ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 1 (1), 2021

МОДЕЛЬ СИСТЕМИ ПРОТИДІЇ ВТОРГНЕННЯМ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

С. Толюпа[1], І. Пархоменко[2], С. Штаненко[3]
[1, 2] Київський національний університет імені Тараса Шевченка,
вул. Володимирська, 60, Київ, 01033, Україна
[3] Військовий інститут телекомунікацій та інформатизації імені Героїв Крут,
вул. Московська, 45/1, Київ, 01011, Україна

Відповідальний за рукопис: С. Толюпа (e-mail: tolupa@i.ua).

(Подано 26 червня 2021)

У статті запропоновано модель системи виявлення вторгнень (СВВ), яка відображає основні процеси, які відбуваються у системі, з метою оптимізації процесів протидії вторгненням. Такі процеси в загальному вигляді можна розглядати як процеси розподілу і використання ресурсів, виділених на захист інформації. Використання методів моделювання із забезпеченням належного рівня захищеності інформації привело до розроблення множини формальних моделей безпеки, що сприяє підтриманню належного рівня захищеності систем на основі об'єктивних і незаперечних постулатів математичної теорії. Запропонована модель протидії порушенням захищеності інформації в ІС, на відміну від подібних відомих сьогодні моделей, які призначені для оцінювання впливів можливих атак і загроз різних рівнів та прийняття обґрунтованого рішення щодо реалізації систем виявлення вторгнення ІС, надає можливість оперативно оцінювати поточний стан захищеності ІС за умов забезпечення працездатності формальних методів за короткими обмеженими вибірками щодо параметрів засобів захисту ІС та параметрів загроз, що впливають на елементи ІС. Застосування запропонованої моделі дасть змогу отримувати поточні оцінки стану захищеності інформації, надати додатковий час на підготовку та здійснення заходів реагування на загрози з метою підвищення безпеки інформації.

Ключові слова: *система виявлення вторгнень; кібератака; інформаційна система; загроза; порушник; модель.*

1. Вступ

Основним засобом захисту інформаційних систем та мереж (ІС) від інформаційно-руйнівних впливів (втручань) у вигляді кібернетичних вторгнень (КВ) є системи виявлення та/або запобігання вторгненням (СВВ/СЗВ/СВА), основне завдання яких зводиться до оперативної їх ідентифікації (встановлення відповідності між об'єктом і його ідентифікатором (унікальним атрибутом) та в ідеальному випадку ініціювання ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів, сервісів. Практика застосування СВВ сформувала два напрями протидії КВ: виявлення зловживань (Misuse detection) та виявлення аномалій (Anomaly detection). Перший підхід орієнтований на виявлення лише класифікованих (відомих) вторгнень на основі підходів синтаксичного порівняння відповідності структурних (сигнатур/патернів), інваріантних та кореляційних ознак виконуваного процесу (системи) з наявною

базою відомих шаблонів. Головними недоліками такого підходу є неможливість виявлення нових модифікацій КВ чи кібернетичних атак нульового дня (0-day) та неможливість автоматичного введення нових шаблонів, що свідчить про їх достатньо низьку ефективність. Другий підхід, навпаки, зводиться до завдання виявлення невідомих КВ на основі знаходження набору ознак, який не відповідає очікуваній поведінці об'єкта (користувача/системи), – шаблони характеристик, які не задовольняють визначене поняття нормальної поведінки, фіксуються як аномалії.

Всі розробники систем виявлення атак і організації, які використовують СВА, повинні розуміти й вивчати їх класифікацію, щоб вибрати кращі рішення для систем захисту інформації. Досліджуючи різні аспекти таксономії й застосовуючи різні варіанти, ми зможемо досягти вищого рівня безпеки інформаційних систем [1–2].

Узагальнений вигляд класифікації систем виявлення загроз наведено на рис. 1.

