КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3(19), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.19.4655
УДК 004.49

Курій Євгеній Олегович
Асистент кафедри “Захист інформації”
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0002-3423-5655
yevhenii.o.kurii@lpnu.ua

Опірський Іван Романович
д.т.н., проф., професор кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

ISO 27001: АНАЛІЗ ЗМІН ТА ОСОБЛИВОСТІ ВІДПОВІДНОСТІ НОВІЙ ВЕРСІЇ СТАНДАРТУ

Анотація. Управління інформаційною безпекою в організації може бути складним завданням, особливо враховуючи те, що ця діяльність може охоплювати багато сфер, від фізичної та мережевої безпеки до безпеки людських ресурсів і управління постачальниками послуг. Саме тут стають у нагоді фреймворки інформаційної безпеки, які допомагають формалізувати і уніфікувати процес розробки та реалізації стратегії безпеки.
Незважаючи на те, що існує безліч різноманітних фреймворків інформаційної безпеки, найбільш поширеним і використовуваним в усьому світі є ISO/IEC 27001. Він поєднує в собі як досить повний набір засобів контролю безпеки, щоб охопити найважливіші сфери безпеки, так і широку застосовність, що дозволяє впроваджувати цей фреймворк для всіх типів організацій.
Проте кіберпростір постійно змінюється, і компаніям потрібно також адаптувати свої підходи до організації процесів інформаційної безпеки. Для реагування на нові виклики і загрози кібербезпеки, Міжнародна організація зі стандартизації (англ. International Organization for Standardization) наприкінці 2022 опублікувала оновлену редакцію стандарту ISO/IEC 27001:2022, яку відтепер повинні брати до уваги усі організації, які мають на меті впровадити та сертифікувати свою систему управління інформаційною безпекою.
Метою статті є короткий огляд нової редакції популярного стандарту, і ключових змін у структурі та описі контролів безпеки, а також розробка рекомендацій для досягнення відповідності вимогам оновленої версії стандарту.

Ключові слова: інформаційна безпека, кібербезпека, ISO/IEC 27001:2013, ISO/IEC 27001:2022, фреймворк інформаційної безпеки, система управління інформаційною безпекою.

ВСТУП

Оскільки кіберзагрози стають все більш прогресивними, а їх кількість продовжує зростати, потреба в оновленні практик інформаційної безпеки ніколи не була більш істотною [1,2]. На початку 2022 року ISO опублікувала оновлену версію стандарту ISO/IEC 27002:2022 [3], що сигналізувало про близьке оновлення і основного стандарту ISO/IEC 27001.

Для вирішення зростаючих глобальних проблем кібербезпеки та підвищення цифрової довіри, наприкінці 2022 року була опублікована оновлена покращена версія стандарту ISO/IEC 27001 [4]. Найвідоміший у світі стандарт управління інформаційною безпекою допомагає організаціям захистити свої інформаційні активи, що є життєво важливим у сучасному цифровому світі.

Постановка проблеми. Міжнародні стандарти ISO/IEC 27001/02 [5,6] допомагають організаціям різних секторів забезпечувати конфіденційність, цілісність та доступність інформації за рахунок застосування процесу управління ризиками та надає впевненості зацікавленим сторонам у тому, що ризики адекватно оцінюються та управляються.

На сьогодні даний стандарт є одним із найпопулярніших фреймворків інформаційної безпеки у світі. За відносно недавніми даними статистики [7], у 2020 році більше 44 000 організацій по всьому світу бути сертифіковані відповідно до вимог ISO/IEC 27001, і відомо, що протягом пандемії ця цифра тільки зросла. Із виходом нової редакції стандарту, всі ці компанії опинилися перед проблемою адаптації існуючої системи менеджменту інформаційної безпеки до вимог нового стандарту.

Хоча ISO передбачає певний період переходу, протягом якого "співіснують" дві версії стандарту [8], і компанії можуть адаптувати свої процеси до нових вимог, цей процес не є швидким і потребує тим більше зусиль, чим більшою і організаційно складнішою є компанія.

Аналіз останніх досліджень і публікацій. У відповідь на глобальні загрози кібербезпеки, у жовтні 2022 року Міжнародна організація зі стандартизації (англ. International Organization for Standardization) опублікувала оновлену версію найпопулярнішого стандарту у сфері інформаційної безпеки - ISO/IEC 27001:2022 – Інформаційна безпека, кібербезпека та захист конфіденційності – Системи управління інформаційною безпекою – Вимоги.

