КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.23.144154
УДК 004.057.2

Курій Євгеній Олегович
Асистент кафедри захисту інформації
Національний університет «Львівська політехніка», Львів, Україна
ORCID 0000-0002-3423-5655
yevhenii.o.kurii@lpnu.ua

Опірський Іван Романович
Доктор технічних наук, професор, завідувач кафедри захисту інформації
Національний університет «Львівська політехніка», Львів, Україна
ORCID 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

БЕЗПЕКА ПЛАТІЖНИХ ОПЕРАЦІЙ: ОГЛЯД І ХАРАКТЕРИСТИКА КЛЮЧОВИХ ЗМІН У НОВІЙ РЕДАКЦІЇ СТАНДАРТУ PCI DSS

Анотація. Ця стаття присвячена дослідженню сучасного стану розвитку кіберзагроз у світі та визначенню ключових напрямів забезпечення безпеки організацій у відповідності з останніми практиками у сфері кіберзахисту. У статті висвітлюється важливість постійного оновлення та удосконалення стратегій кібербезпеки відповідно до найновіших тенденцій та вимог сучасного цифрового середовища. Досліджуються основні виклики, з якими зіштовхуються організації у сфері кібербезпеки, і запропоновані ефективні підходи до їх вирішення. Такий підхід дозволяє не лише адаптуватися до постійно змінного ландшафту кіберзагроз, а й підвищує рівень захисту та знижує ризики для організаційних систем. Стаття підкреслює важливість впровадження і використання фреймворків кібербезпеки як ефективного інструменту для забезпечення стійкості та надійності систем захисту. Використання таких фреймворків дозволяє організаціям створити систематизований підхід до управління інформаційною безпекою, враховуючи сучасні вимоги та найкращі практики галузі. Такий підхід допомагає забезпечити повноту заходів забезпечення безпеки, що є важливим для успішної протидії кіберзагрозам у сучасному цифровому середовищі. Основну увагу стаття приділяє важливості захисту даних власників платіжних карток та дотриманню стандарту PCI DSS. Зберігання та обробка таких даних потребує високого рівня безпеки, оскільки їх несанкціонований витік чи порушення цілісності може призвести до серйозних фінансових втрат для організацій та втрати довіри користувачів. Стандарт PCI DSS встановлює вимоги щодо захисту інформації про платежі, включаючи визначення контрольних заходів та процедур для запобігання несанкціонованому доступу до карткових даних. Оновлена версія стандарту, PCI DSS v.4.0, є важливим кроком у напрямку удосконалення заходів безпеки та протидії сучасним кіберзагрозам в цій сфері. Її детальний аналіз дозволить організаціям підтримувати відповідність з новими вимогами та забезпечувати безпеку даних платіжних карток на високому рівні. Таким чином, аналізуючи ці аспекти, стаття надає читачам усвідомлення про важливість забезпечення відповідності організаційних систем безпеки найсучаснішим стандартам та практикам у сфері кіберзахисту та допомагає зрозуміти сучасні виклики та можливості в області кібербезпеки.

Ключові слова: фреймворк кібербезпеки; кіберзлочин; система управління інформаційною безпекою; критична інфраструктура; дані власників карток; PCI DSS.

ВСТУП

Сучасний ландшафт кіберзагроз постійно еволюціонує, оскільки технології швидко розвиваються, що призводить до появи нових та вдосконалення вже відомих методів кібератак. Недавній стрімкий розвиток Штучного Інтелекту (ШІ) ще більше полегшив

кіберзлочинцям здійснення атак, навіть за умови обмежених ресурсів чи технічних навичок [1].

Зловмисники постійно продовжують адаптовуватися до нових технологій, в той час як по всьому світу з'являються нові гравці та загрози в поєднанні з інноваційними методами використання або застосування існуючих тактик і стратегій [2].

Відповідь на ці виклики вимагає постійного оновлення захисту, активного моніторингу заходів безпеки та співпраці між організаціями для обміну інформацією про загрози та кращі практики в області кібербезпеки. Підтримка постійної готовності та своєчасна реакція на нові загрози стають ключовими аспектами ефективного кіберзахисту. Організації повинні мати стратегії виявлення, реагування та відновлення після інцидентів, а також постійно оновлювати свої заходи безпеки, щоб вони відповідали сучасним викликам і загрозам.

