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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Циватого Дениса Олександровича*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Аудит комерційного банку на відповідність стандарту PSI DSS v4.0*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	професор Котух Є.В.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.	90	відмінно	

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Циватому Денису Олександровичу* **академічної групи** *125м-21-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Аудит комерційного банку на відповідність стандарту PSI DSS v4.0*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.2022 № 1200-с

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання, загальні теоретичні відомості.	17.10.2022
Розділ 2	Застосування стандарту до типової інформаційної системи. Реалізація вимог стандарту	22.11.2022
Розділ 3	Поточні, капітальні витрати, економічна доцільність проведення аудиту .	05.12.2022

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

Дата видачі завдання: 14.09.2022р.

Дата подання до екзаменаційної комісії: 21.12.2022р.

Прийнято до виконання _____ Циватий Д.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 69 ст. , 12 рис. ,5 табл. ,5 додатків,13 джерел.

Об'єкт розробки: процес аудиту комерційного банку на відповідність стандарту PCI DSS v4.0

Мета проекту: адаптація проходження аудиту комерційного банку вимог стандарту PCI DSS v4.0

У першому розділі проведений аналіз проведений аналіз .стандарту PCI DSS v4.0, приведені зв'язки стандарту PCI DSS з іншими стандартами, також обгрунтовано процедуру проходження аудиту.

У другому розділі була описана реалізація виконання вимог стандарту PCI DSS v4.0 на прикладі типової системи на базі СУБД Oracle. Також приведені вимоги до серверів баз даних, файлових сервері та вплив впроваджених рішень на продуктивність системи.

В економічній частині проведений розрахунок капітальних витрат на проведення аудиту .

Практичне значення проекту полягає в розробці процедури проведення аудиту та впровадженні рішень для його проходження.

СТАНДАРТ, АУДИТ, БАЗА ДАННИХ , СИСТЕМА УПРАВЛІННЯ БАЗАМИ ДАНИХ

ABSTRACT

Explanatory note: 69 pages, 12 figures, 5 tables, 5 annexes, 13 sources.

Object of development: the process of auditing a commercial bank for compliance with PCI DSS v4.0.

Purpose of the project: adaptation of the audit procedure for passing the audit of a commercial bank to the requirements of the PCI DSS v4.0 standard

In the first section the analysis of the PCI DSS v4.0 standard was carried out, the connections of the PCI DSS standard with other standards were given, the procedure for passing the audit was also substantiated.

The second section describes the implementation of the requirements of the PCI DSS v4.0 standard on the example of a typical system based on Oracle DBMS. The requirements for database servers, file servers and the impact of the implemented solutions on system performance are also given.

In the economic part of the calculation of capital expenditures for the audit.

The practical significance of the project is to develop an audit procedure and implement solutions for its passage.

STANDARD, AUDIT, DATABASE, DATABASE MANAGEMENT SYSTEM

СПИСОК УМОВНИХ СКОРОЧЕНЬ

API — Application Programming Interface

BIN — Банківській ідентифікаційний номер

PAN — Номер платіжної картки

PCI DSS — Payment Card Industry Data Security Standard

PCI SCC — PCI Security Standards Council

TACACS — Terminal Access Controller Access Control System

АС — Автоматизована система

ДПК — Дані платіжних карток

ДДК — Дані держателів карток

КАД — Критичні автентифікаційні дані

МСП — Малі та середні підприємства

ПЗ — Програмне забезпечення

ПК — Портативний комп’ютер

ОС — Операційна система

ЗМІСТ

ВСТУП

Ринок пластикових карток в Україні почав розвиватися з кінця 20 століття, проте пластикові картки перестали бути для нас екзотикою і стали звичними в найрізноманітніших сферах діяльності - під час одержання заробітної плати, під час оплати товарів і послуг, під час поїздок у відрядження. Сьогодні практично не залишилося жодного банку, який би не пропонував клієнтам розмістити грошові кошти на "пластик".

Тисячі людей і численні організації володіють пластиковими картками міжнародних і внутрішніх платіжних систем, локальними картками різних банків, користуються їх перевагами. Пластикові картки дивують дедалі більше і більше своєю різноманітністю.

Власник картки, прийшовши в пункт обслуговування, пред'являє картку до оплати товарів (послуг) або для отримання готівки. Пунктом обслуговування може бути не тільки торговельно-сервісне підприємство, а й відділення банку або банкомат - у разі видачі готівки. Працівник пункту обслуговування перевіряє справжність картки і повноваження тримача розпоряджатися нею, використовуючи для цього дані, зазначені на самій картці. Потім він проводить процедуру авторизації, здійснюючи запит до Банку, що випустив картку , про підтвердження повноважень держателя картки та його фінансових можливостей. Результатом виконання процедури авторизації є дозвіл або заборона на здійснення операції. Технологія авторизації залежить від схеми платіжної системи, типу картки та технічного оснащення пункту обслуговування.

Авторизаційна інформація вкрай приваблива для різного роду шахраїв, оскільки, володіючи секретними даними, зловмисники з легкістю можуть отримати доступ до коштів клієнта. Таким чином, проблема захисту інформації стоїть дуже гостро. Для захисту інформації існує спеціальний

стандарт PCI DSS, що регламентує процес передачі та зберігання авторизаційної інформації.

Для безпечного використання пластикових карток ухвалено комплекс заходів, сформульованих у вигляді спеціального стандарту з інформаційної безпеки (Payment Card Industry Data Security Standard, PCI DSS).

Дія PCI DSS поширюється на торговельно-сервісні підприємства та постачальників послуг, що працюють з міжнародними платіжними системами, тобто на всіх, хто передає, обробляє і зберігає дані власників карток. Це стосується як загальних даних - номер картки (Primary Account Number, PAN), ім'я власника картки, код обслуговування, дата видачі та закінчення терміну дії, так і критичних даних авторизації (sensitive authentication data) - повний вміст магнітної смуги, коди CVC2/CVV2/CID і PIN-блок. Елементи даних необхідно захищати, якщо вони зберігаються спільно з номером картки, а після завершення процедури авторизації критичні дані не повинні зберігатися навіть у зашифрованому вигляді. Вимоги стандарту PCI DSS не застосовуються, якщо не виконується зберігання, обробка або передача номера картки (PAN)[1].

Вимоги PCI DSS поширюються на всі системні компоненти, зокрема на мережеве обладнання, сервери та додатки, які входять до складу середовища даних платіжних карток (частина мережі, в якій обробляються дані платіжних карток або критичні дані авторизації) або безпосередньо до нього під'єднані. До мережевих компонентів належать (але не обмежуються ними) міжмережеві екрани, комутатори, маршрутизатори, бездротові точки доступу, пристрої захисту інформації та інше мережеве обладнання. Серед типів серверів - сервери Web, сервери баз даних, автендифікаційні та поштові сервери, proxy-, NTP-, DNS- та інші сервери. До переліку додатків входять усі придбані та розроблені додатки, як внутрішні, так і зовнішні.

Банки (для яких, здебільшого, і було розроблено цей стандарт) тільки нещодавно стали проводити будь-які заходи для відповідності вимогам цього

стандарту. Новизна стандарту і мала кількість досліджень механізмів реалізації вимог створює додаткові складнощі при впровадженні PCI DSS.

У межах цієї роботи було поставлено за мету проаналізувати вимоги стандарту і підготувати набір скриптів, що дає змогу спростити адміністраторам АБС проведення робіт із підготовки до аудиту PCI DSS. У цій роботі будуть проводитися дослідження в рамках СУБД Oracle. Таким чином, додатковим завданням роботи є демонстрація тих вимог стандарту, які можна реалізувати засобами СУБД Oracle і дружніх їй технологій.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 ЗАГАЛЬНИЙ АНАЛІЗ СТАНДАРТІВ PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) — стандарт із сфери кібербезпеки, спрямований на максимальний захист карткових даних при їх зберіганні, обробці або передачі. Був розроблений у грудні 2004 року при загальній участі п'яти транснаціональних корпорацій у сфері платіжних карт: Visa, MasterCard, American Express, Discover Financial Services, JCB International.

Версії стандарту наведені у таблиці 1.1.

Таблиця 1.1.Версії стандарту PCI DSS

Версія	Дата впровадження	Коментарі
1.0	15 грудня 2004	Перша версія
1.1	Вересень 2006	Були додані невеликі уточнення та виправлення
1.2	Жовтень 2008	Формулювання були змінені на більш однозначні, підвищена гнучкість стандарту, була здійснені зміни для усунення нових вразливостей та загроз.
1.2.1	Липень 2009	Були приведені невеликі зміни задля ще більшої ясності стандарту та кращої узгодженості між ним та іншими супровідними документами. Зміни у формулюванні у таблиці компенсаційного контролю.
2.0	Жовтень 2010	Були додані пояснення до деяких вимог, змінені деякі посилання на глосарій, введено термін «тримач картки», додано, що сегментація може бути реалізована фізичними та логічними методами. Були дані додаткові рекомендації по вимогам стандарту, окремо винесена інформація о ролі стандарту PCI DSS у захисті карткових даних.

3.0	Листопад 2013	Потерпіли зміни процедури перевірки вимог стосовно використання антивірусу та проведення тестів на проникнення, їх стало загалом більше та вони стали більш конкретними.
3.1	Квітень 2015	Розширена інформація у розділі «компенсаційні міри», розширені пояснення до вимог, змінені деякі посилання на глосарій та офіційний сайт стандарту PCI DSS.
3.2	Квітень 2016	Були додані додаткові вимоги, виключно до сервіс-провайдерів, бажані до виконання.
3.2.1	Травень 2018	Були визнані обов'язковими для виконання вимоги, що стосувалися сервіс-провайдерів. Дійсний наразі стандарт.
4.0	Грудень 2020	Планувалося впровадження у другому кварталі 2021-го року, проте через карантин було відкладене

Дія PCI DSS поширюється на торговельно-сервісні підприємства та постачальників послуг, що працюють з міжнародними платіжними системами, тобто на всіх, хто передає, обробляє та зберігає дані власників карток. Це стосується загальних даних :

- номер картки (Primary Account Number, PAN);
- ім'я власника картки;
- код обслуговування;
- дата видачі та закінчення терміну дії;

Та критичних даних авторизації :

- повний вміст магнітної смуги;
- коди CVC2/CVV2/CID;
- PIN;

Елементи даних необхідно захищати, якщо вони зберігаються спільно з номером картки, а після завершення процедури авторизації критичні дані не повинні зберігатися навіть у зашифрованому вигляді. Вимоги стандарту PCI

DSS не застосовуються, якщо не виконується зберігання, обробка або передача номера картки (PAN).

Вимоги PCI DSS поширюються на всі системні компоненти, зокрема на мережеве обладнання, сервери та додатки, які входять до складу середовища даних платіжних карток (частина мережі, в якій обробляються дані платіжних карток або критичні дані авторизації) або безпосередньо до нього під'єднані. До мережевих компонентів належать міжмережеві екрани, комутатори, маршрутизатори, бездротові точки доступу, пристрої захисту інформації та інше мережеве обладнання. Серед типів серверів - сервери Web, сервери баз даних, автендифікаційні та поштові сервери, proxy-, NTP-, DNS- та інші сервери. До переліку додатків входять усі придбані та розроблені додатки, як внутрішні, так і зовнішні.