Кіберзлочинність стає все більш складним і небезпечним фактором, оскільки хакери розробляють все новіші методи для вчинення кіберзлочинів. У звіті Всесвітнього економічного форуму про перспективи глобальної кібербезпеки вказується [9], що кількість кібератак у всьому світі зросла на 125% у 2021 році, і дані свідчать про те, що зростання продовжуватиметься і в 2022-2023 роках. У цьому змінному ландшафті кіберзагроз, організації змушені застосувати стратегічний підхід до управління ризиками кібербезпеки.

Відповідно, щоб подолати існуючі проблеми кібербезпеки, організації повинні підвищувати свою стійкість і вживати заходів для зменшення рівня і протидії кіберзагрозам. В цьому непростому завданні значну користь може принести використання стандарту ISO/IEC 27001 у якості фреймворку інформаційної безпеки, що допомагає вирішити наступні задання [10]:

- Захистити інформацію в усіх формах, включаючи паперові, хмарні та цифрові дані
- Підвищити стійкість до кібератак;
- Впровадити централізовано керовану структуру, яка захищає всю інформацію компанії;
- Забезпечити захист усієї організації, зокрема від технологічних ризиків та інших загроз;
- Вчасно реагувати на нові загрози безпеці;
- Зменшити витрати на неефективні охоронні технології;
- Захистити цілісність, конфіденційність та доступність даних.

Мета статті. Метою статті є дослідження і аналіз істотних змін у новій редакції міжнародного стандарту ISO/IEC 27001 у порівнянні із попередньою версією 2013 року та розробка рекомендацій по переходу організацій із раніше впровадженим стандартом ISO 27001 на нову версію.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Що змінилося в стандарті ISO/IEC 27001:2022

Хороша новина полягає в тому, що багато змін є редакційними, наприклад, зміна формулювання «міжнародний стандарт» на «документ» та зміна чи ре-організація порядку фраз, щоб забезпечити кращий міжнародний переклад [11].

Також були зроблені зміни для узгодження з принципом гармонізації (англ. harmonized) який пропагує ISO.

Деякі з ключових змін нещодавно оновленого ISO/IEC 27001:2022 такі:

- Назву стандарту було змінено відповідно до ISO/IEC 27002:2022. Нова назва ISO/IEC 27001:2022 – Інформаційна безпека, кібербезпека та захист конфіденційності – Системи управління інформаційною безпекою – Вимоги;
- Назва Додатку А також змінилася з Довідкові цілі контролів та контролі (Reference control objectives and controls) на Довідка про контролі інформаційної безпеки (Information security controls reference);
- Додаток А пролінкований до контролів з ISO 27002:2022. Новий Додаток А тепер містить 93 контролі та включає таку інформацію як назва контролю і безпосередньо опис самого контролю;
- Присутні незначні зміни у використовуваній термінології, формулюваннях і структурі в пунктах 4-10, зокрема в пунктах 4.2, 6.2, 6.3 і 8.1;
- У пункті 6.1.3 c) було переглянуто і змінено примітки. Слово «контроль» було замінено на «контроль інформаційної безпеки», а цілі контролю вилучено;
- У пункті 6.1.3 d) було змінено формулювання для уникнення двозначності;
- Додано вимогу щодо визначення процесів, необхідних для впровадження СУІБ, та їх взаємодії;
- Додано вимогу повідомляти зацікавленим сторонам про організаційні ролі, що стосуються інформаційної безпеки в організації;
- Додано новий пункт 6.3 – Планування змін;
- Додано нову вимогу щодо того, щоб організація вирішила, як комунікувати важливу інформацію (частина пункту 7.4);
- Додано нові вимоги щодо встановлення критеріїв операційних процесів та здійснення їх контролю

Основні зміни, однак, стосуються оновлень поточних контролів в Додатку А, щоб краще узгодити стандарт із нещодавніми змінами до ISO/IEC 27002 – Інформаційна безпека, кібербезпека та захист конфіденційності [12].

Структура контролів

Додаток А стандарту ISO/IEC 27001:2022 містить зміни як у кількості контролів, так і в їх переліку в групах.

Кількість контролів в Додатку А зменшилася зі 114 до 93. Зменшення кількості контролів здебільшого відбулося внаслідок об’єднання багатьох із них [13]:

- 35 контролів залишилися незмінними зі зміною контрольного номера та реорганізацією на 4 секції;
- Додано 11 нових контролів;
- 23 контролі перейменовано для кращого розуміння;
- Незважаючи на те, що кількість контролів було зменшено (зі 114 до 93), ні одного контролю не було виключено;
- 57 контролів було об’єднано в 24 контролі;

- 1 контроль було розділено. Контроль 18.2.3 Огляд технічної відповідності було розділено на:
  - 5.3.6 – Відповідність політикам, правилам і стандартам інформаційної безпеки;
  - 8.8 – Управління технічними вразливостями.

