована

світлодіодній індикатор, необхідно переконається в її працездатності. Перевірити не бовтається чи картоприймач.

Подальшим дією буде перевірка клавіатури. Необхідно візуально її перевірити на великі зазори між корпусом і клавіатурою. Клавіатура не повинна випирати або бути скошена на один бік, також з неї не повинні стирчати якісь дроти. Необхідно перевірити чи не бовтається вона.

Якщо банкомат розміщений на вулиці і у нього є піддашок необхідно перевірити не закріплено чи над клавіатурою будь-якого обладнання. Це можуть бути різного роду коробочки або повноцінна камера.

3. Етап. Рекомендації по роботі з банкоматом

При роботі з банкоматом необхідно переконається чи не стоїть за вами людина досить близько щоб розгледіти ваш пін код. Деякі термінали оснащені спеціальним датчиком, який піщить якщо за вами знаходиться досить близько людина.

Коли ви вводите ПІН-код необхідно прикривати зверху панель з клавіатурою рукою, сумкою або іншим підручним засобом.

За один раз термінал може видати не більше 40 купюр. Таким чином якщо ви знімаєте велику суму грошових коштів переконайтеся що ви можете здійснити дану операцію з купюрами які на даний момент може видавати термінал.

4. Етап. Дії в разі виникнення найбільш поширених помилок при роботі з банкоматом

У разі якщо банкомат не видає вам карту назад, необхідно звернутися в службу підтримки за телефонами вказаними на терміналі. Ні в якому разі не відходите від терміналу поки не отримаєте свою карту назад. У разі якщо з якихось причин ви не можете додзвонитись до підтримки або вам терміново

необхідно залишити місце з терміналом - скористайтеся функцією блокування карти через онлайн сервіс, сайт, додатки вашого банку або в телефонному режимі заблокуйте карту.

У разі якщо ви проводите операцію по зняттю грошових коштів з вашої картки і з якихось причин банкомат не видав вам купюри, необхідно терміново звернеться за номерами гарячої лінії зазначеної на терміналі. Також даний випадок достатньо часто є шахрайством, а не програмним збоєм. Спеціальну накладку яка затримує ваші кошти можна спробувати самостійно зняти. Найчастіше дана накладка це скотч або клейка стрічка. Якщо з якихось причин вам не вдалося отримати грошові кошти обов'язково закінчіть операцію і отримаєте чек. Також в разі додаткової міри, що підтверджує здійснення вами операції з даними платіжним терміналом, буде фотографія на мобільний з датою і часом знімка.

2.4.2 Термінали самообслуговування

Данний вид платіжних терміналів також підвергається атакам. Платіжний термінал цього виду найбільш схильний до скіммінгових атак. Також данний термінал у деяких випадках шахраї можуть підробити. Фальшиві термінали самообслуговування дають змогу злодіям викрадати особисті данні користувачів, окрім підробки карт на основі введених ПІН-кодів та зчитаних карт.

1 Етап. Загальні рекомендації по вибору терміналу самообслуговування:

Термінал слід оберати у громадських місцях.

Термінал не повинен мати видимих пошкоджень.

2 Етап. Загальні рекомендації по перевірці терміналу самообслуговування

На терміналі повинен бути розміщений логотип банку або організації яка встановила термінал - наклейки безпеки, а також серійний номер даного терміналу і контактні номери гарячої лінії на які необхідно телефонувати в разі будь-якої помилки у роботі терміналу.

Перед роботою з терміналом самообслуговування необхідно перевірити картоприймач. Скіммінгове обладнання в більшості випадків візуально помітне. Якщо з картоприймач не є повністю вмонтованим у платіжний термінал, а візуально виділяється на корпусі то з великою вірогідністю можна судити що скіммінговий пристрій. Також якщо при огляді картоприймача видно великі щілини або виникають сумніви необхідно фізично первірити картоприймач на предмет того наскільки добре він закріплений. Якщо картоприймач має відчутний люфт то це ставить під сумнів безпеку проведення операцій з данним терміналом оплати.

3. Етап. Дії у разі виникнення найбільш поширених помилок при роботі з терміналом самообслуговування

Якщо термінал оплати просканував вашу карту і після введення ПІН коду з'явилася помилка є вірогідність того, що данний термінал може бути фальшивим. Якщо у разі повторного проведення данної операції данна помилка повторюється необхідно звернутися на гарячу лінію та визначити що могло бути причиною данної помилки. Якщо немає можливості пітвердити програмний збій і є підозра у тому, що данний термінал є фальшивим необхідно негайно заблокувати платіжну картку банку.

