УДК 004.05
DOI: 10.31673/2409-7292.2025.023969

Кухарська Н.П., Семенюк С.А., Полотай О.І.

КЛЮЧОВІ АСПЕКТИ ОНОВЛЕНОГО СТАНДАРТУ ISO/IEC 27002:2022

У статті проаналізовано основні зміни внесені в ISO/IEC 27002:2022 – стандарт, що містить детальні настанови щодо впровадження заходів забезпечення інформаційної безпеки. Зокрема, розглянуто ключове оновлення, яке стосується скорочення кількості заходів безпеки (засобів контролю) з 114 до 93 шляхом їх об'єднання та оптимізації. Звернено увагу на нову структуру класифікації, згідно якої засоби контролю тепер поділяються на чотири категорії: організаційні, людські, фізичні та технологічні. Детально розглянуто ще одне нововведення – запровадження атрибутів, використання яких дає змогу ефективніше фільтрувати, групувати та застосовувати заходи безпеки відповідно до специфічних потреб організації. Також у статті описано 11 нових засобів контролю, а саме: інформаційна безпека при використанні хмарних послуг, готовність ІКТ до безперервності бізнесу, управління конфігурацією, моніторинг фізичної безпеки, видалення інформації, маскування даних, розвідка загроз, запобігання витоку даних, моніторинг діяльності, фільтрація веб-контенту, безпечне кодування. Внесені в ISO/IEC 27002:2022 зміни спрямовані на підвищення адаптивності стандарту до динамічного розвитку інформаційних технологій та задоволення зростаючих потреб організацій у сфері кібербезпеки. Цей стандарт менеджери з безпеки можуть використовувати для вибору, впровадження та документування заходів захисту інформації відповідно до вимог ISO/IEC 27001:2022, що полегшуватиме процес аудиту та сертифікації.

Ключові слова: інформаційна безпека, система управління інформаційною безпекою, стандарт, ISO/IEC 27002:2013, ISO/IEC 27002:2022, заходи безпеки, засоби контролю.

Вступ

У 2022 році міжнародний стандарт з управління інформаційною безпекою ISO/IEC 27001 і його супутній стандарт ISO/IEC 27002 були переглянуті і оновлені вперше за майже десять років. На думку багатьох експертів, це запізнілий крок, враховуючи стрімкий динамічний розвиток інформаційних технологій в останні роки та усталену практику переглядати стандарти на актуальність кожні 5 років. За час дії стандартів попередньої редакції (2013 року) відбулися значні зміни в ландшафті кібербезпеки і на тлі серйозного технологічного прориву очікуються нові. Такі технології, як штучний інтелект, квантові обчислення, Інтернет речей (IoT) швидко вдосконалюються та впроваджуються, відкриваючи при цьому нові можливості як для організацій, так і для зловмисників.

Також за останнє десятиріччя змінилися підходи до організації роботи, зокрема з погляду:

– використання мобільних пристроїв – особливо це стосується тенденції застосування власних пристроїв для потреб організації (BYOD), у період з 2013 по 2022 рік глобальний ринок BYOD зріс із 75,99 мільярдів доларів США [1] до 401 мільярда доларів США [2];

– поширення хмарних технологій – у цей же період кількість активних користувачів хмарних технологій зросла з 26 % [3] до 63 % [4];

– переходу на віддалену роботу – у 2020 році на тлі пандемії коронавірусу, заборони виходити з дому та зупинки роботи громадського транспорту тисячі організацій по всьому світу вимушено перевели співробітників на віддалену форму роботи. Інструменти, які успішно використовував ІТ-сектор, запровадили інші компанії і оцінили плюси дистанційної роботи. Тепер повна або часткова відмова від роботи в офісі стала загальносвітовим трендом.

Усе вище перелічене створило потребу у нових заходах безпеки, які, власне, і пропонують стандарти ISO/IEC 27001 та ISO/IEC 27002 2022 року редакції.

Мета та постановка проблеми

Трирічний період переходу на стандарти ISO/IEC 27001:2022 [5] та ISO/IEC 27002:2022 [6] розпочався з 31 жовтня 2022 року. Незалежно від дати початкової реєстрації чи сертифікації цей термін є обов'язковим для всіх організацій. Сертифікати, видані або перевидані відповідно до стандарту ISO/IEC 27001:2013 протягом перехідного періоду також мають термін дії до 31 жовтня 2025 р. Після цієї дати усі залишкові сертифікати ISO/IEC

27001:2013 будуть анульовані та вважатимуться застарілими, а організації з простроченими сертифікатами ISO/IEC 27001:2013 органами сертифікації розглядатимуться як нові клієнти за умови повного первинного аудиту.

Маючи на меті допомогти організаціям, які вже знайомі із ISO/IEC 27001 та ISO/IEC 27002 редакції 2013 року, максимально оперативно перейти на стандарти редакції 2022 року, у цій статті детально розглянемо та проаналізуємо усі ключові зміни стандарту ISO/IEC 27002:2022.

