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 *Глушана Ростислава Сергійовича*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Ідентифікація вразливостей програмного забезпечення платіжного термінального обладнання*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н. доц. Герасіна О.В.			
розділів:				
спеціальний	ас. Мілінчук Ю.А			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст.викл. Мєшков В.І.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Глушану Ростиславу Сергійовичу* **академічної групи** *125м-20-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему *Ідентифікація вразливостей програмного забезпечення платіжного термінального обладнання*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 10.12.2021 № 1036-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналізування термінального обладнання	22.11.2021
Розділ 2	Оцінювання загроз та вразливостей для інформації, яка оброблюється на серверному обладнанні, ідентифікація вразливостей програмного забезпечення платіжного термінального обладнання.	07.12.2021
Розділ 3	Розрахунок економічної доцільності впровадження запропонованих поліпшень системи безпеки.	03.02.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 05.10.2021р.

Дата подання до екзаменаційної комісії:

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 85 с., 6 рис., 6 табл., 4 додатка, 22 джерела.

Об’єкт дослідження: програмне забезпечення термінального обладнання.

Предмет дослідження: ідентифікація вразливостей програмного забезпечення термінального обладнання.

Мета кваліфікаційної роботи: проведення ідентифікації вразливостей платіжного термінального обладнання.

Методи дослідження: системний підхід, методи порівняння.

У першому розділі було розглянуто: обладнання платіжних терміналів, бази даних; вразливості термінального обладнання, вразливості інформації, яка обробляється на серверному обладнанні;

У другій частині будо проведено аналіз: операційних систем на терміальному обладнанні; термінального обладнання на можливі загрози та аналіз загроз для оброблювальної інформації на серверному обладнанні; запропоновано: варіанти поліпшення безпеки; побудовано: модель порушника;

В економічному розділі визначено: ефективність впровадження поліпшень безпеки на термінальному обладнанні.

Усі результати досліджень у кваліфікаційній роботі можуть бути використані для подальшого удосконалення систем безпеки.

Практична цінність роботи полягає у наступному: ідентифікація вразливостей платіжного термінального обладнання та розробка рекомендацій щодо впровадження комплексу засобів захисту в інформаційну систему.

ЗАГРОЗИ ПЛАТІЖНОГО ТЕРМІНАЛЬНОГО ОБЛАДНАННЯ, ВРАЗЛИВОСТІ ПЛАТІЖНОГО ТЕРМІНАЛЬНОГО ОБЛАДНАННЯ, ТЕРМІНАЛЬНЕ ОБЛАДНАННЯ.

РЕФЕРАТ

Пояснительная записка: 85 с., 6 рис., 6 табл., 4 приложения, 22 источника.

Объект исследования: программное обеспечение терминального оборудования.

Предмет исследования: идентификация уязвимостей программного обеспечения терминального оборудования.

Цель квалификационной работы: проведение идентификации уязвимостей платежного терминального оборудования.

Способы исследования: системный подход, способы сравнения.

В первой главе было рассмотрено: оборудование платежных терминалов, базы данных; уязвимости терминального оборудования, уязвимости информации, обрабатываемой на серверном оборудовании;

Во второй части был проведен анализ: операционных систем на терминальном оборудовании; терминального оборудования на возможные угрозы и анализа угроз для обрабатывающей информации на серверном оборудовании; предложены: варианты улучшения безопасности; построено: модель нарушителя;

В экономическом разделе определено эффективность внедрения улучшений безопасности на терминальном оборудовании.

Все результаты исследований в квалификационной работе могут использоваться для дальнейшего усовершенствования систем безопасности.

Практическая ценность работы заключается в следующем: идентификация уязвимостей платежного терминального оборудования и разработка рекомендаций по внедрению комплекса средств защиты в информационную систему.

УГРОЗЫ ПЛАТЕЖНОГО ТЕРМИНАЛЬНОГО ОБОРУДОВАНИЯ, УРАЖЕННОСТИ ПЛАТЕЖНОГО ТЕРМИНАЛЬНОГО ОБОРУДОВАНИЯ, ТЕРМИНАЛЬНОЕ ОБОРУДОВАНИЕ.

ABSTRACT

Explanatory note: 85 p., 6 figures, 6 tables, 4 annexes, 22 sources.

Object of research: terminal equipment software.

Subject of research: identification of vulnerabilities of terminal equipment software.

The purpose of the qualification work: identification of vulnerabilities of payment terminal equipment.

Research methods: system approach, comparison methods.

The first section considered: equipment of payment terminals, databases; vulnerabilities of terminal equipment, vulnerabilities of information processed on server equipment;

The second part will analyze: operating systems on terminal equipment; terminal equipment for possible threats and threat analysis for processing information on server equipment; proposed: options to improve security; built: model of the violator;

The economic section defines: the effectiveness of the implementation of security improvements on terminal equipment.

All research results in the qualification work can be used to further improve security systems.

The practical value of the work is as follows: identification of vulnerabilities of payment terminal equipment and development of recommendations for the implementation of a set of means of protection in the information system.

THREATS OF PAYMENT TERMINAL EQUIPMENT, VULNERABILITIES OF PAYMENT TERMINAL EQUIPMENT, TERMINAL EQUIPMENT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ATM - Automated Teller Machine;

DDL – Data Definition Language;

GPRS – General Packet Radio Service; Загальний сервіс пакетної радіопередачі;

GSM – Global System for Mobile Communications – глобальна система мобільного зв'язку;

IDS – Intrusion Detection System; Система виявлення атак (вторгнень);

POS-термінал – Point Of Sale;

SIEM – Security information and event management;

SSL – Secure Sockets Layer – рівень захищених сокетів;

TDE – Transparent Data Encryption;

TFT – Thin film transistor – тонкоплівковий транзистор;

VNC – Virtual Network Computing;

XML-RPC – Extensible Markup Language Remote Procedure Call – виклик відалених процедур;

АС - Автоматизована система;

БД - База даних;

ЕОМ - Електронно-обчислювальна машина;

ОС – Операційна система;

ПЗ – Програмне забезпечення;

СУБД - Система управління базами даних

ЗМІСТ

ВСТУП

Застосування термінального обладнання, яке включає в собі об'єднання різноманітних рішень, та сучасних технологій, які забезпечують комфорт, зручність отримання послуг та раціональне споживання ресурсів для користувачів. Так як інфраструктура термінального обладнання розвивається швидше, ніж засоби її захисту, що залишає великий простір для діяльності зловмисників, і це, в свою чергу, потребує пошуку нових засобів безпеки.На сьогоднішній день люди все частіше використовують платіжне термінальне обладнання. Вносять свої персональні данні, банківські данні, і тому безпека такого обладнання являється важливим аспектом. Доцільно зробити детальний аналіз платіжного термінального обладнання та виявити основні його вразливості.

Термінальний обладнання – це набір сучасних послуг, які безпосередньо пов'язані з користувачем. Високотехнологічні обладнання сьогодні використовуються в багатьох сферах людської діяльності. Завдання термінального обладнання: спростити роботу, підвищити конверсію і точність операцій, зняти з людини певну частку вантажу робіт.

Для забезпечення надійного захисту термінального обладнання необхідно проаналізувати сам пристрій на можливі вразливості та загрози Якщо не проваджувати нові технології для захисту такого обладнання, то все частіше будуть відбуватись крадіжки персональних даних користувачів, а також компанії будуть нести фінансові втрати. Значний вклад в розвиток термінального обладнання в Україні й на пострадянському просторі внесли Росляков А. В., В. Семенов, В. Н. Абрамов, М. Г. Арутюнов и др. Ред. Ю. М. Смирнов.

Актуальність теми кваліфікаційної роботи ідентифікація вразливостей програмного забезпечення термінального обладнання

визначається:

– збільшенням вразливостей термінального обладнання;

– сучасними темпами і рівнем розвитку методів забезпечення захисту інформації, які в значній мірі відстають від рівня розвитку сучасних інформаційних технологій.

Для досягнення поставленої мети в кваліфікаційній роботі необхідно вирішити наступні завдання:

– проаналізувати платіжне термінальне обладнання;

– дослідити термінальне обладнання з точки зору безпеки;

– виконати аналіз вразливостей термінального обладнання;

– дослідити алгоритм передачі даних між клієнтом та серверним обладнанням;

– проаналізувати загрози для оброблювальної інформації на серверному обладнанні;

– побудувати модель порушника;

– розробити рекомендації щодо поліпшення захисту термінального обладнання.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1. Аналіз термінального обладнання

Термінальне обладнання – устаткування, що перетворює призначену для користувача інформацію в дані для передачі по лінії зв'язку і здійснює зворотне перетворення. Таке обладнання може бути як джерелом інформації так і одержувачем, або тим і іншим одночасно. Ці пристрої передають або приймають дані, за допомогою використання кінцевого обладнання лінії зв'язку і каналу зв'язку. До термінального обладнання відносяться:

– платіжні термінали (торгові і банківські термінали, термінали голосової авторизації) та контрольно – касові системи;

– інформаційні термінали.

Розберемо більш детально термінали.

Платіжний термінал – апаратно – програмний комплекс, що забезпечує прийом платежів від фізичних осіб в режимі самообслуговування. Для платіжного термінала характерна висока ступінь автономності його роботи. Контроль роботою цих терміналів можна проводити через мережу Інтернет.

Технічний склад терміналу:

– метало-пластиковий корпус, в який вбудований комп'ютер;

– TFT – монітор з сенсорним екраном;

– пристрій безперебійного живлення;

– купюро – приймач;

– чековий принтер;

– GPRS модем;

– GSM антенна;

– сторожовий таймер.

Щоб збільшити кількість послуг, що надаються, в деякі платіжні термінали вбудовують:

– пристрій для роботи з пластиковими банківськими картами;

– сканер штрих-кодів;

– диспенсер, кардрідер;

– пін–пад клавіатури;

– додатковий TFT-монітор.

Розглянемо алгоритм роботи термінального обладнання (рисунок 1.1).

Рисунок 1.1 – Алгоритм роботи термінального обладнання

Користувач виконує пошук послуг, вказує реквізити та інше за допомогою вбудованого екрану, на якому відображається меню. Після чого вже сам термінал перевіряє правильність введеної інформації, перевіряє існування даного рахунку і можливості його поповнення. Користувач вносить бажану суму готівки, купюро приймач розпізнає справжність готівки, їх номінал, і здійснює повернення купюр, які не пройшли перевірку на справжність. Після закінчення внесення готівкових коштів, термінал у відповідь роздруковує і видає користувачеві чек з інформацією цієї транзакції. За допомогою GPRS – модему, термінальне обладнання пересилає інформацію про платіж серверу, який забезпечую обробку цього платежу. Після обробки даних серверне обладнання передає їх на шлюз сервера організації, після

чого гроші поступають на рахунок одержувача (рисунок 1.1).

Компанія, яка надає можливість користуватись терміналом зазвичай стягує комісію. Комісія може назначатись як у вигляді відсотка від суми операції, так і у вигляді фіксованої суми. Але це все безумовно вказується на самому терміналі (усі комісії, умові зарахування та інше).

Типовий банкомат має три пристрої для вводу інформації та три вихідних пристрої вводу інформації – це зчитувач інформації з карток, цифрова клавіатура й функціональна клавіатура. Вихідні пристрої – електронне табло для повідомлень, пристрій для видачі готівки та принтер, який підтверджує факт виконання операції. За допомогою цих пристроїв здійснюється взаємодія клієнта зі системою.

Здебільшого банкомати забезпечують виконання таких операцій:

– видача готівки: з поточного і строкового рахунків, в рахунку кредитних карток;

– приняття вкладів на поточний, терміновий та інші рахунки;

– переказ грошей: з поточного рахунку на строковий, з термінового на поточний, з рахунку кредитних карток на поточний;

– платежі операцій: списання з поточного і термінового рахунку, післяплата

У термінального обладнання також присутній моніторинг ресурсу, який підвищує загальну якість рішення, що дозволяє підтримувати ефективну працездатність мережі пристроїв. Можливості системи моніторингу залежать від встановленої системи електронних платежів.
Процес моніторингу платіжного терміналу:

– збір та обробка інформації про стан платіжного терміналу;

– стан купюро – приймача;

– стан принтера;

– складання журналів за операціями платіжного терміналу;

– зняття показників датчиків платіжного терміналу;

– управління таймером перезавантаження;

– управління правами доступу адміністраторів;

– складання звітності.

Для характеристики систем ЕОМ, що виконують функцію обробки інформації за угодами в системі розрахунків у торгівельних точках, використовується така термінологія:

– банківська система клієнта – банківська система ЕОМ, в якій зберігається інформація щодо банківських депозитних розрахунків клієнта або карткових рахунків, і обробляється як частина операції в системі розрахунків у торговельних точках;

– система перевірки платоспроможності – це те саме: що й банківська система клієнта;

– банківська система торговельника – система банківських ЕОМ, в якій зберігається інформація, що стосується рахунку торговельної фірми й обробляється як частина операцій в системі розрахунків у торговельних точках.

Банкомат видає трохи більше 40 купюр за один раз. Пов'язано це з механізмом подачі. Тому - знімаючи гроші в банкоматі - якщо він виводить на екрані «В наявності купюри 50, 200» - а вам потрібно зняти більшу суму - відразу можете прикинути скільки максимум грошей банкомат може вам видати. Якщо спробуєте ввести більше 40 банкнот — банкомат подумає і відмовить. А ви залишитеся гадати чому.

Інтервал відповіді для кожної операції після дії клієнта повинен бути не більше 30 секунд. Це вимога міжнародних платіжних систем. Клієнт вставив картку – можна замислитись на 29 секунд і дати відповідь. Вибрав пункт меню – знову можна подумати. І так далі.

У кожного термінального обладнання є, так звана, біла картка супервізора. Йде з кожним банкоматом у комплекті. Як і звичайні карти, теж має PIN-код і термін дії.

Так ось – картка потрібна для виконання інкасації/аудиту банкомату та деяких технічних функцій – можна видати скільки завгодно купюр із касет <godmode ON>, відчиняти дверцятами видачі, поблимати індикаторами та дисплеями тощо. Три рази неправильно ввів код на карті – блокується до наступного дня.

У банкоматі зазвичай 4-6 касет з купюрами. У касету, яка показана на рисунку 1.2 міститься ~2.5 тисяч банкнот. Кожна касета налаштована на конкретну банкноту. Тому навіть якщо при інкасації АТМ переплутати касети місцями – все одно чіп у касеті – не дасть видавати звідти грошей. Зворотний бік медалі – якщо в касету для двадцяток завантажити півтинники – то (при значній частині везіння – якщо характеристики купюр більш-менш схожі) АТМ почне видавати купюри більшого номіналу.

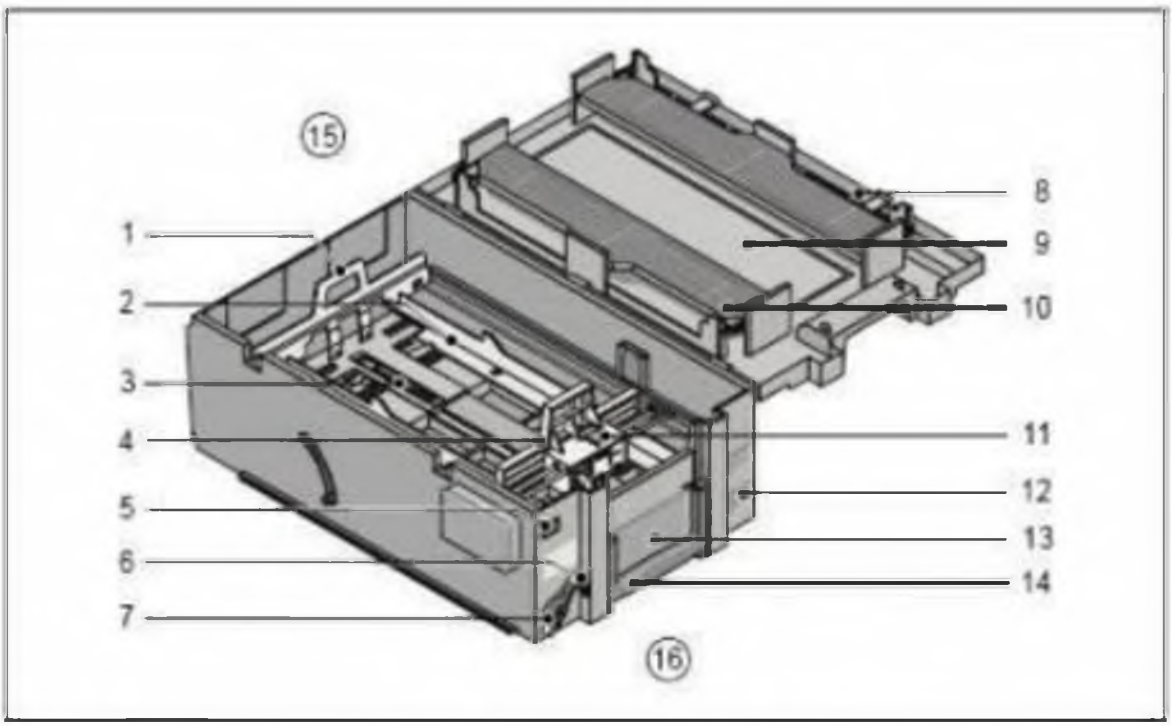

Рисунок 1.2 - Грошова касета

Склеєні банкноти, банкноти, які не подобаються з тих чи інших причин банкомату, а також гроші, які ви не взяли зі щілини видачі – відкидаються до касети вибракування, яка показана на рисунку 1.3. За розмірами вона менша вдвічі стандартною.

