УДК 681.3.06

А.О. Антонюк, В.В. Жора

ВИКОРИСТАННЯ ДОКАЗОВОГО МЕТОДУ ДЛЯ ПРОЕКТУВАННЯ ТА ОЦІНКИ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

Розглядаються питання моделювання захищеної інформаційно-телекомунікаційної системи. Наводяться приклади використання доказового методу для проектування та оцінки рівня захищеності інформаційно-телекомунікаційної системи в залежності від політики безпеки, що застосовується.

Вступ

Практичній роботі з впровадження комплексної системи захисту інформації (КСЗІ) в інформаційно-телекомунікаційній системі (ІТС) або побудови ІТС з інтегрованими засобами захисту передує аналіз поточного стану безпеки інформації шляхом проведення комплексного обстеження ІТС, висунення вимог до рівнів і технологій захисту, що зазвичай знаходять своє відображення у технічному завданні. Одним з найважливіших елементів цієї діяльності є побудова імітаційної моделі ІТС, що включає в себе виділення і класифікацію об'єктів системи, а також моделювання інформаційних потоків між ними.

Ефективним апаратом, що дозволяє спростити і покращити проектування системи захисту інформації, є доказовий метод. Суть його полягає в комбінуванні апарата формальної логіки і об'єктного моделювання для оцінки несуперечливості сформованої моделі ІТС і додаткових умов її функціонування, формалізованих у вигляді тверджень політики безпеки. Схематично алгоритм застосування даного методу можна зобразити у вигляді таких етапів:

- виділення в ІТС об'єктів-користувачів, об'єктів-процесів і пасивних об'єктів [1, 2], їх наступна класифікація і структурування;
- моделювання інформаційних потоків між об'єктами ІТС із зазначенням типу доступу для кожного потоку;
- формулювання умов функціонування ІТС і функціональних послуг захисту за допомогою формалізму, що використовується для моделювання ІТС;
- формулювання у вигляді правил положень політики безпеки;
- доведення тверджень про виконання політики безпеки в даній системі за умов гарантованого виконання функціональних послуг.

1. Загальні положення

Нехай **X** – деякий скінченний алфавіт, X – множина слів скінченної довжини в алфавіті **X**. Вважаємо, що в X певним чином виділено підмножину слів, яку назвемо мовою **L**. Також вважаємо, що будь-яка інформація в ІТС представлена у вигляді слова чи послідовності слів з **L** [3].

Об'єктом в моделі ІТС будемо називати довільну скінченну множину слів мови **L**. Для різних компонентів ІТС об'єкти можуть відрізнятися логічним (зміст, семантика, значення) та фізичним (форма, синтаксис) представленнями. Під об'єктом ІТС будемо розуміти елемент ресурсу ІТС, що характеризується певними атрибутами і поводженням. Для кожного об'єкта визначимо множину слів, що його описують. Під *станом* об'єкта будемо розуміти виділене слово з цієї множини. Множину станів об'єкта буде визначено далі.

Вважаємо, що ІТС являє собою сукупність об'єктів. Функціонально узгоджену групу об'єктів назвемо *компонентом* ІТС. Приймемо також основні положення, на яких базується модель ІТС:

- в захищеній ІТС завжди присутній активний компонент чи декілька компонентів, що виконує функцію контролю за операціями між об'єктами і фактично від-

повідає за реалізацію певної політики безпеки;

- для здійснення операцій з об'єктами в захищеній ІТС необхідна додаткова інформація (і наявність відповідного об'єкта, що її містить) про дозволені та заборонені операції;
- функціонування ІТС і питання ІБ описуються послідовностями доступів одних об'єктів до інших;
- об'єкти в ІТС можуть бути породжені тільки активним компонентом (активним об'єктом) з інших (пасивних) об'єктів;
- властивість деякого компонента ІТС бути активним реалізується у можливості здійснення певних операцій об'єктів, що входять до складу компонента, над іншими.

Визначимо модель ІТС наступним чином. Нехай час є дискретним та приймає значення з множини $\mathbf{N}_0 = \{0,1,2,\ldots\}$. Оскільки зміна станів об'єктів відбувається дискретно, то можна вести мову про відповідність зміни стану системи ряду натуральних чисел (для зручності починаємо відлік з нульового моменту часу). Очевидно, що в сенсі реального часу проміжки між подіями в ІТС можуть бути різної протяжності.

Нехай всю інформацію про ІТС в будь-який момент часу можна представити у вигляді набору станів скінченної множини об'єктів, тобто стан ІТС – це набір станів об'єктів. Під час роботи системи об'єкти як видозмінюються, так створюються і знищуються, тому слід розглядати множину об'єктів в конкретний момент часу t. Позначимо її $\mathbf{M}_t$, $|\mathbf{M}_t| < \infty$ ($t \in \mathbf{N}_0$). Зауважимо також, що в довільний момент часу ця множина не є порожньою.

