УДК 004.056.5

І.В. Рубан, В.О. Мартовицький, С.О. Партика

Харківський національний університет радіоелектроніки, Харків

КЛАСИФІКАЦІЯ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

В статті запропоновані підходи, щодо класифікації методів виявлення аномалій в сучасних системах виявлення атак. Розглянуті та проаналізовані найпоширеніші групи методів виявлення аномалій. Показано, що методи виявлення аномалій в сучасних системах виявлення атак недостатньо опрацьовані в частині формальної моделі атаки, а, отже, для них досить складно суворо оцінити такі властивості як обчислювальна складність, коректність, завершеність.

Ключові слова: *IDS, кластерний аналіз, експертні системи, нейронні мережі, SVM.*

Вступ

Методи виявлення атак в сучасних системах виявлення атак недостатньо опрацьовані в частині формальної моделі атаки, а, отже, для них досить складно суворо оцінити такі властивості як обчислювальна складність, коректність, завершеність тощо [1 – 5].

Прийнято розділяти методи виявлення атак на методи виявлення аномалій і методи виявлення зловживань [6]. До другого типу методів відносяться більшість сучасних комерційних систем (Cisco IPS, ISS, RealSecure, NFR) – вони використовують сигнатурні (експертні) методи виявлення [1, 4].

Існує безліч академічних розробок в області виявлення аномалій, але в промислових системах вони використовуються рідко і з великою обережністю, так як такі системи породжують велику кількість помилкових спрацьовувань.

Основна частина

Методи виявлення аномалій можна класифікувати за різними критеріями, котрі представлені на рис. 1.

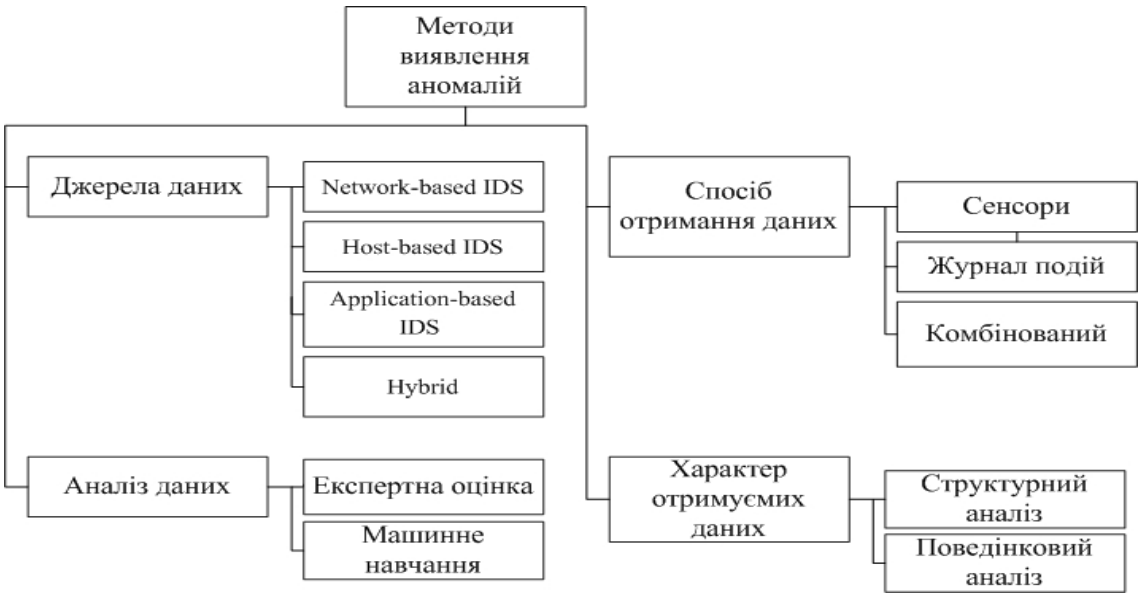

Рис. 1. Класифікація методів виявлення аномалій

Для порівняльного аналізу методів виявлення атак були обрані критерії які часто наводяться в літературі:

Джерела даних: Цей критерій визначає рівень абстракції аналізованих подій в захищуваних системах і визначає межі застосовності методу для виявлення атак в мережах. В рамках даного огляду розглядаються наступні рівні:

- Рівень мережі (Network-based IDS) – спостереження на рівні мережевої взаємодії об'єктів на вузлах мережі; NIDS визначають атаки, захоплюючи і аналізуючи мережеві пакети. Слухаючи мережевий сегмент, може переглядати мережевий трафік від кількох хостів, які приєднані до мережевого сегменту, і таким чином захищати ці хости. Часто складаються з безлічі сенсорів, розташованих у різних точ-

ках мережі. Ці пристрої переглядають мережний трафік, виконуючи локальний аналіз даного трафіку і створюючи звіти про атаки для центральної керуючої консолі. Багато з цих сенсорів розроблені для виконання в "невидимому" режимі, щоб зробити більш важким для атакуючого виявлення їх присутності і розташування[6].

Переваги network-based IDS:

– Кілька оптимально розташованих NIDS можуть переглядати велику мережу.

– Розгортання не робить великого впливу на продуктивність мережі. NIDS зазвичай є пасивними пристроями, які прослуховують мережевий канал без впливу на нормальне функціонування мережі. Таким чином, зазвичай буває легко модифікувати топологію мережі для розміщення NIDS.

– Можуть бути зроблені практично невразливими для атак або навіть абсолютно невидимими для атакуючих.

Недоліки network-based IDS:

– Важко обробляти всі пакети в великий або зайнятої мережі, а, отже, вони можуть пропустити розпізнавання атаки, яка почалася при великому трафіку.

– Багато переваг NIDS незастосовні до більш сучасним мереж, заснованим на мережевих комутаторах (switch). Комутатори ділять мережі на багато маленьких сегментів і забезпечують виділені лінії між хостами. Більшість комутаторів не надають універсального моніторингу портів.

– Не можуть аналізувати зашифровану інформацію.

– Більшість NIDS не можуть сказати, чи була атака успішною; вони можуть лише визначити, що атака була почата.

– Деякі NIDS мають проблеми з визначенням мережевих атак, які включають фрагментовані пакети. Такі фрагментовані пакети можуть призвести до того, що IDS буде функціонувати нестабільно.

- Рівень Хоста (Host-based IDS) – спостереження на рівні операційної системи окремого вузла мережі; HIDS мають справу з інформацією, зібраною всередині єдиного комп'ютера. Таке вигідне розташування дозволяє HIDS аналізувати діяльність з великою вірогідністю і точністю, визначаючи тільки ті процеси і користувачів, які мають відношення до конкретної атаці в ОС. Більш того, HIDS можуть "бачити" наслідки розпочатої атаки, так як вони можуть мати безпосередній доступ до системної інформації, файлів даних і системним процесам, які є метою атаки. HIDS зазвичай використовують інформаційні джерела двох типів: результати аудиту ОС і системні логи. Деякі HIDS розроблені для підтримки централізованої інфраструктури управління і отримання звітів IDS, що може допускати єдину консоль управління для відстеження багатьох хостів. Інші створюють повідомлення у форматі, який сумісний з системами мережного управління [6].

Переваги host-based IDS:

– Можливість стежити за подіями локально щодо хоста, що дає можливість визначити атаки, які не можуть бачити network-based IDS.

– Можуть функціонувати в оточенні, в якому мережевий трафік зашифрований, коли host-based джерела інформації створюються до того, як дані шифруються, і/або після того, як дані розшифровуються на хосту призначення.

– На їхнє функціонування не впливає наявність у мережі комутаторів.

– Працюють з результатами аудиту ОС, вони можуть надати допомогу у визначенні цілісності.

Недоліки host-based IDS:

– Більш складні в управлінні, так як інформація повинна бути налаштована і управлятися для кожного відкритому хості.

– Так як HIDS розташовані на тому ж хості, який є метою атаки, то, як складова частина атаки, IDS може бути атакована і заборонена.

– Не можливість виявити атаку, коли метою є вся мережа, так як вона спостерігає тільки за мережевими пакетами, одержуваними конкретним хостом.

– Можуть бути блоковані окремими DoS-атаками.

– Коли використовує результати аудиту ОС в якості джерела інформації, кількість інформації може бути величезна, що зажадає додаткового локального зберігання в системі.

– Використовують обчислювальні ресурси хостів, за якими вони спостерігають, що впливає на продуктивність спостережуваної системи.

- Рівень додатків (Application-based IDS) – спостереження на рівні окремих додатків вузла мережі; Є спеціальним підмножиною host-based IDS, які аналізують події, що надійшли до додатка. Найбільш загальними джерелами інформації, використовуваними AIDS, є лог-файли транзакцій програми. Здатність взаємодіяти безпосередньо з додатком, з конкретним доменом або використовувати знання, специфічні для програми, дозволяє визначати підозрілу поведінку авторизованих користувачів, що перевищує їх права доступу. Такі проблеми можуть проявитися тільки при взаємодії користувача з додатком[6].

Переваги Application-based IDS:

– Можуть аналізувати взаємодію між користувачем і програмою, що часто дозволяє відстежити неавторизовану діяльність конкретного користувача.

– Можуть працювати в зашифрованих оточеннях, так як вони взаємодіють з додатком в кінцевій точці транзакції, де інформація представлена вже в незашифрованому вигляді.

Недоліки application-based IDS:

– AIDS можуть бути більш вразливі, ніж host-based IDS, для атак на логи додатків, які можуть бути не так добре захищені, як результати аудиту ОС, що використовуються host-based IDS.

– AIDS часто переглядають події на користувальницькому рівні абстракції, на якому зазвичай неможливо визначити порушенням цілісності.

- Гібридний рівень – комбінація спостерігачів різних рівнів. Ця система поєднує позитивні функції обох моделей виявлення проникнення, щоб досягти більш високої точності виявлення, більш низьких помилкових спрацьовувань, таким чином, підвищеного рівня кібернетичної надійності.

Аналіз даних: Даний критерій визначає спосіб аналізу отриманих даних для подальшої роботи методу.

Експертна оцінка базується на основі думок експертів будується адекватна модель майбутнього розвитку об'єкта прогнозування.

Машине навчання навчається на прикладах і після закінчення фази навчання може узагальнювати, тобто не просто вивчає наведені приклади, а розпізнає певні закономірності в даних для навчання.

Спосіб отримання даних: Цей критерій визначає методи та засоби за допомогою, яких методи виявлення аномалій отримують дані для подальшого аналізу.

Сенсори розміщуються у різних точках системи. Ці пристрої переглядають дані, які проходять через них і створюють звіти про атаки для центральної керуючої консолі.

Журнал подій стандартний спосіб для додатків і операційної системи запису і централізованого зберігання інформації про важливі програмні і апаратних події. Служба журналів подій зберігає події від різних джерел в єдиному журналі подій, програма перегляду подій дозволяє користувачеві спостерігати за журналом подій, програмний інтерфейс (API) дозволяє додаткам записувати в журнал інформацію і переглядати існуючі записи.

Характер отриманих даних: Даний критерій характеризує отримані дані за їх виглядом.

Структурний аналіз полягає в дослідженні елементів кожного об’єкта та їхніх зв'язків. Мета структурного аналізу — визначення певної послідовності елементів як цілісний об’єкт, елементи і частини якої співвіднесені й пов'язані строгими зв'язками.

Технологія аналізу поведінки ґрунтується на перехопленні всіх важливих системних функцій або установці міні-фільтрів, що дозволяє відстежувати всю активність в системі користувача. Технологія поведінкового аналізу дозволяє оцінювати не тільки одиничну дію, але і ланцюжок дій, що багаторазово підвищує ефективність протидії вірусним загрозам. Також, поведінковий аналіз є технологічною основою для цілого класу програм - поведінкових блокувань (HIPS - Host-based Intrusion Systems)

Далі в статті будуть розглянуті конкретні групи методів виявлення аномалій.

Статистичний метод:

Дана група методів заснована на побудові статистичного профілю поведінки системи протягом деякого періоду «навчання», при якому поведінка системи вважається нормальним [8, 9]. Для кожного параметра функціонування системи будується інтервал допустимих значень, з використанням деякого відомого закону розподілу. Далі, в режимі виявлення, система оцінює відхилення спостережуваних значень від значень, отриманих під час навчання. Якщо відхилення перевищують деякі задані значення, то фіксується факт аномалії (атаки).

Прикладом таких методів може бути інтервальний метод. З цією метою розбиваємо область можливих значень величини X(потік подій) на B частин де, для вибіркового середнього ознакою аномалії будемо вважати перевищення заданого порогу при відхиленні величини від її середнього значення. Докладно приклад розглядається в статті [10].

В наступному приклад використовується статистика характеристики подій X^2. Величина X^2 підкоряється відомому розподілу X^2 – розподілу з (B-1) ступенями свободи, де B – число подій в потоці. У такому випадки ознакою появи аномалії будемо вважати перевищення величиною X^2 встановленого порогового значення.

З усього цього випливає, що для статистичного аналізу характерний високий рівень помилкових спрацьовувань при використанні в локальних мережах, де поведінка об'єктів не має гладкого, усередненого характеру. Крім того, даний метод стійкий тільки в межах конкретної системи, тобто побудовані статистичні профілі можна використовувати на інших аналогічних системах.

Кластерний аналіз:

Суть даної групи методів полягає в розбитті безлічі спостережуваних векторів-властивостей системи на кластери, серед яких виділяють кластери нормального поведінки [11]. У кожному конкретному методі кластерного аналізу використовується своя метрика, яка дозволяє оцінювати приналежність спостережуваного вектора властивостей системи одному з кластерів або вихід за межі відомих кластерів.

Згідно [12], методи кластерного аналізу можна розділити на 3 класи:

– ієрархічні методи,

– методи розбиття,

– комбіновані методи.

Результатом роботи ієрархічного методу є ієрархія кластерів (таксономія). Самі кластери мо-

жуть бути отримані шляхом розбиття дерева на основі певного критерію.

Результатом роботи алгоритму, заснованого на методі розділення, є безліч кластерів, не пов'язаних між собою певною ієрархією.

Комбіновані методи використовують ієрархічні методи, і методи розбиття. Найбільш часто використовується послідовно спочатку метод розбиття, а потім будується ієрархія на підставі отриманих кластерів (наприклад, [20, 18]). Даний алгоритм є найкращім з даної групи за рахунок двоступеневої кластеризації великих обсягів даних, що працює на обмеженому обсязі пам'яті, є локальним алгоритмом.

Перевагою даної групи методів є те, що він є адаптивним. Недоліком є сильна залежність результату від вибору кількості кластерів і початкового розташування кластерів.

Нейронні мережі:

Нейронні мережі для виявлення аномалій навчаються протягом деякого періоду часу, коли вся поведінка вважається нормальною[13]. Після навчання нейронна мережа запускається в режимі розпізнавання. У ситуації, коли у вхідному потоці не вдається розпізнати нормальна поведінка, фіксується факт атаки.

Нейромережевий підхід вирішення цих завдань полягає в послідовному об'єднанні двох різних нейронних мереж який детально розглянуто у статті [14]. В якості вхідних даних використовуються параметри мережного з'єднання. Кожне мережеве з'єднання характеризується 41-ним параметром мережевого трафіка. В якості вихідних даних використовується 5-мірний вектор, де 5-кількість класів атак плюс нормальний стан.

На першому етапі обробки вхідної інформації відбувається зменшення розмірності вхідного 41-розмірного вектора вхідних даних у 12-розмірний вектор вихідних даних за допомогою нелінійної рециркуляційної нейронної мережі. Це дозволяє перейти від вихідного простору даних до допоміжного, яке характеризується меншою розмірністю та інформативністю вихідного простору. Другий етап полягає у виявленні і розпізнаванні атак. Для цього використовується багатошаровий персептрон, який здійснює обробку стисненого простору вхідних образів з метою розпізнавання класу атаки.

Таким чином, шляхом комбінування двох різних нейронних мереж, можна ідентифікувати і розпізнавати комп'ютерні атаки з досить високим ступенем точності. Основними перевагами використання підходів, заснованих на нейронних мережах, є здатність адаптуватися до динамічних умов і швидкість функціонування, що особливо важливо при роботі системи в режимі реального часу.

Імунні мережі:

Імунні методи роблять спробу поширити принципи виявлення та протидії імунної системи живих істот чужорідним вірусів. Система включає в себе централізовану «бібліотеку генів» формуючу обмежений набір векторів, що характеризують потенційно чужорідні події, і розподілену систему датчиків, які виконують власне детектування впливів, і володіють зворотним зв'язком з «бібліотекою генів».

Алгоритм функціонування імунної системи, можна представити у вигляді послідовності:

1. Генерація початкової популяції імунних детекторів, кожен з яких являє собою штучну нейронну мережу з випадковими синаптичними зв'язками.
2. Навчання сформованих імунних детекторів.
3. Відбір (селекція) імунних детекторів на тестовій вибірці. На даній ітерації знищуються ті детектори, які виявилися нездатними до навчання, і детектори, в роботі яких спостерігаються різні недоліки (наприклад, помилкові спрацьовування)
4. Кожен детектор наділяється часом життя та випадковим чином вибирає файл для сканування з сукупності файлів, які він не перевіряв.
5. Сканування кожним детектором вибраного файлу, в результаті якого визначаються вихідні значення детекторів
6. Якщо і-й детектор виявив вірус в скануємому файлі, то подається сигнал про виявлення шкідливого файлу і здійснюються операції клонування і мутації відповідного детектора.
7. Відбір клонованих детекторів, які є найбільш пристосованими до виявлення шкідливої програми
8. Детектори-клони здійснюють сканування файлового простору комп'ютерної системи до тих пір, поки не відбудеться знищення усіх проявів шкідливої програми.

Більш докладно алгоритм розглянуто у статті [7]. Методи побудовані на таких алгоритмах характеризуються невимогливістю до ресурсів, однак, в деяких умовах формують високий потік помилкових подій.

Експертні системи:

Переваги експертних систем полягають в можливості опису досвіду фахівців інформаційної безпеки у вигляді доступній для аналізу формі системи правил If (Умова) – Then (Наслідок) або дерева рішень, а процес логічного виведення схожий з характером людських міркувань.

Процес опису послідовності міркувань правилами If (Умова) – Then (Наслідок) реалізований в ланцюжках прямих і зворотних міркувань [3, 4].

Заснована на правилах експертна система складається з бази знань, бази даних, механізму логічного висновку, засобів пояснення результатів і користувальницького інтерфейсу. Знання в експертній системі організовані у вигляді ієрархічної системи правил If(Умова) – Then (Наслідок).

Система логічного висновку здійснює підстановку значень з бази даних у поля посилок частини If (Умова) правил бази знань та у разі заповнення полів всіх посилок активізує готові до обробки правила, формуючи укладення у відповідності з частиною Then(Наслідок) правил. Результати роботи експертної системи доступні користувачеві через діалоговий інтерфейс, який дозволяє, в разі потреби, ознайомитися з ходом логічних міркувань системи, що спричинило отримання даного результату.

