Міністерство освіти і науки України

Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступенюмагістра

студента *Масалова Ігора Сергійовича*
академічної групи *125м-21-1*
спеціальності *125 Кібербезпека*
спеціалізації[1]
за освітньо-професійною програмою *Кібербезпека*
на тему *Підвищення рівня захищеності програмного забезпечення платіжного термінального обладнання*

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

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра

студенту *Масалову Ігору Сергійовичу* **академічної групи** *125м-21-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему *Підвищення рівня захищеності програмного забезпечення термінального обладнання.*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.2022№ 12200-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналізування термінального обладнання	20.10.2022
Розділ 2	Оцінювання загроз та вразливостей для інформації, яка оброблюється на серверному обладнанні, ідентифікація вразливостей програмного забезпечення платіжного термінального обладнання.	16.11.2022
Розділ 3	Розрахунок економічної доцільності впровадження запропонованих поліпшень системи безпеки.	05.12.2022

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

Дата видачі: 05.09.2022р.

Дата подання до екзаменаційної комісії:12.12.2022р.

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

РЕФЕРАТ

Пояснювальна записка: 77 с.,3 рис.,6 табл., 4 додатка, 12 джерела.

Об’єкт дослідження: програмне забезпечення термінального обладнання.

Предмет дослідження: ідентифікація вразливостей програмного забезпечення термінального обладнання.

Мета кваліфікаційної роботи: проведення ідентифікації вразливостей платіжного термінального обладнання.

Методи дослідження: системний підхід, методи порівняння.

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

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

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

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

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

ЗАГРОЗИПЛАТІЖНОГОТЕРМІНАЛЬНОГООБЛАДНАННЯ,ВРАЗЛИВОСТІПЛАТІЖНОГОТЕРМІНАЛЬНОГООБЛАДНАННЯ,ТЕРМІНАЛЬНЕОБЛАДНАННЯ.

ABSTRACT

Explanatorynote: 77 p., 3figures, 6 tables, 4 annexes, 12 sources.

Objectofresearch: terminalequipmentsoftware.

Subjectofresearch: identificationofvulnerabilitiesofterminalequipmentsoftware.

Thepurposeofthequalificationwork: identificationofvulnerabilitiesofpaymentterminalequipment.

Researchmethods: systemapproach, comparisonmethods.

Thefirstsectionconsidered: equipmentofpaymentterminals, databases; vulnerabilitiesofterminalequipment, vulnerabilitiesofinformationprocessedonserverequipment;

Thesecondpartwillanalyze: operatingsystemsonterminalequipment; terminalequipmentforpossiblethreatsandthreatanalysisforprocessinginformationonserverequipment; proposed: optionstoimprovesecurity; built: modeloftheviolator;

Theeconomicsectiondefines: theeffectivenessoftheimplementationofsecurityimprovementsonterminalequipment.

Allresearchresultsinthequalificationworkcanbeusedtofurtherimprovesecuritysystems.

Thepracticalvalueoftheworkisasfollows: identificationofvulnerabilitiesofpaymentterminalequipmentanddevelopmentofrecommendationsfortheimplementationof a setofmeansofprotectionintheinformationsystem.

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

СПИСОКУМОВНИХСКОРОЧЕНЬ

ATM - AutomatedTellerMachine;

DDL – DataDefinitionLanguage;

GPRS – GeneralPacketRadioService; Загальний сервіс пакетної радіопередачі;

GSM – GlobalSystemforMobileCommunications – глобальна система мобільного зв'язку;

IDS – IntrusionDetectionSystem; Система виявлення атак (вторгнень);

POS-термінал – PointOfSale;

SIEM – Securityinformationandeventmanagement;

SSL – SecureSocketsLayer – рівень захищених сокетів;

TDE – TransparentDataEncryption;

TFT – Thinfilmtransistor – тонкоплівковий транзистор;

VNC – VirtualNetworkComputing;

XML-RPC – ExtensibleMarkupLanguageRemoteProcedureCall – виклик віддалених процедур;

АС - Автоматизована система;

БД - База даних;

ЕОМ - Електронно-обчислювальна машина;

ОС – Операційна система;

ПЗ – Програмне забезпечення;

СУБД - Система управління базами даних

ЗМІСТ

ВСТУП

В сучасному світі термінальне обладнання грає суттєву роль, воно об’єднує купу різноманітних рішень та технологій, що забезпечує комфортне та зручне отримання послуг для користувачів.

Наразі інфраструктура термінального обладнання розвивається значно швидше ніж засоби її захисту, це дає великі можливості для діяльності зловмисників. З кожним днем використання термінального обладнання дедалі збільшується, люди вносять свої персональні данні та данні своїх банківських карт, саме тому безпека такого обладнання є важливим аспектом для надання якісних послуг. Саме тому доцільно зробити аналіз термінального обладнання та виявити його вразливості.

Термінальний обладнання – це набір різноманітних послуг, які безпосередньо пов'язані з користувачем. Мета термінального обладнання: підвищити точність операцій, зняти з людини низку однотипних робіт та підвищити конверсію.

Щоб забезпечити надійний захист термінального обладнання потрібно проаналізувати його на можливі вразливості та загрози. Якщо не модернізувати та не підвищувати рівень захисту термінального обладнання, то дедалі частіше будуть виникати випадки з крадіжкою персональних даних користувачів, а компанії власниці будуть нести фінансові та репутаційні збитки.

Актуальність теми кваліфікаційної роботи підвищення рівня захищеності програмного забезпечення платіжного термінального обладнання визначається:

– збільшенням вразливостей термінального обладнання;

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

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

– проаналізувати види термінального обладнання;

– дослідити програмне забезпечення термінального обладнання з точки зору безпеки;

– дослідити алгоритм передачі даних між клієнтом та серверним обладнанням;

– проаналізувати загрози для оброблювальної інформації на серверному обладнанні;

– побудувати модель порушника;

– розробити рекомендації щодо поліпшення захисту термінального обладнання.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз термінального обладнання

Термінальне обладнання — це сукупність пристроїв, механізмів, приладів, інструментів тощо, необхідних для якої-небудь діяльності. Використовуються з певною метою, наприклад, реалізації технологічних процесів. Таке обладнання може бути як джерелом інформації так і одержувачем, або тим і іншим одночасно. Вони передають або приймають дані, за допомогою використання кінцевого обладнання лінії зв'язку і каналу зв'язку. Термінальне обладнання буває:

- платіжні термінали;
- інформаційні;

Платіжний термінал — це електронний пристрій, призначений для ініціювання переказу з рахунка, у тому числі видачі готівки, отримання довідкової інформації та друку документа за операцією з використанням спеціального платіжного засобу. Для платіжного терміналу характерний високий рівень автономності його роботи. Контроль роботи платіжного терміналу проводиться через мережу Інтернет.

Термінал складається з:

- 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.

Для збільшення послуг, що надаються платіжними терміналами в деяких з них вбудовуються:

- пристрій для роботи з пластиковими банківськими картами;
- сканер штрих-кодів;

– кардрідер;
– пін–пад клавіатури;
– додатковий TFT-монітор.

Алгоритм роботи термінального обладнання зображений на (рис. 1.1).

