УДК 003.26.09; 519.688
Головецька О., Луцків А.
Тернопільський національний технічний університет імені Івана Пулюя

ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ

Актуальність перевірки захищеності мережевої інфраструктури набуває дедалі більшої актуальності. Захист інформаційних автоматизованих систем державного підпорядкування регламентується цілою низкою нормативних документів: НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-005-99, НД ТЗІ 2.5-006-99, НД ТЗІ 3.6-001-2000, НД ТЗІ 3.7-003-05 та іншими. Водночас є серія державних стандартів у даній предметній області.

Приватні структури (банки, великі організації, підприємства) з розвинутою інфраструктурою, як правило керуються міжнародними стандартами, наприклад: ISO/IEC 17799:2005 («Інформаційні технології — Технології безпеки — Практичні правила менеджменту інформаційної безпеки»); міжнародний стандарт, що базується на BS 7799-1:2005 та цілий ряд інших.

Для оцінювання захищеності мережевої інфраструктури необхідно провести аудит безпеки. Аудит безпеки передбачає перевірку захищеності системи, під якою розуміють: збір, накопичення інформації про події в інформаційній системі, аналіз записів журналів безпеки (з метою перевірки ефективності керування системою), забезпечення гарантій відповідності функціонування системи політиці безпеки та вироблення рекомендацій про необхідні зміни в управлінні, політиці та процесах безпеки.

Особливої актуальності набувають системи аналізу захищеності комп'ютерних систем, які призначені для виявлення вразливостей в програмно-апаратному забезпеченні. Прикладами таких вразливостей можуть бути неправильна конфігурація мережевих служб, наявність програмного забезпечення без встановлених модулів оновлення (service packs, patches, hotfixes), наявність “таємних дверей” тощо.

Цілями проведення аудиту безпеки є:

- аналіз ризиків, пов'язаних з можливістю здійснення загроз безпеки щодо ресурсів ІС;
- оцінювання поточного рівня захищеності ІС;
- локалізація вузьких місць у системі захисту ІС;
- оцінювання відповідності ІС існуючим стандартам в галузі інформаційної безпеки;
- вироблення рекомендацій щодо впровадження нових та підвищення ефективності існуючих механізмів безпеки ІС.

Етапи аудиту: 1) ініціювання процедури аудиту; 2) збір інформації про об’єкт аудиту; 3) аналіз даних аудиту; 4) вироблення рекомендацій; 5) підготовка аудиторського звіту.

Для оцінювання захищеності мережевої інфраструктури використовуються певні методології, які дають змогу оцінити кількісно, а не лише якісно захищеність досліджуваного об’єкту. Такий підхід дає змогу оцінити матеріальні збитки у разі інциденту в безпеці мережевої інфраструктури та зробити більш детальні рекомендації по підвищенню захищеності досліджуваної системи. Оцінюванням об’єктів мережевої інфраструктури займаються автори даної роботи.