УДК 004.384 Вестник УрФО № 4(46) / 2022, с. 88–96

Богер А.М., Соколов А.Н., Морозов И.А.

DOI: 10.14529/secur220410

ОЦЕНКА ВОЗДЕЙСТВИЙ DOS-АТАКИ НА ТРАФИК ОБМЕНА ДАННЫМИ МЕЖДУ ПРОГРАММИРУЕМЫМИ ЛОГИЧЕСКИМИ КОНТРОЛЛЕРАМИ SIMATIC 1510 И SIMATIC 1512[1]

В работе исследована эмуляция распределенного DoS-воздействия на лабораторный стенд, осуществляющий взаимодействие двух программируемых логических контроллеров: SIMATIC 1510 и SIMATIC 1512 в автоматизированной системе управления технологическим процессом. В ходе работы совершены внутреннее и внешнее DoS-воздействие, оценены продолжительность выполнения программного цикла контроллера и возможность передачи данных между контроллером и периферийными устройствами, сделан вывод о значительном влиянии DoS-воздействия на рабочий процесс контроллера.

Ключевые слова: *программируемый логический контроллер (ПЛК), сетевые атаки, кибератака, DDoS, АСУ ТП.*

Boger A.M., Sokolov A.N., Morozov I.A.

EVALUATION OF DOS ATTACK IMPACT ON DATA TRAFFIC BETWEEN SIMATIC 1510 AND SIMATIC 1512 PLCS

The paper studies the emulation of a distributed DoS impact on a laboratory stand that interacts with two programmable logic controllers: SIMATIC 1510 and SIMATIC 1512 in an automated process control system. In the course of work, internal and external DoS impacts were made, the duration of the controller program cycle and the possibility of data transfer between

[1] Исследование поддержано грантом Российского научного фонда (проект № 22-71-10095).

the controller and peripheral devices were estimated, and a conclusion was made about the significant impact of DoS impacts on the controller's workflow.

Keywords: *programmable logic controller (PLC), network attacks, cyberattack, DDoS, ICS.*

Стабильность сетевого взаимодействия между программируемыми логическими контроллерами (далее ПЛК) является очень важной частью работоспособности производственных линий заводов и фабрик. Отсутствие стабильности может привести к невозможности обмена управляющими данными между контроллерами и их периферией. А это в свою очередь может привести к потере прибыли и авариям на производстве.

Для проверки возможности сетей уровня контроля автоматизированными системами управления технологическими процессами (АСУ ТП) поддерживать собственную стабильность было принято решение подвергнуть сетевое соединение двух ПЛК нагрузке в виде эмуляции DoS-атаки. Данный тип атаки был выбран как один из наиболее легко осуществимых и наиболее вероятных [1].

В работе использовался лабораторный стенд, осуществляющий сетевое взаимодействие двух ПЛК. Состав стенда:

- ПЛК-1, SIMATIC 1512;
- ПЛК-2, SIMATIC 1510;
- Коммутатор Scalance XC208;
- АРМ инженера, содержащая ПО для программирования ПЛК;
- HMI- панель для визуализации и управления.

Основной рабочей программой ПЛК является управление машиной непрерывного литья заготовок. На АРМ инженера находится симуляция машины, созданная в среде Unity, которая по протоколу PROFINET передает сигналы датчиков, принимает управляющие сигналы и симулирует работу механизмов машины. Управление исполнительными механизмами машины распределено между двумя ПЛК. В процессе работы ПЛК-1 регулярно осуществляет проверку данных, которые обрабатывает ПЛК-2, сравнивая текущие данные датчиков с данными тех же датчиков, но хранящимися в памяти ПЛК-2. Для создания распределенного воздействия к стенду подключен ноутбук, исполняющий роль компьютера нарушителя и/или закладного устройства (рис. 1).

В качестве источника трафика для DoS-воздействия было выбрано ПО Low Orbit Ion Cannon (LOIC). Этот выбор был сделан по следующим критериям: свободное распространение, открытый код, удобство использования [2].

До начала работы со стендом была произведена оценка воздействия LOIC на персональный компьютер. В результате DoS-воздействия было отмечено увеличение требуемой памяти для системных процессов, связанных с сетевым взаимодействием, более чем в 50 раз (до 15% от возможностей центрального процессора), что говорит о работоспособности приложения LOIC.