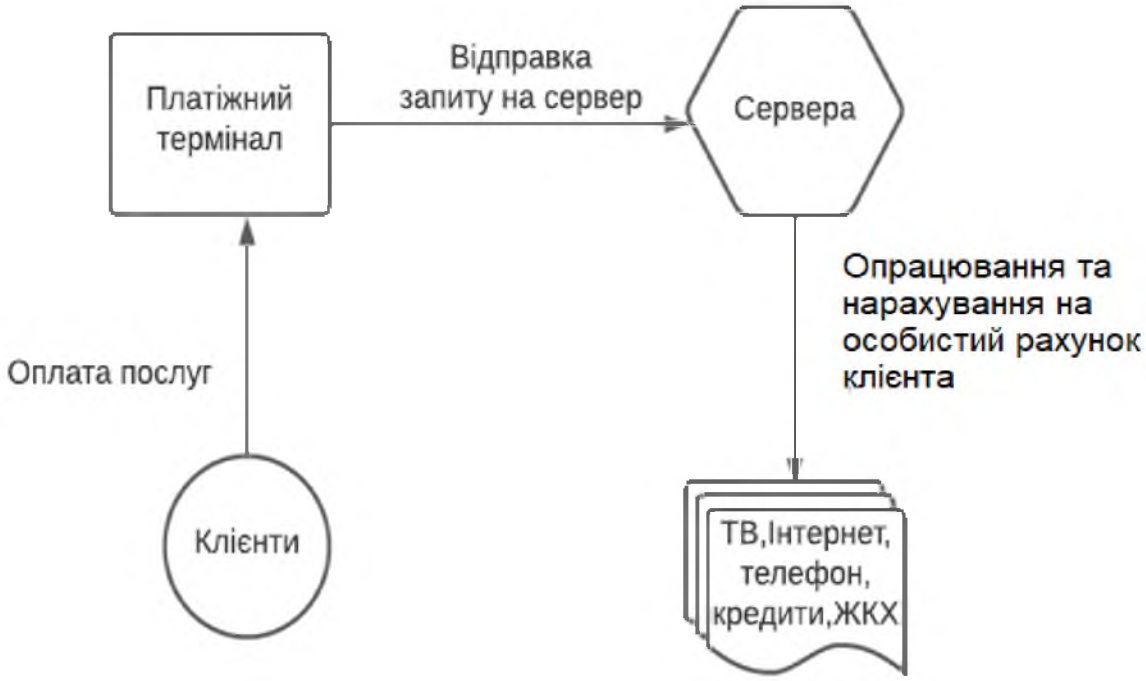

Рисунок 1.1 – Алгоритм роботи термінального обладнання

Користувач виконує пошук послуг, вказує реквізити та інше за допомогою вбудованого екрану, на якому відображається меню. Після чого вже сам термінал перевіряє правильність введеної інформації, перевіряє існування даного рахунку і можливості його поповнення. Користувач вносить бажану суму готівки, купюро приймач розпізнає справжність готівки, їх номінал, і здійснює повернення купюр, які не пройшли перевірку на справжність. Після закінчення внесення готівкових коштів, термінал у відповідь роздруковує і видає користувачеві чек з інформацією цієї транзакції. За допомогою GPRS – модему, термінальне обладнання пересилає інформацію про платіж серверу, який забезпечую обробку цього платежу. Після обробки даних серверне обладнання передає їх на шлюз сервера організації, після чого гроші поступають на рахунок одержувача (рисунок 1.1).

Компанія що володіє термінальним обладнанням зазвичай стягує комісію за надання послуг, у вигляді проценту від суми чи фіксовану суму, яка вказана на дисплеї терміналу.

Розберемо, як влаштовані апарати зсередини та яким чином їм вдається проводити різноманітні платежі :

– Серце терміналу – системний блок, що складається з жорсткого диска, материнської плати та інших комплектуючих. Відповідає за швидкодію та успішне виконання транзакцій;

– Купюроприймач. З зовнішньої сторони – область для прийому купюр. З внутрішньої сторони знаходиться короб, в якому зберігаються купюри. Короб надійно захищений від взлому, доступ до нього мають лише співробітники, що обслуговують термінал;

– Принтер для чеку. Над принтером – область для чекової стрічки;

– Інтернет-модем. Своєрідний мозок, який забезпечує зв'язок платіжного терміналу з сервером. Як проходить платіж всередині терміналу.

Схема розміщення кожного з компонентів платіжного терміналу зображено на рисунку 1.2. Де :

1. Монітор;
2. Модем;
3. Купюроприймач;
4. Термопринтер.

У момент, коли ви здійснюєте платіж, термінал за допомогою інтернет-модему з'єднується з сервером платіжної системи . Інформація передається по захищеним каналам зв'язку. Сервер обробляє інформацію та підтверджує введені дані у постачальника послуг. В результаті відбувається транзакція. Тривалість процесу – декілька секунд.

Рисунок 1.2. — Схема розміщення кожного з компонентів платіжного терміналу.

1.2. Класифікація інформації на серверному обладнанні.

Розглянемо як класифікується інформація на сервері термінального обладнання в таблиці 1.1 надана класифікація інформації на серверному обладнанні.

Таблиця 1.1 — Класифікація інформації на серверному обладнанні.

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

Де рівням конфіденційності інформації відповідають:

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).

Відповідно рівням цілісності інформації відповідають:

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).

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).

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

1.3. Аналіз вразливостей термінального обладнання.

Шкідливе ПЗ для палатіжного термінального обладнання - це шкідливе програмне забезпечення, спеціально написане для крадіжки платіжних даних клієнтів, як-от дані кредитних карток, із роздрібних платіжних систем. Злочинці використовують шкідливе програмне забезпечення палатіжного термінального обладнання для продажу даних замість того, щоб використовувати їх безпосередньо.

Зловмисник може проникнути в бази даних, в яких зберігаються дані, або втрутитися в дані в точці продажу (POS). Хоча фізичні методи можуть використовуватися для крадіжки даних в обох напрямках, ці методи вимагають доступу до торговельного обладнання та часто вимагають дорогого обладнання.

Один із способів - використовувати додатковий зчитувач, прикріплений до картрідера магазину. Другий пристрій зчитує і зберігає дані картки track 2 для швидкої оплати. Дані магнітної смуги доріжки 2 включають номер основної картки та код безпеки, а також іншу інформацію, наприклад, про те, які типи платежів дозволені. Не ступаючи на територію, шкідливе ПЗ для POS-терміналів є набагато простішим і менш небезпечним способом отримання цієї інформації.

Тип скребка пам'яті, відомий як шкідливе ПЗ POS, шукає дані в правильному форматі для даних кредитної картки доріжки 2. Ці дані доступні в пам'яті тільки протягом короткого часу в незашифрованому вигляді. Однак очищення пам'яті призначене для миттєвого збору даних при їх виявленні

шкідливою програмою. Інформація про кредитну картку потім відправляється на віддалені комп'ютери зловмисника, а потім продається на підпільних сайтах.

Шкідливе ПЗ для POS-терміналів призначене для крадіжки даних платіжних карток з POS-терміналів і систем. Він широко використовується кіберзлочинцями, які хочуть перепродати вкрадені дані клієнтів з роздрібних магазинів.

