УДК 004.056.5

В.В. ЛИТВИНОВ[*], Н. СТОЯНОВ[**], І.С. СКІТЕР[***], О.В. ТРУНОВА[*], А.Г. ГРЕБЕННИК[***]

АНАЛІЗ СИСТЕМ ТА МЕТОДІВ ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНИХ ВТОРГНЕНЬ У КОМП'ЮТЕРНІ МЕРЕЖІ

[*]Чернігівський національний технологічний університет, м. Чернігів, Україна
[**]Болгарський інститут оборони імені Цветана Лазарова, м. Софія, Болгарія
[***]Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

Анотація. *Систематизовані, узагальнені і розвинені уявлення про методи і системи аналізу комп'ютерних мереж, які підлягають захисту. Приведений математичний апарат формування образу нормального функціонування систем, визначення узагальненої оцінки стану системи, яка підлягає захисту. Описані основні недоліки та напрями подальшого розвитку систем виявлення вторгнень.*
Ключові слова: *системи виявлення вторгнень, інтегральна оцінка аномальності, профіль інформаційної системи, статистичні методи оцінки, нейронні мережі, профайл системи, генерація патернів.*

Аннотация. *Систематизированы, обобщены и развиты представления о методах и системах анализа компьютерных сетей, подлежащих защите. Приведен математический аппарат формирования образа нормального функционирования систем, определения обобщенной оценки состояния системы, подлежащей защите. Описаны основные недостатки и направления дальнейшего развития систем обнаружения вторжений.*
Ключевые слова: *системы обнаружения вторжений, интегральная оценка аномальности, профиль информационной системы, статистические методы оценки, нейронные сети, профайл системы, генерация паттернов.*

Abstract. *There were systematized, generalized and developed the ideas about methods and systems for analyzing computer networks which are protected. There was given the mathematical device for formation of an image of a normal systems functioning, definition of the generalized estimation of a system state to be protected. The main drawbacks and directions for the further development of intrusion detection systems are described.*
Keywords: *intrusion detection systems, integral estimation of anomalies, profile of the information system, statistical estimation methods, neural networks, system profile, pattern generation.*

1. Вступ

Системи виявлення вторгнень (СВВ) є одним із механізмів аналізу поведінки комп'ютерної мережі і виступають як важливе доповнення інфраструктури мережевої безпеки. СВВ служать механізмами моніторингу та спостереження підозрілої активності, проводять аналіз ресурсів мережі, а також самостійні дії щодо ідентифікації аномальних подій у мережі – реальних порушень і спроб порушень [1, 2].

Існує значний об'єм публікацій та досліджень, присвячених аналізу сучасних СВВ та методів виявлення несанкціонованих вторгнень. У пропонованій статті проводиться порівняльний аналіз систем, наводяться їх переваги та недоліки, загальна характеристика їх структури. Поряд з цим розглянуті математичні методи аналізу стаціонарної поведінки систем та способи виявлення порушення їх стаціонарності на основі аналізу профілю мережі.

© Литвинов В.В., Стоянов Н., Скітер І.С., Трунова О.В., Гребенник А.Г., 2018

ISSN 1028-9763. Математичні машини і системи, 2018, № 1

2. Структура систем виявлення вторгнень

У роботі [3] приведена структура сучасних СВВ, яка включає в себе такі підсистеми:

- підсистема збору інформації про систему, яка підлягає захисту;
- підсистема аналізу для пошуку атак та вторгнень у систему;
- підсистема представлення даних для контролю системи в режимі реального часу.

Підсистема збору інформації отримує дані від автономних модулів, датчиків програмного забезпечення (ПЗ) системи, датчиків хосту, міжмережевих та мережевих датчиків, скомпонованих у залежності від задач структури мережі та типу інформації, яка підлягає аналізу.

Ієрархічно підсистема аналізу як вхідні дані використовує інформацію із попередньої підсистеми і містить у собі набір аналізаторів, скомпонованих за задачами виявлення вторгнень заданого типу. Ефективність виявлення вторгнень залежить від параметрів аналізаторів та їх кількості.

Підсистема представлення даних орієнтована на різні групи користувачів, які контролюють певні підсистеми мережі. Тому в таких СВВ використовують розмежування доступу, групові політики, повноваження та ін.

