УДК 004.056 **І.М. Павлов, С.В. Толюпа, В.І. Ніщенко**

АНАЛІЗ ТАКСОНОМІЇ СИСТЕМ ВИЯВЛЕННЯ АТАК У КОНТЕКСТІ СУЧАСНОГО РІВНЯ РОЗВИТКУ ІНФОРМАЦІЙНИХ СИСТЕМ

Проаналізовані різні погляди на таксономію систем виявлення атак систем захисту інформації та представлено нову класифікацію систем виявлення атак, у якій таксономічні ознаки підібрані таким чином, щоб максимально збільшити кількість характеристик для опису даних систем для подальшого проектування систем захисту інформації відповідно до сучасних умов розвитку інформаційних технологій.

Ключові слова: система виявлення атак, таксономія, ознака, захист інформації, атака, аномалія.

Постановка проблеми

В даний час, при стрімкому розвитку мережевих технологій і глобальної інформатизації суспільства на перший план висуваються проблеми забезпечення високо рівня захищеності інформаційних систем. Зі збільшенням числа комп'ютерних інцидентів, пов'язаних з безпекою, почали стрімко розроблятися системи виявлення атак (СВА). СВА є одним з важливіших рішень для захисту систем і мереж зв’язку.

Традиційно СВА класифікуються відповідно до двох характеристик: методу виявлення і рівня системи на якому здійснюється захист. І не дивлячись на те, що ці дві класифікаційні ознаки є найважливішими при виборі систем виявлення атак, все ж існують й інші характеристики які відіграють не менш важливу роль у проектуванні СВА. Адже найбезпечніше рішення не може бути досягнуто при розгляді одного чи двох аспектів таксономії. Всі розробники систем виявлення атак і організації, які використовують СВА повинні розуміти і вивчати їх класифікацію, щоб вибрати кращі рішення для систем захисту інформації. При дослідженні різних аспектів таксономії і застосуванні різних варіантів ми зможемо досягти більш високого рівня безпеки інформаційних систем.

У зв’язку з цим, авторами і були систематизовані класифікаційні ознаки систем виявлення атак та розроблена класифікація даних систем, що у повному обсязі відповідає всім сучасним тенденціям побудови мереж зв’язку та викликам, що ставляться перед системами захисту інформації в цілому.

Аналіз останніх досліджень і публікацій дає змогу дійти висновку, що більшість існуючих класифікацій СВА дуже абстрактні, не є повними, і у них значні важливі характеристики (елементи) потребують доповнень та узагальнень.

Розглядаючи класифікацію у роботі [1] яка вважається однією з перших спроб класифікації СВА, стає зрозуміло, що автори включають аспекти моніторингу безпеки, такі як оцінки вразливості. Вони класифікують СВА по п'яти ознакам: методу виявлення, поведінці при виявленні, аудиту місцеположення джерела, парадигмі виявлення і частоті використання. Вже через рік автори у [2] додають декілька нових ключових класифікаційних ознак. Проте ще з часом у [3] автори у своїй класифікації показують, що СВА може працювати як автономний централізований додаток або інтегрований додаток, який створює розподілену систему. Але все ж найповніша класифікація, з точки зору таксономічних ознак, представлена у [4] де автори розширюють всі спроби їх попередників та включають в таксономію аж дванадцять класифікаційних ознак, проте не з усіма ними можна погодитись, а деякі вимагають відвертої модернізації та суттєвих доповнень у відповідності до реалій сьогодення.

Таким чином, автори поставили за *мету* систематизувати класифікаційні ознаки та надати актуальний погляд на таксономію систем виявлення атак.

Основна частина

Ця стаття являє собою сучасний погляд на таксономію систем виявлення атак з коротким поясненням та обґрунтуванням кожної ознаки в систематиці. Щоб зробити дану класифікацію всеосяжною і повною окрім звичних ознак, таких як: середовище моніторингу, метод виявлення, архітектура, характер відповіді, принцип роботи та час реакції, були

включені наступні характеристики: джерело аудиту, технологія побудови, парадигма виявлення та режим збору даних (рис. 1.).

