Національний банк України

Платіжна організація
Національної платіжної системи “Український платіжний простір”

ЗАТВЕРДЖЕНО
Рішення Ради Платіжної організації
Національної платіжної системи
“Український платіжний простір”
(протокол від 26.03.2018 № 57/6/2018)

ПОЛОЖЕННЯ
про організацію захисту даних платіжних карток Національної платіжної системи “Український платіжний простір”

м. Київ

Зміст

I. Загальні положення

1. Положення про організацію захисту даних платіжних карток Національної платіжної системи “Український платіжний простір” (далі – Положення) розроблене згідно із Законами України “Про Національний банк України”, “Про банки і банківську діяльність”, “Про платіжні системи та переказ коштів в Україні”, Правилами Національної платіжної системи “Український платіжний простір”, затвердженими рішенням Ради Платіжної організації Національної платіжної системи “Український платіжний простір” (протокол від 07.06.2013 № 213 зі змінами) (далі – Правила) та іншими законодавчими актами України, нормативно-правовими актами Національного банку України.

2. Мета Положення – забезпечення належного стану організації безпеки даних платіжних карток та запровадження єдиних заходів спрямованих на їх захист.

3. Учасники Національної платіжної системи “Український платіжний простір” (далі – ПРОСТІР) зобов’язані забезпечити захист даних платіжних карток, а також несуть відповідальність у разі їх компрометації.

4. Організація та проведення робіт із захисту даних платіжних карток повинна здійснюватися відповідними особами, обов’язком яких є забезпечення контролю за станом організації захисту даних платіжних карток, проведення проектування, розроблення і модернізації систем захисту.

II. Умовні позначення, скорочення і терміни

5. У цьому документі використовуються такі умовні позначення, скорочення і терміни:

1) 802.11 – набір стандартів з комунікації в безпровідній мережевій зоні;

2) PCI PTS (Payment Card Industry PIN Transaction Security) – стандарт безпеки для платіжних терміналів, що використовують PIN-код;

3) RFC1918 (Address Allocation for Private Internets – розподіл адрес в приватних IP-мережах) – документ розглядає питання розподілу адрес в приватних IP-мережах;

4) SSL (Secure Sockets Layer – рівень захищених сокетів) – криптографічний протокол, що забезпечує захищену передачу даних між вузлами мережі Інтернет;

5) SNMP (Simple Network Management Protocol – простий протокол керування мережею) – протокол керування мережами зв’язку на основі архітектури TCP/IP;

6) TLS (Transport Layer Security – захист на транспортному рівні) – криптографічний протокол, який забезпечує захищену передачу даних між вузлами мережі Інтернет. TLS розроблено на специфікації протоколу SSL версії 3.0;

7) автентифікація – процедура, яка дозволяє постачальнику платіжних послуг перевірити особу держателя платіжної картки ПРОСТІР;

8) атака – дії та або спроба дій, направлених на втручання, зчитування, руйнування, зміну, викрадення, блокування, а також спроби несанкціонованого доступу або виконання несанкціонованих дій з ресурсами системи або даними платіжних карток;

9) багатофакторна автентифікація – автентифікація, яка здійснюється за допомогою захищених механізмів двох або більше типів (наприклад, застосування для автентифікації пароля разом із апаратним засобом захисту інформації або біометричної автентифікації разом із паролем);

10) віртуальний хостинг – вид хостингу, при якому необмежена кількість розподілених інформаційних середовищ розташовано на одному ресурсі;

11) геш-функція (гешування) – функція, що перетворює вхідні дані будь-якого розміру в дані фіксованого розміру;

12) держатель платіжної картки ПРОСТІР – користувач електронного платіжного засобу (юридична або фізична особа), якому надано право здійснення операцій з його використанням;

13) ДМЗ – демілітаризована зона, сегмент корпоративної мережі;

14) індексний маркер – це криптографічний маркер, який замінює PAN, що заснований на певному індексі значень та який не піддається обчисленню;

15) інформаційне середовище – сукупність відповідальних осіб, процесів та інформаційних технологій, які зберігають, обробляють та/або передають дані платіжної картки і критичні автентифікаційні дані;

16) критичне приміщення – приміщення оброблення даних, серверні кімнати або інші приміщення, в яких розташовані системи, що зберігають, обробляють або передають дані платіжної картки ПРОСТІР. Винятком є місця розташування платіжних пристроїв;

17) критичні технології – сукупність технологій або окрема технологія, яка має високий потенціал впливу на процеси і інформаційні технологій, які зберігають, обробляють та/або передають дані платіжних карток;

18) одноразовий блокнот – система, в якій секретний ключ, згенерований випадковим чином, використовується тільки один раз для шифрування повідомлення, яке потім розшифровується за допомогою відповідного одноразового блокнота і ключа;

19) персоналізація платіжної картки – операція, під час здійснення якої на платіжну картку записуються відповідні банківські дані, ідентифікатори платіжних додатків платіжної картки, ліміти платіжних додатків та дати закінчення їх дії тощо;

20) постачальник платіжних послуг – емітент або еквайр, який надає платіжну послугу користувачу;

21) мобільний платіжний термінал (термінал POI) – компактний пристрій, що представляє собою підключений до смартфону або портативного персонального комп’ютеру торговий термінал, який може приймати до оплати платіжні картки;

Інші терміни вживаються у значеннях, визначених Законом України “Про платіжні системи та переказ коштів в Україні”, Правилах та інших нормативних документах ПРОСТІР.

III. Дані платіжних карток

6. Дані платіжних карток ПРОСТІР:

1) первинний номер платіжної картки ПРОСТІР (далі – PAN) – цифровий номер з 16 цифр, який вказаний на платіжній картці ПРОСТІР;

2) ім’я та прізвище держателя платіжної картки ПРОСТІР;

3) дата завершення терміну дії платіжної картки ПРОСТІР;

4) сервісний код.

7. Критичні автентифікаційні дані:

1) повні дані доріжок магнітних смуг або їх еквівалент на чипі;

2) код перевірки достовірності платіжної картки;

3) ПІН-коди та/або ПІН-блоки.

8. Вимоги до елементів даних платіжних карток у частині їх збереження в інформаційному середовищі.

Таблиця 1

	Елемент даних платіжної картки	**Збереження дозволено так/ні**	**Збереження даних у вигляді, що унеможливлює їх читання згідно з пунктом 17.4 цього Положення**
Дані платіжної картки ПРОСТІР	PAN	Так	Так
	ім’я, прізвище держателя платіжної картки ПРОСТІР та/або найменування юридичної особи	Так	Ні
	дата завершення терміну дії платіжної картки ПРОСТІР	Так	Ні
	сервісний код	Так	Ні
Критичні автентифікаційні дані	повні дані доріжок магнітних смуг або їх еквівалент на чипі	Ні	заборонено зберігати згідно з пунктом 17.2 цього Положення
	код перевірки достовірності платіжної картки	Ні	заборонено зберігати згідно з пунктом 17.2 цього Положення
	ПІН-коди та/або ПІН-блоки	Ні	заборонено зберігати згідно з пунктом 17.2 цього Положення

IV. Політика з організації захисту даних платіжних карток

9. Пріоритетний підхід з впровадження організаційних та технічних заходів захисту даних платіжних карток складається з таких заходів:

1) видалення критичних автентифікаційних даних і застосування обмежень щодо збереження даних платіжної картки ПРОСТІР.

Метою заходу є зниження ризику з компрометації даних, забезпечення відсутності в інформаційному середовищі критичних автентифікаційних даних, що значно зменшує ризики та їх негативні наслідки;

2) забезпечення захисту периметру внутрішньої та бездротової мережі.

Метою заходу є організація захисту найбільш вразливих та критичних компонентів інформаційного середовища;

3) забезпечення безпеки платіжних додатків.

Метою заходу є організація захисту програмного забезпечення, процесів і серверів, від впливу вразливостей прикладного рівня, що надають можливість для компрометації критичних автентифікаційних даних і даних платіжної картки ПРОСТІР;

4) управління контролем доступу до систем.

Метою заходу є організація постійного моніторингу подій з надання доступу до інформаційного середовища даних платіжної картки ПРОСТІР;

5) захист даних платіжної картки ПРОСТІР, які зберігаються в інформаційному середовищі.

Метою заходу є застосування відповідних засобів для захисту даних платіжної картки ПРОСТІР, які зберігаються в інформаційному середовищі;

6) усунення решти розбіжностей та засвідчення того, що всі вимоги інформаційної безпеки виконані.

Метою заходу є виконання вимог, які залишилися неопрацьованими, доопрацювання політик та процедур, призначених для захисту даних платіжної картки ПРОСТІР в інформаційному середовищі.

10. Застосувати шифрування полів даних платіжних карток у системах, які здійснюють оброблення даних платіжної картки ПРОСТІР.

11. Дані трансакцій, які передаються каналами зв’язку, повинні бути захищені від несанкціонованого доступу та модифікації стійкими до компрометації засобами захисту.

V. Організація захисту даних платіжних карток від платіжного пристрою до еквайрингової установи

12. Слід обмежити обіг даних платіжних карток ПРОСТІР та критичних автентифікаційних даних у відкритому вигляді тільки точками шифрування та розшифрування:

1) дані платіжних карток ПРОСТІР та критичні автентифікаційні дані повинні бути доступні у відкритому вигляді тільки в точках шифрування та розшифрування;

2) усі дані платіжних карток ПРОСТІР та критичні автентифікаційні дані повинні шифруватися тільки тими алгоритмами, що визначені комітетом ANSI X9 або ISO (наприклад, AES, TDES тощо або аналог);

3) усі дані платіжних карток ПРОСТІР та критичні автентифікаційні дані повинні бути зашифровані, крім:

перших шести цифр PAN, які залишаються відкритими для маршрутизації для авторизації;

перших шести і останніх чотирьох цифр PAN, які можуть відображатися на екрані платіжних терміналів та/або бути надрукованим на чеку, в документах щодо здійснення оплати;

4) критичні автентифікаційні дані не повинні зберігатись після завершення авторизації, навіть у зашифрованому вигляді.

