УДК 004.056.53 doi.org/10.33298/2226-8553/2021.2.33.06

Толкаченко Є.А., Данилюк В.С., Семенюк М.О., Фльора А.С.

ОГЛЯД СУЧАСНИХ МЕТОДІВ В СИСТЕМАХ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ ПОТРЕБ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

У статті представлено аналіз сучасних реалізацій алгоритмів систем виявлення вторгнень та їх перспективність використання у інформаційно телекомунікаційних мережах спеціального призначення.

Необхідність в надійних системах виявлення вторгнення стоїть досить гостро. Особливо в сучасних тенденціях збільшення ролі інформаційних технологій в силових відомствах держави та на об'єктах критичної інфраструктури. Застарілі системи захисту дозволяють без особливих труднощів проводити кібератаки, що спонукає до необхідності тримати системи виявлення та захисту інформаційних систем в актуальному стані.

В умовах постійної боротьби з вторгненнями у світі було запропоновано безліч методів та алгоритмів для виявлення атаки на інформаційно-телекомунікаційні системи. Так найбільшу розповсюдженість отримали методи виявлення аномалій в роботі системи. Передовими з таких методів є інтелектуальні. Нейронні мережі, нечітка логіка, імунні системи отримали велику кількість варіантів реалізації в таких системах виявлення вторгнень.

Вдале поєднання переваг методів виявлення для конкретної інфраструктури може дозволити отримати значну перевагу над атакуючим, та зупинити проникнення. Проте на шляху всеохоплюючої реалізації подібних систем стоїть їх висока вартість у сенсі обчислювальної потужності. Питання застарілого парку комп'ютерної техніки і її повільна заміна ставлять в ситуацію постійного компромісу між передовими досягненнями в галузі захисту системи і можливостей самої системи щодо підтримки таких систем.

Ключові слова: *інформаційно-телекомунікаційна система, інформаційна безпека, кібератака, система виявлення вторгнень, загроза інформаційним системам.*

Постановка проблеми. В сучасних умовах глобального інформаційного простору, та високих вимог щодо швидкості та якості обміну інформацією в системах спеціального призначення, гостро постає питання захисту інформації в інформаційно-телекомунікаційних системах.

На сьогоднішній день держава розглядає інформацію, як критичний державний ресурс який потребує всебічного захисту. Згідно звіту національної поліції України у 2020 році кіберзлочини спричинили збитків на загальну суму 241 млн грн. [1].

В умовах гібридної війни побудова системи кібернетичної безпеки України вимагає аналізу сучасних інструментів у сфері захисту інформаційно-телекомунікаційних мереж від кібератак та визначення необхідних технологій та методів, що можуть зміцнити інформаційну безпеку .

В ситуації, що склалася, дуже важливо мати сучасну систему виявлення вторгнень, щоб забезпечити своєчасне виявлення атак на вузли або сегменти мережі інформаційно-телекомунікаційної системи та не допустити розвитку атаки на об'єкти критичної інфраструктури.

Аналіз останніх досліджень і публікацій. Через актуальність захисту різноманітних комерційних телекомунікаційних систем в сучасному світі, виходить велика кількість публікацій присвячених системам виявлення вторгнень [2], [3], [4]. Більшість публікацій присвячено на сьогоднішній день різноманітним варіаціям використання інтелектуальних методів виявлення вторгнення [5], [6], [7], [8].

Метою дослідження є аналіз та обґрунтування вибору методів та алгоритмів для перспективної системи виявлення вторгнень для потреб інформаційно-телекомунікаційних систем спеціального призначення.

Основні результати дослідження. Для порівняння тих чи інших систем виявлення вторгнень потрібно поділити їх на основні напрями, а саме: Сигнатурні методи виявлення, Методи виявлення аномалій та комбіновані методи (рис.1). [9].

Сигнатурні методи – методи побудовані на базі даних відомих атак (сигнатур). При знаходженні співпадіння з базою сигнатур система повідомляє про вторгнення. Дані методи є досить точними, не дають хибних спрацювань, проте не дають змоги розпізнати невідому загрозу.