Виклад основного матеріалу дослідження

ISO/IEC 27002 – це стандарт інформаційної безпеки, опублікований Міжнародною організацією зі стандартизації (англ. International Organization for Standardization, ISO) та Міжнародною електротехнічною комісією (англ. International Electrotechnical Commission, IEC).

Стандарт ISO/IEC 27002 надає еталонний набір засобів контролю інформаційної безпеки, кібербезпеки та захисту конфіденційності, а також загальні настанови щодо їх впровадження на основі міжнародно визнаних передових практик. Загалом кажучи, він дає вказівки щодо впровадження системи управління інформаційною безпекою згідно стандарту ISO/IEC 27001. І хоча ISO/IEC 27002 сам по собі не є тим стандартом, на відповідність якому організації підлягають сертифікуванню, дотримання його настанов щодо інформаційної безпеки, фізичної безпеки, кібербезпеки та управління конфіденційністю наближує будь-яку організацію на один крок до виконання вимог сертифікації стандарту ISO/IEC 27001.

Розглянемо зміни, внесені у 2022 році у стандарт ISO/IEC 27002, а отже, і у Додаток А до стандарту ISO/IEC 27001, оскільки вони є узгоджені. У таблиці 1 наведено зміни високого рівня.

Таблиця 1

Огляд основних змін стандарту ISO/IEC 27002:2022

Область оновлення	**ISO/IEC 27002:2013**	**ISO/IEC 27002:2022**	**Коментар**
Назва	Information technology – Security techniques – Code of practice for information security controls.	Information security, cybersecurity and privacy protection – Information security controls.	“Code of practice” вилучено з назви, щоб краще відобразити мету стандарту як еталонного набору засобів контролю інформаційної безпеки. Що стосується першої частини назви, то вона пов’язана з назвою стандарту ISO/IEC 27001:2022.
Кількість сторінок	90 сторінок.	164 сторінок.	Обсяг стандарту редакції 2022 року збільшився на 82 %. Значна частина засобів контролю тепер містить більш детальні настанови; для кожного засобу контролю подана таблиця, що визначає його атрибути, а також з’явилися два додатки, яких досі не було.
Кількість засобів контролю (елементів управління)	114	93	Стандарт 2022 року значно більший за кількістю сторінок у порівнянні з редакцією 2013 року, тому може бути незрозумілим той факт, що він містить менше засобів контролю. На це є пояснення: у новій редакції стандарту об’єднано велику кількість елементів управління. 56 засобів контролю з стандарту ISO/IEC 27002:2013 було об’єднано у 24 засоби контролю у стандарті ISO/IEC 27002:2022, що є природнім результатом структурних змін, про які мова буде йти нижче. Щоправда, що стосується реалізації та аудиту, то організації тепер мають більше роботи.

© Кухарська Н.П., Семенюк С.А., Полотай О.І. (2025). Ключові аспекти оновленого стандарту ISO/IEC 27002:2022. Сучасний захист інформації, 2(62), 76–87.
https://doi.org/10.31673/2409-7292.2025.023969

Область оновлення	ISO/IEC 27002:2013	ISO/IEC 27002:2022	Коментар
Групування засобів контролю	14 розділів, кожен з яких відображає конкретну сферу безпеки, наприклад, політика інформаційної безпеки, організація інформаційної безпеки, безпека людських ресурсів, управління ресурсами СУІБ, контроль доступу, криптографія тощо.	4 “теми”, які класифікують засоби контролю за сферами безпеки, яких вони стосуються: “організаційний”, “людський”, “фізичний” і “технологічний” контроль.	Ширший підхід, використаний у стандарті 2022 року, відображає більш прозору структуру засобів управління, про яку йтиме мова у наступному рядку таблиці.
Структурування заходів безпеки	Три рівні: 1. Розділ заходів безпеки (14). 2. Основна категорія безпеки (35). 3. Захід безпеки (114).	Два рівні: 1. Тема (4). 2. Захід безпеки (93).	Структуру засобів контролю було зведено з трьох до двох рівнів, що призвело до різкого збільшення обсягу другого рівня. Однак запровадження “атрибутів” (див. наступний рядок таблиці), які можна використовувати для фільтрування засобів контролю, дає змогу сподіватись, що такий дворівневий підхід не створюватимете незручностей у використанні.
Атрибути	Без атрибутів, стандарт містив додатковий (третій) структурний рівень (про що йдеться рядком вище).	У стандарт введено п’ять атрибутів: тип засобу контролю, властивості інформаційної безпеки, концепції кібербезпеки, операційні можливості та домени безпеки. Це різні способи класифікації засобів контролю, що не залежать від згаданих вище чотирьох тем.	Як пояснює ISO/IEC 27002:2022 у пункті 4.2, “Атрибути можна використовувати для фільтрування, сортування або представлення засобів контролю у різних поданнях”. Оскільки за допомогою атрибутів можна створювати багато різних представлень, то перехід на дворівневу структуру є оправданим. Атрибути мають допомогти спростити процес вибору відповідних засобів контролю.
Макет засобів контролю	Назва категорії та ціль (що охоплює кілька засобів контролю), назва засобу контролю, його опис, настанови щодо впровадження та інша інформація (наприклад, деякі юридичні нюанси та посилання на інші стандарти).	Назва засобу контролю, таблиця атрибутів, опис засобу контролю, ціль засобу контролю, настанови щодо впровадження та інша інформація (якісь пояснення чи посилання на відповідні документи).	Стандарт 2022 року надає більше інформації щодо кожного засобу контролю, хоча єдиним дійсно новим елементом є таблиця атрибутів. Оскільки зараз немає еквіваленту категорій, їх назви вилучено. Цілі включено до стандарту 2022 року у вигляді розділу “призначення” для кожного засобу контролю. Настанови щодо впровадження для більшості засобів контролю є значно детальнішими у порівнянні із стандартом 2013 року редакції.
Додатки	Немає.	Два.	Перший додаток пояснює, як використовувати атрибути. У другому додатку заходи безпеки 2022 року порівнюються з набором 2013 року.