У залежності від наборів параметрів оцінки стану системи сучасні СВВ використовують дві групи методів. У випадку фіксованого набору параметрів оцінки і фіксованого часу навчання використовуються методи контрольованого навчання («навчання з учителем»). У випадку, коли множина параметрів оцінки може змінюватися протягом заданого часу дослідження, а процес навчання відбувається весь час, використовуються методи неконтрольованого навчання («навчання без учителя»). У табл. 1–2 представлені характеристики методів навчання СВВ та СВЗ (табл. 3) [4].

Таблиця 1. Виявлення аномалії за методами контрольованого навчання («навчання з учителем»)

Методи виявлення	Системи	Характеристика методу
Моделювання правил	W&S	СВВ протягом процесу навчання формує набір правил нормальної поведінки системи. При аналізі несанкціонованих дій система застосовує отримані правила. У випадку незадовільного співпадіння система подає сигнал про виявлення аномалії
Описова статистика	IDES, NIDES, EMERLAND, JiNao, HayStack	Навчання полягає у збиранні описової статистики множини показників системи, яка підлягає захисту, у спеціальну структуру. Для виявлення аномалії обчислюють «відстань» між векторами показників – поточних та збережених. Стан системи вважається аномальним, якщо «відстань» перевищує певну межу
Нейронні мережі	Hyperview	Використовуються нейромережі різної структури. Навчання проводиться за даними, які характеризують нормальну поведінку системи. Навчена мережа використовується для оцінки аномальності системи. Вихід нейромережі формує висновок про наявність аномалії

Таблиця 2. Виявлення аномалії за методами неконтрольованого навчання («навчання без учителя»)

Методи виявлення	Системи	Характеристика методу
Моделювання множини станів	DPEM, JANUS, Bro	Нормальна поведінка системи описується у вигляді набору фіксованих станів та переходів між ними. Стан системи представляє собою вектор певних значень параметрів системи
Описова статистика	MIDAS, NADIR, Haystack, NSM	Аналогічно методам контрольованого навчання

Таблиця 3. Виявлення зловживань за методами контрольованого навчання («навчання з учителем»)

Методи виявлення	Системи	Характеристика методу
Моделювання станів	USTAT, IDIOT	Вторгнення визначається як послідовність станів. Стан – вектор значень параметрів оцінки системи, яка підлягає захисту. Необхідна і достатня умова вторгнення – наявність вказаної послідовності. Способи представлення сценаріїв вторгнення: послідовність подій, використання мереж Петрі, в яких вузли – події
Експертні системи	NIDES, EMERLAND, MIDAS, DIDS	Процес вторгнення представляють у вигляді різного набору правил. Також використовуються продукційні системи
Моделювання правил	NADIR, HayStack, JiNao, ASAX, Bro	Спрощений варіант експертних систем
Синтаксичний аналіз	NSM	СВЗ виконує синтаксичний розбір з метою виявлення певної комбінації символів, які передаються між підсистемами та системами об’єкта захисту

Основною ідеєю виявлення нестандартної поведінки мережі, яка підлягає захисту, є формування профілю чи образу мережі. Тому основними методами, на яких базується реалізація СВВ, є методи розпізнавання образів. При цьому образ нормальної поведінки формується на основі аналізу параметрів оцінки мережі.

Висновки про аномальну поведінку формуються на основі відхилень значень оцінок параметрів від профілю мережі. Величина та характер відхилень, як правило, в режимі реального часу, дають змогу проводити ідентифікацію аномалії – технічний збій, допустиме відхилення пов’язане із дією зовнішнього середовища, атака на мережу.

Формування профілю чи образу в СВВ проводиться за допомогою таких методів:

• статистичні методи аналізу параметрів оцінки;

• методи множинного опису подій та формальної логіки;

• методи нечіткої логіки та нейронні мережі.

Виходячи із способів формування профілю мережі та методів виявлення аномалій, можна визначити два класи задач:

• вибір оптимальної множини параметрів оцінки;

• визначення загального показника аномальності.

Питання визначення інтегральної оцінки аномальності поведінки мережі на сьогодні є практично не вирішеним завдяки неоднозначності розв'язку задачі формування множини оцінок параметрів мережі, яка підлягає захисту. Крім того, постає ще три питання:

• формування оптимальної множини параметрів;

• зміна сформованої множини в часі;

• оцінка адекватності сформованої множини на заданому інтервалі часу та при зміні типів вторгнень у мережу.