Структура множини об'єктів визначається таким чином. Нехай **U** – множина об'єктів-користувачів, **P** – множина об'єктів-процесів, **O** – множина пасивних об'єктів. Надалі будемо називати їх відповідно множинами користувачів, процесів та пасивних об'єктів. Зрозуміло, що перелічені множини теж мають сенс в конкретний момент часу. Отже,

$$\mathbf{M}_t = \mathbf{U}_t \cup \mathbf{P}_t \cup \mathbf{O}_t, \quad \forall\, t \in \mathbf{N}_0. \qquad (1)$$

Окремі об'єкти будемо позначати так: $U_i \in \mathbf{U}$, $i=1,\ldots,n_U$; $P_j \in \mathbf{P}$, $j=1,\ldots,n_P$; $O_k \in \mathbf{O}$, $k=1,\ldots,n_O$. Будемо вважати, що декомпозиція ІТС є фіксованою. Іншими словами, існує деякий критерій, що дозволяє в будь-який момент часу безпомилково відносити об'єкт до однієї з трьох наведених множин. Основною ознакою, що класифікує об'єкти в системі, є властивість їх активності. Ця властивість, а також і самі множини об'єктів, описані в [1].

Як було відмічено раніше, активність означає можливість виконання операцій над об'єктами. Серед трьох типів об'єктів активними можуть бути лише користувачі та процеси. Таким чином, поняття *суб'єкта*, що використовується в суб'єктно-об'єктній моделі [3], замінюється поняттями користувача та процесу.

Під *користувачем* розуміємо об'єкт, що містить або має доступ до інформації про фізичну особу, яка, в свою чергу здійснює вплив на ІТС. Об'єкт-користувач активізується у процесі входження фізичного користувача в систему. Інакше кажучи, фізичному користувачеві в ІТС відповідає деякий активний об'єкт, що діє від його імені та володіє його повноваженнями. Фізичний користувач сприймає об'єкти та отримує інформацію через об'єкти, якими керує і/або які відображають інформацію у зручному для нього вигляді. В момент проходження процедур ідентифікації, автентифікації, авторизації та реєстрації об'єкт-користувач активізує компонент, що містить дані про ідентифікатори і повноваження в ІТС фізичного користувача. Таким чином, користувач може існувати лише в активному стані. Він створюється під час активізації цього компонента (в даному випадку ряду процесів), тобто на початку сеансу, а наприкінці сеансу знищується. Крім цього, протягом сеансу користувач може активізовувати інші процеси. В початковий момент часу має існувати принаймні один активний об'єкт (користувач). Для зручності назвемо його *системою*.

Процеси – це об'єкти, які реалізують певні перетворення інформації в КС. Для реалізації цього перетворення необхідно виділити певні ресурси і організува-

ти їх взаємодію, що призводить до перетворення інформації. Це означає, що об'єкт-процес може знаходитися в двох станах: пасивному (у формі опису перетворення інформації) і активному. Як приклад можна навести виконуваний файл, що в пасивному стані являє собою набір символів, а в активному – здійснює перетворення інформації. Зазначимо, що об'єкт-процес в пасивному стані володіє всіма властивостями пасивного об'єкта, але до цієї множини не включається, оскільки на відміну від пасивного об'єкта може бути активізований.

Під *пасивним об'єктом*, або просто об'єктом, в загальному випадку будемо розуміти певні структуровані дані. Об'єкт може знаходитися лише в пасивному стані.

Зауважимо, що загрози інформації ми розглядаємо як такі, що спричиняються дією активного компонента (активних об'єктів). В активному режимі компоненти ІТС можуть створювати об'єкти і/або стани системи, що являють загрозу інформації і/або працездатності системи.

Доступ одного об'єкта до іншого завжди реалізується шляхом обміну інформацією, тобто породженням потоку інформації між об'єктами і/або зміною стану системи. *Потоком інформації* між об'єктами O_i та O_j називається [4] довільна операція над O_j, що реалізується деяким активним об'єктом (користувачем або процесом) і залежить від O_i. Однак, в реалізації потоку безпосередньо приймають участь два об'єкти: активний об'єкт-ініціатор та інший активний об'єкт, або активний об'єкт-ініціатор і пасивний об'єкт (процес). Виходячи з цього, *доступом* одного об'єкта до іншого назвемо породження потоку інформації між ними. В процесі доступу беруть участь теж два об'єкти: один – який звертається за доступом, другий – до якого надається дозвіл на доступ. При породженні потоку інформації процесом останній спочатку отримує дозвіл, наприклад, на читання з одного пасивного об'єкта, а потім отримує дозвіл на запис до другого пасивного об'єкта. Очевидно, з точки зору системного часу, ці події не є одночасними.

Нехай **A** – множина всіх видів доступів, що дозволені в системі, $|\mathbf{A}|<\infty$. Процес доступу виду a об'єкта P_i до об'єкта O_j позначається $P_i \xrightarrow{a} O_j$, $a \in \mathbf{A}$ [3]. Серед різноманітних видів доступу доцільно виділити декілька: читання, яке будемо позначати r; запис – w; активізацію – act.

