

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки.
Факультет радіоелектроніки та телекомунікацій
(повне найменування інституту, факультету)

Кафедра «Захисту інформації»
(повне найменування кафедри)

Пояснювальна записка

Магістр
(ступінь вищої освіти)

на тему «Дослідження комплексної системи захисту платіжного шлюзу в мережі Інтернет»

Виконав: студент 2 курсу, групи РТ-811м

Спеціальності 125 Кібербезпека
(код і найменування спеціальності)

Освітня програма (спеціалізація)
«Безпека інформаційних і комунікаційних систем»

Грачов М.Ю.
(прізвище та ініціали)

Керівник Воскобойник В.О.
(прізвище та ініціали)

Рецензент Савченко Ю.В.
(прізвище та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Інститут, факультет Інститут інформатики та радіoeлектроніки,
Факультет радіoeлектроніки та телекомунікацій
Кафедра захисту інформації
Ступінь вищої освіти магістр
Спеціальність 125 – «Кібербезпека»

(код і найменування)

Освітня програма (спеціалізація) «Безпека інформаційних і комунікаційних систем»

(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри Воскобойник В.О.

канд. техн. наук, доцент

«___» _____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТА

Грачова Максима Юрійовича

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Дослідження комплексної системи захисту платіжного шлюзу в мережі Інтернет

керівник проекту (роботи) Воскобойник Володимир Олександрович, кандидат технічних наук, доцент кафедри захисту інформації

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від «08» листопада 2022 року № 371

2. Строк подання студентом проекту (роботи) 15 грудня 2022 року

3. Вихідні дані до проекту (роботи) Несанкціонований доступ, захист платіжних банківських даних від несанкціонованого доступу, електронні платежі банківської системи, платіжні шлюзи в мережі Інтернет, прийняття рішень, модель комплексної системи захисту платіжного шлюзу.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) аналіз предметної області та стану електронних платіжних систем, їх класифікація, структура, принципи взаємодії між собою в мережі Internet; апаратно-програмні ресурси платіжного шлюзу та функціональна безпека; модель порушника інформаційної безпеки платіжного шлюзу в мережі Internet; розробка моделі комплексної системи захисту платіжного шлюзу в мережі Internet.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

11 рисунків; 21 таблиця; презентація магістерської роботи.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основні розділи	Воскобойник В.О., доцент	01.09.2022	
Нормоконтроль	Корольков Р.Ю., ст. викладач		

7. Дата видачі завдання «01» вересня 2022 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Складання та затвердження ТЗ	01.09—10.09	Виконано
2	Підбір літератури	11.09—17.09	Виконано
3	Аналіз предметної області та організації електронних платіжних систем в банківській сфері	18.09—20.09	Виконано
4	Аналіз існуючих схем мережевої взаємодії платіжного шлюзу з іншими вузлами при проведенні платіжних транзакцій	21.09—01.10	Виконано
5	Аналіз апаратно-програмних ресурсів платіжного шлюзу	02.10—04.10	Виконано
6	Аналіз моделей погроз безпеки платіжного шлюзу в мережі Internet	05.10—12.10	Виконано
7	Аналіз модель порушника інформаційної безпеки платіжного шлюзу в мережі Internet	13.10—18.10	Виконано
8	Аналіз існуючих вимог до засобів, методів і способів зменшення рівнів ризиків інформаційної безпеки передачі транзакційних пакетів через платіжні шлюзи, згідно зі стандартами ради PCI SSC	19.10—03.11	Виконано
9	Розробка моделі комплексної системи захисту платіжного шлюзу в мережі Internet.	04.11—26.11	Виконано
10	Оформлення пояснювальної записки	27.11—8.12	Виконано
11	Оформлення графічної частини	8.12—10.12	Виконано

Студент

_____ (підпис)

Керівник проекту (роботи)

_____ (підпис)

Грачов М.Ю.

_____ (прізвище та ініціали)

Воскобойник В.О.

_____ (прізвище та ініціали)

РЕФЕРАТ

ПЗ: 85 сторінок, 11 рисунків, 21 таблиця, 23 джерела, 4 додатка.

ВРАЗЛИВІСТЬ, ДОВІРЕНИЙ ОБ'ЄКТ, ЕЛЕКТРОННА КОМЕРЦІЯ, ІНТЕРНЕТ-ЕКВАЙРИНГ, МОДЕЛЬ, ПЛАТІЖНА СИСТЕМА, ПЛАТІЖНИЙ ШЛЮЗ, ПРОТОКОЛ, РИЗИК, СЕРВЕР, ТРАНЗАКЦІЯ

Магістерська робота присвячена питанню комплексної системи захисту платіжного шлюзу в мережі Інтернет.

Проведено огляд теоретичних аспектів захисту платіжного шлюзу в мережі Інтернет.

Об'єкт дослідження (або розробки): платіжний шлюз, який представляє собою апаратно-програмний комплекс обробки платіжних транзакцій, поступаючих з мережі Internet.

Ціль роботи: створити модель комплексної системи захисту платіжного шлюзу, де в, 1-у чергу, захист буде спрямований на використання захищених, при найсучасніших вимогах стандартів ради PCI SSC, автоматизованих комплексів обробки транзакцій для платіжних шлюзів і процесінгових центрів, а також посилення самої слабкої ланки, існування якої викликано незахищеністю протоколу TCP транспортного рівня моделі взаємодії відкритих з'єднань (OSI) від перехоплення, що встановилося під час сеансу довіреного об'єкта із сервером (в даному випадку платіжним шлюзом).

Дотримання принципу комплексності при створенні моделі системи захисту досягатиметься за рахунок виконання вимог стандарту PCI DSS Version 3.0. Ставиться завдання - звести до мінімуму ймовірності реалізації погроз, завдяки існуючим вразливостям в платіжних шлюзах, для дотримання всіх критеріїв захищеності інформації, переданої в платіжних транзакціях і захисту від втрати матеріальних активів учасників електронного грошового обміну.

Методи дослідження: методи аналізу, статистичні методи.

Результати роботи: у магістерській роботі запропонована модель комплексної системи захисту платіжного шлюзу в мережі Internet.

Новизна роботи: в магістерській роботі пропонується 2-а способу підвищення рівня захищеності передачі транзакційних пакетів від підміни ідентифікаторів відправників: спосіб мережевої ідентифікації між вузлами-учасниками і спосіб контролю маршруту проходження транзакційних пакетів протягом усього процесу здійснення оплати через Internet.

Рекомендації щодо використання результатів роботи: запропонована модель комплексної системи захисту платіжного шлюзу в мережі Internet може бути реалізована й впроваджена для будь-якого процесінгового центру банку або платіжного шлюзу.

Це наочно показує перспективність запропонованої моделі в даній області комунікації й захисту інформації.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	8
ВСТУП.....	9
1 ЕЛЕКТРОННА КОМЕРЦІЯ. ПРИНЦИПИ РОБОТИ Й ЗАХИЩЕНІСТЬ	11
1.1 Основні поняття електронних бізнес систем	11
1.2 Процес переходу підприємств до електронного бізнесу.....	12
1.3 Електронні платіжні системи. Класифікація, структура, принципи взаємодії між собою в мережі Internet.....	14
Висновки до розділу 1	21
2 АНАЛІЗ ПОГРОЗ БЕЗПЕКИ Й КОМПЛЕКСНИЙ ПІДХІД ДО СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ПЛАТІЖНОГО ШЛЮЗУ В МЕРЕЖІ INTERNET	22
2.1 Платіжний шлюз. Схеми мережної взаємодії платіжного шлюзу з іншими вузлами при проведенні платіжних транзакцій.....	22
2.2 Класифікація видів інформації, які обробляються у платіжному шлюзі.....	24
2.3 Апаратно-програмні ресурси платіжного шлюзу.....	28
2.4 Модель погроз безпеки платіжного шлюзу в сети Internet	31
2.5 Модель порушника інформаційної безпеки платіжного шлюзу в мережі Internet.....	42
2.6 Вибір класу й профілю захищеності	48
2.7 Огляд існуючих вимог до засобів, методів і способам зменшення рівнів ризиків інформаційної безпеки передачі транзакційних пакетів через платіжні шлюзи, згідно зі стандартами ради PCI SSC	66
Висновки до розділу 2	69
3 РОЗРОБКА МОДЕЛІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ПЛАТІЖНОГО ШЛЮЗУ В МЕРЕЖІ INTERNET	70
3.1 Вибір оптимальних рішень з погляду безпеки, комплексності, масштабованості й рівня капіталовкладень	69
3.2 Розробка нових способів у міжмережевій безпеці передачі транзакційних пакетів через платіжні шлюзи	72

3.3 Розробка способу мережної ідентифікації між вузлами-учасниками при передачі транзакційних пакетів протягом усього процесу здійснення оплати через Internet	75
3.4 Розробка способу контролю маршруту проходження транзакційних пакетів між вузлами-учасниками протягом усього процесу здійснення оплати через Internet	77
Висновки до розділу 3	78
ВИСНОВКИ	79
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	80
Додаток А Інфраструктура банку – схема мережі.....	83
Додаток Б Потоки ДВК між учасниками процесу еквайрингу.....	84
Додаток В Платіжний шлюз (схема мережі) та область застосування PCI DSS	85
Додаток Г Способи підтвердження відповідності стандарту PCI DSS	86

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БД – База даних

ДВК – Дані про власника карт

КАД – Критичні автентифікаційні дані

МПС – Міжнародна платіжна система

ПШ – Платіжний шлюз

ТСП – Торгово-сервісне підприємство

ACS – Access control system

ATM – Automated Teller Machine

CID – Card identification number

CN – Cardholder Name

CVC1 – Card validation code, Mastercard

CVV1 – Card verification value, Visa

ISA – Internal Security Assessors

PAN – Primary Account Number

PAN – Primary Account Number

PCI SSC – PCIment Card Industry Security Standards Council

POS – Point of Sale

QSA – Qualified Security Assessors

SAQ – Self-Assessment Questionnaire

SSL – Secure Socket Layer

TRACK – Full Magnetic Stripe Data

ВСТУП

Актуальність теми. У даній роботі розглядається проблема існування вразливостей програмного забезпечення платіжних шлюзів, використовуваних для здійснення проведення платіжних транзакцій між клієнтами й постачальниками послуг і товарів використовуючи електронні кошти, за допомогою мережі Internet.

Необхідність зменшення до мінімуму ймовірностей реалізації погроз, через існуючі уразливості в платіжних шлюзах, викликана існуванням вимог міжнародних стандартів інформаційної безпеки в платіжних системах, невідповідність або недотримання яких приведе, як мінімум, до невидачі або не продовженню ліцензії на проведення відповідного класу транзакцій у платіжних шлюзах або до порушення конфіденційності відомостей клієнтів, які становлять коди авторизації або банківську таємницю й, як наслідок, втрату фінансових активів клієнтів, або як максимум, до закриття, банкрутству, матеріальної й кримінальної відповідальності підприємств власників даних шлюзів у мережі Internet.

Можливість розв'язати описану вище проблему можливо при виконанні вимог міжнародних стандартів інформаційної безпеки в платіжних системах, тобто при дотриманні принципу комплексності, поширення якого повинне бути спрямоване як на окремі елементи платіжних систем, так і на об'єднуючі їх високорівневі системи, а також канали зв'язку між ними.

Проблема інформаційної безпеки проведення електронних платежів впливає як на діяльність клієнтів - фізичних осіб так і підприємств різних форм власності й сфер діяльності, а отже впливає й на процеси, пов'язані з виробничими завданнями.

Розв'язання описаної вище проблеми є й буде є актуальною завжди, поки буде існувати електронна комерція з використанням платіжних шлюзів у мережі Internet і поки будуть існувати зловмисники, метою яких є незаконне присвоєння чужих матеріальних активів.

Мета і задачі дослідження. Метою роботи є створення моделі комплексної системи захисту платіжного шлюзу який функціонує в мережі Internet, де в, першу чергу, захист буде спрямований на використання, захищених, за найсучаснішими вимогами стандартів ради PCI SSC, автоматизованих комплексів обробки транзакцій для платіжних шлюзів та процесингових центрів, а також на посилення найслабшої ланки, існування якої викликане незахищеністю протоколу TCP транспортного рівня моделі взаємодії відкритих з'єднань (OSI) від перехоплення сеансу довіреного об'єкту, що встановився з сервером (в даному випадку платіжним шлюзом)

Об'єкт дослідження – платіжний шлюз, який функціонує в мережі Internet і є апаратно-програмним комплексом обробки платіжних транзакцій, що надходять з мережі Internet.

Предмет дослідження – інформаційні технології моніторингу, оцінювання і вибору характеристик надійності та безпеки системи захисту платіжного шлюзу, який функціонує в мережі Internet.

1 ЕЛЕКТРОННА КОМЕРЦІЯ. ПРИНЦИПИ РОБОТИ Й ЗАХИЩЕНІСТЬ

1.1 Основні поняття електронних бізнес систем

Останнім часом усе частіше й частіше використовуються сучасні технології електронних взаєморозрахунків за товари й послуги в мережі Internet. Розвиток економіки будь-якої держави сьогодні неможливо без високоефективної системи грошового обігу та використання сучасних платіжних механізмів. Електронізація грошових відносин є важливим прогресом розвитку ринку в сучасних умовах, який бурхливо поширюється на всі сфери діяльності й розширюється з кожним днем. Тому створення потужної багаторівневої комплексної системи захисту проведення операцій над електронними коштами є дуже актуальним на сьогоднішній час, тому що порушення вище названих принципів захисту або їх не відповідність і не дотримання може привести до більших фінансових втрат як звичайних громадян так і держави в цілому.

Електронний бізнес – це перетворення основних бізнес-процесів компанії шляхом впровадження Інтернет-технологій, націлене на підвищення ефективності діяльності. Електронним бізнесом є всяка ділова активність, що використовує можливості глобальних інформаційних мереж для перетворення внутрішніх і зовнішніх зв'язків компанії. З технічної точки зору, Internet це всесвітнє об'єднання комп'ютерних мереж, якої можуть зв'язувати комп'ютери усередині підприємства, яка називається intranet, або ж об'єднання локальних мереж різних підприємств, яке називається extranet.

Електронний бізнес являє собою будь-яку транзакцію, зроблену за допомогою мережі, по завершенню якої відбувається передача права власності товарів або послуг.

Транзакція – банківська операція по перекладу коштів для якої-небудь мети.

Область додатка електронного бізнесу: фінансові операції в інтерактивному режимі. До них ставляться операції з банківським продуктом, операції зі

страховим продуктом, інтерактивне інвестування, спекулятивні операції з валютою й цінними паперами. Ринки електронної торгівлі. До них ставляться торгівля через візуальні магазини, торгівля інформаційним продуктом, торгівля туристичним продуктом, ринки мобільної торгівлі. Це торгівля через торговельні автомати й ринки торговельних послуг.

У рамках бізнесу Інтернет використовується комунікації різної складності й вартості, для зниження внутрішньо фірмових технологічних витрат і в якості зручного засобу для розробки фірмових інформаційних систем.

Інформаційний обмін це взаємодія між банками, торговельними партнерами, постачальниками, де інформація є товаром.

Інтернет торгівля – це частина електронного бізнесу, у процесі якого зв'язок і обмін відбувається електронним образом.

Види електронного бізнесу: електронні аукціони; електронні банки; електронна комерція; електронна науково-дослідна й дослідно-конструкторська робота; електронні показчики; електронне навчання; електронна пошта; електронний маркетинг.

Електронні банки дозволяють одержувати клієнтам доступ до їхніх рахунків і здійснювати різні фінансові операції за допомогою простого web-сайту[4], який називається платіжним шлюзом.

Ступінь підготовки держави до електронного бізнесу визначається рівнем інвентаризації, рівнем розвитку комунікацій, якістю підготовки фахівців, готовністю фінансових інститутів до електронного бізнесу, увагою уряду до даної галузі.

1.2 Процес переходу підприємств до електронного бізнесу

Приведемо відмінності між електронним бізнесом і електронною комерцією у вигляді таблиці 1.1.

Таблиця 1.1 – Відмінні риси електронного бізнесу й електронної комерції

Електронний бізнес	Електронна комерція
1. Це похідна від терміну електронна пошта, що означає ведення бізнесу через Інтернет, причому це не тільки купівля-продаж, а й обслуговування клієнта та взаємодія з бізнес-партнерами.	1. Це тільки купівля-продаж
2. Це перетворення основних бізнес-процесів за допомогою Інтернет-технологій.	2. Це використання комунікаційних технологій для передачі бізнес-інформації та ведення бізнесу
3. Це будь-яка бізнес-діяльність, що базується на засобах Інтернету, що перетворює зовнішні та внутрішні взаємини для створення нової вартості та використання ринкових можливостей, що надаються новими правилами пов'язаної економіки.	3. Це будь-яка транзакція, що здійснюється через комп'ютерну мережу
4. Це будь-який процес, який організація виробляє через мережу пов'язаних між собою комп'ютерів.	

Перевага електронного бізнесу у тому, що це нова форма організації підприємства, нова форма ведення бізнесу. Також це видно з таблиці 1.1, що електронна комерція це інструменти для ведення електронного бізнесу.

Структура організації електронного бізнесу в системі постачальник-виробник-клієнт зображена на рис. 1.1.