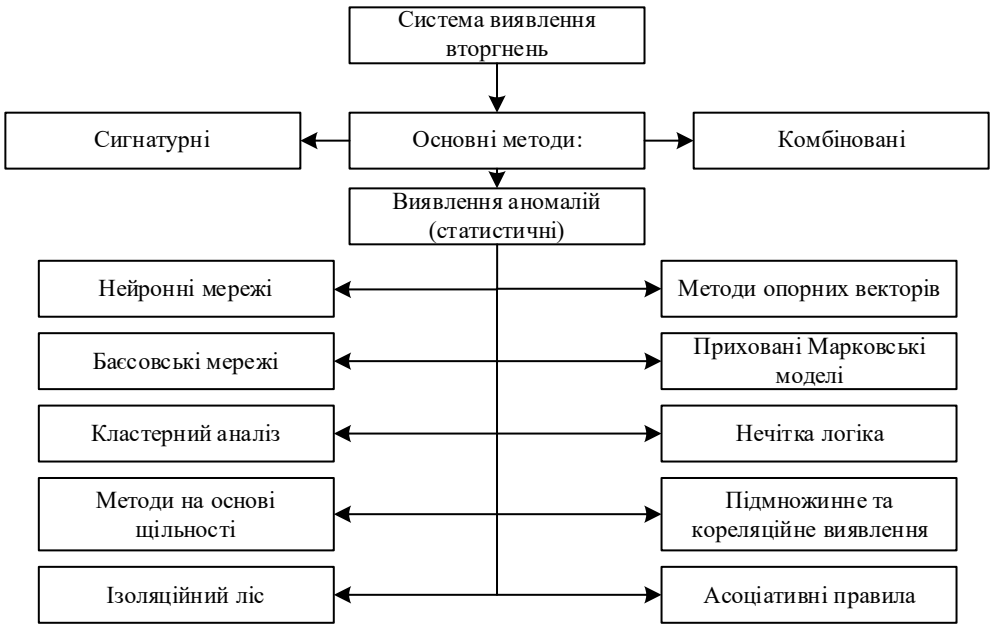

Рисунок 1 – Основні методи виявлення вторгнень

Методи виявлення аномалій або статистичні методи – методи засновані на виявлені відхилень в роботі інформаційно-телекомунікаційної системи від нормального режиму роботи. Суть подібних методів полягає в постійному аналізі процесів, що йдуть в інформаційно-телекомунікаційній системі. Будь-яка система характеризується сталим, звичайним режимом роботи, на який така система і була розрахована і побудована. У разі відхилення від такого режиму в будь-якій частині системи, фіксується аномалія. Вторгнення в систему якраз зазвичай і є подібною аномалією.

Таким системам виявлення вторгнень характерно виявлення невідомих раніше атак, але відхилення в роботі може бути спричинено і іншими факторами, що буде призводити до хибних спрацювань. Крім того системи засновані на методах виявлення аномалій сильно навантажують інформаційно-телекомунікаційну систему та вимагають виділення значних обчислювальних ресурсів.

Проте лише такий підхід дозволяє виявляти невідомі раніше атаки. Саме тому для цього методу реалізовано безліч варіантів основні з яких зображені на рис. 1.

Нейронні мережі – використовуються методи навчання нейронної мережі з метою знаходження відхилень в роботі системи. Має ряд переваг над іншими методами. Наприклад навчена один раз нейронна мережа зможе досить точно відрізняти несанкціоновані дії від збою в системі та буде мати меншу кількість помилкових спрацювань. Дана перевага а також гнучкість в навчанні мережі, простота експлуатації вже робочої системи, зробили такий підхід досить популярним, проте використання графічних прискорювачів, які в умовах сучасного світового дефіциту та дороговизни відеокарт спонукає звернути увагу на інші методи.

Комбіновані методи. Вони засновані на одночасному використанні бази сигнатур та моніторингу відхилень. Такий підхід є найбільш перспективним так як дозволяє поєднати переваги вищезазначених методів та зменшити вплив недоліків. Комбіновані системи виявлення вторгнень добре працюють як з відомими атаками так і виявляють невідомі.

Для інформаційно-телекомунікаційних систем спеціального призначення важливим є не лише виявлення відомих атак, а також попередження ще невідомих, тому використання методів заснованих на виявленні аномалій буде отримувати все більше розповсюдження, з іншого боку, досить повільне оновлення як апаратної так і програмної частини таких систем дозволяють в більшій мірі використовувати сигнатурні методи так як зазвичай програмні продукти що використовують в таких системах досить добре вивчені в плані вразливостей.

Ще одним способом зняти навантаження з інформаційно-телекомунікаційної системи є використання апаратних засобів для моніторингу системи (рис. 2).

