МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРАКОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 20__ р.

На правах рукопису
УДК: 004.056.5

ДИПЛОМНА РОБОТА
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬО СТУПЕНЯ «БАКАЛАВР»

Тема: Системи захисту даних платіжних карток на основі стандартів PSIDSS та SWIFT

Виконавець: А.Є. Кармазіна

Керівник: к.т.н, доцент М.Б. Гумен

Нормоконтролер: к.т.н, доцент М.Б. Гумен

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки комп'ютерної та програмної інженерії
Кафедра: Комп'ютеризованих систем захисту інформації
Освітній ступінь: «Бакалавр»
Спеціальність: 125 «Кібербезпека»
Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____С.В. Казмірчук

«___»_____20__ р.

ЗАВДАННЯ
на виконання дипломної роботи
здобувача вищої освіти Кармазіної Анастасії Євгенівни

1. Тема: Системи захисту даних платіжних карток на основі стандартів PSIDSS та SWIFT, затверджена наказом ректора від «26» квітня.2021 р. № 652/ст.
2. Термін виконання: з 10.05.2020 р. по 20.06.2020 р.
3. Вихідні дані:
4. Зміст пояснювальної:

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Підпис керівника
1.	Уточнення постановки задачі	19.04.2021	*Виконано*
2.	Аналіз літературних джерел	20.04.2021	*Виконано*
3.	Обґрунтування рішення	22.04.2021	*Виконано*
4.	Збір інформації	23.04.2021	*Виконано*
5.	Аналіз стандартів PCI DSS та SWIFT	24.04 — 01.05.2021	*Виконано*
6.	Аналіз стандартів NIST CF, ISO/IEO 2700x, GDPR, НД ТЗІ	01.05 — 03.05.2021	*Виконано*
7.	Встановлення відповідності між всіма проаналізованими стандартами кібербезпеки	4.05.2021	*Виконано*
8.	Розробка та дослідження системи захисту карткових даних відповідно до вимог стандартів PCI DSS та SWIFT	5.05 — 25.05.2021	*Виконано*
9.	Аналіз та оформлення висновків відповідно до проведеної робота	26.05 — 01.06.2021	*Виконано*
10.	Оформлення і друк пояснювальної записки	02.06.2021	*Виконано*
11.	Оформлення презентації	03.06.2021	*Виконано*
12.	Отримання рецензій від рецензентів	11.06.2021	*Виконано*

Здобувач вищої освіти А.Є. Кармазіна

(підпис, дата)

Керівний дипломної роботи Б.М. Гумен

(підпис, дата)

Реферат

Дипломна робота складається зі вступу, двох розділів, загальних висновків, списку використаних джерел, додатків, загальним обсягом робота складає 12616 сторінок, має 11 рисунків, 3 таблиць, 29 сторінок додатків. Список використаних джерел містить 38 найменувань і займає 4 сторінки.

Метою дипломної роботи розробка систем захисту даних платіжних карток на основі стандартів PCI DSS та SWIFT.

В дипломній роботі розглянуті питання комплексного дослідження стандартів PCI DSS та SWIFT, визначення зв'язку стандартів PCI DSS та SWIFT з іншими стандартами комп'ютерної та інформаційної безпеки. Проведено аналіз та конкретизація відповідних вимог стандартів для побудова комп'ютерної та інформаційної безпеки у мережі, що містить карткові дані, що буде PCI DSS та SWIFT compliance.

Ключові слова: стандарт, PCI DSS, SWIFT, карткові дані, безпека, захист.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

API	—	Application Programming Interface
ASV	—	Approved Scanning Vendor
BIN	—	Банківській ідентифікаційний номер
DNS	—	Domain Name System
ENISA	—	The European Union Agency for Cybersecurity
GDPR	—	General Data Protection Regulation
GUI	—	Графічний інтерфейс користувача
HSM	—	Апаратний модуль безпеки
KYC-SA	—	KYC Security Attestation
NIST	—	The National Institute of Standards and Technology
NTP	—	Сервери служби часу
OWASP	—	Open Web Application Security Project
PAN	—	Номер платіжної картки
PCI DSS	—	Payment Card Industry Data Security Standard
PCI SCC	—	PCI Security Standards Council
PKI	—	Інфраструктура відкритих ключів
RADIUS	—	Remote Authentication in Dial-In User Service
RMA	—	Сервіс по управлінню взаємовідносинами SWIFT
SNL	—	SWIFTNet Link. Програмний додаток для використання SWIFTNet
SWIFT	—	Society for Worldwide Interbank Financial Telecommunications
TACACS	—	Terminal Access Controller Access Control System
TLS	—	Transport layer security
QSA	—	Qualified Security Assessor
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

ВСТУП

Актуальність. На сьогодні світ все більше та більше переходить у віртуальний простір. Комп’ютерні мережі зберігають державні таємниці, секрети добробуту корпорацій, гроші (у всіх фінансових системах у світі майже 70% грошей представлено виключно в електронній формі), 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 всі часи людей хвилювала безпека їх фінансових активів. Наразі людство надає перевагу електронному зберіганню фінансових активів. Тому безпека даних електронних активів є вкрай актуальним наразі питанням. Стандарт PCI DSS та концепція SWIFT CSCF створені для покращання та стандартизації систем комп'ютерного та інформаційного захисту систем, що містять у собі будь-які карткові дані.

Все більше у застосунок приходить електронна комерція, все частіше Інтернет виконує роль магазину для всього спектру товарів та послуг. І безпеку «купівлі» в ньому, також контролюють та стандартизують дані стандарти.

Зважаючи на вказані вище фактори, можна зробити висновки, що дане дослідження є актуальним.

Метою дипломної роботи є розробка систем захисту даних платіжних карток на основі стандартів PCI DSS та SWIFT.

Досягнення мети потребує розв’язання наступних **задач:**

- Комплексне дослідження стандартів PCI DSS та SWIFT;
- Визначення зв'язку стандартів PCI DSS та SWIFT з іншим стандартами комп'ютерної та інформаційної безпеки;
- Аналіз та конкретизація відповідних вимог стандартів для побудова комп'ютерної та інформаційної безпеки у мережі, що містить карткові дані, що буде PCI DSS та SWIFT compliance.

Об'єкт дослідження: стандарти PCI DSS та SWIFT.

Предмет дослідження: методи та засоби побудови системи комп'ютерного та інформаційного захисту на основі стандартів PCI DSS ТА SWIFT.

Оцінка сучасного стану проблеми на основі вітчизняної та зарубіжної літератури. Стандарти PCI DSS та SWIFT є міжнародними, проте зазвичай відомі лише тим, хто має безпосереднє відношення до роботи чи захисту карткових даних. Основна література, що стосується даних стандартів, випускається ними же самими, та становить невід'ємну частину розуміння даних стандартів.

Проте з розвитком віртуального середовища та переносом у нього все більшого відсотку фінансової сфери, все більш відомими стають засоби, та стандарти, що контролюють їх використання, захисту карткових (або фінансових) даних.

Галузь застосування. Результати дипломної роботи можуть бути використані в галузі компюторного захисту та інформаційного, зокрема в сучасних інформаційно-комунікаційних системах та мережах, що мають у собі (зберігають, передають або оброблюють) з картковими даними.

Практична цінність полягає в тому, що дане дослідження може бути використано як підґрунтя для побудови власної системи, що буде PCI DSS та SWIFT compliance. Відповідно до вимог зазначених в даній дипломній роботі та прикладам їх виконання, можна будувати систему захисту даних платіжних карток, що буде відповідати всім вимогам зазначеним у стандартах PCI DSS та SWIFT.

РОЗДІЛ 1. ЗАГАЛЬНИЙ АНАЛІЗ СТАНДАРТІВ PCI DSS І SWIFT

1.1 PCI DSS

PCI DSS (Payment Card Industry Data Security Standard, у перекладі з анг. «стандарт безпеки індустрії платіжних карток») — 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.

Кожна із корпорацій мала на меті створити мінімальний рівень захисту для карткових даних при їх зберіганні, обробці або передачі шляхом поєднання напрацювань кожної із сторін: «Програма захисту інформації о тримачах (власниках) карток» від Visa, «Операційна політика по забезпеченню безпеки картковим даним» від American Express, «Політика захисту сайтів» від MasterCard, «Інформаційна безпека та відповідність її вимогам» від Discover Financial Services та «Програма безпеки даних» від JCB International.

Згодом у 2006 році був розроблено та впроваджено PCI DSS (Рада зі стандартів безпеки індустрії платіжних карток), що виконує функції адміністративного/контролюючого органу, відповідального за розвиток та впровадження PCI DSS. Будь-які приватні або незалежні організації можуть приймати участь у розробці стандарту, при умові їх попередньої реєстрації[2].

Наразі існують наступні версії стандарту[5, 6]:

Таблиця 1.1.а

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.

Стандарт PCI DSS — це список чітко визначених вимог, з чітко же прописаними діями при їх перевірці та поясненнями необхідності даних

вимог. Всі вимоги поділяються на шість умовних груп, зв’язаними між собою так званими «цілями контролю»:

1. Створювати та підтримувати безпечну мережу(і) та системи;
2. Захист даних власників карток;
3. Підтримувати програму управління вразливостями;
4. Реалізувати жорсткі заходи контролю доступу;
5. Регулярно відстежувати та тестувати мережу(і);
6. Підтримувати політику інформаційної безпеки в Організації.

Ці шість груп описані у дванадцяті над-вимогам, що є незмінними з першої версії стандарту, хоча «нижчі» вимоги не раз редагувалися та змінювалися. Дванадцять над-вимог, для побудови та підтримання безпечної системи, що містить у собі карткові дані наступні[5]:

1. Встановлення та підтримка конфігурації брандмауера для захисту даних тримачів (власників) карток. Призначення брандмауера — сканувати та фільтрувати весь мережевий трафік, блокувати доступ до системи через ненадійні мережі.
2. Зміна встановлених постачальником значень за замовчуванням для системних паролів та інших параметрів безпеки. Дані паролі легко виявляються через загальнодоступну інформацію та можуть використовуватися зловмисниками для отримання несанкціонованого доступу до систем.
3. Захист збережених даних тримачів (власників) карток та даних самих карток. Шифрування, хешування, маскування та усічення — це методи, які використовуються для захисту даних тримача (власника) картки.
4. Шифрування передачі даних тримачів (власників) карток по відкритим загальнодоступним мережам. Надійне шифрування, включаючи використання тільки надійних ключів та сертифікатів, знижує ризик злому та перехоплення даних зловмисниками.

5. Захист всіх систем від шкідливих програм та регулярне оновлення антивірусного ПЗ. Шкідливе ПЗ може проникати в мережу безліччю способів, включаючи використання Інтернету, електронної пошти співробітників, мобільних пристроїв або пристроїв зберігання інформації. Сучасне антивірусне програмне забезпечення або додаткове програмне забезпечення для захисту від шкідливих програм знизить ризик використання шкідливих програм.
6. Розробка та підтримка безпечних систем та додатків. Вразливості в системах та додатках дозволяють недобросовісним особам отримати привілейований доступ. Необхідно негайно встановити виправлення безпеки, щоб виправити уразливість та запобігти використанню і компрометації даних тримача (власника) картки.
7. Обмеження доступу до даних тримачів (власників) карток тільки уповноваженому персоналу. Необхідно використовувати системи та процеси для обмеження доступу до даних тримачів (власників) карток за принципом «мінімальної службової необхідності».
8. Ідентифікація та автентифікація доступу до системних компонентів. Кожній особі, яка має доступ до компонентів системи, повинен бути присвоєний унікальний ідентифікатор (ID), який дозволяє контролювати доступ до критично важливих систем даних.
9. Обмеження фізичного доступу до даних власників карток. Фізичний доступ до даних власників карток або системам, які зберігають ці дані, повинен бути безпечним, щоб запобігти несанкціонованому доступу або видаленню даних.
10. Відстеження та моніторинг будь-якого доступу до даних власників карток і мережевих ресурсів. Повинні бути передбачені механізми реєстрації для відстеження дій користувачів, які мають вирішальне

значення для запобігання, виявлення або мінімізації впливу компрометації даних.

11. Регулярне тестування систем та процесів безпеки. Постійно виявляються нові уразливості. Системи, процеси та програмне забезпечення необхідно часто тестувати, щоб виявити уразливості, які можуть бути використані зловмисниками.
12. Ведення політики інформаційної безпеки для всього персоналу. Сильна політика інформаційної безпеки включає в себе розуміння персоналом конфіденційності даних та їх відповідальності за їх захист.

Стандарт PCI DSS передбачає декілька умовних рівнів[3], на які поділяються компанії, що підпадають під дію стандарту. Відповідно від рівня відповідності визначається які саме звітні документи необхідно заповнити QSA (аудитору) для PCI DSS сертифікації компанії. Рівні поділяються за кількістю транзакцій щорічно наступним чином:

1. Рівень 1 — більше 6-ти мільйонів транзакцій щорічно;
2. Рівень 2 — від 1-го до 6-ти мільйонів транзакцій щорічно;
3. Рівень 3 — від 20 000 до 1-го мільйона транзакцій щорічно;
4. Рівень 4 — менше 20 000 транзакцій щорічно.

Стандарт PCI DSS застосовується для всіх організацій, залучених в обробку платіжних карток: МСП, процесингових центрів, еквaєрів, емітентів та постачальників послуг, а також будь-яких інших організацій, які зберігають, обробляють або передають ДТК (дані тримача картки, у розумінні: номер картки (PAN), ім’я тримача картки, дата витоку строку працювання картки, сервісний код) та/або КАД (критичні автентифікаційні дані, у розумінні: повні дані треку (дані магнітної полоси картки або чіпа), CAV2/CVC2/CVV2/CID, PIN-коди та/або PIN-блоки).

Серед ДТК найважливішу роль грає PAN, його зберігання строго обмежене, тоді як інші дані можуть Зберігатися більш-менш вільно. КАД загалом заборонено до зберігання, за виключенням банкам та фінансовим

установам, що випускають картки та зберігання КАД у яких є процесинговою необхідністю.

Вимоги PCI DSS застосовуються до всіх системним компонентам, які входять в середу ДТК або підключені до неї. Середа ДТК — це сукупність людей, процесів та технологій, що зберігають, обробляють або передають ДТК або КАД. Термін «системні компоненти» включає в себе мережеві та обчислювальні пристрої, сервери і додатки. Прикладами системних компонентів є, серед іншого[5]:

- системи, які:
  - надають служби безпеки (наприклад, сервери автентифікації);
  - сприяють сегментації мережі (наприклад, внутрішні міжмережеві екрани);
  - можуть впливати на безпеку середовища ДТК (наприклад, сервери розпізнавання імен або веб-переадресації).
- компоненти віртуалізації, наприклад:
  - віртуальні машини;
  - віртуальні комутатори та/або маршрутизатори;
  - віртуальні програми та/або комп'ютери;
  - гіпервізор.
- мережеві компоненти, в тому числі:
  - міжмережеві екрани;
  - комутатори;
  - маршрутизатори;
  - бездротові точки доступу;
  - пристрої мережевої безпеки;
  - інші пристрої безпеки.
- типи серверів, в тому числі:
  - веб-сервери;
  - сервери додатків;
  - сервери баз даних;

- сервери автентифікації;
- поштові сервери;
- проксі-сервери;
- сервери служби часу (NTP);
- DNS-сервери.

- додатки, включаючи всі придбані або замовлені додатки, в тому числі внутрішні і зовнішні (наприклад, доступні через Інтернет);
- будь-який інший компонент або пристрій, розташований всередині середовища ДТК або підключений до неї.

Стандарт PCI DSS велику увагу приділяє також сегментації мережі, за якою середовище, містить карткові дані повинно бути відділене від загальної мережі організації. Сегментація не є обов'язковою, проте є бажаною і значно впливає на сертифікацію за стандартом. У Додатку А приведена процедура перевірки та оцінювання сегментації у організації, що підпадає під стандарт PCI DSS.

Загалом PCI DSS має 255 деталізованих вимог, на які припадає близько 440 процедур їх контролю (що містить під собою як дослідження роботи (опитування, нагляд) персоналу, так і ручну перевірку аудитором конфігурацій, налаштувань та систем).

1.2 SWIFT

SWIFT (Society for Worldwide Interbank Financial Telecommunications, у перекладі з анг. товариство всесвітніх міжбанківських фінансових телекомунікацій) — міжнародна міжбанківська система передачі інформації та здійснення платежів. Ця система робить можливим фінансовим установам (банкам) з усього світу відправляти та отримувати інформацію про будь-які фінансові операції у стандартизованій, надійній та безпечній формі. Воно також має власні розробки та додатки, що продаються фінансовим

установам. Дані розробки частіш за все мають на меті інтегруватися або доповнити мережу SWIFTNet.

Загалом, SWIFT — це кооперативне товариство у відповідності до бельгійського законодавства, що належить його членам-фінансовим установам з офісами по всьому світу. Зауважимо, що членом SWIFT може бути фінансова установа, зареєстрована у будь-якій країні світу, але всі вони у своїй діяльності пов'язаній зі SWIFT повинні дотримуватися норм бельгійського законодавства, як країни, де даний кооператив був створений.

SWIFT був заснований ще 3-го травня 1973-го року під керівництвом його першого генерального директора (Карла Рейтерскельда) та за підтримкою на той момент 239-ти банків у 15-ти країнах світу[10]. Від початку воно стало впроваджувати єдині стандарти банківських переказів, фінансових транзакцій, загальну систему міжбанківського зв'язку та систему обробки відповідних даних, що були розроблені корпорацією Burroughs[11, 12].

Наразі SWIFT займається переводом фінансових платежів (та загалом повідомлень) безпечним шляхом, але не має жодної облікового запису для своїх клієнтів (членів) та не виконує розрахунки чи кліринг у жодній із форм. SWIFT, сам по собі, не сприяє переведенню грошових коштів: швидше, він відправляє платіжні доручення, які повинні оплачуватися кореспондентськими рахунками, відкритими організаціями один одному. Кожна фінансова установа, щоб обмінюватися банківськими операціями, повинна мати банківські відносини, будучи банком або приєднавшись до одного (або кількох) з них, щоб користуватися цими конкретними бізнес-функціями. SWIFT можна назвати деяким міжбанківським платіжним шлюзом, або навіть, точніше, гарантом безпеки деякого міжбанківського платіжного шлюза.

Проте SWIFT все ж таки має і власний платіжний сервіс — «Global Payments Innovation» (GPI), що станом на 2018-тий рік був прийнятий більш ніж 168-ми фінансовими установами та, за зауваженнями самих

представників SWIFT, виконує половину своїх транзакцій вже за 30-ть хвилин[13].

Також SWIFT розробив та підтримує власний стандарт інформаційної безпеки, а точніше концепцію забезпечення безпеки користувачів SWIFT (CSCF)[14].

В даному документі визначається комплекс обов'язкових та рекомендованих елементів контролю безпеки для операційного середовища користувачів SWIFT. Обов'язкові елементи контролю безпеки засновані на існуючих правилах та забезпечують базовий рівень безпеки для всієї спільноти користувачів. Рекомендовані елементи контролю — це передовий всесвітній досвід, який SWIFT рекомендує впроваджувати в своєму операційному середовищі кожному користувачеві[14].

Концепція забезпечення безпеки користувачів SWIFT складається з обов'язкових та рекомендованих елементів контролю для користувачів SWIFT-платежів. Обов'язкові елементи контролю забезпечують базовий рівень безпеки для всієї організації, що використовує SWIFT, та повинні бути впроваджені всіма користувачами мінімум в їх локальної інфраструктурі SWIFT (попередньо виділеною сегментацією в окремий сегмент мережі організації). SWIFT вирішив визначити пріоритетність обов'язкових елементів контролю, щоб встановити реалістичну мету на найближчу перспективу: істотне підвищення рівня безпеки та зниження максимально можливої кількості ризиків. Рекомендовані елементи контролю, засновані на передовому досвіді, пропонуються до застосування користувачам SWIFT, але на власний розсуд організації. Згодом обов'язкові елементи контролю можуть бути змінені у зв'язку з еволюцією загроз, а деякі рекомендовані елементи контролю можуть стати обов'язковими[14].

Всі елементи контролю, що були зазначені у концепції, спрямовані на досягнення трьох головних цілей: «забезпечення безпеки середовища», «знання та обмежування доступу» та «виявлення та реагування». Елементи контролю були розроблені на основі аналізу відомостей про кіберзагрози,

проведеного SWIFT за участю галузевих експертів, та з урахуванням відгуків користувачів. Мається на увазі, що всі зазначені елементи контролю відповідають та ні в якій мірі не заперечують існуючим стандартам інформаційної безпеки.

SWIFT окремо зазначає, що елементи контролю, описані в концепції, є загальними та незалежними від програмного комплексу засобами контролю. Вони не повинні розглядатися як вичерпні або універсальні, не здатні замінити добре структуровану систему забезпечення безпеки та управління ризиками, що охоплює весь наскрізний ланцюжок транзакцій, а також здоровий глузд або відповідність новітнім рекомендаціям в області безпеки. Концепція визначає мінімально необхідні засоби забезпечення безпеки, але користувачі повинні прагнути досягти кращого рівня захищеності, незалежно (проте не протиріччя) від Концепції.

На відміну від PCI DSS, концепція SWIFT змінюється[14], доповнюється та переглядається щонайменше раз у рік, і кожен рік виходить оновлена версія документу. Нова версія CSCF зазвичай публікується на початку липня та включає в себе список обов'язкових та рекомендованих елементів контролю для проведення атестації з липня наступного року, коли ці елементи контролю будуть реалізовані в KYC-SA (KYC Security Attestation, спеціальний додаток для сертифікації компаній у відповідності з CSCF).

Елементи контролю безпеки базуються на трьох всеосяжних цілях, підкріплених вісьмома принципами безпеки. Цілі — це найвищий рівень структури безпеки в локальному середовищі користувача. Пов'язані з ними принципи конкретизують найбільш пріоритетні напрямки діяльності в рамках кожної мети (Додаток Б).

Всі ці цілі та принципи лежать в основі 31 елементів контролю (22 обов'язкових та 9 рекомендованих елементів контролю), докладно викладених концепції. Елементи контролю допомагають зменшити певні ризики кібербезпеки, з якими стикаються користувачі SWIFT в сфері

кібернетичного зв’язку. В рамках кожного з елементів контролю SWIFT документально зафіксував найбільш поширені фактори ризику, а самі елементи контролю розробляються, щоб допомогти їх мінімізувати. Усунення даних ризиків направлено на запобігання або зведення до мінімуму небажаних та потенційно шкідливих наслідків для бізнесу, таких як[14]:

- несанкціонована відправка або зміна даних фінансових транзакцій;
- обробка змінених або несанкціонованих вхідних (тобто отриманих) транзакцій SWIFT;
- ведення бізнесу з несанкціонованим контрагентом;
- порушення конфіденційності (бізнес-даних, комп'ютерних систем або відомостей про оператора);
- порушення цілісності (бізнес-даних, комп'ютерних систем або відомостей про оператора).

Загалом у передмові до концепції SWIFT закликає користувачів розглядати управління кіберризиками в найширшому сенсі, в тому числі за межами області інфраструктури користувачів SWIFT та елементів контролю SWIFT. Для найбільш ефективного управління ризиками користувачі не повинні розглядати впровадження зазначених у концепції елементів контролю ні як разове або одиничне, ні таким, що буде охоплювати всі сфери інформаційної безпеки організації. Користувачам краще включити елементи контролю SWIFT у свою існуючу програму управління кібербезпекою та ризиками, в конкретних рамках своєї організації, яка бере до уваги здоровий глузд та новітні передові практики та враховує специфічну для користувача інфраструктуру та конфігурації (через специфіку інтеграції SWIFT-повідомлень у загальну інфраструктуру організації). В результаті користувачі можуть широко застосовувати існуючі політики, процедури та елементи контролю, що були створені для управління іншими областями та поняттями кіберризиків, ризиками, що існують для інших систем та мереж (але нехтуються SWIFT), та витягати з них вигоду.

Концепція побудована таким чином, щоб поділити всі типи реалізації інфраструктури під SWIFT-перекази на п’ять типів та у відповідності до кожного типу поділити всі елементи контролю на обов’язкові та рекомендовані. В залежності від архітектури та прийнятих інтеграційних рішень деякі елементи контролю не можуть буди виконані або перевірені.

Перша архітектура (Архітектура A1, за найменуванням CSCF) розрахована на організації, що володіють комунікаційним інтерфейсом (та у загальному випадку інтерфейсом обміну повідомленнями). Архітектура, в рамках якої користувач не володіє інтерфейсом обміну повідомленнями, а взаємодіє/володіє тільки комунікаційним інтерфейсом.

На рис. 1.2.а показаний приклад, в якому ліцензії інтерфейсу обміну повідомленнями та комунікаційного інтерфейсу належать користувачу і знаходяться в його середовищі:

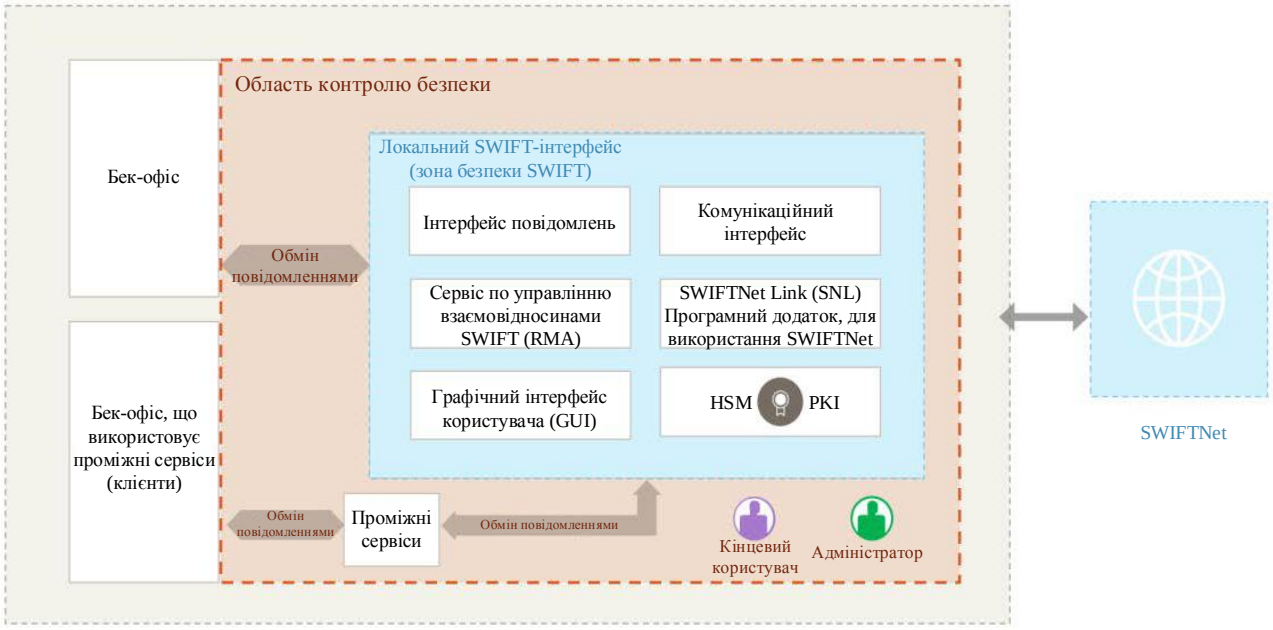


Рисунок 1.2.а

На рис. 1.2.б показаний приклад архітектури в рамках якої користувач взаємодіє/володіє тільки комунікаційним інтерфейсом.

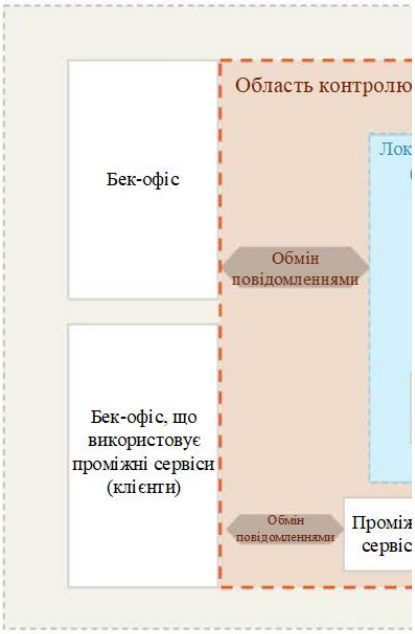


Рисунок 1.2.б

Тип архітектури A1 також включає розміщення рішення, в яких користувач володіє (має ліцензію) комунікаційним інтерфейсом, але при цьому він або працює від імені іншого користувача/користувачів, або експлуатується у себе третьою стороною всередині або поза користувальницького середовища (розміщення).

Друга архітектура (Архітектура A2, за найменуванням CSCF), визначається користувачем, що володіє інтерфейсом обміну повідомленнями без комунікаційного інтерфейсу.

