Тема: Захист інформації в комп’ютерних системах і мережах

План

1. Види інформації за режимом доступу. Властивості інформації, як об’єкту захисту.
2. Поняття, сутність, значення захисту інформації.
3. Класи АС. Загрози інформації.
4. Комплексна система захисту інформації.
5. Особиста безпека в мережі Інтернет.

Проблема захисту інформації не є новою. Вона з'явилася ще задовго до появи комп'ютерів.

З самого початку свого розвитку системи інформаційної безпеки розроблялися для військових відомств. Розголошення такої інформації могло привести до величезних втрат. Тому конфіденційності (тобто нерозголошенню інформації) в перших системах безпеки приділялася особлива увага.

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу привели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності.

Сьогодні наслідки від пошкодження або знищення інформації (даних) є більш значними, ніж втрата матеріальних ресурсів. Нерідко вартість втраченої, наприклад, під час природного лиха або техногенної аварії чи викраденої інформації, може в сотні разів перевищувати вартість будівель чи інших матеріальних цінностей.

У сучасному суспільстві діє відомий принцип: хто володіє інформацією, той володіє світом. Охочих таким чином опанувати світом більш ніж достатньо, а значить і існує стійкий попит на інформацію, отриману незаконним шляхом. У такій ситуації головне завдання власника інформації - це її надійний захист.

Тому на сьогоднішньому занятті ми розглянемо поняття, сутність, значення захисту інформації, принципи інформаційної безпеки, види загроз інформаційній безпеці та правила безпечної роботи в автоматизованих системах та Інтернеті як у майбутній вашій професійній діяльності, так і у повсякденному житті.

Для того, щоб правильно побудувати систему захисту інформації, необхідно дати відповідь на декілька питань:

- Яку ж інформацію ми повинні захищати?
- як зловмисник може отримати до неї доступ?
- яким чином можна перешкодити зловмиснику?

Згідно із Законом України "Про інформацію" за режимом доступу інформація, поділяється на *відкриту* та *з обмеженим доступом*.

Відкрита інформація – це інформація, яка доступна для користування всіх. Ця інформація систематично публікується в офіційних друкованих виданнях (бюлетенях, збірниках, періодичних виданнях), поширюється засобами масової комунікації, безпосередньо надається зацікавленим громадянам, державним органам та юридичним особам.

Інформація з обмеженим доступом – це інформація, яка має довірчий або секретний характер. У свою чергу, інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденційну, службову і таємну.

Конфіденційна інформація – це відомості, які знаходяться у володінні, користуванні та розпорядженні окремих фізичних або юридичних осіб і розповсюджуються за їх бажанням відповідно до передбачених ними умов.

Службова інформація - інформація, що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф "для службового користування".

Таємна інформація – інформація, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, комерційну таємницю та іншу передбачену законом таємницю.

Суб'єктами права власності на інформацію є громадяни, юридичні особи, держава.

Власник інформації щодо обєктів своєї власності має право здійснювати будь-які законні дії.

Захищати потрібно будь-яку інформацію.

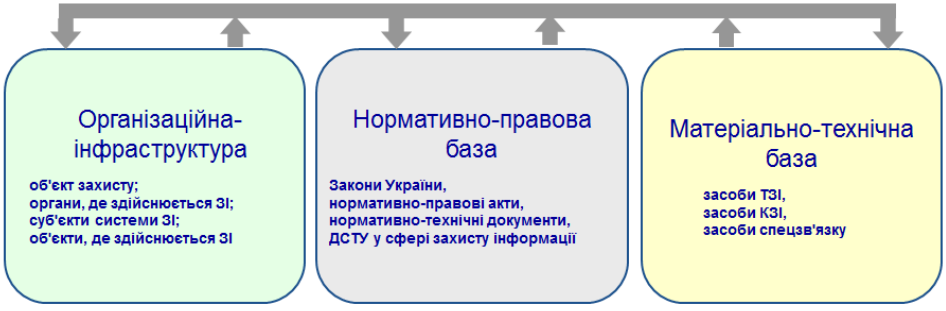
Якщо розглядати інформацію, як об’єкт захисту, то вона має наступні властивості, які її характеризують: конфіденційність, цілісність та доступність.

Широке впровадження комп'ютерів в усі види діяльності, постійне нарощування їхньої обчислювальної потужності, використання комп'ютерних мереж різного масштабу привели до того, що загрози втрати конфіденційної інформації в системах обробки даних стали невід'ємною частиною практично будь-якої діяльності.

Захист інформації – діяльність із забезпечення конфіденційності, цілісності та доступності важливої для особи, суспільства та держави інформації, яка обробляється в інформаційно-телекомукнікаційних (автоматизованих) системах або озвучується на об’єктах інформаційної діяльності, а також із забезпечення використання інформації у відповідності із встановленими правилами.

Сутність захисту інформації – полягає у виявленні, усуненні або нейтралізації джерел негативних впливів, причин і умов впливу на інформацію. Ці джерела становлять загрозу безпеки інформації.

Для захисту інформації в Україні створена система захисту інформації:



Всі заходи та засоби по захисту інформації можна поділити на декілька груп:

- Юридичні – передбачають наявність законів, які визначають відповідальність осіб, що знищують, пошкоджують інформацію, використовують її без належного дозволу, або сприяють цьому.
- Адміністративні (організаційні) – це заходи, що регламентують процес функціонування системи, використання її ресурсів, діяльність персоналу, тощо.
- Фізичні заходи захисту включають охорону приміщень, техніки та персоналу, встановлення на дверях приміщень кодових замків, систем санкціонованого доступу, тощо.
- Технічні засоби передбачають використання пристроїв, які зменшують ймовірність руйнування та викрадання інформації.
- Програмні засоби використовують для : визначення та обмеження прав користувачів до доступу до системи, шифрування інформації, що зберігається,
- Фіксування дій користувачів доступу до системи або інформації, відновлення знищеної інформації на носіях. Подібні програми можуть входити у стандартний комплект поставки того чи іншого програмного продукту загального призначення, або розроблятися під конкретне робоче місце проектувальниками інформаційних систем.
- Технологічні засоби передбачають включення у технологічний процес спеціальних операцій, які будуть перешкоджати та запобігати пошкодженню, руйнуванню та витоку інформації.

Одним з напрямків захисту інформації в інформаційних системах є комплексна система захисту інформації (КСЗІ)

Комплексна система захисту інформації – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Організаційні заходи

Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;
- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;
- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- навчання правилам інформаційної безпеки користувачів.

У разі необхідності, в рамках проведення організаційних заходів може бути створена служба інформаційної безпеки, проведена реорганізація системи діловодства та зберігання документів.

Інженерно-технічні заходи – сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити.

Інженерно-технічні заходи, що проводяться для захисту інформаційної інфраструктури організації, можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування і захисту від несанкціонованого доступу.

У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом.

Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовної) інформації.

Отже, ви як майбутні працівники АС повинні чітко усвідомлювати важливість захисту інформації, дотримання правил роботи в АС. А саме:

- дотримуватись посадових інструкцій;
- не допускати до свого робочого місця сторонніх осіб;
- використовувати систему паролів, які регулярно змінювати, не писати на листочках, залишати на видних місцях;
- використовувати ліцензійне та сертифіковане в Україні програмне забезпечення;
- встановлювати дозволені Державною службою спеціального зв'язку і захисту інформації антивірусні програми
- регулярно оновляти антивірусні бази на сайті Держспецзвязку.
- не використовувати власні носії інформації (флешки, СД-картки, диски).
- слухати адміністратора мережі та адміністратора безпеки по використанню мережі та АС.
- займатись самоосвітою.