ТЕХНИЧЕСКОЕ ЗАДАНИЕ

1. Исполнять агентское поручение в соответствии с условиями заключаемого Договора.

2. Организовать диспетчеризацию работ по подключению, закрытие нарядов и заполнение карточек абонентского оборудования в информационных системах Принципала в соответствии с условиями заключаемого Договора.

3. Предварительные планы по установкам (порты):

Место выполнения работ	2 квартал 2014г.	3 квартал 2014г.	4 квартал 2014г.	Итого:
Красноярский край	2 776	2 706	3 679	9 161
Республика Хакасия	976	951	1 293	3 220
Итого	3 752	3 657	4 972	12 381

4. Начальная (максимальная) стоимость:

№ п/п	Наименование Работ (агентское поручение, предусмотренное п. 1.2.1. Договора)	Максимально допустимая в предложении цена за ед.[1], в руб.	
		без НДС	с НДС
1	Организация линии связи по технологии GPON для предоставления доступа к услугам связи	1 400,00	1 652,00
3	Организация предоставления доступа, дополнительно к организации линии связи, (пункты 1 таблицы) (SIP[2], IP-TV[3], настройка роутера).	150,00	177,00
4	Организация предоставления доступа на уже действующую линию (SIP[2], IP-TV[3], настройка роутера).	500,00	590,00
	Итоговая сумма предельных цен за Работы	**2 050,00**	**2 419,00**

Общая начальная (максимальная) цена инсталляции услуг связи и подключения абонентского оборудования с НДС составляет 9 998 600 (Девять миллионов девятьсот девяноста восемь тысяч шестьсот) рублей 00 копеек.

• НДС 18% - 1 525 210 (Один миллион пятьсот двадцать пять тысяч двести десять) рублей 17 копеек,

• Общая начальная (максимальная) цена без НДС составляет 8 473 389 (Восемь миллионов четыреста семьдесят три тысячи триста восемьдесят девять) рублей 83 копейки.

5. Стоимость договора включает в себя:

-стоимость работ и материалов с учетом расходов на перевозку, страхование, уплаты таможенных пошлин, налогов и других обязательных платежей;

---

[1] Все суммы, указанные в Таблице 1, включают в себя вознаграждение за выполнение агентского поручения, предусмотренного п.п. 1.2.2. - 1.2.4. Договора на соответствующей Площадке.

[2] Услуга традиционной телефонии с использованием аналогового телефонного аппарата подключаемого к интегрированному устройству доступа (порт - FXS IAD, ONT).

[3] Доступ к услуге интерактивного телевидения. Установка (при необходимости) и настройка Ethernet-маршрутизатора / ONU, установка и настройка STB, подключение STB к телевизионному приемнику абонента.

- расходы, связанные с командированием специалистов претендента;
- расходы по проезду специалистов претендента, перевозке необходимого для проведения работ инвентаря, приборов и инструментов претендента к месту проведения вышеуказанных работ и обратно;

- расходы по согласованию и получению всех разрешительных документов для выполнения Работ в объеме, необходимом для полного сооружения и нормальной эксплуатации Объектов, в предусмотренном действующими нормативно-правовыми актами порядке.

6. Место выполнения Работ: Красноярский край, республика Хакасия

7. Сроки выполнения Работ: с даты заключения договора по 31.12.2014 года, в соответствии с п.1.1 Приложения №1 к Договору.

8. Гарантийный срок на выполненные Работы составляет 3 (Три) месяца от даты подписания Актов о приемке выполненных работ Агентом и Абонентом.

Порядок взаимодействия по обеспечению безопасности информационных ресурсов Принципала

1 Общие положения

1.1 Общее руководство и принятие всех решений по вопросам обеспечения режима коммерческой тайны, конфиденциальности и информационной безопасности Агента осуществляет руководитель Агента.

1.2 Организацию мероприятий по обеспечению режима коммерческой тайны, конфиденциальности и информационной безопасности Агента осуществляет подразделение безопасности Агента.

1.3 Агент должен разработать и соблюдать требования локальных нормативных документов по вопросам коммерческой тайны, конфиденциальности и информационной безопасности.

1.4 Для выполнения технологических операций по обеспечению режима коммерческой тайны, конфиденциальности и информационной безопасности Агента, из числа штатных работников Агента назначаются ответственные за информационную безопасность, также допускается выполнение технологических операций по обеспечению безопасности на договорной основе сторонними организациями, согласованными с Принципалом.

1.5 Принципал оставляет за собой право по контролю обеспечения режима коммерческой тайны, конфиденциальности и информационной безопасности, а также участвовать в проведении совместных проверок и расследований по признакам и фактам нарушения Агентом требований безопасности.

2 Безопасность рабочих мест

2.1 Для обеспечения своей деятельности Агент обязан использовать только лицензионное и официально приобретенное программное обеспечение. Применение бесплатного или условно бесплатного программного обеспечения должно согласовываться со Службой безопасности Принципала.

2.2 Для доступа к информационным ресурсам Принципала Агент может использовать программное обеспечение предоставленное (либо сертифицированное) только Принципалом. Использование иного программного обеспечения должно согласовываться с Принципалом. Агент не вправе вносить любые изменения в предоставляемое Принципалом программное обеспечение.

2.3 Настройки политик безопасности операционной системы рабочих мест, с которых осуществляется доступ к информационным ресурсам Принципала, должны соответствовать политикам, принятым в корпоративной информационно-вычислительной сети Принципала.

2.4 На рабочих местах Агента, с которых осуществляется доступ к информационным ресурсам Принципала, использование программного обеспечения, не предназначенного для организации данного доступа, требует обязательного согласования с Принципалом.

2.5 Права пользователя на рабочем месте должны быть ограничены и не должны позволять осуществлять действия по изменению программно-аппаратного обеспечения.

2.6 Права на изменения программно-аппаратного обеспечения, а также заведение новых пользователей и назначение им полномочий в системе, должны иметь специально назначенные работники Агента.

2.7 Применяемое Агентом системное программное обеспечение должно своевременно обновляться с использованием автоматизированных средств обновлений.

2.8 Запрещается хранение конфиденциальной информации Принципала на неучтенных носителях информации, а также на жестких дисках рабочих станций Агента, с которых осуществляется доступ к информационным ресурсам сторонних организаций и в сеть общего пользования Интернет.

2.9 Сегменты сетей Агента и Принципала должны быть разделены средствами межсетевого экранирования с проведением строгой политики управления доступом, в соответствии с политикой принятой в корпоративной информационно-вычислительной сети Принципала, в целях исключения доступа к неразрешенным объектам, а также использования неразрешенных протоколов, сервисов и служб.