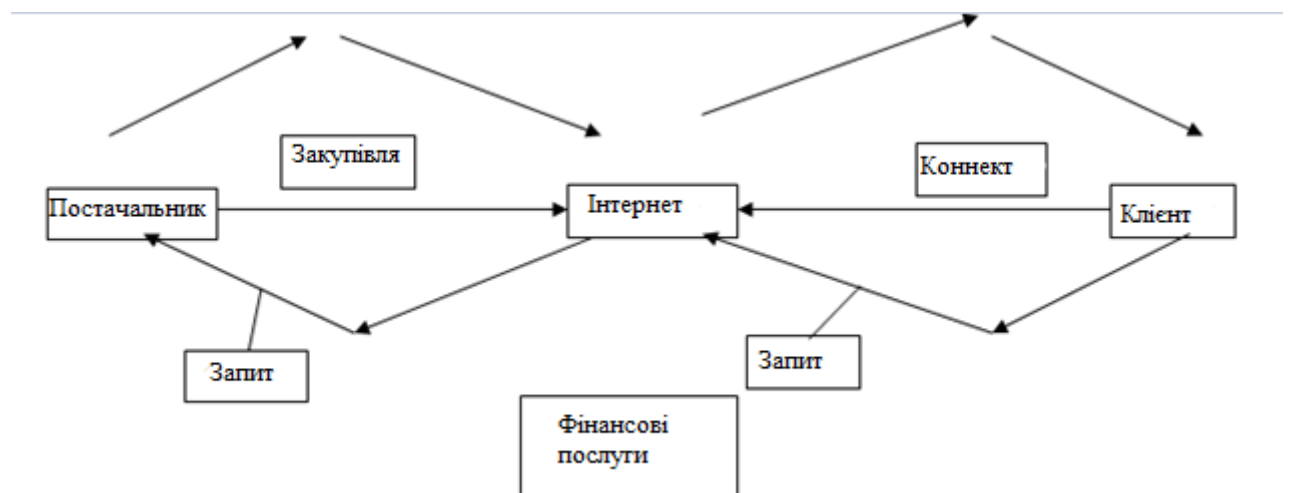


Рисунок 1.1- Структура електронного бізнесу

Опишемо принцип роботи наведеної на рис.1.1 блок схеми:

а) Фірма здійснює пошук сировини й комплектуючих, використовуючи можливості Інтернету й управляє виробництвом за допомогою Інтернету.

б) Виконує фінансові зобов'язання за допомогою організації постачальника фінансових послуг.

в) Веде роботу з потенційними споживачами.

Аналітики виділяють 3 основні стадії, відповідні до вдосконалювання системи електронної комерції:

а) організація веб-вузла компанії, подання електронних каталогів продукції, відомостей про діяльність фірми, статистичної інформації, орієнтація на постачальника товарів та послуг;

б) створення системи електронного бізнесу інтегруючого веб-сайт і внутрішні системи обробки замовлень і керування матеріальними активами, з'являється можливість розміщення замовлень і контроль за їх виконання безпосередньо через веб-інтерфейс сайту компанії-постачальника, подібна організація дозволяє відображати дані про матеріальних запаси, ціни, запаси й поставки. Центральним елементом цієї системи є постачальник і додається споживач, на який орієнтований даний етап;

в) ставить акцент на споживача й орієнтується в цілому на замовника, у результаті чого, технологія автоматизації, інтеграції і т.д. надають максимальні переваги зовнішнім клієнтам. При цьому впроваджується мережа поставок, як складна система ділових взаємозв'язків, завдяки якій зміна в одній з компаній передається в будь-яку зв'язану бізнес-систему.

1.3 Електронні платіжні системи. Класифікація, структура, принципи взаємодії між собою в мережі Internet

Платіжна система - це сукупність методів, що й реалізують їхніх

суб'єктів, що забезпечують у рамках системи умови для використання платіжного інструмента застереженого стандарту як платіжного засобу. Це поняття так само розкривається як "набір механізмів для виконання зобов'язань, що прийняті господарюючими суб'єктами при придбанні ними матеріальних або фінансових ресурсів". До таких механізмів вони відносять "установи, що надають платіжні послуги, різні інструменти, використовувані для передачі платіжних вказівок (включаючи канали зв'язку) і договірні відносини між зацікавленими сторонами". Платіжним інструментом може бути пластикова карта, «електронний гаманець» у відкритій мережі або рахунок в електронній інтерактивній банківській системі. Можна дати визначення банківським платіжним системам з погляду їхньої економічної сутності. З цієї позиції, банківські платіжні системи є частиною системи безготівкових розрахунків, заснованої на власних принципах, способах платежу та формах розрахунків та активно взаємодіючої з усією системою безготівкових розрахунків.

а) Банк-Еквайер – банк, що надає послуги еквайрингу.

б) Банк-Емітент-банк, що випустив платіжну карту.

Міжнародна платіжна система (МПС) – співтовариство банків, що встановило правила обігу платіжних карт (Visa, Mastercard, American Express, Discovery, JCB).

Постачальник послуг – організація, що виявляє послуги в індустрії платіжних карт, пов'язані з обробкою платіжних транзакцій. Прикладами постачальників послуг є банки-емітенти, банки-еквайери, платіжні шлюзи, хостинг-провайдеру.

Торгово-сервісне підприємство (ТСП) – організація, що ухвалює платіжні карти до оплати за товари й послуги.

Еквайринг – процес приймання платіжних карт до оплати за товари й послуги. Розрізняють:

а) банкоматний (Automated Teller Machine, АТМ) еквайринг – видачу готівки по платіжній карті з використанням банкомата;

б) торговельний (Point of Sale, POS) еквайринг – приймання платіжних карт до оплати за товари й послуги торгово-сервісних підприємств із використанням Pos-Терміналів і

в) Інтернет-Еквайринг – приймання платіжних карт до оплати за товари й послуги з використанням засобів електронної комерції.

Емісія – процес випуску (персоналізації) платіжних карт.

Далі в роботі ми будемо аналізувати торговельний і Інтернет-еквайринги.

Одне з основних завдань, розв'язуваних при створенні платіжної системи, полягає у виробленні й дотриманні загальних правил обслуговування вхідних у систему емітентів, проведення взаєморозрахунків і платежів. З організаційної точки зору ядром платіжної системи є заснована на договірних зобов'язаннях асоціація банків. До складу платіжної системи також входять підприємства торгівлі та сервісу, що утворюють мережу точок обслуговування. Для успішного функціонування платіжної системи необхідні та спеціалізовані не фінансові організації, які здійснюють технічну підтримку обслуговування: процесингові та комунікаційні центри, центри технічного обслуговування тощо.

Таким чином, електронні платіжні системи є одним з можливих і найбільш реальних шляхів удосконалювання наявного й безготівкового обігу.

Один з можливих типів схеми роботи платіжної системи представлено на рис. 1.2.

При всій неоднорідності визначення принципів побудови сучасних платіжних систем можна виділити такі принципи як:

а) Принцип безпеки передбачає, що протоколи захисту мають забезпечити повну конфіденційність передачі транзакцій. Сучасні алгоритми цифрової інформації, підписи та шифрування цілком придатні для вирішення цього завдання.

б) Принцип анонімності припускає повну відсутність авторизації транзакцій, щоб виключити будь-яку можливість простежити платежі приватної особи, а значить - вторгнутися в його приватне життя.

в) Принцип портативності припускає, що інструментарій будь-якої електронної платіжної системи дає можливість користувачеві не бути прив'язаним до якогось конкретного технічного обладнання та робить його вільним у пересуваннях, дозволяє купувати бажаний товар незалежно від місця розташування покупця і продавця..

г) Принцип двоспрямованості передбачає, що у платіжних системах гроші можна як віддавати іншій особі, а й отримувати. У платіжних карткових системах ви зазвичай віддаєте (платите) свої гроші одним способом, а отримуєте їх зовсім іншим, що виключає можливість прямої передачі коштів між двома приватними особами.

Г) Крім цього можна виділити принцип швидкості та ефективності проведення транзакцій, принцип проведення операцій у межах власних коштів та отриманих кредитів користувача, принцип мультивалютності платіжних систем, виявляється у тому, що при здійсненні оплати в системі є можливість миттєвої конвертації базової валюти у валюту платежу.

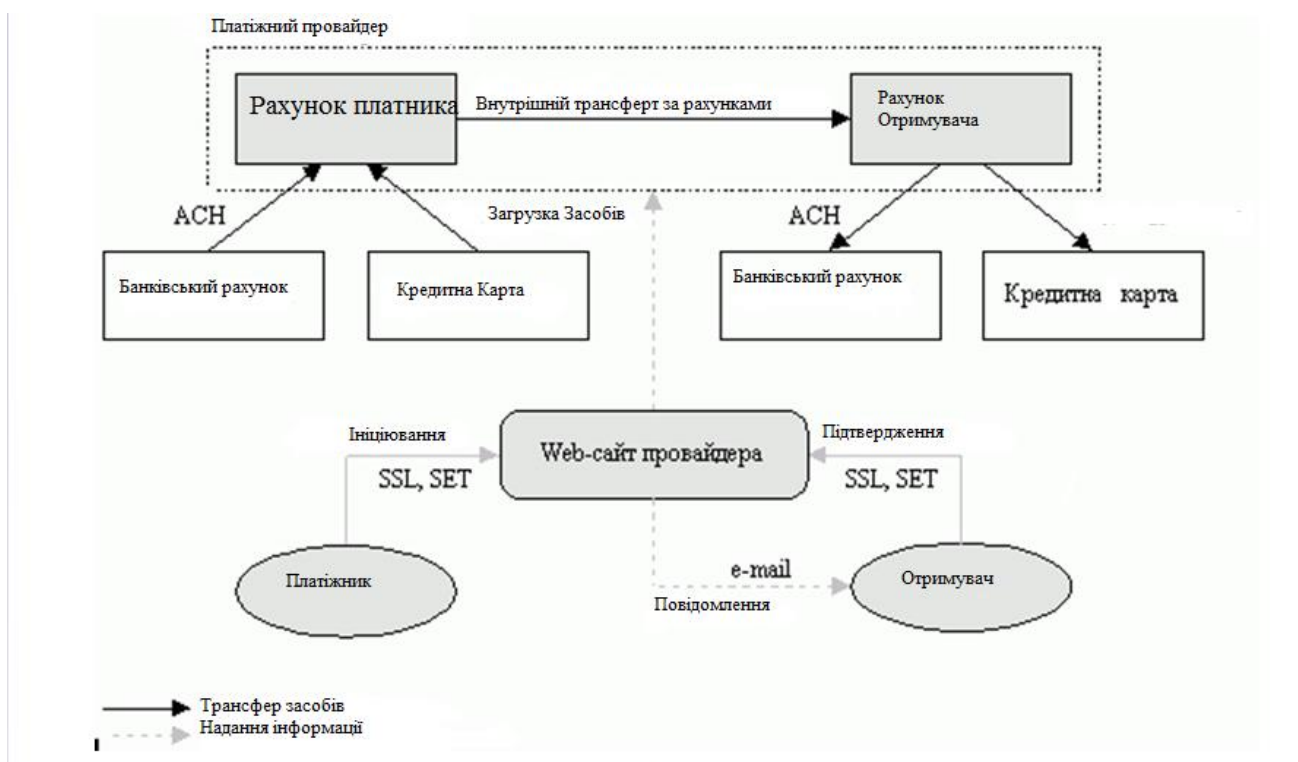


Рисунок 1.2 - Схема роботи платіжної системи

Таким чином, можна зробити висновок про те, що сучасні електронні платіжні системи, маючи власні принципи побудови, є, що виділилися частиною платіжної системи безготівкових розрахунків. Але принципи взаємодії між блоками в схемі роботи будь-якої платіжної системи побудовані на архітектурі взаємодії Клієнт-Сервер, схема роботи якої наведено на рис. 1.3.

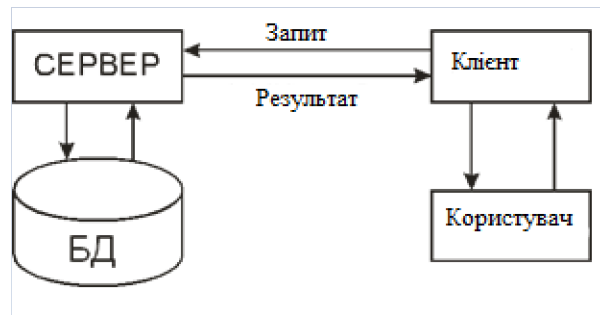


Рисунок 1.3 – Схема архітектури взаємодії Клієнт-Сервер

У цей час не існує єдиного підходу до класифікації Платіжних систем. Так Ю.С. Крупнов у своїй статті «Про природу електронних грошей» визначає види платіжних систем відповідно до п'ятьма грошовими компонентами й платежами, кожний з яких має свої особливості, хоча й виконується платниками в діалоговому режимі:

- а) Виписування рахунків по кредитних картах.
- б) Нагромадження заборгованості по електронних торговельних рахунках.

(Дана система пов'язана із провидінням величезної кількості мікроплатежів, які необхідно акумулювати на суму, розмірну зі звичайною комерційною транзакцією).

- в) Зберігання грошей на електронних рахунках. (Інструментами даної системи є смарт-карта, або «безкарточний» еквівалент смарт-карти у вигляді електронного рахунку, на який попередньо необхідно внести готівку або перевести засобу зі звичайного банківського рахунку.)

- г) Оформлення рахунків по електронних дебетових картах.

- Г) Переклад грошей за допомогою електронних чеків. (Дозволяють

переводити засобу із уже наявних банківських рахунків із правом виписки на них електронних чеків.)

Сучасні платіжні системи можна поділити залежно від схеми їх функціонування на наступні види:

а) Системи в яких реалізовано технологію перенесення інформації в електронному вигляді про «грошові зобов'язання емітента з пристрою одного власника на пристрій іншого власника.

б) Системи в яких відсутня технічна можливість перенесення інформації в електронному вигляді про «грошові зобов'язання» емітента з пристрою одного власника на пристрій іншого власника.

На заході існує наступна класифікація платіжних систем:

а) Системи на базі пластикових карт (based-card).

б) Системи на основі мереж (network-based).

Або розширена класифікація, яка в даній роботі прийнята для розгляду як найбільш оптимальна:

а) Платіжні системи на основі пластикових карт.

б) Системи віддаленого банківського обслуговування.

в) Електронні цифрові платіжні системи.

Електронний банкінг або on-line банкінг - подання банківських продуктів на відстані поза офісом банків без безпосереднього контакту зі співробітниками банку. У глосарії: керування банківськими рахунками за допомогою телефону (телебанкінг), за допомогою персонального комп'ютера й Інтернету – Інтернет-банкінг, з використанням мобільних обладнань – мобільний банкінг. Усі ці системи використовують системи класу банк-клієнт, які призначені для розрахунково-касового обслуговування клієнтів і обміну інформацією між ними й банком. У розрізі даних систем виділяють також домашні банки – це самостійна форма надання банківських послуг, що дає можливість вести багато банківських операцій з використанням сучасної електронної техніки з віддаленого робочого місця. У цьому випадку віддаленим робочим місцем може бути контора, фірма, магазин і т.д. Для ведення банківських операцій у

рамках даної структури необхідно укласти з банком спеціальний договір. Користувач самостійно здобуває необхідне встаткування. Також необхідно одержати від банку необхідне програмне забезпечення. Банк гарантує технічну й методичну підтримку, відновлення програмного забезпечення й можливість консультацій і рекомендацій. Для ведення операцій власник використовує секретний ключ, який уводить при підключенні до банківського комп'ютера, а також ключ необхідної йому операції.

Телебанкінг дає можливість клієнтові одержувати різну довідкову інформацію в мовному й факсимільному виді, а також проводити активні операції зі своїми рахунками. У даній системі банківські операції виконують за допомогою інтерактивного діалогу системи й клієнта. До даної системи можна підключити систему голосова пошта й факсимільна пошта. До гідностей даної системи відноситься – обробка платежів в автоматизованому режимі, до недоліків – інформація про платежі передається операторам – операціоністам [2].

Інтернет-банкінг – надання банківських послуг за допомогою публічних мереж зв'язку за допомогою спеціального програмного апаратного забезпечення. Інтернет-Банкінг являє собою сукупність баз даних програмних і мовних засобів, призначених для нагромадження даних у банківській структурі. Дана форма ведення не відрізняється від класичної.

Існує 3 категорії Інтернет-банкінга:

- а) призначені для надання інформації про рахунок клієнта, наприклад, Інтернет-банк express;
- б) дозволяють здійснювати віддалене керування рахунками – міжбанківські перекази, оплата комунальних послуг і покупка-продаж безготівкової валюти;
- в) системи, що дозволяють клієнтові одержати в режимі on-line практично весь комплекс Інтернет-послуг.

Мобільний банкінг – керування банківським рахунком за допомогою стільникового телефону або портативного комп'ютера з використанням

технологій бездротового доступу. Дана структура дозволяє цілодобово контролювати рух коштів за допомогою повідомлень на телефон.

Висновки до розділу 1

У цьому розділі обґрунтовується актуальність і широке застосування електронної комерції в усіх галузях економіки держави. Також вказується важливість залучення комплексного підходу до розробки системи захисту проведення операцій над електронними коштами, тому що не відповідність вище зазначеному принципу захисту може призвести до великих фінансових втрат як звичайних громадян так і держави в цілому.

