Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный университет   
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

ОТЧЁТ

к лабораторной работе №4

на тему

**ЗАЩИТА ОТ АТАКИ ПРИ УСТАНОВКЕ TCP-СОЕДИНЕНИЯ И ПРОТОКОЛОВ ПРИКЛАДНОГО УРОВНЯ**

Выполнил: студент гр.253504 Давыдовский Д.В.

Проверил: ассистент кафедры информатики Герчик А.В.

Минск 2025

**СОДЕРЖАНИЕ**

[1 Цель работы 3](#_Toc188986632)

[2 Ход работы 4](#_Toc188986633)

[Заключение 7](#_Toc188986634)

# 1 ЦЕЛЬ РАБОТЫ

Цель работы – разработка программных средств для защиты от атак при установке *TCP*-соединения и атак на протоколы прикладного уровня. В ходе работы будет рассмотрено существующие угрозы, методы их предотвращения и разработаны практические решения для повышения безопасности сетевых взаимодействий.

На первом этапе необходимо изучить основные типы атак, возникающих при установке *TCP*-соединения, включая *SYN-flood*, *Man-in-the-Middle* (*MITM*), *IP*-спуфинг и их влияние на стабильность и безопасность сетевых сервисов.

Далее будет разработана архитектура защитной системы, включающая механизмы предотвращения атак на этапе установления TCP-соединения (например, *SYN-cookies*, фильтрацию аномального трафика) и методы защиты на прикладном уровне (шифрование данных, механизмы аутентификации, контроль целостности передаваемых данных).

Следующим этапом является реализация программного решения. Оно должно корректно обрабатывать аномальный трафик, предотвращать попытки перехвата данных, обеспечивать защиту от несанкционированного доступа и атаки на сетевые сервисы.

Ожидаемые результаты включают разработку эффективных методов защиты от атак при установке TCP-соединений и на прикладном уровне, а также создание удобного и надежного программного инструмента, обеспечивающего стабильную и безопасную работу сетевых сервисов.

# 2 ХОД РАБОТЫ

В ходе выполнения поставленной задачи было разработано программное средство, обеспечивающее защиту от атак при установке TCP-соединения и на уровне прикладных протоколов. В рамках работы была реализована система, позволяющая минимизировать риски сетевых атак, таких как *SYN-flood*, перехват данных и перегрузка сервера множественными запросами.

На начальном этапе проводилось исследование механизмов атак на установку *TCP*-соединений и возможных способов их предотвращения. Основной упор был сделан на защиту от перегрузки сервера, блокировку подозрительной активности и использование криптографических методов для обеспечения безопасности передаваемых данных. Было принято решение реализовать серверное приложение с поддержкой *SSL/TLS*, что позволило зашифровать коммуникацию между клиентом и сервером и исключить возможность перехвата передаваемых данных злоумышленниками.

Важной частью разработки стала система контроля подключений. Чтобы избежать перегрузки сервера и возможных *DDoS*-атак, было введено ограничение на количество одновременных соединений. Если число активных клиентов достигает предела, новые подключения автоматически отклоняются. Также реализован механизм мониторинга частоты запросов: в случае превышения допустимого лимита *IP*-адрес клиента временно блокируется, предотвращая массовые атаки на сервер.

Для обеспечения стабильной и эффективной работы сервера была использована многопоточная обработка запросов. Благодаря библиотеке *threading* сервер способен обрабатывать несколько подключений одновременно, распределяя нагрузку и обеспечивая бесперебойную работу системы.

В результате была создана безопасная система, способная противостоять наиболее распространённым угрозам при установке *TCP*-соединений. Реализованные механизмы защиты позволяют обеспечивать надёжную передачу данных, предотвращать перегрузку сервера и блокировать потенциальные источники атак. Итогом работы стало разработанное программное средство, которое не только эффективно справляется с поставленными задачами, но и может быть адаптировано под различные условия эксплуатации, обеспечивая высокий уровень защиты сетевых взаимодействий.

В результате работы также была разработана ещё одна версия сервера, которая не предусматривает защиту от атак или шифрование данных. С помощью программы wireshark наглядно убедимся в том, что основной сервер является более безопасным.