Залежно від кількості оброблюваних за рік транзакцій (до 120 тис., до 600 тис., до 6 млн., понад 6 млн.) компанії присвоюють певний рівень з обов'язковим набором вимог з безпеки. Процедури підтвердження відповідності стандарту включають щорічний аудит, щоквартальне сканування мережі на наявність вразливостей і, в деяких випадках, заповнення аркуша самооцінки (Self Assessment Questionauire). Для виконання аудиту та сканування мереж компанії повинні залучати сторонню організацію, що має статус Qualified Security Assessor (QSA, для аудиту) і Approved Scanning Vendor (ASV, для сканування мережі). Згадані статуси присвоюються радою PCI Security Standards Council.

1.2 ОБЛАСТЬ ЗАСТОСУВАННЯ PCI DSS

Таблиця 1.2 ілюструє найчастіше використовувані елементи даних про власників карток і критичних автендифікаційних даних; дозволене або

заборонене їхнє зберігання; чи повинен бути захищений кожен із цих елементів.

Вимоги PCI DSS застосовні до системи, якщо в ній зберігається, обробляється або передається номер картки (PAN). Якщо PAN не зберігається, не обробляється і не передається, то вимоги PCI DSS не застосовуються

Таблиця 1.2 Вимоги до захисту даних

	Єлементи даних	Зберігання дозволено	Потребується захист
Данні про тримача картки	Номер платіжної картки (PAN)	Так	Так
	Ім'я тримача картки (Cardholder Name)*	Так	Так
	Сервісній код (Service Code)*	Так	Так
	Дата закінчення терміну дії картки (Expiration Date)*	Так	Так
Критичні автендифікаційні данні**	Вся магнітна смуга Карты***	Ні	
	CAV2/CVC2/CVV2/CID	Ні	
	PIN / PIN Block	Ні	

Ці елементи даних мають бути захищені в разі, якщо зберігаються спільно з PAN. Цей захист має відповідати вимогам PCI DSS щодо безпеки середовища даних про тримачів карток. Хоча PCI DSS не вимагає захисту таких даних, якщо не передається, не зберігається та не обробляється PAN, їх захист і розкриття застосовуваних компанією методів обробки та зберігання персональних даних клієнтів може знадобитися згідно з вимогами інших законодавчих актів (наприклад, захист персональних даних, забезпечення конфіденційності, запобігання крадіжці ідентифікатора або забезпечення безпеки даних).

Критичні автендифікаційні дані не повинні зберігатися після авторизації (навіть у зашифрованому вигляді).

1.3 РОЗТАШУВАННЯ ДАНИХ ПЛАТІЖНИХ КАРТ І КРИТИЧНИХ ДАНИХ АВТОРИЗАЦІЇ

Критичні дані авторизації містять магнітну смугу , код перевірки автентичності та PIN-код.

Відповідно до стандартного PCI DSS зберігати критичні дані авторизації заборонено. Бо за допомогою цих даних зловмисники можуть генерувати підроблену інформацію карт і проводити шахрайські операції.

На рисунку 1.1 зображення лицьового та зворотного боку платіжної картки, на яких показано розташування даних платіжних карток і критичних даних авторизації.

Рисунок 1.1 Розташування даних на картці

Зашифровані дані магнітної смуги, які використовуються для авторизації під час транзакцій, що вимагають присутності картки. Ці дані можуть також розташовуватися в образі магнітної смуги на чипі або в іншому місці на карті. Після авторизації організації не повинні зберігати повні дані, зчитані з магнітної смуги. Дозволяється зберігання тільки таких елементів

даних магнітної смуги, як номер картки, ім'я власника картки, дата закінчення терміну дії та сервісний код[3].

Він же CAV, CVC, CVV або CSC - три- або чотиризначне число, надруковане на картці праворуч від місця для підпису або на лицьовому боці картки, що використовується для перевірки транзакцій без присутності картки.

Персональний ідентифікаційний номер (PIN), що вводиться власником картки під час транзакцій, які потребують присутності картки, та/або зашифрований PIN-блок, який присутній у повідомленні транзакції.

Якщо повний образ магнітної смуги на чипі збережено, то зловмисники, отримавши доступ до цих даних, зможуть створювати копії платіжних карток і продавати їх по всьому світу. Крім того, зберігання повного треку порушує правила роботи в платіжних системах і може призвести до штрафів і пені.

На рисунках 1.2 та 1.3 наведено зображення треку 1 і треку 2, а також показано відмінності між ними[7].

Трек 1 містить усі поля треку 1 і треку 2. Максимальна довжина треку становить 79 символів.

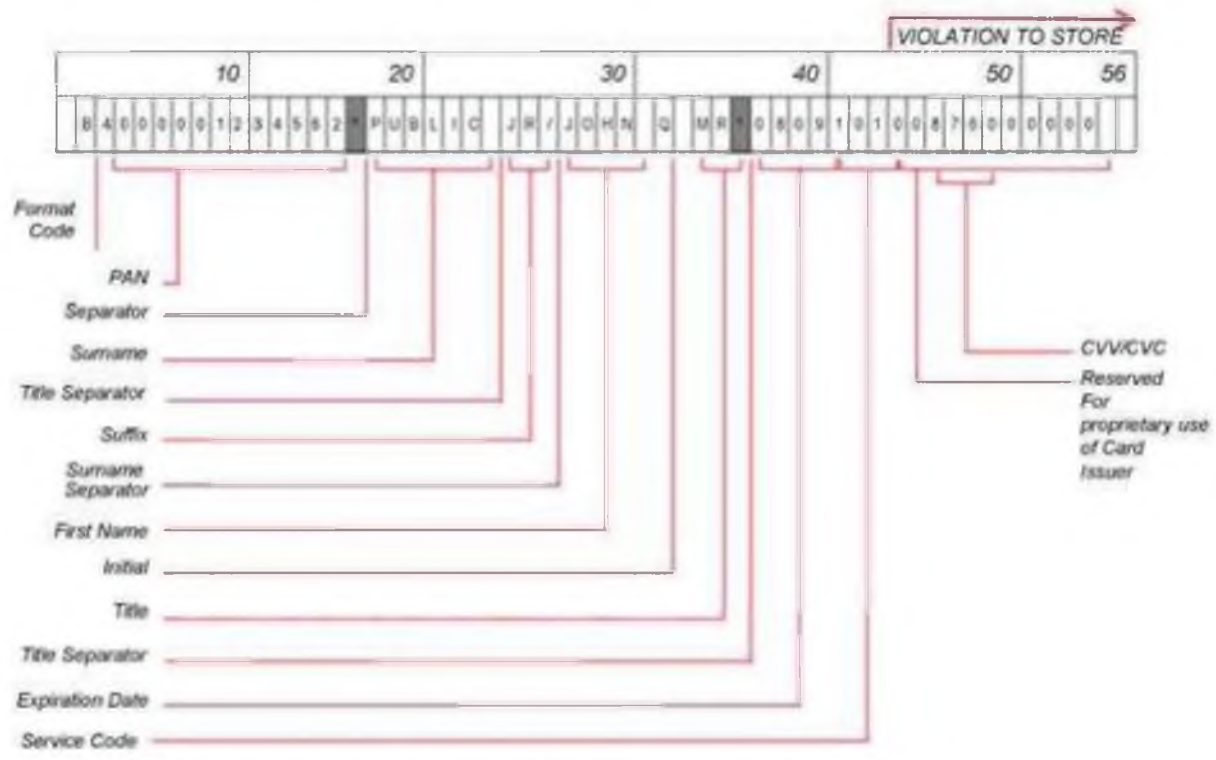


Рисунок 1.2 Вміст образу магнітної смуги(трек 1)

Трек 2 використовується для більш швидкого опрацювання в разі передачі інформації з використанням комутованого з'єднання. Максимальна довжина треку становить 40 символів.

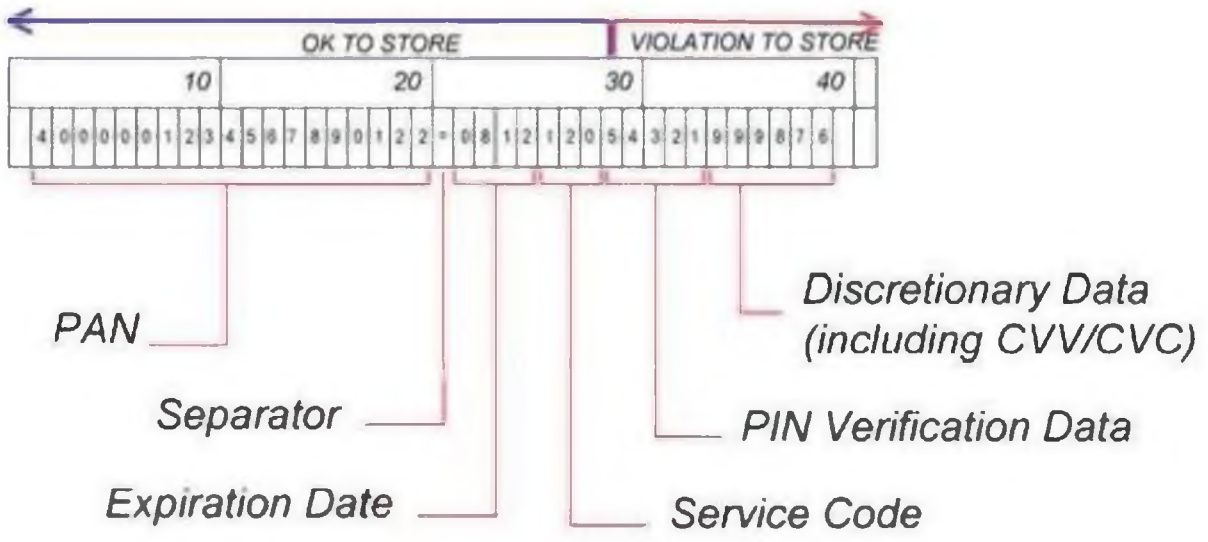


Рисунок 1.3 Вміст образу магнітної смуги(трек 2)

1.4 ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ

На сьогодні світ все більше та більше переходить у віртуальний простір. Комп'ютерні мережі зберігають державні таємниці, секрети добробуту корпорацій, гроші, особисту інформацію кожного. Люди самі довіряють свої таємниці та гроші комп'ютерним системам, не уявляючи іншого, а тому й кількість бажаючих на цьому заробити росте відповідно.

У сферах, що стикаються з картковими даними основними стандартами кібербезпеки є стандарт PCI DSS (розроблений консорціумом запровадженим транснаціональним корпораціям Visa, MasterCard, American Express, Discover Financial Services, JCB International).

Стандарт PCI DSS є більш самостійний, у загальному він (крім вимог, що стосуються виключно карткових даних) підійде як гарний «порадник» та «інструкція» з комп'ютерної безпеки для будь-якої організації, не зважаючи на специфіку її роботи та інформації, що вона зберігає або оброблює[8].

Стандарт PCI DSS v4.0 є новим тому є необхідність в адаптації існуючих методів реалізації до нових вимог стандарту.

У роботі будуть розгянуті вимоги та запропонована їх реалізація відповідно до стандарту PCI DSS :

- парольної автентифікації;
- захисту зберігання даних платіжних карток;
- захисту доступу;
- розмежування доступу;
- впровадження аудиту дій співробітників;
- вимоги до серверів;

2.СПЕЦІАЛЬНА ЧАСТИНА

2.1 Завдання та вимоги стандарту PCI DSS

Стандарт PCI DSS складається з шести завдань і дванадцяти основних вимог. Короткий виклад вимог наведений нижче:

Завдання 1. Побудова та підтримка захищеної мережі.

