DOI: 10.18372/2410-7840.20.13425
УДК 004.056.53(045)

АНАЛІЗ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Світлана Казмірчук, Анна Корченко, Тарас Паращук

З розвитком інформаційних технологій збільшується кількість уразливостей та загроз різноманітним системам обробки даних і тому для забезпечення їх нормального функціонування та попередження вторгнень необхідні спеціалізовані засоби безпеки, а перспективним напрямком, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень в інформаційних системах з боку неавторизованої сторони. Для виявлення мережевих вторгнень використовуються сучасні методи, моделі, засоби і комплексні технічні рішення для систем виявлення та запобігання вторгнень, які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Загалом при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому системи виявлення вторгнень повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні. Серед таких систем є спеціалізовані програмні засоби, які направлені на виявлення підозрілої активності або втручання в інформаційну систему і прийняття адекватних заходів щодо запобігання кібератакам. Аналіз джерел показав, що для сучасних інформаційних систем та мереж гостро стоїть питання оперативного виявлення зловживань та аномалій. В більшості робіт наведений лише частковий аналіз систем виявлення вторгнень та їх класифікація, представлений загальний опис відповідного забезпечення, який не відображає їх широкого спектру та не містить необхідної множини характеристик для інтегрованої оцінки таких систем. Тому, в роботі проведений узагальнений аналіз програмних засобів систем виявлення вторгнень за визначеною базовою множиною характеристик («Клас кібератак», «Адаптивність», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» та «Підтримка операційної системи»). Це дасть певні можливості щодо вибору таких засобів та розробки для них найбільш ефективних механізмів безпеки при впливах кібератак.

Ключові слова: *атаки, кібератаки, аномалії, зловживання, системи виявлення вторгнень, системи виявлення кібератак, системи виявлення аномалій, виявлення аномалій в інформаційних системах.*

Стрімкий розвиток інформаційних систем (ІС) та технологій всебічно впливає на всі сфери діяльності суспільства. Значна кількість сучасних державних та приватних підприємств використовує ІС для управління виробничими процесами, підтримки прийняття рішень, пошуку необхідних даних тощо. Разом з цим збільшується кількість уразливостей та загроз ІС і тому для забезпечення їх нормального функціонування та попередження вторгнень необхідні спеціалізовані засоби безпеки. Слід зазначити, що одним із актуальних напрямів, який активно розвивається у сфері інформаційної безпеки є виявлення кібератак і запобігання вторгнень в ІС з боку неавторизованої сторони (НАС).

Наприклад, низка нещодавно реалізованих кібератак, які завдали шкоди багатьом державним установам та приватним підприємствам і організаціям (Ощадбанк, Укргазбанк, Укрпошта, Укрзалізниця, Укренерго, ДТЕК, Київенерго, Київводоканал, Міжнародні аеропорти «Бориспіль» і «Київ», Rozetka, Київстар, Vodafone Україна, Lifecell, Київський метрополітен, телеканали СТБ і ICTV, Нова пошта, мережа магазинів «Епіцентр», автозаправки WOG і ТНК тощо [1-3]) показали неготовність та недосконалість їх власних систем безпеки до раніше невідомих вторгнень.

Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії. Для виявлення мережевих вторгнень використовуються сучасні методи [4-12], моделі [12, 13], засоби [12, 14-16], програмне забезпечення (ПЗ) [12, 17-27] і комплексні технічні рішення для систем виявлення та запобігання вторгнень [8, 12, 15, 22, 27-29], які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Але на практиці при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому системи виявлення вторгнень (СВВ) повинні постійно досліджуватись і удосконалюватись для забезпечення неперервності в їх ефективному функціонуванні.

Серед таких систем є спеціалізовані програмні засоби, які направлені на виявлення підозрілої активності або втручання в ІС і прийняття адекват-

них заходів щодо запобігання кібератакам. Ці системи та засоби, як правило, достатньо дорогі, мають закритий код та вимагають періодичної підтримки розробників (висококваліфікованих фахівців) щодо їх удосконалення і відповідного налаштування до умов конкретних організацій.

Виходячи з цього, проведення аналізу технічних рішень, спеціальних засобів та ПЗ виявлення кібератак, зловживань та аномалій в ІС для їх використання при виборі і розробці СВВ, а також визначення найбільш ефективних відповідних механізмів захисту РІС є актуальним завданням.

У [10, 20, 24, 26, 30] описано ПЗ Shadow та SnortNet, яке використовується для виявлення порушень за такими характеристиками, як «Клас кібератаки», «Адаптивність», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» та «Підтримка операційною системою (ОС)». Але для більш об'єктивної оцінки сучасного ПЗ важливо розглянути значно ширший спектр відповідних реалізацій, наприклад, Cisco IPS, Kaspersky Anti Targeted Attack Platform, InfoWatch ASAP, Tipping Poing NGIPS, Arbor Networks Spectrum тощо.

Крім того, в [7, 8, 12, 15, 17, 21-23, 25, 26] наведений загальний опис окремих функції та принципи роботи ПЗ EMERALD, OSSIM, CMDS, Shadow, Network Flight Recorder, Tripwire, NetProwler, NetRanger, Centrax та RealSecure, але не проведений аналіз відносно базових характеристик «Методи виявлення», «Реакція на кібератаку», «Захищеність» тощо.

Також в [27] розкриваються основні принципи функціонування найпопулярніших СВВ 2018 року – SolarWinds Log and Event Manager, Suricata, Sagan, Security Onion, AIDE, OpenWIPS-NG і Fail2Ban та визначені ОС, якими вони підтримуються, але не проведений аналіз відносно базових характеристик «Клас кібератак», «Адаптивність», «Захищеність» тощо.

У [18] порівнюються функціональності Real Secure, NetProwler та Форпост, але в цій роботі не проглядається узагальненість підходів та не проаналізовані сучасні засоби Symantec DeepSight Threat Management System, Arbor Networks Spectrum, Axoft invGUARD, DefensePro тощо, а також не визначені їх властивості відносно базових характеристик «Реакція на кібератаку», «Клас кібератак», «Адаптивність», «Методи виявлення» тощо.

В роботах [6, 7, 15, 31] описана низка методів, які використовуються в ПЗ для виявлення атак і аномалій, але не проведена оцінка відносно характеристик «Масштабованість», «Рівень спостереження» та «Реакція на кібератаку».

Також в [33] розглянуто системи виявлення та запобігання вторгнень, функціонування яких базується на аномаліях мережевого трафіку (аномальні системи виявлення та попередження вторгнень), в [12, 15] розкриваються методи та моделі, які використовуються для виявлення вторгнень, в [4-6, 8, 9, 11, 29, 34] порівнюються методи виявлення атак та аномалій, а в [29] акцентується увага на застосуванні нечіткої логіки для ефективного виявлення аномалій. Але в жодному з джерел не здійснено дослідження конкретного ПЗ, оцінки його властивостей та опису базових характеристик.

В [11, 12, 15, 17, 22, 29, 34] запропонована класифікація СВВ та систем запобігання вторгнень, зазначені їх переваги та недоліки і деякі особливості побудови, а в [7, 26] здійснена класифікація щодо виявлення мережевих вторгнень (аномалій і зловживань), але не розглядається існуюче ПЗ відносно визначених базових характеристик.

В роботах [6, 8, 10, 11, 13, 14, 18-20, 24, 26, 28, 29, 35, 36] розглянуті основні можливості, принципи побудови, механізми функціонування та порівняльний аналіз СВВ, але відсутнє конкретне дослідження ПЗ щодо характеристик «Клас кібератак», «Адаптивність», «Методи виявлення» тощо.

У [15] проведений аналіз щодо проектування систем виявлення атак, показані основні принципи створення засобів протидії кібератакам, але відсутній аналіз відносно конкретного ПЗ щодо характеристик «Масштабованість», «Рівень спостереження», «Реакція на кібератаку» тощо.

Аналіз джерел [4-36] показав, що для сучасних ІС та мереж гостро стоїть питання оперативного виявлення зловживань та аномалій. В більшості зазначених робіт наведений лише частковий аналіз СВВ та їх класифікація, представлений загальний опис відповідного забезпечення, який не відображає їх широкого спектру та не містить необхідної множини характеристик для інтегрованої оцінки таких систем.

Виходячи з цього, метою роботи є проведення узагальненого аналізу програмних засобів СВВ за визначеною базовою множиною характеристик. Це надасть певні можливості щодо вибору таких засобів та розробки для них найбільш ефективних механізмів безпеки при впливах кібератак.

Як правило, методи виявлення атак розділяють на методи виявлення зловживань і аномалій

[7, 30, 37, 38]. Зловживання засновані на використанні існуючих недоліків ІС. Основною відмінністю між аномалією і зловживанням є те, що аномалія – це процес, який виникає перед можливим вторгненням в систему або вказує на наявність вже існуючої атаки. Фактично, аномалія – це відхилення від нормального стану системи, незвичайна активність в ній, що може свідчити про певні атакуючі дії. Слід зазначити, що аномалія може виникнути і за інших причин, наприклад, внаслідок неправильної роботи системи.

Саме тому за допомогою ефективного аналізу аномалій, що виникають у системі, можна попередити кібератаки певних типів і вчасно вжити необхідних заходів щодо їх блокування та захисту ІС.

Варто сказати, що широке використання сучасних засобів захисту від кібератак не гарантує безпеки на належному рівні, оскільки останнім часом:

– зростають атаки, спрямовані на корпоративні системи, публічні, конфіденційні та державні інформаційні ресурси;

– кібератаки, постійно модифікуються, удосконалюються і стають більш регулярними;

– виявлення кібератак класичними засобами захисту не завжди є ефективним;

– частішають випадки здійснення складних атак [1-3] на ІС [28, 39, 40].

Це також пов'язане з інтенсивним розвитком програмно-апаратних засобів і глобалізації інформаційних мереж та їх повсякденного використання у всіх сферах діяльності суспільства.

Враховуючи результати відомих досліджень з подальшим їх узагальненням і відображенням на розширений спектр засобів виявлення зловживань та аномалій проведемо аналіз сучасних СВВ відносно базових характеристик «Клас кібератак», «Адаптивність», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» [30] та «Підтримка ОС» (див. таблицю 1).

