МЕХАНІЗМИ КОМПЛЕКСНОЇ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ISO/IEC 27005 ТА NIST SP 800-30

Дрига К.В., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання кількості цілеспрямованих кібератак і динамічність сучасного ландшафту загроз зумовлюють потребу в побудові превентивних систем кіберзахисту. Фундаментом таких систем виступає своєчасна та достовірна оцінка ризиків інформаційної безпеки (ІБ), яка дозволяє обґрунтовано розподіляти матеріальні й часові ресурси підприємства для протидії критичним інцидентам.

Метою доповіді є дослідження та систематизація механізмів комплексної оцінки ризиків ІБ шляхом інтеграції стандарту ISO/IEC 27005 і деталізованого аналітичного апарату рекомендацій NIST SP 800-30 [1].

В доповіді наводяться результати аналізу щодо ефективності поєднання управлінських та технічних механізмів оцінки ризиків інформаційної безпеки. Знизити рівень невизначеності та підвищити точність прогнозування загроз можна, при комплексному застосуванню ISO/IEC 27005 та NIST SP 800-30. У доповіді запропоновано покроковий механізм гармонізації зазначених стандартів, що включає такі взаємопов'язані етапи:

1. Формування повного переліку інформаційних ресурсів підприємства, визначення критеріїв оцінки ризиків та встановлення межі прийнятного ризику відповідно до настанов ISO/IEC 27005 [2].
2. Класифікація потенційних джерел атак, аналіз мотивацій порушника та моделювання сценаріїв реалізації загроз за таксономією рекомендацій NIST SP 800-30 [3].
3. Розрахунок імовірності настання несприятливих подій і масштабу їхнього впливу на конфіденційність, цілісність та доступність даних із застосуванням комбінованих якісно-кількісних матриць ризику.
4. Побудова пріоритезованого реєстру ризиків для вибору відповідних заходів реагування: зменшення, збереження, передача або уникнення ризику.

Поєднання нормативної бази ISO/IEC 27005 та деталізованої аналітичної структури NIST SP 800-30 дозволяє розробити цілісну модель безпеки ІКС, яка оптимізує витрати підприємства на кіберзахист і забезпечує безперервність його ключових бізнес-процесів.

Список літератури

1. Сєвєрінов О.В., Черниш В.І., Молчанова М.Є. Управління інформаційною безпекою згідно міжнародних стандартів // Системи управління, навігації та зв'язку. – 2011. – Вип. 4 (20). – С. 250–253.
2. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. – Geneva: International Organization for Standardization, 2022.
3. NIST Special Publication 800-30 Rev. 1. Guide for Conducting Risk Assessments. – Gaithersburg: National Institute of Standards and Technology, 2012.