УДК 004.056

В. А. Лахно
ЛНАУ, м. Луганськ, valss21@ukr.net

МЕТОДИ РОЗПІЗНАВАННЯ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ ОБРОБКИ ДАНИХ КРИТИЧНОГО ЗАСТОСУВАННЯ

У статті запропоновано новий підхід у методології розпізнавання загроз для інформаційної безпеки (ІБ) інформаційних систем. Розроблено проблемно-орієнтований теоретико-графовий апарат еталонної моделі захищеної автоматизованої системи (ЕМЗАС – мереж), що дозволяє моделювати невразливі технології обробки і передачі інформації з гнучкими захисними механізмами, забезпечуючи формалізацію та дослідження політики безпеки (ПБ) ЕМЗАС.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗИ, РОЗПІЗНАВАННЯ, АВТОМАТИЗОВАНІ ІНФОРМАЦІЙНІ СИСТЕМИ

Вступ

Сучасний підхід до забезпечення захисту інформаційних процесів (ІП) від несанкціонованого доступу (НСД) підтримується на міжнародному рівні стандартом ISO/IEC 15408. На вітчизняному рівні — групою нормативних документів та державних стандартів України (ДСТУ) стосовно створення і функціонування КСЗІ: 1) НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі; 2) Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96; 3) НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі (АС); 4) НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу; 5) НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

Відповідно до цього підходу надійний ІП успішно протидіє існуючим загрозам інформації при заданих зовнішніх умовах його функціонування. Це призводить до постійного вдосконалення як способів і засобів захисту інформації (ЗЗІ), так і способів і засобів реалізації загроз інформаційної безпеки (ІБ), в результаті чого поява нових ЗЗІ призводить до появи нових засобів нападу.

Це, у свою чергу, призводить до необхідності нового трактування поняття «надійність ІП», під якою слід розуміти відсутність у ньому уражень, внаслідок яких можлива реалізація різних загроз ненавмисного і навмисного характеру. Це дозволяє усунути ряд суперечностей у визначенні протистояння ЗЗІ і нападу. При цьому надійність ІП повинна характеризуватися його відповідністю деяким еталонним моделям безпечної (неураженої) циркуляції (обробки і передачі) інформації. У зв'язку з цим існує практична проблема, яка полягає в тому, що подібний стан речей лише частково реалізується на практиці і не знаходить прямого відображення у відповідних стандартах на уніфіковані архітектурні рішення АС, наприклад на транспорті [2, 5, 6], які задовольняють загальноприйнятим еталонним моделям [1, 4].

Причина лежить в принципових теоретичних труднощах моделювання технологій забезпечення надійності та захисту ІП в АС обробки даних критичного застосування (АСОД КЗ), що виникають при спробі з'єднати перспективний підхід до забезпечення надійності та захисту ІП від НСД з гнучкістю захисних механізмів. Слід зауважити, що АСОД КЗ з'явилися в результаті впровадження обчислювальної техніки в сфері критичних об'єктів (військові об'єкти, екологічно небезпечні виробництва, атомні станції, об'єкти транспорту, зв'язку, фінансово – кредитної сфери і т. ін.), що характеризуються неприйнятністю для суспільства збитків від порушення їх працездатності [1, 3, 4, 6].

Будь-яка модель політики безпеки (ПБ) для забезпечення високонадійної обробки інформації (ВНОІ) обов'язково підтримує глобальну ПБ, що характеризує бажані властивості ІП (синтаксис доступу), і може підтримувати локальну ПБ, що характеризує правила переходу ІП між сусідніми станами (семантика доступу). Наявність підтримки локальної ПБ означає динамічність відповідної моделі, а відсутність — статичність. Динамічна модель ПБ, на відміну від статичної, накладає обмеження на стан ІП.

