INTELLIGENT ESTIMATION AND PREDICTIVE MINIMIZATION OF DELAYS IN SERVERLESS PLATFORMS BASED ON HYBRID NEURAL NETWORK ARCHITECTURE CNN-LSTM

The article investigates the problem of cold start in Serverless platforms as one of the main reasons for the deterioration of service quality indicators under conditions of uneven and dynamic load. This problem is particularly difficult for Function-as-a-Service environments, where the stochastic nature of function calls and the presence of periods of inactivity lead to significant delays in the initialization of the computing context. Traditional heuristic resource management policies, in particular fixed timeouts or reactive scaling, often prove ineffective under conditions of sharp load surges. An approach to predictive resource management of Serverless platforms based on a hybrid CNN–LSTM neural network architecture designed to predict the intensity of function calls is proposed. Convolutional neural networks are used to highlight local patterns and short-term peaks in the load time series, while recurrent LSTM blocks provide modeling of long-term time dependencies. The obtained forecasts are used to implement a predictive pre-warming mechanism, which allows to activate computing resources in advance and minimize cold start delays. Experimental research was conducted on real Azure Functions execution routes using scenarios of uneven load and periods of inactivity. The experimental results showed that the proposed CNN–LSTM model provides a 29.3% reduction in the mean square prediction error compared to the standard LSTM and allows to reduce the number of cold starts by an average of 32.4%. The obtained results confirm the feasibility of using hybrid neural network approaches to improve the efficiency and quality of service in modern Serverless systems.

Keywords: serverless computing, Cold Start, CNN-LSTM, load forecasting, Function-as-a-Service, pre-warming, deep learning.

Надійшла до редакції (Received): 20.04.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

УДК 004.056.5:[004.7:336.717 DOI: 10.31673/2409-7292.2026.029908

Кухарська Наталія Павлівна
кандидат фізико-математичних наук, доцент, доцент кафедри безпеки інформаційних технологій
Національний університет “Львівська політехніка”, Львів, Україна
ORCID: 0000-0002-0896-8361
E-mail: nataliia.p.kukharska@lpnu.ua

Полотай Орест Іванович
кандидат технічних наук, доцент, доцент кафедри управління інформаційною безпекою
Львівський державний університет безпеки життєдіяльності, Львів. Україна
ORCID: 0000-0003-4593-8601
E-mail: orest.polotaj@gmail.com

Павлюк Остап-Йосип Сергійович
здобувач першого (бакалаврського) рівня вищої освіти за спеціальністю 125 “Кібербезпека”
Національний університет “Львівська політехніка”, Львів, Україна
ORCID: 0009-0003-7250-9367
E-mail: ostap-iosyp.pavliuk.kb.2022@lpnu.ua

СИСТЕМНІ АСПЕКТИ ПІДГОТОВКИ ОРГАНІЗАЦІЙ ДО ПРОВЕДЕННЯ АУДИТУ НА ВІДПОВІДНІСТЬ ВИМОГАМ PCI DSS

У статті розглянуто організаційні та практичні аспекти забезпечення готовності організацій до аудиту PCI DSS. Обґрунтовано доцільність сприйняття процесу підтвердження відповідності вимогам стандарту не як формальної щорічної процедури, а як безперервного процесу управління інформаційною безпекою. Проаналізовано типові проблеми, що виникають під час аудиту, зокрема помилки у визначенні сфери застосування, недостатній рівень документування процедур та нерегулярність виконання контрольних заходів. У роботі систематизовано основні етапи аудиту, що проводиться кваліфікованим оцінювачем безпеки (QSA), та визначено ключові напрями підготовки організації до зовнішнього оцінювання або самооцінювання. Окрему увагу приділено питанням оптимізації сфери середовища даних власників карток (CDE), проведенню аналізу

© Криворучко В. Ф., Садовенко В. С. Інтелектуальне оцінювання та предиктивна мінімзація затримок у serverless-платформах на основі гібридної нейромережевої архітектури CNN-LSTM. Сучасний захист інформації, 2(66), 88–95. https://doi.org/10.31673/2409-7292.2026.028607

прогалин, впровадженню коригувальних заходів і забезпеченню регулярних операційних процедур у період огляду. Розкрито значення документування процесів, розподілу відповідальності та інтеграції вимог стандарту у повсякденну діяльність організації. Визначено роль внутрішніх перевірок і пробного аудиту як інструментів попереднього виявлення невідповідностей та мінімізації ризиків негативного результату оцінювання. Показано, що комплексний підхід до підготовки та підтримання відповідності вимогам PCI DSS сприяє зниженню ризику інцидентів безпеки, мінімізації фінансових і репутаційних втрат, а також зміцненню довіри клієнтів і партнерів. Отримані результати можуть бути використані організаціями, які обробляють дані платіжних карток, для підвищення ефективності процесу підготовки до аудиту та забезпечення сталої відповідності стандарту.

Ключові слова: управління інформаційною безпекою, PCI DSS, захист платіжних даних, зовнішній аудит, самооцінювання, середовище даних власників карток.

Вступ

Організації, які обробляють, передають та/або зберігають дані власників платіжних карток – торговці (merchants) та постачальники послуг (service providers) – зобов'язані дотримуватися PCI DSS. PCI DSS (Payment Card Industry Data Security Standard) – це комплексний міжнародний стандарт безпеки [1], розроблений та впроваджений провідними платіжними системами: Visa International, MasterCard Worldwide, American Express, JCB, Discover та Diner's Club.