2.4.3 POS-термінали

Данний вид платіжних терміналів найбільш вразливий до підробки чи встановленню скіммінгових пристроїв, але у данному випадку неможливо точно оцінити безпеку проведення операцій за данним платіжним терміналом.

Рекомендації щодо безпечної роботи з POS-терміналами

Проводити оплату послуг через термінал в офіціальних торгових точках.

Проводи усі операції з платіжними термінали в безпосередній присутності власника банківської карти. У кафе, ресторанах або інших громадських місцях де є обслуговуючий персонал - не надавати карту офіціантам для оплати без безпосередньої присутності власника.

В будь-яких магазинах, де є можливим проводити операції карткою, забороняти здійснення операцій по оплаті послуг без візуального підтвердження проведеної операцій. У данному випадку мається на увазі, що співробітник може бути у зговорі з злодіями і проводити операцію оплати через фальшивий або з встановленним скімером термінал в момент коли клієнт не бачить.

2.5 Висновки

У данному розділі було проведено розробку методик вирішення пролем безпеки платіжних терміналів пов'язаних з типовими атаками на данні пристрої. А саме було розроблено основні методи на базі комплексної системи безпеки, яка включає інноваційні методи та пристрої які входять в її склад, що забезпечує безпеку приміщення у якому знаходяться платіжні термінали. Також було розроблено ряд рекомендацій з вирішення типових проблем у роботі платіжних терміналів. Були розроблені методики проведення безпечних опереацій з платіжнимим терміналами.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції:

1. Вартість розробки проекту інформаційної безпеки (розробка схем пристроїв, політики функціонування системи тощо);
2. Вартість створення основного й додаткового програмного забезпечення (ПЗ);
3. Витрати на первіснізакупівліапаратногозабезпечення;
4. Витрати на навчання технічних фахівців і обслуговуючого персоналу.

Спершу розрахуємо час, який буде витрачено на створення ПЗ:

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д}, \text{ годин,} \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання програми на ПК;

$t_{д}$ – тривалість підготовки технічної документації на ПЗ.

Умовна кількість оперантів у програмі:

$$Q = q \cdot c\,(1 + p), \text{ штук,} \quad (3.2)$$

де q – очікувана кількість операторів - 6;

c – коефіцієнт складності програми - 1.5;

p – коефіцієнт корекції програми в процесі її опрацювання - 0.05.

$$Q = 6 \cdot 1.5(1 + 0.05) = 9.45, \text{ штук.}$$

Оцінка тривалості складання технічного завдання на розробку ПЗ tтз– 3 год. Тривалість вивчення технічного завдання:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k} = \frac{9.45 \cdot 1.2}{75 \cdot 0.8} = 0.189, \text{ годин.} \quad (3.3)$$

де В – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, В = 1,2...1,5; k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом: до 2 років – 1,0;

Тривалість розробки блок-схеми алгоритму:

$$t_a = \frac{Q}{(20...25) \cdot k} = \frac{9.45}{20 \cdot 0.8} = 0.591, \text{ годин.} \quad (3.4)$$

Тривалість складання програми за готовою блок-схемою:

$$t_{пр} = \frac{Q}{(20...25) \cdot k} = \frac{9.45}{20 \cdot 0.8} = 0.591, \text{ годин.} \quad (3.5)$$

Тривалість опрацювання програми на ПК:

$$t_{опр} = \frac{1,5Q}{(4...5) \cdot k} = \frac{1.5 \cdot 9.45}{4 \cdot 0.8} = 4.43, \text{ годин.} \quad (3.6)$$

Тривалість підготовки технічної документації на ПЗ:

$$t_д = \frac{Q}{(15...20) \cdot k} + \frac{Q}{(15...20)} \cdot 0,75 = \frac{9.45}{15 \cdot 0.8} + \frac{9.45}{15} \cdot 0.75 = 1.261, \text{ годин.} \quad (3.7)$$

$$t = 4 + 0.189 + 0.591 + 0.591 + 4.43 + 1.261 = 11.062 \text{ годин.}$$

Розрахунок витрат на створення програмного продукту

$$К_{пз} = З_{зп} + З_{мч}. \text{ грн} \quad (3.8)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \cdot З_{пр} = 11.062 \cdot 22.024 = 243.63, \text{ грн,} \quad (3.9)$$