2 АНАЛІЗ ПОГРОЗ БЕЗПЕКИ Й КОМПЛЕКСНИЙ ПІДХІД ДО СТВОРЕННЯ СИСТЕМИ ЗАХИСТУ ПЛАТІЖНОГО ШЛЮЗУ В МЕРЕЖІ INTERNET

2.1 Платіжний шлюз. Схеми мережної взаємодії платіжного шлюзу з іншими вузлами при проведенні платіжних транзакцій

Платіжний шлюз (від англ. Payment Gateway), являє собою комплекси програмно-апаратного забезпечення, розробку й підтримку яких здійснює платіжна система. Апаратно-програмне забезпечення платіжного шлюзу ідентично з апаратно-програмним забезпеченням процесінгового центра банку. Процесінговий центр - це високотехнологічна автоматизована система обробки платежів по банківських картах у сфері електронної комерції (e-commerce). Основне завдання процесінгового центру – надати Інтернет-магазинам можливість ухвалювати платежі по банківських картах. Крім того процесінговий центр координує розрахунки між банком-емітентом карти, банком-еквайером (здійснюючим авторизацію транзакцій), торговельною крапкою й власником банківської карти. Visa/Mastercard пред'являють до цих центрів досить тверді вимоги безпеки (стандарт PCI DSS). Не все банки мають можливість ухвалювати платежі по пластикових картах в Інтернеті. Ті, які це роблять, називаються банками-еквайерами. Вони звичайно мають власні процесінгові центри.

На рис. 2.1 наведена схема алгоритму обміну даними при іІнтернет-еквайрингу.

8) Залежно від результату операції Інтернет-Магазин робить продаж або анулює замовлення.

9) Процесор направляє кліринговий файл для проведення розрахунків у Розрахунковий банк.

10) Розрахунковий банк переводить відшкодування по зроблених операціях на рахунок Інтернет-Магазину.

11) Напрямок підсумкового Акту за результатами звітного періоду.

2.2 Класифікація видів інформації, які обробляються у платіжному шлюзі

Згідно з вимогами міжнародних платіжних систем вимоги стандарту PCI DSS поширюються на все компоненти інформаційної інфраструктури, що обробляють, зберігають або передавальні дані про власників карт. Область аудита – це сукупність компонентів інформаційної інфраструктури, включених у процес оцінки відповідності PCI DSS у рамках виконання ISA- або QSA-Аудита або заповнення аркуша самооцінки SAQ.

У більшості випадків область аудита збігається з областю застосовності PCI DSS.

Схема інфраструктури банку наведена в додатку А.

Інформація щодо діяльності й фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта й взаємин з ним або третім особам при наданні послуг банку, є банківською таємницею. Оскільки ця ж інформація проходить і через платіжні шлюзи при здійсненні взаєморозрахунків між клієнтів і Інтернет-магазином, то до її захисту висуваються такі ж вимоги на стороні платіжного шлюзу як і на стороні банку.

Банківською таємницею, зокрема, є:

1) відомості про банківські рахунки клієнтів, у тому числі кореспондентських рахунках банків у Національному банку України;

2) операції, які були проведені на користь або з доручення клієнта, здійснені їм угоди;

- 3) фінансово-економічний стан клієнтів;
- 4) системи охорони банку й клієнтів;
- 5) інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрямках діяльності;
- 6) відомості щодо комерційної діяльності клієнтів або комерційної таємниці, будь-якого проекту, винаходів, зразків продукції й інша комерційна інформація;
- 7) інформація щодо звітності по окремому банкові, за виключенням тієї, яка підлягає опублікуванню;
- 8) кодів, які використовуються банками для захисту інформації.

В АС банку й платіжних шлюзах обробляється наступна інформація (з "ISO 7812/7816 Numbers and the Domain Name System (DNS)"), крім тієї, яка ставиться до банківської таємниці:

- а) Primary Account Number (PAN) – 19-значний номер, який видавлений або закодований у пластикову картку і який ідентифікує рахунок власника картки;
 - 1 цифра - ідентифікатор індустрії пластикової картки (4,5 для банківської й фінансової сфери);
 - 1-6 цифри – ідентифікатор емітенту (VISA: 4xxxxx, Mastercard: 51xxxx-55xxxx);
 - 7 – (N-1) цифри – номер акаунту власника картки.

Згідно стандарту безпеки PA-DSS v2, вимога 2.2 захисту потребують 7 - (N-4) цифри;

 - N цифра – символ перевірки контрольної суми за алгоритмом Луна.
- б) Cardholder Name – ім'я й прізвище власника карти;
- в) Service Code – код відповіді платіжного доповненню на запит користувача;
- г) Expiration date – строк придатності карти;
- д) Full Magnetic Stripe Data (TRACK) – дата з магнітної стрічки (у загальному випадку там зберігається CVC1 (card validation code, Mastercard) або

CVV1(card verification value, Visa) – код безпеки, необхідний для того, щоб переконатися, що картка була створена банком-емітентом);

е) CVC2/CVV2/CID – 3-х або 4-х значний код безпеки, потрібний для secure card not present transactions, тобто для віддалених транзакцій через Інтернет, надрукований на картці;

- "CID" (card identification number) Discover;
- "CVC" (card validation code) Mastercard;
- "CVV" (card verification value) Visa.

ж) PIN/PIN Block – PIN код (ідентифікаційний номер) картки.

Таблиця 2.1 - Транзакції, у яких використовуються вище відзначена інформація

Категорія транзакції	Вид	Правила зберігання
Дані про власників карт (ДБК)	PAN	При зберіганні слід застосовувати один з методів захисту згідно з вимогою 3.4 стандарту PCI DSS
	CHNAME	Дозволяється зберігати
	EXPDATE	
	SCODE	
Критичні автентифікаційні дані (КАД)	TRACK	Забороняється зберігати після авторизації транзакції, навіть у зашифрованому виді
	CVV2/CVC2/CID	
	PIN і PINBLOCK	

Отже, уся інформація, яка циркулює в АС банку й платіжному шлюзі є інформацією з обмеженим доступом.

Головний об'єкт захисту:

- 1) TRACK + CVC2/CVV2/CID + (PIN і PINBLOCK) ;
- 2) PAN (7-12).

Відповідно вона має наступні правові режими:

Таблиця 2.2 - Правові режими

Інформація	Правовий режим
PAN	перші 6 і останні 4 цифри – конфіденційні інші цифри - таємні
Cardholder Name	конфіденційна
Service Code	конфіденційна
Expiration date	конфіденційна
TRACK + CVC2/CVV2/CID + (PIN і PINBLOCK)	таємна

Схема руху потоків ДБК між учасниками процесу еквайрингу наведена в Додатку Б.

Інформаційні ресурси банку або платіжного шлюзу - це документи, що існують у вигляді файлів на різних носіях інформації або записів в автоматизованих інформаційних і облікових системах(в автоматизованій банківській системі й інших інформаційних і облікових системах, базах даних, системах електронного документообігу, бібліотеках, архівах), інформаційні технології збору, обробки, нагромадження, зберігання, пошуку й передачі інформації, а також засобу забезпечення автоматизованих інформаційних і облікових систем і їх технологій, включаючи програмні і технічні засоби(програми для електронних обчислювальних машин; засобу обчислювальної техніки й зв'язки; схеми електронного документообігу і їх опису, інша експлуатаційна й супровідна документація), використовувані або створювані при проектуванні інформаційних систем і такі, які забезпечують їхню експлуатацію [28].

Схема мережі платіжного шлюзу й область застосовності PCI DSS, а

також схема руху потоків ДВК між платіжним шлюзом і іншими учасниками процесу еквайрингу наведені в Додатку В.

2.3 Апаратно-програмні ресурси платіжного шлюзу

Серверні ресурси включають:

Файловий сервер (file server) - вузол обчислювальної мережі, яка реалізовує початковий рівень архітектури клієнт-сервер. Звичайно файловий сервер працює під керуванням серверної операційної системи*. Основним завданням файл-серверів представляється надійне зберігання й швидкий доступ до даних, які перебувають на загальному дисковому просторі, при якому забезпечується керування доступом до файлів і базам даним. Для досягнення повного збереження даних, у серверах використовуються RAID- контролери з технологіями зеркалювання даних, для корекції помилок, використовується пам'ять FB DIMM ECC, реалізоване резервування харчування з технологією HOT - SWAP, що дозволяє вберегти сервер від зупинки навіть при виході з ладу одного блоку живлення.

Сервер баз даних(database server) обслуговує бази даних і забезпечує цілісність і збереження даних при їхнім зберіганні, а також операціях введення-виведення при доступі клієнта до інформації. Сервер бази даних - один із ключових компонентів в архітектурі обчислювальної мережі типу " клієнт-сервер", у якій призначений для користувача інтерфейс розташовуються на менш потужній машині-клієнті, а функції Систему Керування Базами Даних(СУБД) розміщені на потужному сервері. Сервер баз даних працює під керуванням серверної операційної системи* і одержує клієнтські запити мовою SQL.

Поштовий сервер (post server, mail server, поштовик) призначений для роботи й обслуговування поштових баз і сервісів організації. Під поняттям "Поштовий сервер" розуміють як апаратний сервер, так і поштове серверне

програмне забезпечення. Апаратний поштовий сервер. Завдання поштового сервера - забезпечення роботи й надійне зберігання поштової бази, тому по функціоналу й комплектації апаратний поштовий сервер - це гібрид сервера баз даних і файлового сервера. Поштові сервери або Інтернет-сервери розроблені з урахуванням основних вимог: швидкості обробки даних, надійності й масштабованості. Поштовий сервер. Програмне забезпечення. Сервер електронної пошти, mail- сервер, поштовий сервер це назви для комп'ютерного програмного забезпечення, завдання якого передавати електронну пошту від одного комп'ютера до іншого. У цей час комунікаційні програми працюють у тісному співробітництві з антивірусними програмами, засобами боротьби зі спамом і іншими корисними для користувача доповненнями.

Веб-сервер - це сервер, що ухвалює HTTP- запити від клієнтів, звичайно веб-браузерів, і що видає їм HTTP- відповіді, звичайно разом з HTML- сторінкою, зображенням, файлом, медіа-потокком або іншими даними. Веб називають як програмне забезпечення, яке виконує функції веб, так і безпосередньо комп'ютер, на якому це програмне забезпечення працює. Клієнт, яким звичайно є веб-браузер, передає веб запити на одержання ресурсів, позначених URL- адресами. Ресурси - це HTML- сторінки, зображення, файли, медіа-потоки або інші дані, які потрібні клієнтові. У відповідь веб передає клієнтові запрошені дані. Цей обмін відбувається по протоколу HTTP. Веб може мати різні додаткові функції, наприклад:

- а) автоматизація роботи веб сторінок;
- б) ведення журналу обігу користувачів до ресурсів;
- в) автентифікація й авторизація користувачів;
- г) підтримка динамічно генеруючих сторінок;
- Г) підтримка HTTPS для захищених сполук із клієнтами.

Прінт-Сервер (print server) - програмне забезпечення або обладнання, що дозволяє групі користувачів дротових і бездротових мереж спільно використовувати принтер банку. Має високошвидкісний порт USB 2.0, LPT або COM порти для підключення принтера. Як правило, оснащене

інтерфейсом 10/100BASE Ethernet і часто - високошвидкісним інтерфейсом бездротових мереж 802.11g. Підтримуючи безліч мережних операційних систем, надає високий рівень гнучкості й продуктивності процесу печатки. Також прінт-сервером може виступати комп'ютер у мережі, з одним або більш відкритими в загальний доступ принтерами.

Gsm-Сервер- обладнання є повнофункціональним сервером IP- телефонії із вбудованим GSM- шлюзом [30]

Таблиця 2.3 - Співвідношення серверів і інформації, що на них зберігається

	Назва сервера	Інформація, яка зберігається
	Сервер БД	відомості про банківські рахунки клієнтів; операції, які були проведені на користь або з доручення клієнта, здійснені їм угоди; фінансово-економічний стан клієнтів; інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрямках діяльності; відомості щодо комерційної діяльності клієнтів або комерційної таємниці, будь-якого проекту, винаходів, зразків продукції й інша комерційна інформація; інформація щодо звітності по окремому банкові; PAN, Cardholder Name, Service Code, Expiration date
	Файловий сервер	системи охорони банку й клієнтів; інформація щодо звітності по окремому банкові, за винятком тієї, яка підлягає опублікуванню
	Веб-сервер	інформація, яка підлягає опублікуванню
	GSM-сервер	смс-коди, які використовуються банками для активації проведення платежів

2.4 Модель погроз безпеки платіжного шлюзу в сети Internet

Відповідно вищезгаданої таблиці визначили, що найбільш уразливим до погроз на критерії захищеності є сервер БД.

Керування ризиками банку.

Ціль керування ризиками – моніторинг і контроль рівня й концентрації ризиків, які виникають у зв'язку з діяльністю Банку. Основні категорії ризику, що властиві бізнесу банку – це кредитний ризик, ринковий ризик, географічний ризик, ризик ліквідності, операційний ризик і юридичний ризик. Політика банку в області керування ризиками дозволяє виявляти й аналізувати перераховані вище типи ризиків, установлювати прийнятні ліміти й проводити відповідний моніторинг на постійній основі, опираючись на передові адміністративні й інформаційні системи.

Для визначення погроз розглянемо тільки операційний ризик. Операційний ризик – ризик фінансових втрат, пов'язаних з управлінськими помилками, шахрайством, неефективністю наданих послуг, неможливістю своєчасного вживання банком заходів щодо усунення погроз інтересам банку, зокрема, з боку його співробітників, які зловживають своїми повноваженнями або тих, хто веде свою діяльність із порушенням етичних норм і невинуватено високими ризиками, які приводять до послаблення позицій банку на ринку або до його банкрутства. Інші аспекти операційного ризику – серйозні збої в роботі інформаційно- технологічних систем, а також пожежі й інші стихійні явища.

Операційний ризик банк класифікує як:

- 1) ризик збитку, який виникає через різноманітні людські помилки або збої технічного встаткування;
- 2) ризик збитку, який виникає через непередбачені платежі – платіжний ризик;
- 3) технологічний ризик;
- 4) адміністративний або правовий ризик.

Для контролю й зниження рівня операційного ризику застосовуються

наступні методи:

- 1) внутрішній контроль;
- 2) аудит;
- 3) повідомлення керівництва про виникнення операційних ризиків для прийняття розв'язки по його хешуванню;
- 4) формування загальних резервів.

Модель погроз призначена для виявлення актуальних погроз інформаційної безпеки серверного простору з метою наступної розробки вимог, які визначають організаційно режимні й технічні заходи щодо захисту інформації обмеженого доступу, оброблюваної в типовій схемі організації серверного простору, а також переданої технічними засобами по незахищених каналах передачі даних.

Для формування моделі погроз оберемо документ OWASP Top 10 Application Security Risks.

Open Web Application Security Project (OWASP) – відкрита асоціація, ціль якої сприяння іншим організаціям і компаніям у розробці й підтримці програмних продуктів, яким можна довіряти з погляду безпеки. Ключове місце серед них займає OWASP Top 10 Security Risks – документ, у якому перераховано 10 найпоширеніших атак і уразливостей веб-Пз і безліч посилок спрямованих на допомогу в їхнім усуненні.

OWASP Top 10 Application Security Risks включає наступні вразливості й види атак:

A1 –Injection (such as SQL, OS, and LDAP injection) – атака програмного забезпечення шляхом уведенню в поле для користувача введенню SQL запиту, команд операційної системи, LDAP-Команд, спрямованих на поразку самої ОС, бази даних, веб-інформацію, яка зберігається й таке інше.

A2 –Cross-Site Scripting (XSS) – атака реалізована шляхом передачі на сторону клієнта програмного коду зломисника (Javascript, ACTIVEX, Java, Flash) спрямованого на порушення конфіденційності інформації користувача або порушення цілісності інформації у веб-Пз.

A3 –Broken Authentication and Session Management.

Session Management (Session Fixation) - перехоплення або генерація ID HTTP сесії авторизованого користувача

Broken Authentication (Insufficient Authentication) – вразливість, яка дозволяє порушникові здійснити НСД до ресурсів веб-Пз, що потребує автентифікації.

A4 –Insecure Direct Object References – вразливість, викликана безпосереднім посиланням на об'єкт по його імені.

A5 –Cross-Site Request Forgery (CSRF) – атака, яка змушує користувача посилати http запит на сторонній ресурс. У такий спосіб можливе перехоплення конфіденційної інформації користувача або додатки іншого виду атаки, наприклад, XSS.

A6 –Security Misconfiguration – вразливість, викликана некоректним настроюванням прав доступу користувачів веб-Пз, бази даних, серверу й таке інше. Часто є результатом того, що програмний код, який використовувався для тестування, не був віддалений.

A7 –Insecure Cryptographic Storage - вразливість, яка виникає в результаті використання алгоритмів недостатньої криптостійкості або доступності зловмисникові виклику функцій дешифрації з інтерфейсу веб-Пз.

A8 -Failure to Restrict URL Access – вразливість, що дозволяє здійснити доступ ресурсів веб-Пз в обхід автентифікації й авторизації

A9 -Insufficient Transport Layer Protection - вразливість, викликана недостатнім захистом інформації на транспортному рівні передачі даних. Незахищений прикрашений візерунком трафік може бути перехоплений за допомогою спеціальних програм «сніферів».