Для забезпечення ефективного захисту об'єктів критичної інфраструктури необхідно впроваджувати передові технології та методики кібербезпеки. Стандарти кібербезпеки, такі як PCI DSS, надають систематичний підхід до ідентифікації потенційних ризиків та впровадження заходів з їх запобігання. Вони допомагають упорядкувати процес забезпечення безпеки, створюючи загальноприйняті рамки та вимоги [3].

Постановка проблеми. У цій частині статті описується проблема, розгляду якої присвячене дослідження, у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Постійний розвиток загроз сприяє системному оновленню практик кібербезпеки. У 2022 році було представлено оновлену версію стандарту захисту даних власників платіжних карток PCI DSS. Це створило для організацій, які вже пройшли або планують пройти сертифікаційний аудит на відповідність цьому стандарту, необхідність своєчасного оновлення наявних практик і контролів кібербезпеки. Відповідно, важливим є розуміння ключових змін у новій версії стандарту у порівнянні із попередньою версією, і основних цілей, які ставить перед собою нова редакція.

Аналіз останніх досліджень і публікацій. У нещодавно опублікованому аналізі кіберзагроз за 3 квартал 2023 року компанія BlackBerry проаналізувала події з кібербезпеки з червня по серпень 2023 року. Звіт зосереджений на критичній інфраструктурі та великих організаціях, таких як банки та медичні установи. Згідно зі звітом, зловмисники здійснювали близько 11,5 атак на хвилину в усіх секторах. Охорона здоров'я та фінансовий сектор були одними з найбільш частих цілей цих атак. Зокрема, це зумовлено цінністю і критичністю інформації, яку зберігають ці галузі (інформація про банківські рахунки, дані платіжних карток, особиста інформація та номери соціального страхування), і тим, що ці дані вважаються особливо прибутковим для кіберзлочинців. Їх можна використовувати як матеріал для шантажу або для подальших злочинів, таких як крадіжка особистих даних [4].

У цей вік індустріалізованих кібератак, пристосування до ризиків інформаційної безпеки, що постійно змінюються, вимагає своєчасного та гнучкого підходу до побудови стійкої і захищеної інфраструктури підприємства. З урахуванням постійної еволюції кіберзагроз та їхнього стрімкого збільшення стає очевидною важливість оновлення практик інформаційної безпеки. Необхідність адаптації до найновіших викликів цифрового середовища стала критичною [5].

У відповідь на постійне вдосконалення загроз, оновлення потребують і практики безпеки, зокрема популярні фреймворки кібербезпеки [6].

Нещодавно значне і довгоочікуване оновлення отримав популярний міжнародний стандарт для побудови системи управління інформаційною безпекою — ISO/IEC 27001 [7].

Тому важливим і очікуваним було також оновлення іншого популярного фреймворку, який регламентує захист даних власників платіжних карток — PCI DSS [8].

Мета статті. Метою статті є проведення аналізу сучасного стану розвитку кіберзагроз у світі та визначення ключових напрямів забезпечення безпеки організацій у відповідності з останніми практиками у сфері кіберзахисту. Додатково, метою є детальний огляд і аналіз оновленої версії стандарту забезпечення безпеки даних власників платіжних карток — PCI DSS v.4.0 та порівняння її з попередньою версією — PCI DSS v.3.2.1.

Завдання. Для успішного досягнення мети статті необхідно виконати наступні завдання:

- Провести аналіз сучасного стану розвитку кіберзагроз у світі шляхом збору та аналізу актуальних даних та статистики щодо інцидентів кібербезпеки;
- Провести детальний огляд та аналіз оновленої версії стандарту забезпечення безпеки даних власників платіжних карток — PCI DSS v.4.0, виявивши основні зміни, вдосконалення та нововведення порівняно з попередньою версією PCI DSS v.3.2.1;
- Сформулювати рекомендації щодо впровадження заходів забезпечення безпеки з урахуванням виявлених тенденцій у розвитку кіберзагроз та оновлення стандартів кібербезпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Огляд стандарту безпеки даних власників карток PCI DSS

Будь-яка організація, яка приймає платіжні картки, повинна дотримуватися стандарту PCI DSS відповідно до вимог компаній, що видають кредитні картки. Це міжнародний стандарт, а не національне регулювання. На щастя, цей стандарт є досить вичерпним, технічним та детальним і вважається достатньо самостійним фреймворком для забезпечення кібербезпеки [9].