Користувач володіє інтерфейсом обміну повідомленнями, але постачальник послуг (наприклад, сервіс-бюро, SWIFT або груповий хаб) володіє ліцензією цього комунікаційного інтерфейсу.

На рис. 1.2.в показаний приклад, в якому інтерфейс обміну повідомленнями належить користувачеві та знаходиться в середовищі користувача.

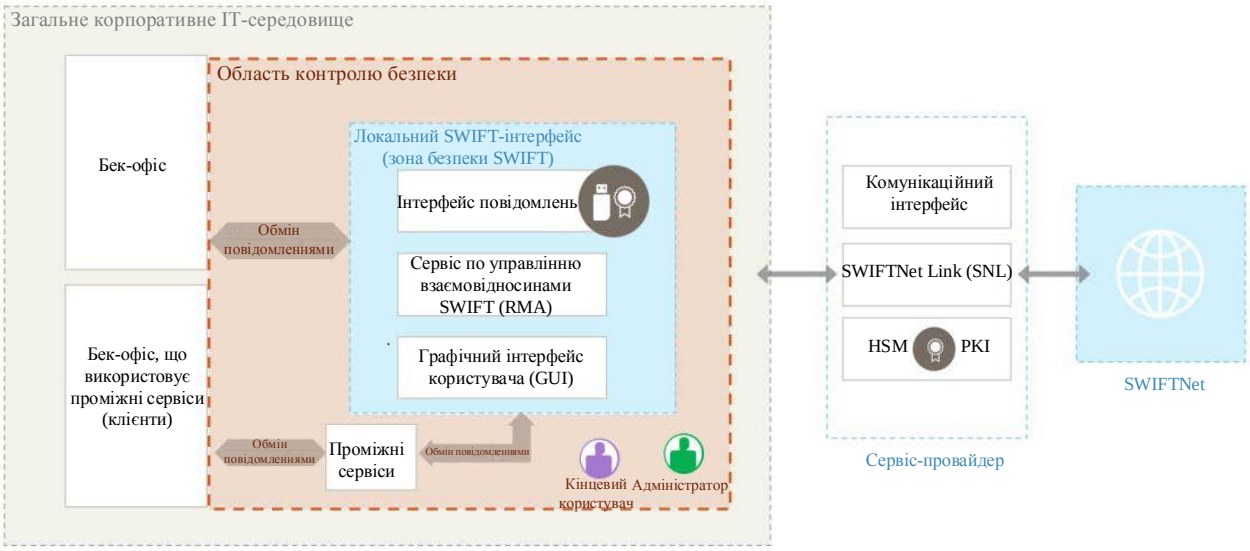


Рисунок 1.2.в

Даний тип архітектури також включає розміщення рішення, в яких користувач має ліцензію на інтерфейс обміну повідомленнями, який управляється їм, третьою стороною або постачальником послуг.

Третій тип архітектури (Архітектура А3, за найменуванням CSCF), визначається коли користувач володіє коннектором SWIFT. Він використовується в середовищі користувача для забезпечення взаємодії додатків з інтерфейсом, розміщеним або в середовищі постачальника послуг (наприклад, сервісного бюро або групового хаба), або у сервісах SWIFT (наприклад, Alliance Cloud, Alliance Lite 2 і, в майбутньому, сервісом обміну повідомленнями або платформою Transaction Platform, які надає SWIFT[14]).

При необхідності цю настройку можна використовувати в поєднанні з GUI-рішенням — графічним інтерфейсом користувача (взаємодія типу «користувач — додаток»). В цьому випадку необхідно реалізувати ЕК, пов'язані з GUI.

Третій тип архітектури також включає в себе розміщення рішення, що бути виконувати роль коннектора SWIFT.

На рис. 1.2.г показаний приклад, де в середовищі користувача використовується конектор SWIFT[14]:

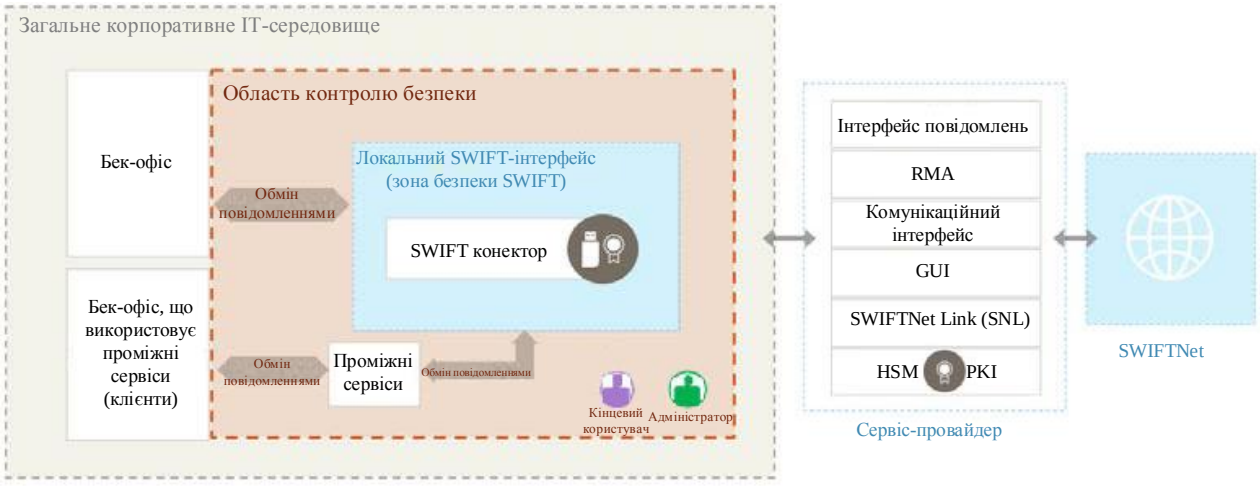


Рисунок 1.2.г

Четвертий тип архітектури (Архітектура A4, за найменуванням CSCF), визначається, коли користувачем використовується клієнтський коннектор.

Сервер, на якому працює прикладне ПЗ (наприклад, рішення для передачі файлів, система проміжного програмного забезпечення, або аналогічні системи, що є клієнтськими коннекторами), застосовується в середовищі користувача для забезпечення взаємодії додатків з інтерфейсом, розміщеним в середовищі постачальника послуг (наприклад, сервісного бюро, постачальника додатків Lite2 Business Application або групового хаба).

На рис. 1.2.д показаний приклад використання проміжного ПЗ/іншого рішення для передачі файлів в якості коннектора:

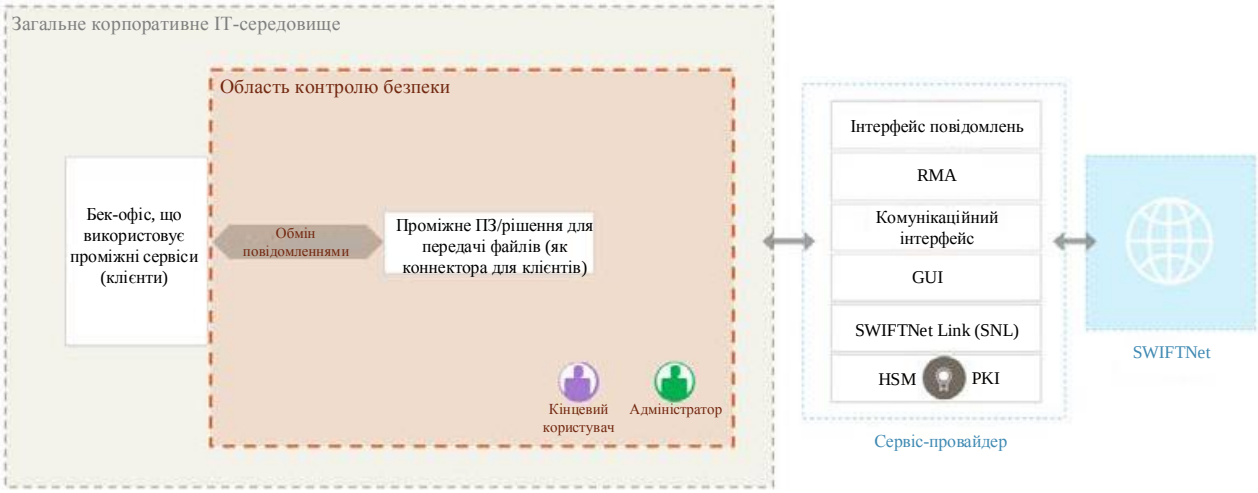


Рисунок 1.2.д

На рис. 1.2.е показаний приклад використання власного клієнтського коннектору (власне API):

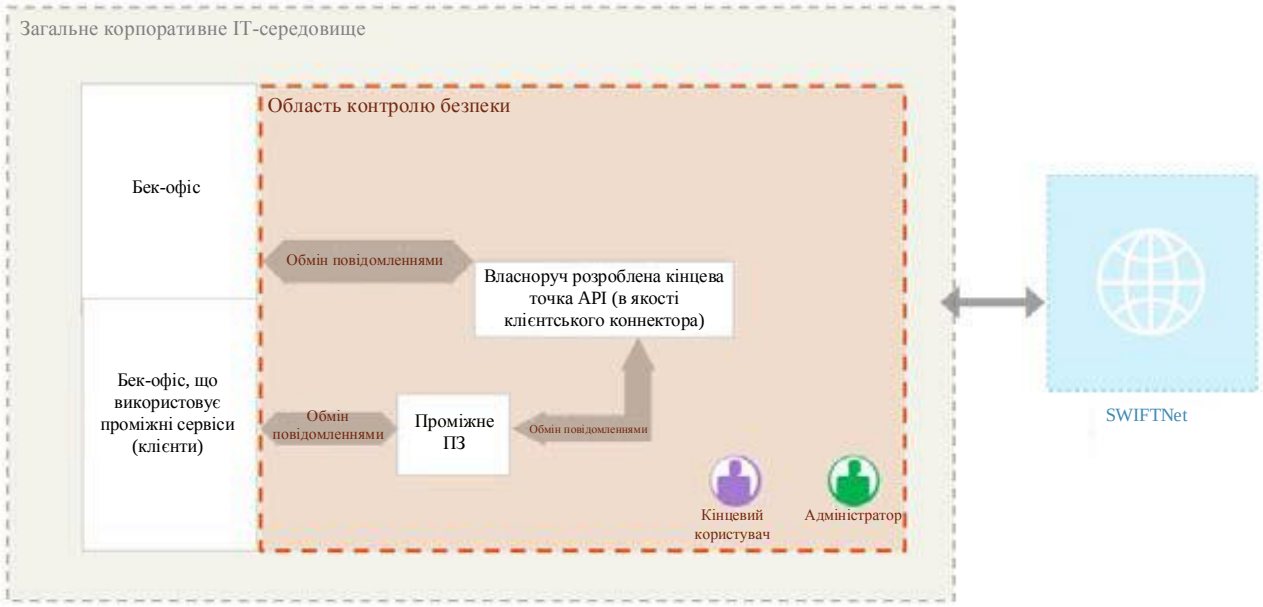


Рисунок 1.2.е

Останній, п’ятий тип архітектури (Архітектура В, за найменуванням CSCF), визначається коли у середовищі організації не використовується інфраструктура, залежна від SWIFT.

Даний тип архітектури реалізується будь-яким з наступних способів:

- Користувачі отримують доступ до сервісів обміну повідомленнями SWIFT тільки через графічний інтерфейс програми у постачальника послуг (взаємодія типу «користувач — додаток»). ПК або пристрій, що використовується такими користувачами для цих цілей, слід розглядати як ПК оператора, який повинен бути захищений відповідним чином (відповідно до норм законодавства та інших стандартів та регламентів інформаційної безпеки, що є застосовані в контексті діяльності даної організації, та окремо відповідно

елементам контролю у CSCF SWIFT, що стосуються ПК операторів загального призначення).

- Коли призначені для користувача додатки бек-офісу безпосередньо взаємодіють з постачальником послуг (взаємодія типу «додаток — додаток»), використовуючи API-інтерфейси постачальника послуг або клієнт проміжного програмного забезпечення (наприклад, MQ Client) без підключення або незалежної передачі бізнес-транзакцій в SWIFT Alliance Cloud, сервіс обміну повідомленнями SWIFT, SWIFT API Gateway (в іншому випадку дане архітектурне рішення організації вважається архітектурою типу A4 з клієнтським коннектором) або, в майбутньому, на платформу Transaction Platform[14], яку надає SWIFT. У цьому випадку постачальник послуг, на умовах раніше прописаних у договорі, що обов'язково закладається між сторонами, повинен забезпечити безпеку свого середовища та обміну даними з користувачами відповідно до елементів контролю CSCF. Віднесення цього варіанту установки до архітектури типу B узгоджується з областю застосування елементів контролю безпеки, які виключають застосування призначеного для користувача бек-офісу, проте остаточне рішення про віднесення архітектури організації до «підходящої» під умови виконання CSCF, залишається за аудитором. Проте SWIFT настійно рекомендує реалізувати все ж таки архітектуру типу A4 для цих додатків з інтеграцією API або клієнта проміжного програмного забезпечення (наприклад, MQ Client), щоб уменшити область можливого ураження.

Даний тип архітектури також включає в себе користувачів, що отримують доступ тільки через браузер або сервіси обміну повідомленнями SWIFT (взаємодія типу «користувач — додаток»), які надаються Alliance Cloud і Alliance Lite2. ПК, що застосовуються цими користувачами для відправки або зміни бізнес-транзакцій, необхідно вважати ПК оператора

загального призначення та вони повинні бути захищені відповідним чином (відповідно до норм законодавства та інших стандартів та регламентів інформаційної безпеки, що є застосовані в контексті діяльності даної організації, та окремо відповідно елементам контролю у CSCF SWIFT, що стосуються ПК операторів загального призначення).

На рис. 1.2.є показаний приклад використання архітектурного рішення без власної інфраструктури з підключенням до стороннього постачальника послуг (не SWIFT):

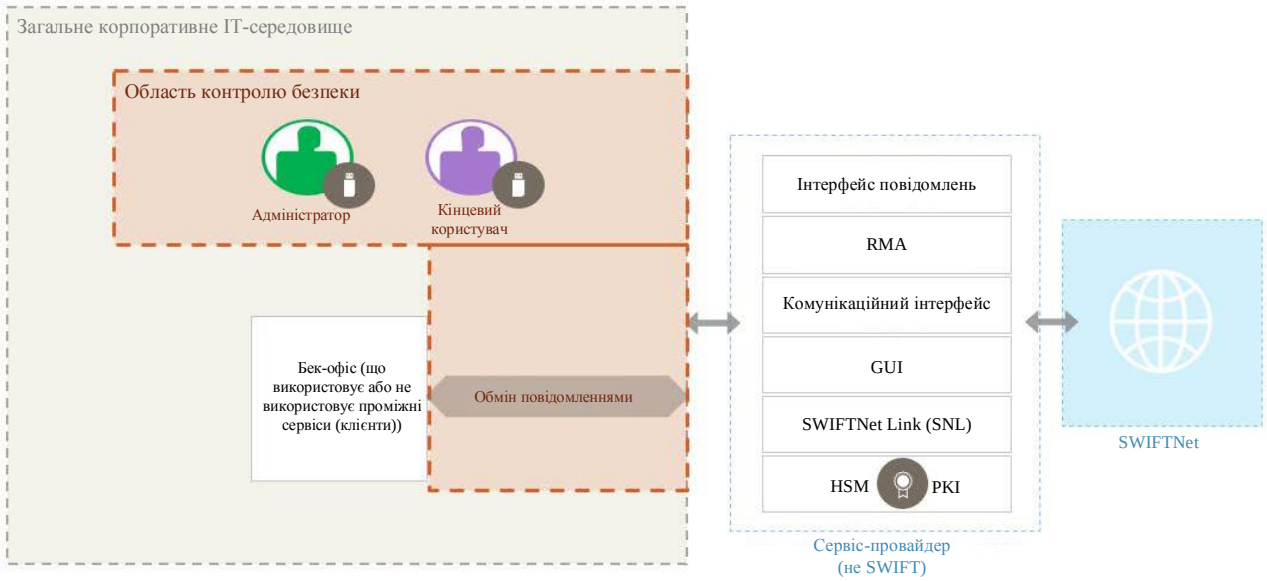


Рисунок 1.2.є

У таблиці нижче приведені відповідності елементів контролю до архітектур різних типів, а також до якого принципу вони відносять. Елементи контролю з літерою «р» після номеру та виділені блакитним є рекомендовані.

Таблиця 1.2.а

Обов'язкові та рекомендовані елементи контролю	**Тип архітектури**		
	A1→A3	A4	B
1. Обмеження доступу в Інтернет та захист найбільш важливих систем від загальної IT-середовища			

1.1 Забезпечення захисту середовища SWIFT	●		
1.2 Контроль за привілейованими обліковими записами операційної системи	●	●	
1.3 Захист платформи віртуалізації	●	●	
1.4 Обмеження доступу в Інтернет	●	●	●
2. Зменшення кількості потенційних векторів атак і вразливостей			
2.1 Захист внутрішнього потоку даних	●		
2.2 Оновлення системи безпеки	●	●	●
2.3 Підвищення надійності системи	●	●	●
2.4р Безпека потоку даних бек-офісу	●	●	●
2.5р Захист зовнішньої передачі даних	●	●	
2.6р Конфіденційність та цілісність сесії оператора	●	●	●
2.7 Сканування на вразливість системи	●	●	●
2.8р Аутсорсинг критично важливих видів діяльності	●	●	●
2.9р Засоби контролю транзакційного бізнесу	●	●	●
2.10 Підвищення надійності додатків	●		
2.11р Засоби контролю RMA (сервісу по управлінню взаємовідносинами SWIFT)	●	●	●
3. Забезпечення фізичного захисту середовища			
3.1 Фізичний захист	●	●	●
4. Запобігання компрометації облікових даних			
4.1 Політика паролів	●	●	●
4.2 Многофакторна автентифікація	●	●	●
5. Управління ідентифікаційними даними та розмежування повноважень			
5.1 Логічний контроль доступу	●	●	●
5.2 Управління токенами	●	●	●
5.3р Процес перевірки персоналу	●	●	●
5.4 Фізичне та логічне зберігання паролів	●	●	●
6. Виявлення аномальної активності в системах та журналах транзакцій			

6.1	Захист від шкідливих програм	●	●	●
6.2	Цілісність програмного забезпечення	●		
6.3	Цілісність бази даних	●		
6.4	Ведення журналу операцій і моніторинг	●	●	●
6.5р	Виявлення вторгнень	●	●	
7.	**План реагування на інциденти та інформування**			
7.1	Планування реагування на кіберінциденти	●	●	●
7.2	Навчання та інформування в сфері безпеки	●	●	●
7.3р	Тест на проникнення	●	●	●
7.4р	Оцінка ризиків	●	●	●

1.3 Зв'язок з іншими стандартами (NIST, ISO 2700x, GDPR, НД ТЗІ України)

NIST, загалом, — це національний інститут стандартів та технології, що відповідає за стандартизацію в усіх областях у Сполучених Штатах Америки.

У кібербезпеці значення має NIST Cybersecurity Framework, що визначає керівництво з комп’ютерної безпеки (в основному) для приватного сектору у США, щоб він мав змогу оцінювати та покращувати свою здатність виявляти та запобігати загрозам комп’ютерній безпеці. У своїй першочерговій структурі NIST Cybersecurity Framework має окреме політичне підґрунтя керівництва, для успішного виконання власних цілей.

Даний стандарт наразі був переведений на багато мов та навіть використовується на офіційному рівні в Японії та Ізраїлі[17].

NIST Cybersecurity Framework за своєю структурою розділений на три частини: «Ядро», «Профіль» та «Рівні». «Ядро стандарту» містить список (ряд) дій, результатів та посилань про більш загальні аспекти та підходи до теми комп’ютерного (та інформаційного) захисту. «Рівні реалізації стандарту» призначені для того, щоб при використанні організацією

прояснювати для неї та її партнерів, як необхідно розглядати ризик кібербезпеки та ступінь складності її (їх) підходу до управління. «Профіль стандарту» — це, по суті, список результатів, що організація вибрала для себе (з урахуванням інфраструктури та бізнес-необхідностей організації) з категорій та підкатегорій на основі своїх потреб та проведених оцінок ризиків.

ISO/IEC 2700x (1-5) — це міжнародний стандарт інформаційної безпеки, що був розроблений спільно Міжнародною організацією зі стандартизації та Міжнародної електротехнічної комісією. Прототип ISO/IEC 2700x (1-5) з'явився ще у 1995 році, під кодом BS 7799 (Частина 1). З розвитком комп'ютерних технологій, а також загроз та величини впливу цих загроз на суспільство, стандарт проходив перетворення, спершу на BS 7799 (Частина 2) у 1998-му році, згодом, у 2000-ному році стандарт був переоформлен як ISO/IEC 7799:2000, далі він вдосконалювався до версії ISO/IEC 7799:2005, прийнятій у 2005-му році. Тим часом BS 7799 (Частина 2) також отримувала нові доповнення, розвиваючись паралельно поки обидві версії не злилися у ISO/IEC 27001:2005 у 2005-му році. Остаточна версія стандарту датується 2013-тим роком та кодується ISO/IEC 27001:2013[21,22] (якщо казати у загальному).

У стандарті докладно викладені вимоги до створення, впровадження, підтримки та постійного вдосконалення системи менеджменту інформаційної безпеки (СМІБ), мета якої — допомогти організаціям зробити інформаційні активи, що вони зберігають, більш безпечними[23]. Європейське оновлення стандарту було опубліковано в 2017 році[24].

У загальному розумінні, ISO/IEC 2700x (1-5) найбільшим чином зосереджен на питаннях людського фактору та менеджменті, майже не торкаясь технічного боку кібербезпеки (на відміну від таких стандартів як PCI DSS, NIST CF).

Всього ISO/IEC 2700x (1-5) має 114 елементів управління, що розбиті на 14-ть груп у 35-ти категоріях контролю.

GDPR (Загальний регламент захисту персональних даних, загальний регламент щодо захисту даних, Генеральний регламент про захист персональних даних, в перекладі з анг. General Data Protection Regulation) — це в першу чергу регламент, що був прийнятий Євросоюзом, задля забезпечення безпеки персональних даних жителів-членів Євросоюзу, у мережі Інтернет. Також однією з основних цілей прийняття GDPR була необхідність спростити (покращити функціонування) міжнародно-економічних зав’язків, шляхом створення єдиної нормативної бази даних та уніфікації її.

Серед ключових (загальних) принципів GDPR виділяють:

- Законність, справедливість та прозорість (як загальний принцип законодавства Євросоюзу) — повинні бути законні підстави в рамках GDPR для збору та використання даних, гарантія дотримання (непорушення) будь-яких законів; загальна відкритість процесу, чесність від початку та до кінця при використанні будь-яких персональних даних;
- Обмеження метою — обробка персональних даних повинна зводитися лише до того, що було заявлено попередньо суб'єкту даних, без відступів у сторону. Всі конкретні завдання повинні бути закріплені в політиці конфіденційності та повинні чітко дотримуватися, без «і» та «але»;
- Мінімізація даних — необхідно використовувати мінімально необхідний обсяг персональних даних для успішного виконання поставлених цілей;
- Точність — персональні дані повинні бути точними та не повинні навмисно чи ні вводити в оману. Помилкові дані підлягають своєчасному коригуванню (під відповідальність власника (того, хто заносить) даних);
- Обмеження зберігання даних — небажано (читай — заборонено) зберігати дані довше, ніж це потрібно; Необхідно періодично

проводити аудит даних та видаляти ті з них, що є невикористовувані;

- Цілісність та конфіденційність/безпека — зберігати дані в безпечному місці та приділяти достатню уваги до збереження цих даних у неспотвореному вигляді;
- Підзвітність — компанія, що зберігає або оброблює персональні дані бере на себе відповідальність за обробку персональних даних та виконання всіх інших принципів GDPR, включаючи записи про конфіденційність, захист, використання, перевірці даних. Всі відповідні дії повинні чиним образом документуватися та повинна бути призначена посадова особа, що буде відповідальна за захист персональних даних у організації (у регламенті навіть виділена повна назва необхідної посади — DPO, data protection officer, відповідальний за захист даних).

GDPR — це в більшій частині законотворчий документ, де немає чітких технічних вимог до організацій, що під нього підпадають. Він вимагає дотримання своїх принципів та положень, проте методи залишає за організацією. Проте не знімає з себе право (можливість) контролювати процес дотримання вимог, накладаючи штрафи та назначаючи переатестацію у разі недотримання.

НД ТЗІ — нормативно-правові документи України, у сфері захисту інформації у комп’ютерних системах. Перші їх редакції відбувалися у 1998-1999-тих роках.

Вони визначають (у тому чи іншому обсязі) методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах та створення нормативних та методологічних документів, регламентуючих питання[31]:

- визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;

- створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;
- оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

НД ТЗІ визначають загальні методології та процеси ведення автоматизованих комп’ютерних та інформаційних систем, порядок побудови систем їх захисту. Вони регламентують створення експертних комісій, їх склад та порядок їх дій, при створені та перевірці (випробувані) систем захисту автоматизованих систем.

Окремо слід виділити два напрями у методології, зазначеній у НД ТЗІ[31]:

- забезпечення і оцінка захищеності інформації в АС, що функціонують;
- реалізація та оцінка засобів захисту, що входять до складу компонентів, з яких будується обчислювальна система АС (програмних продуктів, засобів обчислювальної техніки і т.ін.), поза конкретним середовищем експлуатації.

Загалом, кінцевою метою всіх заходів щодо захисту інформації, які реалізуються, є забезпечення безпеки інформації під час її обробки в автоматизованих системах. Захист інформації повинен забезпечуватись на всіх стадіях життєвого циклу автоматизованої системи, та на всіх технологічних етапах обробки інформації і в усіх її режимах функціонування.

Життєвий цикл автоматизованої системи включає в себе розробку, впровадження, експлуатацію та виведення з експлуатації, після закінчення сертифікаційного періоду чи з будь-якої іншої причини.

НД ТЗІ, це чисто нормативні документи, що не містять конкретних технічних рішень, проте зазначають які категорії рішень необхідно використовувати для тих чи інших автоматизованих систем, в залежності від їх призначення та рівня конфіденційності інформації, що в них зберігається або оброблюється.

Загалом, загальне розуміння кіберзахисту передбачає, що побудова інфраструктури організації у відповідності до будь-якого стандарту (регламенту, концепцію та т.п.) не відміняє та не протирічить іншим стандартам (регламентам, концепціям та т.п.).

Стандарти описані вище не можуть по одинці забезпечити захист комп'ютерного середовища (систем), проте комплексний підхід дозволить якнайширше охопити всі розділи та підрозділи кібербезпеки: від технічної складової до питань менеджменту, оцінки ризиків (з оглядом на бізнес-процеси та необхідності) та максимального нівелювання людського фактору.

Окремо, у деяких своїх вимогах стандарт PCI DSS напряму звертається до рекомендацій інших стандартів (NIST, OWASP):

Вимога 1.1.6 вимагає документування службового обґрунтування та затвердження для використання всіх дозволених служб, протоколів і портів, а також документація по реалізованим засобів захисту тих протоколів, які визнані небезпечними[5]. А у примітках прямо каже: «За поясненнями по службам, протоколам та портам, що вважаються небезпечними, звертайтеся до галузевих стандартів та керівництв (наприклад, NIST, ENISA, OWASP та інші[5])».

Вимога 2.2 каже о необхідності розробити стандарти конфігурації для всіх системних компонентів та переконатися в тому, що ці стандарти враховують всі відомі наразі уразливості, а також узгоджуються з положеннями галузевих стандартів безпечної настройки систем. А серед галузевих стандартів наводить наступний список:

- Центр Інтернет-безпеки (CIS);
- Міжнародна організація по стандартизації (ISO);
- Інститут системного адміністрування, аудіта, мережеве технологій і проблем безпеки (SANS);
- Національний інститут стандартів і технологій (NIST)[5].

Вимога 2.2.3 затверджує необхідність впровадження додаткових захисних заходів для будь-яких необхідних служб, протоколів та/або

керуючих програм, що визнані небезпечними. І знову зсилається на NIST SP 800-52 і SP 800-57, OWASP та інші мережеві стандарти. При аналізі NIST SP 800-52 (Rev. 2) та SP 800-57 знаходиться, що «Безпека транспортного рівня (TLS) надає механізми для захисту даних під час електронного розповсюдження через Інтернет. Ця спеціальна публікація містить керівництво по вибору та налагодженню реалізацій протоколу TLS при ефективному використанні федеральних стандартів обробки інформації (FIPS) і криптографічних алгоритмів, рекомендованих NIST. Він вимагає, щоб TLS 1.2, налаштований за допомогою наборів шифрів на основі FIPS, підтримувався усіма державними серверами та клієнтами TLS, а також вимагає підтримки TLS 1.3 до 1 січня 2024 року. У цій спеціальній публікації також представлені рекомендації по сертифікатах та розширенням TLS, які впливають на безпеку[15].», з чого робиться висновок, що організації, що підпадають під дію стандарту PCI DSS, повинні використовувати лише TLS версії вище 1.1 (не включно). Окремо перевіряючи OWASP знаходиться: «Веб-додатки загального призначення повинні підтримувати тільки TLS 1.2 і TLS 1.3, при цьому всі інші протоколи повинні бути відключені.[16]», що підтверджує попередні висновки.