3 **Доступ к информационным ресурсам**

3.1 Аутентификация пользователя Агента при доступе к информационным ресурсам Принципала должна осуществляться с использованием механизмов усиленной двухфакторной аутентификации (с применением цифровых сертификатов). В отдельных случаях (система не поддерживает двухфакторную аутентификацию) возможно применение уникального персонального идентификатора и пароля. Парольная политика должна соответствовать требованиям, принятым в корпоративной информационно-вычислительной сети Принципала.

3.2 Доступ к информационным ресурсам Принципала должен осуществляться только по доверенным каналам связи, принадлежащим Принципалу, в противном случае должны применяться механизмы шифрования на сетевом уровне. При применении шифрования должны использоваться алгоритмы шифрования, принятые Принципалом, ключи шифрования, выданные Службой безопасности Принципала.

3.3 Подключение к Системе Абонентского Учёта Принципала должно осуществляться через защищенное подключение к КСПД через терминальный сервер с формированием гостевой учетной записи AD. Удаленное защищенное подключение выполняется в соответствии с требованиями Принципала.

3.4 Доступ к информационным ресурсам Принципала предоставляется только штатным работникам Агента на основании заявки оформленной Агентом, подписанной руководителем Агента, согласованной Службой безопасности Агента, начальником отдела организации эксплуатации сетей доступа Принципала владельцем ресурса, ИТ-подразделением Принципала и Службой безопасности Принципала.

3.5 Заявка на доступ к информационным ресурсам должна содержать: наименование информационного ресурса, необходимые права на доступ, ФИО пользователя, подразделение, должность, местонахождение рабочего места, контактный телефон, сетевой идентификатор пользователя (ей), DNS-имя компьютера (список) с которого будет осуществляться доступ.

3.6 Доступ работникам Агента к информационным ресурсам Принципала предоставляется исключительно для выполнения обязательств, предусмотренных Договором.

3.7 Доступ предоставляется минимально необходимый для выполнения работником своих должностных обязанностей. Ответственность за обоснованность запрашиваемого доступа возлагается на руководителя Агента, запросившего доступ.

3.8 Централизованный учет пользователей информационных ресурсов Принципала и его своевременная актуализация возлагается на подразделение Агента. Учет сотрудников Агента, допущенных к конфиденциальной информации, а также проведение служебных расследований по фактам нарушений требований информационной безопасности возлагается на Службу безопасности Агента, с привлечением Службы безопасности Принципала.

3.9 Уволенные работники Агента должны быть лишены допуска ко всем ресурсам (без исключения). Ответственность за своевременное лишение допуска возложена на руководителя Агента оформившего допуск. В целях своевременного лишения допуска к информационным ресурсам Принципала, руководитель подразделения Агента, оформивший допуск информирует ИТ-подразделение Принципала не позднее 3 дней после подачи заявления об увольнении с указанием фактической даты прекращения допуска. Подразделение по работе с персоналом Агента не реже 1 раза в месяц информирует Службу безопасности Принципала об уволенных работниках и работниках переведенных на другие должности.

3.10 Агент должен обеспечивать журналирование (логирование) доступа своих работников к информационным ресурсам Принципала и по требованию предоставлять эту информацию Службе безопасности Принципала.

3.11 Принципал оставляет за собой право контролировать действия работников Агента при осуществлении доступа к информационным ресурсам Принципала и приостанавливать доступ в случаях возникновения ситуаций, создающих угрозу информационной безопасности Принципала, уведомив об этом Агента. Доступ восстанавливается после устранения выявленной угрозы на основании заявки согласованной со Службой безопасности Принципала.

4 Реагирование на инциденты информационной безопасности

4.1 Агент должен информировать Службу безопасности Принципала обо всех случаях возникновения инцидентов информационной безопасности.

4.2 Агент должен безотлагательно предпринимать все необходимые меры по предотвращению и минимизации ущерба при возникновении инцидента информационной безопасности.

4.3 В случаях возникновения угроз информационной безопасности Принципала со стороны сети, рабочих мест или пользователей Агента, а также претензий со стороны государственных контролирующих органов или фактов нарушений, приведших к материальному ущербу, расследование осуществляет Служба безопасности Принципала совместно со Службой безопасности Агента.

5 Применение средств защиты информации

5.1 Установка средств защиты информации Агентом должна в обязательном порядке согласовываться со Службой безопасности Принципала.
5.2 Установка и ввод в эксплуатацию средств защиты информации должна осуществляться в соответствии с эксплуатационной и технической документацией.
5.3 Агент должен проводить обучение лиц, использующих средства защиты информации, правилам работы с ними.
5.4 Учет применяемых средств защиты информации, эксплуатационной и технической документации и носителей конфиденциальной информации возлагается на ответственного работника Агента.
5.5 Контроль за соблюдением условий использования средств защиты информации возлагается на Службу безопасности Агента.
5.6 Средства защиты информации, применяемые Агентом, должны быть подключены к централизованной Системе мониторинга информационной безопасности Принципала.

6 Доступ в сеть Интернет

6.1 Доступ в сеть общего пользования Интернет с рабочих мест, с которых осуществляется доступ к информационным ресурсам Принципала, должен осуществляться в соответствии с требованиями нормативных документов Принципала по использованию сети Интернет.
6.2 Доступ в сеть Интернет должен осуществляться только авторизованными пользователями через средства межсетевого экранирования, журналироваться автоматизированными средствами (Proxy-сервер), контролироваться антивирусным программным обеспечением и автоматизированными средствами обнаружения вторжений и аномалий (IDS). Политики безопасности указанных средств должны соответствовать требованиям Принципала. Изменение политик безопасности должно согласовываться со Службой безопасности Принципала.
6.3 Контент-контроль доступа в сеть Интернет работниками Агента осуществляет Служба безопасности Агента.
6.4 Взаимодействие работников Агента с внешними контрагентами должно осуществляться только с использованием корпоративной электронной почты или специально организованных информационных систем.
6.5 Передача конфиденциальной информации через сеть Интернет запрещена.
6.6 Запрещается использование Интернета для своих личных целей: посещение развлекательных, игровых, музыкальных, порнографических, террористических сайтов.
6.7 Не допускается неуполномоченное представление личной точки зрения точкой зрения Принципала или Агента в сети Интернет.
6.8 Личные бюджеты пользователей онлайновых сервисов Интернет не должны использоваться с рабочих мест Агента.