Дані платіжної картки шифруються end-to-end і розшифровуються тільки в оперативній пам'яті (ОЗП) пристрою в процесі оплати. Шкідлива атака POS проникає в POS-термінали через скомпрометовані або погано захищені системи, шукаючи в оперативній пам'яті дані платіжної картки, які потім надсилають зловмиснику в незашифрованому вигляді.

Атаки на POS-системи зазвичай багатоетапні. Щоб атакувати комп'ютерну мережу жертви, зловмисник повинен спочатку отримати до неї доступ. Зазвичай вони отримують не прямий доступ до CDE, а до асоційованої мережі. Потім вони повинні пройти через мережу і в кінцевому підсумку отримати доступ до POS-систем.

Потім їм необхідно встановити шкідливе ПЗ для крадіжки даних зі скомпрометованих систем. Оскільки малоймовірно, що система POS матиме доступ до зовнішньої мережі, вкрадені дані потім зазвичай надсилають на внутрішній сервер підготовки і зрештою видаляють із мережі роздрібного продавця зловмиснику.

IT-фахівці часто називають шкідливе ПЗ для POS-терміналів сканером процесів, тому що воно сканує активні транзакції на пристроях і збирає все, що може бути корисним, зазвичай дані кредитних карт.

Шкідливе ПЗ платіжного термінального обладнання шукає дані, що відповідають закодованому формату Fragment 1 або Fragment 2 на магнітній смузі кредитної картки. Ці дані включають необов'язкові дані, зокрема ім'я власника картки, номер основної картки, дозволені типи платежів і PIN-коди.

Незашифровані дані можна використовувати тільки протягом короткого часу, коли вони потрапляють у базу даних на пристрої. Шкідливе ПЗ для POS призначене для вилучення даних до того, як вони будуть миттєво зашифровані.

Отримавши дані, шкідливе ПЗ відправляє їх на інший сервер, де кіберзлочинець може впорядкувати дані та знайти номери кредитних карток. Використовуючи дані платіжної картки, кіберзлочинці можуть продавати інформацію в чорному Інтернеті або здійснювати шахрайські покупки з використанням отриманої інформації картки.

1.3.1 Типи шкідливих програм для платіжного термінального обладнання.

BlackPOS призначений для комп'ютерів під управлінням Windows, які є частиною POS-системи. У BlackPOS немає функції вилучення даних в автономному режимі, а вкрадені дані завантажуються онлайн на віддалені сервери. Це дає хакерам більше гнучкості. BlackPOS використовували під час масового злому Target POS у 2013 році.

Dexter - ще одна шкідлива програма POS для Windows з кількома активними змінними. Як і BlackPOS, він аналізує дампи пам'яті транзакцій, пов'язаних із певним програмним забезпеченням POS, яке шукає дані Track 1 і Track 2. Дані Track 1, ім'я власника картки та номери рахунків; Трек 2 - це номер кредитної картки та термін дії.

TreasureHunt був створений виключно групою хакерів, які продавали вкрадені дані кредитних карт. Шкідливе ПЗ TreasureHunt використовує вкрадені або ненадійні облікові дані для встановлення на пристрій і націлене на роздрібних продавців, які все ще використовують застарілі системи прокрутки. TreasureHunt витягує дані кредитної картки з пам'яті пристрою і надсилає їх на сервер управління і контролю.

ChewBaccaTrojan має просту реєстрацію ключів і очищення пам'яті для пошуку звичайних виразів даних магнітної смуги картки. Якщо номер картки знайдено, він видаляється сервером і реєструється.

Шкідливе ПЗ Backoff POS має такі можливості, як очищення пам'яті для фрагментованих даних, реєстрація натискань клавіш, зв'язок команд, управління (C2) і впровадження шкідливого ПЗ в explorer.exe. Шкідливе ПЗ, впроваджене в Explorer.exe, відповідає за збереження в разі збою або примусової зупинки

шкідливого виконуваного файлу. Шкідливе ПЗ відповідає за захоплення пам'яті процесів, запущених на комп'ютері-жертві, і пошук даних відстеження.

Kaptoxa призначений для розміщення в POS-терміналах і для моніторингу інформації, оброблюваної програмами платіжних додатків. У більшості випадків дані платіжної картки зберігаються в незашифрованому вигляді протягом короткого часу в оперативній пам'яті в процесі авторизації платежу. Це точка, в якій Kaptoxa може отримати доступ і скопіювати дані платіжних карток, включно з номерами кредитних і дебетових карток, особистими ідентифікаційними номерами (PIN), датами закінчення терміну дії, адресами електронної пошти, адресами споживачів і номерами телефонів. Після того, як дані скопійовані, вони якийсь час впливають на POS-термінали, поки не будуть зібрані в центральному місці. Потім шкідлива програма Kaptoxa кожні сім годин відправляє інформацію за протоколом TCP на внутрішній хост у скомпрометованій мережі через загальний ресурс NetBIOS. Зловмисник використовує серію віддалених FTP-передач для вилучення даних, вкрадених із цього хоста.

NitlovePOS збирає дані першої та другої платіжних карт, скануючи запущені процеси скомпрометованої машини. Потім він використовує SSL для надсилання вкрадених даних на веб-сервер. Шкідливе ПЗ NitlovePOS також використовує електронні листи зі спамом зі шкідливими вкладеннями, щоб змусити користувачів завантажувати шкідливе ПЗ. Коли шкідливе ПЗ потрапляє на пристрій, воно проявляється не відразу, оскільки копіює себе на диск і перезавантажується, коли хтось намагається його видалити.

PoSeidon встановлює кейлоггер на скомпрометований пристрій і сканує пам'ять пристрою на наявність номерів кредитних карт. Натискання клавіш, які можуть містити паролі та номери кредитних карток, потім кодуються і відправляються на інший сервер. Шкідливе ПЗ Poseidon може як і раніше працювати в пам'яті, якщо користувач виходить із системи, і може залишатися прихованим за допомогою хмарних технологій.

MalumPOS маскує себе як драйвер дисплея на зараженому пристрої. Потім він відстежує транзакції і шукає в пам'яті зараженого пристрою платіжну

інформацію. Шкідливе ПЗ MalumPOS зазвичай націлене на системи, що працюють на Oracle MICROS і доступ до яких здійснюється через Internet Explorer.

1.3.2 Людський фактор.

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

Все платіжне термінальне обладнання знаходиться у більш менш публічних місцях. Що вже робить це обладнання небезпечним для користувачів. В реалізації всіх рішень та застосування їх на практиці беруть участь співробітники компанії якій належить термінальне обладнання, а вони можуть помилятися. Інформаційні технології все більше проникають в різні сфери нашого життя і тому кіберзлочинність набирає обертів з великою швидкістю.

Порушення що, відхиляються 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. Але можна виділити наступні 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 функціональнихзавдань.

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 у роботі програми, ініційовані невмілими діями людини, неправильні команди можуть призводити до повного припинення функціонування системи.