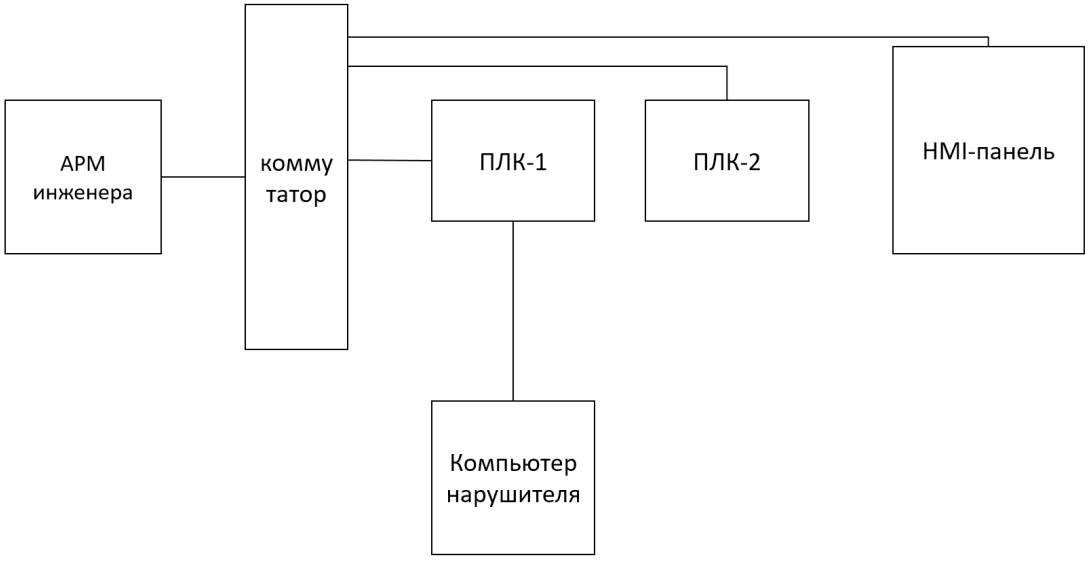

Рис.1. Схема сетевых соединений лабораторного стенда

В качестве метода DoS-воздействия были выбраны UDP-запросы по IP-адресу ПЛК-1 (рис.2). Активность воздействия – около 100000 запросов в секунду. В качестве источников DoS-воздействия были выбраны 2 хоста: ранее упомянутый компьютер нарушителя, представляющий собой внешнее воздействие, и АРМ инженера АСУ ТП, представляющий собой воздействие внутри самой сети АСУ ТП.

В процессе испытаний каждый из хостов по отдельности генерировал DoS-воздействие с интенсивностью до 100000 запросов в секунду. Также было проверено влияние одновременного DoS-воздействия с обоих хостов.

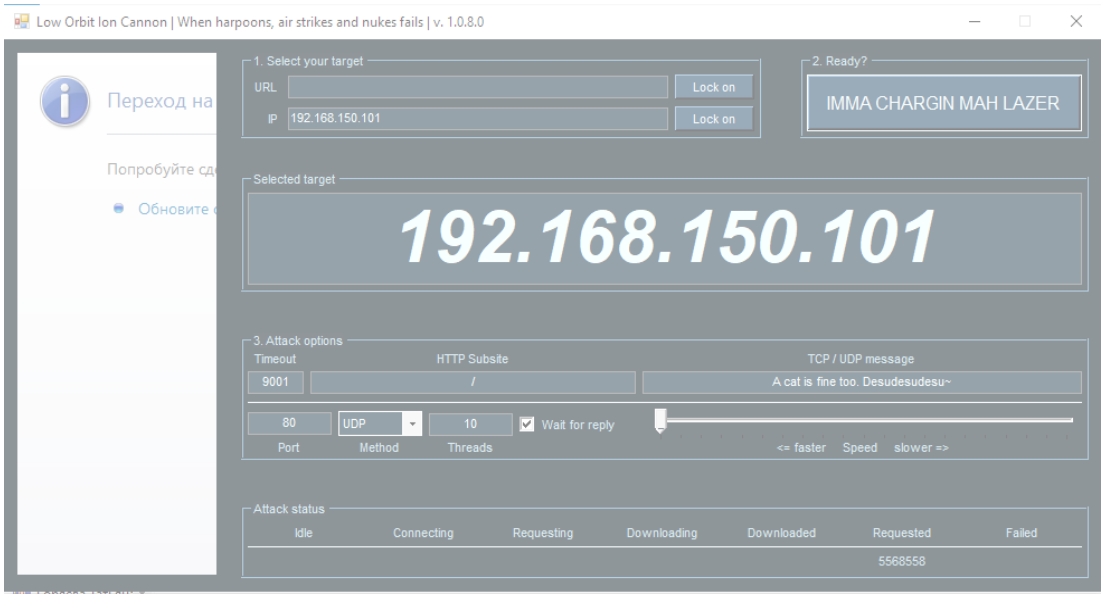

Рис.2. Интерфейс и настройки ПО LOIC

Первоначально тесты проводились при прямом подключении хоста-источника атаки к порту сетевого интерфейса ПЛК-1.