Таблиця 2 детально описує атрибути, запроваджені у стандарті ISO/IEC 27002:2022 та пояснює їх значення.

Таблиця 2

Огляд атрибутів стандарту ISO/IEC 27002:2022 та опис їх значень

Атрибут	**Опис атрибуту**		**Значення атрибута**	**Опис значення**
Тип засобу контролю	Атрибут, який описує як і коли засіб контролю змінює ризик інцидентів інформаційної безпеки.	1	Превентивний	Засіб контролю, застосування якого запобігає виникненню інциденту інформаційної безпеки.
		2	Детективний	Засіб контролю, застосування якого дієве під час інциденту інформаційної безпеки.
		3	Коригувальний	Засіб контролю, який застосовується після інциденту інформаційної безпеки.
Властивості інформа-ційної безпеки	Атрибут вказує на характеристику(и) інформації, збереження якої(их) забезпечує застосування засобу контролю.	1	Конфіденційність	“Властивість, згідно якої інформація не надається або не розкривається неавторизованим особам, організаціям або процесам” (пункт 3.10 ISO/IEC 27000:2020).
		2	Цілісність	“Властивість точності та повноти” (пункт 3.36 ISO/IEC 27000:2020).
		3	Доступність	“Властивість бути доступною і придатною для використання на вимогу авторизованої особи” (пункт 3.7 ISO/IEC 27000:2020).
Концепції кібер-безпеки	Атрибут, що вказує на визначену(і) в ISO/IEC TS 27110:2021 концеп-цію(ї) кібербезпеки, під яку(і) підпадає засіб контролю. Ці концепції узгоджуються також з п’ятьма функціями NIST Cybersecurity Framework (CSF).	1	Ідентифікація	Вироблення розуміння органі-зацією управління ризиками кібербезпеки щодо систем, ресурсів, даних та можливостей.
		2	Захист	Розроблення та впровадження відповідних запобіжних заходів для забезпечення надання послуг; захист ресурсів від неправильного використання, навмисного чи ненавмисного.
		3	Виявлення	Виявлення випадків, коли ресурси можуть бути або вже були використані неналежним чином (тобто виявлення інцидентів).
		4	Реагування	Стримування та пом’якшення виявленого інциденту.
		5	Відновлення	Розроблення та впровадження відповідних заходів для підтримки планів щодо забезпечення стійкості та для відновлення порушених можливостей або послуг після інцидентів.
Операційні можливості	Цей атрибут найбільше пов’язаний із поло-женнями щодо заходів безпеки стандарту ISO/IEC 27002:2013. Він вказує фахівцям на можливості, які має контроль інформаційної безпеки.	1	Керівництво	Потребує уваги з боку вищого керівництва.
		2	Управління_ресурсами	Управління ресурсами шляхом їх відстеження та контролю за їхнім використанням.
		3	Захист_інформації	Захист чутливої та/або конфіденційної інформації.
		4	Безпека_людських_ ресурсів	Заходи безпеки, пов’язані з персоналом, як-от навчання.