13. Захист платіжних пристроїв, що виконує криптографічні операції, від фізичної та логічної компрометації слід здійснювати наступним чином:

1) пристрої, які виконують криптографічні операції, підлягають проведенню зовнішньому незалежному оцінюванню для підтвердження того, що обладнання та програмне забезпечення стійкі до атак;

2) секретні і приватні ключі повинні бути захищені від фізичної та логічної компрометації. Публічні ключі, повинні бути захищені від підміни, їх цілісність і достовірність повинна бути гарантована.

14. Для внутрішніх бізнес-процесів учасника ПРОСТІР рекомендується використовувати додатковий унікальний номер трансакції, що не використовує PAN.

VI. Організація захисту даних платіжних карток

15. Вимога 1: **Встановлення та забезпечення функціонування міжмережевих екранів для організації захисту даних платіжних карток**.

15.1. Розроблення та запровадження стандартів для міжмережевих екранів та конфігурацій маршрутизаторів, які повинні включати таке (захід підпункту 6 пункту 9 розділу IV цього Положення):

15.1.1. Формалізований процес тестування та затвердження всіх мережевих з’єднань і змін до конфігурації міжмережевих екранів, маршрутизаторів (захід підпункту 6 пункту 9 розділу IV цього Положення).

15.1.2. Актуальну схему мережі із зазначенням всіх підключень до середовища даних платіжних карток з інших мереж, включаючи всі бездротові мережі (захід підпункту 1 пункту 9 розділу IV цього Положення).

15.1.3. Актуальну схему, що відображає всі потоки проходження даних платіжних карток у всіх системах та мережах (захід підпункту 2 пункту 9 розділу IV цього Положення).

15.1.4. Вимоги до міжмережевого екранування кожного Інтернет-з’єднання і кожного з’єднання між ДМЗ і внутрішньою мережею установи (захід підпункту 2 пункту 9 розділу IV цього Положення).

15.1.5. Опис груп, ролей та обов’язків, що використовуються для здійснення керування мережевими компонентами (захід підпункту 6 пункту 9 розділу IV цього Положення).

15.1.6. Затверджене керівником установи або уповноваженою ним особою документоване обґрунтування щодо використання сервісів, протоколів і портів в установі, в тому числі опис функцій безпеки, що реалізовані для тих протоколів, які вважаються небезпечними (захід підпункту 6 пункту 9 розділу IV цього Положення).

15.1.7. Вимогу щодо перегляду набору правил міжмережевих екранів та конфігурації маршрутизаторів не менше одного разу на півроку (захід підпункту 6 пункту 9 розділу IV цього Положення).

15.2. Розробити конфігурації налаштування міжмережевих екранів і маршрутизаторів, які обмежують, контролюють зв'язок між недовіреними мережами та усіма системними компонентами в середовищі даних платіжних карток (захід підпункту 2 пункту 9 розділу IV цього Положення).

Недовіреною мережею є будь-яка мережа, яка є зовнішньою мережею по відношенню до мереж установи або яка не контролюється установою.

15.2.1. Вхідний і вихідний трафік повинен бути обмежений тільки тими з'єднаннями, які необхідні для середовища даних платіжних карток, а весь інший трафік повинен бути заборонений (захід підпункту 2 пункту 9 розділу IV цього Положення).

15.2.2. Запровадити безпечну та своєчасну синхронізацію конфігураційних файлів маршрутизаторів (захід підпункту 2 пункту 9 розділу IV цього Положення).

15.2.3. Встановити міжмережеві екрани між усіма бездротовими мережами і середовищем даних про платіжних карток, а також налаштувати зазначені міжмережеві екрани на блокування будь-якого трафіку з бездротовими мережами або дозволити проходження авторизованого трафіку між бездротовою мережею і середовищем даних платіжних карток у тому випадку, якщо такий трафік необхідний в службових цілях (захід підпункту 2 пункту 9 розділу IV цього Положення).

15.3. Заборонити прямий публічний доступ між мережею Інтернет та будь-яким компонентом середовища даних платіжних карток (захід підпункту 2 пункту 9 розділу IV цього Положення).

15.3.1. Запровадити ДМЗ таким чином, щоб обмежити вхідний трафік тільки тими системними компонентами, які забезпечують роботу дозволених загальнодоступних сервісів, протоколів і портів (захід підпункту 2 пункту 9 розділу IV цього Положення).

15.3.2. Обмежити вхідні Інтернет-з'єднання IP-адресами, які розташовані в ДМЗ (захід підпункту 2 пункту 9 розділу IV цього Положення).

15.3.3. Застосовувати заходи протидії підміни IP-адреси з метою виявлення фальшивих вихідних IP-адрес та заблокувати доступ їм у мережу установи (заблокувати Інтернет-трафік з внутрішньою вихідною адресою тощо) (захід підпункту 2 пункту 9 розділу IV цього Положення).

15.3.4. Заборонити несанкціонований вихідний трафік з середовища даних платіжних карток до мережі Інтернет (захід № 2 підпункту 2 пункту 9 розділу IV цього Положення).

15.3.5. Дозволено пропускати в мережу пакети тільки для встановлених з'єднань (захід підпункту 2 пункту 9 розділу IV цього Положення).

15.3.6. Розташовувати системні компоненти, які зберігають дані платіжних карток (бази даних тощо) у внутрішньому сегменті мережі, відокремленому від ДМЗ та інших недовірених мереж (захід № 2 підпункту 2 пункту 9 розділу IV цього Положення).

15.3.7. Не розголошувати приватні IP-адреси і дані про маршрутизацію сторонам, які не мають права доступу до такої інформації (захід підпункту 2 пункту 9 розділу IV цього Положення).

Методи щодо захисту IP-адресації повинні включати, але не обмежуватись таким:

технологія трансляції мережевих адрес (NAT);

розташування серверів, які містять дані платіжних карток за проксі-серверами та міжмережевими екранами;

видалення або фільтрація оголошень про маршрути для приватних мереж, які використовують відкритий адресний простір для зареєстрованих мереж;

внутрішнє використання адресного простору відповідно до RFC1918 замість адресного простору для зареєстрованих мереж.

15.4. Встановити персональні міжмережеві екрани (або його еквівалентні за функціональними можливостями) на будь-які портативні обчислювальні пристрої (в тому числі, що є власністю установи і/або власністю працівника установи), які підключаються до Інтернету під час перебування поза мережею (наприклад, ноутбуки, планшети, смартфони, що використовуються працівниками установи), і які також використовуються для отримання доступу до мережі. Вимоги до конфігурації міжмережевих екранів (або його еквівалент за функціональними можливостями) повинні містити таке (захід підпункту 2 пункту 9 розділу IV цього Положення):

визначені конкретні налаштування для конфігурацій;

персональні міжмережеві екрани (або його еквівалентні за функціональними можливостями) активовано;

налаштування персональних міжмережевих екранів (або його еквівалентні за функціональними можливостями) не можуть бути змінені користувачами та/або власниками портативних обчислювальних пристроїв.

15.5. Переконатися та забезпечити, що політики безпеки і процедури управління міжмережевими екранами задокументовані та виконуються і відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

16. Вимога 2: **Не використовувати початкові паролі та інші початкові системні налаштування, що застосовані виробником.**

16.1. Обов’язково змінювати початкові налаштування, що встановленні виробником (встановлені початкові паролі, рядки доступу SNMP, видалити непотрібні для роботи облікові записи), перед інтеграцією системи в мережеву інфраструктуру (захід підпункту 2 пункту 9 розділу IV цього Положення).

Ця вимога стосується всіх початкових паролів, в тому числі, але не обмежуючись тим, що використовуються в операційних системах, програмного забезпечення, яке надає послуги безпеки, облікових записів додатків і системи, платіжних пристроїв (в точках продажу), платіжних додатків, рядків доступу протоколу SNMP тощо).

16.1.1. Для бездротових мереж, які підключені до середовища даних платіжних карток або передають дані платіжних карток, змінити всі встановлені виробником початкові параметри в тому числі, але не обмежуючись таким: ключі

шифрування для доступу до бездротової мережі, паролі, рядки доступу SNMP, тощо (захід підпункту 2 пункту 9 розділу IV цього Положення).

16.2. Розробити стандарти конфігурацій для всіх системних компонентів. Стандарти повинні враховувати усі відомі ризики з безпеки інформації, а також вимоги міжнародних галузевих стандартів у сфері безпеки (захід підпункту 3 пункту 9 розділу IV цього Положення).

16.2.1. З метою уникнення випадків реалізації на одному сервері функцій, що вимагають різних рівнів захисту, кожний сервер повинен виконувати тільки одну основну функцію (захід підпункту 3 пункту 9 розділу IV цього Положення).

Веб-сервери, сервери баз даних і DNS повинні бути реалізовані на окремих серверах.

При застосуванні технології віртуалізації, необхідно реалізувати тільки одну основну функцію для кожного компоненту віртуальної системи.

16.2.2. Використовувати тільки необхідні сервіси та протоколи, які потрібні для виконання основної функції. Усі непотрібні для роботи сервіси і протоколи повинні бути відключені (захід підпункту 3 пункту 9 розділу IV цього Положення).

16.2.3. Параметри безпеки системи налаштовуються таким чином, щоб виключити можливість некоректного використання системи, будь-яких сервісів, протоколів або компонентів системи, які вважаються небезпечними (захід підпункту 3 пункту 9 розділу IV цього Положення).

У випадках використання SSL та /або попередніх версій TLS, положення додаткової вимоги А2 повинні бути виконані.