У документах, поширюючим основний стандарт PCI DSS: Guidance for PCI DSS Scoping and Network Segmentation. У Додатку Г приведен приклад схеми сегментації, що був представлений як приклад у документі, що доповнює стандарт PCI DSS, «Guidance for PCI DSS Scoping and Network Segmentation». Відповідно до цього прикладу мережа організації поділяється на три умовні зони: що мітить ДТК, для адміністрування зони з ДТК та загальна корпоративна мережа[4].

Завдання 2. Захист даних платіжних карток.

Захист даних на носії забезпечують два компоненти СУБД Oracle - пакети, що реалізують алгоритми шифрування та опція Transparent Data Encryption (TDE). Опція TDE з'явилася у версії СУБД Oracle 10g Release 2 як складова частина технології Advanced Security. Вона дає змогу вибірково шифрувати колонки таблиць із застосуванням алгоритму AES (з довжиною ключа 128, 192 або 256 біт). Керування ключами шифрування перебирає на себе ядро БД, а застосування такого шифрування не потребує переробки клієнтського і серверного прикладного ПЗ. У версії СУБД 11g і вище з'явилася можливість зашифрування табличного простору цілком.

Завдання 3: Реалізація програми управління вразливостями.

Для захисту системи використовується антивірусне ПЗ Cisco AMP.

Використання Cisco AMP надає такі переваги:

- Фільтрація файлів, що порушують політику, з Інтернету, електронної пошти тощо.

- Виявлення і захист від спроб експлойтів на стороні клієнта і спроб експлойтів, спрямованих на клієнтські додатки, як-от Java і Flash.
- Розпізнавання, блокування та аналіз шкідливих файлів.
- Виявлення шкідливих програм і виявлення потенційно зламаних пристроїв.
- Відстеження поширення шкідливих програм і комунікацій.
- Зниження загроз повторного зараження

Завдання 4: Реалізація заходів щодо суворого контролю доступу.

Аутентифікація в контексті Oracle означає перевірку автентичності будь-кого або будь-чого - користувача, застосунку, пристрою, кому або чому потрібен доступ до даних, ресурсів або застосунків. Після успішної процедури аутентифікації слідує процес авторизації, що передбачає призначення певних прав, ролей і привілеїв для суб'єкта аутентифікації.

Завдання 5. Регулярний моніторинг і тестування мереж.

Стандарт PCI DSS передбачає регулярне різнопланове сканування системи, як один з елементів її захисту.

Перший вид сканування — сканування мережі Wi-Fi.

Установка та/або використання бездротових технологій в мережі є одними з найбільш часто використовуваних зловмисниками способів для отримання доступу до мережі та ДТК. Якщо бездротовий пристрій або мережа встановлені без відома організації, зловмисник може легко та непомітно проникати через них у мережу самої організації. Несанкціоновані бездротові пристрої можуть бути приховані або підключені до комп'ютера, іншого компоненту системи або безпосередньо до порту або інших мережних пристроїв, такому як маршрутизатор або комутатор. Будь-який такий несанкціонований пристрій може виконувати роль несанкціонованої точки доступу у мережу. Знаючи, які бездротові пристрої санкціоновані, адміністратори можуть швидко виявляти несанкціоновані бездротові пристрої, а, реагуючи на виявлення несанкціонованих бездротових точок

доступу, організація може завчасно знизити вразливість середовища ДТК до таких дій зловмисників. Оскільки підключити до мережі бездротову точку доступу нескладно, визначити її наявність важко, а ризик від несанкціонованих бездротових пристроїв підвищений, ці процеси слід виконувати навіть при наявності політики, яка забороняє використання бездротових технологій. Розмір та складність певного середовища обумовлює необхідність використання відповідних інструментів та процесів, які досить надійно усунуть можливість встановлення несанкціонованої точки доступу в середовищі[9].

Наступний тип сканування (з вимоги 11.2) — сканування (внутрішнє та зовнішнє) на вразливості. І якщо внутрішнє сканування є самим звичайним, яке кожна організація може сама для себе проводити (тим же Nexpose або Nessus), то зовнішнє сканування має свої особливості, визначені стандартом PCI DSS. Його має право проводити тільки сертифікована для цього компанія (ASV-компанія, від назви самого виду сканування — ASV).У Додатку К надано приклад титульного листу при зеленому звіту після проходження ASV-сканування.

Наступне сканування (вимога 11.3) — тест на проникнення, також зовнішній та внутрішній.

Мета тесту на проникнення — змоделювати реальну атаку, щоб виявити, наскільки глибоко зловмисник зможе проникнути в середу. Завдяки цьому, організація може краще розібратися в своїх потенційних вразливості і розробити стратегію захисту від атак.

Тест на проникнення відрізняється від сканування на наявність вразливостей тим, що перший є активним процесом і він може включати експлуатацію виявлених вразливостей. Сканування на наявність вразливостей може бути першим, але точно не єдиним кроком, який виконує фахівець по тестах на проникнення, щоб визначити стратегію тестування.

Навіть якщо сканування на наявність вразливостей не може виявити відомі уразливості, фахівець по тестах на проникнення часто отримує достатньо інформації про систему, щоб виявити потенційні проблеми безпеки.

Тести на проникнення зазвичай виконуються вручну. Навіть використовуючи автоматизовані засоби, тестувальник повинен застосовувати свої знання систем для проникнення в мережу.

Тести на проникнення, що виконуються за графіком та після значних змін в середовищі організації (її мережі) — це превентивна міра, що дозволяє зменшити ризик доступу зловмисників до середовища ДТК.

І останнє сканування, яке виконується виключно у організаціях, що має сегментовану мережу (вимога 11.3.4) — тест на проникнення для контролю сегментації.

Тест на проникнення для контролю сегментації — це важливий інструмент перевірки, що реалізована сегментація дійсно ізолює середу ДТК від інших мереж. Такий тест на проникнення необхідно націлити на засоби сегментації, які використовуються як на кордоні (периметрі), так і всередині мережі організації, але поза середовищем ДТК. Він повинен підтвердити, що неможливо подолати засоби сегментації та отримати доступ до середовища ДТК. Наприклад, перевіривши мережу та/або просканувавши її на наявність відкритих портів (наприклад, утилітою nmap), можна переконатися, що між мережами, що входять в область застосовності, та іншими мережами підключень нема[10].

Завдання 6. Підтримка політики інформаційної безпеки.

2.1 Опис змін з версії PCI DSS 3.2.1 на 4.0

Нижче наведений список змін між стандартами PCI DSS 3.2.1 та PCI DSS 4.0:

Розділ 1. Розширено спектр мережевих технологій. Уточнено мету з контролю між довіреними та недовіреними мережами, у тому числі бездротовими. Деталізовано та розширено вимоги. Частину пунктів вимог декомпозовано.

Розділ 2. Запроваджується вимога 2.1.2 щодо опису, прийняття та виконання обов'язків. Уточнено вимоги щодо небезпечних служб та протоколів.

Розділ 3. Значно деталізовані вимоги щодо зберігання критичних даних до завершення авторизації (3.2.1, 3.3.2). Без ключової виробничої необхідності дозволяється відображати лише 4 останні цифри під час маскування. Вимоги до Хеш. Шифрування на рівні диска або розділу використовується лише для змінних носіїв. Забороняється використовувати однакові ключі для тестового та виробничого середовищ.

Розділ 4. Про реєстри довірених ключів та сертифікатів, контроль їх термінів дії.

Розділ 5. Розширені вимоги та формулювання щодо антивірусного ПЗ, обліку в оцінці ризиків і навіть захисту від фішингових атак.

Розділ 6. Розділено ПЗ для внутрішнього та стороннього користування. Містить вимогу до реєстру ПЗ. Вимоги щодо усунення загроз для публічних Web додатків. Вимоги до скриптів на платіжних сторінках.

Розділ 7. Нові вимоги щодо перевірки доступу та облікових записів.

Розділ 8. Окремо виокремлено вимоги до терміналів точок продажу. Вимога збільшення довжини пароля з 7 до 12 символів. Окремі зазначені

зменшені вимоги для терміналів точок продажу (у разі одномоментного доступу до 1 PAN).

Вимога впровадження багатофакторної аутентифікації (MFA) для всіх видів доступу до CDE. Заборона хардкодити паролі у файлах та скриптах.

Розділ 9. Окремо виокремлено вимоги до відвідувачів. Змінено вимоги до зберігання, обліку та знищення носіїв.

Розділ 10. Вимагає використання автоматичних механізмів для перевірки журналів аудиту. Цільовий аналіз ризиків. Виявляти, попереджати та оперативно усувати збої критичних систем контролю безпеки.

Розділ 11. Вимога щодо проведення внутрішніх сканувань з автентифікацією. Вимога до управління всіма знайденими вразливістями (а не лише критичними). Вимоги щодо виявлення змін вмісту платіжних сторінок. Виявлення прихованих каналів передачі даних.

Розділ 12. Зміни щодо оцінки ризиків, вимога проведення цільового аналізу ризиків. Для постачальників послуг — документувати та підтверджувати сферу застосування PCI DSS не рідше ніж кожні 6 місяців. Вимога щодо оновлення програми підвищення поінформованості раз на 12 місяців. Частота навчання персоналу має ґрунтуватися на проведеному аналізі ризиків.

Для того щоб показати відповідність системи стандарту було обрано типову систему на базі СУБД Oracle. СУБД Oracle є одною з найпопулярніших СУБД. Також СУБД Oracle має набір вбудованих інструментів які можна використовувати для того, щоб система відповідала вимогам стандарту PCI DSS. [2]

2.2 Застосування стандарту PCI DSS до тестової інформаційної системи

2.2.1 Реалізація вимог до парольної автентифікації

Простота використання парольного захисту не викликає сумнівів. Надійність пароля і, отже, безпека його використання, безпосередньо залежить від його якості (застосовувані символи, їхній регістр, відмінність від осмислених слів). Зручність використання стрімко падає навіть за незначного посилення "безпеки" пароля, адже запам'ятати комбінацію символів, яку неможливо прочитати, досить складно. Звернемося до цифр і фактів. Паролі користувачів зберігаються в СУБД Oracle у вигляді хеш-значень і доступні для читання привілейованим користувачам. Алгоритм обчислення хеша пароля давно відомий. Найповніше дослідження стійкості паролів в Oracle проведено компанією Red - Database - Security GmbH - провідного світового експерта в галузі безпеки продуктів Oracle. Ось деякі дані щодо стійкості паролів для версій СУБД 15-19c:

На комп'ютері з i3 3.7 GHz необхідний час становить (атака простим перебором):

10 секунд усі 5-символьні комбінації;

5 хвилин усі 6-символьні комбінації;

2 години всі 7- символьні комбінації;

2,1 дня всі 8- символьні комбінації;

57 днів усі 9- символьні комбінації;

4 роки всі 10- символьні комбінації.

І це при використанні далеко не найпотужнішого комп'ютера. При нарощуванні продуктивності атака за словником проводиться ще швидше. Не можна сказати, що Oracle не реагує на такий стан справ - у версії СУБД 12c становище значно покращилося. Було посилено алгоритм вироблення хеша і

якість формування паролів. У результаті наведені вище цифри зросли в 2.5-3 рази. Але, незважаючи на такі поліпшення, Oracle рекомендує використовувати засоби посиленої автентифікації, які також були допрацьовані в кращий бік, наприклад, стало можливо використовувати HSM (Hardware Security Module) для автентифікації та зберігання ключів шифрування.

У зв'язку з ситуацією, що склалася, необхідно виконувати деякі вимоги під час реалізації парольної політики.

- Заборонено використовувати поділювані ідентифікатори доступу (облікові записи та паролі), зокрема в адміністративних цілях.

- Кожному користувачеві має бути видано унікальне значення як пароль, що використовується під час первинної реєстрації в системі (first-time password).

