Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к курсовому проекту

на тему

ЛОКАЛЬНАЯ СЕТЬ КВАРТИРЫ

БГУИР КП 1-35 05 01 006 ПЗ

Студент А. А. Пашковский

Руководитель И. И. Глецевич

МИНСК 2016

Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет: ФКСиС. Кафедра: ЭВМ.

Специальность: 40 02 01 «Вычислительные машины, системы и сети»

Специализация: нет

ЗАДАНИЕ

по курсовому проекту студента

Пашковского Антона Анатольевича

**1** Тема проекта: «Локальная сеть квартиры»

**2** Срок сдачи студентом законченного проекта: 15 декабря 2016 г.

**3** Исходные данные к проекту:

**3.1** Используемое оборудование: нет ограничений

**3.2** Количество пользовательских станций: больше 1

**4** Содержание пояснительной записки (перечень подлежащих разработке вопросов):

Введение. 1. Обзор литературы. 2. Структурное проектирование ЛКС.

3. Функциональное проектирование ЛКС. 4. Проектирование структурной кабельной схемы. Заключение. Литература. Приложения.

[ВВЕДЕНИЕ 4](#_Toc469159076)

[**1** ОБЗОР ЛИТЕРАТУРЫ 5](#_Toc469159077)

[**1.1** Классификация локальных компьютерных сетей 5](#_Toc469159078)

[**1.2** Беспроводные локальные компьютерные сети (WLAN) 9](#_Toc469159079)

[**1.3** Безопасность и защита данных в WLAN 10](#_Toc469159080)

[**1.4** Сервисы, используемые в локальных компьютерных сетях 11](#_Toc469159081)

[Заключение 12](#_Toc469159082)

[**2** СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ 13](#_Toc469159083)

[**3** ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ 14](#_Toc469159084)

[**4** ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СХЕМЫ 15](#_Toc469159085)

[ЗАКЛЮЧЕНИЕ 16](#_Toc469159086)

[СПИСОК ЛИТЕРАТУРЫ 17](#_Toc469159087)

# ВВЕДЕНИЕ

На сегодняшний день использование компьютера даёт человеку почти безграничные возможности по обработке информации, возможности, которые казались недостижимыми полвека назад. И параллельно с возрастающими аппаратными возможностями компьютера, развивались и способы их использования, создавалась инфраструктура, которая позволяла людям обрабатывать и распространять информацию в рамках группы компьютеров, разделять дорогостоящие ресурсы (такие как принтеры, дисковая память и т.д.), работать над какими-то проектами совместно, делиться идеями и т.д. И одним из первых примеров таких инфраструктур стали локальные компьютерные сети.

Сейчас локальные компьютерные сети есть повсеместно: корпоративная сеть в офисе любой компании, сети в университетах, сети общежитий и т.д. В операционных системах компьютера по умолчанию встроены все необходимые аппаратные и программные инструменты для того что бы можно было настроить подключение к какой-нибудь локальной сети. Для того что бы настроить себе домашнюю компьютерную сеть нужно лишь понимание того, какую задачу эта сеть будет решать, знания и немного свободного времени.

В рамках данного курсового проекта была поставлена задача создать локальную компьютерную сеть, которая бы работала в рамках квартиры и решала бы какие-либо заранее определённые задачи.

# **1** ОБЗОР ЛИТЕРАТУРЫ

В этом разделе подробно разобрано что такое локальные компьютерные сети и как их можно классифицировать, беспроводные локальные компьютерные сети и способы их защиты. Также будут рассмотрены основные сервисы, которые настраиваются в локальных компьютерных сетях.

## **1.1** Классификация локальных компьютерных сетей

Локальная компьютерная сеть (LAN) – компьютерная сеть покрывающая относительно небольшую территорию или группу зданий. Также существуют локальные компьютерные сети, узлы которых разнесены на большое расстояние (космические станции и орбитальные центры). Несмотря на такие расстояния, такие сети всё равно относят к локальным. [1]

Локальные компьютерные сети можно классифицировать по разным параметрам в зависимости от способа их создания и применения. В основном локальные сети можно классифицировать по следующим параметрам:

1. По классу локальные сети делятся на одноранговые (Peer-to-peer) и клиент-серверные (иерархические) сети;
2. По топологии сети делятся на кольцевые, шинные, звездообразные, гибридные;
3. По типу физической среды передачи – на витую пару, коаксиальный или оптоволоконный кабель, инфракрасный канал, радиоканал.
4. По скорости доступа – на низкоскоростные (до 10 Мбит/с), среднескоростные (до 100 Мбит/с), высокоскоростные (свыше 100 Мбит/с);

**Одноранговая сеть** – это сеть равноправных компьютеров, каждый из которых имеет уникальное имя (имя компьютера) и обычно пароль для входа в него во время загрузки ОС. Имя и пароль входа назначаются владельцем компьютера средствами ОС. Каждый компьютер такой сети может одновременно являться и сервером, и клиентом сети, хотя вполне допустимо назначение одного компьютера только сервером, а другого только клиентом.

Достоинством одноранговых сетей является их высокая гибкость: в зависимости от конкретной задачи сеть может использоваться очень активно, либо совсем не использоваться. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки (к тому же количество компьютеров обычно невелико). Установка одноранговых сетей довольно проста, к тому же не требуются дополнительные дорогостоящие серверы. Кроме того, нет необходимости в системном администрировании, пользователи могут сами управлять своими ресурсами.

К недостаткам одноранговых сетей относятся также слабая система контроля и протоколирования работы сети, трудности с резервным копированием распределенной информации. К тому же выход из строя любого компьютера-сервера приводит к потере части общей информации, то есть все такие компьютеры должны быть по возможности высоконадежными. Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, поскольку трудно обеспечить быстродействие процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети. К тому же компьютеры сети работают не только на сеть, но и решают другие задачи.

Сейчас считается, что одноранговая сеть наиболее эффективна в небольших сетях (около 10 компьютеров). При значительном количестве компьютеров сетевые операции сильно замедлят работу компьютеров и создадут множество других проблем. Тем не менее, для небольшого офиса одноранговая сеть – оптимальное решение.

**Клиент-серверные** локальные сети применяются в тех случаях, когда в сеть должно быть объединено много пользователей и возможностей одноранговой сети уже недостаточно. Тогда в сеть включается специализированный компьютер – сервер.

Сервером называется абонент сети, который предоставляет свои ресурсы другим абонентам, но сам не использует ресурсы других абонентов, то есть служит только сети. Выделенный сервер - это сервер, занимающийся только сетевыми задачами. Невыделенный сервер может заниматься помимо обслуживания сети и другими задачами. Существует ещё и специфический тип сервера – сетевой принтер.

Серверы специально оптимизированы для быстрой обработки сетевых запросов на разделяемые ресурсы и для управления защитой файлов и каталогов. При больших размерах сети мощности одного сервера может оказаться недостаточно, и тогда в сеть включают несколько серверов. Серверы могут выполнять и некоторые другие задачи: сетевая печать, выход в глобальную сеть, связь с другой локальной сетью, обслуживание электронной почты и т.д.

Количество пользователей сети на основе сервера может достигать нескольких тысяч. Одноранговой сетью такого размера просто невозможно было бы управлять. Кроме того, в сети на основе серверов можно легко менять количество подключаемых компьютеров, такие сети называются масштабируемыми.

Достоинством сети на основе сервера можно назвать надёжность. Но это верное только если сам сервер надёжен. В противном случае любой отказ сервера приводит к полному выходу из строя сети в отличие от ситуации с одноранговой сетью, где отказ одного из компьютеров не приводит к отказу всей сети. Так же к достоинствам сетей на основе сервера можно отнести централизованную настройку сети.

К недостаткам сети на основе сервера относятся ее громоздкость в случае небольшого количества компьютеров, зависимость всех компьютеров-клиентов от сервера и высокая стоимость сети вследствие использования дорогого сервера. [2]

Под топологией компьютерной сети обычно понимается расположение компьютеров сети друг относительно друга и способ соединения их линиями связи.

От выбранной топологии зависят требования к оборудованию, тип используемого кабеля, возможные и наиболее удобные методы управления обменом, надежность работы, возможности расширения сети.

Существует три основных топологии сети:

1. шина (bus), при которой все компьютеры параллельно подключаются к одной линии связи и информация от каждого компьютера одновременно передается всем остальным компьютерам. Шина более надёжна, так как отказ одного компьютера не влияет на способность остальных обмениваться информацией, однако эта топология упирается в физические ограничения, связанные с ослаблением сигнала;
2. звезда (star), при которой к одному центральному компьютеру присоединяются остальные периферийные компьютеры, причем каждый из них использует свою отдельную линию связи. Отказ конечных устройств никак не влияет на топологию звезда, однако выход из строя центрального узла полностью разрушает сеть;
3. кольцо (ring), при которой каждый компьютер передает информацию всегда только одному компьютеру, следующему в цепочке, а получает информацию только от предыдущего в цепочке компьютера, и эта цепочка замкнута в «кольцо». Кольцо может содержать большое количество компьютеров и очень устойчиво к большим потокам информации, так как в ней нет конфликтов (как у шины) и нет центрального узла (как у звезды), однако, поскольку информация передаётся через все компьютеры – выход хотя бы одного из них из строя выведет из строя всю сеть;

На практике часто используют комбинации разных топологий, в зависимости от того какая задача решается. [3]

Средой передачи информации называются те линии связи (или каналы связи), по которым производится обмен информацией между компьютерами. В подавляющем большинстве компьютерных сетей (особенно локальных) используются проводные или кабельные каналы связи, хотя существуют и беспроводные сети.

Выбор средства передачи данных зависит от размера сети, требуемой пропускной способности и скорости передачи данных, требуемых служб, работу которых необходимо организовать (передача мультимедиа, речи, простых данных и т.д.) и общей суммы, которую вы готовы потратить на вашу сеть.

Кабели на основе витых пар – самые дешёвые и самые популярные. Неэкранированный кабель слабо защищён от внешних электромагнитных помех и слабой защищённостью от прослушки. Для устранения этих недостатков применяется экранирование. Основные достоинства неэкранированных витых пар - простота монтажа разъемов на концах кабеля, а также простота ремонта любых повреждений по сравнению с другими типами кабеля. Все остальные характеристики у них хуже, чем у других кабелей.

Коаксиальный кабель представляет собой электрический кабель, состоящий из центрального провода и металлической оплетки, разделенных между собой слоем диэлектрика (внутренней изоляции) и помещенных в общую внешнюю оболочку. Коаксиальный кабель ранее был достаточно распространен, что связано с его высокой помехозащищенностью (благодаря металлической оплетке), а также более высокими, чем в случае витой пары, допустимыми скоростями передачи данных (до 500 Мбит/с) и большими допустимыми расстояниями передачи (до километра и выше). К нему труднее механически подключиться для несанкционированного прослушивания сети, он также дает заметно меньше электромагнитных. излучений вовне. Однако монтаж и ремонт коаксиального кабеля существенно сложнее, чем витой пары, а стоимость его выше. Сложнее и установка разъемов на концах кабеля. Поэтому его сейчас применяют реже, чем витую пару. [4]

Оптоволоконный (он же волоконно-оптический) кабель — это принципиально иной тип кабеля по сравнению с рассмотренными двумя типами электрического или медного кабеля. Информация по нему передается не электрическим сигналом, а световым. Главный его элемент - это прозрачное стекловолокно, по которому свет проходит на огромные расстояния (до десятков километров) с незначительным ослаблением. Оптоволоконный кабель обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации. Никакие внешние электромагнитные помехи в принципе не способны исказить световой сигнал, а сам этот сигнал принципиально не порождает внешних электромагнитных излучений. Однако оптоволоконный кабель имеет и некоторые недостатки. Главный из них - высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит затухание в разъеме). Для установки разъемов применяют сварку или склеивание с помощью специального геля, имеющего такой же коэффициент преломления света, что и стекловолокно. В любом случае для этого нужна высокая квалификация персонала и специальные инструменты. Поэтому чаще всего оптоволоконный кабель продается в виде заранее нарезанных кусков разной длины, на обоих концах которых уже установлены разъемы нужного типа. [5]

Наиболее подходящей локальной сетью для квартиры, учитывая небольшое число клиентов и неудобство протяжки кабелей по всей квартире, была выбрана одноранговая сеть с беспроводным подключением внутри и оптоволоконным подключением снаружи. Поэтому устройство, безопасность и настройку беспроводных локальных сетей будет рассмотрено подробнее.

## **1.2** Беспроводные локальные компьютерные сети (WLAN)

Стандарт на локальные беспроводные сети (сокращенно WLAN) разработан Институтом инженеров по электротехнике и электронике (IEEE, Institute of Electrical and Electronics Engineers) и официально именуется как 802.11. Однако для конечных пользователей было придумано более простое название – Wi-Fi, которое, кстати, расшифровывается как «wireless fidelity», то есть «беспроводная безукоризненность».

Стандарт IEEE 802.11 подразделяется на IEEE 802.11a, b, c, d, e, f, g, h, i, j, k, n. Из всей этой кучи широкого практического применения достигли IEEE 802.11b и IEEE 802.11g, (и совсем-совсем недавно Apple объявила о начале промышленного внедрения 802.11n) – именно такие сети и подразумеваются в первую очередь при упоминании слова Wi-Fi. Сети 802.11b и 802.11g работают в диапазоне 2.4ГГц и различаются скоростью передачи данных и радиусом действия. Для сетей 802.11b максимальная скорость составляет 11Мбит/сек, а радиус действия до 250 метров на открытом пространстве и до 20-30 метров в помещении. Сети 802.11g обеспечивают значительно большую скорость – до 54Мбит/сек, радиус действия у них до 300 метров на открытом пространстве. Все современные точки доступа (точка доступа – это устройство, посредством которого поддерживается связь между клиентами беспроводной сети, работают как с 802.11b, так и с 802.11g. Самые современные имеют поддержку стандарта 802.11n.

Радиус действия домашней Wi-Fi сети зависит от типа используемой беспроводной точки доступа или беспроводного маршрутизатора. К факторам, определяющим диапазон действия беспроводных точек доступа или беспроводных маршрутизаторов, относятся:

1. Тип используемого протокола 802.11;
2. Общая мощность передатчика;
3. Коэффициент усиления используемых антенн;
4. Длина и затухание в кабелях, которыми подключены антенны;
5. Природа препятствий и помех на пути сигнала в данной местности.
6. Препятствия в виде кирпичных стен и металлических конструкций могут уменьшить радиус действия Wi-Fi сети на 25% и более. Поскольку стандарт 802.11a использует частоты выше, чем стандарты 802.11b/g, он является наиболее чувствительным к различного рода препятствиям. На радиус действия Wi-Fi сетей, поддерживающих стандарт 802.11b или 802.11g, влияют также помехи, исходящие от микроволновых печей.

Стандарт 802.11n повышает скорость передачи данных практически вчетверо по сравнению с устройствами стандартов [802.11g](https://ru.wikipedia.org/wiki/802.11g) (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с брутто, применяя передачу данных сразу по четырём антеннам. По одной антенне — до 150 Мбит/с.

Устройства 802.11n работают в диапазонах 2,4—2,5 или 5,0 ГГц.

Кроме того, устройства 802.11n могут работать в трёх режимах:

1. наследуемом, в котором обеспечивается поддержка устройств 802.11b/g и [802.11a](https://ru.wikipedia.org/wiki/802.11a);
2. смешанном, в котором поддерживаются устройства 802.11b/g, [802.11a](https://ru.wikipedia.org/wiki/802.11a) и 802.11n;
3. «чистом» режиме — 802.11n (именно в этом режиме и можно воспользоваться преимуществами повышенной скорости и увеличенной дальностью передачи данных, обеспечиваемыми стандартом 802.11n). [6]

## **1.3** Безопасность и защита данных в WLAN

Удобность создания беспроводной локальной компьютерной сети состоит в том, что не нужно протягивать кабель к каждой пользовательской машине. Однако это же и порождает проблему безопасности беспроводных сетей – для того что бы подключится к вашей сети не нужно подключать кабель, достаточно просто сесть где-нибудь неподалёку с ноутбуком. Поэтому, если нет желания поделиться своей сетью со всеми соседями – необходимо настраивать ограниченный доступ к вашей сети.

Технологии защиты беспроводных локальных компьютерных сетей прошли за время своего существования своеобразную эволюцию. Далее по пунктам будет разобрано какие технологии защиты и в каком порядке появлялись и что использовалось для обеспечения этой самой защиты:

1. WEP (Wired Equivalent Privacy, или Защита Эквивалентная Проводной). Этот способ защиты применялся на ранних этапах развития беспроводных сетей. Данные шифруются с помощью специальных ключей, – ключ представляет собой пароль длиной 5 или 13 символов ASCII плюс вектор инициализации, сформированный случайным образом (из трех ASCII символов). Этот самый вектор инициализации несложно подобрать прямым перебором – пару часов работы относительно мощного компьютера, и ключ подобран. Сегодня считается, что использование технологии WEP равносильно ее отсутствию. Использовать не рекомендуется.
2. 802.1X - стандарт сетевой аутентификации IEEE, нашел широкую поддержку у производителей сетевого оборудования и ПО. Основные составляющие — протоколы EAP и RADIUS. Протокол 802.1X работает на канальном уровне и определяет механизм контроля доступа к сети на основе принадлежности к порту (в контексте стандарта порт — точка подключения к сети). Согласно этому протоколу доступ к сети получают только клиенты, прошедшие аутентификацию, если аутентификация не была пройдена, доступ с соответствующего порта будет запрещен. Используются динамические ключи шифрования, то есть те, которые периодически меняются во времени. Пользователи работают сеансами, по окончании сеансов им присылается новый ключ.
3. WPA (Wi-Fi Protected Access) – введен в работу с конца 2003 года. Является по сути суммой нескольких технологий. Из 802.1X позаимствована идея динамической смены ключа, плюс многочисленные улучшения включая проверку целостности сообщений. Очень хорошая технология, рекомендуется для домашних сетей и малого офиса.
4. WPA2 (он же 802.11i). Появился в 2004 году, максимально защищенный стандарт, изначально разработанный для беспроводных сетей (в отличие от VPN). Сочетает средства WPA1 и AES (Advanced Encryption Standard). Технологию можно разделить на WPA2 Personal и WPA2 Enterprise, которые отличаются охватом пользователей и наличием сервера аутентификации.
5. VPN (Virtual Private Network) – эта технология предложена компанией Intel и предназначена для безопасного соединения клиентских ПК с серверами по общедоступным интернет каналам. VPN очень хороша в плане шифрования и надежности аутентификации. Хотя эта технология и не разрабатывалась для применения в беспроводных сетях, она может с успехом применяться и здесь. Состоит из внутренней (может быть несколько) и внешней сети. По внешней сети проходит инкапсулированное соединение. С инкапсулированными пакетами можно делать всё что угодно (шифровать, сжимать и т.д.), главное, чтобы обратное действие проводилось на другой стороне подключения. Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP и UDP). [7]

## **1.4** Сервисы, используемые в локальных компьютерных сетях

HTTP - это протокол передачи гипертекста между распределёнными системами. Общение между хостом и клиентом происходит в два этапа: запрос и ответ. Клиент формирует HTTP запрос, в ответ на который сервер даёт ответ. Доступный ресурс на сервере идентифицируется с помощью специального адреса - URL (Universal Resource Locator). Зная нужный URL можно получить с сервера файл с гипертекстом, который храниться по этому адресу. Таким образом, с помощью HTTP на можно организовать хранение на сервере связанных данных в виде веб-сайта.

TFTP (простой [протокол](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB) передачи [файлов](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB)) - используется главным образом для первоначальной [загрузки](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%B3%D1%80%D1%83%D0%B7%D0%BA%D0%B0_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%B0) [бездисковых рабочих станций](https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%B4%D0%B8%D1%81%D0%BA%D0%BE%D0%B2%D0%B0%D1%8F_%D1%80%D0%B0%D0%B1%D0%BE%D1%87%D0%B0%D1%8F_%D1%81%D1%82%D0%B0%D0%BD%D1%86%D0%B8%D1%8F).

FTP (протокол передачи файлов) — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к FTP серверам, просматривать содержимое каталогов и загружать файлы с сервера или на сервер.

DNS (система доменных имён) — компьютерная [распределённая система](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%91%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B0%D0%B7%D0%B0_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) для получения информации о [доменах](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B5_%D0%B8%D0%BC%D1%8F). Чаще всего используется для получения IP-адреса по имени [хоста](https://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82). [Распределённая база данных](https://ru.wikipedia.org/wiki/%D0%A0%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D1%91%D0%BD%D0%BD%D1%8B%D0%B5_%D0%B1%D0%B0%D0%B7%D1%8B_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) DNS поддерживается с помощью иерархии [DNS-серверов](https://ru.wikipedia.org/wiki/DNS-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80), взаимодействующих по определённому [протоколу](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D1%8B_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85). Основой протокола является иерархическая структура, которая позволяет знать одному DNS – серверу только о какой-то части доменного имени, а остальную часть делегировать DNS серверу верхнего уровня.

AAA ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Authentication, Authorization, Accounting) — используется для описания процесса предоставления доступа и контроля над ним.

SYSLOG ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) system log — [системный журнал](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB_%D1%80%D0%B5%D0%B3%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%86%D0%B8%D0%B8)) — стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания [логов](https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB_%D1%80%D0%B5%D0%B3%D0%B8%D1%81%D1%82%D1%80%D0%B0%D1%86%D0%B8%D0%B8)), использующийся в [компьютерных сетях](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), работающих по протоколу [IP](https://ru.wikipedia.org/wiki/IP).

NTP (протокол сетевого времени) – используется в сетях для синхронизации времени. Даёт точность до 10мс при синхронизации через сеть интернет и 0.2мс и выше, если сервер точного времени находится в локальной компьютерной сети. В OS Windows представлен службой (W32Time), в Linux (Ntpd). [8]

## Заключение

В этом разделе были описаны виды локальных сетей, способы их защиты и основные сервисы которые настраиваются в локальных сетях. Было решено сделать беспроводную локальную компьютерную сеть с WPA2 аутентификацией с FTP сервером для совместного хранения файлов.

# **2** СТРУКТУРНОЕ ПРОЕКТИРОВАНИЕ

# **3** ФУНКЦИОНАЛЬНОЕ ПРОЕКТИРОВАНИЕ

# **4** ПРОЕКТИРОВАНИЕ СТРУКТУРНОЙ КАБЕЛЬНОЙ СХЕМЫ

# ЗАКЛЮЧЕНИЕ

# СПИСОК ЛИТЕРАТУРЫ

1. Сайт – справочник [Электронный ресурс] – Определения основных терминов, связанных с локальными компьютерными сетями. – 2012. – Режим доступа: <https://en.wikipedia.org/wiki/Local_area_network>

2. Сайт с лекциями о локальных компьютерных сетях. [Электронный ресурс] – Классификация локальных компьютерных сетей. – 2014. – Режим доступа: <https://sites.google.com/site/websitecomputernetworks/home/lection/2>

3. Сайт дистанционного обучения. [Электронный ресурс] – Топологии локальных компьютерных сетей. – 2012. – Режим доступа: <http://www.lessons-tva.info/edu/telecom-loc/m1t4_3loc.html>

4. Сайт центра промышленной автоматизации. [Электронный ресурс] – Типы кабелей и проводов. – 2014. – Режим доступа: <http://ruaut.ru/content/publikacii/electro/tipy-kabeley-i-provodov-silovoy-koaksialnyy-optovolokonnyy-kabel-i-vitaya-para.html>

5. Информационный портал. [Электронный ресурс] – Статья об оптоволоконных кабелях. – 2016. – Режим доступа: [https://habrahabr.ru/company/ua-hosting/blog/267859/](https://habrahabr.ru/company/ua-hosting/blog/267859/%20)

6. Сайт о беспроводных компьютерных сетях. [Электронный ресурс] – Беспроводные компьютерные сети, стандартные протоколы передачи данных и защиты соединения. – 2015. – Режим доступа: [http://wi-fi.na.by/](http://wi-fi.na.by/%20)

7. Сайт сервиса предоставляющего услуги по настройке Wi-fi. [Электронный ресурс] – Безопасность в сетях Wi-fi. – 2015. – Режим доступа: [http://www.getwifi.ru/psecurity.html](http://www.getwifi.ru/psecurity.html%20)

8. Cайт о компьютерных сетях. [Электронный ресурс] – Основные сетевые сервисы. – 2013. – Режим доступа: <http://embedded.ifmo.ru/embedded_old/ETC/REFERAT/crc/crc.htm>