Перед початком аналізу розкриємо кожну із зазначених базових характеристик.

«Клас кібератак» – визначає здатність системи виявляти аномалії та зловживання на різних рівнях ІС. Більшість сучасних засобів мають здатність виявляти обидва класи атак (аномалії та зловживання) [30].

«Адаптивність» – дозволяє системі ефективно адаптуватись до нових атак (відсутніх у базі даних сигнатур), наприклад, 0-day та виявляти кібератаки з незначними модифікаціями [30].

«Методи виявлення» – множини методів, що використовуються для виявлення атак і складають математичну основу системи. Найбільш поширеними є методи статистичного і кластерного аналізу, контролю зміни подій, графів атак, сигнатурні, динамічні, машинного навчання, поведінкові, евристичні, експертні, нечітких множин тощо [7, 30, 31, 38, 41].

«Управління системою» – визначає схему управління і його рівень. Управління може здійснюватися централізовано із одного хоста або розподілено із окремих хостів, пов'язаних однією системою. Найбільш оптимальною є організація управління за централізованою схемою з певною множиною центрів, кожний з яких може бути задіяний для управління всією структурою [30]. Централізовані системи реалізують управління всіма засобами (модулями) виявлення аномалій та зловживань з однієї станції [39], а розподілені реалізують управління окремо, де кожний модуль відповідає за свою функцію [42].

«Масштабованість» – можливість розширення системи, її адаптивність до різних мережевих структур та долучення нових аналізованих ресурсів мережі [30].

«Рівень спостереження» – визначає, на якому рівні системи отримуються дані для виявлення кібератак. Застосовуються два рівні отримання даних – мережевий та системний. Сучасні системи, як правило, підтримують обидва рівні спостереження, оскільки саме їх взаємодія дозволяє краще забезпечити захист. Від цієї характеристики залежить швидкість формування первинних даних, їх правильна обробка та отримання точної інформації про поточний стан РІС [30].

Аналіз трафіку мережі здійснюється за допомогою спеціальних сенсорів (мережевих і системних), що застосовуються у системах виявлення атак та аномалій. Мережеві сенсори аналізують дані на мережевому рівні (зазвичай на основі сигнатурного аналізу) і генерують повідомлення про виявлення кібератак та відправляють їх до модулів управління.

Системні сенсори аналізують журнали реєстрації ОС, додатки та програмні застосунки на можливі аномалії чи загрози і генерують відповідні повідомлення, які надходять до модулів управління [30].

«Реакція на кібератаку» – визначає наявність у системі компонентів чи модулів протидії. Тобто, після реєстрації атаки ініціюються дії для редукування подальшого негативного впливу [30].

«Захищеність» – характеризує наявність власних компонентів системи, які відповідають за її захист від кібератак та зовнішнього негативного інформаційного впливу, а також за стійкість до виходу з ладу та зменшення кількості уразливостей розробки в цілому [30].

«Підтримка ОС» – характеризує тип ОС (наприклад, Unix, Linux, Windows, MacOS тощо), що підтримує відповідне ПЗ системи.

Далі з урахуванням запропонованих характеристик розкриємо властивості відповідного СВВ (див. таблицю 1).

Shadow

Мережева СВВ Shadow (Secondary Heuristic Analysis for Defensive Online Warfare, розробник Naval Surface Warfare Center (військово-морський центр), Вірджинія, США) містить станції-давачі і станції-аналізатори [23]. Перші розташовані на зовнішній стороні міжмережевих екранів, а другі у внутрішньому захищеному сегменті мережі. Станція-давач – це сервер, на якому активізований tcpdump, який записує трафік у файл. Давачі виокремлюють заголовки пакетів і зберігають їх у спеціальному файлі. Станція-аналізатор зчитує цю інформацію, фільтрує її і генерує відповідний журнал. Якщо події ідентифіковані і для них існує стратегія реагування, то попереджувальні повідомлення не генеруються. Давачі використовуються для вилучення пакетів утиліти libpcap, а основний аналіз відбувається в модулі tcpdump, який містить фільтри пакетів, що поділяються на прості та складні (з декількох фільтрів). Фактично система використовує низку фільтрів мовою Perl, сенсори і аналізатори. Також Shadow (рис. 1) функціонує на багатьох UNIX-системах, включаючи FreeBSD і Linux та використовує веб-інтерфейс для відображення інформації [43-45]. Завдяки гнучкості мови Perl архітектура, що використовується в Shadow є однією з кращих серед мережевих СВВ.

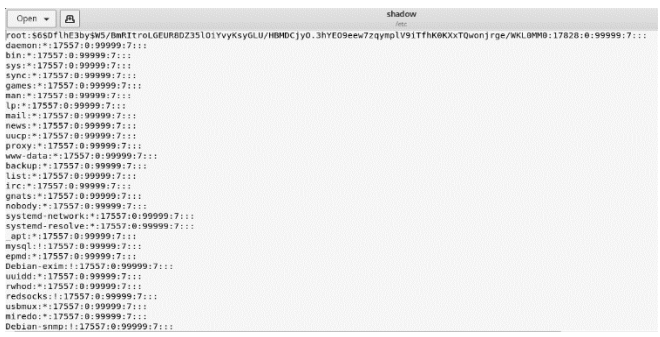

Рис. 1. Робоче вікно Shadow

Система орієнтована на виявлення зловживань та простих аномалій за допомогою методу контролю станів мережі, який не забезпечує систему в повній мірі можливістю адаптивності до нових кібератак. Shadow має закритий початковий код, а відповідні розширення здійснюються лише розробником. Система давачів та сенсорів дозволяє виявляти кібератаки на основі контролю зміни характеристик мережі за допомогою використання журналів стану та певних програмних фільтрів. Управління системою проводиться розподілено через файли конфігурації на всіх вузлах, де розташовані компоненти системи. Архітектура Shadow дозволяє будувати давачі (розташовані у вузлах мережі для збору інформації і запису у журнал) та аналізатори (аналізують всі події зареєстровані у журналі за допомогою давачів) для виявлення атак на різних рівнях мережі незалежно від її розміру [30, 43, 44].

Особливості будови даної системи дозволяють виявляти кібератаки лише на мережевому рівні [46]. Для своєї безпеки Shadow використовує протокол SSH, але не містить спеціальних механізмів протидії вторгненням і не є стійкою до можливих спрямованих на неї кібератак. Вона підтримується ОС Kali Linux (Unix та Linux), є частиною програмного продукту Snort та працює в пасивному режимі для збирання даних про систему [47].

Cisco IPS

Система запобігання вторгнень Cisco IPS (Cisco Intrusion Prevention System, розробка компанії Cisco, США) функціонує в режимі реального часу та забезпечує ідентифікацію і блокування шкідливого трафіку, черв'яків, вірусів, а також запобігання порушенню роботи додатків, інтелектуальне виявлення загроз і захист від них, фільтрацію на основі репутації і глобальні перевірки для запобігання загрозам (рис. 2) [12, 48, 49].

Рис. 2. Моніторинг IPS-давачів з використанням Cisco IPS

Cisco IPS реалізує функцію глибокого пакетного спостереження, яка ефективно протидіє широкому спектру мережевих кібератак. Елемент управління представлений інтегральною системою контролю за загрозою Cisco IOS і доповнений функцією Cisco IOS Flexible Packet Matching. Даний засіб дозволяє ефективно функціонувати комп'ютерній мережі з урахуванням таких чинників:

– контроль доступності мережі (забезпечує мережевий (розподілений) захист від багатьох атак, експлойтів, хробаків та вірусів);

– швидкість виявлення джерела мережевих кібератак та оперативна реалізація контрзаходів;

– гнучкість розгортання та масштабованість (інтерактивне інспектування трафіку за допомогою будь-якої комбінації інтерфейсів локальної мережі та WAN маршрутизатора з налаштованими на протидію визначеним множинам кібератак відповідно до рівня ризику);

– робота з брандмауером Cisco IOS (контроль за функціями безпеки Cisco IOS Software) [50].

Системна архітектура даного програмного засобу складається з чотирьох основних модулів:

– виявлення загроз;

– виявлення мережевих пристроїв (підключень) та неперервний контроль їх роботи;

– комплексного аналізу атак, аномалій та системних подій;

– моніторингу комп'ютерної системи.

Програмний засіб Cisco IOS забезпечує виявлення DoS і DDoS-атак, кібератак на інфраструктуру мережі та нульового дня, моніторинг широкомовних пакетів, виявлення неавторизованих мережевих додатків та захист від шкідливих доменів і IP-адрес. Останні розробки забезпечують:

– спеціалізований захист датацентрів для веб-серверів, баз даних і сховищ;

– безпеку додатків корпоративного класу Oracle, SAP тощо;

– безперервний захист критично важливих серверів від уразливостей ОС і додатків;

– зменшення часу на реагування та IT-витрати;

– легкість розгортання і управління (майстер розгортання включає шаблон сигнатур, орієнтований на дата центр) [48].

Даний програмно-апаратний комплекс призначений для виявлення зловживань та аномалій у мережі. Він частково адаптивний до нових кібератак, оскільки повністю залежний від структури та частоти оновлення бази даних атак. Cisco IPS є закритим програмно-апаратним комплексом з великим спектром налаштувань під особливості мережі і для виявлення вторгнень використовує наявні шаблони сигнатур та певну статистичну інформацію. Управління системою може здійснюватися централізовано або розподілено, залежно від складності побудови мережі. Швидке масштабоване розгортання системи здійснюються за допомогою динамічного управління політиками і установкою необхідних компонент з урахуванням структури та особливості мережі. Даний засіб здійснює безперервний захист критично важливих ресурсів мережі від різного роду уразливостей на рівні ОС та мережі. Cisco IPS дозволяє швидко виявляти джерела мережевих атак та визначати протидію, наприклад, ідентифікувати кібератаку, блокувати її і генерувати відповідне повідомлення. Також система забезпечує захищеність каналів передачі даних про атаку чи аномалію [48, 51, 52]. Cisco IPS працює тільки на FTP і HTTP/HTTPS серверах з ОС Unix, Linux та Windows [53].

