Кібернапади – це найбільші ризики, з якими може стикнутися будь-яка організація. За даними глобального огляду, проведеного об'єднанням ISACA тільки 38% респондентів вважають, що вони підготовлені до кібернападів, решта 83% відносять кібернапади до одною з найнебезпечніших загроз для організації. За наявності великого обсягу персональної та конфіденційної інформації, яку пересилають за допомогою електронних засобів, несанкціонований доступ до неї може спричинити серйозні наслідки.

Набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і технологій, які використовуються для захисту кіберсреди, ресурсів організацій і користувачів – все це система кібербезпеки. Основними завданнями кібербезпеки вважаються: доступність, цілісність, що включає автентичність, а також конфіденційність. Кібербезпека є необхідною умовою розвитку інформаційного суспільства.

Система кібербезпеки, яка базується на міжнародних стандартах надзвичайно важлива у сучасному цифровому світі. Розробкою зазаначених стандартів займаються Міжнародна організація з стандартизації (ISO) спільно з Міжнародною електротехнічною комісією (IEC). Еа сьогодні фахівцями цих організацій розроблена **серія стандартів ISO/IEC 27000** , яка постійно доповнюється новими документами.

Стандарт серії **ISO/IEC 27001 «Інформаційна технологія. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги»** зібрав описи найкращих світових практик в області управління інформаційною безпекою. Документ встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси. Цей стандарт підготовлений як модель для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та поліпшення системи менеджменту інформаційної безпеки.
Нещодавно серія поповнилася новим стандаром **ISO/IEC 27009 «Інформаційні технології. Методи забезпечення безпеки. Галузеве застосування ISO/IEC 27001. Вимоги»** . Метою розробкт документу є забезпечення захисту інформації конкретних секторів: фінансів, транспорту та охорони

здоров’я, а також інфраструктурних проектів, таких як смарт-міста.

Серед інших, серія охоплює такі стандарти:

- ISO/IEC 27011 - для операторів зв’язку,
- ISO/IEC 27017 - для хмарних обчислень,
- ISO/IEC 27019 - для енергетичного сектору,
- ISO/IEC 27017 містить зведення правил щодо контролю за інформаційною безпекою для хмарних обчислювань,
- ISO/IEC 27013:2015 пропонує комплексне рішення для послуг захисту інформації,
- ISO/IEC 27010 є конкретним галузевим доповненням до інструментарію ISO/IEC 27000, який визначає ініціацію, реалізацію, супровід та удосконалення забезпечення інформаційної безпеки під час обміну інформацією між організаціями та галузями,
- ISO/IEC 27039:2015 дає рекомендації для підготовки та розгортання IDPS. Цей стандарт особливо корисний для сучасного ринку, де пропонують велику кількість комерційно доступних продуктів та послуг IDPS з відкритим кодом, заснованих на різних технологіях та підходах,
- ISO/IEC 27006:2015 присвячений питанням аудиту та сертифікації.