

Конфигурирование Windows 10



Урок №4

Конфигурирование сети в Windows 10

Содержание

Конфигурирование сети в Windows 10	4
Сетевая терминология, используемая Microsoft.....	4
Настройка сетевых интерфейсов.....	8
Общие сведения о TCP/IP	38
Преимущества и особенности TCP/IP	38
Основы IP-адресации и конфигурации	40
Общие сведения о типах адресов IPv4	42
Использование адресов IPv6.....	46
Настройка TCP/IPv4 в Windows 10	57
Тестирование сетевой конфигурации	59
Настройка Windows 10 в сети.....	62
Настройка брандмауэра Windows	63
Учетные записи пользователей	71
Работа с учетными записями пользователей.....	76

Управление пользовательскими свойствами.....	84
Управление членством	
в пользовательской группе.....	86
Управление группами	94
Управление безопасностью с использованием локальной политики безопасности	100
Настройка удаленного управления.....	114

Конфигурирование сети в Windows 10

Сетевая терминология, используемая Microsoft

Прежде чем приступить к рассмотрению материала урока, давайте рассмотрим некоторые термины по отношению к серверам и клиентам, которые будут использоваться в этом уроке. Вам, возможно, знакомы некоторые из этих терминов, но повторение всегда полезно.

Сервер (*Server*). Сервер — это компьютер, к которому пользователи подключаются, чтобы иметь доступ к ресурсам, расположенным на этом компьютере. Этими ресурсами могут быть файлы, принтеры, приложения и т.д. Обычно тип сервера зависит от ресурса, который нужен пользователю. Например, сервер печати — это сервер, который управляет принтерами. Файловый сервер содержит файлы. Серверы приложений могут запускать приложения для пользователей. Иногда на тип сервера указывает конкретное приложение, которое может быть запущено. Например, кто-то может сказать: «Это наш SQL-сервер» или «У нас есть сервер Exchange».

Контроллер домена (*Domain Controller*). Это сервер, который содержит реплику базы данных Active Directory. Active Directory — это база данных, содержащая все объекты безопасности в вашей сети, а также любые ресурсы, которые вы публикуете в Active Directory. Контроллер домена — это сервер, содержащий эту базу данных. Все

контроллеры домена равны в сети, и каждый может читать и записывать в базу данных каталога, если только это не контроллер домена только для чтения (RODC). Некоторые контроллеры домена могут содержать дополнительные роли, но все они являются частью одной сети Active Directory.

Рядовой сервер (*Member Server*). Рядовой сервер — это сервер, который является членом сети на основе домена, но не содержит копию Active Directory. Например, Microsoft рекомендует, чтобы сервер Microsoft Exchange загружался на рядовой сервер вместо контроллера домена. Оба типа — контроллер домена и рядовой сервер могут выступать в качестве файл сервера, сервера печати или сервера приложений. Выбор типа сервера зависит от того, нужен ли вам сервер для репликации Active Directory.

Обнаружение сети (*Network Discovery*). Обнаружение сети — это параметр, определяющий, может ли ваша система Windows 10 находить другие компьютеры и устройства в сети, и могут ли другие компьютеры в сети видеть ваш компьютер. Чтобы включить или отключить обнаружение сети, вам необходимо выполнить следующие шаги:

- В поле поиска Windows 10 введите команду «Состояние сети» (*network*), выберите пункт «Центр управления сетями и общим доступом». Затем нажмите «Изменить дополнительные параметры общего доступа» (*Change Advanced Sharing Settings*) с левой стороны.
- Выберите «Включить/Отключить сетевое обнаружение» (*Change Advanced Sharing Settings*), а затем нажмите кнопку «Сохранить изменения» (*Save Changes*).

Автономный сервер (Standalone Server) Это отдельный сервер, не являющийся членом домена. Многие организации могут использовать этот тип сервера для виртуализации. Например, скажем, вы загружаете Windows Server 2012 R2 с Hyper-V (сервером виртуализации Microsoft) на автономный сервер. Затем вы можете создавать виртуальные машины, которые действуют как контроллеры домена для запуска сети.

Клиентский компьютер (Client Machine) Клиентский компьютер — это компьютер, который обычно используется конечными пользователями компании. Операционными системами для клиентского компьютера являются Windows XP, Windows 7, Windows 8 и Windows 10.

DNS-сервер. Сервер DNS имеет на нем службу DNS. DNS — это служба разрешения имен, которая разрешает имя хоста в IP адрес (называемый прямым поиском). DNS также имеет возможность разрешать IP-адрес в имя (называемый обратным поиском).

Когда вы устанавливаете операционную систему, вы указываете имя компьютера. Проблема в том, что компьютеры общаются друг с другом с использованием адресов IP, например, 192.168.1.100. Для большинства пользователей было бы очень сложно запомнить все разные IP-адреса в сети. Поэтому обычно вы подключаетесь к компьютеру, используя его имя. DNS делает для вас преобразование (разрешение) имени хоста в IP-адрес.

Самый простой способ понять, как это работает, — это вспомнить свой номер телефона. Если вы хотите позвонить кому-то, но не знаете номера телефона, вы можете позвонить в Информационную службу. Они по

интересующему вас имени могут предоставить номер телефона. Этот пример демонстрирует как работает DNS. Вы сообщаете DNS имя хоста, и она возвращает номер сетевого телефона (IP-адрес). DNS — обязательна к установке, если вы хотите установить Active Directory. Вы можете установить DNS до или во время установки Active Directory, но для установки Active Directory обязательно потребуется служба DNS.

Сервер DHCP. Сервер протокола динамической конфигурации хоста (DHCP) запускает службу DHCP, которая динамически назначает сетевую конфигурационную информацию вашим компьютерам. Каждому компьютеру необходимы четыре параметра для полноценной работы в сети: IP адрес, маска подсети, шлюз по умолчанию (адрес маршрутизатора) и адрес DNS сервера. Ваши компьютеры могут получить эту минимальную информацию двумя способами: вручную, когда кто-то вручную вводит информацию TCP/IP в настройках сетевого интерфейса, или динамически, когда служба DHCP автоматически назначает машине необходимые параметры. DHCP может назначить не только эти четыре параметра. DHCP может назначать любую информацию о конфигурации TCP/IP, включая адрес сервера WINS, серверов времени и т.д.

Глобальный каталог. Глобальный каталог представляет собой базу данных всех объектов Active Directory в лесу с подмножеством атрибутов объекта. Представьте глобальный каталог в качестве оглавления (содержания) книги. Если вам нужно что-то посмотреть в этой книге, вы должны открыть оглавление и найти, на какую страницу вам нужно обратиться. Когда вам нужно найти ресурс

в домене (пользователь, опубликованный принтер и т.д.), вы можете выполнить поиск в Глобальном каталоге, чтобы найти местоположение этого ресурса.

Номера портов. Номера портов используются приложениями и службами, чтобы они могли связываться по сети. Подумайте о номерах портов, как о номерах на дверях, которые используются для доступа к приложениям или службам. Например, если пользователь хочет подключиться к сервису WWW, он использует номер порта 80.

Настройка сетевых интерфейсов

Прежде чем вы сможете подключить компьютер с ОС Windows 10 к имеющейся в организации сети, вы должны настроить сетевую карту (NIC). Она представляет собой аппаратный компонент, используемый для подключения компьютеров или других устройств к сети, чтобы они могли взаимодействовать друг с другом. Сетевые адAPTERы отвечают за предоставление физического соединения, на основании физического адреса самого сетевого интерфейса.

В настоящее время сетевыми адаптерами оборудуются не только сами компьютеры, но и сетевые принтеры, другие специализированные устройства, такие как системы обнаружения вторжений (IDS) и т.д. Сетевые адAPTERы не обязательно должны быть отдельными картами. Практически все современные материнские платы имеют встроенный сетевой адаптер. Так же существует огромное количество всевозможных устройств, подключаемых к сети.

Сетевые адAPTERы (как и все другие аппаратные устройства) нуждаются в драйвере для связи с операционной системой Windows 10.

Прежде чем физически установить сетевой адаптер, важно прочитать инструкции производителя, поставляемые с оборудованием. Большинство сетевых адаптеров должны быть самонастраивающимися, используя возможности Plug and Play. После установки сетевого адаптера, поддерживающего Plug and Play, он должен определиться операционной системой и начать работать по завершению процедуры установки, если в базе Windows есть подходящий драйвер. Если драйвер не будет найден, система запросит установку драйвера. Возможно, потребуется перезагрузка ОС, но современные операционные системы постоянно улучшаются, и скорее всего устройство будет готово к использованию без необходимости перезагрузки.

Если по какой-то нелепой случайности ваш сетевой адаптер не поддерживает Plug and Play, для его установки вам понадобится установочный диск с записанной на нем программой установки. Если такой диск отсутствует, вы можете воспользоваться мастером установки оборудования, как это было рассмотрено в предыдущем уроке.

После установки необходимых драйверов вы можете получить доступ к сведениям о сетевом подключении и управлять свойствами сетевого подключения через «Центр управления сетями и общим доступом».

Настройка сетевого адаптера

После того, как вы установили сетевой адаптер, можно просмотреть и настроить его через диалоговое окно

«Свойства». Чтобы перейти на страницу свойств сетевого адаптера, откройте «Диспетчер устройств». Для этого нажмите правую кнопку мыши на поле «Пуск» и выберите в списке пункт «Диспетчер устройств».

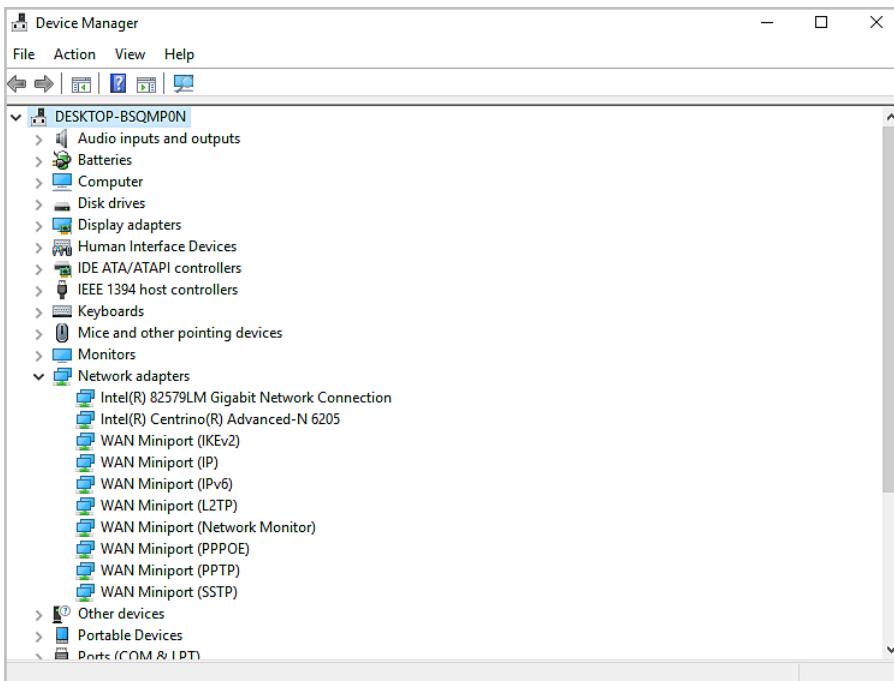


Рисунок 1

На скриншоте (рис. 1) отображается категория устройств «Сетевые адAPTERы» и в ней список адаптеров, установленных на компьютере. Доступ к свойствам сетевого адаптера позволяет нам просматривать и изменять параметры его конфигурации. Для этого необходимо выбрать интересующий нас адаптер и выбрать пункт «Свойства» в контекстном меню. Рассмотрим подробно каждую вкладку.