Таким чином більшість стандартів кібербезпеки пов’язані між собою та мають посилання один на одного.

1.4 Використання стандартів PCI DSS та SWIFT в споріднених умовах, що відрізняються від стандартних

Хоча стандарт PCI DSS та концепція SWIFT CSCF офіційно стосуються лише систем, що містять (зберігають, оброблюють чи передають) карткові дані, проте вимоги описані в них є досить універсальними та можуть використовуватися як основа (або допомога) при проектуванні будь-яких інших систем комп’ютеризованого захисту інформації.

Стандарт PCI DSS у першому розділі (першій над-вимозі) стверджує: «Міжмережеві екрани — це пристрої, які контролюють мережевий трафік, дозволений між локальними (внутрішніми) мережами організації і недовірених (зовнішніми) мережами, а також які контролюють вхідний і вихідний трафік в зонах підвищеної критичності, що знаходяться всередині довірених мереж організації. Середа ДТК є прикладом зони підвищеної критичності всередині довіреної локальної мережі організації.». Проте «зоною підвищеної критичності» можна вважати не тільки середу, що містить карткові дані, але й будь-яку іншу, дані в якій конфіденційні (в мірі, зазначеною самою організацією чи законодавством) або потребують найвищого захисту.

Або опис другого розділу: «Зловмисники (зовнішні і внутрішні по відношенню до організації) часто використовують для компрометації систем паролі та інші параметри за замовчуванням, задані виробником. Ці паролі і параметри добре відомі в спільнотах хакерів, і їх легко отримати з відкритих джерел.» Це загальні дані, що є актуальними для будь-якої системи. Та міри протидії, що приведені у стандарті є «посильні» та не важкі у інтеграції для будь-якої організації.

Шостий розділ стандарту PCI DSS пояснює, що: «Зловмисники використовують уразливості безпеки для отримання привілейованого доступу до систем. Багато з таких вразливостей усуваються за допомогою звичайних регулярних оновлень безпеки, які надаються вендором та які просто повинні встановлюватися організаціями, що управляють системами. На всі системи повинні бути встановлені всі належні оновлення ПЗ, щоб захиститися від експлуатації вразливостей і від компрометації ДТК зловмисниками і шкідливим ПЗ.» Крім того шостий розділ у собі містить питання безпечного кодування, створення звичайних та web-додатків заздалегідь захищеними, ще на етапі розробки наголошує (заставляє) перевіряти код на можливість застосування зловмисником SQL-ін’єкцій, атаки шляхом переповнення буферу, некоректного використання сховищ

даних, можливості передачі даних по небезпечним каналам зв’язку або використання при цьому небезпечних криптографічних алгоритмів.

Все це є важливим і для інших організацій, що ніяк не пов’язанні з транспортуванням, зберіганням або обробкою карткових даних.

У рівні впровадженого захисту завжди велику роль грає доцільність та бізнес-необхідності, коли будь-який ризик розглядається у співвідношенні втрат (фінансових та репутаційних) та складністю (та ціною) його нівелювання. Впровадження всіх вимог стандарту PCI DSS є досить важким та дорогим процесом, проте загальний «настрій», організаційні моменти, регулярні перевірки (тести на уразливості, тести на приникнення), систематизація ресурсів (матеріальних, технічних та людських), якій приділено досить вимог стандарту — може значно підвищити рівень безпеки системи.

Наразі питання комп’ютерної та інформаційної безпеки постоїть дуже гостро, методи зламу та крадіжки інформації постійно еволюціонують і дуже важливо якщо не опереджавати їх — критично не відставати від них. Втрата будь-якої інформації (з причини технічного збою, чи її витоку, чи крадіжки, чи зіпсування) спричиняє чималі втрати — матеріальні та репутаційні. Чим більша організація — тим більшим буде «ефект доміно», як було добро видно на прикладі SolarWinds[33, 34] у грудні 2020-го року. Злом однієї системи призвів до фатальних наслідків у тисячі інших, більш того — у тисячі систем, чия інфраструктура була державна, чия діяльність мала критичну важливість для людей (лікарні, банки, державні установи).

Тому питання взаємодії стандартів, розумного їх поєднання, в жазі до «ідеалу комп’ютерного захисту», наразі є вкрай актуальним. Бо наслідки втрати (крадіжки) інформації (що з маркою «конфіденційна», що без) з кожним роком стають значущі, страшніші.

1.5 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 (бо майже 70% грошей всього світу є лише у електронному вигляді), 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.

Попит породжує пропозицію: ростуть можливі прибутки від злому систем (хакінгу), росте кількість кібер-зловмисників, зростають і методи захисту від них. З'являється нова професія «спеціаліста з кіберзахисту», з'являються норми та стандарти, законодавчі нормативно-правові акти, що регулюють його роботу. Що регулюють рівень мінімального комп'ютерного та інформаційного захисту будь-якої організації.

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) та концепція SWIFT CSCF (розроблена спільно 168-ма фінансовими установами з усього світу).

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.

Концепція SWIFT CSCF у свою чергу повністю залежить від архітектурного рішення, як організація влаштовує SWIFT-перекази. Якщо організація не має ніякого відношення до SWIFT, то дана концепція особливо не зможе їй допомогти, проте якісь окремі моменти — так. Крім того, у SWIFT CSCF є окрема таблиця відповідності з стандартами PCI DSS та NIST CF, що зможе стати у нагоді.

Нарешті, наразі не є розумним концентруватися на якомусь одному стандарті комп'ютерної та інформаційної безпеки, всі вони у тій чи іншій

мірі доповнюють один одного. Якісь стандарти при деяких умовах є обов’язкові для виконання, але нехтувати через це іншими — неправильно.

РОЗДІЛ 2. РОЗРОБКА СИСТЕМИ ЗАХИСТУ ПЛАТІЖНИХ СИСТЕМ НА ОСНОВІ ВСІХ ВИМОГ ТА РЕКОМЕНДАЦІЙ СТАНДАРТІВ PCI DSS І SWIFT

2.1 Мережеве обладнання та міжмережеві екрани

Мережеве обладнання — це пристрої, що необхідні для успішної роботи будь-якої комп'ютерної мережі, наприклад: комутатор, маршрутизатор, концентратор, точка доступу, патч-панель та інші. Можна виділити окремо пасивне та активне мережеве обладнання.

До активного мережевого обладнання відноситься: мережевий адаптер, маршрутизатор (роутер), комутатор (свіч), мережевий трансивер, медіоконвектор, ретранслятор.

До пасивного ж відноситься: кабельна система з усіма її складовими (як різні різновиди кабелів (коаксіальний або кручена пара), , повторювач (репітер), патч-панель, концентратор (хаб), вилка та резетка, та навіть балун для коаксіальних кабелів) та монтажні шафи/стійки, телекомунікаційні шафи.

У загальному, різниця між «активного» та «пасивного» мережевого обладнання у їх «інтелекті».

Мережеве обладнання є також важливою частиною структури будь-якої організації, що підпадає під дії стандарту PCI DSS.

Окремо у стандарті за мережеве обладнання відповідає перший розділ (що вміщує у себе суть першої над-вимоги) та частково доторкується другий розділ.

Перший розділ зазначає: «Встановлювати та забезпечувати належну конфігурацію міжмережевих екранів для захисту ДТК». Проте якщо заглиблюватися у вимоги першого розділу вони напряму залежать від мережевого обладнання. На кінець, важко встановити міжмережевий екран за умови відсутності мережевого обладнання, зокрема маршрутизатора.

Перший етап розробки системи, відповідної до стандарту PCI DSS — проектування мережі організації так, щоб максимально відокремити зону, де

циркулюють карткові дані. Найчастіше це робиться за допомогою принципів сегментації, наведених 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. Прямий доступ з загальної корпоративної мережі до зони ДТК заборонено, а доступ до адміністративної частини має тільки адміністратор для виконання власних службових обов’язків. Більш того, у більшості випадків, він (доступ) передбачається віддаленим, через захищенні канали зв’язку та двухфакторну автентифікацію.

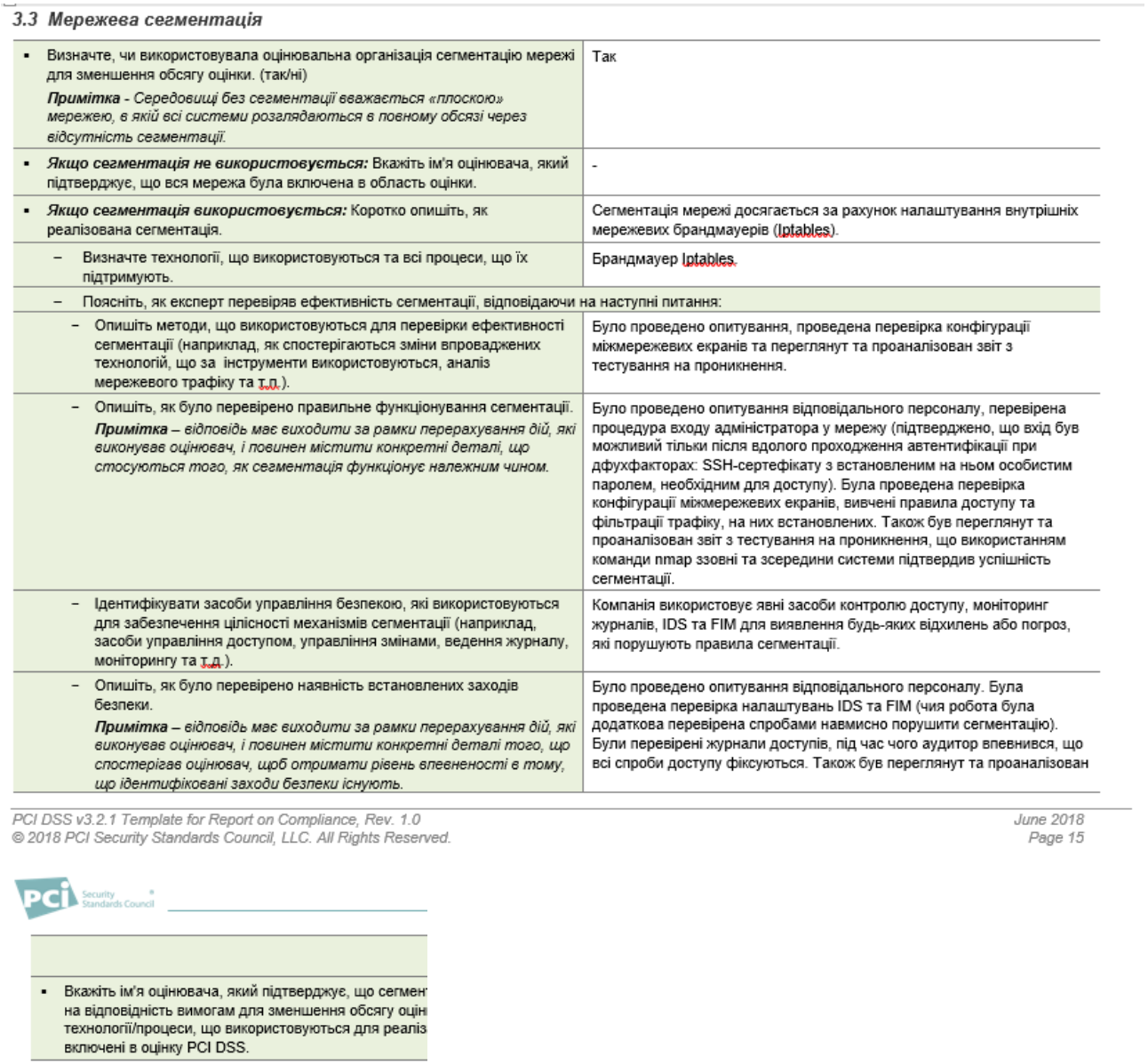
Концепція SWIFT CSCF також вимагає (у елементі контролю 1.1) використання сегментації, для ізолювання систем у яких здіснюються зв'язок для реалізації SWIFT-переказів.

У Додатку Ґ наведена реалізація сегментації ТОВ «Диплом» (вигаданої організації, задля наочного прикладу реалізації захисту карткових даних відповідно стандартів PCI DSS та SWIFT).

У звітному документі — Report on Compliance — є окремий розділ присвячений питанню сегментації, що необхідно заповнити аудитору у відповідності до рішень використовуємих організацією, що проходить сертифікацію на відповідність вимогам стандарту PCI DSS.

І хоча даний документ повинен заповнювати сертифікований QSA аудитор, проте для самоперевірки будь-якій організації буде корисно передивитися його та самостійно відповісти на поставленні запитання. Це допоможе визначити для себе чи дійсно сегментація працює та виконує поставлені завдання, можливо краще зміни принципи її реалізації, або змінити розміри та обсяги сегменту, що був обраний для вмісту ДТК.

На рисунку 2.1.а наведен приклад заповнення відповідного розділу Report on Compliance (приклад приведен на українську мову, хоча насправді увесь звітний документ є виключно на англійській мові та заповнюється відповідно також на англійській мові (оригінал приведений у Додатку Д):



3.3 Мережева сегментація

▪ Визначте, чи використовувала оцінювальна організація сегментацію мережі для зменшення обсягу оцінки. (так/ні) ***Примітка** - Середовищі без сегментації вважається «плоскою» мережею, в якій всі системи розглядаються в повному обсязі через відсутність сегментації.*	Так
▪ ***Якщо сегментація не використовується:*** Вкажіть ім'я оцінювача, який підтверджує, що вся мережа була включена в область оцінки.	-
▪ ***Якщо сегментація використовується:*** Коротко опишіть, як реалізована сегментація.	Сегментація мережі досягається за рахунок налаштування внутрішніх мережевих брандмауерів (Iptables).
– Визначте технології, що використовуються та всі процеси, що їх підтримують.	Брандмауер Iptables.
– Поясніть, як експерт перевіряв ефективність сегментації, відповідаючи на наступні питання:	
– Опишіть методи, що використовуються для перевірки ефективності сегментації (наприклад, як спостерігаються зміни впроваджених технологій, що за інструменти використовуються, аналіз мережевого трафіку та т.п.).	Було проведено опитування, проведена перевірка конфігурації міжмережевих екранів та переглянут та проаналізован звіт з тестування на проникнення.
– Опишіть, як було перевірено правильне функціонування сегментації. ***Примітка** – відповідь має виходити за рамки перерахування дій, які виконував оцінювач, і повинен містити конкретні деталі, що стосуються того, як сегментація функціонує належним чином.*	Було проведено опитування відповідального персоналу, перевірена процедура входу адміністратора у мережу (підтверджено, що вхід був можливий тільки після вдолого проходження автентифікації при дфухфакторах: SSH-сертефікату з встановленим на ньом особистим паролем, необхідним для доступу). Була проведена перевірка конфігурації міжмережевих екранів, вивчені правила доступу та фільтрації трафіку, на них встановлених. Також був переглянут та проаналізован звіт з тестування на проникнення, що використанням команди nmap ззовні та зсередини системи підтвердив успішність сегментації.
– Ідентифікувати засоби управління безпекою, які використовуються для забезпечення цілісності механізмів сегментації (наприклад, засоби управління доступом, управління змінами, ведення журналу, моніторингу та т.д.).	Компанія використовує явні засоби контролю доступу, моніторинг журналів, IDS та FIM для виявлення будь-яких відхилень або погроз, які порушують правила сегментації.
– Опишіть, як було перевірено наявність встановлених заходів безпеки. ***Примітка** – відповідь має виходити за рамки перерахування дій, які виконував оцінювач, і повинен містити конкретні деталі того, що спостерігав оцінювач, щоб отримати рівень впевненості в тому, що ідентифіковані заходи безпеки існують.*	Було проведено опитування відповідального персоналу. Була проведена перевірка налаштувань IDS та FIM (чия робота була додаткова перевірена спробами навмисно порушити сегментацію). Були перевірені журнали доступів, під час чого аудитор впевнився, що всі спроби доступу фіксуються. Також був переглянут та проаналізован

PCI DSS v3.2.1 Template for Report on Compliance, Rev. 1.0 *June 2018*
© 2018 PCI Security Standards Council, LLC. All Rights Reserved. *Page 15*

PCI Security Standards Council

▪ Вкажіть ім'я оцінювача, який підтверджує, що сегмен на відповідність вимогам для зменшення обсягу оцін технології/процеси, що використовуються для реаліз включені в оцінку PCI DSS.

Рисунок 2.1.а

Вимога 2.2 вимагає: «Розробити стандарти конфігурації для всіх системних компонентів. Переконатися в тому, що стандарти враховують всі відомі уразливості, а також узгоджуються з положеннями галузевих стандартів безпечної настройки систем.» А також відсилає до

загальноприйнятих галузевих стандартів щодо безпечної налаштування систем, наприклад:

- Центр Інтернет-безпеки (CIS);
- Міжнародна організація по стандартизації (ISO);
- Інститут системного адміністрування, аудиту, мережевих технологій та проблем безпеки (SANS);
- Національний інститут стандартів і технологій (NIST).

Одне із головніших правил, що необхідно реалізувати на мережевому обладнанню: один сервер — одна роль. Щоб не було пересічення різних рівнів безпеки для різних функцій на одному сервері, що може призвести до загального конфлікту мережі. Або й зниження рівня загальної безпеки.

Наступне завдання, відповідно до вимоги 1.1 «Розробити та впровадити стандарти конфігурації міжмережевих екранів і маршрутизаторів». Відповідно до цього та вимог 1.1.1-1.1.7 стандарти повинні містити у собі наступне:

- Формалізований процес налаштування та тестування нових мережевих з’єднань, протоколів та правил на міжмережевих екранах. Також необхідно заформалізувати процес будь-яких змін у налаштуваннях межмережевих екранів.
- Необхідно створити та підтримувати у актуальному стані схему мережі. Стандарт PCI DSS хвилюють виключно та її частина, що має відношення до обробки, транспортування чи зберігання карткових даних, проте вкрай корисним є також підтримка у актуальному стані схеми мережі всієї організації.
- Необхідно також створити та підтримувати у актуальному стані схему, що відображає потоки всіх карткових даних в та/або з організації.

- Необхідно реалізувати на міжмережевому обладнанні екранування кожного Інтернет-з'єднання та з'єднань між кожною демілітаризованою зоною та внутрішньою загальною мережею.
- Окремо необхідно виділити та розробити опис (та обов’язки) груп та ролей, що відповідальні за управління та налаштування мережевих компонентів.
- Також необхідно обов’язково підтримувати (та впровадити при необхідності) документування службового обґрунтування та затвердження для використання всіх служб, протоколів і портів, що є дозволені до використання на мережевому обладнанні. А також необхідна документація по реалізованим засобів захисту тих протоколів, що були попередньо визнані небезпечними.

У Додатку Е наведено налаштування правил на міжмережевому екрані (iptables) у ТОВ «Диплом».

Організації потрібно визначити та задокументувати усі мережеві потоки, що прямують з та/або в організацію, з вказанням необхідності їх використанням та роллю, що вони мають.

На рисунку 2.1.б наведен приклад даної схеми, з напрямком та обґрунтуванням необхідності даних потоків:

Сервіс	Джерело	
	IP	Порт/Протокол
soap	192.169.18.162 192.169.18.199 192.169.18.197 192.169.18.207	*any/TCP*
oracle	192.169.18.68	*any/TCP*
ssh	192.169.18.68 192.169.18.70 192.169.18.90 192.169.18.108 192.169.18.111	*any/TCP*
ntp	192.169.18.179	*any/TCP*
dns	192.169.18.179	*any/TCP*

Рисунок 2.1.б

Далі, відповідно до вимоги 2.1: «Завжди змінювати параметри за замовчуванням, задані виробниками, а також видаляти або відключати невикористовувані облікові записи за замовчуванням перед установкою

систем в мережі. Дана вимога може бути застосовано до всіх паролів за замовчуванням, включаючи, в тому числі, паролі до операційних систем, захисному програмному забезпеченню, облікового запису програм і системним облікових записів, POS-терміналів (термінали в точках продажів), платіжним додатків, а також рядках доступу SNMP і т.д.»

Зловмисники (зовнішні та/або внутрішні по відношенню до організації) часто використовують налаштування, облікові записи та паролі за замовчуванням, задані виробником, для компрометації операційних систем, додатків та пристроїв, на яких вони встановлені. Оскільки ці настройки за замовчуванням добре відомі та часто публікуються в хакерських спільнотах (та навіть інколи на офіційних сайтах виробників або у літературі відповідної направленості), їх зміна знизить загальну вразливість систем до атак.

Навіть якщо не планується використовувати обліковий запис за замовчуванням, зміна пароля за замовчуванням на надійний унікальний пароль та подальше відключення (а краще загальне видалення) облікового запису не дозволить зловмиснику повторно включити її та отримати доступ за допомогою пароля за замовчуванням.

Наприклад, системний обліковий запис суперкористувача root у Unix-подібних операційних системах неможливо видалити, тому рекомендовано поставити на нього складний пароль (від п’ятнадцяті символів, з використанням кількох абеток, великих та малих літер та спецсимволів).

Так само, як з потоками даних, вимога 2.4 вимагає вести облік всіх системних компонентів, на які поширюється дія стандарту PCI DSS. У Додатку Є наведена відповідна таблиця для організації ТОВ «Диплом» з обліком всіх системних компонентів, на які поширюється дія стандарту PCI DSS.

2.2 Налаштування доступів та облікових записів

У концепції SWIFT CSCF за налаштування доступу та облікових записів відповідають елементи контролю 1.2 (Контроль за превилігійованими обліковими записами) та 5.1 (Логічний контроль доступу). За своєю суттю вони дублюють (у меншому розмасі та конкретиці) відповідні вимоги стандарту PCI DSS, що зазначені нижче.

Сенс сьомого розділу стандарту PCI DSS — у строгому контролю доступу.

Відповідно до нього організація необхідна реалізувати системи та процеси, що бути обмежувати доступ до систем згідно службової необхідності та відповідно до службових обов'язків відповідальних осіб, щоб забезпечити доступ до критичних даними тільки зазначеному вище уповноваженому персоналу.

За визначенням стандарту службовою необхідністю є лише ті умови, коли права доступу надаються тільки до того мінімуму даних та привілеїв, що є необхідними для успішного виконання зазначених службових обов'язків.

Вимога 7.1: «Обмежити доступ до системних компонентів та ДТК тільки тими особами, яким такий доступ необхідний відповідно до їх службовими обов'язків».

Чим більше людей мають доступ до карткових даних, тим вище ризик того, що облікові записи користувачів будуть використовуватися для шкідливих цілей. Тип паче чим більша вибірка людей, тим вищий шанс того, що відповідно до людського фактору хтось забажає скомпрометувати карткові дані. Обмежуючи доступ тільки тими особами, яким він необхідний в службових цілях, організація може запобігти неналежній експлуатації ДТК, пов'язаній з недосвідченістю або злим умислом.

Отже, організації необхідно проаналізувати яке мінімальне коло співробітників необхідне для рівної роботи мережі з картковими даними та відповідно до визначеного кола змінити права та правила доступу осіб до системних компонентів та карткових даних, що вони містять.

У Додатку Є наведено приклад схеми рівня доступу, де до кожної ролі приведено у відповідність кількість співробітників, що її має та рівень конфіденційності інформації, до якої дана роль має доступ.

Далі, відповідно до вмісту вимоги 7.2 необхідно встановити систему (або системи) контролю доступу до системних компонентів, що буде обмежувати доступ відповідно зі службовою необхідністю певного (кожного) користувача та що буде дефолтно налаштована забороняти все, що є явно не дозволеним.

Відповідно до вимог стандарту ця система (або системи) контролю доступу має:

- охоплювати всі системні компоненти;
- призначати повноваження особам згідно їх ролям і зазначеним та документально (приказом) підтвердженим посадовими обов'язками;
- за замовчуванням забороняти будь-який доступ.

Суть восьмої вимоги стандарту PCI DSS полягає у необхідності ідентифікувати та автентифікувати будь-який доступ до системних компонентів, що мають відношення до передачі, обробки або зберіганню карткових даних (включені у область дії стандарту PCI DSS).

Відповідно до неї (її опису у стандарті) призначення унікального ідентифікатора кожній особі, що має доступ до систем (у розрізі стандарту, що містить карткові дані, у загальному розрізі — що має доступ до будь-якої системи), забезпечує однозначну підзвітність кожної (цієї) особи в її діях. Якщо така підзвітність реалізована у організації, то дії, вироблені з критичними даними та системами, проводяться відомими та авторизованими користувачами. Тому процеси та зв'язок між такими діями, що були скоєнні та призвели до тих чи інших наслідків може бути відстежено з повним розумінням (вистежуванням) користувача, що їх скоїв.

Крім того восьмий розділ має в собі дуже строгі вимоги до паролів та парольної політики у цілому. Загалом, на думку стандарту, ефективність пароля багато в чому залежить від пристрою та реалізації системи

автентифікації, зокрема від того, наскільки часто зловмисник може намагатися ввести пароль та які заходи безпеки вживаються для захисту паролів користувачів в точці введення, в момент передачі та під час його зберігання.

Вимога 8.1: «Визначити та впровадити в такий спосіб політики та процедури, що забезпечують належне управління ідентифікацією користувачів, які не є клієнтами, та обліковими записами адміністраторів на всіх системних компонентах, що входять у область дії стандарту PCI DSS».

Унікальний ідентифікатор для кожного користувача — замість використання одного ідентифікатора для кількох працівників — дозволить організації встановлювати індивідуальну відповідальність працівників за їх дії та більш ефективно вести журнал реєстрації подій по кожному з них. Це допоможе прискорити вирішення проблем та протидію їм, коли виявляються випадки некоректного використання або злого умислу.

Для впровадження даної вимоги стандарт вимагає виконати та підтримувати наступні вимоги (8.1.1-8.1.8):

- Призначити всім користувачам унікальні облікові записи, перш ніж надати їм доступ до системних компонентів або ДТК.
- Контролювати додавання, видалення та зміну облікових записів користувачів, облікових даних та будь-яких інших об'єктів ідентифікації. Це необхідно робити, для того щоб гарантувати, що облікові записи користувачів, що отримали (мають) доступ до систем, дійсні та правомочні. Слід застосовувати суворі процеси (нагляд та реакцію) до будь-яких змін у облікових записів користувачів та інших облікових даних (в т.ч. додаванню нових облікових записів, зміни або видалення вже наявних).
- Негайно відкликати доступ у кожного звільненого користувача. Якщо працівник звільнився з компанії та все ще має доступ до мережі через свій профіль, існує чималий ризик несанкціонованого або зловмисного доступу до ДТК через стару та/або невикористану

обліковий запис з боку зловмисника або колишнього працівника. Щоб запобігати несанкціонований доступ, слід відразу (як можна швидше) після того, як працівник відкликати призначені для користувача облікові дані і інші засоби автентифікації.

- Видаляти та/або блокувати не пізніш чим через 90 днів неактивні (ті вхід за якими не був створений ні разу за визначений раніше час) облікові записи. Облікові записи, що використовуються нерегулярно, часто піддаються атакам в зв'язку з меншою ймовірністю того, що зміни (наприклад, зміна пароля) будуть помічені. Отже, такими обліковими записами легше скористатися зловмисникам для доступу до ДТК.
- Необхідно керувати обліковими записами, що використовуються третіми сторонами для віддаленого доступу, підтримки та обслуговування системних компонентів, у наступний спосіб, передбачений стандартом PCI DSS:
  - включати тільки на необхідний проміжок часу і відключати, коли вони не використовуються;
  - вести моніторинг, коли вони використовуються.

  Надаючи вендорам (постачальникам послуг) доступ в мережу організації цілодобово та без вихідних для того, щоб вони могли в разі потреби обслуговувати системи організації, організація збільшує вірогідність несанкціонованого доступу як з боку користувача з середовища вендора, так й з боку зловмисника, який може виявити та відповідно змогти використовувати зовнішню точку входу в мережу постійно доступну для підключень. Включення доступу тільки на необхідні проміжки часу та відключення, коли в ньому більше немає необхідності, запобігає неналежне використання таких підключень.

  Загалом, ведучи моніторинг доступу вендорів, можна переконатися в тому, що вони отримують доступ тільки до необхідних систем та

тільки в узгоджений проміжок часу. Що також є додатковою (та інколи необхідною) перевіркою.