Arbor Networks Spectrum

Система Arbor Networks Spectrum (розробник компанія Arbor Networks, Массачусетс, США) є високопродуктивним рішенням для аналізу мережевого трафіку, визначення шкоди від інцидентів інформаційної безпеки, виявлення вторгнень за допомогою поєднання статистичного, динамічного та сигнатурного методів аналізу. Основним функціоналом Arbor Networks Spectrum (рис. 3) [54] є виявлення DoS і DDoS атак, троянів та їх похідних.

Рис. 3. Вікно перегляду індикаторів загроз у часі

Arbor може бути розгорнута як пристрій або віртуальне рішення стеження за мережевим трафіком забезпечуючи постійне виявлення кібератак та зменшення їх наслідків. Запатентована в Arbor технологія Cloud Signaling успішно інтегрує цей

захист за допомогою хмарних технологій, автоматизуючи ключовий компонент захисту щодо DDoS та скорочуючи час, необхідний для редукування атак. Застосований гібридний багатошаровий захист є достатньо ефективним підходом для захисту даних від DDoS, що забезпечує безпеку корпоративних мереж незалежно від того, який тип DDoS-атак на них направлений [55].

Також Arbor має високоефективні служби управління, що забезпечують високий рівень захисту від відповідних кібератак по всьому світу. Ці служби в режимі онлайн в глобальному просторі мають цілодобову підтримку фахівців щодо редукування DDoS-атак та ведення безперервної розвідки у сфері загроз [56].

Arbor Networks Spectrum забезпечує:

– швидкий і легкий доступ до величин, що характеризують загрози в мережі та створення архіву трафіку;

– візуалізацію характеристик трафіку та загрози;

– централізоване управління щодо виявлення кібератак;

– постійне поновлення бази даних новими видами потенційних атак;

– масштабованість та простоту використання.

Програмний засіб забезпечує повний перегляд всієї активності в мережі з можливістю аналізу пакетних і потокових даних в режимі реального часу. Саме це дозволяє виявляти аномалії та атаки різного рівня. За допомогою функції ATLAS кожен користувач системи може з легкістю отримувати інформацію про нові кібератаки у глобальній мережі у режимі реального часу, що і забезпечує певний рівень адаптивності даної системи. Крім інформації про кібератаки, користувач отримує оновлену політику безпеки і контрзаходи для попередження атак. Часткова відкритість Arbor Networks Spectrum дозволяє покращувати адаптивність системи до нових кібератак, хоча повне оновлення і удосконалення різних модулів централізовано здійснюється розробниками. Система використовує статистичний, динамічний та сигнатурний методи виявлення атак і має централізоване управління за допомогою зручного інтерфейсу Arbor Spectrum. Гнучкі параметри розгортання системи дозволяють організаціям легко масштабувати та налаштувати даний засіб під потреби своєї мережі. Архітектура Arbor Networks Spectrum дозволяє виявляти атаки на мережевому і системному рівнях. Інтелектуальні схеми роботи і засоби аналізу в режимі реального часу дозволяють службам безпеки розслідувати та підтверджувати відповідні загрози і оперативно вживати необхідних заходів протидії [55-57]. Система не містить спеціальних механізмів захисту або вони не розкриті розробниками, а також працює на платформі vSphere Hypervisor, яка підтримує ОС Unix, Linux та Windows [57].

InfoWatch ASAP

Спеціалізований програмно-апаратний комплекс InfoWatch ASAP (InfoWatch Automation System Advanced Protector, розробник компанія InfoWatch, Росія) позиціонує себе як інтелектуальне рішення для виявлення і запобігання кібератак, спрямованих на інформаційну інфраструктуру систем автоматичного управління виробничими і технологічними процесами. Завдяки запропонованому підходу і запатентованим технологіям захисту, рішення має низку переваг перед штатними засобами запобігання вторгнень, які реалізуються виробниками сучасного обладнання [58].

Комплекс InfoWatch ASAP (рис. 4) призначений для створення систем безпеки, адаптований до використання в технологічних мережах і здатний виявляти:

– цілеспрямовані атаки на рівні автоматичного управління та введення або виведення даних виконавчими пристроями;

– вторгнення (сигнатурний і статистичний аналіз) та аномалії в характеристиках технологічної ІС;

– команди для зміни налаштувань і мікропрограм технологічного обладнання;

– несанкціоновані підключення до мережі;

– витік інформації щодо стану технологічного процесу;

– уразливості в технологічних ІС [59].

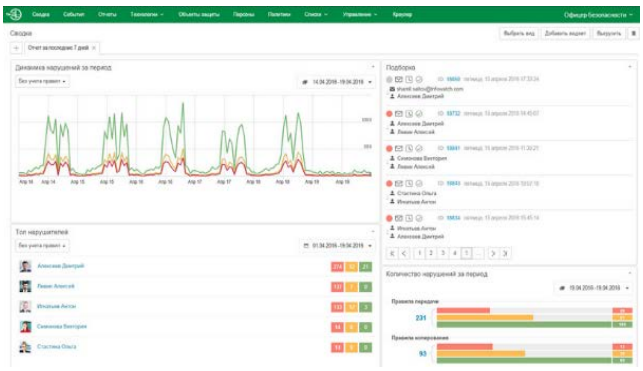

Рис. 4. Вікно звіту InfoWatch Traffic Monitor

Важливою складовою InfoWatch ASAP є методологічна база, що дозволяє будувати засоби захисту та ефективно протидіяти реально існуючим загрозам. Перевагою комплексу є захист від атак на всіх рівнях, незалежно від точки її виникнення. Комплексом підтримується більше 20 протоколів (з урахуванням галузевої специфіки), а також методологія аудиту та побудова моделі загроз, що забезпечує ефективний захист від кібератак [58, 60].

Даний програмно-апаратний засіб має модульну архітектуру (основні і допоміжні модулі), що дозволяє легко адаптуватись та масштабуватись в залежності від потреб комп'ютерної мережі.

До основних компонентів InfoWatch ASAP належать модулі:

– міжмережевого екранування;
– моніторингу та аналізу захищеності;
– виявлення і запобігання вторгнень;
– контролю коректності виконання;
– технологічного процесу.

Також до InfoWatch ASAP належать допоміжні компоненти:

– модуль забезпечення мережевої безпеки;
– підсистема аналітики і зберігання даних;
– графічний інтерфейс користувача.

Модульна структура дозволяє InfoWatch ASAP функціонувати в режимах моніторингу, інформування і попередження та виявляти кібератаки і аномалії на різних рівнях мережі (зовнішні і внутрішні атаки на інформаційну структуру підприємства). Постійне оновлення бази даних атак та наявність підсистеми їх моніторингу говорить про умовну адаптивність розробки, а підтримка ПЗ комплексу здійснюється лише його розробниками. InfoWatch ASAP використовує сигнатурний та статистичний методи виявлення вторгнень, а управління здійснюється централізовано за допомогою адміністраторів. Оскільки даний комплекс в основному орієнтований на внутрішню організацію мережі підприємства і попередження атак внутрішнього сегменту, то він доволі легко адаптується до зазначеної мережі та є легко масштабованим. Особливості його будови дозволяють виявляти кібератаки на мережевому і системному рівнях. Розробники InfoWatch ASAP не розкривають спеціальних механізмів захисту та протидії атакам, які спрямовані на комплекс, який підтримується ОС Unix, Linux, Windows та MacOS [59].

Symantec DeepSight

Система Symantec DeepSight (Symantec Deep Sight Threat Management System, розробник компанія Symantec, Каліфорнія, США) дозволяє розширити можливості захисту шляхом забезпечення раннього оповіщення про активні атаки, потенційні загрози, нові уразливі місця, шпигунські програми, рекламне ПЗ, що дає можливість адміністраторам більш точно передбачити і оцінити ступінь ризику, а також визначити пріоритетність інформаційних ресурсів, яким необхідний першочерговий захист від вторгнень. Також наявність розсилки персоніфікованих повідомлень, які доповнені професійним аналізом загроз, узагальненими оцінками і підтримкою вибору дій роблять Symantec DeepSight Threat Management System (рис. 5) провідною системою раннього оповіщення про глобальні кібератаки. Система має достатньо розгалужену інфраструктуру у глобальному кіберпросторі, яка складається з низки мереж honeypot [61-63].

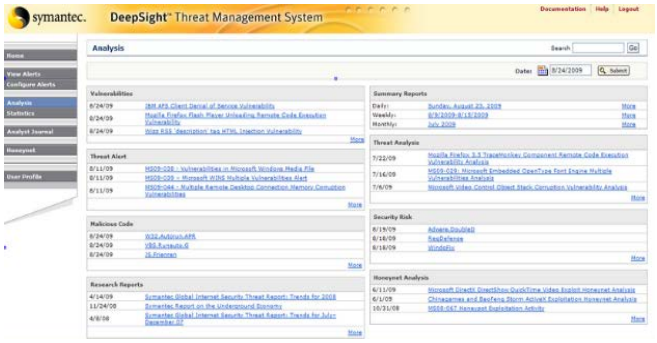

Рис. 5. Вікно Symantec DeepSight Threat Management System

За допомогою даної системи можна аналізувати вхідні потоки даних, що надходять до комп'ютерів через мережу та блокувати загрози до їх реалізації в системі.

Серед особливостей роботи даного програмного засобу слід віднести:

– автоматичне визначення пріоритетів серед існуючих загроз та ресурсів системи, що дозволяє оперативно встановити необхідний рівень протидії чи захисту;

– експертний аналіз даних, які збираються з тисяч джерел у глобальному кіберпросторі, включаючи інформацію про активні глобальні атаки;

– постійне збільшення та розширення баз даних існуючих мережевих загроз, через широке поширення даного програмного продукту;

– автоматизований моніторинг комп'ютерних мереж в реальному режимі часу, з можливістю швидкого сповіщення про загрозу;

– аналіз існуючих потенційних загроз в системі та створення базової стратегії їх попередження;

– здійснення управління програмним засобом спеціальними моніторами контролю функціонування в залежності від особливостей системи;

– стратегію редукування наслідків загроз, яка дозволяє забезпечити кращу пріоритетність, розподіл і розгортання персоналу та відповідних ресурсів безпеки;

– точний аналіз, який відповідає вимогам конкретної системи з урахуванням її мережевої структури, особливостей організації та виду діяльності [61, 63].

