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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Перепаді Іллі Ярославовича*

академічної групи *125-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Обґрунтування засобів підвищення рівня інформаційної безпеки платіжного термінального обладнання*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	д.т.н., проф. Корнієнко В.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2023

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Перепаді І.Я.* **академічної групи** *125-19-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Обґрунтування засобів підвищення рівня інформаційної безпеки платіжного термінального обладнання*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

Розділ	Зміст	Термін виконання
1	Дослідження термінального обладнання з технічного захисту безпеки інформації	30.04.2023
2	Аналіз загроз та вразливостей для оброблюваної інформації на серверному обладнанні, розробка рекомендацій щодо реалізації профілю захищеності	24.05.2023
3	Розрахунок ефективності впровадження профілю захищеності інформації	10.06.2023

Завдання видано _____ Корнієнко В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 17.04.2023

Дата подання до екзаменаційної комісії: 12.06.2023

Прийнято до виконання _____ Перепадя І.Я.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 90 с., 7 рис., 8 табл., 6 додатка, 28 джерел.

Об’єкт дослідження: процес виявлення вразливостей термінального та серверного обладнання.

Мета роботи: аналіз систем безпеки платіжних терміналів та обґрунтування вибору стандартного функціонального профілю захищеності для інформації, що надходить на серверне обладнання.

Методи дослідження: системний підхід, методи порівняння.

У спеціальній частині дана характеристика: платіжним терміналам, базам даних; у роботі досліджено: вразливості термінального обладнання, вразливості інформації, яка обробляється на серверному обладнанні; проведено аналіз: термінального обладнання на можливі загрози та аналіз загроз для оброблювальної інформації на серверному обладнанні; запропоновано: стандартний функціональний профіль захищеності; побудовано: модель порушника; розроблено: варіанти реалізації профілю захищеності інформації.

В економічному розділі визначено: ефективність впровадження стандартного функціонального профілю захищеності.

Практичне значення роботи полягає у дослідженні стандартного функціонального профілю захищеності.

Результати здійснених у дипломній роботі досліджень можуть бути використані для удосконалення систем безпеки.

Наукова новизна дослідження полягає у наступному: аналіз вразливостей платіжного термінального обладнання та розробка рекомендацій щодо впровадження комплексу засобів захисту в інформаційну систему.

КЛЮЧОВІ СЛОВА: ЗАГРОЗИ ПЛАТІЖНОГО ТЕРМІНАЛЬНОГО ОБЛАДНАННЯ, ВРАЗЛИВОСТІ ПЛАТІЖНОГО ТЕРМІНАЛЬНОГО ОБЛАДНАННЯ, ТЕРМІНАЛЬНЕ ОБЛАДНАННЯ.

ABSTRACT

Explanatory note: 90 pages, 7 drawings, 8 charts, 6 annexes, 28 sources.

Object of study: the process of identifying vulnerabilities of terminal and server hardware. Objective: to analyze security systems of self-service terminals and have rationale of the choice of standard functional profile for the security of information received on server hardware.

Research methods: systematic approach, comparative method.

The special part has the characteristic of self-service terminals and databases. In this work, the vulnerability of terminal equipment has been studied, as well as vulnerability of information, that is processed on server hardware; the analysis of terminal equipment has been conducted – to find the potential threats and analyze threats for the information at the server hardware; a standard functional profile of protection has been offered; a model of the offender has been built; some versions of the information security profile have been developed. In the economic section an efficiency of the functional profile protection has been identified.

The practical significance of the study is to make a research of a standard functional profile protection.

The results of the research in this diploma paper can be used to improve security systems.

The scientific novelty of the analysis of vulnerabilities in payment terminal equipment and development of recommendations for the implementation of a complex of remedies in the information system.

KEYWORDS: THREATS OF SELF-SERVICE TERMINAL EQUIPMENT, VULNERABILITY OF SELF-SERVICE 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;

SSL – Secure Sockets Layer – рівень захищеності сокетів;

TFT – Thin film transistor – тонкоплівковий транзистор;

VNC – Virtual Netvork Compuing;

XML-RPC – Extensible Markup Language Remonte Procedure Call – виклик віддалених процедур;

АС – автоматизована система;

БД – база даних;

ЕОМ – електронно-обчислювальна машина;

ОС – операційна система;

ОТЗ – основні технічні засоби;

ПЗ – програмне забезпечення;

СУБД – система управління базами даних;

ТЗІ – технічний захист інформації;

ТО – термінальне обладнання.

ЗМІСТ

С.

ВСТУП

Концепція термінального обладнання включає в себе об'єднання різних сучасних технологій і рішень, здатних забезпечити комфорт і зручність отримання послуг, раціональне споживання ресурсів. Інфраструктура термінального обладнання розвивається швидше, ніж засоби її захисту, що залишає великий простір для діяльності як цікавих дослідників, так і зловмисників. Майже кожного дня людина взаємодіє з даним обладнанням, вносить туди свої дані, телефонні номери, номери банківських карток, і тому треба зробити детальний аналіз термінального обладнання з точки зору безпеки інформації та виявити основні вразливості даного обладнання.

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.

Надійний захист термінальному обладнанню на сьогоднішній день не можливо забезпечити не аналізуючи пристрій на можливі вразливості та загрози. Не впроваджуючи нових технологій захисту інформації все частіше будуть скоюватися крадіжки персональних даних користувачів та безпосередньо компанія буде нести прямі 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 та інші. Серед закордонних науковців варто згадати: Manfred Teuber, Auerbach Publrs та інших.

Актуальність теми даного дипломного проекту визначається:

- збільшенням інформаційних та технічних вразливостей термінального обладнання;
- сучасними темпами і рівнем розвитку методів забезпечення захисту інформації, які в значній мірі відстають від рівня розвитку сучасних інформаційних технологій.

Таким чином, актуальним науковим завданням, що має теоретичне і практичне значення, є розробка нових та удосконалення існуючих систем інформаційної безпеки та аналіз термінального обладнання.

Виходячи з актуальності й ступеня наукової розробки проблеми, метою дослідження є аналіз систем безпеки платіжних терміналів та обґрунтування вибору профілю захищеності для інформації, що надходить на серверне обладнання.

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

- детально проаналізувати термінальне обладнання;
- дослідити термінальне обладнання з точки зору безпеки;
- виконати аналіз вразливостей термінального обладнання;
- дослідити алгоритм передачі даних між клієнтом та серверним обладнанням;
- розробити аналіз загроз для оброблювальної інформації на серверному обладнанні;
- побудувати модель порушника;
- обґрунтувати вибір профілю захищеності;
- наведення рекомендацій щодо приведення системи захисту термінального обладнання до вимог стандартного функціонального профілю захищеності.

Об’єкт дослідження – процес виявлення вразливостей термінального та серверного обладнання.

Предмет дослідження – платіжне термінальне обладнання.

При вирішенні поставлених завдань у дипломній роботі необхідно використати: методи наукової абстракції, індукції та дедукції, аналізу і синтезу; метод спостереження, метод опису; при теоретичних дослідженнях використовують методи абстрагування, метод ідеалізації, метод формалізації, метод моделювання.

Одержання результатів ґрунтується на наступному:

- детальний аналіз технології передачі інформації між терміналом та серверним обладнанням;
- вперше обґрунтовано стандартний функціональний профіль захищеності в комп’ютерній системі, яка входить до складу автоматизованої системи третього класу з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації;

Практична цінність роботи полягає в наступному:

- дослідження загроз та вразливостей, виявлення ряду найнебезпечніших джерел загроз для інформації;
- розробка моделі порушника з прорахування ступня ризику кожної категорії;
- вибір стандартного функціонального профілю захищеності;
- надання рекомендацій щодо реалізації критеріїв профілю захищеності.

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. Термінальне обладнання може бути джерелом інформації, її 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.

Розглянемо більш детально ці 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 принцип роботи термінального обладнання (рисунок 1.1).

