РОЗРОБКА МЕТОДИКИ РОЗРАХУНКУ ІНФОРМАЦІЙНИХ РИЗИКІВ ПІДПРИЄМСТВА

Спєсівцева А.С., Золотарьов В.А.
Харківський національний університет радіоелектроніки, Харків, Україна

В умовах глобалізації забезпечення інформаційної безпеки на підприємстві є дуже важливим моментом і полягає в постійному контролі за джерелами виникнення потенційних загроз та необхідності здійснювати захист інформації будь-якими засобами.

Метою доповіді є визначення та оцінювання ризиків інформаційній безпеці для типової розподіленої інфокомунікаційної мережі підприємства.

Основний акцент зроблено на мінімізацію шкоди від кібератак, спрямованих на доступність програмно-апаратного комплексу інфокомунікаційної системи. Провідним методом для оцінювання та обробки ризиків був обраний якісний метод, як найбільш економічний, в умовах відсутності даних про кількість реалізованих атак на інфокомунікаційну систему за окремий проміжок часу. Ґрунтуючись на бізнес-процесах підприємства були виділені основні та другорядні активи, а також відповідні їм загрози інформаційній безпеці.

В роботі був проведений розрахунок ризиків інформаційній безпеці, заснований на виділенні цінних активів організації, ступеня потенційної шкоди під час реалізації загроз на такі активи та ймовірності реалізації загроз для аналізованої інфокомунікаційної мережі підприємства.

Також були виділені прийняті ризики, обробка яких не потрібна у зв'язку з тим, що фактична вартість їх мінімізації вища від реалізації відповідних їм загроз. Були запропоновані можливі заходи щодо мінімізації ризиків інформаційній безпеці, що включають:

систему резервного копіювання,
систему захисту від несанкціонованого доступу,
систему антивірусного захисту,
міжмережне екранування,
організаційні заходи фізичного захисту.

Була запропонована методика, яка дозволяє однозначно оцінити ризики інформаційній безпеці організації в умовах великого об'єму оброблюємої інформації та необмежного числа користувачів і потребує мінімальних фінансових вкладень. Застосування розглянутого методу на практиці буде сприяти ефективному виявленню основних загроз захисту безпеки та їхній мінімізації.

Список літератури

1. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. Berlin: ISO/IEC JTC 1/SC 27. 2013. 23p.

2. Дорофеев А.В. Менеджмент инфоромационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014.No 3 (4). С. 69–73.