УДК 004.056
В. Оксенюк
Тернопільський національний технічний університет імені Івана Пулюя

ВИКОРИСТАННЯ ПРОГРАМНИХ ЗАСОБІВ ДЛЯ ОЦІНКИ ТА УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

UDC 004.056
V. Okseniuk
(Ternopil Ivan Puluj National Technical University, Ukraine)

USE OF SOFTWARE FOR INFORMATION SECURITY RISK ASSESSMENT AND MANAGEMENT

Однією з головних проблем сучасного бізнесу є оцінка необхідного рівня витрат на інформаційну безпеку (ІБ) для максимальної ефективності інвестицій в дану сферу. Для вирішення проблеми використовуються комплекси аналізу ризиків, що дозволяють оцінити існуючі в системі ризики і вибрати оптимальний за ефективністю варіант захисту. На сьогоднішній день багатьма компаніями, які спеціалізуються в рішенні комплексних проблем ІБ, розроблені і запропоновані власні методики управління інформаційними ризиками, які лежать в основі програмних комплексів. Ці методики різняться, перш за все, за рівнем і досконалістю використовуваних математичних методів, покладених в основу процедур оцінювання ризиків. Залежно від цього вони мають різні можливості адекватного врахування реальних факторів, що в свою чергу, зумовлює точність і надійність отриманих оцінок ризику.

Для розв'язання задачі оцінки ризиків і загроз ІБ в даний час найчастіше використовуються програмні комплекси аналізу і контролю інформаційних ризиків, в основі роботи яких лежать існуючі методики проведення аналізу, розроблені, як правило, на основі вимог міжнародного стандарту ISO 17799:2002: CRAMM, RiskWatch, ГРИФ, FRAP, MSAT, CORAS, NIST, COBRA, Risk Advisor, КОНДОР+, Oracle Crystal Ball, BCM Analyser, RiskPAC, OCTAVE, Proteus Enterprise, Digital Security Office, РискМенеджер, @Risk, MethodWare, Callio Secura 17799, RA2 art of risk, vsRisk, Buddy System та ін. Критерії, за якими можна порівняти наведені інструментальні засоби: види ризиків; способи їх оцінки та керування ними; способи зниження ризику; оперативність та складність визначення ризику; вартість засобу; можливість застосування власних проти заходів; оцінка захищеності; вразливість.

Отже, на ринку інформаційних технологій існує велика кількість програмних засобів, впровадження яких забезпечує якісне керування. Усі програми можна розділити на дві великі групи: програми, що застосовуються якісну (наприклад, «високий», «середній», «низький» чи за шкалою від 1 до 10) та кількісну оцінку ризиків (оцінюється через числове значення, наприклад, розмір очікуваних річних втрат). До першої групи належать, наприклад COBRA, Risk Advisor, КОНДОР+, Proteus, FRAP. До другої, наприклад, – RiskWatch, OCTAVE. Проте, є комплекси, що об’єднують ці два підходи (наприклад, CRAMM, MSAT, ГРИФ, NIST, Buddy System).

Розглянуті інструментальні засоби дозволяють здійснити оцінку рівня поточного стану ІБ бізнес-системи, знизити ймовірні втрати шляхом підвищення стійкості функціонування корпоративної мережі, розробити концепцію і політику безпеки, а також запропонувати плани захисту від виявлених загроз і вразливих місць. В той же час, сьогодні існують різноманітні і складні за своєю структурою бізнес-системи, для яких неможливо використати одну конкретну методику оцінки ризиків, тому для отримання потрібних результатів оцінки необхідно використовувати комплексний підхід до оцінок ризиків на основі вже існуючих методик.

До прийняття остаточного рішення про впровадження котроїсь з методик управління ризиками ІБ, і, як наслідок, того чи іншого програмного засобу, варто переконатися, що вона достатньо враховує бізнес-потреби компанії, її масштаби, а також відповідає кращим світовим практикам і має досить докладний опис процесів і необхідних дій.