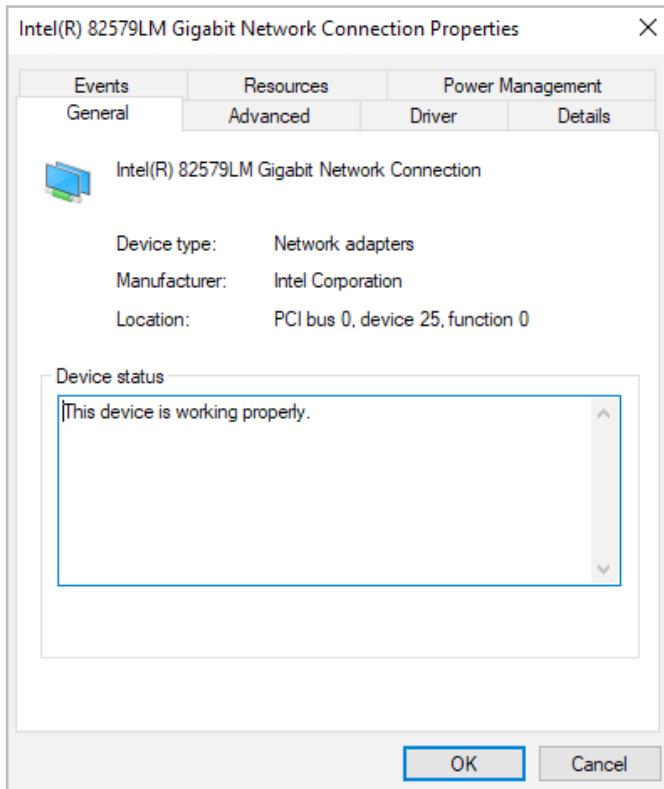


Рисунок 2

Вкладка «Общие» (General) диалогового окна «Свойства сетевого адаптера» (рис. 2) показывает имя адаптера, тип устройства, производителя и местоположение. В поле «Состояние устройства» указывается, правильно ли работает устройство. Если имеются проблемы в работе, в поле «Состояние устройства» отображается код ошибки и краткое описание того, что Windows 10 идентифицирует как проблему. Вы можете выполнить поиск в Интернете кода ошибки, если имеющегося описания недостаточно.

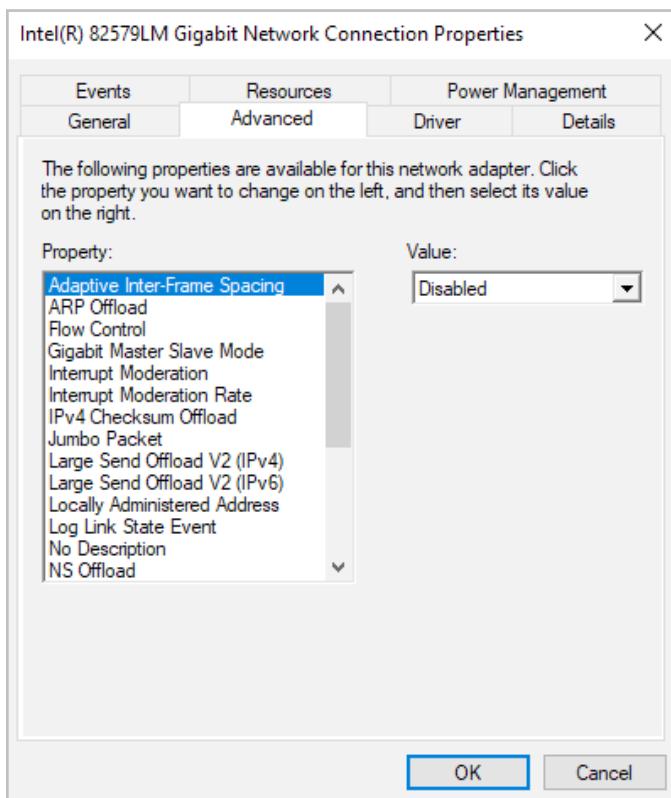


Рисунок 3

Содержимое вкладки «Дополнительно» (Advanced) (рис. 3) зависит от используемого сетевого адаптера и драйвера. На рисунке показан пример вкладки «Дополнительно» для адаптера Fast Ethernet. Чтобы настроить параметры в этом диалоговом окне, выберите свойство, которое вы хотите изменить из доступного списка свойств и укажите желаемое значение для свойства в поле «Значение» справа.

Вкладка «Драйвер» (Driver) содержит следующую информацию о вашем драйвере:

- Поставщик драйвера;
- Дата выпуска драйвера;
- Версия драйвера (полезно при определении того, является ли установленный драйвер самым свежим);
- Цифровая подпись (компания, предоставляющая цифровую подпись для подписания драйвера).

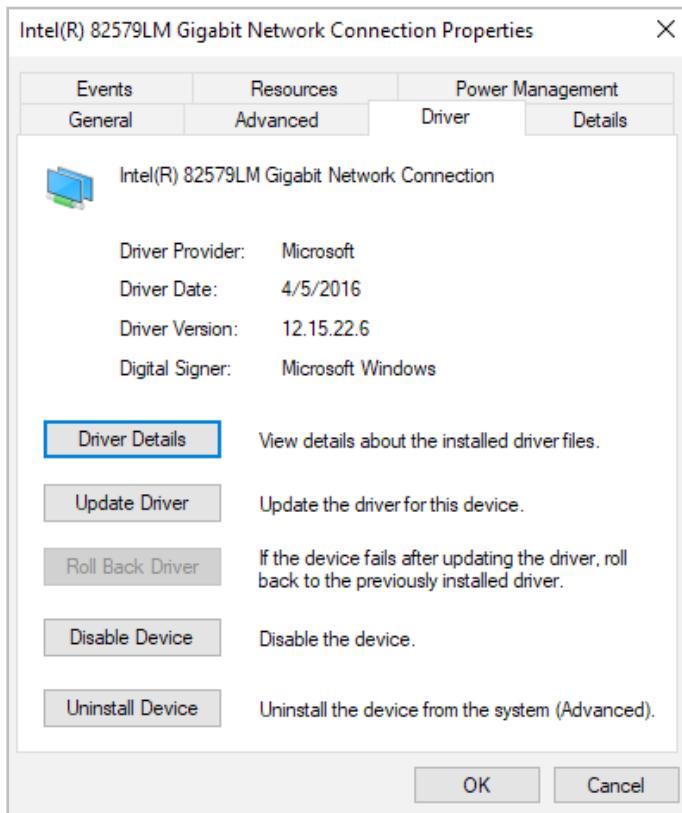


Рисунок 4

Вкладка «Драйвер» для адаптера показана на рис. 4. Информация здесь варьируется от драйвера к драйверу

и даже от поставщика к поставщику. Кнопка «Сведения о драйверах» на вкладке «Драйвер» открывает диалоговое окно «Сведения о файле драйвера», в котором приводятся следующие сведения о драйвере:

- Расположение файла драйвера (полезно для устранения неполадок);
- Оригинальный поставщик драйвера;
- Версия файла (полезная для устранения неполадок)
- Информация об авторе драйвера;
- Цифровой подписчик для драйвера.

Кнопка «Обновить драйвер» запускает мастер по обновлению драйвера для существующего устройства. Кнопка «Откатить» (Roll Back Driver) позволяет вам вернуться к ранее установленному драйверу, если после обновления сетевого драйвера вы столкнетесь с проблемами. На рисунке кнопка «Откатить» недоступна, так как обновление драйвера не производилось или предыдущий драйвер недоступен. Кнопка «Отключить устройство» (Disable) используется для отключения устройства. После отключения устройства кнопка «Отключить» меняется на кнопку «Включить устройство» (Enable), которую вы можете использовать для включения устройства. Кнопка «Удалить» (Uninstall) удаляет драйвер из конфигурации вашего компьютера. Удаление драйвера производится, если вы собираетесь удалить устройство из своей системы, или если вы хотите полностью удалить конфигурацию драйвера из своей системы, чтобы вы могли переустановить ее с нуля в автоматическом, либо ручном режиме.

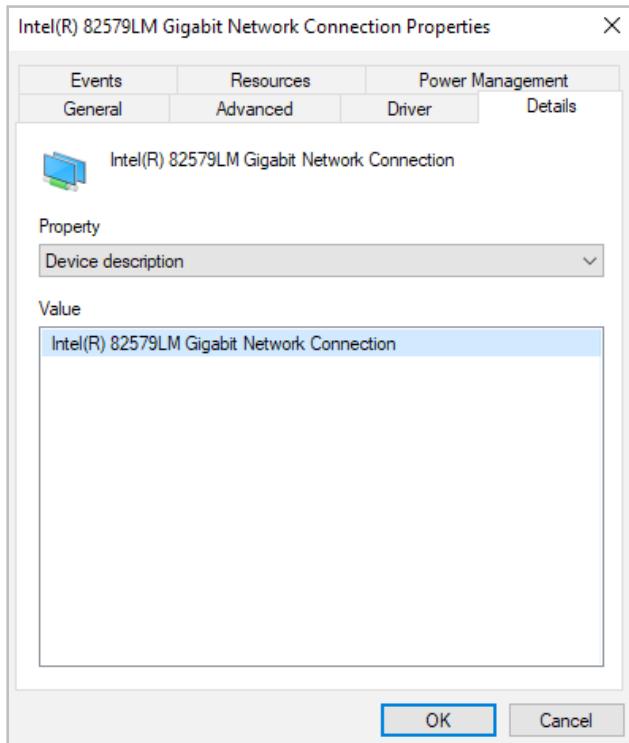


Рисунок 5

Вкладка «Сведения»(Details) (рис. 5) содержит параметры аппаратных ресурсов для вашего сетевого адаптера. Информация, отображаемая на вкладке «Сведения», зависит от аппаратного устройства.

Одним из наиболее важных параметров, перечисленных в выпадающем списке является параметр «ИД оборудования» (Hardware Ids) (рис. 6). Этот параметр однозначно позволяет определить, что это за устройство, если на этапе установки драйверов оно отображается, как неизвестное. Достаточно скопировать первую строку и воспользоваться любой поисковой системой (рис. 7).

Урок №4

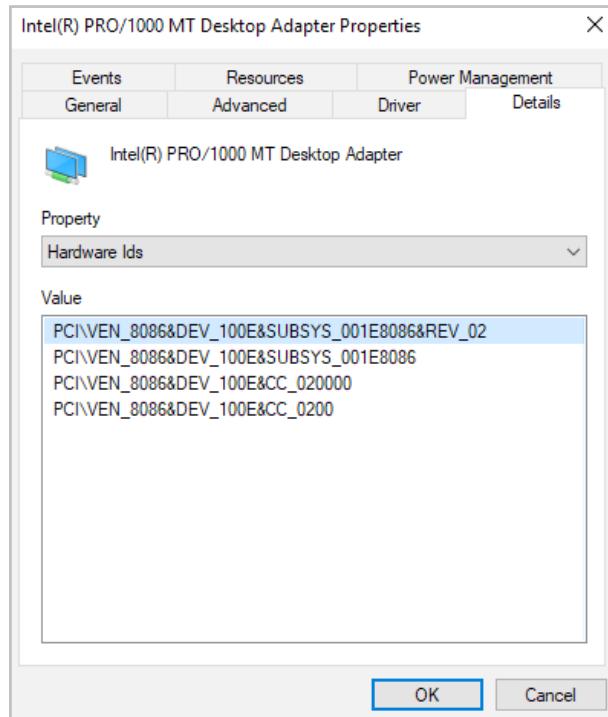


Рисунок 6

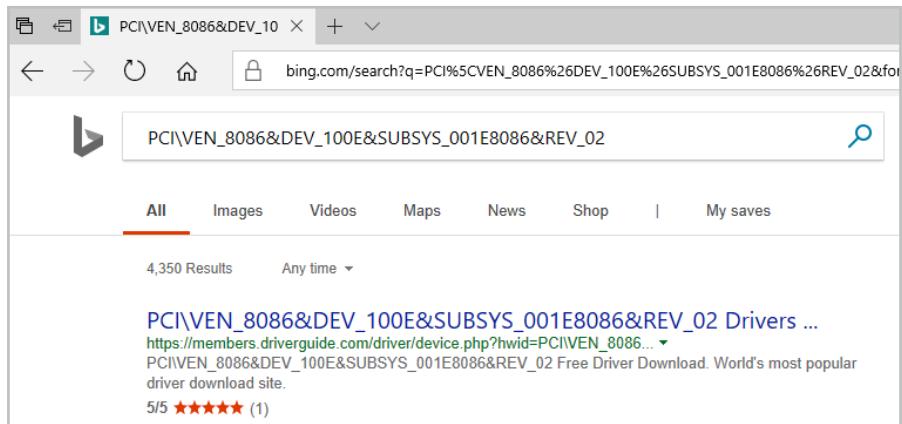


Рисунок 7

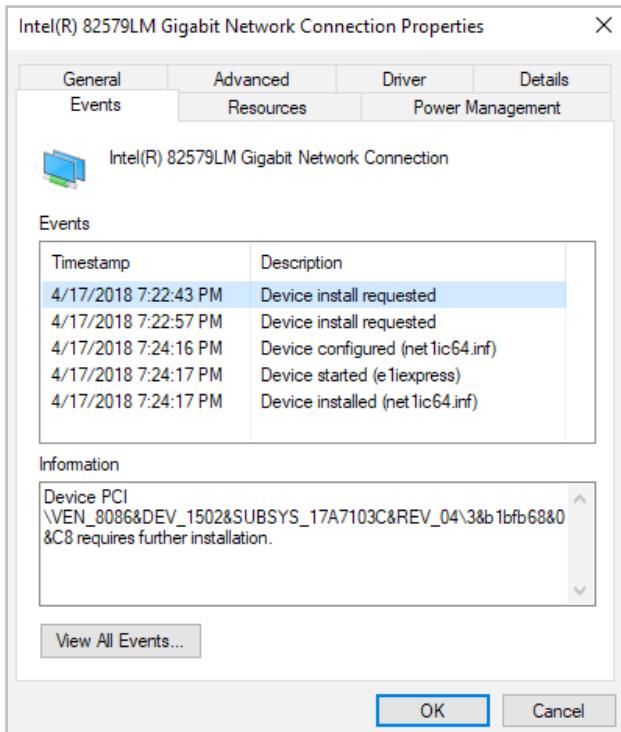


Рисунок 8

На вкладке «События» (Events) отображаются некоторые события устройства, которые произошли с ним в процессе работы. Существует также кнопка «Просмотреть все события» (View All Events), которая открывает оснастку MMC «Просмотр событий» (Event Viewer), в которой отображаются все события для этого устройства. Это хороший способ посмотреть, были какие-либо события или проблемы (например, ошибки или предупреждения) для данного устройства.