7 Антивирусная безопасность

7.1 В целях непрерывного и комплексного обеспечения Агента системой антивирусной безопасности, все рабочие места и сервера Агента должны быть оснащены лицензионным антивирусным программным обеспечением. За поддержание работоспособности антивирусного программного обеспечения и актуальности антивирусных баз назначается штатный работник Агента или должен быть заключен договор на поддержку системы антивирусной безопасности.

7.2 Система антивирусной безопасности Агента должна стоять из трех уровней, каждый из которых должен иметь антивирусное программное обеспечение различных производителей:
- системы, которые непосредственно соединяются с сетью общего пользования;
- сервера: файловые, внутренние почтовые и серверах приложений;
- рабочие станции и сервера рабочих групп, удаленные или мобильные пользователи.

7.3 Система антивирусной безопасности должна иметь систему централизованного обновления и управления.

7.4 В случае если рабочее место, с которого осуществляется доступ к информационным ресурсам Принципала, невозможно оснастить антивирусным программным обеспечением, по согласованию со Службой безопасности Принципала, на рабочем месте должна быть создана замкнутая программная среда, не позволяющая осуществлять запуск любых приложений, кроме штатных.

8 **Контроль состояния информационной безопасности**

8.1 В целях проверки выполнения требований по информационной безопасности, а также предупреждения и своевременного выявления нарушений информационной безопасности, в подразделениях Агента должен осуществляться контроль состояния информационной безопасности Агента.

8.2 Контроль состояния информационной безопасности в подразделениях Агента осуществляют Службы безопасности Агента и Принципала в соответствии с согласованными планами работ.

8.3 Плановым проверкам должны подвергаться все подразделения Агента не реже 1 раза в 3 года.

8.4 Внезапные проверки проводятся Службой безопасности Агента или Принципала в соответствии с внутренними утвержденными планами работ.

8.5 По фактам инцидентов информационной безопасности в обязательном порядке проводится внеплановая проверка состояния информационной безопасности Службой безопасности Агента совместно со Службой безопасности Принципала с целью выявления причин, устранения нарушений и предупреждения подобных нарушений в дальнейшем.

8.6 Внеплановые проверки состояния информационной безопасности проводятся в обязательном порядке при реорганизации подразделений Агента, изменения в технологии работы, состава программно-аппаратного обеспечения.

9 **Обучение персонала**

9.1 Агент должен всех вновь принимаемых работников знакомить под роспись с нормативными документами по вопросам информационной безопасности. Проводить регулярное обучение работников по вопросам информационной безопасности при предоставлении доступа к информационным ресурсам Принципала. Доводить до работников новые нормативные документы под роспись.

9.2 Не реже 1 раза в год проводить плановый Инструктаж по вопросам информационной безопасности.

9.3 Принципал обязуется проводить обучение работников Агента ответственных за информационную безопасность не реже 1 раза в год.

10 **Ответственность**

10.1 Работники Агента, нарушившие действующие требования по информационной безопасности, и руководители подразделений, не обеспечившие их выполнение, привлекаются к дисциплинарной ответственности в соответствии с действующим трудовым законодательством.

10.2 При подозрении на мошенничество или иные преступления, а также в случаях нанесения материального ущерба Принципалу, явившиеся следствием нарушения информационной безопасности, материалы предаются в правоохранительные органы.

Инструкция
по инсталляции линии на базе технологии GPON

1. Список сокращений

ODF	оптический кросс
OLT	optical line terminal – центральный узел
ONT (ONU)	optical network terminal – абонентский терминал
PON	passive optical network – технология пассивных оптических сетей
SPLX	Соединительная мини-муфта для защиты сплайса.
КДЗС	Гильза термоусаживаемая в составе комплекта для защиты сварных стыков
КР	коробка распределительная
ЛКС	линейно-кабельные сооружения
МССС	мультисервисная сеть связи ОАО «Ростелеком»
Общество	ОАО «Ростелеком»
ОВ	оптическое волокно
ОК	оптический кабель
ТФОП	телефонная сеть общего пользования
ШКО	шкаф кроссовый оптический

2. Типовые схемы построения сети на базе технологии PON (FTTH)

Построение сетей связи на базе технологии PON (FTTH) в Обществе производится в соответствии с принятыми типовыми схемами, которые представлены ниже.

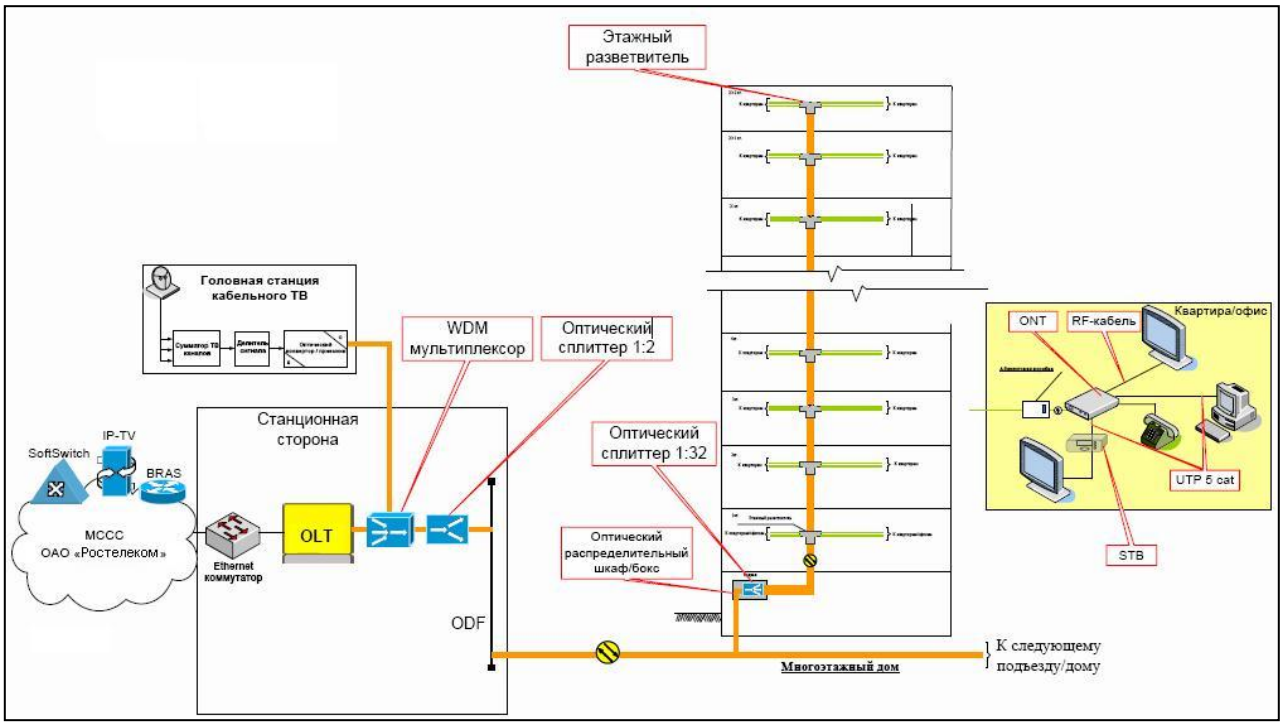


Рисунок 1 - Типовая функциональная схема организации связи.