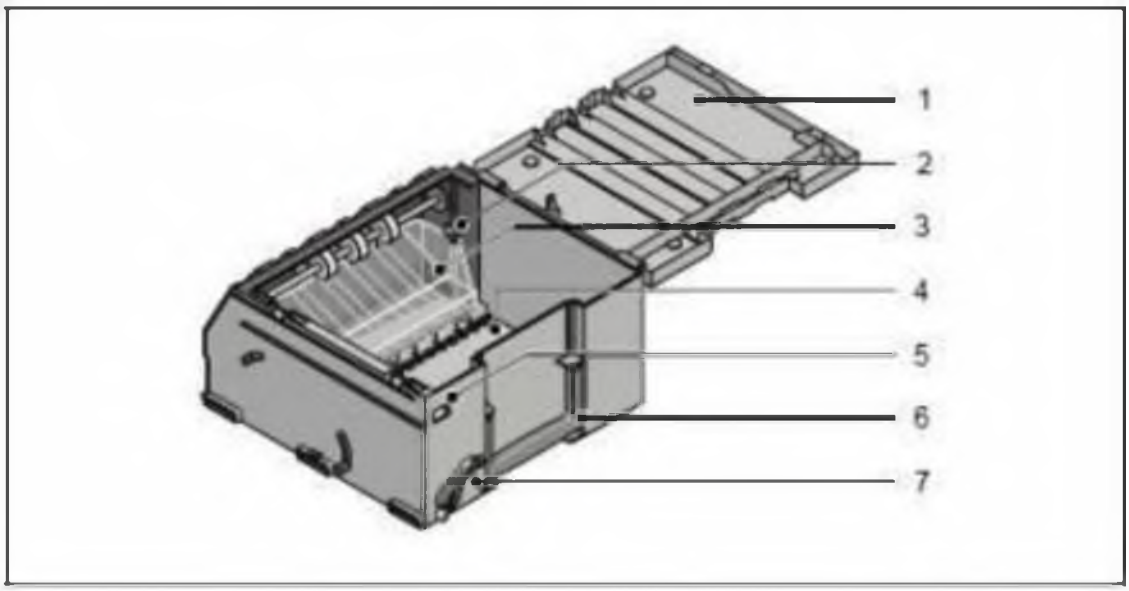

Рисунок 1.3 – Касета відбракування

1.2. Класифікація інформації на серверному обладнанні

Таблиця 1.2 Класифікація інформації на серверному обладнанні

Вид інформації	Рівні конфіденційності		
Інформація про стан та працездатність платіжних	К	Ц	Д
	К2	Ц2	Д2
Персональні дані	К2	Ц2	Д3
Інформація про обробку платежу	К2	Ц2	Д2
Технічна інформація та звіти фінасові	К3	Ц3	Д3

Рівні конфіденційності інформації:

1. Критична – її розголошення призведе до краху роботи суб'єкта або значним його матеріальних втрат (К0).

2. Дуже важлива – її розголошення призведе до значних матеріальних втрат, якщо не будуть зроблені деякі дії (К1).

3. Важлива – її розголошення призведе до деяких матеріальним (може бути, непрямим) або моральних втрат, якщо не будуть зроблені деякі дії (К2).

4. Значна – приносить скоріше моральний збиток, може бути використана тільки в певних ситуаціях (К3).

5. Малозначима – може принести моральну шкоду в дуже рідкісних випадках (К4).

6. Незначна – не впливає на роботу суб'єкта (К5).

Рівні цілісності інформації

1. Критична – її несанкціонованих змін призведе до неправильної роботи всього суб'єкта або значної його частини, наслідки незмінні (Ц0).

2. Дуже важлива – її несанкціонованих змін призведе до неправильної роботи суб'єкта через деякий час, якщо не будуть зроблені деякі дії, наслідки є незмінними (Ц1).

3. Важлива – її несанкціонованих змін призведе до неправильної роботи частини суб'єкта через деякий час, якщо не будуть зроблені деякі дії; наслідки змінювані (Ц2).

4. Значна – її несанкціонованих змін позначиться через деякий час, але не призведе до збою в роботі суб'єкта; наслідки змінювані (Ц3).

5. Незначна – її несанкціоноване зміна не позначиться на роботі системи (Ц4).

6. Несуттєва – в мінімальній мірі впливає на роботу суб'єкта (Ц5).

Рівні доступності інформації

1. Критична – без неї робота суб'єкта зупиняється (Д0).

2. Дуже важлива – без неї можна працювати, але дуже короткий час (Д1).

3. Важлива – без неї можна працювати деякий час, але рано чи пізно вона знадобиться (Д2).

4. Корисна – без неї можна працювати, але її використання заощаджує ресурси (Д3).

5. Несуттєва – застаріла або невживана, що не впливає на роботу суб'єкта (Д4).

6. Шкідлива – її наявність вимагає обробки, а обробка веде до витрати ресурсів, не даючи результатів або приносячи шкоду (Д5).

1.3. Аналіз вразливостей термінального обладнання

Платіжні термінали також регулярно виявляються вектором витоку особистих даних. Згідно з звітом Verizon від 2015 року (на даний момент актуальна офіційна інформація), до третини таких інцидентів трапляються саме внаслідок зламування точок продажу.

Причини цього найчастіше полягають у тому, що додатки, які керують терміналами, пишуться без урахування вимог інформаційної безпеки в принципі, а, отже, можуть утримувати вразливості, через які їх нескладно інфікувати. І те, що вони бувають підключені до інтернету (для доступу до різних баз), лише полегшує роботу зловмисників.

Характерною особливістю термінального обладнання є те, що вони завжди географічно віддалені від сервісних підрозділів, але при цьому знаходяться у внутрішніх мережах компаній і часто мають пряме підключення до інтернету. Сьогодні майже не використовується термінальне обладнання, яке працює по принципу накопичення транзакцій. Тобто термінал збирає якусь кількість транзакцій та після цього відправляє у визначений час на сервер для оброку інформації та операції платежу. Всі термінали працюють із персональними даними або фінансовими транзакціями. Так як термінали дуже сильно пов'язані з нашим життям тому і тема захисту інформації, безпека використання таких приладів для суспільства актуальна. Прикладом використання може бути: поповнення мобільних рахунків, банківських карт, оплата комунальних послуг, поповнення віртуальних гаманців та інше. Як вище зазначувалось більшість платіжних та інформаційних терміналів в основному працюють на операційній системі Windows, але також є термінали, які працюють на ОС Linux . Ці пристрої мають, неважливо на якій ОС, графічну оболонку, яка дозволяє користувачеві використовувати платіжний термінал за своїми потребами, але також вона не дає доступ клієнту до звичних функцій ОС. Проте зловмисники можуть скористатися всіма функціями операційної системи, завдяки технічним і програмним вразливостям та недолікам. Розглянемо деякий тип вразливостей,

пов’язаних з інформаційною безпекою, в термінальному обладнанні. Так як термінали це по суті звичайні ПК замість стандартних периферійних пристроїв до нього підключено спеціалізовані. Один із них — автоматичний пристрій для видачі готівки. Як завжди, зловмисник отримує доступ до нутрощів банкомату за допомогою ключа, який легко купити в Інтернеті. А потім він просто переводить машину в режим обслуговування, витягує потрібний USB-кабель з гнізда і підключає його до «чорної скриньки» — власного дистанційно керованого міні-комп'ютера, який тепер буде віддавати команди пристрою для видачі готівки.

Операція повторюється доти, доки лоток для грошей не спорожніє. Далі залишається лише прибрати з нього «чорну скриньку», і жодних слідів атаки не залишиться. Така атака стає можливою через те, що критично важливі елементи банкомату ніяк не перевіряють справжність свого оточення. Модуль для видачі грошей слухняно виконуватиме команди будь-якого пристрою, до якого він підключений.

Відома атака на термінали Tyupkin, але на даний момент сучасна атака на термінали це по суті модернізована Tyupkin під назвою ATM-Infector.

У нашому випадку злочинці заражали ці пристрої, підключаючись до них безпосередньо або проникаючи в систему з внутрішньої мережі банку.

Усередині банкоматів знаходиться комп'ютер, який і бере під повний контроль Skimer - так він перетворює банківську машину на один великий скіммер. Після зараження шкідлива програма поводиться максимально тихо, чекаючи команди від своїх творців. Так як зв'язок терміналу з сервером відбувається по GPRS / GSM – каналу, і як правило за рахунок технології XML-RPC. На деяких терміналах також може бути присутній SSL – захист, але що б даний захист виправдовував себе, по-перше, даний протокол повинен бути закритим, а по-друге переданий пакет повинен шифруватися, а по – третє сервер повинен не тільки надавати свій кореневої сертифікат, а також вимагати клієнтський сертифікат.

Особливістю термінального обладнання використанням зловмисником смарт – карт, з вбудованим чіпом, в цьому чипі міститься шкідливий програмний код, який може повністю вразити операційну систему терміналу. Також за допомогою смарт – карт, які вставляються в зчитувач карт можна копіювати дані користувачів, пін коди та інше. Як і в інших операційних системах, в платформах термінального

обладнання теж присутні віруси. Основне завдання даних вірусів – це добратися до ядра терміналу, яке відповідає за обробку даних. Після того, як вірус завдав шкоди терміналу, зловмисники можуть вільно зчитувати дані за допомогою особливих карт, на яких присутні магнітна стрічка.

Потрібно розуміти, що є декілька типів вразливостей для терміналів, а саме:

1. Технічні проблеми:
– Відсутність безперебійного живлення
– Оптичний канал витоку інформації
– Закладні пристрої
– Недостатнє обслуговування приладів
2. Програмні проблеми:
– Відкритий протокол передачі даних
– Відсутній на сервері клієнтський сертифікат
– SQL-Injection
– Нестандартна ОС
– Відкриті порти
– Шкідливе програмне забезпечення
– Відкрита фільтрація Web-сторінок
3. Людський фактор:
– Користувач та його дії

А тепер давайте розберемо та проаналізуємо кожну проблему окремо.

1.3.1. Аналіз технічних проблем в термінальному обладнанні

Почнемо наш аналіз з технічних проблем. Безумовно зрозуміло, що відсутність безперебійного живлення є проблемою для термінального обладнання. Так як за допомогою такого живлення термінал може працювати безперебійно не зволікаючи на навантаження на лінії, збоїв, а також профілактичних робіт працівників на цих самих лініях. Також відеоспостереження, яке на даний момент працює набагато краще ніж декілька років назад також у момент відсутності живлення не працює.

Як раз у такий момент зловмисник і може добути собі доступ фізичний до «залізо» терміналу.

Оптичний канал витоку інформації - візуальні методи, фотографування, відео зйомка, спостереження.

В оптичному каналі отримання інформації можливо шляхом:

– візуального спостереження;
– фото-відеозйомки;
– використання видимого та інфрачервоного діапазонів для передачі інформації від приховано встановлених мікрофонів та інших датчиків;

В якості середовища поширення в оптичному каналі витоку інформації виступають:

– безповітряний простір;
– атмосфера;
– оптичні світловоди

Оптичний канал витоку інформації реалізовується безпосереднім сприйняттям оком людини навколишньої обстановки шляхом застосування спеціальних технічних засобів, що розширюють можливості органу зору по баченню в умовах недостатньої освітленості, при віддаленості об'єктів спостереження і недостатності кутового дозволу.

Це і звичайне підглядання з сусіднього будинку через бінокль, і реєстрація випромінювання різних оптичних датчиків у видимому або ІК-діапазоні, яке може бути модулювати корисною інформацією. Спостереження дає великий обсяг цінної інформації, особливо якщо воно пов'язане з копіюванням документації, креслень, зразків продукції і т.д. В принципі, процес спостереження складний, оскільки вимагає значних витрат сил, часу і засобів.

Характеристики всякого оптичного приладу (в т. ч. очі людини) обумовлюються такими першорядними показниками, як кутовий дозвіл, освітленість і частота зміни зображень (кадрів). Спостереження на великих відстанях здійснюють об'єктивами великого діаметру. Велике збільшення забезпечується використанням

довгофокусних об'єктивів, але тоді неминуче знижується кут зору системи в цілому.

Відеозйомка і фотографування для спостереження застосовується досить широко.

Використовувані відеокамери можуть бути дротяними, радіопередавальними, переносимо і т.д. Сучасна апаратура дозволяє вести спостереження при денному освітленні і вночі, на дуже близькій відстані і на великій до декількох кілометрів, у видимому світлі і в інфрачервоному діапазоні.

В умовах поганої освітленості або низької видимості широко використовуються прилади нічного бачення і тепловізори. В основу сучасних приладів нічного бачення закладений принцип перетворення слабкого світлового поля в слабке поле електронів, посилення отриманого електронного зображення за допомогою мікроканального підсилювача, і кінцевого перетворення підсиленого електронного зображення у видиме відображення (за допомогою люмінесцентного екрана) у видимій оком області спектру. Зображення на екрані спостерігається за допомогою лупи або реєструючого приладу. Такі прилади здатні бачити світло на кордоні ближнього ІЧ-діапазону, що стало основою створення активних систем спостереження з лазерним ІЧ - підсвіченням. Конструктивно прилади нічного бачення можуть виконуються у вигляді візирів, біноклів, окулярів нічного бачення, прицілів для стрілецької зброї, приладів для документування зображення.

Тепер давайте проаналізуємо закладні пристрої в термінальному обладнанні. Закладний пристрій - технічний засіб негласного отримання інформації, розміщений на об'єкті інформаційної діяльності з приховуванням від виявлення особою, яка не має відношення до застосування технічного засобу, факту його наявності та/або застосування, внаслідок чого створюється загроза витоку інформації з об'єкта інформаційної діяльності. Частіше всього в термінальне обладнання встановлюються, так званні, апаратні закладки.

Апаратна закладка - пристрій в електронній схемі, потай запроваджується до інших елементів, яке здатне втрутитися в роботу обчислювальної системи. Результатом роботи апаратної закладки можливо як повне виведення системи з ладу, і

порушення її нормального функціонування, наприклад несанкціонований доступом до інформації, її зміна чи блокування.

Також апаратною закладкою називається окрема мікросхема, що підключається зловмисниками до атакованої системи для досягнення тих же цілей.

Так як закладки такого типу збираються зі стандартних модулей. Які використовуються у ПК з невеликою модернізацією, у зловмисників є можливість встановити їх у термінальне обладнання без особливих проблем, та активувати їх за необхідністю. Активація може бути зовнішньою та внутрішньою. У першому випадку для запуску закладки використовується зовнішній сигнал, який приймається антеною або датчиком. Сигналом від датчика може бути результат будь-якого виміру: температури, висоти, тиску, напруги тощо.

Для внутрішньої активації не потрібна взаємодія із зовнішнім світом. І тут закладка чи працює завжди чи запускається за певному умові, закладеному під час її розробки. Умовою внутрішньої активації може бути як певна комбінація внутрішніх сигналів, і певна послідовність виконання операцій.

