УДК 338:358.5
Ю. Петришин
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СИСТЕМИ МЕНЕДЖМЕНТУ, МОДЕЛЬ ISO 27001

UDC 338:358.5
Yu. Petryshyn

MANAGEMENT SYSTEMS, ISO 27001 MODEL

Стандарт ISO/IEC 27001 визначає вимоги до побудови системи управління інформаційною безпекою (СУІБ); включає кілька аспектів безпеки: фізичну, логічну та організаційну. Входить до сімейства стандартів, починаючи від впровадження засобів контролю техніки безпеки та управління ризиками (ISO, 2020). У деяких аспектах логіка впровадження стандартів сімейства ISO 27000 також вимагає посилань на стандарти ISO 31000, що стосується (загального) управління ризиками, і стандарт ISO22301, що стосується безперервності бізнесу. Проаналізувавши сертифікацію ISO 27001 його здатність перетворюватися на організаційний, управлінський та операційний інструмент, повертаючи справжнє уявлення про IT-безпеку.

СУІБ – це систематичний підхід до управління конфіденційною інформацією компанії, щоб тримати її у безпеці. Система застосовує процеси управління персоналом, процесів і технологічних систем, і може бути впроваджено на підприємствах будь-якого розміру (ISO, 2020). Для цього є кілька причин прийняти СУІБ наприклад:

а) Стратегічні, для відповідності уряду зі стратегічних причин, пов'язаних з управлінням корпоративною інформацією;

б) причини, корисні для відносин з клієнтами та постачальниками;

в) контроль використання корпоративних IT-ресурсів;

г) організаційна ефективність управління.

Процес впровадження системи менеджменту на основі стандарту ISO 27001 є суворим і жорстким. Впроваджена система потребує складання організаційно-експлуатаційної документації, що розглядає процедури контролю та аудиту, аспекти лідерства, презентаційну систему управління , процедуру управління менеджментом, системних процедур з підтримка управління ризиками.

З точки зору чистого корпоративного управління IT, сертифікація має переваги у можливості дотримання строгих систем роботи, які дозволяють організоване управління IT-ризику та передбачає періодичний аудит відповідності стандарту.

Сертифікація ISO 27001 наразі не дуже поширена серед компаній:

а) процес сертифікації вимагає важливих передумов щодо обладнання організація IT-структури та процедур управління інформаційними потоками;

б) процес сертифікації вимагає постійних зусиль IT-структури компанії та адаптація до процедур і правил, які не завжди присутні;

в) поновлення сертифікації кожних три роки із щорічним наглядом, вимагає постійної зобов’язання, що не всі організації можуть собі дозволити.

Тому стандарт ISO 27001 не має високої дифузії через вимоги та зобов'язання щодо його впровадження ця сертифікація представляє повну систему для забезпечення інформаційної безпеки. Він охоплює технічні, організаційні та навчальні аспекти, налагодження ефективної робочої логіки та методології.

Література

1. Calder, A. (2018). Implementing Information Security based on ISO 27001/ISO 27002. Van Haren Publishing.