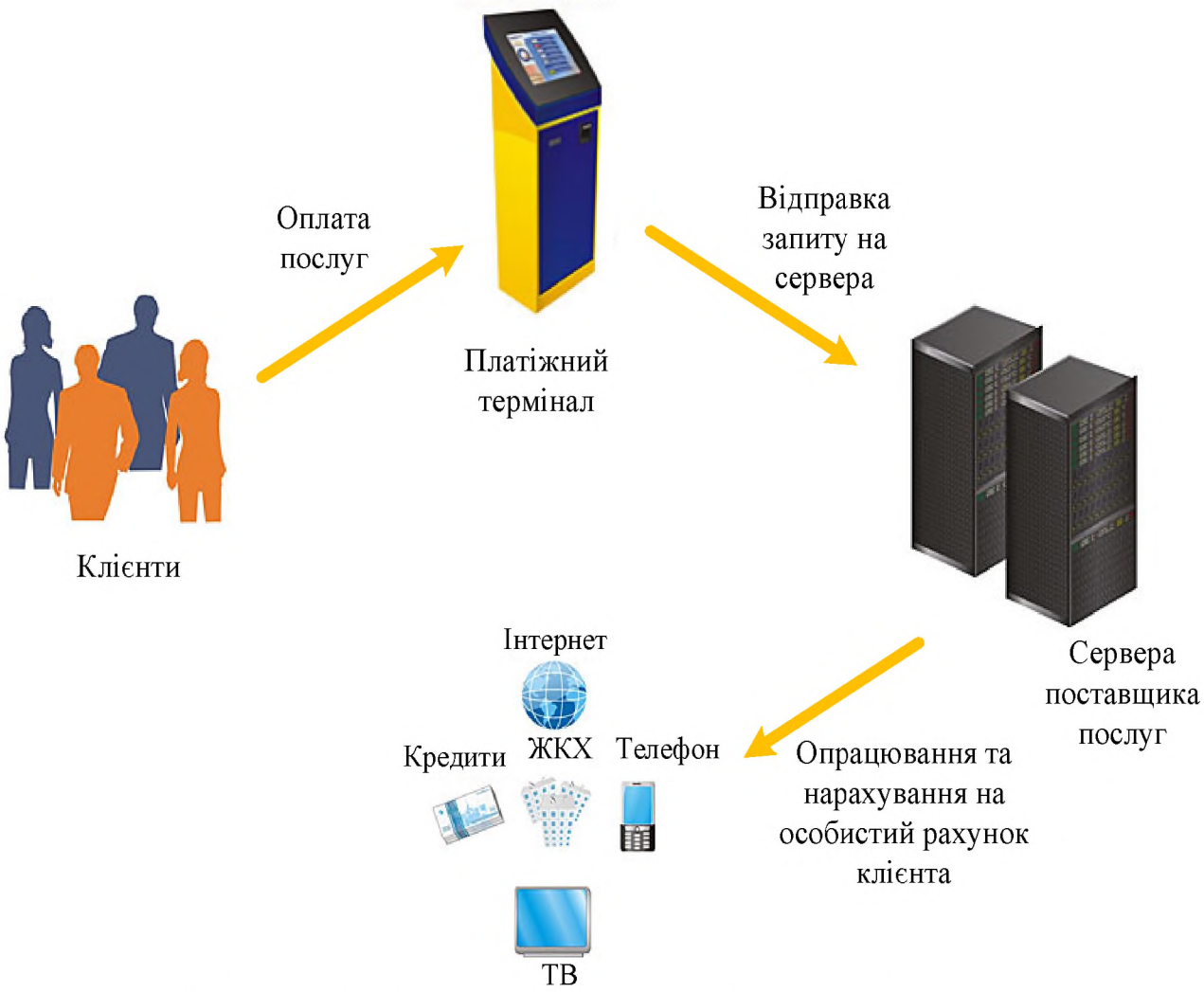

Рисунок 1.1 – Принцип роботи термінального обладнання

За допомогою екранного меню термінала користувач здійснює пошук або вибирає послугу, яку він планує оплатити, вказує необхідні реквізити. Термінал перевіряє правильність введеної інформації і при можливості, 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).

Надання користувачам можливості користуватися терміналом є послугою, за яку компанія – власник терміналу зазвичай стягує з користувачів комісію. Комісія може призначатися або як відсоток від проведеної суми, або у вигляді фіксованої суми. У будь-якому випадку, дані про величину комісії з клієнта і сума грошей, яку він реально отримає на рахунок, відображаються на екрані терміналу в той час, коли він вносить гроші в термінал.

У цих терміналів також присутній моніторинг ресурсу. Система моніторингу встановлюється і працює на окремому сервері. Можливості системи моніторингу залежать від встановленої системи електронних платежів.

– 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.

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 – 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 Embedded, 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 Embedded, 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.

4. Windows 10 IoT Core – є справжньою відмінністю, адже спеціально призначена для вбудованих пристроїв IoT, у той час як Windows 10 Enterprise/Mobile Enterprise керуватиме банкоматами, POS та мініатюрною робототехнікою, IoT Core зосередиться на комерційній сфері, наприклад на шлюзових пристроях. В основі платформи лежить сучасна багатофункціональна операційна система Windows 10.

5. Linux – розроблена на відкритому дистрибутиві Ubuntu Linux LTS 14.04 з ядром 3.19.0. Найважливішою перевагою Linux є мінімальний ризик потрапляння на комп'ютер, під керуванням якого працює термінал, шкідливих програм, що дозволяє заощадити кошти на купівлю антивірусних програм і істотно знижує ймовірність неправомірного доступу до закритих даних системи.

Для роботи Linux не потрібно потужного комп'ютерного обладнання. Платіжна програма буде відмінно функціонувати навіть на помірно потужному за характеристиками обладнанні. Так само варто згадати про високу надійність систем на базі Linux;

6. 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 кросплатформного (багатоплатвормного) централізованого управління.

Наведемо приклад переваг та недоліків даної операційної системи.

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 1.1, 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.

Таблиця 1.1 Основні відмінності між ОС для терміналів

Операційна система / Функції система	Linux	DEPO OS	WE8S	Windows Embedded (XP,7)
Групове управління	Немає	Реалізовано	Немає	Немає
Віддалене управління	Реалізовано (VNC)	Реалізовано (VNC,WEB)	RDP	RDP
Можливість встановлення додаткового ПЗ	За запитом	За запитом	За запитом	Реалізовано (необхідне додаткове погодження)
Підтримка додаткового обладнання	За наявності підтримки Linux	За наявності підтримки Linux	За наявності підтримки Windows 8, за запитом	Можливо, за наявності підтримки Windows XP та Windows 7, за запитом
Захист образу від зміни	Немає	Реалізовано (Стисла файлова система)	Реалізовано (Наявність фільтрів запису)	Реалізовано (Наявність фільтрів записи)
Можливість віддаленого завантаження	Немає	Реалізовано	Реалізовано	Немає

Проаналізувавши таблицю 1, зробимо висновки щодо вибору операційної системи. В сьогоднішній час присутня велика кількість різних операційних систем для термінального обладнання. Невелике підприємство може використати ядро будь – якої операційної системи і підлаштовують дану систему під свої потреби, це є перевагою і в той же час недоліком для даних систем. Одною з основних переваг цих систем є те що, компанія без проблем може видаляти, додавати ту чи іншу функцію, інформацію, тобто налаштовувати операційну систему під свої потреби, недоліком же є те, що найчастіше в таких системах спостерігається велика кількість вразливостей.

Розглядаючи такі потужні платформи, як Windows та Linux, може відразу зробити поверхневий висновок, що у даних платформ менша кількість вразливостей, недоліків, зависань ніж у систем, які перепрограмуванні під певні потреби. Одним з привілеїв платформ Windows і Linux, є те що вони сумісні з широким спектром обладнання на відміну від перепрограмованих систем. Так само у цих платформ може бути відсутнім великий ряд функцій, властивостей, які присутні в оригінальних платформах.

Також розглянемо один з видів терміналів – інформаційний термінал – автоматизований програмно – апаратний комплекс, призначений для надання довідкової інформації. Подібний термінал 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’єм USB, фіскальний реєстратор, аудіо система, додатковий рекламний монітор, сканер штрих – кодів, RFID – приймач, NFC та інше обладнання.

Використовуються такі термінали в людних місцях, школах, університетах, готелях та інших великих центрах.

1.2 Класифікація інформації на серверному обладнанні

Таблиця 1.2 Класифікація інформації на серверному обладнанні

№ п/п	За формую подання в інформаційному середовищі	Вид інформації	Рівні Від К0 до К5 Від Ц0 до Ц5 Від Д0 до Д5		
1.	Електрона	Інформація про платіж (адреса поповнення, сума)	К	Ц	Д
			К1	Ц2	Д2
2.		Інформація про працездатність термінального обладнання	К1	Ц1	Д1
3.		Персональні дані	К2	Ц2	Д3
4.		Інформація про обробку платежу	К2	Ц2	Д2
5.		Інформація про стан вузлів платіжних терміналів	К2	Ц1	Д2
6.	Паперова	Технічні документи	К4	Ц3	Д4
7.		Фінансові звіти за квартал	К1	Ц2	Д1

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

Всі платежі діляться на онлайн і оффлайн. Онлайн - це платіж, який надходить до постачальника послуг негайно, через мережу Інтернет. Оффлайн - це платежі, які накопичуються в базі даних платіжної системи, і в певні проміжки часу відправляються на сервер постачальника послуг.

Наразі термінальне обладнання є не невід'ємною частиною суспільства. Тема захисту інформації на термінальному обладнанні актуальна, бо суспільство використовує функціонал даного обладнання майже кожен день, це поповнення мобільних рахунків, банківських карт, оплата комунальних послуг, поповнення віртуальних гаманців та інше.

Всі платіжні та інформаційні термінали в основному працюють на операційній системі Windows або Linux. Основна відмінність цього обладнання полягає в тому, що кожен з цих пристроїв має графічну інтерактивну оболонку, яка перекриває користувачеві доступ до звичних функцій операційної системи, залишаючи лише обмежений набір можливостей, необхідних для використання терміналу. 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.

Платіжні системи відносяться до питання безпеки в останню чергу, роблячи акцент на швидкості, зручності сервісу, його функціональній частині та неперервності роботи пристрою. Сама по собі концепція онлайн–платежу вже небезпечна, так як термінальне обладнання знаходяться в громадських місцях і будь – який зловмисник не докладаючи великих зусиль може скомпрометувати дані. Ця вразливість відноситься до людського фактору.

Розглянемо основні вразливості програмно-технічного характеру.

З вищесказаного можна вважати, що 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.

Ще однією 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.

Нещодавно було виявлено шкідливу програму, що дозволяє зловмисникам спустошувати касети, де зберігались готівкою гроші, шляхом виконання прямих маніпуляцій з банкоматом.

Ця нова шкідлива програма, Tyupkin актуальна для банкоматів, що працюють під управлінням 32 – розрядної версії Microsoft Windows.

Щоб уникнути виявлення, шкідлива програма використовує кілька прийомів. Перш за все, вона активна тільки в певний час вночі. Крім того, для кожної сесії використовується ключ, що генерується з обраного випадковим чином числа. Без цього ключа взаємодія з зараженим банкоматом неможлива.

При введенні правильного ключа шкідлива програма виводить на екран інформацію про кількість грошей, доступних в кожній касеті, і дозволяє зловмиснику, що має фізичний доступ до терміналу, отримати 40 купюр з обраної

ним касети. Однак автори шкідливих програм не стоять на місці. В її останньому варіанті шкідливий код реалізує захист від аналізу.

Рисунок 1.2. – Класи вразливостей термінального обладнання

Розглянемо три класи вразливостей для термінального обладнання, які наведенні на рисунку 1. Зробимо аналіз кожного класу вразливостей і виберемо той клас в якому уразливості несуть найбільший руйнівний характер для обладнання.

1.3.1 Аналіз технічних проблем в термінальному обладнанні

Витік інформації технічними каналами інформації – це специфічний клас загроз, що вимагає для своєї реалізації спеціальних навичок і устаткування для проведення технічної розвідки. Такі, методи пускаються в хід, коли перехоплена інформація має цінність.

Почнемо розгляд з технічних проблем устаткування. Відсутність відео спостереження і безперебійного живлення веде за собою ряд важливих проблем. Безперебійне живлення дозволяє обладнанню працювати певний проміжок часу в незалежності від наявності живлення в лініях, так само можливих перезавантаженнях ліній, збоїв, проведення робіт працівниками на цих лініях та інше.

Відео спостереження повинно бути невід'ємною частиною даного обладнання, так як термінальне обладнання знаходиться в публічних місцях і може бути предметом дії зловмисників, які можуть мати на меті встановлення шкідливого програмного забезпечення, магнітних карток, впроваджувати закладні пристрої та інше.