A10 –Unvalidatedredirects and Forwards – вразливість, яка дозволяє зловмисникові стирати направити користувача на задану їм посилання.

Таблиця 2.4 - Погрози, які впливають на критерії захищеності інформації

Потенційні погрози інформації	Критерії захищеності інформації			
	К	Ц	Д	Н
погрози об'єктивної природи				
стихійні явища (пожежа, аварії)		+	+	
збої й відмови системи електроживлення		+	+	
збої й відмови обчислювальної технік		+	+	
збої й відмови програмного забезпечення		+	+	
Потенційні погрози інформації	Критерії захищеності інформації			
	К	Ц	Д	Н
збої, відмови й ушкодження носіїв інформації		+	+	
погрози суб'єктивної природи				
Помилки:				
помилки адміністраторів (неправильне налаштування й адміністрування системи захисту, операційної системи; неправомірне відключення засобів захисту).	+	+	+	
порушення технології обробки, введення й виведення інформації, роботи із МНІ (з ІЗОД, резервними й архівними копіями).	+	+	+	
Несанкціоноване перехоплення інформації	+	+	+	+
несанкціоноване підключення до технічних засобів	+			
Порушення нормальних режимів роботи:				
поразка програмного забезпечення комп'ютерними вірусами	+	+	+	+

Продовження таблиці 2.4

втрата засобів розмежування доступу (паролів) і резервних копій	+	+	+	+
несанкціоноване внесення змін у технічні засоби, у програмне забезпечення, у компоненти інф. забезпечення, і таке інше		+	+	+
використання недозволеного ПЗ або модифікація компонентів програмного й інформаційного забезпечення		+	+	+
ушкодження носіїв інформації			+	
Зовнішні погрози:				
несанкціоноване перехоплення інформації за рахунок побічного електромагнітного випромінювання й наведень	+			
A1 – Injection (such as SQL, OS, and LDAP injection)	+	+	+	+
A2 – Cross-Site Scripting (XSS)	+			
A–Broken Authentication and Session Management	+			
A4 –Insecure Direct Object References	+	+	+	+
A5 –Cross-Site Request Forgery (CSRF)	+	+	+	
A6 –Security Misconfiguration	+	+	+	+
A7 –Insecure Cryptographic Storage	+	+		
A8 -Failure to Restrict URL Access	+		+	
A9 -Insufficient Transport Layer Protection	+	+	+	
A10 –Unvalidatedredirects and Forwards	+		+	

Джерела погроз

Джерело погрози безпеки серверного простору - це суб'єкт, матеріальний

об'єкт або фізичне явище, яке створює погрозу безпеки серверного простору, у якому захищається інформації.

Джерела, що діляться на суб'єктивні (залежать від дій персоналу й, в основному, усуваються організаційними заходами й програмно-апаратними засобами) і об'єктивних (залежать від особливостей побудови й технічних характеристик устаткування, застосовуваного в серверному просторі).

До суб'єктивних джерел погроз ставляться:

а) зовнішні суб'єктивні джерела погроз - діяльність зовнішніх порушників, спрямована на здійснення НСД до інформації, яка захищається, серверним, зокрема, за допомогою:

1) внесення апаратних закладок у технічні засоби, передбачувані до додатка в серверному просторі;

2) віддаленого впровадження шкідливого ПЗ у програмні засоби серверного простору;

3) перехоплення інформації, яка захищається, у каналах передачі даних, незахищених від НСД організаційно технічними заходами;

4) добір інформації для автентифікації користувачів серверного простору;

б) внутрішні суб'єктивні джерела погроз безпеки інформації - дії осіб, які мають доступ до роботи зі штатними засобами серверного простору й (або) допуск у межах контрольованої зони.

До об'єктивних джерел відносяться:

1) стихійні джерела потенційних погроз інформаційної безпеки, які є зовнішніми щодо серверного простору й під якими розуміються в першу чергу природні явища (пожежі, землетруси, повені й таке інше);

2) джерела, пов'язані з технічними засобами ІС, які є внутрішніми щодо серверного простору й містять у собі:

3) передачу інформації з ведучих і волоконо-оптичним каналам передачі даних;

в) дефекти, збої й відмови технічних засобів серверного простору (засобів обробки інформації й програмно-технічних засобів захисту інформації

серверного простору);

г) відмови й збої програмних засобів обробки інформації.

Модель погроз для серверного простору

Таблиця 2.5 - Усі погрози між мережною взаємодією для серверу БД

№	Назва погрози	Критерії захищеності інформації			
		К	Ц	Д	Н
1	модифікація, ознайомлення, знищення, блокування інформації, яка захищається, при передачі по каналах зв'язку.	+	+	+	
2	модифікація, знищення, блокування програмних засобів інформаційної системи, програмних засобів захисту, зміна їх характеристик, що ведуть в електронному виді реєстраційних протоколів.		+	+	
3	несанкціоноване відключення засобів захисту інформації;			+	+
4	проведення атак, заснованих на використанні вразливостей засобів, взаємодіючих із засобами захисту інформації й здатних вплинути на їхнє функціонування;			+	+
5	добір інформації для автентифікації користувачів (адміністраторів) серверного простору;	+			
6	аналіз мережного трафіка з перехопленням переданої із системи й прийнятої в систему із зовнішніх мереж інформації;	+			
7	модифікація інформації, яка захищається, при її передачі по каналах зв'язку;		+		

Продовження таблиці 2.5

8	розголошення інформації шляхом передачі її по електронній пошті, системам обміну швидкими повідомленнями;	+			
9	впровадження по мережі шкідливих програм;		+	+	+
10	створення позаштатних режимів роботи програмних (програмно-апаратних) засобів за рахунок навмисних змін службових даних;		+	+	+
11	створення позаштатних режимів роботи програмних (програмно-апаратних) засобів за рахунок навмисних змін переданої інформації;		+	+	+
12	одержання доступу (проникнення) в операційне середовище АРМ із використанням штатного програмного забезпечення й протоколів мережної взаємодії (засобів операційної системи або прикладних програм загального додатка);		+	+	+
13	відмова в обслуговуванні			+	+
14	нав'язування неправильного маршруту шляхом несанкціонованої зміни адресний^-адресних-адресні-маршрутно-адресних даних усередині мережі;			+	
15	нав'язування неправильного маршруту шляхом несанкціонованої зміни адресних-маршрутно-адресних даних у зовнішніх мережах;			+	
16	перегляд інформації на дисплеї особами, не допущеними до обробки даних з використанням технічних (у таким чином оптичних) засобів; підміна довіреного об'єкта;	+			

Продовження таблиці 2.5

17	впровадження неправильного об'єкта як у систему, так і в зовнішніх мережах;			+	+
18	перегляд інформації на дисплеї особами, не допущеними до обробки даних з використанням технічних (у таким чином оптичних) засобів;		+		
19	сканування, спрямоване на виявлення типу або типів використовуваних операційних систем, мережних адрес робочих станцій системи, топології мережі, відкритих портів і служб, відкритих сполук і т.д.;	+			
20	A1 –Injection (such as SQL, OS, and LDAP injection);	+	+	+	+
21	A3–Broken Authentication and Session Management;	+			
22	A5 –Cross-Site Request Forgery (CSRF);	+	+	+	
23	A6 –Security Misconfiguration;	+	+	+	+
24	A7 –Insecure Cryptographic Storage;	+	+		
25	A8 -Failure to Restrict URL Access;	+		+	
26	A9 -Insufficient Transport Layer Protection;	+	+	+	
27	A10 –Unvalidatedredirects and Forwards.	+		+	

Таблиця 2.6 - Імовірності виникнення погроз інформаційного об'єкта

Імовірність виникнення	Значення	Опис
Дуже низька	0,01-0,2	Малоймовірно
Низька	0,21-0,4	1 раз в 3 року
Середня	0,41-0,6	1 раз у рік
Висока	0,61-0,8	Кілька раз у році
Дуже висока	0,81-1	Раз на місяць і частіше

Таблиця 2.7 - Класифікація збитку щодо інформаційного об'єкта

Потенційні збитки	Значення	Визначення з погляду впливу на репутацію банку
Низький рівень	1	Незначний вплив на репутацію банку
Середній рівень	2	Вплив на репутацію компанії середньої значимості
Високий рівень	5	Істотний вплив на репутацію компанії
Дуже високий рівень	10	Банкрутство компанії

Таблиця 2.8 - Оцінка основних ризиків для серверу БД

№	Імовірність	Збитки	Ризик
1	0,8	5	4
2	0,8	5	4
3	0,4	1	0,4
4	0,6	2	1,2
5	0,6	2	1,2
6	0,4	1	0,4
7	0,8	5	4
8	0,4	1	0,4
9	0,4	1	0,4
10	0,4	1	0,4
11	0,4	1	0,4
12	0,4	1	0,4
13	0,8	5	4
14	0,7	2	1,4
15	0,7	2	1,4
16	0,6	2	1,2

Продовження таблиці 2.8

17	0,4	1	0,4
18	0,4	1	0,4
19	0,4	1	0,4
20	0,8	5	4
21	0,4	1	0,4
22	0,4	1	0,4
23	0,8	5	4
24	0,5	2	1
25	0,6	2	1,2
26	0,4	1	0,4
27	0,5	2	1

Таблиця 2.9 - Загальна таблиця ймовірностей і збитку

Ймовірність Збитки	Дуже низька	Низька	Середня	Висока	Дуже висока
Низький	0,01-0,2	0,21-0,4	0,41-0,6	0,61-0,8	0,81-1
Середній	0,01-0,4	0,41-0,8	0,81-1,2	1,21-1,6	1,61-2
Високий	0,01-1	1,01-2	2,01-3	3,01-4	4,01-5
Дуже високий	0,01-2	2,01-4	4,01-6	6,01-8	8,01-10

Таблиця 2.10 - Кольорове маркування

Кольорове маркування	Діапазон значень ризичу	Розв'язок про наступну обробку ризику

Продовження таблиці 2.10

Білий	0,01-2	Ризики незначні. Обробка ризиків не потрібно.
Сірий	2,01-10	Ризики значні. Заходу обробки ризиків обов'язкові.

Тепер можна зробити висновок, що підлягають обробці такі ризики: ризик модифікації, ознайомлення, знищення, блокування інформації, яка захищається, при передачі по каналах зв'язку; ризик модифікації, знищення, блокування програмних засобів інформаційної системи, програмних засобів захисту, зміна їх характеристик, що ведуть в електронному виді реєстраційних протоколів; ризик модифікації інформації, яка захищається, при її передачі по каналах зв'язку; ризик відмови в обслуговуванні; ризик уведенню в поле для користувача введенню SQL запиту, команд операційної системи, LDAP-Команд, спрямованих на поразку самої ОС, бази даних, веб-інформації, яка зберігається й таке інше; ризик, викликаний некоректним налаштуванням прав доступу користувачів веб-Пз, бази даних, серверу й таке інше. Часто це є результатом того, що програмний код, який використовувався для тестування, не був віддалений

2.5 Модель порушника інформаційної безпеки платіжного шлюзу в мережі Internet

Модель порушника розробляється для визначення типового переліку погроз інформаційної безпеки .

Модель порушника системи містить припущення про можливості порушника, які він може використовувати для реалізації погроз, а також про обмеження на ці можливості. Погрози (атаки) готуються й проводяться порушником, причому можливість реалізації погрози обумовлена

можливостями порушника, а саме його інформаційними й технічними знаннями.

Опис потенційного порушника інформаційної безпеки

Під порушником розуміється фізична особа, випадково або навмисно здійснююча дії, наслідком яких є порушення безпеки, яка захищається інформації при її обробці в інформаційній системі.

Цілями несанкціонованих дій порушника, здатних привести до здійснення НСД до серверних ресурсів, які захищаються, і порушенню прийнятих для системи характеристик інформаційної безпеки, є:

- 1) порушення цілісності ресурсів, які захищаються;
- 2) порушення конфіденційності ресурсів, які захищаються;
- 3) порушення доступності ресурсів, які захищаються;
- 4) створення умов для наступного проведення атак.

Можливими напрямками несанкціонованих дій порушника в тому числі є:

1) доступ до інформації, яка захищається, з метою порушення її конфіденційності (розкрадання, ознайомлення, перехоплення);

2) доступ до інформації, яка захищається, з метою порушення її цілісності (модифікація даних);

3) доступ до технічних і програмних засобів інформаційної безпеки з метою постійного або тимчасового порушення доступності, яка захищається інформації для легального користувача;

4) доступ до технічних і програмних засобів інформаційної системи з метою внесення в них несанкціонованих змін, які створюють умови для проведення атак;

5) доступ до засобів захисту інформації з метою зміни їх конфігурації.

Доступ до інформації, яка захищається, порушник може одержати шляхом:

1) подолання (обходу) засобів і системи захисту інформації, систем контролю доступу;

2) використання спеціальних програмних засобів (у тому числі

шкідливого ПЗ) або вразливостей легально використовуваного ПЗ;

3) використання спеціалізованих засобів знімання (одержання) інформації з технічних каналів;

4) використання засобів спеціальних впливів;

5) впровадження апаратного станового встаткування.

Обладнання закладів, як правило, активуються шляхом програмно математичних впливів, реалізованих при безпосередньому фізичному доступі до системи, або шляхом безпосереднього мережного впливу.

Типи порушників інформаційної безпеки

Порушники інформаційної безпеки ІС можуть бути наступних типів:

1) зовнішні порушники;

2) внутрішні порушники;

Залежно від категорії оброблюваних персональних даних змінюються категорії осіб, зацікавлених у несанкціонованому одержанні інформації обмеженого доступу, тобто змінюються можливості потенційного порушника інформаційної безпеки.

Зовнішній порушник може мати наступну інформацію й даними про систему:

1) знаннями функціональних особливостей системи;

2) високим рівнем знань в області технічних засобів;

3) відомостями про засоби захисту інформації;

4) даними про вразливість інформаційної безпеки, включаючи дані про можливості технічних засобів інформаційної системи;

5) інформацією про можливі й існуючі способи (методи) реалізації атак;

6) знаннями в області програмування й обчислювальної техніки.

Можливості внутрішнього порушника інформаційної системи суттєво залежать від діючих у межах системи обмежувальних факторів, основними з яких є організаційні, режимні, інженерно-технічні й інші заходи, спрямовані на:

1) запобігання й припинення несанкціонованих дій осіб, які мають доступ до системи;

- 2) добір і розміщення кадрів для роботи в системі;
- 3) організацію контролю й розмежування доступу фізичних осіб у системі, а також до штатних засобів інформаційної системи й у приміщення, у яких вони розташовані;
- 4) контроль над порядком проведення робіт;
- 5) контроль над дотриманням вимог документації, яка визначає політику безпеки інформаційної системи (у тому числі, контроль над виконанням режимних заходів, які регламентують порядок обігу з інформацією, оброблюваної в системі).

Виходячи із прав доступу осіб до серверних ресурсів, потенційних внутрішніх порушників можна розділити на наступні категорії:

Категорія I : зареєстрований користувач із повноваженнями адміністратора системи (системного адміністратора, адміністратора безпеки). Особи даної категорії є довіреними (у силу реалізованих організаційних, режимних і кадрових заходів), і як порушники інформаційної безпеки не розглядаються. Адміністратори інформаційної системи проходять інструктаж з питань обробки інформації, допускаються до роботи із серверними ресурсами після перевірки знань відповідних посадових інструкцій, у зв'язку із чим розгляд їх помилкових дій, здатних привести до порушення інформаційної безпеки системи, у рамках даної моделі не проводиться.

Категорія II: зареєстрований користувач ресурсів АС. Порушник категорії II може володіти наступною інформацією й даними про систему:

- 1) атрибутами, які забезпечують доступ до ресурсів (наприклад, паролем, легальним іменем доступу);
- 2) відомостями про структуру, функції, принципи, механізми дії й правила роботи технічних засобів і засобів захисту інформації в об'ємі експлуатаційної документації;
- 3) знаннями функціональних особливостей інформаційної системи;
- 4) відомостями про серверні ресурси: порядок і правила створення, зберігання й передачі інформації, формати повідомлень, структура й

властивості інформаційних потоків;

5) даними про вразливість інформаційної системи, включаючи дані про можливості технічних засобів;

6) відомостями про можливих для системи каналах атак;

7) інформацією про способи атак.

Порушник категорії II володіє наступними засобами доступу до ресурсів:

1) штатними засобами (комп'ютером, що підключаються безпосередньо до системи);

2) наявними у вільному продажі програмними засобами прослуховування каналів передачі даних;

3) наявними у вільному продажі програмними засобами модифікації даних при передачі по каналах зв'язку;

4) загальнодоступними комп'ютерними вірусами;

5) загальнодоступним програмним забезпеченням, призначеним для підготовки й здійснення додатка програмних засобів захованого інформаційного впливу.

Категорія III: особи, які мають санкціонований доступ до приміщень але, що не мають санкціонованого доступу до ресурсів інформаційної системи.

Порушник категорії III може володіти наступною інформацією й даними про систему:

1) знаннями про "іменах" (логіні) зареєстрованих користувачів;

2) знаннями функціональних особливостей системи;

3) будь-якими фрагментами інформації про топологію мережі (комунікаційної частини підмережі) і про використовувані в системі комунікаційні протоколи і їх сервісах;

4) даними про вразливість системи, включаючи дані про можливості технічних і програмних засобів;

5) відомостями про можливих для системи каналах атак;

6) інформацією про способи атак.