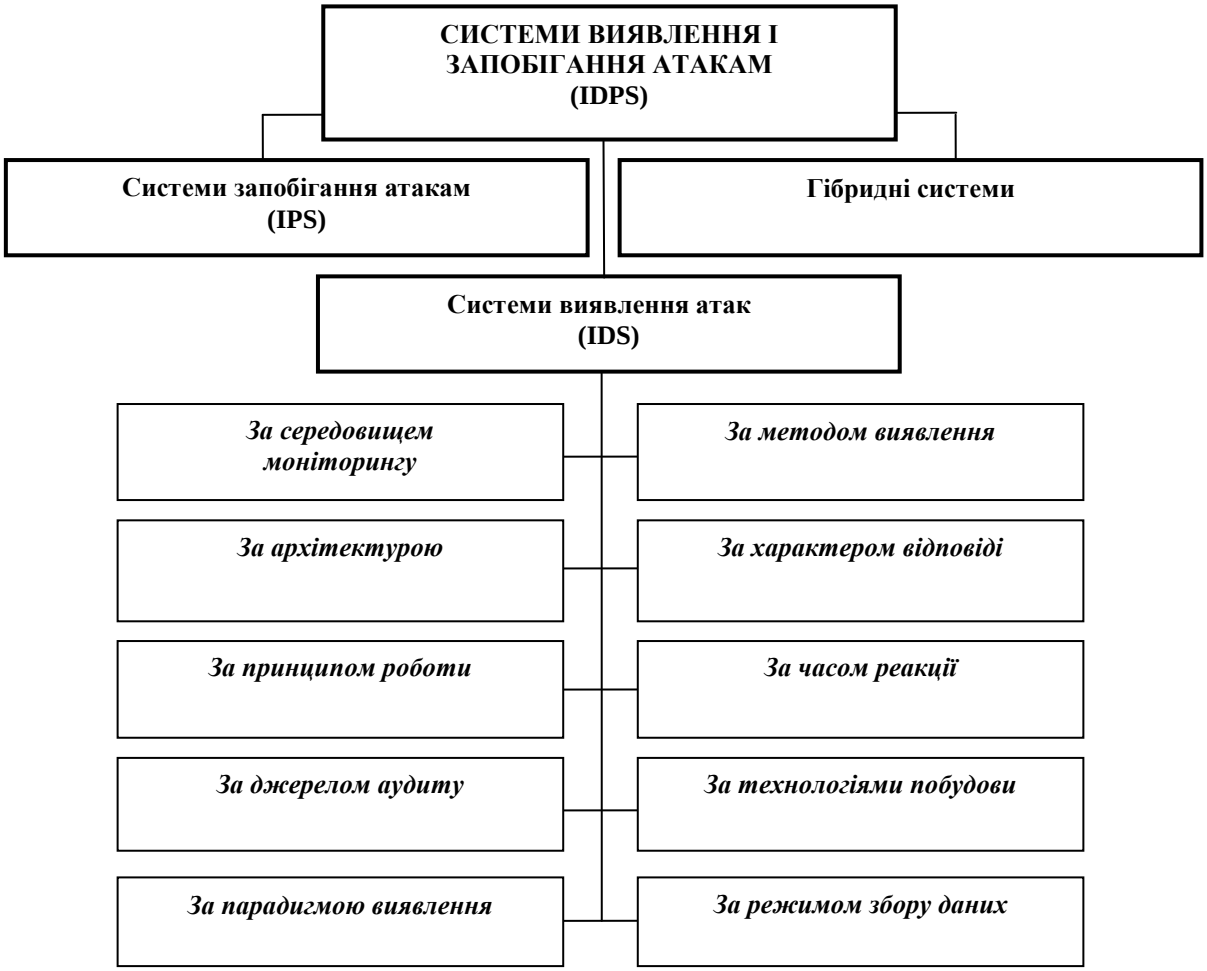

Рис. 1. Класифікаційні ознаки в узагальненій таксономії систем виявлення і запобігання атак

Першою класифікаційною ознакою систем виявлення атак є класифікація **за середовищем моніторингу**, тобто в залежності від того де здійснюється збір інформації: в мережі, на конкретному комп'ютері чи на певних додатках, що працюють на комп'ютері (рис. 2).

Більшість класифікацій представлених у [1], [2], [3] розділяють СВА за даною ознакою на два типи: СВА на рівні мережі та СВА на рівні вузла. Проте сьогодні наявність одного типу зменшує свою ефективність через відсутність іншого, тому досить популярною стає розробка гібридних або комбінованих систем які успішно функціонують як на рівні мережі так і на рівні вузла. А зі збільшенням спектру надання додаткових послуг та появою такого поняття як додаток (application) виникла необхідність моніторингу безпеки на рівні додатків. Тому доцільно класифікувати системи виявлення атак за середовищем моніторингу таким чином: на рівні мережі, на рівні вузла, гібридні (комбіновані) та на рівні додатків.

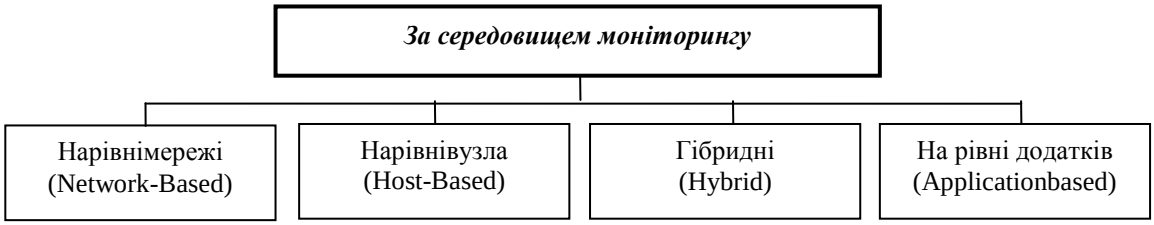

Рис. 2. Класифікація систем виявлення атак за середовищем моніторингу

Другою ознакою класифікації СВА є поділ **за методом виявлення загроз** (рис. 3).

Метод виявлення також згадується в інших класифікаціях, як техніка виявлення, принцип або підхід. Проте не залежно від назви ознаки історично прийнято розділяти системи виявлення атак на ті, що засновані на використанні методу виявлення сигнатур, і ті, що базуються на використанні методу виявлення аномалій. У цьому сходяться думки майже всіх науковців, що працюють над класифікацією СВА. Проте розбіжності спостерігаються далі, коли принципи, що належать конкретно до методів виявлення аномалій ставлять в один ряд з іншими, що являється некоректно. В свою чергу найточнішу класифікацію СВА заснованих на методах виявлення аномалій було представлено у [6].

Сьогодні методи виявлення аномалій являються пріоритетними у побудові систем виявлення атак. Найпопулярнішими серед них можна виділити чотири підгрупи, а саме: статичне виявлення аномалій, виявлення засноване на інтелектуальному аналізі даних, виявлення засноване на існуючих знаннях, виявлення на основі машинного навчання.

Також в більшості класифікацій відсутні гібридні методи, які стрімко досліджуються сьогодні і являють собою синтез сигнатурного методу і методу виявлення аномалій.

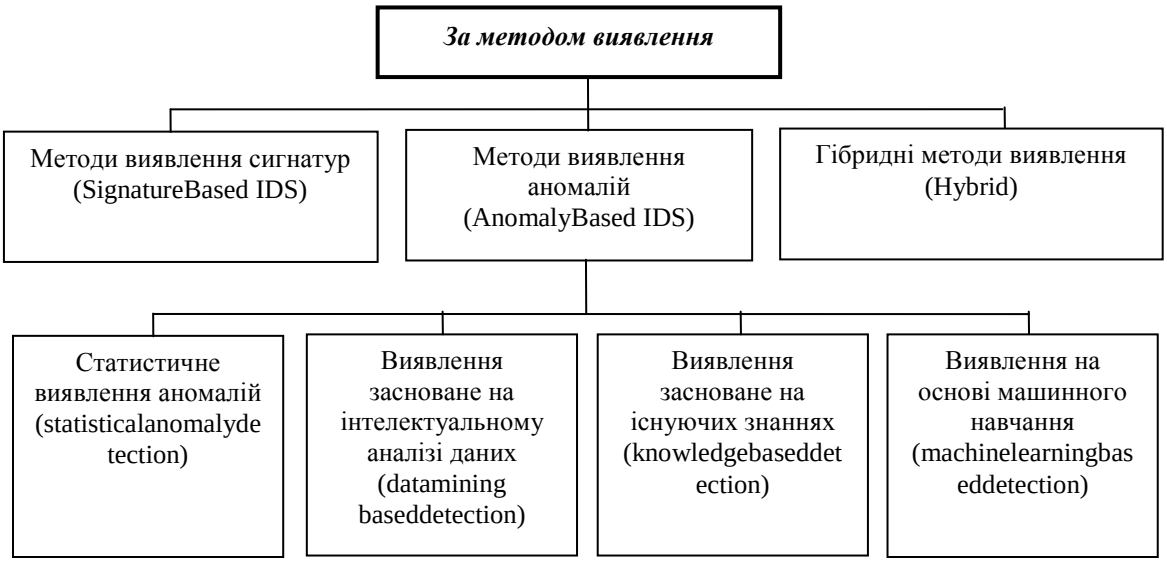

Рис. 3. Класифікація систем виявлення атак за методом виявлення загроз

Наступною класифікаційною ознакою є поділ **за архітектурою** (рис. 4).

В залежності від архітектури СВА виділяють системи, на якій виконується програмне забезпечення (host) і системи, за якими спостерігають (target).

Раніше СВА, переважно, виконувалися на тих же системах, які вони захищали проте з появою робочих станцій і персональних комп'ютерів у більшості архітектур СВА передбачається виконання СВА на окремій системі, тим самим розділяючи системи host і target. Це поліпшує безпеку функціонування СВА.

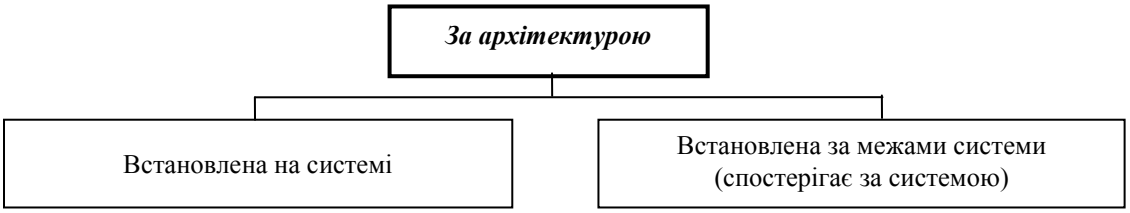

Рис. 4. Класифікація систем виявлення атак за архітектурою

За характером відповіді системи виявлення атак поділяють на активні та пасивні (рис. 5).

СВА може реагувати на вторгнення в пасивній чи активній формі. Пасивні заходи частіше всього являють собою звіт СВА, зроблений для людей, які потім виконують деякі дії на основі даного звіту.

Коли система виявлення атак активно реагує на вторгнення вона може додатково змінити стан об'єкту, що піддався атаці, або, в рідкісних випадках, змінити стан зловмисника. Активні заходи над об'єктом, що піддався атаці, мають на увазі автоматичне втручання в деяку іншу систему (наприклад, керування комутатором або мережним екраном).

Рис. 5. Класифікація систем виявлення атак за характером відповіді

Ще однією ознакою класифікації систем виявлення атак є розподіл **запринципом роботи** на статичні та динамічні (рис.6).

Не кожна сучасна класифікація систем виявлення атак має подібну класифікаційну ознаку, а все через те, що більшість науковців вважають статичні СВА морально застарілими. Проте існують інформаційні системи які не несуть в собі безліч важливої інформації та не підлягають постійному нападу зі сторони зловмисників, тому й не потребують складних механізмів реалізації динамічних СВА.

Статичні системи роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе програмне забезпечення, помилки в конфігураціях, перевіряють версії прикладних програм на наявність відомих вразливостей і слабких паролів, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів.

Динамічні СВА здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережні пакети, що передаються за певний проміжок часу. Динамічні IDS реалізують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи.

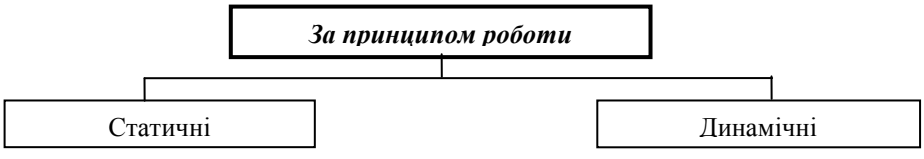

Рис. 6. Класифікація систем виявлення атак за принципом роботи

Наступною ознакою класифікації є розподіл **зачасом реакції** (рис.7).

Багато ранніх систем виявлення атак були пакетного типу, тобто вони цілком залежали від накопичення записів аудита в операційній системі. СВА пакетного режиму не виконують ніяких активних дій у відповідь на виявлені атаки. Даний тип розглядався як єдиний можливий у [1], проте вже через рік у [2] були додані системи виявлення атак у реальному часі.

