КОМБІНОВАНИЙ МЕТОД АНАЛІЗУ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сєвєрінов О. В., Переметчик О. В.
Харківський національний університет радіоелектроніки, Харків, Україна

Наслідком впровадження засобів обчислювальної техніки в управління сучасних підприємств є зростання інформаційної структури організації, що, в свою чергу, призводить до збільшення вразливостей системи і збільшення можливостей доступу до управлінської, комерційної та виробничої інформації з боку зовнішніх і внутрішніх порушників. Інформаційні системи стають потенційно небезпечними для своїх власників, свого роду «міною сповільненої дії».

Саме тому управління інформаційними ризиками є одним з найбільш актуальних напрямків менеджменту в області захисту інформації. Його основне завдання - об'єктивно ідентифікувати і оцінити найбільш значущі для бізнесу інформаційні ризики компанії, а також адекватність використовуваних засобів контролю ризиків для збільшення ефективності і рентабельності економічної діяльності компанії.

Метою доповіді є аналіз підходів, методів, стандартів управління ризиками інформаційної безпеки (ІБ) на підприємстві.

Проведений аналіз існуючих методів визначення ризиків інформаційної безпеки та сучасних міжнародних стандартів [1-3], які регламентують питання ІБ свідчить про те, що характерною основою експертних систем оцінювання ризиків є ймовірність виникнення тієї чи іншої події, яка впливає на ймовірність реалізації загрози. Для точного визначення рівня ризиків ІБ необхідно мати додаткову інформацію, яка отримується в результаті проведення ряду ретельних досліджень, обробка яких здійснюється у більшості експертними методами.

В даний час існують різноманітні і складні за своєю структурою інформаційні системи підприємств, для яких неможливо підібрати конкретну методику оцінки ризиків, тому для отримання точних задовільних результатів оцінки необхідно використовувати комбінований підхід до оцінок ризиків на основі вже існуючих методик, що дозволяє мінімізувати їх недоліки. Даний метод забезпечує більш високу оцінку ризиків інформаційної безпеки для різних моделей інформаційно-телекомунікаційних систем.

Список літератури

1. ISO/IEC 27005:2018. Information technology - Security techniques - Information security risk management

2. Сєвєрінов О.В., Черниш В.І., Молчанова М.Є. Управління інформаційною безпекою згідно міжнародних стандартів //Системи управління, навігації та зв'язку.– Вип. – 2011. – Т. 4. – С. 250-253.

3. Замула А.А., Северинов А.В., Корниенко М.А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации // Наука і техніка Повітряних Сил Збройних Сил України. – 2014. – №. 2. – С. 133-138.