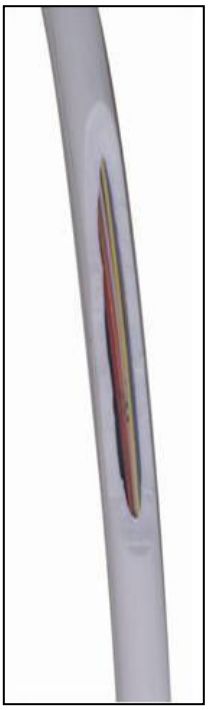
Возможен вариант без установки оптической розетки при условии, что в ONT есть место для размещения запаса оптического волокна и сплайса.

3. Проведение монтажных работ

Перед началом работ, Агент составляет визуальный план проводки кабеля, исходя из особенностей конструкции стен, потолков, лестничных проходов с использованием измерительной рулетки и поисковика скрытой проводки, проверяет трассу на предмет присутствия электрической проводки. Также предварительно инсталлятор с помощью ИОМ проверяет наличие и уровень оптического сигнала в забронированном под данного клиента гнезде. Гнездо и маркировка необходимой ОРК указаны в наряде на выполнение работ. Запрещено задействовать гнезда и ОРК, не соответствующие маркировке, указанной в наряде.

Подключение осуществляется следующим образом:

- с помощью измерителя оптической мощности проверить наличие сигнала в нужном волокне на конце кабеля (кабель может заканчиваться как на самом верхнем, так и на самом нижнем этаже);
- на этаже подключения на проложенном по стояку кабеле с легкоизвлекаемыми волокнами СПЕЦИАЛЬНЫМ ИНСТРУМЕНТОМ для вскрытия оболочки кабеля делается окно 5см (рис.2). ЗАПРЕЩАЕТСЯ РАЗРЕЗАТЬ ВЕРТИКАЛЬНЫЕ НЕСУЩИЕ ЭЛЕМЕНТЫ КАБЕЛЯ, А ТАКЖЕ ВСКРЫВАТЬ КАБЕЛЬ БЕЗ ИСПОЛЬЗОВАНИЯ СПЕЦИАЛЬНОГО ИНСТРУМЕНТА. В случае если подключения на этаже уже были необходимо воспользоваться существующим окном в оболочке кабеля;

– 
– Рисунок 2 – Вскрытие кабеля типа Mini-Breakout.

– необходимые для подключения на этаже N волокна обрезаются на этаже N+X (X – зависит от необходимой длины кабеля до абонента), для этого тоже необходимо вскрыть оболочку кабеля специальным инструментом - на этаже подключения N и на этаже N+X устанавливается устройство защиты и разветвления. Устройство крепится на кабеле с помощью нейлоновых стяжек;

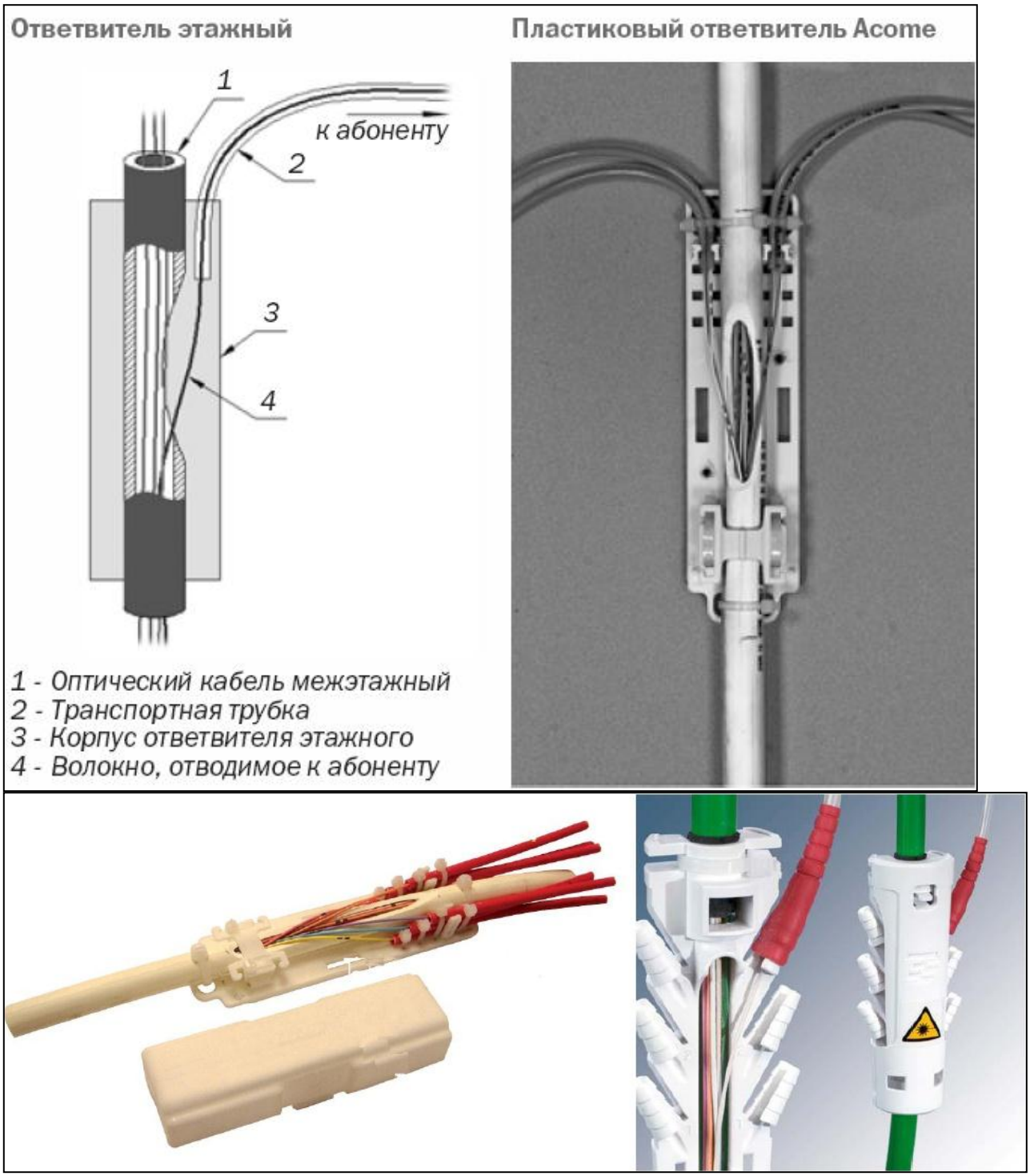


Рисунок 3 – Варианты установки этажного ответвителя.