Побудувати надійну систему безпеки в сучасному комп'ютерному світі дуже непросто. Існує велика кількість слабких місць в системі; процес знаходження нових «дірок» і їх «латання» – це безперервна робота. Для вирішення поточних проблем на зміну застарілим технологіям приходять нові, в яких в свою чергу виявляються свої недоліки. Винаходяться нові прийоми для обходу здавалося б досконалою захисту. Дві протиборчі сторони – комп'ютерні злочинці і фахівці з захисту – знаходяться в безперервній боротьбі. Треба зазначити, що ця сутичка протікає зі змінним успіхом. При цьому поведінка рядових користувачів може нахилити чашу терезів на ту чи іншу сторону. Людина з її непередбачуваною поведінкою може звести нанівець величезні зусилля, витрачені на зведення надійної системи безпеки.

1.4 Аналіз систем керування базами даних на серверному обладнанні.

Система управління базами даних, скор. СУБД - сукупність програмних і лінгвістичних засобів загального або спеціального призначення, що забезпечують управління створенням і використанням баз даних.

Основні характеристики СУБД:

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

Можливості СУБД:

– Дозволяється створювати БД (здійснюється за допомогою мови визначення даних DDL (DataDefinitionLanguage))

– Дозволяється додавання, оновлення, видалення та читання інформації з БД (за допомогою мови маніпулювання даними DML, яку часто називають мовою запитів)

– Можна надавати контрольований доступ до БД за допомогою:

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

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

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

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

Таблиця 1.2 Переваги та недоліки систем управління базами даних

СУБД	Переваги	Недоліки
IBM DB2 UniversalDatabase	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
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 операційної платформи (Win32); менші можливості в порівнянні з Oracle і DB2.

В таблиці 1.2 розглянуті основні переваги та недоліки СУБД. Для роботи системи буде використовуватися.

Microsoft SQL Server - популярна система управління базами даних (СУБД), розроблена компанією Майкрософт. Доступна в декількох редакціях. Може працювати на ПК, ноутбуці, сервері, на віртуальній машині або в хмарі. Microsoft SQL Server має наступні переваги:

– Масштабування системи. Взаємодіяти з нею можна як на простих ноутбуках, так і на ПК з потужним процесором, який здатний обробляти великий обсяг запитів.

– Розмір сторінок - до 8 Кб. Дані витягуються швидко, а складну інформацію зручніше зберігати. Система обробляє транзакції в інтерактивному режимі, є динамічне блокування.

– Автоматизація рутинних адміністративних завдань. Наприклад, управління блокуваннями і пам'яттю, редагування розмірів файлів. У програмі продумані налаштування, можна створювати профілі користувачів.

– Зручний пошук. Його можна здійснювати за фразами, словами, текстом або створювати ключові індекси.

– Підтримка роботи з іншими рішеннями Майкрософт, зокрема з Excel, Access.

Також у програмі передбачена синхронізація, є реплікації через інтернет, служби перетворення інформації та повноцінний web-асистент для форматування сторінок. Додатково в неї інтегрований сервіс інтерактивного аналізу (можна ухвалювати рішення, створювати корпоративні звіти).

У таблиці 1.3 подано зумовлені ролі бази даних Microsoft SQL Server та їхні можливості. Ці ролі існують у всіх базах даних. За винятком відкритої ролі бази даних дозволи, призначені зумовленим ролям бази даних, змінювати не можна.

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 DataProtection API (DPAPI) – це криптографічний інтерфейс, що забезпечує захист даних шляхом їх шифрування;

– симетричні або асиметричні ключі поза SQL Server;

– прозоре шифрування даних TransparentDataEncryption (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.

Таблиця 1.3 – Ролі рівня бази даних та їх опис

Ім'я зумовленої ролі бази даних	Опис
db_owner	Члени зумовленої ролі бази даних db_owner можуть виконувати всі дії з налаштування та обслуговування бази даних, а також видаляти (drop) базу даних у SQL Server. (У База даних SQL і AzureSynapse деякі операції з обслуговування вимагають наявності дозволів на рівні сервера і не можуть бути виконані членами db_owner).
db_securityadmin	Елементи зумовленої ролі бази даних db_securityadmin можуть змінювати членство в ролі (тільки для ролей, що налаштовуються) і керувати дозволами. Елементи цієї ролі потенційно можуть підвищувати свої права доступу, тому необхідно відстежувати їхні дії.
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.

Продовження таблиці 1.3.

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.

Кожен користувач бази даних є членом ролі бази даних public . Якщо для користувача не були надані або заборонені конкретні дозволи на об'єкт, що захищається, такий користувач успадковує дозволи ролі public на цей об'єкт. Користувачів бази даних не можна видалити з ролі public.

1.5 Дослідження найбільш вагомих проблем в термінальному обладнанні

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

– Відсутність програмних об’єктів на пристрої;

– Не правильно розподілені користувачі в системі стосовно їх прав доступу;

– Відсутня конфіденційність при обміні інформації.

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

ОС Windows має широке розповсюдження не тільки на ринку персональних комп'ютерів, але і для платіжних терміналів, інформаційних табло та банкоматів, тому на цих пристроях можуть функціонувати будь-які вірусні програми створені для атаки на ОС Windows. Саме тому треба розуміти специфіку створення шкідливого коду під такі системи: розробити вірус для них здатна тільки технічно

грамотна людина, яка розуміє пристрій апаратури і має безпосередній доступ до обладнання для проведення аналізу та тестування вірусу.

Наслідки зараження платіжного термінального обладнання має катастрофічну загрозу не тільки для користувачів термінального обладнання так і для компанії, яка володіє термінальним обладнанням. Заражене термінальне обладнання буде передавати усю інформацію про кредитні карти зловмисникам.

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

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

1.6 Висновок

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

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

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

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

– досліджені системи керування базами даних на серверному обладнанні;

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

В спеціальному розділі кваліфікаційної роботи необхідно виконати наступне:

– проаналізувати загрози для оброблюваної інформації на серверному обладнанні;

– проаналізувати операційні системи на термінальному обладнанні;

– розробити модель порушника;

– проаналізувати атаки на термінальне обладнання;

– виявити вразливості програмного забезпечення платіжного термінального обладнання;

розробити рекомендації щодо поліпшення захисту інформації на термінальному обладнанні.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз операційних систем на термінальному обладнанні

Існує велика кількість операційних систем для платіжного термінального обладнання кількість видів ОС, в кожній з яких різний рівень захисту, система управління, підтримка додатковий послуг. Нижче розглянемо проаналізуємо ці ОС:

1. Microsoft Windows Embedded Існує 4 основні категорії продуктів для створення широкого спектра пристроїв, починаючи від простих контролерів реального часу і закінчуючи ПЗЗ системами, такими як кіоск самообслуговування або касовий апарат. Windows Embedded доступний через спеціалізованих дистриб'юторів Майкрософт і має постачатися OEM-виробниками у складі готової вбудованої системи, попередньо встановленої на апаратну платформу.