1.3.2. Вплив людського фактора на термінальне обладнання

На даний момент використовується багато захисного ПЗ. Наприклад, антивіруси, міжмережевий екран (фаєрволи), системи виявлення вторгнень.

Система виявлення атак (вторгнень) (англ. Intrusion Detection System, IDS) — програмне або апаратне засіб, призначене для виявлення фактів несанкціонованого доступу до комп'ютерної системи або мережі або несанкціонованого управління ними в основному через Інтернет. Про будь-яку активність шкідливого ПЗ або порушення типової роботи централізовано збирається інформація SIEM-системою (англ. Security information and event management). SIEM-система обробляє дані отримані від багатьох джерел і використовує методи фільтрування тревог для розрізнення несанкціонованої активності від хибного спрацювання тревоги. Про що оповіщається або адміністратор або операційний центр безпеки.

Міжмережевий екран, мережевий екран, брандмауер, фаєрвол, файрвол (англ. Firewall, вогняна стіна) — загальне назва фізичних пристроїв чи програмних

застосунків, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі безпеки.

Антивірусна програма (антивірус) — спеціалізована програма для знаходження комп'ютерних вірусів, а також небажаних (шкідливих) програм загалом та відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики — запобігання зараженню (модифікації) файлів чи операційної системи шкідливим кодом .

У всіх них є певні функції та задачі. Однак всі ми розуміємо, що чим краще програмне забезпечення тим в ньому застосовується самі передові технології, криптостійкі алгоритми, але при цьому не можна бути впевненим на всі сто відсотків, що система невразлива. Людина, будучи частиною системи, був і залишається найбільш вразливим місцем в системі безпеки.

Як було зазначено вище, однією з основних тенденцій останніх років стало те, що хакери переключили свою увагу з окремих користувачів на фінансові організації. Отримавши доступ до банківської системи, зловмисники можуть заробити набагато більше грошей, при цьому відстежити їх все складніше. Хакеру достатньо проникнути в комп'ютер банківського службовця, звідти йому відкривається дорога до внутрішніх систем, у тому числі термінальних мереж. Як злочинець може отримати доступ?

Найпоширеніший спосіб – через електронну пошту. Зловмисник відправляє листа від імені клієнта банку, Центробанку або держорганів. Як тільки співробітник банку відкриває документ із цього листа, в його комп'ютер проникає шкідлива програма, яка відразу починає поширюватися по внутрішній мережі фінансової організації.

Усередині банківської мережі шахраї знаходять комп'ютер співробітника, який має доступ до мережі терміналів, і через нього завантажують на банкомати шкідливе програмне забезпечення. Заражений комп'ютер АТМ відсилає на диспенсер команду видати всі гроші, причому у банківській системі ці зміни не відображаються, банк продовжує вважати, що банкомат сповнений. Потім програма видаляє себе, тому відстежити такі атаки дуже складно.

Людський фактор є причиною успіху багатьох атак, і тому є маса прикладів. Розглянемо, чому ж зловмисники використовують людину, як основну уразливість в системі захисту. Так, наприклад, безпека термінального обладнання знаходиться в поганому стані завдяки тому, що при розробці обладнання та програмного забезпечення, були допущені деякі прорахунки. І навіть при абсолютній бездоганності обраної технології (як при проектуванні, так і в реалізації), її ще треба впровадити.

Все термінальне обладнання знаходиться у більш менш публічних місцях. Що вже робить це обладнання небезпечним для користувачів. В реалізації всіх рішень та застосування їх на практиці беруть участь люди, а людям властиво помилятися. Людина, будучи частиною системи, була і залишається найбільш вразливим місцем в системі безпеки. Інформаційні технології все більше проникають в різні сфери життєдіяльності людини, і тому кіберзлочинність набирає обертів з великою швидкістю.

Будь – які порушення, відхилення від нормативної діяльності можна трактувати або як умисні дії, або як ненавмисні, часто випадкові помилки. Види умисних дій персоналу досить різноманітні і залежать, зрозуміло, від професійного статусу людини і займаного їм місця в посадовій ієрархії. Проте, можна виділити наступні основні усвідомлені дії, що вживаються людиною здебільшого з корисливих методів:

– несанкціонований доступ до інформації з метою усвідомленого знищення,

розкрадання або копіювання інформації, всіх захисних об’єктів на ресурсі;

– модифікація інформації, порушення її цілісності, підробка, зміна даних;

– розкрадання або виведення з ладу носіїв інформації;

– розкрадання, виведення з ладу або модифікація програмного забезпечення;

– розкрадання або руйнування апаратних засобів або іншого технологічного

обладнання, в тому числі систем захисту інформації;

– порушення технології, алгоритмів і процедур вирішення функціональних

завдань.

Саме поняття умисного дії має на увазі, що воно вчиняється з наміром отримати результат, не передбачений професійними обов'язками, спеціально задумано і усвідомлено.

Помилки відбуваються ненавмисно, але, на жаль, результат помилкових дій усвідомлюється тільки після їх здійснення. Вони найчастіше носять випадковий характер, хоча іноді їх можна кваліфікувати як систематичні. Головними причинами, якими вони викликаються, є професійна некомпетентність, найчастіше як наслідок недостатнього рівня підготовки, халатність чи неготовність до діяльності через поточного функціонального стану. Ці помилки також повинні розглядатися, як фактори ризику. Вони властиві, як правило, оперативному і обслуговуючому персоналу. Типові слідства таких помилок:

– спотворення або втрата інформації;

– виведення з ладу або руйнування носіїв інформації;

– виведення з ладу або руйнування програмних або технічних засобів;

– порушення технології, алгоритмів або процедур виконання функціональних завдань.

Зменшення ймовірності таких помилок представляється важливим завданням, рішення якої слід шукати на шляхах постійного контролю рівня підготовки і функціонального стану. Збиток від ненавмисних помилок користувачів, операторів та інших осіб, які обслуговують об’єкти термінального обладнання, може виявитися істотним. До того ж вони зустрічаються досить часто. Іноді такі помилки, неправильно введені дані, збої програми, ініційовані невмілими діями людини, неправильні команди можуть призводити до повного припинення функціонування системи.

Побудувати надійну систему безпеки в сучасному комп'ютерному світі дуже непросто. Існує велика кількість слабких місць в системі; процес знаходження нових «дірок» і їх «латання» – це безперервна робота. Для вирішення поточних проблем на зміну застарілим технологіям приходять нові, в яких в свою чергу

виявляються свої недоліки. Винаходяться нові прийоми для обходу здавалося б досконалою захисту. Дві протиборчі сторони – комп'ютерні злочинці і фахівці з захисту – знаходяться в безперервній боротьбі. Треба зазначити, що ця сутичка протікає зі змінним успіхом. При цьому поведінка рядових користувачів може нахилити чашу терезів на ту чи іншу сторону. Людина з її непередбачуваною поведінкою може звести нанівець величезні зусилля, витрачені на зведення надійної системи безпеки.

1.4. Аналіз систем керування базами даних на серверному обладнанні

Система управління базами даних (СУБД, СУБД англ. Database Management System, DBMS) — набір взаємопов'язаних даних (база даних) та програм для доступу до цих даних. Надає можливості створення, збереження, оновлення та пошуку інформації в базах даних з контролем доступу до даних.

Основні характеристики СУБД:

– Контроль за надлишковістю даних
– Несуперечливість даних
– Підтримка цілісності бази даних (коректність та несуперечливість)
– Цілісність описується за допомогою обмежень
– Незалежність прикладних програм від даних
– Спільне використання даних
– Підвищений рівень безпеки

Можливості СУБД:

– Дозволяється створювати БД (здійснюється за допомогою мови визначення даних DDL (Data Definition Language))
– Дозволяється додавання, оновлення, видалення та читання інформації з БД (за допомогою мови маніпулювання даними DML, яку часто називають мовою запитів)
– Можна надавати контрольований доступ до БД за допомогою:

– Системи забезпечення захисту, яка запобігає несанкціонованому доступу до БД;

– Системи управління паралельною роботою прикладних програм, що контролює процеси спільного доступу до БД;

– Система відновлення — дозволяє відновлювати БД до попереднього несуперечливого стану, що був порушений внаслідок збою апаратного або програмного забезпечення.

В даний час існує досить багато різних серверних систем управління базами даних (СУБД) – це MS SQL Server, Oracle, IBM DB2, Interbase, MySQL. Але широке поширення і застосування на практиці для великих систем отримали три бази даних – MS SQL, Oracle і IBM DB2.

Таблиця 1.3 Переваги та недоліки систем управління базами даних

СУБД	Переваги	Недоліки
IBM DB2 Universal Database	Найпотужніша мова запитів; кращий оптимізатор; можливість писати функції на інших мовах.	Висока вартість; мала поширеність; складність адміністрування.
Oracle Database	Безліч додаткових можливостей; крос– платформний сервер; висока швидкодія.	Дуже висока вартість; не у всіх версіях поставляється засіб адміністрування СУБД; складність адміністрування.
Microsoft SQL Server	Найвища швидкодія; найбільша поширеність; відносно невисока вартість; досить простий в адмініструванні; продукт швидко розвивається, вже впритул наближається до своїх конкурентів.	Існує тільки для однієї платформи (Win32); менші можливості в порівнянні з Oracle і DB2.

В таблиці наведено основні переваги та недоліки розглянутих СУБД. Для системи буде використовуватися СУБД MS SQL 2019. Даний вибір обгрунтовується широким поширенням даної системи, високою продуктивністю при низькій

вартості сервера і простотою підтримки системи. Крім того, серверний комп'ютер буде працювати під управлінням операційної системи з сімейства Windows Server 2019, що забезпечує ще одна перевага MS SQL Server 2008, тому що саме ця СУБД найкращим чином оптимізована для операційної системи Windows.

Microsoft SQL Server – система керування базами даних. Основний використовуваний мову запитів – Transact – SQL, створений спільно Microsoft та Sybase. Використовується для роботи з базами даних розміром від персональних до великих баз даних масштабу підприємства.

MS SQL Server містить великий набір інтегрованих служб з аналізу даних. Доступ до даних, розташованим на MS SQL Server можуть отримати будь – які додатки, розроблені за допомогою технології .Net і середовища розробки Visual Studio, а також додатки пакета Microsoft Office. Для конфігурації, управління і адміністрування всіх компонентів Microsoft SQL Server використовується інструментарій утиліти SQL Server Management Studio. У ній існує підтримка ряду компонент і засобів по створенню і управлінню базами даних, засобів аналітичної обробки даних (Analysis Services), засобів звітності (Reporting Services), а також безліч засобів, що спрощують розробку додатків. У кожного об'єкта, що захищається MS SQL Server є пов'язані права доступу, які можуть надавати учаснику, який є окремою особою, групою або процесом, що отримав доступ до MS SQL Server. Платформа безпеки MS SQL Server управляє доступом до захищених сутностей за допомогою перевірки автентичності та авторизації.

Перевірка автентичності – це процес входу в MS SQL Server, в рамках якого користувач запитує доступ шляхом подачі облікових даних, які перевіряє сервер. Під час перевірки автентичності відбувається ідентифікація користувача або процесу [15].

Авторизація – це процес визначення того, до яких захищених ресурсів учасник може отримати доступ і які операції з цими ресурсами йому дозволені.

MS SQL Server підтримує два режими перевірки автентичності: режим перевірки автентичності Windows і режим змішаної перевірки автентичності. Режим перевірки автентичності Windows є режимом за замовчуванням. Оскільки ця модель безпеки SQL Server тісно інтегрована з Windows, часто її називають

вбудованою функцією безпеки. Користувачі Windows, що пройшли перевірку автентичності, не повинні висувати додаткові облікові дані. Режим змішаної аутентифікації підтримує перевірку автентичності, як засобами Windows, так і засобами SQL Server. Пари імен користувачів і паролів ведуться в SQL Server. Стосовно захисту даних в MS SQL Server шифрує дані, використовуючи ієрархічну структуру засобів шифрування і управління ключами. На кожному рівні дані нижчого рівня шифруються на основі комбінації сертифікатів, асиметричних ключів і симетричних ключів. Асиметричні і симетричні ключі можна зберігати поза модуля розширеного управління ключами MS SQL Server. На кожному рівні ієрархії засобів шифрування, шифруються дані більш нижнього рівня і відображаються найбільш поширені конфігурації шифрування. Доступ до початку ієрархії, як правило, захищається паролем.

Слід враховувати наступні основні особливості в MS SQL Server:

– для кращої продуктивності дані слід шифрувати за допомогою симетричних ключів, а не за допомогою сертифікатів та асиметричних ключів;

– головні ключі бази даних захищені головним ключем служби. Головний ключ служби створюється при установці SQL Server і шифрується API –інтерфейсом захисту даних Windows Data Protection API (DPAPI) – це криптографічний інтерфейс, що забезпечує захист даних шляхом їх шифрування;

– симетричні або асиметричні ключі поза SQL Server;

– прозоре шифрування даних Transparent Data Encryption (TDE) має використовувати симетричний ключ, який називається ключем шифрування бази даних, захищений сертифікатом, який, в свою чергу захищається головним ключем бази даних master або асиметричним ключем, що зберігається в модулі розширеного керування ключами;

– головний ключ служби і всі головні ключі бази даних є симетричними ключами.

Механізми шифрування даних в MS SQL:

Функція Transact-SQL за допомогою цієї функції можна шифрувати окремі елементи по мірі того, як вони вставляються або оновлюються;

– асиметричні ключі;

– симетричні ключі;

– сертифікати.

Сертифікат відкритого ключа, або просто сертифікат, являє собою підписану цифровим підписом інструкцію, яка пов'язує значення відкритого ключа з ідентифікатором користувача, пристрою або служби, що має відповідний закритий ключ. Сертифікати поставляються і підписуються центром сертифікації.

Як правило, сертифікати містять такі відомості:

– відкритий ключ суб'єкта;

– ідентифікаційні дані суб'єкта, наприклад ім'я та адресу електронної пошти;

– термін дії, тобто інтервал часу, протягом якого сертифікат буде вважатися дійсним;

– ідентифікаційні дані постачальника сертифіката;

– цифровий підпис постачальника.

Цей підпис підтверджує дійсність зв'язку між відкритим ключем і ідентифікаційними даними суб'єкта. Для зручності управління дозволами в базах даних MS SQL Server надає кілька ролей, які є суб'єктами безпеки, групуються інших учасників. Вони подібні до груп в операційній системі Microsoft Windows. Дозволи ролей рівня бази даних поширюються на всю базу даних.

У таблиці представлені визначені ролі рівня бази даних і їх можливості. Ці ролі існують у всіх базах даних.

Таблиця 1.4.Ролі рівня бази даних та їх опис

Ім'я ролі рівня бази даних	Характеристика
db_owner	Члени зумовленої ролі бази даних db_owner можуть виконувати всі дії по налаштуванню і обслуговуванню бази даних, а також видаляти базу даних.

db_securityadmin	Елементи зумовленої ролі бази даних db_securityadmin можуть змінювати членство в ролі і управляти дозволами. Додавання учасників до цієї ролі може призвести до випадкового підвищення прав доступу.
db_accessadmin	Члени зумовленої ролі бази даних db_accessadmin можуть додавати або видаляти права віддаленого доступу до бази даних для імен входу і груп Windows, а також імен входу SQL Server.
db_backupoperator	Члени зумовленої ролі бази даних db_backupoperator можуть створювати резервні копії бази даних.
db_ddladmin	Члени зумовленої ролі бази даних db_ddladmin можуть виконувати будь – які команди мови визначення даних (DDL) в базі даних.
db_datawriter	Члени зумовленої ролі бази даних db_datawriter можуть додавати, видаляти або змінювати дані в усіх призначених для користувача таблицях.
db_datareader	Елементи зумовленої ролі бази даних db_datareader можуть зчитувати всі дані з усіх призначених для користувача таблиць.
db_denydatawriter	Члени зумовленої ролі бази даних db_denydatawriter не можуть відправляти повідомлення, змінювати або видаляти дані в призначених для користувача таблицях бази даних.
db_denydatareader	Члени зумовленої ролі бази даних db_denydatareader не можуть зчитувати дані з користувацьких таблиць бази даних.

