# ОБРОБКА І ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Пономарьов А.К.
Науковий керівник – ст. викл. Штих І.А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, кафедра ІМІ, тел. (057) 702-14-29)
e-mail: andrii.ponomarov@nure.ua, тел. 0976501381

The widespread use of computer technologies in automated information processing and management systems has exacerbated the problem of protecting information circulating in computer systems from unauthorized access. The protection of information in computer systems has a number of specific features related to the fact that information is not rigidly connected with the medium, can be copied easily and quickly and transmitted through communication channels. A very large number of threats of information are known, which can be realized both by external violators and by internal violators.

Обробка інформації – це процес, що відбувається в часі.

У ряді випадків він повинен підкорятися заданому темпу надходження вхідної інформації і допустимій границі затримки у виробленні інформації на виході. У цьому випадку говорять про обробку інформації в реальному масштабі часу. Прикладом є управління роботою машин і пристроїв, в тому числі комп'ютера.

В інших випадках час розглядається як дискретний ланцюг миттєвих подій. При цьому важлива лише їх послідовність, а не значення поділяючих подій часових проміжків. Такий підхід застосовується зазвичай при обробці інформації в моделюванні.

Найбільш простою формою обробки інформації є послідовна обробка, вироблена одним процесором, в якому в будь-який момент часу відбувається не більше однієї події. При наявності в системі декількох процесорів, що працюють одночасно, говорять про паралельну обробку інформації.

Основними об'єктами захисту при забезпеченні інформаційної безпеки є:

– всі види інформаційних ресурсів. Інформаційні ресурси (документована інформація) – інформація, зафіксована на матеріальному носії з реквізитами, що дозволяють її ідентифікувати;

– права громадян, юридичних осіб і держави на отримання, поширення та використання інформації;

– система формування, поширення і використання інформації (інформаційні системи і технології, бібліотеки, архіви, персонал, нормативні документи і т.д.);

– система формування суспільної свідомості (СМІ, соціальні інститути і т.д.).

Формальні засоби захисту – виконують захисні функції строго по заздалегідь передбаченою процедурою без участі людини.

Фізичні засоби – механічні, електричні, електромеханічні, електронні, електронно-механічні та інші пристрої і системи, які функціонують автономно від інформаційних систем, створюючи різного роду перешкоди на шляху дестабілізуючих факторів.

Апаратні засоби – механічні, електричні, електромеханічні, електронні, електронно-механічні, оптичні, лазерні, радіолокаційні і тому подібні пристрої, що вбудовуються в інформаційні системи або сполучаються з нею спеціально для вирішення завдань захисту інформації.

Програмні засоби – пакети програм, окремі програми або їх частини, які використовуються для вирішення завдань захисту інформації.

До специфічних засобів захисту інформації відносяться криптографічні методи. В інформаційних системах криптографічні засоби захисту інформації можуть використовуватися як для захисту інформації, що обробляється в компонентах системи, так і для захисту інформації, що передається по каналах зв'язку. Саме перетворення інформації може здійснюватися апаратними або програмними засобами, за допомогою механічних пристроїв, вручну і т.д.

Неформальні засоби захисту – регламентують діяльність людини.

Законодавчі засоби – закони та інші нормативно-правові акти, за допомогою яких регламентуються правила використання, обробки та передачі інформації обмеженого доступу і встановлюються міри відповідальності за порушення цих правил. Поширюються на всіх суб'єктів інформаційних відносин.

Організаційні засоби – організаційно-технічні та організаційно-правові заходи, які здійснюються протягом всього життєвого циклу інформаційної системи, яка захищається.

Морально-етичні засоби – сформовані в суспільстві або в даному колективі моральні норми або етичні правила, дотримання яких сприяє захисту інформації, а порушення прирівнюється до недотримання правил поведінки в суспільстві або колективі, веде до втрати престижу і авторитету.

Список літератури: 1. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 445 с. 2. Защита сетевого периметра: наиболее полное руководство по брандмауэрам, виртуальным частным сетям, маршрутизаторам и системам обнаружения вторжений [Текст] / С. Норткатт [и др.]; науч. ред. Н. И. Алишов. – К.; М.; СПб.: DiaSoft, 2004. – 664 с. 3. Якименко І. З. Критерії оцінки рівня захисту комп’ютерних мереж з врахуванням їх архітектури // Інформатика та математичні методи в моделюванні, 2013. – Т. 3 – №1 – С. 82–90.