Дане ПЗ здатне виявляти атаки і аномалії. Завдяки постійному оновлення бази даних мережевих загроз та розширенню можливостей виявлення кібератак система достатньо легко адаптується до нових видів вторгнень. Підтримка та оновлення Symantec DeepSight здійснюється централізовано розробниками ПЗ. Система використовує експертний, статистичний, динамічний, машинного навчання та сигнатурний методи виявлення кібератак. Залежно від складності побудови системи та мережевої структури, управління може бути централізованим або розподіленим. Система є масштабованою, оскільки має чітку ієрархічну структуру, тобто при розширенні мережі збільшується лише кількість даних для аналізу, які необхідно опрацювати. Зазначена розробка здатна виявляти різного роду кібератаки, які були здійсненні на мережевому рівні, а також в певній мірі аналізувати журнали реєстрації низки програмних засобів та додатків. Symantec DeepSight Threat Management System дозволяє здійснювати завчасне (до нанесення шкоди підприємству) попередження щодо кібератак. Система дозволяє адміністраторам реалізувати превентивні заходи для захисту інфраструктури і компонентів мережі, а також протидіяти втратам продуктивності та нанесенню шкоди репутації компанії. За допомогою автоматизованих сповіщень із заданим пріоритетом на глобальному рівні система формує статистично надійну і дуже детальну інформацію про атаки, з можливістю відстеження даних у часі, країни, галузі промисловості та інших параметрів. Існуючі можливості щодо виявлення кібератак, реалізації контрзаходів і використання методів протидії та додаткових джерел довідкової інформації дозволяє системі діяти негайно та ефективно [61].

Symantec DeepSight Threat Management System не містить спеціальних механізмів захисту або вони не розкриті розробниками. Система підтримується ОС Unix, Linux, Windows і MacOS [64].

IPS

Система IPS (Intrusion Prevention System Software Blade, розробник компанія CheckPoint, США) призначена для запобігання вторгнень та орієнтована на доповнення функцій безпеки міжмережевих екранів для захисту від шкідливого та небажаного мережевого трафіку, включаючи DoS- та DDoS-атаки, уразливості в додатках і серверах (Application and server vulnerabilities), інсайдерські загрози тощо. Intrusion Protection System забезпечує повне та активне попередження вторгнень і складається з базового продукту IPS (рис. 6) та низки додаткових програмних модулів Check Point Software. За їх допомогою достатньо легко можна масштабувати та адаптувати систему під потреби мережі. Також IPS дозволяє здійснювати автоматичну активацію мережевого і системного захисту, навіть за відсутності адміністративного контролю. Система також забезпечує комплексний захист мережі (без погіршення продуктивності шлюзу) від небажаного трафіку в IM і P2P, у тому числі виявлення та попередження існуючих експлойтів, відомих і не відомих уразливостей, спроб тунелювання (які можуть свідчити про витік даних), а також виявлення і запобігання неправильному використанню протоколу, що може вказувати на потенційні загрози та стороннє ПЗ. Також забезпечує захист від інсайдерських загроз та уразливостей додатків і серверів [65, 66].

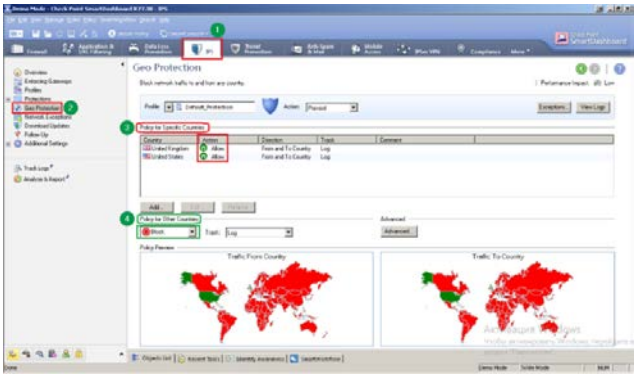

Рис. 6. Функція контролю управління трафіком в IPS (Geo-Protection)

Даний програмний засіб має можливість виявляти кібератаки та аномалії і забезпечувати захист в режимі реального часу. Він постійно оновлює інструментарій протидії новим загрозам, до яких

легко адаптується. Інструментарій є превентивним і забезпечує захист до того, як уразливості будуть виявлені, а експлойти створені. Підтримка та оновлення даного ПЗ здійснюється лише його розробниками. Використання системою додаткових модулів розширення (SmartEvent та інші), крім статистичного і сигнатурного аналізу дозволяє здійснювати і динамічний, що покращує механізми виявлення кібератак та протидії їм. В IPS здійснюється централізоване управління з основного монітора за допомогою відповідного зручного інтерфейсу користувача. Розробка характеризується простим процесом масштабованості системи під потреби мережі. Також є можливість інтеграції з існуючими міжмережевими екранами на підприємстві та подібними програмними засобами. Архітектура системи дозволяє виявляти кібератаки на мережевому і системному рівнях. Реакція на атаку визначається адміністратором безпеки або здійснюється автоматично, відповідно до політики безпеки IPS. Захист трафіку програмного засобу забезпечується протоколом SSL, а гранулярність дозволяє встановлювати винятки для інспекції SSL, щоб не порушити конфіденційність і забезпечити виконання політик безпеки. Зашифрований контент перевіряється, але адміністратор може встановити певні виключення з правил верифікації [65, 66]. IPS працює на ОС Windows [67].

TippingPoing NGIPS

Система TippingPoing NGIPS (TippingPoing Next Generation Intrution Prevention System, розробка компанії TrendMicro, США) є продуктом нового покоління, призначеним для попередження та запобігання вторгнень. Використовується для мережевої безпеки і реалізує комплексний захист від відомих та невідомих уразливостей, запобігає цілеспрямованим атакам, блокує загрози й шкідливі програми, що впроваджуються або поширюються в дата-центрах і корпоративних мережах. Система TippingPoing NGIPS є гнучкою та високопродуктивною і інтегрує технології захисту різних поколінь, включаючи глибокий аналіз пакетів, загроз, репутації URL-адрес та шкідливого ПЗ для клієнтських платформ і додатків [68-70].

Даний продукт розрахований на масштабні комп'ютерні мережі та має високу адаптивність. Серія TippingPoint NX (рис. 7-8) допомагає зменшити витрати часу на адміністрування і розставити пріоритети щодо мережевої безпеки за допомогою рішення Enterprise Vulnerability Remediation (eVR), яке дозволяє клієнтам імпортувати дані сканерів уразливостей в TippingPoint Security Management System, провести їх через фільтри служби цифрової вакцинації Digital Vaccine і оперативно вжити відповідні заходи. Реалізований в системі аналіз загроз забезпечує такий рівень прозорості, який необхідний для оптимізації стану інформаційної безпеки в межах всієї організації [68, 71].

Рис. 7. Інформаційна панель TippingPoint NGIPS (сканування даних в режимі реального часу для пошуку потенційних загроз)

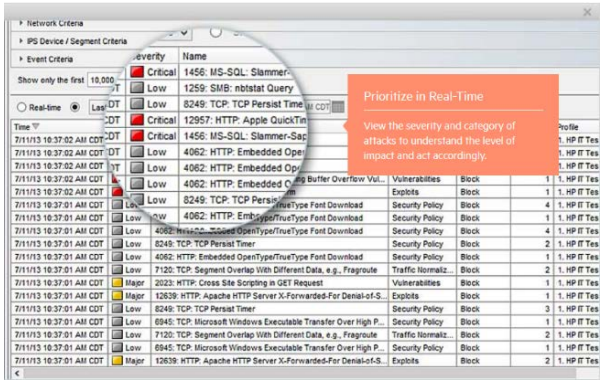

Рис. 8. Функціонування TippingPoint NGIPS в режимі реального часу
(режим перегляду рівня впливу і категорій кібератак)

Даний програмно-апаратний комплекс орієнтований на виявлення зловживань та аномалій у мережі, він адаптується до нових кібератак (містить адаптивний інтелект), оскільки використовує статистичні моделі машинного навчання та динамічні методи аналізу трафіку. Це дозволяє на основі отриманих мережевих даних в режимі реального часу приймати рішення щодо стану безпеки мережі для захисту її від нових та складних атак [68, 70].

Tipping Poing NGIPS є закритим програмно-апаратним комплексом з широкими можливостями і легко адаптується під особливості мережі. Він, на основі отриманих в режимі реального часу мережевих даних, приймає рішення про шкідливість мережевого трафіку для даної системи. Комплекс, також застосовує технології машинного навчання для визначення і блокування відомих і невідомих видів шкідливих програм, які використовують алгоритми генерації доменів (Domain Gene-

ration Algorithms, DGAs) для створення доменних імен командних серверів. Також застосовується статистичний та динамічний методи виявлення атак, використання яких допомагає ефективно виявляти загрози в мережі [68].

Комплекс має модульну архітектуру, що полегшує управління розгалуженими і складними за структурою мережами. Саме тому, залежно від потреб підприємства, управління системою може здійснюватися централізовано або розподілено.

Масштабована NGIPS динамічно захищає всі програми, мережу та дані від нових і розширених загроз. Оперативність щодо масштабованості забезпечується модульною архітектурою, простотою інтеграції політики безпеки під конкретні потреби підприємства та можливістю спільного використання з іншим ПЗ [70].

TippingPoing NGIPS здійснює безперервний захист критично важливих ресурсів мережі, бізнес-процесів та додатків від різного роду уразливостей. Також реалізовані функції інформування про додатки і їх контролю за допомогою глибокого аналізу трафіку, здійснюється перевірка певних типів файлів і захист критично важливої інформації. Саме тому NGIPS забезпечує комплексний захист на мережевому і системному рівнях. Комплекс NGIPS дозволяє швидко виявляти джерела мережевих кібератак та визначати реакцію на них. Наприклад, інтелектуалізоване блокування за контекстом визначених IP-адрес з урахуванням їх репутації. Захищеність каналів передачі даних щодо атак чи аномалій забезпечується шляхом використання новітніх засобів шифрування [68-70]. Комплекс підтримується ОС Windows та MacOS [72].