Вкладка «Ресурсы» (Resources) (рис. 9) показывает параметры ресурсов для вашего сетевого адаптера.

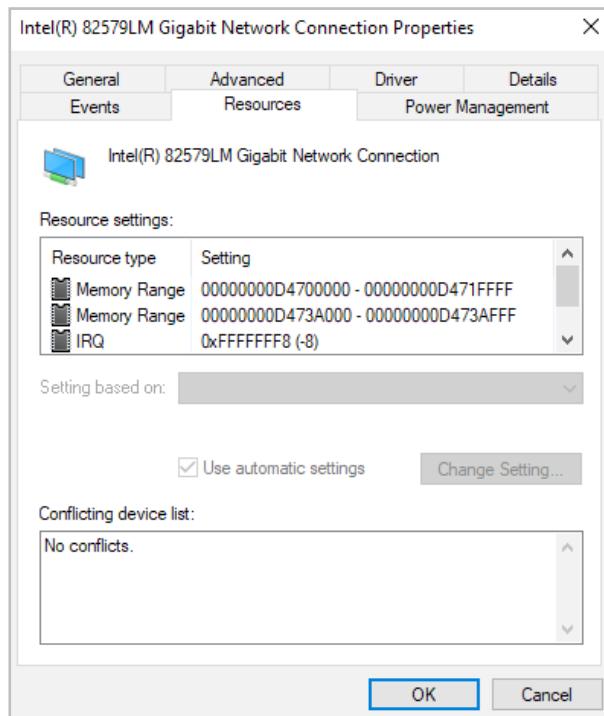


Рисунок 9

Ресурсы включают в себя запрос на прерывания (IRQ) и диапазон адресов памяти. Эта информация может быть важна для устранения неполадок, если другие устройства пытаются использовать одни и те же параметры. Обычно это не так, потому что Windows 10 и спецификация Plug and Play должны настраивать неконфликтные параметры. Если проблемы все таки имеются, то в поле «[Список конфликтующих устройств](#)» внизу вкладки «Ресурсы» будут показаны имеющиеся конфликты.

На вкладке «[Управление питанием](#)»(Power Management) (рис. 10) вы можете настроить, как это устройство может экономить электроэнергию в системе.

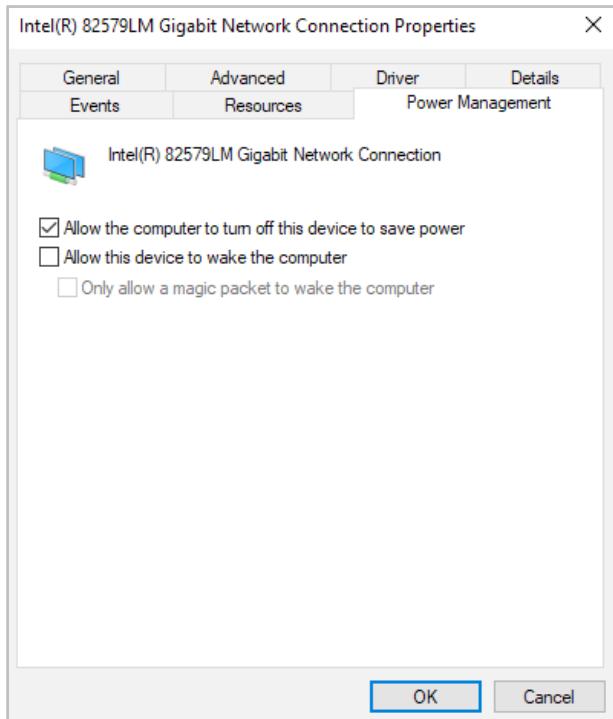


Рисунок 10

Например, вы можете позволить системе отключить это устройство, а также позволить этому устройству вывести систему из спящего режима.

Устранение неполадок сетевого адаптера

При установке сетевого адаптера могут возникнуть некоторые проблемы или ошибки. Давайте рассмотрим некоторые из них и возможные способы их устранения.

Если ваш сетевой адаптер не работает, проблема может быть связана с оборудованием, программным обеспечением драйвера или сетевыми протоколами. Мы обсудим проблемы уровня 3 (сетевой уровень) далее в этом уроке.

Сейчас рассмотрим ситуации, возникающие на 1-м (физическем уровне) и 2-м (уровне передачи данных), которые приводят к возникновению проблем с сетевым адаптером:

- **Сетевой адаптер отсутствует в HCL.** Если устройство не входит в список совместимости оборудования (HCL), используйте интернет-ресурсы, чтобы узнать, возможна ли работа данного адаптера с Windows 10 или обратитесь за консультацией к поставщику оборудования.
- **Устаревший драйвер.** Убедитесь, что у вас самый последний драйвер для вашего адаптера. Вы можете проверить версию драйвера на вкладке «[Драйвер](#)» на странице «[Свойства](#)» для адаптера. Нажав кнопку «[Обновить драйвер](#)» и выбрав поиск лучшего драйвера. Также вы можете проверить наличие последнего драйвера на веб-сайте поставщика оборудования.
- **Сетевой адаптер не распознается Windows 10.** Проверьте диспетчер устройств, чтобы узнать, распознает ли Windows 10 адаптер. Если вы не видите свой адаптер, вы можете попытаться установить его вручную, используя меню «[Действие -> Установить старое устройство](#)». Предварительно поищите информацию и драйвера в интернете.
- **Неправильно настроенная сетевая карта.** Убедитесь, что параметры сетевой карты верны для параметров, известных в вашей сети, и для компьютера, к которому подключен адаптер.
- **Проблема с кабелем.** Проверьте, что все сетевые кабели имеют правильный тип и нормально функционируют. Это означает, что разъем правильно установлен, ка-

бель прямой или кроссовый (в зависимости от того, где он подключен), и кабель не имеет повреждений. Базовая проверка производиться по наличию индикации светодиода на сетевом адаптере. Это не является стопроцентной гарантией работы, но проверить необходимо. Возможна ситуация, когда светодиод светится, а обмен данными не происходит.

- **Проблемы с межсетевыми устройствами.** Убедитесь, что все межсетевые устройства работают правильно. Например, для сети FastEthernet, убедитесь, что используемый коммутатор и его порт работают правильно.

Настройка беспроводных сетевых адаптеров

Беспроводные устройства являются необходимым атрибутом в современном мобильном мире. Windows 10 поддерживает автоматическую настройку беспроводных сетевых адаптеров, что упрощает использование беспроводных сетевых соединений. Windows 10 автоматически обнаружит доступные беспроводные сети и подключит ваш компьютер к предпочтительной беспроводной сети.

Одним из преимуществ настройки Windows 10 и беспроводных подключений является то, что после того, как вы подключились к точке беспроводного доступа (WAP), ваша Windows 10 запомнит это и снова подключит вас к этой предпочтительной беспроводной сети, когда ваше устройство будет находиться в зоне ее действия.

Настройка параметров беспроводной сети

Если у вас есть беспроводной сетевой адаптер, совместимый с Windows 10, он автоматически распознается операционной системой. Это может быть встроенный

адаптер, используемый современными ноутбуками, беспроводная карта, которую вы устанавливаете на компьютер, или даже беспроводной USB-адаптер. После его установки он отображается в диспетчере устройств, а также в «Центре управления сетями и общим доступом» в разделе «Просмотр активных сетей».

Мы использовали Диспетчер устройств в предыдущем разделе для конфигурации сетевого адаптера, поэтому давайте использовать Центр управления сетями и общим доступом для настройки беспроводной сети. На рис. 11. показан «Центр управления Сетями» и общим доступом с одной активной сетью. Беспроводная сеть с именем ITSTEP.

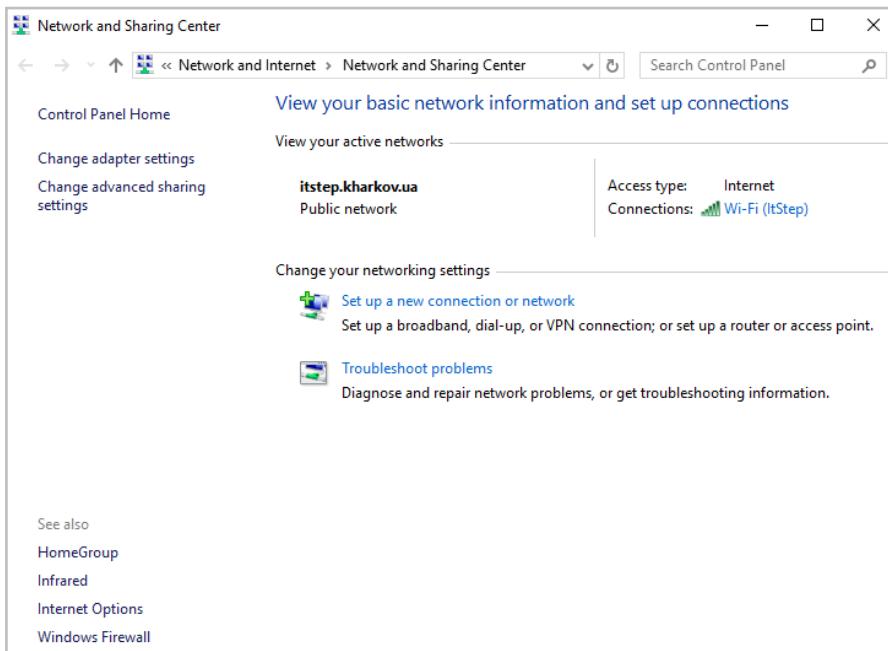


Рисунок 11

Вы можете выполнить любой из следующих шагов для доступа к Центру управления сетями и общим доступом:

- Нажав правую кнопку мыши на «Пуск» — «Сетевые подключения» — «Центр управления сетями и общим доступом».
- Нажав правой кнопкой мыши значок сети в нижнем правом углу панели задач и выбрав «Центр управления сетями и общим доступом».

Другой способ получить доступ сетевым настройкам — нажать комбинацию Win+I, а там выбрать «Сеть и интернет» (Network & Internet).