СВА реального часу обробляють безперервний потік інформації відразу. Виявлення атак, що здійснюється СВА реального часу, приводить до результатів досить швидко, і це дозволяє системам виявлення атак виконувати певні дії у відповідь в автоматичному режимі.

Рис. 7. Класифікація систем виявлення атак за часом реакції

Також доцільно класифікувати системи виявлення атак **за джерелом аудиту** (рис. 8).

СВА виявляють вторгнення на основі аналізу даних, зібраних з використанням різних джерел аудиту. Зібрані дані представляють систему, додатки і поведінку мережі. Успішне виявлення вторгнень залежить від повноти даних зібраних з джерел аудиту, швидкості збору та обробки даних.

Дані з журналів аудиту комп'ютерних систем несуть в собі інформацію про користувальницьку діяльність на даній машині. У разі успішної атаки, вони уразливі для змін, тому вони актуальні лише до моменту здійснення атаки.

Аналіз мережевих пакетів популярний для збору інформації про події, які надходять від мережі. Перехоплювачами можуть слугувати шлюзи прикладного рівня або фільтруючі маршрутизатори. Аналіз пакетів може бути виконаний досить швидко, якщо він проводиться на низькому рівні, виконавши, наприклад, зіставлення із зразком або використавши сигнатурний аналіз.

Використання сенсорів СВА є характерною рисою відносно нового покоління систем виявлення атак, що не виявляють атаки безпосередньо, але мають змогу корелювати інформацію, зібрану з декількох інструментів виявлення вторгнень (сканерів). Такий метод зберігає і зменшує кількість подій, які повинні бути оброблені. Це також вигідно, коли діяльність охоплює кілька користувачів, комп'ютерів або мереж.

Дані журналів додатків є хорошим джерелом для отримання інформації, так як вони є більш точними і більш повним, адже файл містить всю необхідну інформацію і не вимагає повторної зборки так як з дані від мережевих пакетів.

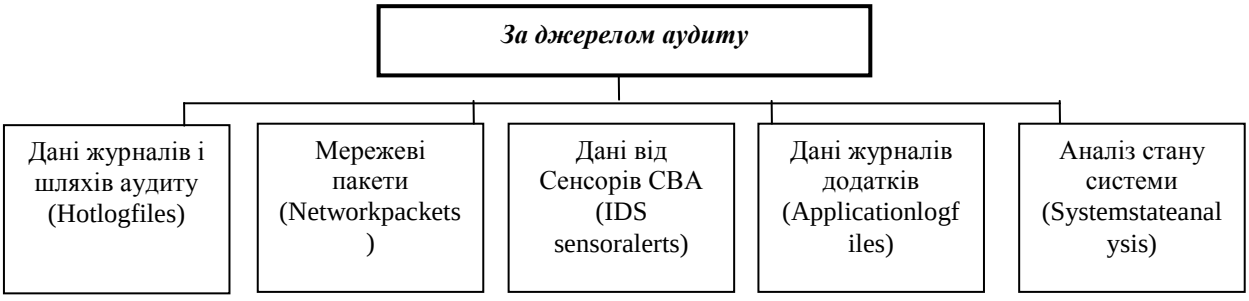

Рис. 8. Класифікація систем виявлення атак за джерелом аудиту

СВА, що використовують аналіз стану системи модулюють атаку, як серію змін станів, починаючи з початкового стану безпеки й закінчуючи станом загрози. Ці системи використовують діаграми для моделювання критичних подій, які повинні відбутися, щоб успішно проникнути в систему.

Ще однією важливою ознакою класифікації систем виявлення атак є розподіл **затехнологіями побудови** (рис.9).

При розгортанні СВА важливо знати, які технології використовуються в побудові інформаційної системи. Адже дротові мережі, порівняно з бездротовими, використовують різні і специфічні методи безпечної передачі, наприклад, шифрування. Тому фізична мережа передачі даних відіграє важливу роль у проектуванні систем виявлення атак.

Як відомо перші класифікації не мали цієї ознаки, вона зародилась лише з появою бездротових технологій, а сьогоднішня тенденція швидкого розвитку та модернізації бездротових технологій вимагає підвищення уваги до таксономії бездротових методів передачі інформації.

