

АНАЛІЗ МІЖНАРОДНИХ СТАНДАРТІВ ТА РЕКОМЕНДАЦІЙ З КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВ

Вінницький національний технічний університет

Анотація

У дослідженні проведено поглиблений аналіз практичних аспектів застосування міжнародних стандартів та нормативних рекомендацій у сфері кібербезпеки. Розглянуто процеси інтеграції підприємствами комплексу технічних, організаційних та правових заходів для ефективного управління кіберризиками в умовах цифрової трансформації. У дослідженні окреслено як переваги, так і недоліки адаптації стандартів ISO/IEC 27001, PCI DSS та регламенту GDPR. Зокрема, ідентифіковано виклики, що виникають при їх впровадженні, питання адаптації для підприємств різного масштабу, а також особливості застосування у специфічних галузях.

Ключові слова: кібербезпека, ISO/IEC 27001, PCI DSS, GDPR, управління ризиками, цифрова трансформація, інтеграція стандартів

Abstract

This paper presents an in-depth analysis of the practical aspects of implementing international cybersecurity standards and regulatory recommendations. It discusses how enterprises integrate a set of technical, organizational, and legal measures for effective cyber risk management in the context of digital transformation. The study outlines both the advantages and limitations of adapting ISO/IEC 27001, PCI DSS, and the GDPR, identifying the challenges encountered during implementation, the adaptation issues for enterprises of various sizes, and the specific application features in diverse industries.

Keywords: cybersecurity, ISO/IEC 27001, PCI DSS, GDPR, risk management, digital transformation, standards integration

Вступ

Сучасний інформаційний простір характеризується не лише надзвичайною динамікою змін, але й експоненційним зростанням кількості кіберзагроз. Це ставить перед підприємствами нагальну необхідність постійного удосконалення систем захисту даних. В епоху цифрової трансформації організації змушені переосмислювати традиційні підходи до управління інформаційною безпекою, інтегруючи багатоаспектні технічні, організаційні та правові заходи. Міжнародні стандарти, зокрема ISO/IEC 27001, PCI DSS і регламент GDPR, виступають інструментами, що дозволяють створити фундамент для системного управління кіберризиками. Проте, практичне застосування цих норм часто виявляється складнішим за теоретичні уявлення. Необхідно враховувати цілу низку факторів: специфіку галузі, розмір підприємства, ресурсні обмеження та культуру організації. Відповідно до зазначеного, основна увага цього дослідження зосереджена на аналізі конкретних викликів впровадження стандартів і рекомендацій, з метою надання практично-орієнтованих настанов для адаптації норм до унікальних умов діяльності.

Результати дослідження

В умовах реального впровадження стандартів управління інформаційною безпекою першочерговим є ретельний аналіз внутрішніх процесів підприємства. Стандарт ISO/IEC 27001, який є загальновизнаним базисом у даній галузі, створює системну основу для аналізу та управління ризиками. Разом з тим, практичний досвід вказує на те, що універсальність цього стандарту може бути водночас і перевагою, і недоліком [1]. На великих підприємствах зі складною структурою та розгалуженими процесами, система, побудована на ISO/IEC 27001, забезпечує детальне картування ризиків, чіткий розподіл відповідальності між структурними підрозділами та безперервний моніторинг ефективності заходів безпеки. На противагу цьому, малі підприємства з обмеженими ресурсами потребують розробки адаптивних, модульних підходів. Це дозволить зосередитися на впровадженні

лише критично важливих компонентів системи, уникаючи надмірної бюрократизації та документообігу [2].

У сфері платіжних систем стандарт PCI DSS набуває особливої ваги, оскільки захист даних платіжних карток є критично важливим для фінансових установ та підприємств, що здійснюють електронні платежі. Проте, існуючі вимоги PCI DSS, розроблені для традиційної комп'ютерної інфраструктури, не повною мірою відповідають сучасним умовам, зокрема в контексті IoT-платежів. У цьому випадку пристрої характеризуються обмеженою обчислювальною потужністю та нестандартними операційними характеристиками [3]. Практичний досвід підтверджує необхідність розробки спрощених процедур шифрування, адаптивних алгоритмів та спеціалізованих протоколів безпеки для пристроїв з обмеженими ресурсами. Такий підхід дозволить забезпечити високий рівень безпеки, мінімізуючи ризики, пов'язані з нестачею ресурсів і необхідністю частих оновлень програмного забезпечення [4].

Регламент GDPR втілює комплексний підхід до захисту персональних даних, що охоплює не тільки технічні аспекти, але й питання організаційної культури та правової відповідальності. Практичні виклики впровадження GDPR полягають у необхідності адаптації процесів обробки даних до високих стандартів прозорості, права на забуття та захисту даних за замовчуванням. Сьогодні організації стикаються з труднощами в інтеграції вимог GDPR в існуючі бізнес-процеси, що часто зумовлює необхідність кардинальних змін у внутрішній структурі та методах роботи. Одним із шляхів вирішення цих проблем є інтеграція GDPR з іншими стандартами, що дозволяє створити синергічну модель управління інформаційною безпекою. Аналіз практичних прикладів свідчить про те, що комбінування нормативно-правових вимог з технічними заходами, розробленими за методологією ISO/IEC 27001, дозволяє не тільки забезпечити відповідність законодавству, але й значно підвищити ефективність управління ризиками [5].