16.2.4. Налаштувати параметри безпеки системи таким чином, щоб унеможливити некоректне використання системи (захід підпункту 3 пункту 9 розділу IV цього Положення).

16.2.5. Видалити з системи функціональність, що не використовується: сценарії (скрипти), драйвери, додаткові можливості, підсистеми, файлові системи, непотрібні для роботи веб-сервери (захід підпункту 3 пункту 9 розділу IV цього Положення).

16.3. При використанні будь-якого віддаленого адміністративного доступу до системи обов’язково шифрувати канал зв’язку засобами стійкої криптографії (захід підпункту 2 пункту 9 розділу IV цього Положення).

У випадках використання SSL та/або попередніх версій TLS, положення додаткової вимоги А2 повинні бути виконані.

16.4. Проводити облік системних компонентів, які зберігають дані платіжних карток у ПРОСТІР (захід підпункту 2 пункту 9 розділу IV цього Положення).

16.5. Переконатися та забезпечити, що політики безпеки і операційні процедури управління початковими паролями та іншими початковими системними налаштуваннями, що застосовані виробником, задокументовані, виконуються та відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

16.6. Постачальники послуг віртуального хостингу повинні забезпечувати безпеку середовищ і даних платіжних карток кожної організації, що розміщені

на хостингу. Ці провайдери повинні відповідати вимогам, описаним в додаткових вимогах А1 (захід підпункту 2 пункту 9 розділу IV цього Положення).

17. Вимога 3: **Захист даних платіжних карток, що зберігаються**.

17.1. Зберігання даних платіжних карток обмежити необхідним мінімумом. Слід розробити політику зберігання, оброблення та знищення даних, процедури і процеси, що повинні містити таке, але не обмежуватись таким (захід підпункту 1 пункту 9 розділу IV цього Положення):

обмеження кількості збережених даних та термінів їх зберігання привести до значень, необхідних для виконання законодавчих, нормативно-правових та/або бізнес-вимог;

визначені вимоги щодо зберігання даних платіжних карток;

процедури гарантованого і безпечного видалення даних у яких вже немає потреби;

щоквартальний процес з виявлення і безпечного видалення збережених даних платіжних карток, які перевищують певні терміни зберігання, встановленні вимоги.

17.2. Забороняється зберігати критичні автентифікаційні дані після авторизації навіть у зашифрованому вигляді. У випадку отримання критичних автентифікаційних даних, слід зробити дані невідновлювальними до завершення процесу авторизації (захід підпункту 1 пункту 9 розділу IV цього Положення).

До критичних автентифікаційних даних належать дані, зазначені у пунктах 7, 20.2.1 – 20.2.3.

17.2.1. Забороняється зберігати повний вміст будь-якого треку (магнітної смуги на зворотному боці картки, еквівалентних даних на чіпі або в іншому місці) після авторизації. (захід підпункту 1 пункту 9 розділу IV цього Положення).

17.2.2. Забороняється зберігати код перевірки достовірності платіжної картки або значення, які використовуються для підтвердження трансакцій, що виконуються без безпосереднього зчитування інформації з платіжної картки після авторизації (захід підпункту 1 пункту 9 розділу IV цього Положення).

17.2.3. Забороняється зберігати ПІН-код, а також зашифрований ПІН-блок після авторизації (захід підпункту 1 пункту 9 розділу IV цього Положення).

17.3. Обов’язково маскувати PAN при його відображенні. Максимальна кількість знаків PAN для відображення – перші 6 і останні 4 цифри.

Ця вимога не відноситься до тих відповідальних працівників, яким для виконання службових обов’язків необхідно бачити весь PAN, також ця вимога не замінює собою інші, більш суворі вимоги щодо відображення даних платіжних карток (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.4. PAN повинен бути представлений у такому вигляді, що унеможливлює його читання у всіх місцях його зберігання, включаючи дані на змінних носіях, резервних копіях та журналах реєстрації подій, а також дані, що одержані через бездротові мережі (захід підпункту 5 пункту 9 розділу IV цього Положення).

Для цього слід використовувати будь-який з наступних методів:

однонаправлену функцію гешування на основі стійкої криптографії (гешування повинно бути всього PAN);

усічення (геш-код не може бути використано для заміни усіченого сегменту PAN);

індексні маркери і шифрувальні блокноти (такі блокноти при зберіганні повинні бути захищені);

стійкі криптографічні алгоритми з відповідними процесами та процедурами управління ключів.

17.4.1. У разі використання шифрування на рівні всього диска (замість шифрування окремих файлів або полів бази даних) управління логічним доступом має здійснюватися окремо та незалежно від механізмів розмежування доступу операційної системи (наприклад, шляхом відмови від використання локальних баз даних облікових записів користувачів або основних облікових даних для входу в мережу). Ключі шифрування не повинні бути прив’язані до облікових записів користувачів (захід підпункту 5 пункту 9 розділу IV цього Положення).

Ця вимога застосовується, як додаткова до всіх інших вимог цього Положення щодо шифрування та управління ключами.

17.5. Документувати та впровадити процедури щодо захисту ключів, які використовуються для забезпечення захисту збережених даних платіжних карток від їх компрометації або несанкціонованого використання в такий спосіб (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.5.1. *Додаткові вимоги для постачальників послуг*: ведення документованого опису криптографічної архітектури, що включає таке (захід підпункту 5 пункту 9 розділу IV цього Положення):

детальну інформацію про всі алгоритми, протоколи та ключі, що використовуються для забезпечення захисту даних платіжних карток, в тому числі довжини ключів та строки їх використання;

опис призначення для кожного ключа;

облік будь-яких криптографічних засобів захисту інформації (HSM, SCD) та інших засобів, що використовуються для управління ключами.

17.5.2. Обмежити доступ до криптографічних ключів. Доступ надається тільки мінімальній необхідній кількості працівників, яким такий доступ необхідний для виконання посадових обов’язків (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.5.3. Зберігати ключі, що використовуються для шифрування та/або розшифрування даних платіжних карток в одній (або більше) з наступних форм (захід підпункту 5 пункту 9 розділу IV цього Положення):

захищені ключем шифрування ключів, який має таку ж криптографічну стійкість, як і ключ шифрування даних, який зберігається окремо від ключа шифрування даних;

у захищеному криптографічному засобі захисту інформації (такому як апаратний модуль безпеки (HSM) або мобільний платіжний термінал, що відповідає вимогам PCI PTS);

у формі як мінімум двох компонентів ключа повної довжини або в формі розділеного секрету відповідно до прийнятого в галузі методу.

17.5.4. Кількість місць, призначених для зберігання криптографічних ключів обмежити необхідним мінімумом (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.6. Задокументувати та описати всі процеси та процедури управління ключами шифрування даних платіжних карток, що повинні містити таке, але не обмежуватись таким (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.6.1. Генерацію криптографічних стійких ключів (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.6.2. Поширення криптографічних стійких ключів (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.6.3. Захист криптографічних стійких ключів (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.6.4. Порядок заміни криптографічних ключів з вичерпаним криптоперіодом (наприклад, по закінченні певного терміну дії та/або отримання за допомогою даного ключа певного обсягу шифротекста) відповідно до вказівок відповідного вендора додатків або власника ключа і на підставі галузевих рекомендацій (наприклад, спеціальної публікації NIST 800-57), інструкцій (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.6.5. Вилучати з використання або змінювати ключі (архівація, знищення та/або скасування) за потреби, у випадку можливого порушення цілісності ключа (наприклад, звільнення співробітника, який володіє інформацією про компоненти ключа) та щодо яких існують підозри з їх компрометації (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.6.6. Якщо процедури управління ключами шифрування у відкритому вигляді здійснюються в ручному режимі, то такі процедури повинні координуватися з використанням принципу поділу знання та подвійного контролю (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.6.7. Виключити можливість здійснення несанкціонованої заміни криптографічного ключа (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.6.8. Визначити обов’язки і відповідальність працівників щодо зберігання і використання ключів з офіційним підтвердженням їх згоди з ознайомленням і прийняттям цих обов'язків та відповідальності під підпис (захід підпункту 5 пункту 9 розділу IV цього Положення).

17.7. Переконатися та забезпечити, що політики безпеки і процедури захисту даних платіжних карток, що зберігаються, документовані, використовуються і відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

18. Вимога 4: **Забезпечити шифрування даних платіжних карток при їх передачі через мережі загального користування.**

18.1. Використовувати стійку криптографію та безпечні протоколи для організації і забезпечення захисту конфіденційних даних платіжних карток під

час їх передачі через відкриті загальнодоступні мережі з урахуванням такого(захід підпункту 2 пункту 9 розділу IV цього Положення):

приймаються тільки довірені ключі та сертифікати;

використовується протокол, що підтримує тільки безпечні версії або конфігурації;

методи та алгоритми шифрування відповідають вимогам прийнятої методології шифрування.

Примітка: Перед використанням SSL/TLS Додаткові вимоги A2 мають бути виконані.

18.1.1. Забезпечити передачу даних платіжних карток через бездротові мережі або підключення до середовища даних платіжних карток з використанням кращих галузевих практик щодо стійкого шифрування для автентифікації і передачі даних (захід підпункту 2 пункту 9 розділу IV цього Положення).

18.2. Забороняється використовувати незахищені технології через персональну мережу обміну повідомлень для кінцевих користувачів під час передачі даних платіжних карток (електронна пошта, обмін миттєвими повідомленнями, SMS, чат тощо) (захід підпункту 2 пункту 9 розділу IV цього Положення).

18.3. Переконатися та забезпечити, що політики безпеки і процедури захисту для шифрування передачі даних платіжних карток документовані, використовуються і відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

19. Вимога 5: **Захист систем від небезпечного програмного забезпечення, регулярне оновлення антивірусного програмного забезпечення або програмного забезпечення.**

19.1. Забезпечити встановлення та налаштування антивірусного програмного забезпечення на всіх системах, що піддаються впливу небезпечного програмного забезпечення (зокрема, персональних комп’ютерів і серверів) (захід підпункту 2 пункту 9 розділу IV цього Положення).