де t – загальна тривалість створення ПЗ, годин;

Зпр– средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

$$З_{пр} = \frac{З_{м}}{168} = \frac{3700}{168} = 22.024, \text{ грн/годину.} \quad (3.10)$$

де $З_{м}$ – середня заробітна плата на місяць – 3700грн.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot С_{мч} + t_{д} = 1.466 \cdot 4.43 + 1.261 = 7.755, \text{грн.} \quad (3.11)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_{д}$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}$$

$$C_{мч} = 0.5 \cdot 2.1 + \frac{4000 \cdot 0.1}{1920} + \frac{800 \cdot 0.5}{1920} = 1.466, \text{ грн/год.} \quad (3.12)$$

де P – встановлена потужність ПК, 0.5 кВт;

C_e – тариф на електричну енергію, 2.1грн/кВт·година;

$Ф_{зал}$– залишкова вартість ПК на поточний рік, 4000 грн.;

$Н_а$ – річна норма амортизації на ПК, 0.1 частки одиниці;

$Н_{апз}$–річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$– річний фонд робочого часу (за 40-годинного робочого тижня $F_р$= 1920 год).

$$К_{пз} = 243.63 + 7.755 = 251.383 \text{грн.} \quad (3.8)$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пз} + К_{навч} + К_н, \text{ тис. грн.} \quad (3.13)$$

де $К_{пз}$ – вартість створення програмного продукту, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Витрати на навчання технічних фахівців і обслуговуючого персоналу, це є підготовчі курси з адміністрування та обслуговування системи виявлення вторгнень, що складають 3 тис. грн;

$К_{навч}$ = 3 тис. грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають, 0.8 тис. грн.

$К_{н}$ = 0.8 тис. грн.

$$К = 0.2 + 3 + 0.8 = \ 4 \text{ тис. грн.} \qquad (3.13)$$

3.2 Експлуатаційні витрати:

$$С_к = С_н + С_а + С_з + С_{єв} + С_е + С_{ел} + С_{тос} \qquad (3.14)$$

де витрати на навчання адміністративного персоналу й кінцевих користувачів ($С_н$). визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації – 1тис. грн.

Річний фонд амортизаційни хвідрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ) – 20% або1317 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод} = 3723 \cdot 12 + 3723 \cdot 0.22 \cdot 12 = 54\ 504{,}72 \text{ грн.} \qquad (3.15)$$

де $З_{осн}$, $З_{дод}$– основнамінімальназаробітна плата на 01.01.2018, грн на рік.

Единий соціальний внесок – 0.22, часткиодиниці;

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 0.5 \cdot 365 \cdot 24 \cdot 2.1 = 9\ 198 грн, \quad (3.16)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки

(визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин

Витрати на технічне й організаційне адміністрування та сервісси стеми виявлення вторгнень визначаються у відсотках від вартості капітальних витрат 2%. А саме:

$$С_{тос} = К \cdot 0.2 = 0.8 \text{ грн}$$

$$Ск = 1 + 1.317 + 54.504 + 9.198 + 0.8 = 66,819 \text{ , тис. грн.} \quad (3.14)$$

3.3 Оцінка можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційно їбезпеки (КСІБ):

1. порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);

2. порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);

3. порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);

4. порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Вихідні дані:

$t_п$ =72 годин – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$=12годин – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$=6 годин – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$=3723грн – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;

$З_с$=4300 грн – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$=2 – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$=3 – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О = 30 000 грн – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі;

$П_{зч}$ = 4000 грн – вартість заміни встаткування або запасних частин, грн;

I=1 – число атакованих вузлів або сегментів корпоративної мережі;

N = 35 – середнє число можливих атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \text{ грн.} \quad (3.15)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за 60 годин простою внаслідок атаки:

$$П_п = \frac{\sum Зс \cdot Чс}{F} \cdot t_п, \quad (3.16)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

$$П_п = \frac{\sum 4300 \cdot 3}{160} \cdot 48 = 3870, \text{грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.} \quad (3.17)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$– витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати 4300 грн 3 співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$=6:

$$П_{ви} = \frac{\sum 4300}{160} \cdot 6 = 161.25, \text{грн.} \quad (3.18)$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ = 12 і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum 3723}{160} \cdot 12 = 279.225, \text{грн.} \quad (3.19)$$

$$П_в = 161.25 + 279.225 + 4000 = 4440.51 \text{ грн.} \quad (3.17)$$

Втрати від зниження очікуваного обсягу продаж в 200 000 грн за 90 годин простою атакованого вузла або сегмента корпоративної мережі виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{О}{Fг} \cdot (t_п + t_в + t_{ви}) = \frac{30000}{9340} \cdot (72 + 12 + 6) = 289.08, \text{ грн} \quad (3.20)$$