2. Windows EmbeddedPOSReady 2009 — це гнучка операційна система, призначена для безперешкодного з'єднання рішень для точок обслуговування з периферійними пристроями, серверами та службами. POSReady 2009 поєднує в собі потужність і зручність Windows XP Professional з меншим розміром і специфічними функціями для комп'ютерів в точках обслуговування (POS). POSReady є значним оновленням Windows EmbeddedforPointofService, яке включає в себе нову назву продукту, нові технології та поліпшення основних функцій. Завдяки вбудованим мережевим можливостям і підтримці стандартів plug-and-play, Windows EmbeddedPOSReady 2009 спрощує підключення POS-пристроїв до периферійних пристроїв, серверів і служб. Крім того, ви можете допомогти знизити витрати і загрози безпеки, налаштувавши POSReady 2009 на використання тільки компонентів, необхідних для вашого POS-рішення. POSReady 2009 можна керувати за допомогою того ж програмного забезпечення, яке ви використовуєте для управління вашими настільними системами - з усією надійністю і постійним обслуговуванням і оновленнями системи, які ви очікуєте від платформи Windows. Ви також отримаєте вигоду від спеціалізованої спільноти

провідних галузевих партнерів та ресурсів, доступних для підтримки на кожному етапі циклу розробки. Ознайомча версія Windows EmbeddedPOSReady 2009 включає повну функціональність англійської версії. Після встановлення ознайомлювальної версії у вас буде 120 днів для ознайомлення з функціями POSReady 2009. Щоб продовжити використання продукту після закінчення 120 днів, необхідно придбати повну ліцензію і ключ продукту, повторно запустити установку, а потім слідувати інструкціям по установці повної версії.

3. Windows Embedded 8 Standard — це продовження лінійки Windows Embedded Standard, компонентизована операційна система на ядрі Windows 8, що підтримує архітектури x86 і x64 і призначена для застосування в пристроях, які не використовують абсолютно всіх можливостей операційної системи одноразово. Для розробки образу операційної системи під конкретний пристрій потрібна наявність і використання відповідного інструментарію; Основне призначення – робота в термінальній сесії з протоколу RDP та з серверами віртуалізації VMware та Citrix. Основне призначення – робота в термінальній сесії з протоколу RDP та з серверами віртуалізації VMware та Citrix.

Інтеграція із існуючими корпоративними IT-системами.

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

Розширені функції інтерфейсу користувача та мультимедіа.

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

Вбудовані засоби керування енергоспоживанням.

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

Підтримувані протоколи:

– RDP 8.1, включаючи підтримку RemoteFX

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

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

– Вбудований інтернет-браузер (Internet Explorer 11.0)

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

У базовий образ також включені наступні компоненти налаштування системи:

– русифікований інтерфейс;

– настроювання дати та часу;

– настроювання локалізації;

– налаштування екрана;

– налаштування робочого столу;

– налаштування мережевих з'єднань;

– встановлення та налаштування принтерів;

– встановлення та налаштування сканерів;

– налаштування віддаленого керування (віддалений доступ до робочого столу по RDP);

– налаштування фільтра захисту від запису (EnchancedWriteFilter);

– керування обліковими записами користувачів;

– Налаштування системи захищено паролем.

Додаткові можливості, які можна підключити у WE8S:

– Rutoken, eToken, SmartCard тощо;

– можливість встановлення клієнта VipNet (підготовлено спеціальний образ);

– додаткових пристроїв (за наявності драйверів для Windows 8);

– мультимедійні функції;

додаткового ПЗ за погодженням із замовником, який не порушує ліцензійну угоду Microsoft.

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

5. ANDROID TERMINAL EMULATOR — це програма, яка емулює термінал комп'ютера всередині деякої іншої архітектури виведення даних на екран. Незважаючи на глибоку синонімічність з оболонкою командного рядка або текстовим терміналом, термін термінал охоплює всі віддалені термінали, включно з графічними інтерфейсами. Емулятор термінала у віконному інтерфейсі користувача часто називається вікном термінала.По суті, термінал виступає як інтерфейс, що надає користувачеві можливість взаємодіяти з локальною або віддаленою операційною системою аналогічно тому, як це відбувається під час використання терміналу.

Проаналізуємо функції, які задані в таблиці 2.1,VirtualNetworkComputing, (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. RemoteDesktopProtocol (RDP), протокол віддаленого робочого стола — протокол прикладного рівня, що використовується для забезпечення віддаленої роботи користувача із сервером, на котрому запущений сервіс термінальних з'єднань.

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

Таблиця 2.1 – Функції ОС для терміналів

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

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

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

Розглянемо інформаційні термінали.

Інформаційний термінал – автоматизований програмно – апаратний комплекс, призначений для надання довідкової інформації. Він призначений для надання користувачу різної інформації без залучення обслуговуючого персоналу. Інформаційні кіоски збирають на базі персонального комп'ютера, оснащеного сенсорним монітором і встановленого в ергономічний сталевий корпус. Додатково на інфо – кіоск може встановлюватися купюро приймач, роз'їм USB, фіскальний реєстратор, аудіо система, додатковий рекламний монітор, сканер штрих – кодів, RFID – приймач, NFC та інше обладнання.

2.2 Програмні проблеми в термінальному обладнанні

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

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

саме є пріоритетом передачі – голосовий трафік або передача даних – обирається оператором зв'язку.

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

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

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

Суть цієї атаки полягає у злому бази даних зі зловмисною метою. Для того, щоб виконати тестування безпеки, спочатку потрібно знайти вразливі частини системи, а потім надіслати через них шкідливий код SQL до бази даних. Якщо ця атака можлива для системи, тоді буде надіслано відповідний зловмисний код SQL і в базі даних можуть бути здійснені шкідливі дії.

Використання класичної SQL – ін’єкції, яка привела до зміни ідентифікатора користувача та пароля. Спочатку зловмисник використовує перехоплювач, щоб захопити дійсний токен сеансу з ім'ям "ID сеансу", потім він

використовує справжній токен для отримання несанкціонованого доступу до веб-сервера.

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

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

Також можна увійти до деяких портів за допомогою протоколу Telnet, але сервіси такого роду парацюють за технологією XML –RPC, що означає що порт може тільки приймати і відправляти POST-запити.

Telnet (англ. TELetypeNETwork) — мережевий протокол для реалізації текстового термінального інтерфейсу через мережу (у сучасній формі - за допомогою транспорту TCP). Назву "telnet" мають також деякі утиліти, що реалізують клієнтську частину протоколу. Сучасний стандарт протоколу описано в RFC 854. Виконує функції протоколу прикладного рівня моделі OSI. Протокол telnet використовувався для віддаленого адміністрування різними мережевими пристроями і програмними серверами, але поступився ssh через безпеку. Проте може бути єдиною можливістю взаємодіяти через cli з embeddedsystems, наприклад, маршрутизаторами, оскільки на них відсутній ssh.

Скіммер є самим популярни шкідливим програмним забезпеченням. Скіммер - мініатюрний зчитувальний переносний пристрій, який може кріпитися до банкомату. Такі пристосування допомагають шахраям красти дані банківських карток: реквізити, ПІН-код тощо, інакше кажучи - всю інформацію, записану на магнітній смузі. Після запуску шкідлива програма дізнається про

тип файлової системи банкомату. У разі використання FAT32 вона копіює в папку System32 динамічну бібліотеку netmgr.dll. Якщо ж застосовується NTFS, то Skimer зберігає netmgr.dll в альтернативному потоці даних файлу SpiService.exe – компоненті банкоматівDiebold, який реалізує XFS, стандартну клієнт-серверну архітектуру для фінансових програм під Windows.