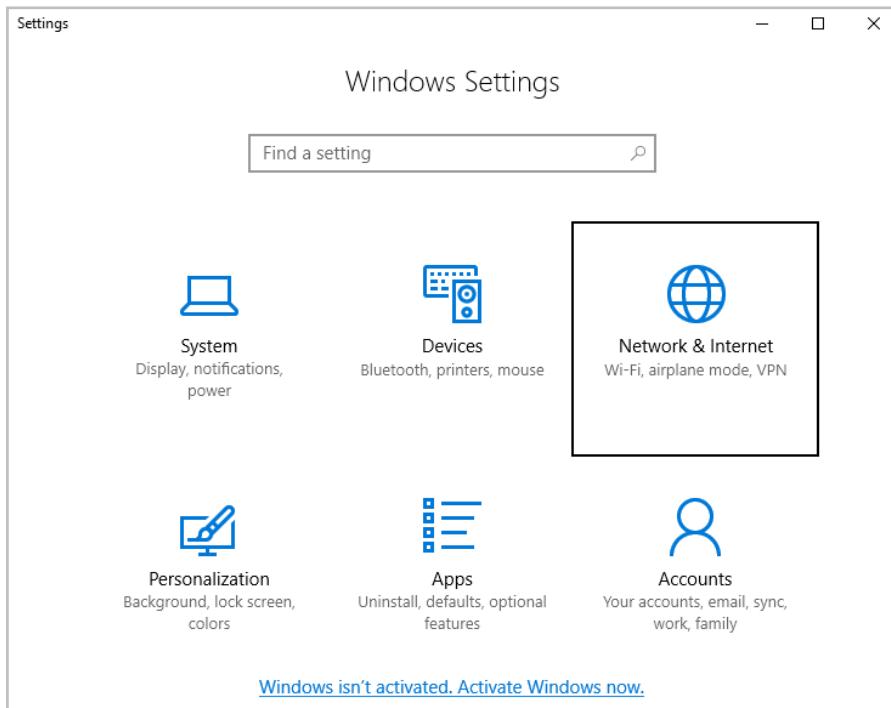


Рисунок 12

В левой части открывшегося окна можно выбрать любой из интересующих элементов и в правой части отобразятся связанные с этим элементом параметры.

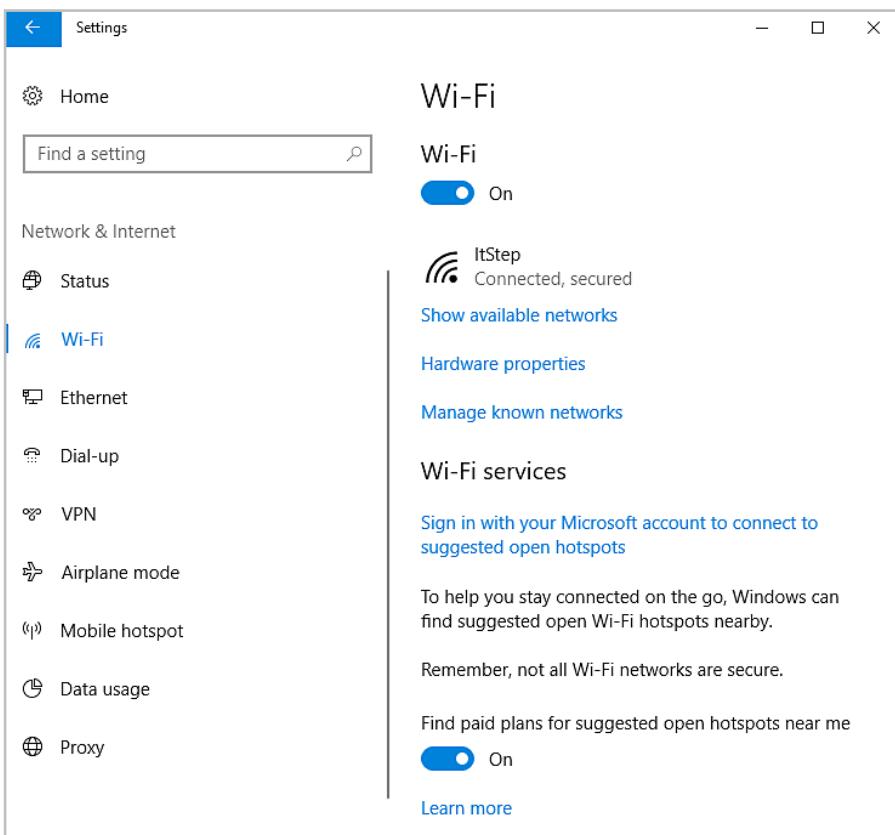


Рисунок 13

Просмотр состояния беспроводного сетевого подключения

Через «Центр управления сетями и общим доступом» вы легко получите доступ к окну состояния беспроводного сетевого подключения, в котором вы можете сначала

просмотреть состояние, а именно статус соединения на 3-м уровне (IPv4 и IPv6), состояние среды передачи, значение идентификатора набора услуг (SSID), время работы сети, согласованную скорость соединения и качество сигнала.

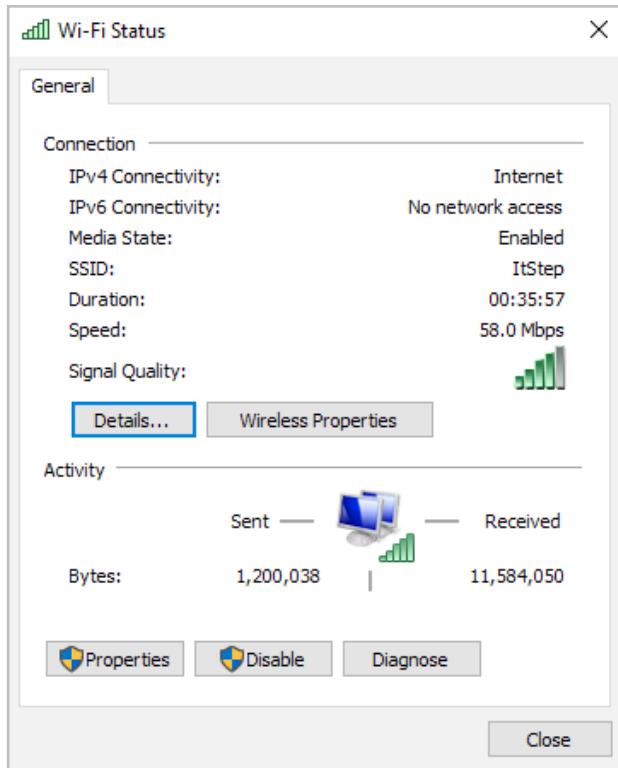


Рисунок 14

Кнопка «Сведения» (Details) (рис. 14) предоставляет информацию, такую как фактический физический адрес (уровень 2), логический адрес (уровень 3), параметры динамической адресации (DHCP), элементы разрешения имен и т.д. После проверки параметров физического уровня эта информация позволяет анализировать состояние или

устранять проблемы с логикой (драйвером/программным обеспечением).

Просмотр сведений о беспроводной сети

В окне состояния беспроводного сетевого подключения есть раздел «**Активность**», показывающий трафик в реальном времени (в байтах), отправляемый и принимаемый беспроводной сетью. В окне состояния беспроводного сетевого подключения вы также получите доступ к свойствам беспроводного сетевого подключения, который включает в себя доступ к страницам конфигурации беспроводного адаптера.

Для этого необходимо нажать кнопку «**Свойства**» (*Properties*) в разделе «**Активность**» (*Activity*) (см. Рис. 14). На странице «**Свойства Wi-Fi**» есть вкладка «**Сеть**», которая показывает, какой сетевой адаптер используется для этого подключения (которое вы можете изменить, если у вас есть несколько доступных).

В разделе «**Отмеченные компоненты используются этим подключением**» (рис. 15), отображаются различные клиенты, службы и протоколы, которые в настоящее время доступны для этого соединения.

Вы можете установить или удалить сетевые клиенты, сетевые службы и сетевые протоколы, нажав соответствующую кнопку. Вы также можете просмотреть свойства клиента, службы или протокола, если они доступны, сначала выделив элемент из списка, а затем нажав кнопку «**Свойства**» для выбранного элемента. Если кнопка «**Свойства**» серая, страница свойств недоступна для элемента. В окне «**Свойства беспроводного сетевого**

подключения» у вас есть доступ к страницам свойств аппаратной конфигурации сетевого адаптера. Это те же страницы, к которым у вас есть доступ через диспетчер устройств.

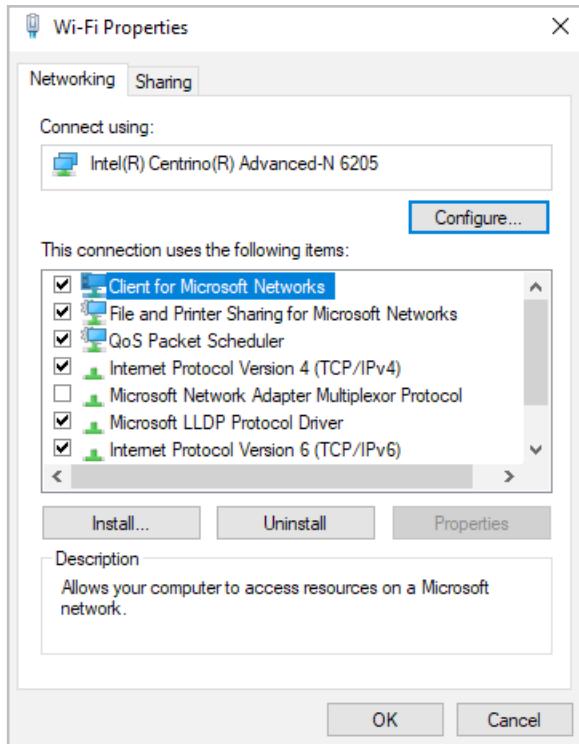


Рисунок 15

Настройка безопасности беспроводной сети

Безопасность беспроводной сети — очень важная часть настройки наших беспроводных сетей. Ориентиром для этого является точка беспроводного доступа или беспроводной маршрутизатор, к которому мы подключаемся. Независимо от того, используете ли вы небольшую

беспроводную сеть или большую беспроводную инфраструктуру, у вас должен быть разработан план по обеспечению безопасной связи и должна быть настроена безопасность беспроводной сети. Существует несколько основных параметров, которые можно настроить на устройствах сетевого доступа для повышения безопасности беспроводной сети:

- Отключить широковещательную рассылку SSID, который является именем беспроводной сети. Когда широковещательная передача SSID отключена, беспроводная сеть не может быть обнаружена автоматически, пока вы вручную не настроите беспроводную сетевую карту для подключения к этому SSID.
- Создать список фильтрации MAC-адресов, чтобы только определенные беспроводные устройства могли подключаться к беспроводной сети.
- Включить шифрование, такое как защищенный доступ Wi-Fi (WPA) или WPA2.

Для крупных сетей есть решения, которые позволяют обеспечивать управление большим количеством точек доступа при помощи беспроводного контроллера, который отвечает за работу точек доступа в сети, обеспечение контроля доступа пользователей и применение политик шифрования. Для небольших реализаций эта функция управления выполняется вручную, когда отдельно настраиваются беспроводные маршрутизаторы или точки доступа.

Политики безопасности устанавливаются на устройстве беспроводного доступа и беспроводном клиенте.

Компоненты клиента Windows 10 должны быть настроены так, чтобы соответствовать настройкам безопасности устройств доступа к беспроводной сети. Конфигурирование самих устройств может быть выполнено через веб-интерфейс, посредством которого можно получить доступ к страницам конфигурации устройства беспроводного доступа.

Большинство современных сетевых устройств имеют встроенный веб-сервер, позволяющий установить HTTP-соединение из веб-браузера. Windows 10 также имеет возможность настроить устройство беспроводного доступа, если поставщик оборудования сделает его доступным. Если какой-либо конкретный компонент отсутствует, вы можете запустить конфигурацию на основе веб-браузера из [«Центра управления сетями и общим доступом»](#).

Если у вас есть Windows 10, настройте беспроводное сетевое соединение или выполните настройку при помощи мастера установки, предлагаемого производителем.

Если вы выполнили простейшую конфигурацию и не настроили параметры безопасности, Windows 10 сможет автоматически подключиться к беспроводной сети без вмешательства пользователя. Этот простой процесс настройки упрощает подключение к домашней или небольшой сети для обычных пользователей. Однако это нехорошее решение.

Если вы настроили параметры безопасности беспроводной сети на сетевом устройстве, вам необходимо и на клиенте Windows 10 настроить правильные параметры безопасности. Окно конфигурации доступно из [«Центра управления сетями и общим доступом»](#).

