УДК 681.004

М. Карпінський[1] , Н. Мороз[2] , А. Яворський[2]
1. Університет в Бєльську-Бялій і Державна вища професійна школа в Новому Сончі, Польща.
2.Тернопільський національний технічний університет ім. Івана Пулюя

ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ЯК ОСНОВА БЕЗПЕКИ МЕРЕЖ

Вразливість інформації в автоматизованих комплексах обумовлена великою концентрацією обчислювальних ресурсів, їх територіальною розподіленністю, довгостроковим збереженням великого об’єму даних на магнітних та оптичних носіях, одночасним доступом до ресурсів багатьох користувачів. У цих умовах необхідність вживання заходів захисту, напевно, не викликає сумнівів. В основі комплексу заходів щодо інформаційної безпеки повинна бути стратегія захисту інформації. У ній визначаються мета, критерії, принцип і процедури, необхідні для побудови надійної системи захисту.

Найважливішою особливістю загальної стратегії інформаційного захисту є дослідження системи безпеки. Можна виділити два основних напрямки: аналіз засобів захисту та визначення факту вторгнення.

Методологічною основою політики розробки практичних заходів для її реалізації є концепція захисту інформації, тобто офіційно прийнята система поглядів на проблему інформаційної безпеки і шляхи її рішення з урахуванням сучасних тенденцій. На базі сформульованих у концепції цілей, задач і можливих шляхів їх рішення формуються конкретні плани забезпечення інформаційної безпеки. Всі заходи протидії комп'ютерним злочинам, що безпосередньо забезпечують безпеку інформації, можна розділити на правові, організаційно-адміністративні (рис.1) та інженерно-технічні (рис.2). Серед них найважливішу роль відіграють саме технічні заходи для забезпечення безпеки. Вони формують потужне ядро, яке включає використання різноманітних засобів, що дозволяє забезпечити захист інформації на найвищому рівні. На основі концепції безпеки інформації розробляються стратегія безпеки інформації, архітектура системи захисту інформації та політика безпеки інформації.

Рисунок 1. Організаційно-адміністративні засоби захисту

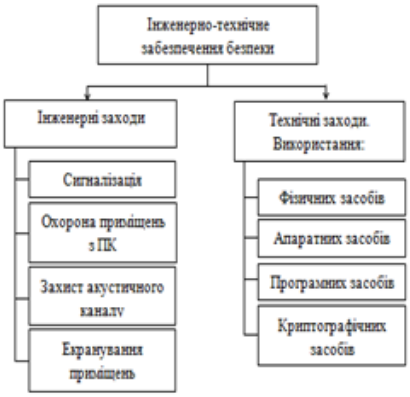

Рисунок 2. Інженерно-технічні засоби захисту

Автоматизований комплекс можна вважати захищеним, якщо всі операції виконуються у відповідності з чітко визначеними правилами, що забезпечують безпосередній захист об'єктів, ресурсів і операцій. Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту. Ці правила, в свою чергу, визначають необхідні функції і заходи захисту.

Захист інформації в комп'ютерній мережі ефективніший в тому випадку, коли проектування і реалізація системи захисту відбувається в три етапи: аналіз ризику, реалізація політики безпеки, підтримка політики безпеки. В сучасних умовах захист інформації стає пріоритетною задачею, але забезпечення належного рівня захисту є складним і трудомістким процесом, який вимагає врахування великої кількості деталей і чіткої концепції захисту інформації.