Атрибут	Опис атрибуту		Значення атрибута	Опис значення
		5	Фізична_безпека	До заходів забезпечення фізичної безпеки інформації належать, наприклад, заходи, пов'язані зі зниженням екологічних загроз
		6	Безпека_систем_і_мереж	Захист систем і мереж, які або зберігають інформацію, або мають доступ до неї, або впливають на її безпеку.
		7	Безпека_застосунків	Захист застосунків, які або зберігають інформацію, або мають до неї доступ, або впливають на її безпеку.
		8	Налаштування_забезпечення	Налаштування, наприклад, програмного забезпечення, відповідно до принципів необхідності знань та найменших привілеїв.
		9	Управління_ідентифікацією_та_доступом	Надання доступу до інформації та інформаційних систем лише авторизованим особам, які мають підтвердити свою ідентичність.
		10	Управління_загрозами_та_вразливостями	Відстеження загроз і вразливостей та їх зниження.
		11	Забезпечення_безперервності_бізне-су	Гарантування того, що критичні бізнес-функції можуть продовжувати працювати на прийнятному рівні під час інциденту безпеки.
		12	Безпека_відносин_з_постачальниками	Захист ланцюга постачання з метою зниження ризиків порушення ІБ з боку третіх сторін.
		13	Юридична_відповідність_питання	Вирішення питань безпеки, що стосуються юридичних, статутних, регуляторних та договірних вимог.
		14	Управління_подіями_інформаційної безпеки	Управління подіями інформаційної безпеки (наприклад, їх реєстрація у журналі) для виявлення та розслідування інцидентів безпеки.
		15	Забезпечення_інформаційної безпеки	Перегляд засобів контролю для вироблення впевненості щодо інформаційної безпеки.
Домени безпеки	Засіб класифікації заходів контролю за широкими категоріями безпеки та управління	1	Управління та екосистема	Охоплює управління безпекою загалом та управління ризиками.
		2	Захист	Охоплює такі області, як: архітектура IT-безпеки та обслуговування, управління ідентифікацією та доступом, тощо.
		3	Оборона	Стосується діяльності з виявлення та управління інцидентами.
		4	Стійкість	Охоплює такі області, як безперервність операцій та управління кризами.

У стандарті ISO/IEC 27002:2022 для кожного засобу контролю атрибути подано у формі, структура якої наведена у таблиці 3.

Таблиця 3

Приклад таблиці атрибутів у стандарті ISO/IEC 27002:2022

Тип засобу контролю	**Властивості інформаційної безпеки**	**Концепції кібербезпеки**	**Операційні можливості**	**Домени безпеки**
#Превентивний	#Конфіденційність #Цілісність #Доступність	#Ідентифікація	#Керівництво	#Управління_та_ екосистема #Стійкість

Слід звернути увагу на те, що:

– кожному значенню атрибута передує хеш тег, щоб його можна було легше знайти;

– будь-який атрибут може мати більше одного значення.

Також у стандарті зазначено, що організації можуть відмовитися від будь-якого пропонованого ним атрибуту. Зрештою, атрибути та їх значення є класифікаціями, призначеними для полегшення пошуку потрібних засобів контролю – вони не підлягають аудиту і не беруться до уваги під час сертифікації за стандартом ISO/IEC 27001:2022. Таким чином, кожен фахівець (організація) може користуватися атрибутами та інтерпретувати їх значення так, як йому зручно. Той факт, що більшість значень атрибутів не мають формальних визначень, говорить про правильність цих міркувань.

Атрибути, визначені стандартом ISO/IEC 27002:2022, можна застосовувати, якщо у цьому є потреба, і до засобів контролю, розроблених в організації її менеджерами безпеки.

Також у стандарті зазначено, що організації можуть створювати власні атрибути та їх значення, пропонуючи у розділі А.2 такий чотирикроковий підхід:

– необхідно зрозуміти чому для організації є потрібним специфічний атрибут і який саме. Ним може бути, наприклад, рівень зрілості, пріоритет чи залучені ресурси;

– слід визначитися з відповідними значеннями атрибутів. Наприклад, для визначення атрибуту “Зрілість” можна скористатися відповідними значеннями із серії ISO/IEC 33000;

– потрібно скопіювати назви та ідентифікатори засобів контролю ISO/IEC 27002 в електронну таблицю чи базу даних і додати відповідні значення атрибутів для кожного засобу контролю;

– далі слід відсортувати електронну таблицю (або сформувати запит у базі даних) для отримання необхідної інформації.

Фактично, це створює власні подання.

Подання – це коли заносять усі засоби контролю та їхні значення атрибутів у електронну таблицю або базу даних, а потім фільтрують чи сортують за певними атрибутами. Подання є ефективним способом спрощення процесу вибору засобів контролю, а також гарантією того, що не буде упущено жодного необхідного контролю. Наприклад, розглядаючи варіанти оброблення певного ризику, ми знаємо, що нам потрібні є детективні засоби контролю і ми їх можемо отримати, фільтруючи за атрибутом “тип засобу контролю” (таблиця 4).

В іншому випадку, наприклад, коли ми вважатимемо, що деякий ресурс потребує захисту своєї цілісності, ми можемо відфільтрувати за “Властивостями інформаційної безпеки”, або, коли для забезпечення загальної безпеки організації бракуватиме заходів для ефективного відновлення після інциденту, то тоді доречним буде фільтрування за “Концепціями кібербезпеки”.

Атрибути також можна використовувати для перевірки повноти вибору засобів контролю. Для цього слід представити вибрані засоби у форматі таблиці 4, наприклад, у вигляді електронної таблиці, а потім перевірити, чи враховані усі типи засобів контролю, властивості інформаційної безпеки, концепції кібербезпеки тощо. Також можна перевірити чи часом не є надмірно або чи недостатньо представлені ті чи інші сфери.