Якщо множину можливих станів АСОД КЗ вдається подати як кінцеву множину, то модель ПБ відноситься до класу моделей кінцевих станів. Теоретичним підґрунтям принципової безпеки таких моделей ПБ служить так звана основна теорема безпеки, яка формулюється і доводиться окремо для кожної моделі [2]. Дискреційна модель, що встановлює повноваження доступу користувачів, у загальному випадку виступаючих у певних ролях, до об'єктів, взагалі не користуючись переходами між станами ІП, найбільш досконалим засобом підтримує глобальну ПБ. Водночас, не відносячись

до моделей кінцевих станів, вона принципово небезпечна. У цьому зв'язку розробка моделей комплексів ПБ є актуальною, так як ці моделі є моделями кінцевих станів по суті і дискреційними за формою. Формалізм таких моделей повинен інтегрувати на теоретико-графовій основі в дискреційний формалізм, що має статичний характер і зручний для опису процесів обробки інформації формалізм мережі, що має динамічний характер. У результаті він повинен конкретно описувати динамічний і статичний доступ до інформації, яка структурується з метою забезпечення єдності розгляду глобальної та локальної ПБ.

У плані конфіденційності та доступності інформації гнучкість захисних механізмів означає гнучкість розмежування доступу, а ураження криються в моделі використовуваної ПБ і в її практичній реалізації. Єдиною справді гнучкою є дискреційна модель ПБ, яка неминуче породжує уразливості. З іншого боку, єдиним принципово безпечним є клас моделей кінцевих станів, що бере свій початок від мандатного методу контролю доступу. Проте можливості застосування існуючих моделей кінцевих станів дуже обмежені через їх принципову негнучкість [1, 4, 5]. Цей недолік даного класу моделей можна усунути, поєднавши даний клас моделей з дискреційною моделлю. Але цьому заважає загальноприйнятий незалежний розгляд процесів захисту інформації від процесів її обробки, а відхід від цього принципу вимагає нових досліджень, результати яких подані в даній роботі.

У плані цілісності інформації гнучкість захисних механізмів зводиться до обмеженості негативного впливу сервісу контролю цілісності (КЦ) на ефективність обробки інформації внаслідок відволікання обчислювальних ресурсів, перш за все, тимчасових, а забезпечення невразливості досягається ступінчастим КЦ при породженні одних суб'єктів іншими в ході реалізації будь-яких процесів обробки інформації. Моделювання потрібних критеріїв якості функціонування сервісу КЦ, як об'єкта управління, повинне ґрунтуватися на формалізмі кінцевих ланцюгів Маркова, що має дискретний характер.

1. Попередні дослідження

У роботах [1-4] проаналізовано шляхи вдосконалення ВНОІ та підвищення захищеності ІП у АСОД КЗ. Залежно від того, в якій інформаційній системі протікають розглянуті ІП, сучасний підхід до забезпечення їх надійності та безпеки задоволений більшою чи меншою мірою. Яскравий приклад слабкої задоволеності дають АСОД КЗ на транспорті [2, 5, 6], і на цій підставі далі будемо розглядати ІП саме в них.

Аналіз сформованого підходу до побудови ЗЗІ від НСД в АСОД КЗ показав, що традиційне використання автономних ЗЗІ НСД із прагненням до їхньої універсалізації відповідно до концепції навісного замка суперечить перспективному підходу до забезпечення надійності та безпеки ІП. Сучасний підхід за принципом задоволення ЗЗІ НСД профілям захисту і завданням з безпеки, що відображає можливості протидії відомим загрозам, не дозволяє усунути ряд суперечностей у визначенні протистояння ЗЗІ і засобів нападу.

Аналіз існуючих методів організації управління процесами захисту ІП від НСД в АСОД КЗ показав актуальність завдання організаційно – технологічного управління сервісом КЦ [1,3]. Вона являє собою завдання оптимального управління сервісом КЦ за рахунок автоматизації його запуску за критеріями якості функціонування, що забезпечує найкращий КЦ при збереженні ефективного функціонування АСОД КЗ. Однак така автоматизація залишається проблемою навіть для використовуваних у сучасних АСОД типових ЗЗІ НСД. Аналіз стандартизованого способу оцінки якості та ефективності комплексів сервісів безпеки (КСБ) як програмних засобів (ПЗ) стосовно специфіки організації управління сервісом КЦ в АСОД КЗ показав неадекватність передбачених характеристик властивостям сервісу КЦ як об'єкта управління. Тому запропоновано ввести нові характеристики і подхарактеристики — критерії якості функціонування сервісу КЦ як об'єкта управління.