З огляду на важливу роль візуальної інформації в житті і діяльності людини, оптичний канал витоку інформації займає домінуючу роль. Слід також врахувати, що інтенсивний розвиток технічних засобів також направлено на те, щоб підвищити ефективність органів зору людини по сприйняттю інформації. Оптичний канал забезпечує отримання інформації в будь – який час доби, в різних погодних умовах.

Безпосереднє спостереження дозволяє отримати таку необхідну інформацію, як текст документа, інформація з екрану дисплея що вводить

користувач, текст який друкується на принтері, розташування приладів на пультах управління, введенні паролі та ідентифікаційні дані.

По оптичному каналу інформація може передаватися без перетворення в електричний сигнал, для чого використовуються оптичні світловоди.

З огляду на різні способи і технічні засоби, що використовуються для перехоплення інформації, а також різні фізичні середовища (атмосфера, вода, оптичні волокна), оптичний канал витоку інформації підрозділяється на ряд каналів, які представлені на рисунку 1.3.

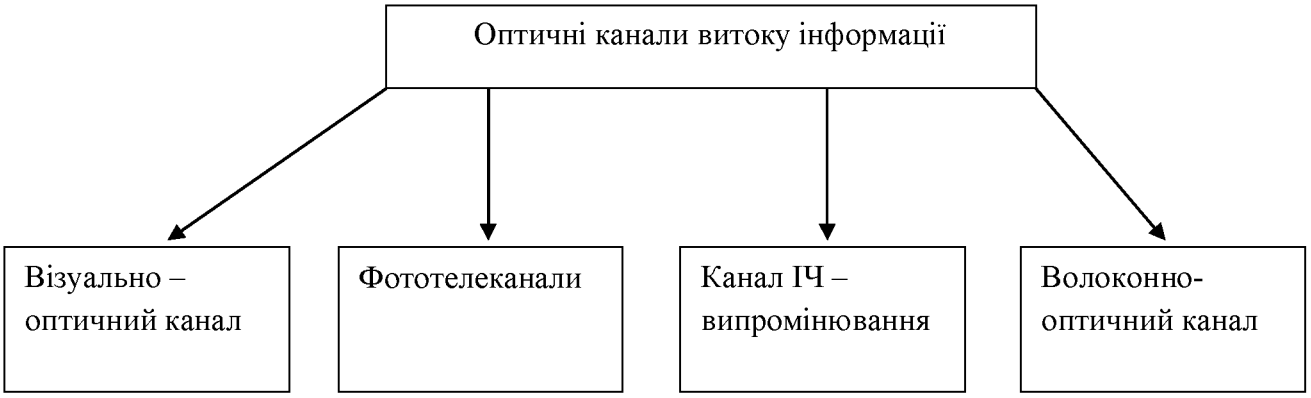

Рисунок 1.3. – Класифікація оптичних каналів витоку інформації

Структурна схема оптичного каналу витоку інформації показана на рисунку 1.4.

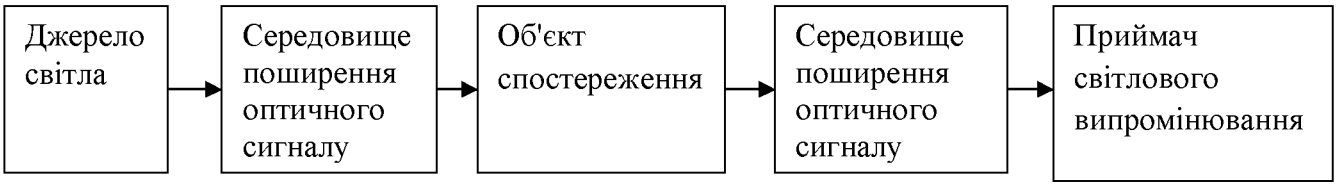

Рисунок 1.4. – Структурна схема оптичного каналу витоку інформації

До засобів, за допомогою яких здійснюють перехоплення інформації, відносять: біноклі, монокуляри, підзорні труби, спеціальні телескопи, оптичні ендоскопи. В досконаліших приладах застосовують електронну стабілізацію зображення, що забезпечує спостереження з рук або з рухомого транспорту.

Для прихованого спостереження віддалених об'єктів застосовують підзорні труби і спеціальні телескопи, які мають об'єктиви з великою фокусною відстанню.

Для візуального спостереження порожнин в різних комунікацій, внутрішніх поверхонь корпусних деталей, прямий доступ до яких в силу ряду причин неможливий, застосовують оптичні ендоскопи. Їх використовують також для спостереження через малі отвори.

Проаналізуймо закладні пристрої в термінальному обладнанні. Закладний пристрій – це потай встановлений пристрій на об'єкті інформаційної діяльності, технічний засіб негласного отримання інформації, який створює загрозу її витоку.

Найчастіше в термінальне обладнання встановлюються апаратні закладки. Під апаратної закладкою зазвичай розуміють електронний пристрій, не санкціоновано і потай встановлений у технічний засіб обробки та передачі інформації з метою забезпечити в потрібний момент часу витік інформації, порушення її цілісності або блокування.

Перехоплена за допомогою апаратних закладок інформація може передаватися в реальному масштабі часу або записуватися на спеціальні пристрої з подальшою передачею по команді. При чому команда на передавання інформації може проводитись дистанційно. У центрі обробки перехоплена інформація відновлюється і аналізується .

Апаратні закладки збираються зі стандартних модулів, використовуваних в персональному комп'ютері, з невеликими доопрацюваннями і встановлюються таким чином, щоб мати доступ до вхідної чи вихідної інформації, наприклад інформації, виведеної на екран монітора. У деяких випадках апаратні закладки можуть бути виконані у вигляді окремих модулів, встановлених в корпусі та підключених до тих чи інших його елементів.

Апаратні закладки можуть використовуватися не тільки для знімання інформації, але і для її руйнування, знищення або виведення з ладу інформації чи пристрою в цілому. Як правило, це відбувається через певний час, наприклад, через певну кількість включень пристрою, або по команді. Для руйнування інформації використовуються спеціальні комп'ютерні віруси, а виведення з ладу пристроїв найчастіше відбувається за рахунок електричного пробою схеми, механічного або хімічного пошкодження окремих її елементів.

1.3.2 Аналіз програмних проблем в термінальному обладнанні

Розглянемо відкритий протокол передачі даних, 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.

У деяких терміналів протокол передачі даних відкритий, тобто шифрування пакету на виході буде безглуздо. У тому випадку, якщо сервер організації не вимагає клієнтського сертифіката, пакет з даними може відправити будь-який бажаючий, правильним чином сформулювавши пакет. 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.

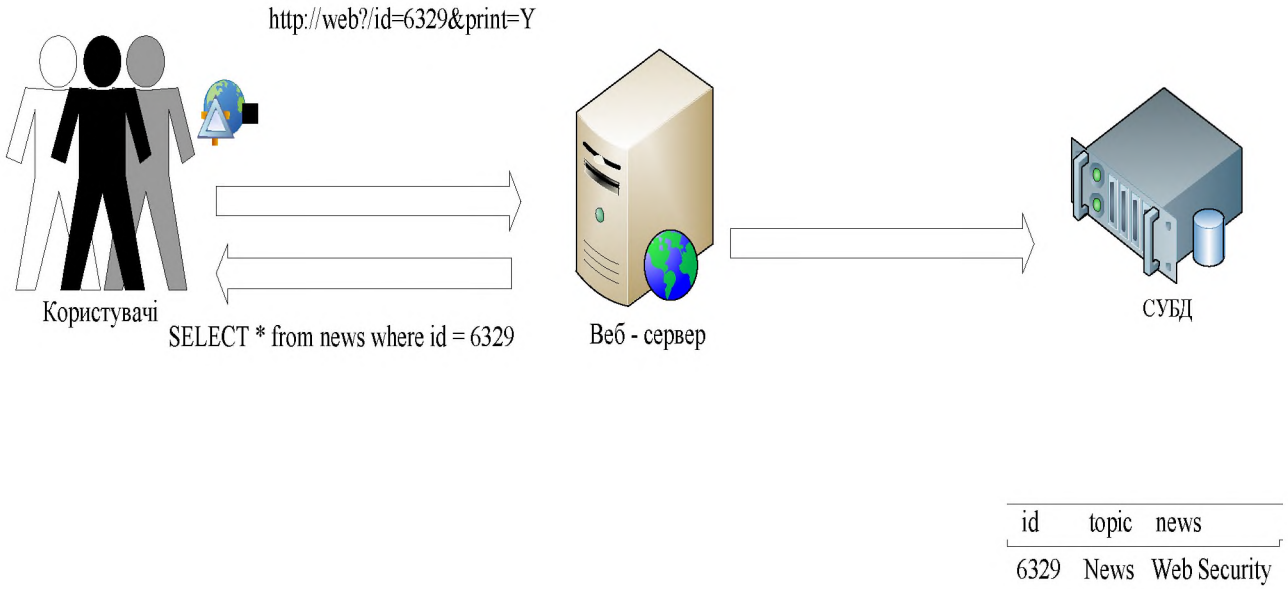

Рисунок 1.5 – SQL-запит користувачів

На Рисунку 1.5 було використано класичну SQL – ін’єкцію, вона 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.