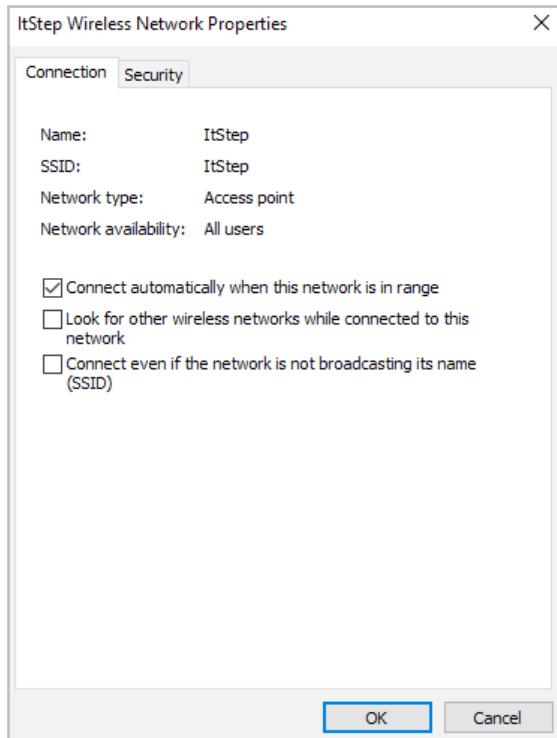


Рисунок 16

В диалоговом окне «Свойства» выберите кнопку «Беспроводная сеть». Здесь вы можете установить или изменить параметры конфигурации клиента Windows 10. Первой вкладкой диалогового окна является вкладка «Соединение» (рис. 16), которая отображает следующую информацию.

- **Имя (Name).** Имя назначенное беспроводной сети.
- **SSID.** Этот параметр определяет идентификатор для беспроводной сети. Обычно это строка, состоящая из ASCII символов. Транслируется широковещательно по умолчанию, позволяя компьютеру или пользователям

выбирать беспроводную сеть для подключения. Некоторые устройства беспроводного доступа позволяют одновременно использовать несколько SSID, создавая несколько беспроводных сетей на одном устройстве.

- **Тип сети (Network Type).** Отображает режим работы беспроводной сети. Если беспроводная сеть находится в режиме инфраструктуры, этот параметр будет точкой доступа. Если беспроводная сеть является *ad hoc*, на экране отобразится Computer-To-Computer.
- **Доступность сети (Network Availability).** Отображает, кому доступна беспроводная сеть: например, все пользователи или только я.
- **Автоматически подключаться, когда эта сеть находится в диапазоне (Connect Automatically When This Network Is In Range).** Когда выбрана, эта опция позволяет автоматически подключаться к этой беспроводной сети. Отмена выбора (снятие галочки) требует от пользователя выбора этой беспроводной сети для подключения.
- **Искать другие беспроводные сети при подключении к этой сети (Look For Other Wireless Networks While Connecting To This Network).** Windows 10 попытается найти другие беспроводные сети, даже если в этот момент вы подключены к сети. Это позволяет пользователю узнать, есть ли лучшие доступные сети, даже после того, как вы подключились к точке беспроводного доступа.
- **Подключаться даже в том случае, если сеть не передает свое имя (SSID) (Connect Even If The Network Is Not Broadcasting Its Name (SSID)).** Если беспровод-

дная сеть, к которой вы пытаетесь подключиться, не транслирует свой SSID, вы должны выбрать эту опцию, чтобы Windows 10 могла автоматически подключаться к ней.

Вторая вкладка в диалоговом окне «Свойства беспроводной сети» — это «Безопасность» (рис. 17), которая позволяет настраивать параметры безопасности, определенные в политике безопасности, и настраивать их на устройствах доступа к беспроводной сети.

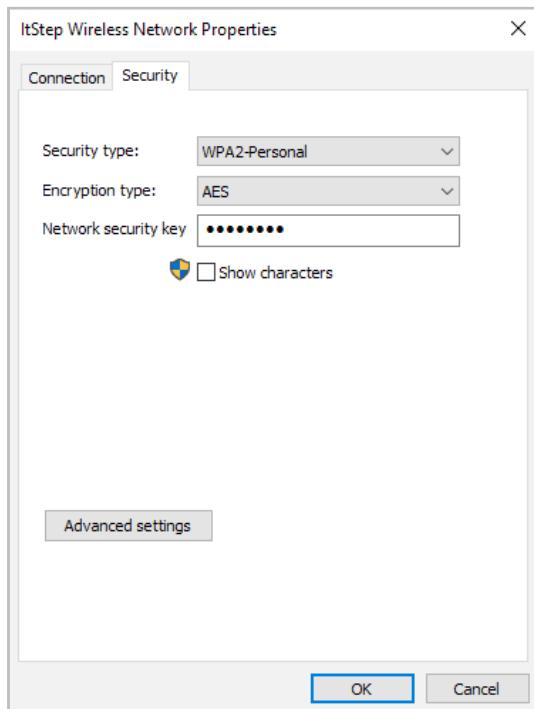


Рисунок 17

На рисунке показан раскрывающийся список «Тип безопасности» (Security Type) вкладки «Безопасность»

с выбранным **WPA2-Personal** и «Типом шифрования» (**Encryption Type**) — AES. Вы также можете увидеть сетевой ключ безопасности, если установите флажок «Показать символы» (**Show Characters**).

Настройка Wi-Fi Direct

Для обеспечения возможности подключения к устройствам без использования WAP, чтобы вы могли подключать устройства напрямую друг к другу через высокоскоростные беспроводные адAPTERЫ на этих устройствах, можно воспользоваться технологией Wi-Fi Direct.

Wi-Fi Direct — это технология, которая позволяет нам напрямую обращаться к другим устройствам, не требуя отдельной точки доступа Wi-Fi. Windows 10 использует технологию ближней связи (более известную как NFC), чтобы позволить системе Windows 10 находить другие устройства с поддержкой NFC Wi-Fi, чтобы их можно было сопрягать вместе.

Когда устройства пытаются соединиться друг с другом, **Near Field Proximity** (NFP) получает информацию о соединении с устройством, которое пытается подключиться. Затем NFP передает информацию о сопряжении в Windows 10. Windows 10 Wi-Fi Direct автоматически выполнит процедуры сопряжения Wi-Fi Alliance Out-Of-Box для соединения.

Во время процесса сопряжения, Windows предложит пользователю дать разрешение на соединение. Если дано разрешение, Windows 10 попытается завершить процесс установки соединения. С этого момента не требуется никакого другого взаимодействия с пользователем.

Windows 10 дает возможность выбрать, нужно ли соединяться с другими устройствами. На (рис. 18) показаны параметры конфиденциальности Windows 10 и способы синхронизации Windows 10 с другими устройствами.

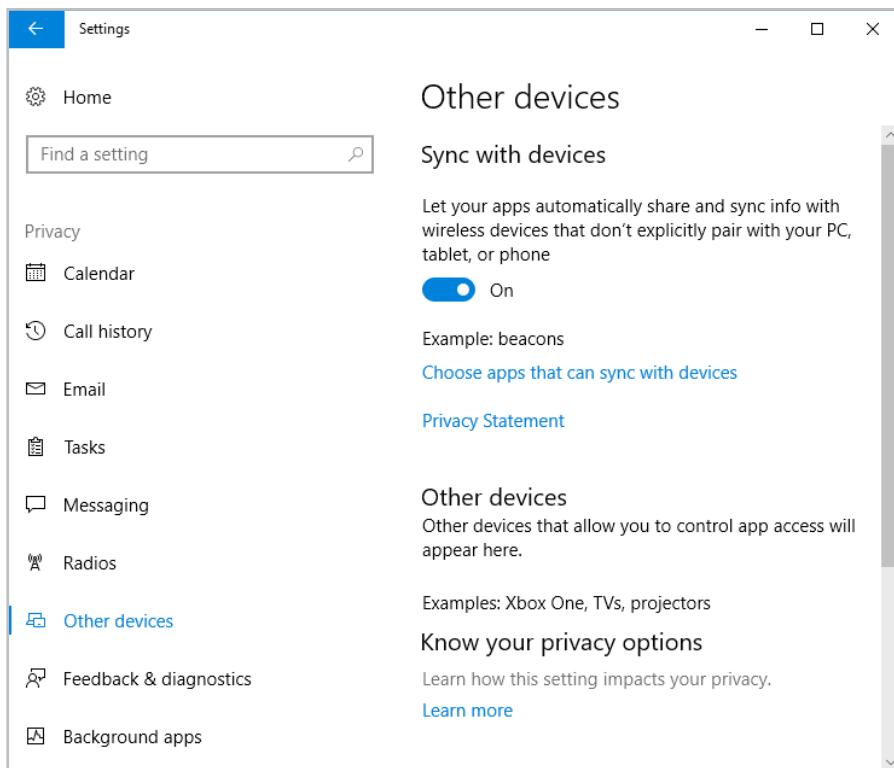


Рисунок 18

Как вы можете видеть на рисунке, также можно выбрать, какие приложения могут синхронизироваться с устройствами. Это дает администратору или пользователю более гибкую возможность разрешить приложениям подключаться к конкретным устройствам или любым приложениям к любому устройству.

Устранение неполадок беспроводной связи

Есть несколько распространенных проблем с беспроводной сетью, на которые вы можете обратить внимание, если у вас возникли проблемы с подключением к беспроводной сети. Ниже приведены несколько проблем и возможные способы их решений:

- **Убедитесь, что ваша беспроводная сетевая карта включена.** Одна из наиболее распространенных причин заключается в том, что у многих ноутбуков и планшетов есть либо переключатель, либо горячая клавиша, которая включает и отключает беспроводное устройство. Часто выключатель ноутбука каким-то образом отключается, или пользователь каким-то образом нажимает последовательность клавиш, чтобы отключить беспроводной интерфейс. Физический уровень всегда является первым для начала поиска.
- **Убедитесь, что ваша беспроводная карта и устройства доступа совместимы.** Карты, совместимые со стандартом 802.11b, могут подключаться только к устройствам доступа 802.11b или 802.11b/g, настроенным на прием b. Карты, использующие 802.11a, могут подключаться только к устройствам доступа 802.11a или 802.11a/b/g, настроенным на прием a. Плата 802.11n должна подключаться к устройству доступа 802.11n для повышения эффективности. Современные беспроводные точки доступа позволяют работать в смешанном режиме и данная проблема актуальна только для устаревшего оборудования. Большинство из них будет автоматически согласовывать лучшие доступные спецификации.

- **Убедитесь, что сигнал точки доступа доступен.** Выходная мощность сигнала может быть высокой, но мощность RF поглощается или ослабляется, когда она проходит через стены, изоляцию или воду. Вы должны убедиться, что уровень помех в допустимых пределах и не препятствует беспроводному сигналу. Кроме этого сами точки доступа могут создавать себе проблемы, так как в густонаселенных районах на квадратный километр могут приходить десятки точек доступа. А каналов у Wi-Fi всего 11 (вообще, согласно стандарту 802.11, каналов 14, но 12, 13 и 14-й не поддерживаются большинством гражданских устройств из-за особенностей законодательства США).
- **Убедитесь, что параметры безопасности настроены одинаково.** SSID, тип шифрования, алгоритм шифрования и ключ безопасности должны быть одинаковыми как на устройстве беспроводного доступа, так и на беспроводном клиенте. В стремлении упростить первоначальную настройку и безопасную настройку для конечных пользователей некоторые поставщики оборудования добавляют небольшую кнопку, которая позволяет устройству доступа к сети согласовывать безопасный набор параметров с клиентом. В некоторых случаях после того, как беспроводная сеть начала работать некорректно, анализ проблемы показал, что параметры настройки стали несовместимы, благодаря тому, что кто-то нажал эту кнопку непосредственно перед сбоем.
- **Обеспечьте автоматическое подключение, если SSID не транслируется.** Если у вас возникли проблемы

с подключением к сети, которая не передает свой SSID, установите флажок «Подключить даже если сеть не широковещательная» в диалоговом окне «Свойства беспроводной сети».

- **Проанализировать, как беспроводной маршрутизатор взаимодействует с проводными устройствами.** Беспроводные маршрутизаторы, которые часто используются, действительно достаточно технологически сложны. У них есть коммутационные порты для подключения проводных устройств в частной сети, а также интернет-порт для подключения к внешнему миру. Беспроводная часть устройства похожа на другой порт коммутатора, что позволяет беспроводным устройствам взаимодействовать с проводными устройствами.