Для предварительного расчета стабильности работы ПЛК под DoS-воздействием было произведено обращение к теории массового обслуживания (ТМО). Согласно ей ПЛК, принимающий сетевые запросы можно представить, как одноканальную систему массового обслуживания (СМО) с ограниченной длиной очереди. Это обуславливается одним процессором и ограниченными оперативной памятью, и сетевым буфером.

Согласно ТМО, существует возможность рассчитать вероятность отказа в обслуживании новому пакету данных, приходящему по сети. Эта вероятность равна

$$\rho_{отк} = \rho^{m+1}\rho_0, \quad (1)$$

где $\rho_{отк}$ – вероятность отказать новому пакету данных в обслуживании, ρ – коэффициент загрузки СМО, m – максимальное количество пакетов, принятых в обработку (число мест в очереди), ρ_0 – вероятность отсутствия пакета данных на обработку.

Коэффициент загрузки системы ρ вычисляется по формуле

$$\rho = \lambda/\mu, \quad (2)$$

где λ – интенсивность поступления пакетов данных или же интенсивность DoS-воздействия, μ – интенсивность обслуживания пакетов данных.

Вероятность отсутствия пакета данных на обработку высчитывается по формуле

$$\rho_0 = \frac{1-\rho}{1-\rho^{m+2}}. \quad (3)$$

Согласно технической документации на ПЛК Siemens 1512C-1 PN, он способен хранить до 1 Мб принятых данных и реагировать на аналогичный объем данных в секунду. С одного хоста LOIC создает около 100000 UDP-запросов в секунду, объем пакета данных каждого запроса равен 48 байтам. Отсюда можно подсчитать, что ПЛК может хранить и обслуживать до 20834 пакетов(m=μ=20834).

Таким образом, используя (1), (2), (3) и описанные данные, можно вывести зависимость вероятности отказа в обслуживании нового пакета данных ротк от интенсивности DoS-воздействия λ:

$$\rho_{отк} = \left(\frac{\lambda}{20834}\right)^{20835} * \frac{1-\lambda/20834}{1-(\lambda/20834)^{20836}}. \quad (4)$$

Очевидно, что при λ<μ вся формула стре-

мится к 0, что означает, что воздействие менее 20000 запросов в секунду не окажет существенного влияния.

При λ>μ единица, стоящая в знаменателе дроби в (4), несущественна и все выражение обращается в следующее уравнение:

$$\rho_{отк} = \frac{1-\lambda/20834}{-\lambda/20834} . \qquad (5)$$

На рис. 3 изображен график зависимости вероятности отказа в обработке от интенсивности DoS-воздействия при λ>μ.

При интенсивности атаки в 100000 запросов в секунду с одного хоста вероятность отказа составит около 79%, при добавлении еще одного хоста вероятность повысится до 89%.

Оценка последствий DoS-воздействия проводилась по следующим категориям:

- продолжительность (время выполнения) программного цикла контроллера;
- возможность передачи данных с контроллера на периферийные устройства.

Замеры времени выполнения программного цикла производились путем использования встроенных инструментов ПО для программирования ПЛК TIAPortal. Как показали