В роботі [5] запропоновано наступну структуру множини доступів. Множина всіх інформаційних потоків поділяється на декілька підмножин: підмножина, яка пов'язана з доступом для ознайомлення з інформацією; підмножина, що пов'язана з можливістю модифікації інформації; підмножина потоків спостереження за процесами обробки інформації. На основі такого поділу можна визначити аналогічний поділ множини всіх можливих доступів до інформації. Отже,

$$\mathbf{A} = \mathbf{A}_1 \cup \mathbf{A}_2 \cup \mathbf{A}_3, \qquad (2)$$

де $\mathbf{A}_1$ – множина доступів, за якими можливе ознайомлення з інформацією; $\mathbf{A}_2$ – множина доступів, за якими можлива модифікація інформації; $\mathbf{A}_3$ – множина доступів, за якими можливе спостереження за обробкою інформації. До цієї множини ми включаємо також доступ на активізацію.

Визначимо, які саме об'єкти можуть отримувати доступи в ІТС. Як вищезазначено, у доступі беруть участь лише два об'єкти.

- $U_i \xrightarrow{a} P_j, i = 1,...,n_U;\ j = 1,...,n_P,$

$a \in \mathbf{A}$ – доступ користувача до процесу;

- $P_i \xrightarrow{a} P_j, i = 1,...,n_P;\ j = 1,...,n_P,$

$a \in \mathbf{A}$ – доступ процесу до процесу;

- $P_i \xrightarrow{a} O_j, i = 1,...,n_P;\ j = 1,...,n_O,$

$a \in \mathbf{A}$ – доступ процесу до об'єкта.

Зауважимо, що протягом певного інтервалу часу $[t,\ t+n]$, $n \geq k$ може бути реалізована ціла послідовність доступів, наприклад:

$$U_i \xrightarrow{act} P_j \xrightarrow{act} P_{j+1} \xrightarrow{act} \dots$$
$$\dots \xrightarrow{act} P_{j+k} \xrightarrow{r} O_m,$$

або скорочено $U_i \xrightarrow{r} *O_m$, де зірочка вказує на те, що мав місце ланцюжок доступів. Згідно з наведеними міркуваннями, до типових доступів також можна віднести такі ланцюжки:

- $U_i \xrightarrow{a} *P_j, i = 1,...,n_U;\ j = 1,...,n_P,\ a \in \mathbf{A}$;
- $U_i \xrightarrow{a} *O_j, i = 1,...,n_U;\ j = 1,...,n_O,\ a \in \mathbf{A}$;
- $P_i \xrightarrow{a} *P_j, i = 1,...,n_P;\ j = 1,...,n_P,\ a \in \mathbf{A}$;
- $P_i \xrightarrow{a} *O_j, i = 1,...,n_P;\ j = 1,...,n_O,\ a \in \mathbf{A}$.

Якщо об'єкт-процес P_i вже активізований в деякий момент часу t, то зрозуміло, що в один з попередніх моментів часу t-k (t, $k \in \mathbf{N}_0$, $t \geq k$) мав існувати об'єкт (користувач або процес), що його активізував. Припустимо, що цей об'єкт єдиний. На практиці, єдиність активізуючого об'єкта забезпечується унікальністю його ідентифікатора. Будемо вважати, що в момент $t = 0$ активізований виділений користувач U_0, якому умовно дамо назву *система*.

З вищенаведених міркувань випливає твердження.

Твердження 1. Якщо в даний момент t активізовано об'єкт-процес P_i, то існує єдиний користувач U_j, від імені якого він активізований, тобто існує ланцюжок

$$U_j \xrightarrow{act} P_{i-k} \xrightarrow{act} P_{i-k+1} \xrightarrow{act} \dots$$
$$\dots \xrightarrow{act} P_{i-1} \xrightarrow{act} P_i,\quad i \geq k.$$

Згідно з припущенням, існує чи існував єдиний об'єкт P_{i-1}, що активізував P_i. Якщо $U_j = P_{i-1}$, то твердження доведено. Якщо $U_j \neq P_{i-1}$, $i=1,\dots,n_P$, то існує чи існував єдиний об'єкт P_{i-2}, що активізував P_{i-1} і т.д. За індукцією прийдемо до того, що процес P_{i-k} був активізований або певним користувачем, або "системою". Єдиність активізуючого користувача забезпечується дискретністю системного часу. Припустимо, що процес P_{i-k} був активізований одночасно двома користувачами U_1 та U_2. Це означає, що обидва ці користувачі в один і той же момент часу здійснили доступ до процесу P_{i-k}, що неможливо, оскільки дискретизація часу обумовлюється зміною станів об'єктів системи.

