УДК 681.3

О.П. Дóренський, Є.С. Мєлєшко

Кіровоградський національний технічний університет, Кіровоград

ПРИНЦИПИ ПОБУДОВИ МОДЕЛІ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ ІНФОРМАЦІНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

Сучасні тенденції розвитку інформаційних технологій (ІТ) створюють умови, при яких завдання забезпечення безпеки інформації (БІ) набуває в даний час все більшу актуальність [1].

Метою захисту ІТ є досягнення необхідного рівня безпеки для ІТ-систем для задоволення нормативних вимог з безпеки [2]. Це досягається відповідним застосуванням стандартних методів захисту в організаційному, кадровому, інфраструктурному і технологічному аспектах.

Загроза БІ – це міра можливості виникнення на якому-небудь етапі життєдіяльності системи такого явища або події, наслідком якої може бути небажані дії на інформацію: порушення (або небезпека порушення) фізичної цілісності, логічної структури, несанкціонована модифікація інформації (або небезпека такої модифікації), несанкціоноване отримання інформації (або небезпека такого отримання), несанкціоноване розмноження (копіювання) і поширення інформації [3].

Під загрозою інформаційної системи (ІС) будемо розуміти потенційну можливість порушити безпеку інформації ІС, а спробу реалізації загрози будемо називати атакою [4]. Загрози інформації інформаціно-телекомунікайної системи (ІТС) залежать від характеристик операційної системи (ОС), фізичного середовища, персоналу, технологій обробки і інших чинників.

Моделювання процесів порушення безпеки доцільно здійснювати на основі розгляду логічного ланцюжка: “загроза – джерело загрози – метод реалізації – вразливість – наслідки”.

Більшість методів аналізу та оцінювання негативних наслідків реалізації загроз побудовані на ідентифікації можливих джерел загроз за допомогою їх класифікації [4, 5]. Проте, наявність різних підходів до класифікаційного поділу загроз БІ та, як наслідок, неоднозначності у їх класифікації [4], дає можливість зробити припущення про неефективність використання таких методів.

Таким чином, альтернативним розв’язком задачі аналізу та оцінювання рівня інформаційної безпеки даних ІТС є побудова моделі загроз БІ, яка на сьогоднішній день є актуальною. В дослідженні [6] зроблено спробу побудови моделі ймовірних загроз і захисту інформації у мережах загального користування. Вона дозволяє на основі теорії графів побудувати базові моделі захисту інформації, які моделюють різноманітні ситуації несанкціонованого доступу. Але на практиці застосування цього підходу може викликати ряд труднощів, що унеможливить організації ІБ.

У доповіді наводиться детальний аналіз задачі моделювання загроз БІ ІТС, основні принципи і підходи побудови моделі загроз БІ.

Список літератури

1. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К.: ООО “Тид “ДС”, 2004. – 992 с.

2. Bundesamt fur Sicherheit in der Informationstechnik. IT Baseline Protection Manual, 1998. – 114 p.

3. Девянин П.Н. Теоретические основы компьютерной безопасности: уч. пособие для вузов / П.Н. Девянин. – М.: Радио и связь, 2000. – 380 с.

4. Дóренський О.П. Дослідження потенційних загроз безпеці інформації інформаційної системи та аналіз їх класифікаційного поділу / О.П. Дóренський // Зб. наук. праць Кіровоградського нац. технічного ун-ту. – Кіровоград, 2007. – Вип. 19. – С. 55-61.

5. Alberts C.J. OCTAVE-s Implementation Guide / C.J. Alberts, S.G. Behrens, R.D. Pethia, W.R. Wilson. – Version 0.9. – Volume 2: Preparation Guidance, 2003. – 236 p.

6. Петров А.А. Модель вероятностных угроз и защиты информации в сетях общего пользования / А.А. Петров // Зб. наук. ст. І Міжнародної науково-практичної конференції “Безпека та захист інформації в інформаційних та телекомунікаційних системах”. – Х.: Вид. ХНЕУ, 2008. – №7. – 95 с.