19.1.1. Антивірусне програмне забезпечення повинно забезпечувати захист від всіх відомих видів небезпечного програмного забезпечення (захід підпункту 2 пункту 9 розділу IV цього Положення).

19.1.2. Для систем, для яких визнано, що вони не мають впливу небезпечного програмного забезпечення, і не мають антивірусного програмного забезпечення проводити періодичні перевірки з метою виявлення та оцінки можливих загроз щодо зараження небезпечним програмним забезпеченням для підтвердження того, що ці системи не потребують, як і раніше, антивірусного програмного забезпечення (захід підпункту 2 пункту 9 розділу IV цього Положення).

19.2. Забезпечити використання антивірусного програмного забезпечення наступним чином (захід підпункту 2 пункту 9 розділу IV цього Положення):

програмне забезпечення та бази даних повинні бути оновлені та актуальні;

постійно працює в активному режимі;

проводить періодичні сканування систем, захист яких забезпечує;

сформовані журнали аудиту зберігаються відповідно до вимоги пункту 27.7 цього Положення.

19.3. Антивірусне програмне забезпечення постійно працює в активному режимі і користувачі не можуть його ні відключити, ні змінити без явного дозволу, який видається керівництвом на кожен конкретний випадок і на обмежений період часу (захід підпункту 2 пункту 9 розділу IV цього Положення).

19.4. Переконатися та забезпечити, що політики безпеки і процедури захисту систем від небезпечного програмного забезпечення, регулярного оновлення антивірусного програмного забезпечення або програмного забезпечення документовані, використовуються і відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

20. Вимога 6: **Розробляти і підтримувати безпечні системи та додатки.**

20.1. Розробити та запровадити процес з виявлення вразливостей за допомогою авторитетних зовнішніх джерел інформації про уразливість та процес оцінки критичності, використавши такі дискретні ступені (градації): низький, середній, високий, для нещодавно виявлених вразливостей (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.2. Гарантувати, що всі системні компоненти та програмне забезпечення захищене від відомих вразливостей шляхом встановлення оновлень безпеки, випущених виробником. Оновлення безпеки повинні бути встановлені протягом місяця з моменту їх випуску виробником (захід підпункту 3 пункту 9 розділу IV цього Положення).

Примітка: Критичні оновлення безпеки повинні бути визначені відповідно до ступенів ризику, визначеним у п. 20.1.

20.3. Розробляти додатки для внутрішнього та зовнішнього використання (включаючи проектування та розробку адміністративного доступу до додатків через веб-інтерфейс) безпечно, з дотриманням таких вимог (захід підпункту 3 пункту 9 розділу IV цього Положення):

відповідно до вимог цього Положення (безпечна автентифікація та ведення журналів реєстрації подій тощо);

на основі галузевих стандартів та/або рекомендацій;

з урахуванням вимог з інформаційної безпеки протягом усього циклу розробки програмного забезпечення.

Примітка: дана вимога відноситься до будь-якого програмного забезпечення власної розробки і програмного забезпечення, розробленого третьою стороною.

20.3.1. Видалити всі облікові записи розробників, тестові облікові записи і/або додаткові облікові записи додатків, ідентифікатори користувачів і паролі перед передачею програмного забезпечення замовникам або введенням його в експлуатацію (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.3.2. Проаналізувати програмний код до передачі клієнту на предмет виявлення вразливостей, які можуть створювати ризик інформаційної безпеки, з урахуванням такого (захід підпункту 3 пункту 9 розділу IV цього Положення):

програмний код перевіряється окремими особами, відмінними від автора вихідного коду, і особами, що мають відповідні знання про методи аналізу програмного коду та захисту кодування;

результати аналізу програмного коду повинні давати гарантії, що код розроблений відповідно до інструкцій та методики безпечного програмування;

всі виправлення, які необхідно виконати, здійснені до передачі замовникам або введення в експлуатацію;

результати аналізу коду перевіряються та затверджуються керівництвом до релізу програмного забезпечення.

20.4. Запровадити процеси контролю і управління змінами, відслідкувати процедури з проведення змін для всіх компонентів системи, які повинні включати таке (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.4.1. Середовища розробки, тестування та виробничого функціонування програмного забезпечення повинні бути відокремлені один від одного (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.4.2. Розподіл обов'язків між розробкою/тестуванням та забезпеченням функціонування виробничого середовища (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.4.3. Виробничі дані (PAN клієнтів) не повинні використовуватися для тестування і розробки (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.4.4. Видалення тестових даних та облікових записів розробників з компонентів системи до введення системи у промислову експлуатацію (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.4.5. Процедури контролю і управління змінами повинні включати таке (захід підпункту 6 пункту 9 розділу IV цього Положення).

20.4.5.1. Документування впливу зміни на систему (захід підпункту 6 пункту 9 розділу IV цього Положення).

20.4.5.2. Затвердження керівництвом установи застосування змін (захід підпункту 6 пункту 9 розділу IV цього Положення).

20.4.5.3. Тестування виробничої функціональності. Метою тестування є підтвердження того, що зміни не містять негативного впливу на безпеку системи (захід підпункту 6 пункту 9 розділу IV цього Положення).

20.4.5.4. Здійснювати процедури резервування системи перед застосуванням змін або скасування зміни (захід підпункту 6 пункту 9 розділу IV цього Положення).

20.4.6. Після застосування змін вимоги цього Положення застосовуються на всіх нових або змінених системах і мережах, а також за потреби оновлюється документація (захід підпункту 6 пункту 9 розділу IV цього Положення).

20.5. Керувати поширенням вразливостей програмного коду в процесі розробки програмного забезпечення в такий спосіб (захід підпункту 3 пункту 9 розділу IV цього Положення):

проведення навчання розробників програмного забезпечення методикам безпечного програмування, включаючи методики з уникнення поширених програмних вразливостей та визначення способу зберігання критичних даних у пам'яті;

розроблення програмного забезпечення відповідно до основних принципів безпечного програмування.

Примітка: Вразливості, перераховані у вимогах 20.5.1 – 20.5.10 були актуальні відповідно до галузевих рекомендацій, що існували на момент затвердження цього Положення. Проте, у випадку оновлення галузевих рекомендацій з управління уразливими (таких, як OWASP, SANS CWE Top 25, CERT Secure Coding тощо) слід використовувати їх актуальні версії.

20.5.1. Ін’єкції, у частині SQL-ін’єкції, а також ін’єкції LDAP, XPath, команд операційної системи тощо (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.5.2. Переповнення буфера (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.5.3. Небезпечне криптографічне сховище (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.5.4. Небезпечна передача даних (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.5.5. Некоректне оброблення помилок (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.5.6. Усі уразливості з високим ступенем ризику, знайдені в процесі виявлення вразливостей (як це визначено в п. 20.1) (захід підпункту 3 пункту 9 розділу IV цього Положення).

Примітка: Пункти Положення 23.5.7-23.5.10, наведені нижче, поширюються на веб-додатки і інтерфейси додатків (зовнішні або внутрішні).

20.5.7. Міжсайтовий скриптинг (XSS) (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.5.8. Помилки в контролі доступу (наприклад, небезпечні прямі посилання на об'єкти, відсутність обмеження доступу по URL, обхід директорій і відсутність обмеження прав доступу користувача до функцій) (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.5.9. Підробка міжсайтових запитів (CSRF) (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.5.10. Протидія компрометації процедур автентифікації та управління сеансами (захід підпункту 3 пункту 9 розділу IV цього Положення).

20.5.11. Постійно управляти новими загрозами та вразливостями загальнодоступних веб-додатків, забезпечити додаткам захист від відомих атак у один з таких методів (захід підпункту 3 пункту 9 розділу IV цього Положення):

перевіряти загальнодоступні веб-додатки на наявність вразливостей з використанням методів ручного або автоматичного аналізу захищеності додатків один раз на рік, а також після внесення змін;

встановлювати автоматизований технічний засіб (наприклад, міжмережевий екран рівня веб-додатків) перед загальнодоступним веб-додатком для постійної перевірки всього трафіку з метою виявлення і попередження атаки.

20.6. Переконатися та забезпечити, що політики безпеки і процедури розробки для забезпечення безпеки систем і додатків документовані,

використовуються і відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

21. Вимога 7: **Обмежити доступ до даних платіжних карток відповідно до службової необхідності.**

21.1. Доступом до обчислювальних ресурсів і даних платіжних карток повинні володіти тільки ті співробітники, яким такий доступ необхідний для виконання їх посадових обов'язків (захід підпункту 4 пункту 9 розділу IV цього Положення).

21.1.1. Визначити права доступу для кожної посади окремо, включаючи (захід підпункту 4 пункту 9 розділу IV цього Положення):

системні компоненти та ресурси даних, доступ до яких необхідно для кожної посади для виконання посадових обов'язків;

необхідний рівень повноважень (користувач, адміністратор тощо) для надання доступу до ресурсів.

21.1.2. Надати користувачам облікових записів з широкими повноваженнями доступ тільки до тих повноважень, які необхідні їм для виконання своїх посадових обов'язків (захід підпункту 4 пункту 9 розділу IV цього Положення).

21.1.3. Призначати права доступу відповідно до функціональних ролей їх посад та їх посадових обов'язків (захід підпункту 4 пункту 9 розділу IV цього Положення).

21.1.4. Встановлення прав доступу повинно супроводжуватись відповідними документами, що погоджені уповноваженими особами, із зазначенням переліку необхідних повноважень (захід підпункту 4 пункту 9 розділу IV цього Положення).

21.2. Встановити систему (або системи) контролю доступу до системних компонентів, що обмежує доступ відповідно до службової необхідності користувача і яка налаштована забороняти все, що не дозволено (захід підпункту 4 пункту 9 розділу IV цього Положення).