На основі проведеного в роботах аналізу [2, 3, 5, 6] визначено мету та завдання дослідження. Відповідно до запропонованого системного підходу основним результатом формування методологічних засад забезпечення надійності та безпеки ІП у АСОД КЗ є еталонна модель захищеної автоматизованої системи (ЕМЗАС) як ідеалізована модель АСОД КЗ, що реалізує принципово безпечну технологію циркуляції інформації. Така модель забезпечує можливість стандартизації уніфікованого архітектурного вигляду різних класів АСОД КЗ шляхом розробки та реєстрації по регламентації стандартів у галузі ІБ. Регламентовані еталонні моделі захищеної автоматизованої системи (ЕМЗАС моделі) комплексів ПБ, з'єднуючи сутність моделей кінцевих станів з дискреційної формою, передбачають, що будь-який дискреційний доступ може реалізовуватися тільки однозначно обумовленою послідовністю переходів між кінцевими станами, для якої можна гарантувати її безпеку.

2. Постановка задачі

Метою дослідження є розробка теоретичних основ моделювання процесів ВНОІ, що забезпечують як недопущення її уразливостей від впливу загроз ненавмисного і навмисного характеру, так і гнучкість захисних механізмів за рахунок інтеграції математичних моделей обробки, розпізнавання загроз ІБ та захисту інформації.

3. Результати дослідження

У ході виконаних досліджень, а також результатів робіт [2, 6], запропонована концептуальна модель організаційно-технологічного управління сервісом КЦ в АСОД КЗ на транспорті, що дозволяє забезпечити розумний компроміс між задоволенням вимог до АСОД КЗ по захисту ІП від НСД і за її цільовим призначенням. Прагнення скоротити тимчасові витрати на проведення перевірок цілісності, з одного боку, і забезпечити своєчасне виявлення порушення цілісності з іншого, викликає необхідність оптимізації стратегії запусків сервісу КЦ на основі, яка задовольняє сформульованому переліку вимог комплексної оцінки якості його функціонування в АСОД КЗ.

Теоретичною базою реалізації монітора звернень до еталонної АСОД служить відома концепція ізольованого програмного середовища (ІПС). Вона є подальшим розвитком класичної загальновизнаної концепції ядра безпеки, заснованої на суб'єктно – об'єктній моделі АСОД, в напрямку обліку породжень суб'єктів.

Якщо концепція ядра безпеки спрямована на вирішення завдання реалізації довільно заданої ПБ, то концепція ІПС спрямована додатково на вирішення завдання гарантування довільно заданої ПБ. Концепція еталонної АСОД у розумінні ЕМЗАС розвиває концепцію ІПС в напрямку регламентації комплексу ПБ ЕМЗАС. Призначенням концепції еталонної АСОД є реалізація заданої локальної ПБ ЕМЗАС, яка гарантує задану глобальну ПБ ЕМЗАС, що забезпечує єдність розгляду динамічного і статичного доступу до інформації. Засобом реалізації даної концепції є організація в АСОД ІПС, що відповідає спеціальному переліку вимог до її суб'єктного наповнення

Побудована концепція організації суб'єктного наповнення еталонної об'єктно-реляційної СУБД із деталізацією даних вимог, що дозволяє використовувати об'єктно-реляційні технології в еталонних АСОД.

Основними засобами реалізації концепції еталонної АСОД є рівневі КСБ. Еталонна АСОД являє собою подобу слоїстого пирога, де ІП, організовані в сусідні функціональні рівні ієрархічної структуризації ресурсів ЕМЗАС, поділяються відповідними рівневими КСБ, які є контролюючими посередниками при взаємодії ІП, що відносяться до сусідніх рівнів ЕМЗАС. Створення нормативної бази реалізації концепції еталонної АСОД вимагає такого підходу до стандартизації уніфікованого архітектурного вигляду різних класів еталонних АСОД, який передбачає стандартизацію їх рівневих інтерфейсів у формі стандартизації інтерфейсів сполучення ІП даного рівня ЕМЗАС із сусідніми з ними за рівнем ЕМЗАС рівневими КСБ. При такому підході до стандартизації АСОД КЗ може будуватися з окремих програмних блоків, гарантовано «щільно припасованих» один до одного без утворення уразливостей для ІБ. Їх можна комплектувати в поступово розширювану бібліотеку ЕМЗАС – класів на зразок базової бібліотеки класів технології *dot net.*