Розв'язок задач формування множини оцінок параметрів та їх динаміки можливий при використанні методу групового врахування аргументів (МГУА), еволюційних та генетичних алгоритмів [5]. Тоді визначення інтегральної оцінки може бути проведене за допомогою ймовірнісних методів на основі Байєсівської статистики [6], аналізу коваріацій параметрів оцінок [6], методів кореляційного аналізу [7], автокореляційних моделей [7].

3. Способи отримання інтегральної оцінки стану захисту системи

Розглянемо систему, яка описується множиною подій (an event) $E = (E_1, E_2, ..., E_n)$ і буде використана для встановлення факту вторгнення. Елемент множини E_i представляє собою окрему подію оцінювання й приймає два значення: 1(true) – подія аномальна, 0(false) – ні. Якщо I – гіпотеза, яка визначає, що в системі присутні вторгнення, то достовірність і чутливість події E_i із множини $E = (E_1, E_2, ..., E_n)$ будуть визначатися умовними ймовірностями $P(E_i / I)$ та $P(E_i / \bar{I})$. Ймовірність вторгнення в систему на основі аналізу множини подій може бути обчислена за теоремою Байєса:

$$P(I/E) = P(I/E_1, E_2, ..., E_n) = \frac{P(I) \cdot P(I/E_1, E_2, ..., E_n)}{P(E_1, E_2, ..., E_n)}. \quad (1)$$

Оскільки на множині подій E кількість умовних імовірностей експоненціально залежить від потужності множини, то для спрощення обчислень введемо гіпотезу про незалежність подій E_i та E_j де $i \neq j$. Умовні ймовірності визначаються як

$$P(E/I) = P(E_1, E_2, ..., E_n/I) = \prod_{i=1}^{n} P(E_i / I), \quad (2)$$

$$P(E/\bar{I}) = P(E_1, E_2, ..., E_n/\bar{I}) = \prod_{i=1}^{n} P(E_i / \bar{I}). \quad (3)$$

Тоді за формулою Байєса:

$$P(I/E) = P(I/E_1, E_2, ..., E_n) = \frac{P(I) \cdot \prod_{i=1}^{n} P(E_i / I)}{P(E_1, E_2, ..., E_n)} = \frac{P(I) \cdot \prod_{i=1}^{n} P(E_i / I)}{P(I) \cdot \prod_{i=1}^{n} P(E_i / I) + P(\bar{I}) \cdot \prod_{i=1}^{n} P(E_i / \bar{I})}. \quad (4)$$

Підвищення точності чи отримання більшої достовірності оцінки $P(I/E_1, E_2, ..., E_n)$ можливе при умові врахування взаємозв'язків між елементами множини E на основі аналізу коваріаційних матриць.

Враховуючи те, що множина подій $E = (E_1, E_2, ..., E_n)$ представляє собою вектор, а зв'язки між елементами вектора можуть бути описані за допомогою коваріаційної матриці $C = (\mathrm{cov}(E_i E_j))$, інтегральна оцінка факту вторгнення в систему може бути визначена як

$$A^{\mathrm{int}} = E^T C^{-1} E . \quad (5)$$

4. Методи формування образу (профілю) нормальної поведінки інформаційної системи

До методів формування образу ІС можна віднести таке:

• створення профайла системи;

• використання нейронних мереж;

• генерація патернів.

Створення профайла системи полягає у накопиченні вимірювань значень параметрів оцінки. Основні вимоги до структури профайла: мінімальний кінцевий розмір; мінімальний час оновлення.

У профайлі використовують декілька типів вимірювань. У роботі [3] наведені такі показники:

• Показник активності – величина, при перевищенні якої активність системи оцінюється як така, що швидко прогресує. Приклад: середнє число записів аудиту, які обробляються за одиницю часу Використовується для виявлення аномалій, пов'язаних із різким прискоренням у роботі.

• Розподіл активності в записах аудиту – будь-яка дія в системі: доступ до файлів, операції вводу-виводу.

• Вимірювання категорій – розподіл певних активностей за категоріями. Приклад: відносна частота реєстрації в системі із кожного фізичного місцезнаходження.

• Порядкові вимірювання – оцінка активності у вигляді цифрових значень, обчислення загальної статистики значень певної активності. Приклад: кількість операцій вводу-виводу від кожного користувача.