Система контролю доступу повинна включати таке:

21.2.1. Охоплювати всі системні компоненти (захід підпункту 4 пункту 9 розділу IV цього Положення).

21.2.2. Призначення повноважень користувачам відповідно до їх посадових обов'язків (захід підпункту 4 пункту 9 розділу IV цього Положення).

21.2.3. За умовчанням забороняти будь-який доступ (захід підпункту 4 пункту 9 розділу IV цього Положення).

21.3. Переконатися та забезпечити, що політики безпеки і процедури обмеження доступу до даних платіжних карток документовані, використовуються і відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

22. Вимога 8: **Ідентифікувати і автентифікувати доступ до системних компонентів**.

22.1. Визначити та впровадити політики і процедури, що забезпечують належне проведення ідентифікації користувачів, які є працівниками установи, і

адміністраторів на всіх системних компонентах (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.1.1. Кожному користувачеві повинен бути призначений унікальний ідентифікатор до надання йому доступу до системних компонентів або даних платіжних карток (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.1.2. Контролювати створення, видалення і зміни ідентифікаторів користувачів, автентифікаційних даних та інших об'єктів ідентифікації (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.1.3. Здійснювати негайне скасування доступу при звільненні користувача (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.1.4. Проводити видалення/блокування неактивних облікових записів не рідше одного разу в 90 днів (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.1.5. Керувати обліковими записами, що використовуються сторонами для віддаленого доступу під час підтримки та обслуговування системних компонентів, у такий спосіб (захід підпункту 4 пункту 9 розділу IV цього Положення):

надавати доступ тільки на необхідний проміжок часу і обов’язково скасовувати, якщо не використовуються;

проводити моніторинг під час його використання.

22.1.6. Блокувати ідентифікатори облікових записів після шести невдалих спроб входу паролю підряд (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.1.7. Встановити період блокування облікового запису рівним 30 хвилинам або до його розблокування адміністратором (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.1.8. Блокувати неактивний сеанс через 15 хвилин з обов’язковою вимогою введення пароля користувача для розблокування, повторної активації терміналу або сеансу (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.2. Крім призначення унікального ідентифікатора, забезпечити належне управління автентифікацією користувачів, які є працівниками установи, і адміністраторів на рівні всіх системних компонентів, застосовуючи один з наступних методів автентифікації для всіх користувачів (захід підпункту 4 пункту 9 розділу IV цього Положення):

володіння інформацією (наприклад, пароль або парольна фраза);

володіння предметом (наприклад, ключі або смарт-картка);

володіння параметрами (наприклад, біометричні параметри).

22.2.1. Всі облікові дані для перевірки автентичності (наприклад, паролі/парольні фрази) зберігаються і передаються тільки в зашифрованому вигляді з використанням стійкої криптографії на всіх компонентах системи (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.2.2. Здійснювати перевірку ідентифікаційних даних користувача перед зміною будь-яких облікових даних (скидання паролю, надання нових токенів або генерації нових ключів тощо) для автентифікації (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.2.3. Паролі/парольні фрази повинні відповідати наступним вимогам (захід підпункту 4 пункту 9 розділу IV цього Положення):

наявність в паролі не менш семи символів;

наявність в паролі і цифр, і букв.

22.2.4. Зміна паролів/парольних фраз користувачів не рідше, ніж один раз на 90 днів (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.2.5. Заборонити користувачу змінювати пароль та/або парольну фразу на будь-який один з чотирьох попередніх паролів/парольних фраз користувача, що використані ним раніше (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.2.6. Забезпечити встановлення унікального початкового пароля/парольної фрази для кожного користувача та обов'язково вимагати їх змінювати при першому вході користувача в систему (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.3. Реалізувати процедуру надання неконсольного адміністративного доступу та віддаленого доступу при автентифікації в конкретній мережі, або в системному компоненті, з використанням технології багатофакторної автентифікації (захід підпункту 4 пункту 9 розділу IV цього Положення).

Використання одного фактору два рази (наприклад, введення двох окремих паролів) не є технологією багатофакторної автентифікації.

22.3.1. Забезпечити обов'язкове використання багатофакторної автентифікації для будь-якого неконсольного доступу при автентифікації в конкретній мережі, або в системному компоненті, для персоналу з правами адміністратора (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.3.2. Здійснювати застосування технології багатофакторної автентифікації до будь-якого віддаленого доступу у внутрішню мережу (користувачам, адміністраторам, в тому числі третім сторонам, що здійснюють підтримку або технічне обслуговування), що походить з зовнішньої мережі (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.4. Задокументувати та проінформувати всіх користувачів щодо процедур та політик автентифікації, включаючи (захід підпункту 4 пункту 9 розділу IV цього Положення):

рекомендації з вибору надійних облікових даних для автентифікації;

рекомендації для користувачів щодо захисту облікових даних для автентифікації;

інструкції з не використання раніше використаних паролів;

інструкції по зміні пароля в разі підозри його компрометації.

22.5. Забороняється використовувати групові, загальні та стандартні облікові записи і паролі, а також інші подібні методи автентифікації та забезпечити виконання таких вимог (захід підпункту 4 пункту 9 розділу IV цього Положення):

стандартні облікові записи заблоковані або видалені;

загальні облікові записи для системного адміністрування та інших критичних функцій відсутні;

загальні та стандартні облікові записи не використовуються для адміністрування будь-яких системних компонентів.

22.5.1. *Додаткові вимоги для постачальників послуг:* постачальники послуг, які мають віддалений доступ до приміщення клієнта (наприклад, для підтримки платіжних терміналів або серверів), зобов'язані використовувати унікальні облікові дані для автентифікації (наприклад, пароль та/або парольна фраза) для кожного клієнта (захід підпункту 4 пункту 9 розділу IV цього Положення).

22.6. У разі використання інших механізмів автентифікації (наприклад, фізичних або логічних токенів безпеки, смарт-карт, сертифікатів тощо), установа зобов’язана (захід підпункту 4 пункту 9 розділу IV цього Положення):

визначити механізми автентифікації для кожного облікового запису окремо, а не для кількох облікових записів відразу;

реалізувати фізичні та/або логічні заходи для отримання доступу у такий спосіб, щоб його міг використати тільки той користувач, для якого вони призначені.

22.7. Будь-який доступ до бази даних платіжних карток (включаючи доступ з боку додатків, адміністраторів, інших користувачів) повинен бути обмежений таким (захід підпункту 4 пункту 9 розділу IV цього Положення):

доступ, запити та операції з базами даних повинні здійснюватися з застосуванням програмних методів;

дозвіл на виконання запиту та прямий доступ до бази даних надається тільки адміністратору бази даних;

облікові записи додатків з управління базами даних можуть використовувати тільки додатки (не користувачі або інші процеси).

22.8. Переконатися та забезпечити, що політики безпеки і процедури ідентифікації та автентифікації доступу до системних компонентів задокументовані, використовуються і відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

23. Вимога 9: **Обмежити фізичний доступ до даних платіжних карток.**

23.1. Використовувати належні засоби контролю доступу до приміщень, для обмеження і контролю фізичного доступ до систем середовища даних платіжних карток (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.1.1. Застосовувати засоби відеоспостереження та/або інші технічні засоби з розмежування доступу для контролю кожного випадку фізичного доступу до критичних приміщень. Перевіряти зібрані дані і зіставляти їх з іншими даними. Зберігати ці дані не менше трьох місяців, якщо законодавством України не визначено інші обмеження (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.1.2. Впровадити механізми фізичного та/або логічного контролю для обмеження доступу до мережевих роз'ємів розташованих у загальнодоступних місцях (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.1.3. Обмежити фізичний доступ до бездротових точок доступу, шлюзів, портативних пристроїв, мережевого або комунікаційного обладнання та ліній зв’язку (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.2. Розробити процедури, що дозволяють однозначно розрізняти персонал установи та відвідувачів, з урахуванням такого (захід підпункту 5 пункту 9 розділу IV цього Положення):

ідентифікацію нових співробітників або відвідувачів;

вимоги зі внесення змін до прав доступу;

вилучення або блокування засобів ідентифікації у працівників об’єкта (установи) або засобів ідентифікації з вичерпаним терміном дії у відвідувачів об'єкта (установи).

23.3. Здійснювати контроль фізичного доступу працівників до критичних приміщень таким чином (захід підпункту 5 пункту 9 розділу IV цього Положення):

права доступу працівників затверджуються відповідно до функціональних ролей їх посад та їх посадових обов’язків;

скасувати доступ одразу після звільнення працівника, вилучити або блокувати всі засоби фізичного доступу (ключі, карти доступу тощо).

23.4. Запровадити процедури ідентифікації та авторизації відвідувачів (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.4.1. Надавати відвідувачам дозвіл на доступ перед їх входом до критичного приміщення, де обробляються або зберігаються дані платіжних карток, та постійно їх супроводжувати на час перебування їх в цих приміщеннях (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.4.2. Ідентифікувати відвідувача та видати йому засіб ідентифікації, що має обмеження терміну дії і дозволяє однозначно відрізнити відвідувача від співробітника установи (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.4.3. Вимагати від відвідувачів повернення виданого засобу ідентифікації при виході з об'єкту або при закінченні його терміну дії (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.4.4. Вести журнал реєстрації відвідувачів на вході до критичних приміщень та на вході до обчислювальних центрів і центрів з оброблення даних, де обробляються або зберігаються дані платіжних карток (захід підпункту 5 пункту 9 розділу IV цього Положення).

У журналі реєструвати ім’я відвідувача, установу, яку він представляє, а також співробітника установи, який дозволив надати відвідувачу доступ.

Журнал зберігати не менше трьох місяців, якщо інший термін не зазначено законодавством.