Провідні мережі, як правило, швидші і дешевші, ніж бездротові. Деякі з мережевих функцій, таких як, поведінка трафіку і топології мережі, можуть бути використані для виявлення вторгнень у провідних мережах зв'язку.

Стаціонарні бездротові мережі розташовані в фіксованих точках. Однією з переваг використання фіксованих бездротових мереж є можливість підключення користувачів у віддалених районах без необхідності прокладки нових кабелів.

Мобільний бездротові мережі являють собою набір мобільних вузлів, що автоматично само-настроюються без допомоги фіксованої інфраструктури або централізованого управління. Вони бувають: ієрархічні, мобільні агенти, автономні та розділенні і кооперативні.

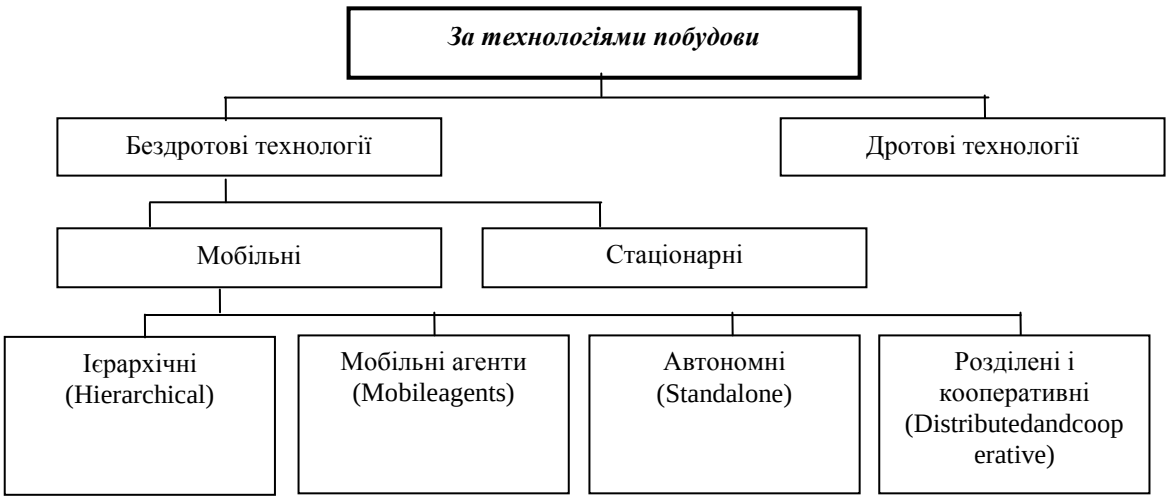

Рис. 9. Класифікація систем виявлення атак за технологіями побудови

Ієрархічні СВА призначені для багатошарових мережевих інфраструктур, де мережа ділиться на кластери.

Мобільний агент має здатність рухатися через великий мережі, призначається для виконання тільки одного конкретного завдання, і поширюється в мережі. Різні агенти призначені для різних функцій, що зменшує споживання енергії. Якщо мережа пошкоджується або деякі агенти знищуються, інші агенти як і раніше можуть працювати. Мобільні агенти не залежать від архітектури платформ.

Автономні СВА встановлюються на кожному вузлу незалежно. Вони обґрунтовують свої рішення тільки на інформації, зібраної на власному вузлу, співпраця між вузлами в мережі неможлива. Вузли не обмінюються даними, і не володіють ситуацією про стан безпеки сусідніх вузлів.

Розподілені та кооперативні СВА задіють у своїй роботі всі вузли мережі. Тобто кожен вузол бере участь у виявленні вторгнень, що забезпечується використанням агентів СВА. СВА агент виявляє і збирає інформацію локальних подій і даних для визначення можливих атак.

За парадигмою виявлення СВА поділяються на ті що оцінюють стан і ті що оцінюють переходи між станами (рис.10).

Парадигма виявлення описує, як СВА оцінює вторгнення і може бути двох типів. Перший тип оцінює стан щоб дізнатись чи є він безпечним чи вразливим. Другий тип оцінює переходи міг станами, а саме переміщення з безпечного стану в незахищений.

Оцінка стану, як і оцінка переходів між станами може проводитися двома способами:

• Не виводячи систему з рівноваги, тобто система виконує спостереження і оцінює вразливості, запитуючи необхідну інформацію, а потім порівнюючи її з таблицями відомих вразливостей.