Крім того, існує ще також роль public, яка міститься в кожній базі даних, включаючи системні бази даних. Її не можна видалити, а також не можна додавати і видаляти учасників з неї. Дозволи, надані ролі public, успадковуються всіма іншими користувачами і ролями, оскільки вони належать до ролі public за замовчуванням. Обліковий запис guest є вбудованої обліковим записом у всіх версіях SQL Server. За замовчуванням обліковий запис guest в нових базах даних відключена. Якщо вона включена, її можна відключити шляхом скасування дозволу CONNECT, виконавши інструкцію REVOKE CONNECT FROM GUEST мови Transact – SQL.

Дослідження резервного копіювання, компоненти резервного копіювання та відновлення SQL Server забезпечує необхідний захист важливих даних, які

зберігаються в базах даних SQL Server. Щоб мінімізувати ризик незворотної втрати даних, необхідно регулярно створювати резервні копії баз даних, в яких будуть зберігатися вироблені зміни даних. Добре продумана стратегія резервного копіювання та відновлення захищає бази від втрати даних при пошкодженнях, що походять із за різних збоїв.

При правильному створенні резервних копій баз даних можна буде відновити дані після багатьох видів збоїв, включаючи наступні:

– збій носія;

– помилки користувачів (наприклад, видалення таблиці помилково);

– збої обладнання (наприклад, пошкоджений дисковий накопичувач або безповоротна втрата даних на сервері);

– стихійні лиха.

Стратегія резервування і відновлення складається з частини, що відноситься до резервування, та частини, що відноситься до відновлення. Частина, що відноситься до резервування, визначає тип і частоту створення резервних копій, тип і швидкісні характеристики обладнання, необхідного для їх створення, спосіб перевірки резервних копій, а також місцезнаходження та тип носія резервних копій включаючи і питання безпеки. Частина, що відноситься до відновлення, визначає відповідального за проведення операцій відновлення, а також методи їх проведення, що дозволяють задовольнити вимоги користувачів по доступності даних і мінімізації їх втрат. Документувати процедури резервування та відновлення і зберігати копію цієї документації в документації по завданню.

1.5. Дослідження найбільш вагомих проблем в термінальному обладнанні

Практично всі проаналізовані загрози вище мають вплив на конфіденційність, цілісність, доступність, спостережливість, доступність. Найбільш вагома загроза для інформації, яка циркулює на термінальному обладнані призводять такі загрози:

– Відсутність програмних об’єктів на пристрої

– Не правильно розподілені користувачі в системі стосовно їх прав доступу

– Відсутня конфіденційність при обміні інформації

Сьогодні автоматизовані системи інтенсивно використовується у всіх областях життєдіяльності людини і тому питання забезпечення безпеки оброблювальної інформації все більш становиться актуальним.

Враховуючи, що на сьогоднішній момент ОС Windows стала де-факто операційною системою не тільки для персональних комп'ютерів, але і для платіжних терміналів, інформаційних табло та банкоматів, то на цих пристроях можуть функціонувати будь-які віруси та черв'яки, створені для атаки на ОС Windows.

Про перших троянців для банкоматів стало відомо у 2009 році. Протягом трьох років до рук антивірусних компаній потрапило ще близько десяти екземплярів подібних шкідливих програм, модифікованих зловмисниками для обходу систем захисту та виправлення деяких помилок.

При цьому потрібно розуміти специфіку створення шкідливого коду під такі системи: розробити вірус для них здатна тільки технічно грамотна людина, яка розуміє пристрій апаратури і має безпосередній доступ до обладнання для проведення аналізу та тестування вірусу.

Є два шляхи доступу до банкомату: флешка та мережа. Спеціальна флешка може бути використана або інсайдером, або просто технічним фахівцем, який може не здогадуватися про її зараження. Спеціально або з необережності термінал все одно опиниться в руках зловмисників. Те саме справедливо і для зараження через мережу. Помилки при проектуванні, налаштування безпеки можуть бути використані або інсайдерами або зловмисниками безпосередньо.

Наслідки зараження банкоматів можуть бути найсерйознішими для користувачів. За досвідом першого такого випадку можна сказати, що, пропрацювавши кілька місяців, заражені банкомати передавали своїм «господарям» всю інформацію, необхідну для зняття грошей з рахунків усіх клієнтів банків, які користувалися такими банкоматами.

В даному випадку ця проблема стосується не банків як таких, а компаній-виробників банкоматів та софту для них. Вихід полягає в тому, щоб реалізовувати

складніші та захищені механізми захисту банкоматів як на фізичному, так і на програмному рівні. Можливо використовувати спеціальні антивірусні рішення.

Говорити про майбутнє таких атак – складно. Тому що на сьогоднішній день подібні сценарії мають скоріше одиничний та концептуальний характер. Найімовірніше, злочинці можуть піти шляхом створення повністю підроблених банкоматів, замість прґоникнення в справжні.

Опираючись на виконаний аналіз вразливостей на термінальному обладнанні, а також дослідження пристрою, інформація, що циркулює на серверному обладнанні не досконально захищена, тому до серверної системи застосовують функціональний профіль захищеності. Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Вибір та реалізація профілю захищеності залишається за користувачем, якому надані відповідні повноваження. Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються. При реалізації профілю захищеності треба брати за увагу рівень автоматизованої системи, рівень та значення інформації, яка оброблюється в даній системі та інші показники, які характеризують даний об'єкт.

ВИСНОВОК

Всі пристрої термінального обладнання схильні до вразливостей, проти яких досить важко влаштувати ефективну протидію. Успішна атака на термінальне обладнання може спричинити великі фінансові втрати його власнику та користувачеві. З кожним разом термінального обладнання поступово поповнюється все новими пристроями, які пов'язані з іншими пристроями і системами. Термінальне

обладнання – це окрема система, яка вимагає спеціального підходу та розробки ефективної системи захисту. В першому розділі кваліфікаційної роботи було проведено:

– аналіз термінального обладнання. Розглянуті технічні складові терміналу, схема принципу перерахування коштів.

– виконана класифікація інформації, що передається на серверне обладнання платіжного терміналу;

– досліджені системи керування базами даних на серверному обладнанні;

– детально проаналізовані всі можливі вразливості термінального обладнання, до цих вразливостей включено такі категорії як технічні, програмні вразливості та людський фактор;

В спеціальному розділі кваліфікаційної роботи необхідно виконати наступне:

– проаналізувати загрози для оброблюваної інформації на серверному обладнанні;

– проаналізувати операційні системи на термінальному обладнанні;

– розробити модель порушника;

– проаналізувати атаки на термінальне обладнання;

– виявити вразливості програмного забезпечення платіжного термінального обладнання;

– розробити рекомендації щодо поліпшення захисту інформації на термінальному обладнанні.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз операційних систем на термінальному обладнанні

Розглянемо операційні системи для термінального обладнання.

На сьогоднішній день існує велика кількість видів ОС, в кожній з яких різний рівень захисту, система управління, підтримка додатковий послуг. Аналіз операційних систем:

1. Microsoft Windows Embedded (IoT)– це вбудована операційна система, яка використовується в спеціалізованих пристроях. Існує кілька категорій продуктів для створення широкого спектра пристроїв, починаючи від простих контролерів реального часу і закінчуючи POS – системами, такі як кіоск самообслуговування або касовий апарат та промисловими системами;

2. Microsoft Windows Embedded POSReady (Windows Embedded for Point of Service) - вбудована операційна система для POS-терміналів, кіосків, систем самообслуговування. Володіє перевагами вбудованих операційних систем Windows IoT, такими як фільтри захисту від запису, вибір компонентів для установки, блокування спливаючих вікон, приховування завантажувальних екранів, знижена вартість ліцензії, довгий термін доступності для замовлення . Однак, на відміну від Windows Iot), Windows Embedded POSReady не вимагає спеціальних навичок для установки та настройки, а також має можливість поставки без попередньо встановленого додатка. Також, як і Windows Embedded Standard, володіє 100% сумісністю з додатками, розробленими для Windows.

3. Windows Embedded 8 Standard – модульна операційна система. Виробник пристроїв має можливість самостійно обрати, які саме сервіси та можливості будуть включені в образ. В основі платформи лежить сучасна операційна система Windows 8. Windows Embedded 8 включає в себе стандартні функції і технології для створення багатофункціональних пристроїв з використанням «multitouch», а також додатковий функціонал, який зазвичай може бути включений тільки в рамках програм корпоративного ліцензування;

Основне призначення – робота в термінальній сесії з протоколу RDP та з серверами віртуалізації VMware та Citrix.

Windows Embedded 8 Standard – це надійна та гнучка ОС для вбудованих систем, заснована на новітній операційній системі Microsoft Windows 7. У ній реалізована підтримка 32- та 64-розрядних процесорів архітектури x86.

Сумісність із найширшим спектром обладнання будь-якої продуктивності.

Windows Embedded 8 Standard повністю сумісна з усіма наявними програмами та драйверами для Windows Embedded 8 Standard що суттєво полегшує міграцію.

Інтеграція із існуючими корпоративними IT-системами.

Windows Embedded 8 Standard – перша вбудована операційна система Microsoft, що повністю підтримує мережевий протокол IPv6. Також Windows Embedded Standard 7 підтримує всі основні мережеві технології корпоративного рівня, такі як Active Directory, політики груп тощо.

Розширені функції інтерфейсу користувача та мультимедіа.

Підтримка 64-розрядних процесорів та новітніх технологій Microsoft дозволяє створювати графічні інтерфейси з необмеженими можливостями. За допомогою таких компонентів ОС, як Internet Explorer 11 і Windows Media Player 12, користувачі отримують доступ до всіх медіаможливостей сучасних настільних систем.

Вбудовані засоби керування енергоспоживанням.

За рахунок покращеного керування живленням пристрою на базі Windows Windows Embedded 8 Standard споживають менше енергії, що знижує вартість їх експлуатації та, як наслідок, підвищує ефективність використання.

Підтримувані протоколи:

– RDP 8.1, включаючи підтримку RemoteFX

– VMware з підтримкою PCoIP Цей набір програмного забезпечення дозволяє користувачам запускати кілька екземплярів x86 або x86-64-сумісних операційних систем на одному фізичному комп'ютері (встановлений клієнт Horizon View версії 3.4.0)

– ICA Citrix з підтримкою HDX (встановлений клієнт версії 4.2.100)

– Вбудований інтернет-браузер (Internet Explorer 11.0)

Протокол Remote Desktop Protocol (RDP) дозволяє віддалено підключитися до робочого стола комп'ютера з Windows і працювати з ним, як це ваш локальний комп'ютер. За промовчанням RDP доступ у Windows заборонено.

У базовий образ також включені наступні компоненти налаштування системи:

– русифікований інтерфейс;
– настроювання дати та часу;
– настроювання локалізації;
– налаштування екрана;
– налаштування робочого столу;
– налаштування мережевих з'єднань;
– встановлення та налаштування принтерів;
– встановлення та налаштування сканерів;
– налаштування віддаленого керування (віддалений доступ до робочого столу по RDP);
– налаштування фільтра захисту від запису (Enchanced Write Filter);
– керування обліковими записами користувачів;
– Налаштування системи захищено паролем.

Додаткові можливості, які можна підключити у WE8S:

– Rutoken, eToken, SmartCard тощо;
– можливість встановлення клієнта VipNet (підготовлено спеціальний образ);
– додаткових пристроїв (за наявності драйверів для Windows 8);
– мультимедійні функції;
– додаткового ПЗ за погодженням із замовником, який не порушує ліцензійну угоду Microsoft.

Також можлива кастомізація системи під потреби замовника.

4. Linux – розроблена на відкритому дистрибутиві Ubuntu Linux LTS 14.04 з ядром 3.19.0. Найважливішою перевагою Linux це мінімальний ризик того, що шкідливі програми (віруси) потраплять на комп'ютер, що у свою чергу дозволяє заощадити кошти на купівлю антивірусних програм і істотно знижує ймовірність неправомірного доступу до закритих даних системи. Для роботи ОС Linux не потрібен потужний комп'ютер. Платіжна програма буде відмінно функціонувати навіть на відносно не потужному за характеристиками обладнанні.

5. Depo ОС – реалізована на ядрі Linux, ця операційна система підтримує велику кількість сучасних протоколів віддаленого доступу. Система володіє

широкими можливостями конфігурації і управління, які можуть здійснюватися як через web – інтерфейс, локально та віддалено, так і за допомогою потужного кро-
сплатформність централізованого управління.

Переваги:

- система розроблена під певні завдання;
- зручний інтерфейс;
- проста у використанні для звичайних користувачів;
- при правильному налаштуванні стабільна в роботі.

Недоліки:

- несумісність з певними комплектуючими;
- імовірність великої кількості вразливостей в даних операційних системах;
- не всі послуги та програми будуть сумісні з даною платформою;
- можлива повільна швидкість роботи;
- уразливість до шкідливого програмного забезпечення;
- відсутність дистанційного налаштування операційної системи.

Проаналізуємо функції, які задані в таблиці 2.1, Virtual Network Computing, (VNC) — протокол надання доступу до віддаленого комп'ютера у мережі TCP/IP з будь – якого іншого комп’ютера або мобільного пристрою з ціллю відслідковування моніторингу та дистанційного керування. Remote Desktop Protocol (RDP), протокол віддаленого робочого стола — протокол прикладного рівня, що використовується для забезпечення віддаленої роботи користувача із сервером, на котрому запущений сервіс термінальних з'єднань.

Windows IoT Enterprise дозволяє створювати пристрої з фіксованою призначенням, такі як ATM-машини, pos-термінали, медичні пристрої, цифрові знаки або кіоски. Режим кіоску допомагає створити виділений та заблокований інтерфейс користувача на цих пристроях з фіксованим призначенням.

В Україну в 2002-2004 роках привозили чимало вживаних АТМ з Європи/США. Тут їх наводили у божеський вигляд, робили обслуговування та продавали банкам. Вони були приблизно в 8-12 разів дешевшими (5-8 тисяч доларів) нових сучасних банкоматів (80-110 тисяч доларів). Працювали вони, скажімо прямо, паршиво, але т.к. картковий бізнес ще тільки зароджувався і доходи були невеликі (банкомати ставляться не для своїх клієнтів, а для чужих) - нові АТМ у необхідних обсягах дозволити собі могли не всі банки. Тому ставили те, що дешевше. На АТМ були старі ЕПТ-монітори з емблемами європейських банків (попередніх власників), що вигоріли. Використовувалась операційна система для АТМ на той час – OS/2.

OS/2 - операційна система фірми IBM. Паралельно з розробкою Windows корпорація Microsoft спільно з IBM вела активну роботу з створення системи OS/2. На початку дев'яностих років шляхи двох гігантів IT-індустрії розійшлися, і розробники в IBM займалися своєю системою самостійно. Було повністю переписано ядро та драйвери, додано TCP/IP та USB-стек.

Після того, як IBM і Microsoft розійшлися в різні боки, Microsoft переробила свою версію OS/2 у Windows NT, а сама OS/2 продовжувала розроблятися у фірмі IBM, яка все ж таки не приділяла цій операційній системі належної уваги. Версію OS/2 Warp 3 серйозно розглядали як догідного конкурента Windows, але версія 4 вже не претендувала на це через рекламну діяльність Microsoft. 26 жовтня 1996 вийшла наступна версія - OS/2 Warp 4.0 (Мерлін). У 1999 з'являється OS/2 Warp Server for e-business (кодове назва "Аврора", версія системи - 4.5).

Microsoft, офіційно відмовившись від підтримки OS/2, продовжувала стежити за розвитком цієї операційної системи. Багато деталей інтерфейсу OS/2 IBM і Microsoft перейшли до нової ОС Microsoft – Windows 95.

Особливою популярністю як домашня операційна система OS/2 ніколи не користувалася, залишаючись у тіні Windows, і пізніше Windows NT. Проте зусилля як самої IBM, так і безлічі корпоративних і незалежних розробників програмного забезпечення не пройшли даремно — OS/2 є стабільною системою з передбаченою поведінкою і гарним набором системних і прикладних програм. При цьому OS/2 є самостійною лінією розвитку операційних систем, відрізняючись від

Windows NT значно меншими вимогами до апаратних засобів, а від GNU/Linux — кращою підтримкою програм для DOS і win16.