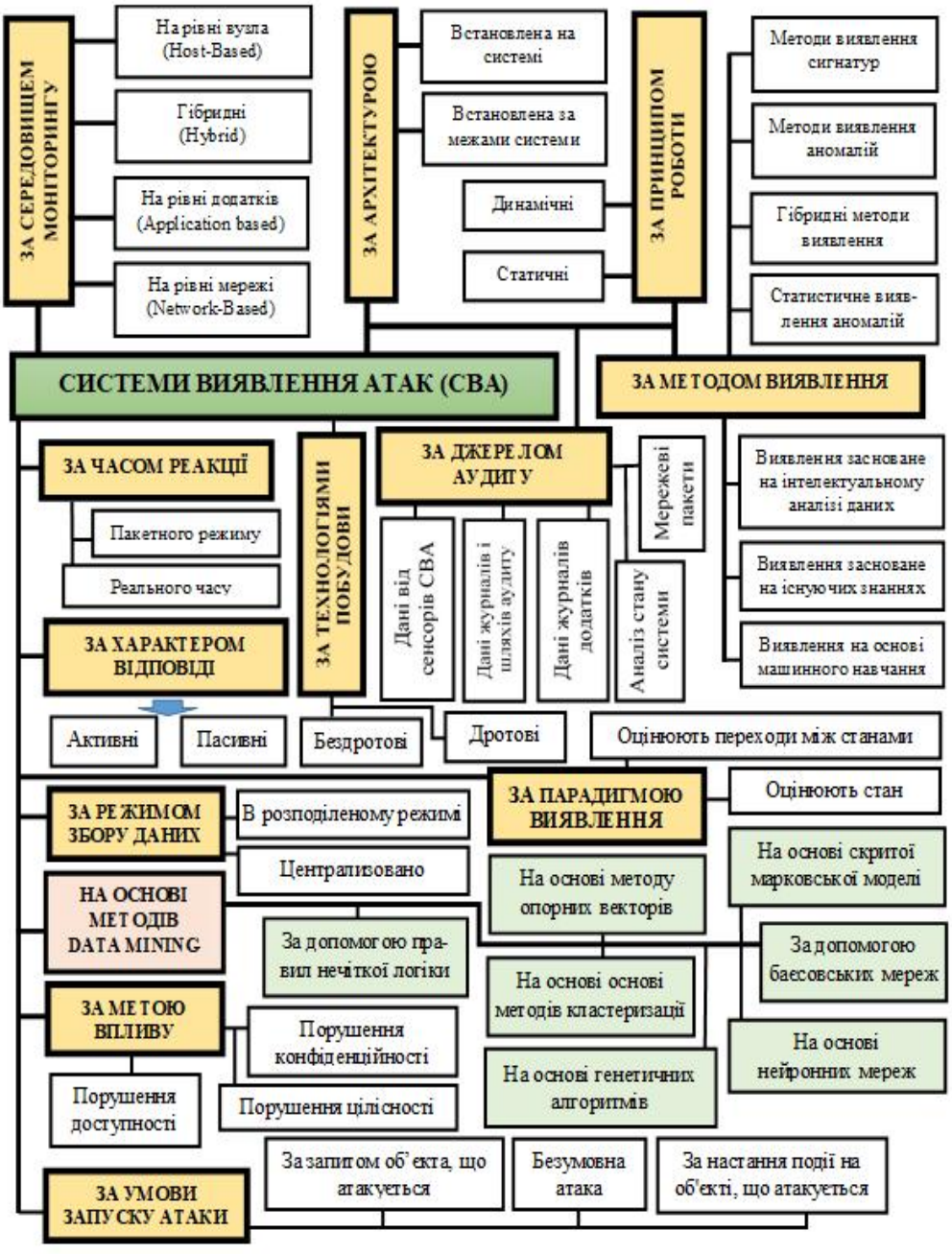

Рис. 1. Узагальнений вигляд класифікації систем виявлення вторгнень та атак

Взагалі кажучи, сучасні системи виявлення вторгнень і атак ще далекі від ергономічних і ефективних із погляду безпеки рішень. Підвищення ефективності необхідне не тільки для виявлення зловмисних дій на інфраструктуру захищених об'єктів інформатизації, але і погляду повсякденної експлуатації цих засобів, а також економії обчислювальних та інформаційних ресурсів власника системи захисту.

Якщо говорити безпосередньо про модулі обробки даних, то кожна сигнатура атаки в системі обробки інформації про атаку є базовим елементом для розпізнавання загальніших дій – розпізнавання фази атаки (етапу її реалізації). Саме поняття сигнатури узагальнюється до деякого вирішального правила. А кожну атаку, навпаки, розділяють на набір етапів її проведення. Чим простіша атака, тим легше її виявити і з'являється більше можливостей для її аналізу.

Сьогодні системи виявлення вторгнень і атак зазвичай являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень у чужі мережі останніми роками істотно збільшилася, системи виявлення атак (СВА) стали необхідним компонентом інфраструктури безпеки більшості організацій.

Сьогодні вирішення питань забезпечення безпеки в ІС та управління станом їх захищеності описано в роботах вітчизняних та закордонних дослідників, а саме: В. Л. Бурячка, С. О. Гнатюка, О. Г. Корченко, О. О. Кузнецова, І. Ю. Субача, С. П. Євсеєва, В. Б. Дудикевича, С. В. Казмирчук, T. Ptaceka, G. Elmasry, P. Albers, O. Camp та інших.

Зазначимо, що одним із актуальних напрямів, який активно розвивається у сфері інформаційної безпеки, є виявлення кібератак і запобігання вторгненням у ІС з боку неавторизованої сторони (НАС). Також слід наголосити, що атаки на ІС з кожним роком стають все досконалішими, глобальнішими та частішими.

Отже, розвиток та впровадження новітніх інформаційних технологій забезпечують безпрецедентні умови для накопичення і використання інформації, а також визначають фундаментальну залежність від їх нормального функціонування усіх сфер життєдіяльності суспільства та держави: економіки, політики, сфери національної та міжнародної безпеки тощо. Така залежність стає вразливим місцем у функціонуванні систем і об'єктів критичних національних інфраструктур і дає можливість негативно налаштованим елементам і угрупованням скористатися нею для реалізації протиправних дій у кібернетичному просторі, порушивши цілісність, доступність й конфіденційність інформації та заподіявши шкоду інформаційним ресурсам та інформаційним системам. Особливе занепокоєння викликає можливість застосування інформаційних технологій у кібернетичному просторі в інтересах здійснення військово-політичного та силового протиборства, тероризму та проведення хакерських атак. Експерти передбачають, що в прийдешньому році повністю зміниться структура кібероперацій і те, як їх здійснюють. Вони стануть непомітнішими для систем виявлення і фаєрволу. Аналіз робіт, що ведуться у цій сфері, показує, що зазначена проблема потребує подальшого вивчення – як побудови адекватних математичних моделей предметної області, так і реалізації ефективних алгоритмів виявлення атак і прийняття рішень, що підтверджує актуальність досліджень у цій предметній області [3].