PCI DSS (Payment Card Industry Data Security Standard, у перекладі з англ. «стандарт безпеки індустрії платіжних карток») — стандарт із сфери кібербезпеки, спрямований на захист карткових даних при їх зберіганні, обробці або передачі. Він був розроблений у грудні 2004 року при участі п’яти транснаціональних корпорацій у сфері платіжних карт: Visa, MasterCard, American Express, Discover Financial Services та JCB International.

Кожна із корпорацій мала на меті створити мінімальний рівень захисту для карткових даних при їх зберіганні, обробці або передачі шляхом поєднання напрацювань кожної із сторін [10].

Стандарт PCI DSS передбачає декілька умовних рівнів, на які поділяються компанії, що підпадають під дію стандарту. Відповідно від рівня відповідності визначається які саме звітні документи необхідно заповнити QSA (аудитору) для PCI DSS сертифікації компанії.

Рівні поділяються за кількістю транзакцій щорічно наступним чином:

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

Стандарт PCI DSS застосовується для всіх організацій, залучених в обробку платіжних карток: провайдерів сервісів, процесингових центрів, екваєрів, емітентів та

постачальників послуг, а також будь-яких інших організацій, які зберігають, обробляють або передають:

– дані власників карток: номер картки (PAN), ім'я власника картки, дата витоку строку роботи картки, сервісний код)

та/або

– критичні автентифікаційні дані: повні дані треку (дані магнітної полоси картки або чіпа), CAV2/CVC2/CVV2/CID, PIN-коди та/або PIN-блоки [11].

Аналіз оновленої версії стандарту PCI DSS

Подібно до стандарту ISO 27001, PCI DSS також розвивається, щоб не відставати від стану електронної комерції та більш складних кіберзагроз, і в 2022 році отримав значне оновлення.

PCI SSC випустив PCI DSS v.4.0 31 березня 2022 року та представив 64 нові вимоги, яких організації повинні дотримуватися, за умови їхньої застосовності до середовища. Як і у випадку з будь-яким великим оновленням фреймворка кібербезпеки, організації повинні застосовувати проактивний підхід між випуском стандарту та датою його вступу в силу. Таким чином всі організації повинні досягти відповідності із новою версією до початку 2025 року.

Ця нова версія PCI DSS знаменує суттєву зміну поточної версії (3.2.1), якою сьогодні користуються організації. Вона також вносить фундаментальну зміну в ключову передумову встановлених стандартів, що матиме постійний і далекосяжний вплив на те, як організації впроваджують, керують і повідомляють про відповідність PCI DSS. Нова версія впроваджує значні зміни у вимогах, зосереджуючись більше на підтримці безперервної безпеки, а також додаючи нові методи для задоволення вимог стандарту [12].

Повноваження, визначені новою версією PCI DSS, набувають чинності в три етапи. Перший стосується 13 нових вимог, які негайно набувають чинності для будь-якого звіту про відповідність PCI DSS 4.0 (ROC) або опитувальника самооцінки (SAQ), поданого після випуску нової версії стандарту. Другий — після 31 березня 2024 року, коли поточна версія стандарту PCI DSS 3.2.1 виходить з експлуатації. Усі оцінки, завершені 1 квітня 2024 року або пізніше, мають відповідати PCI DSS 4.0. Нарешті, решта 51 нова вимога є найкращими практиками до 31 березня 2025 року, і вони повинні бути введені в дію до 1 квітня 2025 року (рис. 1).