• Проактивний спосіб, тобто система здійснює певний вплив на середовище, щоб визначити стан або створити перехід. Даний спосіб активно експлуатується для визначення стану системи, адже він майже не відрізняються від реальних вторгнень.

Рис. 10. Класифікація систем виявлення атак за парадигмою виявлення

Останньою класифікаційною ознакою систем виявлення атак є розподіл **за режимом збору даних** (рис.11).

Дані аудиту можуть бути зібрані в розподіленому режимі з декількох різних місць або джерел, або вони можуть бути зібрані централізовано від одного джерела.

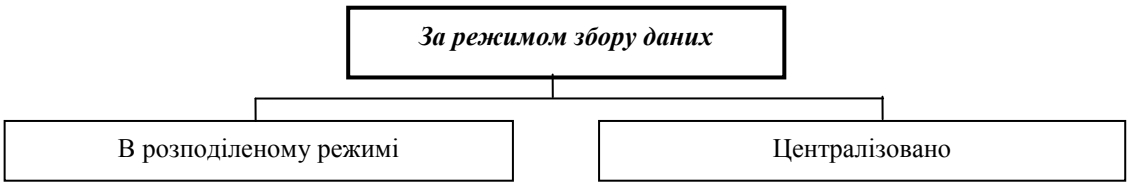

Рис. 11. Класифікація систем виявлення атак за режимом збору даних

Отже, узагальнений вигляд класифікації систем виявлення загроз представлений на рис.12.