Axoft invGUARD

Програмно-апаратний комплекс Axoft invGUARD (розробка компанії Axoft, Росія) здійснює моніторинг мережевого трафіку за допомогою протоколів SNMP, NetFlow, BGP та детектує аномалії і мережеві атаки [73]. Він складається з двох базових компонент:

– система програмно-апаратного комплексу аналізу мережевого трафіку (invGUARD AS);

– система фільтрації та очищення мережевого трафіку (invGUARD CS/CS-01).

Axoft invGUARD орієнтований на аналіз вхідних потоків даних, що надходять в ІС через мережу з метою виявлення DOS- і DDOS-атак, BGP і SNMP аномалій, кібератак на інфраструктуру мережі, широкомовних пакетів та атак на програмні додатки [73, 74].

До основних функцій invGUARD відносять:

– неперервний моніторинг і аналіз трафіку;

– очищення вхідного трафіку з використанням статистичних та сигнатурних моделей;

– блокування зовнішніх мережевих атак на підзахисні сегменти мережі;

– забезпечення функціонування підзахисних сегментів мережі при реалізованих загрозах безпеки;

– централізація управління;

– можливість масштабування та адаптації комплексу до особливостей побудови і сфери функціонування мережі;

– розбір трафіку прикладних протоколів для блокування кібератак, пов'язаних з впливами на веб-інтерфейси і прикладну частину ІС;

– формування звітів за різною інформацією (рис. 9) [74].

Рис. 9. Вікно звіту системи Axoft invGUARD

Особливості будови Axoft invGUARD дозволяють ефективно виявляти зловживання та аномалії у мережі. Це здійснюється завдяки використанню методів статистичного, сигнатурного, евристичного, поведінкового та динамічного аналізу, що певною мірою забезпечує властивість адаптивності. Комплекс є закритим і має широкі можливості щодо адаптації до особливостей мережі. Управління системою здійснюється централізовано, воно направлене на збирання і аналіз мережевих даних та блокування кібератак [74]. Також є можливість адаптування і масштабування шляхом збільшення кількості засобів фільтрації трафіку. Особливості будови Axoft invGUARD дозволяють виявляти атаки на мережевому і системному рівнях [74, 75]. Комплекс не містить спеціальних

механізмів захисту та реакції на атаку (або вони не розкриті розробниками) і працює на ОС Unix і Linux.

DefensePro

Програмно-апаратний засіб DefensePro (DefensePro DDoS Defense & DDoS Prevention Device, розробник компанія RadWare, Ізраїль) призначений для попередження і запобігання мережевим вторгненням та атакам у режимі реального часу, що забезпечує неперервність роботи мережі і додатків (рис. 10). Він захищає від використання уразливостей додатків (неправильне використання додатків), поширення шкідливого ПЗ, мережевих аномалій, шкідливих доменів та IP-адрес, крадіжки інформації, троянів та від кібератак DDoS (DoS), спуфінг, фішинг, нульового дня, на основі SSL і сторінки авторизації та CDN [76, 77].

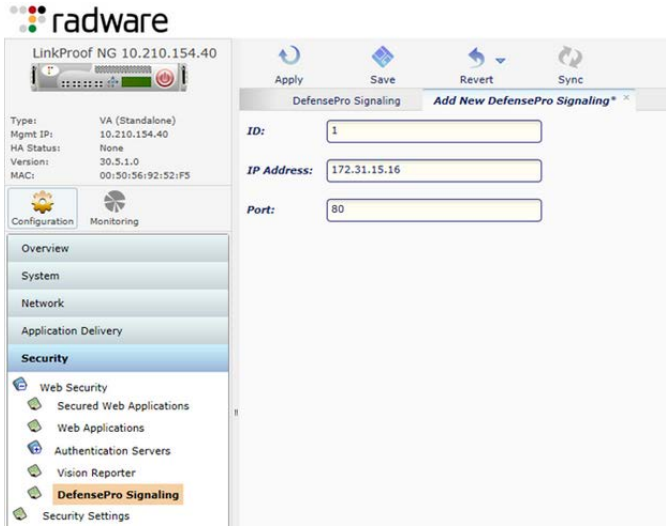

Рис. 10. Вікно ПЗ DefensePro

В DefensePro вбудовано два апаратних компонента, перший з яких DoS Mitigation Engine (DME), що призначений для відбиття масованих DoS- і DDoS-атак без впливу на нормальний трафік комп'ютерної мережі, а другий – StringMatch Engine (SME), який направлений на прискорення виявлення сигнатур, що є характерними для певної комп'ютерної мережі [76, 78].

Також комплекс захищає онлайн послуги, що базуються на веб-додатках та працює з іншими засобами забезпечення безпеки, що дозволяє підвищити рівень захищеності всіх сервісів і додатків [77].

DefensePro інтегрує функції запобігання вторгнень та аналізу поведінки мереж, а постійне оновлення бази даних мережевих загроз та розширення можливостей виявлення кібератак за допомогою операційного центру безпеки Radware дозволяє забезпечити користувачів автоматичною щотижневою доставкою сигнатурних фільтрів, а також необхідними фільтрами для критичних ситуацій. Підтримка та оновлення даного ПЗ здійснюється лише його розробниками. DefensePro заснований на стандартній технології виявлення сигнатур для запобігання відомих уразливостей, та складається з запатентованої технології на основі поведінкового аналізу, що автоматично генерує сигнатури в режимі реального часу. Це дозволяє оперативно запобігти, виявляти або блокувати мережеві атаки [76, 77].

Програмну частину системи складає APSolute Vision з централізованим управлінням і моніторингом та функцією звітності на багатьох пристроях і місцях розташування DefensePro. Це рішення орієнтоване в режимі реального часу здійснювати ідентифікацію, пріоритизацію та протидію порушенням політик безпеки, кібератакам та внутрішнім загрозам [76].

Масштабованість зумовлюється простою структурою побудови системи DefensePro. Модуль реагування програмно-апаратного комплексу на кібератаки здійснює розрив з'єднання з атакуючим об'єктом або його блокування. У поєднанні з SSL Radware AppXcel зазначений комплекс надає потужне і здатне до масштабування рішення для захисту від зашифрованих (заснованих на SSL) атак, які можуть обійти неперервний контроль безпеки. При утворенні оригінального SSL-тунелю між клієнтом і сервером DefensePro копіює SSL трафік на AppXcel, який розшифровує його і передає для перевірки в DefensePro. При виявленні атаки в розшифрованому SSL трафіку DefensePro (в режимі реального часу) блокує шкідливе мережеве з'єднання [76, 77].

Комплекс працює в програмних емуляторах KVM kernel 3.19 (Unix, Linux), QEMU 2.0 (Unix, Linux, Windows, MacOS), VMware (ESX server versions: 5.1, 5.5, 6.0) (Unix, Linux, Windows) [79].

KATA Platform

Система KATA Platform (Kaspersky Anti Targeted Attack Platform, розробка компанії Kaspersky, Росія) орієнтована на розвиток новітніх технологій у сфері корпоративних комп'ютерних мереж і використовується для захисту від комплексних цільових атак будь-якої складності. Рішення KATA Platform інтегрує новітні технології та глобальну аналітику, що дозволяє своєчасно реагувати на цілеспрямовані дії НАС і протидіяти атакам на всіх етапах їх реалізації [80]. Програмний засіб реалізує функції контролю мережевої активності, аналізу поводження об'єктів системи, виявлення комплексних цільових кібератак та аналіз аномалій в комп'ютерних мережах [80, 81].

Для збору первинної інформації про аномалії в KATA Platform (рис. 11) використовуються сенсори (спеціальні агенти), які аналізують IP, веб і e-mail трафік та події на робочих станціях і серверах. Агенти KATA Platform сумісні з іншим програмними засобами захисту і здійснюють мінімальний вплив на продуктивність мережі та комп'ютерів [82].

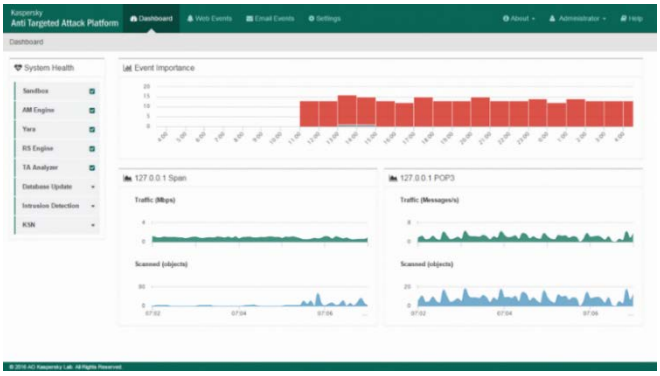

Рис. 11. Вікно ПЗ Kaspersky Anti Targeted Attack Platform

Функціонування KATA Platform базується на чотирьох етапах і є частиною комплексного стратегічного підходу для створення адаптивної моделі захисту від нових загроз і реагування на інциденти інформаційної безпеки:

Етап 1 – виявлення:

– постійний моніторинг активностей, які сигналізують про початок атаки;

– викривання уразливостей в системі безпеки і спроб проникнення в мережу;

– викривання інцидентів, оцінка збитку і пріоритизація подальших дій;

– тренінги з розслідування цільових атак;

– звіти про цільові атаки.

Етап 2 – реагування:

– аналіз шкідливого ПЗ;

– оперативна протидія атакам і редукування пов'язаної з ними шкоди;

– протидія інцидентам та їх розслідування;

– проведення глибокої цифрової криміналістики.

Етап 3 – прогнозування:

– тестування на проникнення;

– оцінка рівня захищеності системи;

– оцінка потенційних ризиків для безпеки в поточній інфраструктурі;

– рекомендації щодо удосконалення заходів захисту і усунення уразливостей;

– проактивний захист, який адаптується до нових і невідомих загроз.

