ISO 31000 ТА ІСЛАНДСЬКА ВУЛКАНІЧНА КРИЗА

(Підготував В. Дерев'янко, науковий співробітник відділу науково-методологічного забезпечення діяльності в міжнародній та європейській стандартизації ДП «УкрНДНЦ» за матеріалами офіційного сайту ISO — www.iso.org)

Хмара пилу від Ісландського вулкану має глобальні впливи: серйозні збитки пасажирів, анулювання сотень тисяч польотів, а шкода авіакомпаній світу оцінюється декількома мільярдами доларів. Деякі авіалінії, можливо, не оговтаються.

Здається, що така подія не має характерних рис ризику, якими авіа- та інші компанії могли б управляти. Закриття Європейського повітряного простору вплинуло на все: від туризму до виробників квітів та свіжих овочів в Африці, виробників одягу в Бангладеш та виробників електронних компонентів на далекому сході.

Виверження пилу є класичним прикладом низької вірогідності, простого наслідку події, яка зазвичай буває не врахована керівництвом під час дослідження потенційних ризиків корпоративних цілей. Дивно, але навіть за наявності знання про діяльність Ісландського вулкану та вплив на авіацію його минулих вивержень в Азії, ніякі плани не були введені в дію для управління ризиком, пов'язаним з дестабілізацією.

Хмара пилу є прикладом ризиків, що постійно змінюються та якими необхідно управляти в умовах зростання глобальної економіки. Декого здивує те, наскільки серйозно, якщо взагалі це відбувається, вище керівництво бере участь у плануванні та випробуванні сценаріїв, пов'язаних з руйнуванням ризиків. Наприклад організація із сильною культурою управління ризиками (UPS) швидко перенаправила авіавантажопотік з Азії до Європи та Стамбулу, а потім завантажила вантажівки для доставки у кінцевий пункт призначення. UPS був одним з тих виключень, що найбільше опікувався питанням, коли пил розвіється та відновляться польоти.

Без ризику не може бути нагороди або прогресу, але якщо в межах організації ним управляють не ефективно, то не можливо максимально реалізувати можливості та мінімізувати загрози.

Ризик тісно пов'язаний з невизначеністю або, що важливіше, ефектом невизначеності у досягненні цілей. 15.11.2009 ISO видала **ISO 31000:2009 «Управління ризиками. Принципи та настанови»**, щоб допомоги організаціям промислового, комерційного та громадського секторів упевнено братися за такі ризики.

ISO 31000:2009 явно відрізняється від існуючих директив щодо управління ризиками в тому, що акцент переставляється з того, що трапляється, на ефект невизначеності цілей. Він встановлює принципи, структуру та процес управління ризиком, що придатні для будь-якого виду організації в громадському або приватному секторі. Він підкреслює той факт, що управління ризиком має бути впроваджене із урахуванням специфічних потреб та структури організації.

Успішні організації, такі як UPS, працюють над розумінням невизначеності у досягненні їхніх цілей і над тим, щоб гарантувати успішний результат в управлінні їхніми ризиками. ■

Кевін Кнайт (Kevin W. Knight),
керівник робочої групи ISO з розроблення стандарту ISO 31000

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Враховуючи, що все більша кількість організацій упроваджують системи управління інформаційною безпекою (СУІБ) як частину своєї стратегії управління ризиками, публікація нового стандарту ISO/IEC на огляд СУІБ була б дуже своєчасною.

Стандарт ISO/IEC 27000:2009 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Огляд і словник» допоможе організаціям усіх видів зрозуміти основи, принципи і концепції вдосконалення захисту своїх інформаційних активів.

Стандарт 1SO/IEC 27000:2009 може застосовуватися організаціями всіх видів і розмірів (наприклад комерційними підприємствами, урядовими установами, некомерційними організаціями) і доповнює серію стандартів ISO/IEC 27000, надаючи введення до управління інформаційною безпекою та визначаючи відповідні терміни.

Сьогодні інформаційні активи організації залежать від інформаційних і комунікаційних технологій. Технологія полегшує створення, опрацювання, зберігання, передавання, захист інформації від знищення.

У міру того як розширюється взаємозв'язане глобальне ділове середовище, підвищуються вимоги до захисту інформації, оскільки вони піддаються значно ширшому колу загроз і вразливості. ■

Сандрін Транчард,
службовець зі зв'язків із громадськістю,
Центральний секретаріат ISO
(За матеріалами «Інформаційного бюлетеня з міжнародної стандартизації», 2009, № 4)