Метою стандарту є зниження ризиків витоку платіжної інформації та запобігання її несанкціонованому використанню на шкоду власникам карток і банкам-емітентам.

Дотримання вимог PCI DSS є обов'язковим для банківських установ, процесингових центрів, інтернет-магазинів, платіжних сервісів, підприємств сфери HoReCa (готелі, ресторани, кафе), туристичних компаній, торговельних мереж і ритейлерів, а також для дата-центрів і хостинг-провайдерів, які забезпечують обробку та/або зберігання даних платіжних карток своїх клієнтів.

В Україні вимоги стандарту PCI DSS інтегровані у нормативно-правову базу платіжного ринку. Зокрема, Національний банк України закріпив їх у власних регуляторних актах (у тому числі Постановою № 95 від 2017 року та подальшими змінами), що регламентують діяльність операторів платіжної інфраструктури та надавачів платіжних послуг. Підтвердження відповідності організації вимогам PCI DSS проводиться щорічно через аудит QSA (Qualified Security Assessor) або заповнення анкети самооцінювання (Self-Assessment Questionnaire, SAQ). Ймовірність залучення кваліфікованого зовнішнього аудитора, зазвичай, зростає зі збільшенням обсягу оброблюваних транзакцій, а також у разі виявлення інцидентів безпеки або порушень вимог стандарту. Організація залишається відповідальною за забезпечення дотримання вимог PCI DSS навіть у тому випадку, коли вона свої платіжні операції або управління середовищем даних власників платіжних карток (Cardholder Data Environment, CDE) передає на аутсорсинг сторонньому постачальнику послуг. Суб'єкти, які зобов'язалися дотримуватися вимог стандарту на договірних засадах, також мають підтверджувати свою відповідність шляхом щорічного заповнення анкети самооцінювання або проходження аудиту.

Для визначення необхідних заходів щодо дотримання вимог PCI DSS організація повинна звернутися до фінансової установи-еквайра (у разі виконання ролі торговця) або до відповідних платіжних брендів (у разі виконання ролі постачальника послуг). Незалежно від встановлених вимог щодо валідації відповідності, процес підтвердження відповідності PCI DSS доцільно розглядати не лише як формальну обов'язкову процедуру, а як інструмент підвищення рівня безпеки. Дотримання вимог стандарту сприяє зниженню ризику порушень інформаційної безпеки та мінімізації операційних, фінансових і репутаційних втрат, пов'язаних з інцидентами [2-3].

Згідно зі звітом компанії A-LIGN щодо контрольних показників відповідності за 2025 рік, 69 % респондентів віднесли аудит PCI DSS до числа найбільш поширених видів аудиту [4]. Водночас, менше ніж 50 % організацій, за даними Verizon, спроможні стабільно з року в рік підтримувати повну відповідність вимогам PCI DSS [5].

У зв'язку з цим метою статті є систематизувати ключові аспекти підготовки організації до аудиту на відповідність вимогам PCI DSS, проаналізувати типові проблеми забезпечення відповідності та визначити основні етапи підготовчого процесу, що дасть змогу сформувати цілісне уявлення про процедуру аудиту та підвищити рівень готовності організації до проходження оцінювання.

Матеріали та методи дослідження

Інформаційною базою роботи є стандарт PCI DSS версії 4.0 та технічна документація щодо методів валідації відповідності. У процесі дослідження було опрацьовано результати критичного аналізу впровадження стандарту, що містять дані про історичний розвиток фреймворку та статистику безпекових інцидентів у сертифікованих організаціях [6-7]. Також використано офіційні настанови щодо класифікації торговців (merchants) та звіти про ефективність методів оцінки, таких як опитувальники самооцінювання (SAQ) та звіти про відповідність (ROC).

Методологічну основу дослідження склали загальнонаукові методи пізнання. Системний підхід застосовано для вивчення структури дванадцяти основних вимог стандарту та шести цілей контролю. Метод аналізу використано для вивчення причин виникнення вразливостей у компаніях із чинним статусом відповідності. Шляхом логічного узагальнення було розроблено практичні рекомендації щодо підготовки організацій до аудиту, які спрямовані на перехід від формальної відповідності вимогам PCI DSS до забезпечення реальної стійкості платіжної інфраструктури.

Аналіз останніх досліджень і публікацій

Сучасний стан нормативного регулювання інформаційної безпеки характеризується завершенням циклу оновлення ключових галузевих стандартів. Зокрема, у жовтні 2022 року було представлено нові редакції міжнародних стандартів ISO/IEC 27001 [8] та ISO/IEC 27002 [9], у яких оптимізовано структуру заходів контролю. Детальний аналіз внесених змін було проведено нами у попередньому дослідженні [10].

Паралельно з цим індустрія платіжних карток здійснила масштабний перехід на PCI DSS версії 4.0. Авторами роботи [11] проаналізовано оновлені вимоги стандарту та проведено їх порівняльне зіставлення з попередньою версією 3.2.1. Важливо підкреслити, що з 1 квітня 2024 року версія 3.2.1 остаточно втратила чинність, що робить питання переходу на нові механізми підтвердження відповідності пріоритетним завданням аудиту.

У статті [12] досліджено стратегію впровадження PCI DSS у платіжних шлюзах, які визначено як критичні вузли захисту даних під час транзакцій. Автор розглядає технічні та операційні аспекти безпеки через призму дванадцяти фундаментальних вимог стандарту, акцентуючи увагу на важливості системного підходу. У роботі обґрунтовано, що забезпечення відповідності є не лише технічним завданням, а складним організаційним процесом, спрямованим на створення стійкої екосистеми оброблення платіжних даних.