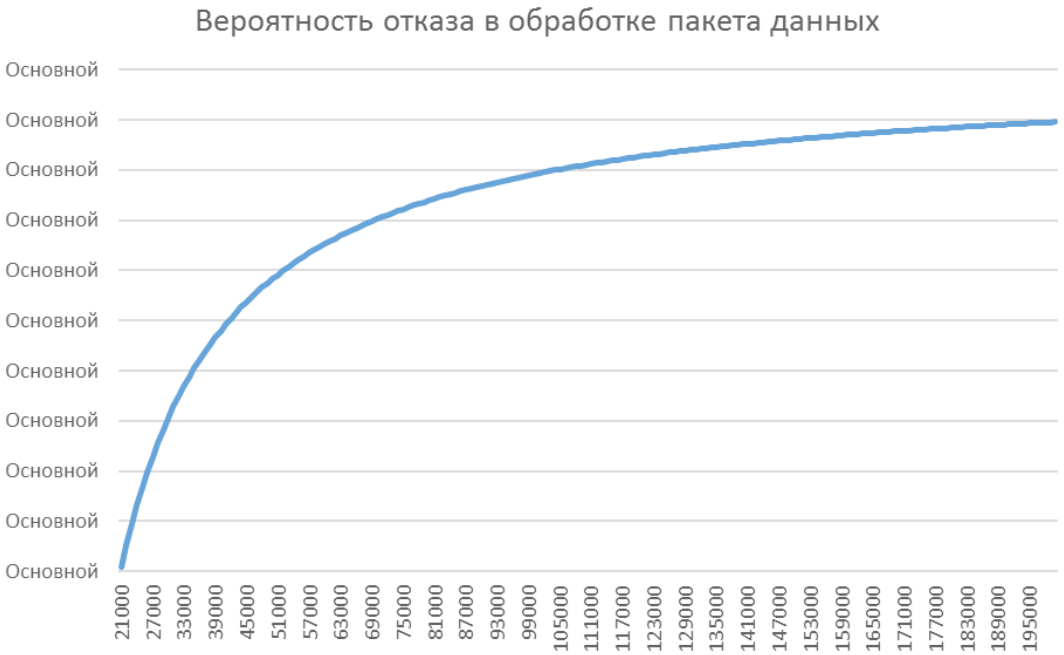

Рис.3. Вероятность отказа в обработке пакета данных при различных интенсивностях DoS-воздействия

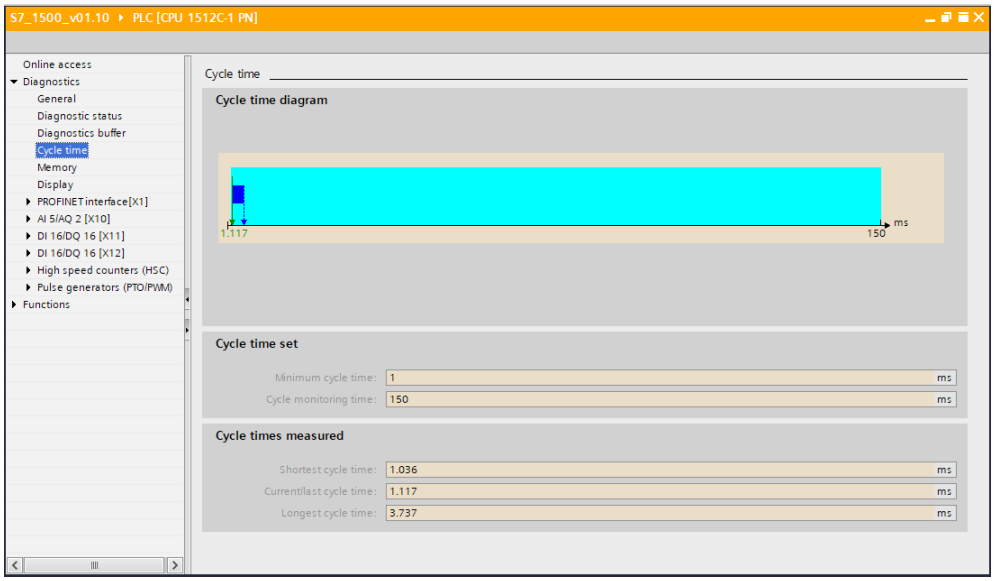

Рис.4. Базовое время цикла

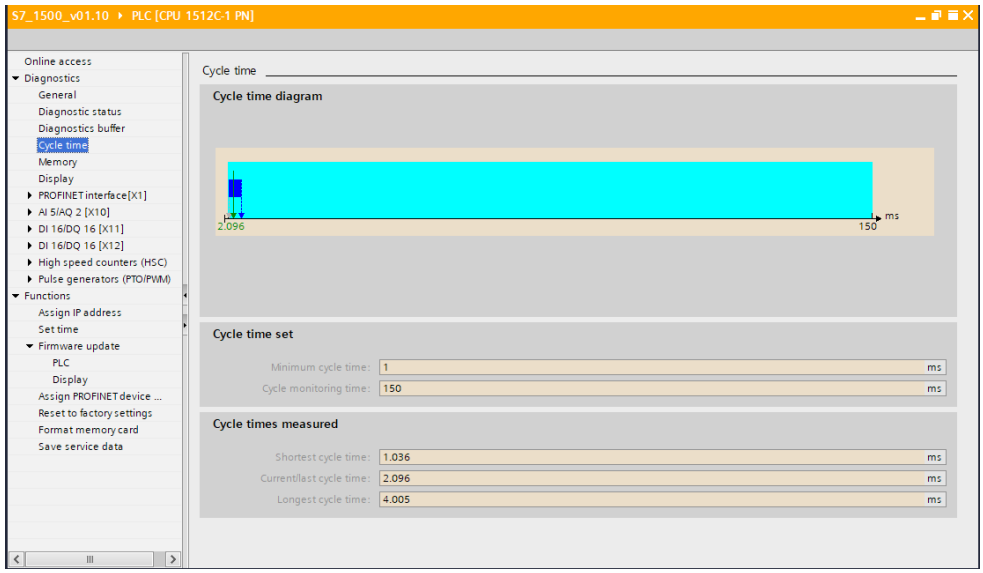

Рис.5. Время цикла под нагрузкой

измерения, среднее время выполнения программного цикла до начала воздействия составляло около 1,1 – 1,2 миллисекунд (рис.4). После подключения DoS-воздействия время выполнения программного цикла увеличивалось до среднего значения около 2,1 – 2,2 миллисекунд, увеличиваясь практически вдвое (рис.5).