- Необхідно використовувати функціональність системи, яка примусово вимагає зміни пароля під час його використання вперше.

- Паролі користувачів задовольняють різним вимогам безпеки:

- довжина пароля не менше 12 символів;
- обов'язкове використання в паролі букв і цифр;
- повторна реєстрація того ж самого пароля можлива тільки через 4 заміни.
- Необхідно встановити обмеження для спроб введення неправильного пароля (не більше ніж 6 разів); у разі перевищення система має блокувати можливість доступу до системи для цього облікового запису щонайменше протягом 30 хвилин або доти, доки адміністратор не розблокує можливість доступу.
- Необхідно використовувати функціональність блокування невикористовуваних облікових записів.

СУБД Oracle дає змогу виконувати перевірку висунутих до паролів вимог за допомогою функцій стандартного SQL-скрипта. Саме за допомогою

цього інструменту можна здійснити відповідність вимогам, пов'язаним із парольною політикою, а конкретно - вимогу 2.8 стандарту. Зокрема виконання автоматичної перевірки якості паролів під час їх формування реалізовано за допомогою функції "PASSWORD_VERIFY_FUNCTION" СУБД Oracle.

Кожен банк у кінцевому підсумку самостійно визначає свою парольну політику, відповідно і функція PASSWORD_VERIFY_FUNCTION розробляється на розсуд банку. Нижче наведено приклад цієї функції для нашої інформаційної системи:

```
grant connect to demo identified by demo
go
call sa_make_object('function','fn_verify_pwd')
go
alter function fn_verify_pwd(uid char(128),pwd char(128))
returns varchar(255)
begin

declare i int;
declare code int;
declare lowerfound int;
declare upperfound int;
declare numfound int;
set upperfound=0;
set lowerfound=0;
set numfound=0;
set i=1;
if length(pwd) < 12 then
message 'Password not changed';
```

```
return( 'Password is not long enough.' );
end if;
if pwd=uid then
message 'Password not changed';
return( 'Password must be different from user name' );
end if;

while i <= length(pwd) loop
set code= ascii(substring(pwd,i,1));
if code between 65 and 90 then
set upperfound=1;
end if;
if code between 97 and 122 then
set lowerfound=1;
message 'lower';
end if;
if code between 48 and 58 then
set numfound=1;
end if;
set i=i+1;
end loop;
message (lowerfound+upperfound+numfound);
if ((lowerfound+upperfound+numfound) < 3) then
message 'Password not changed';
return( 'Password rules have not been satisfied.' );
end if;
return(NULL);
end
go
```

```
alter function fn_verify_pwd set hidden
go
grant execute on fn_verify_pwd to PUBLIC
go
set option PUBLIC.verify_password_function = 'DBA.fn_verify_pwd'
go
```

Слід пред'являти підвищені вимоги до якості паролів для облікових записів користувачів, які володіють правами адміністратора СУБД.

2.2.2 Реалізація вимог до захисту зберігання даних платіжних карток

Оскільки інформація про власника картки зберігається в БД, необхідно забезпечити шифрування критично важливих з точки зору безпеки даних. Для цього рекомендується використовувати технологію Oracle Advanced Security Transparent Data Encryption (TDE)[13].

Нижче наведено схему використання технології Oracle TDE:

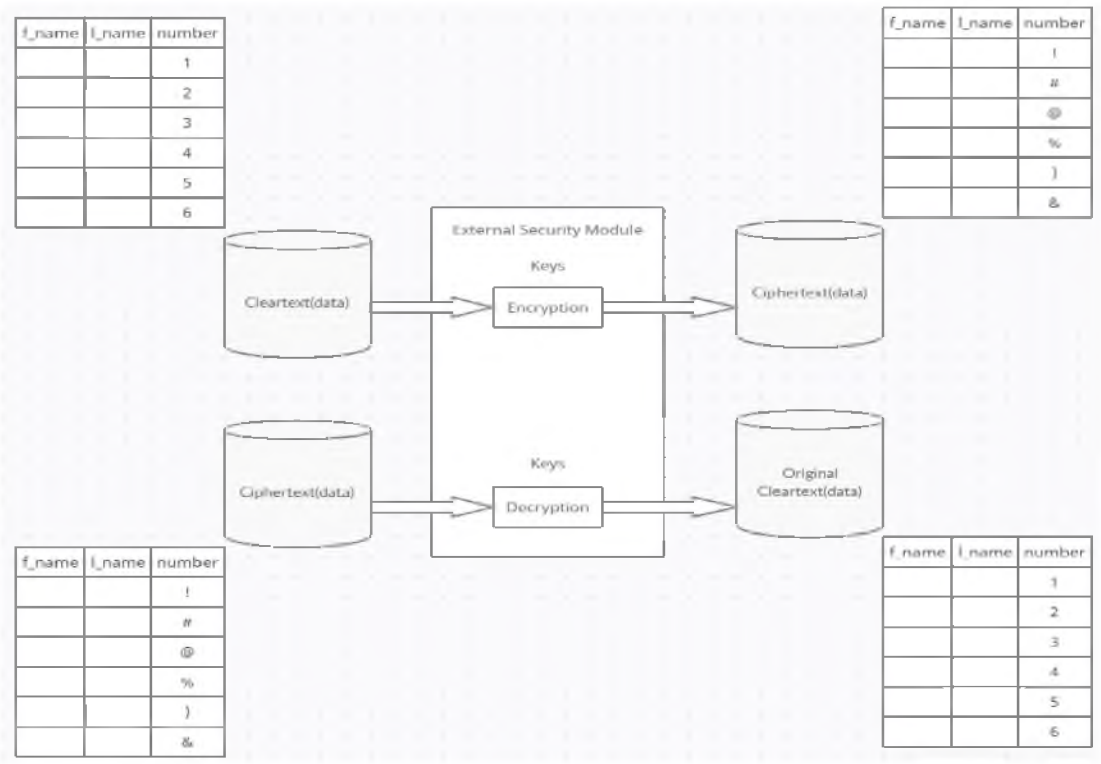


Рисунок 2.1 – Процедура шифрування стовбців

Користувач вибирає набір стовпців, які необхідно піддати шифруванню.

У разі вставки даних у таблицю, інформація у відповідному стовпці шифрується сервером бази даних і зберігається. За необхідності доступу до даних шифрованого стовпця, дані автоматично розшифровуються. Дані шифруються спеціальним ключем, без якого доступ до даних неможливий. Для кожної таблиці використовується свій ключ шифрування.

Для захисту згаданих ключів використовується головний ключ, яким шифрується набір усіх використаних ключів. Цей ключ зазвичай зберігається у файлі операційної системи, який називається wallet або гаманець. Його зберігання необхідно здійснювати в захищеному місці, окремо від даних бази. Під час вставки даних у зашифрований стовпчик, сервер Oracle Database 10g витягує з wallet'a майстер-ключ, розшифровує ключ шифрування для цієї таблиці, який міститься у словнику даних, використовує цей ключ для шифрування вхідного значення і зберігає зашифровані дані в базі даних.

Дані зберігаються зашифрованими, тому всі компоненти нижнього рівня, такі, як резервні копії та архівні журнальні файли, також мають шифрований формат.

Ця технологія дає змогу підвищити безпеку зберігання даних - у разі, якщо дані буде вкрадено з диска, зловмисник не може отримати доступ до них без майстер-ключа, що зберігається в wallet'e. У разі, якщо wallet буде вкрадений, головний ключ не може бути витягнутий з нього без знання пароля гаманця. Отже, зловмисник не зможе розшифрувати дані, навіть якщо він вкрав диски або копії файлів даних.

Для тестової інформаційної системи було розроблено низку скриптів, що дають змогу налаштувати TDE для тих стовпчиків, шифрування яких необхідне. Увімкнення TDE здійснюється в кілька етапів які наведені у таблиці 2.3:

Таблиця 2.1 Скрипти для тестової інформаційної системи

Назва етапу	Основна команда	Коментарі
Визначте розташування гаманця	ENCRYPTION_WALLET_LOCATION = (SOURCE= (METHOD=file) (METHOD_DATA= (DIRECTORY=/orawall)))	У файлі sqlnet.ora створюється блок із посиланням на директорію зберігання wallet'a.
Створення гаманця	alter system set encryption key authenticated by "pwd";	У результаті цієї команди в каталозі, який був визначений на попередньому кроці, створюється гаманець із паролем "pwd"; Також гаманець відкривається для зберігання і вилучення головного ключа засобами TDE.
Відкриття гаманця	alter system set encryption wallet open authenticated by "pwd";	Необхідно явно відкривати гаманець після відкриття бази.
Шифрування стовпців	alter table transaction modify (card_number encrypt);	При первинному використанні цього оператора для таблиці створюється ключ для цієї таблиці. Усі значення стовпця перетворюються в шифрований вигляд.

Додатково необхідно вирішити такі питання:

- де перебуватиме гаманець із майстер-ключем: на зовнішньому диску, на внутрішньому диску або на спеціальному пристрої безпеки;
- як обмежити права доступу до гаманця і запобігти його крадіжці;
- як організувати безпечне резервне копіювання гаманця. Необхідно врахувати, що неприпустимо зберігати гаманець або його копію разом із резервним сховищем бази даних.

Також існує набір компенсаційних заходів, які додатково мають бути виконані для відповідності вимогам до зберігання даних:

- Історичні дані (включно з даними власників карток і криптографічними даними з вичерпаним терміном придатності/необхідності зберігання) повинні автоматично видалятися із системи за допомогою процедур архівування, які необхідно регулярно виконувати. Зберігання архівних даних архівування має здійснюватися в зашифрованому вигляді.
- Необхідно регулярно виконувати архівування файлів обміну з платіжними системами, їх зберігання має здійснюватися в зашифрованому вигляді.
- Необхідно регулярно виконувати архівування звітів, що формуються в системі, їх зберігання має здійснюватися в зашифрованому вигляді.
- Заборонено зберігати будь-які критично важливі з погляду безпеки дані на машинах, що перебувають у демілітаризованій зоні (DMZ).
- Дані, отримані в процесі виявлення причин несправностей у роботі системи, повинні гарантовано видалятися безпосередньо після виконання необхідних процедур.

Крім того, відповідно до вимог платіжних систем заборонено зберігання такої інформації про картку:

- інформацію, що записується на магнітні доріжки (tracks);
- величини Card Validation Value of Code (CAV, CVC, CVV або CSC);

- величини Card Validation Value of Code другого типу (CAV2, CMC2, CVV2 або CID);
- величини PVV;
- зашифровані значення PIN-коду (encrypted PIN).

2.2.3 Реалізація інструменту для пошуку критичної інформації в інформаційній системі.

Для того, щоб захищати будь-яку інформацію, необхідно зрозуміти, де конкретно в системі зберігаються дані про власників карток (PAN), і навіть якщо у компаній є хоч якась схема потоків даних, то на ділі виявляється, що дані виявляються в будь-яких і навіть найнесподіваніших місцях. Основні, але не єдині місця, де можна виявити PAN, - це trace, log, tlog, debug файли СУБД, застосунків і web-служб, а також файлові та поштові сервери, робочі станції операторів, POS-сервери.

Результатом аналізу можливих місць зберігання критичних даних є матриця даних.

Складання матриці даних - це перший етап з'ясування місць знаходження PAN, але не останній, тому що, крім відомих місць, завжди трапляються й невідомі, пошук яких дає змогу побачити реальну картину. Для полегшення робіт з виявлення даних про власників карток можна використовувати розроблені скрипти. Скрипти засновані на регулярних виразах з пошуку номерів карток.