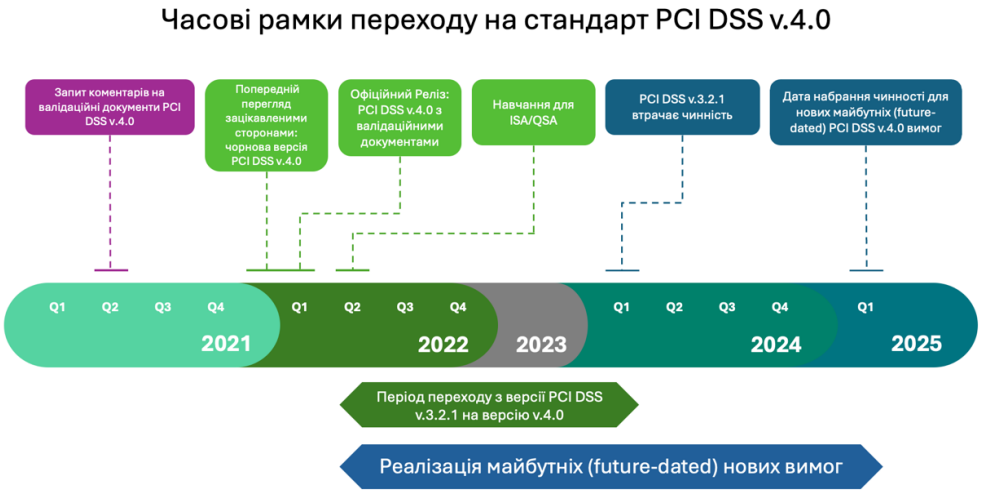

Рис. 1. Часові рамки для переходу на нову версію стандарту PCI DSS v.4.0

Основною метою PCI DSS 4.0 є продовження розвитку стандарту для задоволення мінливих потреб індустрії платіжних карток і нових технологій, які впроваджуються щодня.

PCI DSS 4.0 містить ряд змін, спрямованих на досягнення чотирьох ключових цілей:

- продовження задоволення потреб платіжної індустрії;
- сприяння забезпеченню безпеки як безперервного процесу;
- додавання гнучкості та додаткових методів для підтримки безпеки платежів;
- вдосконалення методів і процедур підтвердження платежів.

Нижче наведено загальний огляд цих змін у порівнянні з попередньою версію PCI DSS 3.2.1 [13].

Таблиця 1

Огляд відмінностей між версіями 4.0 і 3.2.1 стандарту PCI DSS

Мета контролю	PCI DSS вимога/контроль	Огляд відмінностей між версіями 4.0 і 3.2.1
Побудуйте і підтримуйте безпечну мережу та системи Build and Maintain a Secure Network and Systems	1. Встановіть і підтримуйте налаштування брандмауера для захисту даних власників карток Install and maintain a firewall configuration to protect cardholder data	Розширено спектр мережевих технологій. Уточнено мету контролю щодо розмежування між довіреними та недовіреними мережами, у тому числі бездротовими. Деталізовано та розширено деякі вимоги. Частину пунктів вимог декомпозовано.
	2. Не використовуйте дефолтні налаштування, які надає вендор, для паролів та інших параметрів безпеки Do not use vendor-supplied defaults for system passwords and other security parameters	Додано вимогу 2.1.2 щодо опису, прийняття та виконання обов'язків. Уточнено вимоги щодо небезпечних служб та протоколів.
Захищайте дані власників карток Protect Cardholder Data	3. Захищайте дані власників карток, які ви зберігаєте Protect stored cardholder data	Значно деталізовано вимоги щодо зберігання критичних даних до завершення авторизації (3.2.1, 3.3.2). Без ключової виробничої необхідності дозволяється відображати лише 4 останні цифри під час маскування. Окремо описані вимоги щодо використання хешу. Шифрування на рівні диска або розділу використовується лише для змінних носіїв. Забороняється використовувати однакові ключі для тестового та виробничого середовищ.
	4. Шифруйте передачу даних власників карток через відкриті публічні мережі Encrypt transmission of cardholder data across open, public networks	Додано вимогу вести інвентаризацію, контроль використання, термін дії всіх довірених ключів та сертифікатів, які використовуються для захисту повного номера картки під час його передачі.