Загалом, 93 контролі були реорганізовані в чотири групи або секції.

- A.5 Організаційні контролі (Organizational controls) - містить 37 контролів;
- A.6 Контролі направлені на людей (People controls) - містить 8 контролів;
- A.7 Фізичні контролі (Physical controls) - містить 14 контролів;
- A.8 Технологічні контролі (Technological controls) - містить 34 контролі.

Нові контролі безпеки

ISO/IEC 27001:2022 також додав згадані вище 11 нових контролів до Додатку А:

1. Дані про кіберзагрози (Threat intelligence);
2. Інформаційна безпека при використанні хмарних сервісів (Information security for the use of cloud services);
3. Готовність (підготовка) інформаційних і телекомунікаційних технологій для забезпечення безперервності бізнесу (ICT readiness for business continuity);
4. Моніторинг фізичної безпеки (Physical security monitoring);
5. Управління налаштуваннями (Configuration management);
6. Видалення інформації (Information deletion);
7. Маскування даних (Data masking);
8. Запобігання витокам даних (Data leakage prevention);
9. Моніторингова діяльність / Діяльність по моніторингу (Monitoring activities);
10. Веб-фільтрація (Web filtering);
11. Безпечне кодування (Secure coding).

Детальніший опис нових елементів керування а також рекомендовані активності для здійснення переходу на нову версію стандарту наведений у таблиці нижче.

Таблиця 1.

Опис нових елементів керування та рекомендовані активності згідно ISO27001:2022

Пункт	Назва контролю	Контроль	Мета	Активності
A.5.7	Дані про кіберзагрози	Інформація, що стосується загроз інформаційної безпеки, збирається та аналізується для отримання інформації про загрози.	Розуміння зловмисників і їхніх методів у контексті вашого IT-ландшафту.	• Оновити політику управління технічними вразливостями • Оновити документ із контактами з зацікавленими групами

A.5.23	Інформаційна безпека при використанні хмарних сервісів	Процеси отримання доступу, використання, управління та виходу з хмарних сервісів повинні бути встановлені відповідно до вимог організації до інформаційної безпеки.	Всебічний розгляд і впровадження стратегії управління, користування і виходу з хмарних сервісів.	• Створити/оновити реєстр третіх сторін, провести їхню оцінку
A.5.30	Готовність інформаційних і телекомунікаційних технологій для забезпечення безперервності бізнесу	Готовність інформаційних і телекомунікацій-них технологій планується, впроваджується, підтримується та перевіряється на основі цілей безперервності бізнесу та вимог безперервності інформаційних і телекомунікацій-них технологій.	Визначення і впровадження вимог щодо IT-інфраструктури на основі загальних бізнес процесів та можливості відновлення операційних можливостей.	• Оновити план безперервності бізнесу і відповідні плани відновлення
A.7.4	Моніторинг фізичної безпеки	Приміщення повинні постійно контролюватися на предмет несанкціонованого фізичного доступу.	Використання сигналізації та моніторингових систем для запобігання неавторизованому фізичному доступу.	• Оновити політику фізичного захисту • Налаштувати додаткові контролі моніторингу
A.8.9	Управління налаштуваннями	Налаштування, в тому числі налаштування безпеки, апаратного забезпечення, програмного забезпечення, послуг і мереж повинні бути встановлені, задокументовані, реалізовані, контрольовані та перевірені.	Зміцнення та безпечне налаштування IT-систем.	• Створити конфігураційну документацію (бейслайни) для ключових систем і сервісів (сервери, мережеве обладнання, робочі станції і т.д.)