Регулярні вирази, що дають змогу шукати номери карт без пробілів:

```
Visa: ^4[0-9]{12}(?:[0-9]{3})?$
MasterCard: ^5[1-5][0-9]{14}$
```

Однак у деяких випадках номер картки може зустрічатися у вигляді набору цифр, розділених тире або пробілами (наприклад, 3711-078176-01234). У цих випадках для пошуку PAN необхідно використовувати складніший регулярний вираз.

Приклад регулярного виразу, що дає змогу шукати номери карток із можливими пробілами:

```
^((4\d{3})|(5[1-5]\d{2}))(-?|\040?)(\d{4}(-?|\040?)){3}|^(3[4,7]\d{2})(-?|\040?)\d{6}(-?|\040?)\d{5}
```

Цей вираз перевіряє наявність номерів кредитних карток від Visa, MasterCard і Amex як у вигляді рядка з цифр, так і з роздільниками.

Після того, як було знайдено вирази, що потрапляють під регулярні вирази, необхідно провести додаткову перевірку того, що знайдена послідовність дійсно є PAN. Для цього необхідно перевірити коректність контрольної цифри за алгоритмом Луна.

Усі ці перевірки було реалізовано для нашої системи в скрипті find.sql. Під час запуску скрипта find.sql формується файл з інформацією про список файлів, у яких фігурують номери карток у відкритому вигляді.

2.2.4 Захист доступу

Аутентифікація в контексті Oracle означає перевірку автентичності будь-кого або будь-чого - користувача, застосунку, пристрою, кому або чому потрібен доступ до даних, ресурсів або застосунків. Після успішної процедури аутентифікації слідує процес авторизації, що передбачає призначення певних прав, ролей і привілеїв для суб'єкта аутентифікації.

Oracle надає різноманітні способи автентифікації та дає змогу застосовувати один або кілька з них одночасно. Спільним для всіх цих способів є те, що як суб'єкт аутентифікації використовується ім'я користувача. Для підтвердження його автентичності може запитуватися деяка додаткова інформація, наприклад, пароль. Аутентифікація адміністраторів СУБД Oracle вимагає спеціальної процедури, що зумовлено специфікою посадових обов'язків і ступенем відповідальності цього співробітника. Програмне забезпечення Oracle також зашифровує паролі користувачів для безпечного передавання мережею.

Нижче більш детально розглянуто способи аутентифікації під час використання СУБД Oracle .

Аутентифікація засобами операційної системи

Низка операційних систем дозволяють СУБД Oracle використовувати інформацію про користувачів, якими керує власне ОС. У цьому разі користувач комп'ютера має доступ до ресурсів БД без додаткової вказівки імені та пароля - використовуються його мережеві облікові дані. Цей вид аутентифікації вважається небезпечним і використовується, в основному, для аутентифікації адміністратора СУБД.

Аутентифікація за допомогою мережевих сервісів

Цей вид аутентифікації забезпечується опцією сервера Oracle Advanced Security. Розглянемо варіант аутентифікації з використанням протоколу SSL

(Secure Socket Layer) - протокол рівня додатків. Він може використовуватися для автентифікації в БД і в загальному випадку (якщо далі використовується автентифікація користувача засобами СУБД) не залежить від системи глобального управління користувачами, що забезпечується службою каталогу Oracle - Oracle Internet Directory.

2.2.4 Розмежування доступу

Маючи на меті захист БД від інсайдерських загроз, для забезпечення розмежування доступу у версії СУБД 10g Release 3 компанія Oracle випустила новий продукт Database Vault, призначений для запобігання несанкціонованому доступу до інформації користувачів, у тому числі наділених особливими повноваженнями, наприклад, адміністраторів бази даних. Набір правил у Database Vault, що розмежовують доступ, досить широкий. Усі ці правила допомагають реалізувати вимогу 7 стандарту PCI DSS ("доступ до даних платіжних карток має бути обмежений відповідно до службової необхідності"). Таким чином, Database Vault вирішує такі проблеми:

- обмеження доступу до даних адміністратора БД та інших привілейованих користувачів;
- запобігання маніпулюванню з базою даних і зверненню до інших додатків адміністратора додатків;
- забезпечення контролю над тим, хто, коли і звідки може отримати доступ до додатка[13].

2.2.5 Огляд технології Database Vault і реалізація налаштувань для тестової інформаційної системи

Для реалізації розмежування доступу до тестової карткової системи розглядатимемо такі налаштування:

- Можливість обмежувати (виключати) доступ до даних додатків з боку адміністратора бази даних (DBA)
- Можливість забезпечення доступу до даних на основі динамічно настроюваних правил

Обидві ці функціональності дають змогу здійснити вимогу 10.

Розглянемо докладніше пропоновані можливості:

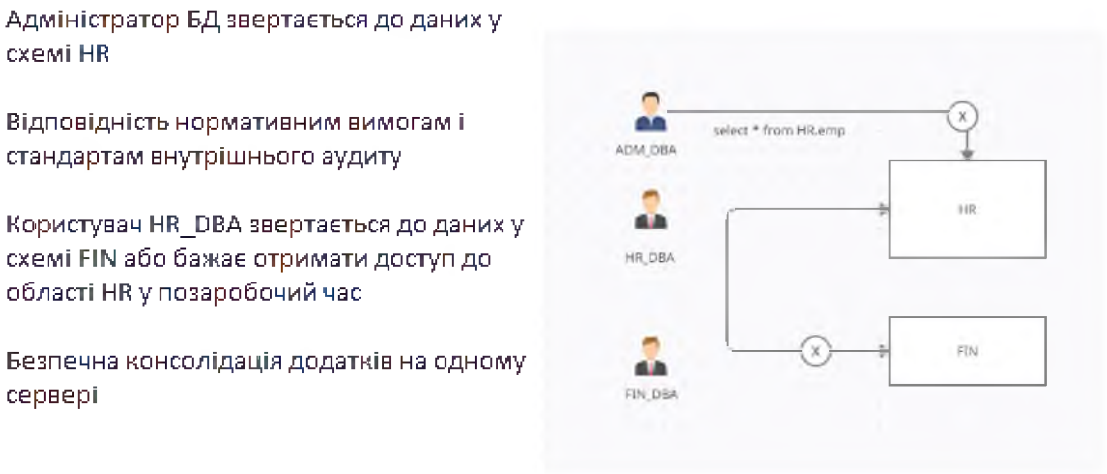


Рисунок 2.2 – Доступ до БД з правами адміністратора

Дійсно, користувач SYS, давши собі, наприклад, привілей SELECT ANY TABLE, може отримати доступ до секретної інформації. З точки зору стандарту PCI DSS така можливість неприпустима. Нижче на рисунку 2.3 наведено приклад звернення користувача з адміністративними привілеями до секретних даних.

```
SQL>
SQL> show user
USER is "SYSTEM"
SQL>
SQL> select user, employee_id, last_name, ssn, salary from hr.employees
  2  where employee_id < 117
  3  /

USER       EMPLOYEE_ID LAST_NAME       SSN           SALARY
---------- ----------- --------------- ----------- ----------
SYSTEM             100 King            111-22-333       24000
SYSTEM             101 Kochhar         222-22-333       17000
SYSTEM             102 De Haan         333-22-333       17000
SYSTEM             103 Hunold          444-22-333        9000
SYSTEM             104 Ernst           555-22-333        6000
SYSTEM             105 Austin          666-22-333        4800
SYSTEM             106 Pataballa       777-22-333        4800
SYSTEM             107 Lorentz         888-22-333        4200
SYSTEM             108 Greenberg       999-22-333       12000
SYSTEM             109 Faviet          123-22-333        9000
SYSTEM             110 Chen            123-22-444        8200
SYSTEM             111 Sciarra         123-22-222        7700
```

Рисунок 2.3 – Звернення до БД з правами адміністратора

Доступ до захищених даних з боку адміністратора відкритий

За допомогою web-інтерфейсу технології Database Vault налаштовується захищена область, до якої у користувача SYS доступу не буде. Нижче наведено інтерфейс налаштувань. У тому числі в системі є можливість увімкнення аудиту на неуспішні спроби доступу до захищених даних. Web-інтерфейс технології Database Vault наведений на рисунку 2.3

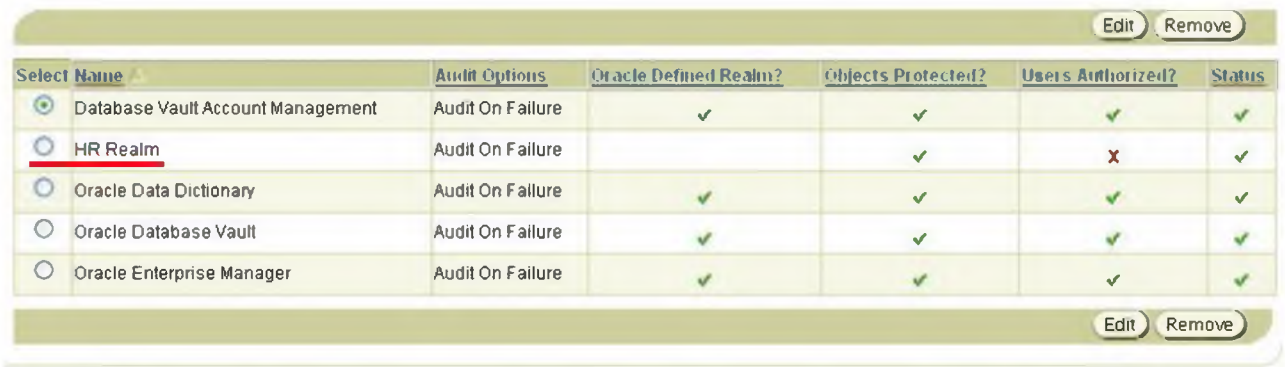


Рисунок 2.4 – Web-інтерфейс технології Database Vault

Налаштування захищеної області

Після цього налаштування навіть користувач із правами адміністратора не може здійснити звернення до захищених даних. Це показано на рисунку 2.4:

```
select user, employee_id, last_name, ssn, salary from hr.employees
                                                    *
ERROR at line 1:
ORA-01031: insufficient privileges
```

Рисунок 2.5 – Звернення до БД з правами адміністратора

Заборона доступу до захищених даних.

Далі розглянемо можливість налаштування динамічних правил для контролю забезпечення доступу до даних. Для банківської інформаційної системи може бути використаний свій набір зумовлених правил. Їх вибір залежить від політики безпеки банку. Наведемо список усіх зумовлених правил безпеки в СУБД Oracle і розглянемо приклад налаштування правила Client IP для нашої інформаційної системи.

Заздалегідь визначені правила безпеки.

Нехай стоїть завдання обмеження виконання команд адміністратором системи віддалено. У системі є можливість налаштування правил для всіх можливих команд адміністратора. На рисунку 2.5 показано перелік команд які можно обмежити.

Select	Command	Object Owner	Object Name	Rule Set Name	Status
◉	ALTER PROFILE	%	%	Can Maintain Accounts/Profiles	✔
○	ALTER USER	%	%	Can Maintain Own Account	✔
○	CREATE PROFILE	%	%	Can Maintain Accounts/Profiles	✔
○	CREATE USER	%	%	Can Maintain Accounts/Profiles	✔
○	DROP PROFILE	%	%	Can Maintain Accounts/Profiles	✔
○	DROP USER	%	%	Can Maintain Accounts/Profiles	✔
○	GRANT	SYS	DBMS_RLS	Can Grant VPD Administration	✔
○	REVOKE	SYS	DBMS_RLS	Can Grant VPD Administration	✔

Рисунок 2.6 – Налаштування правил для команд адміністратора

Під час налаштування правила вибирається конкретна команда адміністратора.