ISO/IEC 27002:2022 запроваджує 11 абсолютно нових засобів контролю, які наведені нижче у таблиці 5. Однак, як можна бачити, якщо організація впровадила набір контролів 2013

року, то, ймовірно, вона вже виконує багато чого з наведеного нижче (хоча, можливо, ще не на необхідному рівні). Тим не менш, є вагома причина розглядати ці заходи як окремі засоби контролю, основним чином, щоб привернути більше уваги до них через їх зростаючу важливість у сучасному ландшафті безпеки. Також є декілька засобів контролю, які є справді новими і зовсім не були охоплені ISO/IEC 27002:2013.

Таблиця 4

Перші два рядки отриманого результату фільтрування засобів контролю за значенням атрибуту #Детективний у розділі “Тип засобу контролю”

	Засіб контролю	**Тип засобу контролю**	**Властивості інформаційної безпеки**	**Концепції кібербезпеки**	**Операційні можливості**	**Домени безпеки**
.7	Розвідка загроз	#Превентивний #Детективний #Коригувальний	#Конфіденційність #Цілісність #Доступність	#Ідентифікація #Виявлення #Реагування	#Управління_загрозами_та_вразливостями	#Оборона #Стійкість
.25	Оцінка та прийняття рішення щодо подій інформаційної безпеки	#Детективний	#Конфіденційність #Цілісність #Доступність	#Виявлення #Реагування	#Управління_подіями_інформаційної_безпеки	#Оборона

Таблиця 5

Огляд нових засобів контролю, запроваджених у стандарті ISO/IEC 27002:2022

Засіб контролю		**Опис контролю ISO/IEC 27002:2022**	**Коментар**
5.7	Розвідка загроз	“Інформація, що стосується загроз інформаційної безпеки, повинна збиратися та аналізуватися для отримання розвідданих про загрози”.	Розвідка загроз є ефективним засобом стеження за середовищем загроз та інформування про заходи щодо зниження ризиків, проте тільки в останні роки вона стала більш застосовною – через що була включена в останню редакцію стандарту. Основні підтеми контролю: типи розвідки загроз, вибір розвідданих та використання отриманої інформації.
5.23	Інформаційна безпека при використанні хмарних послуг	“Процеси придбання, використання, управління та виходу з хмарних послуг повинні бути визначені відповідно до вимог інформаційної безпеки організації”.	Потреба в цьому засобі контролю доволі очевидна: організації зараз більше ніж коли-будь залежать від хмарних послуг. Безпека хмарних сервісів має багато спільного із забезпеченням безпеки інших IT-інфраструктур. Стандарт ISO/IEC 27002:2013 опосередковано охоплював значну частину рекомендацій цього контролю, включаючи аналіз та специфікації вимог інформаційної безпеки (14.1.1), визначення відповідних ролей та обов'язків щодо інформаційної безпеки (6.1.1). Разом з тим, забезпечення безпеки інформації в хмарі пов'язане з унікальними ризиками та викликами. Настанови щодо нового засобу контролю стандарту ISO/IEC 27002:2022 розглядають різні аспекти інформаційної безпеки хмарних послуг, включаючи приклади розглянуті вище, а також визначають на що саме слід звернути увагу в угодах про хмарні послуги.
5.30	Готовність ІКТ до безперервності бізнесу	“Готовність ІКТ повинна бути спланована, впроваджена,	Засіб контролю фокусує увагу на доступності інформації та пов'язаних з нею ресурсів у разі порушення, наприклад, рекомендує застосовувати джерело безперебійного живлення для підтримки роботи ІКТ, щоб організація могла