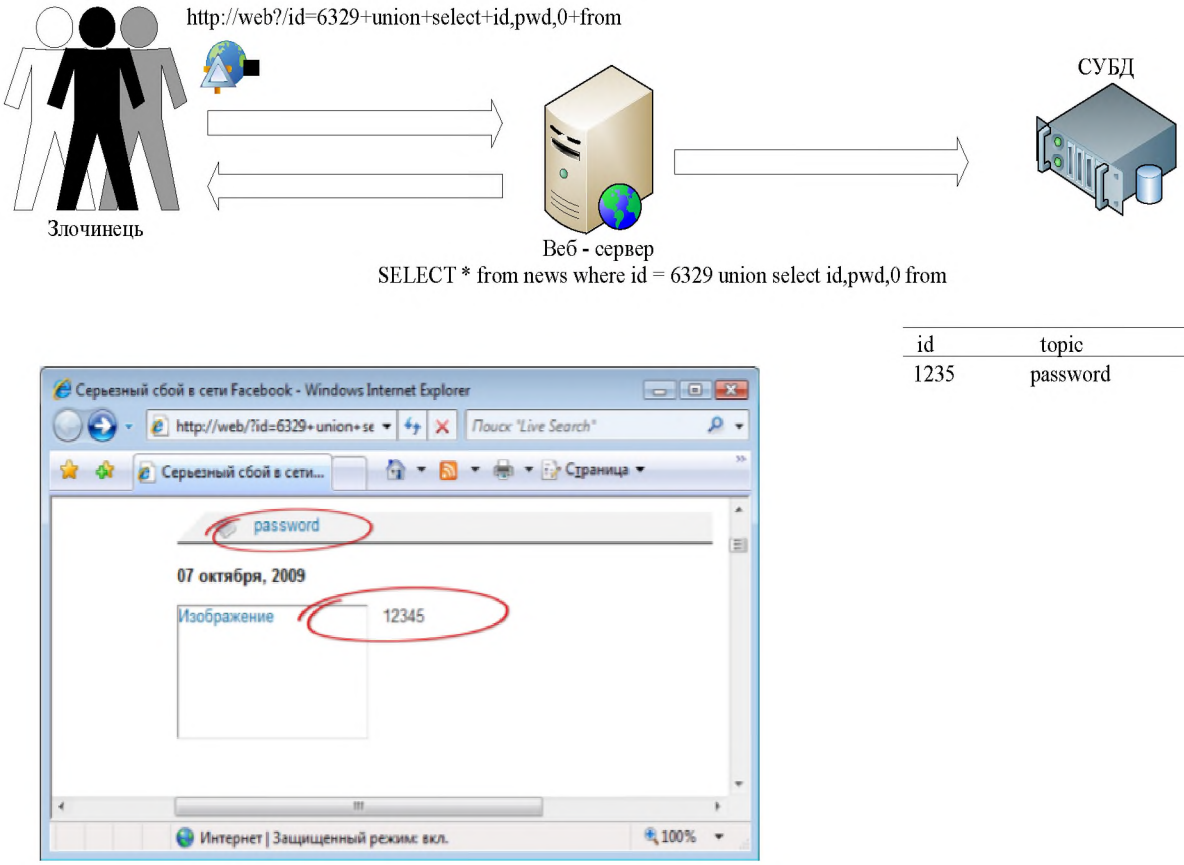

Рисунок 1.6 – Впровадження злочинцем SQL-операторів

Виділяють два види SQL – ін'єкцій.

- Класична SQL – ін'єкція - *приклад*:

SELECT * from table where name = "$_GET['name']"

SELECT id, acl from table where user_agent = '$_ SERVER ["HTTP_US ER _AGENT"]'

В цьому запиті отримуємо інформацію з таблиці «name» та виводимо таку інформацію, як заголовки, шляхи та місця розташування скриптів.

- SQL – ін'єкція у цифровому параметрі - *приклад*:

SELECT login, name from table where id = $_COOKIE["id"]

SELECT id, news from table where news = 123 limit $_POST["limit"]

Виводимо персональну інформацію користувачів браузера, якщо при запиті з'являється помилка, то вразливість присутня.

Стосовно сліпих 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. Метод пов'язаних параметрів підтримується практично всіма інтерфейсами баз даних. Відповідно до цієї технології, SQL-запит створюється разом з «наповнювачами» (на місці кожного параметра встановлюється знак питання), а потім запит компілюється у внутрішню форму. Надалі ця форма виповнюється разом з реальними параметрами. В даному випадку одинарні лапки, крапка з комою, зворотна риска, знак коментаря в SQL, не впливатимуть на SQL-запит, що направляється в базу даних для виконання, тому що введені користувачем значення будуть розумітися як дані.

Поділ і обмеження прав користувачів бази даних. Кожному користувачеві бази даних слід виділити тільки ті права, які потрібні для здійснення його функціональності. Якщо кілька Web – додатків використовують базу даних для різних цілей, рекомендується визначити для них окремо користувачів з тими правами, які необхідні кожному Web – додатку для роботи. В іншому випадку атакуючий може скористатися додатковими правами користувача бази даних.

Повідомлення про помилки, які використовуються розробником і містять налагоджену інформацію, не повинні показуватися користувачеві. Атакуючий може знайти дуже багато корисної йому інформації з цих повідомлень. Повна інформація про помилку корисна розробнику, для користувача ж вона абсолютна марна.

Аналіз відкритих портів в термінальному обладнанні, при пошуку дір в захисті платіжної системи – жертви перше, що варто зробити (це сканування портів і Web-контенту). На відкритих портах часто можна знайти цікаві самописні сервіси для проведення платежів, адміністрування терміналів. Адже жоден

працівник не буде працювати цілодобово разом з платіжними терміналами. Адміністратори застосовують різні засоби віддаленого управління, для власної зручності. Найчастіше вони навіть не замислюються про захист, сподіваючись, що ніхто не наважиться їх зламувати.

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. Щоб дізнатися про структуру запиту і його вміст, можна спробувати просканувати веб – вміст на читання. Велика кількість працівників пишуть свої сервіси з використанням asp – сторінок, які вимагають своїх початкових кодів в тих же каталогах. Якщо адміністратор термінального обладнання, не приділяє великого значення розподілу прав доступу, є велика ймовірність прочитати вихідні asp-сценарії, що при грамотному використанні може допомогти скласти XML – запит. Подібні «діри» були зафіксовані навіть у досить великих платіжних системах.

Розглянемо таке шкідливе програмне забезпечення, як Skimer. Ця шкідлива програма, відома з 2009 року, була нещодавно оновлена. Переглянута і тактика дій кібер злочинців, які її використовують. Жертвами нового вірусу стали термінали по всьому світу.

Замість традиційного підходу – приладнати до банкомату фальшивий пристрій, що читає карти, зловмисники беруть під контроль одразу весь термінал. Спочатку вони встановлюють у терміналі троянця Skimer, маючи фізичний доступ до терміналу, або зламавши внутрішню мережу терміналів.

Троянець заражає ядро пристрою – це частина пристрою, відповідальна за взаємодію з апаратною інфраструктурою в цілому, обробку карт і видачу грошей. На відміну від традиційної крадіжки даних карт за допомогою скімерів, в цьому випадку немає ніяких фізичних ознак того, що прилад заражений, і зловмисники можуть безперешкодно зчитувати дані карт, що вставляються в термінали (включаючи номери банківських рахунків і PIN-коди користувачів), або безпосередньо красти готівку з терміналу.

Зловмисник «активує» заражений пристрій, вставляючи особливу карту, на

магнітну смугу якої записані спеціальні дані. Зчитав цю карту, Skimer здатний виконати жорстко закодовану команду або отримувати команди через спеціальне меню, що активується картою. Інтерфейс Skimer стає видимим на дисплеї лише після вилучення карти і тільки якщо кібер злочинець протягом 60 секунд вводить правильний ключ сеансу. В меню доступний 21 різний варіант дій, у тому числі: видача грошей, збір даних карт, що вставляються в термінал, само видалення або встановлення оновлень. Зловмисник може записати зібрані дані карт на чіп своєї карти або роздрукувати їх.

Зловмисники діють обережно, щоб не привертати уваги. Замість того щоб просто забрати гроші з банкомату вони вичікують, іноді протягом декількох місяців, перед тим як почати діяти. Найчастіше вони збирають дані карт користувачів банкоматів, а потім створюють клони цих карт. Вони використовують клони карт в інших, незаражених банкоматах, непомітно знімаючи гроші з рахунків жертв таким чином, щоб виявити заражений банкомат було неможливо.

У деяких терміналах використовується політика фільтрації web-адреси. Однак доступ до управління політиками в них відкритий, і при бажанні можна додати або видалити будь – який сайт, що в свою чергу, відкриває атакуючому великі можливості компрометації пристрою. Наприклад, можливість доступу до будь-яких фішингових сайтів або сайтів, які розповсюджують шкідливе програмне забезпечення, потенційно ставить під загрозу такі термінали. А додавання в чорний список легітимних сайтів дозволить підвищити ймовірність переходу за фішинговим посиланням.

1.3.3 Вплив людського фактор на термінальне обладнання

Існує багато різного захисного програмного забезпечення, наприклад фаерволи, системи виявлення вторгнень, антивіруси. Кожне з яких виконує певні функції і спрямоване на вирішення певних завдань. Однак ми можемо використовувати найкраще програмне забезпечення, в якому застосовуються 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. 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.

Оскільки людина є споживачем інформації та суб'єктом її обробки, завжди існував ризик, пов'язаний з помилкою прийняття рішення – наприклад, невірно визначити коло осіб з доступом до інформації. Крім того, можливості людини у виконанні тих чи інших рішень завжди були обмежені. Характеристики, що виникають при взаємодії людини і будь – яких технічних систем в тому числі, систем обробки інформації часто називають «людський фактор».

Все термінальне обладнання знаходиться в 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 Дослідження систем керування базами даних на серверному обладнанні

Середовище MS SQL Server надає безліч різних функцій для створення безпечних додатків баз даних. У кожній версії MS SQL Server є свої засоби безпеки, як і в кожної версії Windows, при цьому можливості більш пізніх версій ширше, ніж можливості більш ранніх. Важливо розуміти, що самі по собі засоби безпеки не можуть гарантувати захист програми бази даних. Кожна програма бази даних має унікальні вимоги, середу виконання, модель розгортання, фізичне розташування і кількість користувачів. Деякі програми, які працюють локально, необхідна мінімальна захист, тоді як іншим локальним додатків або додатків, розгорнутим через мережу Інтернет, можуть вимагатися суворі заходи безпеки разом з постійним моніторингом та контролем.

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

	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 2008. Даний вибір обґрунтовується 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 2008, 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.

