УДК 681.3.06

Антонюк А. О.

ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ В ЗАХИЩЕНИХ АВТОМАТИЗОВАНИХ СИСТЕМАХ

У статті розглянуто роль одного з найважливіших понять інформаційної безпеки - політики безпеки. Подано огляд найпоширеніших моделей політик безпеки в захищених автоматизованих системах: дискреційна політика, мандатна політика, рольова політика.

1. Визначення політики 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].

2. Дискреційна політика

Основою *дискреційної політики безпеки* (ДПБ) є дискреційне управління доступом (Discretionary Access Control - DAC), яке визначається двома властивостями:

- усі суб'єкти й об'єкти мають бути однозначно ідентифіковані;
- права доступу суб'єкта до об'єкта системи визначаються на основі певних зовнішніх відносно системи правил.

Назва пункту є дослівним перекладом з англійської терміна Discretionary policy, ще один варіант перекладу - розмежувальна політика. Ця політика - одна з найпоширеніших в світі, в системах по замовчуванню мається на увазі саме ця політика.

ДПБ реалізується за допомогою матриці доступу, яка фіксує множину об'єктів та суб'єктів, доступних кожному суб'єкту.

Наведемо приклади варіантів задания матриці доступу.

1. Листи можливостей: для кожного суб'єкта створюється лист (файл) усіх об'єктів, до яких має доступ даний суб'єкт.
2. Листи контролю доступу: для кожного об'єкта створюється список усіх суб'єктів, що мають доступи до цього об'єкта.

До переваг ДПБ можна віднести відносно просту реалізацію відповідних механізмів захисту. Саме цим зумовлено той факт, що більшість поширених нині захищених АС забезпечують виконання положень саме ДПБ.

Однак багатьох проблем захисту ця політика розв'язати не може. Наведемо найбільш суттєві вади ДПБ.

1. Один з найбільших недоліків цього класу політик - вони не витримують атак за допомогою «Троянського коня». Це, зокрема, означає, що система захисту, яка реалізує ДПБ, погано захищає від проникнення вірусів у систему та інших способів прихованої руйнівної дії.

2. Автоматичне визначення прав. Оскільки об'єктів багато і їх кількість безперервно змінюється, то задати заздалегідь вручну перелік прав кожного суб'єкта на доступ до об'єктів неможливо. Тому матриця доступу різними способами агрегується, наприклад, суб'єктами залишаються тільки користувачі, а у відповідну

клітину матриці вставляються формули функцій, обчислення яких визначає права доступу суб'єкта, породженого користувачем, до об'єкта. Звичайно, ці функції можуть змінюватися з часом. Зокрема, можливе вилучення прав після виконання певної події, також можливі модифікації, що залежать від інших параметрів.

3. Контроль поширення прав доступу. Найчастіше буває так, що власник файла передає вміст файла іншому користувачеві і той відповідно набуває права власника на цю інформацію. Отже, права можуть поширюватись, і навіть якщо перший власник не хотів передати доступ іншому суб'єкту до своєї інформації, то після кількох кроків передача прав може відбутися незалежно від його волі. Виникає задача про умови, за якими в такій системі певний суб'єкт рано чи пізно отримає необхідний йому доступ.

4. При використанні ДПБ виникає питання визначення правил поширення прав доступу й аналізу їх впливу на безпеку АС. У загальному випадку при використанні ДПБ органом, який її реалізує і який при санкціонуванні доступу суб'єкта до об'єкта керується певним набором правил, стоїть задача, яку алгоритмічно неможливо розв'язати: перевірити, призведуть його дії до порушень безпеки чи ні.

Отже, матриця доступів не є тим механізмом, який дозволив би реалізувати ясну і чітку СЗІ в АС. Більш досконалою ПБ виявилася мандатна ПБ.

3. Мандатна політика

Основу *мандатної (повноважної) політики безпеки* (МПБ) становить мандатне управління доступом (Mandatory Access Control - MAC), яке передбачає, що:

- всі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;
- у системі визначено лінійно упорядкований набір міток секретності;
- кожному об'єкту системи надано мітку секретності, яка визначає цінність інформації, що міститься в ньому,- його рівень секретності в АС;
- кожному суб'єкту системи надано мітку секретності, яка визначає рівень довіри до нього в АС,- максимальне значення мітки секретності об'єктів, до яких суб'єкт має доступ; мітка секретності суб'єкта називається його рівнем доступу.

Основна мета МПБ - запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу, тобто протидія виникненню в АС інформаційних каналів згори вниз. Вона оперує, таким чином, поняттями інформаційного потоку і цінності інформаційних об'єктів.

Цінність інформаційних об'єктів (або їх мітки рівня секретності) часто дуже важко визначити. Однак досвід показує, що в будь-якій АС майже завжди для будь-якої пари об'єктів X та Y можна сказати, який з них більш цінний. Тобто можна вважати, що таким чином фактично визначається деяка однозначна функція $c(X)$, яка дозволяє для будь-яких об'єктів X і Y сказати, що коли Y більш цінний об'єкт, ніж X, то $c(Y) > c(X)$. І навпаки, якщо $c(Y) > c(X)$, то Y - більш цінний об'єкт, ніж X. Тоді потік інформації від X до Y дозволяється, якщо $c(X) < c(Y)$, і не дозволяється, якщо $c(X) > c(Y)$. Отже, МПБ має справу з множиною інформаційних потоків, яка ділиться на дозволені і недозволені за дуже простою умовою - значенням наведеної функції.