Когда производится поиск и устранение проблемы, нужно начинать с проверки работоспособности проводных устройств на предмет того, могут ли они общаться друг с другом и работает ли внешний порт. Попробуйте также проверить связь между проводными и беспроводными устройствами. Не рекомендуется использовать беспроводную сеть для настройки беспроводных устройств. Конфигурирование через беспроводной интерфейс в конечном итоге приведет к потере соединения в середине конфигурации и вам так или иначе придется подключиться по кабелю.

Общие сведения о TCP/IP

Еще одна группа элементов, которые нам нужно настроить, прежде чем мы сможем подключить компьютер под управлением Windows 10 к сети, — это стек протоколов, который позволит одному компьютеру взаимодействовать с другими компьютерами. **Протокол управления передачей/Межсетевой протокол** (*Transmission Control Protocol/Internet Protocol*) сокращенно TCP/IP является основным стеком протоколов. Это набор протоколов, которые превратились в отраслевой стандарт для сетевого, межсетевого и прикладного уровней сетевого взаимодействия.

Преимущества и особенности TCP/IP

TCP/IP как стек протоколов был принят в качестве промышленного стандарта в 1980-х годах и по-прежнему является основным стеком протоколов межсетевого взаимодействия. В стандартной установке Windows 10 по умолчанию включены IPv4 и IPv6. TCP/IP имеет следующие преимущества:

- TCP/IP является наиболее распространенным протоколом и поддерживается практически всеми сетевыми операционными системами. Это необходимый стек протоколов для обеспечения доступа в Интернет.
- TCP/IP является надежным и масштабируемым для использования в небольших и крупных сетях.
- Поддержка предоставляется для подключения по взаимосвязанным сетям, независимо от операционных

систем, используемых на верхних уровнях модели OSI или физических компонентах на нижних уровнях модели OSI.

- TCP/IP предоставляет стандартные услуги маршрутизации для перемещения пакетов по взаимосвязанным сегментам сети. Разделение сетей на несколько подсетей оптимизирует сетевой трафик и облегчает управление сетью.
- TCP/IP предназначен для обеспечения надежности передачи данных путем обеспечения логического соединения на транспортном уровне и проверки того, что каждый сегмент данных получен и передан в приложение-получатель данных, путем повторной передачи потерянной информации.
- TCP/IP позволяет классифицировать данные по их важности с использованием качества обслуживания. Это позволяет, например, установить более высокий приоритет для критичного к задержкам потока данных, такого как [Voice over IP](#).
- TCP/IP предназначен для отказоустойчивости. Он способен динамически перенаправлять пакеты, если сетевые пути становятся недоступными, предполагая, что существуют альтернативные пути.

Приложения могут предоставлять такие сервисы, как «протокол динамической конфигурации хоста» (DHCP) для конфигурации TCP/IP и «службы доменных имен» (DNS) для разрешения имени хоста и IP-адреса.

Windows 10 продолжает поддерживать «автоматическую приватную IP-адресацию» (APIPA), используемую

небольшими локальными сетями без DHCP-сервера, чтобы позволить Windows 10 автоматически назначать IP-адрес себе.

Включение альтернативной конфигурации IP позволяет пользователям иметь статический и динамический IP-адрес, сопоставленный с одним сетевым адаптером. Эта функция используется мобильными пользователями, перемещающимися между различными сегментами сети.

IPv6 включает гораздо большее адресное пространство по сравнению с IPv4 и, что более важно, добавляет многие дополнительные функции TCP/IP в стандартизованный протокол. Это важно, потому что вендор, который утверждает, что поддерживает TCP/IP, должен поддерживать версию 1980-х годов и может не поддерживать дополнительные функции, такие, например, как протокол IPSec. IPv6 включает подобные функции, как стандартные, позволяющие осуществлять более качественный и безопасный обмен данными.

Основы IP-адресации и конфигурации

Прежде чем вы сможете настроить TCP/IP, вы должны иметь базовое представление о его конфигурации и адресации. Давайте рассмотрим IP адресацию. Чтобы настроить клиент TCP/IP, вы должны указать IP-адрес, маску подсети и шлюз по умолчанию (если вы собираетесь общаться за пределами локальной сети). В зависимости от вашей сети вы можете настроить DNS-сервер, доменное имя или, возможно, даже WINS-сервер.

На группе скриншотов ниже вы можете увидеть окно Свойств IPv4 Windows 10. Далее мы рассмотрим

элементы конфигурации. Несмотря на то, что обычно включена автоматическая настройка, эти параметры были назначены вручную для примера статической конфигурации.

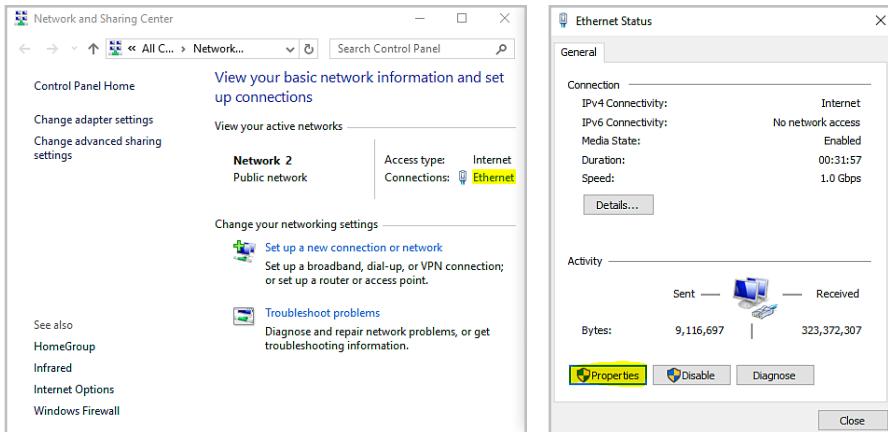


Рисунок 19

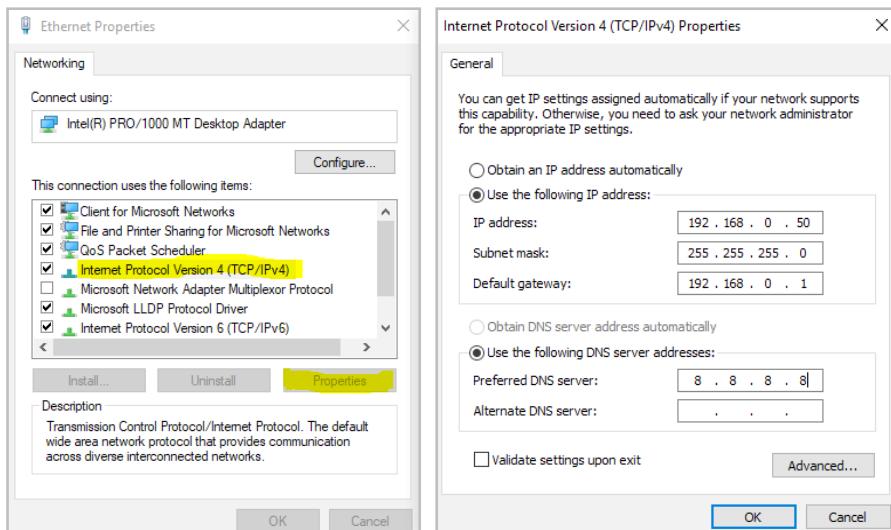


Рисунок 20

Общие сведения о типах адресов IPv4

Схема адресов IPv4 является одной из двух, используемых сегодня в Интернете, а TCP/IP — фактически единственный стек сетевых протоколов, используемый пространстве сетей Интернет. Существует три типа адресов IPv4: широковещательные, групповые и индивидуальные.

- **Широковещательный** (*broadcast*) адрес считывается всеми хостами, которые его слышат (широковещательная передача не будет проходить через маршрутизатор, поэтому только локальные устройства слышат широковещательную передачу). Широковещательный адрес IPv4 выглядит 255.255.255.255; (в двоичном виде каждый бит равен 1).
- **Групповой** (*multicast*) адрес — это специальный адрес, который будет прослушивать одно или несколько устройств, входящее в группу многоадресной рассылки. Только локальные устройства, настроенные для прослушивания подобного адреса, будут принимать и обрабатывать данные пакета с групповым адресом. Групповой адрес будет иметь значение от 224 до 239 в первом октете. Пример группового адреса — 224.0.0.5.
- **Индивидуальный** (*unicast*) адрес однозначно идентифицирует компьютер или устройство в сети. Индивидуальный адрес IPv4 представляет собой 32-битный адрес, представленный в точечно-десятичном виде (пример — 131.107.1.200). Каждое число в десятичной системе с точкой в качестве разделителя пред-

ставляет собой десятичное представление 8 битного двоичного числа, соответственно значение каждого из них может находиться в диапазоне от 0 до 255. Часть адреса IPv4 используется для идентификации сети, в которой находится устройство (или сети назначения устройства), а часть используется для идентификации отдельного хоста в локальной сети или уникального хоста в удаленной сети.

Классы адресов IPv4

Существует три класса индивидуальных IP-адресов. В зависимости от класса, который вы используете, разные части адреса показывают адрес сети и адрес узла. В таблице показаны три класса сетевых адресов и количество сетей и хостов, доступных для каждого сетевого класса.

Класс сети	Значение первого октета	Количество доступных сетей	Количество доступных адресов в сети
A	1–126	126	16,777,214
B	128–191	16,384	65,534
C	192–223	2,097,152	254

Количество октетов, которые вы можете использовать для идентификатора сети или идентификатора хоста, зависит от того, какой класс вы используете для своей сети. Например, если у нас есть адрес класса В 131.107.0.0, первые два октета (131.107) будут идентификатором сети, а два последних октета будут идентификатором хоста. В таблице показаны различные классы и октеты, определяющие идентификатор сети (представленные X),

а октеты определяющие идентификатор хоста (представленные Y).

Класс	Пример	Network ID	Host ID
A	17.1.10.10 (X.Y.Y.Y)	17 (X)	1.10.10 (Y.Y.Y)
B	131.107.14.240 (X.X.Y.Y)	131.107 (X.X)	14.240 (Y.Y)
C	192.168.1.10 (X.X.X.Y)	192.168.1 (X.X.X)	10 (Y)

Маска подсети IPv4

Маска подсети используется для указания, какая часть адреса IPv4 определяет адрес сети, а какая часть определяет уникальное значение хоста. Маска подсети может быть показана либо в виде десятичного числа с точками, как, например, 255.255.255.0, либо как префикс, например /24. Префикс — это значение количества бит в маске, равных 1. Например, 255.255.224.0 на самом деле 11111111.11111111.11100000.00000000, где 19 бит — единицы, соответственно префикс будет выглядеть — /19.

Стандартное значение масок для классовой сетевой адресации показано в таблице.

Класс	Стандартная маска	Префикс
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

Другой задачей маски подсети является разбиение имеющегося диапазона на подсети. Например, маска 255.255.255.224 позволяет использовать восемь подсетей. Для восьми подсетей должно быть восемь диапазонов IP адресов. В таблице показаны количества адресов в получаемой подсети для различных значений маски.

Значение маски	Кол-во адресов в подсети
255	1
254	2
252	4
248	8
240	16
224	32
192	64
128	128

Что это означает для нас? Ну, допустим, у вас есть маска подсети 255.255.255.224. Поскольку 224 допускает восемь подсетей, в каждой подсети будет по 32 адреса. В таблице показаны диапазоны адресов подсети класса С для значения последнего октета маски 224.

Подсеть	Диапазон	Доступные адреса
Диапазон 0	0–31	1–30
Диапазон 1	32–63	33–62
Диапазон 2	64–95	65–94
Диапазон 3	96–127	97–126
Диапазон 4	128–159	129–158
Диапазон 5	160–191	161–190
Диапазон 6	192–223	193–222
Диапазон 7	224–255	225–254

Важный момент!!! В любом диапазоне вы не можете использовать первый адрес диапазона (идентификатор сети) и последний адрес диапазона (ограниченно широковещательный).

Использование адресов IPv6

Когда в 1980-х годах были разработаны и приняты стандарты, касательно работы стека TCP/IP, разработчики протокола IP не предполагали, что в скором времени понадобится более 4 миллиардов адресов (а за вычетом специальных остается доступно к использованию около 2,5 миллиардов), которые возможно назначить для IPv4, опираясь на доступное количество значений у 32-битного двоичного числа. Резкое увеличение использования компьютеров в домашних условиях и на рабочем месте привело к тому, что стала остро ощущаться нехватка адресов. В 1990-х годах программисты поняли, что потребуется новая реализация для протоколов межсетевого уровня. Это была непростая задача, и помимо этого интеграция в существующую инфраструктуру заняла бы много времени. Появилось промежуточное решение, известное как Трансляция сетевых адресов (NAT) и Трансляция портов (PAT). NAT/PAT разрешало нескольким устройствам в частной сети использовать один публичный адрес. В качестве временного решения оно оказалось достаточно удачным, но требовалось что-то более кардинальное. Протокол IPv6 в данном случае решает основную проблему IPv4 — проблему нехватки адресов.