Возможность передачи данных с контроллера на периферийные устройства оценивалась несколькими способами:

• наличие соединения с отслеживающим модулем TIAPortal;

• наличие соединения с HMI-панелью и вторым контроллером;

• наличие отклика сети (команда ping).

Несколько запусков LOIC показали, что в течение 7–10 секунд после начала DoS-воздействия пропадала связь ПЛК с отслеживающим модулем (рис. 6).

Связь с периферийными устройствами также была нарушена: отмечена нестабиль-

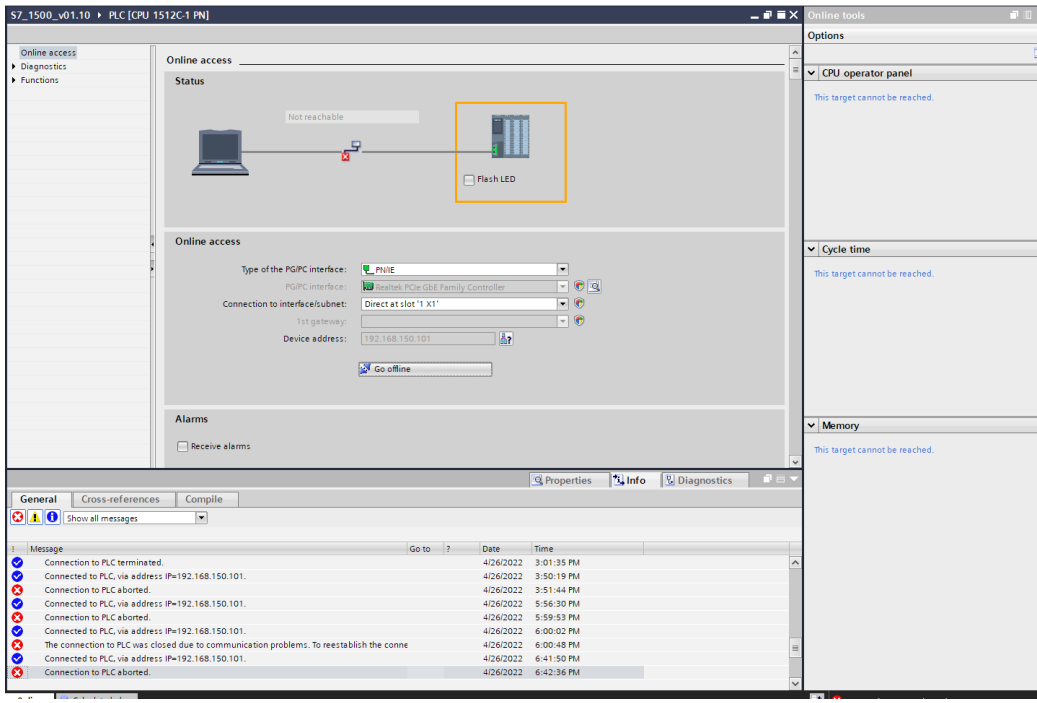

Рис.6. Пропавшее соединение с ПЛК

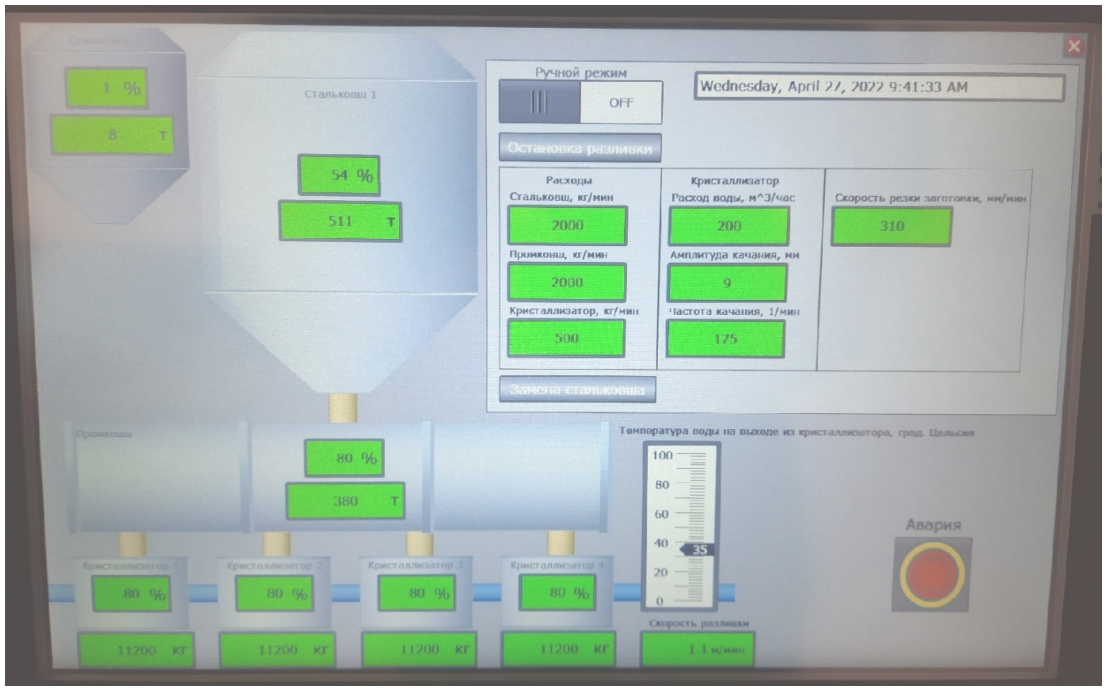

Рис.7. Базовая работа HMI-панели. Данные с контроллера приходят нормально

Рис.8. Работа HMI-панели под нагрузкой. Данные с контроллера не приходят и заменяются на символы «#»

ность поступления данных на HMI-панель и второй ПЛК (рис. 7 и 8).

Дополнительная проверка с помощью команды ping подтвердила сильную нестабильность соединения: увеличение времени отклика в разы и потерю значительной части (около 75%) пакетов данных (рис. 9). Подключение второго атакующего хоста увеличивало эту долю до приблизительного значения в 90%.

Дальнейшим шагом было повторение вышеописанных процедур, но была изменена точка подключения хоста нарушителя с сетевого интерфейса самого ПЛК на маршрутизатор.

Стандартный трафик в сети лабораторного стенда при выполнении проекта составляет около 4-5 килобайт в секунду. 2 хоста, создающие по 100000 запросов в секунду, как было показано ранее, создают поток данных