З твердження випливає, що для кожного $t \in \mathbf{N}_0$ в ІТС для кожного користувача U_i існує і визначена множина $D_t(U_i)$ – об'єкти, до яких користувач U_i може отримати доступ в момент $t+k$, $k \in \mathbf{N}_0$. Позначимо її таким чином:

$$D_t(U_i) = \left\{P_j \middle| U_i \xrightarrow{a} *P_j\right\} \cup$$
$$\cup \left\{O_k \middle| U_i \xrightarrow{a} *O_k\right\},$$

$a \in \mathbf{A}$, $i=1,\dots,n_U$; $j=1,\dots,n_P$; $k=1,\dots,n_O$. $D_t(U_i)$ назвемо множиною об'єктів, асоційованих з U_i, $\mathbf{X}_t = \bigcap_i D_t(U_i)$ – множиною ресурсів спільного доступу, а множину $\mathbf{X}^*_t = \bigcup_i D_t(U_i)$ – загальними ресурсами ІТС.

Нехай процедура породження об'єкта є такою, що створений об'єкт отримує ім'я, що дозволяє унікальним чином ідентифікувати його в системі. З множини $\mathbf{X}^*_t$ загальних ресурсів системи виділимо множину об'єктів, які породив користувач U_i і позначимо її $W_t(U_i)$.

2. Застосування в умовах дискреційної політики безпеки

Особливість дискреційної політики полягає в тому, що керування доступом користувачів до інших об'єктів здійснюється на підставі атрибутів асоційованості (приналежності). Для більш точного визначення дискреційної політики зробимо припущення про єдиність породжуючого користувача: нехай для кожного $O_j \in \mathbf{X}^*_t$, такого, що $O_j \notin \mathbf{X}_t$, для кожного $t \in \mathbf{N}_0$, існує єдиний користувач U_i такий, що $O_j \in W_t(U_i)$. Вважаємо, що $W_t(U_i) \cap \mathbf{X}_t = \varnothing$, тобто якщо користувач створює об'єкт у множині ресурсів спільного доступу, то ідентифікатор, що свідчить про породження цього об'єкта певним користувачем, відсутній.

Припустимо, що в ІТС присутній деякий активний компонент, що в кожний момент часу однозначно визначає множину $D_t(U)$ для кожного користувача, – диспетчер доступу (ДД) [1, 2]. Фактично цей компонент відповідає за реалізацію деякої політики безпеки [1, 3]. Детально власти-

вості диспетчера доступу описані в [6, 7]. Вважаємо головною властивістю ДД таку: він має контролювати всі потоки, тобто обхідні шляхи політики безпеки мають бути відсутніми (неможливість доступу до об'єктів без участі ДД). В даному випадку ДД надає доступ до об'єктів згідно наступної політики безпеки.

Політика безпеки 1. Нехай мав місце ланцюжок доступів $U \xrightarrow{act} *P$. Доступ $P \xrightarrow{a} O$, $a \in \mathbf{A}$ в деякий момент часу $t \in \mathbf{N}_0$ може відбутися лише за умов $O \in W_t(U)$ або $O \in \mathbf{X}_t$.

Визначимо канали реалізації загроз [6, 8]:

$$\exists t \in \mathbf{N}_0,\ \exists a \in \mathbf{A},\ \exists U_i \in \mathbf{U}_t,\ \exists O \in \mathbf{O}_t,\ U_i \xrightarrow{a} *O,$$

$$O \in W_t(U_j),\ i \neq j;\ i, j = 1,\ldots,n_U. \qquad (3)$$

Вважаємо також, що жодний доступ до об'єктів з множини $\mathbf{X}_t$ не створює канал реалізації загрози. Зауважимо, що в даному випадку йдеться про загрози конфіденційності та цілісності, визначення яких наведено в [6].

Теорема 1. Якщо всі доступи здійснюються у відповідності до політики безпеки, то канали реалізації загроз є перекритими.

Припустимо, що має місце канал реалізації загрози (3). Це означає, що в t-й момент часу відбувається несанкціонований доступ (НСД) $a \in \mathbf{A}$ деякого процесу P до об'єкта O: $P \xrightarrow{a} O$. Тоді, можливі три варіанти:

1. $P \in \mathbf{X}_t$;

це фактично означає, що $P \in D_t(U_k)$, $\forall k$. Доступ (3) вказує на те, що $U_i \xrightarrow{act} *P$. Тоді, згідно з політикою безпеки, або $O \in \mathbf{X}_t$, а це не створює каналу реалізації загрози, або $O \in W_t(U_i)$, тобто доходимо до протиріччя в силу припущення про єдиність породжуючого користувача та твердження 1.

2. $P \in D_t(U_j)$, $j = 1,\ldots,n_U$; $P \notin \mathbf{X}_t$;

тоді, $P \in \left\{P \middle| U_j \xrightarrow{a} *P\right\}$. Умова активності процесу означає, що $U_i \xrightarrow{act} *P$. Тобто, $P \in \left\{P \middle| U_i \xrightarrow{a} *P\right\}$. Оскільки $P \notin \mathbf{X}_t$ та в силу твердження 1 про єдиність активізуючого користувача отримуємо, що $U_i = U_j$, тобто $i=j$.

3. $P \in D_t(U_i)$, $i \neq j$; $i, j = 1,\ldots,n_U$; $P \notin \mathbf{X}_t$;

в силу твердження 1 про єдиність активізуючого користувача, $U_i \xrightarrow{act} *P$. У відповідності до політики безпеки, $O \in W_t(U_i)$. Проте, згідно припущення, існує єдиний користувач U_j такий, що $O \in W_t(U_j)$. Отримані протиріччя доводять теорему.

