

ЗАБЕЗПЕЧЕННЯ БАГАТОРІВНЕВОГО ЗАХИСТУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Питання забезпечення безпеки інформації відіграють важливу роль у житті суспільства, а в деяких випадках і визначальну.

Для забезпечення інформаційної безпеки застосовують комбіновані методи захисту, які включають захист інформації від несанкціонованого доступу засобами перевірки повноважень користувачів та обслуговуючого персоналу на використання інформаційних ресурсів; ідентифікацію та аутентифікацію сторін, які виробляють обмін інформацією (підтвердження автентичності відправника та одержувача); розмежування прав користувачів і обслуговуючого персоналу при доступі до інформаційних ресурсів, а також при зберіганні та наданні інформації з обмеженим доступом; розподіл інформації за ступенями захищеності і за категоріями доступу, сертифікація технічних і програмних засобів та інші методи.

Концепція надійної обчислювальної бази є центральною при оцінці ступеня гарантованості, з якою систему можна вважати надійною. Надійна обчислювальна база це сукупність захисних механізмів комп'ютерної системи (включаючи апаратне і програмне забезпечення), що відповідають за проведення в життя політики безпеки. Основне призначення надійної обчислювальної бази - виконувати функції монітора звернень, тобто контролювати допустимість виконання суб'єктами певних операцій (запитів) над об'єктами. Монітор обробки запитів (МОЗ) перевіряє кожне звернення користувача до програм або даними на предмет узгодженості зі списком дій, допустимих для користувача. Від МОЗ потрібне виконання трьох властивостей:

- ізольованості, коли монітор захищений від відстеження своєї роботи;
 - повноти, коли монітор повинен викликатися при кожному зверненні і не повинно бути способів його обходу;
 - верифіцируемості, коли монітор повинен бути компактним, щоб його можна було проаналізувати і протестувати, будучи впевненим у повноті тестування.
- Турбота про можливість витоку інформації покладається на саму систему. Такі системи отримали назву систем багаторівневого захисту. Багаторівневий захист визначається як властивість обчислювальної або інформаційної системи зберігати й обробляти дані різного рівня і категорій користування при наявності персоналу з різними категоріями допуску, таким чином, щоб виключити доступ до інформації або її модифікацію особами, чий допуск не відповідає рівню секретності інформації.

Науковий керівник – к.т.н., доц., Є.Г. Левченко