Технічний звіт ISO/IEC, що описує призначені для аудиторів технічні засоби і рекомендації з підтвердження відповідності вимогам, дозволить підвищити ефективність систем захисту інформації в організаціях.

Технічний звіт *ISO/IEC TR 27008:2011 «Інформаційні технології. Методи забезпечення безпеки. Керівництво для аудиторів засобів управління інформаційною безпекою»* призначений для підвищення надійності базових засобів управління інформаційною безпекою для всіх аспектів, в тому числі бізнес-процеси та інформаційне середовище.

*«Бізнес-середовище постійно змінюється, а разом з ним змінюються загрози для життєздатності компанії. Організації повинні бути у всеозброєнні, а адекватний захист може бути побудований на підставі аудиту коштів, використовуваних для захисту інформації»*, - говорить Едвард Хамфріс, керівник робочої групи, яка розробила документ. - *«ISO/IEC TR 27008:2011 є основою для проведення детальних аудитів безпеки організації і розроблення програм оцінки засобів інформаційної безпеки, яка дозволить підвищити впевненість організації в тому, що засоби застосовуються належним чином і система інформаційної безпеки відповідає цілям».*

Стандарт ISO/IEC 27008 надає рекомендації з аналізу застосування та управління коштами, охоплюючи контроль технічного відповідності. Документ, в першу чергу, призначений для аудиторів інформаційної безпеки, які перевіряють технічну відповідність засобів забезпечення інформаційної безпеки організації вимогам стандарту ISO/IEC 27002 або будь-яким іншим контрольним стандартам, використовуваним в організації. Стандарт ISO/IEC TR 27008 дозволить:

- *виявити і оцінити ступінь потенційних проблем і прогалин у засобах управління інформаційною безпекою;*
- *виявити і оцінити потенційний вплив на організацію неадекватного усунення загроз і вразливостей інформаційної безпеки;*
- *встановити пріоритети заходів щодо усунення ризиків інформаційної безпеки;*
- *упевнитися в тому, що вразливості, які були виявлені раніше або виникли екстрено*

*були адекватно усуненими;*

- *приймати рішення щодо бюджету та інші управлінські рішення, спрямовані на покращення управління інформаційною безпекою, в ході інвестиційного процесу.*

Таким чином, Стандарт ISO/IEC 27008 буде корисний організаціям усіх типів, у тому числі державним і приватним компаніям, державним і некомерційним організаціям. Документ став восьмим у серії стандартів ISO/IEC 27000 на системи управління інформаційною безпекою.

Едвард Хамфріс додає: *«Інформація - ключовий актив для будь-якої моделі бізнесу, організаційної структури і системи, а серія стандартів ISO/IEC 27000 може використовуватися для захисту цього найважливішого бізнес-активу».*

*Джерело:* [http://www.iso.org](http://www.iso.org)