Кроме этого, по прошествии времени с момента принятия стандарта IPv4, появилась необходимость в новых и улучшенных функциональных возможностях межсетевого протокола. В IPv6 не только увеличилось адресное пространство, но также были добавлены дополнительные функциональные возможности, которые стали частью стандарта IPv6.

Например, IPv4 имеет заголовок переменной длины, что усложняет анализ, потому что необходимо прочитать дополнительное поле данных, чтобы увидеть, какой длины заголовок. В большинстве случаев заголовок имеет минимальную длину, поэтому почему бы просто не зафиксировать его длину и добавить расширение в заголовок, если нам нужно больше информации? IPv6 использует IP-заголовок фиксированной длины с возможностью переноса дополнительной информации в отдельную область, называемую заголовком расширения.

Microsoft добавила IPv6 в свои операционные системы с NT 4.0; но он по умолчанию не был включен. Windows 10 (как и Vista и Windows 7/8) поддерживает как IPv4, так и IPv6. Основные различия, которые вы заметите между IPv4 и IPv6, — это формат и размер IP-адреса. Адреса IPv6 составляют 128 бит, которые обычно записываются как восемь групп из четырех шестнадцатеричных символов (*хексстетов*). Адреса IPv4, как вы видели ранее, представляют собой 32 бита-четыре десятичных представления восьми бит. Каждая из восьми групп символов в адресе IPv6 разделяется двоеточием; например, 2001:4860:0000:0000:0012:10FF:FECD:00EF.

Скоро ли IPv6 займет глобальное адресное пространство? Интеграция IPv6 в сетевую инфраструктуру происходит уже достаточно длительное время и сколько ещё это продлится никто не знает. Поэтому переход на IPv6 происходит без отмены использования IPv4 и оба стека протоколов чудесно могут существовать и работать одновременно на межсетевых и клиентских устройствах.

Существует множество механизмов для одновременного использования IPv6 и IPv4, в том числе:

- Двойной стек-компьютер или устройство, одновременно работающее с стеками протоколов IPv4 и IPv6.
- Протокол ISATAP-Intra-Site Automatic Tunnel Addressing Protocol.
- 6to4 — метод инкапсуляции для размещения пакетов с адресами IPv6 в пакетах с адресами IPv4.
- Teredo туннель — еще один метод инкапсуляции для размещения трафика IPv6 в пакете IPv4.

Для некоторых методов динамического перевода IPv6-to-IPv4 требуется, чтобы IPv4-адрес компьютера равнялся последним 32 битам адреса IPv6. Когда эти методы перевода используются, обычно записывают последние 32 бита в обычном для нас точечно-десятичном виде, например 2001:4850::F8:192.168.122.26.

Существует два способа назначения IP-адреса (для IPv4 или IPv6): вы можете вручную назначить IP-адрес на компьютере под управлением Windows 10, или можно использовать DHCP.

Новые концепции и новая реализация старых концепций в IPv6 включают следующее:

- Большое адресное пространство (128 бит по сравнению с 32 битами).
- Автоконфигурация разрешенных в Интернете адресов с или без DHCP (без DHCP это называется автоконфигурацией без сохранения состояния).
- Более эффективный IP-заголовок (меньше полей и контрольной суммы).

- IP-заголовок фиксированной длины (заголовок IPv4 — переменная длина) с заголовками расширений за пределами стандартной фиксированной длины для обеспечения улучшений.
- Встроенная мобильность и безопасность IP (хотя она доступна в IPv4, IPv6 значительно улучшает реализацию).
- Встроенные схемы перехода, позволяющие интегрировать пространства IPv4 и IPv6.
- Сообщения широковещательной передачи ARP заменяются многоадресным запросом.

128-битное адресное пространство. Новое 128-разрядное адресное пространство предоставит уникальные адреса в обозримом будущем. Хотелось бы сказать, что мы никогда не будем использовать все адреса, но прогнозы могут оказаться неправильными. Количество уникальных адресов в пространстве IPv6 равно 2^{128} или $3,4 \times 10^{38}$ адресов. Насколько велика эта цифра? Достаточно для гостей и холодильников (и, может быть, даже для автомобилей), чтобы у всех были свои собственные адреса?

Для примера, расстояние до ближайшей черной дыры от Земли составляет 1600 световых лет. Если бы вы собрали 4-миллиметровые шарики отсюда до ближайшей черной дыры и назад, вам понадобится $7,6 \times 10^{21}$ шариков. Это означает, что вы можете однозначно адресовать каждый шарик с Земли в черную дыру и обратно и все еще останется довольно много адресов.

Другой пример: адресное пространство IPv6 достаточно велико, чтобы обеспечить более 1 миллиона

адресов на квадратный дюйм площади поверхности земли (включая океаны).

Полная конфигурация в сравнении с Автоконфигурацией без сохранения состояния. Автоконфигурация — это еще одно добавление/улучшение в IPv6. Когда вы выбираете использовать DHCP в IPv6, вы можете настроить свои системы для конфигурации Stateful или Stateless. Stateful — это то, что мы сегодня используем для IPv4. Stateful означает, что DHCP собирается предоставить нашим клиентам IPv6 все свои данные TCP/IP (IP-адрес, шлюз по умолчанию и все параметры DHCP).

Что делать, если клиент Windows 10 захочет спросить, в какой сети он работает, и на основе этой информации создать свой собственный IP-адрес заполнить поле — шлюз по умолчанию. Это то, что делает конфигурация Stateless. Конфигурация без сохранения состояния означает, что адрес клиента основан на информации из сообщений маршрутизатора. Это означает, что клиент создает свой собственный IP-адрес и получает адрес шлюза на основе анонса маршрутизатора и своего MAC-адреса. Они все равно могут получить все другие параметры DHCP, но они не получат IP-адрес и шлюз по умолчанию от DHCP.

Улучшенный заголовок. IPv6 Заголовок IPv6 более эффективен, чем заголовок IPv4, поскольку имеет фиксированную длину (с расширениями) и имеет только несколько полей. Заголовок IPv6 состоит из 40 байт, которые использует следующим образом: 32 байта для адресов IPv6 источника и получателя и 8 байт для полей

версии протокола, класса трафика, метки потока, длины полезной нагрузки, наличия дополнительного заголовка и ограничения количества переходов.

Больше не тратится время на проверку контрольной суммы, и не нужно включать длину заголовка IP, поскольку в IPv6 она всегда имеет фиксированную длину.

Улучшенная безопасность. IPv6 имеет встроенную защиту. Защита протокола IP (IPsec) — это компонент, который мы используем сегодня для аутентификации и шифрования, создания защищенных туннелей от источника до пункта назначения. Это может быть туннель от клиента к серверу или между шлюзами. IPv4 позволяет нам это делать, улучшая функциональность IP-заголовка (в основном добавляя второй IP-заголовок при шифровании всего за ним). В IPv6 это добавлено, как стандартная функциональность, с использованием заголовков расширений.

Передача IPv4-to-IPv6. В IPv6 существует несколько механизмов, облегчающих переход IPv4 в IPv6:

Новые методы вещания. Три типа пакетов, используемых в IPv6, являются индивидуальными, групповыми и произвольными (anycast). В отличие от IPv4, IPv6 не использует широковещательный адрес. Однако есть групповой IPv6-адрес для всех узлов, который дает аналогичный результат. IPv6 использует также новый функционал, который называется — обнаружение соседей. Для этого привлекается протокол ICMPv6, который помимо выполнения прежних задач начал использоваться протоколом обнаружения соседей.

Формат адреса IPv6

В формате IPv6-адреса есть несколько существенных изменений. Поэтому нам необходимо привыкнуть к его использованию и анализу. Существует три типа адресов, которые мы будем использовать, а также определенные знания, необходимые для работы с новым адресным пространством.

Для адресов IPv4 мы представляем адреса в виде октетов или точечно-десятичной форме. Четыре октета позволяют записать 32 битное двоичное число. IPv6 расширяет адресное пространство до 128 бит, а для представления используются только шестнадцатеричные цифры. Ниже приведен пример полного IPv6-адреса: 2001:0DB8:0000:0000:1234:0000:A9FE:133E.

Нули в начале каждого хексстета можно не записывать, поэтому мы можем написать наш адрес в виде — 2001:4860:0:0:12:10FF:FECD:EF. Кроме этого, можно использовать двойное двоеточие для сокращения непрерывной последовательности нулей, поэтому мы могли бы записать наш адрес в виде 2001:4860::12:10FF:FECD:EF. IPv6-адрес всегда имеет длину — 128 бит; поэтому, когда вы видите двойное двоеточие, это указание, которое говорит о том, что для того, чтобы получить исходное значение адреса, необходимо дополнить необходимое количество нулей между двоеточиями, чтобы получить адрес длиной 128 бит. У вас может быть только один набор двойных двоеточий; потому что в противном случае вы получите неопределенность по количеству нулей, сокращенных между каждым двойным двоеточием.

DNS обрабатывает адреса IPv6 с использованием записи AAAA. Запись A в пространстве адресов IPv4 составляет 32 бита, поэтому запись AAAA — 128 бит. DNS-сервер обрабатывает записи AAAA и указатели (PTR) для IPv6.

Существует три типа IPv6-адресов.

- **Индивидуальный (unicast):** служит для однозначного определения интерфейса на устройстве под управлением протокола IPv6.
- **Групповой (multicast):** используется для отправки одного IPv6-пакета на несколько адресов назначения.
- **Произвольный (anycast):** любой индивидуальный IPv6-адрес, который может быть назначен нескольким устройствам. Пакет, отправляемый на адрес произвольной рассылки, направляется к ближайшему устройству с этим адресом. Адреса Anycast на самом деле не новы. Концепция anycast существовала в IPv4, но широко не использовалась.

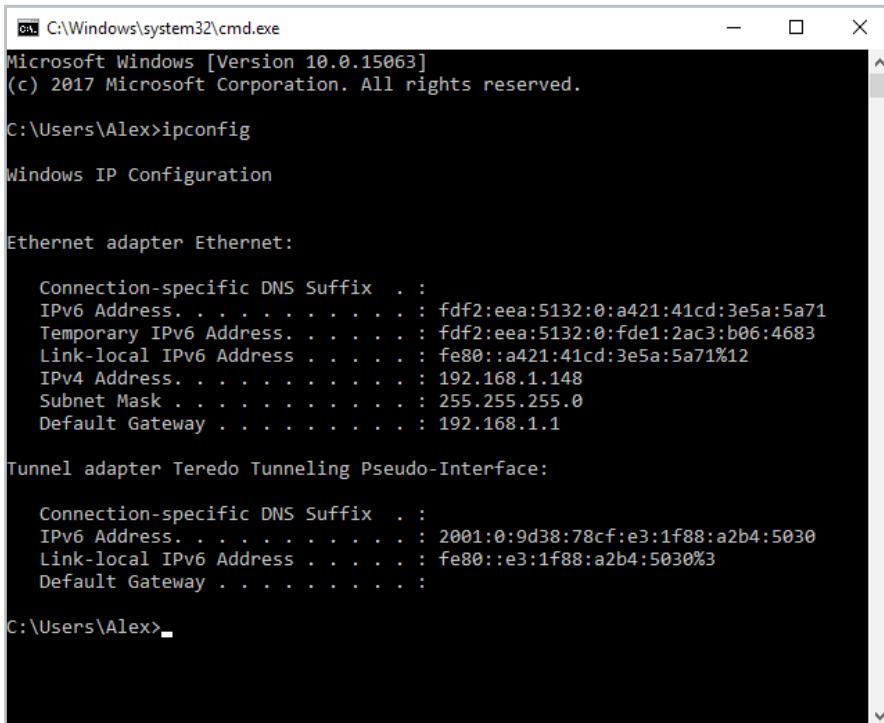
Существует несколько типов индивидуальных адресов:

- **Глобальный индивидуальный адрес (Global Unicast Address).** Глобальное адресное пространство одноадресной рассылки определяется как 2000::/3. 2001::/32 — адреса IPv6, выдаваемые коммерческим структурам. Microsoft был выделен блок адресов 2001:4898::/32. Большинство адресов, используемых в примерах, начинаются с 2001:DB8::/32; так как это пространство зарезервировано для документации.