ISSN 2663 - 4023

A.8.10	Видалення інформації	Інформація, що зберігається в інформаційних системах, на пристроях або будь-яких інших носіях інформації, повинна видалятися, коли вона більше не потрібна.	Дотримання зовнішніх вимог пов'язаних із захистом даних і концепціями видалення даних.	• Оновити політику класифікації інформації
A.8.11	Маскування даних	Маскування даних повинно використовуватися відповідно до політики організації щодо контролю доступу та інших пов'язаних тематичних політик, а також бізнес-вимог, беручи до уваги застосовні законодавчі вимоги.	Підвищення рівня захисту інформації за рахунок використання технік маскування даних таких як анонімізація та псевдонімізація	• Оновити політику класифікації інформації
A.8.12	Запобігання витокам даних	Заходи запобігання витоку даних повинні застосовуватися до систем, мереж і будь-яких інших пристроїв, які обробляють, зберігають або передають конфіденційну інформацію.	Впровадження методів і засобів для запобігання витоку чутливих даних.	• Встановити систему захисту від витоку даних (DLP system) • В іншому випадку, встановити компенсаційні контролі або переглянути і прийняти ризик
A.8.16	Моніторингова діяльність	Мережі, системи та програми слід відстежувати на предмет аномальної поведінки та вживати відповідних дій для оцінки потенційних інцидентів інформаційної безпеки.	Детектування аномалій у мережі і системах за рахунок моніторингу безпеки мережі і поведінки систем і додатків.	• Оновити політику по логуванню і моніторингу • Встановити систему для збору і аналізу подій (SIEM system)

A.8.23	Веб-фільтрація	Доступом до зовнішніх веб-сайтів повинен бути під контролем задля зменшення впливу шкідливого вмісту.	Запобігання перегляду користувачами певних URL-адрес, що містять шкідливий код.	• Оновити політику захисту від шкідливого програмного • Встановити і налаштувати функцію веб-фільтрування
A.8.28	Безпечне кодування	До розробки програмного забезпечення повинні застосовуватися принципи безпечного кодування.	Забезпечення безпечного кодування за рахунок використання спеціалізованих інструментів, коментування, відслідковування змін і уникнення небезпечних методів програмування.	• Забезпечити виконання циклу безпечної розробки для внутрішніх проектів по розробці

Як видно з таблиці, нові контролі є, по суті, доповненням і певним розширенням існуючих доменів попередньої версії стандарту. Тому вони можуть бути відносно легко інтегровані в існуючі процеси організації, система управління інформаційною безпекою якої побудована на основі ISO 27001:2013.

ВИСНОВКИ

Хоч нова версія стандарту і направлена на реагування на змінений ландшафт загроз, у зв'язку із універсальністю попередньої версії, основні міни торкнулися здебільшого структури стандарту і формулювання описів контролів. Було додано 11 нових контролів інформаційної безпеки, які досить легко впровадити у межах існуючих процесів, або які взагалі можуть бути вже наявними в організації, оскільки давно вважаться галузевими хорошими практиками.

Зокрема, щоб бути у відповідності із оновленою редакцією стандарту, необхідно виконати наступні кроки:

1. Компанії повинні переглянути свій реєстр ризиків і застосовані засоби обробки ризиків, щоб забезпечити відповідність переглянутому стандарту.

2. Оновити Заяву про Застосовність (Statement of Applicability - SoA), щоб узгодити її з оновленим Додатком А.

3. Переглянути та оновити свою документацію, включаючи політики та процедури, щоб відповідати новим контролям.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Susukailo, V., Opirsky, I., Yaremko, O. (2021). Methodology of ISMS Establishment Against Modern Cybersecurity Threats. У *Lecture Notes in Electrical Engineering* (с. 257–271). Springer International Publishing. https://doi.org/10.1007/978-3-030-92435-5_15

2 Kurii, Y. Opirskyy, I. (2021). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. *Paper presented at the CEUR Workshop Proceedings, 3288*, 21-32.
3 (2022) ISO/IEC 27002: Information security, cybersecurity and privacy protection — Information security controls. URL: https://www.iso.org/standard/75652.html
4 (2022) ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/82875.html
5 (2013) ISO/IEC 27001: Information Technology — Security Techniques — Information Security Management Systems — Requirements. URL: https://www.iso.org/standard/54534.html
6 (2013) ISO/IEC 27002: Information Technology — Security Techniques — Code of Practice for Information Security Controls. URL: https://www.iso.org/standard/54533.html
7 2020 ISO Survey of Management System Standards reveals 17% increase in certifications. Режим доступу до ресурсу: https://www.quality.org/article/2020-iso-survey-management-system-standards-reveals-17-increase-certifications
8 MSECB Transition Policy on Management System Certification to ISO/IEC 27001:2022. https://msecb.com/wp-content/uploads/2023/01/MSECB-Transition-Policy-on-MS-Certification-to-ISO-IEC-27001.pdf?utm_source=sendinblue&utm_campaign=Clients%20ISOIEC%20270012022%20Transition%20Policy&utm_medium=email
9 Global Cybersecurity Outlook 2022. https://www.weforum.org/reports/global-cybersecurity-outlook-2022
10 ISO/IEC 27001: What's new in IT security? https://www.iso.org/contents/news/2022/10/new-iso-iec-27001.html
11 What Are The ISO 27001 Changes In 2022. https://bestpractice.biz/what-are-the-iso-27001-changes-in-2022/
12 ISO 27001 2013 vs. 2022 revision – What has changed? https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/
13 ISO/IEC 27001 - What are the main changes in 2022? https://pecb.com/article/isoiec-27001---what-are-the-main-changes-in-2022

