УД К 681.3.06

Антонюк А. О.

МОДЕЛЮВАННЯ ДИСПЕТЧЕРА ДОСТУПУ В ЗАХИЩЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

Розглянуто підхід щодо моделювання диспетчера доступу для захищених комп'ютерних систем. У рамках запропонованого формалізму описано деякі аспекти його функціонування, зокрема безпечну обробку запитів. Визначено і вивчено множину можливих політик безпечної обробки запитів.

1. Вступ

Вважають, що комп'ютерна система (КС) є сукупністю певних сутностей, які називатимуть об'єктами згідно з [1; 2]. Функціонально узгоджену групу об'єктів назвемо компонентою КС.

З'ясуємо основні положення, на яких базується подальший розгляд діяльності КС [3; 4]:

- у захищеній КС завжди наявна активна компонента, яка виконує функцію контролю над операціями між об'єктами і, фактично, відповідальна за реалізацію певної політики безпеки (ПБ) [1];
- для здійснення операцій з об'єктами в захищеній КС необхідна додаткова інформація (і наявність об'єкта, що її містить) про дозволені та заборонені операції;
- функціонування КС і питання ПБ описуються послідовностями доступів одних об'єктів до інших [3];
- у будь-якій КС між її об'єктами існує обмін інформацією, який реалізується за допомогою інформаційних потоків між об'єктами, а отже, завжди повинен бути об'єкт-відправникі об'єкт—одержувач інформації;
- вся множина потоків між усіма об'єктами КС у всі моменти часу є об'єднанням потоків за всіма моментами дискретного часу;
- з іншого боку, КС є об'єднанням двох множин, що не перетинаються, одна з якихха-рактеризує несанкціонований доступ (НСД), а друга — множину потоків, що визначають легальний доступ.

Нагадаємо, що згідно з [1], під ПБ інформації слід розуміти набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на її захист від певних загроз.

ПБ інформації в КС є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної КС ПБ інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС (обчислювальна система), фізичного середовища і від багатьох інших чинників.

Необхідною умовою реалізації ПБ є наявність у КС згаданої вище активної її компоненти, яка повинна при виникненні будь-яких інформаційних потоків активізуватися і надалі проводити необхідну їх фільтрацію відповідно до зазначених вище множин потоків. Такою компонентою є диспетчер доступу (ДД) [3;4] — об'єкт КС, який активізується при виникненні потоку від одного об'єкта до іншого і за рахунок фільтрації дозволяє реалізуватися потокам, що належать множині легального доступу. Для досягнення такої мети ДД слід виконувати цілу низку конкретних дій, кожна з яких має визначатися своєю ПБ. Зокрема, при обробці ДД запитів до КС від інших об'єктів реакція ДД у вигляді відповідей або певних дій не повинна спричинювати до виникнення каналів НСД. Тобто політику обробки запитів (ПОЗ) [5] як частину загальної ПБ КС має бути сформульовано таким чином, щоби відповіді ДД не містили таємної інформації і ДД не виконував заборонені для КС дії. Нижче розглянуто один із підходів шодо моделювання ПОЗ, а також визначено і вивчено множину можливих їх модифікацій для захищених КС - множину політик безпечної обробки запитів (ПБОЗ). Цей підхід є розвитком формалізму, який розглянуто в [6] для опису взаємодії мультипрограмних агентів.

2. Диспетчер доступу (ДД)

Під час проектування захисних механізмів необхідно вирішити, якими властивостями має

володіти ДД, щоб реально забезпечити контроль над потоками між об'єктами. Нижче розглянуто ДД, діяльність яких полягає в певній реакції ДД на запити об'єктів-клієнтів: надсилання відповідей або виконання певних дій. Такі дії ДД, наприклад, частково властиві процесу ідентифікації та автентифікації об'єктів при їх вході в КС. Частково, бо в таких процесах діяльність ДД є тривіальною – вона зводиться до відповідей «так» чи «ні». Небезпечнішими є можливості зловмисника спробувати або шось вивідати, або спровокувати неправильну дію ДД. Такі можливості з'являються, наприклад, при втручанні зловмисника в процес взаємодії банків зі своїми розподіленими офісами або клієнтами чи при роботі із захищеними базами даних, де канали витоку можуть виникати за рахунок агрегації даних або логічних висновків [3; 5].

