Організаційно-технічні методи захисту інформації від несанкціонованого доступу

Рожко Д.К., Полотай О.І.

Львівський державний університет безпеки життєдіяльності

Summary. The essence of technical protection of information with the use of organizational and technical methods of protection is described. The main methods and measures for ensuring technical protection of information are given. Described organizational level tasks, which are solved to provide information security in an automated system.

Keywords: information security, unauthorized access, organizational protection, technical protection.

Те, що інформація має цінність, люди усвідомили дуже давно. Її створюють, зберігають, транспортують, продають і купують, а значить – крадуть і підробляють - і, отже, її необхідно захищати. Одним словом, виникнення індустрії обробки інформації призвело до виникнення розробки засобів захисту інформації.

Захист інформації – сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованих систем та осіб, які користуються інформацією.

Несанкціонований доступ – доступ до інформації, що здійснюється з порушенням встановлених в автоматизованих системах правил розмежування доступу.

Залежно від можливих загроз несанкціонованого доступу до інформації методи захисту можна розділити на такі групи: технічні (апаратні), організаційні, програмні.

Технічний захист інформації – це діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Технічний захист інформації в автоматизованих системах і засобах обчислювальної техніки, призначених для формування, пересилання, приймання, перетворення, відображення та зберігання інформації, забезпечується комплексом конструкторських, організаційних, програмних і технічних заходів на всіх етапах їх створення й експлуатації.

У звичному розумінні ця діяльність спрямована на запобігання витоку інформації технічними каналами, її блокуванню та порушенню цілісності.

Основні методи і заходи забезпечення технічного захисту інформації:

- використання захищеного обладнання;
- регламентування роботи користувачів, технічного персоналу, програмних засобів, елементів баз даних і носіїв інформації;
- інженерно-технічне оснащення споруд і комунікацій, призначених для експлуатації автоматизованих систем і засобів обчислювальної техніки;
- пошук, виявлення і блокування закладних пристроїв.

У технічному захисті інформації важливою є атестація об’єкта захисту – офіційне підтвердження органом сертифікації або іншим спеціально уповноваженим органом наявності на об’єкті захисту необхідних й достатніх умов, які забезпечують виконання встановлених вимог та норм ефективності захисту інформації.

Вони або перешкоджають фізичному проникненню, або, якщо проникнення все ж таки відбулося, доступу до інформації, у тому числі за допомогою її маскування. Першу частину завдання вирішують замки, грати на вікнах, захисна сигналізація, другу - генератори шуму, мережеві фільтри, скануючі радіоприймачі і безліч інших пристроїв, що «перекривають» потенційні канали витоку інформації або дозволяють їх виявити. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високою стійкістю до модифікації. Прикладом є екрановані приміщення. Екранування направлене на зниження потужності небажаних випромінювань, які можуть утворити електромагнітний канал витоку інформації. У цілому, екранування приміщень потрібне з метою: віддзеркалення, локалізації, поглинання та зміни структури електромагнітного поля.

Організаційні методи захисту інформації включають заходи та дії, які повинні здійснювати посадові особи в процесі створення й експлуатації системи для забезпечення

заданого рівня безпеки інформації. На організаційному рівні вирішуються наступні завдання забезпечення безпеки інформації в автоматизованій системі:

- організація робіт з розробки системи захисту інформації;
- виховання й навчання обслуговуючого персоналу й користувачів;
- обмеження доступу на об'єкт і до ресурсів системи;
- планування заходів;
- сертифікація засобів захисту інформації;
- атестація об'єктів захисту;
- контроль виконання встановлених правил роботи в системи.

Організаційні методи є базисом комплексної системи захисту інформації в системі. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації в єдину комплексну систему. Вони повинні проводитися при будівництві або ремонті приміщень, у яких буде розміщатися система; проектуванні системи, монтажі й налагодженню її технічних і програмних засобів; випробуваннях і перевірці працездатності системи.

Отже, потрібно чітко розуміти, що будь-які засоби захисту інформації не гарантують абсолютну безпеку і надійність даних, проте вони суттєво мінімізують ризик втрат. При проведенні аналізу та об’єктивної оцінки фахівець з інформаційної безпеки повинен підібрати найефективніші методи та засоби захисту інформації від несанкціонованого доступу, тобто визначити межі розумної безпеки і витрат з одного боку і підтримки системи в працездатному стані з іншого.

Література:

1. Закон України «Про захист інформації в автоматизованих системах» від 05.07.94.
2. Положення про технічний захист інформації в Україні від 11.04.2008.
3. Хоффман Д.Д. Сучасні методи захисту інформації
4. НД ТЗІ 2.5–004–99 критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.