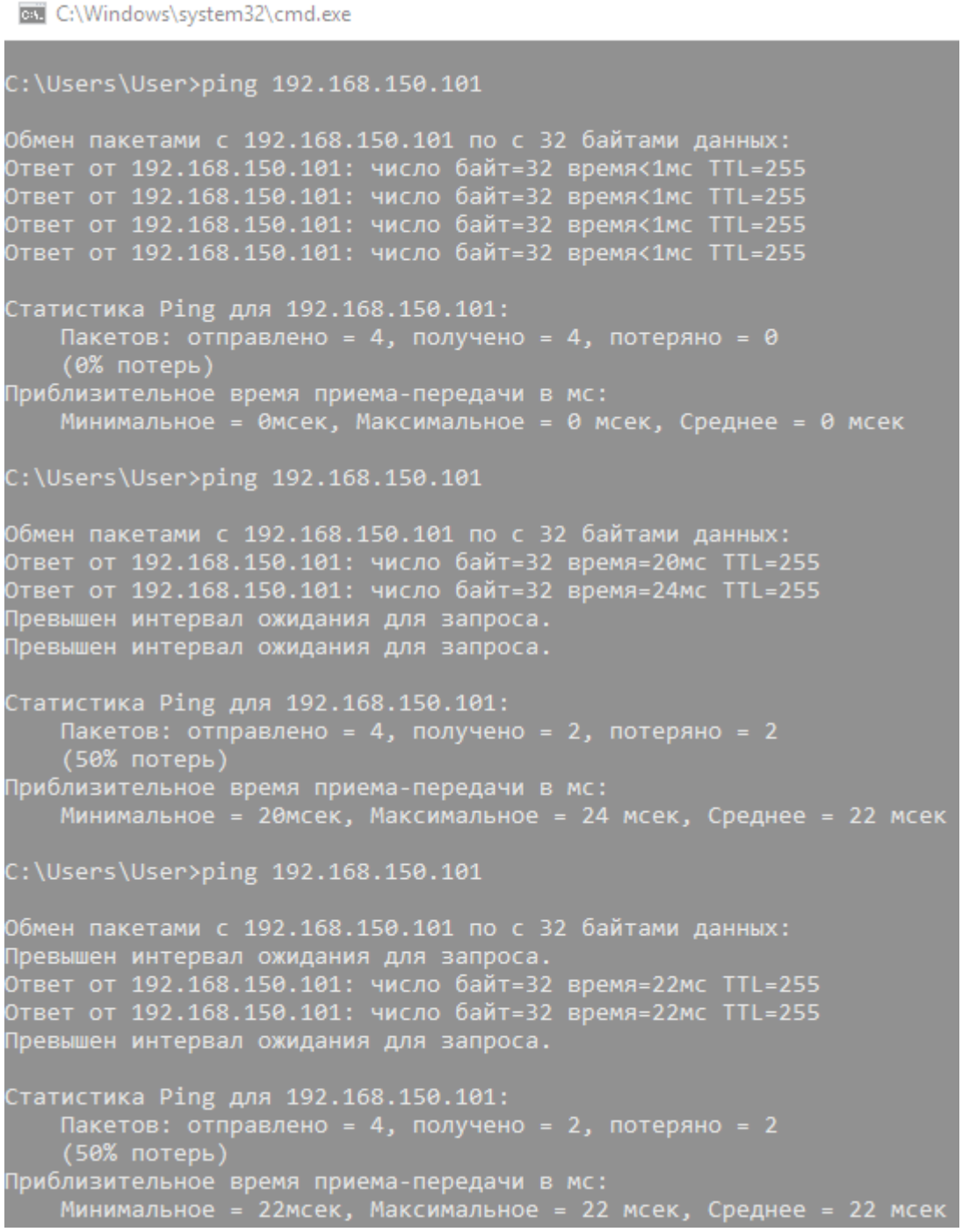

Рис.9. Исполнение команды ping: первый запрос выполнен при нормальной работе, второй и третий – под нагрузкой

приблизительно равный 5 мегабайтам в секунду с одного хоста. Таким образом, трафик данных через маршрутизатор должен увеличиваться до 10 МБ/с.

Для сканирования трафика удаленного маршрутизатора была использована программа Multi Router Traffic Grapher (MRTG) [3], которая позволяет осуществлять сканирование трафика с помощью SNMP, а именно количество байт, проходящих через определенный порт коммутатора в секунду, независимо от их источника, и предоставляет данные в графическом виде. Показания MRTG показаны на рис. 10.

На графике изображен сетевой трафик через порт коммутатора, соединенный с ПЛК-1, выраженный в байтах в секунду. Хорошо заметны 2 пиковых значения, достигающие не-

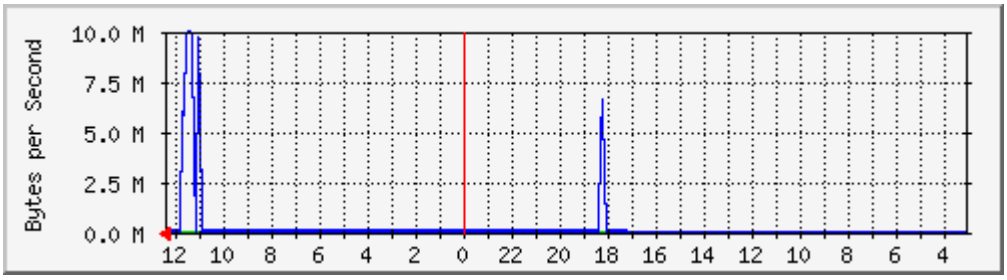

Рис. 10. Сетевой трафик, проходящий через маршрутизатор

скольких мегабайт в секунду. В эти моменты проводилась DDoS-атака. Стандартное сетевое взаимодействие ПЛК в 1000 раз менее активное, поэтому теряется на фоне всплесков. Т.