Отже, виникає проблема забезпечення інформаційної безпеки (ІБ) КС у процесі обміну повідомленнями. Для забезпечення виконання вимог ІБ має існувати механізм, який би гарантував, що ДД, обробляючи запити від інших об'єктів, ніколи не розкриє їм таємну інформацію і не виконає ніяких небажаних дій. Більше того, поняття безпеки слід посилити, наприклад, для випадків, коли ДД, відповідаючи на запит, повинен гарантувати, що об'єкт-клієнт логічно не виведе таємну інформацію, розголошувати яку він не має права. Саме такі канали витоку інформації найскладніше ідентифікувати й перекривати. У зв'язку з цим прості запити (коли відповідь означена чіткими правилами – інструкцією тошо) не розглядатимуться, а надалі оброблятимуться тільки запити, на основі яких з певних даних можна логічно вивести нові дані.

При визначенні властивостей, якими повинен володіти ДД, використовуватимуться такі положення:

- у будь-який момент часу ДД завжди перебуває у певному *стані*;
- у будь-який момент часу ДД містить набір даних *про свої попередні взаємодії* (далі – просто набір даних (НД)) з іншими об'єктами, що важливо для формування його подальших рішень;
- у ДД є *механізм логічних висновків*, який використовується для того, щоб на основі наявних даних логічно виводити нові дані;
- ДД може оцінювати будь-який запит, використовуючи *функцію визначення сервісу*, яка визначає послідовність його дій як реакцію на запит, що надійшов (послугами яких об'єктів потрібно буде скористатися, які потрібно буде виконати запити/операції тощо).

Стан ДД визначається множиною фактів, які є істинними у момент часу, відповідний цьому стану, і синтаксична структура яких представлена у вигляді слова або послідовності слів певної мови. Надалі ДД позначатимемо d.

Розглянемо два типи подій, які можуть змінити стан d, адже всі інші події так чи інакше зводяться до них.

Події-дії, що позначаються відповідними іменами дій, є діями, які d виконує автономно або за запитом іншого об'єкта.

Події-повідомлення, що позначаються трійкою $\{$*відправник*, *одержувач*, *тіло*$\} = \{s, r, m\}$, де відправник s і одержувач r є об'єктами, причому завжди $s \neq r$, а тіло m – це або запит на надання сервісу, або відповідь, яка належить до вхідної множини фактів $F = \{f_1, f_2, ...\}$, де f_i – певні повідомлення (запити або відповіді). До множини фактів d завжди має доступ.

Якщо тип події не має значення, то i-а подія позначатиметься e_i.

Означення 1. Послідовність подій $H = \{e_1, e_2, ...\}$ називають набором даних (НД) для певного d, якщо кожна дія з H може бути виконана d і для кожного повідомлення $\{s, r, m\}$ з H завжди або $s = d$, або $r = d$.

Отже, в НД зберігаються повідомлення, якими він обмінюється з іншими об'єктами, і повідомлення-дії, які d вчиняє. Очевидно, d може мати як повний НД, так і неповний, оскільки з яких-небудь причин (наприклад, ДД повинен працювати в режимі реального часу, внаслідок чого об'єм НД буде невеликим, а отже, не всі повідомлення зберігатимуться) може зберігати не всі події в своїй діяльності. Тобто для кожного d існує ціла множина НД, яку позначатимемо H. Можливе також об'єднання декількох НД (наприклад, для двох НД H_1 і H_2 об'єднанням буде H_1H_2). Події з НД для d визначають його поточний стан.

Означення 2. Для H деякого d стан, що настав одразу ж після послідовності всіх подій H, позначимо $S_d(H)$. Початковий стан d позначимо $S_d(0)$.

Усі НД для певного d повинні бути *коректними* в тому сенсі, що не всі вони можуть описувати можливу його поведінку. Наприклад, певні НД взагалі неможливі, оскільки суперечитимуть закономірностям його поведінки; інші НД взагалі неможливі, оскільки можуть містити повідомлення від об'єктів, з якими d ніколи не спілкувався, тощо. Надалі вважатимемо, що в цьому сенсі множина H завжди є *коректною*.

Очевидно також, що будь-який НД містить кінцеву кількість повідомлень.