Етап 4 – протидія:

– підвищення обізнаності співробітників про актуальні кіберзагрози (навчальні ігри, симуляція загроз тощо);

– тренінги з кібербезпеки для фахівців, що підвищують ефективність протидії цільовим атакам [81, 83].

KATA Platform здатен виявляти аномалії та комплексні цільові атаки різного роду, а постійне і оперативне оновлення бази даних мережевих загроз та розширення можливостей щодо виявлення кібератак, дозволяє забезпечувати користувачам адаптивність до нових вторгнень. Підтримка та оновлення даного ПЗ реалізується лише розробником. Аналіз цільових атак здійснюється на основі інформації від мережевих сенсорів, робочих станцій і серверів для створення типових шаблонів поведінки програм. Далі на основі відхилень від цих шаблонів визначається, чи є активність потенційною частиною цільової атаки. Також підозрілі об'єкти, які виявлені в поштовому і інтернет-трафіку передаються сенсорами в «пісочницю», де кожен такий об'єкт аналізується на предмет шкідливої активності, що дозволяє виявляти атаку на ранній стадії [80].

Система має централізоване та розподілене управління, а також можливості адаптування і масштабування платформи до кількісті вхідного трафіку та архітектури мережі. Особливості будови KATA Platform дозволяють виявляти кібератаки на мережевому і системному рівнях. Також сенсори мережі і робочих станцій дають можливість розташовувати точки контролю в різних сегментах мережі і швидко виявити комплексні загрози. Система оперативно реагує на атаки, що визначені нею у відповідній базі даних та дає можливість проведення цифрової криміналістики [80, 81, 83].

Спеціальні механізми захисту, що містяться в KATA Platform не розкриті розробниками. Система функціонує на основі ОС Unix, Linux, Windows та MacOS.

Проведений аналіз програмних засобів систем виявлення зловживань та аномалій, за рахунок базових характеристик, таких як клас атак, адаптивність, методи виявлення атак, управління системою, масштабованість, рівень спостереження за системою, реакція на атаку, захищеність та підтримувана ОС, дає можливість для розробників і користувачів обрати відповідне сучасне ПЗ для захисту ІС.

Таблиця 1

Зведені дані результатів аналізу СВВ

№	СВВ	Класи кібератак		Адаптивність	Методи виявлення											Управління системою		Масштабованість	Рівень спостереження		Реакція на кібератаку	Захищеність	Підтримка ОС			
		Зловживання	Аномалії		Експертний	Статистичний	Сигнатурний	Графи сценаріїв	Контроль зміни подій	Кластерний	Динамічний	Машинного навчання	Поведінковий	Евристичний	Нечітких множин	Централізоване	Розподілене		Системний	Мережевий			Unix	Linux	Windows	MacOS
1	Shadow	+	+	-	-	-	-	-	+	-	-	-	-	-	-	-	+	+	-	+	-	+	+	+	-	-
2	Cisco IPS	+	+	+	-	+	+	-	-	+	-	-	-	-	-	+	+	+	+	+	+	+	+	+	+	-
3	Arbor Networks Spectrum	+	+	+	-	+	+	-	-	-	+	-	-	-	-	+	-	+	+	+	+	-	+	+	+	-
4	InfoWatch ASAP	+	+	+	-	+	+	-	-	-	-	-	-	-	-	+	-	+	+	+	-	-	+	+	+	+
5	Symantec DeepSight Threat Management System	+	+	+	+	+	+	-	-	-	+	+	-	-	-	+	+	+	+	+	+	-	+	+	+	+
6	IPS	+	+	+	-	+	+	-	-	-	+	-	+	-	-	+	-	+	+	+	+	+	-	-	+	-
7	Tipping Poing NGIPS	+	+	+	-	-	+	-	-	-	+	+	-	-	-	-	+	+	+	+	+	+	-	-	+	+
8	Axoft invGUARD	+	+	-	-	+	+	-	-	-	+	-	+	+	-	+	-	+	+	+	-	-	+	+	-	-
9	DefensePro	+	+	+	-	+	+	-	-	-	-	-	+	-	-	+	-	+	-	+	+	+	+	+	+	+
10	KATA Platform	+	+	+	-	+	+	-	-	-	+	-	+	-	-	-	+	+	+	+	+	+	+	+	+	+

ЛІТЕРАТУРА

[1]. Хакерські атаки на Україну, 2017. [Електронний ресурс]. Режим доступу: https://is.gd/6lkWHY (дата звернення: 17.04.2018).

[2]. Пострадавшие от кибератаки банки и компании: перечень, 2017. [Електронний ресурс]. Режим доступу: https://zn.ua/UKRAINE/postradavshiy-ot-kiberataki-banki-i-kompanii-perechen-252717_.html (дата звернення: 17.04.2018).

[3]. Хакерська атака на Україну: подробиці, 2017. [Електронний ресурс]. Режим доступу: https://www.rbc.ua/ukr/news/hakerskaya-ataka-ukrainu-podrobnosti-1498566985.html (дата звернення: 17.04.2018).

[4]. А. Мустафаев, "Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика", *Вопросы безопасности*, № 2. С. 1-7, 2016. [Электронный ресурс]. Режим доступа: http://e-notabene.ru/nb/article_18834.html (дата обращения: 18.04.2018).

[5]. А. Корниенко, И. Слюсаренко, "Системы и методы обнаружения вторжений: современное состояние и направления совершенствования", [Электронный ресурс]. Режим доступа: http://citforum.ru/security/internet/ids_overview/ (дата обращения: 18.04.2018).

[6]. В. Литвинов, "Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі", *Математичні машини і системи*, № 1, С. 31-40, 2018. [Електронний ресурс]. Режим доступу: URL: https://cyberleninka.ru/article/v/analiz-sistem-ta-metodiv-vi-yavlennya-nesanktsionovanih-vtorgnen-u-kompyuterni-merezhi (дата звернення: 03.07.2018).

[7]. А. Браницкий, А. Котенко, "Анализ и классификация методов обнаружения сетевых атак", *Тр. СПИИРАН*, № 2 (45), С. 207-244, 2016.

[8]. Краткий анализ решений в сфере СОВ и разработка нейросетевого детектора аномалий в сетях передачи данных, 2018. [Электронный ресурс] Режим доступа: https://habr.com/post/358200/ (дата обращения: 03.07.2018).

[9]. О. Колодчак, "Сучасні методи виявлення аномалій в системах виявлення вторгнень", *Вісник Національного ун-т «Львівська політехніка». Комп'ютерні системи та мережі,* № 745, С. 98-104, 2012.

[10]. Д. Даниленко, О. Смірнов, Є. Мелешко, "Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі", *Системи озброєння і військова техніка,* Х.: Харк. нац. ун-т Повітряних Сил ім. І. Кожедуба, № 1, С. 92-100, 2012.

[11]. R. Patel, A. Thakkar, A. Ganatra, "A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems", I*nternational Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, no. 1, pp. 265-260, 2012.

[12]. Al-Sakib Khan Pathan, *The State of the Art in Intrusion Prevention and Detection,* 2014, 516 p. [Electronic resourse]. Online: http://docshare03.docshare.tips/files/20579/205795770.pdf (viewed on August 4, 2018).

[13]. Г. Бекетова, Б. Ахметов, О. Корченко, В. Лахно, "Розробка моделі інтелектуального розпізнавання аномалій і кібератак з використанням логічних процедур, які базуються на покриттях матриць ознак", *Безпека інформації*, Т. 22, № 3, С. 242-254, 2016.

[14]. К. Носенко, О. Півторак, Т. Ліхоузова, "Огляд систем виявлення атак в мережевому трафіку", *Адаптивні системи автоматичного управління,* К : НТУУ КПІ, № 1 (24), С. 67-75, 2014.

[15]. М. Радченко, "Аналіз системи виявлення вторгнень та комп'ютерних атак", *Междисциплинарные исследования в науке и образовании*, № 2, 2013.

[16]. Amrit Pal Singh, Manik Deep Singh, "Analysis of Host-Based and Network-Based Intrusion Detection System", *I. J. Computer Network and Information Security*, vol. 8, pp. 41-47, 2014.

[17]. В. Мєшков, В. Віролайнен, "Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах", *Проблеми безпеки інформації в інформаційно-комунікаційних системах,* Д.: НТУУ КПІ РТФ, 2015. С. 4. [Електронний ресурс]. Режим доступу: http:// ela. kpi. ua/ bitstream/ 123456789/ 17609/1/meshkov.pdf (дата звернення: 06.07.2018).

[18]. А. Лось, Ю. Даниелян, "Сравнительный анализ систем обнаружения вторжений, представленных на отечественном рынке", *Вестник Московского финасово-юридического университета*, № 3. С. 181-187, 2014.

[19]. А. Белова, Д. Бородавкин, "Сравнительный анализ систем обнаружения вторжений", *Актуальные проблемы авиации и космонавтики*, Сибирь: СФУ, Т. 1, № 12, С. 742-744, 2016.

[20]. А. Завада, О. Самчишин, В. Охрімчук, "Аналіз сучасних систем виявлення атак і запобігання вторгненням", *Інформаційні системи*, Житомир: Збірник наукових праць ЖВІ НАУ, Т. 6, № 12, С. 97-106, 2012.

[21]. Обзор систем обнаружения вторжений. Металургический журнал. Отрасли народного хозяйства. Исследования рынка, 2003. [Электронный ресурс] Режим доступа: http://www.metclad.ru/pat-a-587-list/ (дата обращения: 10.07.2018).

[22]. В. Бабошин, В. Васильев, "Обзор зарубежных и отечественных систем обнаружения компьютерных атак", *Информация и космос.* СПб : Санкт-Петербургская научно-техническая общественная организация «Институт телекоммуникаций», № 2, С. 36-41, 2015.

[23]. С. Гриняев, Системы обнаружения вторжений, № 10, 2001. [Электронный ресурс]. Режим доступа: https://www.bytemag.ru/articles/detail.php?ID=6563 (дата обращения: 10.07.2018).

[24]. Е. Абрамов, И. Половко, "Выбор характеристик систем обнаружения атак для выработки заключения о функциональных возможностях", *Известия Южного федерального университета. Технические науки.* Таганрог : ЮФУ, № 12 (125), С. 88-96, 2011.