Виходячи того, що Windows найбільш популярна операційна система та більше всього використовується на термінальному обладнанні будемо розглядати саме її. Проаналізувавши офіційні джерела, на сьогоднішній день в Україні близько 59% термінального обладнанні використовують Windows IoT, як показано на рисунку 2.1.

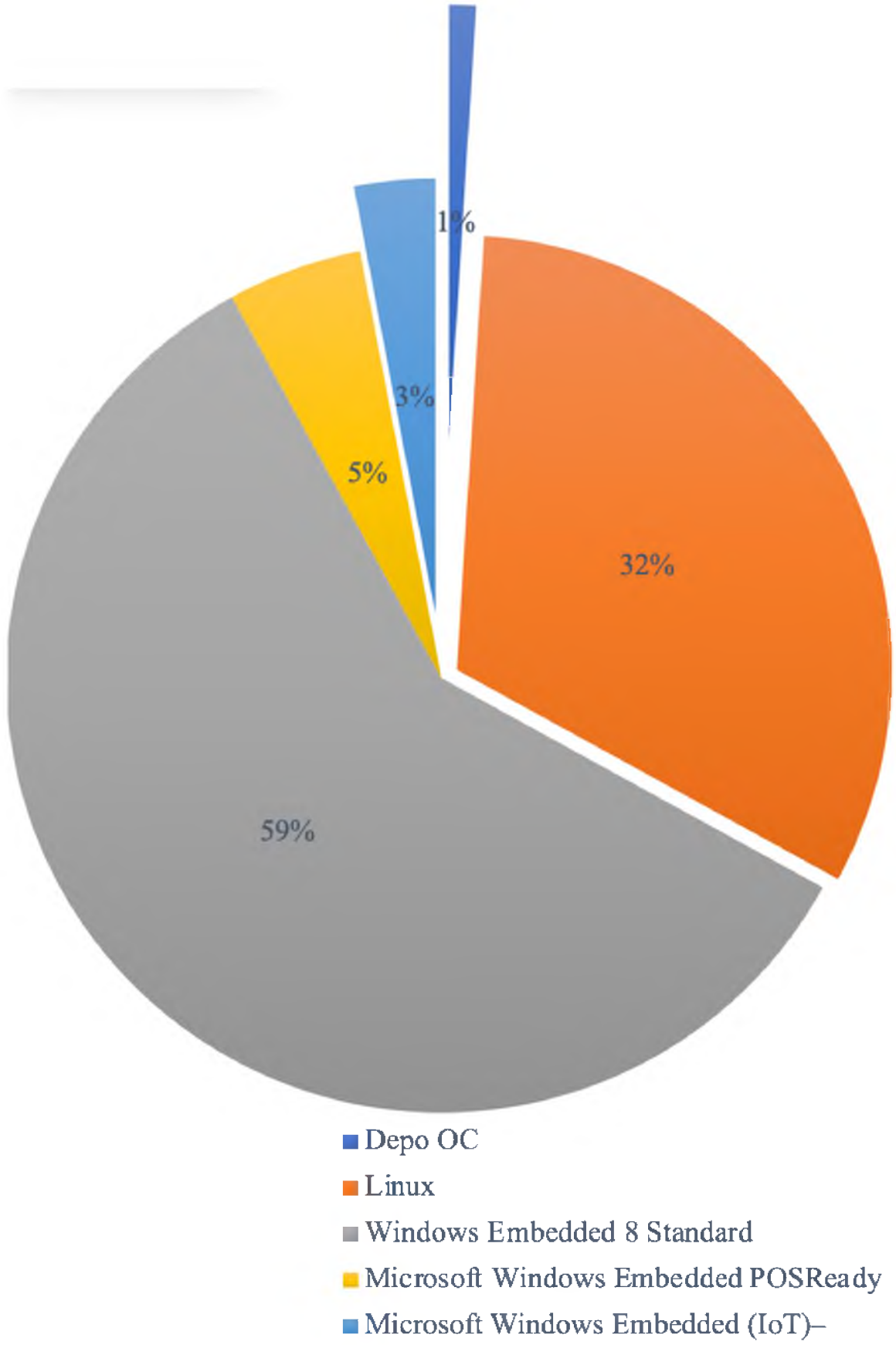

Рисунок 2.1 - Діаграма популярності використання ОС на термінальному обладнанні

Таблиця 2.1 Функції ОС для терміналів

Операційна система / Функції	Windows Embedded (IoT)	WE8S	Linux	DEPO OS
Групове управління	Не реалізовано	Не реалізовано	Не реалізовано	Реалізовано
Віддалене управління	RDP	RDP	Реалізовано (VNC)	Реалізовано (VNC,WEB)
Можливість встановлення додаткового ПЗ	Реалізовано (необхідне додаткове погодження)	За запитом	За запитом	За запитом
Підтримка додаткового обладнання	Можливо, за наявності підтримки Windows 8 та Windows 10, за запитом	За наявності підтримки Windows 8, за запитом	За наявності підтримки Linux	За наявності підтримки Linux
Захист образу від зміни	Реалізовано (Наявність фільтрів запису)	Реалізовано (Наявність фільтрів запису)	Не реалізовано	Реалізовано (Стисла файлова система)
Можливість віддаленого завантаження	Не реалізовано	Реалізовано	Не реалізовано	Реалізовано

Якщо проаналізувати таблицю 2.1 можна зробити висновки яку ОС вибрати. Сьогодні великий вибір серед ОС, які можуть відмінно працювати на термінальному обладнанні. Насправді можна вибрати та використати будь-яке ядро і налаштувати ОС під свої потреби. Але налаштування «під себе» має як позитивне значення, так і негативне. А саме такі системи налаштовані компаніями самостійно зазвичай і мають найбільший ризик, та мають велику кількість вразливостей.

Зрозуміло, що ОС Windows та Linux, мають менше, недоліків, «багів» ніж платформи, які перепрограмуванні під певні потреби. Розглянемо інформаційні термінали.

Інформаційний термінал – автоматизований програмно – апаратний комплекс, призначений для надання довідкової інформації. Він призначений для надання користувачу різної інформації без залучення обслуговуючого персоналу.

Інформаційні кіоски збирають на базі персонального комп'ютера, оснащеного сенсорним монітором і встановленого в ергономічний сталевий корпус. Додатково на інфо – кіоск може встановлюватися купюро приймач, роз'їм USB, фіскальний реєстратор, аудіо система, додатковий рекламний монітор, сканер штрих – кодів, RFID – приймач, NFC та інше обладнання.

2.2 Аналіз програмних проблем в термінальному обладнанні

Шифрування і відправки пакетів на сервер відбувається за допомогою GPRS/GSM – каналу та за допомогою технології XML – RPC.

GPRS – радіозв'язок загального користування, здійснює пакетну передачу даних. GPRS дозволяє користувачеві мережі мобільного зв'язку здійснювати обмін даними з іншими пристроями в мережі GSM та із зовнішніми мережами, в тому числі через мережу Інтернет. GPRS передбачає тарифікацію за обсягом переданої та отриманої інформації, а не за часом, проведеним онлайн. При використанні GPRS, інформація збирається в пакети і передається через невикористовуванні в даний момент голосові канали. Така технологія передбачає більш ефективне використання ресурсів мережі GSM. При цьому, що саме є пріоритетом передачі – голосовий трафік або передача даних – обирається оператором зв'язку.

GSM – глобальний стандарт цифрового мобільного зв'язку, з поділом каналів за часом (TDMA) і частоті (FDMA), відноситься до мереж другого покоління.

У стандарті GSM застосовується GMSK-модуляція з величиною нормованої смуги BT – 0,3, де B – ширина смуги фільтра за рівнем мінус 3 дБ, T – тривалість одного біта цифрового повідомлення. GSM на сьогоднішній день є найбільш поширеним стандартом зв'язку.

XML – RPC – протокол виклику віддалених процедур, що використовує XML для кодування своїх повідомлень і HTTP в якості транспортного механізму. Є «прабатьком» Simple Object Access Protocol (SOAP), відрізняється винятковою простотою в застосуванні. XML – RPC, як і будь-який інший інтерфейс Remote Procedure Call (RPC), визначає набір стандартних типів даних і команд, які програміст може використовувати для доступу до функціональності іншої програми, що знаходиться на іншому комп'ютері в мережі. Так як деякі термінали використовують відкритий протокол передачі даних, шифрування пакету на виході безглуздо. При відправці даного пакета звичайно ж канал буде зашифрований, але для злому термінального обладнання будуть потрібні всього лише ідентифікаційні дані. SQL ін'єкція – один з поширених способів злому програм, які працюють з базами даних, заснований на впровадженні в запит довільного SQL – коду. Це вірний спосіб отримати величезну кількість необхідних даних для проведення платежів, імітуючи платіжний термінал.

Основна форма атаки SQL – ін'єкція полягає в прямій вставці коду в призначені для користувача вхідні змінні, які об'єднуються з командами SQL і виконуються. Менш явна атака впроваджує небезпечний код в рядки, призначені для зберігання в таблиці або в вигляді метаданих. Коли згодом збережені рядки об'єднуються з динамічної командою SQL, відбувається виконання небезпечного коду.

Атака здійснюється за допомогою передчасного завершення текстового рядка і приєднання до неї нової команди. Оскільки до вставленої команди перед виконанням можуть бути додані додаткові рядки, зловмисник закінчує запроваджувану рядок міткою коментаря «–». Весь подальший текст під час виконання не враховується.

Впровадження SQL, в залежності від типу використовуваної системи управління базами даних (СУБД) і умов впровадження, може дати можливість атакуючому виконати запит до бази даних наприклад, прочитати вміст будь – яких таблиць, видалити, змінити або додати дані, отримати можливість читання та запису локальних файлів.

Використання класичної SQL – ін'єкції, яка привела до зміни ідентифікатора користувача та пароля. Спочатку зловмисник використовує перехоплювач, щоб захопити дійсний токен сеансу з ім'ям "ID сеансу", потім він використовує справжній токен для отримання несанкціонованого доступу до веб-сервера.

Впровадження операторів SQL – спосіб нападу на базу даних в обхід мережевого захисту. У цьому методі параметри, що передаються до бази даних через Web – додатки, змінюються таким чином, щоб змінити виконуваний SQL – запит.

Є також сліпі SQL – ін'єкцій, вони використовуються, коли веб-додаток вразливий до SQL – ін'єкцій, але зловмисник не бачить їх результатів. Сторінка з такою вразливістю може не відображати дані, але вона буде змінюватися в залежності від результату логічного твердження, впровадженого в виконуваний на ній SQL – запит. На вчинення подібної атаки може знадобитися чимало часу, оскільки, щоразу після отримання нової інформації запит доводиться переробляти. Існує кілька інструментів для автоматизації таких атак, але користуватися ними можна тільки після виявлення цільової інформації і знаходження вразливості.

До деяких портів можна спробувати увійти за протоколом telnet, але як показує практика, в основному такі сервіси працюють за технологією XML –RPC, а це означає, що порт може тільки приймати і відправляти POST-запити.

Telnet (англ. TELetype NETwork) - мережевий протокол для реалізації текстового інтерфейсу по мережі (у сучасній формі - за допомогою транспорту TCP). Назва «telnet» мають також деякі утиліти, що реалізують клієнтську частину протоколу. Протокол надає за замовчуванням мінімальну функціональність, що розширюється за рахунок опцій. Принцип обумовлених опцій вимагає проводити переговори при включенні кожної з опцій. Одна сторона ініціює запит, а інша сторона

може або прийняти, або відкинути пропозицію. Якщо запит приймається, то опція негайно набирає чинності. Опції описані окремо від протоколу як такого, і їх підтримка програмним забезпеченням довільна. Клієнту протоколу (мережному терміналу) пропонується відкидати запити на включення непідтримуваних і невідомих опцій.

На даний момент популярне шкідливе програмне забезпечення Skimer. Після запуску шкідлива програма дізнається про тип файлової системи банкомату. У разі використання FAT32 вона копіює в папку System32 динамічну бібліотеку netmgr.dll. Якщо ж застосовується NTFS, то Skimer зберігає netmgr.dll в альтернативному потоці даних файлу SpiService.exe – компоненті банкоматів Diebold, який реалізує XFS, стандартну клієнт-серверну архітектуру для фінансових програм під Windows.

Встановивши бібліотеку, шкідлива програма додає у SpiService.exe виклик, що завантажує netmgr.dll, та перезапускає систему. В результаті троян отримує повний доступ до XFS та контроль над усіма можливостями пристрою.

Шкідливою програмою можна керувати за допомогою спеціальних карток з магнітною смугою, на другій доріжці якої записані інструкції для Skimer. Інший тип карт дозволяє зловмисникам активувати одну з 21 відомих трояну команд, користуючись цифровою клавіатурою банкомату.

Зазвичай Skimer збирає дані банківських карток, вставлених у банкомат. За командою зловмисника він може роздрукувати накопичену інформацію або видати йому готівку. Крім того, у програмі передбачені команди для налагодження, оновлення та видалення трояна.

Нова версія Skimer, помічена на початку травня, захищена популярним протектором Themida, який, серед іншого, ускладнює використання налагоджувача, заважає робити дамп пам'яті, шифрує ресурси та не дозволяє моніторити файл та реєстри. Очевидно, це зроблено у тому, щоб утруднити аналіз шкідливої програми.

Пристрій для зчитування даних із кредиток (скіммер) нового типу було виявлено у Європі. Про це повідомляє у своєму блозі фахівець з безпеки Браян Кребс, який отримав інформацію від European ATM Security Team, некомерційної

організації, яка займається питаннями безпеки банкоматів. Замість класичних сканерів-накладок зловмисники використовують пристрій невеликого розміру, який встановлюється всередину банкомату поруч із слотом для карток через спеціально просвердлений отвір. Після цього отвір закривається наклейкою, внаслідок чого скіммер практично неможливо помітити.

Скіммер приєднується всередині банкомату до пристрою для карт, що зчитує, і працює на принципі прослуховування. Зловмисник вивужує через отвір дроти, що йдуть від зчитувача, приєднує пристрій до них і потім він інтерпретує дані, що передаються зчитувачем.

Пристрої для крадіжки інформації з карт стають все витонченішими, і помітити їх важче. Тільки цього літа було виявлено новий тип скіммерів, який оформляється як накладки на щілину зчитувача карт, а вставляється прямо всередину. Він складається з двох металевих пластин, електронної схеми та батарейки, яка дозволяє пристрою працювати автономно протягом кількох тижнів. Пристрій не запам'ятовує дані, а одразу передає їх на приймач, розташований неподалік.

За статистикою EAST, злочинці стали рідше використовувати скіммінг, віддаючи перевагу трапінгу та фізичним диверсіям. Чимало клопоту фахівцям з безпеки завдає ще один новий тренд — вірусні атаки на банкомати. Тут і Trojan.Skimer, і Backdoor.Ploutus, і зовсім новий зловред Tyupkin, і інші «додатки», відомі і не дуже. Малвар завантажується в комп'ютер банкомату, зазвичай із зовнішніх носіїв, і використовується для несанкціонованої видачі грошей чи перехоплення карткових даних.

Найпопулярніший мініатюрний контролер Raspberry Pi. Пристрій легко ховається всередині корпусу і не привертає уваги технічного персоналу, який, наприклад, змінює папір у вбудованих принтерах і має ключі від сервісної зони.

Знайти документацію з описом інтерфейсів банкоматів не так складно і про це ще п'ять років тому писав Олексій Лукацький у своїх «Міфах інформаційної безпеки». Обладнання АТМ та платіжних терміналів, незалежно від виробника, має спільний API для доступу та управління різними модулями та працює на платформі

Windows відповідно до єдиного стандарту «розширень для фінансових послуг» (XFS).

Знаючи API, можна отримати контроль над хост-комп'ютером банкомату і безпосередньо управляти різними периферійними пристроями, встановленими всередині шафи ATM, - картридером, клавіатурою для набору PIN-коду, сенсорним дисплеєм, диспенсером банкнот і т. п. Не варто забувати також про вразливість операції системи банкомату, які в Windows багато років уперед припасено.

Перш ніж встановити Raspberry Pi та підключити пристрій до портів Ethernet, USB або RS-232, банкомат необхідно розкрити. У верхній частині ATM є сервісна зона. Саме тут розташований комп'ютер, що управляє пристроями банкомату, мережеве обладнання (зокрема, погано захищені GSM/GPRS-модеми). Сервісна зона практично не контролюється, тому що використовується обслуговуючим персоналом для різних робіт. Отримати доступ до неї значно простіше, ніж до сейфа з грошима, розташованому внизу. Її можна відкрити нескладними у виготовленні ключами або простими підручними засобами.