23.5. Забезпечити фізичну безпеку всіх типів носіїв інформації (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.5.1. Зберігати носії інформації з резервними копіями даних в безпечному місці, бажано в віддаленому підрозділі, наприклад, в альтернативному або резервному місці, або на території установи, що забезпечує безпечне зберігання. Організація безпеки місць зберігання перевіряється не рідше одного разу на рік (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.6. Організувати та забезпечувати контроль за переміщенням всіх типів носіїв інформації всередині установи та поза її межами (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.6.1. Класифікувати носії інформації в такий спосіб, який однозначно визначає рівень критичності збережених даних (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.6.2. Пересилання носіїв даних платіжних карток здійснювати тільки з довіреним кур'єром або у інший спосіб, який може бути проконтрольований та дозволяє відслідковувати пересилання (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.6.3. Будь-яке винесення носіїв інформації за межі установи (включаючи передачу носіїв приватним особам) здійснюється за дозволом керівництва (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.7. Забезпечити контроль за зберіганням носіїв інформації і управлінням доступу до них (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.7.1. Підтримувати в актуальному стані журнали інвентаризації всіх носіїв інформації. Інвентаризація носіїв інформації проводитися один раз на рік (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.8. Носії інформації, зберігання яких більше не потрібно для виконання завдань або вимог законодавства, знищуються в такий спосіб (захід підпункту 5 пункту 9 розділу IV цього Положення):

23.8.1. Методом фрагментарного подрібнення, спалювання або перетворення паперового носія в такий стан з якого дані платіжних карток неможливо відновити. Контейнери для матеріалів, приготованих для знищення, повинні бути захищені (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.8.2. Знищення даних платіжних карток на електронному носії здійснюється у такий спосіб, що однозначно виключає можливість їх відновлення (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.9. Забезпечити захист платіжних пристроїв, що обробляють дані платіжних карток шляхом прямої фізичної взаємодії з карткою, від фізичного втручання та підміни (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.9.1. Забезпечити складання списку платіжних пристроїв та підтримувати його в актуальному стані. Список повинен містити таку інформацію (захід підпункту 5 пункту 9 розділу IV цього Положення):

марку і модель платіжного пристрою;

опис місця знаходження платіжного пристрою (адреса установи або підрозділу, в якому знаходиться платіжний пристрій тощо);

серійний номер платіжного пристрою або інший унікальний ідентифікатор.

23.9.2. Періодично перевіряти платіжний пристрій на виявлення ознаки фізичного втручання або підміни (захід підпункту 5 пункту 9 розділу IV цього Положення).

23.9.3. Проводити навчання працівників щодо розпізнавання ознак фізичного втручання або підміни платіжних пристроїв (захід підпункту 5 пункту 9 розділу IV цього Положення). Навчати працівників такому:

перевіряти особистість будь-яких третіх осіб, що видають себе за ремонтників або фахівців техобслуговування, перед наданням їм доступу на внесення змін або усунення проблем з платіжними пристроями;

не встановлювати, не замінювати або не повертати платіжні пристрої без перевірки;

знати ознаки підозрілої поведінки поблизу платіжних пристроїв (спроби сторонніх осіб здійснити відключення або відкриття платіжного пристрою тощо);

інформувати керівництво або працівників служби безпеки про виявлені ознаки фізичного втручання або підміни платіжних пристроїв.

23.10. Переконатися та забезпечити, що політика безпеки і процедури щодо обмеження фізичного доступу до даних платіжних карток задокументовані, використовуються і відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

24. Вимога 10: **Контроль та відстеження будь-якого доступу до мережевих ресурсів і даних платіжних карток.**

24.1. Впровадити журнал реєстрації подій, що ведуться у автоматичному режимі та зв’язують будь-який доступ до системних компонентів з конкретним користувачем (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.2. Реалізувати автоматизовані журнали реєстрації подій на всіх системних компонентах, для фіксації таких подій (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.2.1. Всі сеанси персонального доступу користувача до даних платіжних карток (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.2.2. Всі дії, що вчинені будь-якою особою з повноваженнями суперкористувача (root) або з адміністративними повноваженнями (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.2.3. Доступ до всіх журналів реєстрації подій (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.2.4. Невдалі спроби логічного доступу (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.2.5. Використання та зміна засобів ідентифікації і автентифікації, включаючи, крім іншого, створення нових облікових записів, з підвищенням рівня повноважень, а також усі зміни з доповнення, видалення облікових записів здійснених з правами суперкористувача (root) або з адміністративними повноваженнями (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.2.6. Початок, зупинка або припинення ведення журналів реєстрації подій (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.2.7. Створення та видалення об'єктів системного рівня (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.3. Для кожної події кожного системного компонента записувати в журналах реєстрації подій мінімум такі параметри (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.3.1. Ідентифікатор користувача (захід № 4 підпункту 4 пункту 9 розділу IV цього Положення).

24.3.2. Тип події (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.3.3. Дата і час події (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.3.4. Кінцевий статус події: успішний або неуспішний (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.3.5. Джерело події (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.3.6. Ідентифікатор або назва даних системного компонента, або ресурсу, на які вплинула подія (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.4. Системні годинники та системний час на критичних системах повинні бути синхронізовані за допомогою механізмів синхронізації часу. Забезпечити виконання наступних вимог при отриманні, поширенні та зберіганні даних про час (захід підпункту 4 пункту 9 розділу IV цього Положення).

Примітка: Прикладом технології синхронізації є Протокол синхронізації часу (Network Time Protocol).

24.4.1. Встановити на критичних системах точний та узгоджений час (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.4.2. Дані про час повинні бути захищені (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.4.3. Отримання налаштувань часу здійснювати від загальновизнаних безпечних джерел (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.5. Журнали реєстрації подій повинні бути захищені від змін (захід підпункту 6 пункту 9 розділу IV цього Положення).

24.5.1. Обмежити доступ до журналів реєстрації подій тільки тим працівникам, яким такий доступ необхідний для виконання своїх посадових обов'язків (захід підпункту 6 пункту 9 розділу IV цього Положення).

24.5.2. Забезпечити захист журналів реєстрації подій від несанкціонованої модифікації або знищення (захід підпункту 6 пункту 9 розділу IV цього Положення).

24.5.3. Оперативно зберігати резервні копії журналів реєстрації подій на централізованому сервері реєстрації подій або на носії, де їх несанкціонована модифікація значно ускладнена (захід підпункту 6 пункту 9 розділу IV цього Положення).

24.5.4. Зберігати копії журналів реєстрації подій доступних з зовнішньої мережі технологій на безпечний і централізований внутрішній сервер протоколювання або носій (захід підпункту 6 пункту 9 розділу IV цього Положення).

24.5.5. Застосовувати програмне забезпечення з моніторингу цілісності файлів або виявлення змін у журналах реєстрації подій для виключення можливості зі внесення змін в існуючі дані журналів без автоматичного створення повідомлення. Проте додавання нових даних до журналу реєстрації подій не повинно створювати повідомлення (захід підпункту 6 пункту 9 розділу IV цього Положення).

24.6. Запровадити процедури перевірки журналів реєстрації подій і подій безпеки на всіх системних компонентів з метою виявлення підозрілої активності (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.6.1. Перевірка не рідше одного разу на день такого (захід підпункту 6 пункту 9 розділу IV цього Положення):

всіх подій безпеки;

журналів всіх системних компонентів, які здійснюють зберігання, оброблення або передачу даних платіжних карток і/або критичних автентифікаційних даних;

журналів всіх критичних компонентів системи;

журналів всіх серверів і системних компонентів, що виконують функції безпеки.

24.6.2. Періодично вивчати журнали інших системних компонентів на підставі політик і стратегії управління ризиками, яка визначається в рамках щорічної оцінки ризиків (захід підпункту 6 пункту 9 розділу IV цього Положення).

24.6.3. Вивчати виключення та підозрілу активність, що виявлені під час перевірки (захід підпункту 6 пункту 9 розділу IV цього Положення).

24.7. Зберігати журнали реєстрації подій не менше одного року, для оперативного доступу зберігати журнали не менше трьох місяців, якщо законодавством не накладені інші обмеження (захід підпункту 4 пункту 9 розділу IV цього Положення).

24.8. *Додаткові вимоги для постачальників послуг*: запровадити процес своєчасного виявлення та звітності щодо помилок в критичних системах управління безпекою, включаючи серед іншого помилки (захід підпункту 5 пункту 9 розділу IV цього Положення):

міжмережевих екранів;

систем виявлення та/або запобігання вторгнень;

систем моніторингу цілісності файлу;

антивірусного програмного забезпечення;

фізичних механізмів контроля доступу;

логічних механізмів контролю доступу;

механізмів ведення журналів реєстрації подій;

засобів сегментації (якщо вони використовуються).

24.8.1. *Додаткові вимоги для постачальників послуг:* запровадити процеси своєчасного реагування на виявленні інциденти безпеки будь-яких критично важливих системи безпеки. Процеси реагування на інциденти безпеки повинні містити таке (захід підпункту 5 пункту 9 розділу IV цього Положення):

відновлення функцій забезпечення безпеки;

визначення та документування тривалості (дати і часу початку і кінця) помилки в процесі забезпеченні безпеки;

визначення та документування причини (причин) помилки, включаючи початкову помилку, та документування необхідних заходів для усунення початкової помилки;

визначення та усунення будь-яких проблем безпеки, що виникли під час помилки;

виконання оцінки ризику для визначення того, які потрібно запровадити подальші дії щодо запобігання виникнення інциденту безпеки;

впровадження елементів управління для унеможливлення виникнення виявлених помилок у майбутньому;

відновлення моніторингу засобів контролю безпеки.