к. основное предназначение DDoS-атаки – заполнение канала передачи, а ширина канала маршрутизатора стенда достигает лишь 100 мегабит в секунду, то очевидно, что 2 атакующих хоста практически полностью занимают канал передачи и не дают ПЛК стабильного доступа к легитимным сигналам. Сетевой трафик через остальные порты маршрутизатора остался неизменным. Поведение ПЛК в свою очередь ничем не отличалось от предыдущего этапа проверки. ПЛК-2 под DoS-воздействием показал поведение, аналогичное ПЛК-1: замедление программного цикла, невозможность приема/передачи данных по сетевому протоколу. Проверка данных, которую осуществляет ПЛК-1, заканчивается провалом, при этом система выдает соответствующее предупреждение.

Последним этапом работы стала проверка работы ПЛК под нагрузкой при отсутствии сетевых соединений. В результате было отмечено, что ПЛК работает в штатном режиме без явного замедления и может передавать данные через дискретные и аналоговые модули ввода/вывода.

В заключение необходимо отметить некоторые методы защиты от подобных воздействий:

1. Изоляция сети АСУ ТП. Если изолировать АСУ ТП от Интернета и от основной локальной сети предприятия, внешние воздействия становятся невозможны. Однако остаются осуществимы атаки изнутри самой сети АСУ ТП. Также подобный вариант отбрасывается с расчетом повышения удобства работы с самой промышленной сетью.