Після вибору команди, яку необхідно обмежити, вибираємо налаштування CLIENT IP, параметризуючи клієнтську ip-адресу. На рисунку 2.6 показано можливість доступу тільки з однієї IP адреси.

Рисунок 2.7 – Налаштування можливості доступу тільки з однієї IP-адреси.

Після налаштування цієї опції користувач із правами адміністратора не може отримати доступ до системи в разі, якщо доступ здійснюється віддалено зі сторонньої IP-адреси. Також варто зазначити, що невдалі спроби доступу можна аудіювати.

```
Connected to:
Oracle Data Vault Release 10.2.0.1.0 - Development
With the Partitioning, Oracle Label Security, OLAP, Data Mining
and Oracle Data Vault options

SQL>
SQL> show user
USER is "SYSTEM"
SQL>
SQL> alter system switch logfile;
alter system switch logfile
*
ERROR at line 1:
ORA-01031: insufficient privileges
```

Рисунок 2.8 – Неможливість доступу з сторонньої IP-адреси.

Неможливість здійснення доступу адміністратором системи зі сторонньої IP-адреси.

На рисунку 2.9 приведено список команд для яких доступні налаштування:

Alter Database	Alter Database	Alter Table
Alter Function	Audit	Alter Tablespace
Alter Package Body	Alter Procedure	Alter Profile
Alter Session	Alter System	Alter Synonym
Alter Table	Alter Trigger	Alter User
Password	Alter Tablespace	Alter View
Change Password	Connect	Comment
Create Function	Create Index	Create Package
Create Database Link	Create Procedure	Create Role
Create Package Body	Create User	Create View
Create Table	Grant	Insert
Noaudit	Rename	Lock Table
Create Tablespace	Create Trigger	Truncate Table
Update	Insert	Delete
Execute	Select	

Рисунок 2.9 – Список команд .

2.2.5 Впровадження аудиту дій співробітників

Найцікавішою є реалізація вимоги 10 стандарту PCI DSS (доступ до мережевих ресурсів і даних платіжних карт слід контролювати). Для забезпечення цієї вимоги найзручніше використовувати вбудований засіб СУБД Oracle - аудит. Ця технологія дає змогу контролювати як доступ до даних, так і події реєстрації/виходу та зміни структури БД. Також з 9 версії СУБД oracle дає змогу вмикати детальний аудит (Fine Grained Audit Control). Ця опція дає змогу проводити аудит доступу за умовами, які визначаються досить гнучкими правилами, що налаштовуються. Розглянемо докладніше цю технологію і реалізацію налаштувань для нашої інформаційної системи.

Усі активності в системі можна розбити на 2 групи: активності користувача й активності адміністратора. Нижче у таблиці 2.1 наведено список основних активностей у базі даних:

Таблиця 2.2 Список основних активностей у БД

Название действия	User actions	Admin actions	Чи потрібно вести аудит дій
MODIFYING DB SCHEME	Ні	Так	Так
EDITING PRIVILIGES	Ні	Так	Так
GRANT/REVOKE	Ні	Так	Так
SELECT	Так	Так	Так
UPDATE	Так	Так	Так
INSERT	Так	Так	Так
DELETE	Так	Так	Так

Увімкнення аудиту здійснюється за допомогою такої команди:

alter system set audit_trail=xml, extended scope=spfile;

Ця команда дає змогу здійснювати зберігання журналів аудиту на дисковій системі, а не у файлах БД. Це налаштування вкрай важливе, оскільки відповідно до стандарту безпеки PCI DSS, необхідно обмежити доступ DBA до файлів аудиту.

Розташування файлу задається параметром "audit_file_dest" СУБД Oracle.

Для тестової інформаційної системи було реалізовано пакет audit.sql, за допомогою якого можна ввімкнути аудит і легко здійснити налаштування аудіювання.

За допомогою цього пакета вмикається аудит дій адміністратора. У різних банківських системах правила аудиту можуть відрізнятися (аудит - це завжди компроміс між безпекою і продуктивністю).

Нижче наведено приклад команди для ввімкнення аудиту дій адміністратора:

```
audit
alter system,
CLUSTER,
DATABASE LINK,
INDEX,
MATERIALIZED VIEW,
NOT EXISTS,
PROCEDURE,
PUBLIC DATABASE LINK,
PUBLIC SYNONYM,
ROLE,
SEQUENCE,
SESSION,
SYSTEM AUDIT,
SYSTEM GRANT,
TABLE,
TABLESPACE,
TRIGGER,
USER, VIEW
by access
```

Приклад використання пакета audit для налаштування аудиту користувачів:

```
audit.audit_object(object => 'client', columns => null);
```

Команда встановлює аудит на доступ до таблиці client. У разі, якщо в параметрі columns вказується список стовпців, аудит буде вестися тільки при

доступі до конкретних полів таблиці. В інших випадках журналювання не ведеться.

У разі якщо необхідно вимкнути аудит для всіх таблиць - використовується команда audit.noaud_forall;

Крім описаних вище вимог на підставі інформації, витягнутої зі стандарту PCI DSS, можна висунути такі вимоги.

2.3 Вимоги до серверів

2.3.1 Вимоги до сервера бази даних

Сервер бази даних (БД) повинен знаходитися в окремому сегменті внутрішньої мережі банку, доступ до якого захищений за допомогою окремого міжмережевого екрана (firewall).

Будь-яка мережева взаємодія із сервером БД здійснюється тільки дротовими каналами зв'язку. Використання бездротових каналів зв'язку суворо заборонено.

Невикористовувані облікові записи користувачів СУБД, у тому числі службові, мають бути заблоковані або видалені. Для використовуваних службових облікових записів користувачів, зокрема створених за замовчуванням і під час встановлення програмного забезпечення, мають бути змінені паролі доступу.

Не використовуються незахищені протоколи віддаленого доступу.

Зупинено або заблоковано всі невикористовувані, а також потенційно небезпечні сервіси операційної системи і додатки на сервері.

Ведеться аудит засобами операційної системи. Журнали аудиту зберігаються не менше трьох місяців. Старі журнали вивантажуються і зберігаються разом з іншими архівними даними.

У разі необхідності виконати трасування запитів до СУБД Oracle рекомендується його виконувати без збереження значень Bind-змінних.

Виконуються рекомендації згідно з документом "Oracle Database Security and the Payment Card Industry Data Security Standard".

2.3.2 Вимоги до файлового сервера

Файловий сервер знаходиться в окремому сегменті внутрішньої мережі банку, доступ до якого захищений за допомогою окремого міжмережевого екрана.

Будь-яка мережева взаємодія з файловим сервером здійснюється тільки дротовими каналами зв'язку. Використання бездротових каналів зв'язку суворо заборонено.

Не використовуються незахищені протоколи віддаленого доступу.

Зупинено або заблоковано всі невикористовувані, а також потенційно небезпечні сервіси операційної системи (зокрема Restore Points ОС Windows) і додатки на сервері.

Ведеться аудит засобами операційної системи. Журнали аудиту зберігаються не менше трьох місяців. Старі журнали вивантажуються і зберігаються разом з іншими архівними даними.

2.3.3Вимоги до робочих станцій користувачів

Доступ у зовнішню мережу з робочих станцій має здійснюватися тільки через міжмережеві екрани.

Автоматичне блокування клієнтських додатків має виконуватися через 15 хвилин простою.

Мережева взаємодія між віддаленими робочими місцями та внутрішньою мережею банку повинна виконуватися тільки дротовими

каналами зв'язку і при використанні захищеного з'єднання (VPN або TLS/SSL). Використання бездротових каналів зв'язку суворо заборонено.

Рекомендується при організації доступу з віддалених робочих місць використовувати фіксовані MAC- і IP-адреси.

ODBC-трасування на робочих станціях має бути вимкнено.

Зупинено або заблоковано всі невикористовувані, а також потенційно небезпечні сервіси операційної системи (зокрема Restore Points ОС Windows), і сторонні додатки.

2.3.4 Вимоги для доступу до даних

Кожному користувачеві має бути присвоєно унікальний ідентифікатор (створено обліковий запис) для доступу в систему. Заборонено використовувати поділювані ідентифікатори доступу, зокрема в адміністративних цілях.

Для доступу користувачів до даних, що містяться в БД, повинні використовуватися тільки додатки, що поставляються в комплекті з системою, при роботі з якими в системних журналах гарантовано ведеться аудит дій користувачів, а також не використовуються адміністративні облікові записи (такі як "sys") для доступу до даних.

Після закриття доступу для облікових записів користувачів ці облікові записи мають бути видалені протягом 90 днів.

При будь-якому віддаленому доступі до системи повинен використовуватися механізм двофакторної аутентифікації.

Для шифрування неконсольного адміністративного доступу до системи мають використовуватися протоколи SSH, SSL/TLS або VPN.

2.3.5 Вимоги до передачі даних

Будь-яка передача даних, що містять інформацію про карткові контракти, клієнтів та іншу критично важливу з погляду безпеки інформацію (у тому числі дані, отримані в процесі виявлення причин несправностей у роботі системи), може здійснюватися тільки в зашифрованому вигляді. Шифрування даних має забезпечуватися зовнішніми технічними засобами.

Передача PIN-блока на будь-якому з підтримуваних інтерфейсів повинна здійснюватися в зашифрованому вигляді з використанням ключа подвійної довжини.

2.3.6 Вимоги до конфігурації системи

Для відповідності вимогам безпеки необхідне виконання таких умов у конфігурації системи:

Доступ до форм, що містять інформацію про карткові дані та держателів карток, обмежений і видається тільки в разі службової необхідності.

Засобами архівування даних регулярно (щодня) видаляються дані, зберігання яких заборонено, з відповідних таблиць бази даних.

Будь-яка система, що містить компоненти платіжних додатків, має бути розміщена у внутрішній мережі банку, ізольованій від демілітаризованої зони.

2.3.7 Вимоги до даних, що використовуються під час тестування системи

Не допускається використовувати реальні дані в тестових цілях.

Якщо тестова система формується з виробничої, то дані про карткові контракти, клієнтів, значення ключів та інша критична з погляду безпеки інформація має бути попередньо шифрована.

Вимоги до даних, що використовуються під час налагодження системи

Збір критичної з погляду безпеки (передавторизаційної) інформації, необхідної для налагодження роботи системи, допускається тільки за явної необхідності вирішення певної ситуації. Обсяг інформації не повинен перевищувати обсягу, достатнього для усунення неполадок у ситуації, що виникла.

Ця інформація має зберігатися в строго обумовлених місцях, доступ до неї має бути обмежений. Зберігання інформації має здійснюватися в зашифрованому вигляді.

Інформація, що використовується для налагоджувальних робіт, має гарантовано видалятися негайно після усунення неполадок.

2.3.8Вплив на продуктивність

Після приведення системи до відповідності вимогам стандарту постає питання обмежень. Головним чином позадеренні технології впливають на продуктивність системи. Нижче буде розглянуто вплив технологій Oracle Audit і Oracle TDE на роботу тестової інформаційної системи.

У рамках даної роботи було проведено стрес-тестування, спрямоване на приблизне прогнозування падіння продуктивності при використанні заявлених технологій. Для здійснення стрес-тестування були написані скрипти, за допомогою яких емулювалося навантаження на розроблену тестову карткову систему. Скрипти здійснюють операції вибірки, вставки, видалення та модифікації даних. Усі операції здійснюються в циклі для забезпечення необхідного навантаження на базу даних.