- Блокувати ідентифікатор користувача вже після шести невдалих спроб входу поспіль (максимальна кількість, на власний розсуд організація може поставити меншу межу невдалих спроб, чотири або п’ять разів). Якщо механізм блокування облікових записів не реалізований, зловмисник може безперервно намагатися підібрати пароль вручну або з використанням автоматизованих засобів (програм перебору паролів) до тих пір, поки йому це не вдасться, та він не отримає доступ до облікового запису користувача, що може призвести до компрометації карткових (або будь-яких інших конфіденційних) даних.
- Встановити період блокування ідентифікатора користувача рівним 30 хвилинам або до тих пір, поки його не розблокує адміністратор (у разі «спрацювання» пункту вище, блокування ідентифікатора користувача після що найбільш шести невдалих спроб доступу). Якщо обліковий запис користувача блокується в результаті безперервних спроб підбору пароля, захисні заходи у вигляді затримки активації заблокованих облікових записів допоможуть зупинити зловмисника від безперервного підбору пароля (він буде змушений зупинитися, принаймні, на 30 хвилин до автоматичної активації облікового запису). Крім того, якщо буде запрошена повторна активація, адміністратор або фахівець технічної підтримки може встановити, чи дійсно її запросив власник облікового запису.
- Якщо сеанс був неактивний протягом 15 хвилин та більше, система повинна вимагати у користувача пройти повторну автентифікацію для відновлення роботи терміналу або сеансу. Коли користувачі відлучаються від працюючих комп'ютерів, що мають доступ до критичних системних компонентів мережі або ДТК, ці комп'ютери

можуть бути використані будь-ким за відсутності цих користувачів, що призведе до несанкціонованого доступу до облікового запису та/або некоректного її використання.

Повторна перевірка справжності може бути застосована на системному рівні для захисту всіх сеансів, запущених на комп'ютері, або на рівні додатків, це не має різниці, головне, щоб була реалізована.

Окремо, відповідно до вимоги 8.2.1 необхідно привести всі облікові дані для автентифікації (наприклад, паролі та/або парольні фрази) до нечитабельного виду, з використанням стійкої криптографії, коли вони передаються мережею або зберігаються на будь-яких системних компонентах.

Багато мережевих пристроїв та додатків передають незашифровані паролі (для читання) по мережі та/або зберігають їх у незашифрованому вигляді. Зловмисник може легко перехопити незашифровані паролі при їх передачі, використовуючи аналізатор пакетів, або отримати прямий доступ до незашифрованих паролів у файлах, в яких вони зберігаються (наприклад, всім відомі LM Hash та NT Hash у ОС Windows), та використовувати ці дані для отримання несанкціонованого доступу.

За парольну політику відповідають вимоги 8.2.3-8.2.6. За ними паролі повинні мати наступні параметри:

- Необхідно змінювати пароль та/або парольну фразу щонайменше раз у 90 днів (для усіх облікових записів, крім сервісних, виконання даної вимоги на яких може призвести до збою у роботі мережі);
- Довжина паролів повинна бути:
    - Для звичайних користувачів — не менше 7 символів;
    - Для системних адміністраторів — не менше 13 символів (рекомендація стандарту, але не вимога);
    - Для сервісних облікових записів — не менше 20 символів (рекомендація стандарту, але не вимога).

- Пароль в собі обов'язково містить (для всіх типів облікових записів):
  - Верхній та нижній регістрів літер;
  - Цифри;
  - Спецсимволи (рекомендація стандарту, але не вимога);
  - Декілька абеток (рекомендація стандарту, але не вимога).
- Заборонено використовувати при зміні пароля останні чотири використовувані пароля (для всіх типів облікових записів);
- Повинна бути налагодженою системна вимога про зміну пароля при його першому використанні;
- Повинна бути налагодженою системна вимога про зміну пароля при його скиданні;
- Паролі (тимчасові та/або постійні) завжди повинні бути унікальними.

У концепції SWIFT за парольну політику відповідає елемент контролю 4.1 (Політика паролей) та вона біль «щадна» ніж парольна політика передбачана стандартом PCI DSS. Відповідно до цього у ТОВ «Диплом» реалізовано парольну політику з оглядом на вимоги PCI DSS, бо головне правило «не менш ніж».

Також стандарт PCI DSS вимагає захистити всі індивідуальні неконсольні адміністративні доступи та всі видалені доступи в мережу з ДТК з використанням мультифакторній автентифікації (вимога 8.3).

Мультифакторна автентифікація, в даному разі, вимагає від користувача надання, як мінімум, двох окремих форм автентифікації (як описано в вимозі 8.2) перед тим, як доступ до мережі буде надано.

Мультифакторна автентифікація забезпечує додаткову впевненість в тому, що особи, що намагаються отримати доступ, є тими, за кого себе видають. При використанні мультифакторній автентифікації зловмисникові доведеться скомпрометувати, як мінімум, два різних автентифікаційних механізмів, що підвищує складність компрометації і таким чином зменшує

ризик. «Я знаю» та «я володію», два відомих принципи, при співставленні яких і отримується мультифакторна автентифікація.

Мультифакторна автентифікація не обов'язково повинна бути одночасно на обох рівнях — на системному рівні та на рівні додатків — для певного системного компонента. Мультифакторна автентифікація може виконуватися або при вході в певну мережу, або при вході в окремий (певний) системний компонент, в залежності від реалізованих методів мультифакторної автентифікації.

Приклади технологій мультифакторній автентифікації включають серед іншого віддалену автентифікацію та систему RADIUS з токенами або ж систему TACACS з токенами та будь-які інші технології, які підтримують мультифакторну автентифікацію.

У концепції SWIFT за багатофакторну автентифікацію відповідає елемент контролю 4.2 (Багатофакторна автентифікація) та вона повністю відповідає вимогам, зазначеним у стандарті PCI DSS.

Вимога 8.5 дещо дублює вимогу 2.1, проте окремо додає ще про групові та загальні облікові записи та паролі: «Не застосовувати препарат групові, загальні та стандартні облікові записи і паролі, а також інші подібні методи автентифікації».

Якщо кілька користувачів використовують одні й ті ж облікові дані для автентифікації (наприклад, обліковий запис admin та відповідний пароль), простежити за доступом в систему та діями того чи іншого користувача (персоніфіковано) стає неможливо. Це, в свою чергу, не дозволить організації встановлювати відповідальність за дії конкретного користувача, або фактично реєструвати події, пов'язані з тими чи іншими його діями, оскільки ці дії можуть бути здійснені будь-яким членом групи, якій відомі облікові дані для автентифікації.

2.3 Криптографія. Канали передачі карткових даних

Питанню криптографічного захисту карткових даних, а також захисту каналів передачі карткових даних у стандарті PCI DSS присвячено третій та четвертий розділи.

У концепції SWIFT значення має лише захист даних при їх передачі (проходження) через SWIFT-перекази, проте всі її вимоги дублюються вимогами стандарту PCI DSS, зазначеними у третьому та четвертому розділі.

Третій розділ відповідає за захист ДТК. Такі методи захисту, як шифрування, усічення, маскування та хешування є найважливішими компонентами захисту ДТК. Якщо зловмисник обходить інші захисні заходи та отримує доступ до зашифрованих даних без належного криптографічного ключа, то ці дані залишаються для зловмисника нечитабельним та відповідно непридатними для використання. Інші ефективні методи захисту даних, що зберігаються також слід розглядати як потенційні можливості зниження ризику. Наприклад, методи мінімізації ризику включають в себе також повну відмову від зберігання ДТК, крім випадків крайньої необхідності, усічення ДТК, якщо повний PAN (номер картки) не потрібен, та відмову від передачі PAN в незахищеному вигляді з використанням технологій обміну повідомленнями для кінцевих користувачів, таких як електронна пошта та системи миттєвого обміну повідомленнями.

Вимога 3.1 каже, що необхідно звести ДТК до мінімуму за допомогою політик, процедур та процесів зберігання та знищення даних. PCI DSS вимагає, щоб усі сховища ДТК (наприклад, бази даних) виконували наступні вимоги:

- обмежити кількість збережених даних та терміни їх зберігання до значень, необхідних для виконання законодавчих, нормативних та/або службових вимог;
- розробити та дотримуватися конкретних вимог щодо зберігання ДТК;
- реалізувати процеси безпечного видалення даних, коли в них вже немає необхідності;

- виконувати щоквартальний процес виявлення та безпечного видалення ДТК, за якими перевищено строки зберігання, встановлені вимогами (або політиками організації чи банка-еквaєра, якщо на заканодавчому рівні не вказано іншого).

Офіційна політика зберігання даних визначає, які дані необхідно зберігати та де повинні знаходитися ці дані, щоб їх можна було безпечно знищити або видалити, коли вони вже більше не потрібні.

Після авторизації дозволяється зберігати тільки номер карти (PAN) (приведений у нечитаний вид), дату закінчення терміну дії картки, ім'я власника картки та сервісний код (якщо він є).

Знання місць зберігання ДТК необхідно для реалізації їх належного зберігання або видалення, коли вони більше не потрібні. Щоб визначити належні вимоги до зберігання, організації спочатку слід з'ясувати свою службову необхідність, а також будь-які законодавчі або нормативні вимоги, які застосовні до її галузі та/або до типу даних, що в ній зберігаються.

Наступна вимога, 3.2, забороняє зберігати КАД після авторизації, навіть у нечитаємому вигляді. Виключення стосується виключно банків та фінансових установам, що випускають картки та зберігання КАД у яких є процесинговою необхідністю.

Консорціум накладає заборону на зберігання КАД, бо вони складаються з повних даних треків (магнітної полоси чи чіпу), коду або значення перевірки автентичності карти та даних ПІН-коду. Ці дані становлять велику цінність для зловмисників, тому що останні, використовуючи такі дані, можуть генерувати підроблені платіжні картки та здійснювати шахрайські транзакції.

Вимога 3.3 пояснює, у якому вигляді можливе зберігання PAN: «Маскувати PAN при його відображенні (максимально можлива кількість відображуваних цифр — перші шість та останні чотири), щоб тільки працівники з обґрунтованою службовою необхідністю могли бачити більше ніж перші шість та/або останні чотири цифри PAN».

Повний номер картки для зловмисника, це гарна нагода вкрасти гроші, навіть пряме запрошення до цього. А скільки шахрайских схем на цьому базується…

Відображення повного PAN на екранах комп'ютерів, чеках про оплати з використанням платіжних карт, на факсах або в паперових звітах може привести до того, що ці дані стануть відомі стороннім особам та можуть бути використані в шахрайських цілях. Відображення повного PAN тільки тим особам, у яких є така обґрунтована службова необхідність, мінімізує ризики того, що сторонні особи отримають доступ до даних PAN.

Метод маскування завжди повинен забезпечувати відображення мінімальної кількості цифр, які необхідні для виконання конкретної виробничої функції. Наприклад, якщо тільки останні чотири цифри потрібні для виконання виробничої функції, PAN маскується так, що працівник, що виконує дану функцію, може бачити тільки останні чотири цифри. Інший приклад: якщо виробнича необхідність вимагає доступ до банківського ідентифікаційному номеру (BIN) для маршрутизації, відображаються тільки цифри BIN (зазвичай це перші шість цифр) протягом виконання цієї виробничої функції.

Проте вимога 3.3 стосувалася виключно відображення PAN на екранах або паперових (будь-яких матеріальних) носіях. Існує також вимога 3.4, що окремо регламентує у якому вигляді PAN повинен зберігатися в усіх сховищах.

Відповідно до неї, його необхідно привести до нечитабельного вигляду у всіх місцях його зберігання (включаючи журнали подій (логи), резервні копії, знімні цифрові носії), використовуючи для цього будь-який з наступних методів:

- односпрямоване хешування на основі стійкої криптографії (хеш-код повинен бути сформований з цілого PAN);
- усічення (хеш-код не може використовуватися для заміни усіченого сегмента PAN);

- індексні маркери і шифрувальні блокноти (такі блокноти при зберіганні повинні бути захищені);
- стійка криптографія з супутніми процесами і процедурами управління ключами.

Основна меті цієї вимоги — захистити всі PAN, що зберігаються в основних сховищах (базах даних, неструктурованих файлах, таких як текстові файли, таблиці і т.д.), а також в усіх допоміжних сховищах (резервних копіях, журналах реєстрації подій, журналах винятків та налагодження і т.д.).

Для приведення ДТК до нечитабелого вигляду можна використовувати функції односпрямованого хешування на основі стійкої криптографії. Його використання доцільне тоді, коли немає необхідності у відновленні вихідного номера (так як односпрямоване хешування є незворотнім). Бажано (але на даний момент стандарт не визначає це вимогою) додавати додаткові вхідні значення до ДТК перед початком хешування, щоб у зловмисника було менше можливостей для порівняння даних (та отримання в результаті первісного PAN) з таблицями попередньо підрахованих значень хеш-кодування.

Мета усічення полягає в тому, щоб безповоротно видаляти частину PAN, так що збереженою залишається лише частина PAN (як правило, не більше шести перших та чотирьох останніх цифр), що у разі компрометації не наробить лиха.

Індексний маркер — це криптографічний маркер, який замінює PAN, заснований на певному індексі значень, що не піддаються прямому обчисленню. Одноразовий блокнот — це система, в якій секретний ключ, згенерований випадковим чином, використовується тільки один раз для шифрування повідомлення, яке потім розшифровується за допомогою відповідного одноразового блокнота та ключа.

Мета стійкої криптографії (у сенсі, що криптографічна стійкість — це здатність криптографічного алгоритму протистояти криптоаналізу. Стійким вважається алгоритм, який для успішної атаки вимагає від противника

недосяжних обчислювальних ресурсів, недосяжного обсягу перехоплених відкритих і зашифрованих повідомлень чи ж такого часу розкриття, що по його закінченню захищена інформація буде вже не актуальна, і т.д. У більшості випадків крипостійкість не можна математично довести, можна тільки довести уразливості криптографічного алгоритму) полягає в тому, що шифрування має ґрунтуватися на використанні протестованих та загальноприйнятих галузевих алгоритмів з високою надійністю криптографічних ключів (а не пропрієтарних або «самописних» алгоритмів).

Зіставляючи хешовані та усічені версії PAN, зловмисник може легко обчислити вихідний PAN. Заходи, які використовуються, щоб запобігти зіставлення цих даних, допомагають забезпечити нечитаність вихідного PAN.

Якщо використовується шифрування PAN, то у дію ступають вимоги 3.5.2-3.5.4, що вимагають розподіл обов'язків між співробітниками, що мають доступ до ключів шифрування та співробітників, що мають доступ до зашифрованих PAN (все виключно зі службової необхідності). Іншими словами, співробітник, що має доступ до ключів шифрування не повинен мати право доступу до баз даних або будь-яких інших місць зберігання зашифрованих PAN, а співробітник, що має доступ до зашифрованих PAN, не може мати права доступу до ключів шифрування.

Враховуючи все вище сказане була побудована та структурована таблиця 2.3.а:

Таблиця 2.3.а

Варіант маскування	**Суть**	**Недоліки**	**Доцільність**

Односпрямоване хешування на основі стійкої криптографії (хеш-код повинен бути сформований з цілого PAN).	Використання функції односпрямованого хешування на основі стійкої криптографії для шифрування PAN.	Неможливе обернене перетворення.	Коли немає необхідності у відновленні вихідного номера (так як односпрямоване хешування є незворотнім).
Усічення (хеш-код не може використовуватися для заміни усіченого сегмента PAN).	Мета усічення полягає в тому, щоб безповоротно видаляти частину PAN, залишаючи «безпечну» частину (як правило, не більше шести перших та чотирьох останніх цифр).	Неможливе обернене перетворення.	Коли немає необхідності у відновленні вихідного номера.
Індексні маркери та шифрувальні блокноти (такі блокноти при зберіганні повинні бути додатково захищені).	Індексний маркер — це криптографічний маркер, який замінює PAN, заснований на певному індексі значень, що не піддаються прямому обчисленню. Одноразовий	Якщо існує можливість «відкату» шифрування, то нею може скористатися зловмисник.	Коли є вірогідність необхідності зворотного перетворення зашифрованого PAN у відкритий.

	блокнот — це система, в якій секретний ключ, згенерований випадковим чином, використовується тільки один раз для шифрування повідомлення, яке потім розшифровується за допомогою відповідного одноразового блокнота та ключа.		
Стійка криптографія з супутніми процесами і процедурами управління ключами.	Шифрування має ґрунтуватися на використанні протестованих та загальноприйнятих галузевих алгоритмів з високою надійністю криптографічних ключів.	Якщо існує можливість «відкату» шифрування, то нею може скористатися зловмисник.	Коли є вірогідність необхідності зворотного перетворення зашифрованого PAN у відкритий.

Також стандарт вимагає додаткового захисту для самих ключів шифрування PAN, аж до їх шифрування або зберігання у спеціальному

криптографічному модулі. Крім того ключі необхідно зберігати у мінімальній кількості місць.

Четвертий розділ відповідальний же за безпеку передачі карткових даних. Відповідно до нього критична інформація повинна бути зашифрована при передачі її через мережі, до яких зловмисники можуть легко отримати доступ. Неправильно сконфігуровані бездротові мережі та уразливості застарілих протоколів шифрування та автентифікації залишаються й наразі бажаними (та першими) цілями для зловмисників, які використовують дані уразливості, щоб отримати привілейований доступ до середовища ДТК.

Відповідно вже пункт 4.1 вимагає, використовувати стійку криптографію та безпечні протоколи, щоб захистити критичні ДТК при їх передачі через відкриті загальнодоступні мережі. Крім того необхідно брати до уваги наступне:

- приймаються тільки довірені ключі та сертифікати;
- використовуваний протокол підтримує тільки безпечні версії і конфігурації;
- якість шифрування відповідає використовуваної методології шифрування.

Критична інформація повинна шифруватися при передачі по мережах загального користування, тому що зловмисник без праці може перехопити та/або змінити її маршрут при передачі.

Безпечна передача ДТК вимагає використання довірених ключів та/або сертифікатів, безпечного протоколу передачі та шифрування належної стійкості для шифрування ДТК. Не слід приймати запити на підключення від систем, що не підтримують необхідну якість шифрування, так як це може призвести до небезпечного (та несанкціонованого) підключенню.

Слід зазначити, що деякі версії протоколів (наприклад, SSL, SSH 1.0 та ранні версії TLS (якими на сьогодні вважаються всі версії до 1.1 включно)) містять відомі уразливості, які можуть бути використані зловмисником для отримання контролю над системою, що має у собі відповідні вразливості.

Незалежно від того, який протокол використовується, слід переконатися, що він налаштований на те, щоб використовувати тільки безпечні конфігурації та версії для запобігання небезпечного підключення. Наприклад, використовувати тільки надійні сертифікати та підтримувати виключно стійке шифрування (не підтримувати нестійкі, небезпечні протоколи або методи).

Дана вимога також доповнює вимогу 2.3 «При використанні будь-якого неконсольного адміністративного доступу до системи завжди шифрувати канал з використанням стійкої криптографії».

ТОВ «Диплом» використовує TLS 1.1, що видно з наведеному у Додатку З витягу з конфігураційних файлів. Це необхідно виправити, шляхом підвищення версії протокола TLS до 1.2.

Перевірка того, що сертифікат є довіреним (наприклад, термін дії його не закінчився, та він отриманий з довіреного джерела), допомагає забезпечити цілісність безпечного підключення. Саме тому стандарт PCI DSS не рекомендує використовувати самопідписані сертифікати загалом, а для підключення до мереж з ДТК (або при передачі ДТК) категорично забороняє їх використання.

У вимозі 4.1.1 стандарт окремо наголошує на необхідності звертатися до передового галузевого досвіду, для визначення, які протоколи є безпечними, а які ні: «Переконатися, що при використанні бездротових мереж, що передають ДТК або підключених до середовища ДТК, застосовується передовий галузевий досвід, щоб реалізувати стійке шифрування при автентифікації та передачі даних».

Це логічно, бо дуже часто зловмисники використовують вільно поширювані та широкодоступні засоби для прослуховування бездротового трафіку, не займаючись без крайньої потреби винаходженням велосипеду. Використання стійкої криптографії може обмежити розкриття критичної інформації, переданої по бездротовим мережам.

Щоб запобігти доступу зловмисників до бездротових мереж або використання ними бездротових мереж для отримання доступу до інших внутрішніх мережах або даними, необхідна стійка криптографія для автентифікації та передачі ДТК.

И наостанок, необхідно заборонити пересилання PAN через електронну пошту або інші методи миттєвого зв’язку. Повідомлення, надіслані електронною поштою, за допомогою систем миттєвого обміну повідомленнями, в чаті, або SMS можуть бути перехоплені в процесі доставки, як у внутрішній, так і в зовнішній загальнодоступній мережі. Не слід використовувати ці засоби передачі повідомлень для відправки PAN, якщо вони не забезпечують стійкого шифрування (а вони не забезпечують).

Крім того, якщо організація запитує PAN через технології обміну повідомленнями для кінцевих користувачів, вона повинна забезпечити засіб або метод захисту таких PAN за допомогою стійкої криптографії або приведення PAN до нечитабельним увазі перед передачею. Крім того, дана організація повинна або надати письмову гарантію надійності такої передачі, чи окремі пункти щодо цього повинні бути прописані у договорі.

2.4 IDS/IPS, FIM, Antivirus. Журналювання

IDS (система виявлення вторгнень) — це це пристрій або програмний додаток, який відстежує мережу або системи на предмет зловмисних дій або порушень політики. Про будь-які вторгнення або порушеннях зазвичай повідомляється адміністратору або збирається централізовано за допомогою системи управління інформацією і подіями безпеки (SIEM). Система SIEM об'єднує вихідні дані з декількох джерел і використовує методи фільтрації сигналів тривоги, щоб відрізнити шкідливу активність від хибних сигналів[36].

Типи IDS варіюються від окремих комп'ютерів до великих мереж. Найбільш поширеними класифікаціями є: системи виявлення мережевих

вторгнень (NIDS) та системи виявлення вторгнень на основі хостів (HIDS). Система, що відстежує важливі файли операційної системи, є прикладом HIDS, а система, яка аналізує вхідний мережевий трафік, є прикладом NIDS. Також можливо класифікувати IDS за методом виявлення. Найбільш відомі варіанти — це виявлення на основі сигнатур (розпізнавання поганих шаблонів, на кшталт шкідливих програм) та виявлення на основі аномалій (виявлення відхилень від моделі «хорошого» трафіку, яка часто заснована на машинному навчанні). Інший поширений варіант — це виявлення вторгнень на основі репутації (розпізнавання потенційної загрози з показниками репутації). Деякі продукти IDS можуть реагувати на виявлені вторгнення. Системи з можливістю реагування зазвичай називають системою запобігання вторгнень (IPS)[37]. Системи виявлення вторгнень також можуть служити певним цілям, доповнюючи їх налаштованим інструментами, такими як використання пасток для залучення та визначення характеристик шкідливого трафіку[38].

Стандарт PCI DSS у пункті 11.4 вимагає використовувати методи виявлення та/або запобігання вторгнень для виявлення та/або запобігання вторгнення в мережу. Необхідно здійснювати моніторинг всього мережевого трафіку по периметру середовища ДТК та в критичних точках всередині середовища ДТК, та сповіщати працівників про підозри на компрометацію.

Вкрай необхідно підтримувати в актуальному стані системи виявлення та запобігання вторгнень, їх сигнатури та правила.

Методи виявлення та/або запобігання вторгнень (наприклад, система виявлення або запобігання вторгнень, IDS/IPS) зіставляють трафік, що надходить у мережу з тисячами відомих сигнатур та/або моделей шкідливої поведінки (інструментарій зловмисників, троянське та інше шкідливе ПЗ та т.д.), а також у виявленні підозри чи атаки відправляють попередження та/або блокують спробу проведення атаки. Не використовуючи превентивні заходи для виявлення несанкціонованої діяльності, можна легко не помітити атаки на комп'ютерні ресурси (або їх неналежне використання) в момент

виконання. Для блокування спроб вторгнень необхідно вести постійний моніторинг повідомлень, що генеруються даними засобами. Прикладом такої системи може слугувати OSSEC, CloudFlare або Snort.

ТОВ «Диплом» використовує CloudFlare у якості системи для виявлення та/або запобіганню вторгнень. Увесь трафік, що надходить до організації з мережі Інтернет, проходить спочатку через CloudFlare, а лише потім потрапляють (якщо пройшли перевірку) на брандмауер. Також, як додатковий захист, компанією використовується OSSEC, проте всі його логи (дані журналювання) перенаправляються на Wazuh, про що буде йтися нижче.

Вимога 11.5 наполягає (вимагає) на необхідність знаходження у системі моніторингу цілісності файлів (FIM). Іншими словами, вона вимагає впровадити засіб виявлення змін (наприклад, моніторинг цілісності файлів), щоб повідомляти працівників про несанкціоновані зміни (включаючи, зміни, додавання та видалення) критичних системних файлів, конфігураційних файлів або файлів даних. Необхідно налаштувати програмне забезпечення так, щоб воно зіставляло критичні файли не рідше одного разу на тиждень (а краще щодня. З точки зору доцільності, краще у ночі, коли напруга на сервери падає).

Засоби виявлення змін, наприклад, інструменти для моніторингу цілісності файлів перевіряють критичні файли на зміни, додавання та видалення та повідомляють при виявленні змін. Якщо такий засіб впроваджено неналежним чином, а його звіт не перевіряється, то зловмисник може додати, видалити або змінити вміст конфігураційних файлів, програми операційної системи або виконувані файли додатків. Непомічені несанкціоновані зміни можуть погіршити роботу захисних заходів та/або привести до крадіжки ДТК без помітного впливу на процеси обробки.

ТОВ «Диплом» у своїй роботі використовує Wazuh у якості FIM. Проте також Wazuh виконує дуже важливу роль сповіщення про загрози та загальної аналітики. Організація виконала переадресацію усіх логів з OSSEC

та Syslog (вбудована утиліта журналювання у Unix-подібних системах) (конфігураційний файл, що дозволив таку переадресацію наведено у Додатку І) та завдяки зручному інтерфейсу та багаточисельним функціям Wazuh може робити аналітику відносно будь-яких подій безпеки.

У Додатку И представлено приклад вигляду інтерфейсу Wazuh.

Питанню антивірусного захисту присвячено увесь п’ятий розділ стандарту PCI DSS.

Шкідливе ПЗ, включаючи віруси, черв'яків та трояни, проникає в мережу під час виконання багатьох дозволених бізнесом дій, включаючи використання працівниками електронної пошти, мережі Інтернет, мобільних комп'ютерів, а також запам'ятовуючих пристроїв, що призводить до експлуатації вразливостей системи. Антивірусне ПЗ повинно використовуватися на всіх системах, зазвичай піддаються впливу шкідливого ПЗ, щоб захистити системи від поточних і можливих загроз з боку шкідливого ПЗ. Додаткові рішення для захисту від шкідливого ПЗ можуть використовуватися в якості доповнення до антивірусного ПЗ; однак такі додаткові рішення не знімають вимога про обов'язкову наявність антивірусного ПЗ.

Відповідно до вимоги 5.1 необхідно розгорнути антивірусне ПЗ на всіх системах, що зазвичай піддаються впливу шкідливого ПЗ (особливо на персональних комп'ютерах та серверах). І всі наступні вимоги розділу стосуються необхідності регулярного оновлення сигнатур антивірусного ПЗ, необхідності заборони можливості користувачу самостійно вимикати або призупиняти роботу антивірусного ПЗ.

Проте якщо організація використовую системи (сервери, персональні комп’ютери тощо) з Unix-подібною ОС, то ці вимоги для неї стають необов’язкові. Обов’язковою є лиш вимога 5.1.2: «Проводити періодичні перевірки в системах, які зазвичай вважаються не податними зараженню шкідливим ПЗ, виявляючи та оцінюючи загрози зараження новими формами

шкідливого ПЗ, для того, щоб перевіряти, що ці системи як і раніше не вимагають антивірусного ПЗ».

ТОВ «Диплом», що розглядається як організація, що проходить сертифікацію на відповідність PCI DSS, відповідно до своєї матриці (списку) мережевого обладнання (що приведений у Додатку Є) має якраз Unix-подібну ОС на системах. Проте вимога 5.1.2 нею не дотримується, що необхідно виправити.

Питанню журналювання присвячено увесь десятий розділ стандарту PCI DSS та 6.4 елемент контролю з концепції SWIFT.

Механізми реєстрації подій та можливість простежити дії користувачів є критичними для виявлення, запобігання та мінімізації впливу від компрометації даних. Наявність журналів реєстрації у всіх середовищах дозволяє ретельно відстежувати, створювати оповіщення та проводити аналіз при виникненні позаштатних ситуацій. Без журналів реєстрації дій у системі визначити причини компрометації важко, якщо взагалі можливо.