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

Yevhenii O. Kurii
Cybersecurity department assistant
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-3423-5655
yevhenii.o.kurii@lpnu.ua

Ivan R. Opirskyy
Dc.S., Professor, Professor of Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

ISO 27001: ANALYSIS OF CHANGES AND COMPLIANCE FEATURES OF THE NEW VERSION OF THE STANDARD

Abstract. Managing information security in the organization may be a daunting task, especially considering that it may encompass many areas from physical and network security to human resources security and management of suppliers. This is where security frameworks come in handy and put formality into the process of the design and implementation of the security strategy.
While there are a bunch of different information security frameworks out in the wild, the most commonly-found and preferred by security professionals worldwide is ISO/IEC 27001. It combines both the quite comprehensive set of security controls to cover the most important security areas and wide applicability which allows applying this framework to all kinds of organizations.
While cyberspace is constantly changing, companies should also adapt their approaches to the organization of information security processes. In order to respond to new challenges and threats to cyber security, the International Organization for Standardization (ISO) at the end of 2022 has published an updated version of the ISO/IEC 27001:2022 standard, which from now on should be taken into account by all organizations that aim to implement and certify its information security management system (ISMS).
The purpose of this article is to provide a brief overview of the new edition of the popular standard, фтв describe the key changes in the structure and description of security controls; as well as develop recommendations for achieving compliance with the requirements of the updated version of the standard.

Keywords: information security, cybersecurity, ISO/IEC 27001:2013, ISO/IEC 27001:2022, information security framework, information security management system.

REFERENCES

1 Susukailo, V., Opirsky, I., Yaremko, O. (2021). Methodology of ISMS Establishment Against Modern Cybersecurity Threats. У *Lecture Notes in Electrical Engineering* (с. 257–271). Springer International Publishing. https://doi.org/10.1007/978-3-030-92435-5_15
2 Kurii, Y. Opirskyy, I. (2021). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. *Paper presented at the CEUR Workshop Proceedings, 3288*, 21-32.
3 (2022) ISO/IEC 27002: Information security, cybersecurity and privacy protection — Information security controls. URL: https://www.iso.org/standard/75652.html
4 (2022) ISO/IEC 27001: Information security, cybersecurity and privacy protection — Information security management systems — Requirements. URL: https://www.iso.org/standard/82875.html
5 (2013) ISO/IEC 27001: Information Technology — Security Techniques — Information Security Management Systems — Requirements. URL: https://www.iso.org/standard/54534.html
6 (2013) ISO/IEC 27002: Information Technology — Security Techniques — Code of Practice for Information Security Controls. URL: https://www.iso.org/standard/54533.html
7 2020 ISO Survey of Management System Standards reveals 17% increase in certifications. Режим доступу до ресурсу: https://www.quality.org/article/2020-iso-survey-management-system-standards-reveals-17-increase-certifications
8 MSECB Transition Policy on Management System Certification to ISO/IEC 27001:2022. https://msecb.com/wp-content/uploads/2023/01/MSECB-Transition-Policy-on-MS-Certification-to-ISO-IEC-

27001.pdf?utm_source=sendinblue&utm_campaign=Clients%20ISOIEC%20270012022%20Transition%20Policy&utm_medium=email
9 Global Cybersecurity Outlook 2022. https://www.weforum.org/reports/global-cybersecurity-outlook-2022
10 ISO/IEC 27001: What's new in IT security? https://www.iso.org/contents/news/2022/10/new-iso-iec-27001.html
11 What Are The ISO 27001 Changes In 2022. https://bestpractice.biz/what-are-the-iso-27001-changes-in-2022/
12 ISO 27001 2013 vs. 2022 revision – What has changed? https://advisera.com/27001academy/blog/2022/02/09/iso-27001-iso-27002/
13 ISO/IEC 27001 - What are the main changes in 2022? https://pecb.com/article/isoiec-27001---what-are-the-main-changes-in-2022