Порушник категорії III має наступні засоби доступу до серверних

ресурсів:

- 1) залишеними без огляду штатними засобами;
- 2) наявними у вільному продажі програмними засобами прослуховування каналів передачі даних;
- 3) наявними у вільному продажі програмними засобами модифікації даних при їхній передачі по каналах зв'язку;
- 4) загальнодоступними комп'ютерними вірусами;
- 5) загальнодоступним програмним забезпеченням, призначеним для підготовки й здійснення додатка програмних засобів захованого інформаційного впливу.

Категорія IV: співробітники підрозділів (організацій), які виконують розробку прикладного програмного забезпечення, ремонт і поновлення працездатності інформаційної системи.

Особи категорії IV:

- 1) мають інформацію про програми обробки інформації в системі, а також про реалізованих у даних програмах алгоритмах;
- 2) мають можливості внесення помилок (у тому числі шкідливого ПЗ) в інформаційній системі на стадії розробки й супроводу;
- 3) можуть мати у своєму розпорядженні будь-які фрагменти інформації про топологію локальної обчислювальної мережі, технічних засобах обробки й засобах захисту інформації, застосовуваних у системі.

У нашій АС платіжного шлюзу ми будемо допускати, що можливі два класів порушників, що відносяться до рівнів 1 і 3 відповідно.

До першого рівня відноситься «Кардер».

Кардер (англ. Carder) - це людей, яка краде номери банківських, кредитних карток, гроші із цих карток.

Ціль: Одержання конфіденційної й таємної інформації, яка обробляється в АС платіжного шлюзу.

- 1) порушник має перший рівень;
- 2) за рівнем знань про АС: володіють високим рівнем знань у галузі

обчислювальної техніки й програмування, проектування й експлуатації АС;

3) за використовуваними методами й способами: використовують винятково агентурні методи одержання відомостей;

4) за місцем здійснення дії: без одержання доступу на контрольовану територію організації (АС).

До третього рівня ставиться «Інсайдер».

Інсайдер — особа (юридична або фізична), яка має доступ до конфіденційної інформації про справи банку завдяки своєму службовому становищу, участі в капіталі банку, сімейним зв'язуванням і має можливість використовувати своє положення у власних інтересах.

Ціль: Одержання конфіденційної й таємної інформації, що пройшла процедуру обробки в АС.

1) порушник має третій рівень;

2) за рівнем наявних знань про наявні АС: мають інформацію про функції й процес роботи механізму дії засобів захисту.;

3) за використовуваними методами й способами: використовують способи й засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження й використання спеціального ПЗ і таке інше).

4) за місцем де проходить здійснення дії: з одержанням доступу до можливих місць нагромадження й потенційного зберігання цінних даних (баз даних, архівів, АРМ відповідних адміністраторів і таке інше).

2.6 Вибір класу й профілю захищеності

При здійсненні створення, процесів впровадженні й розвитку складних, розподільчих і інформаційно-телекомунікаційних систем (ІТС) мається потреба у гнучкому, що тиражуються, якісному формуванні й особливих додатах

гармонізованої сукупності базових складових стандартів і документів нормативного характеру з різними рівнями що мають атрибути, виділення в них певних вимог і конкретних рекомендацій, необхідних для здійснення реалізації заданих у певних функціях ІТС. У зв'язку із цією потребою було виділено, а також сформувалося поняття "профілів" ІТС, у якості базового інструмента виконання функціональної стандартизації. Профіль – це сукупність декількох (або підмножина одного) базових стандартів із чітко певними підмножинами обов'язкових і факультативних можливостей, призначена для реалізації заданої функції або групи функцій. Профіль не може створювати ситуацію при якій буде суперечити використаним у ньому нормативним документам. На базі однієї певної сукупності стандартів базового характеру можуть бути сформовані й також затвердженні різні унікальні профілі для різних проектів ІТС а також областей потенційного застосування застосування.

Визначимо базові за функціями та використанням профілі захищеності в КС, що є базовою складовою АС класу 3 (вимоги що у повній мірі відповідають процесам і типам даних що проходять процедуру обробки у певних платіжних шлюзах), з зростанням рівня вимог до забезпечення якості збереження конфіденційності, цілісності, а також доступності оброблюваної інформації:

$$\begin{aligned}
 3.КЦД.5 = \{ & КД-4, КА-4, ПО-1, КК-2, КВ-4 \\
 & ЦД-4, ЦА-4, ЦВ-2, ЦВ-3 \\
 & ДР-3, ДС-3, ДЗ-3, ДВ-3 \\
 & НР-5, НІ-2, НК-2, АЛЕ-3, НЦ-3, НТ-2, НА-1, НП-1, НВ-2, \\
 & НА-1, НП-1 \}
 \end{aligned}$$

Критерії конфіденційності.

Для того, щоб КС могла пройти процес оцінки на предмет наявності відповідності певним критеріям із сфери конфіденційності, КЗЗ оцінюваної КС повинен виконати надання особливої послуги із проведення захисту виділених об'єктів від потенційного несанкціонованого ознайомлення з наявним у них змістом (компрометації). Конфіденційність має пройти процедуру забезпечення

через такі послуги: конфіденційність довірчого типу, конфіденційність адміністративного типу, використання об'єктів за повторним принципом, аналіз наявності схованих каналів, конфіденційність при проведенні процедури обміну.

Довірча конфіденційність що носить абсолютний характер (КД-4). Даний рівень дозволяє провести забезпечення повного керування наявними потоками інформації у середі КС. Атрибути доступу до наявного користувача, процесу, а також об'єкту повинні містити у собі певну інформацію, яка використовується у межах КЗЗ з метою визначення певних користувачів, а також процесів і пар наявних процесів/користувачів, що можуть бути отриманими від об'єкта. У такий спосіб виконується гарантування, того що інформація що була послана об'єктом який потрібен певному користувачу через виконання процесу авторизації. КЗЗ повинен виконати процес забезпечення високої за вибірковістю керування наявних тем, які авторизовані користувачі можуть одержати інформацію від певного об'єкта чи в іншому випадку здійснити ініціювання процесу. Для системи такого типу можна здійснити побудову повної матриці доступу до користувачів, а також наявних процесів і пар користувач/процес до об'єктів і процесів що мають певний рівень захищеності. Необхідні умови : ДО-1, НІ-1

Абсолютна адміністративна конфіденційність (КА-4). Данна послуга надає дозвіл до адміністраторам чи користувачеві із певним рівнем повноважень здійснювати процес керування та використання певними потоками інформації від об'єктів що мають захищеність до звичайних користувачів без рівня доступу до спеціальної інформації. Рівні цієї послуги, що має ранжування через наявність підстави повноти рівня захисту й вибіркової керування. Політика конфіденційності адміністративного характеру, яка реалізується КЗЗ, повинна бути відноситись до усіх наявних об'єктів у межах КС. КЗЗ повинен здійснювати процедуру розмежування доступу на підставі наявних атрибутів доступу до певного користувача, а також процесу й захищеного об'єкта. Запити на надання зміни у праві доступу

повинні оброблятися через використання КЗЗ у винятковому випадку, якщо вони мають надходити лише від адміністраторів або від користувачів, із певним рівнем доступу до інформації та процесів. КЗЗ повинен надавати можливість усім адміністраторам або користувачам, які мають відповідні до цієї процедури особливі повноваження, для кожного об'єкта який має рівень захищеності шляхом керування приналежністю користувачів, процесів і об'єктів до відповідних доменам визначити конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають доступу до можливості одержувати інформацію через відсутність прав до доступу у використанні певного об'єкта. КЗЗ повинен надавати певну можливість адміністраторам чи певним користувачам, які мають бути забезпечені відповідними за значеннями повноваженнями, для кожного із процесів через здійснення керування до потрібної приналежності користувачів, а також процесів до відповідних доменам провести процедуру визначення конкретних користувачів (і групи користувачів), які мають можливість використання права, а також тих, які не мають цього права на проведення ініціювання процесу. Права доступу до кожного захищеного об'єкта повинні бути встановлюваними в певний момент його створення, або ініціалізації. Як окрема частина політики конфіденційності адміністративного характеру повинні бути представлені певні правила збереження атрибутів доступу об'єктів під час їх експорту й імпорту. Необхідно використання умов: ПО-1, АЛЕ-1, НІ-1.

Повторне використання об'єктів (ПО-1). Політика проведення повторного використання у межах об'єктів, яке реалізується у певній КЗЗ, повинна бути поставлена до у всіх без винятку об'єктів КС. Перш ніж користувач, або процес зможе об'єкт звільнений від іншого користувача, установлені для старого користувача або процесу права доступу до виділеного об'єкта повинні бути скасовані. Перш ніж потрібний користувач або процес зможе бути одержаним у своє розпорядження звільненим від використання іншим користувачем або процесом об'єкт, уся інформація, яка проходить процес утримання у цьому об'єкті, повинна бути недосяжною.

Контроль прихованих каналів (КК-2). Аналіз прихованих каналів проводиться із метою виявлення й здійснення усунення потоків інформації, які існують, але не можуть бути під контролем інших послуг. Рівні вказаної послуги, що мають рівень ранжування на підставі того, що здійснюється виконання чи тільки проведення виявлення, контролю, або перекриття наявних прихованих каналів. Усі сховані канали, які існують у межах апаратного, а також програмного забезпечення, а також у певних програмах ПЗП, повинні пройти процедуру документації.. Для схованих каналів, які можуть використовуватися спільно, повинна бути документуєма сукупна пропускну здатність. КЗЗ повинен здійснювати процедуру із забезпечення реєстрації використання затвердженого підмножини знайдених схованих каналів. Необхідні умови : ПО-1, НР-1, Г-3.

Абсолютна конфіденційність при обміні (КВ-4). Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, яка втримується в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги, що аранжується на підставі повноти захисту й вибіркової керування. Політика конфіденційності при обміні, який реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів. Політика конфіденційності при обміні, який реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, які використовуються, і можливість користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, яка втримується в об'єкті, який передається. Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження. Запити на експорт захищеного об'єкту повинні оброблятися передаючим КЗЗ на підставі атрибутів доступу інтерфейсного процесу й приймачем об'єкта. Запити на імпорт захищеного об'єкта повинні оброблятися приймальням КЗЗ на підставі атрибутів доступу інтерфейсного процесу й джерела об'єкта. Вистава

захищеного об'єкта повинне бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела й приймача.

Критерії цілісності.

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям цілісності, КЗЗ оцінюваної КС повинен надавати послуги по захисту оброблюваної інформації від несанкціонованої модифікації. Цілісність забезпечується такими послугами: довірча цілісність, адміністративна цілісність, відкрит, цілісність при обміні.

Абсолютна довірча цілісність (ЦД-4). Ця послуга дозволяє користувачеві керувати потоками інформації від інших користувачів до захищених об'єктів, які належать його домену. Рівні даної послуги, що ранжується, на підставі повноти захисту й вибіркової керування. Політика довірчої цілісності, яка реалізується КЗЗ, повинна відноситись до всіх об'єктів КС. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу, користувача й захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, який ініціює запит і об'єкта. КЗЗ повинен надавати користувачеві можливість для кожного захищеного об'єкта, який належить його домену, визначити конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права модифікувати об'єкт. КЗЗ повинен надавати користувачеві можливість для кожного процесу, який належить його домену, визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту й імпорту. Необхідні умови: ПО-1, НІ-1.

Абсолютна адміністративна цілісність (ЦА-4). Ця послуга дозволяє адміністраторові або спеціально авторизованому користувачеві керувати

потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжуються на підставі повноти захисту й вибіркової керування. Політика адміністративної цілісності, яка реалізується КЗЗ, повинна ставитися до всіх об'єктів КС. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу, користувача й захищеного об'єкта. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністраторові або користувачеві, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування приналежністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права модифікувати об'єкт. КЗЗ повинен надавати можливість адміністраторові або користувачеві, який має відповідні повноваження, для кожного процесу шляхом керування приналежністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту й імпорту. Необхідні умови: ПО-1, АЛЕ-1, НІ-1.

Повний відкит (ЦВ-2). Ця послуга забезпечує можливість скасувати операцію або послідовність операцій і повернути (відкотити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжуються на підставі множини операцій, для яких забезпечується відкит. Політика відкоту, який реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона ставиться. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачеві або процесу відкотити або скасувати всі операції, виконані над захищеним об'єктом за певний проміжок часу. Необхідні умови: НІ-1.

Повна цілісність при обміні (ЦВ-3). Ця послуга дозволяє забезпечити

захист об'єктів від несанкціонованої модифікації інформації, яка втримується в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжуються на підставі повноти захисту й вибірковості керування. Політика цілісності при обміні, який реалізується КЗЗ, повинна визначати множина об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, яка забезпечується використовуваними механізмами, і можливість користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, яка міститься в об'єкті, який передається, а також фактів його видалення або дублювання. Запити на експорт захищеного об'єкта повинні оброблятися передатним КЗЗ на підставі атрибутів доступу інтерфейсного процесу й приймального об'єкта. Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу й джерела об'єкта. Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження. Вистава захищеного об'єкта повинне бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела й приймального. Необхідні умови : АЛЕ-1, НВ-1.

Критерії доступності.

Для того, щоб КС могла бути оцінена на відповідність критеріям доступності, КЗЗ оцінюваної КС повинен надавати послуги щодо забезпечення можливості використання КС у цілому, окремих функцій або оброблюваної інформації на певному проміжку часу й гарантувати можливість КС функціонувати у випадку відмови її компонентів. Доступність може забезпечуватися в КС такими послугами: використання ресурсів, стійкість до відмов, гаряча заміна, поновлення після збоїв.

Пріоритетність використання ресурсів (ДР-3). Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжуються на підставі повноти захисту й вибірковості керування доступністю

послуг КС. Політика використання ресурсів, яке реалізується КЗЗ, повинна ставитися до всіх об'єктів КС. Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (об'єм ресурсів), які виділяються окремому користувачеві й довільним групам користувачів. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. Повинна існувати можливість установлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть привести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку окремого користувача й довільних груп користувачів. Необхідні умови: АЛЕ-1.

Стійкість без погіршення характеристик обслуговування (ДС-3). Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій або КС у цілому) після відмови її компонента. Рівні даної послуги ранжуються на підставі можливості КЗЗ забезпечити можливість функціонування КС залежно від кількості відмов і послуг, доступних після відмови. Розроблювач повинен провести аналіз відмов компонентів КС. Політика стійкості до відмов, що реалізується КЗЗ, повинна ставитися до всіх компонентів КС. Повинні бути чітко зазначені рівні відмов, при перевищенні яких відмови приводять до зниження характеристик обслуговування або неприступності послуги. Відмова одного захищеного компонента не повинен приводити до неприступності всіх послуг або до зниження характеристик обслуговування. КЗЗ повинен бути здатний повідомити адміністратора про відмову будь-якого захищеного компонента. Необхідні умови: АЛЕ-1.

Гаряча заміна будь-якого компонента (ДЗ-3). Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС у цілому) у процесі заміни окремих компонентів. Рівні даної послуги ранжуються на підставі повноти реалізації. Політика гарячої заміни,

яка реалізується КЗЗ, повинна забезпечувати можливість заміни будь-якого компонента без переривання обслуговування. Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість замінити будь-який захищений компонент. Необхідні умови: АЛЕ-1, ДС-1.

Вибіркове поновлення (ДВ-3). Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжуються на підставі заходу автоматизації процесу поновлення. Політика поновлення, яке реалізується КЗЗ, повинна визначати множина типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко зазначені рівні відмов, у випадку перевищення яких необхідна повторна інсталяція КС. Після будь-якої відмови КС або переривання обслуговування, яке не приводить до необхідності заново інстальовати КС, КЗЗ повинен бути здатним виконати необхідні процедури й безпечним чином повернути КС до нормального функціонування або, у найгіршому разі, функціонування в режимі з погіршеними характеристиками обслуговування.

Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС із режиму з погіршеними характеристиками обслуговування в режим нормального функціонування. Необхідні умови: АЛЕ-1.

Критерії спостереження.

Для того, щоб КС могла бути оцінена на предмет відповідності критеріям спостереження, КЗЗ оцінюваної КС повинен надавати послуги по забезпеченню відповідальності користувача за свої дії й з підтримки можливості КЗЗ виконувати свої функції. Спостереження забезпечується в КС такими послугами: реєстрація (аудит), ідентифікація й автентифікації, достовірність

каналу, розподіл обов'язків, цілісність КЗЗ, самотестування, ідентифікація й автентифікація при обміні, автентифікація відправника, автентифікація одержувача.

Аналіз у реальному часі (НР-5). Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжуються залежно від повноти й вибіркової контролю, складності засобів аналізу даних журналів реєстрації й можливості прояву потенційних порушень. Політика реєстрації, яка реалізується КЗЗ, повинна визначати перелік подій, які реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, які мають безпосереднє або непряме відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, типі й успішності або неуспішності кожного зареєстрованого події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу й/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори й користувачі, яким надані відповідні повноваження, повинні мати у своєму розпорядженні засоби перегляду й аналізу журналу реєстрації. КЗЗ повинен бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушеннях політики безпеки КС. КЗЗ повинен бути здатним негайно інформувати адміністратора про перевищення порогів безпеки й, якщо реєстраційні небезпечні події повторюються, здійснити неруйнуючі дії щодо припинення повторення цих подій. КЗЗ повинен бути здатним виявляти й аналізувати несанкціоновані дії в реальному часі. Необхідні умови: НІ-1, АЛЕ-1.