Розглянемо стандартні функціональні *послуги* захисту, що можуть надаватися в ІТС, згідно [9]. Серед наявних і визначених у [6] послуг захисту доцільно навести властиві для ІТС класу 1 (за класифікацією [10]).

1. Довірча конфіденційність:

$$U_2 \xrightarrow{a} *O,\ a \in \mathbf{A}_1 \Leftrightarrow$$
$$\Leftrightarrow \begin{cases} O \in D_t(U_2), \\ O \in W_{t-k}(U_1),\ (U_1 \xrightarrow{a} *O,\ a \in \mathbf{A}_2) \Rightarrow \\ \Rightarrow O \in D_t(U_2),\ t, k \in \mathbf{N}_0. \end{cases} \qquad (4)$$

2. Повторне використання об'єктів:

$!\exists O \in \mathbf{O}$: якщо $U_i \xrightarrow{a} *O$ в момент $t \in \mathbf{N}_0$, $a \in \mathbf{A}$, то $U_j \xrightarrow{a} *O$ в момент $t+k$, $i \neq j$, якщо $O(t) = O(t+k)$ та за умови $O \notin \mathbf{X}_t$.

3. Довірча цілісність:

$$U_2 \xrightarrow{a} *O,\ a \in \mathbf{A}_2 \Leftrightarrow$$
$$\Leftrightarrow \begin{cases} O \in D_t(U_2), \\ O \in W_{t-k}(U_1),\ (U_1 \xrightarrow{a} *O,\ a \in \mathbf{A}_2) \Rightarrow \\ \Rightarrow O \in D_t(U_2),\ t, k \in \mathbf{N}_0. \end{cases} \qquad (5)$$

4. Реєстрація.
5. Ідентифікація та автентифікація.
6. Достовірний канал.
7. Цілісність комплексу засобів захисту.

Проаналізувавши наведені послуги, помітимо, що 1 – 3 виконуються за умови виконання політики безпеки. Решта послуг є внутрішніми властивостями системи ДД і покликані забезпечити виконання політики безпеки.

Теорема 2. Якщо в системі справедливе твердження 1, виконується припущення про єдиність породжуючого корис-

тувача, присутній ДД, що характеризується головною властивістю, та діють послуги 4–7, то виконується дискреційна політика.

Потрібно довести, що за умови реалізації ланцюжка доступів $U \xrightarrow{act} *P$ доступ $P \xrightarrow{a} O$, $a \in \mathbf{A}$ в деякий момент часу $t \in \mathbf{N}_0$ може відбутися лише за умов $O \in W_t(U)$ або $O \in \mathbf{X}_t$. Згідно твердження 1, якщо відбувся доступ $U \xrightarrow{act} *P$, то користувач U єдиний. Також, якщо об'єкт $O \notin \mathbf{X}_t$, то існує єдиний користувач U^*, що $O \in W_t(U^*) \subset D_t(U^*)$. Якщо ж $O \in \mathbf{X}_t$, то за визначенням множини $\mathbf{X}_t$, $O \in D_t(U)$, $\forall U$. Якщо в ІТС реалізовані послуги 4 – 7, тобто реєстрація, ідентифікація/автентифікація, достовірний канал та цілісність комплексу засобів захисту, то ДД однозначно може визначити приналежність об'єкта до тієї чи іншої множини. Якщо $U=U^*$, то природно $O \in D_t(U)$. Якщо $U \neq U^*$, то ДД перевірить атрибути доступу, що містяться в списку доступу. Тоді, якщо $O \notin W_t(U)$ та $O \notin \mathbf{X}_t$, то доступ надано не буде, а якщо $O \in D_t(U)$ та $O \in \mathbf{X}_t$, то $P \xrightarrow{a} O$.

3. Застосування в умовах мандатної політики безпеки

Зміст мандатної політики безпеки полягає в тому, що контроль доступу до об'єкта здійснюється окремо від користувача-породжувача об'єкта. Керуюча компонента визначає, до якої інформації і кому може бути наданий доступ. Користувач, що породив об'єкт, не може змінити права доступу. Ця властивість, зокрема, є характерною для систем обробки інформації з обмеженим доступом, де присутнє поняття грифу секретності, що знаходить відображення у введенні шкали цінності об'єктів. У такій системі користувач не може визначати ні гриф секретності об'єкта, ні змінювати його.

Введемо в ІТС поняття категорії доступу, що в [2] визначено як комбінацію ієрархічних і неієрархічних атрибутів доступу, що відображає рівень критичності інформації або повноважень користувача щодо доступу до такої інформації. Категорію доступу активного об'єкта будемо називати *рівнем допуску* і позначати $C(U)$ або $C(P)$. Категорію доступу пасивного об'єкта будемо називати *класом цінності* і позначати $C(O)$ або $C(P)$. На множині категорій доступу також визначено частковий порядок "≥". Припустимо, що рівні допуску та класи цінності присвоюються об'єктам під час створення за однаковою шкалою та можуть змінюватися протягом життєвого циклу системи.