До впровадження інструментарію було виконано заміри, що дають змогу визначити продуктивність системи. Існує безліч різних метрик продуктивності інформаційних систем, як-от: кількість транзакцій на секунду, середній час проходження транзакції, кількість транзакцій, час виконання певних процедур на базі (наприклад, видалення даних із таблиць). У цій роботі як метрику було обрано показник кількості транзакцій за секунду або, як зазвичай його називають, - TPS (Transactions per second).

Після ввімкнення аудиту та шифрування на тестовій інформаційній системі було повторно проведено низку тестів. При цьому показники продуктивності змінилися таким чином:

Таблиця 2.3 Падіння продуктивності при ввімкненні аудиту

Опція, що вмикається	Падіння продуктивності(%)	Додаткові коментарі
ORACLE Audit	10	Падіння продуктивності безпосередньо залежить від ступеня деталізації аудиту. Необхідно використовувати аудіювання з найменшим можливим ступенем деталізації (з точки зору безпеки).
Oracle TDE	30	Необхідно скоротити кількість стовпців, що шифруються, до можливого мінімуму (з погляду безпеки). Необхідно проводити аналіз планів запитів під час шифрування індексованих стовпців.

Нижче наведено аналіз причин падіння продуктивності під час увімкнення цих технологій.

Під час увімкнення аудиту продуктивність системи падає, оскільки в системі генерується велика кількість подій під час доступу до того чи іншого об'єкта. Число цих подій безпосередньо залежить від ступеня деталізованості аудиту. Для кожної такої події породжується запис у журналі аудиту. Усі ці події впливають на продуктивність системи.

У разі ввімкнення шифрування в разі, якщо запит звертається до незашифрованих стовпців таблиці, продуктивність збігається з продуктивністю системи без опції шифрування. У разі звернення до шифрованих стовпців, витрачаються ресурси на дешифрування зашифрованих даних. Однак варто зазначити, що ввімкнення опції Oracle TDE може докорінно впливати на продуктивність окремих запитів. Подібний вплив є наслідком використання індексів. Розглянемо цю ситуацію на прикладі створеної тестової інформаційної системи:

У системі існує індекс PK_TRANSACTIONS за стовпцем TRANSACTIONS.ID. Отже, якщо запит до таблиці TRANSACTIONS використовує діапазонне сканування до цього індексу до впровадження шифрування, то після ввімкнення опції Oracle TDE така дія втратить будь-який сенс, тому що в разі, якщо стовпчик ID зашифрували, то фактичні значення в індексі відрізнятимуться, і записи, що мають схожі фактичні значення, можуть бути розкидані по всьому індексу. Це є причиною зростання вартості використання даного індексу. Сервер Oracle в даному випадку може взагалі ігнорувати індекс і використовувати full scan всієї таблиці. Це зі свого боку може призвести до різкого зростання часу виконання запиту.

Таким чином, перед шифруванням полів, що індексуються, необхідно проводити глибокий аналіз запитів на предмет можливого впливу шифрування на плани цих запитів.

ВИСНОВКИ

У сферах, що стикаються з картковими даними основним стандартом кібербезпеки є стандарт PCI DSS .При умові побудови системи з урахуванням вимог стандартів PCI DSS вона може вважатися такою, що є безпечною для зберігання в ній карткових даних. Проте так само така система може надійно зберігати будь-які конфіденційні дані.

Загалом, було проведене комплексне дослідження стандартів PCI DSS, що дало змогу зробити відповідні висновки, щодо їх «самостійності» та технічній складовій у них зазначеній. Відповідно до цього стандарт PCI DSS є більш технічно визначений, з чіткими та детальними вимогами до технічної частини. Відповідно до яких нормуються використання різних методів шифрування каналів зв'язку, загальним напрям налаштувань міжмережевого екрану (за яким все що не відповідає максимальній службовій необхідності, повинно бути вимкнено).

Було проведено детальний аналіз вимог стандартів PCI DSS та розроблена тестова система, структура якої створювалася з оглядом на вимоги стандартів. Результатом є структуровані поради та приклади яким чином виконуються ті або інші вимоги зазначених стандартів.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічних розрахунків кваліфікаційної роботи є обґрунтування доцільності запровадження запропонованих в роботі рішень.

Для виконання економічного розділу необхідно:

- розрахувати капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення та ін.;
- розрахувати річні експлуатаційні витрати на утримання і обслуговування об'єкта ;
- визначити річний економічний ефект;
- визначити показники економічної ефективності.

3.1 Розрахунок капітальних витрат на аудит

Спочатку, необхідно визначити трудомісткість аудиту.

Трудомісткість проведення аудиту визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з проведення аудиту):

$$t = t_{тз} + t_к \text{ годин}, \qquad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на проведення аудиту;

$t_к$ – тривалість розробки концепції проведення аудиту ;

t =35 год+60 год

t = 95 год.

Розрахуємо витрати на проведення аудиту. Розрахунок проводиться за формулою 3.2:

$$K_{рп} = З_{зп} + З_{мч} \text{ грн.} \quad (3.2)$$

де $K_{рп}$ – витрати на проведення аудиту;

$З_{зп}$ – заробітна плата аудитора;

$З_{мч}$ – вартість витрат машинного часу, що необхідні для проведення аудиту. Витрати на заробітну плату аудитора розраховуються за формулою 3.3:

$$З_{зп} = t \cdot З_{іб}, \text{ грн,} \quad (3.3)$$

де t – загальна тривалість проведення аудиту, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Средньогодинна заробітна плата аудитора становить – 115 грн/год.

Відповідно до формули 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 95 \text{ год} \cdot 115 \text{ грн/год,}$$

$З_{зп}$ = 10925 грн.

У свою чергу, витрати машинного часу визначаються за формулою 3.4:

$$З_{мч} = t \cdot С_{мч} \text{ грн.} \quad (3.4)$$

де t – трудомісткість проведення аудиту на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

$$С_{мч} = P \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р} \text{, грн,} \quad (3.5)$$

де P – встановлена потужність ПК, кВт;

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

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

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

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

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

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

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$C_{мч} = 0,75 \cdot 1 \cdot 1,57 + (22000*0,04)\backslash 1920 + (13300*0,1)\backslash 1920 \text{ грн},$$

$$C_{мч} = 2,33 \text{ грн.}$$

$$З_{мч} = 2,33*95=221,35 \text{ грн}$$

Отже, витрати на проведення аудиту за формулою 3.2 становлять:

$$K_{рп} = 211,35+10925= 11136,35 \text{ грн.}$$

В результаті розрахунків, вартість капітальних витрат на розробку методикипроведення аудиту становить – 11136,35 гривень.

3.2 Розрахунок поточних(експлуатаційних) витрат

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

Оскільки аудит потрібно проводити 2 роки то експлуатаційні витрати за рік можна порахувати за формулою 3.6:

$$t = (t_{па} + t_{ас} + t_{ва}) \times 2 \text{ годин}, \quad (3.6)$$

$t_{па}$ – тривалість процесу первинного аудиту системи;

$t_{ас}$ – тривалість проведення аудиту СМИБ;

$t_{ва}$ – тривалість віддаленого аудиту (якщо він потрібен);

$t_{тд}$ – тривалість заповнення технічної документації після проведення процедури аудиту ;

$$t = (15 \text{ год} + 11 \text{ год} + 6 \text{ год} + 17 \text{ год}) \times 2$$

$$t = 98 \text{ год.}$$

Розрахуємо витрати на проведення аудиту. Розрахунок проводиться за формулою 3.7:

$$K_{рп} = З_{зп} + З_{мч} \text{ грн.} \quad (3.7)$$

де $K_{рп}$ – витрати на проведення аудиту;

$З_{зп}$ – заробітна плата аудитора;

$З_{мч}$ – вартість витрат машинного часу, що необхідні для проведення аудиту. Витрати на заробітну плату аудитора розраховуються за формулою 3.8:

$$З_{зп} = t \cdot З_{іб}, \text{ грн,} \quad (3.8)$$

де t – загальна тривалість проведення аудиту, годин;

$З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Средньогодинна заробітна плата аудитора становить – 115 грн/год.

Відповідно до формули 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 98 \text{ год} \cdot 115 \text{ грн/год},$$

$$З_{зп} = 11270 \text{ грн}.$$

У свою чергу, витрати машинного часу визначаються за формулою 3.9:

$$З_{мч} = t \cdot С_{мч} \text{ грн}. \quad (3.9)$$

де t – трудомісткість проведення аудиту на ПК, годин;

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

Вартість 1 години машинного часу ПК визначається за формулою 3.10:

$$С_{мч} = P \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн}, \quad (3.11)$$

де P – встановлена потужність ПК, кВт;

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

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

H_a – річна норма амортизації на ПК, частки одиниці;

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

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

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

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$C_{мч} = 0{,}75 \cdot 1 \cdot 1{,}57 + (25000*0{,}04)\backslash 1920 + (13300*0{,}1)\backslash 1920 \text{ грн},$$

$$C_{мч} = 2{,}42 \text{ грн.}$$

$$З_{мч} = 2{,}42*98=237{,}16 \text{ грн}$$

Отже, витрати на проведення аудиту за формулою 3.7 становлять:

$$K_{рп} = 237{,}16+11270= 11507{,}16 \text{ грн.}$$

В результаті розрахунків, вартість проведення аудиту становить – 11507,71 гривень.

3.3 Розрахунок витрат при виникненні загроз

Метою цієї оцінки є визначення обсягів матеріальних збитків, виходячи з імовірності реалізації конкретної загрози й можливих матеріальних втрат від неї.

Вірогідність проходження аудиту вираховується за формулою 3.7

$$П_Н = 100 - ((\ К_В * 100) / К_О) \quad (3.8)$$

де $П_Н$ – відсоток реалізації загрози , %;

$К_О$ – загальна кількість вимог, шт;

$К_В$ – кількість вимог , яким відповідає банк , шт;

Таким чином, згідно з формулою 3.8:

$$П_Н = 100 - (10*100)/12 = 16{,}7\%$$

При непроходженні аудиту стандарту PSI DSS комерційний банк не має можливості працювати з даними тримачів карток . Результат непроходження аудиту закриття комерційного банку . Витрати при непроходженні аудиту можна розрахувати за формулою 3.8 становить:

$$U = (П_п \times П_в) \times П_Н \text{ грн}, \quad (3.8)$$

де $П_п$ – середня сума транзакції, грн;

$П_в$ – середня кількість транзакцій за рік , шт;

$П_н$ – відсоток реалізації загрози ;

Таким чином, згідно з формулою 3.8:

$$U = 427 \times 12000000 \times 0{,}167 = 855708000 \text{ грн}$$

Таким чином втрати при непроходжені аудиту становитимуть 855708000 грн.

3.4 Висновок економічної частини

Під час виконання економічної частини проведені основні розрахунки капітальних витрат на проведення аудиту.

А саме під час підрахунків було визначено, що:

1. Капітальні витрати на проведення аудиту становлять 10252,71 грн.
2. Повна вартість річних експлуатаційних витрат становить 11507,16 грн

3. При непроходжені аудиту банк лишається можливості обробляти данні тримачів карток , тобто працювати з даними емітентів , проходження аудиту являється обов'язковим для будь-якого банку. Втрати при непроходженні аудиту становитимуть приблизно 855708000 грн.

Отже дані які були отримані в ході виконання економічної частини, вказують на доцільність проходження аудиту за для відповідності стандарту PCI DSS v4.0.

