Негативні наслідки широкого кола загроз інформаційної безпеки (починаючи від атак хакерів і закінчуючи діями інсайдерів, які використовують свої знання і права доступу до даних компанії для своєї вигоди) можна зменшити, використовуючи підхід до управління інцидентами інформаційної безпеки, описаний в новому міжнародному стандарті ISO/IEC 27035 : 2011.

Порушення в області інформаційної безпеки можуть ставити під загрозу функціонування бізнес-систем і порушувати роботу бізнесу. Від підготовленості та своєчасності і ефективності реагування може залежати, чи виллється інцидент в незначну пригоду або стане катастрофою для бізнесу. Застосування системи управління інцидентами інформаційної безпеки дасть організаціям інструменти управління і процедури, що дозволяють контролювати широкий діапазон інцидентів і вразливостей.

Стандарт *ISO/IEC 27035:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки»* надає практичні рекомендації з виявлення, реєстрації і оцінки випадків порушення інформаційної безпеки і вразливостей.

Він допоможе організаціям реагувати на інциденти інформаційної безпеки, зокрема, вводити відповідні інструменти контролю для їхнього запобігання та скорочення, а також відновлення, і, таким чином, витягувати уроки та покращувати загальний підхід.

Інтеграція системи управління інцидентами інформаційної безпеки дає ряд переваг:

- *підвищення загального рівня інформаційної безпеки;*
- *зменшення негативних наслідків для бізнесу;*

- *посилення акценту на попередження інцидентів інформаційної безпеки,*

- *призначення пріоритетів і збору даних;*

- *внесок в обгрунтування рішень щодо виділення бюджету та ресурсів;*
- *поліпшення якості результатів оцінки та управління ризиками інформаційної безпеки;*

- *поліпшення інформованості в галузі інформаційної безпеки і допомога у підготовці матеріалів для навчання;*
- *надання додаткової інформації для розроблення політики інформаційної безпеки та супутньої документації.*

Едвард Хамфріс, під керівництвом якого була розроблена початкова версія стандарту ISO/IEC TR 18044:2004, коментує: «Ефективне і своєчасне вирішення серйозних інцидентів може вирішити долю організації, що стоїть перед альтернативою порятунку чи загибелі». Новий стандарт ISO/IEC 27035 пропонує перевірені рішення в галузі процесів і методів забезпечення ефективного управління інцидентами інформаційної безпеки.

«*Ступінь критичності інцидентів може варіювати від незначних, які можуть вплинути на працездатність ізольованої системи, до великих, які охоплюють усі бізнес-системи. Одні інциденти можуть призвести до збою в роботі організації та використання її бізнес-ресурсів на 24-72 і більше годин, інші можуть призвести до серйозних втрат та/або знищення даних, а деякі можуть зробити організацію, яка винна у серйозному злочині. Стандарт ISO/IEC 27035:2011 пропонує рішення* ».

Стандарт ISO/IEC 27035:2011 замінює технічний звіт ISO/IEC TR 18044:2004 та узгоджується з загальними принципами, встановленими в стандарті *ISO/IEC 27001:2005 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги».*

Новий стандарт може застосовуватися в будь-якій організації, незалежно від її розміру. Стандарт поширюється на широкий діапазон інцидентів інформаційної безпеки, навмисних чи випадкових, викликаних технічними або фізичними причинами.

Стандарт *ISO/IEC 27035:2011 «Інформаційні технології. Методи забезпечення безпеки. Управління інцидентами інформаційної безпеки»* розроблений підкомітетом *SC*

27 «Методи забезпечення безпеки» спільного технічного комітету ISO/IEC JTC 1 «Інформаційні технології».

Джерело: http://www.iso.org