Якщо підсумувати всі вимоги десятого розділу, можна визначити наступні положення.

Необхідно реєструвати наступні події на системних компонентах, що містять ДТК:

- Будь-який доступ користувача до даних власників карток;
- Будь-які дії, вчинені з використанням адміністративних повноважень;
- Будь-який доступ до записів про події в системі;
- Неуспішні спроби логічного доступу;
- Ідентифікації та автентифікації користувачів;
- Розширення повноважень;
- Будь-які зміни, додавання або видалення облікових записів з правами суперкористувача або адміністратора;
- Зупинка або припинення ведення журналів протоколювання подій;

- Факти створення та видалення об'єктів системного рівня.

Для кожної події кожного системного компонента повинна бути записана як мінімум наступна інформація:

- Ідентифікатор користувача;
- Тип події;
- Дата та час;
- Успішним або неуспішним була подія;
- Джерело події;
- Ідентифікатор або назва даних, системного компонента або ресурсу, на які вплинуло подія.

Журнали протоколювання подій повинні бути захищені від змін:

- Доступом до журналів протоколювання подій повинні володіти тільки ті співробітники, яким такий доступ необхідний відповідно до їх посадовими обов'язками;
- Журнали протоколювання подій повинні бути захищені від несанкціонованого зміни;
- Резервні копії журналів протоколювання подій повинні оперативно зберігатися на централізований сервер протоколювання або окремий носій, де їх зміна була б утруднено;
- Копії журналів протоколювання подій для технологій, до яких можливий доступ ззовні, повинні зберігатися на безпечний і централізований внутрішній сервер протоколювання або носій;
- Слід використовувати додатки контролю цілісності файлів для захисту журналів реєстрації подій від несанкціонованих змін (проте додавання нових даних не повинно викликати тривожного сигналу).

Вивчати журнали протоколювання подій та події безпеки всіх системних компонентів з метою виявлення аномалій або підозрілої активності (окремо стандарт передбачає, що для забезпечення відповідності

даній вимозі можуть використовуватися засоби збору та аналізу журналів протоколювання подій, а також засоби оповіщення).

Стандарт вимагає перевіряти не рідше одного разу в день:

- Всі події безпеки.
- Журнали всіх системних компонентів, що здійснюють зберігання, обробку або передачу даних власників карток і (або) критичних автентифікаційних даних, або впливають на їх безпеку.
- Журнали всіх критичних компонентів системи.
- Журнали всіх системних компонентів, що виконують функції безпеки (наприклад, брандмауерів, систем виявлення і запобігання вторгнень, серверів автентифікації та т.д.).

Періодично вивчати журнали інших системних компонентів на підставі політик та стратегії управління ризиками, яка визначається в рамках щорічної оцінки ризиків.

Вивчати виключення та аномалії, виявлені під час перевірки.

Журнали реєстрації подій потрібно зберігати не менше одного року, також потрібно забезпечити доступ до журналів в оперативному режимі (не менше трьох місяців).

ТОВ «Диплом», як уже було сказано раніше, використовує для журналювання вбудовану утиліту Unix-подібних систем Syslog. З якої налаштовано збір та переправка всіх логів у Wazuh, який у свою чергу виконує їх аналіз та повідомляє у разі виявлення будь-якої аномалії (або знаходження ситуації, яка винесена у окремий «алярм»).

2.5 Фізична безпека

Фізичній безпеці присвячено увесь дев’ятий розділ стандарту PCI DSS та елементи контролю 3.1 у концепції SWIFT CSCF.

Будь-який фізичний доступ до даних або системам, що містить ДТК, надає зловмисникам можливість отримати доступ до пристроїв або даними,

видалити системи або друковані матеріали. Такий доступ повинен бути відповідним чином обмежений, задля унеможливлення (або максимальної мінімізації) проникнення зловмисника.

Пункт 9.1 вимагає: «Використовувати належні засоби контролю проходу на територію, щоб обмежувати і відстежувати фізичний доступ до систем середовища ДТК».

Без механізмів контролю фізичного доступу (наприклад, бейджів та контролю за входом в приміщення) сторонні можуть без зусиль отримати доступ до приміщень з метою крадіжки, відключення, псування або знищення критичних систем та ДТК.

Блокування екрану входу в консоль не дозволить стороннім особам отримати доступ до критичної інформації, внести зміни в системну конфігурацію, занести уразливості в мережу або знищити записи.

І відповідно до вимог 9.1.1-9.1.3 необхідно встановити (виконувати) наступне:

- Використовувати або камери відеоспостереження, які механізми контролю доступу (або обидва варіанти) для відстеження кожного випадку фізичного доступу до критичних приміщень. Перевіряти зібрані дані та зіставляти їх з іншими даними. Зберігати ці дані не менше трьох місяців, якщо законодавством не накладені інші обмеження;
- Впровадити механізми фізичного та/або логічного контролю, щоб обмежити доступ до мережевих роз'ємів на задній в загальнодоступних місцях;
- Обмежити фізичний доступ до бездротових точок доступу, шлюзів, портативних пристроїв, мережевого або комунікаційного обладнання та ліній зв'язку.

Далі йде вимога 9.2, що передбачає розроблення процедур(и), що дозволяють легко розрізняти працівників об'єкта (організації) від відвідувачів та які передбачають:

- ідентифікацію працівників об'єкта або відвідувачів (наприклад, шляхом видачі бейджів);
- вимоги до внесення змін до права доступу;
- вилучення або блокування засобів ідентифікації у працівників об'єкта або коштів ідентифікації з вичерпаним терміном дії (наприклад, бейджів) у відвідувачів.

Сенс даної вимоги полягає у необхідності ідентифікуючи авторизованих відвідувачів так, щоб їх можна було легко відрізняти від працівників об'єкта (організації). Таким чином можна виключити надання доступу стороннім відвідувачам до місць зберігання ДТК.

Вимога 9.3. передбачає контроль фізичного доступу працівників об'єкта (організації) до критичних приміщень наступним чином:

- стверджувати права доступу згідно персональним посадовими обов'язками;
- відкликати доступ відразу після звільнення працівника; забирати або відключати всі засоби фізичного доступу (наприклад, ключі, карти доступу та т.д.).

Контроль фізичного доступу до критичних приміщень дозволяє забезпечити, щоб доступ надавався тільки уповноваженим працівникам, яким він дійсно необхідний для виконання своїх посадових обов'язків.

Якщо працівник звільняється з організації, відразу після звільнення (якомога швидше) слід забрати або відключити всі засоби фізичного доступу, щоб працівник не міг отримати фізичний доступ до критичних приміщень (що перекликається з вимогою відразу відзивати доступ у звільненого співробітника до систем та мереж організації, приведеною у сьомому розділі).

Всі ці вимоги будуть стосуватися організації виключно, якщо вона є власником (відповідальною стороною) приміщень, де знаходяться сервери або персональні комп’ютери (або будь-яка інша техніка) з доступом до карткових даних. Якщо ж організація винаймає сервери у якогось дата-

центру, зберігає їх в тому самому дата-центрі, то відповідальність за них лежать саме на ньому — дата-центрі. Потрібен бути заключений договір поміж організацією та дата-центром, з обов’язковими пунктами, щодо дотримання політик інформаційної безпеки, що прийняті у організації.

ТОВ «Диплом» використовує якраз другий варіант, дана організація орендую стійку у дата-центрі «Гігацентр Україна», що має власний сертифікат PCI DSS.

У Додатку Й приведен сертифікат відповідності PCI DSS з посиланням на нього же на офіційному сайті дата-центру.

2.6 Людський фактор та організаційні питання

У стандарті PCI DSS різним організаційним (процесуальним) питанням, у тому числі, дотикаючись до питання (та ризику) людського фактору, присвячено дванадцятий розділ. Та окрім того, наприкінці кожного розділу є окрема вимога, при документування всіх вимог у вигляді політик компанії та дотримання їх організацією.

Вимога 12.1 саме й вимагає створення та підтримання політики інформаційної безпеки. Політика інформаційної безпеки компанії повинна визначати план дій, що реалізують захисні заходи для найбільш цінних ресурсів. Всі працівники повинні знати про критичність даних та свої обов'язки щодо їх захисту.

Вимога 12.4 вимагає гарантій, що політика та процедури безпеки чітко визначають обов'язки щодо забезпечення інформаційної безпеки для всіх працівників. Якщо ролі та обов'язки щодо забезпечення інформаційної безпеки чітко не визначені, то взаємодія між працівниками, які відповідають за безпеку, буде неефективним, що може привести до небезпечного впровадження технологій або використання застарілих або небезпечних технологій.

Щодо нівелювання людського фактору, стандарт PCI DSS у вимозі 12.6 вимагає впровадити офіційну програму підвищення обізнаності працівників з питань безпеки, щоб вони знали політику і процедури захисту ДТК. Також необхідно проводити навчання співробітників інформаційній безпеці відразу від прийому на роботу.

Якщо працівники не знають про свої обов'язки щодо забезпечення інформаційної безпеки, реалізовані захисні заходи і процеси можуть стати неефективними через помилки або навмисних дій.

Якщо програма підвищення обізнаності з питань інформаційної безпеки не передбачає перепідготовку, працівники можуть забути найважливіші процеси та процедури забезпечення безпеки або знехтувати ними, що призведе до уразливості критичних ресурсів та ДТК.

Так само й концепція SWIFT CSCF, вимагае у елементі контролю 7.2 проводити навчання та інформування у сфері інформаційної та комп'ютерної безпеки співробітників.

Окремо, є вимога (12.7), щодо перевірки нових співробітників при прийомі на роботі, відносно їх біографії, судимостей, попередніх місць роботи та іншого. Це необхідно, щоб мінімізувати ризик інсайдерських атак.

Ретельне вивчення біографії потенційних працівників, які мають доступ до ДТК, до їх прийому на роботу, знижує ризик несанкціонованого використання PAN та інших ДТК особами з сумнівним або кримінальним минулим.

Також необхідно впровадити план реагування на інциденти. План реагування на інциденти повинен бути детальним та містити всі ключові елементи, які дозволять організації ефективно реагувати, якщо виникає порушення безпеки, яке піддає ризику ДТК.

Відповідно до плану реагування на інциденти, необхідно також створити групу реагування на інциденти, що зможе працювати у режимі 24/7. Якщо відсутня навчена група швидкого реагування на інциденти, мережі може бути завдано серйозної шкоди, а критичні дані та системи можуть бути

пошкоджені через неналежне поводження з цільовими системами. Це може перешкодити розслідуванню інциденту.

У Додатку Ї приведена Політика інформаційної безпеки ТОВ «Диплом», що повність за своїм складом відповідає вимогам стандарту PCI DSS.

2.7 Регулярне сканування системи, як частина захисту

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

На рисунку 2.7.а зображено таблицю, де відображені різновиди необхідних сканувань та з якою періодичністю необхідно їх проводити:

Вид сканування
Сканування Wi-Fi
Сканування на вразливості
Тест на проникнення
Тест на контроль сегментації

Рисунок 2.7.а

Перший вид сканування (описаний у вимозі 11.1) — 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.

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. Часто тестувальник використовує кілька типів експлойтів разом, щоб обійти кілька рівнів захисту. Наприклад, якщо тестувальник знаходить спосіб отримати доступ до сервера додатків, він використовує скомпрометований сервер як майданчик для нової атаки, де використовує ресурси, доступ до яких має сервер. Таким чином, тестувальник може імітувати методи, якими користуються зловмисники, для виявлення потенційних вразливостей середовища.

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.

Напроти, концепція SWIFT CSCF позначає елемент контролю з тестом на проникнення як бажаний, проте не обов'язковий процес, проте тут знову йде перехлест і вимоги PCI DSS, як більш строгі є у приорітеті.

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 немає.

2.8 Використання сучасних хмарних технологій в системі захисту

З розвитком хмарних технологій, все більше людей довіряються свої дані «хмарам». Вони дешевші, займають менше місця — взагалі не займають для звичайних людей — вони не можуть впасти та зламатися, втративши всі дані, як будь-який жорсткий диск. А навіть якщо це станеться, вся відповідальність буде на сервіс-провайдері хмарної технології (хмарного сховища). Але з урахуванням політики постійного бєк-апу (резервного копіювання)… Шанс втратити дані із хмарного сховища менший, ніж з матеріального носія інформації.

Проте можливість вкрасти інформацію з хмарного сховища більша, ніж з матеріального носія, що схований під матрацом. Тому перед сервіс-провайдерами, що надають послуги хмарного сховища або хмарної інфраструктури, для розміщення власних віртуальних серверів для тих чи інших цілей, дуже гостро постає питання комп’ютерного захисту їх технологій.

За своєю структурою, хмарні технології — це складна структура, побудована на системах та методах віртуалізації. Тонка взаємодія усіх компонентів дозволяє тримати у «хмарі» — віртуальному просторі — терабайти інформації, налаштовувати сервери та реалізовувати складні обчислювальні технології.

Наразі багато компаній переносять свої потужності у хмари відомих сервіс-провайдерв: Amazon AWS, GigaCloud, DigitalOcean, Microsoft Azure, Google Cloud, Alibaba Cloud, IBM Cloud, Oracle та інших. У тому числі і

організації, що зберігають, передають чи оброблюють карткові дані та, відповідно, підпадають під дію стандарту PCI DSS.

На рис. 2.8.а наведен приклад, як на базі хмари Amazon AWS розмістити системи, що містять карткові дані:

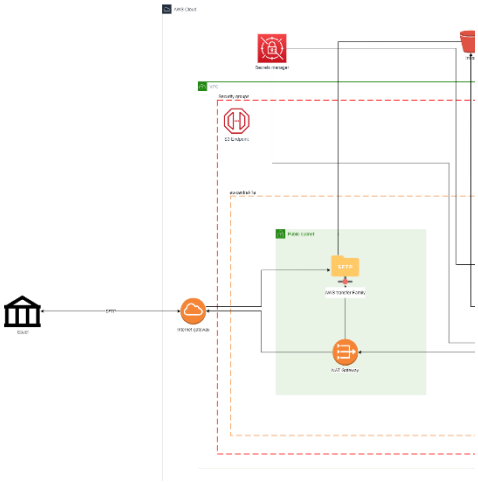


Рисунок 2.8.а

2.9 Аналіз вбудованих служб, сервісів та протоколів в ОС Linux та Windows

Відповідно до вимоги 2.2.2 на серверах з картковими даними дозволяються включати тільки необхідні служби, протоколи, керуючі програми та т.п., що необхідні для функціонування системи.

Як було сказано у вимозі 1.1.6, існує багато протоколів, що можуть бути необхідні для роботи (або включені за замовчуванням) та які зазвичай використовуються зловмисниками для компрометації мережі. Включення цієї вимоги в стандарти конфігурації та пов'язані з ним процеси організації гарантує, що будуть включені тільки необхідні служби та протоколи, що зменшить шанс компрометації конференційної інформації.

Проаналізувавши всі вбудовані служби, сервіси, протоколи, керуючі програми ОС Linux та Windows, побудувала наступну таблицю (таблиця 2.9.а), де зазначені ті служби, сервіси, протоколи та керуючі програми, що

необхідно (доцільно) вимкнути, відповідно до вимоги 2.2.2 стандарту PCI DSS:

Таблиця 2.9.а

Linux/FreeBSD	*anacron*		*apmd*	*autofs*
Windows		*Alerter*		
Опис та обгрунтування відключення	Anacron — асинхронний cron. Завдання з нього запускаються з заданим інтервалом часу, що зручно для систем, що працюють нерегулярно. Проте сервери з картковими даними працюють постійно.	Служба посилає обраним користувачам та комп'ютерам адміністративні сповіщення, що є зайвим на серверах, що обробляють карткові дані.	Демон apmd стежить за настанням заданих подій підсистеми розширеного управління живленням і, при настанні однієї з цих подій, виконує відповідну послідовність команд. Що є зайвим на серверах с картковими даними.	Autofs — це пакет дозволяє автоматично підключати різноманітні ресурси, наприклад переносні пристрої, жорсткі диски при їх використанні і також автоматично їх відключати при припиненні використання. Але до систем з картковими даними заборонене підключення сторонніх пристроїв.

Linux/FreeBSD		*bluetooth*	*btseed*	*chargen-dgram*	*chargen-streamcups*
Windows	*Background Intelligent Transfer Service*	*Bluetooth*			
Опис та обгрунтування відключення	Дана служба дозволяє використовувати для передачі даних резерви мережі по пропускної здатності. Служба використовується для передачі асинхронних даних через http 1.1 сервера. Її використання на серверах з картковими даними є недоцільним.	Bluetooth є незахищеним каналом передачі даних і передавати через нього карткові дані заборонено.	Потрібен для BitTorent, що на серверах з картковими даними точно не використовується.	Дана служба використовується для тестування та відладки TCP/UDP портів. Проте у розрізі серверів з картковими даними, просто відкриває один порт для зловмисника, протирічя основному принципу — тільки необхідні служби.	

Linux/FreeBSD			*cups*	*cpuspeed*
Windows	*ClipBook*	*Computer Browser*		
Опис та обгрунтування відключення	Служба дозволяє переглядати сторінки папок обміну віддалених комп'ютерів. Проте сервери з картковими даними не повині бути підключені до будь-яких інших віддалених пристроїв.	Обслуговує список комп'ютерів в мережі і видає його програмам за запитом. Виклик такого списку на сервері з картковими даними є недоцільним, а отже служба потрібна бути вимкнена.	Система друку CUPS. Так як до серверів з картковими даними не можуть бути підключені принтери, то дану службу необхідно вимкнути.	Цей демон змінює швидкість роботи центрального процесора з метою зниження енергоспоживання. Якщо ЦПУ простоює, можна знизити швидкість, тим самим знижуючи витрати енергії, а для підвищення продуктивності пріхоодітся енергоспоживання збільшувати. Його використання на серверах з картковими даними є недоцільним.

Linux/FreeBSD	*daytime-dgram*	*daytime-stream*	*dm*	*dnsmap*	
Windows					*Extensible Authentication Protocol Service*
Опис та обгрунтування відключення	Даний протокол призначений для тестування і вимірювання в комп'ютерних мережах формату дат. Проте у серверів з картковими даними повине бути підключення до єдиного NTP-серверу, а відображення дати не предумоване взагалі.		Диспетчер дисплея. Якщо не планується використання графічного режиму, то службу необхідно вимкнути.	Запускає кешуючий DNS-сервер. Його активація на серверах з картковими даними є заборонена, тому службу необхідно вимкнути.	Дозволяє клієнтам Windows використовувати службу протоколу EAP. EAP — фреймворк аутентифікації, який часто використовується в бездротових мережах і з'єднаннях точка-точка. EAP використовується для вибору методу аутентифікації, передачі ключів і обробки цих ключів модулями званими методами EAP. Сервери з картковими даними точно не можуть виконувати роль точки доступу, тому на них даний протокол слід вимкнути.

Linux/FreeBSD	*echo-dgram*	*echo-stream*		
Windows			*Fast User Switching Compatibility*	*Fax Service*
Опис та обгрунтування відключення	Протокол був розроблений для тестування та вимірювання часу прийому-передачі в IP-мережах. Що є зайвим на серверах с картковими даними.		Дана служба здійснює управління додатками, які вимагають підтримки в багатокористувацької середовищі. У більшості випадків доступ до серверів з картковими даними має доступ мінімальна кількість людей, для підтримки роботи яких багатокористувацький режим не потрібен.	До серверів з картковими даними не можуть бути підключенні ніякі Fax-пристрої.

Linux/FreeBSD			*finger*	*firstboot*
Windows	*File Services for Macintosh*	*Print Server for Macintosh*		
Опис та обгрунтування відключення	Файлові служби для Macintosh — це додаткова служба в Windows Server 2003, яка дозволяє користувачам Macintosh отримувати доступ до папок та файлів, що зберігаються на Windows Server 2003. Для серверів з картковими даними заборонено вмикати будь-який загальний доступ. Так само Print Server — це додаткова служба в Windows Server 2003, яка дозволяє користувачам Macintosh отримувати доступ до принтерів, що під'єднані до Windows Server 2003.		Функція для перевірки того які користувачі під'єднуються до локальної мережі. Проте для серверів з картковими даними підкоючення чітко регламентовано.	Це помічник початкового налаштування системи після установки. Проте для систем з картковими даними вын не потрібен, що найменш — їх не буде налаштовувати новичок, якомі потрібен помічник. А ось зловмисним може використати дану службу.

Linux/FreeBSD	*ftp*		*gpm*	*haldaemon/haid*	
Windows	*FTP Publishing Service*	*Trivial FTP Daemon*			*Help and Support*
Опис та обгрунтування відключення	FTP — протокол передачі файлів по мережі. Виник ще до HTTP, тому є досить небезпечним за визначенням.		GPM — сервер миші загального призначення. Виконує функцію миші на серверах без графічного інтерфейсу, проте у випадку серверов з картковими даними є надмірністю.	Hald — це демон, який підтримує базу даних пристроїв, підключених до системної системі, в режимі реального часу. Демон підключається до системної шини повідомлень D-Bus, щоб надати API, який додатки можуть використовувати для виявлення, відстеження і виклику операцій на пристроях. Проте до серверів з картковими даними підключення стороніх пристроїв не є бажаним.	Забезпечує можливість роботи центру довідки та підтримки на цьому комп'ютері. На серверах з картковими даними є надмірною та непотрібною.

Linux/FreeBSD	*hidd*	*hddtemp*	*hplip*		*identd*
Windows				*Human Interface Device Access*	
Опис та обгрунтування відключення	Демон HIDD, що забезпечує підтримку пристроїв вводу інформації, що працюють через Bluetooth. Так як використання Bluetooth заборонено на серверах з картковими даними, то й робота даного демону є недоцільна.	Надає інформацію щодо температури жорсткого диску. Його використання на серверах з картковими даними є недоцільним.	Надає драйвера для принтерів HP. Так як друк не використовується на серверах з картковими даними — службу необхідно вимкнути.	Забезпечує універсальний доступ до HID-пристроїв (Human Interface Devices), який активізує і підтримує використання заздалегідь визначених клавіш швидкого виклику на клавіатурі, пристроях управління або інших пристроях мультимедіа. Так як до серверів з картковими даними не можуть бути підключені жодні мультимедійні пристрої, дана служба повина бути відключена.	Він (протокол) забезпечує спосіб ідентифікації користувача для конкретного з'єднання TCP. Його використання на серверах з картковими даними є недоцільним.

Linux/FreeBSD			*inetd*	*isdn*	*kudzu*	
Windows	*IIS Admin Service*	*Indexing Service*				*License Logging Service*
Опис та обгрунтування відключення	Дозволяє адмініструвати веб- та FTP-служби за допомогою оснастки IIS. Використання на серверах з картковими даними є недоцільним.	Індексує вміст і властивості файлів на локальному і віддалених комп'ютерах, забезпечує швидкий доступ до файлів за допомогою гнучкої мови запитів. Проте на серверах з картковими даними є надмірною, крім того — займає багато ресурсів, що може уповільнити роботу сервера.	Демон, що запускає в разі потреби деякі інші мережеві серверні процеси. Його використання на серверах з картковими даними є недоцільним.	Сервіс підтримки ISDN-ліній. Так як зазначені лінії не використовуються на серверах з картковими даними, то його необхідно вимкнути.	Сервіс визначення нових пристроїв. Його використання на серверах з картковими даними є недоцільним.	Це інструмент, який спочатку був розроблений для допомоги клієнтам в управлінні ліцензіями на серверні продукти Microsoft, які ліцензуються за моделлю Server Client Access License (CAL). Її використання на серверах з картковими даними є недоцільним.

Linux/FreeBSD	*lm_sensors*		*mdmonitor*	*mdmpd*	*messagebus*
Windows		*Logical Disk Manager Administrative Service*			
Опис та обгрунтування відключення	Цей демон забезпечує моніторинг температур і напружень на материнській платі. Для роботи системи моніторингу необхідна наявність відповідних датчиків в апаратурі. Доцільність його використання на серверах з картковими даними є спірна.	Виконує налаштування жорстких дисків і томів. Ця служба виконується тільки під час процесів налаштування конфігурації та після цього стає непотрібна та, відповідно, її необхідно відключити.	Mdmonitor запускає, зупиняє і перезапускає mdadm (multipath device monitoring and management) - програмну службу моніторингу та управління RAID. Якщо система не має RAID-пристроїв, то ці демони необхідно зупинити.		"Шина" повідомлень D-BUS, що не потрібна на серверах з картковими даними.

Linux/FreeBSD					*named*
Windows	*Messenger*	*Microsoft POP3 Service*	*MS Software Shadow Copy Provider*	*Volume Shadow Copy*	
Опис та обгрунтування відключення	Дана служба посилає і отримує повідомлення, передані адміністраторами або службою сповіщень. Якщо служба зупинена, сповіщення не буде передано. Ця служба дозволяє обмінюватися повідомленнями між клієнтами і серверами. Дана служба не має відношення до програма Windows Messenger, це WinPopUp. Слід відключити дану службу для того, щоб заборонити net send повідомлення для приховування вашого комп'ютера від мережі Інтернет.	Служба для управління POP3 протоколом. Так як на серверах з картковими даними електрона пошта не використовується — службу необхідно вимкнути.	Управляє тіньовими копіями, отриманими за допомогою тіньового копіювання тому. Якщо використання тіньових копій не є необхідним для вдалої роботи серверу, дану службу необхідно вимкнути.		Це демон, який виконує функції сервера доменних імен (Domain Name Server). Ви повинні його запускати тільки в тому випадку, якщо машина є DNS-сервером для вашої мережі.

Linux/FreeBSD	*nifd*	*netdump*	*netdump-server*	*netfs*		*netplug*	*ifplug*
Windows					*NetMeeting Remote Desktop Sharing*		
Опис та обгрунтування відключення	Цей демон стежить за станом мережних інтерфейсів і посилає повідомлення демонам autoipd і mDNSResponder в тому випадку, якщо змінюється IP-адреса або статус мережевого інтерфейсу. nifd повинен бути запущений на системах, які використовують autoipd і mDNSResponder для автоматичного отримання Link-Local IPv4 адрес і службу Zeroconf. Його використання на серверах з картковими даними є недоцільним.	Завантажує і конфигурирует модуль ядра, який при красі системи посилає повідомлення про це, і дамп оперативної пам'яті на комп'ютер, на якому запущено netdump-сервер. Використовується в разі, коли треба вирішити проблему, використовуючи gdb і образ ядра. Його використання на серверах з картковими даними є недоцільним.		Забезпечує підтримку мережевих файлових систем. Що є заборонені на серверах з картковими даними.	Системна служба загального доступу до робочого столу NetMeeting дозволяє пройшли перевірку користувачам дистанційно керувати робочим столом Windows за допомогою програми Windows NetMeeting з іншого комп'ютера по внутрішній мережі підприємства. Дана служба збільшує вирогідність успішного злому злоумисником, тому її необхідно вимкнути.	Демон управління нестатичними мережевими інтерфейсами. Його використання на серверах з картковими даними є недоцільним.	

Linux/FreeBSD				*nfs*	*nfsd*	*nfslock*	*NTP server*	*ntdp*
Windows	*Network DDE*	*Network DDE DSDM*	*Network News Transport Protocol (NNTP)*					
Опис та обгрунтування відключення	Забезпечує мережевий транспорт і безпеку для динамічного обміну даними (DDE) для програм, що виконуються на одному або на різних комп'ютерах. У випадку з картковими даними є небезпечною, бо їх передача є небажаною.		NNTP — основний протокол, за допомогою якого користувачі можуть підключатися до news-серверів і брати участь у дискусіях. Його використання на серверах з картковими даними є недоцільним.	Демон nfsd здійснює підтримку протоколу мережевих комунікацій nfs, який служить для надання доступу до мережевих ресурсів в TCP/IP-мережах. Його використання на серверах з картковими даними є недоцільним.			Служба синхронізації часу з загальноприйнятими джерелами, що може бути зайвою лазівкою для зловмисника. Краще її відключити, виключення, коли сервер використовується як сервер часу.	

Linux/FreeBSD	*PCMCIA*	*pcscd*		*portmap*		
Windows			*Portable Media Serial Number*		*Print Spooler*	*QoS RSVP*
Опис та обгрунтування відключення	Необхідний виключно для підтримки PCMCIA-карт. Так як сервер з картковими даними не може їх мати — службу необхідно вимкнути.		Отримує серійні номери всіх переносних медіа-пристроїв, підключених до системи. Її використання є недоцільним у більшості випадків взагалі, не кажучи вже про сервери с картковими даними.	Забезпечує маппинг портів. Загалом, на серверах корисний, проте на сервері з картковими даними є недоцільним.	Він керує чергами друку в системі, а також взаємодіє з драйверами принтерів і компонентами введення-виведення, наприклад USB-портами і протоколами сімейства TCP/IP. Так як друк не використовується на серверах з картковими даними — службу необхідно вимкнути.	Дана служба забезпечує контроль трафіку в мережі, використовуючи IPSEC, програми, а також адаптери, що підтримують технологію QoS. Планувальник пакетів QoS автоматично встановлюється для кожного TCP/IP з'єднання. Її використання на серверах з картковими даними є недоцільним.