- для защиты от повреждения, выведенное из кабеля волокно необходимо завести в транспортную трубку и проложить волокно в трубке до квартиры. НЕ ДОПУСКАЕТСЯ ВЫТЯГИВАНИЕ СОСЕДНИХ ВОЛОКОН ИЗ КАБЕЛЯ кроме волокна для подключения абонента. Транспортную трубку необходимо зафиксировать нейлоновой стяжкой в этажном ответвителе и закрыть ответвитель защитной крышкой (рис.3);
- если длины волокна не хватает, то допускается соединение волокон, которое производится ТОЛЬКО С ИСПОЛЬЗОВАНИЕМ СВАРКИ ИЛИ СПЕЦИАЛЬНЫХ СИСТЕМ ДЛЯ МЕХАНИЧЕСКОГО СОЕДИНЕНИЯ

ВОЛОКОН. В связи с этим организации запаса длины вертикального кабеля не требуется. Использование коннекторов для соединения оптических волокон не допускается;

- места соединения оптических волокон должны быть защищены. Если соединение производится в кабельном стояке, необходимо с помощью нейлоновых дюбелей и саморезов закрепить на любой стене стояка абонентскую розетку ШКОН-ПА1 (рис.4); соединить волокна; завести волокна в транспортных трубках (от абонента и от ответвителя) в ШКОН-ПА1; зафиксировать транспотные трубки нейлоновыми стяжками; уложить сплайс или гильзу КДЗС и закрыть крышкой абонентскую розетку. Если соединение производится в квартире абонента, то необходимо транспортную трубку и сплайс (гильзу КДЗС) закрепить в корпусе ONT или абонентской розетки. Если кабель прокладывается от стояка до квартиры абонента по стене и требуется его наростить, необходимо с помощью нейлоновых дюбелей и саморезов закрепить абонентскую розетку ШКОН-ПА1; зафиксировать в ней нейлоновыми стяжками транспортные трубки; уложить запас волокна и сплайс и закрыть розетку крышкой (рис.5).

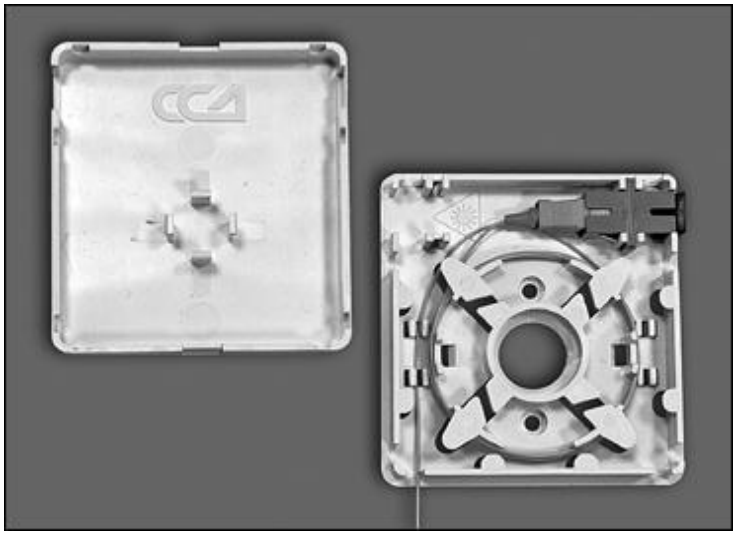


Рисунок 4 – Абонентская розетка ШКОН ПА-1.

Рисунок 5 – Защита места соединения оптических волокон в подъезде с применением абонентской розетки ШКОН ПА-1.

- в квартире абонента кабель протягивается до места расположения абонентской розетки или оборудования ONT, если установка розетки не планируется. Транспортную трубку с волокном необходимо зафиксировать на стене клипсами типа Command 3M на всем протяжении свободного участка, не допуская провисания;
- место размещения ONT выбирается по согласованию с абонентом, по возможности ближе к розетке 220В;
- ONT закрепляется на стене с помощью нейлоновых дюбелей;
- волокно оконечивается разъемом SC с полировкой APC и подключается к абонентской розетке, либо запас волокна укладывается в ONT. Транспортная трубка должна быть зафиксирована нейлоновой стяжкой в розетке или в ONT. Допускается использование предподготовленного пигтейла, который с использованием механического соединителя сваривается с оптическим модулем;
- ONT подключается к абонентской розетке с использованием оптического патчкорда с разъемами SC/APC.
-

4. Нормы на технологическое обеспечение процесса инсталляции услуг связи

Для инсталляции домовой распределительной сети (в том числе абонентских проводок) должно применяться оптическое волокно (полиэтиленовая трубка с инсталлированным в неё оптическим модулем при применении оптического кабеля

Mini-Breakout или его аналога). Абонентская проводка должна выполняться по возможности единым отрезком кабеля. При выборе и прокладке трассы для абонентских проводок следует учитывать существующее ограничение на длину оптического волокна, вытягиваемого из общего оптического кабеля, которая может составлять 20 м. При необходимости наращивания абонентской проводки сростка производится только с одноволоконным оптическим патчкордом с применением сварного соединения или механического соединителя.

В качестве рекомендаций при прокладке абонентской проводки можно использовать требования ОСТН-600-93.

Трасса для абонентской проводки должна удовлетворять следующим основным требованиям:

- учитывать расположение в помещениях электрических и радиотрансляционных проводок;
- быть кратчайшей, прямолинейной, иметь минимальное число пересечений с другими проводками;
- внутри зданий проходить по стенам на высоте 2,3 – 3 м от пола и не менее 50 мм от потолка или по каналам закладных устройств скрытой проводки;
- по наружным стенам проходить под карнизами на высоте 2,5 – 3 м;
- проходить по местам, доступным в любое время для обслуживания.

При выполнении монтажа оптических кабелей следует учитывать, что минимальный радиус при протяжке и установке должен составлять 15мм.

На участках горизонтальной прокладки крепление кабеля следует производить через каждые 250 мм, при вертикальной прокладке – через 350 мм, в местах поворота провода – на расстоянии 50 мм от вершины угла. Кабель должен плотно прилегать к стене без волнистости и перекручиваний. Кабели, идущие в одном направлении, следует прокладывать параллельно и вплотную друг к другу. При пересечении трубопроводов газа, водопровода, канализации кабель прокладывается под ними, а в случае пересечения труб отопления кабель прокладывается по верху теплоизоляции. Звонковая и сигнализационная проводки, проложенные вплотную к стене, пересекаются кабелем сверху.

При прокладке абонентской проводки в помещении абонента необходимо руководствоваться вышеприведенными рекомендациями. Помимо этого нужно выполнять следующие требования:

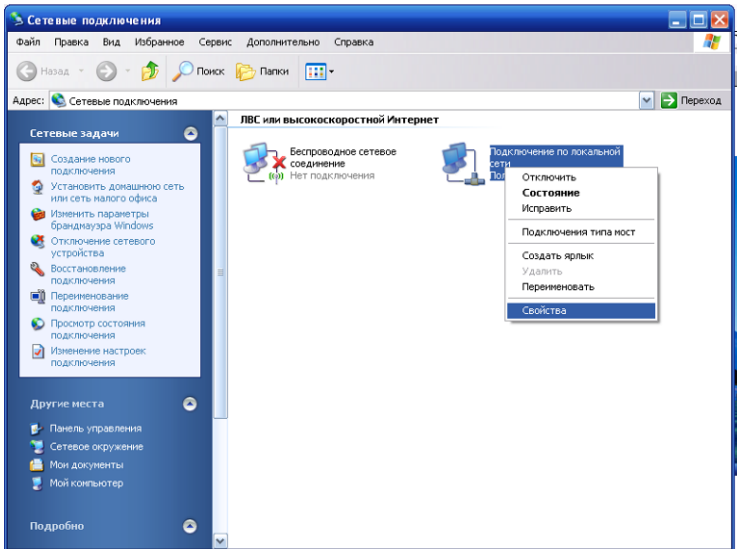
1. Прокладка абонентской проводки и выбор места размещения абонентской коробки выполняются по согласованию с абонентом по возможности ближе к розетке 220В;
2. При вводе абонентской проводки в помещение абонента высота ввода от пола не регламентируется;
3. При выборе трассы для прокладки абонентской проводки следует по возможности не пробивать отверстия через капитальные стены, исключение составляет ввод кабеля в помещение абонента;
4. Через перегородки и дверные коробки кабель необходимо прокладывать через отверстия, просверленные в углах переплетов;
5. В помещениях с декоративной отделкой следует прокладывать кабель над или под плинтусами, наличниками окон или дверей для защиты от механических повреждений. Разрешается прокладка абонентской проводки по деревянному плинтусу помещений (квартир);
6. Запрещается прокладка абонентской проводки по временным перегородкам стен, наличникам дверей и по рамам окон, а также установка абонентской коробки на плинтусе, над дверями, проёмами и окнами;

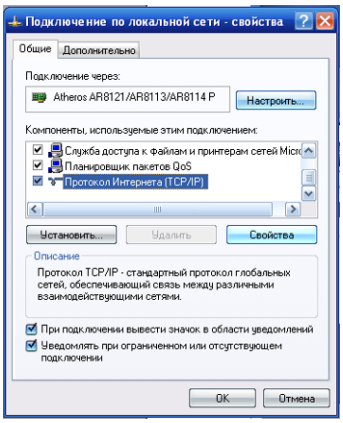
7. Кабель абонентской проводки следует крепить к стенам деревянным, оштукатуренным кирпичным и шлакоблочным, гипсолитовым и т.п. специальными пластиковыми держателями со стальными гвоздями диаметром 1,5 мм длиной 15 или 20 мм. По стенам из бетона, стеклоблоков, камня, кафеля и подобных материалов, в которые забивка гвоздей и проволочных скоб невозможна, а сверление гнезд затруднительно, производить крепление кабеля следует специальными скобами, приклеиваемыми к стеновому основанию клеем [4];
8. Допускается осуществление скрытой прокладки кабеля абонентской проводки, при этом прокладывая его в ПВХ-рукавах под фальшполом и в стяжке полов, за подвесными и подшивными потолками, по стенам в штробах, в кабель-каналах (защитных пластиковых коробах).