2. Фильтрация трафика. Настроенные межсетевые экраны и/или списки доступа позволят не допустить вредоносный трафик до управляющих узлов. Недостатки этого метода состоят в том, что лишь малая часть ПЛК имеют встроенные механизмы для настройки фильтрации. Фильтрации определенных сетевых протоколов в свою очередь создает необходимость тщательного подбора комплектующих и разработки архитектуры.

3. Мониторинг целостности сети. Позволит отслеживать изменение состава АСУ ТП с целью поиска недоверенных хостов. Но это метод не предупредит о DoS-воздействии с одного из доверенных элементов сети.

4. Сервисы по защите от DDoS-атак. Основной недостаток состоит в том, что подобные сервисы не способны работать с ПЛК, но вполне применимы для компьютерной части.

По результатам эксперимента можно сделать вывод о том, что сеть ПЛК не может сохранять стабильную работу под сравнительно слабым воздействием в 200000 запросов в секунду. В случае, если программа ПЛК имеет прием/передачу данных через TCP/IP соединение, происходит замедление работы программы, что может сказаться на синхронизации процессов. Соединение контроллеров с отслеживающим модулем и человеко-машинный интерфейс при тестовом испытании перестали работать в штатном режиме. Время выполнения программного цикла автономной работы ПЛК при этом не изменяется, возможность управления исполнительными механизмами и датчиками через модули ввода/вывода ПЛК сохраняется.

Также стоит отметить, что в этой работе исследовалась АСУ ТП, построенная на протоколе PROFINET со стандартным управлением потоком данных TCP, и одно из дальнейших направлений исследований - проверка при использовании АСУ ТП режима реального времени.

Литература

1. Классификация сетевых атак [Электронный ресурс]. –– URL: https://www.internet-technologies.ru/articles/newbie/klassifikaciya-setevyh-atak.html#header-8116-7 (Дата обращения: 20.04.2022).

2. Adeyemo, A. A. A study of denial-of-service attack with its tools and possible mitigation techniques / A. A. Adeyemo, K. A. Ganiyu // Computer Sciences and Telecommunications. – 2019. – № 2(57). – С. 36 - 45. –– URL: https://www.elibrary.ru/item.asp?id=45620382 (Дата обращения: 20.04.2022).

3. Теория систем массового обслуживания: учеб. пособие / И. В. Сол- нышкина. – Комсомольск-на-Амуре: ФГБОУ ВПО «КнАГТУ», 2015. – 76 с. – URL: https://knastu.ru/media/files/page_files/page_421/posobiya_2015/_Teoriya_sistem_massovogo_obsluzhivaniya.pdf

4. Tobi Oetiker's MRTG – The Multi Router Traffic Grapher [Электронный ресурс]. – URL: https://oss.oetiker.ch/mrtg/ (Дата обращения: 20.07.2022).

References

1. Klassifikacija setevyh atak –– URL: https://www.internet-technologies.ru/articles/newbie/klassifikaciya-setevyh-atak.html#header-8116-7

2. Adeyemo, A. A. A study of denial-of-service attack with its tools and possible mitigation techniques / A. A. Adeyemo, K. A. Ganiyu // Computer Sciences and Telecommunications. – 2019. – № 2(57). – S. 36-45. –– URL: https://www.elibrary.ru/item.asp?id=45620382

3. Teorija sistem massovogo obsluzhivanija: ucheb. posobie / I. V. Sol- nyshkina. – Komsomol'sk-na-Amure: FGBOU VPO «KnAGTU», 2015. – 76 s.–URL: https://knastu.ru/media/files/page_files/page_421/posobiya_2015/_Teoriya_sistem_massovogo_obsluzhivaniya.pdf

4. Tobi Oetiker's MRTG – The Multi Router Traffic Grapher [Jelek-tronnyj resurs]. – URL: https://oss.oetiker.ch/mrtg/

БОГЕР Александр Максимович, преподаватель кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, 76. E-mail: bogeram@susu.ru

СОКОЛОВ Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, 76. E-mail: sokolovan@susu.ru

МОРОЗОВ Игорь Александрович, младший научный сотрудник НОЦ «Информационная безопасность» ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». Россия, 454080, г. Челябинск, проспект Ленина, 76. E-mail: morozovia@susu.ru.

BOGER Aleksandr Maksimovich, Lecturer of Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: bogeram@susu.ru

SOKOLOV Alexander Nikolaevich, Ph.D., Associate Professor, Head of Department of Information Security, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: sokolovan@susu.ru

MOROZOV Igor Alexandrovich, Junior researcher of Information Security Research and Education Centre, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)". 76, Lenin prospekt, Chelyabinsk, Russia, 454080. E-mail: morozovia@susu.ru.