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 Аналіз технології передачі інформації між терміналом та серверним обладнанням

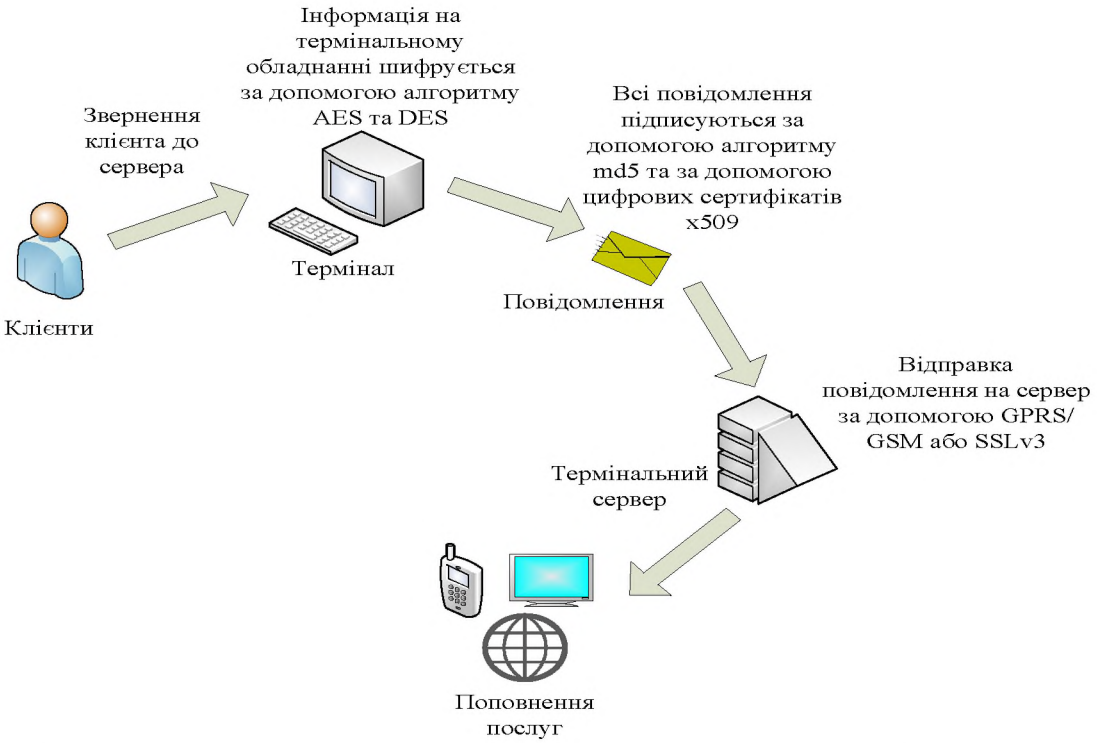

Рисунок 1.7 – Алгоритм передачі даних між клієнтом та сервером

Для передачі даних між клієнтом і сервером використовується технологія подвійного електронного цифрового підпису. Всі повідомлення підписуються з використанням авторизаційних даних вводяться на терміналі за допомогою алгоритму Message Digest 5 (md5), що робить неможливим зміну інформації, яка передається.

MD5 – 128–бітний алгоритм хешування. Призначений для створення «відбитків» або «дайджестів» повідомлень довільної довжини.

Додатково використовується розроблена технологія безпечної передачі даних на рівні повідомлень, передані дані шифруються і підписуються за допомогою цифрових сертифікатів x509 і одноразових ключів якими обмінюються клієнт і сервер перед початком обміну повідомленнями. Інформація на терміналі зберігаються в зашифрованому вигляді, що виключає можливість їх читання і спотворення.

GSM/GPRS – модулі бездротових систем M2M (Machine-to-Machine), сьогодні на Україні набрали велику популярність.

M2M – загальна назва технології, яка дозволяє машинам обмінюватися інформацією або ж передавати її в односторонньому порядку.

Основна перевага GPRS-мереж полягає в тому, що користувач оплачує тільки обсяг переданої чи отриманої інформації, а не час знаходження в мережі.

В GSM – мережі для передачі даних найчастіше використовуються такі сервіси:

- SMS (Short Message Service);
- CSD (Circuit Switched Data);
- GPRS (General packet radio Service).

SMS – послуга обміну, передача та прийом коротких текстових повідомлень в телекомунікаційній мережі, обмеження на обсяг переданих даних 160 символів, відносно висока вартість та відсутність «гарантованої доставки».

CSD – сервіс з комутацією каналів, швидкість до 9,6 кбіт/с (14,4 кбіт/с при використанні HSCSD в одному слоті). HSCSD (High-Speed Circuit-Switched Data) – технологія передачі даних для мереж GSM, покращена версія CSD. При з'єднанні, данні передаються по виділеному каналу. Підтримується протокол стиснення і корекції помилок V.42bis. Перевагою даної технології є те що, при встановленні з'єднання дані дійдуть за фіксований час. Недоліками даної системи є присутність погодинної оплати та складність використання в системах, що вимагають швидкої реакції на подію.

GPRS – сервіс з пакетною передачею даних, швидкість до 171 Кбіт/с, постійне з'єднання з мережею. Передача пакетів йде по не використовуваним в даний момент голосовим каналам, які завжди є в проміжках між розмовами абонентів. Використання для передачі відразу декількох каналів забезпечує підвищення швидкості. Перевагою даної технології є постійна готовність до передачі даних і тарифікація обсягу переданих даних, а не часу з'єднання.

Виділення слотів для передачі даних за залишковим принципом є недоліком даної передачі.

Технологія GPRS забезпечує пакетну передачу даних, від абонента до абонента на основі IP – протоколу. Наявність такої служби особливо необхідна для Інтернет – додатків, робота яких заснована саме на пакетному обміні інформацією. Технологія GPRS реалізовує гнучкий і ефективний механізм використання мережевих ресурсів GSM, коли виникає необхідність в частій передачі невеликих обсягів інформації та в менш частій передачі великих обсягів інформації (відповіді веб – сервера) при наявності тривалих пауз.

Впровадження GPRS не вимагає кардинальної модернізації інфраструктури GSM, оскільки служба передачі GPRS надбудовується над існуючою мережею GSM.

Відразу після включення і ініціалізації в GSM – мережі модем починає встановлювати GPRS – з'єднання і, в разі успішного з'єднання, отримує IP–адресу. Час очікування відповіді на один запит на з'єднання становить не більше 90 сек. Якщо протягом цього часу сервер не відповідає, модем перезавантажується, і процес повторюється, починаючи з ініціалізації модему в GSM-мережі. У разі, якщо під час очікування від сервера приходить відповідь про неможливість виділення на даний момент IP-адреси, то після закінчення захисного інтервалу в 5 секунд GPRS модем висилає повторний запит на сервер. Протягом 10 хвилин повторюваних запитів модем не отримує IP-адресу, модем також перезавантажується, і процес повторюється, починаючи з ініціалізації модему в GSM – мережі.

Системи GPRS першого покоління забезпечували надання пакетних послуг в з'єднанні «точка – точка» (Point-to-Point – PTP). Є дві версії PTP: PTP –CONS (CONS – Connection Oriented Network Service) – мережева служба PTP, орієнтована на встановлення логічного з'єднання, і мережева служба PTP-CLNS без встановлення логічного з'єднання (CLNS – Connection Less Network Service).

Служба PTP-CONS підтримує програми, засновані на протоколі X.25 і TCP/IP. Служба PTP-CLNS орієнтована на протокол UDP. У системах GPRS другого покоління реалізована багато адресна або багато крапкова пакетна передача PTM (Point-to-Multipoint).

Основні норми при організації каналів по GPRS з’єднані:

– швидкість передачі максимум 171 кбіт/с;

– час доставки даних до 15 і більше секунд;

– девіація часу доставки до ± 15 с.

Як наслідок, тимчасові таймаути повинні становити більше 30 секунд, і необхідно враховувати можливі тимчасові розриви передачі самого повідомлення наприклад, коли кілька байтів приходять через 2 секунди після відправки, а решта частина затримується на 13 секунд.

Розглянемо причини затримок доставки даних:

– Власне затримка доставки кадрів канального рівня, що визначається:

– затримкою на інтерфейсі передачі (наприклад, викликаної механізмом RTS/CTS). RTS / CTS – механізм CSMA / CA, який використовується в бездротових мережах стандарту IEEE 802.11 для виключення колізій кадрів;

– часом збирання-розбирання кадрів і їх обробки, що включає завадостійке кодування, диспетчеризацію потоків з різною якістю обслуговування, шифрування;

– затримкою передачі кадру, що включає виділення вільних слотів і поширення сигналу в фізичному каналі.

– Втрати кадрів канального рівня при їх передачі по радіолінії:

– виникнення канальних помилок;

– розрив лінії зв'язку, що виникає, наприклад, під час процедури хендовера (handover) – переходу мобільного терміналу з однієї соти в іншу;

– транспортний протокол зі своїм механізмом захисту від помилок іноді некоректно взаємодіє з аналогічними механізмами канального рівня, здійснюючи повторну передачу затриманих або загублених пакетів поряд з їх повторною канальним протоколом.

З'єднання GPRS має на увазі використання мережевого протоколу TCP/IP (Transmission Control Protocol/Internet Protocol). Оператор GSM надає для мобільного терміналу точку входу в мережу – APN (Access Point Name). Мережею

може бути Інтернет, локальна мережа, корпоративна мережа користувача. Сервер видає терміналу IP-адрес, тип якого визначається тарифним планом:

- локальний – належить оператору і невидимий з боку Інтернету;
- публічний – доступний з боку Інтернету;
- динамічний – змінюється при перевстановлені з'єднанні;
- статичний – жорстко прив'язаний до SIM-картки.

Локальні статичні адреси дозволяють організувати передачу даних між мобільними терміналами без виходу в мережу Інтернет. Забезпечується максимально швидке встановлення з'єднання. Обмін даними локалізовано в мережі оператора. Локальні динамічні адреси використовуються для доступу до ресурсів Інтернету без можливості опитування мобільного терміналу з боку Інтернету. Це найдешевші тарифи, але їх використання в системах не завжди зручно. Публічні динамічні адреси дозволяють організувати різні схеми передачі даних і багато в чому оптимальні по співвідношенню ціни і можливостей. Обмін поточними адресами здійснюється через буферний FTP-сервер. Публічні статичні адреси в основному використовуються в системах з VPN-тунелями.

Стосовно безпеки передачі даних по мережі GPRS. Розглянемо частину засобів:

- при передачі даних від терміналу до обслуговуючого вузла дані шифруються відповідно до алгоритм GEA 1,2,3. Алгоритм шифрування в технології GPRS (GEA1, GEA2, GEA3) відрізняються від алгоритмів шифрування в GSM (A5 / 1, A5 / 2, A5 / 3), але розроблений на їх основі.
- захист локальної мережі оператора забезпечується блокуванням доступу з зовнішніх мереж по RFC 1918.

Окремо можна виділити сервіс, значимість і кількість інсталяцій якого постійно зростають, а вартість падає це VPN – тунель (Virtual Private Network).

VPN – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж.