Одиночна ідентифікація й автентифікація (НІ-2). Ідентифікація й автентифікація дозволяють КЗЗ визначити й перевірити особистість користувача, який намагається одержати доступ до КС. Рівні даної послуги, що ранжується, залежно від числа задіяних механізмів автентифікації. Політика ідентифікації й автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання

яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачеві виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен аутентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування. Необхідні умови: НК-1.

Розподіл обов'язків на підставі привілеїв (АЛЕ-3). Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача й обмежити авторитарність керування. Рівні даної послуги, що ранжується, на підставі вибіркової керування можливостями користувачів і адміністраторів. Політика розподілу обов'язків, який реалізується КЗЗ, повинна визначати ролі адміністратора й звичайного користувача й властиві їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки й іншого адміністратора. Функції, властиві кожній з ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Політика розподілу обов'язків повинна визначати множина ролей користувачів. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, які підтверджують прийняття їм цієї ролі. Необхідні умови: НІ-1.

КЗЗ із функціями диспетчера доступу (НЦ-3). Ця послуга визначає захід здатності КЗЗ захищати себе й гарантувати свою можливість керувати захищених об'єктів. Політика цілісності КЗЗ повинна визначати домен КЗЗ і інші домени, а також механізми захисту, які використовуються для реалізації розподілу доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації й/або втрати керування. КЗЗ повинен гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і все запити на доступ до захищених об'єктів контролюються КЗЗ.

Саме тестування при старті (НТ-2). Саме тестування дозволяє КЗЗ перевірити й на підставі цього гарантувати правильність функціонування й

цілісність певного множини функцій КС. Рівні даної послуги ранжуються на підставі можливості виконання тестів у процесі запуску або штатної роботи. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ повинен бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися по запиту користувача, який має відповідні повноваження, при ініціалізації КЗЗ. Необхідні умови: АЛЕ-1.

Базова автентифікація відправника (НА-1). Ця послуга дозволяє забезпечити захист від відмови від авторства й однозначно встановити приналежність певного об'єкта певному користувачеві, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжуються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною. Політика автентифікації відправника, який реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, який передається, користувача-відправника й інтерфейсного процесу, а також процедури, які б дозволяли однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем. Встановлення приналежності повинне виконуватися на підставі затвердженого протоколу автентифікації. Необхідні умови: НІ-1.

Базова автентифікація одержувача (НП-1). Ця послуга дозволяє забезпечити захист від відмови від одержання й дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги, що ранжується, на підставі можливості підтвердження результатів перевірки незалежною третьою стороною. Політика автентифікації одержувача, який реалізується КЗЗ, повинна визначати множина властивостей і атрибутів об'єкта, який передається, користувача-одержувача й інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був отриманий певним користувачем. Установлення одержувача повинне виконуватися на підставі затвердженого протоколу автентифікації. Необхідні

умови: НІ-1.

Автентифікація джерела даних (НВ-2). Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (установити й перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодія. Рівні даної послуги, що ранжується, на підставі повноти реалізації. Політика ідентифікації й автентифікація при обміні, який реалізується КЗЗ, повинна визначати множина атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати й аутентифікувати цей КЗЗ із використанням захищеного механізму підтвердження ідентичності повинен виконуватися на підставі затвердженого протоколу автентифікації. КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, який експортується й імпортується.

Необхідні умови.

Усі послуги є більш-менш незалежними. Якщо ж така залежність виникає, тобто реалізація якої-небудь послуги неможлива без реалізації іншої, то цей факт відбивається як необхідні умови для даної послуги (або її рівня).

Опис умов необхідних для реалізації певних профілів захищеності.

Зовнішня ідентифікація й автентифікація (НІ-1). Політика ідентифікації й автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач та послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачеві виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен з використанням захищеного механізму одержати від деякого зовнішнього джерела автентифікаційний ідентифікатор цього користувача.

Зовнішній аналіз (НР-1) - реєстрація. Політика реєстрації, яка реалізується КЗЗ, повинна визначати перелік подій, які реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, які мають безпосереднє

відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, типі й успішності або неуспішності кожного зареєстрованого події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу й/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен бути здатним передавати журнал реєстрації в інші системи з використанням певних механізмів захисту.

Виділення адміністратора (АЛЕ-1). Політика розподілу обов'язків, який реалізується КЗЗ, повинна визначати ролі адміністратора й звичайного користувача й властиві їм функції. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, які підтверджують прийняття їм цієї ролі.

Автентифікація вузла (НВ-1). Політика ідентифікації й автентифікація при обміні, яка реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ. КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати й аутентифікувати цей КЗЗ із використанням захищеного механізму підтвердження ідентичності та повинен виконуватися на підставі затвердженого протоколу автентифікації.

Стійкість при обмежених відмовах(ДС-1). Розроблювач повинен провести аналіз відмов компонентів КС. Політика стійкості до відмов, що реалізується КЗЗ, повинна визначати множина компонентів КС, до яких вона ставиться, і типи їх відмов, після яких КС у стані продовжувати функціонування. Повинні бути чітко зазначені рівні відмов, при перевищенні яких відмови приводять до зниження характеристик обслуговування або неприступності послуги. Відмова одного захищеного компонента не повинен приводити до неприступності всіх послуг, а повинен у найгіршому разі проявлятися в зниженні характеристик обслуговування. КЗЗ повинен бути здатний повідомити адміністратора про відмову будь-якого захищеного компонента.

Односпрямований достовірний канал (НК-1). Політика достовірного каналу, який реалізується КЗЗ, повинна визначати механізми встановлення

достовірному зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації й автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися винятково користувачем.

Критерії гарантій.

Критерії гарантій включають вимоги до архітектури КЗЗ, середовищу розробки, послідовності розробки, середовища функціонування, документації й випробувань КЗЗ. У цих критеріях уводиться сім рівнів гарантій, які є ієрархічними. Вимоги викладаються за розділами. Для того, щоб КС одержала певний рівень гарантій (якщо вона не може одержати більш високий), повинні бути задоволені всі вимоги, певні для даного рівня в кожному з розділів.

Г-3

Архітектура.

Вимоги до архітектури забезпечують гарантії того, що КЗЗ у стані повністю реалізувати політикові безпеки:

- КЗЗ повинен реалізовувати політикові безпеки. Усі його компоненти повинні бути чітко визначені.
- КЗЗ повинен складатися з добре певних і максимально незалежних компонентів. Кожний з компонентів повинен бути спроектований відповідно до принципу мінімуму повноважень.

Середовище розробки.

Вимоги до середовища розробки забезпечують гарантії того, що процеси розробки й супроводи оцінюваної КС є повністю керованими з боку Розроблювача.

Процес розробки:

- Розроблювач повинен визначити всі стадії життєвого циклу КС, розробити, впровадити й підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Повинні бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги.

- Розроблювач повинен описати стандарти кодування, яким необхідно користуватися в процесі реалізації, і повинен гарантувати, що всі вихідні коди компілюються відповідно до цих стандартів. Усі залежні від реалізації параметри немов програмування або компіляторів повинні бути документуємі.

Керування конфігурацією:

- Розроблювач повинен розробити, впровадити й підтримувати в робочому стані документуємі методики щодо керування конфігурацією КС на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти об'єктних кодів, тестового покриття й документації. Система керування конфігурацією повинна гарантувати постійну відповідність між усією документацією й реалізацією поточної версії КЗЗ.

Послідовність розробки.

Вимоги до процесу проектування (послідовності розробки) забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис КС і реалізація КС точно відповідає вихідним вимогам (політиці безпеки).

Функціональні специфікації (політика безпеки):

- на стадії розробки технічного завдання Розроблювач повинен розробити функціональні специфікації КС. Представлені функціональні специфікації повинні включати неформалізований опис політики безпеки, яка реалізується КЗЗ. Політика безпеки повинна містити перелік і опис послуг безпеки, які надаються КЗЗ.

Функціональні специфікації (модель політики безпеки).

- відповідність політиці безпеки (показ);
- функціональні специфікації повинні включати модель політики безпеки;
- стиль специфікації: частково формалізовано.

Середовище функціонування

Вимоги до середовища функціонування забезпечують гарантії того, що КС поставляється Замовникові без несанкціонованих модифікацій, а також інсталується й ініціюється Замовником так, як це передбачається

Розроблювачем:

- розроблювач повинен представити засоби інсталяції, генерації й запуску КС, які гарантують, що експлуатація КС починається з безпечного стану. Розроблювач повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації й запуску;

- повинна існувати система технічних, організаційних і фізичних заходів безпеки, яка гарантує, що програмне й програмно-апаратне забезпечення КЗЗ, яке поставляється Замовникові, точно відповідає еталонній копії.

Документація

Вимоги до документації є загальними для всіх рівнів гарантій:

- у вигляді окремих документів або розділів (підрозділів) інших документів Розроблювач повинен подати опис послуг безпеки, які реалізуються КЗЗ, установки адміністраторові щодо послуг безпеки, установки користувача щодо послуг безпеки;

- в описі функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, яка реалізується КЗЗ оцінюваної КС, а також самі послуги;

- установки адміністраторові щодо послуг безпеки повинні містити опис засобів інсталяції, генерації й запуску КС, опис усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації й запуску КС, опис властивостей КС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, яка експлуатує КС;

- установки користувачеві щодо послуг безпеки повинні містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором);

Випробування комплексу засобів захисту:

- розроблювач повинен подати для перевірки програму й методику

випробувань, процедури випробувань усіх механізмів, які реалізують послуги безпеки. Повинні бути представлені аргументи для підтвердження достатності тестового покриття;

- розроблювач повинен подати доказу тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, для того, щоб отримані результати могли бути перевірені шляхом повторення тестування;

- розроблювач повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки минулого усунуті й не з'явилися нові “слабкі місця”.

2.7 Огляд існуючих вимог до засобів, методів і способам зменшення рівнів ризиків інформаційної безпеки передачі транзакційних пакетів через платіжні шлюзи, згідно зі стандартами ради PCI SSC

Радою по стандартах безпеки індустрії платіжних карт (рада PCI SSC (Payment Card Industry Security Standards Council)), який був створений колективним розв'язком п'яти міжнародних платіжних систем Visa, Mastercard, Americanexpress, JCB і Discover (як міжнародний регулювальний орган у сфері безпеки обігу платіжних карт) були розроблені й підтримуються стандарти забезпечення безпеки даних індустрії платіжних карт PCI DSS, PCI PA-DSS і PCI PTS.

Стандарт PCI DSS (Payment Card Industry Data Security Standard) – стандарт безпеки даних індустрії платіжних карт – документ, що визначає вимоги до постачальників послуг і торгово-сервісним підприємствам по забезпеченню безпеки обігу платіжних карт.

Стандарт PCI PA-DSS (Payment Card Industry Payment Application Data Security Standard) – стандарт безпеки даних у платіжних додатках індустрії платіжних карт – документ, що визначає вимоги до додатків, що обробляють дані про власників карт і процесу їх розробки.

Керівництва PCI PTS (Payment Card Industry PIN Transaction Security) – набір керівних документів, що містять вимоги до обладнань, що обробляють персональний ідентифікаційний номер – PIN. До таких пристроїв ставляться Pos-Термінали, що шифрують PIN – клавіатури (EPP), апаратні модулі безпеки (HSM).

Метою даних стандартів є розробка вимог, відповідність яким, дасть зниження рівнів ризиків інформаційної безпеки передачі транзакційних пакетів, що містять у собі ДБК і КАД.

Стандарт PCI DSS.

Об'єкт застосування: організація, в інформаційній інфраструктурі якої зберігаються, обробляються або передаються дані про власників карт.

Критерій застосовності: зберігання, обробка або передача хоча б одного номера карти (PAN) який-небудь із п'яти міжнародних платіжних систем – учасниць Ради PCI SSC (Visa, Mastercard, Americanexpress, JCB і Discover).

Критерій відповідності: виконання 100% застосовних до організації вимог стандарту.

Спосіб підтвердження відповідності: визначається міжнародною платіжною системою й банком – еквайєром окремо для різних типів організацій.

Регулярність підтвердження відповідності: щорічно.

Стандарт PCI PA-DSS.

Об'єкт застосування: додаток, який зберігає, обробляє або передає дані про власників карт (платіжний додаток), а також процес його розробки.

Критерій застосовності: зберігання, обробка або передача хоча б одного номера карти (PAN) який-небудь із п'яти міжнародних платіжних систем – учасниць Ради PCI SSC (Visa, Mastercard, Americanexpress, JCB і Discover) у процесі авторизації транзакції або виконання взаєморозрахунків. Не застосуємо до додатків, розроблених самостійно для власних потреб, а також до додатків,

розроблених на замовлення для одного замовника.

Критерій відповідності: виконання 100% застосовних до додатка вимог стандарту.

Спосіб підтвердження відповідності: перевірка безпеки додатка аудиторською організацією (PA-QSA), сертифікованої Радою PCI SSC.

Регулярність підтвердження відповідності: щорічно, спосіб залежить від значимості відновлень додатка з погляду безпеки обробки карткових даних.

Структура стандарту PCI DSS.

Стандарт PCI DSS актуальний і містить у собі 288 перевірочних процедур, розподілених по дванадцяти розділам:

- 1) Захист обчислювальної мережі.
- 2) Конфігурація компонентів інформаційної інфраструктури.
- 3) Захист збережених даних про власників карт.
- 4) Захист переданих даних про власників карт.
- 5) Антивірусний захист інформаційної інфраструктури.
- 6) Розробка й підтримка інформаційних систем.
- 7) Керування доступом до даних про власників карт.
- 8) Механізми автентифікації.
- 9) Фізичний захист інформаційної інфраструктури.
- 10) Протоколювання подій і дій.
- 11) Контроль захищеності інформаційної інфраструктури.
- 12) Управління інформаційною безпекою.

Для забезпечення найвищого рівня безпеки, платіжні шлюзи й процесінгові центри, що підтвердили відповідність вимогам стандартів PCI DSS v.2.0, повинні готуватися до процесу підтвердження вимог PCI DSS v.3.0, який містить багато змін і додавань в відношенні до v.2.0.

Способи підтвердження відповідності стандарту PCI DSS і класифікація по строках переатестації Visa (торгово-сервісні підприємства) наведені в Додатку Г.

Висновки до розділу 2

У даній главі приводяться схеми взаємодії платіжних шлюзів з іншими учасниками обміну транзакційними пакетами. Також приводяться типи інформації, оброблювані в платіжних шлюзах і їх розподіл по рівнях захищеності, а також робиться аналіз впливу погроз і порушника на всі типи оброблюваної інформації, і робиться висновок про б уразливі місця й рівні ризику по кожному з них. Також у даній главі робиться вибір класу й профілю захищеності автоматизованої системи, якої є самої платіжний шлюз або процесінговий центр банку. Також особлива увага приділена вимогам ради PCI SSC.

3 РОЗРОБКА МОДЕЛІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ПЛАТІЖНОГО ШЛЮЗУ В МЕРЕЖІ INTERNET

3.1 Вибір оптимальних рішень з погляду безпеки, комплексності, масштабованості й рівня капіталовкладень

Серед розроблювачів автоматизованих програмних комплексів обробки платіжних електронних транзакцій розглянемо такі, які надають тільки готові рішення для процесування міжнародних карт, які також підходять для впровадження в платіжні-шлюзи. Найпростіший спосіб одержати список вендорів – це звернутися в міжнародні платіжні системи де вони нададуть список рекомендованих постачальників. Не варто думати, що є список «сертифікованих» постачальників ПЦ. У рамках проекту сертифікації банку (сертифікується саме банк із конкретним програмно-апаратним комплексом) можна сертифікувати навіть самописне програмне забезпечення ПЦ, але в той же час набагато простіше проходити сертифікацію із програмним забезпеченням, яке вже сертифікувалося в якому-небудь банку (і чим більше було таких сертифікацій, тем швидше й простіше пройде процес). Звичайно регіональні офіси платіжних систем надають список вендорів, які працюють на даному ринку. На ринку колишнього СНД питаннями розроблення автоматизованих програмних комплексів обробки платіжних електронних транзакцій займались наступні компанії (перераховані за абеткою), які наведені на рис. 3.1.

Проаналізувавши можливості наведених програмних продуктів, зупинилися на самому оптимальному продукті, з позицій комплексності захисту, масштабованості, керованості й інтегруємості – Tranzware Online, фірми Compass Plus.

Приведемо список переваг ПЗ Tranzware Online:

1) Гнучка система налаштувань.

2) Простота конфігурації.

3) Зручний користувацький інтерфейс сприяє підвищенню продуктивності персоналу, якісно поліпшуючи обслуговування клієнтів.

4) Підтримка безлічі каналів обслуговування, типів карт і обладнань, мереж і хостів.

5) Розвинені засоби моніторингу, що підвищує якість роботи системи.

6) Можливість дистанційного доступу до процесінгового центру (FIMI).

7) Створення правил авторизації й керування сценаріями з використанням Tranzware Online Algorithmix.

8) Білялінійна, необмежена масштабованість: ріст у міру розвитку бізнесу.