Введемо наступні позначення для нашої моделі: L – число рівнів ЕМЗАС-мережі (L=13 [1, 4]), $k=\overline{1,L}$, $l=\overline{1,L}$, $k\neq l$; S – множина позицій, $S=Q\cup V\neq$ Ш, $Q\cap V=$ Ш, $|S|<\infty, |Q|=|V|$;

Q, V – множини простих і дозвільних позицій,

$$|Q|<\infty, |V|<\infty, Q=\bigcup_{l=1}^{L}Q_l\neq \text{Ш},\quad Q_k\cap Q_l=\text{Ш},$$

$$V=\bigcup_{l=1}^{L}V_l\neq \text{Ш},\ V_k\cap V_l=\text{Ш};$$

Q_l, V_l – множини простих і дозвільних позицій l-го рівня, $|Q_l|=|V_l|\neq 0$;

U – множина модулів,

$$U=\bigcup_{l=1}^{L}U_l\neq \text{Ш},\ |U|<\infty,\ U_k\cap U_l=\text{Ш};$$

U_l – множина модулів l-го рівня;

$I(u)=i_1.i_2.....i_{L-l}$ – індекс модуля $u\in U_l$ та блоку, у якого цей модуль верхній (№ 0 у блоці), зокрема, $I(u)=0$ при $l=L$;

$K[I]$ – число нижніх модулів у блоці з індексом I;

$I.j$ – індекс нижнього модуля з номером $j=\overline{1,K[I]}$ у блоці з індексом I;

якщо I, J – індекси модулів, то

$$(J\subset I)\Leftrightarrow(I\supset J)\Leftrightarrow(I=J.i_1.i_2....i_k),$$

$$(J\subseteq I)\Leftrightarrow(I\supseteq J)\Leftrightarrow((J\subset I)\vee(I=J)).$$

Для завдання структури ЕМЗАС-*мережі* вводяться такі позначення: N – число номерів авторизації, $\lambda=\overline{1,N}$ – номер авторизації; $r=r[I,\lambda]$ – булева ознака допустимості авторизації λ у модулі з індексом I; $M_{in}=M_{in}[I,\lambda]$, $M_{out}=M_{out}[I,\lambda]$ – вхідна й вихідна функції розмітки, що визначають маркування вхідних і вихідних позицій модулів у формі булевої змінної (показують, чи містить позиція фішку, причому кожна позиція може містити не більше однієї фішки).

Формальне подання модуля ЕМЗАС- *мережі* заданої структури має вигляд

$$u=\langle I, q=q[I,\lambda], v=v[I,\lambda]\rangle\in U_l, \qquad (1)$$

де $I=I(u)$ – індекс модуля; $q=q[I,\lambda]\in Q_l$, $v=v[I,\lambda]\in V_l$.

А формальне подання структури ЕМЗАС-*мережі* наступне:

$$\varepsilon=\left\langle\begin{matrix}N, K=K[I], r=r[I,\lambda], M_{in}=\\ =M_{in}[I,\lambda], M_{out}=M_{out}[I,\lambda]\end{matrix}\right\rangle. \qquad (2)$$

Введення апарату ЕМЗАС – мереж відкриває шлях для систематичного дослідження їх

математичних властивостей як інструменту розробки АСОД КЗ на основі ЕМЗАС. Головним кроком на цьому шляху є побудова з використанням апарату ЕМЗАС-мереж методу моделювання комплексу ПБ еталонної АСОД у вигляді ПБ на ЕМЗАС-*мережі*.

Глобальна (*g*) ПБ і дискреційна *l*-го рівня подаються множиною дозволених ними позицій: $\Psi_g \subseteq V_I$; $\Psi_{dl} \subseteq V_l$, а рівнева локальна (*l*) має вигляд

$$\Psi_{ll} = \left\{ \left\langle I(u), \lambda, r[I(u), \lambda] \right\rangle \middle| u \in U_l, \lambda = \overline{1, N} \right\}. \quad (3)$$