Дослідження [6] висвітлює еволюцію стандарту від розрізнених корпоративних програм до уніфікованого світового фреймворку. Водночас автори вказують на критичний розрив між формальною валідацією відповідності та реальним рівнем захищеності. На прикладі різних рівнів торговців доведено, що успішне проходження сертифікації не завжди гарантує захист від складних кібератак, про що свідчать резонансні витоки даних у компаніях із чинними статусами відповідності.

На підтвердження цієї тези у статті [7] представлено результати системного тестування процесу сертифікації на базі спеціально розробленого модельованого середовища (BUGGYCART) з контрольованими вразливостями. Експериментально встановлено, що жоден із протестованих сертифікованих сканерів (ASV) не здатний виявити всі наявні загрози. З огляду на виявлені розбіжності між задокументованими контролями та їхньою практичною ефективністю, виникає потреба у детальному описі структурованого алгоритму проведення аудиту та наданні практичних рекомендацій. Це дозволить організаціям системно

підготуватися до перевірки, забезпечивши перехід від формального підтвердження відповідності до побудови системи безперервної безпеки платіжних даних.

Найпоширеніша проблема під час аудиту

Перед детальним розглядом процедури аудиту доцільно звернути увагу на найбільш поширену, пов'язану з PCI DSS проблему. Відповідність стандарту сприймається часом організаціями як разова щорічна подія, а не як безперервний процес, що охоплює сукупність регулярних операційних заходів. Саме такий підхід часто стає першопричиною більшості недоліків, виявлених під час аудиту.

Найефективнішим способом уникнення цієї помилки є проведення періодичних внутрішніх перевірок (у тому числі позапланових), які можуть здійснюватися і за участю зовнішнього аудитора. Особливу увагу під час таких перевірок доцільно зосередити на сферах, у яких найчастіше виникають порушення вимог стандарту, а саме:

- документація – наявність повного комплекту документів та відповідність їх змісту актуальним вимогам стандарту;
- аутсорсинг – перевірка того, чи сторонні постачальники послуг, які залучаються до обробки платіжних даних, відповідають вимогам PCI DSS (зокрема у випадках, коли вони приймають карткові платежі від інших організацій);
- регулярні операційні процедури – виконання стандартних для бізнесу дій, таких як аналіз журналів подій та тестування безпеки, з періодичністю, визначеною стандартом PCI DSS, і на належному рівні якості.

Проведення регулярних перевірок сприяє формуванню розуміння того, що дотримання вимог PCI DSS є безперервним процесом та дає змогу переконатися у коректності впроваджених заходів безпеки. Такі перевірки є також гарною нагодою для отримання консультацій з деяких питань, наприклад, чи потрібно проводити тестування на проникнення після змін, внесених в інформаційну інфраструктуру або чи впливає залучення сторонніх постачальників послуг на рівень відповідності вимогам PCI DSS. Відповіді на подібні запитання доцільно отримувати у письмовій формі з метою формування аудиторського журналу. Важливим чинником інтеграції вимог PCI DSS у повсякденну діяльність організації є чітке документування обов'язків і процесів. Закріплення відповідальності за конкретні заходи за визначеними працівниками підвищує ймовірність їх своєчасного виконання та контролю за дотриманням установлених термінів. Наявність формалізованих і задокументованих процедур забезпечує методичне керівництво для персоналу, а встановлення вимоги щодо затвердження керівництвом окремих видів діяльності або їх результатів сприяє інтеграції процесів відповідності у стандартні операційні процеси організації. Окрему увагу необхідно приділяти плануванню щорічних заходів з підтвердження відповідності. Зокрема, слід забезпечити завчасне до початку офіційного аудиту завершення сканувань на вразливості та тестувань на проникнення. Це дасть змогу усунути виявлені недоліки та, за потреби, провести повторні перевірки перед офіційним залученням зовнішнього аудитора.

Процес аудиту. Опишемо процес аудиту, який здійснює кваліфікований оцінювач безпеки (Qualified Security Assessor, QSA) – акредитований незалежний аудитор, сертифікований Радою зі стандартів безпеки індустрії платіжних карток (PCI Security Standards Council) для проведення оцінювання відповідності вимогам PCI DSS.

Метою такого огляду є сформувати розуміння етапів аудиту та значення підготовчих дій, які розглядатимемо далі.

Вступна зустріч з керівництвом

Процес аудиту, зазвичай, розпочинається з вступної наради з представниками керівництва організації. QSA роз'яснює основні аспекти проведення аудиту, погоджує формат взаємодії із персоналом (наприклад, шляхом проведення співбесід). На цьому етапі на загальному рівні домовляються про обсяг аудиту для забезпечення єдиного розуміння обома сторонами його меж та цілей.

© Кухарська Н. П., Полотай О. І., Павлюк О.-Й. С. Системні аспекти підготовки організацій до проведення аудиту на відповідність вимогам PCI DSS. Сучасний захист інформації, 2(66), 95–105. https://doi.org/10.31673/2409-7292.2026.029908

Збір та аналіз документації

З метою формування доказової бази QSA здійснює збір та аналіз документації, що підтверджує відповідність організації вимогам PCI DSS, зокрема:

- політик, процедур і регламентів безпеки;
- схем мережевої інфраструктури та потоків даних;
- звітів про сканування вразливостей та тестування на проникнення;
- записів контрольних заходів (журналів моніторингу, матеріалів внутрішнього аудиту);
- підтверджень відповідності (Attestation of Compliance, AoC) від постачальників послуг, що входять до сфери аудиту;
- звіту про відповідність (Report on Compliance, RoC) за попередній період, якщо аудит проводиться не вперше.

