6.2. ПРИНЦИПИ ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ

Захист інформації в АІТУ повинен ґрунтуватися на наступних основних принципах:

- системності;
- комплексності;
- безперервності захисту;
- достатності;
- гнучкості управління і застосування;
- відвертості алгоритмів і механізмів захисту;
- простоти застосування захисних заходів і засобів.

Системний підхід до захисту комп'ютерних систем припускає необхідність обліку всіх взаємопов'язаних та взаємодіючих елементів, що змінюються в часі, умов і чинників, істотно значущих для розуміння і розв'язування проблеми забезпечення безпеки АІТУ. Під час створення системи захисту необхідно враховувати всі слабкі, найуразливіші місця системи обробки інформації, а також характер, можливі об'єкти і напрями атак на систему з боку порушників (особливо висококваліфікованих зловмисників), шляхи проникнення в розподілені системи і несанкціонованого доступу до інформації. Система захисту має будуватися з урахуванням не тільки всіх відомих каналів проникнення і несанкціонованого доступу до інформації, але і з урахуванням можливості появи принципово нових шляхів реалізації загроз, щодо безпеки.

Захист інформації — це не разовий захід і навіть не сукупність проведених заходів і встановлених засобів захисту, а безперервний цілеспрямований процес, що припускає використання відповідних заходів на всіх етапах життєвого циклу АІТУ, починаючи з ранніх стадій проектування, а не лише на етапі її експлуатації. Розробка системи захисту повинна вестися паралельно з розробкою системи, що потребує захисту. Це дозволить врахувати вимоги безпеки під час проектування архітектури і створити більш ефективніші (як за витратами ресурсів, так і за стійкістю) захищені системи. Більшості фізичних і технічних засобів захисту для ефективного виконання їх функцій необхідна постійна організаційна (адміністративна) підтримка (своєчасна зміна і забезпечення правильного зберігання і застосування імен, паролів, ключів шифрування, перевизначення повноважень). Перерви в роботі засобів захисту можуть бути використані для аналізу вживаних методів і засобів захисту, для впровадження спеціальних програмних і апаратних «закладок» та інших засобів подолання системи захисту після відновлення її функціонування.

Створити абсолютну систему захисту принципово неможливо. При достатній кількості часу і засобів можна подолати будь-який захист. Тому має сенс вести мову тільки про деякий прийнятний (розумно достатній) рівень безпеки. Високоефективна система захисту має велику вартість, використовує під час роботи істотну частину потужності і ресурсів комп'ютерної системи і може створювати відчутні додаткові незручності користувачам. Важливо правильно вибрати той достатній рівень захисту, при якому витрати, ризик і розмір можливого збитку були б прийнятними (завдання аналізу ризику).

Часто доводиться створювати систему захисту в умовах великої невизначеності. Тому вжиті заходи і встановлені засоби захисту, особливо спочатку їх експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Природно, що для забезпечення можливості варіювання рівнів захищеності, засоби захисту мають володіти визначеною гнучкістю. Особливо важливим ця властивість є в тих випадках, якщо установку засобів захисту необхідно здійснювати в працюючих системах, не порушуючи процесу її нормального функціонування. Крім того, зовнішні умови і вимоги з часом міняються. У таких ситуаціях можливість позбавити власників АІТУ від необхідності вживання кардинальних заходів щодо повної заміни засобів захисту на нові.

Для побудови ефективної системи захисту необхідно провести наступні роботи:

- визначити рівень безпеки інформації;
- виявити можливі канали просочування інформації і несанкціонованого доступу (НСД) до даних, потребують захисту;
- побудувати модель потенційного порушника;
- вибрати відповідні заходи, методи, механізми і засоби захисту;
- побудувати замкнуту, ефективну комплексну систему захисту, проектування якої починається з проектування самих автоматизованих систем і технологій.

Найбільш поширеними шляхами несанкціонованого доступу до інформації є:

- перехоплення електронних випромінювань;
- примусове електромагнітне опромінювання ліній зв'язку з метою отримання певної модуляції;
- застосування підслуховуючих пристроїв;
- дистанційне фотографування;

- перехоплення акустичних випромінювань і відновлення тексту принтера;
- розкрадання документальних носіїв інформації;
- читання залишкової інформації в пам'яті системи після виконання санкціонованих запитів;
- копіювання носіїв інформації з подоланням заходів захисту;
- незаконне підключення до апаратури і ліній зв'язку;
- впровадження і використання комп'ютерних вірусів.

Визначення конкретних значень характеристик можливих порушників в значній мірі суб'єктивно. Модель порушника, побудована з урахуванням особливостей конкретної предметної області і технології обробки інформації, може бути представлена переліком декількох варіантів його зовнішності. Кожен порушник повинен бути охарактеризований значеннями характеристик, наведених вище.