Блокова ПБ (*b*) подається установкою ознак допустимості всіх авторизацій у модулях даного блоку, погодженої за наступними правилами ($\lambda = \overline{1, N}$, $I = I(u)$, $u \in U \setminus U_1$):

$$(\exists_j \in \overline{1, K[I]})(r[I.j, \lambda] = 1) \Rightarrow (r[I, \lambda] = 1); \quad (4)$$

$$(r[I, \lambda] = 0) \Rightarrow (\forall_j \in \overline{1, K[I]})(r[I.j, \lambda] = 0). \quad (5)$$

Локальна ПБ подається у такий спосіб:

$$\Psi_l = \bigcup_{l=1}^{L} \Psi_{ll} = \left\{ \left\langle I(u), \lambda, r[I(u), \lambda] \right\rangle \middle| u \in U, \lambda = \overline{1, N} \right\}, \quad (6)$$

де всі $r[I(u), \lambda]$ взаємно погоджені за всіма блоками відповідно до правил ($\lambda = \overline{1, N}$, $I - I(u)$):

$$(r[I, \lambda] = 1) \Rightarrow (\forall J \subset I)(r[J, \lambda] = 1), \quad u \in U \setminus U_L; \quad (7)$$

$$(r[I, \lambda] = 0) \Rightarrow (\forall J \supset I)(r[J, \lambda] = 0), \quad u \in U \setminus U_1. \quad (8)$$

Дискреційна ПБ подається своїм можливим $\Psi_{\text{др}}$ або глобалізованим Ψ_{dg} поданням:

$$(v[I, \lambda] \in \Psi_{\text{дг}}) \Leftrightarrow ((v[I, \lambda] \in \Psi_{\text{др}}) \wedge \wedge (\forall J \supset I)(v[J, \lambda] \notin \Psi_{\text{др}}));$$

$$\Psi_{\text{др}} = \bigcup_{l=1}^{L} \Psi_{dl} \subseteq V, \ \Psi_{dg} \subseteq \Psi_{\text{др}}, \ \lambda = \overline{1, N}, \ I = I(u), \ u \in U, \quad (9)$$

причому множини Ψ_{dl} погоджено за правилами ($\lambda = \overline{1, N}$):

$$(v[I, \lambda] \in \Psi_{\text{др}}) \Rightarrow (\forall J \subset I)(v[J, \lambda] \in \Psi_{\text{др}}), \quad I = I(u), \ u \in U \setminus U_L; \quad (10)$$

$$(v[I, \lambda] \notin \Psi_{\text{др}}) \Rightarrow (\forall J \supset I)(v[J, \lambda] \notin \Psi_{\text{др}}), \quad I = I(u), \ u \in U \setminus U_1. \quad (11)$$

Індукування дискреційної політики безпеки глобальною означає, що $\Psi_g = \Psi_{\text{дг}}$, а локальної — політикою безпеки дискреційною –

$$(\forall v = v[I, \lambda] \in V)((v \in \Psi_{\text{др}}) \Leftrightarrow (r[I, \lambda] = 1)). \quad (12)$$

У ході досліджень були розроблені математичні моделі синтезу політики безпечної взаємодії ІП в еталонній АСОД, що дають можливість розглядати ПБ окремих ІП (на різних структурних компонентах ЕМЗАС-*мережі*) з можливістю їх подальшого поєднання (пошаровий синтез ПБ на ЕМЗАС-*мережі*).

У ході досліджень виконано моделювання організаційно-технологічного управління сервісом КЦ у випадку захисту ІП типової ЗЗІ НСД і у випадку еталонної АСОД. В обох випадках для підтримки прийняття адміністратором захисту інформації відповідних рішень пропонується використовувати нову підсистему — підсистему автоматизованого управління сервісом КЦ інформації.

Обґрунтований комплекс критеріїв якості функціонування сервісу КЦ як об'єкта управління:

1) динамічні — «*адекватність функціонування*» E_{af}, «тимчасова агресивність функціонування» E_{ta};

2) статичні (булеві) — «*функціональність*» E_f, «*ресурсна агресивність функціонування*» E_{ra}, «*функціональна агресивність функціонування*» E_{fa}, «*зручність використання*» E_{yu}.

Розроблено математичні моделі оцінки критеріїв якості функціонування сервісу КЦ. Допустиме значення статичних критеріїв означає, що контролюються на цілісність тільки ті ІП і тоді, що і коли передбачається експлуатаційною документацією на АСОД.