Виявлення аномалій із використанням профайла проводиться на основі статистичних методів оцінки [7]. При цьому поточні значення вимірювань профайла $PM^c = (PM_1^c, PM_2^c, ..., PM_n^c)$ порівнюють із збереженими $PM^s = (PM_1^s, PM_2^s, ..., PM_n^s)$. Результат порівняння представляє собою показник аномальності в даному вимірюванні: $A_i = PM_i^c - PM_i^s$. Загальний показник аномальності може бути обчислений як функція від значень показника аномальності в кожному вимірюванні профайла, наприклад, зважена мультиплікативна виду

$$A^{\Sigma} = \sum_{i=1}^{n} w_i A_i^2 = w_1 A_1^2 + w_2 A_2^2 + ... + w_n A_n^2 , \quad (6)$$

де w_i – відносна вага метрики PM_i.

До переваг методу відносять використання добре відомих статистичних методів.

До недоліків:

• нечутливість до послідовності схожих подій;

• можливість навчання зловмисником системи, при якому аномальна поведінка буде вважатися нормальною;

• складність визначення порогу, при якому аномалії розглядають як вторгнення. Зменшення порогу приводить до похибок першого роду (false positive), а завищення – до похибок другого роду (false negative);

• обмеження у використанні статистичних методів. Для виявлення аномалій необхідне припущення, що вхідні дані поступають від квазістатичного процесу.

Використання нейронних мереж для формування профілю нормальної поведінки системи полягає у навчанні мережі на основі аналізу команд, їх структури, періодичності тощо. Результатом навчання є так званий «нормальний профіль». Використання навчання мережі проводиться на основі результатів прогнозування її поведінки та порівняння реальних та передбачених команд, чисельних характеристик відмінностей в командах.

До переваг методу відносять:

• незалежність від природи вхідних даних;

• автоматичне врахування зв'язків між різними вимірюваннями;

• продуктивність при роботі з даними, які мають значний рівень шуму.

До недоліків:

• створення адекватної топології та визначення ваг проводиться на основі великого періоду навчання;

• вибір оптимального розміру «вікна» даних для навчання для достатньої продуктивності системи.

У роботі [8] представлення профілю системи за допомогою генерації патернів базується на тому припущенні, що поточні значення параметрів оцінки можна пов’язати з поточним станом системи і функціонування системи може бути представлене у вигляді послідовності подій або станів. Тоді патерни, як масив значень оцінок параметрів нормальної роботи системи, повинні формуватися за правилами, представленими у [8].

Ці правила формуються індуктивно, у процесі навчання вони динамічно змінюються тими, які мають більшу ймовірність їх виникнення, є оптимальними за змістом оцінок та більш адекватно описують систему, яка підлягає захисту.

Тоді вказана множина правил, яка створюється індуктивно під час спостереження, складає профіль системи. Реєстрація факту аномальної поведінки відбувається шляхом порівняння послідовності подій, яка відповідає визначеним правилам та після подій.

До переваг методу відносять:

• урахування залежностей між подіями та їх послідовністю;

• обробка результатів зі значним розмахом поведінки при строго визначеній послідовності патернів;

• виділення на всій підозрілій сесії спостережень окремих важливих подій безпеки;

• чутливість до виявлення порушень за рахунок наявності семантики процесів, що дозволяє виявляти дії зловмисників щодо перенавчання системи.

До недоліків слід віднести те, що патерни нерозпізнаної поведінки можуть бути не прийняті за аномальні, так як не відповідають лівим частинам сформованих правил.

5. Методи виявлення зловживань

Для повного аналізу мережі на предмет безпеки поряд з методами виявлення аномалій у більшості СВВ також використовують технології виявлення зловживань, які базуються на прогнозуванні аномальної поведінки мережі, та наступним аналізом реальних аномалій [9]. Як образ чи профіль при виявленні зловживань використовують представлення дій зловмисника у вигляді сигнатури вторгнень, які визначають умови та зв'язок подій при проникненні в систему чи при інших зловживаннях. Крім того, сигнатури також є корисними при виявленні спроб незаконних дій, коли частковий збіг сигнатур означає спробу вторгнення в систему.

Для виявлення зловживань можна використовувати таке:

• продукційні/експертні системи;

• аналіз зміни станів;

• спостереження за натисканням клавіш;

• методи моделювання поведінки.