Роль QSA не обмежується лише формальною перевіркою наявності документації. Аудитор також оцінює ступінь практичного впровадження політик, процедур і процесів, а також рівень обізнаності персоналу щодо їх змісту. Все це перевіряється під час співбесід та аналізу вибіркових доказів на наступних етапах аудиту. QSA повинен отримати підтвердження актуальності схем мережі та потоків даних. Також він має переконатися у проведенні заходів щодо усунення виявлених вразливостей. Важливе значення мають записи, що свідчать про регулярний перегляд процедур обробки даних власників платіжних карток та інших процесів, пов’язаних із виконанням вимог PCI DSS. Навіть такі документи, як службове листування між відповідальними особами з питань PCI DSS (наприклад, директором з інформаційної безпеки (Chief Information Security Officer, CISO), IT-менеджером або менеджером з відповідності) та QSA, можуть слугувати додатковим доказом того, що дотримання вимог стандарту інтегроване у звичайну операційну діяльність організації.

Перевірка та підтвердження обсягу аудиту

QSA здійснює аналіз задокументованого обсягу оцінювання, щоб з’ясувати чи він охоплює всі системні компоненти, персонал, процеси та технології, які зберігають, обробляють або передають дані власників платіжних карток чи конфіденційні дані автентифікації. Іншими словами, сфера аудиту повинна включати всі активи, що належать до середовища даних власників карток (CDE) або мають з ним безпосередній зв’язок.

Суттєві розбіжності, що стосуються обсягу аудиту, можуть стати підставою для його припинення. Особливо під час підготовки до першої оцінки (як зовнішнього аудиту, так і самооцінювання) доцільно проаналізувати можливість зменшення обсягу перевірки з метою зниження навантаження, пов’язаного з дотриманням вимог стандарту.

Вибір зразків для тестування

У разі наявності значної кількості системних компонентів у сфері аудиту QSA формує репрезентативну вибірку, яка відображає всі типові варіації у межах відповідної групи (наприклад, сервери на базі різних операційних систем). Якщо об’єкт аудиту може підтвердити наявність єдиних стандартів конфігурації або автоматизованих механізмів контролю для відповідної групи систем, розмір вибірки може бути зменшений. У випадку, коли окремі вимоги не застосовуються до певних елементів вибірки, організація має узгодити це з QSA. Такі ситуації виникають рідко, а спроби виключити компоненти з вибірки можуть викликати додаткові запитання з боку аудитора. Відсутність обґрунтованих пояснень також може стати підставою для припинення аудиту.

Проведення співбесід та перевірка доказів

Однією з ключових вимог PCI DSS є обов’язкове проведення QSA співбесід із керівництвом та відповідальним персоналом для підтвердження достовірності наданих доказів, зокрема документації.

У ході співбесід встановлюється рівень обізнаності керівництва та ключових працівників щодо:

- активів, які входять до сфери аудиту;

© Кухарська Н. П., Полотай О. І., Павлюк О.-Й. С. Системні аспекти підготовки організацій до проведення аудиту на відповідність вимогам PCI DSS. Сучасний захист інформації, 2(66), 95–105. https://doi.org/10.31673/2409-7292.2026.029908

- впроваджених заходів контролю PCI DSS;
- порядку виконання відповідних процедур безпеки.

Також на цьому етапі QSA перевіряє дотримання всіх релевантних вимог і підвимог стандарту. У разі виявлення невідповідностей аудитор інформує відповідальну особу з питань PCI DSS про виявлені недоліки та необхідні коригувальні заходи або додаткові докази.

Перевірка вибірки

Після завершення співбесід QSA здійснює перевірку фактично впроваджених заходів щодо системних компонентів, відібраних на попередньому етапі, та підтверджує їх відповідність задокументованим процедурам і поясненням, наданим персоналом.

Підсумкова зустріч

Перед формуванням звіту про відповідність (Report on Compliance, RoC) QSA проводить підсумкову зустріч із відповідальною особою з питань PCI DSS організації з метою обговорення виявлених невідповідностей і стану виконання коригувальних заходів. Процес аудиту PCI DSS може тривати до 90 днів (тривалість залежить від вимог платіжного бренду). У разі виявлення невідповідностей організації надається визначений період для їх усунення. Якщо всі коригувальні дії виконані у встановлені строки, QSA завершує підготовку RoC та офіційно підтверджує відповідність вимогам стандарту. Разом з тим зазначений період доцільно розглядати виключно як резервний механізм, а не як основну стратегію проходження аудиту. Процес оцінювання слід розпочинати лише за умови повної готовності організації до підтвердження відповідності вимогам стандарту, з розрахунком на його успішне завершення без потреби у суттєвих доопрацюваннях.

Формування звіту про відповідність (RoC)

Після виконання всіх необхідних коригувальних заходів QSA формує звіт про відповідність (RoC). У ньому узагальнюється інформація, зібрана під час аудиту, та здійснюється її зіставлення з вимогами PCI DSS. Для кожної вимоги звіт має містити достатній рівень деталізації, щоб підтвердити відповідність об’єкта аудиту або належне обґрунтування застосування виулючень.