У принципі, «інтелектуальні» d можуть шляхом висновків одержувати нові факти, виходячи з інформації, що зберігається в їх НД. Моделювання процесу логічних висновків (відношення слідування) об'єкта d грунтується на його НД і множині фактів.

Означення 3. Функцію D називають відношенням слідування, якщо певній підмножині фактів $X \subseteq F$ ставиться у відповідність така множина $D(X)$, за якої $X \subseteq D(X)$, тобто функція $D(X)$ повертає всі факти, що пов'язані із вхідною множиною X, плюс деякі висновки відповідно до поняття слідування, прийнятого для даного d. Для відношення $D(X)$ справедливе очевидне співвідношення $D(D(X))=D(X)$.

Надалі вважатимемо, що кожний ДД обробляє тільки один запит і не суміщає обробку двох різних запитів одночасно. Крім того, кожен запит на надання сервісу обробляється відповідно до певного шаблону поведінки: спочатку, якщо необхідно, d спілкується з іншими об'єктами (щоб отримати певну інформацію, зарезервувати ресурси тощо), потім чекає від них відповідей, виконує деякі внутрішні дії (без комунікації з іншими об'єктами) і, нарешті, відповідає на запит об'єкта-клієнта (якщо потрібно). Цей шаблон поведінки спрощує моделювання обробки запиту на надання сервісу з погляду потреб безпеки, оскільки дає змогу окремо розглядати послідовність дій d, викликаних запитом і відповіддю на запит.

Припустимо, що є d і H – деякий його НД, в якому остання подія – це вхідне повідомлення $\{b, d, p\}$, де b – об'єкт-відправник повідомлення, p – запит (наприклад, на надання певного сервісу). Визначимо функції, які використовує d для обробки запитів:

- функція визначення контактів C, входом якої є НД H, а виходом – послідовність вихідних повідомлень, тобто

$$C(H)=\{\{d, c_1, p_1\},...,\{d, c_n, p_n\}\};$$

- функція визначення дій A, входом якої є НД H і послідовність вхідних повідомлень $Resp$, тобто множина дій – це функція $A(H, Resp)$, де послідовність вхідних повідомлень $Resp$ є відповіддю на послідовність запитів (контактів) $C(H)$ і позначається

$$Resp(C(H)) =\{\{c_1, d, p_1\},...,\{c_n, d, p_n\}\};$$

- функція визначення відповідей Q, яка має вхід попередньої функції і певну початкову множину фактів X, а вихід – множина відповідей $Q(H, Resp, X)$;
- об'єднання наведених функцій назвемо функцією обробки запиту $Z(H) = (H, C(H), Resp(C(H)), A(H, Resp), \{d, b, Q(H, Resp, X)\})$, причому b у цьому записі позначає останній об'єкт, який звернувся до ДД за запитом.

Зазначимо, що практична реалізація наведених функцій вимагає впровадження в КС цілого комплексу апаратних, програмних та організаційних механізмів та заходів, тобто фактично регламентує порядок обробки запитів у КС, тому цілком правомірно назвати трійку $\{C, A, Q\}$ ПОЗ.

Очевидно, що $Z(H)$ доповнює НД H подіями, викликаними останнім запитом $\{b, d, p\}$ (цей запит має місце у кінці НД H до його доповнення). Частини обробки запиту, в яких робляться необхідні дії і повертаються запитані дані, залежать від відповідей, модельованих за допомогою $Resp(C(H))$. Оскільки трійка $\{C, A, Q\}$ однозначно визначає функцію обробки запиту $Z(H)$, надалі використовуватимемо також символічне позначення $Z(H) = \{C, A, Q\}$.

3. Безпечна обробка запитів

На основі описаного формалізму перейдемо до визначення ПБОЗ. З усіх відомостей НД, яким володіє d, виділимо ті дані, які він повинен приховувати від інших об'єктів, а також дії, які він не повинен виконувати для інших об'єктів. Це демонструють означення, наведені нижче.

Означення 4. Функція секретів S_d довільному об'єкту $b \neq d$ ставить у відповідність підмножину фактів $F_d \subseteq F$, які d хотів би тримати в секреті від об'єкта b, тобто $S_d(b) = F_d \subseteq F$, або інакше – для всіх $\{d, b, p\}$ $p \notin S_d(b)$.