Але просто відкрити мало – треба зробити це швидко та непомітно.

На конференції Black Hat дослідники Positive Technologies продемонстрували, скільки часу знадобиться зловмисникам, щоб встановити мікрокомп'ютер у сервісну зону ATM для використання його в ролі сніфера – перехоплювача PIN-коду та номера кредитної картки – або апаратного скімера, який не залишає слідів на зовнішньому вигляді банкомату. Знадобилося дві хвилини, щоб розблокувати корпус банкомату, інтегрувати мікрокомп'ютер, замаскувати та підключити його до інтернету.

У процесі підготовки до виступу Raspberry Pi був запрограмований управління периферійними модулями ATM. До мікрокомп'ютера підключався Wi-Fi-адаптер, до якого можна було підключитися з будь-якого пристрою, наприклад, зі смартфона. Команди на видачу грошей до диспенсера відправлялися за допомогою спеціально реалізованого веб-інтерфейсу. Як приклад було показано видача кількох банкнот, а після деякого доопрацювання коду, що відправляється, банкомат відразу ж розлучався з усіма закладеними купюрами. До речі, у кожній касеті

типового АТМ міститься від двох до трьох тисяч купюр, і таких касет зазвичай чотири для декількох номіналів.

2.3 Аналіз загроз для оброблюваної інформації на серверному обладнанні

Обумовлені діями суб'єкта (антропогенні джерела) — суб'єкти, дії яких можуть призвести до порушення безпеки інформації, дані дії можуть бути кваліфіковані як навмисні або випадкові злочини. Джерела, дії яких можуть призвести до порушення безпеки інформації можуть бути як зовнішніми, так і внутрішніми. Ці джерела можна спрогнозувати, і прийняти адекватні заходи.

Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації.

До них відносяться:

- потенційні злочинці та хакери;
- представники силових структур.
- несумлінні партнери;
- представники наглядових організацій і аварійних служб;

Внутрішні суб'єкти, як правило, представляють собою висококваліфікованих фахівців в області розробки і експлуатації програмного забезпечення та технічних засобів, знайомі зі специфікою вирішуваних завдань, структурою та основними функціями і принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного обладнання і технічних засобів мережі. До них відносяться:

- основний персонал (користувачі, програмісти, розробники);
- представники служби захисту інформації;
- допоміжний персонал (прибиральники, охорона);
- технічний персонал.

Техногенні джерела загроз – ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки. Технічні засоби, які є джерелами потенційних загроз безпеки інформації так само можуть бути зовнішніми:

- засоби зв'язку;

– мережі інженерних комунікації (водопостачання, каналізації);

– транспорт.

Внутрішні джерела загроз:

– неякісні технічні засоби обробки інформації;

– неякісні програмні засоби обробки інформації;

– допоміжні засоби (охорони, сигналізації, телефонії);

– інші технічні засоби, що застосовуються в установі.

Ранжування джерел загроз

Всі джерела загроз мають різну ступінь небезпеки ($К_{оп}$)i, яку можна кількісно оцінити, провівши ранжування. В якості критеріїв порівняння можна, наприклад, вибрати:

– Можливість виникнення джерела (К1)i – визначає ступінь доступності до захищеного об'єкту (для антропогенних джерел), віддаленість від об'єкта, що захищається (для техногенних джерел) або особливості обстановки (для випадкових джерел).

– Готовність джерела (К2)i – визначає ступінь кваліфікації і привабливість здійснення діянь з боку джерела загрози (для антропогенних джерел), або наявність необхідних умов (для техногенних та стихійних джерел).

– Фатальність (К3)i – визначає ступінь непереборності наслідків реалізації загрози.

Кожен показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Причому, 1 відповідає мінімальному впливу оцінюваного показника на небезпеку використання джерела, а 5 – максимальної. (К$оп$)i для окремого джерела можна визначити, як відношення добутку вище наведених показників до максимального значення (125).

$$(K_{ОП})_i = \frac{K_1 \cdot K_2 \cdot K_3}{125} \quad (2.1)$$

Таблиця 2.1. Аналіз загроз для оброблюваної інформації на серверному обладнанні

Інформація	Джерело загроз	Загрози	Ранжування джерела загрози від К1 до К5	Вразливості	Ранжування вразливостей від К1 до К5
Інформація про платіж (адреса поповнення, сума)	Антропогенні зовнішні	Умисне спотворення інформації та видалення інформації потенційними злочинцями чи хакерами	К4 $(Коп)i = \frac{4 \cdot 3 \cdot 5}{125} = 0{,}48$	Порушення режиму охорони та захисту, доступ до технічних засобів, низька кваліфікація працівників	$(Коп)f = \frac{3 \cdot 4 \cdot 3}{125} = 0{,}28$
	Антропогенні внутрішні	Порушення конфіденційності інформації в результаті ненавмисних дій	К4 $(Коп)i = \frac{4 \cdot 4 \cdot 1}{125} = 0{,}128$	Відсутність в компанії системи захищеного документообігу	К4 $(Коп)f = \frac{4 \cdot 5 \cdot 1}{125} = 0{,}16$
	Техногенні зовнішні	Засоби зв'язку, інженерні комунікації	К3 $(Коп)i$ =0,48	Кабелі не захищені коробами, можливе електромагнітне випромінювання на лінії та провідники	К4 $(Коп)f$=0,28
	Техногенні внутрішні	Неякісні програмні та технічні засоби обробки інформації	К4 $(Коп)i$ =0,128	Відсутність нового обладнання, розмагнічування носіїв інформації, збої програмного забезпечення, прикладних програм	К5 $(Коп)f$=0,16
	Стихійні зовнішні	Пожари, форс – мажорні обставини	К5 $(Коп)i$ =0,48	Відсутність систем резервування, пошкодження життєзабезпечуючих комунікацій	К3 $(Коп)f$=0,28

Продовження таблиці 2.1.

1	2	3	4	5	6
Інформація про працездатність термінального обладнання	Антропогенні зовнішні	Недобросовісні партнери, представники силових структур	К4 $(Коп)i=\frac{4\cdot4\cdot3}{125}=0,38$	Відсутність відео спостереження, порушення доступу до технічних засобів	К3 $(Коп)f=\frac{3\cdot4\cdot2}{125}=0,192$
	Антропогенні внутрішні	Умисна чи випадкова модифікація інформації основними працівниками організації	К5 $(Коп)i=\frac{5\cdot3\cdot1}{125}=0,12$	Низька кваліфікація працівників помилки працівниками при модифікації чи введенні інформації	К3 $(Коп)f=\frac{3\cdot2\cdot1}{125}=0,048$
	Техногенні зовнішні	Транспорт, інженерні комунікації	К4 $(Коп)i=0,38$	Відсутній захист коробами ліній електроживлення, можливість електричного випромінювання на лінії та провідники, електромагнітне випромінювання	К4 $(Коп)f=0,192$
	Техногенні внутрішні	Неякісні програмні та технічні засоби обробки інформації	К3 $(Коп)i=0,12$	Старіння і розмагнічування носіїв інформації, збої програмного забезпечення, прикладних програм	К2 $(Коп)f=0,048$
	Стихійний	Пожари, урагани, форс- мажорні обставини.	К3 $(Коп)i=0,38$	Відсутність систем резервування, пошкодження життєзабезпечуючих комунікація	К2 $(Коп)f=0,192$
Персональні дані	Антропогенні зовнішні	Перехоплення інфор-мації силовими, кримі-нальними структурами, недобросовісними партнерами	К5 $(Коп)i=\frac{5\cdot3\cdot2}{125}=0,24$	Відсутність відео спостереження, порушення доступу до технічних об'єктів	К5 $(Коп)f=\frac{5\cdot3\cdot2}{125}=0,24$
	Антропогенні внутрішні	Розголошення інформації про користувача технічним та основним персоналом	К5 $(Коп)i=\frac{5\cdot4\cdot1}{125}=0,16$	Порушення режиму обробки та обміну інформації	К4 $(Коп)f=\frac{4\cdot2\cdot1}{125}=0,064$

Продовження таблиці 2.1.

1	2	3	4	5	6
Персональні дані	Техногенні зовнішні	Перехоплення інформації через засоби зв'язку, інженерні телекомунікації	К3 $(Коп)i$=0,24	Важливі телекомунікаційні кабелі не захищені коробами, електричне випромінювання на лінії та провідники	К3 $(Коп)f$=0,24
	Техногенні внутрішні	Допоміжні засоби обробки інформації, збій програмного забезпечення	К4 $(Коп)i$ =0,16	Наведення електромагнітного сигналу на допоміжні засоби, відсутність регулярного оновлення антивірусного програмного забезпечення	К2 $(Коп)f$=0,064
	Стихійний	Пожар, форс - мажорні обставини	К2 $(Коп)i$ =0,24	Відсутність систем резервування, пошкодження життєзабезпечуючих комунікацій	К2 $(Коп)f$=0,24
Інформація про обробку платежу	Антропогенні зовнішні	Умисне перехоплення інформації силовими структурами, хакерами, випадкове привласнення інформації представниками надзорних організацій	К5 $(Коп)i = \frac{5 \cdot 2 \cdot 1}{125} = 0{,}08$	Порушення доступу до об'єкта, порушення режиму використання інформації	К4 $(Коп)f = \frac{4 \cdot 4 \cdot 1}{125} = 0{,}128$
	Антропогенні внутрішні	Умисна чи випадкова модифікація або видалення інформації працівниками організації.	К3 $(Коп)i = \frac{3 \cdot 4 \cdot 1}{125} = 0{,}096$	Низька кваліфікація працівників помилки при експлуатації програмного забезпечення, помилки при обробці інформації, пошкодження інформації працівниками в неробочий час	К4 $(Коп)i = \frac{4 \cdot 5 \cdot 1}{125} = 0{,}16$

Продовження таблиці 2.1.

1	2	3	4	5	6
Інформація про обробку платежу	Техногенні зовнішні	Перехоплення інформації через засоби зв'язку, інженерні телекомунікації	К2 $(Коп)i$ =0,08	Важливі телекомунікаційні кабелі не захищенні коробами. Можливість перехоплення через наводки електромагнітних випромінювань.	К4 $(Коп)f$ =0,128
	Техногенні внутрішні	Збій програмного забезпечення	К4 $(Коп)i$ =0,096	Застаріле обладнання.	К5 $(Коп)f$ =0,16
	Стихійний	Пожар, форс - мажорні обставини	К1 $(Коп)i$ =0,08	Відсутність систем резервування, пошкодження життєзабезпечуючих комунікацій	К1 $(Коп)f$ =0,128
Інформація про стан вузлів платіжних терміналів	Антропогенні зовнішні	Недобросовісні партнери, представники силових структур	К3 $(Коп)i=\frac{3\cdot 4\cdot 2}{125}=0,192$	Порушення доступу до об'єкта, порушення режиму використання інформації	К4 $(Коп)f=\frac{4\cdot 4\cdot 2}{125}=0,256$
	Антропогенні внутрішній	Умисна чи випадкова модифікація або видалення інформації працівниками організації	К3 $(Коп)i=\frac{3\cdot 2\cdot 1}{125}=0,048$	Низька кваліфікація працівників помилки при експлуатації програмного забезпечення, помилки при обробці інформації	К5 $(Коп)f=\frac{5\cdot 3\cdot 1}{125}=0,12$
	Техногенні зовнішні	Перехоплення інформації через засоби зв'язку, інженерні телекомунікації	К4 $(Коп)i$ =0,192	Можливість перехоплення через наведення електромагнітних випромінювань	К4 $(Коп)f$ =0,256
	Техногенні внутрішні	Збій програмного забезпечення	К2 $(Коп)i$ =0,048	Застаріле обладнання	К3 $(Коп)f$ =0,16
	Стихійний	Пожар, форс – мажорні обставини.	К2 $(Коп)i$ =0,192	Відсутність систем резервування, пошкодження життєзабезпечуючих комунікацій	К2 $(Коп)f$ =0,256

Виконаний аналіз загроз оброблювальної інформації на серверному обладнанні. Відносно до захищеного об'єкта стихійні джерела загроз можуть бути тільки зовнішні, для розрахунку ранжування внутрішніх загроз та вразливостей було прийнято значення «1». За допомогою ранжування загроз та вразливостей було виявлено ряд найнебезпечніших джерел:

– зовнішні загрози щодо інформації про обробку платежу (К*оп*)*і*=0,08 та інформація про стан вузлів платіжних терміналів (К*оп*)*і*=0,192;

– загрози внутрішні щодо інформації про обробку платежу (К*оп*)*і*=0,096 та інформація про стан вузлів платіжних терміналів (К*оп*)*і*=0,048;

– вразливості зовнішні щодо інформації про працездатність термінального обладнання (К*оп*)*ƒ* =0,192 та інформації про обробку платежу (К*оп*)*ƒ* =0,128;

– вразливості внутрішні щодо інформації про працездатність термінального обладнання (К*оп*)*ƒ* =0,48 та персональні дані користувачів (К*оп*)*ƒ* =0,064.

Успішне використанні вразливостей оброблюваної інформації серверного обладнання може заподіяти повну втрату інформації та прямі фінансові витрати.

2.4 Побудова моделі порушника

Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ.

Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту. Таким чином, порушника можна розглядати як особу, яка з помилки, по незнанню чи свідомо здійснює спробу виконання заборонених операцій і використовує для цього різні можливості, методи і засоби.

Реальні можливості порушника багато в чому визначаються станом об'єкту захисту, наявністю потенційних каналів витоку інформації, якістю засобів захисту інформації.

Уміння і навички можуть бути реалізовані при умові знаходження у конкретних місцях об'єкта, звідки можна реалізувати загрозу. Тому, крім рівня знань

порушника, його кваліфікації, підготовленості до реалізації своїх намірів, для формування найбільш повної моделі порушника необхідно визначити категорію осіб, до якої може належати порушник. Важливе значення мають можливості кожної категорії осіб по доступу до інформаційних ресурсів.

При формуванні моделі порушника необхідно розподілити всіх співробітників не тільки по їх можливостях щодо доступу до інформаційних ресурсів, але і по можливим втратам від дій персоналу, по потенційним збиткам від кожної категорії користувачів. Одним з варіантів розподілу збитків може бути таким:

1. Найбільші – 5;
2. Підвищені – 4;
3. Середні – 3;
4. Обмежені – 2;
5. Низькі – 1;
6. Немає – 0.

Таким чином, кожний користувач у відповідності зі своєю категорією, а значить рівнем професійних знань і можливостей доступу до інформаційних ресурсів, може нанести більші або менші збитки шляхом доступу до конкретних елементів системи обробки інформації.

Також, в модель порушника занесена інформація про те, яку саму загрозу може реалізувати порушник – модифікувати, знищити, розкрити інформацію, блокувати доступ до неї, тощо.

Таблиця 2.2 Модель порушника

Категорія осіб	Об'єкт середовища системи	Ступінь ризику відносно даних осіб до системи від 1 до 5			Спосіб реалізації загрози
		Технічна оснащеність	Можливе місце та час	Обмеження та припущення про можливий характер дій	
Системний адм тор	База даних, програмний код, який оброблює запити від користувачів технічні документи	5 К, 4Ц, 4Д	4 К	3 К, 4Ц, 2Д	Втрата інформації
Програмний інженер	База даних, програмний код, який оброблює запити від користувачів	4 К, 3Ц, 3 Д	4К, 4Д	2 К, 3Д	Відмова в обслуговуванні
Інженер інформаційної безпеки	База даних, Налаштування технічних систе безпеки, технічн документи	5 К, 5Ц, 5Д	3 Ц, 4Д	4 К, 4Д	Модифікація інформації
Користувач системи	Робота з офісним ментами	2К,1Ц, 2Д	2 Д	1 Д	Модифікація інформації

Побудувавши модель порушника, було визначено, які особи мають доступ до ресурсів системи та ступінь ризику цих осіб до інформації. Також, до об'єктів середовища системи було прийнято надати ймовірний ступінь ризику відносно об'єкта середовища, який встановлений в даній системі.