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

Шкідливою програмою можна керувати за допомогою спеціальних карток з магнітною смугою, на другій доріжці якої записані інструкції для Skimer. Зазвичай Skimer збирає дані банківських карток. За командою зловмисника він може роздрукувати накопичену інформацію або видати йому готівку. Крім того, у програмі передбачені команди для налагодження, оновлення та видалення трояна.

Нова версія Skimer, помічена на початку травня, захищена популярним протектором Themida, який, серед іншого, ускладнює використання налагоджувача, заважає робити дамп пам'яті, шифрує ресурси та не дозволяє моніторити файл та реєстри. Очевидно, це зроблено у тому, щоб утруднити аналіз шкідливої програми. Замість класичних сканерів-накладок зловмисники використовують пристрій невеликого розміру, який встановлюється всередину банкомату поруч із слотом для карток через спеціально просвердлений отвір. Після цього отвір закривається наклейкою, внаслідок чого скіммер практично неможливо помітити.Скіммер приєднується банкомату до пристрою для карт, що зчитує, і працює на принципі прослуховування. Зловмисник вивужує через отвір дроти, що йдуть від зчитувача, приєднує пристрій до них і потім він інтерпретує дані, що передаються зчитувачем. Пристрої для крадіжки інформації з карт стають все витонченішими, і помітити їх важче. Тільки цього літа було виявлено новий тип скіммерів, який оформляється як накладки на щілину зчитувача карт, а вставляється прямо всередину. Він складається з двох металевих пластин, електронної схеми та батарейки, яка дозволяє пристрою працювати автономно

протягом кількох тижнів. Пристрій не запам'ятовує дані, а одразу передає їх на приймач, розташований неподалік.

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

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

Також були виявлені проблеми з NFC обладнанням. Багато моделей зчитувачів уразливі до відносно простих атак. Наприклад, деякі зчитувачі не перевіряють, як багато даних вони отримують - іншими словами, систему можна перевантажити величезною кількістю даних для виконання т. зв. атаки "переповнення буфера". Так маючи смартфон на Android, що використовує спеціальне програмне забезпечення, піднісши смартфон з NFC-модулем до зчитувача, можна заблокувати його для подальшого використання і навіть витягти інформацію про окремі банківські картки.

Також компанії часом дуже повільно випускають патчі для усунення виявлених проблем у сотень тисяч машин, розкиданих по всьому світу. Найчастіше віддалений доступ до пристрою не передбачений, і кожну точку необхідно особисто відвідати для встановлення ПЗ - тому багато систем не отримують регулярних оновлень безпеки. Найчастіше віддалений доступ до пристрою не передбачений, і кожну точку необхідно особисто відвідати для встановлення ПЗ - тому багато систем не отримують регулярних оновлень безпеки.

2.3 Аналіз загроз для оброблюваної інформації на серверному обладнанні

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

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

До них відносяться:

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

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

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

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

– засоби зв'язку;
– мережі інженерних комунікації (водопостачання, каналізації);
– транспорт.

Внутрішні джерела загроз:

– неякісні технічні засоби обробки інформації;

– неякісні програмні засоби обробки інформації;

– допоміжні засоби (охорони, сигналізації, телефонії);

– інші технічні засоби, що застосовуються в установі.

Ранжування джерел загроз

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

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

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

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

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

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

Таблиця 2.2. Аналіз загроз для оброблюваної інформації на серверному обладнанні

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

Продовження таблиці 2.2.

1	2	3	4	5	6
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 $(Коп)f = \frac{3 \cdot 2 \cdot 1}{125} = 0,048$
	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	К2 $(Коп)f$ =0,192
Персональні дані	Антропогенні зовнішні	Перехоплення інформації силовими, кримінальними структурами, недобросовісними партнерами	К5 $(Коп)i = \frac{5 \cdot 3 \cdot 2}{125} = 0,24$	Відсутність відео спостереження, порушення доступу до технічних об’єктів	К5 $(Коп)f = \frac{5 \cdot 3 \cdot 2}{125} = 0,24$

Продовження таблиці 2.2.

1	2	3	4	5	6
	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	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 2.2.

1	2	3	4	5	6
	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 кабел і не захищенні коробами. Можливість перехоплення через наводки електромагнітних випромінювань.	К4 $(Коп)f$ =0,128
	Техногенні внутрішні	Збій програмного забезп ечення	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	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

Продовження таблиці 2.2.

1	2		4	5	6
Інформація про стан вузлів платіжних терміналів	Техногенні внутрішні	Збій програмного забезпечення	К2 (К*оп*)*і* =0,048	Застаріле обладнання	К3 (К*оп*)*f* =0,16
	Стихійний	Пожар, форс – мажорні обставини.	К2 (К*оп*)*і* =0,192	Відсутність систем резервування, пошкодження життєзабезпечуючих комунікацій	К2 (К*оп*)*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.

2.4 Побудова моделі порушника

Рівень порушника э 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.

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.

Рівні збитків :

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. Детальна характеристика наведена у таблиці 2.2.

Таблиця 2.3 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

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.

2.5 Основні проблеми програмного забезпечення термінального обладнання

Проаналізувавши роботу термінального обладнання та його програмне забезпечення можемо зробити висновок що:

забезпечення, беручи до уваги усі атаки, можна зробити список основних проблем:

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

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

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

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

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

– відсутність в системі будь якого захисту цілісності при обміні інформацією

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

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

2.6 Рекомендації щодо поліпшення захисту програмного забезпечення термінального обладнання

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

Для підвищення рівня безпеки платіжного термінального обладнання впровадити наступні міри та програмні коплекси:

– За допомогою стандартних функцій Windows Server 2016 таких, як ActiveDirectoryRightsManagementServices, 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 відкри вати, змінювати, друкувати, перенаправляти інформацію або виконувати інші дії з нею. Для цього потрібно:

1) Відкрити консоль служби керування правами ActiveDirectory та розгорнути кластер AD RMS. У дереві консолі розкрити вузол Політики довіри та виберіть Довірені домени публікації . В області результатів виберіть сертифікат домену, який потрібно експортувати. На панелі Дії виберіть команду Експортувати довірений домен публікації . У вікні Файл домену публікації натисніть кнопку Зберегти як , щоб зберегти файл у відомому місці розташування на локальному комп'ютері. Введіть ім'я файлу, вкажіть .xmlрозширення імені файлу та натисніть кнопку " Зберегти" .У полях Пароль та Підтвердження пароля введіть надійний пароль, який використовується для шифрування файлу довіреного домену публікації. Цей пароль потрібно вказати при імпорті довіреного домену публікації до хмарної поштової організації.
2) Після експорту TPD у файл XML слід імпортувати його в Exchange Online.Щоб імпортувати TPD, виконайте наведену нижче команду в

Exchange OnlinePowerShell : Import-RMSTrustedPublishingDomain -FileData ([System.IO.File]::ReadAllBytes('<pathtoexported TPD file>')) -Name "<nameof TPD>" -ExtranetLicensingUrl<URL> -IntranetLicensingUrl<URL>. Під час запуску цієї команди потрібно ввести пароль. Введіть пароль, вказаний під час експорту TPD із сервера AD RMS.