Наступним необхідним кроком є введення функцій безпеки дій d, яка визначатиме, які дії він повинен або не повинен виконувати за запитом деякого іншого об'єкта.

Означення 5. Функцією безпеки дій d називається функція S_d, яка довільному об'єкту $b \neq d$ ставить у відповідність множину, що містить лише:

- вихідні повідомлення вигляду $\{d, c, p\}$, де $\forall\, c \neq b$;
- послідовності заборонених дій.

Перше обмеження означає, що S_d повинна містити множину повідомлень до інших об'єктів, на які d не відповідатиме на вимогу b, оскільки такі відповіді теж є діями. Друге ж фіксує послідовності дій, які d не повинен виконувати на запит об'єкта b.

З метою забезпечення безпеки потрібно модифікувати звичайну ПОЗ таким чином, щоб

отримати ПБОЗ, яка належала б d, захищала б інформацію і запобігала б виконанню недозволених послідовностей дій. Надалі ПБОЗ і її модифіковані компоненти позначатимемо за допомогою риски, щоб відрізняти їх від відповідних небезпечних компонент.

Фактично ПБОЗ – це та ж ПОЗ на сервіси, але додатково забезпечує безпеку при їх обробці, тобто $\bar{Z}(H) = (H, \bar{C}(H), Resp((\bar{C}(H)), \bar{A}(H, Resp), \{d, b, \bar{Q}(H, Resp, F_d)\})$.

Трійку $\{\bar{C}, \bar{A}, \bar{Q}\}$, або $\bar{Z}(H) = \{\bar{C}, \bar{A}, \bar{Q}\}$, називатимемо ПБОЗ. Звичайно, з метою забезпечення безпеки d повинен обробляти вхідні запити вже відповідно до модифікованих функцій $\bar{C}, \bar{A}, \bar{Q}$. Слід зауважити, що поки не йшлося про те, що саме означає для модифікованої політики (МП) бути безпечною. Оскільки функція обробки запиту $\bar{Z}(H)$ визначає реакцію об'єкта d на вхідні повідомлення, множина можливих наборів даних для d повинна бути сумісною з поведінкою, яка визначається $\bar{Z}(H)$. При цьому необхідно враховувати діяльність d щодо розв'язання проблем:

- захисту даних d за допомогою функції S_r;
- запобігання виконання небажаних дій, яке визначається функцією $S_a(b)$.

Розглянемо ці проблеми детальніше.

4. Захист даних

Для забезпечення захисту даних d найпростішим підходом була б вимога від КС (будь то об'єкти, бази тощо) просто не включати таємну інформацію в їх відповіді на будь-які запити. Проте така цілком розумна вимога безпеки недостатньо забезпечує захист даних, унаслідок чого назвемо її слабкою безпекою.

Означення 6. Модифікована функція $\bar{Z}(H)$ з функціями $\bar{Q}$ і $\bar{C}$ задовольняє вимоги слабкої безпеки, якщо для всіх наборів даних H з останньою подією – запитом від об'єкта b і для всіх відповідей виконується умова $\bar{Q}(H, Resp(\bar{C}(H)), X) \cap S_r(b) = \varnothing$, тобто будь-яка відповідь d просто не повинна містити таємної інформації.

Для простих користувацьких об'єктів цієї мінімальної форми безпеки в більшості випадків може бути достатньо, однак це не гарантує захист інформації від інтелектуальних об'єктів, оскільки в цьому означенні не враховується можливість, використовуючи своє відношення слідування, логічно виводити нову інформацію. Отже, d не повинен допустити, щоб об'єкт b шляхом логічних висновків прийшов до фактів з $S_r(b)$.

Простим рішенням цієї проблеми могло б бути затвердження обмеження типу: модифікована функція $\bar{Z}(H)$ задовольнятиме вимогам безпеки даних, якщо об'єкти-користувачі b об'єкта d ніколи не зможуть не тільки отримати, а й логічно вивести таємну інформацію про d. Проте таке обмеження не враховує тривіальну ситуацію, коли порушення безпеки можуть бути викликані деяким іншим об'єктом $c \neq b$, тобто об'єкт c просто повідомляє об'єкту b якусь таємну інформацію, і тоді порушення безпеки аж ніяк не залежить від d. Причому це може трапитися навіть тоді, коли згідно зі своєю ПБ d зберігатиме повне мовчання.