Науковці розглядають у своїх роботах наслідковий підхід до реалізації засобів протидії зовнішньому дестабілізувальному впливу для забезпечення властивості функціональної стійкості складних технічних систем. Але із розвитком об'єктів захисту, зі зміною способів їх функціонування такий підхід до реалізації властивості функціональної стійкості щодо, наприклад, кібернетичних загроз видається доволі архаїчним [4].

Крім того, актуальною проблемою нині є розроблення комплексу аналітичних моделей і методів моніторингу процесу функціонування розподілених інформаційних систем та взаємодії агентів під час оцінювання її стану.

2. Модель систем виявлення вторгнень

Модель систем виявлення вторгнень (СВВ) повинна відображати основні процеси, які відбуваються у системі, з метою оптимізації процесів захисту інформації. Такі процеси в загальному вигляді можна подати як процеси розподілу і використання ресурсів, які виділено на захист інформації. Сьогодні існує велика кількість засобів та способів забезпечення захисту інформації, що обробляється в ІС [5–9]. Удосконалення СВВ потребує побудови моделі протидії порушенням захищеності інформації в ІС, враховуючи системний вплив на ІС різних за характером, місцем застосування та фізичною природою загроз.

Використання методів моделювання із забезпеченням належного рівня захищеності інформації привело до розроблення множини формальних моделей безпеки [10], що сприяє підтриманню належного рівня захищеності систем на основі об'єктивних і незаперечних постулатів математичної теорії.

Метою моделювання у системі забезпечення безпеки ІС є побудова моделі, яка враховувала б найбільшу кількість чинників впливу і давала б змогу розраховувати ймовірність виникнення вразливості та реалізації загрози, обчислювати час реалізації загрози і можливі збитки, визначати ефективність упровадження засобів захисту та стан захищеності системи [11–12].

Основою побудови моделі є опис об'єктів у вигляді сукупності елементів, пов'язаних між собою певними відносинами. Моделі опису атак [13]:

- етапна модель – розглядає атаку як послідовність декількох ізольованих етапів, не надає можливості оцінити успішність кожного етапу;
- дерева атаки – забезпечує високий ступінь деталізації та можливість введення оцінок за деякими критеріями, але не може бути використана для моделювання атак, оскільки не надає засобів динамічного моделювання, введення у модель умов зовнішнього впливу та не забезпечує вибору наступного етапу на підставі результатів попереднього;
- графова модель – призначена для оцінювання складності порушення безпеки ІС, враховує поточні значення параметрів ІС та передбачає аналіз умов, необхідних для реалізації атаки [12–13].

Захищеність ІС характеризує ступінь адекватності механізмів захисту інформації, які реалізовані в ІС, ризиків, що існують у середовищі, та загрози безпеці. Взаємодію загроз, ресурсів ІС та СВВ описує узагальнена типова модель процесу захисту із повним перекриттям загроз [14], яку наведено на рис. 2.

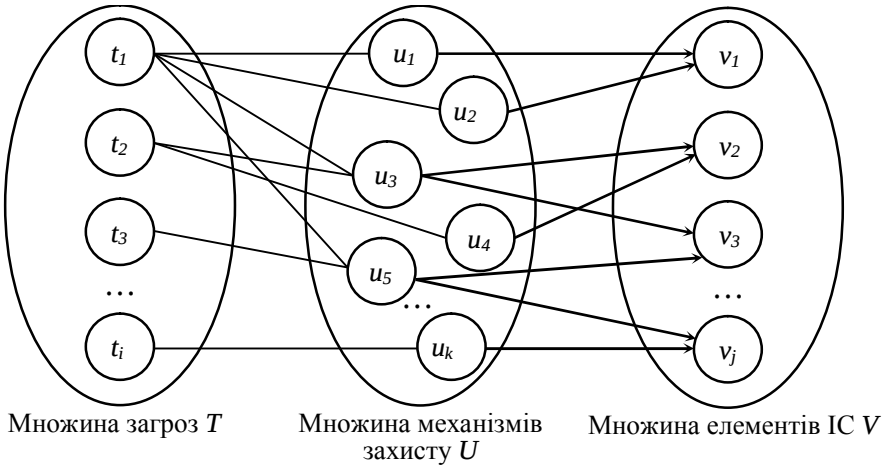

Рис. 2. Типова модель процесу захисту інформації з повним перекриттям

У цій моделі вважається, що кожній загрозі СВВ протистоїть певний механізм захисту. Побудована за таким принципом СВВ не дає загрозам змоги впливати на області, які захищаються. Основним положенням захисту із повним перекриттям є теза про те, що ІС повинна мати хоча б один засіб захисту (ЗЗ) на кожному можливому шляху впливу загроз на ресурси ІС. Цю модель доцільно використовувати в поєднанні з іншими типами моделей СВВ. Під час синтезу систем забезпечення безпеки в ІС такий підхід дозволяє мінімізувати витрати ресурсів ІС для забезпечення заданого рівня захищеності інформації.

