

Федеральное государственное бюджетное  
образовательное учреждение высшего образования



«Московский государственный технический  
университет имени Н. Э. Баумана (национальный  
исследовательский университет)»



Факультет «Машиностроительные технологии»

Кафедра «Электронные технологии в  
машиностроении»

## ОТЧЁТ

по дисциплине «Научно-исследовательская работа»

на тему:

«Способы автоматизации вакуумных систем»

Выполнил:

студент группы МТ11-62Б

Зотов М.С.

Руководитель:

Колесник Л.Л.

Дисциплина	Результат защиты (нужное выделить)			
	НЕУД	УДОВЛ	ХОР	ОТЛ
Научно-исследовательская работа				
Зачёт принял _____ подпись	( _____ ) расшифровка			

Москва

2021 г.

## РЕФЕРАТ

Отчёт по дисциплине «Научно-исследовательская работа» содержит 79 страниц, 7 таблиц, 17 рисунков, список литературы из 33 источников.

АВТОМАТИЗАЦИЯ, ВАКУУМНАЯ СИСТЕМА, ПРОМЫШЛЕННЫЙ ПРОТОКОЛ, ПРОМЫШЛЕННАЯ СЕТЬ, СИСТЕМА SCADA, ТРАНСПОРТНЫЙ ПРОТОКОЛ, MODBUS, PROFIBUS, FIELDBUS, TCP, UDP.

Отчёт выполнен с использованием среды L<sup>A</sup>T<sub>E</sub>X

Работа посвящена автоматизации и дистанционному управлению вакуумным оборудованием. Описывается актуальность применения дистанционного управления оборудованием. Рассмотрены различные варианты дистанционного управления. Проведён сравнительный анализ литературных источников, в которых описывались методы дистанционного управления.

Рассмотрены основные протоколы транспортного уровня, используемые для передачи данных. Приведены и проанализированы основные промышленные протоколы. Выбрано наиболее подходящее сочетание протокола транспортного уровня и промышленного протокола.

# СОДЕРЖАНИЕ

<b>ВВЕДЕНИЕ</b>	<b>5</b>
<b>1 Подготовка и организация поиска информационных материалов</b>	<b>7</b>
1.1 Терминологический словарь . . . . .	7
1.2 Сокращения . . . . .	10
1.3 Поисковые запросы . . . . .	13
1.3.1 Ключевые слова . . . . .	13
1.3.2 Разработка поисковых запросов . . . . .	14
1.3.3 Корректировка поисковых запросов . . . . .	15
<b>2 Обоснование и выбор области и средств поиска</b>	<b>17</b>
2.1 Планируемые результаты поиска . . . . .	17
2.2 Области и средства поиска . . . . .	17
<b>3 Краткий обзор информационных материалов</b>	<b>19</b>
3.1 Оценка качества материалов, их достоверности . . . . .	19
3.2 Краткое резюме по каждому источнику информации. Основные результаты, полученные авторами . . . . .	30
<b>4 Систематизация и обобщение информации</b>	<b>36</b>
4.1 Протоколы транспортного уровня в промышленных сетях . . .	36
4.1.1 Уровни модели OSI . . . . .	37
4.1.2 Транспортный протокол TCP . . . . .	38
4.1.2.1 Функции TCP . . . . .	38
4.1.2.2 Структура TCP пакета . . . . .	39
4.1.2.3 Применение TCP . . . . .	42
4.1.3 Протокол UDP . . . . .	43
4.1.3.1 Структура UDP датаграммы . . . . .	43

4.1.4	Сравнение TCP и UDP . . . . .	44
4.1.5	Вывод . . . . .	45
4.2	История разработки промышленных протоколов . . . . .	45
4.2.1	Предыстория появления автоматизации . . . . .	45
4.2.2	Технология Fieldbus: возникновение и требования . . . .	46
4.2.3	Modbus . . . . .	47
4.2.4	Profibus . . . . .	47
4.2.5	Foundation Fieldbus . . . . .	48
4.3	Принципы работы протоколов . . . . .	49
4.3.1	Понимание термина Fieldbus . . . . .	49
4.3.2	Принцип работы промышленной сети . . . . .	50
4.3.2.1	Принцип работы промышленной автоматики .	50
4.3.2.2	Топология сети . . . . .	50
4.3.2.3	Основные характеристики сетей . . . . .	53
4.3.2.4	Режимы обмена данными . . . . .	53
4.3.3	Modbus . . . . .	54
4.3.3.1	Краткое резюме . . . . .	54
4.3.3.2	Принцип работы . . . . .	55
4.3.3.2.1	Физический уровень . . . . .	55
4.3.3.2.2	Логический (канальный) уровень . . .	56
4.3.3.2.3	Modbus RTU . . . . .	56
4.3.3.2.4	Modbus TCP . . . . .	58
4.3.4	Profibus . . . . .	59
4.3.4.1	Краткое резюме . . . . .	59
4.3.4.2	Принцип работы . . . . .	60
4.3.4.2.1	Физический уровень . . . . .	61
4.3.4.2.2	Канальный уровень . . . . .	61
4.3.4.2.3	Передача сообщений . . . . .	62
4.3.4.3	Profinet . . . . .	63

4.3.5	Foundation Fieldbus . . . . .	63
4.4	SCADA-системы . . . . .	64
4.4.1	Что такое SCADA - система . . . . .	64
4.4.2	Задачи SCADA - систем . . . . .	65
4.4.3	Структура системы . . . . .	66
4.4.4	Пример применения SCADA систем . . . . .	66
4.5	Сравнение протоколов передачи данных промышленных сетей .	66
4.5.1	Modbus . . . . .	66
4.5.2	Profibus . . . . .	68
4.5.3	Итог . . . . .	69
4.6	Примеры применения протокола Modbus для автоматизации . .	69
4.7	Преимущества автоматизации . . . . .	70
4.8	Дальнейшая работа . . . . .	70
	<b>ВЫВОДЫ И РЕЗУЛЬТАТЫ</b>	<b>71</b>
	<b>ЗАКЛЮЧЕНИЕ</b>	<b>73</b>
	<b>Список литературы</b>	<b>74</b>

## ВВЕДЕНИЕ

Требование точности к продукции выдвигает критерий повторяемости на первый план. Повторяемость может быть достигнута путём автоматизации технологического процесса, исключая человеческий фактор при его проведении. С этим может справиться дистанционное автоматизированное управление, которое решает следующие проблемы:

- простой оборудования в связи с отсутствием оператора;
- уменьшение производительности в связи с необходимостью ручного управления;
- ухудшение качества продукции в связи с неточным следованием инструкциям.

*Целью работы является анализ современных протоколов передачи данных между оборудованием и системами человек-оборудование, а также выбор наиболее оптимальных для осуществления автоматизации вакуумных систем.*

### **Задачи:**

- составить терминологический словарь и список ключевых слов;
- сформировать поисковые запросы;
- найти литературу по данной теме и провести анализ на основе полученных данных:
  - проанализировать протоколы транспортного уровня;
  - проанализировать протоколы промышленного интернета, узнать их достоинства и недостатки;
- провести краткий обзор информационных материалов;

- систематизировать и обобщить информацию.
- сделать выводы о преимуществах автоматизации, предложить протокол, способный реализовать поставленную задачу.

# 1 Подготовка и организация поиска информационных материалов

Определим основные термины и ключевые слова, по которым будет совершаться поиск, разработаем поисковые запросы с последующим их улучшением.

## 1.1 Терминологический словарь

1. **Fieldbus** термин, обозначающий соединение полевых устройств (датчики, сенсоры, ПЛК) с человеко - машинным интерфейсом.
2. **Foundation Fieldbus** открытая архитектура, является цифровой, последовательной, двусторонней системой связи, которая служит в качестве базового уровня сети в заводских или фабричных системах автоматизации. Более подробно см **4.3.5. Foundation Fieldbus**.
3. **H1** одна из реализаций протокола Foundation Fieldbus.
4. **ModBus** открытый коммуникационный протокол, основанный на архитектуре ведущий — ведомый (master-slave). Широко применяется в промышленности для организации связи между электронными устройствами.
5. **Profibus Process Field Bus** – шина полевого уровня – открытая промышленная сеть, прототип которой был разработан компанией Siemens AG для своих промышленных контроллеров Simatic. Очень широко распространена в Европе, особенно в машиностроении и управлении промышленным оборудованием.
6. **Profisafe** набор технологий для предотвращения несчастных случаев на производстве.



- 7. SCADA Supervisory Control And Data Acquisition** (диспетчерское управление и сбор данных) — программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. Используется везде, где требуется обеспечить контроль оператора за АСУ ТП.
- 8. АСУ ТП** Автоматизированная система управления технологическим процессом — группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.
- 9. Автоматизация** машинное производство, обычно осуществляемое под контролем компьютера и не требующее непосредственного вмешательства человека. Автоматизация особенно полезна в тех случаях, когда необходима чрезвычайная точность, а также при работе с опасными материалами, когда обеспечение безопасности человека оказывается слишком трудным и дорогостоящим.
- 10. Датаграмма** блок информации, передаваемый протоколом через сеть связи без предварительного установления соединения и создания виртуального канала. Протоколы, использующие датаграммы работают быстрее, но не гарантируют доставки сообщений получателю.
- 11. Коллизия** в терминологии компьютерных и сетевых технологий наложение двух и более кадров от станций, пытающихся передать кадр в один и тот же момент времени в среде передачи коллективного доступа.
- 12. Маркерный доступ** по сети перемещается небольшой блок данных, называемый маркер. Владение этим маркером гарантирует право передачи. Если узел, принимающий маркер, не имеет информации для отправки,

он просто переправляет маркер к следующей конечной станции. Каждая станция может удерживать маркер в течение определённого максимального времени (по умолчанию — 10 мс). Используется в топологии кольцо (см. 4.3.2.2. Топология сети).

- 13. **Октет** — восемь двоичных разрядов. В русском языке октет обычно называют байтом.
- 14. **Полевая шина** — канал общения между контроллером и другими устройствами.
- 15. **Полевой датчик** — под этим термином понимается некое устройство, расположенное на удалении от системы контроля и занимающееся сбором и передачей информации.
- 16. **Программируемый логический контроллер** — специальная разновидность электронной вычислительной машины, чаще всего используется для автоматизации.
- 17. **Протокол связи** — набор определённых правил или соглашений интерфейса логического уровня, который определяет обмен данными между различными устройствами. Эти правила задают единообразный способ передачи сообщений и обработки ошибок.
- 18. **Сокет** — название программного интерфейса для обеспечения обмена данными между процессами. Процессы при таком обмене могут выполняться как на одной ЭВМ, так и на различных ЭВМ, связанных между собой сетью. Сокет — абстрактный объект, представляющий конечную точку соединения.
- 19. **Сторожевой таймер** — аппаратно реализованная схема контроля над зависанием системы. Представляет собой таймер, который периодически сбрасывается контролируемой системой. Если сброса не произошло в течение

некоторого интервала времени, происходит принудительная перезагрузка системы.

**20. Удалённый доступ** система, позволяющая пользователю подключаться к аппаратуре, не находясь в непосредственной близости к ней.

## **1.2 Сокращения**

**21. ACK Acknowledgement field** (поле подтверждения).

**22. ADU Application Data Unit** (пакет *Modbus* целиком с заголовками, PDU и контрольной суммой).

**23. DA Destination Address** (адрес получателя).

**24. DD Device Description** (описание устройства).

**25. DDL Device Description Language** (язык описания устройств).

**26. DP Decentralized Peripherals** (Децентрализованные периферийные устройства).

**27. DU Data Unit** (данные).

**28. ECE ECN-Echo** (сообщает о том, что получатель поддерживает *ECN*).

**29. ECN Explicit Congestion Notification** (уведомление о переполнении канала трафика без потери пакетов).

**30. ED End Delimeter** (конечный разделитель).

**31. FC Function Code** (код функции).

**32. FIN Finished sending data** (окончание приёма, окончание соединения).

**33. FMS Fieldbus Message Specification** (спецификация сообщений Fieldbus).

- 34. FTP File Transfer Protocol** (протокол передачи данных).
- 35. HSE High Speed Ethernet** (высокоскоростной интернет). Одна из реализаций протокола Foundation Fieldbus.
- 36. HTTP Hypertext Transfer Protocol** (протокол передачи гипертекста).
- 37. IMAP Interactive Mail Access Protocol** (интерактивный протокол доступа к почте).
- 38. LE Length of telegram** (длина телеграммы).
- 39. LEr Length of telegram reserved** (длина телеграммы зарезервированная для защиты).
- 40. MBAP Modbus Application Protocol** (прикладной протокол Modbus).
- 41. MMI Machine Man Interface** (интерфейс соединения человека и машины, например - экран монитора).
- 42. OSI Open Systems Interconnection model** – представляет собой концептуальную модель, которая характеризует и стандартизирует коммуникационные функции телекоммуникационной или вычислительной системы безотносительно к лежащей в ее основе внутренней структуре и технологии. Его цель – взаимодействие различных систем связи со стандартными протоколами связи.
- 43. PA Process Automation** (автоматизация процессов).
- 44. PDU Protocol Data Unit** (элемент данных протокола).
- 45. POP Post Office Protocol** (почтовый протокол).
- 46. PSH Push function** (функция отправки).