9) Об'єднання всіх каналів роздрібного обслуговування на єдиній платформі.

10) Доступність 24x7 завдяки відмовостійкому програмному рішення, що багаторазово підтверджене досвідом реальної експлуатації.

11) Вичерпний набір транзакцій.

12) Засобу контролю ризиків.

13) Інтеграція з будь-якими продуктами сімейства Tranzware і існуючими системами й компонентами сторонніх виробників.

14) Система має англomовний і російськомовний інтерфейси.

Tranzware Online є високоефективним, відмовостійким рішенням, що володіє унікальним набором функціональних можливостей front-office у комбінації з оптимальними ціновими характеристиками. Tranzware Online надає можливість керування проходження коштів термінальними обладнанням – банкоматами (у тому числі – Cash-in), POS-терміналами, кіосками та ін., маршрутизації й авторизації транзакцій, взаємодії із платіжними системами (VISA, Mastercard, AMEX, Diners Club, JCB, локальними й регіональними) і авторизованими хостами сторонніх виробників. Гнучкість рішення підтверджується й різноманіттям варіантів настроювання: клієнт може настроїти продукт у повній відповідності з поточним або прогнозованим

процесінговим середовищем.

Tranzware Online дозволяє здійснювати різні операції з банкоматами (завантаження параметрів, робота з обладнаннями, різні нестандартні операції, включаючи виконання платежів, обмін валюти, Cash-In та ін.), маршрутизацію транзакцій, конфігурування обладнань (редагування екрана, створення сценаріїв, налаштування комісій та ін.), планування витрати готівки, а також підтримує систему оповіщень обслуговуючого персоналу через різні канали й безліч інших функцій. Tranzware Online має гнучку й масштабовану систему моніторингу банкоматів, що включає такі графічні функції як, наприклад, навігацію по карті розташування банкоматів, відображення статусу банкомата й т.п.). Система дозволяє аналізувати/розраховувати стан мережі й оперативно реагувати на зміни.

Для банків, що володіють більшими розподіленими мережами банкоматів, керування якими вимагає боєм зроблених інструментів, в Tranzware Online існує альтернативний модуль, відповідальний за керування банкоматною мережею – Tranzware Online ATM Monitoring. Даний модуль Atm-Моніторингу надає можливість керування термінальною мережею на принципово іншому якісному рівні. Реалізовані в модулі інноваційні механізми покликані забезпечити конкурентна перевагами за рахунок параметризованих механізмів контролю працездатності мережі й, в остаточному підсумку, оптимізації витрат на сервісне обслуговування. Модуль ATM Monitoring забезпечує більш високий рівень масштабованості й гнучкості системи, дозволяє ефективно проводити оперативний моніторинг і поглиблений аналіз усієї мережі, груп терміналів і окремого банкомату в різноманітних розрізах.

Tranzware Online у повному об'ємі підтримує всі компоненти, що становлять POS-процесінг, включаючи підтримку різних типів POS-терміналів, типів транзакцій і безлічі термінальних протоколів роботи з POS-терміналами й інтелектуальними кіосками.

Tranzware Online є масштабованим розв'язком, здатним забезпечити

якісну роботу мереж банкоматів і Pos-Терміналів будь-якого масштабу (від десятків до тисяч термінальних обладнань) і сполуки, а також повністю відповідає вимогам усіх провідних платіжних систем.

Розв'язок Tranzware Online підтримує графічний інтерфейс і дає можливість виконання цілого ряду транзакцій на основі карт різних технологій (включаючи EMV), що забезпечує якісний сервіс клієнтів.

Будучи центром обробки транзакцій, Tranzware Online інтегрується не тільки із продуктами Tranzware, але й із системами сторонніх виробників. Існує механізм online-взаємодії із системою back-office. Це, у першу чергу, Tranzware Card Management System, але існують і інші реалізації сумісної взаємодії іншими автоматизованими банківськими системами.

3.2 Розробка нових способів у міжмережевій безпеці передачі транзакційних пакетів через платіжні шлюзи

Основною особливістю розподіленої обчислювальної мережі (РОМ) є те, що її об'єкти розподілені в просторі й зв'язок між ними фізично здійснюється по мережевим сполуках та програмно - тобто повідомлення й дані, що пересилаються між об'єктами РОМ, передаються по мережевим сполуках у вигляді пакетів. Ця особливість привела до появи специфічного для РОМ типового віддаленого впливу, що полягає в «прослуховуванні» каналу зв'язку. Назвемо даний типовий віддалений вплив аналізом мережевого трафіку (або, скорочено, мережним аналізом).

Аналіз мережевого трафіка дозволяє:

1) вивчити логіку роботи РОМ, тобто одержати однозначну відповідність подій, що відбуваються в системі, і команд, що пересилаються один одному її об'єктами, у момент появи цих подій. Це досягається шляхом перехоплення й аналізу пакетів обміну на каналному рівні. Знання логіки роботи РВС дозволяє на практиці моделювати й здійснювати типові віддалені атаки, які будуть розглянуті в наступних пунктах на прикладі конкретних РОМ.

2) перехопити потік даних, якими обмінюються об'єкти РОМ. Таким чином, віддалелена атака даного типу полягає в одержанні на віддаленому об'єкті несанкціонованого доступу інформації, якою обмінюються два мережні абоненти. Відзначимо, що при цьому відсутня можливість модифікації трафіка й сам аналіз можливий тільки усередині одного сегмента мережі. Прикладом перехопленої за допомогою даної типової віддаленої атаки інформації можуть служити ім'я й пароль користувача, що пересилаються в незашифрованому виді по мережі.

По характеру впливу аналіз мережного трафіка є пасивним впливом (клас 1.1). Здійснення даної атаки без зворотнього зв'язку (клас 4.2) веде до порушення конфіденційності інформації (клас 2.1) усередині одного сегмента мережі (клас 5.1) на каналному рівні OSI (клас 6.2). При цьому початок здійснення атаки є безумовним стосовно мети атаки (клас 3.3).

Підміна довіреного об'єкта або суб'єкта системи

Однієї із проблем безпеки РОМ є недостатня ідентифікація й аутентифікація її віддалених друг від друга об'єктів. Основні труднощі полягають в здійсненні однозначної ідентифікації повідомлень, переданих між суб'єктами й об'єктами взаємодії. Зазвичай у РОМ ця проблема вирішується в такий спосіб: у процесі створення віртуального каналу об'єкти РОМ обмінюються певною інформацією, яка унікально ідентифікує даний канал. Такий обмін звичайно називається «рукоштовуванням» (handshake). Однак, необхідно відзначити, що не завжди для зв'язку двох віддалених об'єктів у РВС створюється віртуальний канал. Практика показує, що найчастіше, особливо для службових повідомлень (наприклад, від маршрутизаторів) використовується передача одиночних повідомлень, що не вимагають підтвердження.

Для адресації повідомлень у РОМ використовується мережева адресація, яка унікальна для кожного об'єкта системи (на каналному рівні моделі OSI - це апаратна адреса мережевого адаптера, на мережному рівні - адреса визначається залежно від використовуваного протоколу мережного рівня

(наприклад, IP-адреса). Мережева адреса також може використовуватися для ідентифікації об'єктів РОМ. Однак мережева адреса досить просто підробляється й тому використовувати її як єдиний засіб ідентифікації об'єктів неприпустимо.

У тому випадку, коли РОМ використовує нестійкі алгоритми ідентифікації віддалених об'єктів, то виявляється можливість типової віддаленої атаки, що полягає в передачі по каналах зв'язку повідомлень від імені довільного об'єкта або суб'єкта РВС.

При цьому існують два різновиди типової віддаленої атаки шляхом підміни довіреного об'єкта або суб'єкта РОМ:

1) атака при встановленому віртуальному каналі. У випадку встановленої віртуальної сполуки атака буде полягати в присвоєнні прав довіреного суб'єкта взаємодії, який легально підключився до об'єкта системи, що дозволить атакуючому вести сеанс роботи з об'єктом розподіленої системи від імені довіреного суб'єкта. Реалізація віддалених атак даного типу звичайно полягає в передачі пакетів обміну з атакуючого об'єкта на мету атаки від імені довіреного суб'єкта взаємодії (при цьому передані повідомлення будуть сприйняті системою як коректні). Для здійснення атаки даного типу необхідно подолати систему ідентифікації й аутентифікації повідомлень, яка, у принципі, може використовувати контрольну суму, що розраховується за допомогою відкритого ключа, динамічно створеного при встановленні каналу (випадкові многобитные лічильники пакетів і мережні адреси станцій). Однак на практиці, наприклад, у протоколі ТСР для ідентифікації використовуються два 32-бітних лічильника.

б) атака без установленого віртуального каналу. Для службових повідомлень у РОМ часто використовується передача одиночних повідомлень, що не вимагає підтвердження, тобто не потрібне створення віртуальної сполуки. Атака без установленої віртуальної сполуки полягає в передачі службових повідомлень від імені мережних керуючих пристроїв, наприклад, від імені маршрутизаторів. Очевидно, що в цьому випадку для ідентифікації

пакетів можливо лише використання статичних ключів, певних заздалегідь, що досить незручно й вимагає складної системи керування ключами. Однак, при відмові від такої системи ідентифікація пакетів без встановленого віртуального каналу буде можлива лише по мережній адресі відправника, яку легко підробити. Наприклад, типова віддалена атака, що використовує нав'язування неправильного маршруту шляхом посилки невірних керуючих повідомлень спирається на описану ідею.

3.3 Розробка способу мережевої ідентифікації між вузлами-учасниками при передачі транзакційних пакетів протягом усього процесу здійснення оплати через Internet

Підміна довіреного об'єкта РОМ є активним впливом (клас 1.2), вчиненим з метою порушення конфіденційності (клас 2.1) і цілісності (клас 2.2) інформації по настанню на об'єкті, що атакується, певного події (клас 3.2). Дана віддалена атака може бути як внутрішньосегментною (клас 5.1), так і міжсегментною (клас 5.2), як зі зворотним зв'язком (клас 4.1), так і без зворотного зв'язку (клас 4.2) з об'єктом, що атакується та здійснюється на мережному (клас 6.3) і транспортному (клас 6.4) рівнях моделі OSI.

Проаналізувавши існуючі недоліки в протоколі TCP, у даній магістерській роботі пропонується новий спосіб підтвердження справжності відправника й одержувача транзакційних пакетів шляхом запису хеш-образу Ір-Відправника або ІР-Одержувача в блоці даних після заголовка TCP в залежності від кого виходить пакет. За хеш-функцію пропонується обрати алгоритм CRC-32 (одержуваний хеш якого займає 32 біта), який використовується для знаходження контрольної суми та призначений для перевірки цілісності даних. CRC є практичним додатком завадостійкості кодування, заснованому на певних математичних властивостях циклічного коду.

На рис. 3.2 наведена структура заголовку сегмента TCP:

Структура заголовка				
Біт	0 — 3	4 — 9	10 — 15	16 — 31
0	Порт джерела			Порт призначення
32	Номер послідовності			
64	Номер підтвердження			
96	Довжина Заголовку	Зарезервовано	Прапора	Розмір Вікна
128	Контрольна сума			Вказівник важливості
160	Опції (необов'язкове, але використовується майже завжди)			
160/192+	Данні			

Рисунок 3.2 – Структура заголовку сегмента TCP

Приклад: IP-клієнта = 213.154.198.66 і IP-платіжного шлюзу = 85.10.225.103. Хеш IP-клієнта буде = 565bc801, Хеш IP- платіжного-шлюзу буде = 3a54edf1

3.4 Розробка способу контролю маршруту проходження транзакційних пакетів між вузлами-учасниками протягом усього процесу здійснення оплати через Internet

Для додаткової гарантованості дійсності від відправника й одержувача транзакційних пакетів у даній роботі пропонується також новий спосіб ідентифікації маршруту проходження пакету із записом найближчих до відправника й одержувача IP-шлюзів у блок даних після заголовка TCP у вигляді хеш-образів, використовуючи також алгоритм хешування CRC-32. На рис. 3.3 приводиться трасування маршруту пакету від клієнта до платіжного шлюзу. На маршруті видно, що найближчим до вузла клієнта є шлюз і з IP = 213.154.198.1, його хешем буде = a3ca07c4; а найближчим до вузла платіжного-шлюзу є шлюз і з IP = 144.76.79.221, його хешем буде = 12ad5bca.

```

cmd.exe
tracert www.interkassa.com

Трассировка маршрута к www.interkassa.com [85.10.225.103]
с максимальным числом прыжков 30:

  1  <1 ms    <1 ms    <1 ms    192.168.1.1
  2  19 ms    19 ms    21 ms    192.168.1.1
  3  40 ms    23 ms    19 ms    213.154.198.66 [ispwz-zp.aikar.net]
  4  23 ms    24 ms    20 ms    213.154.198.1
  5  35 ms    34 ms    34 ms    62.221.41.149 [ucomline.net]
  6  62 ms    64 ms    65 ms    80.81.194.177 [edge-3-2-5-231.kiev.ucomline.net]
  7  67 ms    64 ms    64 ms    80.81.193.164 [decix2-gw.hetzner.de]
  8  67 ms    69 ms    64 ms    213.239.245.21 [core4.hetzner.de]
  9  70 ms    113 ms   69 ms    213.239.245.13 [core21.hetzner.de]
 10  69 ms    70 ms    69 ms    213.239.245.110 [juniper3.rz19.hetzner.de]
 11  73 ms    74 ms    70 ms    213.239.243.166 [hos-tr2.ex3k20.rz19.hetzner.de]
 12  71 ms    75 ms    74 ms    85.10.225.103 [back.interkassa.com]

Трассировка завершена.

```

Рисунок 3.3 – Трасування маршруту пакета від клієнта до платіжного шлюзу

Висновки до розділу 3

У данному розділі пропонується покласти в основу розроблюваної моделі комплексної системи захисту платіжного шлюзу в мережі Internet автоматизований програмний комплекс Tranzeware Online компанії Compass Plus, який відповідає вимогам стандарту PCI DSS Version 3.0 (тобто виконує принцип комплексності захисту) і є масштабованим та інтегрованим. Також пропонується два способи підвищення рівня захищеності передачі транзакційних пакетів від підміни ідентифікаторів відправників: спосіб мережевої ідентифікації між вузлами-учасниками та спосіб контролю маршруту проходження транзакційних пакетів протягом усього процесу здійснення оплати через Internet.

ВИСНОВКИ

В ході виконання магістерської роботи була розроблена модель комплексної системи захисту платіжного шлюзу в мережі Internet, в основу якої запропоновано покласти автоматизований програмний комплекс Tranzeware Online компанії Compass Plus, який відповідає вимогам стандарту PCI DSS Version 3.0 (тобто виконує принцип комплексності захисту) і є масштабованим та інтегровальним.

Новизною розробки даного магістерської роботи є пропозиція двох способів підвищення рівня захищеності передачі транзакційних пакетів від підміни ідентифікаторів відправників: способу мережевої ідентифікації між вузлами-учасниками й способу контролю маршруту проходження транзакційних пакетів протягом усього процесу здійснення оплати через Internet.

Запропонована в роботі модель комплексної системи захисту платіжного шлюзу в мережі Internet може бути реалізована й впроваджена для будь-якого процесингового центру банку або платіжного шлюзу.

Це наочно показує перспективність запропонованої моделі в даній області комунікації й захисту інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про інформацію»
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
3. Закон України « Про банки та банківську діяльність»
4. Закон України « Про платіжні системи та переказ коштів в Україні».
5. НД ТЗИ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
6. НД ТЗИ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
7. НД ТЗИ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
8. НД ТЗИ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
9. НД ТЗИ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
10. НД ТЗИ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
11. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення .
12. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
13. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.
14. Положення про технічний захист інформації в Україні .
15. Положення про державну експертизу у сфері технічного захисту інформації . Концепція інформаційної безпеки України.

16. Архитектура " клиент – сервер ". [Електронний ресурс], URL: http://www.mstu.edu.ru/study/materials/zelenkov/ch_7_1.html.
17. Електронний цифровий підпис. [Електронний ресурс], URL: http://www.cryptomach.com/ua/crypto_asymm_cifpodp.html.
18. Защита баз данных (Oracle Database Security). [Електронний ресурс], URL: <http://www.oracle.com/us/products/database/security/index.html>.
19. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. [Електронний ресурс], URL: <http://www.viche.info/journal/598/>.
20. Інформаційна безпека у контексті розвитку інформаційного суспільства. [Електронний ресурс], URL: http://urzona.com/index.php?option=com_content&view=article&id=473:2011-01-13-08-00-07&catid=57:2010-06-11-16-45-54&Itemid=66.
21. Інформаційна безпека України: поняття, сутність та загрози. [Електронний ресурс], URL: <http://www.justinian.com.ua/article.php?id=2463>.
22. Клієнт – серверна архітектура. [Електронний ресурс], URL: <http://uk.wikipedia.org/wiki/>.
23. Криптографічний захист інформації та заходи захисту інформаційної безпеки. [Електронний ресурс], URL: http://pidruchniki.com.ua/12920522/finansii/kriptografichniy_zahist_informatsiyi_zahodi_zahistu_informatsiynoyi_bezpeki.
24. Основні засоби і методи захисту комп'ютерної інформації. [Електронний ресурс], URL: http://adhdportal.com/book_1704_chapter_7_1.3.Osnovn%D1%96_zasobi_%D1%96metodi_zakhistu_komp'juterno%D1%97_%D1%96nforma%D1%81%D1%96%D1%97.html.
25. Поняття та сутність інформаційної безпеки. [Електронний ресурс], URL : http://www.naiu.kiev.ua/biblio/books/inform_OVS/part4.html.
26. ПриватБанк. [Електронний ресурс], URL : <http://privatbank.ua/>.
27. Протоколы взаимодействия клиента и сервера. [Електронний ресурс], URL: <http://net.e-publish.ru/p214aa1.html/>

28. Разработка комплексной системы защиты информации в телекоммуникационных сетях. [Электронный ресурс], URL: http://www.rusnauka.com/3_SND_2010/ Informatica/58041.doc.htm.

