Додаток
до аналітичної записки з питань
порівняльного законодавства Європейського Союзу,
держав–членів ЄС та інших держав
щодо забезпечення кібербезпеки

Реферативний огляд
міжнародних стандартів
у сфері інформаційної безпеки групи ISO 27000

Група міжнародних стандартів ISO визначають технічні та організаційні вимоги до механізму управління інформаційною безпекою, включно з кібербезпекою, демонструють кращі практики протидії ризикам у відповідній сфері. Зазначена група стандартів також охоплює методи протидії кіберризикам, порушенням конфіденційності інформації, закріплює засоби технічного захисту інформації з урахуванням правових режимів і сфери поширення інформації.

Нині, до чинних стандартів ISO, які стосуються інформаційної та кібербезпеки, належать:

ISO/IEC27000:2019 – Інформаційні технології – Методи і засоби забезпечення безпеки – Системи управління інформаційною безпекою – Загальні відомості і словник.

ISO/IEC 27001:2013 – Інформаційні технології – Методи захисту – Системи управління інформаційною безпекою – Вимоги. Стандарт містить опис загальних вимог щодо забезпечення інформаційної безпеки, закріплює термінологічний словник у цій сфері регулювання, який має застосовуватися у нормативній та технічній документації, що стосується інформаційної безпеки.

ISO/IEC 27002:2013/COR 2:2015 – Інформаційні технології – Методи захисту – Звід рекомендованих правил для управління інформаційною безпекою. Стандарт, окрім опису засобів забезпечення інформаційної безпеки, також надає опис кращих моделей забезпечення інформаційної безпеки, методів управління ризиками, зокрема, у цифровому середовищі.

ISO/IEC 27003:2017 – Інформаційні технології – Методи безпеки – Системи управління інформаційною безпекою – Керівництво. Стандарт є продовженням вимог попередніх стандартів у частині кращих практик управління процесами забезпечення інформаційною безпекою.

ISO/IEC 27004:2016 – Інформаційні технології – Методи безпеки – Управління інформаційною безпекою – Моніторинг, вимір, аналіз і оцінка. Стандарт ISO 27004 дозволяє організаціям оцінювати продуктивність інформаційної безпеки та ефективність системи управління інформаційною безпекою з метою відповідності вимогам стандарту ISO/IEC 27001.

Зокрема, стандарт стосується:

– моніторингу та вимірюванню продуктивності інформаційної безпеки;

– моніторингу та вимірюванню ефективності інформаційної безпеки системи менеджменту (СУІБ), включаючи її процеси та засоби захисту;

– аналізу та оцінки результатів моніторингу та вимірюванню.

Оскільки ISO/IEC 27004 тісно пов’язаний із ISO/IEC 27001, його буде оновлено через 2–3 роки.

ISO/IEC 27005:2022 – Інформаційні технології – Методи безпеки – Управління ризиками інформаційної безпеки. ISO 27005 надає вказівки щодо управління ризиками інформаційної безпеки. ISO/IEC 27005 є доповненням до ISO/IEC 27001 та ISO/IEC 27002. Стандарт надає вказівки, які допоможуть:

– відповідати вимогам ISO/IEC 27001 щодо ризиків інформаційної безпеки;

– здійснювати діяльності щодо управління ризиками інформаційної безпеки (зокрема, оцінка ризиками).

ISO 27705 – Управління ризиками інформаційної безпеки. Стандарт спрямований на управління ризиками, які можуть поставити під загрозу інформаційну безпеку організації.

ISO/IEC 27006:2015/AMD 1:2020 – Інформаційні технології – Методи безпеки – Вимоги до органів, які проводять аудит і сертифікацію систем управління інформаційною безпекою. Положення цього стандарту стосуються вимог до органів сертифікації та аудиту систем управління інформаційною безпекою.

ISO/IEC 27007:2020 – Інформаційна безпека, кібербезпека і захист конфіденційності – Настанови щодо здійснення аудитів систем управління інформаційною безпекою. Стандарт містить вказівки щодо управління програмою аудиту системи управління інформаційною безпекою (СУІБ), проведення аудитів і компетентність аудиторів СУІБ, на додаток до настанов, що містяться в ISO 19011.

ISO/IEC TS 27008:2019 – Методи безпеки – Вказівки для оцінки засобів контролю інформаційної безпеки. Стандарт спрямовує на перегляд та оцінювання впровадження та функціонування засобів контролю інформаційної безпеки (включаючи технічну оцінку механізмів безпеки інформаційної системи), відповідно до вимог інформаційної безпеки, встановлених організацією (включаючи технічну відповідність критеріям оцінки).