Канали реалізації загроз конфіденційності визначимо наступним чином:

$$\exists t \in \mathbf{N}_0,\ \exists a \in \mathbf{A_1},\ \exists U \in \mathbf{U}_t,\ \exists O \in \mathbf{O}_t,$$
$$U \xrightarrow{a} *O,\ C(O) > C(U). \qquad (6)$$

Користуючись вищенаведеними визначеннями, сформулюємо мандатну політику безпеки.

Політика безпеки 2. Нехай мав місце ланцюжок доступів $U \xrightarrow{act} *P$. Доступ $P \xrightarrow{a} O$, $a \in \mathbf{A}$ у деякий момент часу $t \in \mathbf{N}_0$ може відбутися лише за умови $C(P) \geq C(O)$.

Очевидно, що така політика є дуже загальною, оскільки в цьому випадку не враховано структуру множини доступів. Існує декілька типових моделей мандатної політики, які здатні ефективно протистояти певній множині загроз.

Політика безпеки 3 (Bell, La Padula [11,12]). Нехай мав місце ланцюжок доступів $U \xrightarrow{act} *P$.

- Доступ $P \xrightarrow{a} O$, $a \in \mathbf{A}_1$ в деякий момент часу $t \in \mathbf{N}_0$ може відбутися лише за умови $C(P) \geq C(O)$ (проста властивість безпеки).
- Якщо в деякий момент часу $t_1 \in \mathbf{N}_0$ відбувся доступ $P \xrightarrow{a} O_1$, $a \in \mathbf{A}_1$, то доступ $P \xrightarrow{a} O_2$, $a \in \mathbf{A}_2$ в деякий момент часу $t_2 \in \mathbf{N}_0$ може відбутися лише за умови $C(O_2) \geq C(O_1)$, $O_1, O_2 \in \mathbf{O}$ (*-властивість).

Проста властивість безпеки означає, що для здійснення доступу на читання рівень допуску ініціатора потоку має бути не нижчим за клас цінності об'єкта доступу. *-властивість забороняє переміщення інформації з об'єкта з вищим класом цінності до об'єкта з більш низьким класом цінності.

Зробимо також припущення про те, що доступ на активізацію належить множині доступів $\mathbf{A}_1$.

Таким чином, політика безпеки 3 перешкоджає загрозам конфіденційності, оскільки користувач може читати інформацію класу цінності, що відповідає його рівню допуску або нижче за нього. Крім того, користувач не може записувати критичну інформацію в об'єкти з більш низьким класом цінності, що дозволяло б ознайомлюватись з нею користувачам, які не мають на це відповідних повноважень. Проте, дана політика не здатна перешкодити загрозам цілісності інформації, оскільки користувач, рівень допуску якого не дозволяє ознайомлюватись з інформацією, може вільно її модифікувати. Протистояти загрозам цілісності може наступна політика, для якої поняття категорії доступу C замінюється на категорію цілісності I.

Політика безпеки 4 (Biba [13]). Нехай мав місце ланцюжок доступів $U \xrightarrow{act} *P$.

- Доступ $P \xrightarrow{a} O$, $a \in \mathbf{A}_2$ в деякий момент часу $t \in \mathbf{N}_0$ може відбутися лише за умови $I(P) \geq I(O)$ (проста властивість цілісності).
- Якщо в деякий момент часу $t_1 \in \mathbf{N}_0$ відбувся доступ $P \xrightarrow{a} O_1$, $a \in \mathbf{A}_2$, то доступ $P \xrightarrow{a} O_2$, $a \in \mathbf{A}_1$ в деякий момент часу $t_2 \in \mathbf{N}_0$ може відбутися лише за умови $I(O_2) \geq I(O_1)$, $O_1, O_2 \in \mathbf{O}$ (*-властивість цілісності).

Теорема 3. Якщо всі доступи здійснюються у відповідності до політики безпеки 3, то канали реалізації загроз конфіденційності є перекритими.

Припустимо, що має місце канал реалізації загрози (6). Це означає, що в t-й момент часу відбувається НСД $a \in \mathbf{A_1}$ деякого процесу P до об'єкта O: $P \xrightarrow{a} O$. Тоді, можливо два варіанти:

1) $C(P) \geq C(O)$. Водночас, процес P в момент часу $t–k$ (t, $k \in \mathbf{N}_0$, $t \geq k$) був активізований процесом P_k. Згідно з політикою безпеки 3 $C(P_k) \geq C(P)$. Користуючись твердженням 1, за індукцією прийдемо до ланцюжка доступів, з якого $C(U) \geq C(P_m) \geq C(P_l) \geq \geq \ldots \geq C(P_k) \geq C(O)$. За нашим припущенням про існування каналу реалізації загрози $C(O) > C(U)$. З транзитивності часткового порядку "≥" отримуємо протиріччя.

