УДК 007.51 Вестник УрФО № 2(52) / 2024, с. 68–76

Быкасов А. В., Соколов А. Н. DOI: 10.14529/secur240207

СТАТИСТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ ВЛИЯНИЯ КОМБИНИРОВАННОГО МЕТОДА АКТИВНОГО СКАНИРОВАНИЯ НА СТАБИЛЬНОСТЬ ФУНКЦИОНИРОВАНИЯ СЕТИ АСУ ТП

Методы активного сканирования все шире применяются в системах обнаружения вторжений (СОВ) для сбора и анализа сетевой информации. Поскольку активное сканирование предполагает отклик от устройств сети, это может повлиять на стабильность работы сетевого оборудования, что является критичным для промышленных сетей.

В работе представлена статистическая модель оценки влияния комбинированного метода активного сканирования на стабильность функционирования сети АСУ ТП. Проведены эксперименты для оценки влияния комбинированного метода активного сканирования на стабильность функционировании сети АСУ ТП. Полученные результаты, представленные в сравнении с результатами для распространенного инструмента сетевого сканирования Nmap, дают сделать вывод о том, что комбинированный метод активного сканирования оказывает меньшее влияние на сеть, а также обеспечивает стабильность при сканировании, тем самым не нарушая работоспособность сети АСУ ТП.

Ключевые слова: *автоматизированная система управления технологическим процессом (АСУ ТП), активное сканирование, система обнаружения вторжений (СОВ), контроль сетевых устройств, протокол определения адреса (ARP), протокол межсетевых управляющих сообщений (ICMP).*

STATISTICAL MODEL FOR ASSESSING THE IMPACT OF THE COMBINED ACTIVE SCANNING METHOD ON THE STABILITY OF THE INDUSTRIAL CONTROL NETWORK

Active scanning methods are increasingly used in intrusion detection systems (IDS) to collect and analyze network information. Since active scanning involves response from network devices, this can affect the stability of network equipment, which is critical for industrial networks.

The paper presents a statistical model for assessing the influence of the combined active scanning method on the stability of the functioning of the industrial control network. Experiments were carried out to evaluate the influence of the combined active scanning method on the stability of the industrial control network. The results obtained, presented in comparison with the results for the common network scanning tool Nmap, lead to the conclusion that the combined method of active scanning has less impact on the network, and also provides stability during scanning, thereby not disrupting the functionality of the ICS network.

Keywords: *industrial control system (ICS), active scanning, intrusion detection system (IDS), control of network devices, address resolution protocol (ARP), internet control message protocol (ICMP).*

Для обеспечения информационной безопасности сетей автоматизированных систем управления технологическими процессами (АСУ ТП) применяются системы обнаружения и предотвращения вторжений (СОВ и СПВ). Эти системы предназначены для мониторинга целостности сетевого трафика и программного обеспечения, функционирующего на узлах сети. Данный функционал может быть реализован полностью посредством пассивного анализа сети, включающего сниффинг и пассивный анализ трафика. Однако такой метод требует значительных временных затрат и в некоторых случаях может не обеспечивать достаточную точность. Поэтому системы обнаружения вторжений часто дополняются методами активного сканирования [1], суть которых заключается в отправке СОВ специально сформированных запросов целевым узлам, всем узлам, периферийному оборудованию или всем типам устройств, а затем интерпретации полученных ответов [2].

Более оперативное получение информации об используемых устройствах, установленном ПО и конфигурациях в сети АСУ ТП обеспечивается путем интеграции СОВ с установленным на рабочие станции специализированным программным обеспечением — агентом инвентаризации, который передает информацию либо непосредственно в СОВ, либо через систему управления информационной безопасностью (SIEM). Этот метод применим только к устройствам, на которые возможно свободно устанавливать прикладное ПО. Однако множество встраиваемых систем в АСУ ТП, таких как программируемые логические контроллеры (ПЛК), распределённый ввод-вывод, сетевое оборудование и т.д., обычно не позволяют установить дополнительное ПО [3 – 5].

Таким образом, возникает необходимость применения активного сканирования, запускаемого средствами самой СОВ или сторонними ресурсами. Однако такие методы

нарушают принцип невмешательства СОВ в рабочий процесс сети АСУ ТП для получения информации. Следовательно, для обеспечения информационной безопасности сетей АСУ ТП и одновременной минимизации вмешательства в их рабочий процесс необходима разработка специализированных методов активного сканирования [6,7].

Целью работы является разработка статистической модели для оценки влияния методов активного сканирования на стабильность функционирования сети АСУ ТП. Модель должна позволять на основе статистических данных работы метода активного сканирования делать заключение о пригодности метода для его применения в сетях АСУ ТП.

Для оценки метода берутся такие показатели, как время выполнения каждого этапа сканирования (если это возможно), среднее время сканирования, а также средний показатель всплесков трафика, возникающих при сканировании. В качестве статистических показателей для оценки работы модели рассчитываются:

выборочное математическое ожидание

$$M = \frac{\sum_{i=1}^{n} a[i]}{n} \quad (1)$$

где $a[i]$ – элемент экспериментально полученного статистического набора данных, n – объем выборки;

и выборочная дисперсия:

$$D = \frac{\sum_{i=1}^{n} (a[i]-M)^2}{n-1} \quad (2)$$

где $a[i]$ – элемент выборки, n – объем выборки.

Рассмотренный комбинированный метод активного сканирования [8] состоит из 4-х этапов сканирования:

1. ARP-сканирование. На этом этапе отправляется широковещательный запрос в сеть с целью обнаружения подключенных хостов, а также нахождения их IP- и MAC-адресов. В качестве входных данных используется подсеть или IP-адрес устройства. В результате получается список устройств, содержащий IP- и MAC-адреса.

2. CMP-сканирование. В качестве входных данных используется список IP-адресов, полученный на предыдущем этапе. Далее, на каждое устройство из списка отправляется ping-запрос. Если ответ приходит, мы считаем это устройство «живым». В результате получаем список «живых» IP-адресов.

3. SNMP-сканирование. На данном этапе проводится опрос устройств по протоколу SNMP с целью получения информации об устройстве: марка, модель, имя в сети и т.д. В качестве входных данных используется результат ICMP-сканирования.

4. Сканирование портов. На данном этапе проводится поиск открытых портов устройств посредством отправки TCP-пакетов. Сканирование может проводится как по определенному заранее списку «популярных» портов, так и по заданному вручную. В качестве входных данных также используется список IP-адресов, полученный на этапе ICMP-сканирования.

Nmap – инструмент для сканирования сетей, поддерживающий как пассивные, так и активные методы активного сканирования. Он может быть использован для проверки

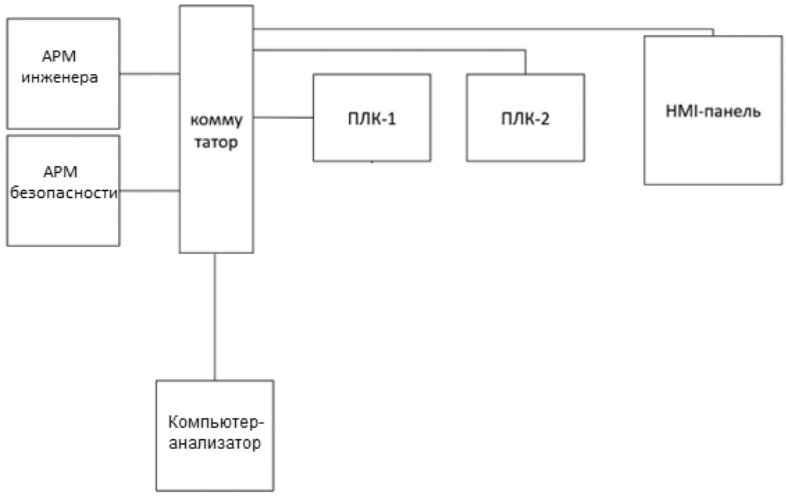

Рис. 1. Схема сетевых соединений первого сегмента лабораторного стенда

Рис. 2. Схема сетевых соединений второго сегмента лабораторного стенда

безопасности, просто для определения сервисов, запущенных на узле, для идентификации ОС и приложений и т.д.

Экспериментальные исследования проводились на лабораторном стенде, состоящем из двух сегментов. Первый сегмент осуществляет сетевое взаимодействие двух ПЛК (рис. 1). Состав оборудования:

- ПЛК-1, Siemens-1512;
- ПЛК-2, Siemens-1510;
- Коммутатор Scalance XC208;
- АРМ инженера, содержащая ПО для программирования ПЛК;
- АРМ оператора системы безопасности;
- HMI- панель для визуализации и управления.
- На ПЛК загружена программа, эмулирующая металлонарезной станок.

Для проверки методов сканирования к стенду подключен ноутбук, исполняющий роль внешнего сканирующего устройства.

Второй сегмент лабораторного стенда состоит из одного ПЛК, на котором эмулируется программа управления насосами. Состав оборудования второго сегмента сети (рис. 2):

- ПЛК KEAZ OptiLogic L-CPU-2-M;
- Коммутатор;
- АРМ инженера, содержащая ПО для программирования ПЛК;
- АРМ оператора системы безопасности;
- HMI- панель для визуализации и управления.

Для статистической оценки влияния метода активного сканирования на промышленную сеть проведен ряд экспериментов для накопления статистической базы. Для каждого сегмента лабораторного стенда проведены сканирования с использованием комбинированного метода активного сканирования и инструмента Nmap.

При сканировании первого сегмента сети оба инструмента показали следующий результат: все хосты в сети были найдены, все ответили на ping-запрос, хостам присвоен статус «жив». От двух хостов получена информация путем сканирования методом SNMP. Все открытые порты были найдены. При этом, рассмотренные методы сканирования оказали различное влияние на сеть.

На рисунке 3 представлены статистические результаты для среднего показания всплесков трафика, возникавших при сканированиях. Верхняя кривая соответствует результатам сканирования с использованием Nmap (выборочное математическое ожидание равно 1835,7, выборочная дисперсия – 84427,41). Нижняя кривая соответствует результатам сканирования с использованием комбинированного метода активного сканирования (выборочное математическое ожидание равно 184,733, выборочная дисперсия – 116,929). Из графиков видно, что выборочное математическое ожидание среднего показателя всплесков для Nmap на порядок больше, чем для комбинированного метода. Поэтому можно сделать заключение о том, что Nmap оказывает значительно большее влияние на сеть, чем комбинированный метод. Выборочная дисперсия для комбинированного метода в несколько раз меньше, чем у Nmap. Следовательно, комбинированный метод показывает более стабильные результаты.

На рисунке 4 представлены статистические результаты общего времени сканирования. Верхняя кривая соответствует результа-

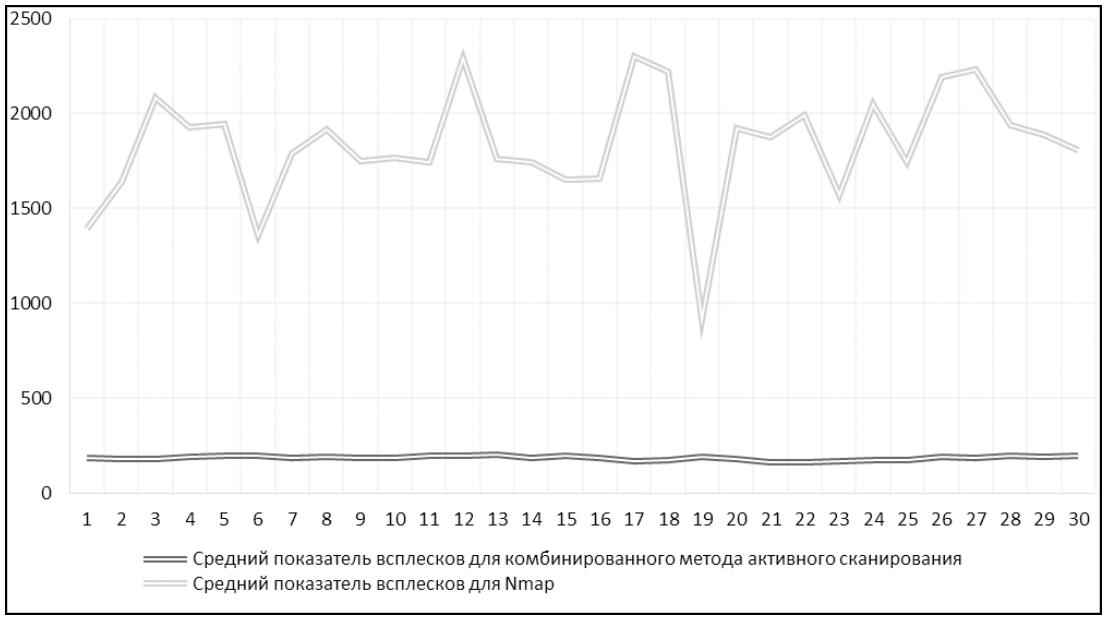

Рис. 3. Сравнение среднего показателя всплесков для 1 сегмента сети

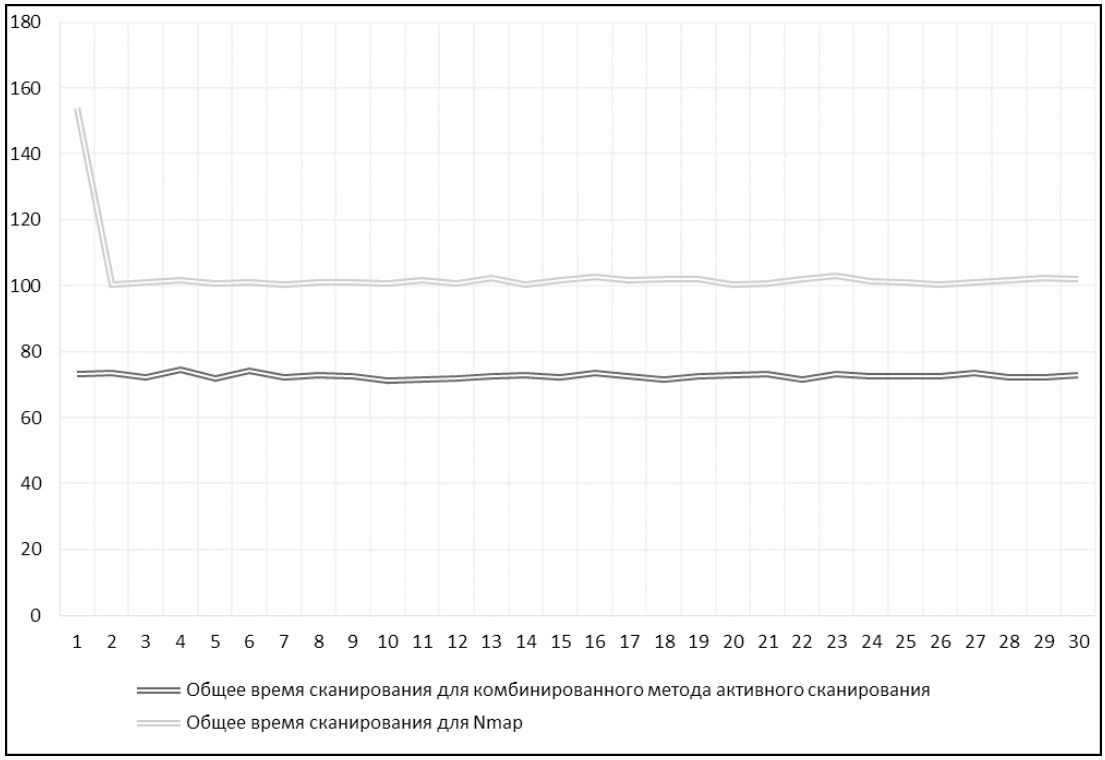

Рис. 4. Сравнение общего времени сканирования для 1 сегмента сети

там сканирования с использованием Nmap (выборочное математическое ожидание равно 103,129, выборочная дисперсия – 89,593). Нижняя кривая соответствует результатам сканирования с использованием комбинированного метода активного сканирования (выборочное математическое ожидание равно 72,714, выборочная дисперсия – 0,596.). Из графиков видно, что выборочное математическое ожидание общего времени сканирования для Nmap больше, чем для комбинированного метода. Выборочная дисперсия для комбинированного метода в несколько раз меньше, чем у метода Nmap. Следовательно, комбинированный метод показывает более стабильные результаты сканирования, и про-