Важливим аспектом є розробка інтегрованої стратегії впровадження, що базується на поетапному розгортанні заходів безпеки. Такий підхід дозволяє оптимізувати використання ресурсів і гарантувати безперервність операцій навіть у випадку виникнення кібератак. Реалізація цих заходів передбачає створення систем внутрішнього навчання, регулярне проведення аудитів безпеки та застосування автоматизованих інструментів моніторингу, що дозволяють в режимі реального часу аналізувати ефективність системи та оперативно виявляти потенційні загрози.

Окрім того, формування корпоративної культури, орієнтованої на захист інформації, є ключовим фактором успішного впровадження стандартів. Це включає в себе не тільки технічну підготовку співробітників, але й виховання відповідального ставлення до обробки персональних даних, підвищення рівня обізнаності щодо актуальних кіберзагроз та постійне оновлення внутрішніх політик безпеки.

Висновок

Підсумовуючи проведений аналіз, можна стверджувати, що ефективне застосування міжнародних стандартів з кібербезпеки досягне лише за умови інтеграції технічних, організаційних і правових заходів, адаптованих до конкретної специфіки діяльності підприємства. Стандарт ISO/IEC 27001 слугує надійною основою для систематичного управління ризиками, однак для малих організацій більш доцільними є гнучкі модульні підходи. PCI DSS у контексті динамічного розвитку IoT-платежів вимагає модернізації процедур захисту з урахуванням обмежень ресурсоефективних пристроїв. Регламент GDPR встановлює високі вимоги до захисту персональних даних, що зумовлює необхідність комплексного підходу, який поєднує нормативно-правові, технічні та організаційні аспекти.

Отже, розробка інтегрованої системи кібербезпеки, заснованої на поетапному впровадженні заходів, регулярному моніторингу ефективності та безперервному навчанні співробітників, є оптимальним шляхом до забезпечення високого рівня захисту в умовах цифрової трансформації. Цей підхід сприяє не тільки відповідності міжнародним стандартам, але й підвищенню довіри клієнтів, конкурентоспроможності підприємства та його стійкості до сучасних кіберзагроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стайкуца С. В., Кільдішев В. Й., Сєдов К. С., Левандовська О. В. Аналіз міжнародних стандартів, політик та регламентів з кібербезпеки // *Молодий вчений*. – 2023
2. Kitsios F., Chatzidimitriou E., Kamariotou M. The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector // *Sustainability*. – 2023. – Vol. 15, p. 5828. – DOI: 10.3390/su15075828.

3. Mumtaz Bhutta M. N., Bhattia S., Alojail M. A., Nisar K., Cao Y., Chaudhry S. A., Sun Z. Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS) // *Wireless Communications and Mobile Computing*. – 2022. – No. 1, Article ID 9942270. – DOI: 10.1155/2022/9942270.

4. Курій, С. Опірський, І. «БЕЗПЕКА ПЛАТІЖНИХ ОПЕРАЦІЙ: ОГЛЯД І ХАРАКТЕРИСТИКА КЛЮЧОВИХ ЗМІН У НОВІЙ РЕДАКЦІЇ СТАНДАРТУ PCI DSS» // Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2024. – Т. 3, № 23, с. 145–155. – DOI: 10.28925/2663-4023.2024.23.145155.

5. Zaguir N. A., de Magalhães G. H., Spinola M. de Mesquita. Challenges and Enablers for GDPR Compliance: Systematic Literature Review and Future Research Directions // *IEEE Access*. – 2024. – Vol. 12, pp. 81608–81630. – DOI: 10.1109/ACCESS.2024.3406724.

6. Стайкуца С., Кільдішев В., Солоїд В., Виноградов Д. Огляд платформи підвищення рівня кібербезпеки критично важливих структур NIST Cybersecurity Framework // *Scientific Collection «InterConf»*. – 2023. – № 176. – С. 212–217.

7. Melwin Syafrizal, Siti Rahayu Selamat, Nurul Azma Zakaria. Analysis of Cybersecurity Standard and Framework Components // *International Journal of Communication Networks and Information Security*. – 2020. – Т. 12, № 3. – С. 417–432. – DOI: 10.17762/ijcnis.v12i3.4817.

Волинець Віталій Володимирович – аспірант групи 125-24а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: volynets1026@gmail.com

Войтович Олеся Петрівна – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail voytovych.olesya@vntu.edu.ua

Volynets Vitalii V. – Faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: volynets1026@gmail.com

Voytovych Olesya P. – Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail voytovych.olesya@vntu.edu.ua