Для виявлення аномалій виявляється діяльність, яка відрізняється від шаблонів, встановлених для користувачів або груп користувачів автоматизованої системи. Але головний недолік таких систем – висока обчислювальна складність (в загальному випадку).

Support vector machines (SVM).

Метод опорних векторів (Support vector machines) SVM – це математичний метод отримання функції, що вирішує завдання класифікації [16]. Ідея виникла геометричній інтерпретації задачі класифікації.

Розглянемо типовий приклад. Нехай дві множини точок можна розділити площиною (в двовимірному просторі – прямий). Тоді таких площин буде нескінченна безліч.

В якості оптимальної площині вибирається така площина, відстані до якої найближчих точок обох класів рівні. Найближчі точки-вектори називаються опорними. Пошук оптимальної площині приводить до задачі квадратичного програмування при безлічі лінійних обмежень-нерівностей.

Достоїнствами SVM з використанням п. ф. є:

1) отримання функції класифікації з мінімальним рівнем помилки класифікації;

2)можливість використання лінійного класифікатора для роботи з нелінійно розділяються даними, поєднуючи простоту ефективністю;

3) можливість роботи з різнорідними складно структурованими даними за рахунок використання різних п. ф.;

40 у разі зміни структури аналізованих даних, досить замінити тільки використовувану п. ф., без заміни самого алгоритму;

5) по суті в SVM вирішується головним чином задача квадратичного програмування, що має єдине рішення, і для неї існує безліч вивчених ефективних методів оптимізації, що дозволяє працювати в режимі реального часу.

Однак SVM має незначні недоліки, а саме:

1. вирішальна функція f(x) залежить від параметра v, встановлюваного апріорі;

2. SVM чутливий до наявності шуму в тренувальному наборі.

Для подолання цих недоліків у якості одного з варіантів пропонується використовувати математичний апарат нечітких множин. Однак це збільшує обчислювальну складність алгоритму.

Сигнатурні методи:

Найбільш часто використовувана група методів, суть яких полягає в складанні деякого алфавіту з спостережуваних в системі подій і описі безлічі сигнатур атак у вигляді регулярних виразів (у загальному випадку) в побудованому алфавіті . Як правило, сигнатурні методи працюють на найнижчому рівні абстракції і аналізують дані, які безпосередньо передаються по мережі, параметри системних викликів і запису файлів журналів. Принцип роботи даного методу розглянутий в статті.

Сигнатурні методи примітні тим, що для них добре застосовні апаратні прискорювачі, але при цьому метод не є адаптивним.

В табл. 1 представлений результат порівняльного аналізу методів виявлення аномалій.

Таблица 1

Анализ методов обнаружения аномалий

	Статист. Метод	Кластерний анализ	Нейронні мережі	Імунні мережі	Експертні системи	SVM	Сигнатурні методи
Уровень наблюдения	NIDS HIDS	Hybrid NIDS HIDS	NIDS HIDS	NIDS, HIDS	NIDS HIDS AIDS	NIDS HIDS	Hybrid AIDS
Ошибка I-рода ложные срабатывания)	7,98%	2,9%	4,8%	8,1%	2,88%	2,1%	2,1%
Ошибка II-рода (пропущено вторжений)	17%	15.8%	18,21%	20,85%	28,1%	14,44%	12,6%
Вычислительная сложность	Линейная и выше	Логарифм.	Линейная и выше	Линейная и выше	В общем случае NP	Логарифм.	Линейная и выше

Висновок

Методи, засновані на підході виявлення аномалій володіють тою чи іншою адаптивністю в залежності від методу реалізації.

Вони можуть лише виявити аномальну поведінку системи, але не можуть класифікувати виявлену аномалію (наприклад, як атаку одного з класів атак).

Перспектива розробки методів виявлення аномалій обумовлена здатністю виявляти раніше невідомі атаки в тому випадку, коли поведінка системи в процесі атаки є статистично відмінною від нормальної поведінки системи, відображеної в побудованій моделі нормальної поведінки.