24.9. Переконатися та забезпечити, що політики безпеки і процедури для моніторингу будь-якого доступу до мережевих ресурсів та даних платіжних карток задокументовані, використовуються і відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

25. Вимога 11: **Регулярно проводити тестування систем та процесів безпеки.**

25.1. Запровадити процеси з щоквартальної перевірки наявності бездротових точок доступу (802.11) з метою виявлення та ідентифікації санкціонованих і несанкціонованих безпровідних точок доступу (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.1.1. Вести перелік санкціонованих бездротових точок доступу та документувати обґрунтування їх необхідності (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.1.2. Запровадити процедури реагування на інцидент з виявлення несанкціонованих безпровідних точок доступу (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.2. Проводити зовнішнє і внутрішнє сканування мережі на наявність вразливостей один раз в квартал, а також після внесення значних змін (установки нових системних компонентів, зміни топології мережі, зміни правил міжмережевих екранів, оновлення продуктів) (захід підпункту 2 пункту 9 розділу IV цього Положення).

25.2.1. Проводити щоквартальне внутрішнє сканування на наявність вразливостей та, у разі необхідності, повторні сканування доки не будуть усунуті всі виявленні вразливості, що мають високу ступінь ризику (згідно з визначенням наведеним у пункті 20.1 цього Положення). Сканування повинні виконувати кваліфіковані працівники (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.2.2. Проводити щоквартальне зовнішнє сканування на наявність вразливостей за допомогою постачальника послуг сканування. За необхідності проводити повторні сканування до досягнення позитивного результату сканування (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.2.3. Проводити внутрішнє і зовнішнє сканування та, у разі необхідності, проводити повторне сканування після будь-якої значної зміни в мережі. Сканування повинні виконувати кваліфіковані працівники (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.3. Впровадити методологію проведення тестування на проникнення, котра (захід підпункту 6 пункту 9 розділу IV цього Положення):

заснована на загальноприйнятих галузевих підходах до проведення тестування на проникнення;

охоплює весь периметр інформаційного середовища платіжних карток та критичні системи;

включає тестування мережі як ззовні, так і в всередині мережі;

включає тестування на наявність механізмів сегментації і зменшення охоплення;

вимагає включати у тести на проникнення на рівні додатку перевірку на наявність вразливостей, наведених у пункті 20.5;

вимагає включати у перелік тестів з проникнення на рівні мережі охоплення не тільки операційних систем, але й інших компонентів, що підтримують взаємодію на мережному рівні;

включає аналіз та оцінку загроз і вразливостей, виявлених за останні 12 місяців;

регламентує зберігання результатів тестів на проникнення та вжитих заходів щодо усунення виявлених вразливостей.

25.3.1. Проводити зовнішній тест на проникнення не рідше одного разу на рік, а також після модифікації або оновлення інфраструктури та додатків (оновлення операційної системи, додавання підмережі, установки веб-сервера тощо) (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.3.2. Проводити внутрішній тест на проникнення не рідше одного разу на рік, а також після модифікації або оновлення інфраструктури та додатків (оновлення операційної системи, додавання підмережі, установки веб-сервера тощо) (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.3.3. Після усунення небезпечних вразливостей, виявлених під час проведення тестування на можливість проникнення, провести повторне тестування для перевірки виправлень (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.3.4. Якщо використовується сегментація мережі для ізоляції даних платіжних карток від інших мереж, проводити тести на проникнення, щорічно і після будь-яких змін засобів та/або методів сегментації для підтвердження того, що методи сегментації дійсно ізолюють від інших мереж усі системи, які знаходяться в середовищі даних платіжних карток (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.3.5. *Додаткові вимоги для постачальників послуг*: якщо використовується сегментація, відповідність вимогам Положення підтверджується шляхом проведення тестування на проникнення засобів сегментації, як мінімум, кожні 6 місяців і після будь-якої зміни засобів та/або методів сегментації (захід підпункту 6 пункту 9 розділу IV цього Положення).

25.4. Використовувати методи виявлення та/або запобігання вторгнень для виявлення та/або запобігання вторгнень у мережу. Здійснювати моніторинг мережевого трафіку по периметру середовища даних платіжних карток та в критичних точках в межах середовища даних платіжних карток. Негайно інформувати працівників служби безпеки про підозрілі дії або інциденти (захід підпункту 2 пункту 9 розділу IV цього Положення).

Системи виявлення та запобігання вторгнень, їх сигнатури і бази даних, повинні підтримуватися в актуальному стані.

25.5. Впровадити механізм захисту від змін (моніторинг цілісності файлів, тощо) для забезпечення своєчасного інформування персоналу про несанкціоновані зміни критичних системних файлів, конфігураційних файлів і файлів даних. Порівняльний аналіз критичних файлів повинен проводитися не менше одного разу на тиждень (захід підпункту 5 пункту 9 розділу IV цього Положення).

25.5.1. Запровадити процес реагування на повідомлення/інциденти засобів захисту від змін (захід підпункту 5 пункту 9 розділу IV цього Положення).

25.6. Переконатися та забезпечити, що політики безпеки і процедури моніторингу, перевірки та контролю стану безпеки задокументовані, використовуються і відомі всім зацікавленим особам (захід підпункту 6 пункту 9 розділу IV цього Положення).

26. Вимога 12: **Підтримувати політику інформаційної безпеки для всіх працівників**.

26.1. Розробити та поширити політику безпеки, що підтримується в актуальному стані (захід № 6 підпункту 6 пункту 9 розділу IV цього Положення).

26.1.1. Політика безпеки повинна переглядатися щорічно та оновлюватися в разі зміни умов функціонування інформаційного середовища установи (заходи підпунктів 1 – 6 пункту 9 розділу IV цього Положення).

26.2. Запровадити процес оцінки ризиків, який (захід підпункту 6 пункту 9 розділу IV цього Положення):

здійснюється один раз на рік або після значних змін інформаційного середовища установи;

виявляє критичні активи, загрози і вразливості;

завершується формалізованим і документованим аналізом оцінки ризиків.

26.3. Розробити політики експлуатації критичних технологій, з якими безпосередньо працюють відповідальні працівники, визначити безпечні правила щодо використання цих технологій. Політики повинні передбачати таке (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.3.1. Процедуру погодження з боку уповноважених осіб (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.3.2. Автентифікацію перед використанням критичної технології (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.3.3. Перелік всіх засобів, що використовують критичні технології, та працівників, що мають доступ до цих засобів (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.3.4. Процедуру, яка надає можливість однозначно та оперативно визначити власника, його контактні дані та призначення пристрою критичної технології (шляхом маркування, кодування та/або інвентаризації пристроїв тощо) (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.3.5. Дозволені способи використання технологій (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.3.6. Дозволені місця розміщення технологій в мережі (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.3.7. Погоджений з боку уповноважених осіб установи перелік дозволених до використання продуктів (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.3.8. Автоматичне відключення сесій віддаленого доступу після певного періоду простою (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.3.9. Включення механізмів віддаленого доступу для вендорів і ділових партнерів тільки в разі потреби такого доступу, з негайним його вимкненням після завершення використання (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.3.10. Заборону копіювання, переміщення та зберігання даних платіжних карток на локальних жорстких дисках і змінних електронних носіях працівникам, які мають доступ до даних платіжних карток через технології віддаленого доступу, якщо вони не мають відповідних повноважень для виконання цих дій у межах певної службової необхідності.

При наявності підтвердженої службової необхідності політики використання повинні вимагати захищати дані відповідно до вимог Положення (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.4. Політика та процедури безпеки повинні однозначно визначати обов'язки щодо забезпечення інформаційної безпеки для всіх працівників установи (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.4.1. *Додаткові вимоги для постачальників послуг*: Керівництво учасника повинно встановити відповідальність за недотримання вимог з захисту даних платіжних карток та запровадити програму щодо дотримання вимог Положення, яка повинна включати таке (захід підпункту 6 пункту 9 розділу IV цього Положення):

загальну відповідальність за дотримання вимог Положення;

визначення статуту програми забезпечення відповідності вимогам Положення та комунікації та/або взаємодії з виконавчим керівництвом.

26.5. Визначеному відповідальному працівнику або групі відповідальних працівників призначити обов'язки з управління інформаційною безпекою, які мають включати такі функції, але не обмежуючись ними (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.5.1. Розроблення, документування та поширення політики і процедур безпеки (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.5.2. Моніторинг і аналіз повідомлень та інформації про події, що мають відношення до безпеки, інформування відповідних працівників (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.5.3. Розроблення, документування та поширення процедур з реагування на інциденти інформаційної безпеки, процедур ескалації для забезпечення своєчасного та ефективного опрацювання і управління всіма ситуаціями (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.5.4. Адміністрування облікових записів користувачів, включаючи їх додавання, видалення та зміну (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.5.5. Моніторинг та контроль будь-якого доступу до даних (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.6. Розробити та впровадити програму навчання та перевірки знань з питань безпеки даних платіжних карток для всього персоналу з метою забезпечення обізнаності персоналу щодо вимог політики безпеки даних платіжних карток (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.6.1. Навчання відповідальних працівників повинно проводитися при їх прийомі на роботу, а також не менше одного разу на рік (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.6.2. Працівники не менше одного разу на рік повинні підтверджувати свої знання та розуміння політики і процедур з інформаційної безпеки (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.7. Здійснювати перевірку кандидатів (майбутній персонал) при прийомі на роботу для мінімізації ризику внутрішніх атак (захід підпункту 6 пункту 9 розділу IV цього Положення).

Кадрові перевірки можуть проводитись за такими напрямками: вивчення послужного списку, записів правоохоронних органів, кредитної історії, перевірки рекомендацій з попередніх місць роботи тощо.

Для кандидатів на певні посади, такі як, наприклад, касир, які мають доступ лише до одного номеру платіжної картки, тільки в момент проведення трансакції, ця вимога носить рекомендаційний характер.

26.8. Впровадити та підтримувати наступні політики і процедури взаємодії з постачальниками послуг, які мають доступ до даних платіжних карток або котрі можуть вплинути на безпеку даних платіжних карток (захід підпункту 2 пункту 9 розділу IV цього Положення).