ISO/IEC27017 – Інформаційна технологія. Технічні засоби безпеки. Керування інформаційною безпекою в хмарних середовищах. Надає вказівки щодо принципів інформаційної безпеки, які застосовуються до надання та використання хмарних послуг. Стандарт передбачає додаткові вказівки щодо впровадження відповідних засобів контролю, викладених у ISO/IEC 27002; додаткові заходи безпеки з інструкціями щодо впровадження, які стосуються саме хмарних служб. Ці настанови містять вказівки щодо впровадження як для постачальників хмарних послуг, так і для споживачів хмарних технологій. Стандарт востаннє переглядався та підтверджувався у 2021 році. Тому ця версія залишається чинною

ISO/IEC 27018 – Інформаційні технології – Техніка безпеки – Практичний кодекс з захисту особисто ідентифікованої інформації (OII) в публічних хмарних обчислювальних середовищах, що діють як обробники OII. Встановлює загальноприйняті цілі безпеки, запобіжні заходи та вказівки щодо впровадження заходів щодо персональної ідентифікаційної інформації (PII) відповідно до

принципів конфіденційності ISO/IEC 29100 для загальнодоступного середовища хмарних обчислень. Стандарт ISO 27018 містить вказівки на основі ISO/IEC 27002, враховуючи нормативні вимоги щодо захисту персональних даних, які можуть застосовуватися в контексті ризику інформаційної безпеки постачальника хмарних послуг. ISO 27018 поширюється на всі організації, які надають послуги з обробки інформації як обробники персональних даних через хмарні обчислення за контрактами з іншими організаціями. Рекомендації в цьому стандарті також можуть застосовуватися до організацій, які виконують функції аудиторів ідентифікаційної інформації. Однак на контролерів персональних даних можуть поширюватися додаткові закони, нормативні акти та зобов'язання щодо захисту персональних даних, які не застосовуються до суб'єктів, що обробляють персональні дані. Цей документ не призначений для покриття таких додаткових зобов'язань.

ISO/IEC 27701 – Інформаційні технології – Технічні засоби захисту – Розширення ISO/IEC 27001 та ISO/IEC 27002 для управління конфіденційністю інформації – Вимоги та рекомендації. Є розширенням до ISO/IEC 27001 та ISO/IEC 27002 для управління конфіденційною інформацією. Стандарт встановлює вимоги, пов'язані з PIMS, і містить вказівки щодо засобів захисту ідентифікаційної інформації та обробників ідентифікаційної інформації, які відповідають за обробку ідентифікаційної інформації. Стандарт ISO/IEC 27701 застосовується до всіх організацій, які є володільцями (контролерами) персональних даних та/або розпорядниками (обробниками) персональних даних, які обробляють персональні дані в рамках СУІБ.

ISO 27799:2016 – Інформаційна технологія. Менеджмент безпеки для охорони здоров'я. Стандарт встановлює рекомендації та загальні принципи для забезпечення безпеки і конфіденційності інформації в організаціях у сфері охорони здоров'я, зокрема таких, які пов'язані з обробкою медичної інформації.

ISO 27799 надає вказівки щодо організаційних стандартів безпеки інформації та практики управління інформаційною безпекою, включаючи вибір, впровадження та управління безпекою, беручи до уваги ризик інформаційної безпеки в організації. Надає вказівки щодо впровадження механізмів безпеки, описаних у ISO/IEC 27002, і доповнює їх (за необхідності) з метою ефективного використання для управління безпекою медичної інформації. Завдяки впровадженню ISO 27799:2016 організації охорони здоров'я та інші зберігачі медичної інформації зможуть забезпечити мінімально необхідний рівень безпеки, який відповідає їхнім організаційним обставинам, і підтримуватимуть конфіденційність, цілісність і доступність персональних даних про здоров'я, які знаходяться в їхньому нагляді. Стандарт застосовується до медичної інформації в усіх її аспектах, незалежно від форми інформації (слова та цифри, звукозаписи, малюнки, відео та медичні зображення), незалежно від того, як вона зберігається (надрукована чи написана на папері чи зберігається в електронній формі), і будь-якими засобами, використовуваними для її передачі (вручну, факсом, через комп'ютерні мережі чи поштою), оскільки інформація завжди належним чином захищена.