Підтримуйте програму по управлінню ризиками Maintain a Vulnerability Management Program	5. Захищайте всі системи від шкідливого програмного забезпечення і регулярно оновлюйте антивірусне програмне забезпечення Protect all systems against malware and regularly update antivirus software or programs	Цей розділ має п’ять нових вимог. Саме у п’ятому розділі вперше з’являється нове для стандарту PCI DSS поняття targeted risk analysis — цільовий аналіз ризику. Версія стандарту 4.0 пропонує організаціям самостійно заповнювати таблицю, шаблон якої наведено у новій версії стандарту, де аналізується той чи інший ризик та робляться висновки щодо його (ризику) прийняття, компенсації, чи уникнення тощо. Також, заповнення даної таблиці вимагає визначати періодичність та частоту сканування систем антивірусними засобами, а також періодичність перевірок систем, які вважаються такими, що не піддаються вірусним загрозам. Додано вимогу, що визначає, що антивірус відтепер повинен сканувати всі знімні носії, а також повинен бути організований захист організації від фішингу.
	6. Розробіть і підтримуйте захищені системи і додатки Develop and maintain secure systems and applications	Додано три нові вимоги. Додано вимогу щодо створення та підтримання реєстру всіх користувачів ПЗ, а також всіх ПЗ третіх сторін. Додано вимогу для власників веб-сторінок платіжних систем вести список усіх сценаріїв скрипту на цій сторінці з обґрунтуванням необхідності кожного з них. Використання WAF стає обов’язковим для організації.
Впровадьте суворі заходи контролю доступу Implement Strong Access Control Measures	7. Обмежте доступ до даних про власників карток відповідно до потреб бізнесу Restrict access to cardholder data by business need to know	Сьомий розділ отримав три нові вимоги. Необхідно впровадити перевірку всіх облікових записів на легітимність їх існування та прав щонайменше раз на шість місяців, а також окремо виділено вимоги до технічних та сервісних облікових записів.
	8. Ідентифікуйте та автентифікуйте доступ до компонентів системи Identify and authenticate access to system components	У цьому розділі виникло п’ять нових вимог. Мультифакторній автентифікації приділяється особлива увага. Висуваються вимоги до облікових записів, які можна використовувати для інтерактивного входу. Окремо виокремлено вимоги до терміналів точок продажу. Вимога збільшення довжини пароля з 7 до 12 символів.

		Вимога впровадження багатофакторної аутентифікації (MFA) для всіх видів доступу до CDE. Заборона хардкодити паролі у файлах та скриптах.
	9. Обмежте фізичний доступ до даних власників карток Restrict physical access to cardholder data	Цільовий аналіз ризику визначає необхідність перевірок пристрою POI на відсутність підробки. Також зазначено, з якою періодичністю мають відбуватися дані перевірки. Окремо виокремлено вимоги до відвідувачів. Змінено вимоги до зберігання, обліку та знищення носіїв.
Регулярно перевіряйте та тестуйте мережі Regularly Monitor and Test Networks	10. Відстежуйте та контролюйте всі доступи до мережевих ресурсів і даних власників карток Track and monitor all access to network resources and cardholder data	Цей розділ вимагає використання автоматичних механізмів для перевірки журналів аудиту. Додано вимогу виявляти, попереджати та оперативно усувати збої критичних систем контролю безпеки.
	11. Регулярно тестуйте системи та процеси безпеки Regularly test security systems and processes	Одинадцятий розділ отримав п’ять нових вимог. Конкретизуються особливості та порядок дій при внутрішньому скануванні на вразливості (проводити яке мають право лише авторизовані компанії), а також додано вимогу, що системи IDS/IPS повинні виявляти та усувати приховані канали передачі шкідливих програм. Додано вимогу до управління всіма знайденими вразливостями (а не лише критичними). З'являється поняття multi-tenant service providers — будь-які дата-центри та хмарні провайдери підпадають під даний контроль. Всі вони повинні будуть проходити додаткову перевірку за програмою A1.
Підтримуйте політику інформаційної безпеки Maintain an Information Security Policy	12. Підтримуйте політику безпеки інформації для всього персоналу Maintain a policy that addresses information security for all personnel	Цей розділ отримав тринадцять нових вимог. Важливо відзначити, що дві вимоги з них є обов’язковими для виконання ще з 2024 року. Це необхідність проводити вже згаданий «targeted risk analysis» щонайменше раз на рік, а також необхідність підтримувати документований опис зони відповідності стандарту в актуальності та проводити перевірку щонайменше раз на рік або за істотних змін даного середовища. Решта нових вимог також зосереджена в основному на документуванні того чи іншого

		аспекту підтримки організацією відповідності вимогам стандарту PCI DSS. Для постачальників послуг додано вимогу документувати та підтверджувати сферу застосування PCI DSS не рідше ніж кожні 6 місяців. Додалася вимога щодо оновлення програми підвищення поінформованості раз на 12 місяців. Частота навчання персоналу має ґрунтуватися на проведеному аналізі ризиків.

