УДК 004.031
О.В. Шевчук, Р.М. Небесний
Тернопільський національний технічний університет імені Івана Пулюя

ЗАХОДИ БЕЗПЕКИ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ СИСТЕМАХ

O. Shevchuk, R. Nebesnyy

MEASURES OF SAFET OF INFORMATION IN COMPUTER SYSTEMS

Останнім часом спостерігаються швидкі темпи розвитку комп'ютерних і телекомунікаційних технологій. Впровадження цих технологій у всі сфери людського життя, зробило їх незамінними.

З розвитком комп'ютерних і телекомунікаційних технологій зростає рівень злочинності в комп'ютерному просторі. В зв'язку з цим, для використання комп'ютерних мереж потрібно задіяти ефективні системи захисту, та усунути загрози безпеки інформації в комп'ютерних системах.

Під загрозою розуміють потенційно можливу подію, дію, процес або явище, яке може привести до нанесення шкоди чиїм-небудь інтересам. Загроза інформаційній безпеці КС – можливість реалізації дії на інформацію, що обробляється в КС, що приводить до спотворення, знищення, копіюванні доступу до інформації, а також можливість дії на компоненти КС, що приводить до втрати, знищення або збою функціонування носія інформації, засобів взаємодії або засобів його управління. У даний час розглядається великий перелік загроз інформаційній безпеці КС, що налічує сотні пунктів.

Завдання можливих загроз інформаційній безпеці проводиться з метою визначення повного переліку вимог до системи захисту, що розробляється. Перелік загроз, оцінка ймовірності їх реалізації, а також модель порушника служать основою для аналізу реалізації загроз і формулювання вимог до системи захисту КС. Окрім виявлення можливих загроз має бути проведений аналіз цих загроз на основі їх класифікації за рядом ознак. Кожна з ознак класифікації відображає одну з узагальнених вимог до системи захисту. При цьому загрози, відповідні кожній ознаці класифікації, дозволяють деталізувати певну вимогу до системи захисту.

Необхідність класифікації загроз інформаційній безпеці КС обумовлена тим, що архітектура сучасних засобів автоматизованої обробки інформації, організаційна, структурна і функціональна побудова інформаційно-обчислювальних систем і мереж, технології і умови автоматизованої обробки інформації такі, що схильні до випадкових впливів надзвичайно великого числа чинників, через що стає неможливим формалізувати завдання повного опису загроз. Як наслідок, для системи, що захищається, визначають не повний перелік загроз, а перелік класів загроз.

Вся безліч потенційних загроз за природою їх виникнення розділяється на два класи: природні (об'єктивні) і штучні (суб'єктивні).

Природні загрози – це загрози, викликані діями на АС і її елементи об'єктивних фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні загрози – це загрози КС, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:

– ненавмисні (ненавмисні, випадкові) загрози, викликані помилками в проектуванні КС і її елементів, помилками в програмному забезпеченні, помилками в діях персоналу і т.п;

– навмисні (умисні) загрози, пов'язані з корисливими інтересами людей (зловмисників).

Основними видами загроз безпеки КС і інформації (загроз інтересам суб'єктів інформаційних стосунків) є:

– стихійні лиха й аварії (повінь, ураган, землетрус, пожежа і тому подібне);
– збої й відмови устаткування (технічних засобів) КС;
– наслідки помилок проектування і розробки компонентів КС, а саме апаратних засобів, технології обробки інформації, програм, структур даних і тому подібне;
– помилки експлуатації (користувачів, операторів і іншого персоналу);
– навмисні дії порушників і зловмисників (скривджених осіб з числа персоналу, злочинців, шпигунів, диверсантів і тому подібне).

Українська система основних нормативних документів із захисту інформації або стандарт із захисту, або "критерії", складається із чотирьох документів.

Серед найбільш важливих понять у стандарті подані основні властивості інформації, що визначають її цінність, і називаються фундаментальними властивостями захищеної інформації (ФВЗІ).

Фундаментальні властивості захищеної інформації – конфіденційність, цілісність, доступність і спостережність – характеризуються важливими особливостями: незалежністю одна від одної, конструктивністю, можливістю повторного їх дублювання при використанні різних механізмів і засобів захисту, можливістю врахування конкретних загроз інформації, можливістю визначення послуг забезпечення кожної з властивостей залежно від рівня важливості інформації, очікуваних загроз інформації, цілей і завдань захисту.

Конфіденційність інформації – суб'єктивно визначена характеристика інформації, яка вказує на необхідність введення обмежень на коло суб'єктів, що мають доступ до даної інформації, і забезпечувана здатністю системи зберігати вказану інформацію в таємниці від суб'єктів, що не мають повноважень доступу до неї.

Цілісність інформації – існування інформації в неспотвореному вигляді.

Точніше кажучи, суб'єктів цікавить забезпечення ширшої властивості – достовірності інформації, яке складається з адекватності відображення стану предметної області і безпосередньо цілісності інформації.

Доступність інформації – властивість системи, в якій циркулює інформація, що характеризується здатністю забезпечувати своєчасний безперешкодний доступ суб'єктів до інформації, що цікавить їх, і готовність відповідних автоматизованих служб до обслуговування запитів.

Завжди існують можливості порушення або невиконання властивостей інформації, тобто можливості загроз.

Загрози інформації розглядаються з точки зору їх будь-якого небажаного впливу на будь-яку із цих властивостей і можливого їх порушення, тобто загроза – це потенційно можлива несприятлива дія на інформацію.

Таким чином, відповідно до існуючих підходів, прийнято вважати, що інформаційна безпека КС забезпечена у випадку, якщо для будь-яких інформаційних ресурсів в системі підтримується певний рівень конфіденційності, цілісності, доступності та спостережності.

Література:

1. Алферов А.П. Основы криптографии. Учебное пособие / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М. Гелиос АРВ, 2002. – 480 с. – ISBN 5-85438-025-0.

2. Бобунов А.І. Захист інформації в автоматизованих системах / А.І. Бобунов, В.І. Шестаков. – Житомир: ЖВІРЕ, 2004. – С. 16 - 43.