Підготовка сертифіката відповідності (AoC)

Після завершення звіту про відповідність (RoC) QSA готує сертифікат відповідності (AoC) для офіційного подання. Цей документ підписує QSA (або уповноважена особа компанії QSA) та представник об’єкта аудиту. Сертифікат засвідчує, що організація відповідає вимогам PCI DSS.

Підготовка до зовнішнього аудиту PCI DSS

Наведені нижче сім кроків мають допомогти організаціям підготуватися до зовнішнього аудиту PCI DSS. Для організацій, яким необхідно лише заповнити анкету самооцінювання (SAQ), більшість із цих кроків також є актуальними. Їх виконання сприятиме не лише успішному проходженню оцінювання, а й підтриманню відповідності вимогам PCI DSS протягом звітного періоду.

Крок 1. Отримання підтримки вищого керівництва

Поширеною помилкою є сприйняття відповідності PCI DSS як виключно зони відповідальності IT-підрозділу. Насправді до процесу мають бути залучені різні структурні одиниці організації, зокрема фінансовий департамент, служби продажів і маркетингу. Наявність задокументованих процедур не гарантує ефективності, якщо вони виконуються лише окремими працівниками. Підтримання відповідності потребує скоординованих зусиль усієї організації. Тому важливо забезпечити чітку та публічну підтримку з боку вищого керівництва, що сприятиме дотриманню встановлених процесів і виділенню необхідних ресурсів.

Крок 2. Вибір і налагодження взаємодії з QSA

У випадку залучення QSA необхідно переконатися, що аудитор має чинний статус сертифікації. Перелік сертифікованих QSA-компаній оприлюднюється та регулярно

© Кухарська Н. П., Полотай О. І., Павлюк О.-Й. С. Системні аспекти підготовки організацій до проведення аудиту на відповідність вимогам PCI DSS. Сучасний захист інформації, 2(66), 95–105. https://doi.org/10.31673/2409-7292.2026.029908

оновлюється PCI Security Standards Council. Хоча всі QSA проходять сертифікацію за єдиними вимогами, на практиці їхній досвід, підхід до інтерпретації вимог PCI DSS та рівень ретельності можуть відрізнятися. Належним чином обраний QSA здатний не лише провести аудит, а й допомогти виявити ризики безпеки та надати практичні рекомендації з досягнення й підтримання відповідності з урахуванням специфіки діяльності та бюджету організації.

Ефективна співпраця передбачає регулярну взаємодію з QSA, а не лише під час щорічного аудиту. Для досягнення максимально ефективного результату аудитор має глибоко розуміти галузеві особливості та технологічне середовище організації. Тому доцільно обирати QSA з релевантним досвідом у сфері діяльності організації та з урахуванням специфіки її IT-інфраструктури. Визначена сфера аудиту суттєво допоможе в процесі відбору.

Крок 3. Документування сфери застосування

Документування сфери застосування є одним із ключових етапів досягнення відповідності вимогам стандарту PCI DSS, однак на практиці цьому аспекту часто приділяється недостатня увага. Документ, що визначає сферу застосування, повинен містити:

- перелік залученого персоналу, процесів і технологій, пов'язаних із обробкою, зберіганням або передаванням даних облікових записів;
- діаграми потоків даних;
- схеми мережевої інфраструктури;
- перелік системних компонентів, що входять до сфери застосування;
- усі точки зберігання, обробки та передавання даних облікових записів, включно з резервними копіями.

У документі мають бути чітко визначені та обґрунтовані межі сфери застосування, а також описані засоби контролю, що формують ці межі. Документація повинна охоплювати всі елементи: людей, процеси, технології та системні компоненти, що входять до сфери оцінювання. Крім того, до сфери застосування мають включатися й ті компоненти, які опосередковано впливають на середовище даних власників платіжних карток (CDE), навіть якщо вони безпосередньо не належать до нього (наприклад, сервер служби каталогів).

Сфера застосування є основою проєкту з досягнення відповідності PCI DSS, оскільки саме вона визначає, які вимоги стандарту підлягають виконанню. Цей документ є важливим інструментом під час взаємодії з потенційними QSA, оскільки дозволяє обом сторонам оцінити відповідність досвіду аудитора технічному середовищу організації, зокрема щодо використовуваних технологій і масштабу сфери оцінювання. Організаціям, особливо тим, які проходять аудит уперше, доцільно проаналізувати можливість зменшення обсягу середовища даних власників карток (CDE), оскільки розширення сфери застосування безпосередньо призводить до зростання витрат на підтримку відповідності вимогам PCI DSS. Необхідно перевірити, чи справді всі компоненти інформаційної системи потребують доступу до даних власників карток, а також слід переконатися у відсутності зберігання даних, що не є необхідними для бізнес-процесів.