Засіб контролю		Опис контролю ISO/IEC 27002:2022	Коментар
		підтримувана та протестована на основі цілей безперервності бізнесу та вимог безперервності ІКТ".	продовжувати виконувати свої завдання незалежно від обставин. Цей засіб контролю, ймовірно, міг бути підмножиною 5.29 у наборі контролів стандарту 2022 року (інформаційна безпека під час порушень) або у наборі 17.1 стандарту 2013 року (безперервність інформаційної безпеки). Однак, ISO виокремила цей засіб контролю, щоб підкреслити важливість такої властивості інформації як доступність у межах збереження загальної безпеки ресурсів під час порушення. Стандарт ISO/IEC 27002:2022 рекомендує визначити вимоги до безперервності, проводячи оцінювання впливу на бізнес (BIA).
7.4	Моніторинг фізичної безпеки	"Приміщення повинні постійно моніторитися на предмет несанкціонованого фізичного доступу".	Стандарт ISO/IEC 27002:2013 містив деякі настанови, які надає цей контроль, наприклад, у пункті 11.1.1.f (встановлення систем виявлення зловмисників). Разом з тим, 7.4 по своїй суті є новим засобом контролю. Він рекомендує встановлювати системи відеоспостереження та сигналізації, а також запобігати їх віддаленому відключенню.
8.9	Управління конфігурацією	"Конфігурації, включаючи конфігурації безпеки, обладнання, програмного забезпечення, послуг і мереж повинні бути встановлені, задокументовані, впроваджені, моніторовані та переглянуті".	Безпечна конфігурація є базовим і важливим засобом захисту інформації. Стандарт ISO/IEC 27002:2013 розглядав її переважно у пунктах 12.1.1 (документовані процедури експлуатації) та 12.5.1 (інсталяція програмного забезпечення в системах, що перебувають в експлуатації), але у доволі обмеженому обсязі – не на тому рівні, як це вимагає засіб контролю 8.9 стандарту редакції 2022 року. Створення окремого засобу контролю (8.9) дало змогу узгодити стандарт ISO/IEC 27002 з іншими стандартами передової практики, у тому числі PCI DSS. Основні підтеми нового засобу контролю: визначення шаблонів безпечної конфігурації, управління конфігураціями та моніторинг конфігурацій.
8.10	Видалення інформації	"Інформація, що зберігається в інформаційних системах, пристроях або на будь-яких інших носіях інформації, повинна бути видалена, коли вона більше не потрібна".	Видалення інформації є тією процедурою, основні аспекти якої розглядали різні засоби контролю у стандарті редакції 2013 року, а саме: 8.1.1 (інвентаризація ресурсів СУІБ), 8.1.2 (володіння ресурсами СУІБ) та 11.2.7 (безпечне вилучення або повторне використання обладнання, хоча цей засіб контролю залишився окремим 7.14 у редакції стандарту 2022 року). Однак з 2013 року тема видалення даних та інформації стала набагато більш помітною як окрема практика безпеки та конфіденційності. Наприклад, Загальний регламент про захист даних (General Data Protection Regulation, GDPR), опублікований у 2016 році, визначає "обмеження зберігання" як один з шести ключових принципів обробки даних. Включення у стандарт ISO/IEC 27002:2022 "Видалення інформації" у вигляді окремого засобу контролю дало змогу розробникам узгодити його із сучасними найкращими практиками безпеки. Цей захід безпеки, в основному, пропонує настанови щодо вибору відповідного методу видалення та збору доказів видалення.
8.11	Маскування даних	"Маскування даних повинно використовуватися відповідно до політики організації щодо контролю доступу та інших пов'язаних	Маскування даних – такі як псевдонімізація та анонімізація (вони є основним фокусом цього нового засобу контролю) – зазвичай застосовують для захисту персональних даних (PII). Проте ці заходи можуть бути використані для захисту й інших типів конфіденційних даних, включаючи дані платіжних карток. Оскільки стандарт 2013 року взагалі не розглядав такі техніки, це можна вважати справді новим засобом контролю, ймовірно, запровадженим через те, що ці

Засіб контролю		Опис контролю ISO/IEC 27002:2022	Коментар
		тематичних політик, а також вимог бізнесу, з урахуванням чинного законодавства”.	техніки стали більш поширеними останніми роками, в основному, через законодавство про конфіденційність, таке як GDPR. Крім надання рекомендацій щодо самих технік маскування, контроль також пропонує настанови щодо використання цих технік відповідно до політик контролю доступу: деякі особи повинні мати доступ до немаскованих даних, інші – лише до замаскованих даних. Маскування даних є ефективною технікою безпеки, але не універсальним рішенням.
8.12	Запобігання витоку даних	“Заходи запобігання витоку даних повинні застосовуватися до систем, мереж та будь-яких інших пристроїв, які обробляють, зберігають або передають конфіденційну інформацію”.	Стандарт ISO/IEC 27002:2013 коротко згадував про запобігання витоку інформації як частину деяких заходів контролю, наприклад 8.3.2 (вилучення носіїв), але не охоплював цю тему в повному обсязі, незважаючи на її очевидну важливість у контексті інформаційної безпеки і на доцільність бути її окремим контролем. Настанови цього засобу контролю охоплюють аспекти, які слід враховувати для запобігання витоку даних, а також описують як використовувати інструменти, призначені для цієї цілі. Цей засіб контролю розглядає також поведінкові навички, яким необхідно навчити персонал для запобігання витоку даних.
8.16	Моніторинг діяльності	“Мережі, системи та програми слід відстежувати на предмет аномальної поведінки та вживати відповідних заходів для оцінки потенційних інцидентів інформаційної безпеки”.	Стандарт 2013 року рекомендував організаціям створювати, зберігати та регулярно переглядати журнали подій у контролі 12.4.1 (журнал аудиту подій), що входив до категорії безпеки “Ведення журналів аудиту та моніторинг”. Ведення журналів аудиту та моніторинг, звісно, пов'язані; проте це окремі види діяльності, які потребують окремих настанов, і тому вони розділені на два великі контролі в стандарті 2022 року: 8.15 (журнали аудиту подій) та 8.16 (моніторинг діяльності), опис яких займає майже п’ять сторінок. Також варто зазначити, що настанови щодо моніторингу у наборі контролів 2013 року були надзвичайно обмеженими, і тому, направду, їх можна вважати новим контролем. Нові настанови 8.16 рекомендують, що необхідно враховувати, встановлюючи систему моніторингу. Зокрема, насамперед слід визначити що таке “нормальна” поведінка, щоб потім можна було, відштовхуючись від неї, моніторити, залучаючи автоматизоване програмне забезпечення, та надсилати повідомлення відповідним службам про аномальні події. Система моніторингу також може отримувати інформацію від розвідки загроз (5.7).
8.23	Фільтрація веб-контенту	“Потрібно контролювати доступ до зовнішніх веб-сайтів для зменшення впливу шкідливого контенту”.	Цей контроль, по суті, є розширенням 12.2.1.c із стандарту ISO/IEC 27002:2013, який рекомендував організаціям розглянути “запровадження заходів безпеки, які запобігають чи виявляють використання відомих чи очікувано зловмисних веб-сайтів (наприклад, чорний список)”. Цей новий контроль є не лише підмножиною 8.7 з 2022 року та 12.2 з 2013 року (захист від зловмисного коду). Він крім усього цього розглядає й інші потенційно шкідливі типи контенту, такі як веб-сайти, що поширюють незаконний контент, та “небажані або неприйнятні веб-сайти та веб-застосунки” загалом, які не були охоплені стандартом попередньої редакції. Настанови надають список типів веб-сайтів, які слід розглянути для блокування, а також рекомендують визначити

