О.О. Лугових, асист.
І.М. Данилін, студ., гр. АТ-20-3м
Житомирський державний технологічний університет

ЗАХИСТ ІНФОРАЦІЇ ВІД РАДІОЧАСТОТНОГО ВИПРОМІНЮВАННЯ

Особливість сучасного розвитку суспільства полягає у всебічному застосуванні в різних його сферах інформаційних ресурсів та засобів, що їх отримують та обробляють. Ми є свідками переходу людства до інформаційного суспільства, в якому інформація стає більш важливим ресурсом, ніж матеріальні або енергетичні. Тому в умовах зростаючої залежності суспільства від інформаційного ресурсу актуальною потребою є його захист від несанкціонованого доступу, пошкодженням або зло навмисного знищення.

Дослідження і аналіз численних випадків впливів на інформацію показують, що загрози, які походять від людей або предметів і наносять шкоду, можна поділити на такі класи: випадкові або навмисні, внутрішні або зовнішні, структурні або не структурні. До випадкових та навмисних загроз можна віднести такі фактори: помилки або навмисне втручання обслуговуючого персоналу і користувачів; втрата інформації, обумовлена неправильним зберіганням архівних даних; випадкове або навмисне знищення або зміна даних; збої обладнання і електроживлення, кабельної системи; збої дискових систем, архівних даних; збої роботи серверів, робочих станцій, мережних карт; некоректна робота програмного забезпечення; враження системи комп'ютерними вірусами; розкриття і модифікація даних і програм, їх копіювання; перехват і ознайомлення з інформацією, що передається по канал зв'язку та в нашому випадку перехват або втрата інформації через побічне випромінювання ЕОМ та засобів передачі даних.

На сьогоднішній день існує велика кількість методів захисту інформації. Всі їх різноманіття можливо поділити на:

- методи апаратного або схемного захисту;
- програмні методи;
- метод захисних перетворень;
- організаційні заходи;
- пасивний метод;
- метод маскування.

Програмний метод захисту – це сукупність алгоритмів та програм, що забезпечують розподіл доступу і виключення несанкціонованого використання інформації.

Сутність **методу захисних перетворень** полягає в тому, що інформація, яка зберігається в системі і передається по каналах зв'язку, представляється в деякому коді, який виключає можливість її безпосереднього використання.

Організаційний метод захисту включають в себе сукупність дій по підбору і перевірці персоналу, який задіяний в експлуатації програм і перевірці персоналу, якій задіяний в експлуатації програм та інформації, суворе регламентування процесу розробки та функціонування АС.

Метод апаратного або схемного захисту полягає в тому, що в пристроях і технічних засобах обробки інформації передбачається наявність спеціальних технічних рішень, які забезпечують захист і контроль інформації, або схеми перевірки інформації на парність, здійснюючи контроль за правильності передачі між різними пристроями ІС.

Пасивний метод полягає в тому, що в серверних ставляться екрануючи пластини на вікна, які локалізують електромагнітні випромінювання. Але пасивні методи складно, а іноді неможливо застосовувати в розподілених АС, або АС розміщених на великі площі. Також складно це реалізовувати для мобільних систем. В таких випадках доцільно використовувати апаратні методи захисту – зокрема метод маскування.

Метод маскування полягає в тому, що в серверних та інших системах ставиться пристрій, якій за допомогою додаткового випромінювання маскує корисні сигнали. Такий метод досить просто реалізувати особливо в мобільних системах, так як засоби, що забезпечують цей метод є компактними. Іншою суттєвою перевагою є простота налаштування на необхідний частотний діапазон та невисока вартість.

Для того, щоб перехопити необхідну інформацію з комп'ютера зловмиснику необхідно налаштуватися на частоту передачі даних в комп'ютері та частоту формування відеоданих, яку випромінює монітор на ЕПТ. Отже, виходячи з структурою втрати інформації, обрано метод маскування.