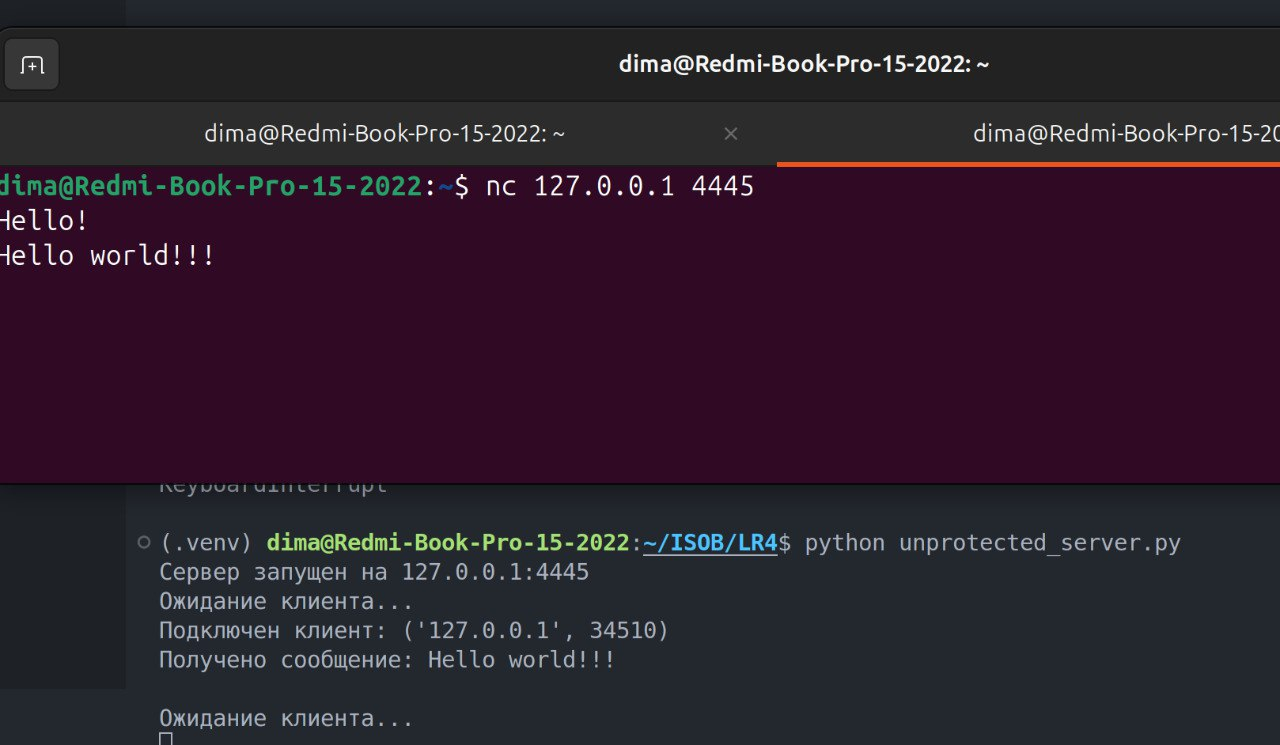


Рисунок 1 – Результат работы сервера без защиты

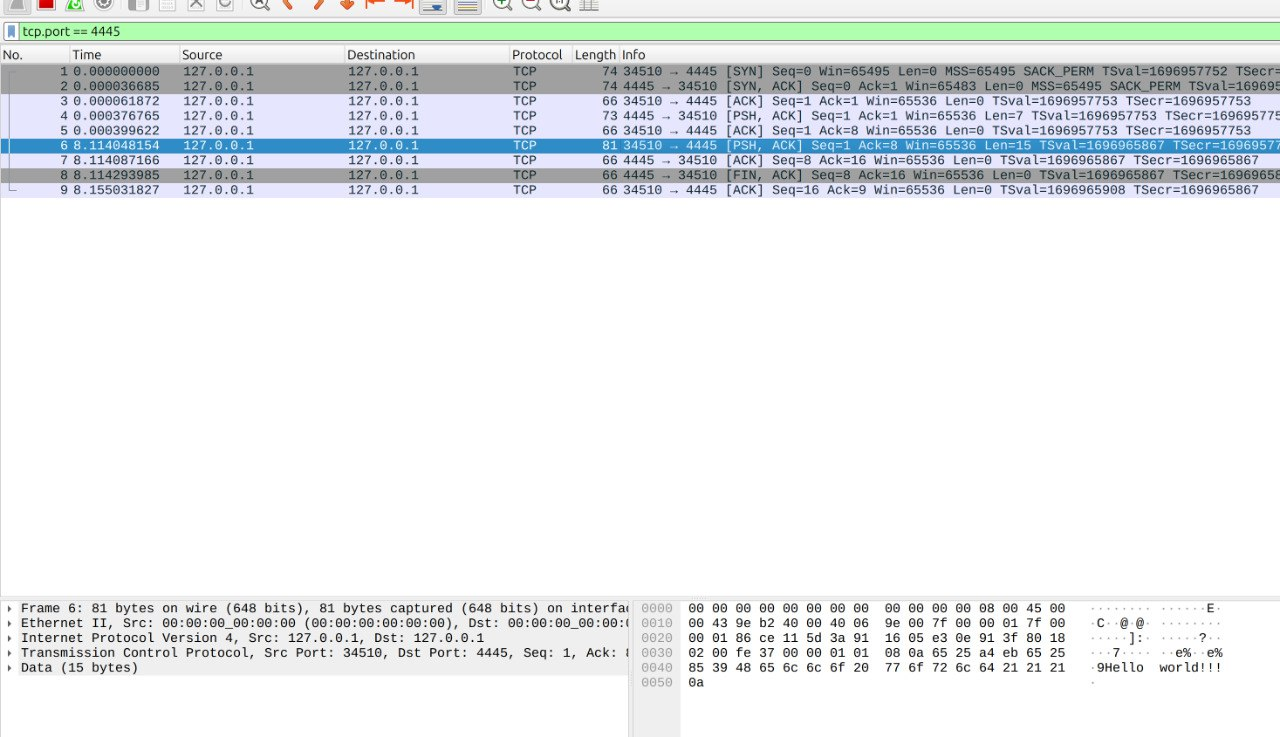


Рисунок 2 – Перехват сообщения с помощью *Wireshark*

Как видно из рисунков 1 и 2, обладая небольшой настойчивостью, мы можем перехватывать весь интернет-трафик, отправляемый на сервер, что, конечно же, является большим плюсом для нас и огромным минусом для владельца сервера.

Рассмотрим теперь второй сервер, который оснащён мерами защиты.