У новій версії стандарту PCI DSS 4.0 спостерігається не лише збільшення обсягу з 180 до 360 сторінок, а й поглиблення аналізу вимог щодо забезпечення безпеки даних. Деталізація та уточнення вимог дають більш чітке їхнє розуміння, що сприяє їх кращому і ефективнішому впровадженню. Важливим аспектом є перехід до ризик-орієнтованого підходу, який дозволяє організаціям ефективніше виявляти та управляти потенційними загрозами для безпеки даних. Категоризація вимог та даних сприяє більш систематичному підходу до їх впровадження, що в свою чергу сприяє підвищенню ефективності заходів забезпечення безпеки. Додатково, нові вимоги та контролі безпеки відповідають сучасним тенденціям та загрозам у сфері кібербезпеки, що допомагає забезпечити вищий рівень захисту даних власників платіжних карток.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Ця стаття детально досліджує та аналізує стандарт захисту даних власників платіжних карток — PCI DSS, зосереджуючись на його новій версії, PCI DSS v.4.0. Вона надає читачам огляд ключових аспектів цього стандарту, включаючи його основні зміни та вдосконалення у порівнянні з попередньою версією.

Зазначений порівняльний аналіз покликаний допомогти організаціям зрозуміти важливість вдосконалення стратегій та заходів безпеки для відповідності новим вимогам стандарту. Враховуючи швидкий розвиток технологій та постійне зростання кіберзагроз, розуміння та впровадження відповідних заходів захисту є критичним для забезпечення безпеки та захисту конфіденційності платіжних даних.

Детальний аналіз PCI DSS v.4.0 виявляє нові вимоги та рекомендації, спрямовані на підвищення ефективності захисту та протидії сучасним кіберзагрозам. Розглядаючи ці зміни, організації можуть вдосконалити свої стратегії безпеки та забезпечити відповідність з останніми вимогами стандарту.

Отже, стаття є цінним ресурсом для організацій, що працюють з платіжними даними, а також для фахівців з кібербезпеки, які прагнуть розуміти та впроваджувати найбільш ефективні стратегії захисту.

Результати дослідження ключових змін у версіях стандарту буде використано у подальшому дисертаційному дослідженні автора для побудови ефективної методології перехресного впровадження стандартів аудиту кібербезпеки в об’єктах критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Susukailo, V., Opirsky, I., & Yaremko, O. (2022). Methodology of ISMS Establishment Against Modern Cybersecurity Threats. *Future Intent-Based Networking. Lecture Notes in Electrical Engineering, 831*. https://doi.org/10.1007/978-3-030-92435-5_15
2. *Global Cybersecurity Outlook 2024*. (2024). Weforum. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/
3. Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards – A Review and Comprehensive Overview. *Electronics, 11(14).* https://doi.org/10.3390/electronics11142181
4. *Global Threat Intelligence Report*. (n.d.). Blackberry. https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report
5. Kurii, Y., & Opirskyy, I. (2021). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. *Cybersecurity Providing in Information and Telecommunication Systems, 3288*, 21–32.
6. Kurii, Y., Opirskyy, I., & Bortnik, L. (2023). ISO/IEC 27001:2022 – Analysis of Changes and Compliance Features of the New Version of the Standard. *Materials of IXth International Scientific and Technical Conference Information Protection And Information Systems Security*, 15–17.
7. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* (ISO/IEC 27001). (2022).
8. PCI DSS: v4.0. (n.d.). https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
9. Lincke, S. (2024). *Complying with the PCI DSS Standard. Information Security Planning. Springer*. https://doi.org/10.1007/978-3-031-43118-0_3
10. Mustafa, N. (2023) PCI DSS v4.0: achieving more with limited resources. *Brighttalk Webinar Series.* https://doi.org/10.13140/RG.2.2.17152.20486
11. *Payment Card Industry Security Standards*. (n.d.). https://listings.pcisecuritystandards.org/pdfs/pcissc_overview.pdf
12. *PCI DSS version 4.0 is here: What you need to know now*. (n.d.). https://rsmus.com/insights/services/risk-fraud-cybersecurity/pci-dss-version-4-point-0-is-here-what-you-need-to-know-now.html
13. *PCI DSS Summary of Changes: v3.2.1 to v4.0.* (n.d.). https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (23), 2024
ISSN 2663 - 4023