У [10] у продукційних системах інформація про вторгнення кодується у вигляді правил виду *« if….причина then …рішення»*, причому при додаванні правил причина відповідає події, яка реєструється системою збирання інформації СВВ. У частині «*if*» правила кодуються при умові атаки. Коли всі умови в лівій частині правила задоволені, виконується дія його правої частини.

При використанні продукційних систем для виявлення вторгнень є можливість розділити причини і розв'язки проблем, які виникають. Але крім вказаних переваг продукційних систем, до основних проблем їх використання слід віднести недостатню ефективність при роботі з великими масивами даних та врахування залежностей даних параметрів оцінки.

До недоліків систем можна віднести:

• можливість виявлення тільки тих вразливостей, для яких відома сигнатура;

• видалення чи додавання правил приводить до зміни всієї множини правил;

• ефективність експертної системи досягається тільки за умови, коли навички адміністратора, які підлягають моделюванню, не суперечливі;

• відсутність обробки порядку послідовностей у даних, які підлягають аналізу;

• поєднання різних вимірювань вторгнень та створення цілісної картини вторгнення призводить до того, що часткові причини стають не визначеними.

Метод аналізу зміни станів описаний і реалізований в [11] та [12] відповідно. У вказаних роботах ідентифікація вторгнення в систему проводиться на основі сигнатури, сформованої на основі зміни станів системи. Також аналіз переходів станів системи використовується для розробки моделі ідентифікації вторгнень у систему. Такий підхід моделює вторгнення як послідовність переходів станів системи, описаних у термінах дій та фіксації станів. Тоді патерн вторгнення відповідає певному стану системи і має відповідну логічну функцію. Перехід системи в інший стан фіксується фактом виконання цієї функції.

Аналіз системи за допомогою переходів станів, направлений на ідентифікацію вторгнення, має перевагу в тому, що є незалежним від аналізу сигнатури і формується на окремих переходах системи. Він має більшу ефективність особливо при наявності модифікації вторгнень з відомою сигнатурою.

Технології спостереження за натисканням клавіш відносять до технологій поведінкової біометрії. Ідентифікація вторгнення базується на створенні патерну поведінки користувача на основі масиву даних шаблонів поведінки користувача та навчання системи. Для патерну поведінки встановлюється поріг для визначення переходу до аномальної поведінки – ймовірнсть аномальності поведінки. Результатом навчання системи є шаблон, на основі якого проводиться оцінка ризику. Якщо величина ризику є достатньо високою, то зі значною долею ймовірності робиться висновок про наявність вторгнення. Недоліками технологій є залежність результату виявлення вторгнень від заданого порогу ризику. Занадто високий поріг приводить до похибок першого роду (false positive), а занадто низький – похибок другого роду (false negative). Але в цілому поведінкові методи аналізу забезпечують меншу кількість похибок першого роду, ніж інші методи розпізнавання.

Одним із методів, які базуються на моделюванні поведінки, є метод поєднання моделі зловживання з очевидними причинами [13].

Суть методу полягає у такому [4]: база даних сценаріїв атак містить послідовності поводжень, які становлять атаку. У будь-який момент часу існує можливість того, що в системі має місце одна з цих підмножин сценаріїв атак. Проводиться перевірка припущення про їх наявність шляхом пошуку інформації в записах аудиту. Результатом пошуку є певна кількість фактів, достатня для підтвердження або спростування гіпотези. Перевірка виконується в одному процесі – антисипаторі. Антисипатор, грунтуючись на поточній активній моделі, формує таку можливу множину поведінки, яку необхідно перевірити в записах ау-

диту, і передає їх планувальнику. Планувальник визначає, як прогнозована поведінка відображається в записах аудиту і трансформує їх у системний аудитозалежний вираз [14]. Структура цих виразів повинна бути простою для пошуку в записах аудиту і мати високу ймовірність появи в записах аудиту.

Зміна ймовірностей підозр на зловживання для сценаріїв – збільшення чи зменшення їх – приводить до зменшення списку моделей активностей. Обчислення причин вбудовано в систему й дозволяє оновлювати ймовірності виникнення сценаріїв атак у списку моделей активності.

До переваг методу слід віднести:

• можливість зменшення кількості обробок для одного запису аудиту за рахунок ранжування важливості подій і подальшої більш точної обробки подій з високою ймовірністю;

• забезпечення планувальником незалежності представлення від форми даних аудиту.