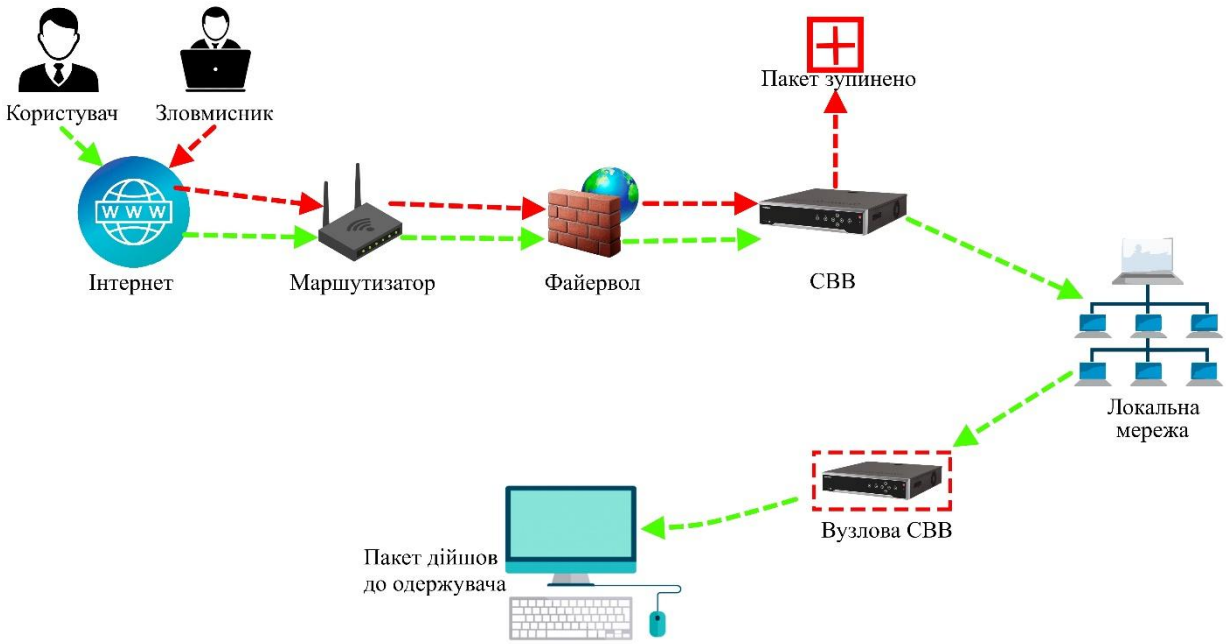

Рисунок 2 – Побудова мережі з встановленою апаратною мережевою системою виявлення вторгнень

Проте такий підхід вимагає окремих апаратних засобів що пов’язано з значними фінансовими витратами.

Висновки. Для потреб інформаційно-телекомунікаційних систем спеціального призначення варто звернути більшу увагу на комбіновані методи виявлення вторгнень, що дозволить з одного боку збільшити швидкодію та точність роботи такої системи, та зменшити кількість хибних спрацювань. Поєднання сигнатурного методу та одного з

інтелектуальних може дати можливість зменшити навантаження на інформаційно-телекомунікаційну систему. Що дозволить використовувати такі системи виявлення на застарілих обчислювальних машинах.

ЛІТЕРАТУРА

1. Звіт Національної поліції України про результати роботи у 2020 році. [Електронний ресурс]. – Режим доступу: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf
2. H. Bahsi, S. Nomm and F. B. La Torre, "Dimensionality reduction for machine learning based IoT botnet detection", Proc. 15th Int. Conf. Control Autom. Robot. Vis. (ICARCV), pp. 1857-1862, Nov. 2018.
3. Сєвєрінов О.В. Аналіз сучасних систем виявлення вторгнень / О.В. Сєвєрінов, А.Г. Хрєнов // Системи обробки інформації. – 2013. – Вип. 6(122). – С. 122 – 124.
4. Павлов І.М. Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем / І.М. Павлов, С.В. Толюпа, В.І. Ніщенко // Сучасний захист інформації. – 2014. – Вип. 4. – С.44 – 52.
5. Multi-attribute SCADA-specific intrusion detection system for power networks / Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E.G. Im, B. Pranggono, H.F. Wang // IEEE Trans. on Power Delivery. – 2014. – Vol. 29, P. 1092-1102.
6. A survey on intrusion detection and prevention systems in digital substations / S.E. Quincozes, C. Albuquerque, D. Passos, D. Mossé // Computer Networks. – 2021. – Vol. 184. – Article 107683.
7. Multidimensional intrusion detection system for IEC 61850-based SCADA networks / Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, S. Sezer // IEEE Trans. Power Deliv. – 2017. – Vol. 32, № 2. – P. 1068-1078.
8. V. C. Loi, M. Nicolau and J. McDermott, "Learning neural representations for network anomaly detection", IEEE Trans. Cybern., vol. 49, no. 8, pp. 3074-3087, Aug. 2019.
9. Liu C, Yang J, Chen R, Zhang Y, Zeng J (2011) Research on immunity-based intrusion detection technology for the internet of things. In: 2011 seventh international conference on natural computation, IEEE, vol 1, pp 212–216