Yevhenii Kurii
Assistant, Department of Information Security
Lviv Polytechnic National University, Information Security Department, Lviv, Ukraine
ORCID 0000-0002-3423-5655
yevhenii.o.kurii@lpnu.ua

Ivan Opirskyy
Doctor of Technical Sciences, Professor, Head of the Department of Information Security
Lviv Polytechnic National University, Information Security Department, Lviv, Ukraine
ORCID 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

SECURITY OF PAYMENT TRANSACTIONS: OVERVIEW AND CHARACTERISTICS OF KEY CHANGES IN THE NEW EDITION OF THE PCI DSS STANDARD

Abstract. This article is devoted to the study of the current state of development of cyber threats in the world and the identification of key areas of ensuring the security of organizations in accordance with the latest practices in the field of cybersecurity. The article highlights the importance of constantly updating and improving cybersecurity strategies in accordance with the latest trends and requirements of today's digital environment. The main challenges faced by organizations in the field of cybersecurity are investigated, and effective approaches to their resolution are proposed. This approach allows not only to adapt to the constantly changing landscape of cyber threats but also increases the level of protection and reduces risks for organizational systems. The article emphasizes the importance of implementing and using cybersecurity frameworks as an effective tool for ensuring the stability and reliability of systems' security. The use of such frameworks allows organizations to create a systematic approach to information security management, taking into account modern requirements and industry best practices. This approach helps to ensure the completeness of security measures, which is essential for successfully combating cyber threats in today's digital environment. The article focuses on the importance of the protection of cardholder data and compliance with the PCI DSS standard. The storage and processing of such data requires a high level of security, as their unauthorized leakage or breach of integrity can lead to serious financial losses for organizations and loss of user trust. The PCI DSS standard establishes requirements for protecting payment information, including defining controls and procedures to prevent unauthorized access to cardholder data. The updated version of the standard, PCI DSS v.4.0, is an important step in the direction of improving security measures and countering modern cyber threats in this area. Its detailed analysis will allow organizations to maintain compliance with new requirements and ensure the security of cardholder card data at a high level.

Keywords: cybersecurity framework; cybercrime; information security management system; critical infrastructure; cardholder data, PCI DSS.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Susukailo, V., Opirsky, I., & Yaremko, O. (2022). Methodology of ISMS Establishment Against Modern Cybersecurity Threats. *Future Intent-Based Networking. Lecture Notes in Electrical Engineering, 831*. https://doi.org/10.1007/978-3-030-92435-5_15
2. *Global Cybersecurity Outlook 2024.* (2024). Weforum. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/
3. Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards – A Review and Comprehensive Overview. *Electronics, 11(14).* https://doi.org/10.3390/electronics11142181
4. *Global Threat Intelligence Report.* (n.d.). Blackberry. https://www.blackberry.com/us/en/solutions/threat-intelligence/threat-report

5. Kurii, Y., & Opirskyy, I. (2021). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. *Cybersecurity Providing in Information and Telecommunication Systems, 3288*, 21–32.
6. Kurii, Y., Opirskyy, I., & Bortnik, L. (2023). ISO/IEC 27001:2022 – Analysis of Changes and Compliance Features of the New Version of the Standard. *Materials of IXth International Scientific and Technical Conference Information Protection And Information Systems Security*, 15–17.
7. *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* (ISO/IEC 27001). (2022).
8. PCI DSS: v4.0. (n.d.). https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
9. Lincke, S. (2024). *Complying with the PCI DSS Standard. Information Security Planning. Springer*. https://doi.org/10.1007/978-3-031-43118-0_3
10. Mustafa, N. (2023) PCI DSS v4.0: achieving more with limited resources. *Brighttalk Webinar Series.* https://doi.org/10.13140/RG.2.2.17152.20486
11. *Payment Card Industry Security Standards.* (n.d.). https://listings.pcisecuritystandards.org/pdfs/pcissc_overview.pdf
12. *PCI DSS version 4.0 is here: What you need to know now.* (n.d.). https://rsmus.com/insights/services/risk-fraud-cybersecurity/pci-dss-version-4-point-0-is-here-what-you-need-to-know-now.html
13. *PCI DSS Summary of Changes: v3.2.1 to v4.0.* (n.d.). https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf