УДК 004.056.53

Мамарєв В.М. (КОЦ ДКА України)

АНАЛІЗ СУЧАСНИХ МЕТОДІВ ВИЯВЛЕННЯ АТАК НА РЕСУРСИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

У статті розглянуто основні групи методів виявлення атак із врахуванням сучасних тенденцій їх розвитку. Висвітленні основні принципи, проведено аналіз ефективності функціонування згідно запропонованих критеріїв.

Ключові слова: методи виявлення аномалій, методи виявлення зловживань, нейронні мережі, імунні системи, сигатурні методи виявлення, кластерний аналіз, графи сценаріїв атак, MARS, SVM.

Вступ. Швидкий розвиток мереж і їх об'єднання в мережу Інтернет привів до зростання числа злочинів, пов'язаних з порушенням засадничих принципів інформаційної безпеки. Незважаючи на розвиток систем виявлення атак (СВА), кількість вторгнень в інформаційно-телекомунікаційні системи (ІТС) компаній та установ зростає з кожним роком. Статистика вторгнень свідчить, що сучасні комерційні СВА не дозволяють досягти оптимальних характеристик виявлення атак.

Аналіз останніх досліджень і публікацій [1-5] показав, що основним недоліком переважної кількості сучасних комерційних СВА є низька, близька до нуля, ефективність виявлення невідомих атак [1-3]. Більшість сучасних СВА використовують на базовому рівні ту чи іншу реалізацію сигнатурного методу виявлення. Реалізації відрізняються рівнем розгляду системи, алфавітом сигнатур і «движком», що використовується. За минулі роки в рамках академічних розробок були створені десятки СВА для різних платформ: від систем класу mainframe до сучасних операційних систем загального призначення, СУБД і поширених додатків [1, 2, 4, 5], але в промислових системах вони майже не використовуються, оскільки мають принципові обмеження, пов'язані з вимогами верифікованості, стійкості, складності обчислювальних алгоритмів і великим числом помилок другого роду.

Мета статті полягає в аналізі методів виявлення атак та вибору методу, що дозволив би досягти достатнього рівня надійності виявлення атак при мінімальному значенні помилок першого і другого роду.

Основна частина

На сьогоднішній день «ідеальна» СВА повинна задовольняти наступним вимогам:

- повнота системи (покриває всі види атак);
- глобальність спостереження за системою (аналізує поведінку ІТС на всіх рівнях);
- адаптивність (використовує адаптивний метод виявлення);
- масштабованість;
- відкритість;
- наявність вбудованих механізмів реагування на атаки;
- захищеність від атак на власні компоненти.

Однак на даному етапі розвитку «реальні» СВА не можуть повною мірою задовольнити перераховані вище вимоги. Їх реалізація пов’язана з певними обмеженнями, що зумовлені використанням конкретних методів виявлення атак. Вибір методу виявлення має ґрунтуватися на основі детального розгляду вимог до системи. Для порівняльного аналізу методів виявлення атак виберемо наступні критерії: рівень спостереження за системою, верифікованість, стійкість, адаптивність і обчислювальна складність. Зважаючи на відсутність в публікаціях детальної інформації про повноту і точність методу, до переліку критеріїв, що розглядаються, останні включатись не будуть.

Розглянемо перераховані критерії більш детально.

Рівень спостереження за системою. Цей критерій визначає рівень абстракції подій, що аналізуються в системі і визначає межі застосовності методу для виявлення атак в мережах. У рамках даної статті розглядатимуться такі рівні:

- HIDS - спостереження на рівні операційної системи окремого вузла мережі;
- NIDS - спостереження на рівні мережної взаємодії об'єктів на вузлах мережі;
- AIDS - спостереження на рівні окремих додатків вузла мережі;
- Hybrid - комбінація спостережень різних рівнів.

Верифікованість методу. Дозволяє провести експертну оцінку коректності методу та його реалізації у довільний момент часу, в тому числі в процесі експлуатації системи виявлення на його основі. Властивість веріфікованості методу важлива (в якості засобу збору доказової бази про атаки) при експлуатації системи виявлення атак в реальній обстановці. Можливі значення: висока (В), низька (Н).

Стійкість. Цей критерій характеризує незалежність виходу методу від системи, що підлягає захисту - для одного і того ж входу метод повинен давати один і той же вихід, незалежно від системи, що підлягає захисту. Проблема стійкості особливо гостро стоїть для статистичних методів, які аналізують абсолютні значення параметрів продуктивності та завантаженості ресурсів мережі та вузлів, які можуть істотно відрізнятися на різних вузлах і в різних мережах. Методи виявлення атак, що аналізують семантику введення, більш стійкі, ніж статистичні. Локальною будемо називати стійкість що забезпечується в межах системи де проводилось навчання і відсутня у всіх інших мережах. Так як процедура навчання зазвичай вимагає використання великої кількості ресурсів і часу - кількість процедур навчання бажано мінімізувати. Можливі значення: глобальна (Г), локальна (Л).

Адаптивність методу. Критерій дозволяє провести оцінку стійкості методу до незначних змін її реалізації, які не змінюють результат атаки. Адаптивність є єдиною суттєвою перевагою «альтернативних» методів виявлення атак перед «сигнатурними». Відсутність адаптивності не дозволяє системі захисту оперативно реагувати на невідомі атаки і вимагає організації системи регулярного оновлення баз відомих атак, за аналогією з антивірусними системами. Можливі значення: висока (В), низька (Н).

Обчислювальна складність. При розгляді даного критерію обмежемося розглядом тільки складності методу в режимі виявлення, без урахування можливих попередніх етапів налаштування і навчання.

Із перерахованих вище критеріїв ключовими, з огляду на вимоги до «ідеальної» СВА, слід вважати можливість застосування методу для виявлення аномалій та зловживань, адаптивність і рівень спостереження за системою. Вибір саме цих критеріїв обумовлений наступними умовами:

- необхідність використання методу, що гарантує ідентифікацію всіх порушень безпеки;
- необхідність виявлення «старих» і «нових» реалізацій атак;
- необхідність застосування методу на різних рівнях спостереження за системою.

У роботі [6] виділяються два класи методів виявлення атак: методи виявлення аномалій і методи виявлення зловживань. Спираючись на запропоновані критерії проведемо аналіз кожного із класів.

Методи виявлення аномалій базуються на наявності готового опису нормальної поведінки об'єктів, що спостерігаються, і будь-яке відхилення від нормальної поведінки вважається аномальним (порушенням). Загальний алгоритм роботи методів виявлення аномалій представлено на рис. 1.

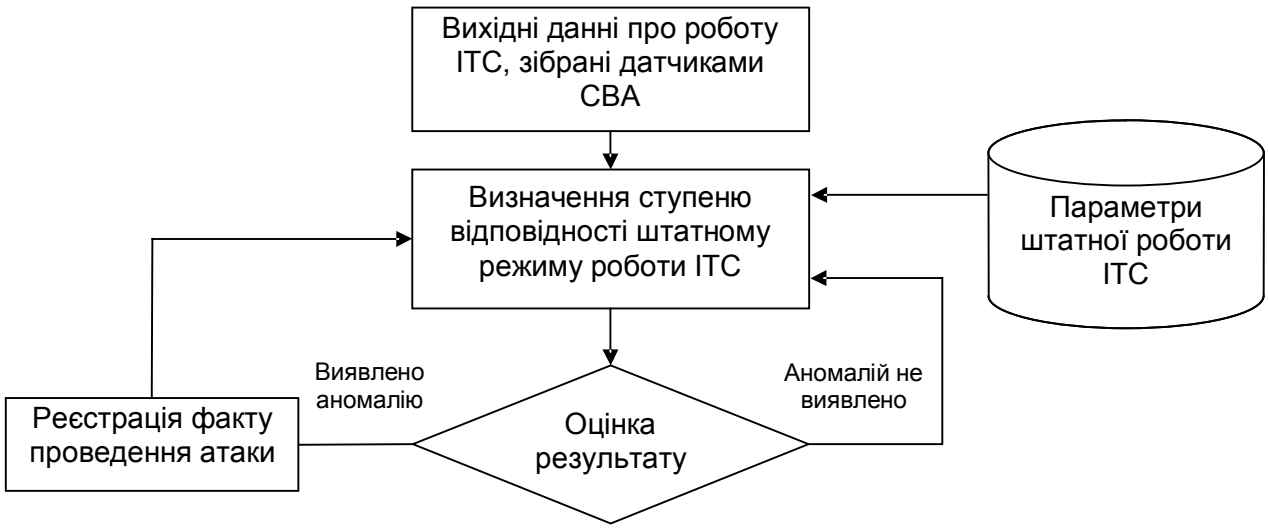

Рис.1. Загальний алгоритм роботи методів виявлення аномалій

Аналіз систем переходів. Даною групою методів [7] функціонування системи, що підлягає захисту, представляється через множину станів і множину переходів між ними, тобто у вигляді орієнтованого графа (як правило, нескінченного). Суть методу виявлення атак полягає в тому, що частина шляхів у такому графі позначаються як неприпустимі; кінцевий стан кожного такого шляху вважається небезпечним для системи, що підлягає захисту. Процес виявлення атаки представляє собою побудову частини графа станів системи, переходів між ними і пошук в отриманому графі відомих неприпустимих шляхів. Виявлення послідовності переходів, що приводить в небезпечний стан, означає успішне виявлення атаки. Відповідно до введених критеріїв, дані методи є гібридними з точки зору рівня спостереження за системою, верифікованими, стійкими, мають низьку обчислювальну складність (лінійну щодо довжини траси переходів, що спостерігаються, і числа станів), але не є адаптивними.

Графи сценаріїв атак. У роботі [8] запропоновано підхід до виявлення атак на основі використання методів формальної специфікації на моделях. На вхід системи верифікації подається кінцева модель системи, що підлягає захисту і деяка формальна властивість коректності, яка виконується тільки для дозволеної поведінки системи. Дана властивість коректності ділить всю множину поведінок на два класи - припустимі поведінки, для яких властивість виконується, і неприпустимі, для яких вона не виконується. Відмінність цього методу від звичайних систем верифікації полягає в тому, що їх завдання, зазвичай, знайти один контрприклад з безлічі неприпустимих поведінок, а в запропонованому методі будується повний набір таких прикладів для конкретної системи, що підлягає захисту, що дає на виході опис можливих шляхів атаки. Через високу обчислювальну складність (NP) даний метод може бути використаний для пошуку вразливостей при проектуванні систем та інших складних для виявлення вразливостей, але для задачі виявлення атак в реальному часі він непридатний. За іншими критеріями метод є гібридним, верифікованим, стійким і адаптивним.

Нейронні мережі. Так як задачу виявлення атак можна розглядати як задачу розпізнавання образів (або задачу класифікації), то для її вирішення також застосовуються нейронні мережі [9]. Для цього функціонування системи, що підлягає захисту, та зовнішніх об'єктів, що взаємодіють з нею, представляється у вигляді траєкторій у деякому числовому просторі ознак. В якості методу виявлення зловживань нейронні мережі навчаються на прикладах атак кожного класу і надалі використовуються для розпізнавання приналежності поведінки одному з класів атак. Основна складність у використанні нейронних мереж полягає в коректній побудові такого простору ознак, який дозволив би розділити класи атак

між собою і відокремити їх від нормальної поведінки. Крім того, для класичних нейронних мереж характерним є тривале навчання, при цьому час навчання залежить від розміру навчальної вибірки. Відповідно до введених критеріїв, нейронні мережі використовуються на мережному і вузловому рівнях, є адаптивними, мають порівняно низьку обчислювальну складність. При цьому вони не є верифікованими і, як правило, локально стійкими, що істотно обмежує можливість застосування методу.

Імунні мережі. Зазначений метод є механізмом класифікації і будується за аналогією з імунною системою живого організму. Основна перевага імунних мереж полягає у можливості отримання «антитіл» до невідомих атак [10]. У роботі [11] запропоновано модель формального пептиду, для якої заявлена можливість використання в системах виявлення атак. Відповідно до введених критеріїв, дана група методів може бути застосовна для мережевого і вузлового рівнів, не верифікована, адаптивна, стійка тільки локально, має середню обчислювальну складність.

Support vector machines (SVM). Метод подання та розпізнання шаблонів, який дозволяє формувати шаблони в результаті навчання [12]. Даний метод вимагає невеликої кількості даних для навчання і дозволяє обробляти вектори ознак великої розмірності, що корисно для підвищення точності СВА і зниження часових затрат на навчання і перенавчання. Метод застосовується як для виявлення зловживань, так і для виявлення аномалій. SVM має такі ж переваги і недоліки для рішення задачі виявлення зловживань, як і нейронні мережі, тобто є адаптивним, але неверіфікованим.

Експертні системи. Використання експертних систем для виявлення атак базується на описі функціонування системи у вигляді безлічі фактів і правил виведення, в тому числі для атак [13]. На вхід експертна система отримує дані про події в системі у вигляді фактів. На підставі фактів і правил виводу система робить висновок про наявність чи відсутність атаки. Дана група методів задовольняє практично всім критеріям (верифікована, адаптивна, стійка), але в загальному випадку має дуже велику обчислювальну складність, так як для неї може спостерігатися явище «комбінаторного вибуху» і повного перебору великої кількості альтернатив.

Методи, засновані на специфікаціях. В основі цього методу лежить опис обмежень на заборонену поведінку об'єктів в системі, що захищається у вигляді специфікацій атак [14]. У специфікацію може входити: обмеження на завантаження ресурсів, на список заборонених операцій та їх послідовностей, на час доби, протягом якого застосовуються ті чи інші обмеження. Невідповідність поведінки специфікації вважається атакою. Специфікації використовуються для мережного рівня, є верифікованими, локально стійкими і мають низьку обчислювальну складність. Даний підхід близький до класу методів виявлення аномалій. Основні недоліки - низька адаптивність і складність розробки специфікацій.

Multivariate Adaptive Regression Splines (MARS). Один з методів апроксимації функцій, заснований на сплайнах [15]. Аналогічно нейронним мережам та кластерному аналізу MARS оперує в багатовимірному просторі ознак. Поведінка мережевих об'єктів відображається в послідовності векторів цього простору. Завдання процедури MARS полягає в побудові оптимальної апроксимації поведінки за заданою історією у вигляді навчальної множини векторів, при цьому в якості апроксимуючої функції використовуються сплайни зі змінним числом вершин. У ході «навчання», за допомогою переборного процесу, вибирається оптимальне число вершин для заданої вибірки. Побудований сплайн є «шаблоном» атаки. У режимі розпізнавання поведінка, що спостерігається, відображається в параметричний простір і порівнюється з апроксимуючою функцією. Переваги і недоліки даного методу аналогічні методам SVM і нейронних мереж.

Сигнатурні методи. Група методів, суть яких полягає у складанні певного алфавіту з подій в системі і описі множини сигнатур атак у вигляді регулярних виразів (у загальному випадку) у складеному алфавіті [16]. Як правило, сигнатурні методи працюють на найнижчому рівні абстракції і аналізують безпосередньо передані мережею дані, параметри

системних викликів і записи файлів журналів. У найбільш розвиненому вигляді являє собою реалізацію регулярних виразів над різними трасами (мережевий трафік, системні виклики, записи журналів додатків і т.п.). Сигнатурні методи відрізняються тим, що до них легко застосовуються апаратні прискорювачі, але при цьому метод не є адаптивним. За іншими критеріями дана група методів є гібридною, глобально стійкою, не верифікованою.

Методи виявлення зловживань базуються на описі відомих (сигнатур) порушень або атак: якщо поведінка деякого об'єкта, що спостерігається співпадає з описом відомої атаки, поведінка об'єкта вважається атакою. Загальний алгоритм роботи методів виявлення зловживань представлено на рис. 2.

Статистичний аналіз. Дана група методів базується на побудові статистичного профілю поведінки системи протягом періоду «навчання», при якому поведінка системи вважається нормальною [17]. Для кожного параметра функціонування системи будується інтервал допустимих значень, з використанням деякого відомого закону розподілу. Далі, в режимі виявлення, система оцінює відхилення значень, що спостерігаються від значень, отриманих під час навчання. Якщо відхилення перевищують визначені межі допустимих значень, то фіксується факт аномалії (атаки). Для статистичного аналізу характерний високий рівень помилок другого роду при використанні в локальних мережах, де поведінка об'єктів не має усередненого характеру. Даний метод є локально стійким, тобто побудовані статистичні профілі не можна використовувати на інших аналогічних системах. Не дає можливості верифікації результатів виявлення. Задовільняє умові адаптивності.

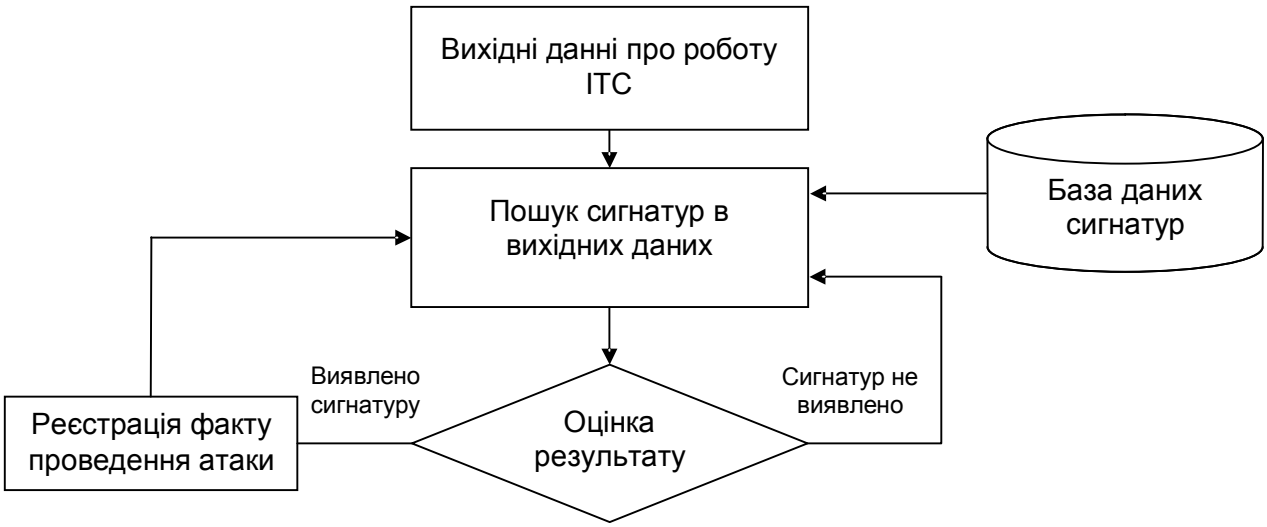

Рис. 2. Загальний алгоритм роботи методів виявлення зловживань

Кластерний аналіз. Алгоритм функціонування даної групи методів полягає в розбитті множини векторів-властивостей системи, що спостерігається, на кластери, серед яких виділяють кластери нормальної поведінки [18]. У кожному конкретному методі кластерного аналізу використовується своя метрика, яка дозволяє оцінювати приналежність вектора властивостей системи, що спостерігається, до одного з кластерів або вихід за межі відомих кластерів. Кластерний аналіз є адаптивним, але не верифікованим, стійким в межах конкретної системи, в якій збиралися дані для побудови кластерів.

Нейронні мережі. Нейронні мережі для виявлення аномалій навчаються протягом деякого періоду часу, доки вся поведінка, що спостерігається, вважається нормальною. [9]. Після навчання нейронна мережа запускається в режимі розпізнавання. У ситуації, коли у вхідному потоці не вдається розпізнати нормальну поведінку, фіксується факт атаки. У разі використання репрезентативної навчальної вибірки нейронні мережі дають хорошу стійкість в межах заданої системи; але складання подібної вибірки є серйозним і складним завданням.

Класичні нейронні мережі мають високу обчислювальну складність навчання, що ускладнює їх застосування на великих потоках даних. За іншими критеріями нейронні мережі є адаптивними, не верифікованими, локально стійкими.

Імунні мережі. Виявлення аномалій є одним з можливих застосувань імунних мереж [10]. Так само, як і нейронні мережі вони базуються на біологічній моделі імунної системи людини. За допомогою алгоритму т.з. "негативного відбору" виявлювач на їх базі може бути навчений класифікувати процеси, що відбуваються в ІТС як штатні події або атаки. Класифікатори на базі імунних мереж є не верифікованими, локально стійкими, адаптивними і мають середню обчислювальну складність.

Експертні системи: Інформація про нормальну поведінку для подібних систем представляється у вигляді правил, а поведінка, що спостерігається, у вигляді фактів. На підставі фактів і правил приймається рішення про відповідність поведінки, що спостерігається, «нормальній», або про наявність зловживань. Головний недолік подібних систем - висока обчислювальна складність (у загальному випадку). У тому числі при виявленні аномалій [13].

Поведінкова біометрія. Включає в себе методи, які не потребують спеціального обладнання (сканерів сітківки, відбитків пальців), тобто методи виявлення атак, засновані на спостереженні клавіатурного почерку та використання миші. В основі методів лежить гіпотеза про відмінність «почерку» роботи з інтерфейсами введення-виведення для різних користувачів. На базі побудованого профілю нормальної поведінки для даного користувача виявляються відхилення від цього профілю, викликані спробами інших осіб працювати з клавіатурою або іншими фізичними пристроями введення. Поведінкова біометрія має тільки локальну стійкість, є адаптивною і слабо верифікованою [19].

Support vector machines (SVM). SVM застосується як для виявлення зловживань, так і для виявлення аномалій, при цьому метод має переваги і недоліки, аналогічні нейронним мережам [12].

Узагальнення результатів аналізу методів виявлення атак наведені в табл. 1.

Результати порівняння методів виявлення атак Таблиця 1

Критерій / Метод	Рівень спостереження	Аномалії/ Зловживання	Верифікованість	Адаптивність	Стійкість	Обчислювальна складність
Системи переходів	Hybrid	-/+	В	Н	Г	O(n)
Графи атак	Hybrid	-/+	В	В	Г	Np
Нейронні мережі	NIDS, HIDS	+/+	Н	В	Л	O(n) і вище
Імунні мережі	NIDS, HIDS	+/+	Н	В	Л	O(n)
SVM	NIDS, HIDS	+/+	Н	В	Л	Ln(n)
Експертні системи	NIDS, HIDS	+/+	В	В	Г	У загальному випадку Np
Специфікації	NIDS	-/+	В	Н	Л	Ln(n)
MARS	NIDS, HIDS	-/+	Н	В	Л	O(n) і вище
Сигнатурні	Hybrid	-/+	В	Н	Г	Ln(n)
Статистичні	NIDS, HIDS	+/+	Н	В	Л	O(n) і вище
Кластерний аналіз	Hybrid	+/+	Н	В	Л	O(n) і вище
Поведінкова біометрія	HIDS	+/-	Н	В	Л	O(n) і вище

Проведений аналіз показав, що для більшості методів виявлення атак характерна слабка верифікованість і низька глобальна стійкість. Серед методів з низькою обчислювальною складністю, таких що задовольняють умовам глобальної стійкості і верифікованості, слід відмітити простий сигнатурний метод і метод аналізу систем переходів. Однак жоден з них не задовольняє умові адаптивності, крім того не може бути застосованим для виявлення аномалій. Метод імунних мереж дає можливість отримання «антитіл» до невідомих атак, може бути використаним як для виявлення аномалій та і зловживань, забезпечує спостереження на рівнях NIDS та HIDS і має відносно низьку обчислювальну складність.

Висновки. Статистика втручань в ІТС засвідчує низьку ефективність методів, що реалізовані в сучасних комерційних СВА, тому виникає необхідність вибору методу, що дозволив би досягти достатнього рівня надійності виявлення атак при мінімальному значенні помилок першого і другого роду і принаймі середній обчислювальній складності.