- 47. RLogin Remote Login** (удалённый доступ).
- 48. RST Reset the connection** (разрыв соединения).
- 49. RTU Remote Terminal Unit**, устройство связи с объектом. Используется для ввода сигналов с объекта в автоматизированную систему и вывода сигналов на объект.
- 50. SA Source Address** (адрес отправителя).
- 51. SAP Service Access Points** (сервисные точки доступа, команда).
- 52. SD Start Delimeter** (стартовый разделитель).
- 53. SMTP Simple Mail Transfer Protocol** (простой почтовый протокол).
- 54. SND Send Data with No acknowledge** (отправка данных без уведомления).
- 55. SRD Send and Receive Data with acknowledge** (приём и отправка данных с уведомлением).
- 56. SSH Secure Shell** (безопасная оболочка).
- 57. SYN Synchronize sequence numbers** (флаг, используемый для установки соединения).
- 58. TCP Transmission Control Protocol** (протокол управления передачей) – один из самых популярных протоколов транспортного уровня.
- 59. UDP User Datagram Protocol** (протокол пользовательских датаграмм).
- 60. URG Urgent Pointer Field** (поле срочности).
- 61. ПАК Программно - Аппаратный Комплекс.**
- 62. ПЛК Программируемый Логический Контроллер.**

**63. РСУ** Распределённая Система Управления.

**64. ЦПС** Цифровые промышленные сети.

## **1.3 Поисковые запросы**

### **1.3.1 Ключевые слова**

**Ключевые слова** — это слова, отражающие содержание контента, описывают общую тему публикуемых материалов, например, статьи, диссертации, книги, материала сайта или блога.

Для систематизации и упрощения поиска сформулирован перечень ключевых слов, их синонимов и их аналогов на иностранном языке (в основном — английский). Перечень ключевых слов, используемых в данной работе, приведён в табл. 1.

Таблица 1. Перечень ключевых слов

<b>Ключевое слово</b>	<b>Синонимы</b>	<b>Ключевые слова на иностранном языке</b>
Управление	контроль, регулирование	control, administration
Удалённый доступ	терминальный доступ	remote access
Автоматизация	компьютеризация, механизация	automation, computerization
Вакуумная установка	вакуумная система, вакуумное оборудование	vacuum unit, vacuum system, vacuum equipment
Программное обеспечение	программный продукт, программный пакет	software

Ключевое слово	Синонимы	Ключевые слова на иностранном языке
Протокол связи	обмен сообщениями, протокол передачи данных	communication protocol, messaging
Технологический процесс	технологический цикл, технологическая цепочка	technological process, technological cycle
Передача данных	обмен информацией, передача показаний	data transfer, information exchange
Программируемый логический контроллер	промышленный контроллер, блок управления	programmable logic controller, industrial controller, control block
Диспетчерское управление	управление и сбор данных, контроль, анализ данных	SCADA, supervisory control

### 1.3.2 Разработка поисковых запросов

Сформированные с целью поиска информации поисковые запросы приведены в табл. 2

Таблица 2. Поисковые запросы

<b>Цель поиска</b>	<b>Поисковая конструкция, сложный запрос</b>	<b>Дополнительные параметры отбора</b>
Найти информацию о способах передачи данных по сети	протоколы + передачи + данных & интернет	релевантность Google
Найти информацию о способах удалённого управления техникой	виды + удалённого + доступа   терминальный доступ	релевантность Google
Найти информацию о протоколе, который лучше всего подходит под задачи автоматизации вакуумной техники	автоматизация + вакуумной + техники   протокол + связи + электронных + устройств   modbus	релевантность Google
Найти информацию о протоколах ModBus и Profibus	modbus   profibus   протоколы	релевантность Google

### 1.3.3 Корректировка поисковых запросов

После предварительного поиска, была проведена корректировка поисковых запросов, представленная в табл. 3

Таблица 3. Уточнённые поисковые запросы

<b>Цель поиска</b>	<b>Исходный запрос</b>	<b>Уточнённый запрос</b>
--------------------	------------------------	--------------------------



Цель поиска	Исходный запрос	Уточнённый запрос
Найти информацию о способах передачи данных по сети	протоколы + передачи + данных & интернет	протоколы + передачи + данных   communication + protocol
Найти информацию о способах удалённого управления техникой	виды + удалённого + доступа   терминальный доступ	протоколы + удалённого + доступа   remote + access + protocol
Найти информацию о протоколе, который лучше всего подходит под задачи автоматизации вакуумной техники	автоматизация + вакуумной + техники   протокол + связи + электронных + устройств   modbus	automation + vacuum + system   modbus + tcp
Найти информацию о протоколах ModBus и Profibus	modbus   profibus   протоколы	(modbus & profibus)   protocols   comparison   fieldbus

## 2 Обоснование и выбор области и средств поиска

### 2.1 Планируемые результаты поиска

Найденная литература должна отвечать следующим требованиям:

- **Актуальность** – публикации не ранее 1998 (статьи выбраны с таким разбросом, поскольку некоторые протоколы на рынке практически полвека, в связи с чем новизна для некоторых из цитируемых статей не требуется)
- **Достоверность** – публикации, прошедшие рецензирование и опубликованные на соответствующих для этого ресурсах (научные журналы или модерируемый компетентным сообществом сайт);
- **Соответствие запросу** – содержание публикации соответствует направлению исследования.

### 2.2 Области и средства поиска

1. **Научные статьи, патенты, диссертации** – наиболее обширный раздел поиска. Даты написания варьируются от 1998 до 2021 года. Весь материал изложен кратко и понятно, с сохранением основной сути статьи и цели поиска.
2. **Книги** – много полезной информации, однако поиск затруднён в связи с обилием информации, не представляющей интереса для исследования.
3. **Материалы из проверенных онлайн - ресурсов** – материалы из таких источников, как *habr.com* и ему подобные, поскольку статья перед публикацией проходит тщательный отбор модераторами и сообществом.

Поиск источников осуществлялся с помощью поисковых систем *Google*, *Google Scholar* и *ScienceDirect*, так как данные системы ориентированы на по-

иск научных ресурсов больше, чем другие, что позволило быстро найти необходимую информацию и источники.

### 3 Краткий обзор информационных материалов

#### 3.1 Оценка качества материалов, их достоверности

Таблица 4. Результаты поиска по запросам

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объём, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	“Performance Comparison of Transport Layer Protocols” <a href="https://www.academia.edu/download/61590964/Performance_Comparison_of_Transport_Layer_Protocols-_vol5-issue12-2015_20191223-12686-v59wb2.pdf">https://www.academia.edu/download/61590964/Performance_Comparison_of_Transport_Layer_Protocols-_vol5-issue12-2015_20191223-12686-v59wb2.pdf</a> (дата обр. 10.04.2021)	International Journal of Advanced Research in Computer Science and Software Engineering	5	[1]
Поисковая система Google Scholar	“Survey on Transport Layer Protocols” <a href="https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.734.7346&amp;rep=rep1&amp;type=pdf">https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.734.7346&amp;rep=rep1&amp;type=pdf</a> (дата обр. 10.04.2021)	International Journal of Computer Applications	6	[2]

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объем, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	“Chapter 4 - The Fundamentals in Understanding Networking Middleware” <a href="https://www.sciencedirect.com/science/article/pii/B9780750684552000042">https://www.sciencedirect.com/science/article/pii/B9780750684552000042</a> (дата обр. 10.04.2021)	Elsevier Inc.	93—190	[3]
Поисковая система Google Scholar	“Обзор протоколов Интернета вещей” <a href="http://www.sut.ru/doci/nauka/review/20172/1-12.pdf">http://www.sut.ru/doci/nauka/review/20172/1-12.pdf</a> (дата обр. 10.04.2021)	Информационные технологии и телекоммуникации	12	[4]
Поисковая система Google Scholar	“ОБЗОР ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ ПРИБОРОВ УЧЕТА ДЛЯ РОССИЙСКОГО РЫНКА” <a href="https://www.mzta.ru/images/1085/3-6.pdf">https://www.mzta.ru/images/1085/3-6.pdf</a> (дата обр. 11.04.2021)	ООО «Научно - технический центр МЗТА»	4	[5]

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объем, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	<p>“Краткий экскурс в историю промышленных сетей”</p> <p><a href="https://cyberleninka.ru/article/n/kratkiy-ekskurs-v-istoriyu-promyshlennyh-setey">https://cyberleninka.ru/article/n/kratkiy-ekskurs-v-istoriyu-promyshlennyh-setey</a></p> <p>(дата обр. 11.04.2021)</p>	Компоненты и Технологии	110—114	[6]
Поисковая система Google Scholar	<p>“Промышленные сети: цели и средства” <a href="https://www.cta.ru/pdf/2002-4/promnet1_2002_4.pdf">https://www.cta.ru/pdf/2002-4/promnet1_2002_4.pdf</a></p> <p>(дата обр. 10.04.2021)</p>	Современные технологии автоматизации	6—17	[7]
Поисковая система Google Scholar	<p>“ОБЗОР ТЕХНОЛОГИЙ В INDUSTRIAL ETHERNET”</p> <p><a href="https://elibrary.ru/item.asp?id=35627705">https://elibrary.ru/item.asp?id=35627705</a></p> <p>(дата обр. 11.04.2021)</p>	Инноватика-2018	532—534	[8]

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объем, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	“Profibus and Modbus: a comparison” <a href="https://scadahacker.com/library/Documents/ICS_Protocols/Siemens%20-%20Profibus%20and%20Modbus%20Comparison.pdf">https://scadahacker.com/library/Documents/ICS_Protocols/Siemens%20-%20Profibus%20and%20Modbus%20Comparison.pdf</a> (дата обр. 11.04.2021)	Automation.com	1—5	[9]
Поисковая система Google Scholar	“Advanced remote controls for rectifiers” <a href="https://www.sciencedirect.com/science/article/pii/S0026057609802936">https://www.sciencedirect.com/science/article/pii/S0026057609802936</a> (дата обр. 11.04.2021)	Metal Finishing	48—50	[10]
Поисковая система Google Scholar	“Modbus - Протокол Передачи Данных” <a href="https://www.elibrary.ru/item.asp?id=44684618">https://www.elibrary.ru/item.asp?id=44684618</a> (дата обр. 12.04.2021)	Наука и Просвещение	66—68	[11]

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объем, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google	<i>Как общаются машины</i> <a href="https://habr.com/ru/company/advantech/blog/450234/">https://habr.com/ru/company/advantech/blog/450234/</a> (дата обр. 12.04.2021)	Advantech IoT ( <i>habr.com</i> )	1	[12]
Поисковая система Google	<i>Системы автоматизации на основе Foundation Fieldbus</i> <a href="https://habr.com/ru/company/phoenix_contact/blog/489256/">https://habr.com/ru/company/phoenix_contact/blog/489256/</a> (дата обр. 12.04.2021)	Phoenix Contact ( <i>habr.com</i> )	1	[13]
Поисковая система Google	<i>Шины и протоколы в промышленной автоматике</i> <a href="https://habr.com/ru/post/454156/">https://habr.com/ru/post/454156/</a> (дата обр. 12.04.2021)	Promwad ( <i>habr.com</i> )	1	[14]



Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объем, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	“Протоколы и сети Modbus и Modbus TCP” <a href="https://www.reallab.ru/images/editor/downloads/articles/Modbus.pdf">https://www.reallab.ru/images/editor/downloads/articles/Modbus.pdf</a> (дата обр. 12.04.2021)	Современные технологии автоматизации	90—94	[15]
Поисковая система Google Scholar	“What is SCADA?” <a href="https://cds.cern.ch/record/532624/files/mc1i01.pdf">https://cds.cern.ch/record/532624/files/mc1i01.pdf</a> (дата обр. 10.04.2021)	International Conference on Accelerator and Large Experimental Physics Control Systems	339—343	[16]
Поисковая система Google Scholar	“Системы SCADA и анализ их применения” <a href="https://elibrary.ru/item.asp?id=38316519">https://elibrary.ru/item.asp?id=38316519</a> (дата обр. 12.04.2021)	филиал ФГБОУ ВО РГУПС г. Воронеж	10—14	[17]

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объем, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	“Общие принципы построения SCADA-систем” <a href="http://auts.esrae.ru/pdf/2013/2(4)/117.pdf">http://auts.esrae.ru/pdf/2013/2(4)/117.pdf</a> (дата обр. 10.04.2021)	Автоматизация и управление в технических системах	8	[18]
Поисковая система Google Scholar	“Что должна уметь система SCADA” <a href="https://www.cta.ru/pdf/1998-3/tools1_1998_3.pdf">https://www.cta.ru/pdf/1998-3/tools1_1998_3.pdf</a> (дата обр. 12.04.2021)	Современные технологии автоматизации	44—46	[19]

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объем, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	<p>“Особенности организации передачи данных между программируемыми логическими контроллерами по протоколу Modbus” <a href="https://cyberleninka.ru/article/n/osobennosti-organizatsii-peredachi-dannyh-mezhdu-programmiruemymi-logicheskimi-kontrollerami-po-protokolu-modbus">https://cyberleninka.ru/article/n/osobennosti-organizatsii-peredachi-dannyh-mezhdu-programmiruemymi-logicheskimi-kontrollerami-po-protokolu-modbus</a></p> <p>(дата обр. 10.04.2021)</p>	Вестник Казанского технологического университета	230—234	[20]

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объем, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	“Разработка системы автоматического управления вакуумной и газовой систем установки MBTY-11-1MC” <a href="https://elibrary.ru/item.asp?id=41786874">https://elibrary.ru/item.asp?id=41786874</a> (дата обр. 10.04.2021)	Будущее машиностроения России	188— 192	[21]
Поисковая система Google Scholar	“Introduction to industrial control networks” <a href="http://www.rfidblog.org.uk/Preprint-GallowayHancke-IndustrialControlSurvey.pdf">http://www.rfidblog.org.uk/Preprint-GallowayHancke-IndustrialControlSurvey.pdf</a> (дата обр. 01.05.2012)	IEEE Communication surveys & tutorials	860— 880	[22]
Поисковая система Google Scholar	<i>Промышленные сети:</i> <i>учебное пособие</i> <a href="https://elar.urfu.ru/bitstream/10995/80673/1/978-5-7996-2963-2_2020.pdf">https://elar.urfu.ru/bitstream/10995/80673/1/978-5-7996-2963-2_2020.pdf</a> (дата обр. 10.04.2021)	Издательство Уральского университета	128	[23]

