Стандарт ISO/IEC 27001 допоможе підготуватися до інцидентів у галузі інформаційної безпеки

ISO/IEC 27001:2013.
Очікувані зміни нової версії стандарту

Опубліковано переглянуту редакцію популярного стандарту ISO/IEC 27001 *«Інформаційні технології. Методи убезпечення. Системи управління інформаційною безпекою. Вимоги»*. Стандарт допоможе компаніям убезпечити свої інформаційні активи, життєво важливі у сучасному світі, де зростає кількість та складність кібератак.

Згідно з дослідженням, опублікованим на початку цього року у Великій Британії, кількість інцидентів у галузі інформаційної безпеки в британських компаніях продовжує зростати.

Стандарт містить вимоги щодо побудови та ефективного функціювання систем управління (СУ) інформаційною безпекою організацій. Його розробниками є Міжнародна організація зі стандартизації (ISO) та Міжнародна електротехнічна комісія (**IEC**).

Наразі документ перебуває на стадії голосування за остаточним проектом міжнародного стандарту (**FDIS**). Голосування триватиме до кінця вересня, а після остаточного редагування його буде опубліковано, а попередня версія — скасована.

Однак для організацій, які вже впровадили та сертифікувались за **ISO/IEC 27001:2005**, координаційною радою **IAF** (International Accreditation Forum (Міжнародний Форум з акредитації)) буде визначено перехідний період, який зазвичай триває два роки.

За цей час організації зможуть підтвердити свою відповідність новій версії стандарту шляхом проходження чергових наглядових або ре-сертифікаційних аудитів.

Що стосується первинної сертифікації, то з часу публікації оновленої версії стандарту, вона проходитиме тільки за вимогами **ISO/IEC 27001:2013**.

Едвард Хампфріс, голова робочої групи, відповідальної за розроблення і супровід стандарту **ISO/IEC 27001**, у своєму інтерв'ю, опублікованому в новинах сайту ISO, зауважує: «Ми актуалізували нову редакцію, враховуючи досвід користувачів, які вже впровадили стандарт або отримали сертифікат на відповідність вимогам **ISO/IEC 27001:2005**. Основна мета — забезпечити більш гнучкий, оптимізований підхід, який забезпечив би ефективніше управління ризиками».

Перш за все, зміни стосуються ризиків і загроз інформаційній безпеці. Йдеться про можливість крадіжки особистих даних, загрозах, пов'язаних з використанням мобільних пристроїв тощо, які в 2005 році не були настільки актуальними. Це, звичайно, знайшло своє відображення в стандарті у виді низки змін у показниках безпеки, перерахованих у додатку А.

Крім того, необхідно звернути увагу на оновлену структуру стандарту, яка відповідає моделі PDCA («планування — дія — перевірка — коригування») і є базовою під час побудови всіх СУ у стандартах ISO. Це дозволить організаціям, які бажають упровадити декілька систем СУ, гармонійно інтегрувати вимоги **ISO/IEC 27001** та, наприклад, **ISO 9001** (СУЯ) або **ISO/IEC 20000-1** (СУ ІТ послуг).

Зміна структури зазвичай веде до перегляду розділів. Наприклад, вимоги щодо відповідальності вищого керівництва організацій у рамках функціонування СУ інформаційною безпекою буде переглянуто та оформлено у виді нового розділу *«Клас лідерства» («Leadership clause»)*. Також буде актуалізовано розділи, в яких описано поставлення цілей, аналіз, моніторинг та виміри в СУ інформаційною безпекою, зміст яких стане чіткішим та узгодженішим із вимогами інших стандартів на СУ.

Зміни, пов'язані з вимогами щодо оцінювання ризиків, були необхідні, щоб гармонізувати **ISO/IEC 27001** зі стандартом **ISO 31000:2009** «Менеджмент ризиків. Принципи та керівні вказівки». Терміни та визначення, надані в попередній редакції ISO/IEC 27001, буде актуалізовано та перенесено до стандарту ISO/IEC 27000 «Інформаційні технології. Методи убезпечення. Системи управління інформаційною безпекою. Огляд і словник», який наразі перебуває на перегляді на стадії DIS (проект міжнародного стандарту). ■