де $F_г$ – річний фонд часу роботи організації становить близько 9340 ч.

$$U = П_п + П_в + V = 3870 + 4440.51 + 289.08 = 8599.59 \text{ грн.} \quad (3.15)$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum_i \sum_n U = 8599.59 \cdot 35 \cdot 1 = 300985.65 \text{ грн.} \quad (3.21)$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C = 300985.65 \cdot 0.6 - 66.819 = 180524.57 \text{ грн,} \quad (3.22)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

R – очікувана імовірність атаки на вузолабо сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{E}{K} = \frac{180.524}{4} = 45.131, \text{ частки одиниці,} \quad (3.23)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн. Термін окупності:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = 0.022 \text{ років.} \quad (3.24)$$

3.5 Висновки

В економічному розділі у результаті розрахованих витрат потрібних на реалізацію методик безпечного проведення операцій з платіжними терміналами, була доведена економічна ефективність і період окупності витрат. Проект економічно доцільний та його можно використовувати на підприємстві.

ВИСНОВОК

Проблема безпеки проведення операцій з платіжними терміналами на даний момент є однією з ключових проблем в банківській сфері. Як звичайні користувачі не хочуть втратити свої кошти і не стати жертвою шахрайства так і банки бажають зберегти свою репутацію. З кожним днем з'являються все нові більш вдосконалені атаки на платіжні термінали проте в основному вони базуються на вже існуючих видах атак.

Таким чином складений ряд рекомендацій для користувачів платіжних терміналів буде служити великою вигодою як з боку користувачів так і банків. Дотримуючись цих методик користувач зможе бути впевненим в тому що операції здійснюються за допомогою платіжних терміналів буду найбільш безпечними і скоротять ризик шахрайства до мінімуму. Данні методики спрямовані на збільшення рівня проінформованості звичайних користувачів.

Також розроблені рекомендації щодо вирішення найбільш трапляємих помилок платіжних терміналів прискорять вирішення данних проблем або уникнути їх в майбутньому. Більшість помилок виникають також через несвоєчасне технічного обслуговування терміналів оплати.

Звернення уваги на дану проблеми стане одним з ключових факторів по боротьбі з шахрайством у сфері терміналів оплати. Також важливим моментом в даному питанні є увага і зацікавленість користувачів даною проблемою і бажання дізнатися як себе вести у разі виникнення проблем.

ПЕРЕЛІК ПОСИЛАНЬ

1. Термінали оплати, ремонт і профілактика.[Электронний ресурс]/ Subam.ru. – Режим доступу: subam.ru/tex-voprosi/tex-kypuropriemnik.php

2. Процес зняття готівкових грошей[Электронний ресурс]/ uml2.ru. – Режим доступу: uml2.ru/forum/index.php?topic=6260.0

3. Оптимізація розміщеня купюр у банкоматах [Электронний ресурс]/ habrahabr.ru. – Режим доступу: http://habrahabr.ru/company/croc/blog/152649/

4. Засоби адміністрування служб терміналів [Электронний ресурс]/ msdn.microsoft.com. – Режим доступу: https://msdn.microsoft.com/ru-ru/library/cc759024(v=ws.10).aspx

5. Захист термінальних систем[Электронний ресурс]/ confonline.susu.ru. – Режим доступу: http://confonline.susu.ru/terminaly

6. Особливості створення систем захисту інформації термінальних клієнтів [Электронний ресурс]/ okbsapr.ru. – Режим доступу: http://okbsapr.ru/schastniy_2007_1.html

7. Взлом платіжних терміналів [Электронний ресурс]/ subam.ru. – Режим доступу: http://subam.ru/Kluchi

8. платіжні термінали [Электронний ресурс]/ xakep.ru. – Режим доступу:https://xakep.ru/2007/05/25/38327/

9. Віддалений доступ [Электронний ресурс]/ itsec.ru. – Режим доступу:http://www.itsec.ru/articles2/Oborandteh/ydalennii-dostup-kabinetnie-resheniya

10. Пристрої, термінали і процеси [Электронний ресурс]/ intuit.ru. – Режим доступу: http://www.intuit.ru/studies/courses/22/22/lecture/20390?page=3

11. Інструкція з експлуатації [Электронний ресурс]/ philosoft.ru. – Режим доступу: http://www.philosoft.ru/ktsinstr.zhtml

12. Андреев А. А., Белов М. Ю., Быстров Л. В. Пластикові картки. – 4-е вид. перероб. й доп. М.: БДЦ-Пресс, 2002. 576с.

