УДК 681.12

М. В. Каневський
Т. І. Коробейнікова

МЕТОД ПАРАЛЕЛЬНОГО МОНІТОРИНГУ ПАРАМЕТРІВ КОРПОРАТИВНИХ МЕРЕЖ

Вінницький національний технічний університет

Анотація. Запропонований підхід для моніторингу найважливіших параметрів корпоративних мереж підприємств на основі декількох систем моніторингу та системи агрегації оповіщень. Розглянуто найбільш відомі, безкоштовні та гнучкі системи моніторингу та основні параметри їх взаємодії між собою та мережевими пристроями.

Ключові слова: моніторинг, системи моніторингу, система агрегації.

Abstract. The proposed approach is to monitor the most important parameters of enterprise corporate networks based on several monitoring systems and a system of aggregation of alerts. The most well-known, free and flexible monitoring systems and the main parameters of their interaction with each other and network devices are considered.

Keywords*: monitoring, monitoring systems, alerts aggregation system.*

Вступ

Жодна комп'ютерна мережа не може існувати без підтримки. Для полегшення роботи системного адміністратора та для забезпечення швидкої та ефективної роботи над збоями в мережі використовують системи які дозволяють візуалізувати процеси що протікають всередині мережі та відображають її поточний стан в режимі реального часу.Такі системи називаються «системами моніторингу» і широко використовуються в підприємствах із власними корпоративними мережами. Інформаційна система моніторигу – це комплексне рішення, що включає в себе декілька систем моніторингу, систему оповіщень та систему агрегації цих оповіщень, що являє собою зручний та зрозумілий користувацький інтерфейс.

Основні можливості систем моніторингу:

- збір інформації про події з різних пристроїв забезпечення інформаційної безпеки і мережевих пристроїв;
- візуалізацію подій в режимі реального часу;
- підтримку сигнатурних і «поведінкових» методів виявлення аномалій і атак;
- можливість створення власних правил кореляції;
- можливість управління активними мережевими пристроями з метою блокування шкідливого трафіку;
- прогнозування результатів атаки;
- аналіз ризику захищаємої системи;
- автоматичне визначення статусу події (атака, сканування тощо);
- можливість обробки та аналізу інцидентів безпеки;
- фокусування уваги на пріоритетних захищаємих вузлах;
- вбудована система роботи з інцидентами, можливість інтеграції з існуючою;
- автоматична реакція на інциденти.

Результати дослідження

Даний метод полягає у тому, що декілька систем моніторингу взаємодіють між собою проводячи повний обсяг моніторингу одних і тих же параметрів або бізнес процесів у корпоративній мережі. Також цей метод передбачає взаємодію систем моніторингу на етапі самоперевірок та паралельних перевірок системи моніторингу, тобто одна система моніторингу моніторить іншу систему на предмет збоїв та не коректної роботи.

Усі результати моніторингу систем одна одної можна відобразити у системі віртуалізації даних що дозволить:

- легко помічати недоліки в роботі системи моніторингу;
- покрити моніторингом саму інформаційну систему;
- прогнозувати розвиток інформаційної системи;

– вчасно масштабувати потужності на яких знаходиться інформаційна система моніторингу.

Ще однією важливою функцією є можливість додати до системи агрегації оповіщення що до несправності або не коректної роботи однієї с систем моніторингу, що дозволить системному адміністратору швидко усунути проблему. Також при використанні методу паралельних перевірок є 100% гарантія того, що при несправності однієї з систем моніторингу, інша візьме на себе всі функції і це ніяк не вплине на подальший моніторинг корпоративної мережі поки проблема з однією з систем не буде вирішено.

Метод паралельних перевірок не означає, що для цього необхідно використовувати у двічі потужніші сервери на яких будуть знаходитись системи моніторингу, оскільки усі системи можуть використовувати спільні бази даних. Це дає можливість зекономити 100% витрат на апаратне устаткування. Практичну схему методу паралельних перевірок з використанням реальних систем моніторингу подано на рисунку 1.