Аналіз доводить що досить перспективною є побудова СВА на основі технології імунних мереж. Цей метод має низку переваг у порівнянні з іншими, а також забезпечує: високу швидкість роботи, порівняно простий алгоритм навчання, досить низьку ресурсоємність.

Література

1. Stefan Axelsson Research in Intrusion-Detection Systems: A Survey // Department of Computer Engineering, Chalmers University of Technology, Goteborg. – 1999.

2. Stefan Axelsson Intrusion detection systems: A survey and taxonomy // Technical Report 99-15, Chalmers University of Technology, Goteborg. - 2000.

3. Смелянский Р.Л., Гамаюнов Д. Ю. Современные некоммерческие средства обнаружения атак // Факультет Вычислительной Математики и Кибернетики, МГУ им. М. В. Ломоносова, Москва. - 2002.

4. Hakan Kvarnstrom A survey of commercial tools for intrusion detection // Technical Report 99-8, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden. - 1999.

5. Tomas Lunt Automated Audit Trail Analysis and Intrusion Detection: A Survey // Proceedings of the 11th National Security Conference, Baltimore, MD. - 1988.

6. Сердюк В. А. Новое в защите от взлома корпоративных систем.- Москва: Техносфера, 2007.- 360 с.

7. An Attack Language for State-based Intrusion Detection / S.T. Eckmann, G. Vigna, and R. A. Kemmerer // Dept. of Computer Science, University of California, Santa Barbara. - 2000.

8. Sheyner Oleg Scenario Graphs and Attack Graphs // PhD thesis, SCS, Carnegie Mellon University. - 2004.

9. Смелянский Р.Л., Качалин А.И. Применения нейросетей для обнаружения аномального поведения объектов в компьютерных сетях // Факультет Вычислительной Математики и Кибернетики, МГУ им. М. В. Ломоносова, Москва. - 2004.

10. S.A. Hofmeyr An immunological model of distributed detection and its application to computer security // Ph.D. thesis, University of New Mexico. - 1999.

11. M.P.Zielinski Applying Mobile Agents in an Immune-system-based intrusion detection system // University of South Africa. - 2004.

12. Srinivas Mukkamala, Andrew H. Sung, Ajith Abraham Intrusion detection using an ensemble of intelligent paradigms // Journal of Network and Computer Applications. - 2005.

13. R.A. Whitehurst Expert Systems in Intrusion Detection: A Case Study //Computer Science Laboratory, SRI International, Menlo Park, CA. - 1987.

14. Calvin Ko Execution Monitoring of Security-critical Programs in a Distributed System: A Specification-based Approach // PhD thesis, Department of Computer Science, University of California at Davis, USA. - 1996.

15. S. Smaha Haystack: an intrusion detection system // 4th Aerospace Computer Security Applications Conf. - 1988. - pp. 37–44.

16. Sandeep Kumar and Eugene H. Spafford An application of pattern matching in intrusion detection // Technical Report CSD-TR-94-013, The COAST Project, Dept. of Computer Sciences, Purdue University, West Lafayette, IN, USA. - 1994.

17. Detecting unusual program behavior using the statistical component of the next generation intrusion detection system (NIDES) / Debra Anderson, Teresa F. Lunt, Harold Javitz, Ann Tamaru, and Alfonso Valdes // Technical Report SRI-CSL-95-06, Computer Science Laboratory, SRI International, Menlo Park, CA, USA. - 1995.

18. Architecture design of a scalable intrusion detection system for the emerging network infrastructure / Y. Frank Jou, Fengmin Gong, Chandru Sargor // Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University, Releigh, N.C, USA. - 1997.

19. Ahmed Awad E. Ahmed, Issa Traore Anomaly Intrusion Detection based on Biometrics // Proceedings of the 2005 IEEE, Workshop on Information Assurance, United States Military Academy, West Point, NY. - 2005.

Надійшла: 27.05.2011 р.

Рецензент: д.т.н., проф. Кузнецов Г.В.