**Лекція 6 ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ**

При розгляді проблем захисту даних в мережі передусім виникає питання про класифікацію збоїв і порушень прав доступу, які можуть привести до знищення або небажаної модифікації даних.

***Серед таких потенційних "загроз" можна виділити :***

 1. Збої устаткування :

* збої кабельної системи;
* перебої електроживлення;
* збої дискових систем;
* збої систем архівації даних;
* збої роботи серверів, робочих станцій, мережевих карт і так далі

2. Втрати інформації через некоректну роботу ПЗ :

* втрата або зміна даних при помилках ПЗ;
* втрати при зараженні системи комп'ютерними вірусами.

3.Втрати, пов'язані з несанкціонованим доступом :

* несанкціоноване копіювання, знищення або підробка інформації;
* ознайомлення з конфіденційною інформацією що становить таємницю, сторонніх осіб;

4. Втрати інформації, пов'язані з неправильним зберіганням архівних даних.

5. Помилки обслуговуючого персоналу і користувачів :

* випадкове знищення або зміна даних;
* некоректне використання програмного і апаратногозабезпечення, що веде до знищення або зміниданих;

Залежно від можливих видів порушень роботи мережі (під порушенням роботи я також розумію і несанкціонований доступ) численні види захисту інформації об'єднуються в ***три основні класи :***

* засоби фізичного захисту, включаючі засоби захисту кабельної системи, систем електроживлення, засобу архівації, дискові масиви і так далі
* програмні засоби захисту, у тому числі: антивірусні програми, системи розмежування повноважень, програмні засоби контролю доступу.
* адміністративні заходи захисту, що включають контроль доступу в приміщення, розробку стратегії безпеки фірми, планів дій в надзвичайних ситуаціях і так далі

Слід зазначити, що подібне ділення досить умовно, оскільки сучасні технології розвиваються у напрямі поєднання програмних і апаратних засобів захисту. Найбільше поширення такі програмно-апаратні засоби отримали, зокрема, в області контролю доступу, захисту від вірусів і так далі

Концентрація інформації в комп'ютерах - аналогічно концентрації готівки у банках - примушує усе більш посилювати контроль в цілях захисту інформації. Юридичні питання, приватна таємниця, національна безпека - усі ці міркування вимагають посилення внутрішнього контролю в комерційних і урядових організаціях. Роботи в цьому напрямі привели до появи нової дисципліни : безпека інформації.

Фахівець в області безпеки інформації відповідає за розробку, реалізацію і експлуатацію системи забезпечення інформаційної безпеки, спрямованої на підтримку цілісності, придатності і конфіденційності накопиченої в організації інформації. У його функції входить забезпечення фізичного (технічні засоби, лінії зв'язку і видалені комп'ютери) і логічного (ці, прикладні програми, операційна система) захисту інформаційних ресурсів.

Складність створення системи захисту інформації визначається тим, що дані можуть бути викрадені з комп'ютера і одночасно залишатися на місці; цінність деяких даних полягає у володінні ними, а не в знищенні або зміні.

Забезпечення безпеки інформації - дорога справа, і не стільки із-за витрат на закупівлю або установку засобів, скільки через те, що важко кваліфіковано визначити межі розумної безпеки і відповідної підтримки системи в працездатному стані.

Якщо локальна мережа розроблялася в цілях спільного використання ліцензійних програмних засобів, дорогих кольорових принтерів або великих файлів загальнодоступної інформації, то немає ніякої потреби навіть в мінімальних системах шифрування/дешифрування інформації.

Засоби захисту інформації не можна проектувати, купувати або встановлювати до тих пір, поки не зроблений відповідний аналіз. Аналіз ризику повинен дати об'єктивну оцінку багатьох чинників (схильність появі порушення роботи, вірогідність появи порушення роботи, збиток від комерційних втрат, зниження коефіцієнта готовності системи, громадські стосунки, юридичні проблеми) і надати інформацію для визначення відповідних типів і рівнів безпеки.

Комерційні організації усі більшою мірою переносять критичну корпоративну інформацію з великих обчислювальних систем в середу відкритих систем і зустрічаються з новими і складними проблемами при реалізації і експлуатації системи безпеки. Сьогодні все більше організацій розгортають потужні розподілені бази даних і додатка клієнт/сервер для управління комерційними даними. При збільшенні розподілу зростає також і ризик неавторизованого доступу до даних і їх спотворення.

Шифрування даних традиційно використовувалося урядовими і оборонними департаментами, але у зв'язку зі зміною потреб і деякі найбільш солідні компанії починають використати можливості, що надаються шифруванням для забезпечення конфіденційності інформації.

Фінансові служби компаній (передусім в США) представляють важливу і велику призначену для користувача базу і часто специфічні вимоги пред'являються до алгоритму, використовуваного в процесі шифрування. Опубліковані алгоритми, наприклад DES, є обов'язковими. В той же час, ринок комерційних систем не завжди вимагає такого строгого захисту, як урядові або оборонні відомства, тому можливе застосування продуктів і іншого типу, наприклад PGP (Pretty Good Privacy).