Для оцінки динамічних критеріїв запропоновано напівмарківські моделі, що формуються для звичайної АСОД на базі вихідної Е-*мережі*, а для еталонної АСОД — вихідної ЕМЗАС-*мережі*. Ці напівмарківські моделі дають можливість враховувати вірогідний характер переходів між різними станами і довільність законів розподілу часу переходів у припущенні незалежності ймовірності і часу переходу від попередніх переходів. У випадку захисту ІП типової ЗЗІ НСД моделі для оцінки двох динамічних критеріїв подаються відповідно двома кінцевими напівмарківськими процесами (КНП) з різними початковими і кінцевими станами. Згідно з еталонною АСОД два динамічних критерія виражаються через один допоміжний *критерій динамічної ефективності E,* модель для оцінки якого представляється своїм КНП. Кожен КНП записується своєю напівмарківською матрицею $H(\tau) = \left\| H_{ij}(\tau) \right\|$, $i = \overline{1, n}$, $j = \overline{1, n}$, сформованою на базі вихідної мережі . Її елемент є $H_{ij}(\tau) = p_{ij} G_{ij}(\tau)$, де p_{ij}, $G_{ij}(\tau)$ – імовірність і функція розподілу ймовірностей часу переходу КНП, що знаходиться у стані ***i***, безпосередньо у стан ***j***.

Кожен із критеріїв E_{af}, E_{ta} (у випадку захисту ІП типовий СЗІ), E (у випадку еталонної АСОД) є можливість своєчасного досягнення відповідним КНП поглинаючого стану. Таким чином, динамічні критерії формалізовані як імовірносно-тимчасові характеристики (ІТХ) функціонування сервісу КЦ інформації, яка обробляється в АСОД. Вихідною основою для дослідження такого роду

ІТХ та часів життя КНП використовується у загальному випадку система рівнянь динаміки КНП, що має в оригіналах і зображеннях вигляд:

$$Q_i(\tau) = H_{in}(\tau) + \sum_{j=1, j\neq i}^{n-1} \int_0^{\tau} H_{ij}(t) \cdot Q_j(\tau - t)dt, i = \overline{1,n-1}\ ; \quad (13)$$

$$\begin{aligned} (I - \overline{H}(v))q(v) &= h(v), \\ (I - \overline{H}(0))\alpha &= h(0), \end{aligned} \quad (14)$$

де I – одинична матриця; $\overline{H}(v) = \left\| h_{ij}(v) \right\|$, $i = \overline{1,n-1}$, $j = \overline{1,n-1}$; $h(v) = (h_{in}(v))$, $q(v) = (q_i(v))$, $\alpha = q(0) = (\alpha_i)$, $i = \overline{1,n-1}$; $h_{ij}(v)$, $i = \overline{1,n-1}$, $j = \overline{1,n}$ – перетворення Лапласа-Стилтьеса функції $H_{ij}(\tau)$; α_i, $Q_i(\tau)$ – вірогідність поглинання КНП у стані $\boldsymbol{i}$ за будь-який час та менше τ, $q_i(v)$ – перетворення Лапласа-Стилтьеса функції $Q_i(\tau)$.

Залежності (13) і (14) виходять при застосуванні формалізму напівмарківських матриць, інтегруючих матричний формалізм кінцевих ланцюгів Маркова та операторний формалізм випадкових процесів при єдиному розгляді безперервного часу і дискретних станів.

Результати застосування моделей неуразливих технологій циркуляції інформації до типової бази даних, керованої еталонної об'єктно-реляційною СУБД, свідчать про широкі можливості цих моделей для забезпечення доступності та конфіденційності інформації, що обробляється в перспективних АСОД КЗ.

Для посилення ступеня захисту інформаційних ресурсів керівникам підприємств запропоновано [2, 6] використовувати безперервне коригування профілів активних користувачів, зокрема, так званий ітераційний алгоритм (ІА). Сенс ітераційного алгоритму полягає в неявному зворотному зв'язку сервера з користувачем, що реалізується через облік статистики запитів. Отримана оцінка поточного профілю користувача використовується для поділу користувачів на групи за ступенем небезпеки для ресурсів ІС: а) користувач, б) потенційно небезпечний користувач; в) небезпечний користувач; г) порушник. Для синтезу процедури автоматичної класифікації застосований апарат дискретних процедур розпізнавання загроз і пошуку уразливостей, детально описаний у роботах [2, 6].

