УДК 004.056

А. С. Янко, к.т.н.,
В. С. Горбань, студент гр. 401-ТК,
Полтавський національний технічний
університет імені Юрія Кондратюка

ОЦІНКА ЗАГРОЗ ЦІЛІСНОСТІ ІНФОРМФЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ

До появи персональних комп'ютерів і комп'ютерних мереж основними засобами для роботи з повідомленнями були книги, телефон, телеграф тощо. Але тепер інформаційні технології займають важливу роль в житті кожного із нас. На даний момент тяжко уявити людей, які не користуються сучасною технікою. Необхідність їх використання вже не викликає сумнівів, оскільки інформаційні технології – це одна з розвинутих галузей сучасного життя. Тому дуже важливою є тема захисту інформаційних мереж та їх користувачів від загроз [1].

Загроза – це потенційна можливість порушити інформаційну безпеку. Спроби реалізації загрози називаються «атакою», яку вчиняє зловмисник. Найчастіше загроза є наслідком наявності вразливих місць в захисті автоматизованої системи [2].

Одним з найнебезпечніших способів проведення атак є впровадження в системи, які атакують, шкідливого програмного забезпечення. Спектр шкідливих функцій необмежений, оскільки вірус як і будь-яка інша програма, може володіти якою завг*одно* складною логікою, але зазвичай віруси призначаються для:

- впровадження іншого шкідливого програмного забезпечення;
- отримання контролю над системою;
- агресивного споживання ресурсів;
- зміни або руйнування програм й/або даних.

Є два типу поширення шкідливого програмного забезпечення віруси та network worms. Вірус це код, що володіє здатністю до поширення шляхом впровадження в інші програми, а network worms здатні самостійно викликати поширення своїх копій по інформаційній системі. Віруси поширюються локально, у межах вузла мережі, для передачі по мережі їм потрібна зовнішня допомога, така як пересилання. Network worms навпаки, орієнтовані, в першу чергу, на подорожі по мережі. Вікно небезпеки для шкідливого програмного забезпечення з'являється з випуском нового різновиду шкідливого програмного забезпечення і перестає існувати з оновленням бази даних антивірусних програм і накладенням інших необхідних параметрів захисту.

На другому місці по масштабу збитку стоять крадіжки й підробки. Обсяг збитків перевищує мільярди доларів на рік. У більшості випадків винуватцями виявлялися штатні співробітники організацій, що добре знали

режим роботи й заходи захисту. Це ще раз підтверджує небезпеку внутрішніх загроз, хоча говорять і пишуть про їх значно менше, ніж про зовнішні [2].

Тому потрібно думати не тільки про загрози порушення цілісності, а і про небезпеку «сліпої» довіри комп'ютерної інформації. А також пам'ятати, що характерною особливістю електронних даних є можливість легко і непомітно спотворювати, копіювати або знищувати їх. Тому необхідно організувати безпечне функціонування даних в будь-яких інформаційних системах. Несанкціоновані дії на інформацію, будівлі, приміщення і людей можуть бути викликані різними причинами і здійснюватися за допомогою різних методів впливу [3].

Потенційно уразливі з точки зору порушення цілісності не тільки дані, але і програми. Впровадження шкідливого програмного забезпечення – приклад подібного порушення. Найбільших збитків інформації та інформаційних систем наносять неправомірні дії співробітників і комп'ютерні віруси. Для захисту інформації в комп'ютерах і інформаційних мережах широко використовуються різноманітні програмні та програмно-технічні засоби захисту.

Література

1. Андрощук О. В. Інформаційні технології та їх вплив на розвиток суспільства / О. В. Андрощук, 2014.

2. http://www.pki-exam.narod.ru/ib/t3/index.html (наиболее распространенные угрозы)

3. http://poznayka.org (основные угрозы целостности и конфиденциальности. Законодательный уровень информационной безопасности.)