Таку парадоксальну ситуацію можна усунути шляхом введення більш жорсткого поняття безпеки. Суть його полягає в тому, що d повинні бути відповідальні тільки за свої власні відповіді на запити. МП буде безпечною, якщо вона ніколи не збільшуватиме множину секретів, відомих іншим об'єктам, тобто вона повинна задовольняти вимогам захисту даних так довго, як довго об'єкт b не зможе логічно вивести нові секрети, використовуючи відповіді d. Це означає, що об'єкту b слід мати певні властивості, які притаманні d. Отже, вважаємо, що кожний об'єкт b має свій НД, який позначимо H_b – стан, що настав одразу ж після послідовності всіх подій $H_b - S_b(H_b)$, де $S_b(0)$ – початковий стан. Тепер можна визначити більш сильне поняття безпеки даних.

Спочатку введемо поняття сумісності (строгої сумісності) НД.

Означення 7. НД H_1 і H_2 об'єктів d і b є db-сумісними (позначається $H_1 \xleftrightarrow{db} H_2$), якщо будь-які підпослідовності послідовностей H_1 і H_2, отримані шляхом видалення з них всіх повідомлень, окрім повідомлень типу $\{d, b, ...\}$ і $\{b, d, ...\}$, збігаються. Якщо ж і останні події в $H_1 \xleftrightarrow{db} H_2$ збігаються, то НД H_1 і H_2 називаються строго db-сумісними, що позначатиметься $H_1 \xleftrightarrow{\overline{db}} H_2$.

Як приклад розглянемо два НД:

$$H_1 \{\{b, d, p_1\}, \{d, c, p_2\}, \{c, b, p_3\}, ..., \{d, b, p_n\}\};$$

$$H_2 \{\{b, d, p_1\}, \{d, c, p_4\}, \{c, b, p_3\}, ..., \{d, b, p_n\}\}.$$

Легко дійти висновку, що НД H_1 і H_2 є db-сумісними і bc-сумісними, але не dc-сумісними. Більше того, НД і є строго db-сумісними

і строго *bc*-сумісними, оскільки останні події в цих НД однакові.

Далі введемо означення множини секретів *d*, які можуть бути логічно виведені об'єктом *b* в деякий момент часу, грунтуючись на деякому НД H_b для об'єкта *b*. Нагадаємо, що відповідно до означень 3,4 $D(S_b(H_b))$ – множина фактів, які можуть бути виведені об'єктом *b* в поточному стані, $S_r(b)$ – множина фактів, які *d* хотів би тримати в секреті від об'єкта *b*.

Означення 8. Розкритими секретами називається множина $V(H_b) = D(S_b(H_b)) \cap S_r(b)$.

Це означення дає змогу формалізувати більш сильне поняття безпеки даних, сутність якого полягає в тому, що МП об'єкта задовольняє умову безпеки даних, якщо вона гарантовано не збільшує множину секретів, розкритих іншими об'єктами.

Нехай для деякого *d* остання подія *e* в НД *H* – це запит від об'єкта *b*.

Означення 9. МП $\overline{Z}(H)$ задовольняє умову безпеки даних у момент *H*, якщо для всіх НД $H_b e \subseteq H$, таких що $H_b e \xleftarrow{\overline{bd}} \overline{Z}(H)$ виконується умова $V(H_b) \supseteq V(H_b e)$.

Щоб зрозуміти це означення, пригадаємо, що $\overline{Z}(H)$ – це НД об'єкта *d* відразу ж після його відповіді на запит об'єкта *b*. Таким чином, умови $H_b e \subseteq H$ і $H_b e \xleftarrow{\overline{bd}} \overline{Z}(H)$ вимагають, щоб $H_b e$ був можливим НД для об'єкта *b*, коли він отримає відповідь від *d*. Далі помітимо, що з $H_b e \xleftarrow{\overline{bd}} \overline{Z}(H)$ та означення $\overline{Z}(H)$ випливає, що *e* – це відповідь *d* об'єкту *b*, яка має вигляд $\{d, b, \overline{Q}(H, Resp(\overline{C}(H)))\}$. Включення в означенні 9 означає, що множина розкритих об'єктом *b* секретів не збільшиться після отримання відповіді від *d*. Для всіляких НД $H_b e$ з вищезазначеними властивостями необхідно, щоб дані були захищені незалежно від того, які дії може зробити об'єкт *b* перш ніж отримати відповідь, включаючи його запити до інших об'єктів і отримання відповідей від них.