Засіб контролю		**Опис контролю ISO/IEC 27002:2022**	**Коментар**
			правила безпечного використання онлайн-ресурсів та навчити персонал їх дотримуватися.
8.28	Безпечне кодування	“Принципи безпечного кодування повинні застосовуватися до розроблення програмного забезпечення”.	Оскільки розроблення програмного забезпечення зараз набагато більш поширене, ніж у 2013 році, і продовжує бути зростаючим ринком, що пов’язано, зокрема, з розвитком штучного інтелекту, виникла чітка потреба в цьому новому засобі контролю, теми якого були лише коротко згадані в пункті 14.2.1 (політика безпечного розроблення) стандарту редакції 2013 року. Забезпечення застосування принципів безпечного кодування у процесі розроблення програмного забезпечення гарантуватиме, що у програмне забезпечення потрапить менше вразливостей, а це не тільки зменшить ризики на початковому етапі, але й у подальшому вплине на процес управління безпекою програмного забезпечення, зробить його простішим і дешевшим. Настанови цього засобу контролю насамперед розглядають загальні аспекти, такі як встановлення відповідних процесів і моніторинг реальних загроз і вразливостей, а потім детально описують самі принципи, розділяючи їх на три етапи: до, під час і після кодування.

Загалом, 56 засобів контролю з стандарту ISO/IEC 27002:2013 об’єднані у 24 засоби контролю стандарту ISO/IEC 27002:2022. Більшість із тих об’єднань є очевидними, які навряд чи заплутають тих, хто готується перейти на використання стандарту нової редакції.

З урахуванням цього, у таблиці 6 наведені лише ті об’єднані засоби контролю, які, на нашу думку, найбільш ймовірно можуть спричинити плутанину (здебільшого через питання, куди поділися деякі засоби контролю).

Таблиця 6

Огляд об'єднаних у стандарті ISO/IEC 27002 редакції 2022 року контролів у порівнянні із стандартом редакції 2013 року

ISO/IEC 27002:2013 засіб контролю		**ISO/IEC 27002:2022 засіб контролю**		**ISO/IEC 27002:2022 опис засобу контролю**	**Коментар**
6.1.5	Інформаційна безпе-ка в управлінні проектами	5.8	Інформаційна безпека в управлінні проектами	“Інформаційна безпека повинна бути інтегрована в управління проектами”.	Новий опис засобу контролю 5.8 у значній мірі збігається з описом контролю “Інформаційна безпека в управлінні проектами” (6.1.5) стандарту 2013 року. У той час, засіб контролю “Аналіз та специфікація вимог щодо інформаційної безпеки” (14.1.1) стандарт ISO/IEC 27002:2022 розглядає як підмножину 5.8. Іншими словами, нові або вдосконалені інформаційні системи слід також вважати проектами.
14.1.1	Аналіз і специфікація вимог щодо інформаційної безпеки				
18.1.1	Ідентифікація застосовного законодавства та контрактних вимог	5.31	Юридичні, статутні, регуляторні та договірні вимоги	“Юридичні, статутні, регуляторні та договірні вимоги, що стосуються інформаційної безпеки та підходу організації до виконання цих	Опис засобу контролю 2022 року дуже схожий на опис “Ідентифікація застосовного законодавства та контрактних вимог” (18.1.1) з набору 2013 року. Однак, на відміну від ISO/IEC 27002:2013, оновлений стандарт розглядає виконання таких вимог з точки зору використання
18.1.5	Нормативи щодо криптографічних засобів				