До недоліків:

• додаткове навантаження на особу, яка створює модель виявлення вторгнення, пов’язане з визначенням масиву змістовних і точних кількісних характеристик для різних частин графічного представлення моделі;

• відсутність оцінки ефективності такого підходу та програмного прототипу.

6. Недоліки існуючих систем виявлення вторгнень

До недоліків сучасних систем виявлення вторгнень можна віднести дві групи проблем: недоліки, пов’язані зі структурою СВВ, та недоліки реалізованих методів виявлення. Характеристика недоліків структур представлена в табл. 4.

Таблиця 4. Недоліки структур систем виявлення вторгнень

Проблема	Причина
Відсутність загальної методології побудови	Новий напрям дослідження. Недостатність загальних правил та понять формування термінології
Ефективність	Орієнтованість на виявлення всіх видів атак; суттєве споживання ресурсів; орієнтованість командних інтерпретаторів на власний набір правил; множина правил дозволяє тільки непрямі залежності послідовності зв'язків між подіями
Портативність	Орієнтованість СВВ для використання на конкретному обладнанні, для конкретних задач. Складність переорієнтації СВВ для роботи в інших системах і задачах
Можливості оновлення	Складність оновлення існуючих систем новими технологіями. Труднощі забезпечення взаємодії нових підсистем із всією системою
Установка СВВ	Необхідність додаткових навичок, знань нових експертних систем
Продуктивність і допоміжні тести	Складність оцінки продуктивності СВВ у реальних умовах. Відсутній набір правил для тестування СВВ, на основі яких оцінюється доцільність використання системи в заданих умовах
Тестування	Відсутність ефективних способів тестування

У роботі [4] приведені такі недоліки систем виявлення вторгнень:

• неприпустимо високий рівень похибок першого та другого роду;

• слабкі можливості щодо виявлення нових видів атак;

• неможливість виявлення більшості вторгнень на початкових етапах;

• надзвичайні складнощі з ідентифікацією мети атаки та атакуючого;
• відсутність оцінок точності та адекватності результатів роботи;
• неможливість виявлення відомих атак з новими стратегіями;
• складність виявлення вторгнень у режимі реального часу з необхідною повнотою в високошвидкісних мережах.

Крім вказаних недоліків, проблемою є також значне перевантаження систем, які використовують СВВ, в режимі реального часу та автоматизація процесу виявлення складних атак.

7. Висновки

У практичній площині накопичений значний досвід розв'язку проблем виявлення вторгнень. Системи виявлення вторгнень, які використовуються на сьогодні, значною мірою базуються на емпіричних схемах процесу виявлення вторгнень. Тому, проаналізувавши структури СВВ, методи, які використовуються, їх переваги та недоліки, можна зробити висновок, що подальші напрями розвитку СВВ пов'язані з впровадженням в теорію і практику методів та моделей загальної теорії систем, методів аналізу і синтезу інформаційних систем, деталізації апарату теорії розпізнавання образів тощо.

Так, наприклад, з точки зору теорії систем, СВВ не описана як підсистема інформаційної системи: не визначені елементи СВВ, її структура, зв'язки з інформаційною системою, не визначений узагальнюючий показник якості СВВ.

У зв'язку з наявністю значної кількості факторів різної природи, функціонування інформаційної системи та СВВ має ймовірнісний характер. Тому є актуальним обґрунтування ймовірнісних законів конкретних параметрів функціонування.

Окремо необхідно виділити завдання обґрунтування виду функції аномалій інформаційної системи, яка визначається у відповідності з її цільовою функцією і на області значень параметрів функціонування системи. Тобто, цільова функція повинна бути визначена не тільки на експертному рівні, але й відповідати сукупності параметрів функціонування всієї інформаційної системи та її задачам. Тоді за [4] узагальнюючий показник якості СВВ – це один із параметрів, який максимально впливає на цільову функцію, а його припустимі значення є припустимими значеннями функції аномальної поведінки.

На наступному етапі постає завдання отримання формалізованими методами оптимальної структури СВВ у вигляді сукупності математичних моделей (операцій), за допомогою яких стає можливим встановлення залежностей показників якості функціонування інформаційної системи від параметрів її функціонування.