Подключение услуги ШПД

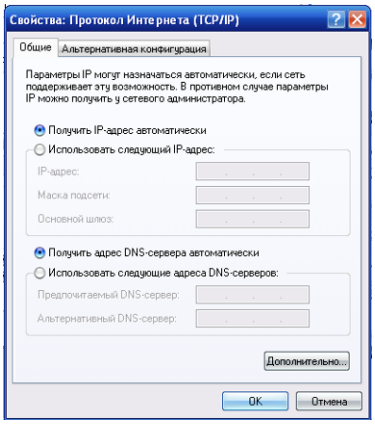
Настройка соединения

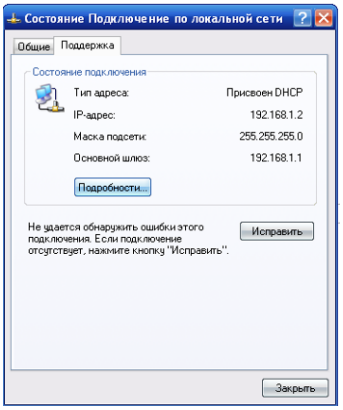
1. Перенастраиваем сетевую карту на ПК



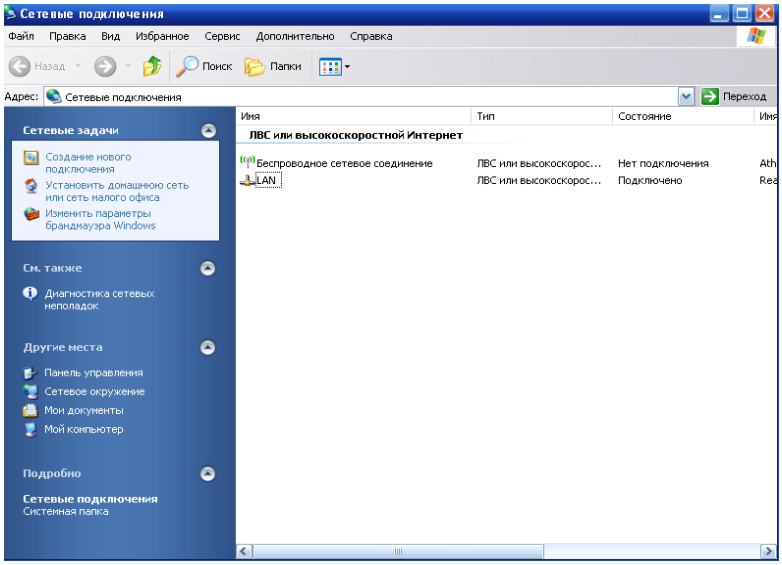


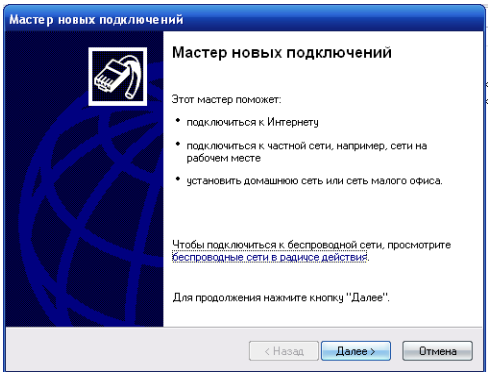
2. Настраиваем под автоматическое получение адреса по DHCP

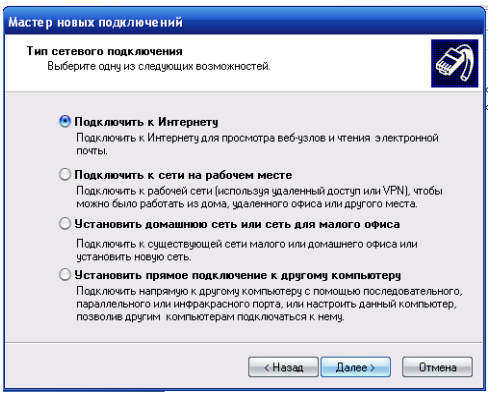


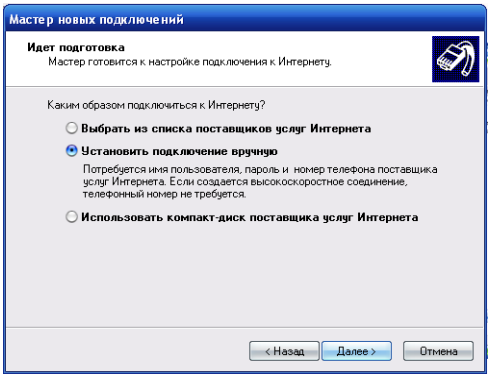


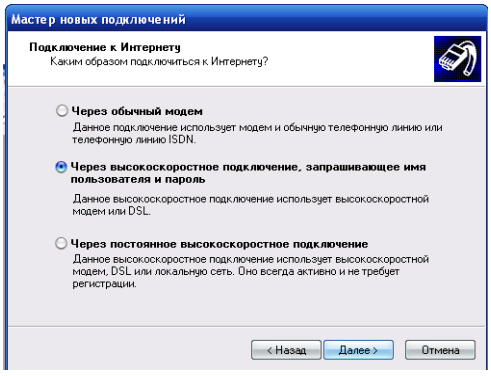
3. «Создание нового подключения»

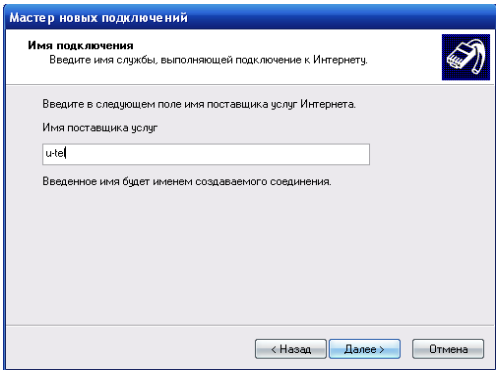


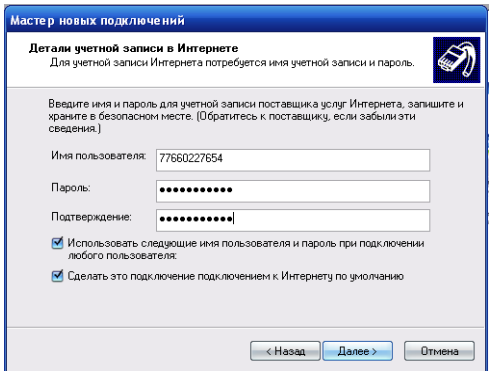

Мастер новых подключений
Мастер новых подключений
Этот мастер поможет:
подключиться к Интернету
подключиться к частной сети, например, сети на рабочем месте
установить домашнюю сеть или сеть малого офиса.
Чтобы подключиться к беспроводной сети, просмотрите беспроводные сети в радиусе действия.
Для продолжения нажмите кнопку "Далее".
< Назад
Далее >
Отмена

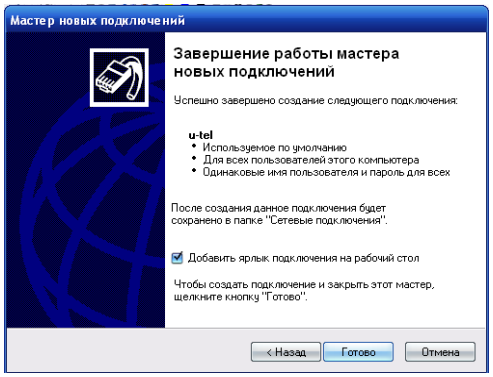

Мастер новых подключений
Тип сетевого подключения
Выберите одну из следующих возможностей.
Подключить к Интернету
Подключить к Интернету для просмотра веб-узлов и чтения электронной почты.
Подключить к сети на рабочем месте
Подключить к рабочей сети (используя удаленный доступ или VPN), чтобы можно было работать из дома, удаленного офиса или другого места.
Установить домашнюю сеть или сеть для малого офиса
Подключить к существующей сети малого или домашнего офиса или установить новую сеть.
Установить прямое подключение к другому компьютеру
Подключить напрямую к другому компьютеру с помощью последовательного, параллельного или инфракрасного порта, или настроить данный компьютер, позволив другим компьютерам подключаться к нему.
< Назад
Далее >
Отмена