Слабку безпеку можна представити як окремий випадок безпеки даних. Справді, якщо об'єкт-клієнт *b* тільки зберігає відповіді об'єкта *d* і не робить з них ніяких висновків, то слабка безпека і безпека даних просто збігаються. У деяких випадках вони збігаються завжди, що підтверджує наведене нижче твердження.

Теорема 1. Якщо в деякій КС НД для *d* і *b* мають вигляд $H_n = \{q_1, a_1, ..., q_n, a_n\}$, де q_i – запит об'єкта *b* до *d*, а a_i – відповідь на q_i, причому $S_b(0) = \varnothing$, $S_b(H_n) = \bigcup_{i=1}^{n} a_i$ і $D(H_n)$ – тотожне відображення для всіх станів *b*, тобто $D(H_2) = H_2$, то для таких КС слабка безпека збігається з безпекою даних.

Доведення. Розглянемо найпростішу КС, яка складається з двох об'єктів *d* і *b*. Очевидно (за умов теореми), що $V(S_b(0)) = \varnothing$ і $\overline{Z}(H)$ задовольняє умову безпеки даних тоді і тільки тоді, коли $V(S_b(0)) \supseteq V(H_1) \supseteq V(H_2) \supseteq ... \supseteq V(H_n)$. Однак тоді $V(H_n) = \varnothing$ для $\forall i$, $i = 1, ..., n > 0$. Оскільки $V(H_n) = \bigcup_{i=1}^{n} a_i \cap S_r(b)$, то $\overline{Z}(H)$ задовольняє умову безпеки даних тоді і тільки тоді, коли для $\forall_i$ буде $a_i \cap S_b(0) = \varnothing$. Але це якраз еквівалентно тому, що $\overline{Z}(H)$ задовольняє умову слабкої безпеки. Теорему доведено.

З іншого боку, безпека даних не завжди викликає слабку безпеку. Наприклад, *d* може передавати об'єкту *b* секрети, які об'єкт *b* вже знає. У цьому випадку формально безпека даних дотримується, тоді як слабка безпека порушується.

5. Безпека дій

Аналогічно поняттю МП, що задовольняє безпеці даних, можна визначити поняття МП, що задовольняє безпеці дій.

Припустимо, що *H* – певний НД для *d*, останньою подією якого є запит {*b*, *d*, *p*}.

Означення 10. МП $\overline{Z}(H)$ задовольняє умову безпеці дій у момент *H*, якщо для всіх послідовностей вхідних повідомлень $Resp(\overline{C}(H))$ відповідного типу повідомлення із $\overline{C}(H)$ не входять до $S_a(b)$, тобто $\overline{C}(H) \cap S_a(b) = \varnothing$, і жодна частина послідовності $\overline{A}(H, Resp(\overline{C}(H)))$ не міститься в $S_a(b)$, тобто $\overline{A}(H, Resp(\overline{C}(H))) \cap S_a(b) = \varnothing$.

Це означення фіксує ситуацію, коли всі вихідні повідомлення від *d* контролюються ним і не містять заборонених дій. За його допомогою, зокрема, неважко виділити клас КС, для

яких МП $\bar{Z}(H)$ напевне задовольнятиме умову безпеки дій.

Теорема 2. Якщо в деякій КС НД для d містить всю інформацію про всі об'єкти b (d «знає» все про всіх своїх клієнтів), тобто $H_b \subseteq H, X_b \subseteq X$, і має місце тотожність відображення $D_b(X) = X$ для $\forall X$, то для таких КС МП $\bar{Z}(H)$ задовольняє безпеці дій. Тут X_b – початкова множина фактів b, D_b – його відношення слідування.