Linux/FreeBSD	*readahead_early*	*readahead_later*			
Windows			*Remote Access Auto Connection Manager*	*Remote Access Connection Manager*	*Remote Desktop Help Session Manager*
Опис та обгрунтування відключення	Демон readahead забезпечить регулярне пам'ять програм, що використовуються при старті системи, до того, як вони будуть використовуватися, що скорочує час початкового завантаження. Його використання на серверах з картковими даними є недоцільним.		Створює мережеве підключення. Дана служба необхідна при використанні загального доступу до Інтернету. Проте сервери з картковими даними не повини мати вихід на Інтернет.		Управляє можливостями віддаленого помічника. Її використання на серверах з картковими даними є недоцільним.

Linux/FreeBSD						
Windows	*Remote Installation*	*Remote Registry Service*	*Remote Server Monitor*	*Remote Storage Notification*	*Remote Storage Server*	*Removable Storage*
Опис та обгрунтування відключення	Компонент серверних операційних систем компанії Microsoft для віддаленої установки операційних систем за допомогою локальної мережі. Його використання на серверах з картковими даними є недоцільним.	Дозволяє віддаленим користувачам змінювати параметри реєстру на цьому комп'ютері. Її використання на серверах з картковими даними є недоцільним.	Для виконання моніторингу без агента використовується служба Remote Monitoring Server. Її використання на серверах з картковими даними є недоцільним.	Служба використовується для віддаленого зберігання даних. Проте у випадку з картковими даними її використання є недоцільним та в багатьох випадках протиречіть вимогам стандарту PCI DSS.		Дана служба управляє знімними носіями, дисками і бібліотеками. У випадку, коли змінні носії не під'єднуються до серверов з картковими даннми слід її вимикати.

Linux/FreeBSD	*rhnsd*		*rlogin*	*rpcgssd*	*rpcsvcgssd*	*rpcidmapd*	*rsh*	*rwhod*
Windows		*RIP Listener*						
Опис та обгрунтування відключення	Цей демон періодично перевіряє, які операції повинні бути виконані через мережевий інтерфейс Red Hat (Red Hat Network web interface), і запускає їх. Ці операції включають інсталяцію, видалення або оновлення програмного забезпечення, перезавантаження системи, установку конфігураційних файлів і так далі. Його використання на серверах з картковими даними є недоцільним.	Приймає поновлення маршрутів, відправлені маршрутизаторами, які використовують протокол RIPv1. Проте протокол RIPv1 не використовується серверами з картковими даними.	Rlogin встановлює сеанс віддаленої реєстрації з терміналу на віддаленій машині. Його використання на серверах з картковими даними є недоцільним.	Демони rpcgssd і rpcsvcgssd служать для забезпечення безпеки при роботі через RPC. Rpcidmapd перетворює імена користувачів в номери UID і GID. Його використання на серверах з картковими даними є недоцільним.			Віддалений командний інтерпретатор. Його використання на серверах з картковими даними є недоцільним.	Сервер підтримки бази даних програм rwho і ruptime. Його використання на серверах з картковими даними є недоцільним.

Linux/FreeBSD	*SCTP*	*sendmail*	*postfix*	*setroubleshoot*	*smartd*		*smb (SAMBA)*
Windows					*Smart Card*	*Smart Card Helper*	
Опис та обгрунтування відключення	SCTP — один з протоколів транспортного рівня, як UDP та TCP. При використанні двух зазначених вище протоколів використання SCTP є невиправденим, бо підвищує можливості зловмиснику проникнути у мережу.	Необхіден для реалізації власного сервера відправки повідомлення. Так як дві ролі на сервері заборонено, дану службу необхідно вимкнути.		Це демон дозволу проблем SELinux. Setroubleshooter забезпечує в реальному часі зворотний зв'язок з користувачами при відмовах SELinux AVC (Access Vector Cache). Його використання на серверах з картковими даними є недоцільним.	Дана служба управляє доступом до пристроїв читання смарт-карт. Проте крім випадків, коли доступ до сервера з картковими даними вимагає смарт-карту її використання є недоцільним.		Демон, що забезпечує роботу по протоколу smb, що надає доступ до відритим ресурсів комп'ютера для комп'ютерів, що працюють під ОС Windows. Його використання на серверах з картковими даними є недоцільним.

Linux/FreeBSD		*snmp*		*spamassassin*		
Windows	*Simple Mail Transfer Protocol (SMTP)*	*SNMP Trap Service*	*SNMP Service*		*SSDP Discovery Service*	*Task Scheduler*
Опис та обгрунтування відключення	Передає по мережі повідомлення електронної пошти. Так як будь-яка передача карткових даних через електрону пошту заборонено — дану службу необхідно вимкнути.	Приймає повідомлення перехоплення, створені локальними або віддаленими агентами SNMP і пересилає їх програмами управління SNMP, запущеними на цьому комп'ютері. У загальному, якщо іншого не вимагає встановлений антивірус — службу краще відключити.	Включає агентів, які виробляють спостереження за роботою мережевих пристроїв і виводить результати на робочу станцію мережевої консолі. Проте до серверів з картковими даними неповині бути підключенні мережеві пристрої.	Цей демон використовує програму Apache SpamAssassin для перевірки пошти на наявність спаму. Він зазвичай запускається спільно з сервером доставки пошти (a mail deleivery agent (MDA) server). Його використання на серверах з картковими даними є недоцільним.	Дана служба включає виявлення UPnP-пристроїв в домашній мережі. Проте сервери з картковими даним и не можуть бути розміщені ні в якій домашній мережі.	Дозволяє виконувати програми в призначений час. У більшості випадків її використання є недоцільним або невиправданим на серверах з картковими даними. Тому її необхідно вимкнути.

Linux/FreeBSD			*telnet*		*tcpmux-server*	
Windows	*TCP/IP NetBIOS Helper Service)*	*Telephony*	*Telnet*	*Themes*		*Universal Plug and Play Device Host*
Опис та обгрунтування відключення	Включає підтримку служби NetBIOS через TCP/IP (NetBT) і дозволу NetBIOS-імен в адреси. Дана служба необхідна для нормальної підтримки NetBIOS через TCP/IP. Якщо мережа не використовує NetBIOS або WINS, то необхідно вимкнути цю службу.	Забезпечує підтримку Telephony API (TAPI) для програм, які керують телефонним обладнанням і голосовими IP-підключеннями на цьому комп'ютері, а також через ЛВС - на серверах, де запущена відповідна служба. З серверів, що містять карткові дані керування телефоним обладнанням є неможливим (забороненим), отже службу необхідно вимкнути.	Telnet визнан небезпечним протоколом, тому його використання для карткових даних заборонено.	Дана служба дозволяє управляти темами оформлення. Її використання на серверах з картковими даними є недоцільним.	Мережевий протокол для зв'язку безлічі служб через один порт. Його використання на серверах з картковими даними є недоцільним.	Дана служба забезпечує підтримку універсальних PnP-пристроїв вузла. Її використання на серверах з картковими даними є недоцільним, якщо PnP-пристрої вузла не використовуються.

Linux/FreeBSD					
Windows	*Wired AutoConfig*	*Wireless Configuration*	*WMI Performance Adapter*	*Windows Image Acquisition (WIA)*	*Windows Management Instrumentation Driver Extension*
Опис та обгрунтування відключення	Дана служба виконує перевірку автентичності IEEE 802.1X для інтерфейсів Ethernet. Якщо підключення Ethernet не планується — краще відключити.	Надає автоматичне налаштування 802.11 адаптерів. Для збільшення рівня захисту від впливу несанкціонованих точок доступу, дану службу краще вимкнути.	Надає інформацію про бібліотеки продуктивності від постачальників WMI HiPerf. Якщо WMI HiPerf не використовується — необхідно вимкнути.	Забезпечує служби отримання зображень зі сканерів і цифрових камер. Проте до серверів з картковими даними не можуть бути під'єднанні ніякі сканери.	Забезпечує обмін керуючою інформацією з пристроями. Так як до серверів з картковими даними підключення сторонніх пристроїв заборонено — використання даної служби є недоцільним.

Linux/FreeBSD			*vsftpd*	*xfs*	*yppasswdd*	*ypserv*	*ypxfrd*
Windows	*Windows Media Server*	*World Wide Web Publishing Services*					
Опис та обгрунтування відключення	Unicast-протокол мультімедіамовлені корпорації Microsoft, який використовується в Microsoft Media Services (раніше називався NetShow Services). Проте у 2003-му році вийшов новий, оновлений протокол, тому даний слід вимкнути.	Забезпечує зв'язок і адміністрування веб-вузла за допомогою оснащення IIS. Її використання на серверах з картковими даними є недоцільним.	Vsftpd — це програма, яка створює легкий, захищений FTP-сервер. Проте при правилі один сервер — одна роль, її використання на серверах з картковими даними заборонене.	Це сервер шрифтів (font server). Цей демон завантажує шрифти в пам'ять для того, щоб графічні додатки працювали швидше, ніж в тому випадку, коли вони змушені завантажувати шрифти з жорсткого диска. Його використання на серверах з картковими даними є недоцільним.	Служба, що дозволяє користувачам змінювати свої паролі в NIS. Її використання на серверах з картковими даними є недоцільним.	Демон NIS сервера. Його використання на серверах з картковими даними є недоцільним.	Служба, що відповідає за передачу карти NIS по мережі. Її використання на серверах з картковими даними є недоцільним.

2.10 Висновки до другого розділу

Згідно всіх наведених доказів, прикладів та обгрунтувань, ТОВ «Диплом» має виправити лише дві невідповідності та може вважатися PCI DSS та SWIFT compliance.

ТОВ «Диплом» має сегментовану мережу, у якій всі карткові дані виділені у окремий сегмен, що відділяється від основної мережі двома комутаторами та маршрутизатором, з ввімкненим та налаштованим відповідно вимог стандарту міжмережевим екраном.

ТОВ «Диплом» завчастно заблокував всі вбудованні облікові данні (логіни та паролі), а ті, блокування яких неможливе (root на серверах з Unix-

подібною мережею), були забороненні для використання політикою організації щодо користування обліковими засобами та захищенні паролем на 15-ть символів з урахуванням усіх вимог парольної політики.

ТОВ «Диплом» використовує у себе CloudFlare у якості IDS/IPS, OSSEC як додатковий рівень контроль та спостереження, Wazuh як FIM, а Syslog для збору усіх логів з мережевого обладнання та серверів. Також організація сконфігорувала перенаправлення усіх даних з OSSEC та Syslog на Wazuh, для реалізації кращого рівня контролю за системами та більш швидкої реакції при виявленні якогось інциденту.

ТОВ «Диплом» орендує стійку для свого мережевого обладнання у ТОВ «Гигацентр Україна», що є сертифікаваним PCI DSS, та за умовами договору забов'язаний дотримуватися політики інформаційної безпеки організації ТОВ «Диплом» та вимогам PCI DSS.

ТОВ «Диплом» розробив та строго дотримується політик інформаційної безпеки, що серед іншого передбачають строге виконання вимог PCI DSS та SWIFT.

ТОВ «Диплом» регулярно проводить сканування своїх систем на вразливості, а також тести на проникнення та для контролю сегментації.

Загалом, кажучи про розробки систем захисту карткових даних згідно стандартів PCI DSS та SWIFT, краще (та дешевше) від початку впроваджувати системи та мережі таким чином, щоб вони відповідали вимогам стандарту. Бо, окрім іншого, це значно підвищує загальну безпеку організації.

ВИСНОВКИ

У сферах, що стикаються з картковими даними основними стандартами кібербезпеки є стандарт PCI DSS та концепція SWIFT CSCF.

При умові побудови системи з урахуванням вимог стандартів PCI DSS та SWIFT 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 та SWIFT, 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).
- Концепція SWIFT строго вимагає (з технічної частини) лише дотримання одного з типів запропонованих у стандарті архітектур та регламентує порядок використання обладнанням (або ПЗ), що є виробленим та наданим SWIFT.
- Стандарт PCI DSS більш всеосяжний та детальний, він зачіпає більше тем (та більш детально), ніж концепція SWIFT.

Хоча напряму стандарти PCI DSS та SWIFT не мають звя'зків один з одним або з будь-яким іншим міжнародним стандартом комп'ютерного та інформаційного захисту, всі вони за суттю доповнюють один одним. Стандарт SWIFT, застосований тільки тоді, коли у організації є SWIFT-перекази, а це вже за визначенням — фінансові установи. Що в свою чергу вже обов'язково підпадають під дію стандарту PCI DSS.

Крім того, у самих стандартах є посилання на «загальногалузеві стандарти», якими визнаються інші стандарти кібербезпеки, задля більш всебічного огляду проблем та процесів (елементів) захисту.

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

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

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

3. «Що потрібно знати про відповідність стандартам PCI DSS: Витрати та контрольний список у Великобританії» // [Електронний ресурс] – Режим доступу: https://storekit.com/payments/pci-dss/

4. Морз Едуард. Равал Васант. «Приватне замовлення з точки зору закону: досягнення захисту споживачів за допомогою заходів безпеки платіжних карток». DePaul Business & Commercial Law Journal 10, №. 2 (зима 2012)» // [Електронний ресурс] – Режим доступу: https://heinonline.org/HOL/P?h=hein.journals/depbcl10&i=217

5. Рада зі стандартів безпеки PCI. «Стандартні вимоги до безпеки платежних карток (PCI) та процедури оцінки безпеки, версія 3.2.1, травень 2018 р.» // [Електронний ресурс] – Режим доступу: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

6. Рада зі стандартів безпеки PCI. «Огляд змінень в версії PCI DSS 2.0 у порівнянні із версією 1.2.1» // [Електронний ресурс] – Режим доступу: https://ru.pcisecuritystandards.org/_onelink_/pcisecurity/en2ru/minisite/en/docs/PCI_DSS_v2.pdf

7. Рада зі стандартів безпеки PCI. «Звіт про відповідність» // [Електронний ресурс] – Режим доступу: https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-ROC-Reporting-Template.pdf?agreement=true&time=1622589390418

8. Рада зі стандартів безпеки PCI. «Словник термінів, скорочень та акронімів» // [Електронний ресурс] – Режим доступу: https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf

9. Рада зі стандартів безпеки PCI. «Керівництво з PCI DSS та сегментації мережі» // [Електронний ресурс] – Режим доступу: https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf

10. Скотт Сьюзен. «Суспільство всесвітнього міжбанківського фінансового телекомунікаційного зв'язку (SWIFT): Кооперативне управління для мережевих інновацій, стандартів та спільноти»–. ISBN 978-1-317-90953-8 // [Електронний ресурс] – Режим доступу: https://books.google.com/books?id=eTnjAQAAQBAJ&pg=PA16

11. Морган Брайан «Всього на сьогоднішній день: Еволюція додавальної машини: Історія Берроуза». Burroughs Adding Machine Limited. Лондон // [Електронний ресурс] – Режим доступу: https://history-computer.com/burroughs-adding-machine-history-of-the-burroughs-adding-machine/

12. Дворак Джон. "IBM і сім гномів — Гном Перший: Берроузи". // [Електронний ресурс] – Режим доступу: http://www.dvorak.org/blog/ibm-and-the-seven-dwarfs-dwarf-one-burroughs/

13. Мартин Арнольд «Ripple та Swift розбиття на транскордонні платежі». Financial Times. // [Електронний ресурс] – Режим доступу: https://www.ft.com/content/631af8cc-47cc-11e8-8c77-ff51caedcde6

14. «SWIFT Framework управління безпекою клієнтів v2021» // [Електронний ресурс] – Режим доступу: https://www.swift.com/ru/node/300801

15. Офіційна документація з Computer Security Resource Center. «Вказівки щодо вибору, конфігурації та використання реалізації захисту транспортного рівня (TLS)» // [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

16. Офіційна документація OWASP Cheat Sheet Series «Шпаргалка з захисту транспортного рівня» // [Електронний ресурс] – Режим доступу: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html

17. Офіційна документація зі стандартів NIST. «Документація фреймворку» // [Електронний ресурс] – Режим доступу: https://www.nist.gov/cyberframework/framework

18. Офіційний сайт PricewaterhouseCoopers. «Чому вам слід прийняти систему кібербезпеки NIST». // [Електронний ресурс] – Режим доступу: http://www.pwc.com/us/en/increasing-it-effectiveness/publications/adopt-the-nist.html

19. Кєллєр Ніколь. "Проект фреймворку кібербезпеки, версія 1.1". // [Електронний ресурс] – Режим доступу: https://www.nist.gov/cyberframework/draft-version-11

20. Офіційна документація зі стандартів NIST. // [Електронний ресурс] – Режим доступу: https://www.nist.gov/cyberframework

21. Офіційна документація зі стандарту ISO/IEC 27001 «International Information Security Standard published». // [Електронний ресурс] – Режим доступу: https://www.bsigroup.com

22. Бьорд Кетті. " НОВА ВЕРСІЯ ISO/ IEC 27001 для кращого вирішення ризиків безпеки ". // [Електронний ресурс] – Режим доступу: https://iso.org

23. Офіційна документація зі стандарту ISO/IEC 27001:2013. // [Електронний ресурс] – Режим доступу: https://www.iso.org/standard/54534.html

24. BSI Group "BS EN ISO/IEC 27001: 2017 - що змінилося?". // [Електронний ресурс] – Режим доступу: www.bsigroup.com..

25. Феррейра, Ліндемберг Наффа; да Сільва Константе, « Процес сертифікації електронних рахунків-фактур у штаті Мінас-Жерайс за стандартом ISO 27001». – 47-а Міжнародна конференція Карнахан з технологій безпеки (ICCST). Медельїн: IEEE: 1–4. doi: 10.1109 / CCST.2013.6922072. ISBN 978-1-4799-0889-9.

26. Ст.30 «РЕГЛАМЕНТ (ЄС) 2016/679 ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ ТА РАДИ» // [Електронний ресурс] – Режим доступуhttp://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3265-1-1

27. Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 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

28. 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/Hunton-Guide-to-the-EU-General-Data-Protection-Regulation.pdf

29. Європейський парламент. «Законодавча резолюція Європейського Парламенту від 12 березня 2014 року щодо пропозиції регламенту Європейського Парламенту та Ради про захист фізичних осіб при обробці персональних даних та про вільне переміщення таких даних (Загальний регламент про захист даних)» // [Електронний ресурс] – Режим доступу: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN

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

31. 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

32. Журнал «Security Boulevard». «CISA зазначає, що хакери не лише використовували SolarWinds для проникнення» // [Електронний ресурс] – Режим доступу: https://securityboulevard.com/2021/01/hackers-didnt-only-use-solarwinds-says-cisa/

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

34. Коментар компанії SolarWinds щодо проникнення до ПЗ «Оріон» // [Електронний ресурс] – Режим доступу: https://habr.com/ru/news/t/533220/

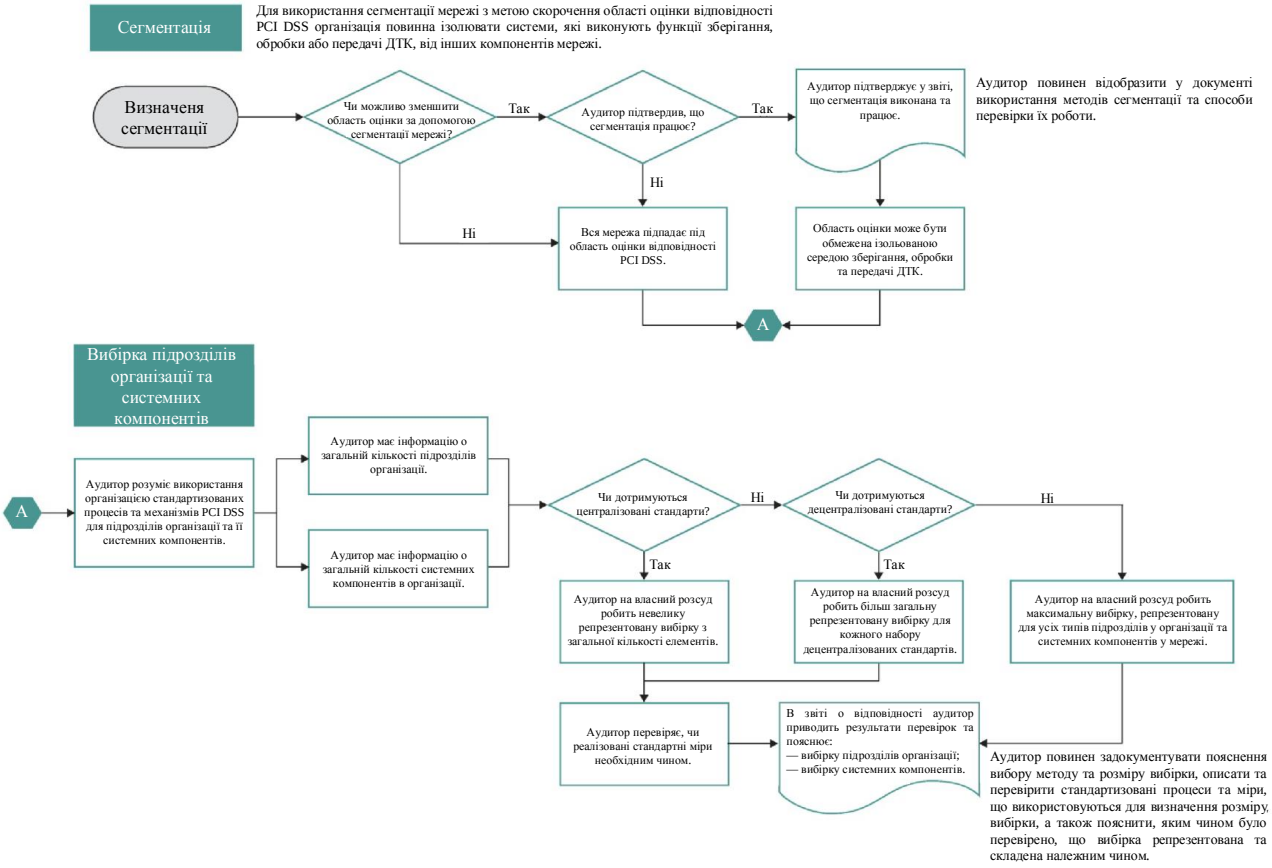
35. Cisco Systems, Inc. «Програма мережевої академії Cisco CCNA 3 та 4. Допоміжне керівництво» ISBN 1-58713-113-7.

36. 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/D-mining/Anomaly-D/Intrusion-detection/taxonomy.pdf

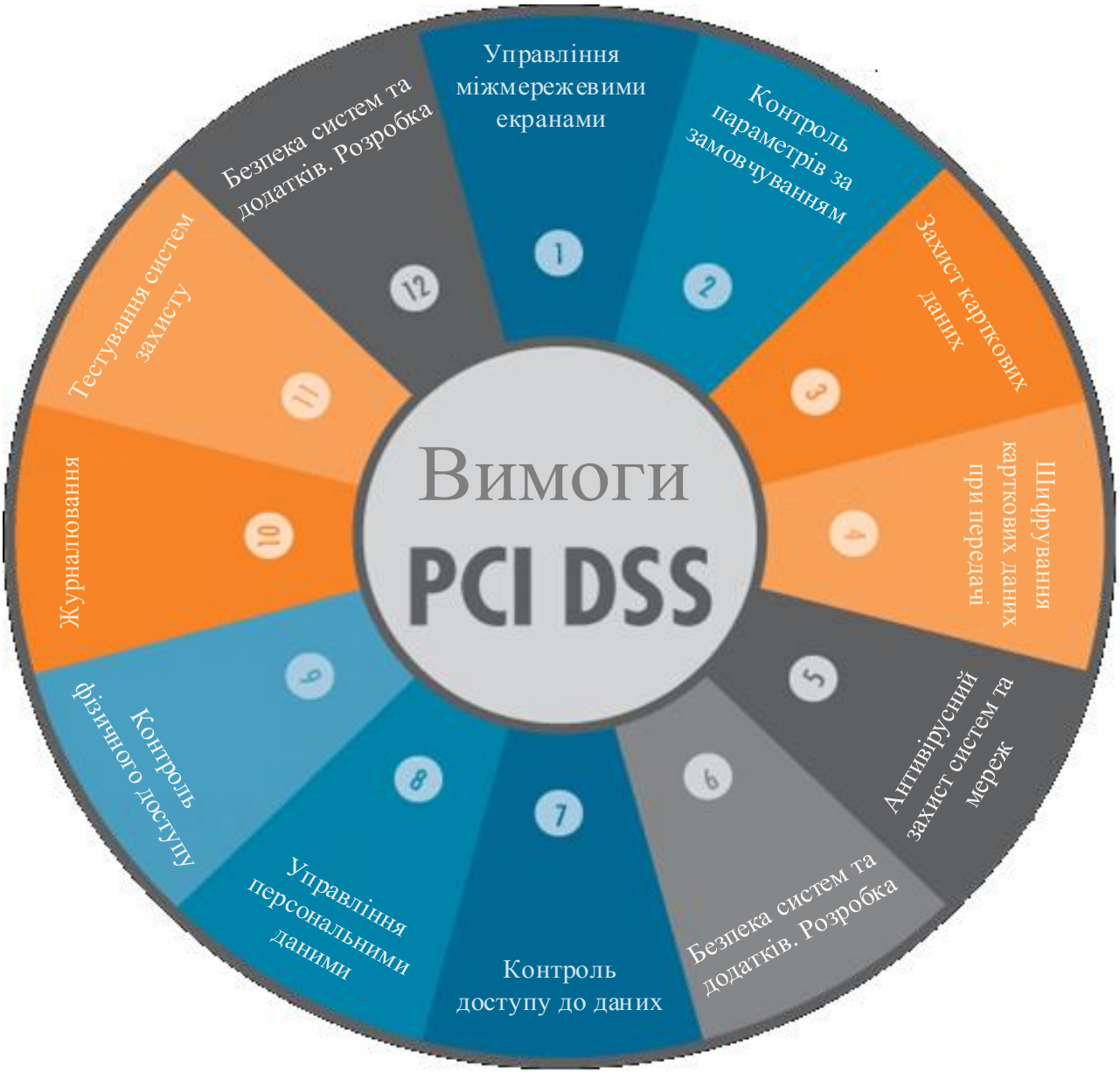
37. Ньюман Роберт «Комп’ютерна безпека: захист цифрових ресурсів». ISBN 978-0-7637-5994-0

38. Моссен Мухамед; Рейман Хабіб «Медоноски та маршрутизатори: Збір атак через Інтернет.» CRC Press. ISBN 978-1-4987-0220-1

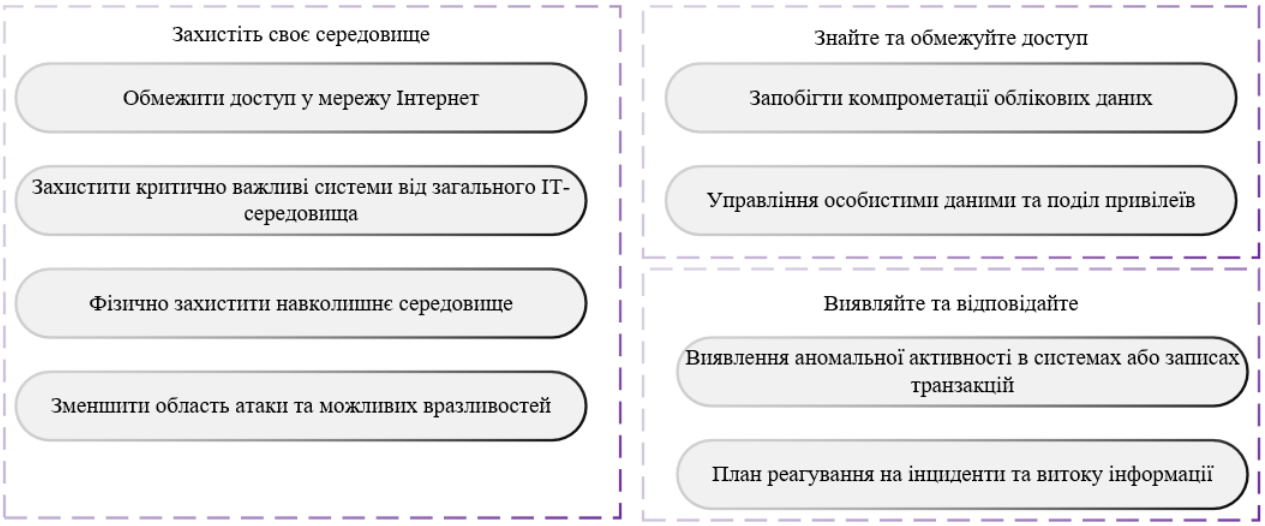
Додаток А


Сегментація
Для використання сегментації мережі з метою скорочення області оцінки відповідності PCI DSS організація повинна ізолювати системи, які виконують функції зберігання, обробки або передачі ДТК, від інших компонентів мережі.
Визначення сегментації
Чи можливо зменшити область оцінки за допомогою сегментації мережі?
Так
Аудитор підтвердив, що сегментація працює?
Так
Аудитор підтверджує у звіті, що сегментація виконана та працює.
Аудитор повинен відобразити у документі використання методів сегментації та способи перевірки їх роботи.
Ні
Ні
Вся мережа підпадає під область оцінки відповідності PCI DSS.
Область оцінки може бути обмежена ізольованою середою зберігання, обробки та передачі ДТК.
A
Вибірка підрозділів організації та системних компонентів
A
Аудитор розуміє використання організацією стандартизованих процесів та механізмів PCI DSS для підрозділів організації та її системних компонентів.
Аудитор має інформацію о загальній кількості підрозділів організації.
Аудитор має інформацію о загальній кількості системних компонентів в організації.
Чи дотримуються централізовані стандарти?
Ні
Чи дотримуються децентралізовані стандарти?
Ні
Так
Так
Аудитор на власний розсуд робить невелику репрезентовану вибірку з загальної кількості елементів.
Аудитор на власний розсуд робить більш загальну репрезентовану вибірку для кожного набору децентралізованих стандартів.
Аудитор на власний розсуд робить максимальну вибірку, репрезентовану для усіх типів підрозділів у організації та системних компонентів у мережі.
Аудитор перевіряє, чи реалізовані стандартні міри необхідним чином.
В звіті о відповідності аудитор приводить результати перевірок та пояснює:
— вибірку підрозділів організації;
— вибірку системних компонентів.
Аудитор повинен задокументувати пояснення вибору методу та розміру вибірки, описати та перевірити стандартизовані процеси та міри, що використовуються для визначення розміру вибірки, а також пояснити, яким чином було перевірено, що вибірка репрезентована та складена належним чином.