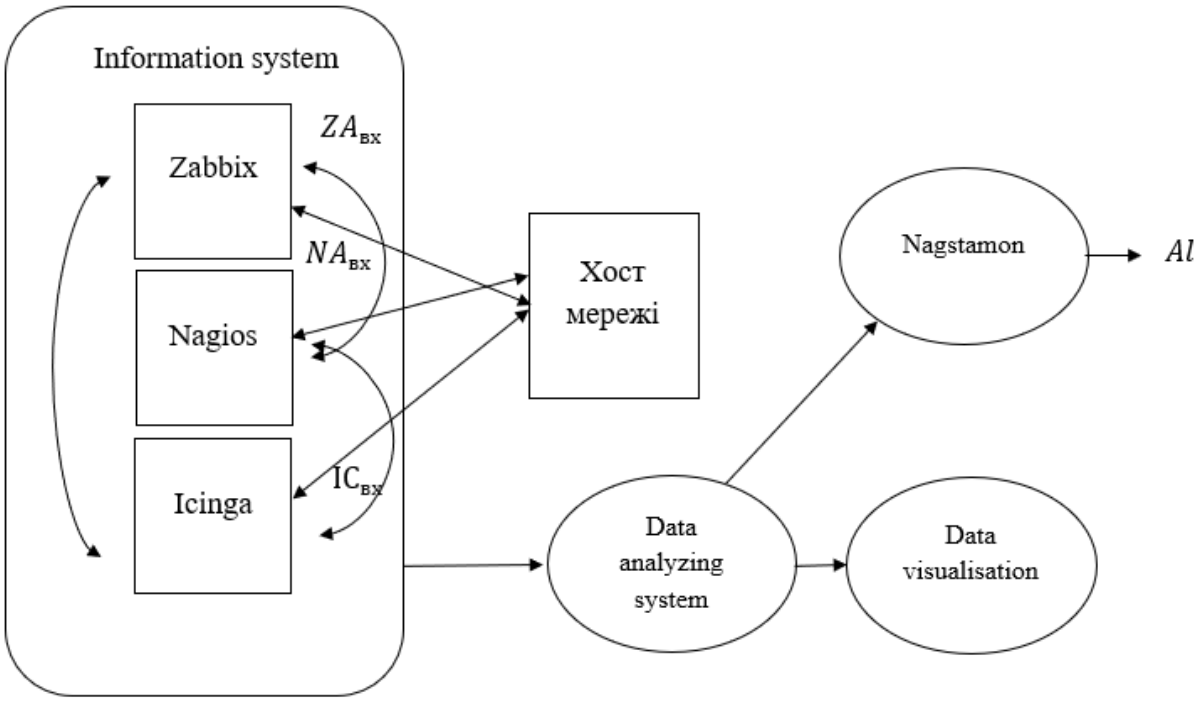

Рисунок 1 – Схема методу паралельних перевірок

Висновки

Використання методу паралельних перевірок із залученням декількох систем моніторингу дає більш надійну та чітку картину процесів у мережі. Даний метод можна використовувати, як для моніторингу бізнес процесів, так і для відстеження продуктивності мережевих пристроїв та навантаження на них. Даний метод дозволяє значно підвищити надійність та актуальність процесу моніторингу корпоративних мереж.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Побудова швидкісних мультисервісних мереж / Трояновська Т. І., Савицька Л. А., Максюта М. О., Поліщук Д. М. // Міжнародна науково-технічна конференція “Smart and Young”. – Київ, 2016. – №8, с. 25–27.
2. Zabbix. Практичний посібник / Андреа Далле Вакке. // ДМК Пресс. – Київ, 2017, с. 10–26.
3. Nagios / Sykley Julie-Anne // USA, 2011. с. 309–315.
4. Буров Є.В.. Комп’ютерні мережі. / 2-е вид., оновл. і доп. – Львів –Бак, 2003
5. Болілий В.О., Котяк В.В. Комп'ютерні мережі. Навчальний посібник. - Кіровоград: ЦОП Авангард, 2008.- 146с.
6. Кулаков Ю.О., Луцький Г.М. Комп’ютерні мережі. Підручник –К.: Юніор, 2003. -400с.
7. Нанс. Б. Комп’ютерні мережі: пер. з англ. / Нанс Бернард- М.: БИНОМ, 2006. - 400 с.
8. Браун С. Віртуальні приватні мережі / Браун Сімеон - М.: Лорі, 2009. - 502с.
9. Абрамов В. О., Клименко С. Ю. Базові технології комп’ютерних мереж, навчальний посібник, Київ 2011 – 291 с.

Каневський Микола Володимирович – аспірант, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: brainiac.kanevskii@gmail.com

Коробейнікова Тетяна Іванівна – канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет

Mykola V. Kanevskyi – Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: brainiac.kanevskii@gmail.com

Tatyana I. Korobeinikova – Cand. Sc. (Eng.), Assistant Professor of the Computer Techniques Chair, Vinnytsia National Technical University.