Для зменшення обсягу CDE організація повинна застосовувати такі заходи:

1. Ефективна сегментація мережі. CDE має бути відокремлене від інших бізнес-сегментів мережі. Це дозволить економічно оправдано застосовувати посилені заходи безпеки лише до CDE. У разі компрометації сегментів мережі, що перебувають поза межами сфери застосування, середовище обробки даних платіжних карток залишиться ізольованим і захищеним;
2. Використання мережевих схем. Слід окремо аналізувати вхідний і вихідний мережевий трафік для виявлення зайвих або небезпечних каналів доступу;
3. Обмеження підключення баз даних. Бази даних не повинні бути підключені до вхідних каналів зв'язку, якщо необхідна інформація може надходити через вихідні канали;
4. Обмеження або повне припинення бездротового доступу до CDE. Бездротові мережі становлять підвищений ризик безпеки. Якщо їх використання є неминучим з бізнесових

© Кухарська Н. П., Полотай О. І., Павлюк О.-Й. С. Системні аспекти підготовки організацій до проведення аудиту на відповідність вимогам PCI DSS. Сучасний захист інформації, 2(66), 95–105. https://doi.org/10.31673/2409-7292.2026.029908

причин, необхідно розгорнути додатковий брандмауер навколо бездротового сегмента та обмежити доступ до мінімально необхідного рівня;

5. Зберігання первинних номерів рахунків (Primary Account Number, PAN), дозволене стандартом PCI DSS, суттєво збільшує кількість вимог і заходів контролю, які необхідно впровадити. З цієї причини доцільно мінімізувати обсяг збереження таких даних або виключити його повністю, якщо це можливо.

Крім того, для зменшення обсягу сфери застосування рекомендується застосовувати такі технічні рішення:

1. Для організацій електронної комерції ефективним підходом є використання механізмів перенаправлення веб-сторінок на платіжні сервіси провайдера, що дає змогу застосовувати спрощений набір вимог PCI DSS;

2. Рішення для маскування двотонального багаточастотного набору (DTMF) у разі приймання платежів телефоном. Це виключає передачу даних платіжних карток через внутрішню мережу організації та зменшує обсяг систем, що підлягають перевірці на відповідність;

3. Використання шифрування «точка-точка» (P2PE). Такі рішення значно скорочують кількість компонентів системи, що входять до сфери застосування, а у випадку використання сертифікованих рішень PCI SSC – спрощують перелік вимог PCI DSS, які необхідно виконувати.

Крок 4. Проведення аналізу прогалин

Організаціям, які вперше проходять оцінювання відповідності, до початку впровадження відсутніх технічних засобів контролю та документації доцільно визначити фактичний рівень відповідності вимогам PCI DSS незалежно від того, чи передбачено проходження зовнішнього аудиту, чи заповнення анкети самооцінювання (SAQ). Ефективний спосіб зробити це – провести аналіз прогалин (gap analysis), під час якого на основі порівняння використовуваних організацією заходів безпеки з вимогами стандарту визначають наявні невідповідності. У разі їх виявлення необхідно задокументувати:

- перелік коригувальних заходів;
- відповідальних осіб за їх виконання;
- строки реалізації.

Якщо якась вимога не застосовується до організації, це має бути обґрунтовано та зафіксовано документально. Аналогічно, у разі використання компенсуючих контролів необхідно детально описати їх характеристики та ефективність. Усі такі обґрунтування й альтернативні заходи підлягають перевірці з боку QSA та відображаються ним у звіті про відповідність (RoC). Таким чином, наявність відповідної документації значно спростить та прискорить процес аудиту. Додатковою можливістю, передбаченою стандартом PCI DSS версії 4.0, є застосування «індивідуального підходу», що дозволяє досягати цілей окремих вимог альтернативними способами. Водночас використання цього підходу потребує дотримання чітко визначеної процедури та обов’язкових консультацій із QSA, оскільки будь-які неузгодженості у їх тлумаченні можуть призвести до затягування аудиту або його негативного результату.

Крок 5. Усунення виявлених прогалин

Після визначення невідповідностей організація повинна впровадити відсутню документацію та технічні засоби контролю відповідно до результатів аналізу прогалин і затвердженого плану коригувальних дій. Хоча підготовка повного комплекту внутрішньої документації може бути трудомістким процесом, саме відсутність технічних заходів контролю найчастіше унеможливлює успішне проходження аудиту. Вимоги PCI DSS у частині технічної реалізації мають бінарний характер – вони або виконані, або ні.

Якщо аудит проводиться не вперше та за попередній період відсутні необхідні журнали подій, записи моніторингу чи інші докази виконання вимог, це, як правило, означає

© Кухарська Н. П., Полотай О. І., Павлюк О.-Й. С. Системні аспекти підготовки організацій до проведення аудиту на відповідність вимогам PCI DSS. Сучасний захист інформації, 2(66), 95–105. https://doi.org/10.31673/2409-7292.2026.029908

негативний результат перевірки. У такій ситуації найбільш доцільним рішенням є перезапустити аудит після повного виконання коригувальних заходів, що є значно менш ефективним варіантом порівняно з попередньою ґрунтовною підготовкою до оцінювання.

З огляду на це, процес аудиту доцільно розпочинати лише за умови впевненості в готовності організації до підтвердження відповідності вимогам PCI DSS.