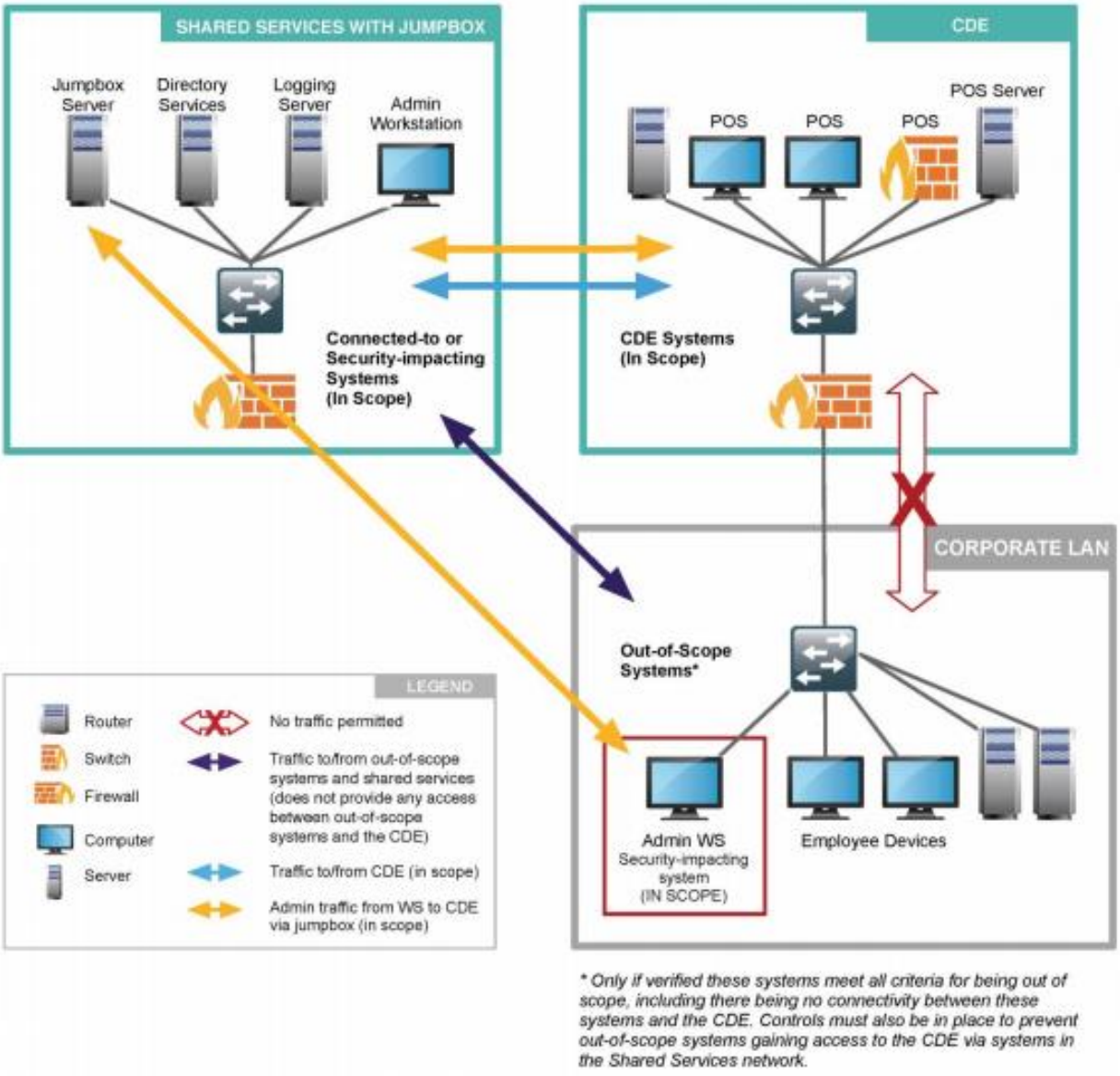
Додаток Б


Вимоги
PCI DSS
1
Управління міжмережевими екранами
2
Контроль параметрів за замовчуванням
3
Захист карткових даних
4
Шифрування карткових даних при передачі
5
Антивірусний захист систем та мереж
6
Безпека систем та додатків. Розробка
7
Контроль доступу до даних
8
Управління персональними даними
9
Контроль фізичного доступу
10
Журналювання
11
Тестування систем захисту
12
Безпека систем та додатків. Розробка

Додаток В

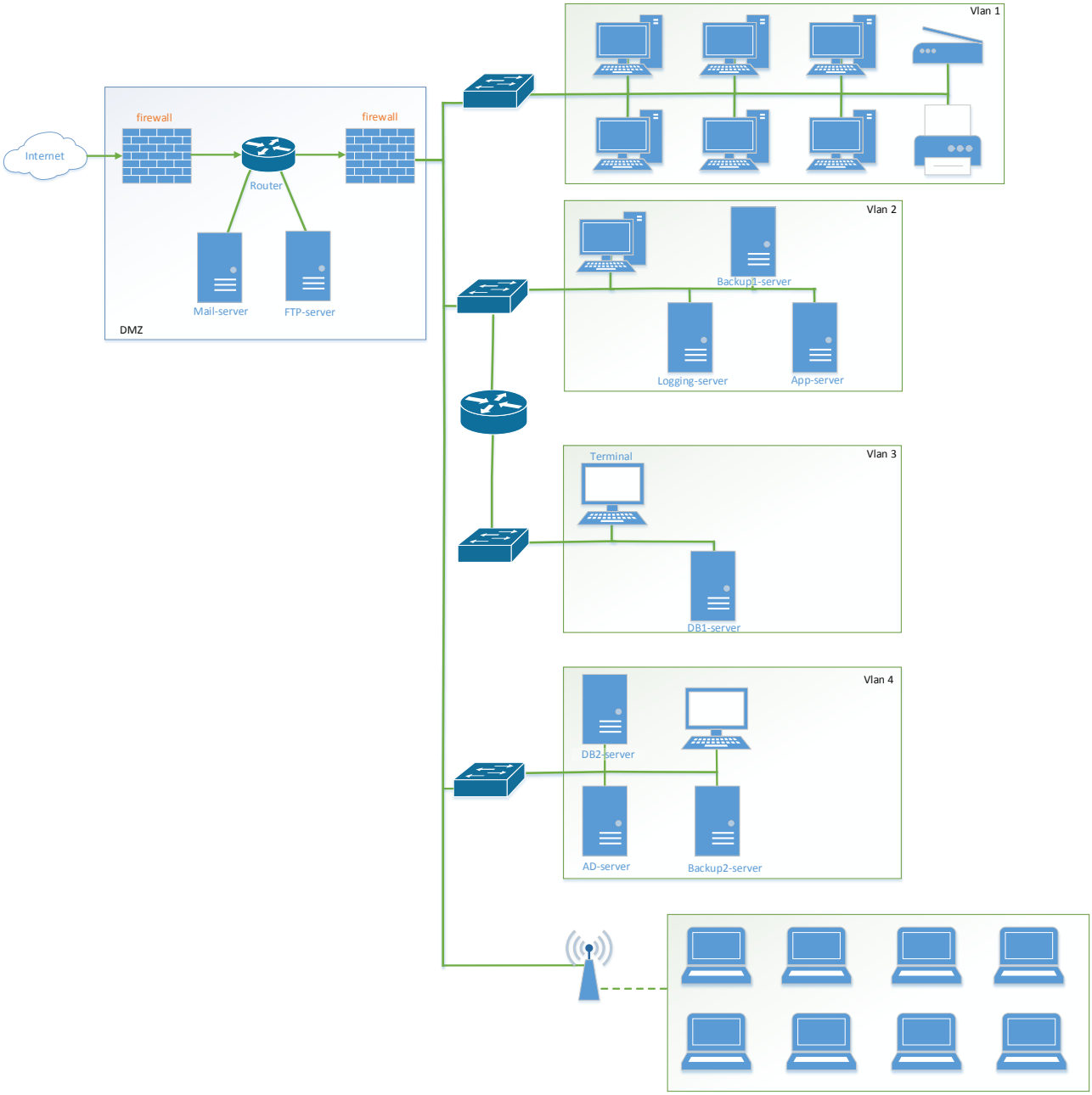

Захистіть своє середовище
Обмежити доступ у мережу Інтернет
Захистити критично важливі системи від загального IT-середовища
Фізично захистити навколишнє середовище
Зменшити область атаки та можливих вразливостей
Знайте та обмежуйте доступ
Запобігти компрометації облікових даних
Управління особистими даними та поділ привілеїв
Виявляйте та відповідайте
Виявлення аномальної активності в системах або записах транзакцій
План реагування на інциденти та витоку інформації

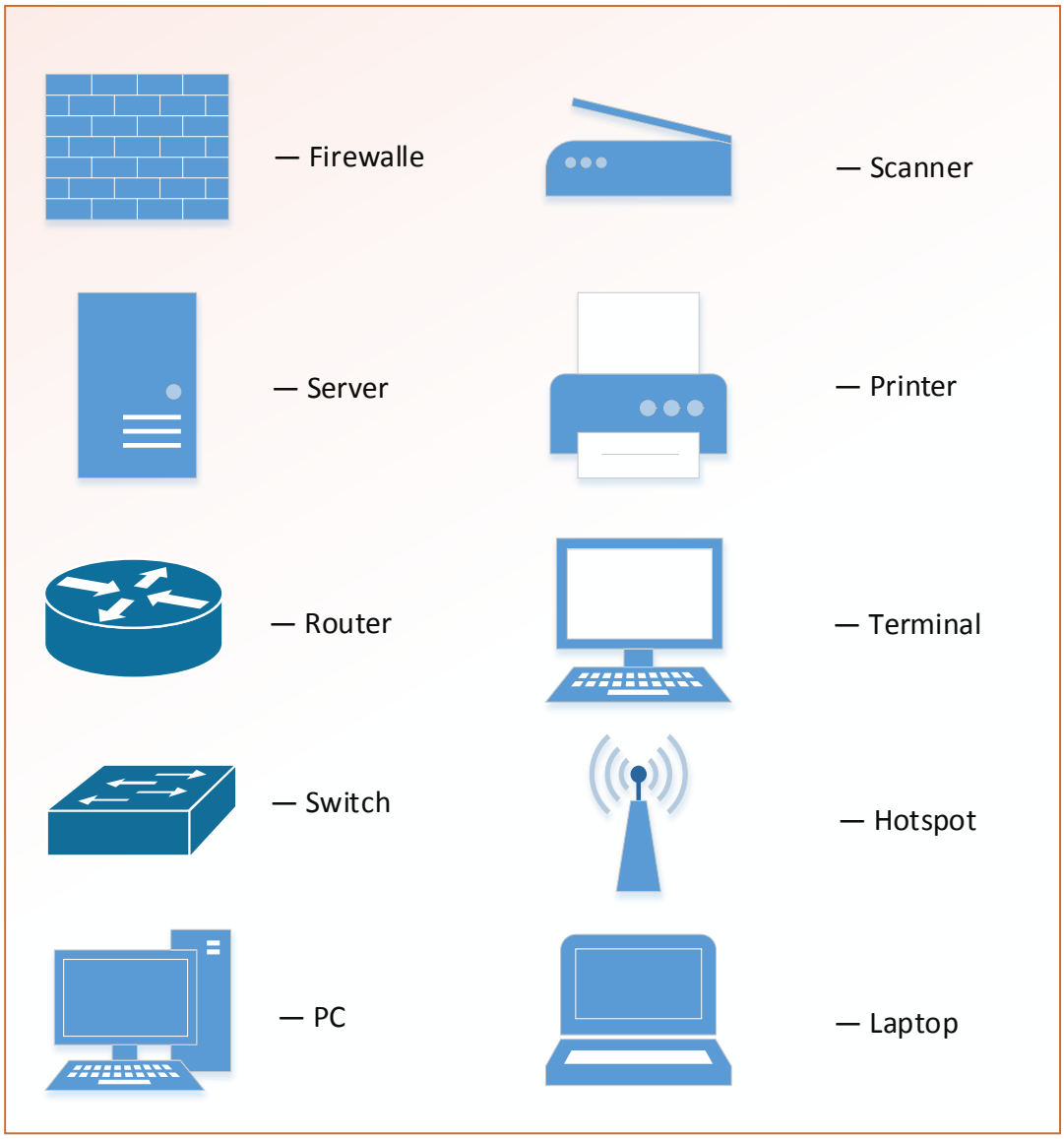
Додаток Г



** 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


Vlan 1
firewall
firewall
Internet
Router
Mail-server
FTP-server
DMZ
Vlan 2
Backup1-server
Logging-server
App-server
Terminal
Vlan 3
DB1-server
Vlan 4
DB2-server
AD-server
Backup2-server


— Firewalle
— Scanner
— Server
— Printer
— Router
— Terminal
— Switch
— Hotspot
— PC
— Laptop

Додаток Д

8.3 Network segmentation

▪ Identify whether the assessed entity has used network segmentation to reduce the scope of the assessment. **(yes/no)** ***Note*** *– An environment with no segmentation is considered a "flat" network where all systems are considered in scope due to a lack of segmentation.*	Yes
▪ ***If segmentation is not used:*** Provide the name of the assessor who attests that the whole network has been included in the scope of the assessment.	N/A
▪ ***If segmentation is used:*** Briefly describe how the segmentation is implemented.	Network segmentation is achieved by configuring internal network firewalls (iptables).
– Identify the technologies used and any supporting processes	Firewalls iptables
– Explain how the assessor validated the effectiveness of the segmentation, as follows:	
– Describe the methods used to validate the effectiveness of the segmentation (for example, observed configurations of implemented technologies, tools used, network traffic analysis, etc.).	The survey was conducted, the firewall configuration was verified, and the penetration test report was revised and analyzed.
– Describe how it was verified that the segmentation is functioning as intended ***Note*** *– the response must go beyond listing the activities that the assessor performed and must provide specific details regarding how segmentation is functioning as intended.*	A survey of the responsible personnel was carried out, a verified procedure for the administrator's login to the network (it was confirmed that the login was possible only after passing the authentication with two factors: an SSH certificate with a personal password set on it, which is necessary for access). We checked the configuration of firewalls, studied the rules of access and filtering traffic installed on them. The penetration test report was also revised and analyzed to confirm the success of the segmentation using the nmap command from outside and from within the system.
– Identify the security controls that are in place to ensure the integrity of the segmentation mechanisms (e.g., access controls, change management, logging, monitoring, etc.).	The company uses explicit access controls, log monitoring, IDS and FIM to identify any anomalies or threats that violate segmentation rules.
– Describe how it was verified that the identified security controls are in place ***Note*** *– the response must go beyond listing the activities that the assessor performed and must provide specific details of what the assessor observed to get the level of assurance that the identified security controls are in place.*	A survey of the responsible personnel was carried out. The IDS and FIM settings were checked (whose work was further verified by attempts to deliberately break segmentation). The access logs were checked, during which the auditor made sure that all access attempts were recorded. The Penetration Testing Report was also revised and reviewed, which indicated a failed attempt to access the segmented network.
▪ Provide the name of the assessor who attests that the segmentation was verified to be adequate to reduce the scope of the assessment AND that the technologies/processes used to implement segmentation were included in the PCI DSS assessment.	Anastasiia Karmazina

Додаток Е

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate
RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
INPUT_direct  all  --  anywhere             anywhere
INPUT_ZONES_SOURCE  all  --  anywhere             anywhere
INPUT_ZONES  all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere             ctstate INVALID
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-
prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate
RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
FORWARD_direct  all  --  anywhere             anywhere
FORWARD_IN_ZONES_SOURCE  all  --  anywhere             anywhere
FORWARD_IN_ZONES  all  --  anywhere             anywhere
FORWARD_OUT_ZONES_SOURCE  all  --  anywhere             anywhere
FORWARD_OUT_ZONES  all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere             ctstate INVALID
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-
prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
OUTPUT_direct  all  --  anywhere             anywhere

Chain FORWARD_IN_ZONES (1 references)
target     prot opt source               destination
FWDI_trusted  all  --  anywhere             anywhere             [goto]
FWDI_drop  all  --  anywhere             anywhere             [goto]

Chain FORWARD_IN_ZONES_SOURCE (1 references)
target     prot opt source               destination

Chain FORWARD_OUT_ZONES (1 references)
```

```
target     prot opt source               destination
FWDO_trusted  all  --  anywhere             anywhere             [goto]
FWDO_drop  all  --  anywhere             anywhere             [goto]

Chain FORWARD_OUT_ZONES_SOURCE (1 references)
target     prot opt source               destination

Chain FORWARD_direct (1 references)
target     prot opt source               destination

Chain FWDI_drop (1 references)
target     prot opt source               destination
FWDI_drop_log  all  --  anywhere             anywhere
FWDI_drop_deny  all  --  anywhere             anywhere
FWDI_drop_allow  all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere

Chain FWDI_drop_allow (1 references)
target     prot opt source               destination

Chain FWDI_drop_deny (1 references)
target     prot opt source               destination

Chain FWDI_drop_log (1 references)
target     prot opt source               destination

Chain FWDI_trusted (1 references)
target     prot opt source               destination
FWDI_trusted_log  all  --  anywhere             anywhere
FWDI_trusted_deny  all  --  anywhere             anywhere
FWDI_trusted_allow  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain FWDI_trusted_allow (1 references)
target     prot opt source               destination

Chain FWDI_trusted_deny (1 references)
target     prot opt source               destination
REJECT     icmp --  anywhere             anywhere             icmp timestamp-reply
reject-with icmp-host-prohibited
```

```
REJECT     icmp --  anywhere             anywhere             icmp timestamp-request
reject-with icmp-host-prohibited

Chain FWDI_trusted_log (1 references)
target     prot opt source               destination

Chain FWDO_drop (1 references)
target     prot opt source               destination
FWDO_drop_log  all  --  anywhere             anywhere
FWDO_drop_deny  all  --  anywhere             anywhere
FWDO_drop_allow  all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere

Chain FWDO_drop_allow (1 references)
target     prot opt source               destination

Chain FWDO_drop_deny (1 references)
target     prot opt source               destination

Chain FWDO_drop_log (1 references)
target     prot opt source               destination

Chain FWDO_trusted (1 references)
target     prot opt source               destination
FWDO_trusted_log  all  --  anywhere             anywhere
FWDO_trusted_deny  all  --  anywhere             anywhere
FWDO_trusted_allow  all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain FWDO_trusted_allow (1 references)
target     prot opt source               destination

Chain FWDO_trusted_deny (1 references)
target     prot opt source               destination

Chain FWDO_trusted_log (1 references)
target     prot opt source               destination

Chain INPUT_ZONES (1 references)
target     prot opt source               destination
IN_trusted  all  --  anywhere             anywhere             [goto]
```

```
IN_drop    all  --  anywhere            anywhere            [goto]

Chain INPUT_ZONES_SOURCE (1 references)
target     prot opt source               destination

Chain INPUT_direct (1 references)
target     prot opt source               destination
ACCEPT     icmp --  195.210.46.137       anywhere
ACCEPT     icmp --  195.210.46.137       anywhere

Chain IN_drop (1 references)
target     prot opt source               destination
IN_drop_log  all  --  anywhere             anywhere
IN_drop_deny  all  --  anywhere            anywhere
IN_drop_allow  all  --  anywhere           anywhere
DROP       all  --  anywhere             anywhere

Chain IN_drop_allow (1 references)
target     prot opt source               destination
ACCEPT     tcp  --  195.210.46.137       anywhere            tcp dpt:zabbix-agent
ctstate NEW,UNTRACKED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh ctstate
NEW,UNTRACKED

Chain IN_drop_deny (1 references)
target     prot opt source               destination

Chain IN_drop_log (1 references)
target     prot opt source               destination

Chain IN_trusted (1 references)
target     prot opt source               destination
IN_trusted_log  all  --  anywhere           anywhere
IN_trusted_deny  all  --  anywhere          anywhere
IN_trusted_allow  all  --  anywhere         anywhere
ACCEPT     all  --  anywhere             anywhere

Chain IN_trusted_allow (1 references)
target     prot opt source               destination

Chain IN_trusted_deny (1 references)
```

```
target     prot opt source               destination
REJECT     icmp --  anywhere             anywhere             icmp timestamp-reply
reject-with icmp-host-prohibited
REJECT     icmp --  anywhere             anywhere             icmp timestamp-request
reject-with icmp-host-prohibited

Chain IN_trusted_log (1 references)
target     prot opt source               destination

Chain OUTPUT_direct (1 references)
target     prot opt source               destination
```

Додаток Є

Мережеве обладнання

Умовне скорочення	IP-адреса	Призначення	Відповідальна особа	Виробник	Модель	Версія ОС/мікрокоду
R-001	192.168.0.10	router	Головний інженер Іванов І.І.	Cisco	ISR 4331	ISO XE 16.10
R-002	192.168.2.10	router	Головний інженер Іванов І.І.	Cisco	ASR 903	-
Sw-001	192.168.1.10	switch	Головний інженер Іванов І.І.	Cisco	ws-c3750x-48t-s	12.2 SE3
Sw-002	192.168.2.20	switch	Головний інженер Іванов І.І.	Cisco	ws-c3750x-48t-s	12.2 SE4
Sw-003	192.168.3.10	switch	Головний інженер Іванов І.І.	Cisco	ws-c3750x-48t-s	12.2 SE5
Sw-004	192.168.4.10	switch	Головний інженер Іванов І.І.	Cisco	ws-c3750x-48t-s	12.2 SE6
Pr-001	192.168.1.11	printer	Головний інженер Іванов І.І.	Canon	I-SENSYS MF112	-
Pr-002	192.168.1.12	printer	Головний інженер Іванов І.І.	Canon	I-SENSYS MF112	-
Sc-001	192.168.1.13	scanner	Головний інженер Іванов І.І.	Canon	DR-M260	-

Сервери

Умовне скорочення	IP-адреса	Назва хоста	Призначення	Відповідальна особа	Виробник	Модель	ОС	Наявність антивірусу
S-001	192.168.0.11	mail-server	Поштовий сервер	Головний інженер Іванов І.І.	IBM	x86	Debian 9	No
S-002	192.168.0.12	ftp-server	Сервер FTP	Головний інженер Іванов І.І.	IBM	x86	Debian 9	No
S-003	192.168.2.11	backup1-server	Сервер резерного копіювання для БД1	Головний інженер Іванов І.І.	IBM	x86	Debian 9	No
S-004	192.168.2.12	logging-server	Сервер журналювання	Головний інженер Іванов І.І.	IBM	x86	Debian 9	No
S-005	192.168.2.13	app-server	Сервер додатку	Головний інженер Іванов І.І.	IBM	x86	Debian 9	No
S-006	192.168.3.11	db1-server	Сервер з БД для даних карток	Головний інженер Іванов І.І.	IBM	x86	Debian 9	No
S-007	192.168.4.11	db2-server	Сервер з БД для всього іншого	Головний інженер Іванов І.І.	IBM	x86	Debian 9	No
S-008	192.168.4.12	ad-server	Active Directory сервер	Головний інженер Іванов І.І.	IBM	x86	Debian 9	No
S-009	192.168.4.13	backup2-server	Сервер резерного копіювання для БД2	Головний інженер Іванов І.І.	IBM	x86	Debian 9	No

Робочі станції

Умовне скорочення	Операційна система	Версія ОС	Виробник	Модель	До якої мережі належить
PC-001	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-002	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-003	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-004	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-005	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-006	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-007	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-008	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-009	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-010	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-011	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-012	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-013	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-014	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-015	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-016	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-017	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-018	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 1
PC-019	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 2
PC-020	Ubunto	20.04 LTS	Impression	Desktop Initio I1047	Vlan 2
LT-001	iOS	11.2.1	Apple	MacBook Air M1	-
LT-002	iOS	11.2.1	Apple	MacBook Air M1	-
LT-003	iOS	11.2.1	Apple	MacBook Air M1	-
LT-004	Ubunto	20.04 LTS	HP	ProBook 4340s	-
LT-005	Ubunto	20.04 LTS	HP	ProBook 4340s	-
LT-006	Ubunto	20.04 LTS	HP	ProBook 4340s	-
LT-007	Ubunto	20.04 LTS	HP	ProBook 4340s	-

Додаток Ж

Посада	Кількість співробітників	Доступ до техніки	Рівень доступу (заборонене все, крім)
CEO	1	PC + Laptop	Доступ до всього, крім CDE.
HR	1	PC	Доступ до інформації низького рівня, середнього, особових справ працівників.
PM	2	PC	Доступ до інформації низького рівня, середнього, угод з клієнтами.
Sysadmin	2	PC + Laptop	Доступ до інформації низького рівня, середнього, документація щодо налаштування внутрішньої комп'ютерної мережі (крім документації щодо додатку)
Адміністратор CDE	1	PC	Доступ до CDE, інформації низького та середнього рівня.
Адміністратор БД	2	PC	Доступ до інформації низького рівня, середнього, клієнської БД.
Адміністратор додатку	2	PC	Доступ до інформації низького рівня, середнього, технічної інформації щодо додатку.
Аналітик	1	PC	Доступ до інформації низького рівня, середнього, клієнської БД, угод, фінансової документації.
Бізнес аналітик	1	PC	Доступ до інформації низького рівня, середнього, клієнської БД, угод.
Бухгалтер	1	PC	Доступ до інформації низького рівня, середнього, угод, фінансової документації.
Економіст	1	PC	Доступ до інформації низького рівня, середнього, фінансової документації.
Маркетолог	1	PC	Доступ до інформації низького рівня, середнього, угод.
Розробник	2	Laptop	Доступ до інформації низького рівня, середнього, технічної інформації щодо додатку.
Секретар	1	PC	Доступ до інформації низького рівня, середнього.
Співробітник технічної підтримки	2	PC + Laptop	Доступ до інформації низького рівня, середнього, клієнської БД, технічної документації.
Юрист	2	PC	Доступ до інформації низького рівня, середнього, юридичних документів, угод.

Додаток 3

