УДК 004.056.5

О. В. Войцеховська, В. В. Бохенко
(Україна, Вінниця, Вінницький національний технічний університет)

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ДАНИХ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ

Анотація. Проведено аналіз методів захисту інфокомунікаційних систем для гарантування їхньої безпеки. Розглянуто недоліки в роботі з такими системами та можливі шляхи їх подолання.

Ключові слова: інфокомунікаційна система, несанкціоноване втручання.

Abstract. The analysis of methods of infocommunication systems protection for guaranteeing their safety is carried out. The disadvantages of working with such systems and possible ways of overcoming them are considered.

Keywords: infocommunication system, unauthorized interference.

На сьогодні технологічний прогрес так стрімко пішов угору, що передача даних, текстових, аудіо та відеоповідомлень вийшла на зовсім новий рівень і потребує досить потужних систем передачі. Багато людей підключається, а ще більше вже підключено до мережі інтернет. Це дозволяє будь де знаходити потрібну інформацію, підключатись до баз даних, виконувати складні розрахунки, миттєво обмінюватись інформацією з кожною людиною, яка підключена до мережі.

Такі системи та неправильне їх використання спричинили ряд проблем, одна з яких – несанкціоноване втручання в інфокомунікаційну систему. Дуже вразливими залишаються телекомунікаційні мережі. Тому багато людей намагаються забезпечити захист даних в інфокомунікаційній системі.

Відповідно до законодавчої бази України основним об'єктом захисту в інформаційних системах є інформація з обмеженим доступом, що становить державну або іншу, передбачену законодавством України, таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження [1].

Загалом, об'єктом захисту в інформаційній системі є інформація з обмеженим доступом, яка циркулює та зберігається у вигляді даних, команд, повідомлень, що мають певну обмеженість і цінність як для її власника, так і для потенційного порушника технічного захисту інформації.

Яскравим прикладом стала атака вірусу «Petya», який з серпня 2017 року завдав шкоди багатьом ІТ-системам у декількох країнах світу та в Україні. Атаки були завдані по найбільшим секторам, в яких використовуються інфокомунікаційні мережі, а саме банки, державні ограни, великі телекомунікаційні, фармацевтичні компанії, тощо.

Зловмиснику достатньо зробити кілька кроків для несанкціонованого входу, адже нажаль досить багато державних об’єктів мають старе програмне забезпечення, не оновлюють базу своїх антивірусних програм та мають старі комп’ютери.

Тож можна виділи такі «мінуси» наших систем та людей, які ними користуються:

- легкі паролі, що складаються з коротких слів і фраз, або тільки з цифр по типу «1111» тощо;
- нешифрована передача даних;
- старі версії програмного забезпечення;
- використання неліцензійного програмного забезпечення, що може мати вразливі місця;
- перехід за шкідливими посиланнями у мережі інтернет;
- витрачання коштів на зовнішній захист, при цьому ігнорування внутрішнього;
- використання робочого комп’ютеру не за призначенням.

Для уникнення таких недоліків, достатньо застосовувати базові правила гарантування інформаційної безпеки, зокрема:

- відмова від надання прав «адміністратора» звичайним користувачам;
- зберігання важливої інформації в шифрованому, або закритому доступі;
- застосовування складних паролів з використанням різноманітних символів;
- перехід на ліцензійне програмне забезпечення;
- постійне оновлення баз даних антивірусів;
- використання брандмаузерів та веб-додатків для захисту в мережі інтернет;
- заведення бази програм та сторінок в інтернеті які можна використовувати;
- система штрафів за використання комп’ютера не за призначенням.

Отже, при поєднанні новітнього обладнання та викостовуючи елементарні правила безпеки, можна суттєво знизити ризики витоку забороненої інформації та захиститись від несанкціонованого втручання в інфокомунікаційну систему.

Література

1. Закон України «Про внесення змін до Закону України «Про захист інформації в автоматизованих системах»». Режим доступу: http://zakon3.rada.gov.ua/laws/show/ru/2594-15.