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объем, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	<p>“Design of Industrial Data Monitoring Device Using IOT through MODBUS Protocol” <a href="https://www.researchgate.net/publication/344378128_Design_of_Industrial_Data_Monitoring_Device_Using_IOT_through_MODBUS_Protocol">https://www.researchgate.net/publication/344378128_Design_of_Industrial_Data_Monitoring_Device_Using_IOT_through_MODBUS_Protocol</a></p> <p>(дата обр. 10.04.2021)</p>	International Journal of Scientific & Technology Research	77—86	[24]
Поисковая система Google Scholar	<p><i>Open modbus/tcp specification</i> <a href="http://www.dankohn.info/projects/Fieldpoint_module/Open_ModbusTCP_Standard.pdf">http://www.dankohn.info/projects/Fieldpoint_module/Open_ModbusTCP_Standard.pdf</a> (дата обр. 10.04.2021)</p>	Modicon	25	[25]

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объем, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	“Fieldbus technology in industrial automation” <a href="https://tinyurl.com/rjr2c346">https://tinyurl.com/rjr2c346</a> (дата обр. 01.05.2012)	Proceedings of the IEEE	1073—1101	[26]
Поисковая система Google	<i>Обзор современных протоколов в системах промавтоматики</i> <a href="https://habr.com/ru/post/473992/">https://habr.com/ru/post/473992/</a> (дата обр. 16.04.2021)	Phoenix Contact ( <i>habr.com</i> )	1	[27]
Поисковая система Google	<i>Энциклопедия АСУ ТП</i> <a href="https://bookasutp.ru/">https://bookasutp.ru/</a> (дата обр. 10.04.2021)	д.т.н. Виктор Денисенко	1	[28]
Поисковая система Google	<i>INTRODUCTION TO PROFIBUS DP</i> <a href="http://www.diit.unict.it/users/scava/dispense/II/Profibus.pdf">http://www.diit.unict.it/users/scava/dispense/II/Profibus.pdf</a> (дата обр. 16.05.2021)	Acromag Inc.	1	[29]

Область поиска, система	Наименование материала на языке оригинала, ссылка на источник	Оценка достоверности	Объём, кол-во страниц	Номер позиции в списке литературы
Поисковая система Google Scholar	“FOUNDATION fieldbus high speed ethernet control system” <a href="http://fieldbusinc.net/downloads/hsepaper.pdf">http://fieldbusinc.net/downloads/hsepaper.pdf</a> (дата обр. 11.04.2021)	Fieldbus Inc	9	[30]
Поисковая система Google Scholar	<i>The Foundation fieldbus PRIMER</i> <a href="https://www.fieldbusinc.com/downloads/primer1_1.pdf">https://www.fieldbusinc.com/downloads/primer1_1.pdf</a> (дата обр. 17.04.2021)	Fieldbus Inc.	36	[31]
Поисковая система Google Scholar	“FOUNDATION FIELDBUS или PROFIBUS PA” <a href="https://www.cta.ru/cms/f/366625.pdf">https://www.cta.ru/cms/f/366625.pdf</a> (дата обр. 10.04.2021)	Современные технологии автоматизации	16—20	[32]

### 3.2 Краткое резюме по каждому источнику информации.

#### Основные результаты, полученные авторами

[1] — в данной работе проведён анализ протоколов, используемых для передачи данных в сети. На практике проанализированы два протокола обмена данных *установка – компьютер*, приведенных их достоинства и

недостатки при помощи диаграмм и таблиц. Сделаны выводы о возможностях применения этих протоколов в различных ситуациях.

[2] — в статье проведён подробный разбор двух популярных протоколов связи. Цель работы — ознакомить читателя с ключевыми терминами и в теории разъяснить разницу между двумя протоколами. Приведены достоинства и недостатки, а также границы применения каждого из них.

[3] — в этой главе книги сжато и понятно показывается разница между двумя доминирующими транспортными протоколами: *TCP* и *UDP*.

[4] — статья описывает различные стандарты и протоколы для связи и автоматизации. Статья включает в себя описание протоколов прикладного, транспортного, сетевого и канального уровней модели *TCP/IP*. Данная обзорная статья способствует более корректному выбору протоколов при построении сети, обнаружении и управлении устройствами, налаживанию взаимодействия между объектами автоматизации.

[5] — приводится обзор широко используемых и перспективных протоколов передачи данных приборов учета, используемых в России и Европе (*Modbus, DLMS/COSEM, M-BUS, IEC 61344, Euridis*). В обзоре рассматриваются протоколы, отвечающие российским/европейским стандартам, и не рассматриваются частные фирменные разработки, из-за их ограниченной сферы применения.

[6] — в данной статье автор провёл анализ наиболее часто применяемых протоколов связи для автоматизации в современном мире. На примере популярных стандартных решений рассмотрена проблема практического применения промышленных сетевых технологий. Приведены виды топологий сети (*общая шина, кольцо, звезда*). Проведён анализ протоколов *Foundation Fieldbus* и *Profibus*.



[7] — в статье рассматриваются вопросы построения распределённых систем АСУ ТП на базе современных сетевых решений. Приведены наиболее популярные Цифровые промышленные сети (ЦПС): *can*, *interbus*, *profibus*, *fieldbus*. Рассмотрены варианты объединения частей сети, работающей по разным протоколам в одну.

[8] — в статье был проведён краткий разбор сетевых технологий промышленного интернета: *Modbus*, *EtherCAT*, *PROFINET*, *Powerlink* с целью ознакомления с различными технологиями.

[9] — в статье сравниваются два самых популярных в настоящее время протокола для автоматизации: *Modbus* и *Profibus*. Описаны сильные и слабые стороны технологий. Рассмотрены применения протоколов вместе и по отдельности. Сделаны выводы о сферах использования. Статья написана разработчиком стандарта *Profibus* и может несколько принижать *Modbus*.

[10] — статья сравнивает возможности таких протоколов, как *Modbus*, *Profibus* и др. Сравнение выполнено в виде списков с особенностями, преимуществами и недостатками.

[11] — в статье рассмотрен самый распространённый не только в мире, но и в России протокол *Modbus RTU*. Приведены расшифровки аббревиатур для упрощения понимания. Описан формат передаваемого в сети пакета. Указаны достоинства и недостатки стандарта. Приведены его характеристики.

[12] — в статье разобрана реализация протокола *Modbus*, форматы данных, программное обеспечение для работы с протоколом. Приведено подробное описание работы протокола, а также примеры применения.

[13] — в статье рассказывается о системах автоматизации на основе про-

токола *Foundation Fieldbus*. Описаны возможности технологии, приведены составляющие компоненты сети. Описана топология, параметры сети и назначение каждого из компонентов системы.

[14] — в статье подробно описана работа автоматизированных объектов на аппаратной и программной части. Рассмотрены способы сбора данных и подачи команд. Проведён разбор нижнего и верхнего уровней. Приведены виды проверенных и современных протоколов.

[15] — в статье описывается протокол *Modbus*. Объяснена популярность на территории России. Описан формат передаваемого с помощью протокола пакета. Приведены отличия *Modbus TCP* от *Modbus RTU*. Указаны достоинства и недостатки протокола.

[16] — в статье расшифровывается термин *SCADA*, аппаратная и программная архитектура, способы связи между устройствами. Приведены данные по возможности масштабирования такой системы. Приведены стадии разработки программного обеспечения для автоматизации. Сделаны выводы о преимуществах таких систем с оговоркой на правильный инжиниринг.

[17] — в статье разъяснён термин *SCADA*. Приведены компоненты, входящие в *SCADA* - систему. Выявлена целевая функция таких систем. Выполнен анализ применения систем диспетчерского управления и сбора данных для автоматизации управления техническими процессами. Выделены структурные компоненты таких систем. Приведены примеры *SCADA* - систем.

[18] — в статье приведён набор функций, повторяющийся во всех проектах по автоматизации. Приведены достоинства внедрения *SCADA* - систем.

[19] — в статье приводятся основные функции, которые должна выполнять SCADA - система. Приводятся достоинства и недостатки совмещения функций автоматического управления и операторского интерфейса. Приведены качества, которые должны быть присущи системе.

[20] — в данной статье рассматриваются основы протокола Modbus и его базовые принципы работы, а также приводится конкретный пример работы с ним. Приводятся преимущества и недостатки протокола. Приведённые в статье таблицы упрощают понимание материала.

[21] — авторы статьи на примере похожей установки производит автоматизацию по протоколу *Modbus TCP*.

[22] — данная статья повествует небольшую историю об индустриальных сетях. Приводятся популярные протоколы индустриальных сетей. Цель статьи — послужить вводом в промышленные сети и сравнить их с обычными.

[23] — учебное пособие УрФУ охватывает не только общетехнические аспекты сетей передачи данных, но и сконцентрировано на темах применения сетей в промышленной автоматизации технических систем.

[24] — в статье проектируется устройство, которое способно собирать любые данные и передавать их в сеть. Пример реализации протокола *Modbus*;

[25] — в данном материале приводится спецификация протокола *Modbus*, основные команды и принципы работы с ним. Документ составлен компанией Modicon, которая ответственна за разработку *Modbus*.

[26] — в данной статье прослеживается история зарождения Fieldbus, принципиальные стадии развития. Проанализировано и классифицировано различие протоколов.

[27] — в статье рассмотрено, какие протоколы используются в системах по всему миру. Рассмотрен протокол *Profibus*.

[28] — энциклопедия инженера автоматизации, изданная д.т.н. Виктором Денисенко (автор одной из цитируемых статей [15]);

[29] — документация по *Profibus* от одного из лидеров рынка промышленной автоматизации и интернета вещей.

[30] — описан стандарт *Foundation FieldBus* и два его подстандарта H1 и HSE. Приведено описание физического уровня коммуникации (в соответствии со стандартом *OSI/ISO*). В деталях рассказано про архитектуру протокола.

[31] — документация стандарта *Foundation Fieldbus*, созданная разработчиком этого протокола.

[32] — в статье приводится сравнение двух современных протоколов автоматизации: *Profibus* и *Foundation FieldBus*. Приведены сходства и различия, достоинства и недостатки. Сделан вывод о выборе наилучшего протокола.

## 4 Систематизация и обобщение информации

### 4.1 Протоколы транспортного уровня в промышленных сетях

Протоколы транспортного уровня предназначены для доставки данных. При этом неважно, какие данные передаются, откуда и куда, протокол предоставляет сам механизм передачи. Блоки данных он разделяет на фрагменты, размеры которых зависят от протокола: короткие объединяет в один, а длинные разбивает. Протоколы этого уровня предназначены для взаимодействия типа точка-точка.

На рис. 1 показана структура идеальной модели *OSI*. Модель определяет различные уровни взаимодействия систем. Каждый уровень выполняет определённые функции при таком взаимодействии.

Данные	Прикладной доступ к сетевым службам
Данные	Представления представление и кодирование данных
Данные	Сеансовый Управление сеансом связи
Блоки	Транспортный безопасное и надёжное соединение точка-точка
Пакеты	Сетевой Определение пути и IP (логическая адресация)
Кадры	Канальный MAC и LLC (Физическая адресация)
Биты	Физический кабель, сигналы, бинарная передача данных

Рис. 1. Уровни модели OSI

В настоящее время двумя самыми популярными протоколами являются *TCP* и *UDP*.

### 4.1.1 Уровни модели OSI

Из рис. 1 и [2] уровни модели OSI делятся на:

- **физический**: предназначен непосредственно для передачи потока данных. Осуществляет передачу электрических или оптических сигналов в кабель или в радиоэфир и, соответственно, их приём и преобразование в биты данных в соответствии с методами кодирования цифровых сигналов;
- **канальный**: полученные с физического уровня данные проверяет на ошибки, если нужно исправляет, упаковывает во фреймы, проверяет на целостность, и отправляет на сетевой уровень;
- **сетевой**: определяет пути передачи данных. Отвечает за трансляцию логических адресов и имён в физические, за определение кратчайших маршрутов, коммутацию и маршрутизацию, за отслеживание неполадок и заторов в сети;
- **транспортный**: организует доставку данных без ошибок, потерь и дублирования (не все) в той последовательности, как они были переданы. Разделяет данные на фрагменты равной величины, объединяя короткие и разбивая длинные (размер фрагмента зависит от используемого протокола);
- **сеансовый**: управляет созданием/завершением сеанса связи, обменом информацией, синхронизацией задач, определением права на передачу данных и поддержанием сеанса в периоды неактивности приложений. Синхронизация передачи обеспечивается помещением в поток данных контрольных точек, начиная с которых возобновляется процесс при нарушении взаимодействия;

- **представления**: на этом уровне может осуществляться преобразование протоколов и сжатие/распаковка или кодирование/декодирование данных, а также перенаправление запросов другому сетевому ресурсу, если они не могут быть обработаны локально;
- **прикладной**: уровень приложений (англ. Application layer). Обеспечивает взаимодействие сети и приложений пользователя, выходящих за рамки модели OSI. На этом уровне работают изученные в работе протоколы автоматизации промышленных сетей.

#### 4.1.2 Транспортный протокол TCP

**TCP** [3] – один из основных протоколов транспортного уровня. Он обеспечивает надёжную доставку потока байтов от одного устройства к другому. *TCP* ориентирован на качество соединения, а не на скорость. В нём присутствует механизм признания (acknowledgement) и механизм предотвращения скоплений, что уменьшает передачу в то время, как сеть загружена.

Этот протокол можно назвать стабильным, поскольку он способен адаптироваться к различным ситуациям, происходящим в сети. После отправки пакета в сеть, он сохраняется в буфере и дожидается пакета, подтверждающего получение данных приёмником, что крайне важно при передаче данных с приборов.

##### 4.1.2.1 Функции TCP

- **передача данных**: передаёт непрерывный поток данных в форме сегментов для передачи через сеть;
- **надёжная доставка**: пакеты ACK (см. 4.1.2.2. Структура TCP пакета) помогают удостовериться в том, что пакет получен там, где необходимо;
- **управление потоком**: получатель контролирует объём полученных данных при помощи возврата “окна” с каждым пакетом ACK. В этом окне

содержится то количество данных, которое готов принять приёмник;

- **мультиплексирование**: возможность использовать несколько портов для одновременного обмена данными. Объединение адреса сети и хоста образует сокет.

#### 4.1.2.2 Структура TCP пакета

На рис. 2 приведена структура TCP. Краткое резюме по полям:

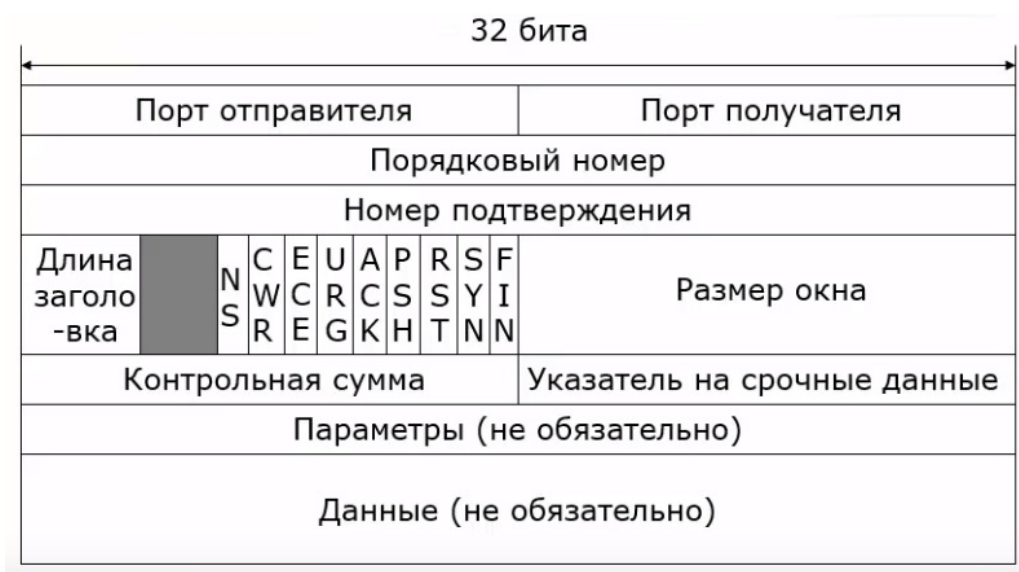


Рис. 2. Структура TCP сегмента

- **порт отправителя**: 16-ти битный номер, определяющий отправителя пакета;
- **порт получателя**: 16-ти битный номер, который отправитель использует для отправки пакета получателю;
- **порядковый номер**: в этом поле содержится первый номер байта в сегменте;
- **номер подтверждения (ACK)**: обеспечивает гарантию доставки сообщений. Например, был получен байт 2459, значит в пакете ACK будет передан следующий ожидаемый байт – 2460;



- **длина заголовка:** число 32-х разрядных слов в заголовке;
- **резерв:** 3 - 6 битов, зарезервированные для дальнейшего развития протокола и установлены на значение 0;
- **контрольные биты (флаги):** определяют использование сегмента или служат проверкой действительности для других полей:
  - **NS:** экспериментальный флаг, используется для защиты от случайного злонамеренного сокрытия пакетов от отправителя;
  - **CWR:** используется хостом, чтобы указать, что он получил пакет с установленным флагом *ECE*;
  - **ECE:** получатель поддерживает ECN (взаимное уведомление хоста и пира о переполнении канала без потери пакетов);
  - **URG:** флаг срочности используется для уведомления получателя о необходимости обработки срочных пакетов перед обработкой всех других пакетов. Получатель будет уведомлен, когда будут получены все известные срочные данные. В табл. 5 приводится отличие флагов *PSH* и *URG*;;
  - **ACK:** используется для подтверждения успешного получения пакета;
  - **PSH:** используется для информирования отправителя о том, что требуется более высокая пропускная способность, поэтому, если возможно, данные должны передаваться с более высокой пропускной способностью, то есть отправленных пакетов будет больше, однако скорость обмена информацией будет быстрее (что критично для систем реального времени). В табл. 5 приводится отличие флагов *PSH* и *URG*;
  - **RST:** используется для сброса TCP-соединения при возникновении

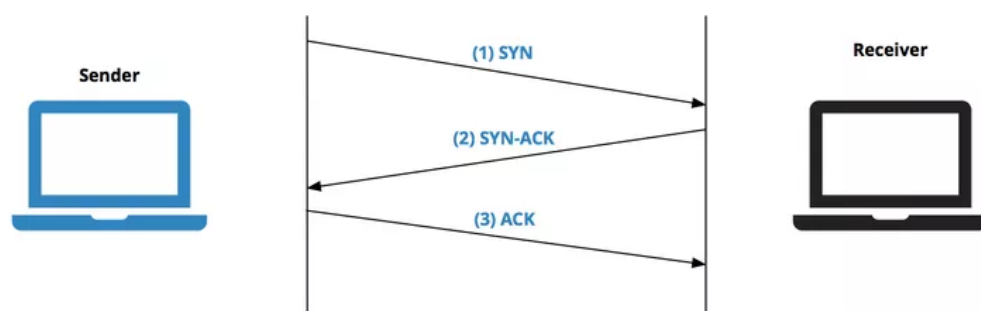


Рис. 3. Трёхстороннее рукопожатие с пакетом SYN

путаницы в порядковых номерах. В табл. 6 приведено отличие *FIN* от *RST*;

- **SYN**: флаг синхронизации используется в качестве первого шага в установлении трехстороннего рукопожатия между двумя хостами. Этот флаг должен быть установлен только для первого пакета от отправителя и получателя. На рис. 3 показан процесс трехстороннего рукопожатия;
  - **FIN**: флаг завершения означает, что от отправителя больше нет данных. Следовательно, он используется в последнем пакете, отправленном отправителем. В табл. 6 приведено отличие *FIN* от *RST*;
- **размер окна**: в этом поле получатель указывает, сколько данных он может принять. Поле используется для управления потоком;

Таблица 5. Отличие флагов PSH и URG

PSH	URG
Все данные из буфера передаются отправителю/приёмнику	Только данные, помеченные флагом <i>URG</i> будут переданы приёмнику (немедленно)
Данные отправляются последовательно	Данные передаются в случайном порядке

Таблица 6. Отличие флагов PSH и URG

FIN	RST
Аккуратно завершает соединение	Резко сообщает другой стороне общения о завершении передачи
Нет потери данных	Данные сбрасываются
Устройство, получившее этот флаг может продолжать делать запросы	Получатель этого флага должен перестать передавать данные

- **контрольная сумма:** используется для проверки правильности доставки данных, если контрольная сумма, рассчитанная получателем, не совпадает с контрольной суммой в заголовке TCP, то этот сегмент отбрасывается;
- **указатель на срочные данные:** поле указывает порядковый номер октета, которым заканчиваются важные (urgent) данные. Поле принимается во внимание только для пакетов с установленным флагом URG;
- **параметры:** необязательный параметр, применяемый для тестирования и увеличения пропускной способности канала;
- **данные:** сообщение протокола верхнего уровня.

#### 4.1.2.3 Применение TCP

Технология TCP применяется в следующих областях [2]:

1. **HTTP:** самый распространённый протокол передачи данных по сети;
2. **FTP:** протокол обмена данными по сети;
3. **IMAP:** доступ к электронной почте;

4. **POP**: доступ к электронной почте;
5. **RLogin**: удалённый доступ к оборудованию;
6. **SMTP**: доступ к электронной почте;
7. **SSH**: создание защищённых соединений для удалённого доступа;
8. **Modbus TCP**: протокол Modbus, “завёрнутый” в оболочку TCP.

### 4.1.3 Протокол UDP

**UDP** [2] – один из основных протоколов обмена данными. Хост отправляет сообщения в форме датаграммы без предварительной установки соединения. Подходит для случаев, когда важна скорость, а не гарантия доставки.

#### 4.1.3.1 Структура UDP датаграммы

На рис. 4 приведена структура UDP датаграммы. Краткое резюме по всем



Рис. 4. Структура UDP датаграммы

полям:

- **source port (порт отправителя)**: порт процесса, который отправляет датаграмму;

- **destination port (порт назначения)**: порт процесса, принимающего датаграмму;
- **length (длина)**: длина датаграммы (вместе с *Header*);
- **checksum (контрольная сумма)**: опциональное поле. Контрольная сумма позволяет принимающему устройству проверять целостность заголовка пакета и полезной нагрузки. Это необязательно в IPv4, но стало обязательным в IPv6;
- **data (данные)**: передаваемые пакетом данные.

#### 4.1.4 Сравнение TCP и UDP

По теоретическим данным [2, 3] и экспериментальным данным [1], можно сделать следующие выводы:

Таблица 7. Сравнительная таблица TCP и UDP

TCP	UDP
Надёжное соединение без перегрузки сети	Не гарантирует надёжность и порядок отправляемых пакетов
Создание подключения осуществляется при помощи 3 рукопожатий, см рис. 3. После установки соединения данные передаются в обе стороны [2]	Сразу отправляет данные [3]
Пропускная способность [1] (количество успешно принятых пакетов) у TCP составила 740 kbps	Пропускная способность [1] у UDP составила 586 kbps
Задержка у TCP составила 0.059 ms [1]	Задержка у UDP составила 0.051 ms [1]

TCP	UDP
TCP потерял 8 пакетов [1]	UDP потерял 311 пакетов [1]
TCP доставил 96.92% пакетов [1]	UDP доставил 74.12% пакетов [1]
TCP применяется там, где необходима надёжность соединения	UDP применяется там, где время играет ключевую роль

#### 4.1.5 Вывод

После рассмотрения протоколов транспортного уровня, можно сделать вывод, что для автоматизации вакуумной установки лучше всего пойдёт *TCP*, поскольку в нашем случае важнее не скорость отправки и получения, а надёжность соединения.

Хочется отметить, что хоть TCP и медленнее, но он теряет гораздо меньше пакетов, доставляет куда больший процент пакетов и экономит трафик, поскольку нет необходимости в повторной отправке потерянных пакетов [2].

Как показала практика, задержки у TCP не сильно выше, чем у UDP [1].

## 4.2 История разработки промышленных протоколов

### 4.2.1 Предыстория появления автоматизации

Автоматизация подразумевает в себе соединение воедино различного оборудования. С развитием промышленности требования всё возрастали, что создало спрос на различного вида интерфейсы между измерительным прибором или устройством с системой измерения и управления. К тому же появилась необходимость записи полученных данных [10].

В течение многих лет системы обмена данными строились вокруг одного мощного вычислительного устройства, к которому шло огромное количество кабелей. Подобная структура была дорога в обслуживании и отличалась низкой степенью автоматизации.

Альтернативой стали так называемые ЦПС, которые состоят из узлов, обменивающихся данными цифровым способом. На сегодняшний момент таких систем насчитывается большое количество [7].

Уже более 30 лет широко применяется слово *FieldBus*. Обычно под этим термином понимается сеть, которая соединяет различного рода устройства (ПЛК, сенсоры) с человеко - машинным интерфейсом (ММИ). В это понятие входит множество протоколов, разнообразие которых обусловлено [26]:

- нуждой разнообразных компаний из разных областей в средстве сбора и обмена данными в промышленных сетях;
- огромному числу разнообразных сенсоров, датчиков и устройств, которые необходимо было соединить между собой.

#### **4.2.2 Технология Fieldbus: возникновение и требования**

Есть несколько причин возникновения концепта *FieldBus*, но их можно разделить на 2 основные группы [26]:

1. Потребности пользователей (предприятий):
  - 1.1. Необходимость единого стандарта;
  - 1.2. Концепт предприятия, управляемого компьютерами.
2. Возможности технологий:
  - 2.1. Модель OSI (см. рис. 1)
  - 2.2. Возможности микроэлектроники (внедрение “интеллекта” даже в маленькие датчики, “распределённый интеллект”).

Последующее развитие индустрии показало, что пользователи выбирают открытые протоколы, поскольку в отличие от проприетарных решений они обладают следующими преимуществами [22]:

- большее число поддерживаемого оборудования;
- возможность разделить стоимость разработки протокола между компаниями, которые готовы вкладываться в разработку свободного ПО;
- качество поддержки открытого ПО обычно выше, чем у проприетарного.

### 4.2.3 Modbus

Протокол *Modbus* RTU был разработан компанией Modicon (в настоящее время - Schneider Electric) в 1979 году для использования в ПЛК собственного производства. На текущий момент является де-факто стандартом для связи устройств промышленной сети [6, 10].

Изначально протокол работал по интерфейсу RS-232, позднее появилась реализации протокола для интерфейсов RS-485 и TCP. Протокол быстро набрал популярность, и многие производители стали внедрять его в своих устройствах.

Позже права на протокол были переданы некоммерческой организации Modbus Organization, которая до сегодняшнего дня владеет стандартом [12].

По распространённости в России конкурирует только с *Profibus* [15].

### 4.2.4 Profibus

Если протокол *Modbus* можно назвать “дедушкой” протоколов, то *Profibus*— “молодой атлет”: худой и быстрый. Он был разработан в 90-х годах прошлого века для удовлетворения всех потребностей промышленной связи как для автоматизации производства, так и для автоматизации процессов [9].

*Profibus* настроен как универсальная и открытая (открыт не до конца [6]) система связи. Первоначально разработанный для обеспечения дискретного производства, он расширился до автоматизации процессов и корпоративных приложений. *Profibus* включает в себя несколько спецификаций протокола промышленной шины, включая [10]:



- *Profibus-DP*;
- *Profibus-PA*;
- *PROFINet* и другие.

Разработавшая его компания Siemens AG до сих пор является основным разработчиком вариаций данной платформы. Несмотря на то, что стандарт позиционируется как открытый, открытыми являются только нижние уровни сетевого взаимодействия. Протоколы доступа к среде, форматы кадров, интерфейсы взаимодействия с приложениями прикладного уровня регламентируются проприетарными протоколами фирмы Siemens. Для получения доступа к ним требуется вступление в группу разработчиков стандарта *Profibus* [6].

#### 4.2.5 Foundation Fieldbus

*Foundation FieldBus* является цифровой системой связи, применяемой в автоматизации наряду с такими, как *Profibus* и *Modbus*. В настоящий момент включает в себя два протокола информационного обмена между участниками сети [13]:

- H1;
- HSE.

Стандарт был разработан *American Fieldbus Foundation* в ответ на задержки по созданию международного стандарта *FieldBus* [22].

Изначально разработанный для решений низкоуровневых задач автоматизации протокол *FieldBus* теперь носит название *Fieldbus H1* в связи с появлением таких решений, как:

- *Foundation Fieldbus Safety Instrumented Functions* для использования в местах, где необходима безопасность;

- *Foundation Fieldbus High Speed Ethernet* (высокоскоростной интернет). Одна из реализаций протокола *Foundation Fieldbus (HSE)* для работы на высоких скоростях.

## 4.3 Принципы работы протоколов

### 4.3.1 Понимание термина *Fieldbus*

В дословном переводе термин *FieldBus* означает “промышленная сеть”, однако это не определённый протокол передачи данных и не тип архитектуры. Под этим термином лучше всего представить сферу применения.

Промышленная сеть – это [6]:

- среда передачи данных, отвечающая жёстким и, зачастую, противоречивым требованиям;
- набор стандартных протоколов обмена данными, позволяющих связать воедино оборудование различных производителей, а также обеспечить взаимодействие нижнего и верхнего уровней

Обычно *FieldBus*– это двунаправленная цифровая сеть, используемая для контроля и автоматизации. Сеть состоит из [10]:

- человеко - машинный интерфейс;
- главная контролирующая система (master);
- набор интерфейсов (slave) между датчиками, насосами, и прочим оборудованием.

Использование подобной системы способно уменьшить время простоя, заранее сообщая диагностические данные оператору.

## 4.3.2 Принцип работы промышленной сети

### 4.3.2.1 Принцип работы промышленной автоматики

В процессе автоматизации всё делится на 2 уровня. Пример построения такой системы показан на рис. 5 [14]:

- **нижний:** уровень связи устройств управления и подведомственного оборудования (их ещё называют полевые устройства);
- **верхний:** панель управления оператора, через которую он может отслеживать происходящее на объекте автоматизации. Именно на верхнем уровне располагается система управления и автоматизации SCADA (см. 4.4. SCADA-системы).

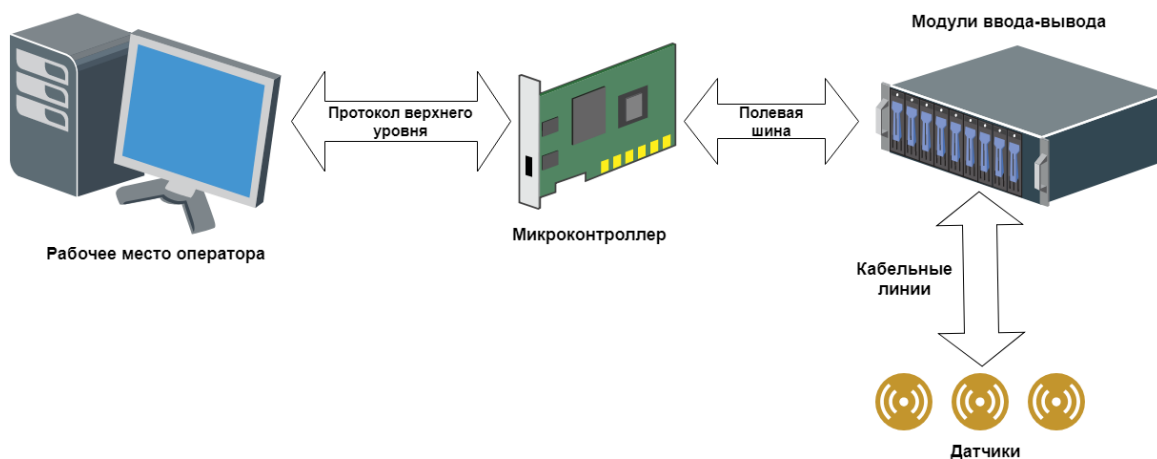


Рис. 5. Общая схема автоматизации объекта

### 4.3.2.2 Топология сети

Существует три наиболее значимых топологии сети автоматизации [6].

1. **Общая шина.** Структура топологии приведена на рис. 6.

- **Достоинства:**
  - простая;
  - недорогая;

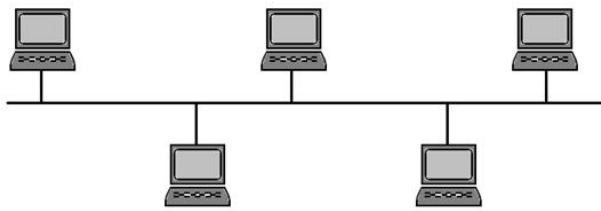


Рис. 6. Топология “общая шина”

- лёгкая в настройке;
- хорошо подходит для сильно распределённых объектов.
- **Недостатки:**
  - присутствие в каждой точке сети общего трафика;
  - потеря связи при одиночном обрыве канала.

2. **Кольцо.** Структура топологии приведена на рис. 7.

- **Достоинства:**
  - абсолютная предсказуемость трафика;
  - хорошая пропускная способность.
- **Недостатки:**
  - высокая стоимость организации канала связи;
  - нерациональное использование сетевого трафика при неправильной конфигурации;
  - потеря всей синхронизации при отключении хотя бы одного из узлов.

3. **Звезда.** Обычно является частью большей сети. Структура топологии приведена на рис. 8.

- **Достоинства:**

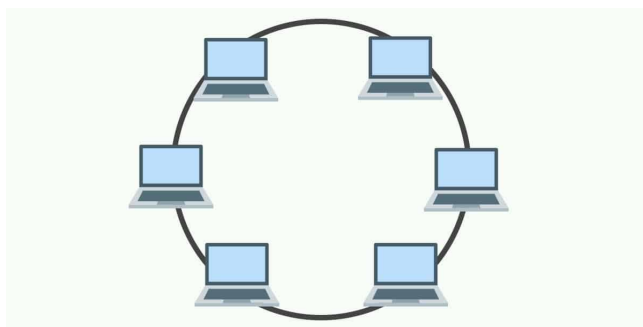


Рис. 7. Топология “кольцо”

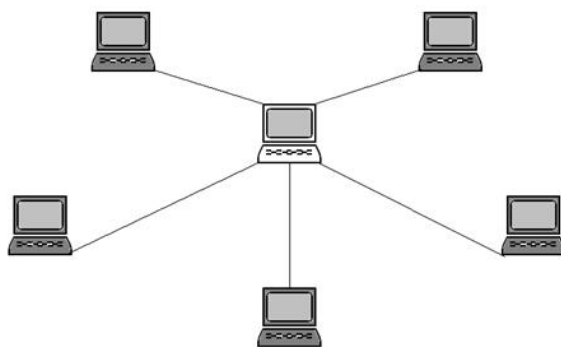


Рис. 8. Топология “звезда”

- дополнительная защита сети от выхода из строя или отключения узлов;
- простая масштабируемость;
- оптимизация трафика;
- допускаются коллизии.

— **Недостатки:**

- обмен идёт через один высоконагруженный компьютер;
- потеря связи при одиночном обрыве канала;
- ограничение числа рабочих станций числом портов центрального компьютера.

### 4.3.2.3 Основные характеристики сетей

С развитием техники стало возможным наделить “интеллектом” каждый из полевых датчиков. Каждый из узлов цепи способен [7]:

- принимать команды от других узлов сети;
- считывать данные с подключенных датчиков;
- оцифровывать полученные данные в случае их представления аналоговым способом;
- передавать информацию другим узлам сети.

### 4.3.2.4 Режимы обмена данными

В промышленной автоматизации существует три режима обмена данными [7, 26]:

1. **Ведущий - ведомый.** Ведущее устройство последовательно опрашивает подчинённые узлы. В зависимости от запроса ведомый узел может:
  - выполнить полученную команду;
  - передать ведущему устройству данные с подключенных к нему датчиков.

Примером таких сетей могут быть *Modbus* и *Profibus*.

2. **Клиент - сервер.** Очень похож на предыдущий тип. Клиент запрашивает данные, а сервер их предоставляет. Функции клиента и сервера могут быть исполнены одним устройством. Отличие от предыдущего пункта – в отличие от топологии master-slave, топология client-server позволяет серверу автоматически отправлять данные (ведомые устройства этого сделать не могут). Представитель – *Foundation FieldBus*.

3. **Подписка.** Узел, нуждающийся в периодическом поступлении информации, подписывается на получение её от другого узла и получает регулярную рассылку без дополнительных запросов. Есть два режима работы:

3.1. Данные передаются циклически, с определённым интервалом;

3.2. Данные передаются только в случае их изменения.

Примером такой сети также может быть *Foundation FieldBus*.

### 4.3.3 Modbus

#### 4.3.3.1 Краткое резюме

Открытый коммуникационный протокол для обмена данными между сетевыми устройствами, основанный на архитектуре ведущий - ведомый (master-slave). Обмен данными представляет собой транзакции, состоящие из запросов и ответов [4].

**Достоинства протокола [5]:**

- открытость;
- простота;
- массовость;
- дешевизна;
- отсутствие необходимости в специальных интерфейсных контроллерах [15];
- надёжный метод контроля ошибок.

**Недостатки протокола:**

- невозможность передавать данные по мере получения, необходим постоянный опрос slave - устройств [15];

- сетевые адреса прописываются на этапе проектирования системы и не могут быть изменены [4];
- длина запроса ограничена, а данные могут быть запрошены только из последовательно расположенных регистров;
- не предусмотрен способ, с помощью которого подчиненное устройство могло бы обнаружить потерю связи с ведущим;
- соответствие регистров типам измерений и измерительным каналам не регламентировано, что может приводить к несовместимости протоколов счетчиков разных типов даже одного производителя;
- нет защиты от сторонних несканционированных команд, нельзя передавать конфиденциальные данные [11].

#### 4.3.3.2 Принцип работы

##### 4.3.3.2.1 Физический уровень

Протокол *Modbus* может быть использован со следующими интерфейсами:

- **RS-232/422/485**: последовательные интерфейсы, широко распространенные в промышленности. Интерфейсы RS-422/485 обеспечивают дальность сигнала до 1200 метров. Используются протоколы *Modbus RTU/ASCII*
- **TCP/IP**: физическим каналом передачи данных могут любые ethernet-интерфейсы. Используется протокол *Modbus TCP*.

Существует 3 разновидности протокола *Modbus* [11]:

1. *Modbus ASCII*: в котором данные кодируются символами из таблицы ASCII (рис. 1) и передаются в шестнадцатеричном формате и данный формат протокола встречается довольно редко;



2. *Modbus RTU*: самый распространенный вариант протокола *Modbus*, который кодирует данные в двоичном формате и разделяет пакеты с помощью временного интервала;
3. *Modbus TCP*: данные кодируются в двоичном формате и упаковываются в TCP - пакет, для передачи по IP-сетям и предназначен для работы в локальных сетях.

На рис. 9 показан пример построения схемы контроля за неким объектом при помощи протокола *Modbus* [12].

#### 4.3.3.2.2 Логический (канальный) уровень

Протокол *Modbus* предполагает 1 ведущее устройство и до 247 ведомых. Обмен данными начинается ведущим устройством. Ведомые не могут начинать передачу и обмениваться данными между собой. В любой момент времени может происходить только один акт обмена. Структуры пакетов *Modbus* при работе 3 способами приведены на рис. 10.

#### 4.3.3.2.3 Modbus RTU

Сообщение начинает восприниматься как новое после паузы длиной в 14 бит. На рис. 11 показан формат пакета. У пакета есть следующие поля [15]:

- **Адрес:** содержит адрес ведомого устройства. Адрес отправляется даже при ответе на запрос мастера, тем самым всегда понятно, откуда пришёл ответ;
- **Код функции:** говорит модулю о том, что ему необходимо сделать;
- **Данные:** тут может содержаться информация о параметрах, которые используются в исполнении команд мастера или показания, передаваемые мастеру;

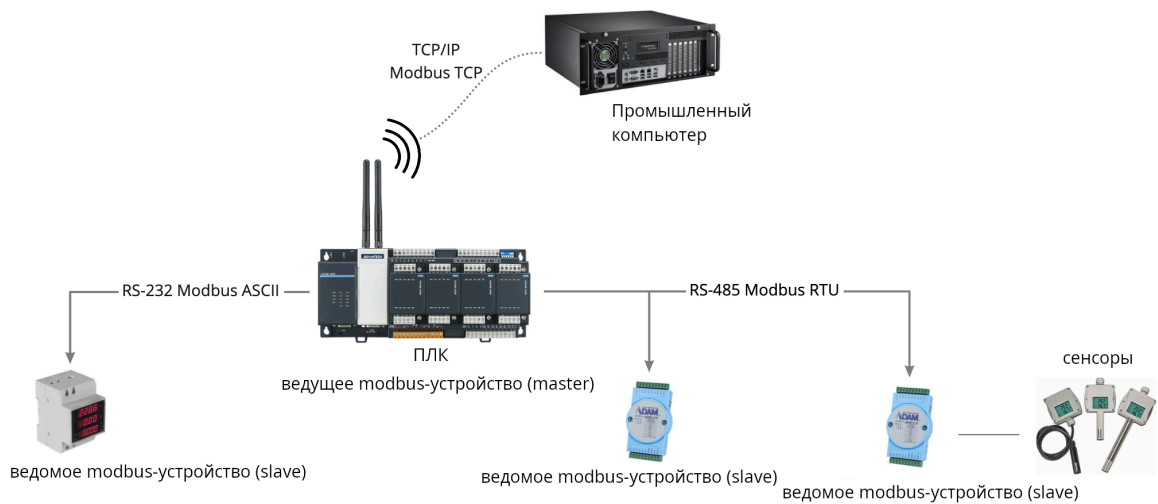


Рис. 9. Физический уровень протокола *Modbus*

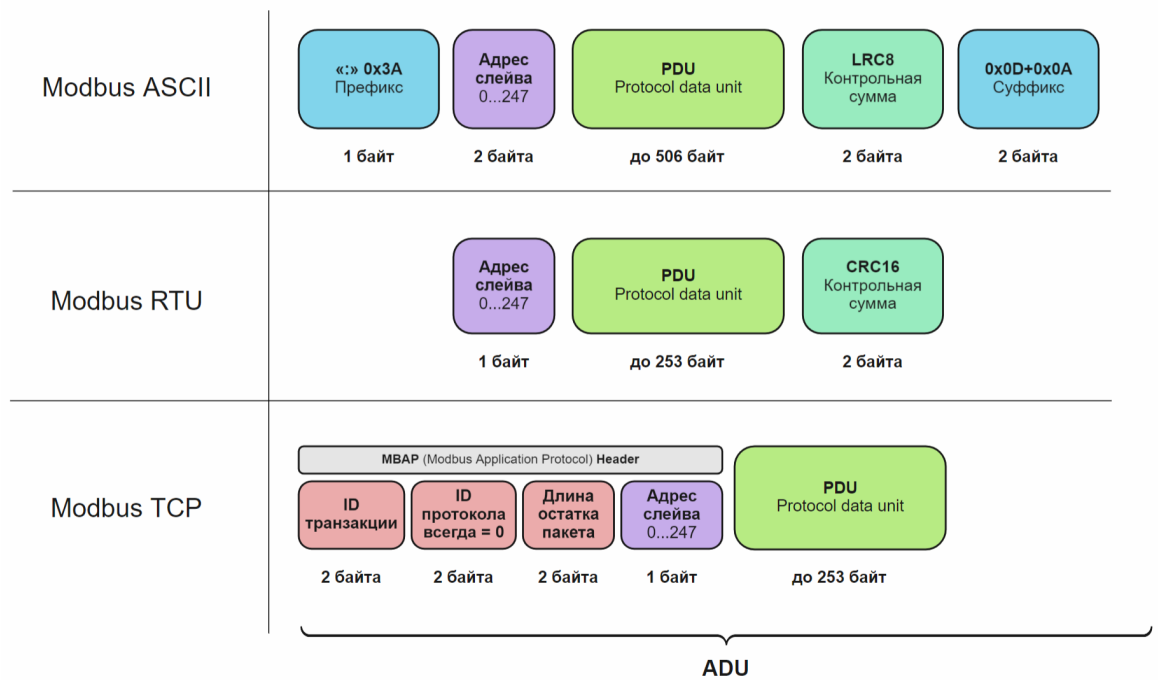


Рис. 10. Структура пакета *Modbus*



Рис. 11. Формат кадра протокола *Modbus RTU*

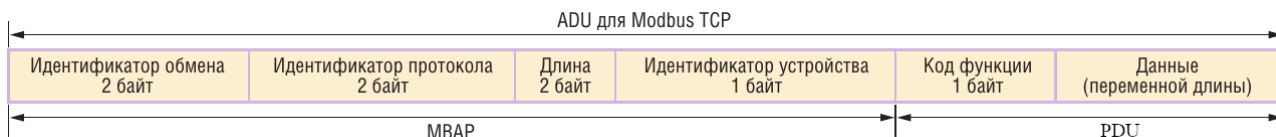


Рис. 12. Формат кадра протокола *Modbus TCP*

- **Контрольная сумма:** используется для проверки целостности пакета.

#### 4.3.3.2.4 Modbus TCP

Данный протокол используется для того, чтобы подключить устройства, работающие по протоколу *Modbus* к сети *Internet* [8]. То есть, в соответствии со стандартом *OSI/ISO* (см. рис. 1) на транспортном уровне используется протокол *TCP*, а на прикладном – *Modbus*. В этом случае проверка целостности пакета ложится на протокол *TCP*. Структура протокола *Modbus TCP* приведена на рис. 12. У пакета есть следующие поля [15]:

- **Идентификатор обмена:** используется для идентификации сообщения в случае, когда в пределах одного *TCP* - соединения клиент посылает серверу несколько сообщений без ожидания ответа после каждого сообщения;
- **Идентификатор протокола:** всегда выставлен на 0 (как и у протокола *TCP*);
- **Длина:** указывает количество следующих байтов;
- **Идентификатор устройства:** адрес slave - устройства;
- **Код функции:** аналогично 4.3.3.2.3. **Modbus RTU**;
- **Данные:** аналогично 4.3.3.2.3. **Modbus RTU**.

Как можно заметить, *Modbus RTU* оказывается “вшит” в пакет *TCP*, тем самым получается *Modbus TCP*. На рис. 13 показан принцип работы такой системы [15]:

- коды функций передаются с прикладного уровня на транспортный (*Modbus–TCP*), добавление заголовка *TCP*;
- передача на сетевой уровень, добавление блока *IP*;
- передача на канальный уровень, а затем на физический (*Ethernet*)

После прохождения через канал связи пакет начинает обратное движение согласно модели *OSI/ISO* (см. рис. 1).

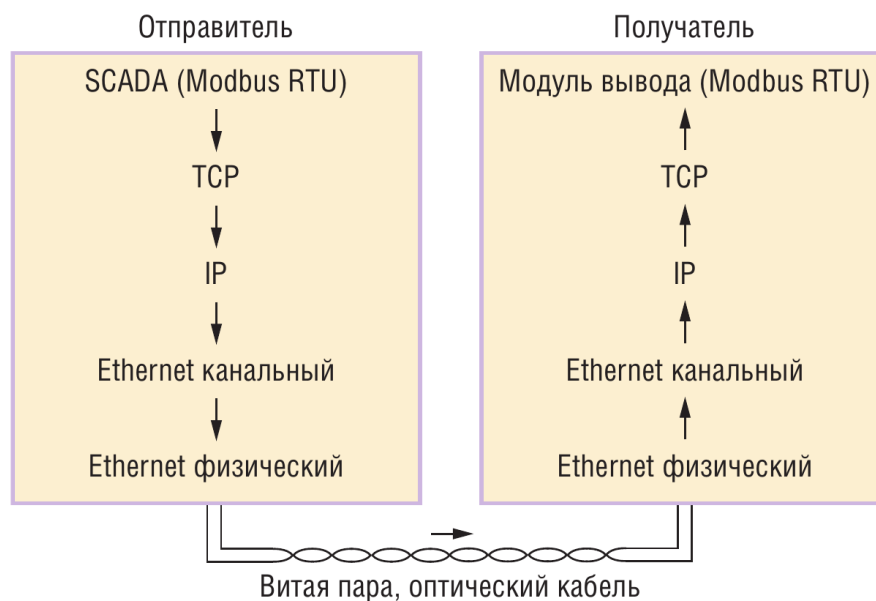


Рис. 13. Процесс передачи пакетов *Modbus RTU* по сети *TCP*

Более подробно о работе с протоколом *Modbus* можно узнать в документации [25].

#### 4.3.4 Profibus

##### 4.3.4.1 Краткое резюме

*Profibus*— один из самых популярных и широко применяемых протоколов при автоматизации. Протокол работает по такой же системе, что и *Modbus*: master - slave.

Этот протокол используется для передачи полевых данных в системы управления технологическими процессами и обеспечивает прямое управление и

обслуживание устройств. При смене полевого устройства новое устройство автоматически берет на себя роль предыдущего устройства, что позволяет легко осуществлять смену устройств без прерывания работы системы.

Существует 3 подвида *Profibus* [6, 7, 22]:

1. *Profibus DP*: быстрый протокол с одним мастером. Обеспечивает высокую скорость передачи данных (до 12 Мбит/с). Отлично подходит для построения систем контроля и сбора данных с одним ведущим узлом. Работает на низком уровне;
2. *Profibus FMS*: предназначен для работы с системами производителей, не поддерживающих *Profibus DP* [6, 27];
3. *Profibus PA*: используется во взрывоопасных местах. Подключается к *Profibus DP* через разветвители.

#### 4.3.4.2 Принцип работы

*Profibus* как и *Modbus* работает по протоколу master - slave. Однако, в отличие от *Modbus*, этот протокол способен работать с несколькими мастерами благодаря кольцевой топологии (см. **4.3.2.2. Топология сети**) и маркерному доступу [9].

Каждое устройство должно пройти через “инициализацию”, во время которой оно подключается к сети. У каждого ведомого устройства есть “таймер отказоустойчивости” – если мастер не разговаривал с ним некоторое время, устройство возвращается в “спячку” и ему придётся повторить процедуру инициализации снова. В комбинации со сторожевым таймером это даёт гарантию того, что передача данных будет происходить каждый “цикл”.

Цикл проходит так (см. рис. **14**): мастер А получает токен, опрашивает своих подопечных и передаёт токен дальше.

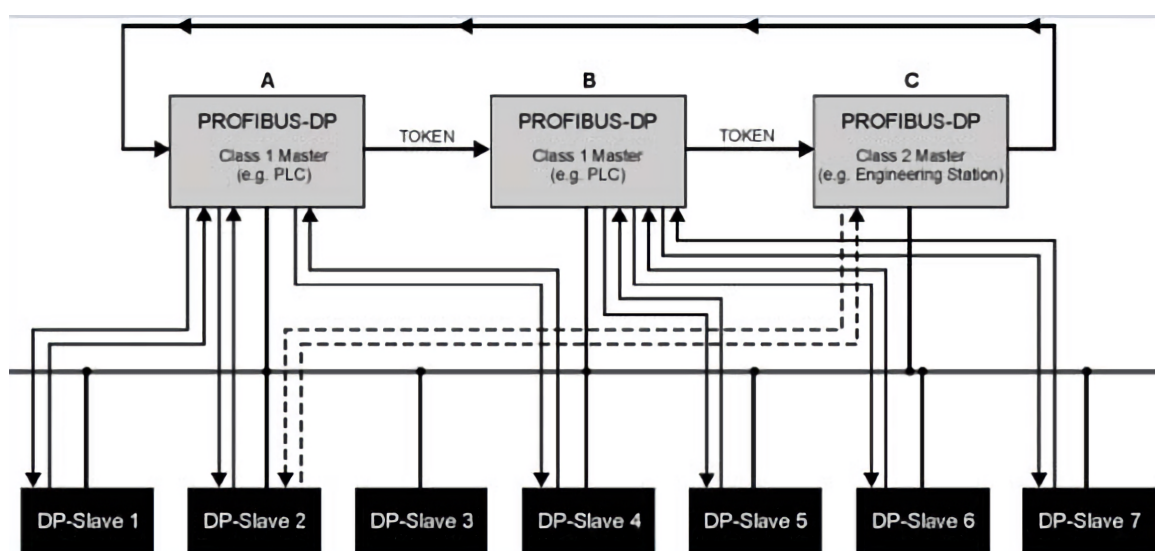


Рис. 14. Цикл *Profibus*

#### 4.3.4.2.1 Физический уровень

На физическом уровне *Profibus* использует стандарт RS-485 при скорости передачи до 12 Мбит/с и с размерами сегментов сети до 32 устройств. Количество устройств можно увеличить с помощью повторителей интерфейса [9].

Протокол устойчив к помехам и шумам. В случае правильной установки и настройки представляет из себя сверхнадёжную систему [9].

#### 4.3.4.2.2 Канальный уровень

Обеспечиваются следующие требования:

- в процессе коммуникации между ведущими устройствами необходимо обеспечить выполнение каждым из них своей задачи в течение заранее определенного интервала времени;
- взаимодействие ведущих устройств (контроллеров) с ведомыми должно происходить максимально быстро.

Используемый в протоколе метод передачи маркера по кольцу показан на рис. 14.

SD	LE	LEr	SD	DA	SA	FC	DSAP	SSAP	DU(1...244 байт)	FCS	ED
----	----	-----	----	----	----	----	------	------	------------------	-----	----

Рис. 15. Структура телеграммы *Profibus*

#### 4.3.4.2.3 Передача сообщений

У *Profibus* есть два типа сервисов передачи сообщений [28]:

1. **SRD**: позволяет отправить и получить данные в одном цикле обмена. Этот способ обмена наиболее распространен в *Profibus* и очень удобен при работе с устройствами ввода-вывода, поскольку в одном цикле можно и отправить и получить данные;
2. **SND**: используется, когда надо отправить данные одновременно группе ведомых устройств (многоабонентский режим) или всем ведомым устройствам (широковещательный режим). При этом ведомые устройства не отправляют свои уведомления мастеру.

Пакет данных в *Profibus* называется телеграмма. Её структура приведена на рис. 15. Расшифровка полей телеграммы [28, 29]:

- **SD**: стартовый разделитель. Используется для указания начала телеграммы и ее формата;
- **LE**: длина передаваемых данных (DA+SA+FC+DSAP+SSAP+DU);
- **LEr**: повторение поля LE с целью его резервирования;
- **DA**: адрес устройства-получателя телеграммы;
- **SA**: адрес отправителя;
- **FC**: код типа телеграммы (запрос, уведомление, ответ, диагностические данные, тип устройства - мастер или ведомый, приоритет, уведомление);

- **DSAP:** устройство-получатель использует это поле, чтобы определить, какой тип сервиса нужно выполнить;
- **SSAP:** COM порт отправителя;
- **DU:** данные длиной от 1 до 244 байт;
- **FCS:** контрольная сумма телеграммы (сумма значений полей DA+SA+FC+DU, по модулю 255);
- **ED:** признак конца.