В цій моделі виділяють три основні множини:

$V = \{v_j\}$ – множина елементів ІС, що захищаються, де j – кількість елементів, що підлягають захисту $j = \overline{1, J}$;

$M = \{m_k\}$ – множина механізмів безпеки, де k – кількість механізмів безпеки, $k = \overline{1, K}$;

$T = \{t_l\}$ – множина загроз безпеки, де l – кількість загроз, $l = \overline{1, L}$.

Можливість здійснення визначеної загрози щодо конкретного об'єкта являє собою уразливість СВВ. На практиці під уразливістю розуміють не саму можливість здійснення атаки, а ті властивості СВВ, які сприяють здійсненню атаки або потенційно можуть бути використані.

У механізмах захисту (m_k) СЗІ існують такі області:

1. Області уразливості механізмів захисту *U*, на які впливають загрози, де $U = \{u_r\}$ – набір уразливих місць СВВ; $r = \overline{1, R}$ – кількість уразливих місць.

2. Бар'єри захисту *B*, які встановлюються в СЗІ для блокування загроз, що впливають на області уразливості СВВ, де $B = \{b_g\}$ – набір бар'єрів захисту, які є в СВВ; $g = \overline{1, G}$ – кількість бар'єрів захисту.

СВВ при цьому розглядається як сукупність місць уразливості системи та бар'єрів, що блокують ці небезпечні області:

$$M = \{m_k\} = \{U \times B\}.$$

При цьому кожній уразливості відповідає набір бар'єрів $[b_1, ..., b_p]$, де $p = \overline{1, P}$ – кількість бар'єрів, а для СВВ із повним перекриттям виконується умова:

$$\forall \langle t_i v_j \rangle \in M \exists \{\langle u_r b_g \rangle \mid f(t_i\ v_j)\}, \quad (1)$$

де функціонал $f(t_i\ v_j)$ – опис умов забезпечення захисту об'єкта v_j за наявності загрози t_i.

Для СВВ із повним перекриттям для всіх загроз існують бар'єри, які перешкоджають здійсненню цих загроз. Усі загрози повинні проходити тільки через механізм захисту, інакше від цієї моделі немає користі [15].

Вплив загроз аналітично описують у вигляді функціональних залежностей, які зв'язують характеристики різних типів загроз $t_i \in T$ та об'єкти захисту $v_j \in V$.

Кожна із величин $v_j \in V$ залежить від координат уразливостей r та координат бар'єрів g. Ступінь залежності величин v_j залежить від уразливостей $u_r \in U$ та бар'єрів $b_g \in B$ і визначається відповідно до передатних функцій $a_{ik}(p), c_{ik}(p), d_{ik}(p)$, де p – оператор Лапласа.

В такому випадку СВВ описується системою рівнянь:

$$\begin{cases} v_1(p) = t_1(p)a_{11}(p) + t_2(p)a_{12}(p) + ... + t_l(p)a_{1j}(p) + \\ +u_1(p)c_{11}(p) + u_2(p)c_{12}(p) + ... + u_r(p)c_{1j}(p) + \\ +b_1(p)d_{11}(p) + b_2(p)d_{12}(p) + ... + b_g(p)d_{1j}(p), \\ v_2(p) = t_1(p)a_{21}(p) + t_2(p)a_{22}(p) + ... + t_l(p)a_{2j}(p) + \\ +u_1(p)c_{21}(p) + u_2(p)c_{22}(p) + ... + u_r(p)c_{2j}(p) + \\ +b_1(p)d_{21}(p) + b_2(p)d_{22}(p) + ... + b_g(p)d_{2j}(p), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ v_j(p) = t_1(p)a_{j1}(p) + t_2(p)a_{j2}(p) + ... + t_l(p)a_{jj}(p) + \\ +u_1(p)c_{j1}(p) + u_2(p)c_{j2}(p) + ... + u_r(p)c_{jj}(p) + \\ +b_1(p)d_{j1}(p) + b_2(p)d_{j2}(p) + ... + b_g(p)d_{jj}(p) \end{cases} \quad (2)$$

Ця система рівнянь характеризує СВВ та показує залежність вихідних величин від вхідних.

Використовуючи матричні визначення, можна записати цю систему рівнянь у вигляді векторів:

$$V(p) = T(p)' A(p) + U(p)' C(p) + B(p)' D(p) \quad (3)$$

де $V(p), T(p), U(p), B(p)$ – матриці-стовпці розмірності $j' 1$; $A(p), C(p), D(p)$ – матриці-стовпці розмірності $1' j$.

Отже, аналітичний вираз моделі інформації має вигляд:

$$\begin{Vmatrix} v_1(p) \\ v_2(p) \\ \ldots\ldots \\ v_j(p) \end{Vmatrix} = \begin{Vmatrix} t_1(p) \\ t_2(p) \\ \ldots\ldots \\ t_j(p) \end{Vmatrix}' \begin{Vmatrix} a_{11}(p) & a_{12}(p) & \ldots & a_{1j}(p) \\ a_{21}(p) & a_{22}(p) & \ldots & a_{2j}(p) \\ \ldots & \ldots & \ldots & \ldots \\ a_{j1}(p) & a_{j2}(p) & \ldots & a_{jj}(p) \end{Vmatrix} + \\ + \begin{Vmatrix} u_1(p) \\ u_2(p) \\ \ldots\ldots \\ u_j(p) \end{Vmatrix}' \begin{Vmatrix} c_{11}(p) & c_{12}(p) & \ldots & c_{1j}(p) \\ c_{21}(p) & c_{22}(p) & \ldots & c_{2j}(p) \\ \ldots & \ldots & \ldots & \ldots \\ c_{j1}(p) & c_{j2}(p) & \ldots & c_{jj}(p) \end{Vmatrix} + \begin{Vmatrix} b_1(p) \\ b_2(p) \\ \ldots\ldots \\ b_g(p) \end{Vmatrix}' \begin{Vmatrix} d_{11}(p) & d_{12}(p) & \ldots & d_{1j}(p) \\ d_{21}(p) & d_{22}(p) & \ldots & d_{2j}(p) \\ \ldots & \ldots & \ldots & \ldots \\ d_{j1}(p) & d_{j2}(p) & \ldots & d_{jj}(p) \end{Vmatrix} \quad (4)$$

На практиці отримати точні значення *A* та *C* важко, оскільки складно формалізувати поняття загрози, бар'єра та уразливості. Розглянутий підхід не розкриває зв'язків у самій СВВ, не дає змоги адаптувати СВВ у режимі реального часу залежно від реалізованих атак та не враховує впливів загроз, про які ще відсутні будь-які відомості.

Розглянуті моделі повинні використовуватися на етапі проєктування систем захисту інформації, коли ще не сформована архітектура системи, і необхідно попередньо оцінити ефективність проєктованої СВВ.

З метою виправлення зазначених недоліків та урахування особливостей обробки інформації засобами ІС поставимо множину вимог:

– робота в режимі реального часу;

– врахування загроз, характерних для ІС;

– адаптивне функціонування системи захисту інформації із самоорганізацією;

– децентралізація управління та ієрархічно-розподільна структура;

– збільшення достовірності та повноти прийняття управлінського рішення;

– зменшення математичної складності та ресурсної обтяжливості методів;

– простота побудови математичної моделі оцінки впливу загроз на стан захищеності.

На основі проаналізованих уразливостей ІС обробки інформації та з метою оцінювання ефективності СВВ і стану захищеності інформації, що в них циркулює, доцільно побудувати модель протидії порушенням захищеності інформації в ІС.

Сутність моделі полягає у зміні структури функціонування елементів моделі порівняно із вищезазначеним прикладом. На стан захищеності елементів ІС та ІР загалом впливає у певний момент часу множина зовнішніх і внутрішніх загроз, які спрямовані на порушення цілісності, доступності, конфіденційності елементів СВВ та ІС або здійснення деструктивного впливу на програмну, апаратну, інформаційні складові самої системи. Також на стан захищеності ІС впливає множина механізмів захисту, які реалізовані в ІС та націлені на забезпечення безпеки. У ІС механізми захисту реалізуються на основі алгоритмів навчання з учителем на етапі розроблення самої ІС, та алгоритму навчання без учителя, який реалізується під час функціонування ІС. Саме перетин зазначених множин та наявність інструментів захищеності ІС загалом визначають поточний стан захищеності самої ІС. А це дає змогу запропонувати управлінське рішення для підтримки належного стану безпеки та визначити механізми протидії кожній окремій загрозі на підставі цільової функції або мети управління безпекою.

Відомі підходи до оцінювання захищеності ІС та її складових [2–3] використовують схожі методики багатовимірного порівняльного аналізу, які ґрунтуються здебільшого на методах таксономії з елементами факторного аналізу. Результати застосування методик залежать від кваліфікації виконавця внаслідок помітної частки суб'єктивізму та функціональних особливостей моделей.

Щоб зменшити обсяг вхідних даних для оцінювання стану захищеності ІС і підвищити об'єктивність і оперативність, пропонуємо здійснити визначення порядку математичного аналізу вхідних даних, якими є оцінки захищеності ІС, з метою визначення стану захищеності інформації загалом. Математичний апарат оцінки має бути гнучким до переліку загроз безпеці інформації та параметрів атак за умови забезпечення оперативного оцінювання поточного стану захищеності ІС. За таких умов важлива вимога забезпечення працездатності формальних методів за короткими обмеженими вибірками щодо стану захищеності.

Розпізнавання станів захищеності ІС здійснюється так. Є деяка множина станів, які належать до p різних класів. Компонентами вектора є окремі загрози безпеці інформації. Необхідно, використовуючи інформацію про стани ІС та їх класифікацію, знайти таке правило, за допомогою якого можна було б з мінімальною кількістю помилок класифікувати нові стани за даними про отримані параметри атак.

Узагальнену типову модель, що описує взаємодію загроз, засобів захисту ІС та множину станів захищеності ІС, подано на рис. 3.

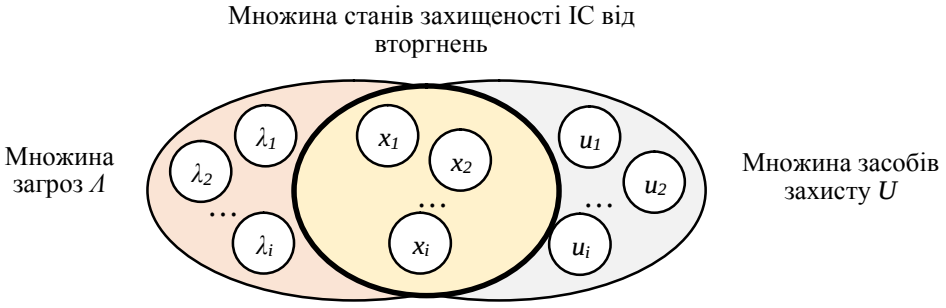

Рис. 3. Типова модель протидії порушенням захищеності інформації в ІС

Класами можуть бути стани захищеності ІС. Приклад для двох класів: стан захищеності ІС погіршується; стан захищеності ІС покращується. Приклад для трьох класів: стан захищеності ІС погіршується; стан захищеності ІС залишається без змін; стан захищеності ІС покращується. Очевидно, що кількість класів може бути довільною та визначатися умовою однозначної класифікації поточної ситуації.