Крок 6. Реалізація заходів у період огляду

Після впровадження всієї необхідної документації та технічних засобів контролю організація повинна переглянути й, за потреби, запровадити регулярні операційні процедури, які мають стати складовою повсякденної діяльності. До таких процедур належать, але ними не обмежуються, процедури описані далі:

1. Щоденний перегляд журналів подій. З метою своєчасного виявлення можливих інцидентів безпеки необхідно постійно здійснювати моніторинг систем і мереж шляхом ведення журналів доступу та мережевого трафіку. Ці журнали мають аналізуватися щоденно для виявлення аномалій, що можуть свідчити про порушення безпеки. У разі їх виявлення слід вжити коригувальних заходів відповідно до затверджених політик і процедур;

2. Щоквартальне внутрішнє та зовнішнє сканування вразливостей. Регулярне сканування вразливостей дає змогу виявляти помилки конфігурації та відомі вразливості вебресурсів, прикладних програм та інфраструктури. PCI DSS вимагає проведення таких перевірок не рідше одного разу на квартал, включно з внутрішнім скануванням (кваліфікованим персоналом організації) та зовнішнім скануванням, що виконується затвердженим постачальником сканування (ASV);

3. Щопівріччний перегляд правил брандмауера. У процесі експлуатації мережевої інфраструктури правила брандмауерів потребують періодичного оновлення у зв'язку зі змінами конфігурацій та появою нових загроз. Не рідше одного разу на шість місяців необхідно переглядати та видаляти застарілі, надлишкові або некоректні правила, залишаючи лише ті, що відповідають задокументованим політикам і бізнес-обґрунтуванням;

4. Оцінювання ризиків. Оцінка ризиків є обов'язковою складовою системи безпеки та спрямована на виявлення, аналіз і реагування на ризики, що можуть впливати на захист даних власників платіжних карток і середовище CDE. PCI DSS передбачає проведення низки спеціалізованих оцінок ризиків, зокрема для визначення періодичності виконання окремих контрольних заходів (наприклад, проведення перевірок на предмет несанкціонованого доступу на пристроях зчитування карток). Оскільки такі оцінки часто не інтегровані у загальну систему корпоративного ризик-менеджменту, організаціям доцільно передбачати окремі процедури для їх виконання;

5. Щорічне внутрішнє та зовнішнє тестування на проникнення. Регулярне тестування на проникнення дозволяє виявляти та усувати вразливості в системах, мережах і механізмах контролю до того, як ними скористається зловмисник. Таке тестування має охоплювати внутрішні й зовнішні компоненти, а також механізми сегментації мережі, і проводитися незалежним кваліфікованим спеціалістом. Зазвичай у процесі тестування здійснюється спроба практичного використання виявлених вразливостей у вигляді доказу концепції без заподіяння шкоди інфраструктурі. На відміну від сканування вразливостей, яке дозволяє виявляти лише відомі типи вразливостей, тестування на проникнення дає змогу використовувати будь-яку інформацію, отриману під час перевірки, навіть ту, що може здаватися незначною для автоматизованих інструментів. Фахівець з тестування може поєднувати декілька низькорівневих вразливостей, виявлених під час автоматизованого аналізу, для реалізації більш складних і потенційно небезпечних сценаріїв атак. У разі використання сегментації або інших механізмів зменшення сфери застосування їх ефективність повинна підтверджуватися шляхом тестування на проникнення;

6. Щорічне тестування плану реагування на інциденти. Для забезпечення своєчасного реагування на інциденти безпеки PCI DSS вимагає наявності формалізованого плану

© Кухарська Н. П., Полотай О. І., Павлюк О.-Й. С. Системні аспекти підготовки організацій до проведення аудиту на відповідність вимогам PCI DSS. Сучасний захист інформації, 2(66), 95–105. https://doi.org/10.31673/2409-7292.2026.029908

реагування, доведеного до відома всіх відповідальних осіб. Такий план має перевірятися щонайменше один раз на рік із фіксацією результатів у документації, що може бути надана QSA як доказ ефективності процедур.

Усі зазначені заходи мають розглядатися як регулярні елементи операційної діяльності організації з чітким розподілом відповідальності між працівниками. У протилежному випадку вони виконуватимуться лише напередодні щорічного аудиту PCI DSS (з участю QSA або у формі SAQ), а відсутність підтверджувальних записів щодо щоденних перевірок журналів, щоквартальних сканувань чи щорічних тестів може суттєво ускладнити процес аудиту або призвести до негативного результату оцінювання відповідності.

Крок 7. Проведення пробного аудиту

На завершальному етапі підготовки до офіційного аудиту доцільно провести пробний (попередній) аудит. Незалежно від того, виконується він власними силами чи із залученням зовнішніх фахівців, така перевірка дозволить персоналу зрозуміти процедуру аудиту, особливо у випадку першого проходження оцінювання, а також своєчасно виявити та усунути можливі невідповідності.

Висновки

У статті систематизовано ключові організаційні та технічні аспекти підготовки організацій до аудиту на відповідність вимогам PCI DSS. Ці аспекти розглядаються як взаємопов’язані елементи єдиної стратегії, що базується на таких висновках:

1. Зміна парадигми відповідності. Обґрунтовано, що критичний розрив між формальною сертифікацією та реальною захищеністю виникає через сприйняття організаціями аудиту як епізодичної щорічної події. Аргументовано необхідність переходу до моделі безперервного управління безпекою, де виконання контрольних заходів інтегроване у повсякденні операційні процеси організації;

2. Стратегічне значення сфери застосування (CDE). Визначено, що коректне встановлення меж середовища даних платіжних карток є першочерговим етапом підготовки. Запропоновано комплекс заходів із мінімізації обсягу CDE через мережеву сегментацію та впровадження технологій маскування (P2PE, DTMF), що дозволяє не лише знизити вартість аудиту, а й суттєво зменшити поверхню потенційної атаки;

3. Структурування етапів підготовки до аудиту. Сформовано цілісну послідовність підготовчих заходів, ключовими елементами якої визначено аналіз прогалин (gap analysis) та проведення пробного аудиту. Такий підхід дає змогу організаціям превентивно виявляти невідповідності у критичних зонах (документування, регулярність ASV-сканувань, тестування на проникнення) та мінімізувати ризики негативного результату офіційної перевірки;

4. Конструктивна роль кваліфікованої експертизи. Висвітлено значення взаємодії з оцінювачами QSA не лише як контролерами, а як консультантами, чия роль полягає у валідації специфічних для організації методів контролю (зокрема “індивідуального підходу” у версії 4.0). Застосування запропонованого системного підходу до організації підготовчих процесів дозволяє трансформувати аудит із формальної процедури контролю на ефективний інструмент забезпечення кіберстійкості та довгострокового захисту платіжної інфраструктури.