Доведення. Умови $H_b \subseteq H, X_b \subseteq X$ означають, що в будь-який момент d може завжди точно визначити множину $S_a(b)$ для будь-якого b до відправлення повідомлення за допомогою функції $\bar{C}(H)$, тобто фактично може контролювати зміст цих множин, а отже, $\bar{C}(H) \cap S_a(b) = \varnothing$. Будь-який об'єкт b, зважаючи на $D_b(X_b) = X_b$, не зможе отримати нічого нового з повідомлення $\bar{C}(H)$. Це означає, що зміст множини $\bar{A}\left(H, Resp\left(\bar{C}(H)\right)\right)$ теж під контролем d, оскільки в $Resp\left(\left(\bar{C}(H)\right)\right)$ не може виникнути нічого нового. Отже, $\bar{A}\left(H, Resp\left(\bar{C}(H)\right)\right) \cap S_a(b) = \varnothing$. Теорему доведено.

6. Модифікації політики безпеки

Попередні означення спричинюють виникнення ряду інших означень.

Означення 11. МП (або ПБОЗ) $\bar{Z}(H)$ є безпечною у будь-який момент H, якщо вона задовольняє умови безпеки даних і безпеки дій.

Існує багато способів реалізації МП обробки запитів і дій. Один із тривіальних способів – взагалі не відповідати на запити і не робити ніяких дій. Проте це дуже нераціональний спосіб поведінки. Іншою крайністю є така модифікація функції обробки сервісу, за якої модифікована функція, а отже, і поведінка об'єкта, найменше відрізняється від оригінальної і при цьому все ж забезпечує безпеку об'єкта. Необхідний баланс між безпекою і ступенем модифікації залежить від багатьох чинників, які, своєю чергою, – від додатків, серед яких слід зазначити якість функціонування конкретного сервісу і час відгуку на запит (враховуючи час існування таємної інформації).

Незалежно від пошуку компромісу вищенаведені міркування припускають існування якогось наближення або ступеня модифікації відповіді/дії. У відповідь на запит можна мати допустиму множину відгуків-реакцій (у тому числі модифікованих). Якщо розглядати цю множину як простір з метрикою, то може виявитися, що один із цих відгуків ближче до оригінального, ніж інші. Можна також ввести відношення часткового порядку на множині відповідей-відгуків.

Для розуміння суті такого балансу розглянемо деякі приклади. Припустимо, що деякий користувач хоче отримати інформацію (протокол) про поточний стан КС. Якщо для i моментів часу цю інформацію позначити L_i, то, звичайно, L_{30} є більш придатною модифікацією істинної відповіді L_0, ніж, наприклад, L_{60}.

Інший приклад. Нехай деякий агент шукає людей за певною ознакою. Припустимо, що агент, до якого він робив запит, подав список з 10 імен таких людей. Тоді відповідь, що складається з 9 імен, буде точнішим наближенням (*а модифікація придатнішою*) *до реального, ніж* відповідь, що складається тільки з 5 імен.

Таким же чином, якщо об'єкт робить запит щодо виконання дії, яка не може бути повністю виконана з міркувань безпеки, можна порадити йому зробити дію, яка є максимально наближеною до запитуваної, але не порушує безпеку. Припустимо, що об'єкт отримує запит на забезпечення пересування на час подорожі. Нормальною реакцією буде, наприклад, замовлення квитків в аеропорту і забезпечення пересування до аеропорту. Але якщо з міркувань безпеки виконання цих дій тимчасово заборонено, то більш прийнятним варіантом поведінки може бути пошук відповідного потягу, замовлення місць і забезпечення транспортування на залізничний вокзал.

Припустимо, що *Ans* – множина можливих відповідей, які d може надати іншим об'єктам, і для *Ans* задане відношення часткового порядку $\leq_n$. Аналогічно, *Act* – множина фактичних дій d, і $\leq_c$ – відношення часткового порядку, задане на послідовності дій в *Act*. Наприклад, для L_i з попереднього прикладу відношення часткового порядку вводиться дуже просто – звичайний знак нерівності. У складніших випадках можна скористатися включенням множин. Звернемо увагу на те, що це взагалі різні відношення часткового порядку.