Вважатимемо, що стан ІС задано вектором x, а його класифікація – числом w (w може набувати p значень: 0, 1, …, p - 1). Практично вектором стану ІС буде вектор, компонентами якого виступатимуть числові оцінки захищеності інформації. Розмірність вектора відповідатиме кількості загроз, які потрібно розглянути.

Отже, необхідно, маючи послідовність із l станів захищеності та класифікацій $x_1, w_1; \ldots; x_l, w_l$, побудувати вирішуюче правило $\omega = F(x)$, яке з найменшою кількістю помилок класифікуватиме нові стани ІС.

Для формалізації слова "помилка" вважатимемо, що існує деяке правило Φ, що визначає для кожного вектора x класифікацію $\omega = \Phi(x)$, яку називають "істинною". Помилкою кла сифікації вектора x за допомогою правила $F(x)$ назвемо таку класифікацію, за якої $F(x)$ та $\Phi(x)$ не збігаються.

Правило $F(x)$ є однією із функцій деякої заданої множини функцій $\{F(x)\}$, а правило класифікації $\Phi(x)$ визначається умовною ймовірністю $P(\omega|x)$.

Наступний крок: необхідно надати точний зміст тому, як формуються стани ІС, за якими формулюється правило для класифікації, та як вибрати параметри атак, за якими визначається якість побудованого правила.

Вважатимемо, що на просторі векторів x існує невідома нам імовірнісна міра (надалі позначатимемо її щільністю $P(x)$). Відповідно до $P(x)$ випадково і незалежно з'являються ситуації x, які класифікуються за допомогою правила $P(\omega|x)$. Отже, визначається навчальна послідовність

$$x_1, w_1; \ldots; x_l, w_l \tag{5}$$

Для будь-якого вирішуючого правила $F(x)$ визначимо імовірність різної класифікації за допомогою правила $F(x)$ та правила $P(\omega|x)$. Чим менша ця імовірність, тим краща якість. Формально якість вирішуючого правила подамо у вигляді:

$$I(F) = \sum_{i=0}^{p-1} \int \Theta\left(F(x) - \omega_i\right) P\left(\omega_i \middle| x\right) P(x)\, dx \tag{6}$$

де $\Theta(z) = \begin{cases} 0, & z = 0 \\ 1, & z \neq 0 \end{cases}$.

Безпосередньо обчислити імовірність безпомилкової класифікації впливу загроз на стан ІС для будь-якого вирішуючого правила $F(x)$ неможливо, тому що щільності $P(x)$ та $P(\omega|x)$ заздалегідь не відомі.

Тим не менш завдання полягає у тому, щоб, використовуючи вибірку (5), знайти у класі $\{F(x)\}$ таке правило, яке мінімізує функціонал (6).

Надалі вважатимемо, що:

1) змінна w набуває тільки два значення: 0 та 1 (тобто ситуація x належить до одного з двох класів); це обмеження не є принциповим, оскільки послідовним розділенням на два класи можна отримати розділення на будь-яку скінченну кількість класів;

2) клас індикаторних функцій $\{F(x)\}$, тобто функцій, що набувають два значення: 0 та 1, є параметричним $\{F(x,a)\}$ (a – параметр, що належить множині Λ, конкретне значення якого $a = a^*$ визначає функцію $F(x,a^*)$ класу $F(x,a)$; знайти потрібну функцію у класі – значить встановити потрібне значення параметра в класі; вивчення лише параметричного класу функцій ніяк не знижує загальності у завданні класу функцій, оскільки множина Λ довільна: вона може бути множиною скалярних величин, множиною векторів чи множиною абстрактних елементів;

3) функціонал (6) запишемо у вигляді

$$I(\alpha) = \int (\omega - F(x,\alpha))^2 P(x,\omega)\, dx d\omega, \qquad (7)$$

де функція $P(x,\omega) = P(\omega|x)P(x)$ – сумісна щільність пар x, ω.

Отже, задача розпізнавання станів захищеності полягає у тому, щоб у класі індикаторних функцій $F(x,a)$ відшукати таку, яка б мінімізувала функціонал (7) в умовах, коли сумісна щільність $P(x,w)$ невідома, але задана імовірна і незалежна вибірка пар, отриманих відповідно до цієї щільності.

В основу алгоритмів розпізнавання станів захищеності ІС покладено спеціальний метод пошуку вирішуючого правила, який ґрунтується на побудові гіперплощини, яка розділяє.