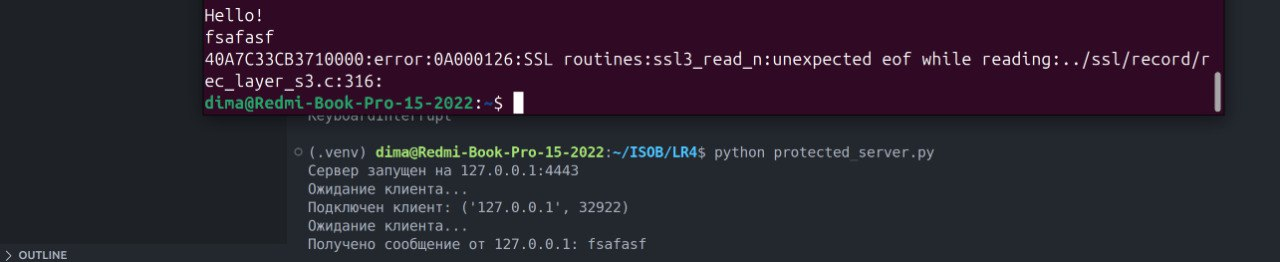


Рисунок 3 – Результат работы сервера с защитой

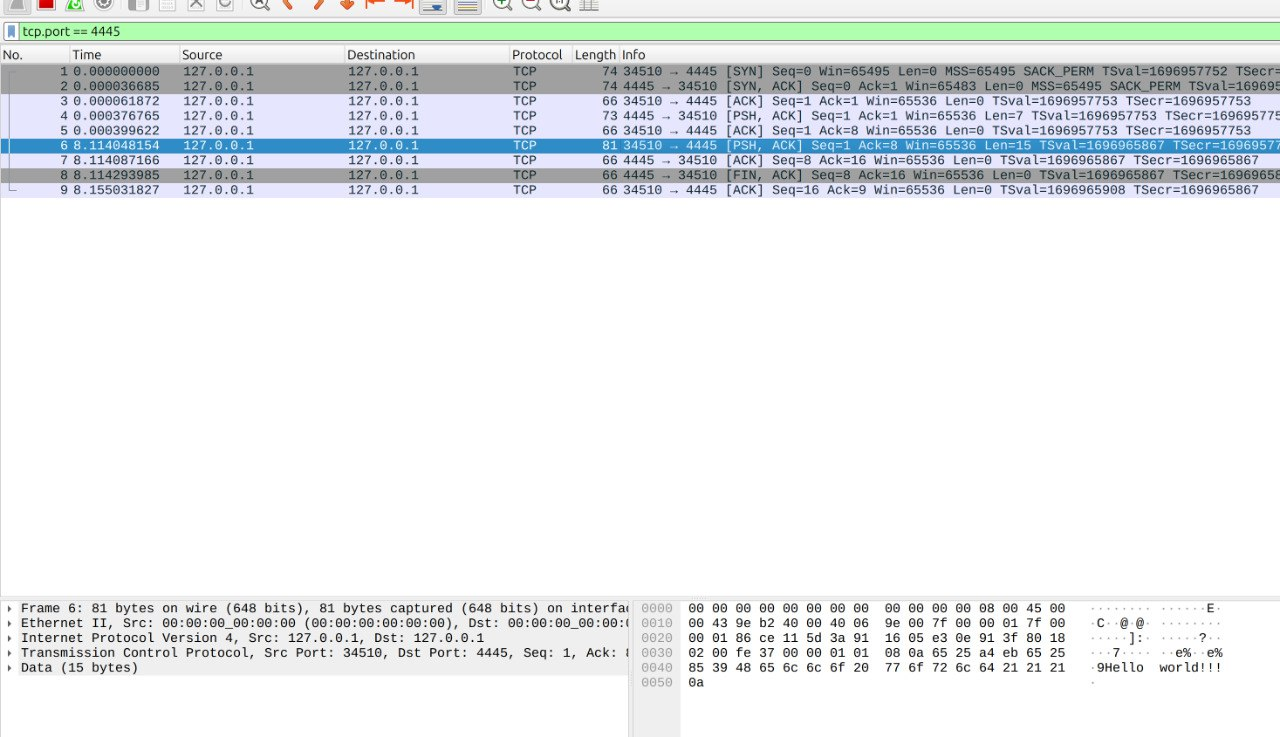


Рисунок 4 – Перехват сообщения с помощью *Wireshark*

Как видно из рисунков 3 и 4, сервер, реализованный с поддержкой *SSL/TLS*, напрямую не передаёт сообщения. Весь обмен трафиком происходит в зашифрованном виде, что, конечно же, является огромным минусом для нас и большим плюсом для владельца сервера.

Помимо поддержки *SSL/TLS*, сервер оснащен защитой от *DDoS*-атак, *SYN-flood* атак. Количество одновременных подключений на сервере ограничено числом 5, а время ожидания от подключенного пользователя составляет 10 секунд. Эти два фактора помогают защититься от перегрузки сервера из-за огромного наплыва пользователей и в добавок защититься от *RUDY* атаки, при которой злоумышленник медленно отправляет данные на сервер, что заставляет сервер игнорировать иные подключения.

# ЗАКЛЮЧЕНИЕ

В ходе выполнения данной работы была разработана и реализована система защиты от атак при установке *TCP*-соединения и атак на уровне прикладных протоколов. Созданный сервер поддерживает безопасное взаимодействие с клиентами, используя протокол *SSL/TLS* для шифрования передаваемых данных, а также механизмы ограничения подключений и блокировки подозрительной активности.

Разработанный алгоритм контроля соединений позволяет предотвращать перегрузку сервера и атаки типа *DDoS*, ограничивая количество одновременных подключений и анализируя частоту запросов с одного IP-адреса. В случае обнаружения подозрительной активности сервер автоматически блокирует вредоносные клиенты, что повышает его устойчивость к атакам.

Использование многопоточной обработки запросов позволило реализовать эффективную и масштабируемую систему, способную обрабатывать множество соединений одновременно без значительного увеличения нагрузки на ресурсы сервера. Встроенное логирование подключений обеспечивает возможность мониторинга работы сервера и анализа потенциальных угроз.

Таким образом, разработанное программное средство не только выполняет свою основную задачу – защиту *TCP*-соединений от атак, – но и обладает гибкостью для дальнейшего расширения и интеграции с более сложными системами безопасности. Реализованные методы защиты позволяют обеспечить надежную и стабильную работу сервера в условиях возможных сетевых атак, что делает его пригодным для практического использования в реальных условиях эксплуатации.