[25]. Mohammad Sazzadul Hoque, Md. Abdul Mukit, Md., Abu Naser Bikas, "An implementation of intrusion detection system using genetic algorithm", *International Journal of Network Security & Its Applications (IJNSA)*, Sylhet, Vol. 4, no. 2, pp. 109-120, 2012.

[26]. O. Lawal, "Analysis and Evaluation of Network-Based Intrusion Detectionand Prevention System in an Enterprise Network Using Snort Freeware", *African Journal of Computing & ICT*, Ibadan, Vol. 6, no. 2, pp. 169-184, 2013.

[27]. S. Cooper, 11 Top Intrusion Detection Tools for 2018. [Electronic resource]. Online: https://www.comparitech.com/net-admin/network-intrusion-detection-tools/ (viewed on August 12, 2018).

[28]. Т. Зоріна, "Системи виявлення і запобігання атак в комп'ютерних мережах", *Вісник східноукраїнського національного університету імені Володимира Даля*, № 5 (204), С. 48-52, 2013.

[29]. Liu Hua Yeo, Understanding modern intrusion detection systems: a survey, 2017. [Electronic resource]. Online: https:// arxiv. org/ ftp/ arxiv/ papers/ 1708/ 1708.07174.pdf (viewed on August 12, 2018).

[30]. Д. Гамаюнов, Р. Смелянский, "Современные некоммерческие средства обнаружения атак", *Программные системы и инструменты. Тематический сборник.* М. : Ф-т ВМиК МГУ, С. 20, 2002.

[31]. А. Корниенко, И. Слюсаренко, "Системы и методы обнаружения вторжений: современное состояние и направления совершенствования", 2009. [Электронный ресурс]. Режим доступа: http://citforum. ru/ security/ internet/ ids_overview/ (дата обращения: 15.07.2018).

[32]. Е. Явтуховский, "Анализ систем обнаружения вторжений на основе интеллектуальных технологий", *Технические науки: теория и практика: материалы III Междунар. науч. конф.,* С. 27-30, 2016. [Электронный ресурс]. Режим доступа: https:// moluch. ru/ conf/ tech/archive/165/10049/ (дата обращения: 17.07.2018).

[33]. A. Kuznetsov, "The statistical analysis of a network traffic for the intrusion detection and prevention

systems", *Telecommunications and Radio Engineering*, Kharkiv, vol. 74, no. 1, 2015.

[34]. Marjan Kuchaki Rafsanjani, Zahra Asghari Varzaneh, "Intrusion Detection By Data Mining Algorithms: A Review", *Journal of New Results in Science*, Tokat : Gaziosmanpasa University, no. 2. pp. 76-91, 2013.

[35]. О. Кузнецов, О. Смірнов, Д. Даниленко, "Дисперсійний аналіз мережевого трафіку для виявлення та запобінання вторгнень в телекомунікаційних системах і мережах", *Системи обробки інформації,* Х. : Харк. нац. ун-т Повітряних Сил ім. І. Кожедуба, Вип. 2, С. 124-133, 2014.

[36]. Neyole Misiko Jacob, Muchelule Yusuf Wanjala, "A Review of Intrusion Detection Systems", *Global Journal of Computer Science and Information Technology Research. Framingham : Global Journals Inc.*, Vol. 5, no. 4, pp. 1-5, 2017.

[37]. А. Большев, В. Яновский, "Подход к обнаружению аномального трафика в компьтерных сетях с использованием методов кластерного анализа", *Известия Государственного Электротехнического Университета, серия Информатика, управления и компьютерные технологии,* СПб. : Изд-во СПбЭТУ, Вып. 3. С. 38-45, 2006.

[38]. А. Корченко, С. Ахметова, "Классификация систем обнаружения вторжений", *Інформаційна безпека.* № 1 (13); № 2 (14). С. 168-175, 2014..

[39]. В. Мєшков, В. Віролайнен, "Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах", *Проблеми безпеки інформації в інформаційно-комунікаційних системах.* К. : НТУУ КПІ РТФ, №. 1. С. 1-4, 2015.

[40]. М. Грайворонський, О. Новіков, *Безпека інформаційно-комунікаційних систем : навч. посіб,* К. : Видавнича група BHV, 2009, 608 с.

[41]. А. Корченко, *Построение систем защиты информации на нечетких множествах. Теория и практические решения,* К. : МК-Пресс, 2006, 320 с.

[42]. О. Матов, В. Василенко, "Модель загроз у розподілених мережах", *Реєстрація, зберігання та обробка даних,* К. : НАУ, Т. 10, № 1. С. 91-102, 2008.

[43]. S. Northcutt, *Intrusion Detection: Shadow Style-Step by Step Guide*, Dahlgren : SANS Institute, 1998.

[44]. Mark Alexander Bain, Build an IDS with Snort, Shadow, and ACID, 2005. [Electronic resource]. Online: https:// www. linux. com/ news/ build-ids-snort-shadow-and-acid (viewed on August 28, 2018).

[45]. Guy Bruneau, *About the Technical Reviewers,* Dertified Information Systems Security Professional : Training Guide. Indianapolis : Que Publishing, 2002.

[46]. Naval Surface, *Warfare Center SHADOW Arbitrary Code Execution Vulnerability*, San Jose : Cisco Multivendor Vulnerability Alerts, 2002. [Electronic resource]. Online: https://tools.cisco.com/security/center/viewAlert.x?alertId=3711 (viewed on August 30, 2018).

[47]. Index of downloads/ids/shadow-slack. Ottawa, 2012. [Electronic resource]. Online: http://www.whitehats.ca/downloads/ids/shadow-slack/ (viewed on August 30, 2018).

[48]. Cisco IPS 4500 Series. Описание продукта Cisco IPS 4500. Київ : ТОВ Інфобезпека, 2018. [Електронний ресурс]. Режим доступа: http://www.infobezpeka.com/products/apatnye/Cisco_IPS_4500_Series/ (дата звернення: 11.09.2018).

[49]. David Burns, *Cisco IPS Initialization, Inline, & Managed*, San Jose : Cisco Press, 2011. [Electronic resource]. Online: https:// community. cisco. com/ t5/security-documents/cisco-ips-initialization-inline-managed/ta-p/3127040 (viewed on September 12, 2018).

[50]. Cisco IOS Intrusion Prevention System (IPS). San Jose : Cisco Systems Inc, 2008. [Electronic resource]. Online: https://www.cisco.com/c/en/us/products/security/ios-intrusion-prevention-system-ips/index.html (viewed on September 12, 2018).

[51]. А. Дугин, *Cisco IDS/IPS. Безопасная настройка*, 2009. [Електронний ресурс]. Режим доступу: http://samag.ru/archive/article/2075 (дата обращения: 12.09.2018).

[52]. D. Burns, O. Adesina, K. Barker, *CCNP Security IPS 642-627 Official Cert Guide*, San Jose : Cisco Press, 2011, 672 p. [Electronic resource]. Online: http://www.ciscopress.com/ store/ ccnp- security- ips- 642-627-official-cert-guide-9781587142550 (viewed on September 12, 2018).

[53]. *Cisco Intrusion prevention system sensor CLI Configuration Guide for IPS 7.0*, Configuration Guides. San Jose : Cisco Press, 2014. [Electronic resource]. Online: https://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/cli/cliguide7/cli_system_images.html (viewed on September 12, 2018).

[54]. Arbor Networks Spectrum [Электронный ресурс]. Режим доступа: http://netwell.net.ua/content/uploads/ds_spectrum_rus2016.pdf (дата обращения: 15.09.2018).

[55]. Kevin Whalen, *Arbor networks is 2017 award winner*, Burlington : NetScout Systems Inc., 2017. [Electronic resource]. Online: https://www.netscout.com/news/press-release/ddos-2017-award-winner (viewed on September 16, 2018).

[56]. *Arbor DDoS Solutions*, Westford : NetScout Systems Inc., 2017. [Electronic resource]. Online: https://www.netscout.com/arbor-ddos (viewed on September 16, 2018).

[57]. Arbor Networks Spectrum, Data Sheet. Burlington : Arbor Networks Inc., 2017. [Electronic resource]. Online: http:// resources. arbornetworks. com/wp-content/uploads/DS_Spectrum_EN.pdf (viewed on September 16, 2018).

[58]. InfoWatch automation system advanced protector. Защита от атак на информационную инфраструктуру АСУ ТП. Москва : ГК InfoWatch, 2018. [Электронный ресурс]. Режим доступа: http://m.infowatch.ru/sites/default/files/products/asap/InfoWatch_asap_Datasheet.pdf (дата обращения: 16.09.2018).

[59]. InfoWatch Automation System Advanced Protector. Обнаружение и предотвращение вторжений и аномалий технологических процессов. Москва : ГК InfoWatch, 2018. [Электронный ресурс]. Режим доступа: https://www.infowatch.ru/products/asap (дата обращения: 17.09.2018).

[60]. InfoWatch ASAP, Для защиты АСУ ТП. СПб : AIM Systems, 2018. [Электронный ресурс]. Режим доступа: https:// www. aimsys. ru/solutions/actualasp (дата обращения: 17.09.2018).

[61]. Symantec DeepSight Threat Management System. Cupertino : Symantec Corporation, 2003. [Electronic resource]. Online: http://www.symantec.com/region/ru/earlyalert/images/RussianThreatManagementSys.pdf (дата обращения: 20.09.2018).

[62]. Online Threat Management Services, 2012. [Electronic resource]. Online: https://thejimmahknows.com/ online- threat- management- services/ (viewed on September 21, 2018).

[63]. Introduction to Symantec DeepSight Threat Management System 7.0. Cupertino : Symantec Corporation, 2003. [Electronic resource]. Online: https://support.symantec.com/en_US/article.TECH112914.html (viewed on September 21, 2018).

[64]. Symantec DeepSight Threat Management System, Data Sheet. Cupertino : Symantec Corporation, 2007, 3 p. [Electronic resource]. Online: http://eval. symantec.com/mktginfo/enterprise/fact_sheets/ent-datasheet_symantec_deepsight_threat_management_system_09-2007.en-us.pdf (viewed on Sep-tember 22, 2018).