13. Бабинова Н. В., Гризов А. И., Сальников Д. М., Сидоренко М. С., Смородинов О. В. Нові платіжні технології. Информаційно-справочну видання./Під. ред. А. И. Гризова. М.: АОЗТ «Рекон», 2001. 272с.

14. Сергеев М.П. Міжнародні карточні платіжні системи [Электронный ресурс] / www.g-news.com.ua - Режим доступу: http://www.g-news.com.ua/content/view/1284/39/

15. Рубинштейн Т.Б. Прогрес банківської системи й інноваційні банківські продукти. Пластикові картки//Т.Б. Рубинштейн, О.В. Мирошкина. – М.: Гелиос АРВ, 2002. – 192 с.

16. Рудакова О. С. Банковскі электронні послуги. Навчальний посібник для вузів. – М.: Банки та біржі, ЮНИТИ, 1997. – 261 с.

17. Облік та аудит у банках: Учебник / А.М. Герасимович, Л. М. Киндрацька, Т. В. Кривовьяз и др.; Под ред. проф. А. М. Герасимовича. – К.: КНЕУ, 2004. – 536 с

18. Банківські операці: Підручник / А. М. Мороз, М. И. Савлук, М.Ф. Пуховкина и др.; Під ред. д – ра экон. наук, проф. А. М. Мороза. – К.: КНЕУ, 2000. – 384 с.

19. Єрьоміна Н.В. Банківські інформаційні системи: Навч. посібник. – К.:КНЄУ, 2000. – 220 с.

20. Афоніна С.В. Электронні гроші: Навч. посібник /С.В. Афоніна. - СПб. й інші: Питер, 2006. - 120 с.

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Зміст		
3	А4	Вступ		
4	А4	1 Розділ		
5	А4	2 Розділ		
6	А4	3 Розділ		
7	А4	Висновки		
8	А4	Перелік посилань		
9	А4	Додаток А	1	
10	А4	Додаток Б	1	
11	А4	Додаток В	1	
12	А4	Додаток Г	1	

ДОДАТОК Б. Перелік файлів на електронному носії

1. Пояснювальна Записка.docx
2. Презентація_Диплом.pttx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник: _____ к.е.н, доц. Пілова Д. П.
(підпис)

ДОДАТОК Г. ВІДГУК

на дипломну роботу магістра на тему:
Безпека операцій з платіжними терміалами.
студента групи 125м-17-1
Добровольського Дмитра Михайловича

Пояснювальна записка розташована на ___ сторінках та містить __ рисунків, 20 джерел та 4 додатка. Тема і зміст дипломної роботи повністю відповідає освітньо-професійній программі 125 Кібербезпека.

Розробка методик безпечного проведення операцій з платіжними терміналами є перспективною задачою, від вирішення якої залежить захищенность матеріальних активів білшості населення та репутації банків. Актуальною проблемою платіжних терміналів є ряд реалізуємих на них атак з метою крадіжки грошових активів громадян, а також однією з проблем виступає не освідченність громадян у данному питанні, що ставить під загрозу безпеку проведення операцій з ними. Аналіз типових атак і вразливостей платіжних терміналів створює ряд питаннь вирішення яких дає змогу підвищити безпеку проведення операцій з платіжними терміналами.

Зміст та структура дипломної роботи дозволяють розкрити данне питання, що полягає у створенні методик безпечного проведення оперцій та створенням методів боротьби з атаками на платіжні термінали на основі їх аналізу.

Студент показав добрий рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. В дипломному проекті відображені типові атаки на платіжні термінали, що ставлять під загрозу проведення операцій з ними.

Робота оформлена та написана відповідно до вимог щодо написання дипломної роботи магістра. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і заслуговує на оцінку _____, а її автор Добровольський Дмитро Михайлович присвоєння йому звання магістра та кваліфікації професіонал із організації інформаційної безпеки.

Керівник дипломної роботи
к.т.н., доцент О.В. Герасина
Керівник спеціальної частини
асистент кафедри БІТ Ю. А. Мілінчук