УДК 004.056.5

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Шиптицька І.І.

Цибуляк Б.З., ЛДУ БЖД, доцент, канд. фіз.-мат. наук

Львівський державний університет безпеки життєдіяльності

Сучасний період розвитку суспільства характеризується значним впливом на нього інформаційних технологій, які забезпечують поширення інформаційних потоків, утворюючи глобальний інформаційний простір. Зараз важко знайти сферу діяльності, в якій не використовуються інформаційні технології. Вони є найважливішою складовою процесу використання інформаційних ресурсів суспільства. Основними технічними засобами технології переробки інформації є комп'ютери і це істотно вплинуло як на концепцію побудови й використання технологічних процесів, так і на якість вихідної інформації. Широке впровадження персональних комп'ютерів у інформаційну сферу й застосування телекомунікаційних засобів зв'язку визначили новий етап розвитку інформаційних технологій.

Проте, стрімка інформатизація суспільства крім ряду позитивних рис, пов’язаних з можливістю легкого доступу до необхідної інформації, розвитку телекомунікаційних технологій на базі Інтернету, можливості швидкої передачі великих об’ємів даних, проведення електронних платежів тощо несе небезпеку, пов’язану із можливістю несанкціонованого перехоплення, викрадення, редагування чи знищення даних з метою отримання особистого зиску. Такі дії можуть спричинити не лише значні фінансові збитки, а й принести шкоду життю та здоров’ю людей, безпеці життєдіяльності.

Категорію людей, які займаються несанкціонованим проникненням в мережу, бази даних, зломом програмного забезпечення та ін. отримала назву хакери. Метою їхніх дій можуть бути грошова винагорода, навмисна шкода чи навіть просто цікавість. Так, наприклад, один хакер викрав з кредитних карток Парекс банку близько 7000 доларів; з комп’ютерної бази поліції одного з міст Америки зникла вся база даних про автомобілі, що перебували у розшуку. Також зафіксовано ряд нападів на дані медичних досліджень і особисті файли пацієнтів, що призвело до втрати важливої інформації з відділу гематології науково-медичного центру США, а один з італійських університетів втратив всі

напрацювання за один рік досліджень в області СНІДу. Комп'ютерний вірус, розроблений хакерами, вразив одну велику лікарню на північному сході США, знищивши понад 40% інформації про пацієнтів. У Сполучених Штатах Америки шкода, спричинена хакерами і комп'ютерними шахраями, складає біля $10 млрд. за рік. У Великій Британії комп'ютерна злочинність зросла в чотири рази тільки за останні декілька років і збитки склали 5 млрд. фунтів стерлінгів. Шпигунство з використанням найсучасніших технологій стає звичайним явищем, а кількість хакерів, що займаються цим, постійно зростає.

Для уникнення цього шкідливого явища виділяють наступні підходи в організації захисту інформації: фізичні, законодавчі, управління доступом та криптографічне шифрування [1]. Фізичні методи ґрунтуються на створенні матеріальних обмежень для зловмисника, закриваючи шлях до захищеної інформації. Проте такі способи захищають тільки від зовнішніх зловмисників і не захищають інформацію від тих осіб, які володіють правом входу в приміщення. До законодавчих способів захисту відносяться правові акти, які регламентують правила використання та обробки інформації обмеженого доступу і встановлюють міру відповідальності за порушення цих правил. Сюди ж можна віднести і внутрішньо-організаційні методи роботи й правила поведінки. Під управлінням доступом розуміють захист інформації шляхом регулювання доступу до всіх ресурсів системи (технічних, програмних, елементів баз даних). Встановленою політикою інформаційної безпеки чітко регламентується порядок роботи користувачів і персоналу, право доступу до окремих файлів у базах даних тощо.

Криптографічні способи захисту інформації є найефективнішими у комп’ютерних системах і характеризуються найвищим рівнем захисту. Для цього використовуються програми криптографічного перетворення (шифрування) та захисту юридичної значимості документів (цифровий підпис). Шифрування забезпечує надійне засекречування інформації та використовується в ряді інших сервісних служб [2].

Отже, інформаційної технології відіграють дуже важливу роль у нашому житті, адже вони сприяють науково-технічного прогресу, створюють інформаційний фундамент розвитку науки і всіх інших технологій, не зважаючи на ряд описаних негативних моментів. А використання досвіду подолання комп’ютерної злочинності може суттєво підвищити рівень захисту конфіденційної інформації.

Література:

1. Гундарь, К.Ю. Защита информации в компьютерных системах / К.Ю. Гундарь, А.Ю. Гундарь, Д. А. Янишевский. – К.: Изд–во Корнейчук, 2000. – 152 с.
2. Вербіцький, О.В. Вступ до криптології / О.В. Вербіцький. – Львів.: Вид–во наук.–техн. л–ри, 1998. – 247 с.