

Сьогодні, з розвитком цифрових технологій, значною загрозою для діяльності організацій стало порушения безпеки даних та кібератаки. Нерідко значною причиною цього є брак обізнаності щодо ризиків.

Нещодавно переглянутий стандарт **ISO/IEC 27005:2018 «Інформаційні технології. Методи безпеки. Управління ризиками інформаційної безпеки»** допоможе внести ясність у цю проблему.

Документ містить керівні вказівки для організацій про те, як впоратися з наявними викликами, забезпечивши основу для ефективного управління ризиками.

Стандарт був переглянутий відповідно до нової версії стандарту ISO/IEC 27001, а це є гарантією якнайкращого забезпечення задоволення потреб сучасних організацій.

Стандарт містить детальні настанови щодо управління ризиками, які допоможуть задовольнити відповідні вимоги, зазначені ISO/IEC 27001. Він є ключовим інструментом у низці інструментів ISO/IEC, які сприяють зниженню рівня кібер-ризиків.

Стандарт ISO/IEC 27005 містить інформацію про те «чому, що і як» необхідно робити в організаціях, щоб ефективно управляти своїми ризиками щодо інформаційної безпеки. Документ також допомагає демонструвати клієнтам організацій або зацікавленим сторонам адаптовані процеси щодо виявлення ризику, гарантуючи впевненість у плідній співпраці».

Стандарт ISO/IEC 27005 це один з десяти стандартів серії ISO/IEC 27000, який є сукупністю інструментів для боротьби з кібер-ризиками. Перший стандарт серії - ISO/IEC 27001встановлює вимоги до систем управління інформаційною безпекою, а інші містять

документи щодо захисту інформаційної безпеки в хмарі, інформаційної безпеки в телекомунікаційних і комунальних секторах, кібербезпеки, аудиту ISMS тощо.

Стандарт ISO/IEC 27005 розроблено робочою групою WG 1 «Інформаційна безпека систем управління» технічного комітету ISO/IEC JTC 1 «Інформаційні технології» підкомітету 27 «Методи і засоби забезпечення безпеки IT», секретаріат якого веде DIN, член ISO від Німеччини.