Мета VPN – забезпечити прозорий захищений доступ до ресурсів локальної мережі користувача з мобільного терміналу через незахищену мережу Інтернет або виділені канали. Оператор зв'язку створює унікальну точку доступу – APN – сервер, що підтримує IP – адреси, виділені оператором, або належать користувачеві. Організовується тунель від сервера до локальної мережі користувача (протоколи: L2TP, GRE, IPSec). У додаткові сервіси включено повноцінне шифрування даних.

1.6 Дослідження найбільш вагомих проблем в термінальному обладнанні

Більшість проаналізованих загроз безпосередньо впливають на інформацію, а саме на конфіденційність, цілісність, доступність, спостережливість.

Дослідивши проблеми термінального обладнання, найбільш вагому загрозу для інформації, яка циркулює на пристрої призводять такі загрози як: відсутність тих чи інших програмних об’єктів на обладнанні, не правильно розподілені користувачі в системі стосовно їх прав доступу, відсутня конфіденційність при обміні інформації.

У зв’язку з інтенсивним використанням автоматизованих систем в різних областях життєдіяльності все більш актуальним стає питання забезпечення безпеки оброблюваної інформації.

Згідно з проаналізованих вразливостей на термінальному обладнанні та ретельного дослідження приладу, інформація, яка надходить та обробляється на серверному обладнанні є не досконально захищеною, тому до серверної системи застосують стандартний функціональний профіль захищеності.

Відповідно до нормативних документів кожен стандартний функціональний профіль захищеності є набором відповідних функціональних критеріїв. Кожен критерій є набором функцій, що дозволяє противостояти певним загрозам, при чому кожен критерій включає в себе кілька рівнів. Вибір та реалізація профілю захищеності залишається за користувачем, якому надані відповідні повноваження.

Функціональний профіль захищеності – це мінімальний набір послуг

для забезпечення рівня захищеності. 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.

1.7 Висновки

Більшість пристроїв термінального обладнання схильні до вразливостей, проти яких досить важко організувати ефективну протидію. Успішно проведена атака на термінальне обладнання може заподіяти прямі фінансові втрати його власнику. Зловмисник може використовувати «підлеглий» термінал для злому інших, адже вони часто об'єднані в мережу.

З кожним роком термінальна інфраструктура 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 магістерської дипломної роботи зроблений детальний аналіз платіжного термінального обладнання. В ході аналізу були отримані наступні результати:

- виконаний детальний аналіз термінального обладнання. Розглянуті технічні складові терміналу, схема принципу перерахування коштів. Проаналізовані операційні системи термінального обладнання, виділені переваги та недоліки систем, які можуть бути встановлені на термінальному обладнанні;
- виконана класифікація інформації, що передається на серверне обладнання платіжного терміналу;

- детально проаналізовані всі можливі вразливості термінального обладнання, до цих вразливостей включено такі категорії як технічні, програмні вразливості та людський фактор;
- досліджені системи керування базами даних на серверному обладнанні;
- досліджена технологія передачі даних з терміналу на серверне обладнання. Проаналізовані переваги та недоліки передачі інформації на серверному обладнанні.

В спеціальному розділі магістерської дипломної роботи необхідно навести наступні заходи:

- проаналізувати загрози для оброблюваної інформації на серверному обладнанні;
- розробити модель порушника;
- обґрунтувати вибір та проаналізувати об'єкти на предмет виконання стандартного функціонального профілю захищеності інформації від несанкціонованого доступу;
- розробити рекомендації щодо приведення системи захисту термінального обладнання до вимог стандартного функціонального профілю захищеності ЗКЦД.1.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз загроз для оброблюваної інформації на серверному обладнанні

Антропогенними джерелами загроз в безпеці інформації виступають суб'єкти, дії яких можуть бути кваліфіковані, як умисні або випадкові. Ця група найбільш поширена і представляє інтерес з точки зору організації захисту, так як дії суб'єкта не завжди можна оцінити, спрогнозувати і вжити адекватних заходів.

Зовнішні джерела можуть бути випадковими або навмисними і мати різний рівень кваліфікації. До них відносяться:

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

Внутрішні суб'єкти, як правило, представляють собою висококваліфіковани х 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. Даний клас джерел загроз в безпеці інформації є особливо актуальним в сучасних умовах, тому що зростання числа техногенних катастроф, викликаних фізичним і моральним старінням технічного парку використовуваного обладнання, а також відсутністю

матеріальних коштів на його оновлення. 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:

1. 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).

2. 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).

3. 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. $(Коп)i$ для окремого джерела можна визначити, як відношення добутку вище наведених показників до максимального значення (125).

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

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 в ипромінювання 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 $(Коп)f = 0,28$
Інформація про працездатність термінального обладнання	Антропогенні зовнішні	Недобросовісні партнери, представники силових структур	К4 $(Коп)i = \frac{4 \cdot 4 \cdot 3}{125} = 0,38$	Відсутність відео спостереження, порушення доступу до технічних засобів	К3 $(Коп)f = \frac{3 \cdot 4 \cdot 2}{125} = 0,192$
	Антропогенні внутрішні	Умисна чи випадкова модифікація інформації основними працівниками організації	К5 $(Коп)i = \frac{5 \cdot 3 \cdot 1}{125} = 0,12$	Низька кваліфікація працівників помилки працівниками при модифікації чи введенні інформації	К3 $(Коп)f = \frac{3 \cdot 2 \cdot 1}{125} = 0,048$

Продовження таблиці 2.1.

1	2	3	4	5	6
Інформація про працездатність термінального обладнання	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, недобросовісним и партнерами	К5 $(Коп)i = \frac{5 \cdot 3 \cdot 2}{125} = 0,24$	Відсутність відео спостереження, порушення доступу до технічних об'єктів	К5 $(Коп)f = \frac{5 \cdot 3 \cdot 2}{125} = 0,24$
	Антропогенні внутрішні	Розголошення інформації про користувача технічним та основним персоналом	К5 $(Коп)i = \frac{5 \cdot 4 \cdot 1}{125} = 0,16$	Порушення режиму обробки та обміну інформації	К4 $(Коп)f = \frac{4 \cdot 2 \cdot 1}{125} = 0,064$
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 $(Коп)f = \frac{4 \cdot 4 \cdot 1}{125} = 0,128$

Продовження таблиці 2.1.

1	2	3	4	5	6
Інформація про обробку платежу	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 $(Коп)i = \frac{4 \cdot 5 \cdot 1}{125} = 0,16$
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 ко мунікацій	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*) f =0,192 та інформації про обробку платежу (К*оп*) f =0,128;
- вразливості внутрішні щодо інформації про працездатність термінального обладнання (К*оп*) f =0,48 та персональні дані користувачів (К*оп*) f =0,064.

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

2.2 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 адміністратор	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 систем безпеки, технічні документи	5 К, 5Ц, 5Д	3 Ц, 4Д	4 К, 4Д	Модифікація інформації
Користувач системи	Робота з офісними документами	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.

2.3 Обґрунтування вибору стандартного функціонального профілю захищеності від несанкціонованого доступу для захисту інформації, що циркулює на термінальному обладнанні

Розглянута система відноситься до автоматизованої системи третього класу.

Автоматизована система третього класу – розподілений, багатомашинний, багато користувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Стандартний функціональний профіль захищеності в КС, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:

3.КЦД.1 = { КД – 2, КО – 1, КВ – 1,

ЦД – 1, ЦО – 1, ЦВ – 1,

ДР – 1, ДВ – 1,

НР – 2, НИ – 2, НК – 1, НО – 2, НЦ – 2, НТ – 2, НВ – 1 }

Умовні позначення:

- АС – автоматизована система;
- КС – комп'ютерна система;
- ОС – операційна система;
- КЗЗ – комплекс засобів захисту.

Критерії.

Довірча конфіденційність. Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших

користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Базова довірча конфіденційність (КД – 2). Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації. Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту

Повторне використання об'єктів. Послуга дозволяє забезпечити коректність повторного використання розділених об'єктів, гарантуючи, що в разі, якщо розділений об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

Повторне використання об'єктів (КО – 1). Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Конфіденційність при

обміні. Послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна конфіденційність при обміні (КВ – 1). Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Довірча цілісність. Послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна довірча цілісність (ЦД – 1). Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відносить користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту. *Відкат*. Послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

Обмежений відкат (ЦО – 1). Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Цілісність при обміні. Послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Мінімальна цілісність при обміні (ЦВ – 1). Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів та/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання. Використання ресурсів. Послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Квоти (ДР – 1). Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

Відновлення після збоїв. Послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

Ручне відновлення (ДВ – 1). Політика відновлення, що реалізується КЗЗ,

повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС. Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування. *Реєстрація*. Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Захищений журнал (НР – 2). Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Ідентифікація і автентифікація. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

Одиночна ідентифікація і автентифікація (НИ – 2). Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці

атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікований ідентифікатор цього користувача.

Достовірний канал. Послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ран жируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

Одно направлений достовірний канал (НК – 1). Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

Розподіл обов'язків. Послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Розподіл обов'язків адміністраторів (НО – 2). Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

Цілісність комплексу засобів захисту. Послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

КЗЗ з гарантованою цілісністю (НЦ – 2). Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен

підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ран жируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

Самотестування при старті (НТ – 2). Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

Ідентифікація і автентифікація при обміні. Послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Автентифікація вузла (НВ – 1). Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму. Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

2.4 Аналіз об’єктів на предмет виконання вимог функціонального профілю захищеності інформації

Таблиця 2.3 Аналіз виконання вимог стандартного функціонального профілю захищеності інформації

Критерії які входять в 3.КЦД.1	Реалізація критеріїв
Базова довірча конфіденційність (КД – 2)	Не реалізується, КЗЗ не надає можливості 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.
Повторне використання об'єктів (КО – 1)	Не реалізується, в даній системі немає механізму очищення для видалення інформації з пристрою, політика повторного використанні об’єктів не відноситься до всіх об’єктів КС.
Мінімальна конфіденційність при обміні (КВ – 1)	Не реалізується, 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.
Мінімальна довірча цілісність (ЦД – 1)	Критерій реалізований частково , 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.
Обмежений відкат (ЦО – 1)	Критерій реалізований, за допомогою функції в Windows Server 2008R «відновлення системи» можна повернути частину об'єкт до заданої точки відновлення.
Мінімальна цілісність при обміні (ЦВ – 1)	Критерій не реалізований, відсутність в системі будь якого захисту цілісності при обміні інформацією.
Квоти (ДР – 1)	Критерій не реалізований, немає можливості контролювати обсяг ресурсів, який виділяється користувачу, відсутні користувачі або адміністратори яким надані повноваження на обробку запитів.
Ручне відновлення (ДВ – 1)	Критерій реалізований, для відновлення системи адміністратор заходить під правами адміністратора і відновлює систему за допомогою стандартних

	засобів Windows. Для відновлення стану системи можна використовувати команду Wbadmin.