#### 4.3.4.3 Profinet

Как и у *Modbus*, у *Profibus* есть аналог для работы с сетью. Только в отличие от инкапсулирования обычного пакета в *TCP*, *Profinet* – протокол, который был разработан для того, чтобы использовать все преимущества сети *Ethernet* (включая такую функцию, как *Profisafe*) [9].

Более подробно с протоколами семейства *Profibus* можно ознакомиться в документации стандарта [29].

#### 4.3.5 Foundation Fieldbus

Один из самых молодых протоколов, появился в 1995 как результат консорциума крупных производителей в ответ на задержки в разработке единого стандарта “полевой шины” [22].

Многим этот протокол схож с *Profibus PA* [7] :

- работа во взрывоопасных зонах;
- передача сигнала вместе с питанием.

*Foundation FieldBus* – двухуровневый сетевой протокол, который [6]:

- объединяет компьютеры верхнего уровня;



- объединяет датчики, контроллеры, исполнительные механизмы.

К самым главным **преимуществам** стандарта можно отнести [7, 31]:

- *Foundation FieldBus* – открытый протокол, для связи и создания приложений контроля;
- протокол делает ставку на распределённый интеллект, а не на центральный аппарат. *Foundation FieldBus* ориентирован на обеспечение одноранговой связи между узлами без центрального ведущего устройства. Этот подход даёт возможность реализовать системы управления, распределённые не только физически, но и логически, что во многих случаях позволяет повысить надёжность и живучесть автоматизированной системы;
- все устройства, работающие по протоколу *Foundation FieldBus*, должны работать между собой вне зависимости от производителя без дополнительных ухищрений;
- существует специальный язык описания конечных устройств (DDL), позволяющий легко расширять сеть. Достаточно физически подключить новое устройство, и оно тут же самоопределится на основании заложенного описания DD, после чего все функциональные возможности нового узла становятся доступными в сети.

Однако, у протокола есть и существенный недостаток:

- малая распространённость в России, где конкурируют только *Modbus* и *Profibus*.

## 4.4 SCADA-системы

### 4.4.1 Что такое SCADA - система

SCADA – Supervisory Control And Data Acquisition (диспетчерское управление и сбор данных) — программный пакет, предназначенный для разработки

или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. Используется везде, где требуется обеспечить контроль оператора за АСУ ТП [16].

Понятие SCADA - система включает в себя [17]:

- комплекс программ разработки ПО для обеспечения систем автоматизации;
- Программно - Аппаратный Комплекс (ПАК) систем управления процессом, который осуществляет контроль и сбор данных.

#### 4.4.2 Задачи SCADA - систем

Современная SCADA - система должна решать такие задачи, как [16, 17, 18]:

- обмен данными с контроллерами, платами вывода и прочими устройствами (желательно в реальном времени);
- обработка полученной информации;
- отображение информации на **Machine Man Interface** (интерфейс соединения человека и машины, например - экран монитора) (ММИ);
- ведение базы данных;
- аварийная сигнализация и управление тревожными сообщениями;
- связь с приложениями во внешней среде;
- автоматическое управление и корректирование в связи с изменением условий процесса;
- обеспечение оператора языком программирования для составления запросов к оборудованию;

- иметь в себе драйвера всех подключаемых устройств.

#### 4.4.3 Структура системы

Структуру современной SCADA - системы можно описать так (см. рис. 16): оборудование/датчики передают данные на ПЛК, которые отправляют данные оператору на MMI (**M**achine **M**an **I**nterface (интерфейс соединения человека и машины, например - экран монитора)).

#### 4.4.4 Пример применения SCADA систем

SCADA - системы применяются во всех отраслях промышленности. На рис. 17 показана SCADA - система компании Advantech.

### 4.5 Сравнение протоколов передачи данных промышленных сетей

В 4.3.3. **Modbus**, 4.3.4. **Profibus** и 4.3.5. **Foundation Fieldbus** были рассмотрены 3 протокола передачи данных для промышленных сетей.

Сравнение будет проводиться только среди *Modbus* и *Profibus*, поскольку хоть *Foundation FieldBus* и является самым популярным протоколом с открытым стандартом и множеством возможностей, она не так широко распространена в мире и России, нет достаточной поддержки оборудования [6, 32].

#### 4.5.1 Modbus

Особенности:

- 3 разновидности: TCP, TRU и ASCII;
- имеется контрольная сумма для проверки целостности;
- технология master - slave, только одно ведущее звено;

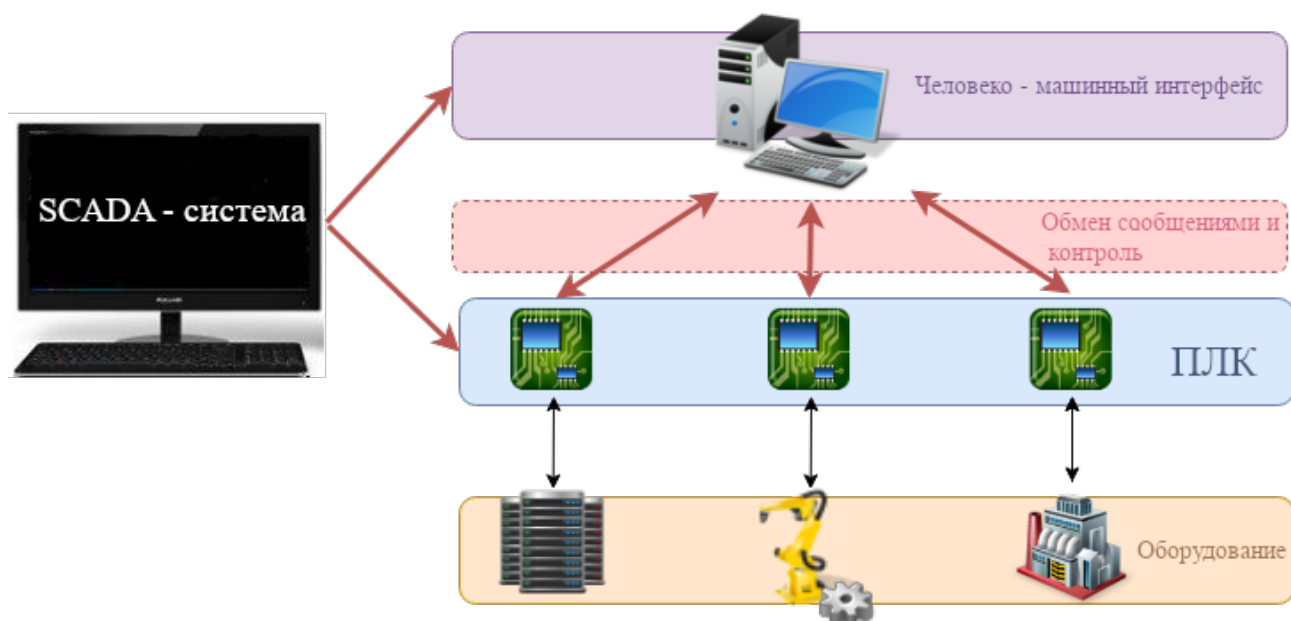


Рис. 16. Топология SCADA - системы

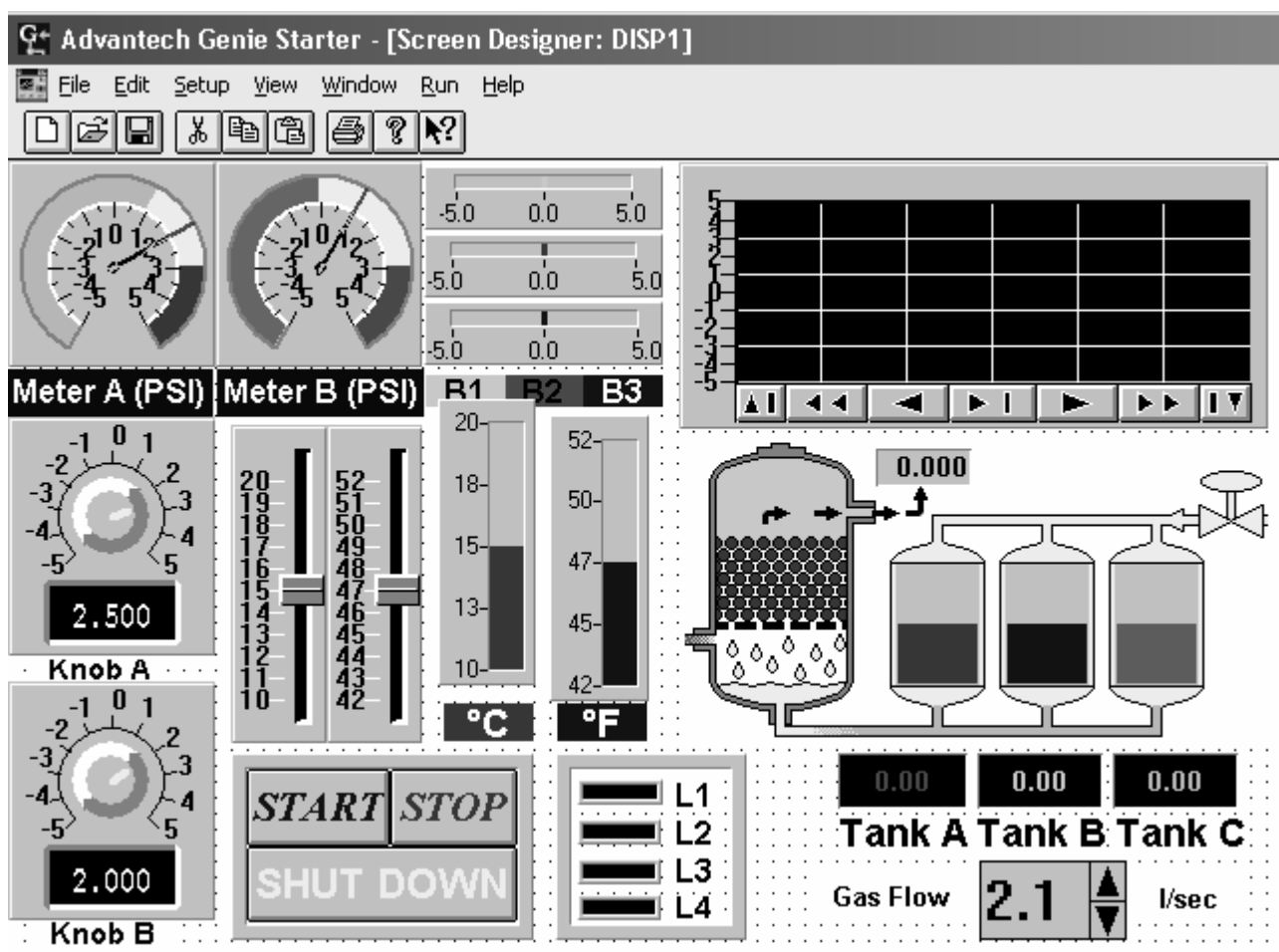


Рис. 17. SCADA - система Advantech Genie

- максимум 32 устройства в сети (64 с повторителями).

Достоинства [10]:

- хорошая документация;
- открытость;
- большое число поддерживаемых устройств.

Недостатки:

- нет возможности диагностировать проблемы с устройствами, если такие случаются;
- некоторые производители могут добавить “от себя” и весь смысл стандартизации теряется.

#### **4.5.2 Profibus**

Особенности:

- может иметь несколько ведущих звеньев, передающих важность при помощи маркера (см. **4.3.4.2. Принцип работы**);
- имеется контрольная сумма для проверки целостности;
- технология master - slave;
- максимум 127 устройств;
- все устройства проходят сертификацию, поэтому совместимы без дополнительных ухищрений.

Достоинства:

- поддержка цифрового и аналогового форматов;

- поддержка нескольких ведущих звеньев;
- простая масштабируемость и лёгкое добавление новых устройств.

Недостатки:

- стандарт открыт не полностью (см. [23]);
- сложнее в освоении, чем *Modbus*;
- в СНГ *Modbus* более популярен.

#### 4.5.3 Итог

Несмотря на все достоинства протокола *Profibus*, описанные в [9], выбор пал на протокол *Modbus TCP* в связи с:

1. Простой документацией;
2. Полной открытостью;
3. Наличием в современных средах разработки поддержки протокола *TCP* (что облегчает работу с протоколом *Modbus TCP*);
4. Оборудованием ОВЕН, работающем по протоколу *Modbus*.

#### 4.6 Примеры применения протокола *Modbus* для автоматизации

Протокол применяется в разнообразных сферах деятельности человека:

1. Передача показаний приборов учёта [5];
2. Автоматизация вакуумной установки [21]. Исследование показало, что автоматизация установки минимизирует количество ошибок оператора, тем самым повышается надёжность процесса и облегчается работа оператора;

3. Мониторинг теплиц, мониторинг системы нагрева воды солнечной энергией [12].

## **4.7 Преимущества автоматизации**

К преимуществам автоматизации можно отнести:

- уменьшение количества ошибок оператора;
- упрощение контроля за процессом;
- повышение надёжности процесса.

## **4.8 Дальнейшая работа**

На основе проведённой научной работы и выбора протоколов передачи данных для автоматизации технологического процесса необходимо изучить одну из современных сред разработки, которая позволяет использовать все возможности протоколов *Modbus* и *TCP*.