Найбільший рівень загрози має інженер інформаційної безпеки, в своєму рівні порушник є фахівцем вищої кваліфікації, знає все про автоматизовану систему і зокрема, про систему і засобах її захисту.

Порушник – це особа, яка може одержати доступ до роботи з включеними до складу КС засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами КС.

2.5 Основні проблеми програмного забезпечення термінального обладнання

Проаналізувавши роботу термінального обладнання та його програмне забезпечення, беручи до уваги усі атаки, можна зробити список основних проблем:

– не надається можливість визначати конкретних користувачів або групи користувачів, які мають право ініціювати процес, КЗЗ не здійснює розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта;

– немає механізму очищення для видалення інформації з пристрою, політика повторного використанні об’єктів не відноситься до всіх об’єктів КС;

– розподілені обов'язки, які реалізуються КЗЗ, визначають роль адміністратора і звичайного користувача. В даній локальній мережі є тільки один тип адміністраторів;

– немає можливості контролювати обсяг ресурсів, який виділяється користувачу, відсутні користувачі або адміністратори яким надані повноваження на обробку запитів;

– політика конфіденційності при обміні не визначає рівень захищеності, який забезпечується механізмами, що використовуються процесами або користувачами. КЗЗ не забезпечує захист з ознайомленням інформації при обміні.

– відсутність в системі будь якого захисту цілісності при обміні інформацією

– політика довірчої цілісності не визначає множину об’єктів КС, до яких вона відносить користувача та захищений об’єкт, за допомогою компоненту Security Reference Monitor, адміністратор може обмежувати доступ до об'єктів.

Беручи всі ці недоліки, які є актуальні для термінального обладнання, яке працює на операційній системі під назвою Windows Embedded (IoT) можна зробити рекомендації щодо поліпшення безпеки.

2.6 Рекомендації щодо поліпшення захисту програмного забезпечення термінального обладнання

Проаналізувавши загрози для оброблюваної інформації на серверному обладнанні та виявивши за допомогою ранжування найнебезпечніші загрози для інформації, з метою пониження рівня загроз був приведений аналіз технічних об'єктів на предмет вразливостей.

Було розроблено такий варіант щодо поліпшення безпеки:

– За допомогою стандартних функцій Windows Server 2016 таких, як Active Directory Rights Management Services, який призначений для того, щоб надавати доступ до файлів тільки тим користувачам, які мають на це право. Права можна налаштувати таким чином, щоб дати можливість користувачу відкривати, змінювати, друкувати, перенаправляти інформацію або виконувати інші дії з нею.

– Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем чи процесом об'єкт, спеціально назначений адміністратор цієї системи повинен повністю скасувати права доступу до об'єктів. За допомогою стека програмних продуктів таких, як « CClener 5.3, Reg Seever 7.81, Ram Def 2.6, Гриф 3» адміністратор системи може очистити повністю всі тимчасові файли та данні, які знаходяться в оперативній пам'яті.

– Надати відповідні повноваження персоналу на розподіл ресурсів. За допомогою стандартного програмного забезпечення Гриф 3, при перевищенні користувачем граничного значення генерується відповідний запис у протоколі аудиту, спроби виділення користувачу дискового простору понад квоти блокуються. Запити на зміну значень дискових квот обробляються тільки в тому випадку, якщо вони надходять від адміністраторів КЗЗ.

– Політику розподілу обов'язків повинна визначати мінімум дві адміністративні ролі, за допомогою програмного забезпечення Гриф 3, можна розподіляти користувачів системи на такі ролі як: системний адміністратор, адміністратор КЗЗ, адміністратор безпеки та користувач системи.

– Застосовувати в системі програмний засіб шифрування інформації при обміні, такий як «PGP 9.1», за допомогою цього програмного засобу можна керувати рівнем захищеності інформації, що передається, а також за допомогою стандартних функцій в Windows Server таких, як Служба сертифікатів (Active Directory Certificate Services), яка використовуються для посвідчення користувачів і комп'ютерів та для шифрування даних при їх передачі по незахищеним лініям. Служба сертифікатів Active Directory застосовуються для підвищення безпеки за рахунок зв'язування ідентифікаційних даних користувача, пристрою або служби з відповідним закритим ключем. Сертифікат і закритий ключ зберігаються в Active Directory, що допомагає захистити ідентифікаційні дані; служби Active Directory стають централізованим сховищем для отримання додатками відповідної інформації за запитом. Обмеження фізичного доступу до лінії і апаратури зв'язку.

– Встановлювати в систему програмний засіб «PGP 9.1», за допомогою якого можна реалізовувати цілісність при обміні інформацією.

– На даному рівні користувач, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів. Матриця доступу це таблиця, за допомогою якої можна визначати тип доступу, застосувати на практиці матрицю доступу можна за допомогою Active Directory, створити списки доступу на маршрутизаторах, розподілити користувачів по групам.

Програмний комплекс засобів захисту інформації від несанкціонованого доступу «Гриф» версії 3.

Def може дефрагментувати ОЗУ при досягненні рівня попередження або мовчки (з параметрами командного рядка). Вона відрізняється в плані надійності і

швидкості, і повної підтримки, яку вона пропонує своїм користувачам, з файлами довідки, керівництва з усунення неполадок, поради, онлайн допомоги, а форум гарантує вам спокій разом з екстремальною продуктивності.

CCleaner (раніше Crap Cleaner) — безкоштовна утиліта із закритим вихідним кодом, яка надає користувачам потужний і простий у використанні інструмент для очищення та оптимізації 32- та 64-розрядних операційних систем Microsoft Windows.

Служби управління правами (англ. Active Directory Rights Management Services, AD RMS, також відомі як Rights Management Services або RMS до Windows Server 2008) - серверне програмне забезпечення для управління правами доступу до інформації, що постачається з Windows Server. Воно використовує шифрування та відмову від вибіркової функціональності для обмеження доступу до таких документів, як корпоративні електронні листи, документи Microsoft Word та веб-сторінки, а також авторизованих користувачів, які працюють із ними.

PGP (англ. Pretty Good Privacy) — комп'ютерна програма, також бібліотека функцій, що дозволяє виконувати операції шифрування та цифрового підпису повідомлень, файлів та іншої інформації, поданої в електронному вигляді, у тому числі прозоре шифрування даних на запоминаючих пристроях, наприклад, на жорсткому диску.

GP поєднує в собі найкращі сторони симетричної криптографії та криптографії з відкритим ключем. PGP – це гібридна криптосистема.

Коли користувач зашифровує дані за допомогою PGP, програма для початку їх стискає. Більшість криптоаналітичних техніків засновано на статистичному аналізі шифротексту у пошуках ознак відкритого тексту. Стиск зменшує число таких ознак, що істотно підсилює опірність криптоаналізу.

Потім, PGP створює сеансовий ключ, тобто одноразовий симетричний ключ, застосовуваний тільки для однієї операції. Як тільки дані зашифровані, сеансовий ключ також шифрується, але вже є відкритим ключем одержувача. Цей зашифрований відкритим ключем сеансовий ключ прикріплюється до шифротексту і передається разом з ним одержувачеві, що показано на рисунку 2.2.

Розшифрування відбувається у зворотному порядку, як показано на рисунку 2.3. PGP одержувача використовує його закритий ключ для витягу сеансового ключа з повідомлення, яким шифротекст вихідного повідомлення відновлюється у відкритий текст. Таким чином, комбінація цих двох криптографічних методів поєднує зручність шифрування відкритим ключем зі швидкістю роботи симетричного алгоритму.

Рисунок 2.2 – Шифрування за допомогою PGP

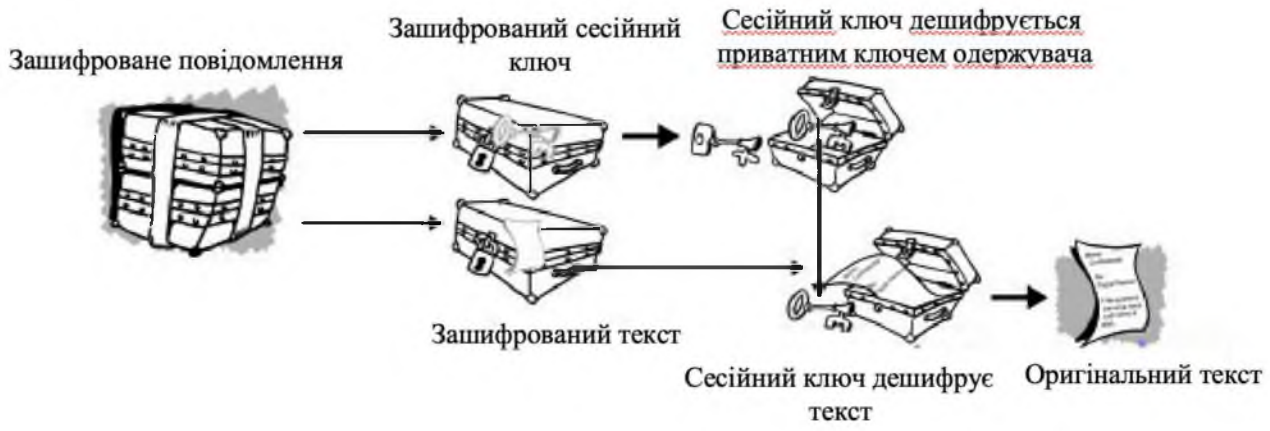

Рисунок 2.3 – Дешифрування за допомогою PGP

ВИСНОВОК

Загрози інформації можуть заподіяти велику шкоду як обладнанню. В спеціальній частині магістерської дипломної роботи був проведений аналіз загроз для оброблюваної інформації, в якій чітко визначено можливі загрози, які можуть

впливати на інформацію та пристрій в цілому. За допомогою отриманих результатів були визначенні найнебезпечніші вразливості, які можуть вплинути на інформацію та систему критично. Застосувавши ранжування загроз та вразливостей, було виявлено ряд найнебезпечніших джерел:

– зовнішні загрози щодо інформації про обробку платежу (К*оп*)*і*=0,08 та код оператора (К*оп*)*і*=0,192;

– загрози внутрішні щодо інформації про обробку платежу (К*оп*)*і*=0,096 та код оператора (К*оп*)*і*=0,048;

– вразливості зовнішні щодо інформації про працездатність термінального обладнання (К*оп*)*ƒ* =0,192 та інформації про обробку платежу (К*оп*)*ƒ* =0,128;

– вразливості внутрішні щодо інформації про працездатність термінального обладнання (К*оп*)*ƒ*=0,48 та персональні дані користувачів (К*оп*)*ƒ* =0,064.

Модель порушника – це комплексна характеристика, яка відображає можливий психологічний стан, рівень фізичної та технологічної підготовленості, дозволяє оцінити його ступінь практичної реалізації на порушення. За допомогою моделі порушника, можна побачити ступінь ризику, який належить працівнику організації. Адже обслуговуючий персонал з числа співробітників організації мають найбільш широкі можливості щодо здійснення несанкціонованих дій, в наслідок наявності в них певних повноважень по доступу до ресурсів та доброго знання технології обробки інформації і захисних заходів. Дії цих осіб безпосередньо пов'язано з порушенням діючих в організації правил та інструкцій.

Найбільший рівень загрози має інженер інформаційної безпеки, в своєму рівні порушник є фахівцем вищої кваліфікації, знає все про автоматизовану систему і зокрема, про систему і засобах її захисту.

Було проаналізовано операційні системи термінального обладнання, виділені переваги та недоліки систем, які можуть бути встановлені на термінальному обладнанні.

Проаналізовані атаки на термінальне обладнання, виявлені вразливості програмного забезпечення платіжного термінального обладнання, розроблені рекомендації щодо поліпшення захисту інформації на термінальному обладнанні.

РОЗДІЛ 3 ЕКОНОМІЧНА ЧАСТИНА

Компанія «Венера» – провідний виробник високотехнологічних систем автоматизації, компанія направлена на розробку контрольно – касових машин. Корпорація з мільоним оборотом займає одне з лідируючих положень в Україні. Річні прибутки підприємства – 1,5 млн. грн. Веде свою діяльність з 1991 року. Підприємство знаходиться в м. Дніпро, Проспект Слобожанський 109А. Чисельність

співробітників атакованого вузла чи приладу складає чотири чоловіка, чисельність адміністраторів системи та програмних інженерів складає 3 чоловіка.

3.1 Визначення трудомісткості розробки та опрацювання поліпшень.

Трудомісткість створення програмного забезпечення визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації за умови роботи одного програміста:

$$t = t_{\text{тз}} + t_{\text{а}} + t_{\text{д}} + t_{\text{пр}} + t_{\text{опр}} + t_{\text{д}} = 4 + 1{,}65 + 4{,}1 + 4{,}1 + 30{,}9 + 9{,}6 = 54{,}35 \; \textit{людино} - \textit{годин} \quad (3.1)$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку та реалізацію програмного продукту;

$t_{\text{а}}$ – тривалість вивчення технічного завдання, літературних джерел;

$t_{\text{д}}$ – тривалість розробки блок – схеми алгоритму;

$t_{\text{пр}}$ – тривалість реалізації профілю захищеності;

$t_{\text{їїд}}$ – тривалість опрацювання програми на персональному комп'ютері ;

$t_{\text{д}}$ – тривалість підготовки технічної документації на програмному засобі.

Складові трудомісткості визначаються на підставі умовної кількості операторів у програмному продукті Q (з урахуванням можливих уточнень у процесі роботи над алгоритмом і програмою).

Умовна кількість оперантів у програмі:

$$Q = q \cdot c\,(1 + p) = \; 40 \cdot 1{,}5 \cdot (1 + 0{,}1) = 66 \; \textit{штук} \quad (3.2)$$

де q =40

C =1,5

p =0,1

де q – очікувана кількість оперантів;

c – коефіцієнт складності програми;

p – коефіцієнт корекції програми в процесі її опрацювання.

Коефіцієнт складності програми ***c*** визначає відносну складність програми щодо типового завдання, складність якого дорівнює одиниці. Діапазон його зміни – 1,25...2,0.

Коефіцієнт корекції програми p визначає збільшення обсягу робіт за рахунок внесення змін в алгоритм або програму внаслідок уточнення технічного завдання. Його величина знаходиться в межах 0,05...0,1, що відповідає внесенню 3...5 корекцій і переробці 5 –10% готової програми.

Оцінка тривалості складання технічного завдання на розробку програмного забезпечення $t_{тз}$ залежить від конкретних умов і визначається на підставі експертних оцінок за узгодженням із керівником проекту.

Тривалість вивчення технічного завдання, з урахуванням уточнення технічного завдання і кваліфікації програміста можливо оцінити за формулою:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k} = \frac{66 \cdot 1{,}5}{75 \cdot 0{,}8} = 1{,}65 \, годин \qquad (3.3)$$

де B – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, B = 1,2...1,5;

k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом:

– до 2 років – 0,8;
– від 2 до 3 років – 1,0;
– від 3 до 5 років – 1,1...1,2;
– від 5 до 7 років – 1,3...1,4;

Тривалість розробки блок – схеми алгоритму:

$$t_a = \frac{Q}{(20...25) \cdot k} = \frac{66}{20 \cdot 0{,}8} = 4{,}1 \ годин \qquad (3.4)$$

Тривалість реалізації поліпшень:

$$t_{пр} = \frac{Q}{(20...25) \cdot k} = \frac{66}{20 \cdot 0{,}8} = 4{,}1 \, годин \qquad (3.5)$$

Тривалість опрацювання програми на персональному комп'ютері:

$$t_{оп} = \frac{150}{(45) \cdot k} = \frac{1{,}5 \cdot 66}{4 \cdot 0{,}8} = 30{,}9 \, годин \qquad (3.6)$$

Тривалість підготовки технічної документації на програмному засобі:

$$t_д = \frac{Q}{(15...20)\cdot k} + \frac{Q}{(15...20)} \cdot 0,75 = \frac{66}{15\cdot 0,8} + \frac{66}{15\cdot 0,8} \cdot 0,75 = 5,5 + 4,125 = 9,6 \text{ годин}. \quad (3.7)$$

3.2 Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту Кпз складаються з витрат на заробітну плату виконавця програмного забезпечення Ззп і вартості витрат машинного часу *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 13587,5 + 5887,74 = 19475,24 \text{ грн} \quad (3.8)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на пенсійне страхування і визначається за формулою:

$$З_{зп} = t \cdot З_{пр} = 54,35 \cdot 250 = 13587,5 \text{ грн} \quad (3.9)$$

де t – загальна тривалість створення програмного забезпечення, годин;

Зпр – середньогодинна заробітна плата програміста у Дніпропетровській області з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на персональному комп'ютері визначається за формулою:

$$З_{мч} = t \cdot С_{мч} = 54,35 \cdot 108,33 = 5887,74 \text{ грн} \quad (3.10)$$

де $t_{опр}$ – трудомісткість налагодження програми на персональному комп'ютері, годин;

$t_д$ – трудомісткість підготовки документації на персональному комп'ютері, годин;

$C_{мч}$ – вартість 1 години машинного часу персональному комп'ютері, грн./година.

