Міжнародний стандарт *ISO/IEC 27005:2011* описує принципи управління ризиками, що дозволяють керівникам та персоналу департаментів IT управляти ризиками в системах управління інформаційною безпекою (ISMS).

Ризики інформаційної безпеки являють серйозну загрозу для бізнесу внаслідок виникнення потенційної можливості фінансових збитків або шкоди, виходу з ладу ключових мережевих служб, втрати репутації та довіри клієнтів. Управління ризиками є одним з ключових елементів, що дозволяють запобігати інтернет-шахрайство, перехоплення ідентифікаторів, пошкодження Веб-сайтів, крадіжку персональних даних та інші комп'ютерні інциденти. Без солідної основи організації піддають себе численним типам кібер-ризиків.

Новий міжнародний стандарт *ISO/IEC 27005:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки»* допоможе організаціям усіх типів краще управляти інформаційними ризиками.

У ньому описана процедура і супутні заходи на основі загальних принципів, описаних у стандарті *ISO/IEC 27001:2005 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги»*

Голова спільної ISO/IEC робочої групи, яка розробила стандарт Едвард Хамфрі коментує: «Стандарт ISO/IEC 27005:2011 - найважливіший стандарт для тих, хто хоче

ефективно управляти ризиками, особливо, у відповідності з популярним стандартом на системи управління інформаційної безпеки ISO / IEC 27001 . Управління ризиками відіграє ключову роль у належному управлінні бізнесом, і цей стандарт допоможе організаціям рекомендаціями з питань навіщо, чому і як управляти в інформаційній безпеці для підтримки бізнес-цілей».

У даному виданні були переглянуті і оновлені відповідно до вимог наступних документів принципи, викладені в стандарті ISO/IEC 27005:

- *Стандарт ISO 31000:2009 «Управління ризиками. Принципи та настанови»;*
- *Стандарт ISO/IEC 31010:2009 «Управління ризиками. Методики оцінки ризиків»;*
- *Стандарт ISO Guide73:2009 «Управління ризиками. Словник».*

Даний стандарт призначений для забезпечення повної відповідності зі стандартом ISO 31000:2009 з метою допомоги організаціям, які хочуть керувати ризиками інформаційної безпеки аналогічно управлінню іншими ризиками.

Стандарт ISO/IEC 27005:2011 допоможе користувачам при впровадженні стандарту ISO/IEC 27001, який базується на підході управління ризиками. Знання принципів, моделей, процедур і термінології стандартів ISO/IEC 27001 та ISO/IEC 27002:2005 «Інформаційні технології. Методи забезпечення безпеки. Звід правил з управління інформаційною безпекою» грає важливу роль для повного розуміння даного міжнародного стандарту. Процедура управління ризиками інформаційної безпеки включає в себе:

- *визначення контексту;*
- *оцінка ризиків;*
- *розгляд ризиків;*
- *визначення ступеня допустимого ризику;*
- *інформування про ризики;*
- *моніторинг ризиків та звітність про ризики.*

Однак стандарт ISO/IEC 27005:2011 встановлює не конкретні методи управління ризиками інформаційної безпеки, а лише загальний підхід. Організація визначає свій власний підхід до управління ризиками, в залежності, наприклад, від області застосування системи управління інформаційною безпекою в залежності від контексту

або галузі промисловості.

Стандарт ISO/IEC 27005:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки» розроблений підкомітетом *SC 27«Методи забезпечення захисту IT» спільного технічного комітету ISO/IEC JTC 1 «Інформаційні технології».*

Джерело: *http://www.iso.org*