В наш цифровий час дуже швидкими темпами розвиваються різноманітні інформаційні технології, але на жаль разом з ними розвивається і кіберзлочинність.

Ключовим моментом захисту від кіберзлочинності є підготовка і виявлення вразливих місць, а також стійкість з точки зору взаємодії з загальними системами управління. Керувати інформаційною безпекою, а також визначити злочинців і притягнути їх до відповідальності допоможуть стандарти серії **ISO/IEC 27000**, розроблені спільним технічним комітетом Міжнародної організації з стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC) - ISO/IEC JTC 1.

Перший стандарт серії, **ISO/IEC 27001** щодо систем управління інформаційною безпекою (ISMS), опубліковано вже більше 20 років тому. З того часу у серії видано понад 40 міжнародних стандартів, що охоплюють все: від створення спільного словника (
ISO/IEC 27000
), управління ризиками (
ISO/IEC 27005
), безпеки у хмарних технологіях (
ISO/IEC 27017 і ISO/IEC 27018
) до методів судової експертизи, що використовують для аналізу цифрових доказів та розслідування інцидентів І
SO/ IEC 27042 та ISO/IEC 27043
відповідно).

Наприклад, **ISO/IEC 27043** пропонує настанови, що описують процеси та принципи, які застосовують до різних видів досліджень, включаючи несанкціонований доступ, пошкодження даних, збої в системі або корпоративні порушення інформаційної безпеки, а також будь-які інші цифрові дані розслідування.

Розробники стандартів серії **ISO/IEC 27000** зазначають, що основоположний стандарт серії **ISO/IEC 27001** постійно

вдосконалюється, що дає можливість підприємствам постійно оновлюватися у боротьбі з кіберзлочинністю. Завдяки впровадженню стандарту
ISO/IEC 27001
організація може оцінювати свої ризики, впроваджувати засоби контролю щодо їх пом'якшення, а потім контролювати та переглядати свої ризики та контроль за ними, покращуючи, за необхідності, захист. Таким чином, вона завжди готова до атак.

Системи управління інформаційною безпекою ISMS застосовують до всіх типів організацій та всіх видів підприємницької діяльності, зокрема для малих та середніх підприємств (SMEs), які є частиною ланцюгів постачання, і тому дуже важливо, щоб вони контролювали та керували своєю інформаційною безпекою та кібер-ризиками, щоб захистити себе та інших.

А нещодавно почалась розробка нового стандарту у сфері інформаційної безпеки - **ISO/IEC 27552 «Методи захисту. Розширення ISO/IEC 27001 та ISO/IEC 27002 для управління інформацією про конфіденційність. Вимоги та керівні вказівки»**
, який додатково розширює
ISO/IEC 27001
для вирішення конкретних потреб у сфері конфіденційності. Наразі, на стадії проекту, документ визначає вимоги та надає настанови щодо підтримання та постійного вдосконалення управління приватним життям у контексті організації.

Таким чином, стандарти серії ISO/IEC 27000 дійсно допомагають зробити безпечнішими усі сфери інформаційного життя, захищаючи приватність, фінанси, індивідуальну або корпоративну репутацію, при цьому постійно розвиваючись і вдосконалюючись.