2) $C(P) < C(O)$, але в такому разі згідно з політикою безпеки 3 доступ не може бути наданий.

Також можна сформулювати наступну теорему, доведення якої аналогічне попередньому.

Теорема 4. Якщо всі доступи здійснюються у відповідності до політики безпеки 4, то канали реалізації загроз цілісності є перекритими.

В термінах мандатної політики множини асоційованих об'єктів мають вигляд

$$D_t(U_i) = \{P_j | C(U_i) \geq C(P_j)\} \cup \cup \{O_k | C(U_i) \geq C(O_k)\},$$

$$i=1,\ldots,n_U;\ j=1,\ldots,n_P;\ k=1,\ldots,n_{O?} \qquad (7)$$

$$D_t^*(U_i) = \{P_j | I(U_i) \geq I(P_j)\} \cup \cup \{O_k | I(U_i) \geq I(O_k)\},$$

$$i=1,\ldots,n_U;\ j=1,\ldots,n_P;\ k=1,\ldots,n_O. \qquad (8)$$

В ІТС класу 1 з мандатною політикою безпеки замість послуг 1, 3 запровадимо наступну послугу:

8. Адміністративна конфіденційність і цілісність:

$$\exists U \in \mathbf{U},\ \forall P, O \in D_t^*(U), \forall t. \qquad (9)$$

Фактично дана послуга вимагає наявність адміністратора, який має ексклюзивні повноваження щодо зміни категорій доступу та цілісності для об'єктів, що проявляється у потребі введення ще однієї послуги.

9. Розподіл обов'язків.

Самі об'єкти під час створення набувають тієї ж самої категорії доступу або цілісності, що є у породжуючого користувача/процесу. Але, на відміну від дискреційної політики, в даному випадку породжуючий користувач не може змінювати права доступу до об'єкта.

4. Застосування в умовах рольової політики безпеки

Основним поняттям рольової політики є *роль* – сукупність функцій щодо керування ІТС, комплексу засобів захисту та обробки інформації, доступних користува-

чеві. Також можна визначити її як багатозначне відношення між множинами користувачів і повноважень, що регламентується набором функціональних обов'язків фізичних користувачів [14]. Множину всіх ролей позначимо **R**.

$$\mathbf{T} = \mathbf{P} \times \mathbf{O} \times \mathbf{A} \ . \qquad (10)$$

Як часову характеристику ІТС можна розглядати поняття сеансу, що фактично відповідає часу роботи користувача в системі. Кожний сеанс $S \in \mathbf{S}$ – це відображення користувача на набір ролей, що йому присвоєні.

Відношення призначення користувачів позначимо $\mathbf{UA} \subseteq \mathbf{U} \times \mathbf{R}$. Вибірка з цієї множини для фіксованої ролі виводить список користувачів, яким присвоєна дана роль, тобто тих користувачів, які можуть виконувати функціональні обов'язки згідно даної ролі в ІТС:

$$assigned\_users(R) = \\ = \{U \in \mathbf{U}_t \mid (U,R) \in \mathbf{UA}_t\}, \ R \in \mathbf{R}_t \ . \qquad (11)$$

Відношення призначення повноважень $\mathbf{TA} \subseteq \mathbf{R} \times \mathbf{T}$ дає змогу визначити набір всіх повноважень ролі в контексті її роботи в системі як вибірку з цієї множини для фіксованої ролі:

$$assigned\_privileges(R) = \\ = \{T \in \mathbf{T}_t \mid (T,R) \in \mathbf{TA}_t\}, \ R \in \mathbf{R}_t \ . \qquad (12)$$

Цілком природним буде вимагати, щоб в залежності від сеансу роботи в системі користувач міг мати різні повноваження. Це необхідно в тому разі, коли одна і та ж людина виконує функціональні обов'язки відповідно до різних посад. Під час одного сеансу цьому користувачеві може бути присвоєна одна роль, а протягом наступного – зовсім інша. Взагалі, на початку сеансу користувач може активізувати певну підмножину ролей:

$$session\_roles(S) \subseteq \\ \subseteq \{R \in \mathbf{R}_t \mid (U(S),R) \in \mathbf{UA}_t\}, \ S \in \mathbf{S}_t \ , \qquad (13)$$

де $U(S)$ – користувач, що ініціював даний сеанс. Він є єдиним, тому кожний сеанс асоційований з одним користувачем, водночас як кожний користувач асоційований з одним або більше сеансами.

Суть рольової політики полягає в тому, що не користувач або процес асоційований з об'єктами, як це спостерігалось в дискреційній та мандатній політиках, а роль асоційована з набором повноважень. Отже, користувач може отримати певний доступ до об'єкта тільки якщо набуде ролі, якій призначено відповідні повноваження.