ISO/IEC 27002:2013 засіб контролю		ISO/IEC 27002:2022 засіб контролю		ISO/IEC 27002:2022 опис засобу контролю	Коментар
				вимог, повинні бути ідентифіковані, задокументовані та підтримувані в актуальному стані".	криптографії ("Нормативи щодо криптографічних засобів" (18.1.5) тут виступають як підмножина).
8.3.1	Управління змінними носіями	7.10	Носії інформації	"Носії інформації потрібно контролювати протягом їх життєвого циклу: придбання, використання, транспортування та утилізації відповідно до класифікаційної схеми організації та вимог щодо оброблення".	ISO/IEC 27002:2013 фактично розділив різні етапи життєвого циклу носіїв на окремі заходи контролю, тоді як стандарт 2022 року об'єднав їх в один. Також стандарт нової редакції об'єднав терміни: "змінні носії", "носії" та "обладнання, інформація або програмне забезпечення" в один "носії інформації".
8.3.2	Вилучення носіїв				
8.3.3	Фізичні носії під час передавання				
11.2.5	Переміщення майна				
6.2.1	Політика щодо мобільного обладнання	8.1	Кінцеві пристрої користувачів	"Інформація, що зберігається, обробляється або доступна через кінцеві пристрої користувачів, повинна бути захищена".	Заходи контролю 6.2.1 і 11.2.8 зі стандарту редакції 2013 року стосуються відповідно "мобільних пристроїв" та "обладнання, залишеного без нагляду"; ISO/IEC 27002:2022 об'єднав їх у "кінцеві пристрої користувачів", при цьому вимагаючи, щоб збережена на них інформація "була захищена".
11.2.8	Обладнання користувачів, залишене без нагляду				
12.6.1	Управління технічною вразливістю	8.8	Управління технічними вразливостями	"Інформація про технічні вразливості використовуваних інформаційних систем має бути отримана, оцінка впливу на організацію таких вразливостей повинна бути проведена і мають бути вжиті відповідні заходи".	Опис засобу контролю 8.8 2022 року дуже схожий на опис "Управління технічною вразливістю" (12.6.1) з 2013 року. Разом з тим, оновлений стандарт розглядає старий контроль "Перевірка технічної відповідності" (18.2.3) як підмножину контролю "Управління технічними вразливостями", оскільки вони обидва переслідують ціль зменшити технічні вразливості в інформаційних системах.
18.2.3	Перевірка технічної відповідності				
12.4.1	Журнал аудиту подій	8.15	Журнал аудиту подій	"Журнали, у яких реєструють діяльність, винятки, збої та інші релевантні події, повинні створюватися, зберігатися, захищатися та аналізуватися".	Хоча це об'єднання заходів контролю може здатися доволі очевидним, у новому засобі контролю 8.15 порівняно з набором 2013 року була внесена важлива зміна: журнали тепер мають бути "проаналізовані", а не просто "регулярно переглянуті". Це стає зрозуміло не лише з опису засобу контролю, а й із самих настанов. Настанови стандарту 2013 року переважно зосереджувалися на тому, які журнали зберігати та як їх захищати, тоді як контроль 8.15 зі стандарту 2022 року, крім всього цього, надає також детальні рекомендації щодо аналізу журналів.
12.4.2	Захист інформації журналів реєстрації				
12.4.3	Журнали реєстрації адміністратора та оператора				

Висновки

Стандарт ISO/IEC 27002:2022 значно змінився, представивши абсолютно нову структуру, новий спосіб групування заходів безпеки, а також кілька нових засобів контролю на додаток до деяких значних об'єднань. Ще одним корисним доповненням оновленого стандарту є атрибути, використання яких спрощують процес вибору та валідації контролів. Разом з тим, що варто зауважити, внесені інновації залишаються в керованих рамках: реструктуризація каталогу заходів безпеки робить стандарт більш прозорим і, безсумнівно, є правильним рішенням з огляду на зростання складності та зменшення прозорості архітектур безпеки. А більш детальні настанови ISO/IEC 27002:2022 щодо заходів безпеки полегшують процес впровадження стандарту, особливо для нових користувачів.

Перелік посилань

1. Million Insights: Market Research Reports, Industry Analysis. 2014. Bring Your Own Device (BYOD) Market Size & Forecast Report 2012 – 2020. URL: https://www.millioninsights. Com / industry-reports / bring-your-own-device-byod-market ? utm_source=pressrelease & utm_ medium=referral&utm_campaign=Abnewswire_Shweta_ Sept12&utm_content=Content.

2. Global Bring-Your-Own-Device (BYOD) Industry Research Report, In-Depth Analysis of Current Status and Outlook of Key Countries 2023-2028. URL: https://www.industryresearch.biz/ global-bring-your-own-device-byod-industry-23044218.

3. Right Scale State of the Cloud Report 2013. URL: https://www.slideshare.net/arms8586/ rightscale-state-of-the-cloud-report-2013.

4. Flexera 2022 State of the Cloud Report. URL: https://m3comva1.frb.io/uploads/docs/ Flexera-State-of-the-Cloud-Report-2022.pdf.

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

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

Надійшла 03.05.2025