Лекція 19. Автоматизоване керування політикою безпеки

При розгляді питань безпеки інформації в автоматизованих системах (АС) завжди говорять про наявність деяких «бажаних» станів системи. Ці бажані стани (які бувають звичайно представлені в термінах моделі самої АС) описують «захищеність» системи. Поняття «захищеності» принципово не відрізняється від інших властивостей технічної системи, наприклад «надійної роботи». Особливістю поняття «захищеність» є його тісний зв'язок з поняттям «загроза» (те, що може бути причиною виведення системи із захищеного стану).

Отже, виділяються три компоненти, що пов'язані з порушенням безпеки системи:

• «загроза» - зовнішнє відносно системи джерело порушення властивості «захищеність»;

• «об'єкт атаки» - частина системи, на яку діє загроза;

• «канал дії» - середовище перенесення зловмисної дії.

Інтегральною характеристикою, яка об'єднує всі ці компоненти, є політика безпеки (ПБ) - якісний (або якісно-кількісний) вираз властивостей захищеності в термінах, що представляють систему. Опис ПБ повинен включати або враховувати властивості загрози, об'єкта атаки та каналу дії.

За означенням [1, 2], під ПБ інформації розуміється набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін «політика безпеки» може бути застосований до організації, АС, операційної системи (ОС), послуги, що реалізується системою (набору функцій) для забезпечення захисту від певних загроз, і т. ін.

Чим дрібніший об'єкт, щодо якого вживається цей термін, тим конкретніші й формальніші стають правила.

ПБ інформації в АС є частиною загальної ПБ організації і може успадковувати, зокрема, положення державної політики у сфері захисту інформації. Для кожної АС ПБ інформації може бути індивідуальною і залежати

від конкретної технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища та багатьох інших чинників. Частина ПБ, яка регламентує правила доступу користувачів і процесів до ресурсів комп'ютерної системи (КС), становить правила розмежування доступу.

Розробка і підтримка ПБ майже завжди означає досягнення компромісу між альтернативами, які обирають власники цінної інформації для її захисту. Отже, будучи результатом компромісу, ПБ ніколи не задовольнить усі сторони, що беруть участь у захисті інформації.

Водночас вибір ПБ - це остаточне рішення: що добре й що погано в поводженні з цінною інформацією. Після прийняття такого рішення можна будувати захист, тобто систему підтримки виконання правил ПБ. Тоді цілком природним критерієм якості системи захисту інформації (СЗІ) стає такий: побудована СЗІ вдала, якщо вона надійно підтримує виконання правил ПБ, і, навпаки, СЗІ невдала, якщо вона ненадійно підтримує ПБ. Такий розв'язок проблеми захищеності інформації і проблеми побудови СЗІ дає змогу залучити до теорії захисту точні математичні методи [3, 4], тобто доводити, що певна СЗІ в заданих умовах підтримує ПБ. Саме в цьому полягає суть доказового підходу щодо захисту інформації, який дозволяє говорити про «гарантовано захищену систему». Сенс «гарантованого захисту» в тому, що за додержання вихідних умов заздалегідь виконуються всі правила ПБ. Термін «гарантований захист» уперше зустрічається в стандарті міністерства оборони США на вимоги до захищених систем («Оранжева книга»).

Зважаючи на технічні та програмно-апаратні проблеми, що виникають при організації захисту в захищених АС, у багатьох випадках належний рівень захищеності досягається за рахунок вдало реалізованої ПБ, причому іноді ПБ може залишитися майже єдиним засобом забезпечення захисту. Тому розробка, дослідження та правильне застосування ПБ є надзвичайно актуальною проблемою сучасних СЗІ.

Побудова ПБ - це звичайно такі кроки:

• в інформацію вноситься структура цінностей і проводиться аналіз ризику;

• визначаються правила для будь-якого процесу користування певним видом доступу до елементів інформації, які мають певну оцінку цінностей.

Однак реалізація цих кроків є дуже складним завданням. Результатом помилкового або бездумного визначення правил ПБ здебільшого є руйнування цінності інформації без порушення ПБ. Тобто при незадовільній ПБ навіть надійна СЗІ може бути «прозорою» для зловмисника.

ПБ може бути викладена як на описовому рівні, так і за допомогою певної формальної мови. Вона є необхідною (а іноді й достатньою) умовою безпеки системи. Формальний вираз політики безпеки називають моделлю ПБ [3-6].

Основна мета створення ПБ інформаційної системи й опису її у вигляді формальної моделі - це визначення умов, яким має підпорядковуватися поведінка системи, вироблення критерію безпеки і проведення формального доведення відповідності системи цьому критерію при додержанні встановлених правил і обмежень. На практиці це означає, що тільки уповноважені користувачі можуть отримати доступ до інформації і здійснювати з інформацією тільки санкціоновані дії.

Незважаючи на те що створення формальних моделей вимагає суттєвих витрат, вони складні для розуміння і вимагають певної інтерпретації для застосування в реальних системах. Слід констатувати, що формальні моделі потрібні, тому що тільки за їх допомогою можна довести безпеку системи, спираючись на об'єктивні й незаперечні постулати математичної теорії.

Загальним підходом щодо всіх моделей є поділ множини сутностей, що становлять систему, на множини суб'єктів і об'єктів, хоча самі визначення понять «об'єкт» і «суб'єкт» у різних моделях можуть істотно відрізнятися. Взаємодії в системі моделюються встановленням відношень певного типу між суб'єктами та об'єктами. Множина типів відношень визначається у вигляді набору операцій, які суб'єкти можуть здійснювати над об'єктами. Усі операції в системі контролюються певним спеціально призначеним для цього суб'єктом і забороняються або дозволяються відповідно до правил ПБ. ПБ задається у вигляді правил, відповідно до яких мають виконуватися всі взаємодії між

суб'єктами та об'єктами. Взаємодії, що призводять до порушень цих правил, припиняються засобами контролю доступу й не можуть бути здійснені.

Серед моделей ПБ найвідоміші дискреційна, мандатна та рольова. Перші дві досить давно відомі й детально досліджені [3-6], а рольова політика є недавнім досягненням теорії та практики захисту інформації [3].