26.8.1. Ведення списку постачальників послуг з додаванням опису послуг, які ними надаються (захід підпункту 2 пункту 9 розділу IV цього Положення).

26.8.2. Укладання та підтримка письмової угоди, в якій постачальники послуг підтверджують, що вони несуть відповідальність за безпеку даних платіжних карток, які вони зберігають, обробляють або передають від імені клієнта, або несуть відповідність в тій мірі, в якій вони можуть впливати на безпеку середовища даних платіжних карток клієнта (захід підпункту 2 пункту 9 розділу IV цього Положення).

26.8.3. Процес залучення постачальників послуг, який включає в собі перевірку благонадійності, що проведений до початку робіт з постачальником послуг (захід підпункту 2 пункту 9 розділу IV цього Положення).

26.8.4. Підтримку процедури з відстеження статусу відповідності постачальника послуг вимогам Положення не менше одного разу на рік (захід підпункту 2 пункту 9 розділу IV цього Положення).

26.8.5. Складання та підтримка інформації в актуальному стані про те, за які вимоги Положення несе відповідальність кожен постачальник послуг, а за які

несе відповідальність установа (захід підпункту 2 пункту 9 розділу IV цього Положення).

26.9. *Додаткова вимога для постачальників послуг*: постачальники послуг повинні письмово підтверджувати, що вони відповідають за безпеку даних платіжних карток, які вони зберігають, обробляють або передають від імені клієнта, або відповідають в тій мірі, в якій вони можуть впливати на безпеку інформаційного середовища даних платіжних карток клієнта (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.10.Впровадити план реагування на інциденти безпеки. Установа повинна у найкоротший термін реагувати на порушення безпеки в роботі системи (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.10.1. Розробити план реагування на інциденти безпеки, що застосовується у випадку порушення безпеки системи (захід підпункту 6 пункту 9 розділу IV цього Положення).

План повинен містити:

ролі, обов'язки, порядок оповіщення, алгоритм встановлення контактів в разі компрометації даних;

процедури реагування на інциденти;

процедури відновлення і забезпечення безперервності установи;

процеси резервного копіювання даних;

процедури щодо сповіщення про факти компрометації;

охоплення всіх критичних компонентів системи.

26.10.2. Здійснювати перегляд і тестування плану, включаючи всі елементи, що зазначені в пункті 26.10.1, один раз на рік (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.10.3. Призначити відповідний персонал, який забезпечить реагування на повідомлення цілодобово та без вихідних (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.10.4. Працівники, що відповідальні за реагування на порушення безпеки, повинні бути навчені належним чином (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.10.5. План повинен включати в себе процедури реагування на попередження систем моніторингу безпеки, включаючи серед іншого, системи виявлення та запобігання вторгнень, міжмережевих екранів, а також системи моніторингу цілісності файлів (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.10.6. Розробити процес зміни та удосконалення плану реагування на інциденти відповідно до отриманого досвіду та розробок в галузі безпеки даних платіжних карток (захід підпункту 6 пункту 9 розділу IV цього Положення).

26.11. *Додаткові вимоги для постачальників послуг*: здійснювати щоквартальні перевірки того, як працівники дотримуються вимог політики безпеки і операційних процедур. Звіти за результатами перевірки повинні охоплювати такі процеси (захід підпункту 6 пункту 9 розділу IV цього Положення):

щоденну перевірку журналів реєстрації подій;

перевірку правил міжмережевих екранів;

застосування стандартів конфігурацій для нових систем;

реагування на повідомлення або попередження з безпеки;

процеси управління змінами.

26.11.1. *Додаткові вимоги для постачальників послуг*: вести документацію щодо квартальної перевірки, яка містить таке (захід підпункту 6 пункту 9 розділу IV цього Положення):

документування результатів перевірки;

перевірка та врахування результатів здійснюється працівником, відповідальним за виконання програми відповідності вимогам цього Положення.

27. Додаткові вимоги A1: **Для постачальників послуг віртуального хостингу.**

27.1. Забезпечити захист середовища і даних розміщених на віртуальному хостингу кожної установи.

27.2. Гарантувати, що кожна установа використовує тільки ті процеси, у яких є доступ до її середовища даних платіжних карток.

27.2.1. Обмежити доступ і повноваження кожної установи тільки її власним середовищем даних платіжних карток.

27.2.2. Переконатися, що ведення журналів з реєстрації подій включено, а самі журнали є унікальними для кожного середовища даних платіжних карток кожної установи і відповідають вимогам пункту 29.

27.2.3. Впровадити процеси, що дозволяють провести своєчасне розслідування в разі компрометації будь-яких торговельно-сервісних підприємств або постачальника послуг, розміщених на хостингу.

28. Додаткові вимоги A2: **Для установи, що використовують SSL та/або попередні версії TLS.**

28.1. У тих випадках, коли використовуються SSL та/або попередні версії TLS на платіжний термінал/мобільний платіжний термінал (і місця термінації SSL та/або TLS, з якими вони з’єднуються), установа повинна застосувати будь-який один з таких заходів:

підтвердити, що платіжні пристрої не містять відомі вразливості для цих протоколів;

мати затверджений в установі план зі зменшення впливу ризиків та міграції на безпечні версії протоколу.

28.2. Установи з існуючими рішеннями відмінними від дозволених у пункті 28.1, які використовують SSL та/або попередні версії TLS, повинні мати затверджений в установі план зі зменшення впливу ризиків та міграції на безпечні версії протоколу.

28.3. *Додаткові вимоги A2 тільки для постачальників послуг*: постачальник послуг повинен забезпечувати підтримку безпечних протоколів.

VII. Методи протидії шахрайству

29. Опис системи безпеки емітента в ПРОСТІР повинен складатися з таких документів.

1) Затверджений керівництвом банку порядок емісії платіжних карток. Порядок емісії платіжних карток повинен визначати запропоновані банком продукти платіжних карток та їх користувачів, допустимі ризики, процедури оброблення заяв клієнтів, доставку та видачу платіжних карток клієнтам банку, апаратно-програмні засоби та заходи захисту банку з протидії шахрайству, розподіл відповідальності між підрозділами банку та дії персоналу і керівництва у випадку виявлення атаки/інцидентів безпеки.

2) Затверджені процедури приймання/оброблення заяв від клієнтів, доставки та видачі платіжних карток і критичних автентифікаційних даних клієнтам банку, повторного випуску платіжної картки, знищення невиданих платіжних карток.

3) Механізми безпечної персоналізації платіжних карток банку.

4) Процедури проведення перевірок параметрів платіжної картки, її держателя та операцій автентифікації в системах проведення трансакції.

5) Процедури блокування/розблокування платіжних карток банку.

6) Процедури забезпечення інформаційної безпеки при обробці даних платіжних карток та інформації, яка містить комерційну/банківську таємницю.

7) Процедури взаємодії у разі виявлення несанкціонованих дій з використанням платіжних карток.

30. Заходи безпеки емітента в ПРОСТІР.

1) Здійснювати випуск нових платіжних карток у неактивному стані. Активація платіжної картки здійснюється клієнтом у відділеннях банку та /або будь-якому платіжному пристрої, який належить емітенту, або за допомогою телефонного дзвінка з використанням кодового слова.

2) Процедури з випуску нових платіжних карток банку на заміну скомпрометованих.

3) Застосування сучасних технологій, що дозволяють підвищити безпеку процедур автентифікації держателя платіжної картки (багатофакторна автентифікація тощо).

4) Застосування систем моніторингу трансакцій, що дозволяють виявити операції, які викликають підозру з точки зору шахрайських операцій.

5) Оповіщення держателя платіжної картки про операції, що проводяться по його рахунку, за допомогою смс-повідомлення та інших наявних засобів інформування.

6) Використання дистанційного банківського обслуговування мобільного/інтернет банкінгу, який дозволить держателю платіжної картки здійснювати операції з розблокування платіжної картки перед проведенням трансакції та заблокувати її після використання.

7) Проведення навчання працівників банку для подальшого інформування клієнтів банку щодо безпечного використання платіжних карток.

31. Заходи з запобігання використанню викрадених/втрачених платіжних карток.

1) Блокування платіжних карток у системі емітента у разі їх викрадення/втрати.

2) Включення викрадених/загублених платіжних карток до стоп-листів.

32. Заходи з протидії операціям за невиданими платіжними картками.

1) Процедури знищення невиданих платіжних карток.

2) Включення невиданих платіжних карток до стоп-листів до моменту знищення або видачі.

3) Використання системи моніторингу трансакцій для виявлення операцій з невиданими платіжними картками.

33. Заходи з запобігання використання підроблених платіжних карток.

1) Генерація номерів платіжних карток у випадковому порядку.

2) Перевірка терміну дії платіжної картки.

3) Перевірка в системі емітента коду перевірки достовірності платіжної картки.

4) Ведення стоп-листів підроблених платіжних карток.

VIII. Документування процесу захисту даних платіжних карток

34. Учасник ПРОСТІР проводить планові та позапланові перевірки стану організації захисту даних платіжних карток.

35. Результати перевірки стану організації захисту даних платіжних карток в установі, відображається в акті, який складається у довільній формі.

36. Перевірка стану організації захисту даних платіжних карток проводяться один раз на рік.

Директор Департаменту безпеки	О. А. Скомаровський
Заступник директора департаменту-начальник управління безпеки інформації Департаменту безпеки	А. М. Кудін
Начальник відділу проектування і розробки перспективних систем захисту банківської інформації та електронних платіжних систем управління безпеки інформації Департаменту безпеки	С. Т. Іванишин
Старший інженер відділу проектування і розробки перспективних систем захисту банківської інформації та електронних платіжних систем управління безпеки інформації Департаменту безпеки	В. О. Куліш