Означення 12. МП $\bar{Z}(H) = \{\bar{C}, \bar{A}, \bar{Q}\}$ є більш придатною відносно даних (відповідно дій), ніж інша МП $\bar{Z}'(H) = \{\bar{C}', \bar{A}', \bar{Q}'\}$, якщо для всіх НД H об'єкта d і для всіх відповідей $Resp(C(H))$ і $Resp(C'(H))$ виконується:

$$\bar{Q}'\left(H, Resp\left(\bar{C}'(H), F_d\right)\right) \leq \bar{Q}'\left(H, Resp\left(C(H)\right), F_d\right)$$

(відповідно

$$\overline{Q'}\left(H, Resp\left(\overline{C'}(H), F_d\right)\right) \le \overline{Q'}\left(H, Resp\left(C(H)\right), F_d\right)$$

Позначимо це $Z'(H) \le_n \overline{Z}(H)$ (відповідно $Z'(H) \le_c \overline{Z}(H)$).

Зауважимо, що МП $\overline{Z}(H)$ не повинна повертати інформації більше, ніж $Z(H)$. Відповідно, вона не повинна і робити для об'єкта b більше, ніж не МП. Таким чином, останнє означення встановлює:

- відношення порядку між МП;
- існування цілої множини МП.

Отже, очевидним є наступне означення.

Означення 13. МП $\overline{Z}(H)$ є допустимою (відносно $Z(H)$), якщо $\overline{Z}(H) \le_n Z(H)$ і $\overline{Z}(H) \le_c Z(H)$.

З попередніх означень виникає можливість формалізувати поняття максимально придатної МП. Проте виявляється, що слід враховувати обмеження: збереження безпеки, допустимість та кінцевість допустимих МП.

Означення 14. МП $\overline{Z}(H)$ є максимально придатною відносно даних (відповідно дій), якщо вона допустима відносно $Z(H)$ і для будь-яких модифікацій $\overline{Z}'(H)$, допустимих відносно $Z(H)$, $\overline{Z}'(H) \le_n \overline{Z}(H)$ (відповідно $\overline{Z}'(H) \le_c \overline{Z}(H)$). Коли $\overline{Z}(H)$ максимально придатна відносно даних і дій одночасно, вважатимемо, що МП $\overline{Z}(H)$ є максимально придатною.

Теорема 3. У рамках наведених означень на множині допустимих МП існує максимально придатна МП.

Доведення. Справедливість твердження виникає за наявності відношення часткового порядку між МП (означення 12), їх допустимості (означення 13), означення максимально придатної МП (означення 14) і кінцевості допустимих МП.

7. Висновки

Отже, запропонований підхід доводить можливість моделювання певних видів діяльності в процесі функціонування ДД. Більше того, виявляється, що для забезпечення належного рівня захищеності КС для ДД є можливість визначення і подальшого вибору цілої множини стратегій поведінки – МП безпеки. Однак залишається дуже важливе питання про формулювання необхідних та достатніх умов реалізації МП безпеки в КС.

Цей підхід також може бути основою для подальшого розвитку моделі ДД, яка дасть змогу будувати систему захисту КС за критерієм її вартості. Такий підхід може базуватися на визначенні функції вартості на множині можливих МП безпеки. Крім того, він може слугувати формальним обгрунтуванням стандарту із захисту інформації.

1. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99.- Київ: ДСТСЗІ СБ України, 1999.- 16 с
2. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2—004-99.- Київ: ДСТСЗІ СБ України, 1999.- 55 с
3. *Грушо А. А., Тимонина Е. Е.* Теоретические основы защиты информации.- М.: Яхтсмен, 1996.- 192 с.
4. *Щербаков А. Ю.* Введение в теорию и практику компьютерной безопасности.- М: Изд. С. В. Молгачева, 2001.- 352 с.
5. *Антонюк А. А., Синицын И. П.* Управление данными регистрации в защищенных системах // Проблемы программирования,— 2001,- № 3—4,— С. 33—37
6. *Subrahmanian V.* S., *Bonatti P., Dix J., Eiter Th., Kraus S., Ozcan F., Ross R.* Heterogeneous Agent Systems.— MIT Press, Cambridge, MA, 2000.- 305 p.

A. O. Antoniuk

MODELING THE DISPATCHER OF ACCESS FOR THE PROTECTED COMPUTER SYSTEMS

The approach to modeling the dispatchers of access for the protected computer systems is considered. Within the framework of the offered formalism some aspects of his functioning — safe processing of inquir are described. The set of possible policies of safe processing of inquiries is defined and studied.