УДК 621.326

Берчук О. – ст. гр. ОКС-405
Технічний коледж Тернопільського державного технічного університету імені Івана Пулюя

ЗАХИСТ ІНФОРМАЦІЇ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Науковий керівник: Лісовий В.М.

В роботі перераховано різні типи шкідливих програм, що зустрічаються на практиці: комп'ютерні віруси, черв'яки, логічні бомби, троянські об'єкти, програми Backdoor, програмні засоби для здобуття несанкціонованого доступу до комп'ютерних систем.

Крім комп'ютерних вірусів існують і інші шкідливі програми, такі як черв'яки, логічні бомби, троянські об'єкти, програми Backdoor, програми Spyware і Adware, клавіатурні шпигуни, а також програми, призначені для здобуття несанкціонованого доступу до комп'ютерних систем. У міру розвитку комп'ютерних технологій можна чекати появи шкідливих програм нових типів, що використовують особливості нових технологій.

Вивчено всі основні об'єкти і канали розповсюдження шкідливих програм: файли виконуваних програм, файли офісних документів, завантажувальні сектори дисків і дискет, повідомлення електронної пошти, пірінгові мережі, інтрамережі або інтернет, драйвери ОС.

Розглянуто шкідливі дії комп'ютерних вірусів і інших шкідливих об'єктів. Шкідливі об'єкти можуть впливати на файли, сектори диска, бази даних і інші критично важливі ресурси комп'ютерних систем.

Перелічено всі основні методи виявлення комп'ютерних вірусів і інших шкідливих програм, такі як сканування, евристичний аналіз, виявлення змін, аналіз мережевого трафіку, аналіз баз даних поштових програм і баз даних систем автоматизації документообігу, а також вакцинація.

Проаналізовані способи видалення шкідливого коду без застосування антивірусних програм, а також із застосуванням антивірусів.

Захист інтрамереж і ресурсів інтернету вимагає застосування спеціальних антивірусних комплексів, оснащених мережевим центром управління. Допускаючи повне управління антивірусним захистом з єдиного центру, такі антивірусні комплекси дозволяють контролювати одночасно сотні і тисячі комп'ютерів.

Міжмережеві екрани дозволяють підсилити захист від комп'ютерних вірусів і інших шкідливих програм, оскільки вони здатні блокувати мережевий трафік, створюваний шкідливими об'єктами. Можливе використання комбінації антивіруса і міжмережевого екрану.

Надійність захисту від шкідливих програм забезпечується тільки при комплексному підході до рішення проблеми. Створюючи систему захисту, необхідно вивчити можливі канали, по яких шкідливий програмний код може потрапити в інформаційну систему, і передбачити засоби для блокування всіх таких каналів. Необхідно поєднувати програмно-технічні заходи з адміністративними заходами, постійно стежити за станом справ у області захисту від шкідливих програмних об'єктів. Обмежувати права користувачів, дозволяючи їм доступ тільки до тих ресурсів, які їм дійсно необхідні для роботи.