Політика безпеки 5. Нехай мав місце ланцюжок доступів $U \xrightarrow{act} *P$. Доступ $P \xrightarrow{a} O$, $a \in \mathbf{A}$, $O \in \mathbf{O}$ в деякий момент часу $t \in \mathbf{N}_0$ може відбутися лише за умови:

$$((U,R) \in \mathbf{UA}_t) \wedge ((R,T) \in \mathbf{TA}_t) \wedge \\ \wedge (T = T(P,O,a)) \wedge \\ \wedge (R \in session\_roles(S)) = \text{True}, \\ R \in \mathbf{R}_t, \ S \in \mathbf{S}_t \ .$$

Таким чином, канал реалізації загрози визначимо наступним чином:

$$\exists t \in \mathbf{N}_0, \exists a \in \mathbf{A}, \exists U \in \mathbf{U}_t, \\ \exists O \in \mathbf{O}_t, \exists R \in \mathbf{R}_t, \exists S \in \mathbf{S}_t, \ U \xrightarrow{a} *O, \qquad (14)$$

$$((U,R) \in \mathbf{UA}_t) \wedge ((R,T) \in \mathbf{TA}_t) \wedge \\ \wedge (T = T(P \in D_t(U),O,a)) \wedge \quad . \\ \wedge (R \in session\_roles(S)) = \text{False}.$$

Теорема 5. Якщо всі доступи здійснюються у відповідності до політики безпеки 5, то канали реалізації загроз конфіденційності й цілісності є перекритими.

Зауважимо, що для реалізації довірчого і адміністративного керування доступом в системі з рольовою політикою безпеки мають бути запроваджені послуги 1 – 9.

Висновки

На даному етапі отримані результати використання доказового методу для аналізу захищеності ІТС класу 1. Дослідження можливості поширення результатів на ІТС класів 2 і 3, зокрема, в частині застосування рольової політики, тривають з урахуванням вимог нормативних документів у сфері захисту інформації.

Використання доказового методу при побудові захищених ІТС дозволяє мінімізувати кількість і значимість можливих помилок у проектуванні за рахунок глибокого аналізу захищеності системи на прикладі формальної моделі ІТС на ранніх етапах її створення. Даний метод також

може бути застосований для перевірки адекватності вже побудованої системи захисту інформації. Визначення об'єктів та інформаційних потоків на першому та другому етапах алгоритму, поданому у вступі, дозволяє на третьому етапі сформувати функціональні послуги захисту застосовно до конкретної системи. Формулювання політик безпеки (четвертий етап) залежить від умов функціонування системи, що розглядається. На п'ятому етапі перевірка справедливості відповідних теорем (за зразком теорем 1, 3, 4, 5) дозволяє з'ясувати рівень теоретичної захищеності ІТС. Остання не означає абсолютної захищеності, оскільки навряд чи можливо гарантувати абсолютно правильну реалізацію функціональних послуг та адекватне їх застосування.

Доказовий метод є універсальним інструментарієм для оцінки рівня захищеності ІТС. Схожі методи застосовувались Беллом та Ла Падулою [11], іншими авторами, проте вони в переважній більшості є проблемно-орієнтованими та спрямованими на перевірку можливості реалізації конкретних загроз інформації.

1. *Загальні* положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99. – К.: ДСТСЗІ СБ України, 1999. – 16 с.
2. *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.
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., Жора В.В.* Моделювання доступу та каналів витоку в інформаційних системах // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – № 3. – С. 156–160.
6. *Антонюк А.А., Жора В.В., Мостовой В.Н.* Угрозы информации и услуги безопасности // Проблемы программирования. – 2003. – № 4. – С. 65–71.
7. *Антонюк А.О.* Про деякі важливі поняття захисту інформації в автоматизованих системах // Наукові записки НаУКМА. – 2002. – № 2. – 8 с.
8. *Антонюк А.А., Жора В.В.* Загрози інформації і канали витоку // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – № 1. – С. 42–46.
9. *Критерії* оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5–004–99. – К.: ДСТСЗІ СБ України, 1999. – 55 с.
10. *Класифікація* автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5–005–99. – К.: ДСТСЗІ СБ України, 1999. – 23 с.
11. *Bell D.E., La Padula L.J.* Secure Computer Systems: Mathematical foundations and model // Report ESD-TR-73-278, Mitre Corp., Bedford, MA, March 1976.
12. *McLean J.* A Comment on the 'Basic Security Theorem' of Bell and La Padula // Information Processing Letters. – Elsevier, 1985. – Vol. 20. – P. 67–70.
13. *Biba K.J.* Integrity Considerations for Secure Computer Systems // ESD-TR-76-372, NTlS# AD-A039324, Electronic Systems Division, Air Force Systems Command, April 1977.
14. *Жора В.В.* Підхід до моделювання рольової політики безпеки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2003. – № 7. – С. 45–49.

Отримано 06.04.2007

Про авторів:

Антонюк Анатолій Олександрович,
кандидат фізико-математичних наук,
доцент,

Жора Віктор Володимирович,
молодший науковий співробітник.

Місце роботи авторів:

Академія державної податкової
служби України,
м. Ірпінь, вул. Карла Маркса, 31,

Інститут програмних систем
НАН України, 03680, Київ 187,
проспект Академіка Глушкова, 40.
E-mail: victor.zhora@gmail.com