3) Поширення шаблону політики прав AD RMS за допомогою командної консолі Exchange для цього у консолі введіть Get-RMSTemplate -TypeAll | fl. Щоб розповсюдити шаблон, виконайте наведену команду Set-RMSTemplate -Identity "<nameofthetemplate>" -TypeDistributed.
4) Увімкнути керування правами на доступ до даних за допомогою командної консолі Exchange. Щоб увімкнути керування правами на доступ до даних для своєї хмарної поштової організації потрібно ввести наступну команду Set-IRMConfiguration -InternalLicensingEnabled $true

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

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

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

адміністратор КЗЗ, адміністратор безпеки та користувач системи.Реєстрація облікових записів адміністраторів виконується в такому порядку:

1) у процесі інсталяції реєструється обліковий запис системного адміністратора;
2) системний адміністратор реєструє обліковий запис адміністратора безпеки (системний адміністратор може створити скільки завгодно облікових записів, але активізувати може єдиний обліковий запис адміністратора безпеки - облікові записи інших адміністраторів можуть бути активізовані тільки вже наявним адміністратором безпеки, а звичайних користувачів - адміністратором безпеки або адміністратором КСЗ);
3) системний адміністратор реєструє облікові записи адміністратора(ів) КСЗ;
4) адміністратор безпеки активізує облікові записи адміністратора(ів) КСЗ;
5) администраторы КСЗ создают необходимые учетные записи пользователей, регистрируют защищенные каталоги и выполняют другие необходимые действия.

Для входу в режим управління базою даних користувачів слугує пункт "Вид Користувачі" головного меню програми АРМ адміністратора КСЗ. Після вибору цього пункту або відповідної піктограми на панелі інструментів активізується вікно браузера "Облікові записи користувачів".

Для реєстрації нового користувача необхідно натиснути кнопку [Додати], післячого в закладці "Загальні" можна задати необхідні атрибути нового користувача.

У закладці "Загальні" необхідно задати ім'я адміністратора, групу (Адміністратори безпеки або Адміністратори КСЗ), а також рівень допуску.

Після завдання основних атрибутів можна перейти на закладку "Права і обмеження". У закладці "Права та обмеження" необхідно задати повноваження імпорту/експорту і для адміністраторів КСЗ - "Адміністративні

права".

Після введення всіх необхідних атрибутів слід згенерувати інформацію щодо

аутентифікації користувача. Для цього необхідно натиснути кнопку [Генерація], після чого з'явиться діалог введення (і підтвердження) пароля.

Необхідно вибрати тип носія даних аутентифікації, на який буде збережено інформацію аутентифікації користувача, ввести (і підтвердити) новий

пароль, після чого під'єднати носій даних аутентифікації користувача та натиснути

кнопку [Підтвердити]. Програма згенерує нову інформацію аутентифікації користувача

користувача і занесе її в БД і на носій даних аутентифікації

– 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 CertificateServices), яка використовуються для посвідчення користувачів і комп'ютерів та для шифрування даних при їх передачі по незахищеним лініям. Служба сертифікатів Active Directory застосовуються для підвищення безпеки за рахунок зв'язування ідентифікаційних даних користувача, пристрою або служби з відповідним закритим ключем. Сертифікат і закритий ключ зберігаються в ActiveDirectory, що допомагає захистити ідентифікаційні дані; служби Active Directory стають централізованим сховищем для отримання додатками відповідної інформації за запитом. Обмеження фізичного доступу до лінії і апаратури зв'язку.

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

– На даному рівні користувач, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів. Матриця доступу це

таблиця, за допомогою якої можна визначати тип доступу, застосувати на практиці матрицю доступу можна за допомогою ActiveDirectory, створити списки доступу на маршрутизаторах, розподілити користувачів по групам.

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

Def може дефрагментувати ОЗУ при досягненні рівня попередження або мовчки (з параметрами командного рядка). Вона відрізняється в плані надійності і швидкості, і повної підтримки, яку вона пропонує своїм користувачам, з файлами довідки, керівництва з усунення неполадок, поради, онлайн допомоги, а форум гарантує вам спокій разом з екстремальною продуктивності.

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

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

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

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

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

Рисунок 2.1 — Шифрування за допомогою PGP.

Потім, PGP створює сеансовий ключ, тобто одноразовий симетричний ключ, застосовуваний тільки для однієї операції. Як тільки дані зашифровані, сеансовий ключ також шифрується, але вже є відкритим ключем одержувача. Цей зашифрований відкритим ключем сеансовий ключ прикріплюється до шифротексту і передається разом з ним одержувачеві, що показано на рисунку 2.1. Розшифрування відбувається у зворотному порядку. PGP одержувача використовує його закритий ключ для витягу сеансового ключа з повідомлення, яким шифротекст вихідного повідомлення відновлюється у відкритий текст. Таким чином, комбінація цих двох криптографічних методів поєднує зручність шифрування відкритим ключем зі швидкістю роботи симетричного алгоритму.

2.7 Висновок

В спеціальній частині магістерської роботи був проведений аналіз загроз для оброблюваної інформації, визначені можливі загрози, що можуть впливати на

пристрій та інформацію на ньому, завдяки отриманим результатам було визначено найнебезпечніші вразливості, які можуть вплинути критично на інформацію та систему. Потім було виявлено ряд загроз та вразливостей де найнебезпечніші з них:

– зовнішні загрози щодо інформації про обробку платежу (К*оп*)*і*=0,08та 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.

Було створено модель порушника та проаналізовано операційні системи термінального обладнання, виділені переваги та недоліки систем. Проаналізовано атаки на термінальне обладнання, виявлені вразливості програмного забезпечення платіжного термінального обладнання, розроблені рекомендації щодо поліпшення захисту інформації на термінальному обладнанні.

РОЗДІЛ 3 ЕКОНОМІЧНА ЧАСТИНА

Компанія «Європа» – найбільший небанківський оператор платіжних та фінансових сервісів в Україні, якому належить інтегрована платіжна мережа, що дозволяє здійснювати платежі offline та online та через мобільні додатки. Та яка має 14 000 платіжних терміналів. Річні прибутки підприємства – 20 млн. грн. Компанія розпочала роботу у 2007 році штаб квартира знаходиться у місті Київ за адресою вул. Богдана Хмельницького 52-а.

3.1 Визначення трудомісткості розробки та опрацювання поліпшень.

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

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

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

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

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

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

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

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

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

Умовна кількість оперантів у програмі:

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

де q =40

C =1,5

p =0,1

де q – очікувана кількість операндів;

c – коефіцієнт складності програми;

p – коефіцієнт корекції програми в процесі її опрацювання.