ПЕРЕЛІК ПОСИЛАНЬ

1.Офіційний сайт Стандарту PCI DSS //[Електронний ресурс] – Режим доступу: https://www.pcisecuritystandards.org/

2. Короткий огляд змін від PCI DSS версії 3.2.1 до 4.0//[Електронний ресурс] – Режим доступу: https://listings.pcisecuritystandards.org/documents/PCI-DSS-Summary-of-Changes-v3_2_1-to-v4_0.pdf

3. Джинг Лю. Янг Сяо. «Огляд стандарту безпеки даних платіжних карток» // [Електронний ресурс] – Режим доступу : https://ieeexplore.ieee.org/document/5455788

4. Рада зі стандартів безпеки PCI. «Стандартні вимоги до безпеки платежних карток (PCI) та процедури оцінки безпеки, версія 4.0, травень 2018 р.» // [Електронний ресурс] – Режим доступу: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

5. Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2020 року про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення або переслідування кримінальних правопорушень або виконання кримінальних покарань, а також щодо вільного руху таких даних, а також скасування Рамкового рішення Ради 2008/977 / ПВР. // [Електронний ресурс] – Режим доступу: http://data.europa.eu/eli/dir/2016/680/oj/eng

6. Європейська комісія. «Пропозиція до Загального регламенту ЄС про захист даних» // [Електронний ресурс] – Режим доступу: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2015/06/HuntonGuide-to-the-EU-General-Data-Protection-Regulation.pdf

7. Посібник з питань анонімізації та псевдонімізації "Хочете дотримуватись GDPR?". // [Електронний ресурс] – Режим доступу: https://www.iapp.org.

8. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» // [Електронний ресурс] – Режим доступу: https://tzi.com.ua/downloads/1.1-002-99.pdf

9. Вайттокер Зак. Журнал «Techcrunch» // [Електронний ресурс] – Режим доступу: https://techcrunch.com/2021/02/23/solarwinds-hackers-targetednasa-federal-aviation-administration-networks/

10. Коментар компанії SolarWinds щодо проникнення до ПЗ «Оріон»// [Електронний ресурс] – Режим доступу: https://habr.com/ru/news/t/533220/35. Cisco Systems, Inc. «Програма мережевої академії Cisco CCNA 3 та 4. Допоміжне керівництво» ISBN 1-58713-113-7.

11. Аксельсон С. "Системи виявлення вторгнень: опитування та таксономія" // [Електронний ресурс] – Режим доступу: http://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/Dmining/Anomaly-D/Intrusion-detection/taxonomy.pdf

12. Ньюман Роберт «Комп'ютерна безпека: захист цифрових ресурсів». ISBN 978-0-7637-5994-0

13. Офіційний сайт Oracle Database //[Електронний ресурс] – Режим доступу: https://docs.oracle.com/en/database/oracle/oracle-database/index.html

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних позначень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	Стан питання. Постановка задачі	7	
6	А4	Спеціальна частина	32	
7	А4	Економічна частина	7	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	1	

ДОДАТОК Б. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

Циватий_Д.О._125-21м-1.docx

Циватий_Д.О._125-21м-1.pptx

ДОДАТОК В. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

Відгук керівника кваліфікаційної роботи:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Керівник розділу _____ _____

(підпис) (ініціали,прізвище)

ДОДАТОК Е. Відгук керівника економічного розділу

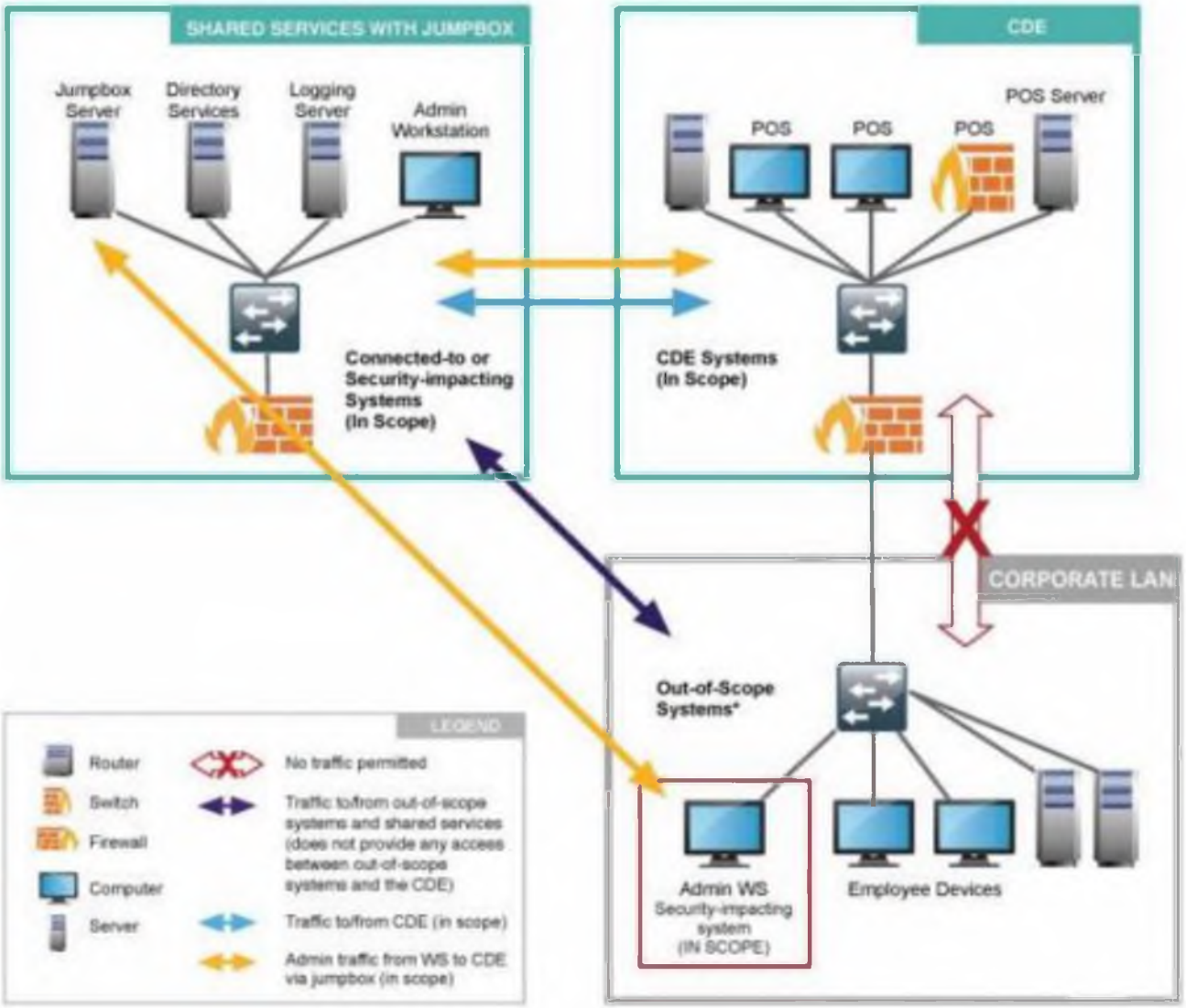
Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

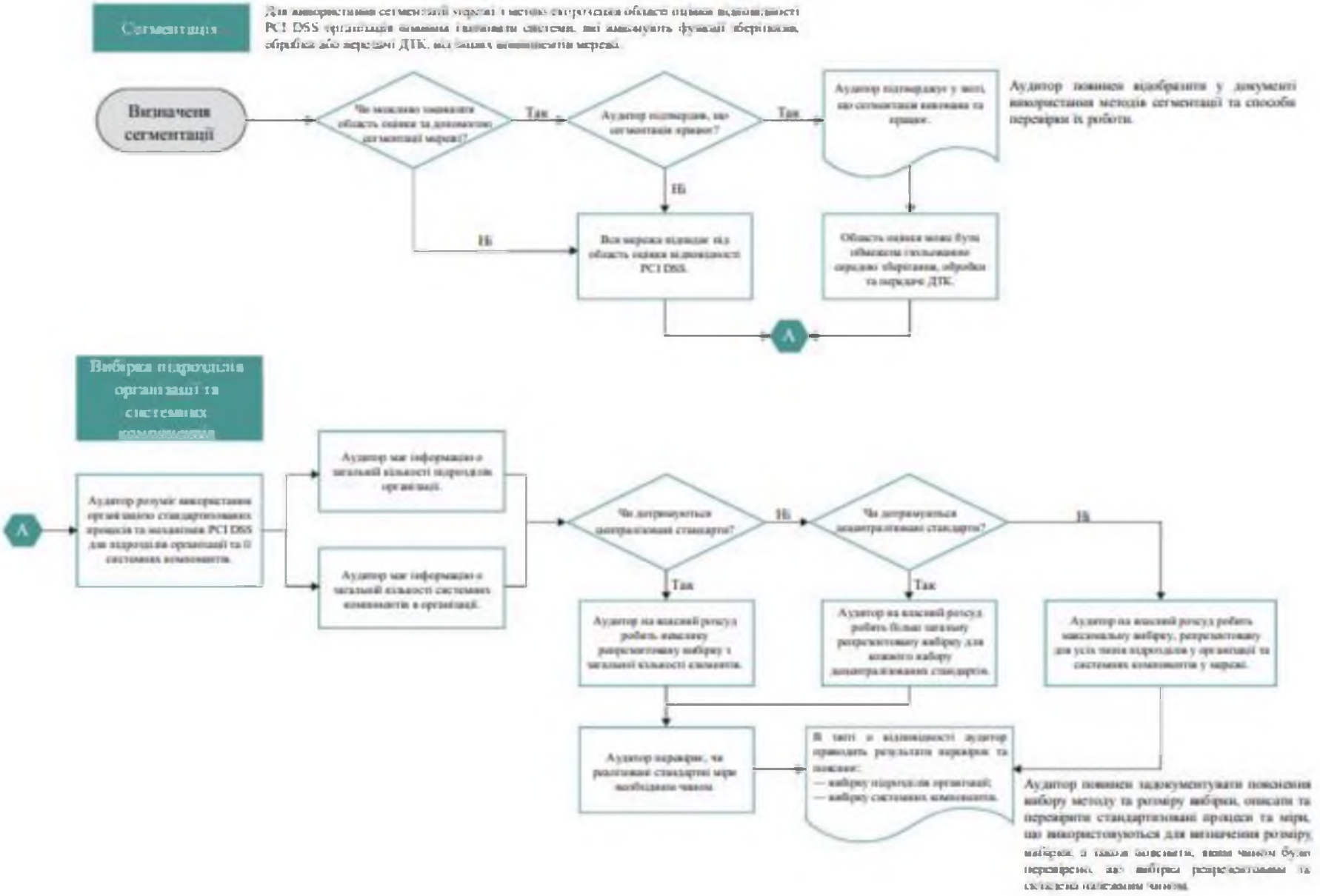
(підпис) (ініціали, прізвище)

ДОДАТОК Г



** Only if verified these systems meet all criteria for being out of scope, including there being no connectivity between these systems and the CDE. Controls must also be in place to prevent out-of-scope systems gaining access to the CDE via systems in the Shared Services network.*

ДОДАТОК Г


Сегментація
Визначення сегментації
Так
Так
Аудитор повинен відобразити у документі використання методів сегментації та способи перевірки їх роботи.
Ні
Ні
A
Вибірка підрозділів організації та системних компонентів
A
Так
Так
Ні
Ні
Так
Так
Ні
Ні
Аудитор повинен задокументувати показники вибору методу та розміру вибірки, описати та перевірити стандартизовані процеси та міри, що використовуються для визначення розміру вибірки. З цією метою аудитор повинен перевірити, що вибірки репрезентативні та достатньо великими.