Продовження таблиці 2.3

1	2
Захищений журнал (НР – 2)	Критерій реалізований, за допомогою журналу подій в операційній системі Windows можна простежувати час, дату входу в систему, так само даний журнал можна імпортувати, доступ до журналу подій має тільки адміністратор.
Зовнішня ідентифікація і автентифікація (НИ – 2)	Критерій реалізований, КЗЗ автентифікує користувача за допомогою протоколу парольної автентифікації Password Authentication Protocol (PAP) – це протокол простої перевірки автентичності, який передбачає відправку імені користувача і пароля на сервер відкритим текстом. Встановлена система, яка забезпечує захист від несанкціонованого доступу.
Однонаправлений достовірний канал (НК – 1)	Критерій реалізований, достовірний канал використовується для ідентифікації і автентифікації користувачів, ці два параметра розпізнають користувача в системі та перевіряють справжність введених даних користувача за допомогою контролера домену. Реалізація контролера домену відбувається за допомогою служби каталогів Active Directory.
Розподіл обов'язків адміністраторів (НО – 2)	Критерій реалізований частково, розподілені обов'язки, які реалізуються КЗЗ, визначають роль адміністратора і звичайного користувача. В даній локальній мережі є тільки один тип адміністраторів.
КЗЗ з гарантованою цілісністю (НЦ– 2)	Критерій реалізований, засоби захисту в змозі визначати домен, а також механізми захисту, які використовуються для реалізації розподілених доменів за допомогою контролера доменів, яка виконується в Active Directory .
Самотестування при старті (НТ– 2)	Критерій реалізований, при включенні обладнання відбувається самотестування, критичні функції тестуються за допомогою стандартних функцій Windows таких як Power – On self-test (POST) це програма самотестування комп'ютера,яку виконує центральний процесор після подачі живлення або отримання команди RESET.

Автентифікація вузла (НВ– 1)	Присутня ідентифікація та автентифікація КЗЗ при обміні інформацією за допомогою протоколу IP Security.

Проаналізувавши стандартний функціональний профіль захищеності в комп'ютерній системі, що входять до складу автоматизованої системи третього класу з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації, а саме 3.КЦД.1, можемо зробити висновки щодо того, які критерії комплекс засобів захисту реалізує, а які не реалізує.

2.5 Рекомендації щодо приведення системи захисту термінального обладнання до вимог стандартного функціонального профілю захищеності 3.КЦД.1

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 виконання стандартного функціонального профілю захищеності інформації.

Критерії щодо реалізації профілю захищеності наведені в таблиці 2.4:

Таблиця 2.4 Варіанти реалізації профілю захищеності інформації

Нереалізовані критерії	Рекомендації щодо реалізації критеріїв захищеності
Базова довірча конфіденційність (КД – 2)	За допомогою стандартних функцій Windows Server 2008R 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.
Повторне використання об'єктів (КО – 1)	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

Продовження таблиці 2.4

1	2
Повторне використання об'єктів (КО – 1)	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.
Квоти (ДР – 1)	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.
Розподіл обов'язків адміністраторів (НО – 2)	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.
Мінімальна конфіденційність при обміні (КВ – 1)	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

Продовження таблиці 2.4

1	2
Мінімальна конфіденційність при обміні (КВ – 1)	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.
Мінімальна цілісність при обміні (ЦВ – 1)	Встановлювати в систему програмний засіб «PGP 9.1», за допомогою якого можна реалізовувати цілісність при обміні інформацією
Мінімальна довірча цілісність (ЦД – 1)	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.

В таблиці 2.4 розроблене рішення критеріїв, реалізація яких дозволяє забезпечити повноцінний захист інформації.

Конфіденційність забезпечується такими послугами: базова довірча конфіденційність, повторне використання об'єктів, мінімальна конфіденційність при обміні.

Цілісність забезпечується такими послугами: мінімальна довірча цілісність, мінімальна цілісність при обміні.

Доступність забезпечується такими послугами: «квоти».

Цілісність забезпечується такими послугами: «розподіл обов'язків адміністраторів».

2.6Висновки

Загрози інформації можуть заподіяти велику шкоду як обладнанню, яке належить підприємству, так і користувачеві. 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.

Профіль захищеності – це мінімально необхідний рівень послуг, який повинен реалізувати комплексу засобів захисту обчислюваної системи АС щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС. Стандартний функціональний профіль захищеності слугує засобом для мінімізації вразливостей, які представленні в таблиці «Аналіз загроз оброблюваної інформації».

Проаналізовані послуги, які входять до стандартного функціонального профілю 3.КЦД.1, ретельно досліджено функції цього профілю, які можуть реалізовуватися за допомогою встановленої в організації системи засобів захисту, а які послуги не можливо реалізувати за існуючої системи захисту. Також були обґрунтовані вразливості, які шкодять системі та інформації та запропоновані заходи щодо їх запобігання за допомогою реалізації послуг стандартного профілю захищеності.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

Компанія «ІТЕРА-ТОП» – провідний виробник високотехнологічних систем автоматизації. Діяльність направлена на розробку контрольно – касових машин. Компанія з мільйонними оборотами, займає одну з лідируючих позицій в Україні. Річні прибутки підприємства досягають – 1,5 млн. грн. Веде свою діяльність з 2002 року. Підприємство знаходиться в м. Дніпро, проспект Сергія Нігояна, 63.
Чисельність співробітників атакованого вузла чи приладу - 4 особи.
Чисельність адміністраторів системи та програмних інженерів - 3 особи.

3.1. Визначення трудомісткості розробки та опрацювання профілю захищеності

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

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д} = 4+4,1+1,65+4,1+30,9+8,25 = 53 \text{ людино/годин} \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку та реалізацію профілю захищеності – 4л/г;

$t_{в}$ – тривалість вивчення технічного завдання, літературних джерел – 4,1л/г;

$t_{а}$ – тривалість розробки блок – схеми алгоритму – 1,65л/г;

$t_{пр}$ – тривалість реалізації профілю захищеності – 4,1л/г;

$t_{опр}$ – тривалість опрацювання програми на персональному комп’ютері -30,9л/г;

$t_{д}$ – тривалість підготовки технічної документації на програмному засобі – 8,25л/г.

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:

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

де q – очікувана кількість оперантів – 40;

c – коефіцієнт складності програми – 1,5;

p – коефіцієнт корекції програми в процесі її опрацювання – 0,1.

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 дипломником на підставі експертних оцінок за узгодженням із керівником проекту.

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

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

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:

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

Тривалість реалізації профілю захищеності:

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

Тривалість опрацювання програми на персональному комп'ютері:

$$t\,опр = \frac{1{,}5Q}{(4...5)\cdot k} = \frac{1{,}5\cdot 66}{4\cdot 0{,}8} = 30{,}9 \text{ годин} \quad (3.6)$$

Тривалість підготовки технічної документації на програмному засобі:

$$t_д = \frac{Q}{(15...20)\cdot k} + \frac{Q}{(15...20)}\cdot 0{,}75 = 5{,}5+5{,}5\cdot 0{,}75=8{,}25 \text{ годин} \quad (3.7)$$

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, що необхідний для опрацювання програми на персональному комп'ютері *Змч*:

$$К_{ПЗ} = З_{ЗП} + З_{МЧ} = 7579 + 10274{,}1 = 17853{,}1 \text{ грн.} \quad (3.8)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також обов'язкові відрахування (податок на доходи фізичних осіб (ПДФО) - 18% та військовий збір (ВЗ) - 1,5%), визначається за формулою:

$$З_{зп} = t \cdot З_{пр} = 53\text{год} \cdot 143 \text{ грн/год} = 7\,579\text{грн.} \quad (3.9)$$

де t – загальна тривалість створення програмного забезпечення, годин;

Зпр – середньогодинна заробітна плата програміста по Дніпропетровській області з нарахуваннями станом на перше півріччя, грн/годину.

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

$$З_{мч} = t \cdot С_{МЧ} = 53 \cdot 193,85 = 10274,1 грн. \quad (3.10)$$

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:

$$C_{мч} = P \cdot t \cdot C_e + \frac{Ф_{зал} \cdot Н_a}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p} \quad (3.11)$$

$C_{мч} = (0,8 \cdot 53 \cdot 4,43) + (22000 \cdot 0,5/2024) + (3600 \cdot 0,33/2024) = 193,85 грн/год$

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

C_e – тариф на електричну енергію, грн/кВт·година (*4,43 грн. з ПДВ – тариф діє станом на травень 2023 року для малих непобутових споживачів, що приєднані до мережі АТ «ДТЕК»);*

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

$Н_a$ – 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_p – річний фонд робочого часу у 2023 році за 40 – годинного робочого тижня (календарний фонд (365 днів) – вихідні та святкові (112 днів).

У годинах Fp = (днів 365-112=253) днів · 8 годин/день 2024 год/рік).

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.

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

$$С = С_в + С_к + С_{ак} = 13804 + 48178 + 3863 = 65\ 845 грн \quad (3.13)$$

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:

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

Ск = 16380 + 2404,2 + 16500 + 4,43 + 10512 + 2,4 + 2375 = 48 178грн

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 ($С_н$) *(16380)*.

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів програмного забезпечення *(2404,2)*.

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

$$С_з = З_{осн} + З_{дод} = 15000 + 1500 = 16500грн/місяць \quad (3.15)$$

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

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:

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 0,5 \cdot 8760 \cdot 2,4 = 10512 \text{ грн} \quad (3.16)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму цілодобової роботи системи інформаційної безпеки - 365днів·24год. = 8760);

$С_е$ – 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.