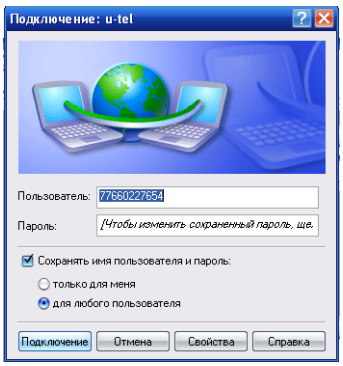

Мастер новых подключений
Идет подготовка
Мастер готовится к настройке подключения к Интернету.
Каким образом подключиться к Интернету?
Выбрать из списка поставщиков услуг Интернета
Установить подключение вручную
Потребуется имя пользователя, пароль и номер телефона поставщика услуг Интернета. Если создается высокоскоростное соединение, телефонный номер не требуется.
Использовать компакт-диск поставщика услуг Интернета
< Назад
Далее >
Отмена


Мастер новых подключений
Подключение к Интернету
Каким образом подключиться к Интернету?
Через обычный модем
Данное подключение использует модем и обычную телефонную линию или телефонную линию ISDN.
Через высокоскоростное подключение, запрашивающее имя пользователя и пароль
Данное высокоскоростное подключение использует высокоскоростной модем или DSL.
Через постоянное высокоскоростное подключение
Данное высокоскоростное подключение использует высокоскоростной модем, DSL или локальную сеть. Оно всегда активно и не требует регистрации.
< Назад
Далее >
Отмена









Подключение услуги IPTV

Технологическая карта по инсталляции абонентского комплекта IPTV

Состав комплекта

В состав комплекта IPTV входит телевизионная абонентская приставка (STB; Set-top box; телеприставка IP) с блоком питания, комплект кабелей для подключения к телевизионному приемнику абонента, Ethernet-кабель и пульт дистанционного управления STB

1. Пульт дистанционного управления (ПДУ)
2. Ethernet-кабель UTP (3 м)
3. Кабель аудио-видеосигналов (AV кабель)
4. Блок питания
5. Телевизионная абонентская приставка (STB)

Примечание: при включении питания устройству может потребоваться некоторое время для выполнения автоматической загрузки последней версии программного обеспечения (предоставляемого оператором). По завершении загрузки устройство отобразит основное меню.

Подключение

Подключение всего комплекта оборудования не вызывает затруднений (см. рисунок). Для подключения необходимо иметь в наличии следующее:

— телевизор с входом Composite, Component либо HDMI

— розетку электросети (напряжением 220В) с достаточным свободным пространством для подключения блока питания телеприставки.

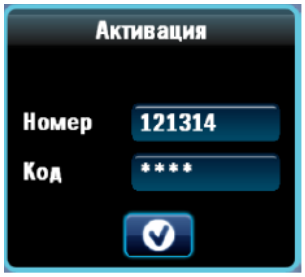
1. Соедините телеприставку и телевизор с помощью AV-кабеля.
2. Соедините свободный Ethernet-порт абонентского терминала ONT и порт Network RJ45 на телеприставке с помощью Ethernet-кабеля. Настройка абонентского терминала ONT производится дистанционно техническими специалистами оператора, предоставляющего услугу IPTV.
3. Согласно инструкции пользователя телевизором на телевизоре выберите вход, к которому подключена телеприставка IP.
4. Включите блок питания телеприставки IP.
5. Если после включения телеприставки IP на экране ТВ не отобразился процесс загрузки услуги, то необходимо выключить питание телеприставки IP, затем выключить и снова включить питание ONT для автоматического получения абонентским терминалом ONT новых настроек. После этого снова включить питание телеприставки IP.

Загрузка и активация устройства

После включения телеприставки IP на экране ТВ появится номер версии приложения и процесс загрузки. На задней панели телеприставки IP должен загореться «желтый» светодиод, информирующий о подключенном канале ШПД и замигать «зеленый» светодиод, информирующий об активности порта передачи данных на телеприставке IP.

На экране телевизора должен отобразиться процесс загрузки телеприставки IP

По окончании загрузки при первом включении телеприставки IP появится окно активации устройства:



Для активации абонентской приставки необходимо в поля «*Номер*» и «*Код*» ввести соответствующие данные, полученные при заключении договора на предоставление услуги IPTV у оператора услуги.

Ввод значений производится с помощью цифровых кнопок пульта дистанционного управления. Для удаления неверно введенного значения используется кнопка «*Влево*». Перемещение между полями меню активации производится с помощью кнопок направлений.

После ввода номера и кода нажмите «*ОК*».

При успешной загрузке клиентского приложения, на экране ТВ начинается вещание телеканала с порядковым номером 1, на экране отображается «*Меню ТВ каналов*» интерфейса пользователя.

Инсталляция услуги IPTV успешно завершена.

Возможные неполадки:

1. После включения телеприставки IP через 3-10 сек. на лицевой панели должен загореться «красный» светодиод. Если он не засветился, то неисправна приставка или ее блок питания. Произвести замену неисправного блока.

2. На задней панели телеприставки IP должен загореться «желтый» светодиод, информирующий о подключенном канале ШПД и замигать «зеленый» светодиод, информирующий об активности порта передачи данных на телеприставке IP. В случае неисправности линии (желтый светодиод горит, но зеленый светодиод не мигает) – проверить соединительные кабели канала ШПД. При необходимости заменить кабели. В случае неисправности канала ШПД организовать устранение неисправности согласно существующим процедурам.

3. В случае возникновения каких-либо проблем с загрузкой клиентского приложения (как правило, связанных с работой сети), на экран выводятся сообщения об ошибках, и инициируется процедура перезагрузки приставки.

4. В случае повторения ошибок при загрузке, проверьте правильность подключения комплекта абонентского оборудования, наличие установленного соединения с оператором. При необходимости свяжитесь со службой технической поддержки оператора услуги Internet.

5. Если указанные значения в полях «*Номер*» и «*Код*» введены неверно, то появится сообщение «*Неверный номер*». В таком случае, проверьте правильность введенных данных и повторите попытку. Помимо этого возможно появление следующих сообщений после корректного ввода номера и кода: *«Счет удален», «Счет активирован», «STB уже активирован», «Ошибка подключения STB»*. При появлении этих сообщений, обратитесь к оператору услуги IPTV.

6. В случае возникновения проблем при управлении меню (зависание, отсутствие реакции при нажатии клавиш) необходимо отсоединить штекер адаптера питания от телеприставки IP на несколько секунд и вставить его обратно. В данном случае произойдет перезагрузка системы

Примечание: для выявления, локализации неисправностей при подключении телеприставки IP к телевизору абонента инсталлятору необходимо использовать

тестовую телеприставку IP, настроенную на технологический тарифный план, а также иметь в наличии ноутбук.