Ступінь небезпеки кожної загрози залежить від значень ряду факторів, що підвищують або знижують захищеність об'єкту інформаційної безпеки (ОІБ) від даної загрози. Фактори, що знижують захищеність ОІБ, будемо називати факторами ризику, а ті, що підвищують її – факторами захищеності. Інтегральна оцінка уразливості й захищеності ОІБ є функцією його захищеності від кожного виду загроз. Інформація, яка є основою побудови дискретних процедур розпізнавання та протидії загрозам (ДПРПЗ) ІБ, може бути подана в різних формах, наприклад, у вигляді важко з'ясовних ознак НСД $\{p_{ax1},...,p_{axn}\}$ у комп'ютерних системах, діапазонів граничних значень, параметрів вхідного вихідного трафіка, непередбачуваних адрес пакетів, атрибутів, часових параметрів, запитів і т.д.

Позначимо через MI загальне число загроз інформації; PA – число можливих цілей порушника в захищуваній АІСТП; B_{p_a} — множину номерів загроз інформації, реалізованих порушником при досягненні p_a-ї мети.

Досліджується деяка множина об'єктів, у нашому випадку це PA – число можливих цілей порушника. Об'єкти цієї множини описуються системою ознак $\{p_{ax1},...,p_{axn}\}$. Відомо, що множина PA представлена у вигляді об'єднання непересічних підмножин (класів) загроз інформації – $(KL_1,...,KL_l) = (B_{p_{a1}},...,B_{p_{al}})$. Існує остаточний набір об'єктів $\{sp_{a1},...,sp_{am}\}$ з PA, про які відомо, до яких класів вони належать (це прецеденти, тобто об'єкти, використовувані для навчання – ОВН). Потрібно за пред'явленим набором значень ознак, тобто описом деякого об'єкта sp_{an} з PA, про який невідомо, до якого класу він належить, визначити цей клас і, відповідно, вибудувати роботу ЗЗІ таким чином, щоб вона могла ефективно протидіяти загрозі в межах даного класу.

При вирішенні завдань розпізнавання загроз ІБ з використанням представницьких наборів довелося відмовитися від вимоги безвихідності представницького набору, тому що перевірка безвихідності значно знижує швидкість роботи алгоритму. Використовувалися представницькі набори обмеженої довжини. Максимальна довжина набору бралася рівною 3. При меншій максимальній довжині більша частина об'єктів не містила жодного представницького набору. А збільшення максимальної довжини до 4 різко збільшувало час роботи алгоритму. Був отриманий такий результат, див. рис. 1 ($-1 \le IZ_{p_{axj}} \le 1$ де інформативність значення ознаки інформаційної атаки).

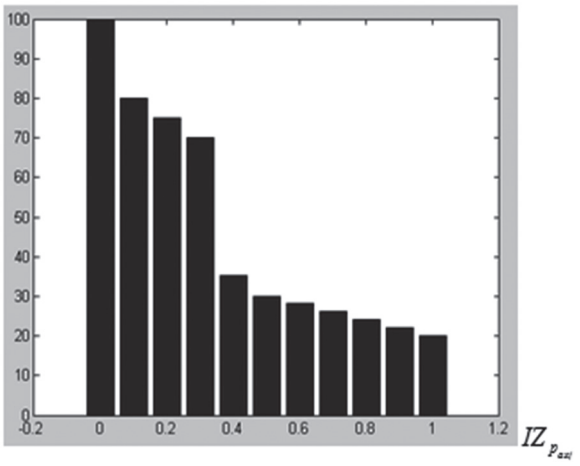

Рис. 1. Розподіл інформативності ознак для завдання комп'ютерної DoS (DDoS) – атаки

Таким чином, побудова множини елементарних класифікаторів для модельованого класу загроз інформації зводиться до такого: 1) задається характеристична функція; 2) будується ДНФ, що реалізує цю функцію. Найбільшу складність становить побудова ДНФ із максимальних кон'юнкцій (скороченої ДНФ) характеристичної функції; 3) обчислюється припустима (максимальна) кон'юнкція $\Re$, що визначає приналежність об'єкта до певного класу загроз.