```
openssl s_client -servername 192.168.0.10-connect 192.168.0.10:443
CONNECTED(00000003)
depth=0 CN = xxx-xxxx-01.diplom.local, C = US
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = xxx-xxxx-01.diplom.local, C = US
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
0 s:/CN=xxx-xxxx-01.diplom.local/C=US
  i:/CN=CA/DC=vsphere3/DC=local/C=US/ST=California/O=xxx-xxxx-
01.diplom.local/OU=Cisco
---
….
SSL-Session:
   Protocol  : TLSv1.1
   Cipher    : ECDHE-RSA-AES256-GCM-SHA384
```

Додаток І

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>ossecm@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
  </global>

  <cluster>
    <name>wazuh</name>
    <node_name>{{ inventory_hostname }}</node_name>
{% if inventory_hostname in groups['wazuh-master'] %}
    <node_type>master</node_type>
{% else %}
    <node_type>worker</node_type>
{% endif %}
    <key>{{ wazuh_cluster_key }}</key>
    <port>1516</port>
    <bind_addr>0.0.0.0</bind_addr>
    <nodes>
      <node>master.wazuh.service.consul</node>
    </nodes>
    <hidden>no</hidden>
  </cluster>

  <!-- Choose between plain or json format (or both) for internal logs -->
  <logging>
    <log_format>plain</log_format>
  </logging>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>
```

```
<remote>
  <connection>secure</connection>
  <port>1514</port>
  <protocol>udp</protocol>
</remote>

<!-- Policy monitoring -->
<rootcheck>
  <disabled>no</disabled>
  <check_unixaudit>yes</check_unixaudit>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>
  <ignore type="sregex">^/etc/</ignore>

  <!-- Frequency that rootcheck is executed - every 12 hours -->
  <frequency>43200</frequency>

  <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>

  <skip_nfs>yes</skip_nfs>
</rootcheck>

<wodle name="open-scap">
  <disabled>yes</disabled>
  <timeout>1800</timeout>
  <interval>1d</interval>
  <scan-on-start>yes</scan-on-start>
  <content type="xccdf" path="ssg-debian-8-ds.xml">
    <profile>xccdf_org.ssgproject.content_profile_common</profile>
  </content>
  <content type="oval" path="cve-debian-oval.xml" />
</wodle>

<wodle name="syscollector">
```

```
    <disabled>no</disabled>
    <interval>1h</interval>
    <scan_on_start>yes</scan_on_start>
    <hardware>yes</hardware>
    <os>yes</os>
    <network>yes</network>
  </wodle>
<!--
  <wodle name="key-request">
    <enabled>yes</enabled>
    <timeout>60</timeout>
    <script>my_script.sh</script>
    <threads>4</threads>
    <queue_size>1024</queue_size>
  </wodle>

  <wodle name="agent-key-polling">
    <enabled>yes</enabled>
    <timeout>60</timeout>
    <exec_path>/usr/bin/python /home/script.py</exec_path>
    <threads>1</threads>
    <queue_size>1024</queue_size>
    <force_insert>yes</force_insert>
  </wodle>
-->

  <vulnerability-detector>
    <enabled>yes</enabled>
    <interval>24h</interval>
    <ignore_time>6h</ignore_time>
    <run_on_start>yes</run_on_start>
    <provider name="debian">
      <enabled>yes</enabled>
      <os>stretch</os>
      <os>jessie</os>
      <os>buster</os>
      <update_interval>1h</update_interval>
    </provider>
  </vulnerability-detector>

  <!-- File integrity monitoring -->
```

```
<syscheck>
  <disabled>no</disabled>
  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>
  <scan_on_start>yes</scan_on_start>
  <!-- Generate alert when new file detected -->
  <alert_new_files>yes</alert_new_files>
  <!-- Don't ignore files that change more than 3 times -->
  <auto_ignore>no</auto_ignore>
  <!-- Directories to check  (perform all possible verifications) -->
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>
  <!-- Files/directories to ignore -->
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
  <ignore>/etc/mail/statistics</ignore>
  <ignore>/etc/random-seed</ignore>
  <ignore>/etc/random.seed</ignore>
  <ignore>/etc/adjtime</ignore>
  <ignore>/etc/httpd/logs</ignore>
  <ignore>/etc/utmpx</ignore>
  <ignore>/etc/wtmpx</ignore>
  <ignore>/etc/cups/certs</ignore>
  <ignore>/etc/dumpdates</ignore>
  <ignore>/etc/svc/volatile</ignore>
  <ignore>/sys/kernel/security</ignore>
  <ignore>/sys/kernel/debug</ignore>
  <!-- File types to ignore -->
  <ignore type="sregex">.log$|.swp$</ignore>
  <!-- Check the file, but never compute the diff -->
  <nodiff>/etc/ssl/private.key</nodiff>
  <skip_nfs>yes</skip_nfs>
  <skip_dev>yes</skip_dev>
  <skip_proc>yes</skip_proc>
  <skip_sys>yes</skip_sys>
  <!-- Nice value for Syscheck process -->
  <process_priority>10</process_priority>
  <!-- Maximum output throughput -->
  <max_eps>100</max_eps>
  <!-- Database synchronization settings -->
```

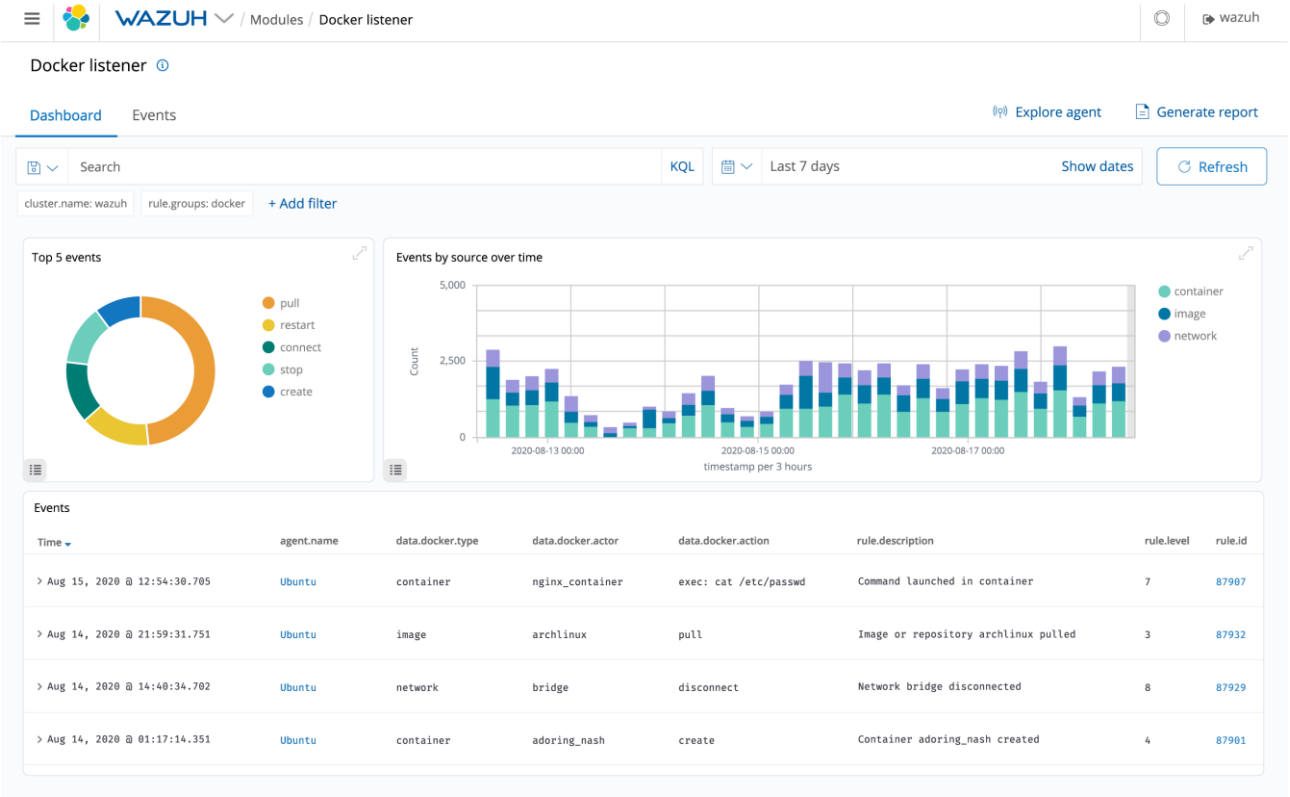
```
  <synchronization>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <response_timeout>30</response_timeout>
    <queue_size>16384</queue_size>
    <max_eps>10</max_eps>
  </synchronization>
</syscheck>

<!-- Active response -->
<global>
  <white_list>127.0.0.1</white_list>
  <white_list>^localhost.localdomain$</white_list>
  <white_list>10.0.0.2</white_list>
</global>

<command>
  <name>disable-account</name>
  <executable>disable-account.sh</executable>
  <expect>user</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>restart-ossec</name>
  <executable>restart-ossec.sh</executable>
  <expect />
</command>

<command>
  <name>firewall-drop</name>
  <executable>firewall-drop.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>host-deny</name>
  <executable>host-deny.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
```

```
</command>

<command>
  <name>route-null</name>
  <executable>route-null.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<command>
  <name>win_route-null</name>
  <executable>route-null.cmd</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>

<!--
<active-response>
 active-response options here
</active-response>
-->

<!-- Log analysis -->
<localfile>
  <log_format>syslog</log_format>
  <location>/var/ossec/logs/active-responses.log</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/messages</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/syslog</location>
```

```
</localfile>

<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
</localfile>

<localfile>
  <log_format>full_command</log_format>
  <command>netstat -tan |grep LISTEN |grep -v 127.0.0.1 | sort</command>
  <frequency>360</frequency>
</localfile>

<localfile>
  <log_format>full_command</log_format>
  <command>last -n 5</command>
  <frequency>360</frequency>
</localfile>

<ruleset>
  <!-- Default ruleset -->
  <decoder_dir>ruleset/decoders</decoder_dir>
  <rule_dir>ruleset/rules</rule_dir>
  <rule_exclude>0215-policy_rules.xml</rule_exclude>
  <list>etc/lists/audit-keys</list>
  <!-- User-defined ruleset -->
  <decoder_dir>etc/decoders</decoder_dir>
  <rule_dir>etc/rules</rule_dir>
</ruleset>

<!-- Configuration for ossec-authd
    To enable this service, run:
    ossec-control enable auth
-->

<auth>
  <disabled>no</disabled>
  <port>1515</port>
  <use_source_ip>no</use_source_ip>
  <force_insert>yes</force_insert>
```

```
    <force_time>0</force_time>
    <purge>yes</purge>
    <use_password>no</use_password>
    <!-- <ssl_agent_ca></ssl_agent_ca> -->
    <ssl_verify_host>no</ssl_verify_host>
    <ssl_manager_cert>/var/ossec/etc/sslmanager.cert</ssl_manager_cert>
    <ssl_manager_key>/var/ossec/etc/sslmanager.key</ssl_manager_key>
    <ssl_auto_negotiate>no</ssl_auto_negotiate>
  </auth>
</ossec_config>
```

Додаток И


WAZUH / Modules / Docker listener
wazuh
Docker listener
Dashboard
Events
Explore agent
Generate report
Search
KQL
Last 7 days
Show dates
Refresh
cluster.name: wazuh
rule.groups: docker
+ Add filter
Top 5 events
pull
restart
connect
stop
create
Events by source over time
5,000
2,500
0
Count
2020-08-13 00:00
2020-08-15 00:00
2020-08-17 00:00
timestamp per 3 hours
container
image
network
Events
Time
agent.name
data.docker.type
data.docker.actor
data.docker.action
rule.description
rule.level
rule.id
> Aug 15, 2020 @ 12:54:30.705
Ubuntu
container
nginx_container
exec: cat /etc/passwd
Command launched in container
7
87907
> Aug 14, 2020 @ 21:59:31.751
Ubuntu
image
archlinux
pull
Image or repository archlinux pulled
3
87932
> Aug 14, 2020 @ 14:40:34.702
Ubuntu
network
bridge
disconnect
Network bridge disconnected
8
87929
> Aug 14, 2020 @ 01:17:14.351
Ubuntu
container
adoring_nash
create
Container adoring_nash created
4
87901

Додаток Й

IT SPECIALIST

PCI DSS Certified

CERTIFICATE OF COMPLIANCE

AWARDED TO

GigaCenter Ukraine LLC

37V Vasylkivska St, Kyiv, 03022, Ukraine

The present certificate is issued to certify hereby that GigaCenter Ukraine LLC has successfully completed an assessment by IT Specialist LLC and was found to be compliant in accordance with Version 3.2.1 of the Payment Card Industry Data Security Standards (PCI DSS), as endorsed by VISA, MasterCard, American Express and other leading payment brands.

PCI Level:	1	**Certificate ID:**	#169-2021
Category:	Service Provider	**Issued on:**	May 25, 2021
On-site Assessment:	May 20, 2021	**Valid through:**	May 24, 2022
Service(s) Covered:	Physical space (co-location)		

QSA-Auditor:

Anatolii Zhuravlev
PCI QSA #204-557, CISSP, ISO 27001

Conditions of Issuing:

1. This certificate offers no guarantee or warranty to any third party that the company is invulnerable to attacks or breaches in its security, and IT Specialist LLC accordingly accepts no liability to any third party in the event of loss or damage of any description caused by any failure in, or breach of, the subject's security environment either on prospective or retrospective basis.

2. This certificate is issued by IT Specialist LLC as a commercial representation, and is not officially sanctioned by either the PCI SSC or any payment brand making up its body. All queries regarding this certificate should be directed to IT Specialist LLC at qsa@my-itspecialist.com

PCI VISA MasterCard

https://gigacenter.ua/ru/about/

Додаток Ї

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Список погодження

Редакція від (ДД/ММ/РРРР)	ПІБ	Посада	Погоджено	
			Дата	Підпис
	Петров П.П.	Відповідальний за PCI DSS	2.06.2021	

Адміністративна інформація

Документ	**Версія:** 1.1	**Статус:** Активна	**Рівень конфіденційності:** Середній
Дата	2.06.2021		
Файл	**Політика інформаційної безпеки.docx**		

Історія змін

Дата внесення зміни (ДД/ММ/РРРР)	Короткий опис зміни

Зміст

1. ВВЕДЕННЯ

Політика інформаційної безпеки (далі - Політика ІБ) визначає консолідовану позицію ТОВ «Диплом» (далі - Організація) з питань безпеки інформації, метою якої є зведення до мінімуму всіх ризиків, пов'язаних з використанням та управлінням інформаційними активами.

Перелік заходів щодо реалізації Політики інформаційної безпеки, а також структура управління системою захисту інформації та відповідальність посадових осіб можуть варіюватися відповідно до особливостей побудови та організацією інформаційної системи (далі - ІС) Організації, з метою досягнення розумного компромісу між захищеністю, зручністю роботи та вартістю системи захисту інформації.

2. МЕТА ДОКУМЕНТУ

Дана Політика ставить своєю кінцевою метою впровадження системи вимог до інформаційної безпеки Організації. Є первинним документом, що використовуються в Політиці поняття та визначення використовуються в інших документах, повністю або частково описують вимоги до інформаційної безпеки. Ці документи є невід'ємною частиною цієї політики.

Метою забезпечення інформаційної безпеки є збереження конфіденційності, цілісності та доступності інформації. Конфіденційність інформації забезпечується в разі надання доступу до даних тільки авторизованим особам, цілісність - в разі внесення в дані виключно авторизованих змін, доступність - при забезпеченні можливості отримання доступу до даних авторизованим особам в потрібний для них час.

Основними завданнями забезпечення ІБ є:

- Захист від загроз витоку, втрати та несанкціонованої модифікації;
- Нейтралізація наслідків від реалізованих загроз;
- Забезпечення відповідності законодавству та стандарту PCI DSS.

3. ТЕРМІНИ ТА ВИЗНАЧЕННЯ

Payment Card Industry Data Security Standard (PCI DSS) – стандарт безпеки даних платіжних карт, розроблений Радою за стандартами безпеки індустрії платіжних карток (Payment Card Industry Security Standards Council, PCI SSC), заснованим міжнародними платіжними системами Visa, MasterCard, American Express, JCB та Discover.

Політика - сукупність керівних принципів, правил, процедур та практичних прийомів у області безпеки, які регулюють управління, захист та розподіл цінної інформації.

Інформаційна система (далі по тексту ІС) - сукупність організаційних та технічних засобів для зберігання та обробки інформації з метою забезпечення інформаційних потреб користувачів. Інформаційна система включає в себе технічні засоби обробки даних, середовище передачі даних та відповідний персонал.

Інформаційний актив - це матеріальний або нематеріальний об'єкт, який є інформацією або містить інформацію, служить для обробки, зберігання або передачі інформації, належить Організації та має дійсну або потенційну цінність для Організації.

Дані власника картин - це строго регламентований перелік інформації про власника карти, а також технічна інформація, необхідна для роботи з карткою, розголошення якої може привести до фінансових втрат. До даних платіжних карт відносяться номер платіжної картки міжнародних платіжних систем, ім'я власника платіжної картки, сервісний код, дата закінчення терміну дії карти.

Критичні дані авторизації - дані (включаючи коди/значення перевірки справжності картки (CVC/CVV), повні дані магнітної смуги, PIN-коди), які використовуються для автентифікації користувачів та/або авторизації карткових платежів.

Інформаційна безпека (далі по тексту ІБ) - сукупність процесів та заходів, що мають на меті забезпечення цілісності, конфіденційності, доступності інформації, крім того можуть враховуватися інші властивості, такі, як автентичність, незаперечність та надійність.

Адміністратор ІС - співробітник відділу інформаційних технологій, відповідальний за створення та експлуатацію інформаційних систем Організації. Призначається наказом керівника відділу інформаційних технологій та здійснює свою діяльність в рамках своєї посадової інструкції.

Користувач - співробітник Організації або інша особа, які відповідно для встановленого порядку отримали доступ до ІС Організації.

Загроза Інформаційної безпеки - сукупність умов та факторів, що створюють небезпеку несанкціонованого доступу до інформації, що циркулює в інформаційних системах, а також можливі наслідки впливів порушника на систему, не запобігання, не виявлення та не ліквідація яких, може привести до погіршення заданих якісних характеристик функціонування систем або порушення їх працездатності, а також до спотворення та витоку інформації.

Несанкціонований доступ (НСД) - доступ до закритої для публічного доступу інформації з боку осіб, які не мають дозволу на доступ до цієї інформації, в тому числі доступ до інформації при порушенні посадових повноважень співробітником. Також несанкціонованим доступом в окремих випадках називають отримання доступу до інформації особою, яка має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

Власник (Інформаційних активів/систем) - юридична або фізична особа, яка здійснює користування та розпорядження інформаційними активами та інформаційними системами в межах повноважень, встановлених законодавством або договором.

Угода про нерозголошення конфіденційної інформації (NDA) - письмова угода, що визначає повноваження та відповідальність сторін при отриманні, зберіганні, використанні конфіденційної інформації.

Антивірусне програмне забезпечення - спеціалізована програма для виявлення комп'ютерних вірусів, а також небажаних (вважаються шкідливими) програм взагалі та відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики - запобігання зараженню (модифікації) файлів або операційної системи шкідливим кодом.

Система резервного копіювання - процес створення копії даних на носії (жорсткому диску, flash та т.д.), призначеному для відновлення даних в оригінальному або новому місці їх розташування в разі їх пошкодження або руйнування.

Публічна інформація - це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, яка допущена до публікації керівництвом Організації, була отримана або створена в процесі виконання співробітниками Організації своїх посадових обов'язків та знаходиться у володінні Організації.

Конфіденційна інформація - інформація, до якої немає вільного доступу на законних підставах. Порядок та умови віднесення інформації до конфіденційної, а також порядок та умови її поширення визначаються керівництвом Організації.

4. ЗОНА ЗАСТОСУВАННЯ

Дана Політика обов'язкове для виконання всіма співробітниками Організації, а також іншими особами, які в установленому порядку отримують доступ до будь-яких інформаційних систем або ресурсів Організації в рамках укладених контрактів.

5. ЗАГАЛЬНЕ ПОЛОЖЕННЯ

5.1.1. Політика інформаційної безпеки затверджується керівництвом Організації.

5.1.2. Керівництво Організації бере на себе відповідальність за реалізацію Політики та є гарантом виконання її вимог.

5.1.3. Керівництво Організації сприяє у створенні, впровадженні, контролі та підтримці інформаційної безпеки на належному рівні.

5.1.4. Затверджені керівництвом Організації рішення та рекомендації в області інформаційної безпеки, є безперечними та обов'язковими для виконання всіма співробітниками Організації.

5.1.5. Доступ до інформації надається тільки особам, яким він необхідний для виконання посадових або контрактних зобов'язань в мінімально достатньому обсязі.

5.1.6. Для зниження ризиків розголошення, розкрадання або знищення конфіденційної інформації всі співробітники Організації, а також особи, які в установленому порядку отримують доступ до будь-яких інформаційних активів або системам Організації, підписують зобов'язання про нерозголошення конфіденційної інформації (NDA).

5.1.7. З метою підвищення рівня знань та поінформованості у питаннях інформаційної безпеки всі співробітники Організації повинні проходити регулярне навчання (інструктаж).

5.1.8. Порядок роботи з криптографічними системами та ключами визначений відповідними внутрішніми нормативними документами Організації, які засновані на вимогах законодавства України та міжнародного стандарту PCI DSS.

5.1.9. Для захисту інформаційних активів та систем Організації від руйнівного впливу шкідливого коду використовується антивірусне програмне забезпечення.

5.1.10. Для запобігання несанкціонованого доступу до конфіденційних даних Організації, які обробляються на ноутбуках, їх жорсткі диски повинні бути зашифровані.

5.1.11. Для забезпечення цілісності та достовірності електронної інформації Організації та захисту її від програмних та апаратних збоїв використовується система резервного копіювання та дублювання найбільш цінних інформаційних активів. Дана система дозволяє забезпечити можливість відновлення даних з резервних копій з мінімальними втратами інформації за прийнятний час.

5.1.12. В Організації складаються, вводяться в дію, систематично тестуються та оновлюються плани безперебійної роботи на випадок різних непередбачених критичних ситуацій.

5.1.13. Відповідність вимог щодо забезпечення безперервності бізнесу та безпеки інформаційних систем Політикам безпеки, стандартам та міжнародним рекомендаціям, забезпечується системою заходів, що включає систематичний контроль та проведення незалежних аудиторських перевірок.

5.1.14. Оцінка ризиків інформаційної безпеки проводиться щорічно, а також у разі значних змін в структурі та бізнес-процесах Організації. При оцінці ризиків враховується вплив реалізації загроз інформаційної безпеки на фінансове становище та ринкову репутацію Організації.

5.1.15. Заходи захисту інформації впроваджуються за результатами проведеної оцінки ризиків інформаційної безпеки.

5.1.16. Вартість вжитих заходів не повинна перевищувати розмір вартості можливих збитків, що виникає при реалізації загроз, крім випадків, коли можлива загроза визначена як обов'язкова до усунення за чинним законодавством України.

6. ВЛАСНИКИ ІНФОРМАЦІЙНИХ АКТИВІВ

6.1.1. Для кожного інформаційного активу визначається відповідальна особа відповідного підрозділу Організації (власник), що відповідає за надання доступу до даного активу та ефективне функціонування заходів захисту інформації.

6.1.2. Власником є автор оригінальної версії інформаційного активу. Оригінальна версія може бути створена шляхом об'єднання кількох існуючих одиниць інформації або шляхом створення нової одиниці в письмовій, електронній чи вербальної формі. Власниками інформації можуть бути окремі особи, групи осіб, юридичні особи або організації.

6.1.3. Власник самостійно визначає рівень безпеки наявних у нього інформаційних активів виходячи з суті, мети та цільової аудиторії. Власник повинен обробити та дбати про безпеку інформаційних активів відповідно до їх категорії, відповідно до затвердженої класифікації інформації.

7. КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ

7.1.1. Інформація, що циркулює в Організації, класифікується за режимом доступу, уразливості та цінності для визначення необхідності, пріоритетів та ступеня захисту при її обробці.

7.1.2. За режимом доступу вся інформація в Організації ділиться на публічну та конфіденційну.

7.1.3. Конфіденційна інформація, що циркулює в Організації, ділиться на чотири категорії:

- Для внутрішнього користування (ДВК);
- Конфіденційна (К);
- Комерційна таємниця (КТ);
- Персональні дані (ПД).

7.1.4. Для кожної категорії інформації визначається період конфіденційності, порядок її звернення, зберігання, передачі та знищення.

7.1.5. Організація залишає за собою право протоколювати та контролювати дії співробітників при роботі з інформацією, що є її власністю.

8. ФІЗИЧНА БЕЗПЕКА

8.1.1. Всі об'єкти критичні з точки зору інформаційної безпеки (файл-сервера, сервера баз даних та бізнес додатків, телефонна станція, маршрутизатори, факсокси та т.д.) повинні знаходитися в виділеному приміщенні, доступ до якого обмежений та контролюється.

8.1.2. Доступ до приміщення Організації в позаурочний час або у вихідні та святкові дні здійснюється з письмового дозволу керівництва. В екстреному випадку (поломки ключового обладнання та т.д.) доступ здійснюється після телефонного дзвінка Керівництва, без письмового дозволу.

8.1.3. Вимоги до системи пожежної безпеки, системи відеоспостереження та системи контролю та управління доступом (СКУД) визначені відповідними внутрішніми нормативними документами, а також регулюючими нормативними та законодавчими актами України.

8.1.4. Порядок виносу/виносу матеріальних цінностей, перетину периметра фізичної безпеки транспортними засобами визначено відповідними внутрішніми нормативними документами.

9. КОНТРОЛЬ ТА ВІДПОВІДАЛЬНІСТЬ

9.1.1. Кожен співробітник Організації бере участь в підтримці відповідного рівня інформаційної безпеки Організації. В рамках своїх обов'язків та повноважень співробітники зобов'язані виконувати та відповідати за дотримання вимог законодавства України та внутрішніх нормативних документів Організації.

9.1.2. Відділ ІБ відповідає за визначення конкретних вимог до інформаційної безпеки Організації та контролює їх виконання.

9.1.3. Співробітники несуть персональну відповідальність за дотримання вимог даної Політики.

9.1.4. Про кожний інцидент, пов'язаний з порушенням даної Політики, співробітники зобов'язані негайно повідомити адміністратора ІС або співробітнику відділу ІБ та довести до відома свого безпосереднього керівника.

9.1.5. По кожному такому інциденту відповідальні особи Організації проводять аналіз. На підставі проведеного аналізу приймаються відповідні коригувальні та запобіжні заходи, спрямовані на недопущення повторення подібних інцидентів.

9.1.6. Відповідальність за своєчасне доведення вимог даної Політики до відома співробітників несе відділ ІБ.

9.1.7. Організація залишає за собою право вживати заходів дисциплінарного характеру до співробітників, які порушують норми та вимоги даної Політики.

9.1.8. За невиконання або недотримання вимог даної Політики співробітники несуть адміністративну, цивільно-правову або іншу відповідальність відповідно до чинного законодавства України.

10. ТЕРМІН ДІЇ ТА ПЕРЕГЛЯДУ ДОКУМЕНТУ

10.1.1. Політика вступає у дію з моменту його затвердження керівництвом Організації;

10.1.2. Внесення змін та доповнень у дану Політику відзначається у таблиці «Історія змін» та здійснюється після узгодження з керівником відділу ІБ;

10.1.3. Всі зміни, що були внесені у документ, повинні бути відображені у таблиці «Історія змін» із зазначенням дати внесення змін та короткого опису;

10.1.4. Політика переглядається по мірі необхідності, але не рідше одного разу на 12 місяців, а також, у разі зміни законодавчих та інших норм та вимог;

10.1.5. Після перегляду, зміни або внесення доповнень дана Політика затверджується керівництвом Організації;

10.1.6. У разі вступу окремих пунктів даного документа в протиріччя з новими законодавчими актами, ці пункти втрачають юридичну силу до моменту внесення змін до даної Політики.

Додаток К

Payment Card Industry (PCI) Technical Report

04/29/2021

ASV Scan Report Attestation of Scan Compliance

A1. Scan Customer Information				A2. Approved Scanning Vendor Information			
Company:	ТОВ «Диплом»			Company:	ТОВ «Дослідження»		
Contact Name:		Job Title:		Contact Name:	Кармазіна Анастасія	Job Title:	
Telephone:		Email:		Telephone:		Email:	
Business Address:				Business Address:			
City:	Київ	State/Province:		City:	Kyiv	State/Province:	None
ZIP/postal code:		Country:	Україна	ZIP/postal code:		Country:	Ukraine
URL:				URL:			

A3. Scan Status			
Date scan completed	04/29/2021	Scan expiration date (90 days from date scan completed)	07/28/2021
Compliance Status	PASS	Scan report type	Full scan
Number of unique in-scope components scanned			3
Number of identified failing vulnerabilities			0
Number of components found by ASV but not scanned because scan customer confirmed components were out of scope			0

A.4 Scan Customer Attestation

ТОВ «Диплом» attests on 04/29/2021 at 16:09:36 GMT that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions -including compensating controls if applicable- is accurate and complete.

ТОВ «Диплом» also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by ТОВ «Досліження» under certificate number XXXX-XX 3, according to internal processes that meet PCI DSS requirement 11.2.2 and the ASV Program Guide.

ТОВ «Досліження» attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by Anatoliy Zhuravlev