МПБ у сучасних системах захисту на практиці реалізується мандатним контролем на найнижчому апаратно-програмному рівні, що дає змогу досить ефективно будувати захищене середовище для механізму мандатного контролю. Пристрій мандатного контролю називають монітором звернень. Мандатний контроль, який ще називають обов'язковим, оскільки його має проходити кожне звернення суб'єкта до об'єкта, організується так: монітор звернень порівнює мітки рівня секретності кожного об'єкта з мітками рівня доступу суб'єкта. За результатом порівняння міток приймається рішення про допуск.

Найчастіше МПБ описують у термінах, поняттях і визначеннях властивостей моделі Белла-Лападула [3-7]. У рамках цієї моделі доводиться важливе твердження, яке вказує на принципову відмінність систем, що реалізують мандатний захист, від систем з дискреційним захистом: *якщо початковий стан системи безпечний і всі переходи системи зі стану до стану не порушують обмежень, сформульованих ПБ, то будь-який стан системи безпечний.*

Наведемо ряд переваг МПБ порівняно з ДПБ.

1. Для систем, де реалізовано МПБ, є характерним вищий ступінь надійності. Це пов'язано з тим, що за правилами МПБ відстежуються не тільки правила доступу суб'єктів системи до об'єктів, а й стан самої АС. Таким чином, канали витоку в системах такого типу не закладені первісно (що є в положеннях ДПБ), а можуть виникнути тільки при практичній реалізації систем внаслідок помилок розробника.

2. Правила МПБ ясніші і простіші для розуміння розробниками і користувачами АС, що також є фактором, який позитивно впливає на рівень безпеки системи.

3. МПБ стійка до атак типу «Троянський кінь».

4. МПБ допускає можливість точного математичного доведення, що система в заданих умовах підтримує ПБ.

Однак МПБ має дуже серйозні вади - вона дуже складна для практичної реалізації і вимагає значних ресурсів КС. Це пов'язано з тим, що інформаційних потоків у системі величезна кількість і їх не завжди можна ідентифікувати. Саме ці вади часто заважають її практичному використанню.

МПБ прийнята всіма розвинутими державами світу. Вона розроблялася, головним чином, для збереження секретності (тобто конфіденційності) інформації у військових організаціях. Питання ж цілісності за її допомогою не розв'язуються або розв'язуються частково, як побічний результат захисту секретності.

4. Рольова політика

Рольову політику безпеки (РПБ) (Role Base Access Control - RBAC) не можна віднести ані до дискреційної, ані до мандатної, тому що керування доступом у ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів [3]. Отже, рольова модель є цілком новим типом політики, яка базується на компромісі між гнучкістю керування доступом, характерною для ДПБ, і жорсткістю правил контролю доступу, що притаманна МПБ.

У РПБ класичне поняття *суб'єкт* заміщується поняттями *користувач* і *роль*. Користувач - це людина, яка працює з системою і виконує певні службові обов'язки. Роль - це активно діюча в системі абстрактна сутність, з якою пов'язаний обмежений, логічно зв'язаний набір повноважень, необхідних для здійснення певної діяльності.

РПБ застосовується досить широко, тому що вона, на відміну від інших більш строгих і формальних політик, є дуже близькою до реального життя. Справді, по суті, користувачі, що працюють у системі, діють не від свого власного імені - вони завжди виконують певні службові обов'язки, тобто виконують деякі ролі, які аж ніяк не пов'язані з їх особистістю.

Тому цілком логічно здійснювати керування доступом і призначати повноваження не реальним користувачам, а абстрактним (не персоніфікованим) ролям, які представляють учасників певного процесу обробки інформації. Такий підхід до ПБ дозволяє врахувати розподіл обов'язків і повноважень між учасниками прикладного інформаційного процесу, оскільки з точки зору РПБ має значення не особистість користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання його службових обов'язків. Наприклад, у реальній системі обробки інформації можуть працювати системний адміністратор, менеджер баз даних і прості користувачі.

У такій ситуації РПБ дає змогу розподілити повноваження між цими ролями відповідно до їх службових обов'язків: ролі адміністратора призначаються спеціальні повноваження, які дозволять йому контролювати роботу системи і керувати її конфігурацією, роль менеджера баз даних дозволяє здійснювати керування сервером БД, а права простих користувачів обмежуються мінімумом, необхідним для запуску прикладних програм. Крім того, кількість ролей у системі може не відповідати кількості реальних користувачів - один користувач, якщо він має різні повноваження, може виконувати (водночас або послідовно) кілька ролей, а кілька користувачів можуть користуватися однією й тією ж роллю, якщо вони виконують однакову роботу.