29. Информация с сайта компании ООО «Compass Plus» [Электронный ресурс], URL: <http://www.compassplus.ru/>.

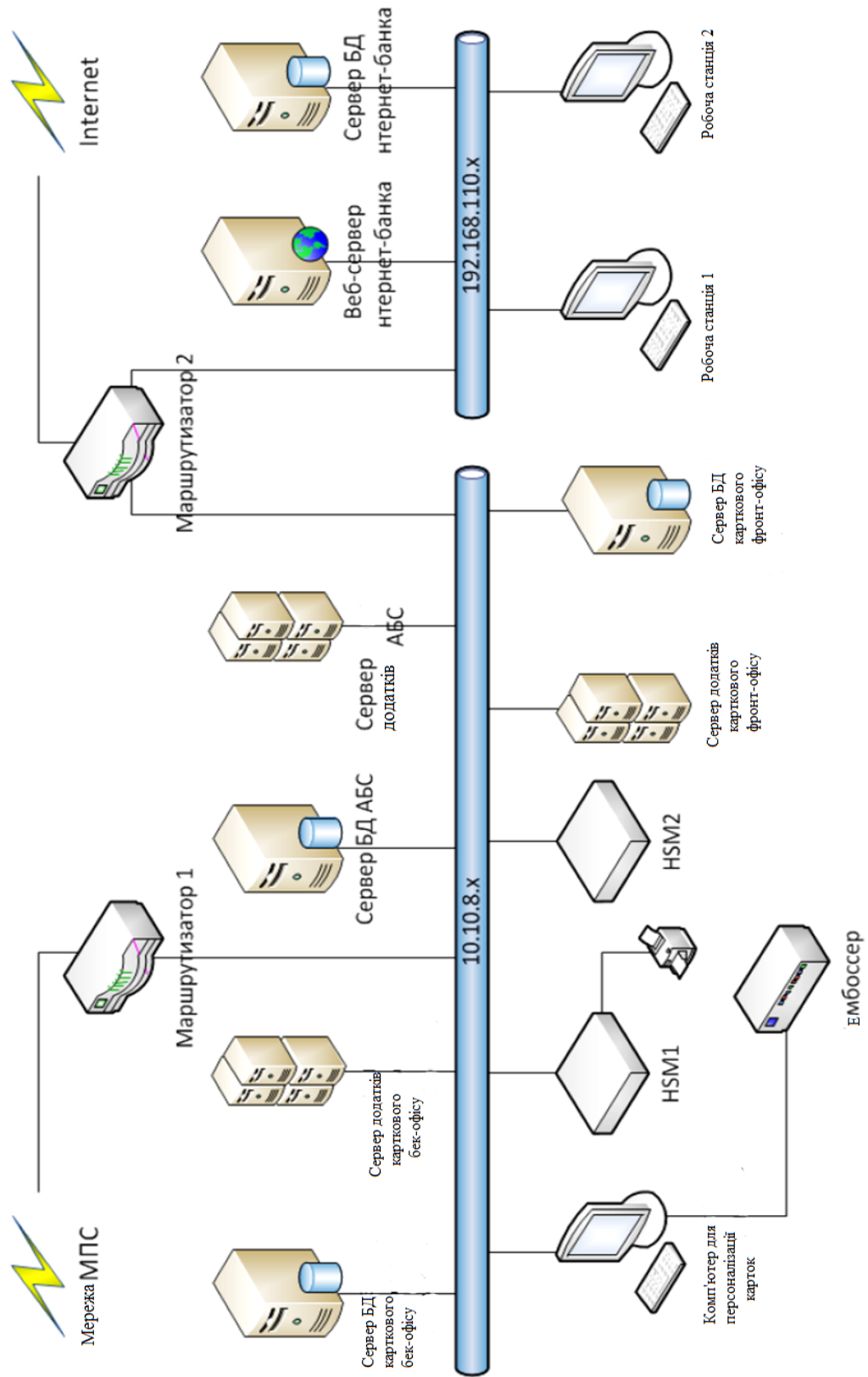
30. Выбор программного обеспечения для построения процессингового центра [Электронный ресурс], URL: <http://blog.chirkov.net/articles/article1/>.

31. Validated Payment Applications [Электронный ресурс], URL: https://www.pcisecuritystandards.org/mobile/approved_companies_providers/padss_company_details.php?cid=300096

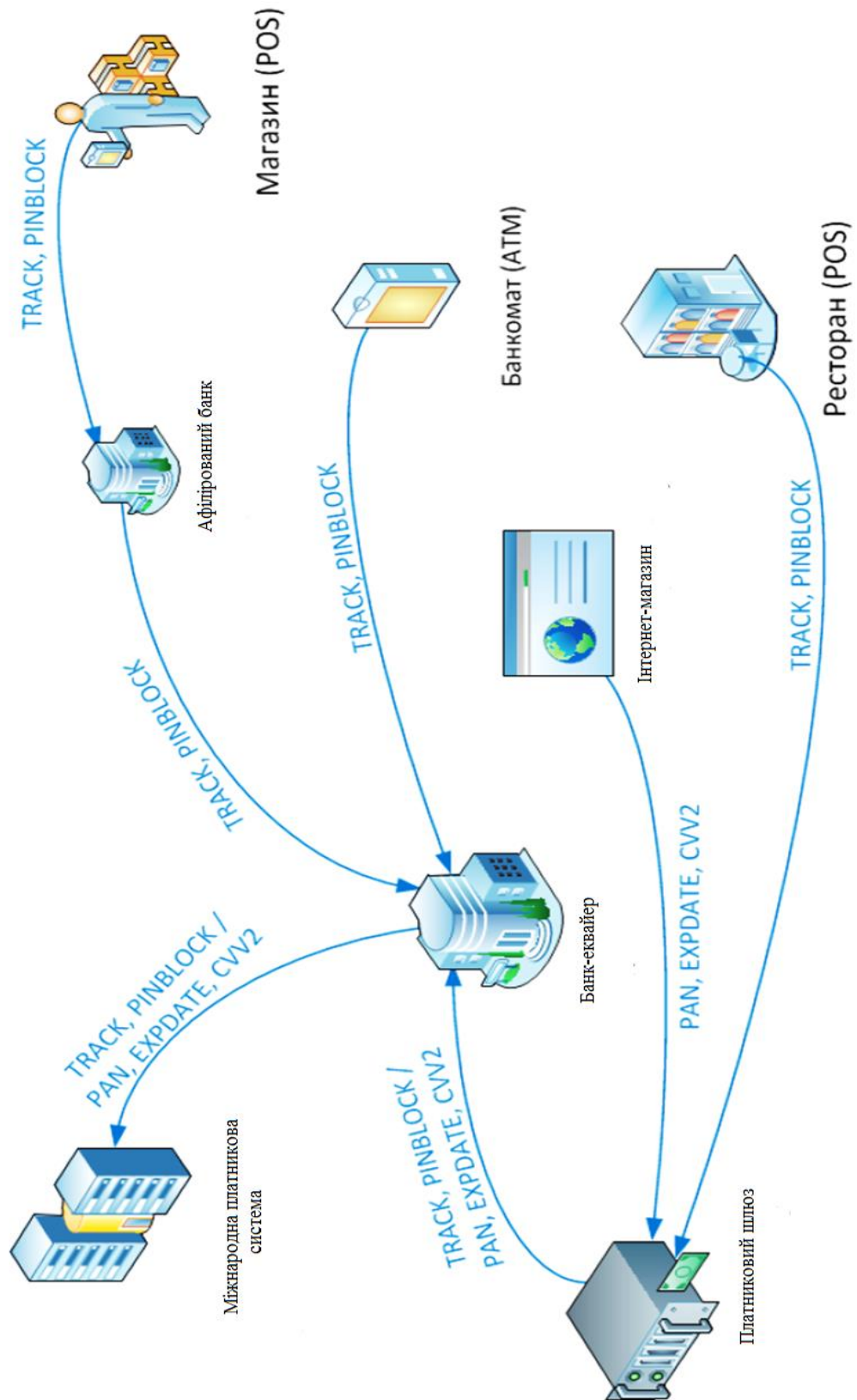
32. PCI Security Standards Council [Электронный ресурс], URL: <https://www.pcisecuritystandards.org/>.

33. Deiteriy PCI DSS Training [Электронный ресурс], URL: <http://pcidsstraining.ru/materials/>.

Додаток А Інфраструктура банку – схема мережі



Додаток Б Потоки ДВК між учасниками процесу еквайрингу



Додаток В Платіжний шлюз (схема мережі) та область застосування PCI DSS

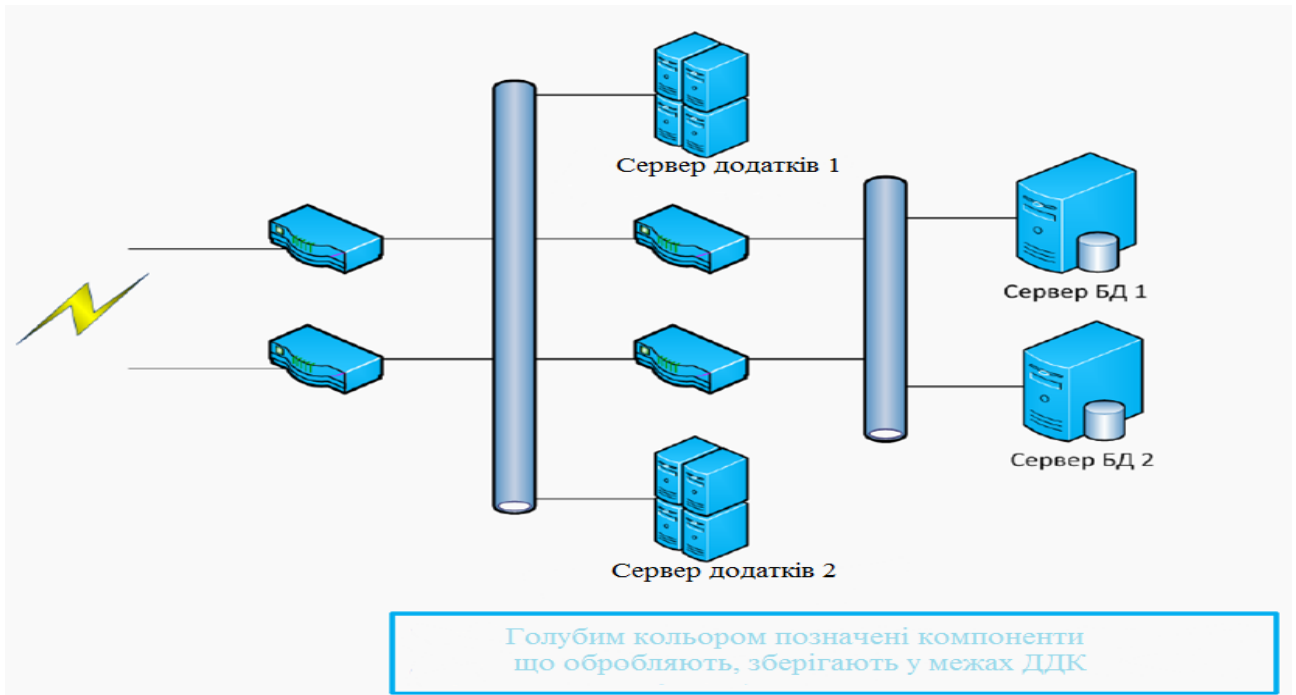
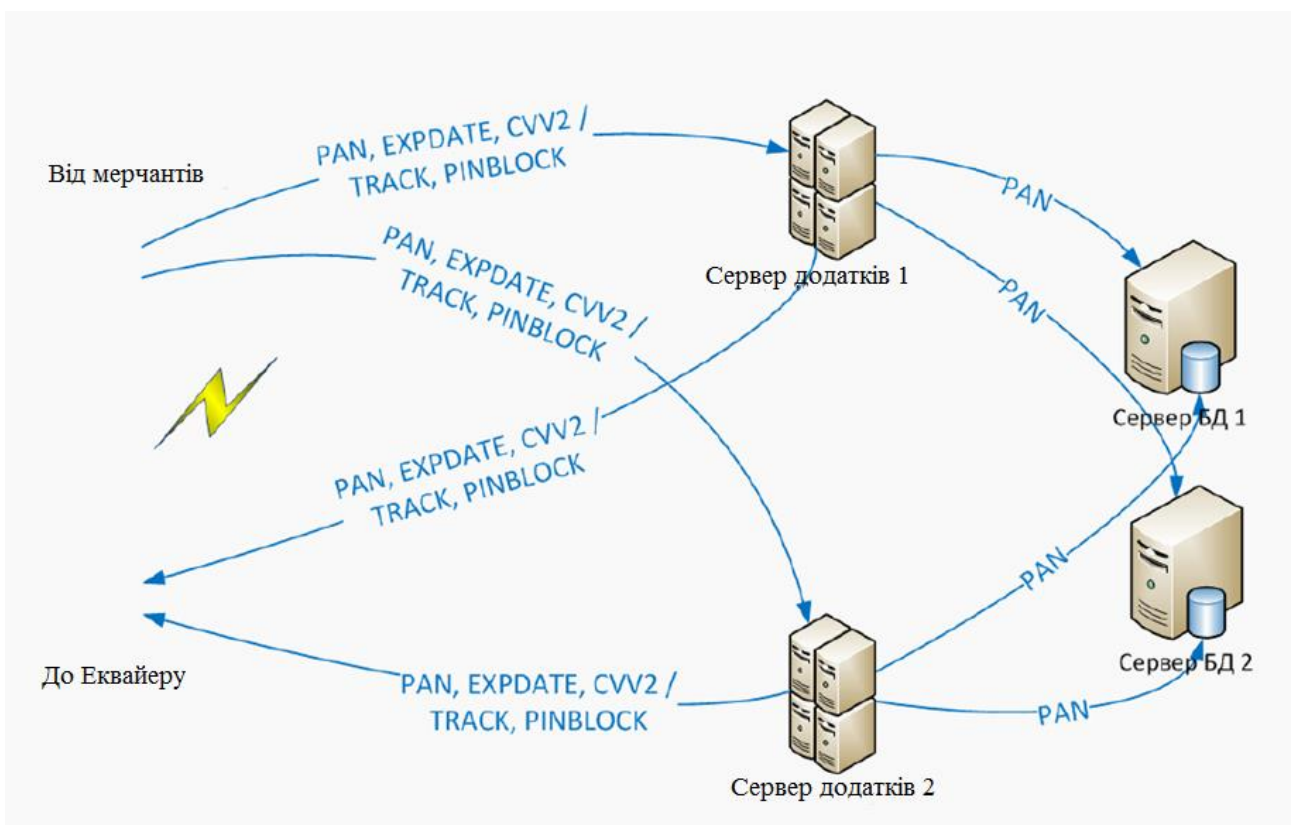


Схема руху потоків ДВК між платіжним шлюзом та іншими учасниками процесу еквайрингу



Додаток Г Способи підтвердження відповідності стандарту PCI DSS

Зовнішній аудит (QSA)	Внутрішній аудит(QSA)	Самооцінка(SAQ)
Виконується зовнішньою аудиторською організацією (Qualified Security Assessor, QSA), сертифікований Радою PCI SSC	Виконується внутрішнім навчаним і сертифікованим за програмою Ради PCI SSC аудитором (Internal Security Assessor, ISA).	Виконується самостійно шляхом заповнення листу самооцінки(Self-Assessment Questionnaire, SAQ)
У ході проведення QSA-аудитори збирають свідоцтва виконання вимог до стандарту й зберігають їх протягом трьох років	В ході перевірки ISA-фудитори збирають свідоцтва виконання вимог стандарту і зберігають їх протягом трьох років	Збір свідоцтв виконання вимог стандарту не потребується
За результатами QSA робить звіт у відповідності до (Report on Compliance, ROC)	За результатами ISA робить звіт у відповідності до (Report on Compliance, ROC)	Відмінним документом є самостійно заповнений лист самооцінки SAQ

Класифікація Visa, торгово-сервісні підприємства

Рівень	Критерій	Підтвердження згідно з PCI DSS
1	- обробка більше 6 млн. транзакцій на рік, або - вирішення о призначенні 1 рівня	- QSA або ISA щорічно - ASV щоквартально
2	- обробка від 1 до 6 млн. транзакцій на рік	- SAQ щорічно - ASV щоквартально
3	- обробка від 20 тис. до 1 млн. транзакцій на рік з використанням електронної комерції	- SAQ щорічно - ASV щоквартально
4	- обробка до 20 тис. транзакцій на рік з використанням електронної комерції, або до 1 млн. транзакцій на рік іншими засобами	- SAQ щорічно - ASV щоквартально