ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ

Борзов М. М., Цуранов М. В.

Харківський національний університет внутрішніх справ, Харків

В наш час дистанційне впровадження комп'ютерних вірусів за допомогою ВЧ-нав'язування не є актуальною загрозою, проте в майбутньому зможе наносити суттєвий збиток державним і комерційним структурам. В докладі наведенні існуючі засоби та пристрої, за допомогою яких можливо протистояти цій загрозі.

Ідея загрози нав'язування полягає у формуванні направленого спеціального електромагнітного імпульсу з метою примусового дистанційного запису вірусної програми у пам'ять ЕОМ. При цьому в пам'яті ОЗП можлива активізація вірусного коду безпосередньо як у момент його нав'язування, так і у будь який інший момент вибраний зловмисником, в такому випадку шкідливий код буде записано на жорсткий диск ПК.

У докладі наведенні можливі способи захисту інформації, яка циркулює в ЕОМ. Приведено можливість реалізації цих засобів за допомогою організаційних і технічних мір.

До організаційних заходів можна віднести:

– збільшення радіусу контрольованої території навколо об'єкта електронно-обчислювальної техніки;

– навчання персоналу по знаходженню ознак впливу ВЧ-сигналів;

– здійснення контролю доступу до ліній зв'язку, терміналам, мережам електроживлення і іншим елементам мереж;

– розташування електронно-обчислювальної техніки в загублених приміщеннях.

До додаткових технічних мір відносять:

– створення і використання системи попередження про застосування «вірусної зброї» шляхом проведення постійного радіоконтролю на предмет виявлення сильних електромагнітних сигналів близько ЕОМ;

– екранування персонального комп'ютера, з'єднання кабелів, іншого обладнання;

– установка фільтрів в ланцюгах електропостачання, управління і зв'язку.

Слід відзначити можливу неефективність програмних засобів захисту вид даного типу загроз. Це пояснюється тим, що жоден програмний засіб не може протистояти ВЧ-нав'язуванню. Протидія можлива тільки спеціальними технічними засобами, які здатні не тільки вчасно виявити загрозу, але й протидіяти ним.

Підсумовуючи усе вище сказане слід сказати, що загрозі інформаційної безпеки при використанні ВЧ-нав'язування можливо протиставити відомі і відносно недорогі засоби захисту інформації.