Перелік посилань

1. PCI DSS v4.0.1. URL: https://www.pcisecuritystandards.org/document_library/.

2. PCI compliance audit checklist: An expert guide to passing your audit in 2025. URL: https://www.scrut.io/hub/pci-dss/pci-compliance-audit-checklist.

3. PCI Audit: Requirements and 5 Steps to Prepare for Your Audit. URL: https://www.exabeam.com/explainers/pci-compliance/pci-audit-requirements-and-5-steps-to-prepare-for-your-audit/.

4. Compliance benchmark. Report 2025. URL: https://go.a-lign.com/Benchmark-Report-2025?_ga=2.121865032.29657354.1742913437-1057260875.1742913437.

5. 2024 Payment Security Report. URL: https://www.verizon.com/business/reports/payment-security-report/.

6. Chippagiri, S, Rames, A. (2025). PCI DSS: a critical analysis of implementation, effectiveness, and legislative impact in payment card security. International journal of scientific research in computer science, engineering and information technology, 11 (1), 1258-1266. https://doi.org/10.32628/CSEIT251112115.

© Кухарська Н. П., Полотай О. І., Павлюк О.-Й. С. Системні аспекти підготовки організацій до проведення аудиту на відповідність вимогам PCI DSS. Сучасний захист інформації, 2(66), 95–105. https://doi.org/10.31673/2409-7292.2026.029908

7. Rahaman, S., Wang, G., & Yao, D. (2019). Security certification in payment card industry: Testbeds, measurements, and recommendations. Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. November 11–15, 2019, London, United Kingdom. 481-498. https://doi.org/10.1145/3319535.3363195.

8. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection, Information security management systems, Requirements. URL: https://www.iso.org/standard/54534.html.

9. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection, Information security controls. URL: https://www.iso.org/standard/75652.html.

10. Кухарська, Н. П, Семенюк С. А., & Полотай, О. І. (2025). Ключові аспекти оновленого стандарту ISO/IEC 27002:2022. Сучасний захист інформації, 2, 76-87. https://doi.org/10.31673/2409-7292.2025.023969.

11. Курій, Є., & Опірський, І. (2024). Безпека платіжних операцій: огляд і характеристика ключових змін у новій редакції стандарту PCI DSS. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 3(23), 145–155. https://doi.org/10.28925/2663-4023.2024.23.145155.

12. Joshi, P. K. (2024). Achieving PCI-DSS compliance in payment gateways: a comprehensive approach. Journal of technology and systems, 6(7), 13–31. https://doi.org/10.47941/jts.2299.

Natalia Kukharska
Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Information Technology Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0000-0002-0896-8361
E-mail: nataliia.p.kukharska@lpnu.ua

Orest Polotai
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Information Security Management
Lviv State University of Life Safety, Lviv. Ukraine
ORCID: 0000-0003-4593-8601
E-mail: orest.polotaj@gmail.com

Ostap-Yosyp Pavlyuk
applicant of the first (bachelor's) level of higher education in specialty 125 "Cybersecurity"
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0009-0003-7250-9367
E-mail: ostap-iosyp.pavliuk.kb.2022@lpnu.ua

SYSTEMIC ASPECTS OF PREPARING ORGANIZATIONS FOR A PCI DSS COMPLIANCE AUDIT

The article examines the organizational and practical aspects of ensuring organizations' readiness for PCI DSS audits. It justifies the feasibility of perceiving the process of confirming compliance with the standard requirements not as a formal annual procedure, but as a continuous information security management process. It analyzes typical problems that arise during the audit, in particular, errors in determining the scope of application, insufficient level of documentation of procedures, and irregularity in the implementation of control measures. The paper systematizes the main stages of an audit conducted by a qualified security assessor (QSA) and identifies key areas for preparing an organization for an external assessment or self-assessment. Particular attention is paid to the issues of optimizing the cardholder data environment (CDE), conducting gap analysis, implementing corrective actions, and ensuring regular operating procedures during the review period. The importance of documenting processes, allocating responsibilities, and integrating the standard requirements into the organization's daily activities is revealed. The role of internal audits and mock audits as tools for early detection of non-conformities and minimizing the risks of a negative assessment result is determined. A comprehensive approach to preparing for and maintaining PCI DSS compliance has been shown to reduce the risk of security incidents, minimize financial and reputational losses, and build trust with customers and partners. The findings can be used by organizations that process payment card data to improve audit preparation and ensure ongoing compliance.

Keywords: information security management, PCI DSS, payment data protection, external audit, self-assessment, cardholder data environment.

Надійшла до редакції (Received): 22.04.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

© Кухарська Н. П., Полотай О. І., Павлюк О.-Й. С. Системні аспекти підготовки організацій до проведення аудиту на відповідність вимогам PCI DSS. Сучасний захист інформації, 2(66), 95–105. https://doi.org/10.31673/2409-7292.2026.029908