REFERENCES

1. Звіт Національної поліції України про результати роботи у 2020 році. [Електронний ресурс]. – Режим доступу: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2020/npu-zvit-2020.pdf
2. H. Bahsi, S. Nomm and F. B. La Torre, "Dimensionality reduction for machine learning based IoT botnet detection", Proc. 15th Int. Conf. Control Autom. Robot. Vis. (ICARCV), pp. 1857-1862, Nov. 2018.
3. Сєвєрінов О.В. Аналіз сучасних систем виявлення вторгнень / О.В. Сєвєрінов, А.Г. Хрєнов // Системи обробки інформації. – 2013. – Вип. 6(122). – С. 122 – 124.
4. Павлов І.М. Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем / І.М. Павлов, С.В. Толюпа, В.І. Ніщенко // Сучасний захист інформації. – 2014. – Вип. 4. – С.44 – 52.
5. Multi-attribute SCADA-specific intrusion detection system for power networks / Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E.G. Im, B. Pranggono, H.F. Wang // IEEE Trans. on Power Delivery. – 2014. – Vol. 29, P. 1092-1102.
6. A survey on intrusion detection and prevention systems in digital substations / S.E. Quincozes, C. Albuquerque, D. Passos, D. Mossé // Computer Networks. – 2021. – Vol. 184. – Article 107683.

7. Multidimensional intrusion detection system for IEC 61850-based SCADA networks / Y. Yang, H.-Q. Xu, L. Gao, Y.-B. Yuan, K. McLaughlin, S. Sezer // IEEE Trans. Power Deliv. – 2017. – Vol. 32, № 2. – P. 1068-1078.

8. V. C. Loi, M. Nicolau and J. McDermott, "Learning neural representations for network anomaly detection", IEEE Trans. Cybern., vol. 49, no. 8, pp. 3074-3087, Aug. 2019.

9. Liu C, Yang J, Chen R, Zhang Y, Zeng J (2011) Research on immunity-based intrusion detection technology for the internet of things. In: 2011 seventh international conference on natural computation, IEEE, vol 1, pp 212–216

Tolkachenko E., Danyliuk V., Semeniuk M., Flora A.

OVERVIEW OF MODERN METHODS IN INVASION DETECTION SYSTEMS FOR THE NEEDS OF SPECIAL PURPOSE INFORMATION AND TELECOMMUNICATION SYSTEMS

The article presents an analysis of modern implementations of algorithms for intrusion detection systems and their prospects for use in information and telecommunications networks for special purposes.

The need for reliable intrusion detection systems is quite acute. Especially in the current trends of increasing the role of information technology in state law enforcement agencies and critical infrastructure. Outdated security systems allow cyberattacks to be carried out without much difficulty, which makes it necessary to keep information detection and protection systems up to date.

In the context of the constant fight against invasions in the world, many methods and algorithms have been proposed to detect attacks on information and telecommunications systems. Thus, the most common methods of detecting anomalies in the system. Advanced of such methods are intelligent. Neural networks, fuzzy logic, immune systems have received a large number of implementation options in such intrusion detection systems.

A successful combination of the advantages of detection methods for a particular infrastructure can provide a significant advantage over the attacker, and stop the penetration. However, on the way to the comprehensive implementation of such systems is their high cost in terms of computing power. The issue of outdated fleet of computer equipment and its slow replacement puts in a situation of constant compromise between the advanced achievements in the field of system protection and the capabilities of the system itself to support such systems.

Key words: *information and telecommunication system, information security, cyberattack, intrusion detection system, threat to information systems.*