## ВЫВОДЫ И РЕЗУЛЬТАТЫ

1. Был составлен терминологический словарь, сформированы поисковые запросы и найдена литература по промышленным протоколам и автоматизации;
2. В результате проведённого литературного обзора были изучены два самых популярных сетевых протокола обмена данными:
  - TCP;
  - UDP.

Был выбран протокол *TCP*, поскольку он:

- ориентирован на качество соединения, а не на скорость;
  - проверяет пакеты на целостность;
  - имеет задержку передачи данных не сильно ниже, чем у *UDP*, который славится своей быстротой;
  - не нагружает канал, поскольку отправляет новый пакет только после подтверждения получения предыдущего.
3. Были проанализированы три протокола промышленных сетей:
    - *Modbus*;
    - *Profibus*;
    - *Foundation FieldBus*.

По результатам анализа всех трёх протоколов был выбран *Modbus*, поскольку он:

- прост в освоении;



- проверен временем и поддерживается большим числом производителей;
- является полностью открытым стандартом (в отличие от *Profibus*);
- является наиболее распространённым (в странах СНГ протокол *Foundation Fieldbus*, несмотря на свои преимущества, не используется).

4. Сделаны выводы о преимуществах автоматизации:

- уменьшение количества ошибок оператора;
- упрощение контроля за процессом;
- повышение надёжности процесса.

5. Была начата разработка собственной системы управления и контроля SCADA.

## ЗАКЛЮЧЕНИЕ

Технологии плотно вошли во все сферы нашей жизни. Не обходится без них и промышленность: благодаря наработкам *IT*-индустрии мы имеем огромное количество протоколов обмена данными между устройствами и большое число промышленных протоколов, среди которых можно выделить три самых популярных:

1. *Modbus*;
2. *Profibus*;
3. *Foundation FieldBus*.

Промышленные протоколы используются при построении SCADA-систем для контроля за процессом производства. Эти системы помогают избежать таких недостатков ручного управления, как:

- простой оборудования в связи с отсутствием оператора;
- уменьшение производительности в связи с необходимостью ручного управления;
- ухудшение качества продукции в связи с неточным следованиям инструкциям.

По результатам работы, проделанной в дисциплине «Научно-исследовательская работа», была начата разработка собственной SCADA-системы при помощи библиотек Qt.

# Список литературы

## Научные статьи

1. *Hussein Wheeb A.* Performance Comparison of Transport Layer Protocols // International Journal of Advanced Research in Computer Science and Software Engineering. — 2015. — 12 янв. — Т. 5, № 12. — С. 5. — ISSN 22776451, 2277128X. — URL: [https://www.academia.edu/download/61590964/Performance\\_Comparison\\_of\\_Transport\\_Layer\\_Protocols-\\_vol5-issue12-2015\\_20191223-12686-v59wb2.pdf](https://www.academia.edu/download/61590964/Performance_Comparison_of_Transport_Layer_Protocols-_vol5-issue12-2015_20191223-12686-v59wb2.pdf) (дата обр. 10.04.2021).
2. *Kumar S., Rai S.* Survey on Transport Layer Protocols: TCP & UDP // International Journal of Computer Applications. — 2012. — 1 мая. — Т. 46, № 7. — С. 6. — URL: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.734.7346&rep=rep1&type=pdf> (дата обр. 10.04.2021).
4. *Москаленко Т. А., Киричек Р. В., Кучерявый А. Е.* Обзор протоколов Интернета вещей // Информационные технологии и телекоммуникации. — 2017. — Т. 5, № 2. — С. 12. — URL: <http://www.sut.ru/doci/nauka/review/20172/1-12.pdf> (дата обр. 10.04.2021).
5. *Борисов Г. Б.* ОБЗОР ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ ПРИБОРОВ УЧЕТА ДЛЯ РОССИЙСКОГО РЫНКА // ООО «Научно-технический центр МЗТА». — 2016. — 11 янв. — С. 4. — URL: <https://www.mzta.ru/images/1085/3-6.pdf> (дата обр. 11.04.2021).
6. *Сергей Г.* Краткий экскурс в историю промышленных сетей // Компоненты и Технологии. — 2001. — № 12. — С. 110—114. — ISSN 2079-6811. — URL: <https://cyberleninka.ru/article/n/kratkiy-ekskurs-v-istoriyu-promyshlennyh-setey> (дата обр. 11.04.2021).

7. *Кругляк К.* Промышленные сети: цели и средства // Современные технологии автоматизации. — 2002. — № 4. — С. 6—17. — URL: [https://www.cta.ru/pdf/2002-4/promnet1\\_2002\\_4.pdf](https://www.cta.ru/pdf/2002-4/promnet1_2002_4.pdf) (дата обр. 10.04.2021).
8. *Юшин О. Е., Кудрявцев Д. Н., Концов А. В.* ОБЗОР ТЕХНОЛОГИЙ В INDUSTRIAL ETHERNET // Инноватика-2018. — 2018. — С. 532—534. — URL: <https://elibrary.ru/item.asp?id=35627705> (дата обр. 11.04.2021).
9. *Powell J., Eng P.* Profibus and Modbus: a comparison // Automation. com. — 2013. — С. 1—5. — URL: [https://scadahacker.com/library/Documents/ICS\\_Protocols/Siemens%20-%20Profibus%20and%20Modbus%20Comparison.pdf](https://scadahacker.com/library/Documents/ICS_Protocols/Siemens%20-%20Profibus%20and%20Modbus%20Comparison.pdf) (дата обр. 11.04.2021).
10. *Gorp P. van.* Advanced remote controls for rectifiers: A comparison of features among Modbus, Profibus, and conventional control systems // Metal Finishing. — 2009. — 1 июня. — Т. 107, № 6. — С. 48—50. — ISSN 0026-0576. — DOI: 10 . 1016 / S0026 - 0576 (09 ) 80293 - 6. — URL: <https://www.sciencedirect.com/science/article/pii/S0026057609802936> (дата обр. 11.04.2021).
11. *Евдокимов Д. А., Ярыш Р. Ф.* Modbus - Протокол Передачи Данных //. — Наука и Просвещение, 2021. — С. 66—68. — URL: <https://www.elibrary.ru/item.asp?id=44684618> (дата обр. 12.04.2021).
15. *Денисенко В.* Протоколы и сети Modbus и Modbus TCP // Современные технологии автоматизации. — 2010. — Т. 4. — С. 90—94. — URL: <https://www.reallab.ru/images/editor/downloads/articles/Modbus.pdf> (дата обр. 12.04.2021).
16. *Daneels A., Salter W.* What is SCADA? // (International Conference on Accelerator and Large Experimental Physics Control Systems). — Trieste, Italy : CERN, 1999. — С. 339—343. — URL: <https://cds.cern.ch/record/532624/files/mc1i01.pdf> (дата обр. 10.04.2021).

17. *Гордиенко Е. П., Гордиенко С. Н.* Системы SCADA и анализ их применения // — филиал ФГБОУ ВО РГУПС г. Воронеж, 2019. — С. 10—14. — URL: <https://elibrary.ru/item.asp?id=38316519> (дата обр. 12.04.2021).
18. Общие принципы построения SCADA-систем / А. Г. Сальный, В. Н. Кухаренко, А. Б. Николаев, А. В. Остроух // Автоматизация и управление в технических системах. — 2013. — № 2. — С. 8. — URL: [http://auts.esrae.ru/pdf/2013/2\(4\)/117.pdf](http://auts.esrae.ru/pdf/2013/2(4)/117.pdf) (дата обр. 10.04.2021) ; Publisher: Общество с ограниченной ответственностью Научно-инновационный центр.
19. *Локотков А.* Что должна уметь система SCADA // Современные технологии автоматизации. — 1998. — № 3. — С. 44—46. — URL: [https://www.cta.ru/pdf/1998-3/tools1\\_1998\\_3.pdf](https://www.cta.ru/pdf/1998-3/tools1_1998_3.pdf) (дата обр. 12.04.2021).
20. *Гайнуллина А., Байтимиров Д.* Особенности организации передачи данных между программируемыми логическими контроллерами по протоколу Modbus // Вестник Казанского технологического университета. — 2013. — Т. 16, № 23. — С. 230—234. — ISSN 1998-7072. — URL: <https://cyberleninka.ru/article/n/osobennosti-organizatsii-peredachi-dannyh-mezhdu-programmiruemymi-logicheskimi-kontrollerami-po-protokolu-modbus> (дата обр. 10.04.2021).
21. *Голованов Д. А., Прохоров Е. П., Мусеев К. М.* Разработка системы автоматического управления вакуумной и газовой систем установки MBТУ-11-1МС // Будущее машиностроения России. — 2017. — С. 188—192. — URL: <https://elibrary.ru/item.asp?id=41786874> (дата обр. 10.04.2021).
22. *Galloway B., Hancke G. P.* Introduction to industrial control networks // IEEE Communications surveys & tutorials. — 2012. — Т. 15, № 2. — С. 860—880. — URL: <http://www.rfidblog.org.uk/Preprint-GallowayHancke-IndustrialControlSurvey.pdf> (дата обр. 01.05.2012) ; ISBN: 1553-877X Publisher: IEEE.

24. Design of Industrial Data Monitoring Device Using IOT through MODBUS Protocol / S. A, M. Gunasekar, K. N, T. K.S, S. S. // International Journal of Scientific & Technology Research. — 2020. — 1 янв. — Т. 09. — С. 77—86. — ISSN 2277-8616. — URL: [https://www.researchgate.net/publication/344378128\\_Design\\_of\\_Industrial\\_Data\\_Monitoring\\_Device\\_Using\\_IOT\\_through\\_MODBUS\\_Protocol](https://www.researchgate.net/publication/344378128_Design_of_Industrial_Data_Monitoring_Device_Using_IOT_through_MODBUS_Protocol) (дата обр. 10.04.2021).
26. *Thomesse J.-P.* Fieldbus technology in industrial automation // Proceedings of the IEEE. — 2005. — Т. 93, № 6. — С. 1073—1101. — DOI: [10.1109/JPROC.2005.849724](https://doi.org/10.1109/JPROC.2005.849724). — URL: <https://tinyurl.com/rjr2c346> (дата обр. 01.05.2012) ; ISBN: 0018-9219 Publisher: IEEE.
30. *Vincent S. J.* FOUNDATION fieldbus high speed ethernet control system // Fieldbus Inc. — 2001. — С. 9. — URL: <http://fieldbusinc.net/downloads/hsepaper.pdf> (дата обр. 11.04.2021).
32. *Гунта А., Капо Р.* FOUNDATION FIELDBUS или PROFIBUS PA // Современные технологии автоматизации. — 1999. — С. 16—20. — URL: <https://www.cta.ru/cms/f/366625.pdf> (дата обр. 10.04.2021).

## Онлайн-издания

12. *Advantech.* Как общаются машины: протокол Modbus. — 06.05.2019. — URL: <https://habr.com/ru/company/advantech/blog/450234/> (дата обр. 12.04.2021).
13. *Contact P.* Системы автоматизации на основе Foundation Fieldbus. — 20.02.2020. URL: [https://habr.com/ru/company/phoenix\\_contact/blog/489256/](https://habr.com/ru/company/phoenix_contact/blog/489256/) (дата обр. 12.04.2021).
14. *Promwad.* Шины и протоколы в промышленной автоматике: как всё это работает. — 30.05.2019. — URL: <https://habr.com/ru/post/454156/> (дата обр. 12.04.2021).

27. *Promwad*. Обзор современных протоколов в системах промавтоматики. — 31.10.2019. — URL: <https://habr.com/ru/post/473992/> (дата обр. 16.04.2021).

## Разделы книг

3. *Noergaard T.* Chapter 4 - The Fundamentals in Understanding Networking Middleware // *Demystifying Embedded Systems Middleware* / под ред. Т. Noergaard. — Burlington : Newnes, 01.01.2010. — С. 93—190. — ISBN 978-0-7506-8455-2. — DOI: [10.1016/B978-0-7506-8455-2.00004-2](https://doi.org/10.1016/B978-0-7506-8455-2.00004-2). — URL: <https://www.sciencedirect.com/science/article/pii/B9780750684552000042> (дата обр. 10.04.2021).

## Книги

23. *Тимаев А. А.* Промышленные сети: учебное пособие. — Издательство Уральского университета, 2020. — 128 с. — ISBN 978-5-7996-2985-4. — URL: [https://elar.urfu.ru/bitstream/10995/80673/1/978-5-7996-2963-2\\_2020.pdf](https://elar.urfu.ru/bitstream/10995/80673/1/978-5-7996-2963-2_2020.pdf) (дата обр. 10.04.2021).
28. *Денисенко В.* Энциклопедия АСУ ТП. — reallab.ru, 2015. — URL: <https://bookasutp.ru/> (дата обр. 10.04.2021).
33. Индивидуальный лабораторный практикум. Часть 1 / А. Беликов [и др.] ; под ред. Ю. Панфилова. — Издательство МГТУ им. Н.Э. Баумана, 2018. — 80 с. — (Дата обр. 10.04.2021).

## Документация

25. *Swales A.* Open modbus/tcp specification. — 1999. — URL: [http://www.dankohn.info/projects/Fieldpoint\\_module/Open\\_ModbusTCP\\_Standard.pdf](http://www.dankohn.info/projects/Fieldpoint_module/Open_ModbusTCP_Standard.pdf) (дата обр. 10.04.2021).

29. *ACROMAG*. INTRODUCTION TO PROFIBUS DP. — 2002. — URL: <http://www.diit.unict.it/users/scava/dispense/II/Profibus.pdf> (дата обр. 16.05.2021).
31. The Foundation fieldbus PRIMER. — 14.06.2001. — URL: [https://www.fieldbusinc.com/downloads/primer1\\_1.pdf](https://www.fieldbusinc.com/downloads/primer1_1.pdf) (дата обр. 17.04.2021).