УДК 004.056:621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.140

АНАЛІЗ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ МЕРЕЖ

Михайлова А.С., Чеботарьова Д.В.
Науковий керівник – доц. Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: anna.hmyria1@nure.ua
e-mail: dariia.chebotarova@nure.ua

This work is devoted to the issues of information security in information networks, namely the analysis of intrusion detection and prevention systems (IDS/IPS). The purpose of the report is a multi-criteria analysis of intrusion detection and prevention systems, taking into account a set of quality indicators. All considered IDS/IPS systems have their own characteristics, so the choice of the optimal system will vary depending on the circumstances, conditions and needs of a particular network.

Сьогодні електронні комунікації, зокрема інформаційні мережі, є ключовою частиною нашого життя. Інформаційні мережі широко використовуються в побуті та різних галузях, таких як навчання, бізнес, інфокомунікації, виробництво, комерція, розваги, охорона здоров'я тощо. Найбільш значною проблемою інформаційних мереж є безпека інформації, яка передається мережею, а також зберігається та опрацьовується в кінцевих пристроях мережі. Останнім часом кількість загроз та атак суттєво збільшується, тому питання захисту інформації в інформаційних мережах стає все більш актуальним.

Питання безпеки інформаційної мережі є одним із найбільш важливіших. Саме тому для попередження атак, мінімізації загроз та захисту мереж необхідно використовувати найбільш потужні засоби безпеки. До таких засобів відносяться спеціальні пристрої та програми, а також методи моніторингу, сповіщення та перевірки мережних з'єднань. Серед таких засобів великої популярності також набули сьогодні системи виявлення та запобігання вторгненням (IDS/IPS - (Intrusion Detection System /Intrusion Prevention System), які дають можливість виявити мережні атаки та запобігти вторгненню, ще до того як вони завдадуть шкоди та призведуть до негативних наслідків.

Метою доповіді є багатокритеріальний аналіз систем виявлення та запобігання вторгненням для захисту інформаційної мережі. В процесі багатокритеріального порівняння необхідно враховувати велику кількість параметрів систем IDS/IPS.

В наш час на ринку існує багато пропозицій IDS/IPS [1]. Сучасні системи виявлення та запобігання вторгнень є досить різноманітними, базуються на використанні різних методів, але окрім переваг, мають також

свої певні недоліки. Ці недоліки можуть бути пов'язані зі структурою систем або з реалізованим методом виявлення вторгнень [2].

Саме тому вибір оптимальної системи IDS/IPS для захисту конкретної інформаційної мережі з урахуванням сукупності показників якості та особливостей мережі є досить складною задачею. Компанії можуть вибирати з низки недорогих і потужних рішень IDS/IPS, які відповідають різноманітним потребам - від стартапів з обмеженим бюджетом до глобальних підприємств. Деякі з них є окремими рішеннями, а інші – функціями, доданими до інших продуктів безпеки [1]. У переважній більшості системи IDS/IPS використовують поєднання різних рішень на базі синтезу відповідних методів [2].

Зазвичай при виборі оптимальної системи IDS/IPS трьома найважливішими факторами при прийнятті рішення є функціональність, надійність і ціна [3].

В роботі проведено огляд та аналіз найбільш сучасних систем IDS/IPS за версією [1]: AIDE, BluVector Cortex, Check Point Quantum IPS, Cisco NGIPS, Fail2Ban, Fidelis Network, Hillstone Networks, Kismet, NSFOCUS, OpenWIPS-NG, OSSEC, Palo Alto Networks, Sagan, Samhain, Security Onion, Semperis, Snort, SolarWinds Security Event Manager IDS/IPS, Suricata, Trellix (McAfee + FireEye), Trend Micro, Vectra Cognito, Zeek, ZScalar Cloud IPS. В роботі пропонується порівнювати ці системи з урахуванням таких показників якості: підтримувані платформи та пристрої, типи виявлення загроз, вартість, відкритість коду, масштабованість, ємність, необхідність додаткового апаратного чи програмного забезпечення, затримка, тип ідентифікатору (HIDS, NIDS), інтеграція з іншими засобами безпеки, зручність інтерфейсу.

Усі розглянуті системи IDS/IPS мають свої особливості, переваги та недоліки. Тому вибір найкращої системи буде змінюватись в залежності від обставин, умов та потреб конкретної мережі.

Список використаних джерел:

1. Samson R. Top 10 Intrusion Detection And Prevention Systems [Електронний ресурс] / Ron Samson // ClearNetwork. – 2023. – Режим доступу до ресурсу: https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/.

2. Лукова-Чуйко Н. В. Методи виявлення вторгнень у сучасних системах IDS / Н. В. Лукова-Чуйко, С. В. Толюпа, І. І. Пархоменко // Безпека інформаційних систем і технологій. Інформаційна та кібернетична безпека. – 2021. – № 1(5). – С. 19 – 26.

3. Hock F. Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks / Filip Hock, Peter Kortiš // Research Gate. – 2015. – Режим доступу до ресурсу: https://www.researchgate.net/publication/307853397.