Список літератури

1. Amoroso, Edward, G., Intrusion Detection // 1st ed., Intrusion.Net Books, Sparta, New Jersey, USA, 1999.

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

3. Stefan Axelsson, "Intrusion detection systems: A survey and taxonomy." // Technical Report 99-15, Chalmers Univ., March 2000.

4. Håkan Kvarnström, "A survey of commercial tools for intrusion detection". // Technical Report 99-8, Department of Computer Engineering, Chalmers University of Technology, Göteborg, Sweden, 1999

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

6. [Електрон. ресурс]. – Режим доступу: http://www.intuit.ru/studies/courses/20/20 /lecture/631?page=3.

7. Д. Ю. Гамаюнов, Современные некоммерческие средства обнаружения атак, 2002, http://istina. msu.ru/media/publications/articles/1de/f5b/4490957/free-ids-survey.pdf.

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

9. Guangzhi Qu, Salim Hariri, Mazin Yousif "Multivariate Statistical Analysis for Network Attacks Detection." // Computer Systems and Applications, 2005.

10. Нестеренко В.А. Статистические методы обнаружения нарушений безопасности в сети / В.А. Нестеренко// Информационные процессы. – 2006. – Т. 6, № 3. – С. 208-217.

11. Y. Frank Jou, Fengmin Gong, Chandru Sargor, Shyhtsun FelixWu, and CleavelandW Rance, "Architecture design of a scalable intrusion detection system for the emerging network infrastructure." // Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University, Releigh, N.C, USA, April 1997.

12. Jain A.K, Murty M.N, Flynn P.J. Data Clustering A review [PDF] (http://www.cs.rutgers.edu/~mlittman/courses/ lightai03/jain99data.pdf).

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

14. Головко В.А. Проектирование интеллектуальных систем обнаружения аномалий / В.А. Головко, С.В. Безобразов// Open Semantic Technologies for Intelligent Systems – OSTIS-2011.

15. Безобразов С.В., Алгоритмы искусственных иммунных систем и нейронныхсетей для обнаружения вредоносных программ / С.В. Безобразов, В.А. Головко // ees.kdu.edu.ua/wp-content/uploads/2013/04/86.pdf.

16 Kalle Burbeck, "Adaptive Real-time Anomaly Detection for Safeguarding Critical Networks." // Department of Computer and Information Science, Linköpings universitet, Linköping, Sweden, Linköping, 2006.

Надійшла до редколегії 1.08.2016

Рецензент: д-р техн. наук, проф. К.С. Смеляков, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків.

КЛАССИФИКАЦИЯ МЕТОДОВ ОБНАРУЖЕНИЯ АНОМАЛИЙ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

И.В. Рубан, В.А. Мартовицкий, С.А Партыка

В статье предложены критерии классификации методов обнаружения аномалий в современных системах обнаружения атак. Рассмотрены и проанализированы наиболее распространенные группы методов обнаружения аномалий. Показано, что методы обнаружения атак в современных системах обнаружения атак недостаточно проработаны в части формальной модели атаки, а, следовательно, для них достаточно сложно строго оценить такие свойства как вычислительная сложность, корректность, завершимість.

Ключевые слова: *IDS, Кластерный анализ, Экспертные системы, Нейронные сети, SVM.*

CLASSIFICATION OF METHODS OF ANOMALY DETECTION IN INFORMATION SYSTEMS

I.V. Ruban,V.A. Martovytskyi, S.O. Partyka

The article suggests the classification criteria of methods for anomaly detection in modern systems of detection of attacks. Reviewed and analyzed the most common group of methods is anomaly detection. It is shown that methods of detection in modern systems of detection of attacks, weak in parts a formal model of attack, and, consequently, they are difficult to rigorously evaluate properties such as computational complexity, correctness.

Keywords: *IDS, Cluster analysis, Expert systems, Neural networks, SVM.*