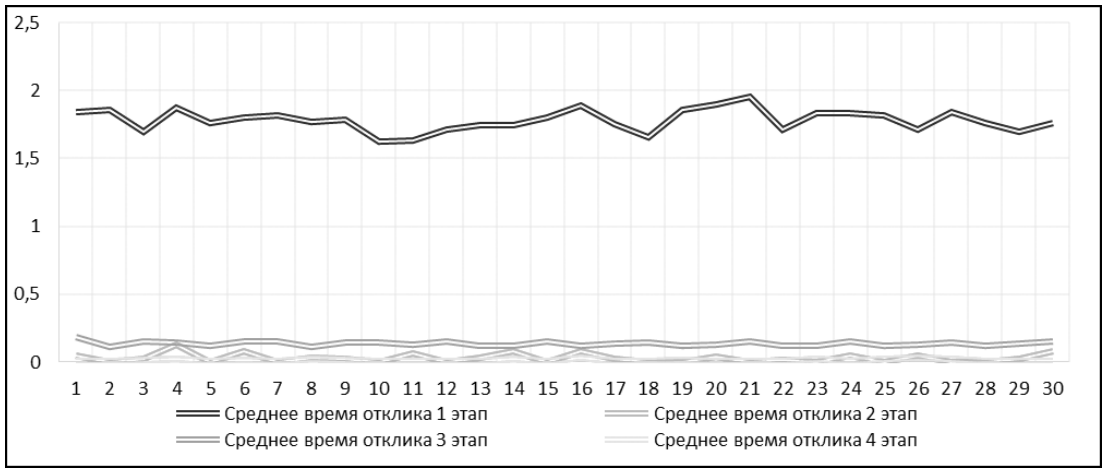

Рис. 5. Сравнение среднего времени отклика для этапов комбинированного метода активного сканирования для 1 сегмента сети

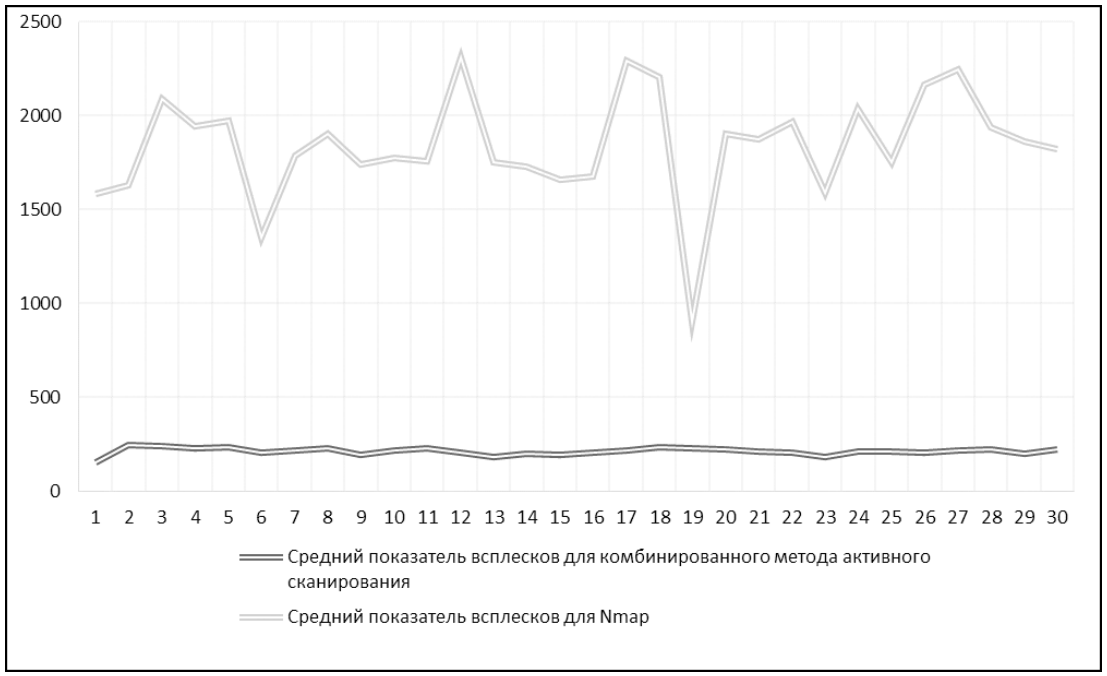

Рис. 6. Сравнение среднего показателя всплесков для 2 сегмента сети

должительность сканирования при этом меньше, чем у Nmap.

На рисунке 5 представлены статистические результаты среднего времени отклика для этапов комбинированного метода активного сканирования. Их выборочные математические ожидания небольшие, а выборочные дисперсии близки к нулю. Следовательно, можно сделать заключение о предсказуемости результатов работы комбинированного метода с точки зрения минимального влияния на работу сети. При этом Nmap не позволяет оценить среднее время отклика.

При сканировании второго сегмента сети оба инструмента показали следующий результат: все хосты в сети были найдены, все ответили на ping-запрос, хостам присвоен статус «жив». Поскольку хосты не настроены на взаимодействие по протоколу SNMP, получить информацию о них невозможно. Все открытые порты были найдены. При этом рассмотренные методы сканирования оказали различное влияние на сеть.

На рисунке 6 представлены статистические результаты для среднего показания всплесков трафика, возникавших при сканированиях. Верхняя кривая соответствует результатам сканирования с использованием Nmap (выборочное математическое ожидание равно 1840,693, выборочная дисперсия - 80926,009). Нижняя

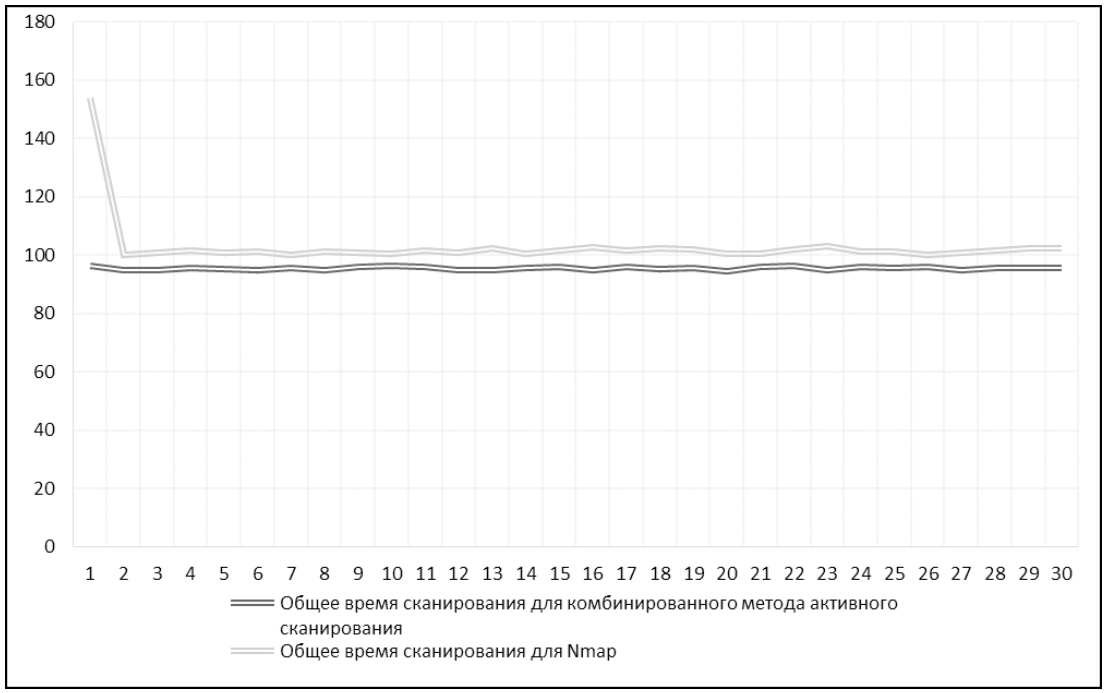

Рис. 7. Сравнение общего времени сканирования для 2 сегмента сети

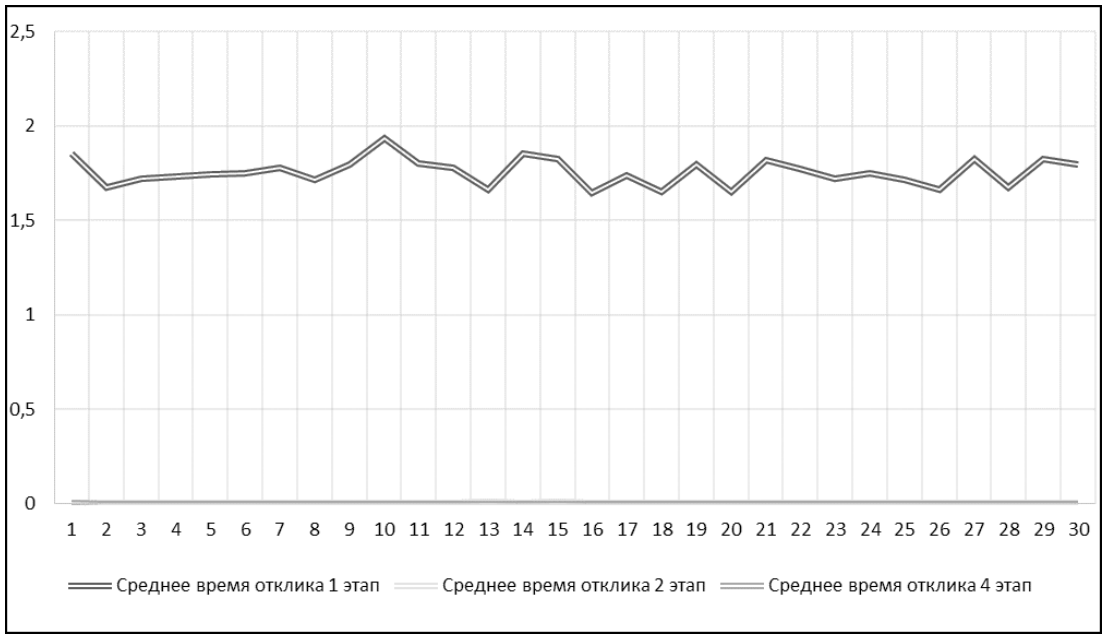

Рис. 8. Сравнение среднего времени отклика для этапов комбинированного метода активного сканирования для 2 сегмента сети