При використанні РПБ керування доступом здійснюється в дві стадії: по-перше, для кожної ролі вказується набір повноважень, що представляють набір прав доступу до об'єктів, і, по-друге, кожному користувачеві призначається список доступних йому ролей. Повноваження призначаються ролям відповідно до принципу найменших привілеїв, з якого випливає, що кожний користувач повинен мати тільки мінімально необхідні для виконання своєї роботи повноваження.

У моделі РПБ визначаються множини: множина користувачів, множина ролей, множина повноважень на доступ до об'єктів, наприклад, у вигляді матриці прав доступу, множина сеансів роботи користувачів з системою.

Для перелічених множин визначаються відношення, які встановлюють для кожної ролі набір наданих їй повноважень, а також для кожного користувача- набір доступних йому ролей.

Правила керування доступом РПБ визначаються певними функціями, які для кожного сеансу визначають користувачів, набір ролей, що можуть бути одночасно доступні користувачеві в цьому сеансі, а також набір доступних у ньому повноважень, що визначається як сукупність повноважень усіх ролей, що беруть участь у цьому сеансі.

Як критерій безпеки рольової моделі використовується правило: *система вважається безпечною, якщо будь-який користувач системи, що працює в певному сеансі, може здійснити дії, які вимагають певних повноважень тільки в тому випадку, коли ці повноваження належать сукупності повноважень усіх ролей, що беруть участь у цьому сеансі.*

З формулювання критерію безпеки рольової моделі випливає, що управління доступом здійснюється, головним чином, не за допомогою призначення повноважень ролям, а шляхом встановлення відношення, яке призначає ролі користувачам, і функції, що визначає доступний у сеансі набір ролей. Тому численні інтерпретації рольової моделі відрізняються видом функцій, що визначають правила керування доступом, а також обмеженнями, що накладаються на відношення між множинами.

Завдяки гнучкості та широким можливостям РПБ суттєво перевершує інші політики, хоча іноді її певні властивості можуть виявитися негативними. Так, вона практично не гарантує безпеку за допомогою формального доведення, а тільки визначає характер обмежень, виконання яких і є критерієм безпеки системи. Хоча такий підхід дозволяє отримати прості й зрозумілі правила контролю доступу (перевага), які легко застосовувати на практиці, проте позбавляє систему теоретичної доказової бази (вада). У деяких ситуаціях ця обставина утруднює використання РПБ, однак у кожному разі оперувати ролями набагато зручніше, ніж суб'єктами (знову перевага), оскільки це більше відповідає поширеним технологіям обробки інформації, які передбачають розподіл обов'язків і сфер відповідальності між користувачами.

Крім того, РПБ може використовуватися одночасно з іншими ПБ, коли повноваження ролей, що призначаються користувачам, контролюється ДПБ або МПБ, що дозволяє будувати багаторівневі схеми контролю доступу.

5. Значення політики безпеки

Наведений огляд сучасних ПБ визначає основні принципи їх функціонування, а також підкреслює їх роль і виключну важливість при побудові та експлуатації захищених АС. Додамо, що в багатьох сучасних програмних засобах захисту інформації розглянуті ПБ уже реалізовані. Однак слід зазначити, що це зовсім не означає їх механічного застосування. Зрозуміло, що спочатку в конкретній організації має бути проведений ретельний аналіз процесів обробки інформації, на основі якого потім створюється і застосовується конкретна ПБ.

Необхідно також зазначити, що, крім загального опису поняття ПБ, в Українському стандарті з технічного захисту інформації [1, 2] більш конкретних нормативних та методичних матеріалів з розробки ПБ для АС поки що немає. Зауважимо, що, в більшості організацій (як державних, так і недержавних) про поняття ПБ навіть не мають уявлення. Але парадокс якраз полягає в тому, що фактично в будь-якій організації завжди існують конкретні правила, що регламентують процес її функціонування, зокрема і процес захисту інформації, а саме ці правила і є політикою. Отже, фактично в будь-яких АС окремі елементи ПБ завжди наявні.

1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1—003—99.— К.: ДСТСЗІ СБ України, 1999.- 26 с
2. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99.- К.. ДСТСЗІ СБ України, 1999- 16с.
3. Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжды- М: Яхтсмен, 1996- 302 с.
4. *Грушо А. А., Тимонина Е. Е.* Теоретические основы защиты информации-М.: Яхтсмен, 1996.- 192 с.
5. Теоретические основы компьютерной безопасности / Девянин П. Н. и др.- М.: Радио и связь, 2000- 192 с.
6. *Щербаков А. Ю.* Введение в теорию и практику компьютерной безопасности-М.: Изд. С. В. Молгачева, 2001 -352 с.
7. *Галашенко В. А.* Информационная безопасность: практический подход. - М : Наука, 1998-301 с.

AntoniukA. O.

THE INFORMATION SECURITY POLICY IN SECURITY INFORMATION SYSTEMS

The role of security policy, one of the most important notions of information security, is considered. Review of the most used models of security policy in security information systems such as discretionary policy, mandatory policy, and role-base policy are given in this article.