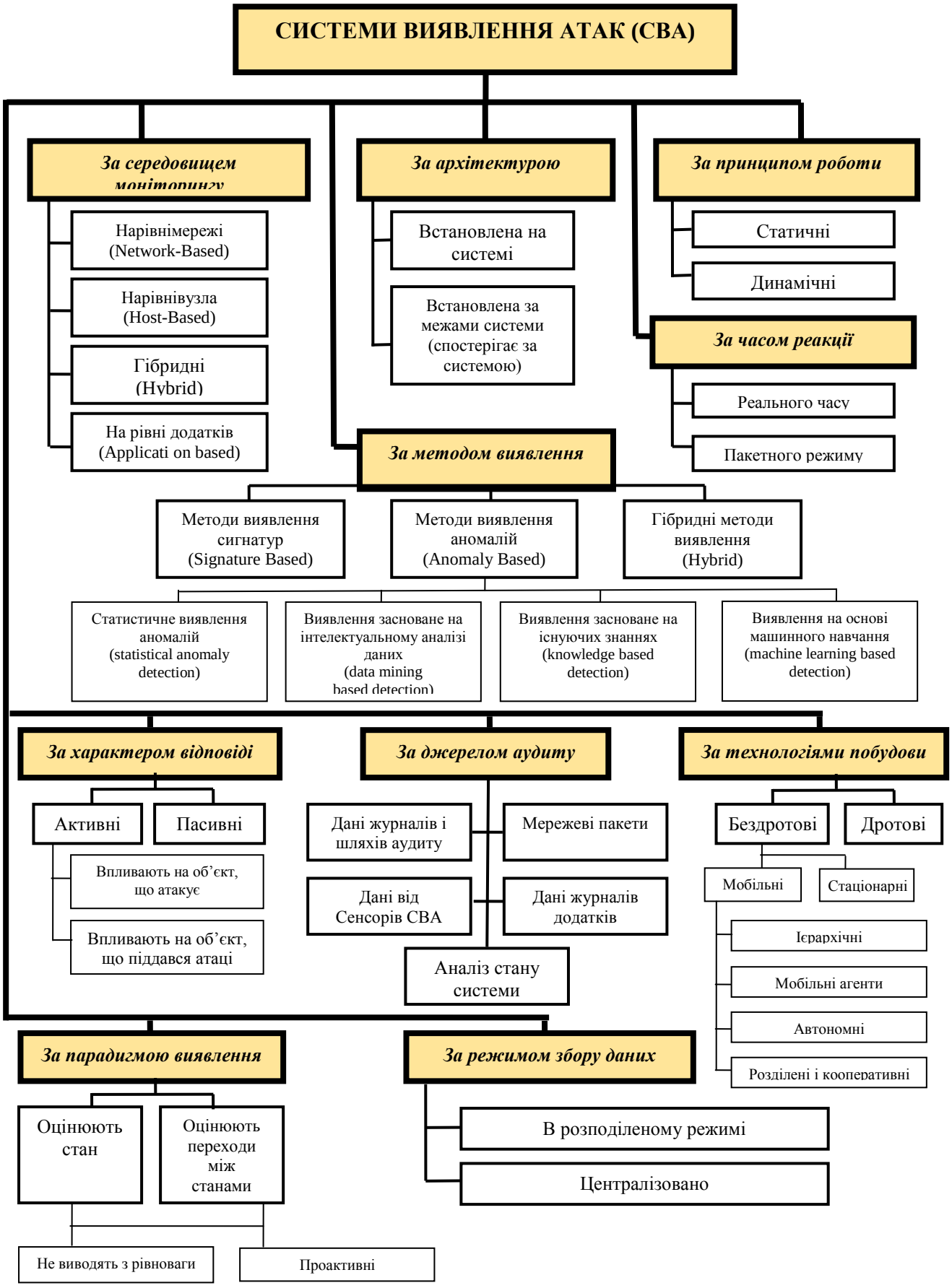

Рис. 12. Класифікація систем виявлення атак відповідно до сучасних тенденцій розвитку інформаційних систем

Висновок

Більшість попередніх класифікацій систем виявлення атак були вельми абстрактними, не завершеними, і у них були пропущенні важливі характеристики. У статті розроблена класифікація для СВА, у якій таксономічні ознаки підібрані таким чином, щоб максимально збільшити кількість характеристик для опису систем виявлення атак для подальшого проектування систем захисту інформації. Адже всеосяжна класифікація дозволяє організаціям володіти точною інформацією про тип СВА, яку слід використати відповідно до встановлених в організації стандартів безпеки і типу інформаційної системи.

На нашу думку повний набір класифікаційних ознак включає в себе: середовище моніторингу, метод виявлення, архітектуру, принцип роботи, час реакції, характер відповіді, джерело аудиту, технологію побудови, парадигму виявлення та режим збору даних.

Представлена класифікація може слугувати підґрунтям не лише для створення системи захисту, але й для адаптації організацій до СВА, що відповідає їх потребам. Наприклад, коли бюджет організації обмежений, дана класифікація може допомогти в ідентифікації найпріоритетніших компонентів, які в комплексному рішенні, призведуть до більш високого рівня захисту інформації в сучасних інформаційних системах.

Література

1. Debar, H., Dacier, M., andWespi, A. (1999), “Towards a TaxonomyofIntrusionDetectionSystems,” ComputerNetworks, vol. 31, 1999, pp. 805-22

2. Debar, H., Dacier, M., andWespi, A. (2000), “A RevisedTaxonomyforIntrusion-DetectionSystems,” presentedatAnnalesdesT?l?communications, vol. 55, 2000, pp. 361-78

3. Kabiri, P., andGhorbani, A., A. (2005), “ResearchonIntrusionDetectionandResponse: A Survey”, InternationalJournalofNetworkSecurity, Vol.1, No.2, Sep. 2005,pp.84-102

4. Amer, S.H., Hamilton, J.A., “IntrusionDetectionSystems, (IDS) Taxonomy – A ShortReview,” DOD SoftwareTechNews, vol. 13, no. 2, June 2010, DOD Data&AnalysisCenterforSoftware, AirForceResearchLaboratory, Rome, N.Y., pp. 23 - 30

5. Ali A. Ghorbani, WeiLu, andMahbodTavallaee, NetworkIntrusionDetectionandPrevention: conceptsandtechniques. London: Springer, 2010, p. 27-49.

6. Manasi G.; Rana; Yadav, “TaxonomyofAnomalyBasedIntrusionDetectionSystem: A Review” InternationalJournalofScientificandResearchPublications, Vol. 2, Issue 12, Dec. 2012

7. Бабенко Л.К. Разработкакомплекснойсистемыобнаружения атак / Л.К. Бабенко, О.Б. Макаревич, О.Ю. Пескова // Информационнаябезопасность: материалы V междунар. науч. - практ. конф. 2003. №4(33). С.235 - 239

8. Остапенко А.Г., Иванкин М.П., Савенков Г.А. Обнаружение и нейтрализациявторжений в распределенныхинформационных системах: учеб. пособие. – Воронеж : ФГБОУ ВПО «Воронежскийгосударственныйтехническийуниверситет», 2013.

Надійшла 21.11.2014 р. Рецензент: д.т.н., проф. Дудикевич В.Б.