Для цього можна використовувати один з методів інтелектуального розподілу даних – метод опорних векторів. Метод опорних векторів (англ. Support Vector Machine, SVM) – це набір схожих алгоритмів категорії "навчання з учителем", які застосовують у задачах класифікації та регресійного аналізу. Цей метод належить до сім'ї лінійних класифікаторів. Характерною особливістю методу опорних векторів є постійне зменшення емпіричної помилки класифікації та збільшення зазору між класами. Тому цей метод часто називають методом класифікатора із максимальним зазором [3].

Метод відшукує елементи, розміщені на кордонах між двома класами, які й називають опорними векторами.

Метод опорних векторів здійснює пошук лінійної функції, яка дає змогу зарахувати елементи набору даних до одного із двох класів. Завдання бінарної класифікації можна сформулювати як пошук лінійної функції $f(x)$, яка набуває значення, менше від нуля для елементів одного класу і більше від нуля для елементів іншого.

Розподілена гіперплощина має такий вигляд:

$$f(x) = w^* x - b = 0,$$

де w – вектор, перпендикулярний до розподіленої гіперплощини; параметр b визначає відстань гіперплощини від початку координат.

Гіперплощини, паралельні до оптимальної гіперплощини і найближчі до опорних векторів двох класів, можна описати такими рівняннями:

$$\begin{cases} wx - b = 1 \\ wx - b = -1 \end{cases}.$$

Якщо навчальна множина даних лінійно нероздільна, то можна вибрати гіперплощини так, щоб в смугу між ними не потрапляла жодна точка навчальної вибірки, і потім максимізувати відстань між гіперплощинами. Ширина смуги в цьому випадку дорівнює $\frac{2}{\|w\|}$, тому потрібно мінімізувати $\|w\|$. Для вилучення усіх точок зі смуги повинна виконуватися умова:

$$c_i(w^* x_i - b) \geq 1, 1 \leq i \leq n$$

де c_i – мітка класу, що набуває значення –1 і +1; x_i – вектор робочої вибірки з міткою класу c_i.

Це завдання квадратичної оптимізації еквівалентне задачі пошуку сідлової точки функції Лагранжа:

$$\begin{cases} -L(\lambda) = \sum_{i=1}^{n} \lambda_i + \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \lambda_j c_i c_j (x_i x_j) \to \min_{\lambda} \\ \lambda_i \geq 0, 1 \leq i \leq n \\ \sum_{j=1}^{n} \lambda_i c_i = 0 \end{cases},$$

де L – функція Лагранжа; λ_i – множники Лагранжа.

Щоб узагальнити SVM на випадок лінійної нероздільності, вводять константу C – внутрішній параметр методу, що дає змогу регулювати відношення між максимізацією ширини розділової смуги і мінімізацією сумарної помилки.

Основною проблемою застосування методу опорних векторів у завданні бінарної класифікації є складність пошуку лінійної межі між двома класами. Якщо таку межу побудувати не вдається, одне з рішень – збільшення розмірності (перенесення даних в інший простір, вищої розмірності), де існує можливість побудови площини, що розділяє безліч елементів на два класи [17].

Дві скінченні множини векторів: множина $X = x_1, ..., x_a$ та множина $\bar{X} = \bar{x}_1, ..., \bar{x}_b$ розділені орієнтованою гіперплощиною, якщо для деякого $k < 1$ існує такий вектор φ, що виконуються нерівності $x_i^T \varphi \geq 1$, $i = \overline{1, a}$ та $\bar{x}_j^T \varphi \leq k$, $j = b$.

Очевидно, що якщо існує вектор φ, для якого виконуються зазначені нерівності, то існує і множина векторів φ, що задовольняє ці умови. Знайдемо серед них мінімальний за модулем.

Серед параметричної сім'ї векторів існує вектор φ_0, що визначає такий напрямок, на якому проєкції множин X та $\bar{X}$ найбільше віддалені одна від одної:

$$\varphi_0 = \arg\max_{\varphi} \left[\min_{x_i \in X} x_j^T \varphi - \max_{\bar{x}_j \in \bar{X}} \bar{x}_j^T \varphi \right]. \quad (8)$$

Цей вектор φ_0 є оптимальним, а отримана за його допомогою розділова гіперплощина $x\varphi_0 = c_0$ – оптимальна розділова гіперплощина, де

$$c_0 = \frac{\min_{x_i \in X} x_i^T \varphi_0 + \max_{\bar{x}_j \in \bar{X}} \bar{x}_j^T \varphi_0}{2}. \quad (9)$$

Оптимальна гіперплощина відділяє точки множини X (для цих точок $x\varphi_0 > c_0$) від точок множини $\bar{X}$ (для цих точок $\bar{x}\varphi_0 < c_0$) та найбільш віддалена від елементів об'єднаної величини $X \cup \bar{X}$.

Висновки

Отже, зміна стану захищеності інформації як процес відбувається у певній фізичній системі, яку неможливо подати детермінованою системою.

Розглянуті вирази свідчать про те, що оцінювання стану захищеності ІС залежатиме від швидкості адаптації наявних СВВ до нових загроз, коректної ідентифікації вхідного трафіку та виявлення параметрів атак за внутрішніми або зовнішніми ознаками.