кривая соответствует результатам сканирования с использованием комбинированного метода активного сканирования (выборочное математическое ожидание равно 212,7, выборочная дисперсия - 358,477). Из графиков видно, что выборочное математическое ожидание среднего показателя всплесков для Nmap на порядок больше, чем для комбинированного метода. Поэтому можно сделать заключение о том, что Nmap оказывает значительно большее влияние на сеть, чем комбинированный метод. Выборочная дисперсия для комбинированного метода в несколько раз меньше, чем у Nmap. Следовательно, комбинированный метод показывает более стабильные результаты.

На рисунке 7 представлены статистические результаты общего времени сканирования. Верхняя кривая соответствует результатам сканирования с использованием Nmap (выборочное математическое ожидание равно 103,348, выборочная дисперсия - 84,847). Нижняя кривая соответствует результатам сканирования с использованием комбинированного метода активного сканирования (выборочное математическое ожидание равно 95,513, выборочная дисперсия - 0,295). Из графиков видно, что выборочное математическое ожидание общего времени сканирования для Nmap больше, чем для комбинированного метода. Выборочная дисперсия для комбинированного метода в разы меньше, чем у Nmap. Следовательно, комбинированный метод показывает более стабильные результаты сканирования, и продолжительность сканирования при этом меньше, чем у Nmap.

На рисунке 8 представлены статистические результаты среднего времени отклика для этапов комбинированного метода активного сканирования. Их выборочные математические ожидания небольшие, а выборочные дисперсии близки к нулю. Следовательно, можно сделать заключение о предсказуемости результатов работы комбинированного метода с точки зрения минимального влияния на работу сети. При этом Nmap не позволяет оценить среднее время отклика.

Исходя из результатов экспериментов можно сделать вывод, что комбинированный метод активного сканирования имеет следующие статистические характеристики, в сравнении с Nmap. Выборочное математическое ожидание для среднего показателя всплесков и для общего времени сканирования меньше, чем у Nmap. Следовательно, комбинированный метод активного сканирования оказывает меньше влияния на сеть, а также занимает меньше времени при сканировании сети. Выборочная дисперсия для среднего показателя всплесков и для общего времени сканирования значительно меньше, чем у Nmap. Из этого можно сделать вывод, что комбинированный метод активного сканирования показывает стабильные результаты сканирования, тем самым не нарушая работоспособность сети АСУ ТП.

Литература

1. Павленко А. Сканирование на наличие уязвимостей. / А. Павленко // Отус онлайн-образование. – 2022. – URL: https://otus.ru/nest/post/2468/ (дата обращения 21 апреля 2024 г.)

2. Проведение активных опросов устройств с помощью Kaspersky Industrial CyberSecurity for Networks. - https://support.kaspersky.com/ KICSforNetworks/4.0/ru-RU/236044.htm (дата обращения 21 апреля 2024 г.)

3. Активное сканирование с помощью Nozomi Networks Guardian. - https://www.nozominetworks.com/downloads/US/Nozomi-Networks-Smart-Polling-Data-Sheet.pdf (дата обращения 21 апреля 2024 г.)

4. Hansson A. Analyzing Internet-connected industrial equipment. / A. Hansson, M. Khodari, A. Gurtov. // 2018 International Conference on Signals and Systems (ICSigSys). – 2018. – С. 29-35. – DOI: 10.1109/ICSIGSYS.2018.8372775 – URL: https://www.researchgate.net/publication/325635836_Analyzing_Internet-connected_industrial_equipment (дата обращения 21 апреля 2024 г.)

5. Исследование: более 4 000 устройств АСУ ТП уязвимы для удаленных атак / InfoWatch. – 2021. – URL: https://www.infowatch.ru/resources/blog /issledovanie-bolee-4-000-ustroystv-asu-tp-uyazvimy-dlya-udalennykh-atak (дата обращения 21 апреля 2024 г.)

6. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования [Текст]: ГОСТ Р МЭК 61508-1-2012. – Введ.2013-08-01. – М.: Федеральное агентство по техническому регулированию и метрологии, 2012. – 586 с.

7. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению [Текст]: ГОСТ Р МЭК 61508-3-2012. – Введ. 2013-08-01. – М.: Федеральное агентство по техническому регулированию и метрологии, 2012. – 588 с.

8. Обеспечение безопасности сети АСУ ТП при использовании комбинированного метода активного сканирования // БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА. Сборник научных трудов XXII Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. 2024. – С. 159-166.

References

1. Pavlenko A. Skanirovaniye na nalichiye uyazvimostey. / A. Pavlenko // Otus onlayn-obrazovaniye. – 2022. – URL: https://otus.ru/nest/post/2468/ (data obrashcheniya 21 aprelya 2024 g.)

2. Provedeniye aktivnykh oprosov ustroystv s pomoshch'yu Kaspersky Industrial CyberSecurity for Networks. Rezhim dostupa: https://support.kaspersky.com /KICSforNetworks/4.0/ru-RU/236044.htm (data obrashcheniya 21 aprelya 2024 g.)

3. Aktivnoye skanirovaniye s pomoshch'yu Nozomi Networks Guardian. Rezhim dostupa: https://www.nozominetworks.com/downloads/US/Nozomi-Networks-Smart-Polling-Data-Sheet.pdf (data obrashcheniya 21 aprelya 2024 g.)

4. Hansson A. Analyzing Internet-connected industrial equipment. / A. Hansson, M. Khodari, A. Gurtov. // 2018 International Conference on Signals and Systems (ICSigSys). – 2018. – C. 29-35. – DOI: 10.1109/ICSIGSYS.2018.8372775 – URL: https://www.researchgate.net/publication/325635836_Analyzing_Internet-connected_industrial_equipment (data obrashcheniya 21 aprelya 2024 g.)

5. Issledovaniye: boleye 4 000 ustroystv ASU TP uyazvimy dlya udalennykh atak / InfoWatch. – 2021. – URL: https://www.infowatch.ru/resources/blog /issledovanie-bolee-4-000-ustroystv-asu-tp-uyazvimy-dlya-udalennykh-atak (data obrashcheniya 21 aprelya 2024 g.)

6. Funktsional'naya bezopasnost' sistem elektricheskikh, elektronnykh, programmiruyemykh elektronnykh, svyazannykh s bezopasnost'yu. Chast' 1. Obshchiye trebovaniya [Tekst]: GOST R MEK 61508-1-2012. – Vved. 2013-08-01. – M.: Federal'noye agentstvo po tekhnicheskomu regulirovaniyu i metrologii, 2012. – 586 s.

7. Funktsional'naya bezopasnost' sistem elektricheskikh, elektronnykh, programmiruyemykh elektronnykh, svyazannykh s bezopasnost'yu. Chast' 3. Trebovaniya k programmnomu obespecheniyu [Tekst]: GOST R MEK 61508-3-2012. – Vved. 2013-08-01. – M.: Federal'noye agentstvo po tekhnicheskomu regulirovaniyu i metrologii, 2012. – 588 s.

8. Obespecheniye bezopasnosti seti ASU TP pri ispol'zovanii kombinirovannogo metoda aktivnogo skanirovaniya // BEZOPASNOST' INFORMATSIONNOGO PROSTRANSTVA. Sbornik nauchnykh trudov XXII Vserosciyskoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh. 2024. – S. 159-166.

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой «Защита информации» федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, Уральский федеральный округ, Челябинская область, г. Челябинск, просп. В.И. Ленина, д. 76. E-mail: sokolovan@susu.ru

БЫКАСОВ Андрей Витальевич, аспирант федерального государственного автономного образовательного учреждения высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, Уральский федеральный округ, Челябинская область, г. Челябинск, просп. В.И. Ленина, д. 76. E-mail: andreybikasov@gmail.com

SOKOLOV Alexander Nikolaevich, Candidate of Technical Sciences, Associate Professor, Head of the Information Security Department of the Federal State Autonomous Educational Institution of Higher Education South Ural State University (National Research University). 454080, Ural Federal District, Chelyabinsk Region, Chelyabinsk, prosp. IN AND. Lenina, d. 76. E-mail: sokolovan@susu.ru

BYKASOV Andrey Vitalievich, post-graduate student of the Federal State Autonomous Educational Institution of Higher Education "South Ural State University (National Research University)". 454080, Ural Federal District, Chelyabinsk Region, Chelyabinsk, prosp. IN AND. Lenina, d. 76. E-mail: andreybikasov@gmail.com