УДК 681.3:621.396

ПРОЕКТУВАННЯ СИСТЕМ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА

А.В. Дудатьев, к.т.н., доцент,
О.П. Войтович, к.т.н., ст. викладач
Вінницький національний технічний університет
e-mail: andreysaf60@mail.ru

Інформаційна система підприємства, як правило, складається з декількох рівнів управління, які в тій чи іншій мірі пов'язані між собою. Тому у зловмисників завжди знайдеться певний набір методів і засобів, які дозволять обійти політику безпеки підприємства, якщо він проник хоча б на один з них. Офіційна статистика представляє факти, які говорять про те, що більшість несанкціонованих спроб доступу до інформаційних ресурсів залишаються навіть невиявленими. Наприклад, за даними Національного відділення ФБР кількість невиявлених атак знаходиться в межах від 85% до 97%.

Звичайно, не всі недоліки, що привели до результативних несанкціонованих доступів до інформаційних ресурсів, в тому числі, і до найбільш захищених у світі, відомі. Тому постійно актуальним є питання проектування і оцінювання ефективності систем інформаційного захисту, які максимально ефективно реалізують відповідну політику безпеки.

Стандарт ISO/IEC 15408 визначає профіль системи захисту як сукупність функціональних і гарантійних вимог, які дозволяють реалізувати систему захисту з необхідним рівнем інформаційної безпеки. Методологія оцінювання

інформаційної безпеки профілю захисту базується на використанні методів аналізу і ідентифікації множини факторів, зокрема активи підприємства, недоліки в захисті, загрози, потенційні атаки тощо.

Необхідно зазначити, що відсутня чітка статистична інформація відносно об'єкта, який оцінюється і навпаки більшість процесів характеризуються невизначеністю. Все це робить неможливим практичне використання точних моделей, які базуються на класичній математичній теорії. Щоб вирішити ці проблеми, зручно використовувати апарат нечіткої логіки, де залежність входів системи та виходів задаються на основі лінгвістичної людської логіки, а не точних цифр, з якими складно працювати. Показники таких систем набагато вищі, ніж систем на чітких числах. Застосування конкретної діагностичної моделі залежить від виду порушення нормального ходу, вхідної інформації, знань експерта. У зв'язку з цим для отримання кількісної оцінки, що характеризує ефективність варіанта профілю захисту, пропонується використовувати експертні оцінки, що представляються у вигляді нечітких множин. Вибір значень елементів множини завжди пов'язаний з ризиком того, що обрані значення показників не забезпечують необхідного рівня безпеки. Наслідком цього є можливість провести ефективну атаку на відповідні інформаційні ресурси. Пошук наочного представлення знань приводить до систем на основі нечіткої логіки, яка забезпечує представлення словесно інтерпретованих знань.

Для забезпечення можливості прийняття рішення при не тільки кількісних, але й якісних характеристик, запропоновано використання нечіткого ієрархічного дерева, на основі якого будується база знань системи безпеки. Такий комплексний підхід надає можливість отримати на етапі проектування оптимальний варіант системи інформаційної безпеки підприємства.