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

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

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

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

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

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

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

- Rдо 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 поліпшень:

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

Тривалість опрацювання програми на персональному комп'ютері:

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

Тривалість підготовки технічної документації на програмному засобі:

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

3.2 Розрахунок витрат на створення програмного продукту

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

$$К_{\text{пз}} = З_{\text{зп}} + З_{\text{мч}} = 27175 + 5887{,}74 = 33\,062{,}74 \text{ грн} \quad (3.8)$$

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

$$З_{\text{зп}} = t \cdot З_{\text{пр}} = 54{,}35 \cdot 500 = 27175 \text{грн} \quad (3.9)$$

де t – загальна тривалість створення програмного забезпечення, годин;

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

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

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

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

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

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

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

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

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

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

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

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

H_a – річна норма амортизації на персональному комп'ютері, частки одиниці;

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

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

F_p– річний фонд робочого часу (за 40 – годинного робочого тижня F_p= 1920 год).

3.3 Розрахунок поточних (експлуатаційних) витрат

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

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

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

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

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

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

– навчання адміністративного персоналу й кінцевих користувачів;

– амортизаційні відрахування від вартості обладнання та програмного забезпечення;

– заробітна плата обслуговуючого персоналу;

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

– навчальні курси й сертифікація обслуговуючого персоналу;

– технічне й організаційне адміністрування й сервіс.

Витрати на 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:

$$С_к = С_н + С_а + С_з + С_е + С_{ел} + С_о + С_{тос} = 18546 + 1617,3 + 47580 + 10512 + 2,4 + 12,2 + 1695,9 = 79\,965,83 \text{грн.} \quad (3.13)$$

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

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

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

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

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

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

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 0,5 \cdot 8760 \cdot 2,4 = 10512 \text{ грн} \quad (3.15)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$– річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

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

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

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

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

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

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

$$С = С_в + С_к + С_{ак} = 9860 + 79\,965,833 + 3863 = 93\,688,83 \text{грн} \quad (3.16)$$

3.4Оцінка 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 (

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

Необхідні вихідні дані для розрахунку:

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

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

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

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

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

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

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

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

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

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

I – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число можливих атак на рік.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.5 Загальний ефект від впровадження поліпшень

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

$$E = B \cdot R - C = 59088{,}57 \cdot 2 - 93\,688{,}83 = 24\,488{,}31 \text{ грн} \qquad (3.24)$$

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

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

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

3.6 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

– Сукупна вартість володіння (ТСО);

- Коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (ReturnonInvestmentforSecurity);
- Термін окупності капітальних інвестицій.

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

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

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

$$ROSI = \frac{E}{K} = \frac{24\,488{,}31}{19475{,}24} = 1{,}3 \qquad (3.25)$$

де E – загальний ефект від впровадження системи інформаційної безпеки;

K – капітальні інвестиції.

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

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{19475{,}24}{24\,488{,}31} = 0{,}79 \text{ рока (}\sim\text{8 місяців)} \qquad (3.26)$$

Виходячи з формули (3.26) можна побачити, що термін окупності дорівнює 8місяців.

ВИСНОВОК

Успішно реалізована атака на термінальне обладнання може заподіяти фінансові витрати компанії. Проаналізовано весь об’єкт з економічної точки зору на впровадження системи інформаційної безпеки.

На підставі проведених розрахунків можна зробити наступні висновки:

1. Визначено та детально розраховано трудомісткість реалізації поліпшень;
2. Прораховані усі фінансові витрати на поліпшення системи безпеки для програмного забезпечення платіжного термінального обладнання;
3. Прораховані збитки після проведених атак на систему;
4. Розраховано ефективність впровадження систем інформаційної безпеки.

Розрахувавши всі критерії можемо зробити висновок, що впровадження цієї інформаційної безпеки є економічно доцільним. Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе 59088,57 грн, після впровадження системиінформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки становить24 488,31грн.

ВИСНОВОКИ

У кваліфікаційній роботібуло порушено питання про удосконалення існуючих систем інформаційної безпеки було проаналізованоплатіжне термінальне обладнання з точки зору безпекитермінального обладнання.

А саме :

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

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

Проведено аналіз вразливостей на платіжних терміналів, а саме:

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

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

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

– розроблена таблиця порівняння баз даних, розкриті всі переваги та недоліки систему управління базами даних. На серверному обладнанні буде використовуватися система керування базами даних MS SQL. Причини вибору

даної системи обґрунтовується широким поширенням системи, високою продуктивністю при низькій вартості сервера і простотою підтримки системи;

– проведений повний аналіз технології передачі інформації між платіжним терміналом та серверним обладнанням, досліджені методи передачі запросів на сервера та методи захисту інформації. Обрана технологія передачі інформації «GeneralPacketRadioService», 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;

Була розрахована економічна доцільність впроваджень. Якщо не реалізуватівсі запропоновані поліпшень загальний збиток від атак буде складати 59088,57 грн грн, а після впровадження загальний ефект буде складати 24 488,31грн, тобто реалізація поліпшень є економічно ефективним рішенн

ПЕРЕЛІК ПОСИЛАНЬ

1. Термінальне обладнання [Електронний ресурс]— https://dengi.polnaya.info/platezhnye_sistemy/terminalnoe_oborudovanie/
2. Операційні системи терміналів [Електронний ресурс] — https://www.iterator.com.ua/ua/poleznye-materialy/202-shcho-take-sistema-pos-i-yak-vibrati-sistemu-pos, https://www.iterator.com.ua/ua/poleznye-materialy/202-shcho-take-sistema-pos-i-yak-vibrati-sistemu-pos;
3. Протокол надання доступу до віддаленого комп'ютера[Електронний ресурс]— https://bankchart.com.ua/finansoviy_gid/groshi_rodini/statti/viddalene_upravlinnya_komp_yuterom_cherez_internet#:~:text=RDP%20(Remote%20Desktop%20Protocol)%20%2D,%D0%B2%D1%96%D0%B4%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%B8%D0%B9%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%20%D0%B4%D0%BE%20%D0%BA%D0%BE%D0%BC%D0%BF'%D1%8E%D1%82%D0%B5%D1%80%D0%B0;
4. Класифікація інформаційних об'єктів [Електронний ресурс] — https://studfile.net/preview/7519639/page:2/;
5. Термінальні проломи: злом мереж платіжних терміналів [Електронний ресурс] — https://www.pcidssguide.com/how-to-protect-your-pos-system-from-pos-malware/;
6. Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки. Методики виявлення закладних пристроїв. НД ТЗІ 2.7-011-2012 – Київ 2012 р.;
7. Методи і засоби пошуку електронних пристроїв перехоплення інформації [Електронний ресурс]Режим доступу:http://www.analitika.info/poisk.php?page=1&full=block_article35;
8. SQL ін'єкції [Електронний ресурс] —https://www.pcidssguide.com/how-to-protect-your-pos-system-from-pos-malware/;
9. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99 – Київ 1999;

10. GSM/GPRS-модулі — https://diylab.com.ua/ua/p107642952-gsm-gprs-modul.html;
11. Vpn з'єднання [Електронний ресурс] — https://nordvpn.com/uk/what-is-a-vpn/;
12. Класифікація загроз в інформаційній безпеці [Електронний ресурс] — https://pidru4niki.com/12631113/ekonomika/ponyattya_klasifikatsiya_zagroz_bezpeki_informatsiyi.

ДОДАТОК А. Відомість матеріалів кваліфікаційноїроботи

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

ДОДАТОК Б. Перелік документів на оптичному носії

1 Пояснювальна записка Масалов І.С.docx

2Презентація Масалов І.С.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)