Оскільки реальна інформаційна система та СВВ як її підсистема складаються із різнорідних елементів, саме цей факт викликає складність застосування до СВВ формалізованого апарату аналізу і синтезу інформаційних систем. Крім того, СВВ можуть бути описані різними розділами теорії систем, зокрема, системами масового обслуговування, кінцевими автоматами, теорією ймовірностей, теорією розпізнавання образів тощо. У такому випадку математичні моделі можна отримати тільки для окремих частин СВВ (об'єкт дослідження є агрегатним), що ускладнює аналіз і синтез СВВ в цілому. Саме подальша конкретизація використання формалізованого апарату аналізу і синтезу надасть змогу побудувати оптимальну СВВ як систему математичних моделей та її структури.

Подяка

Робота проведена та фінансована в рамках проекту HATO CyRADARS (Cyber Rapid Analysis for Defense Awareness of Real-time Situation – CyRADARS) – grant agreement number: G5286.

СПИСОК ДЖЕРЕЛ

1. Моделювання та аналіз безпеки розподілених інформаційних систем / В.В. Литвинов, В.В. Казимир, І.В. Стеценко [та ін.]. – Чернігів: Чернігівський національний технологічний університет, 2017. – 206 с.
2. Методи аналізу та моделювання безпеки розподілених інформаційних систем. Навчальний посібник / В.В. Литвинов, В.В. Казимир, І.В. Стеценко [та ін.]. – Чернігів: Чернігівський національний технологічний університет, 2016. – 254 с.
3. Denning D. An Intrusion Detection Model / D. Denning // IEEE Transactions on Software Engineering. – 1987. – Vol. SE-13, N I. – P. 222 – 232.
4. Корниенко А.А. Системы обнаружения вторжений: современное состояние и направления совершенствования [Электронный ресурс] / А.А. Корниенко, И.М. Слюсаренко. – Режим доступа: http://citforum.ru/security/internet/ids_overview.
5. Калініна І.В. Використання генетичних алгоритмів в задачах оптимізації / І.В. Калініна, О.І. Лісовиченко // Адаптивні системи автоматичного управління: міжвідомчий наук.-техн. зб. – 2015. – № 1 (26). – С. 48 – 61.
6. Next Generation Intrusion Detection Expert System (NIDES) / D. Anderson [et al] // Software Design, Product Specification and Version Description Document, Project 3131. – 1994. – July 11. – P. 1 – 94.
7. Модифікація методики вейвлет-аналізу для виявлення аномалій у трафіку комп'ютерної мережі / В.В. Литвинов, І.С. Скітер, О.В. Трунова [та ін.] // Технічні науки та технології. – 2017. – № 2 (8). – С. 99 – 109.
8. Мутилин В.С. Паттерны проектирования тестових сценариев / В.С. Мутилин // Труды Института системного программирования РАН. – 2009. – Т. 9. – С. 97 – 128.
9. Лаптев В.Н. Применение метода индуктивного прогнозирования состояний для обнаружения компьютерных атак в информационно-телекоммуникационных системах / В.Н. Лаптев, О.В. Сидельников, В.А. Шарай // Научный журнал КубГАУ. – 2011. – № 72 (08). – С. 3 – 13.
10. Ленков С.В. Методы и средства защиты информации / Ленков С.В., Перегудов Д.А., Хорошко В.А.; под ред. В.А. Хорошко. – К.: Арий, 2010. – Т. 1: Несанкционированное получение информации. – 464 с.
11. Ilgun K. State Transition Analysis: A Rule-Based Intrusion Detection System / K. Ilgun, R.A. Kemmerer, P.A. Porras // IEEE Trans. Software Eng. – 1995. – Vol. 21, N 3. – P. 181 – 199
12. Ilgun K. USTAT: A Real-time Intrusion Detection System for UNIX / Ilgun K. – Santa Barbara: University of California, 1992. – 224 p.
13. Борисов А.В. Использование симулятора ns-3 для моделирования поведения сетевых протоколов / А.В. Борисов, А.В. Карпухин, Л.И. Маркова // Вісник Харківського національного університету. – 2010. – № 926. – С. 53 – 59.
14. Кириченко Л.О. Алгоритм предупреждения перегрузки компьютерной сети путем прогнозирования средней длины очереди / Л.О. Кириченко, Т.А. Радивилова, А.В. Стороженко // Зб. наук. праць Харківського університету повітряних сил ім. І. Кожедуба. – 2007. – Вип. 3 (15). – С. 84 – 97.

Стаття надійшла до редакції 10.01.2018