Вартість 1 години машинного часу персонального комп'ютера визначається за формулою:

$$C_{мч} = P \cdot t \cdot C_e + \frac{Ф_{зал} \cdot Н_a}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p} = 0,8 \cdot 54,35 \cdot 2,4 + \frac{15000 \cdot 0,5}{2020} + \frac{2000 \cdot 0,33}{2020} =$$

$$= 104,3 + 3,7 + 0,33 = 108,33 \text{ грн/год} \quad (3.11)$$

де P – встановлена потужність персонального комп'ютера, кВт;

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

$Ф_{перв}$– первісна вартість персонального комп'ютера на початок року, грн.;

$Н_а$ – річна норма амортизації на персональному комп'ютері, 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).

3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період, що виражені у грошовій формі.

За методикою Gartner Group до поточних (експлуатаційних) варто відносити наступні витрати:

– вартість Upgrade – відновлення й модернізації системи ($С_в$);

– витрати на керування системою в цілому ($С_к$);

– витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ – "активність користувача").

Під "витратами на керування системою" маються на увазі витрати, пов'язані з керуванням і адмініструванням серверів та інших компонентів системи інформаційної безпеки. До цієї статті витрат можна віднести наступні витрати:

– навчання адміністративного персоналу й кінцевих користувачів;

– амортизаційні відрахування від вартості обладнання та програмного забезпечення;

– заробітна плата обслуговуючого персоналу;

– аутсорсинг (тобто залучення сторонніх організацій для виконання деяких видів обслуговування);

– навчальні курси й сертифікація обслуговуючого персоналу;

– технічне й організаційне адміністрування й сервіс.

Витрати на Upgrade відновлення й модернізацію системи інформаційної безпеки ($С_в$), цей параметр має на увазі, заміну технічного обладнання, яке вийшло із строю чи застаріло, а саме центрального процесора, жорсткого диску, оперативної пам'яті, відео карти, монітора та реалізація програмних продуктів (Гриф 3 , Лоза), які забезпечують захист інформації.

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_е + С_{ел} + С_о + С_{тос} = 13640 + 1717,3 + 47580 + 10512 + 2,4 + 12,2 + 1695,9 = 75159,8 \text{ грн.} \quad (3.13)$$

Витрати на навчання адміністративного персоналу у кількості 3 чоловік й кінцевих користувачів у кількості 2 чоловік визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації тощо ($С_н$).

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів програмного забезпечення.

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

$$С_з = З_{осн} + З_{дод} = 39000 + 8580 = 77580 \text{ грн/рік} \quad (3.14)$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8 – 10% від основної заробітної плати.

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 0,5 \cdot 8760 \cdot 24 = 10512 \text{грн} \quad (3.15)$$

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);

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

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу ($С_о$) визначаються за даними організації.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються за даними організації або у відсотках від вартості капітальних витрат (1 – 3%).

Витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$) можна орієнтовно визначити, користуючись даними табл. 1 про вагові частки статей витрат у сукупній вартості системи інформаційної безпеки.

У кожному конкретному випадку можуть бути враховані й інші види поточних витрат, що визначаються специфікою експлуатації проектованої системи інформаційної безпеки.

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак} = 9860 + 75159,8 + 3863 = 88882,8 \text{ грн} \quad (3.16)$$

3.4 Оцінка величини збитку

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (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).

Можна виділити й деякі універсальні форми нанесення збитку, наприклад, порушення конфіденційності, доступності, цілісності або автентичності ресурсу

можна характеризувати як компрометацію ресурсу, тобто втрату довіри до нього користувачів (це може мати прямий збиток, зв'язаний, наприклад, з переустановленням програмного забезпечення або проведенням розслідування).

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

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

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

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

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

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

Заробітна плата не повинна бути нижче мінімальної заробітної плати на 01 січня поточного року. Ставка єдиного соціального внеску 22% и більше згідно класу професійного ризику підприємства, на якому проводиться захист інформації.

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та програмних інженерів), осіб.;

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

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

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

I – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число можливих атак на рік.

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

$$U = П_п + П_в + V = 5450 + 11563,5 + 2682,69 = 19696,19 \text{ грн} \quad (3.17)$$

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), 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 час простою внаслідок атаки:

$$П_п = \frac{\sum З_с \cdot Ч_с}{F} \cdot t_п = \frac{\sum 10900 \cdot 4}{160} \cdot 20 = 5450 \text{ грн} \quad (3.18)$$

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч} = 1362,5 + 1701 + 8500 = 11\,563,5 \text{ грн} \quad (3.19)$$

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 співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с \cdot Ч_с}{F} \cdot t_{ви} = \frac{\sum 10900 \cdot 4}{160} \cdot 5 = 1362,5 \text{ грн} \quad (3.20)$$

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

$$П_{пв} = \frac{\sum З_о \cdot Ч_о}{F} \cdot t_в = \frac{\sum 15120 \cdot 3}{160} \cdot 6 = 1701 \text{ грн} \quad (3.21)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньо годинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) = \frac{180000}{2080} \cdot (20 + 6 + 5) = 2682{,}69 \text{ грн} \quad (3.22)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5 – ти денний робочий тиждень, 8 – ми годинний робочий день) становить близько 2080 ч.

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

$$B = \sum\sum U \cdot N \cdot I = \sum\sum 19696{,}19 \cdot 1 \cdot 3 = 59088{,}57 \text{ грн} \quad (3.23)$$

3.5 Загальний ефект від впровадження поліпшень

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

$$E = B \cdot R - C = 59088{,}57 \cdot 2 - 88882{,}8 = 29294{,}34 \text{ грн} \quad (3.24)$$

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

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

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

3.6 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині кваліфікаційній роботі, здійснюється на основні визначення та аналізу наступних показників:

- Сукупна вартість володіння (TCO);
- Коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- Термін окупності капітальних інвестицій.

Ключовою перевагою показника TCO є те, що він дозволяє зробити висновки про доцільність реалізації проекту в області інформаційної безпеки на підставі оцінки одних тільки витрат.

Показник сукупної вартості володіння (TCO) використовується, якщо величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі важко або неможливо визначити у вартісній формі.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K} = \frac{29294{,}34}{19475{,}24} = 1{,}5 \qquad (3.25)$$

де E – загальний ефект від впровадження системи інформаційної безпеки;
K – капітальні інвестиції.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження комплексу заходів інформаційної безпеки:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{19475{,}24}{29294{,}34} = 0{,}66 \text{ рока } (\sim 8 \text{ місяців}) \qquad (3.26)$$

Виходячи з формули (3.26) можна побачити, що термін окупності дорівнює 4,5 роки.

ВИСНОВОК

Успішно реалізована атака на термінальне обладнання може заподіяти прямі фінансові витрати організації. Економічно проаналізовано весь об’єкт на впровадження системи інформаційної безпеки.

На підставі проведених розрахунків можна зробити наступні висновки:

1. Визначена та детально розрахована трудомісткість реалізації поліпшень;

2. Досліджені всі можливі фінансові витрати на поліпшення системи безпеки для програмного забезпечення термінального обладнання;
3. Проаналізована величина збиту після проведених атак на систему;
4. Розрахована ефективність впровадження систем інформаційної безпеки.

Розрахувавши всі критерії можемо зробити висновок, про те що є ефективно впровадження цієї інформаційної безпеки. Так, як загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе 59088,57 грн, а після впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки становить 29294,34 грн.

ВИСНОВКИ

У кваліфікаційній роботі розв'язано актуальне наукове завдання щодо розробки нових та удосконалення існуючих систем інформаційної безпеки та аналізу термінального обладнання з точки зору безпеки.

Дослідження вразливостей, стану платіжних терміналів та серверного обладнання на якому циркулює інформація дало змогу зробити ряд висновків науково – теоретичного та прикладного характеру:

– викладено детальний аналіз платіжного термінала, а саме основні технічні характеристики платіжних терміналів, проаналізовані операційні системи, які встановлюється на обладнання та виявлені їх переваги та недоліки, як в функціональному плані так і в плані безпеки обробляємої інформації;

– класифікована інформація на серверному обладнанні, розподілена інформація на рівні конфіденційності, цілісності та доступності, визначена найцінніша інформація;

Проведено аналіз вразливостей на платіжних терміналів, а саме:

– технічні проблеми з відсутністю безперебійного живлення, відео спостереження, оптичного каналу витоку інформації, що веде за собою застосування різноманітних приладів перехоплення інформації, закладні пристрої застосовуються для доступу вихідної чи вхідної інформації;

– проаналізовані програмні проблеми, які використовуються в термінальному обладнанні та безпосередньо шкодять системі, а саме відкритий протокол передачі даних, SQL – ін'єкції за допомогою цієї атаки порушник впроваджує небезпечний код у систему, та може мати доступ до бази даних, в деякому термінальному обладнанні присутні відкриті порти передачі даних, порушники також впроваджують шкідливе програмне забезпечення для знімання інформації з приладу;

– розглянутий людський фактор, який безпосередньо вливає на систему в цілому та може мати навмисні чи випадкові дії на систему;

– розроблена таблиця порівняння баз даних, розкриті всі переваги та недоліки систему управління базами даних. На серверному обладнанні буде використовуватися система керування базами даних MS SQL. Причини вибору даної системи обґрунтовується широким поширенням системи, високою продуктивністю при низькій вартості сервера і простотою підтримки системи;

– проведений повний аналіз технології передачі інформації між платіжним терміналом та серверним обладнанням, досліджені методи передачі запросів

на сервера та методи захисту інформації. Обрана технологія передачі інформації «General Packet Radio Service», що використовує для передачі відразу декілька каналів;

– проведений повний аналіз загроз для оброблюваної інформації на серверному обладнанні, визначені основні загрози та вразливості, які можуть негативно вплинути на інформацію, яка обробляється на серверному обладнанні, за допомогою ранжування джерел загроз та вразливостей виявленні найбільш небезпечні чинники. Побудована модель порушника в якій визначається ступінь ризику відносно даних осіб до системи;

– дослідивши загрози для оброблюваної інформації на серверному обладнанні та виявивши за допомогою ранжування найнебезпечніші загрози для інформації, яка циркулює на серверному обладнанні з метою пониження рівня загроз. До проаналізованих загроз для оброблюваної інформації на серверному обладнанні рекомендовано поліпшення;

– розрахована трудомісткість реалізації поліпшень безпеки, розраховані можливі фінансові витрати на реалізацію та впровадження поліпшень. Якщо не реалізувати всіх запропонованих поліпшень загальний збиток від атак буде складати 59088,57 грн грн, а після впровадження загальний ефект буде складати 29294,34 грн. грн, тобто реалізація поліпшень є економічно ефективним рішенням.

ПЕРЕЛІК ПОСИЛАНЬ

1. Термінальне обладнання [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D1%82%D1%91%D0%B6%D0%BD%D1%8B%D0%B9_%D1%82%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B0%D0%BB;

2. Операційні системи терміналів [Електронний ресурс] – Режим доступу: https://www.depo.ru/article_a14913_r991.aspx;
3. Протокол надання доступу до віддаленого комп'ютера [Електронний ресурс] – Режим доступу: https://habrahabr.ru/post/76237/;
4. Класифікація інформаційних об'єктів [Електронний ресурс] – Режим доступу: http://www.razgovorodele.ru/security1/safety04/inf08.php;
5. Термінальні проломи: злом мереж платіжних терміналів [Електронний ресурс] – Режим доступу: https://xakep.ru/2008/03/28/43001/;
6. Tyupkin, маніпулювання банкоматами за допомогою шкідливого програмного забезпечення [Електронний ресурс]: Режим доступу:https://securelist.ru/blog/issledovaniya/23950/tyupkin-manipulirovanie-bankomatami-s-pomoshhyu-vredonosnogo-po/;
7. Оптичний канал витоку інформації [Електронний ресурс] Режим доступу http://213.182.177.142/kafedr/22.Special'-nih_informacionnih_tehnologii/teor_inf_bez_i_met_sashit_inf3/lec/%D0%9B15.htm;
8. Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки. Методики виявлення закладних пристроїв. НД ТЗІ 2.7-011-2012 – Київ 2012 р.;
9. Методи і засоби пошуку електронних пристроїв перехоплення інформації [Електронний ресурс]Режим доступу:http://www.analitika.info/poisk.php?page=1&full=block_article35;
10. Термінальні проломи: злом мереж платіжних терміналів [Електронний ресурс] – Режим доступу: https://xakep.ru/2008/03/28/43001/;
11. GSM [Електронний ресурс] :Режим доступу: https://ru.wikipedia.org/wiki/GSM;
12. SQL ін'єкції [Електронний ресурс] Режим доступу:https://xakep.ru/2011/12/06/57950;

13. Цільові атаки і шкідливі кампанії [Електронний ресурс]– Режим доступу: https://securelist.ru/analysis/malware-quarterly/29037/it-threatevolution-in-q2-2016-overview/;
14. Людський фактор в забезпеченні безпеки інформаційної [Електронний ресурс]– Режим доступу: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/03a9dfb8b576994dc3256d5700403104
15. Майк Хотек Реалізація і обслуговування Microsoft SQL Server 2008.- Русская Редакция-2011.- 576 с;
16. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99 – Київ 1999;
17. MD5 [Електронний ресурс]– Режим доступу: https://ru.wikipedia.org/wiki/MD5;
18. GSM/GPRS-модулі [Електронний ресурс]: http://www.geolink.ru/products/components/gsm.html;
19. Vpn з'єднання [Електронний ресурс] Режим доступу:https://habrahabr.ru/post/164301/;
20. Класифікація загроз в інформаційній безпеці [Електронний ресурс] Режим доступу: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml;
21. Модель порушника. Мета та принципи розробки [Електронний ресурс] Режим доступу: http://www.rusnauka.com/11_EISN_2010/Informatica/63866.doc.htm;

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	26	
6	А4	2 Розділ	30	
7	А4	3 Розділ	10	
8	А4	Висновки	12	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Пояснювальна записка Глушан Р.С.docx

2 Презентація Глушан Р.С.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

В І Д Г У К

на кваліфікаційну роботу магістра студента групи 125м-20-2

Глушана Ростислава Сергійовича

на тему: "Ідентифікація вразливостей програмного забезпечення платіжного термінального обладнання"

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 85 сторінках.

Метою кваліфікаційної роботи є проведення ідентифікації вразливостей програмного забезпечення платіжного термінального обладнання.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека», а зміст та структура проекту дозволяють розкрити поставлену тему повністю.

У зв'язку з тим, що кількість атак на платіжне термінальне обладнання збільшується з кожним роком, а саме термінальне обладнання не відповідає необхідному рівню безпеки, ідентифікація вразливостей для програмного забезпечення платіжного термінального обладнання зараз дуже актуальне та необхідне для зменшення вірогідності реалізації атаки на термінали.

Практична цінність полягає у ідентифікації вразливостей програмного забезпечення платіжного термінального обладнання та розробці рекомендацій щодо впровадження комплексу засобів захисту в інформаційну систему.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів

В ході виконання кваліфікаційної роботи студент Глушан Р.С. проявив самостійність та показав добрий рівень володіння теоретичними положеннями з обраної теми. Автор уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення та заслуговує присвоєння кваліфікації магістра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «добре».

Керівник кваліфікаційної роботи

к.т.н доцент кафедри БІТ **Олександра ГЕРАСІНА**

Керівник спец. розділу

асистент кафедри БІТ **Юлія МЛІНЧУК**