Використання нечітких змінних в запропонованій моделі суттєво підвищує гнучкість програми класифікації й дозволяє реалізувати функціональність, необхідну для оперування такими сутностями, як інформаційні атаки. Кожному значенню ознаки об'єкта ставиться у відповідність нечітка змінна, здатна відобразити ступінь упевненості експерта (програми) у значенні якої-небудь ознаки.

Висновки

Розроблено проблемно-орієнтований теоретико-графовий апарат ЕМЗАС-*мереж*, що дозволяє моделювати невразливі технології обробки і передачі інформації з гнучкими захисними механізмами, забезпечуючи формалізацію та дослідження ПБ ЕМЗАС. Він використовує деталізацію не тільки процесів передачі, але й обробки даних в межах запропонованої ієрархічної структуризації ресурсів ЕМЗАС для уніфікованого моделювання динамічного і статичного доступу до інформації на основі інтеграції *E*-мережевого і дискреційного формалізмів.

Розроблено метод моделювання на ЕМЗАС-*мережах* регламентованої ЕМЗАС ПБ для забезпечення ВНОІ, що дозволяє з'єднати гнучкість дискреційної моделі з безпекою моделей кінцевих станів ПБ.

Список літератури: 1. *Герасименко В.А.* Защита информации в автоматизированных системах обработки данных / В.А. Герасименко В 2-х кн. – М.: Энергоатомиздат, 1994. Т1. – С. 132-138. **2.** *Лахно В.А.* Обеспечение защищенности автоматизированных информационных систем транспортных предприятий при интенсификации перевозок: Монография / В.А. Лахно, А.С Петров. – Луганск: изд-во ВНУ им. В.Даля, 2010. – 280 с. **3.** *Томашевський О.В.* Визначення надійності технічних засобів захисту інформації / О.В. Томашевський // Інформаційні технології та захист інформації: Зб. наук. праць. 1999. №1. – С. 97-103. **4.** *Багаев М. А.* Методические основы проектирования программных систем защиты информации: монография / М. А. Багаев, А. С. Дубровин, Е. А. Рогозин, В. И. Сумин [и др.]. – Воронеж: Воронеж. ин-т радиоэлектроники, 2006. – 178 с. **5.** *Волынская А.В.* Повышение стойкости информационных систем при организации производства на транспорте: автореф. дис. на соис. уч. степ. канд. техн. наук: 05.22.01 «Транспортные и транспортно-технологические системы страны, ее регионов и городов, организация производства на транспорте» / А.В. Волынская. – Екатеринбург, 2004. – 20 с. **6.** *V. Lahno.* Ensuring security of automated information systems, transportation companies with the intensification of traffic /V. Lahno, A. Petrov.: Monograph. Lugansk. 2011.-190 p.

Надійшла до редколегії 14.06.2013

УДК 004.056

Методы распознавания угроз для информационной безопасности в системах обработки данных критического применения В.А. Лахно // Бионика интеллекта: науч.-техн. журнал. – 2013. – № 2 (81). – С. 81-86.

В статье предложен новый подход в методологии распознавания угроз для информационной безопасности (ИБ) информационных систем. Разработан проблемно-ориентированный теоретико-графовый аппарат эталонной модели защищенной автоматизированной системы (ЭМЗАС – *сетей*), которая позволяет моделировать неуязвимые технологии обработки и передачи информации с гибкими защитными механизмами, обеспечивая формализацию и исследование политики безопасности ЭМЗАС.

Ил. 1. Библиогр.: 6 назв.

UDK 004,056

Methods for detection of threats to information security in the data processing systems of critical application V.A. Lahno // Bionics of Intelligense: Sci. Mag. – 2013. – № 2 (81). – P. 81-86.

This paper proposes a new approach to the methodology for the identification of threats of information security (IS) information systems. Developed a task-oriented graph-theoretic apparatus of the reference model of the protected automation system (RMPAS – *networks*), which allows you to simulate invulnerable processing and transmission of information with flexible protective mechanisms, providing a formalization of research and security policy RMPAS.

Fig. 1. Ref.: 6 items.