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. Основна ставка єдиного соціального внеску (ЄСВ) - 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/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:

$$U = П_п + П_в + V = 5909,1 + 12418,2 + 6432,8 = 24\ 760,1 \text{ грн} \quad (3.17)$$

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:

$$П_п = \frac{\sum З_с * Ч_с}{F} \cdot t_п = (13000 \cdot 4 / 176) \cdot 20 = 5909{,}1 \text{грн} \quad (3.18)$$

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

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

$$П_в = П_{ви} + П_{пв} + П_{зч} = 1477{,}3 + 1534{,}1 + 9406{,}8 = 12418{,}2 \text{ грн} \quad (3.19)$$

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 *(9406,8грн)*.

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 $t_{ви}$:

$$П_{ви} = \frac{\sum З_с * Ч_с}{F} \cdot t_{ви} = (13000 \cdot 4 / 176) \cdot 5 = 1477{,}3 \text{грн} \quad (3.20)$$

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):

$$П_{пв} = \frac{\sum З_о * Ч_о}{F} \cdot t_в = (15000 \cdot 3 / 176) \cdot 6 = 1534{,}1 \text{ грн} \quad (3.21)$$

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:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) = (420000 / 2024) \cdot (20+6+5) = 6432{,}8 \text{ грн} \quad (3.22)$$

де $F_г$ – річний фонд часу роботи організації у 2023 році становить 2024 год.

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

$$B = \sum\sum U*N*I = 24760{,}1 \cdot 1 \cdot 3 = 74\,280{,}3 \text{грн} \quad (3.23)$$

3.5 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C = 74280{,}3 \cdot 2 - 65845 = 82\,715{,}6 \text{грн} \quad (3.24)$$

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 Висновки

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

досліджений стандартний функціональний профіль захищеності на економічну ефективність який впроваджується в інформаційну систему.

На підставі проведених розрахунків можна зробити наступні висновки:

- визначена та детально розрахована трудомісткість реалізації профілю захищеності;
- досліджені всі можливі фінансові витрати на реалізацію профілю захищеності;
- проаналізована величина збиту після проведених атак на систему;
- розрахована ефективність впровадження систем інформаційної безпеки.

Розрахувавши всі критерії можемо зробити висновок про економічну ефективність впровадження запропонованої безпекової системи. Так, як загальний збиток від атаки на вузли/сегменти корпоративної мережі компанії складе 148 560,6грн, а після впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки становить 82 715,6 грн.

ВИСНОВКИ

У кваліфікаційній роботі розв'язано актуальне 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 платіжні термінали, 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;

– обрана та проаналізована система керування базою даних, 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, приведений аналіз технічних об’єктів на предмет виконання стандартного функціонального профілю захищеності інформації. До проаналізованих загроз для оброблюваної інформації на серверному обладнанні рекомендовано застосовати стандартний функціональний профіль захищеності «ЗКЦД.1»;

– прораховані об’єкти на підприємстві: розрахована трудомісткість реалізації профілю захищеності, розраховані можливі фінансові затрати на

реалізацію та впровадження профілю захищеності. Без реаліхації профілю захищеності загальний збиток від атак складатиме 148 560,6 грн, тоді як з впровадженням профілю захищеності загальний ефект складатиме 82 715,6 грн, тобто реалізація профілю захищеності є економічно доцільним.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 2.7-011-2012. Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки, 2012.

2. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, 1999.

3. НД ТЗІ 2.5-005-1999. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу, 1999.

4. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, 1999.

5. Внутрішньобанківські платіжні системи. URL:https://bank.gov.ua/payments/paymentsystems?page=2&perPage=5&search=&system%5BВнутрішньобанківська%20платіжна%20система%5D=6&country=&indication=https://bank.gov.ua/payments/paymentsystems?page=2&perPage=5&search=&system%5BВнутрішньобанківська%20платіжна%20система%5D=6&country=&indication.

6. Рівень інформаційної безпеки та кіберзахист у сфері переказу коштів планується підвищити. URL:https://bank.gov.ua/ua/news/all/riveninformatsiynoyi-bezpeki-ta-kiberzahist-u-sferi-perekazu-koshtiv-planuyetsyapidvischiti.

7. Термінальне обладнання. URL:http://dengi.polnaya.info/platezhnye_sistemy/terminalnoe_oborudovanie/; URL:https://www.iterator.com.ua/ru/pos-systemy/pos-systems/titan-s-360-pos-terminal.html.

8. Операційні системи терміналів. URL:https://www.interator.com.ua/ua/poleznye-materialy/202-shcho-take-sistema-pos-i-yak-vibrati-sistemu-pos.

9. Платіжна система. URL:http://dengi.polnaya.info/platezhnye_sistemy /funkcii_platezhnyh_sistem/.

10. Протокол надання доступу до віддаленого комп'ютера URL:https://techukraine.net/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%_D0%B5-rdp-%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB-%D0%B2%D1%96%D0%B4%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%BE%D0%B3%D0%BE-D1%80%D0%BE%D0%B1%D0%BE%D1%87%D0%BE

11. Класифікація інформаційних систем. URL:https://ua.kursoviks.com.ua/metodychki/275-lektsiya-priznachennya-kharakteristika-osnovni-etapi-rozvitku-ta-klasifikatsiya-informatsiynikh-sistem#:~:text=%D0%97%D0%B0%D0%BB%D0%B5%D0%B6%D0%BD%D0%BE%20%D0%B2%D1%96%D0%B4%20%D0%BC%D0%B5%D1%82%D0%B8%20%D1%84%D1%83%D0%BD%D0%BA%D1%86%D1%96%D0%BE%D0%BD%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D1%82%D0%B0,%D1%82%D0%B0%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8%20%D0%BF%D1%96%D0%B4%D1%82%D1%80%D0%B8%D0%BC%D0%BA%D0%B8%20%D0%BF%D1%80%D0%B8%D0%B9%D0%BD%D1%8F%D1%82%D1%82%D1%8F%20%D1%80%D1%96%D1%88%D0%B5%D0%BD%D1%8C.

12. Інформаційний об'єкт: визначення, види та особливості. URL:https://yrok.pp.ua/serednya-osvta/211-nformacyniy-obyekt-viznachennya-vidi-ta-osoblivost.html.

13. Термінальні проломи: злом мереж платіжних терміналів. URL:https://www.pcidssguide.com/how-to-protect-your-pos-sistem-from-pos-malware/.

14. Оптичний канал витоку інформації. URL:http://213.182.177.142/kafedr/22.Special'nih_informacionnih_tehnologii/teor_inf_bez_i_met_sashit_inf3/lec/%D0%9B15.htm.

15. Методи і засоби пошуку електронних пристроїв перехоплення інформації. URL:http://www.analitika.info/poisk.php?page=1&full=block_article35;

16. GSM/GPRS-модулі. URL:https://diylab,com.ua/ua/p107642952-gsm-gprs-mobil,html/

17. SQL ін'єкції/ URL:https://www,pcidssguide,com/how-to-protect-your-system-from-pos-mslware.

18. Основні види кібератак на бізнес в Україні. URL:https://glavcom.ua/country/society/osnovni-vidi-kiberatak-na-biznes-v-ukrajini-eksperti-rozpovili-yak-ne-potrapiti-u-pastku--820594.html.

19. Людський фактор в забезпеченні безпеки інформаційної. URL:http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/03a9dfb8b576994dc3256d5700403104.

20. Vpn з'єднання. URL:https://habrahabr.ru/post/164301/.

21. Класифікація загроз в інформаційній безпеці. URL:http://pidru4niki.com/12631113/ekonomika/ponyattya_klasifikatsiya_zagroz_bezpeki_informatsiyi.

22. Модель порушника. Мета та принципи розробки URL:http://www.rusnauka.com/11_EISN_2010/Informatica/63866.doc.htm.

23. Адабашев Т. К. До питання класифікації платіжних систем, що функціонують в Україні. Вісник Національного університету «Юридична академія України імені Ярослава Мудрого. 2013. № 2. С. 142–152.

24. Міщенко С. В. Вдосконалення системи безготівкових роздрібних платежів. Вісник Київського національного університету імені Тараса Шевченка. 2014. № 5. С. 22–28.

25. Гребенніков В. В. Лекції / Вадим Вікторович Гребенніков // Комплексні системи захисту інформації. Проектування, впровадження, супровід / Вадим Вікторович Гребенніков., 2013. – С. 28–43. URL:https://dspace.uzhnu.edu.ua/jspui/handle/lib/10070.

26. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський: [навч. посібник]. – К.: КНТ, 2006. – 280с.

27. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019. – 16 с.

28. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека / Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	Розділ 1. Стан питання. Постановка задачі	38	
6	А4	Розділ 2. Спеціальна частина	22	
7	А4	Розділ 3. Економічна частина	11	
8	А4	Висновок	2	
9	А4	Перелік посилань	3	
10	А4	Додаток А. Відомість матеріалів дипломної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгук керівника економічного розділу	1	
13	А4	Додаток Г. Відгук керівника дипломної роботи	1	
14	А4	ДОДАТОК Д. Вразливості платіжних та інформаційних терміналів	2	
15	А4	ДОДАТОК Е. Вразливості програмного забезпечення серверного обладнання	2	

ДОДАТОК Б. Перелік документів на оптичному носії

- Пояснювальна записка Перепадя І.Я. 125-19-2.docx
- Презентація Перепадя І.Я. 125-19-2.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник економічного розділу к.е.н., доц. Пілова Д.П.

Дата: _____ Підпис: _____

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

ВІДГУК
на кваліфікаційну роботу студента групи 125-19-2
Перепаді Іллі Ярославовича
на тему: «Обґрунтування засобів підвищення рівня інформаційної безпеки платіжного термінального обладнання»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 90сторінках.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека».

Мета кваліфікаційної роботи є актуальною, адже спрямована на удосконалення існуючих систем інформаційної безпеки термінального обладнання.

При виконанні роботи продемонстровано задовільний рівень теоретичних знань та практичних навичок. Виконано аналіз загроз та вразливостей термінального обладнання та інформації, яка оброблюється на серверному обладнанні, на основі цих відомостей розроблено модель удосконалення існуючих систем.

Практична цінність роботи полягає в розробці критеріїв щодо реалізації ефективного профілю захищеності платіжного термінального обладнання.

До окремих недоліків слід віднести нечіткості в формулюванні окремих понять та незначні невідповідності вимогам оформлення.

Автор Перепадя І.Я. виявив здатність самостійно вирішувати поставлені задачі та заслуговує на присвоєння кваліфікації бакалавра 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 «_____».

Керівник кваліфікаційної роботи,

д.т.н., проф. **В.І. Корнієнко**