Запропонована модель протидії порушенням захищеності інформації в ІС, на відміну від подібних відомих сьогодні моделей, які призначені для оцінювання впливів можливих атак і загроз різних рівнів та прийняття обґрунтованого рішення щодо реалізації СВВ ІС, надає можливість оперативно оцінювати поточний стан захищеності ІС за умов забезпечення працездатності формальних методів за короткими обмеженими вибірками щодо параметрів засобів захисту ІС та параметрів загроз, що впливають на елементи ІС. Застосування запропонованої моделі дасть змогу отримувати поточні оцінки стану захищеності інформації, надати додатковий час на підготовку та здійснення заходів реагування на загрози з метою підвищення безпеки інформації.

Список використаних джерел

[1] *Павлов І. М., Толюпа С. В., Ніщенко В. І. Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем. Сучасний захист інформації. 2014, № 4. С. 44–52.*

[2] *Толюпа С. В., Штаненко С. С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут. 2018. Вип. № 3. С. 56–66.*

[3] *Довбешко С. В., Толюпа С. В., Шестак Я. В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. Сучасний захист інформації: наук.-техн. журнал. 2019. № 1. С. 56–62.*

[4] *Toliupa S., Nakonechnyi V., Uspenskyi O. Signature and statistical analyzers in the cyber attack detection system. Information technology and security. Ukrainian research papers collection. Vol. 7, Iss. 1 (12). С. 69–79.*

[5] *Сальник С. В., Сторчак А. С., Микитюк А. В. Модель порушення захищеності інформаційних ресурсів комунікаційних систем. Information Technology And Security. 2019. Вип. 7(1). С. 25–34.*

[6] *Бурячок В. Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем. Захист інформації. 2011. Вип. 3(52). С. 19–27.*

[7] *Хусаінов П. В. Показник кібернетичної безпеки автоматизованої системи у часі. Збірник наукових праць ВІТІ. 2015. Вип. 1. С. 101–111.*

[8] *Куцаєв В. В., Радченко М. М., Козубцова Л. М., Терещенко Т. П. Методика оцінки кібернетичної захищеності інформаційно-телекомунікаційного вузла зв'язку. Збірник наукових праць ВІТІ. 2018. Вип. 2. С. 67–76.*

[9] *Raiyn J. A survey of Cyber Attack Detection Strategies. International Journal of Security and Its Applications. 2014. Vol. 8, issue 1. P. 247–256. DOI: 10.14257/ijsia.2014.8.1.23*

[10] *Дудикевич В. Б., Опірський І. Р. Аналіз моделей захисту інформації в інформаційних мережах держави. Системи обробки інформації. 2016. Вип. 4 (141). С. 86–89.*

[11] *Павлов І. М., Толюпа С. В. Аналіз підходів оцінки ефективності математичних моделей при проектуванні систем захисту інформації. Сучасний захист інформації. 2014. Вип. 3. С. 36–44.*

[12] *Кучернюк П. В., Довгаль А. О. Модель загроз безпеки в інформаційно-комунікаційних системах на основі регресійного аналізу. Електроніка та зв'язок. 2017. Вип. № 2(97), т. 22. С. 79–84.*

[13] *Давыдова Е. Н. Математическое моделирование распределенных систем защиты информации. Программные продукты и системы. 2011. Вип. 2. С. 57–61.*

[14] *Павлов І. М., Хорошко В. О. Проектування комплексних систем захисту інформації. К.: ВІТІ, ДУІКТ, 2011. 245 с.*

[15] *Толюпа С. В., Пархоменко І. І. Побудова комплексних систем захисту складних інформаційних систем на основі структурного підходу. Сучасний захист інформації. 2015. № 4. С. 96–104.*

[16] *Козубцов І. М., Козубцова Л. М., Куцаєв В. В., Терещенко Т. П. Методика оцінки кібернетичної захищеності системи зв'язку організації. Сучасні інформаційні технології у сфері безпеки та оборони. 2018. Вип. 1 (31). С. 43–46.*

[17] Толюпа С. В., Наконечний В. С. Застосування комплексного підходу до рішення задач управління в системах передачі даних на основі інтелектуальних технологій. Вісник Інженерної академії України. 2015. № 4. С. 63–71.

MODEL OF INTRUSION DETECTION SYSTEM IN INFORMATION SYSTEMS

S. Tolyupa[1], I. Parkhomenko[2], S. Shtanenko[3]

[1, 2] Taras Shevchenko National University of Kyiv, 60, Volodymyrska Str., Kyiv, 01033, Ukraine

[3] Military Institute of Telecommunications and Information Technologies named after Heroes of Kruty, 45/1, Moscow Str. Kyiv, 01011, Ukraine

The article proposes a model of intrusion detection systems (IDS), which reflects the main processes that take place in the system in order to optimize the processes of anti-intrusion. Such processes in general can be represented as processes of allocation and use of resources that are allocated for the protection of information. The use of modeling techniques to ensure the appropriate level of information security has led to the development of many formal security models that help maintain the appropriate level of security of systems based on objective and indisputable postulates of mathematical theory. The proposed model of counteracting information security breaches in IP, in contrast to similar existing models, which are designed to assess the impact of possible attacks and threats of various levels and make an informed decision on the implementation of IP intrusion detection systems, provides an opportunity to quickly assess the current state of IP security. efficiency of formal methods on short limited samples about parameters of means of protection of IP and parameters of threats influencing elements of IP. The application of the proposed model will allow to obtain current assessments of the state of information security, to provide additional time for the preparation and implementation of measures to respond to threats in order to enhance information security.

Key words: intrusion detection system; cyberattack; information system; threat; intruder; model.