[65]. IPS Software Blade contracts, SecureKnowledge. San Carlos : Check Point Software Technologies Ltd., 2015. [Electronic resource]. Online: https:// supportcenter. checkpoint. com/ supportcenter/ portal?js_peid=P-14d3e69bf07-10000 &eventSubmit_doGoviewsolutiondetails&solutionid=sk44175 (viewed on September 23, 2018).

[66]. Check Point IPS Software Blade. Datasheet. Tel Aviv-Yafo : Check Point Software Technologies Ltd., 2013, 2 p. [Electronic resource]. Online: https://www. checkpoint.com/downloads/product-related/ datasheets/ds-ips.pdf (viewed on September 24, 2018).

[67]. IPS Geo Protection drops the wrong traffic when it is configured as a whitelist. San Carlos : Check Point Software Technologies Ltd., 2016. [Electronic resource]. Online: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk110683 (viewed on September 25, 2018).

[68]. Trend Micro TippingPoint, Москва, 2017. [Электронный ресурс]. Режим доступа: http://www.tadviser.ru/index.php/Продукт:Trend_Micro_TippingPoint (дата обращения: 27.09.2018).

[69]. TippingPoint Threat Protection System. Irving : Trend Micro Incorporated, 2017. [Electronic resource]. Online: https://www.trendmicro.com/ en_hk/business/products/network/intrusion-prevention/tipping-point- threat- protection- system. html (viewed on September 27, 2018).

[70]. HP TippingPoint Next Generation Intrusion Prevention System. Geert Busse. Vilvoorde: Westcon-Comstor, 2018. [Electronic resource]. Online: http://be. westcon.com/ content/ vendors/ hp-enterprise-security-solutions/hp-tippingpoint-ngips (viewed on September 27, 2018).

[71]. Dave Shackleford, *SANS – Intrusion Prevention with TippingPoint,* SANS Analyst Program. Swansea : SANS Institute by Trend Micro, 2015. [Electronic resource] Online: https:// www. trendmicro. com/ content/ dam/trendmicro/global/en/business/products/network/integrated-atp/SANS_TrendMicroTippingPoint2600NX.pdf (viewed on September 27, 2018).

[72]. Darktrace vs. Trend Micro TippingPoint NGIPS. Intrusion Detecting and Prevention Software. New York : IT Central Station, 2018. [Electronic resource], Online: https://www.itcentralstation.com/products/comparisons/darktrace_vs_trend-micro-tippingpoint-ngips (viewed on September 27, 2018).

[73]. Система invGUARD AS, 2017. [Электронный ресурс]. Режим доступа: https://axoft.ru/vendors/inoventika-tehnolodjes/sistema-invGUARD-AS/ (дата обращения: 01.10.2018).

[74]. Система защиты от сетевых атак invGuard, 9th Annual Worldwide Infrastructure Security Report. M.: Inoventica Technologies, 2014. 36 с. [Электронный ресурс]. Режим доступа: https:// www. runnet.ru/docs/crimea2015/crimea-innoventica-invguard2015. pdf (viewed on October 1, 2018).

[75]. Система invGUARD AS. Отчет. M. : Inoventica Technologies, 2014. 10 с. [Электронный ресурс] // Режим доступа: http://www.inoventica-tech.ru/doc_reestr/Описание применения ПК invGuard AS-SW.pdf (дата обращения: 01.10.2018).

[76]. Chris Rodriguez, *DefensePro DDoS Defense & DDoS Prevention Device,* Mahwah : Radware, 2018. [Electronic resource]. Online: https://www.radware.com/ products/defensepro/ (viewed on October 3, 2018).

[77]. Radware Defense Pro, Київ : ТОВ Інфобезпека, 2018. [Электронный ресурс]. Online: http:// www.infobezpeka.com/products/apatnye/?view=395 (дата звернення: 03.10.2018).

[78]. Radware DefensePro Series, Irvine : Virtual Graffiti Inc, 2014. [Electronic resource]. Online: https:// www.radappliances.com/DefensePro.asp (viewed on October 3, 2018).

[79]. *Radware DefensePro*, DefensePro Tech Specs. Tel Aviv: Radware, 2018, 3 p.

[80]. Kaspersky Anti Targeted Attack (KATA) Platform, M.: АО Лаборатория Касперского, 2017. [Электронный ресурс]. Режим доступа: http://webcache.googleusercontent.com/search?q=cache:DUbVaOAeaBEJ:https://support.kaspersky.ru/13882&hl=en&gl=ua&strip=1&vwsrc=0 (дата обращения: 07.10.2018).

[81]. Передовая платформа для защиты от целевых атак и сложных угроз, Минск : Газета Правда, 2017. [Электронный ресурс]. URL: https://squalio.com/by-ru/programmnoe-obespechenie/kaspersky-anti-targeted-attack-platform/ (дата обращения: 07.10.2018).

[82]. Е. Касперский, *Большая картина,* M. : LiveJournal, 2016. [Электронный ресурс]. Режим доступа:

https://e-kaspersky.livejournal.com/297341.html (дата обращения: 07.10.2018).
[83]. *Kaspersky Anti Targeted Attack Platform*, Kaspersky Lab. M. : АО Лаборатория Касперского, 2016. С. 1-12. [Электронный ресурс]. Режим доступа: https://www.all-smety.ru/upload/KATA%20-%20Kaspersky_Anti_Targeted%20_Attack_Platform_WhitePaper_RU.PDF (дата обращения: 07.10.2018).

АНАЛИЗ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

С развитием информационных технологий увеличивается количество уязвимостей и угроз разнообразным системам обработки данных и поэтому для обеспечения их нормального функционирования и предотвращения вторжений необходимы специализированные средства безопасности, а перспективным направлением, которое активно развивается в сфере информационной безопасности является выявление кибератак и предотвращение вторжений в информационные системы неавторизованной стороны. Для обнаружения сетевых вторжений используются современные методы, модели, средства и комплексные технические решения для систем обнаружения и предотвращения вторжений, которые могут оставаться эффективными при появлении новых или модифицированных видов киберугроз. В общем при появлении новых угроз и аномалий, порожденных атакующими действиями с неустановленными или нечетко определенными свойствами, указанные средства не всегда остаются эффективными и требуют длительных временных ресурсов для их соответствующей адаптации. Поэтому системы обнаружения вторжений должны постоянно исследоваться и совершенствоваться для обеспечения непрерывности в их эффективном функционировании. Среди таких систем есть специализированные программные средства, направленные на выявление подозрительной активности или вмешательства в информационную систему и принятия адекватных мер по предотвращению кибератак. Анализ источников показал, что для современных информационных систем и сетей остро стоит вопрос оперативного выявления злоупотреблений и аномалий. В подавляющем большинстве работ приведен лишь частичный анализ систем обнаружения вторжений и их классификация, представлено общее описание соответствующего обеспечения, которое не отражает их широкого спектра и не содержит необходимого множества характеристик для интегрированной оценки таких систем. Поэтому в работе проведен обобщенный анализ программных средств систем обнаружения вторжений по определенным базовым множествам характеристик («Класс кибератак», «Адаптивность», «Методы выявления», «Управление системой», «Масштабируемость», «Уровень наблюдения», «Реакция на кибератаки», «Защищенность» и «Поддержка операционной системы»). Это даст определенные возможности выбора таких средств и разработки для них наиболее эффективных механизмов безопасности при воздействиях кибератак.

Ключевые слова: атаки, кибератаки, аномалии, злоупотребления, системы обнаружения вторжений, системы обнаружения кибератак, системы обнаружения аномалий, выявление аномалий в информационных системах.

ANALYSIS OF INTRUSION DETECTION SYSTEMS

As information technologies progress further, the number of vulnerabilities and threats to various data processing systems increases, creating a need for specialized security tools to ensure proper systems functioning and intrusion prevention. A promising area of rapid growth within the field of information security is cyberattack detection and information systems intrusion prevention of unauthorized party access. To identify network intrusions, intrusion detection and prevention systems use modern methods, models, controls and integrated technical solutions that can remain effective when new or modified types of cyberthreats occur. In general, whenever new threats and anomalies are generated by attacks with unidentified or vaguely defined properties, these tools do not always remain effective and require extended time resources to adapt to aforementioned security gaps. Thus, intrusion detection systems must be continuously researched and refined to ensure their effective operational continuity. Such systems include specialized software that is designed to detect suspicious activities or information system intrusions and take sufficient measures to prevent cyberattacks. Source analysis has shown that the issue of rapid detection of exploits and anomalies is a major concern for modern information systems and networks. Most papers only include a partial analysis and classification of intrusion detection systems, and provide a general description of corresponding controls that does not address their wide variety and does not include a required set of characteristics needed for an integrated assessment of such systems. Therefore, the paper presents a generalized analysis of intrusion detection software using a defined basic set of characteristics ("Cyberattack Category", "Adaptivity", "Detection Methods", "System Management", "Scalability", "Observation Level", "Cyberattack Response", "Security"and" Operating System Support"), which will provide certain options when choosing such tools and developing for them the most efficient security mechanisms possible for mitigating cyberattack impacts.

Keywords: Attacks, Cyberattacks, Anomalies, Exploits, Intrusion Detection Systems, Cyberattack Detection Systems, Anomaly Detection Systems, Information Systems Anomaly Detection.

Казмирчук Светлана Владимировна, доктор технических наук, зав. кафедры кафедры компьютеризированных систем защиты информации Национального авиационного университета.
E-mail: sv.kazmirchuk@gmail.com.
Казмірчук Світлана Володимирівна, доктор технічних наук, зав. кафедри кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету.

Kazmirchuk Svitlana, Dr Eng (Information security), Head of Computerised Information Security Systems Academic Department, National Aviation University.

Корченко Анна Александровна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: annakor@ukr.net.
Корченко Анна Олександрівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Korchenko Anna, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.

Паращук Тарас Іванович, студент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Email: taras1039@ukr.net.
Паращук Тарас Иванович, студент кафедры безопасности информационных технологий Национального авиационного университета.
Paraschuk Taras, student of IT-Security Academic Department, National Aviation University.