Существуют специальные адреса и форматы адресов, которые вы увидите в процессе использования. Адрес loopback в IPv4 — 127.0.0.1. В IPv6 адрес loopback

равен ::1 (или 0:0:0:0:0:0:0001). При использовании двойного стека в Windows Server вы можете увидеть адрес в формате FE80::5EFE:192.168.1.200. Эта форма адреса используется в модели интеграции IPv6.

- **Локальный адрес канала (Link-Local Address).** Локальные адреса канала определяются как FE80::/10. Если вы посмотрите на вывод команды `ipconfig`, вы увидите локальный IPv6-адрес канала в виде FE80::a421:41cd:3e5a:5a71. Последние 8 байтов (64 бит) являются случайными, чтобы обеспечить высокую вероятность случайности для этого адреса.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Alex>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
IPv6 Address . . . . . : fdf2:eea:5132:0:a421:41cd:3e5a:5a71
Temporary IPv6 Address . . . . . : fdf2:eea:5132:0:fde1:2ac3:b06:4683
Link-local IPv6 Address . . . . . : fe80::a421:41cd:3e5a:5a71%12
IPv4 Address . . . . . : 192.168.1.148
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2001:0:9d38:78cf:e3:1f88:a2b4:5030
Link-local IPv6 Address . . . . . : fe80::e3:1f88:a2b4:5030%3
Default Gateway . . . . . :

C:\Users\Alex>
```

Рисунок 21

Локальные адреса канала должны использоваться только в пределах одного сегмента сети и пакет с таким адресом не маршрутизируется.

Существует другая форма локального IPv6-адреса канала, который называется 64-разрядным (EUI-64) расширенным интерфейсом пользователя. Этот адрес сформирован на основе MAC-адреса физического интерфейса и вставки последовательности FFFE между третьим и четвертым байтами MAC адреса. Первый байт также изменяет значение на 02, что позволяет установить универсальный/локальный бит равным 1, как определено в спецификации кадра IEEE 802. Для примера, адрес EUI-64 для физического (MAC) адреса 00-03-FF-11-02-CD будет выглядеть, как — FE80::0203:FFFF:FE11:02CD.

- **Анонимные адреса** (*AnonymousAddress*). Microsoft Server 2012 R2, 2016 использует случайное значение идентификатора хоста, вместо использования техники EUI-64. Случайное значение называется анонимным адресом. При необходимости он может быть изменен на адрес, полученный по алгоритму EUI-64.
- **Уникальный локальный адрес** (*Unique Local Address*). К уникальным локальным адресам относятся адреса из диапазона FC00::/7 — FDFF::7 и используются как приватные адреса аналогично IPv4. Уникальные локальные адреса описаны в RFC 4193. Они, как ожидается, не будут маршрутизоваться в глобальном Интернете. Они маршрутизируются внутри ограниченной области, такой как сайт. Они также могут быть маршрутизированы между ограниченным набором сайтов.

- **Групповые адреса.** (*Multicast Address*) Адреса для связи «один ко многим». Пакеты многоадресной рассылки идентифицируются по их первому байту (самый старший байт, крайний левый байт, крайние левые 2 полу-байта, самые левые 8 бит и т.д.). Адрес многоадресной рассылки определяется как FF00::/8.

Существует несколько зарезервированных групповых адресов. Например, если вы хотите отправить пакет всем узлам в области локальной сети, вы отправляете пакет на адрес FF02::1. Групповой адрес для всех маршрутизаторов — FF02::2.

Групповая рассылка также используется для получения MAC-адреса устройства, с которым мы пытаемся связаться. Вместо использования ARP-механизма IPv4, IPv6 использует сообщения ICMPv6 для поиска соседей (NS) и ответа от соседа (NA). Сообщения NS и NA ICMPv6 являются частью нового протокола обнаружения соседей (NDP).

В таблице описаны известные префиксы адресного пространства IPv6 и некоторые известные адреса.

Префикс	Назначение
2000:: /3	Global unicast space prefix
FE80:: /10	Local link address prefix
FC00:: /7	Unique local unicast prefix
FF00:: /8	Multicast prefix
2001:DB8:: /32	Global unicast prefix used for documentation
::1	Reserved local loopback address
2001:0000: /32	Teredo prefix*
2002:: /16	6to4 prefix*

Настройка TCP/IPv4 в Windows 10

Windows 10 может использовать IPv4 или IPv6 для связи с другими компьютерами в сети, но компьютер под управлением Windows 10 должен каким-то образом получить IP-адрес. Существует два способа, при помощи которых Windows 10 может получить IP-адрес: статически или динамически.

Статическая конфигурация

Как администратор вы можете вручную настроить компьютер Windows 10 (статическая конфигурация). Для этого вы должны знать следующее:

- Какой IP-адрес необходимо назначить?
- Какая маска подсети используется в данной сети?
- Какой адрес шлюза по умолчанию (адрес маршрутизатора)?
- Какой адреса DNS-сервера?

Динамическая конфигурация

Динамическая конфигурация IP предполагает, что у вас есть DHCP-сервер в вашей сети, доступный клиентам DHCP. DHCP-серверы настроены так, чтобы автоматически предоставлять DHCP-клиентам всю информацию о своей IP-конфигурации, включая IP-адрес, маску подсети, адрес шлюза и адрес DNS-сервера.

Для больших сетей, DHCP — это самый простой и надежный способ управления конфигурациями IP. По умолчанию компьютер Windows 10 настроен как клиент DHCP для динамической конфигурации IP.

Если вы используете DHCP и при этом не подключаетесь к другим компьютерам должным образом, вы можете ввести команду `ipconfig /all` в командной строке, чтобы узнать, какой IP-адрес получен.

Если ваш IP адрес начинается с 169.254.x.x, вы не подключились к серверу DHCP. Вместо этого на вашем компьютере с Windows 10 используется APIPA.

Понятие APIPA

Автоматическая приватная IP-адресация (APIPA) используется для автоматического назначения частных IP-адресов для домашних или небольших бизнес-сетях, которые содержат одну подсеть, не имеют DHCP-сервера и не используют статическую IP-адресацию. Если APIPA используется, клиенты смогут общаться только с другими клиентами в той же подсети, которые также используют APIPA. Преимущество использования APIPA в небольших сетях заключается в том, что он не требует настройки и поэтому имеет меньше шансов на ошибки конфигурации, чем статическое назначение IP-адресов.

APIPA используется с Windows 10 при следующих условиях:

- Когда компьютер настроен как клиент DHCP, но DHCP-сервер недоступен для обслуживания запросов от клиентов DHCP
- Когда клиент изначально получил аренду DHCP с сервера DHCP, но когда клиент попытался продлить аренду DHCP, сервер DHCP был недоступен и срок аренды истек

APIPA использует сетевое адресное пространство класса B, зарезервированное для его использования.

Адресное пространство — это сеть 169.254.0.0, где для хоста назначается диапазон 169.254.0.1-169.254.255.254.

APIPA работает следующим образом:

1. Клиент Windows 10 отправляет запрос DHCP-серверу(ам) для получения конфигурационных настроек, но DHCP-серверы не отвечают.
2. Клиент Windows 10 выбирает случайный адрес из диапазона адресов 169.254.0.1-169.254.255.254 и использует маску подсети 255.255.0.0.
3. Клиент использует метод повторного обнаружения адресов, чтобы убедиться, что выбранный адрес не используется в сети.
4. Если адрес уже используется, клиент повторяет шаги 1 и 2. Если адрес еще не используется, клиент настраивает своим сетевом интерфейсе этот адрес, выбранный им случайным образом. Учитывая диапазон адресов, из которых клиент APIPA может выбрать себе адрес (65 534 адресов), шансы выбора дубликата очень низкие.
5. Клиент Windows 10 продолжает поиск DHCP-сервера каждые пять минут. Если DHCP-сервер отвечает на запрос, конфигурация APIPA удаляется, и клиент получает новые параметры IP конфигурации от сервера DHCP.

Тестирование сетевой конфигурации

После того, как вы установили и настроили параметры TCP/IP, вы можете проверить конфигурацию IP с помощью команд `ipconfig`, `ping` и `nbtstat`. Эти команды будут полезны при устранении ошибок конфигурации

IP. Вы также можете графически просмотреть сведения о подключении через раздел «Состояние подключения к локальной сети» в Центре управления сетями и общим доступом.

Использование команды ipconfig

Команда ipconfig отображает вашу IP-конфигурацию. В таблице перечислены параметры, которые можно использовать с командой ipconfig.

Параметр	Описание
/?	Показывает все параметры справки для ipconfig
/all	Показывает подробные сведения о вашей конфигурации IP, включая физический адрес вашего компьютера, используемый вами DNS-сервер и используете ли вы DHCP
/allcompartments	Показывает информацию IP для всех подразделений
/release	Освобождает IPv4-адрес, назначенный через DHCP
/release6	Освобождает IPv6-адрес, назначенный через DHCP
/renew	Обновляет IPv4-адрес через DHCP
/renew6	Обновляет IPv6-адрес через DHCP
/flushdns	Очищает кеш DNS
/registerdns	Обновляет аренду DHCP и повторно регистрирует DNS-имена
/displaydns	Отображает содержимое кэша DNS
/showclassid	Перечисляет идентификаторы классов DHCP, разрешенные компьютером
/setclassID	Позволяет изменить идентификатор класса DHCP

Использование других команд TCP/IP

Вы можете использовать многочисленные команды для просмотра, проверки и настройки сетевых параметров Windows 10. В частности, вы можете использовать утилиту `netsh`, утилиту `route`, а также стандартные утилиты `ping` и `tracert`. В лабораторной работе будут рассмотрены примеры использования этих утилит.

Устранение неполадок TCP / IP

Если у вас возникли проблемы с подключением к сетевым ресурсам, проверьте в первую очередь:

- Если вы можете получить доступ к ресурсам в своей локальной подсети, но не можете подключиться к удаленной подсети, проверьте настройки шлюза по умолчанию на вашем компьютере. Получение сообщения `Destination Unreachable` при выполнении команды `ping` также говорит о неправильной конфигурации шлюза по умолчанию.
- Если вы можете получить доступ к некоторым, но не ко всем устройствам в своей локальной подсети или удаленной подсети, вы должны проверить настройки маски подсети, кабели к этим устройствам или состояние межсетевых устройств между вашим компьютером и этими устройствами.
- Используйте утилиту `ipconfig`, чтобы убедиться, что вы не получили адрес APIPA. Если да, попробуйте определить, почему вы не получаете настройки IP-адреса с вашего DHCP-сервера.
- Если вы можете получить доступ к устройству (например, путем выполнения утилиты `ping` к этому компьютеру)

по IP-адресу, но не по имени, проверьте настройки DNS на своем компьютере.

Настройка Windows 10 в сети

В крупных корпоративных сетях клиентские компьютеры под управлением Windows 10 будут подключены к доменной среде. Использование Windows 10 как клиента домена дает много преимуществ для администрирования:

- Вы можете развернуть объекты групповой политики из одного места вместо LGPO на каждом компьютере.
- Пользователи могут хранить свои данные на сервере. Таким образом, резервные копии будут также включать информацию пользователя.
- Вы можете управлять пользователями и группами из одного центра (Active Directory), а не на каждом компьютере Windows 10.
- Вы можете управлять безопасностью ресурсов на серверах, а не на каждом компьютере индивидуально.

Другой тип сети, который вам, возможно, придется настроить в Windows 10, — это Домашняя группа (HomeGroup). Домашняя группа позволяет легко подключать два или более компьютеров под управлением Windows 10 в домашней сети. Windows 10 после подключения к сети ищет существующую домашнюю группу, и, если она найдена, подключается к ней после ввода пароля. Если домашняя группа не найдена, мастер создания сети автоматически создает пароль для HomeGroup. Этот пароль позволяет подключать все другие компьютеры к одной и той же сети, и его можно изменить в любое время после установки Windows 10.

Добавление Windows 10 в домен и в домашнюю группу будет рассмотрено в соответствующих лабораторных работах. Ниже (рис. 22) показана последовательность смены имени компьютера и присоединения его к домену.

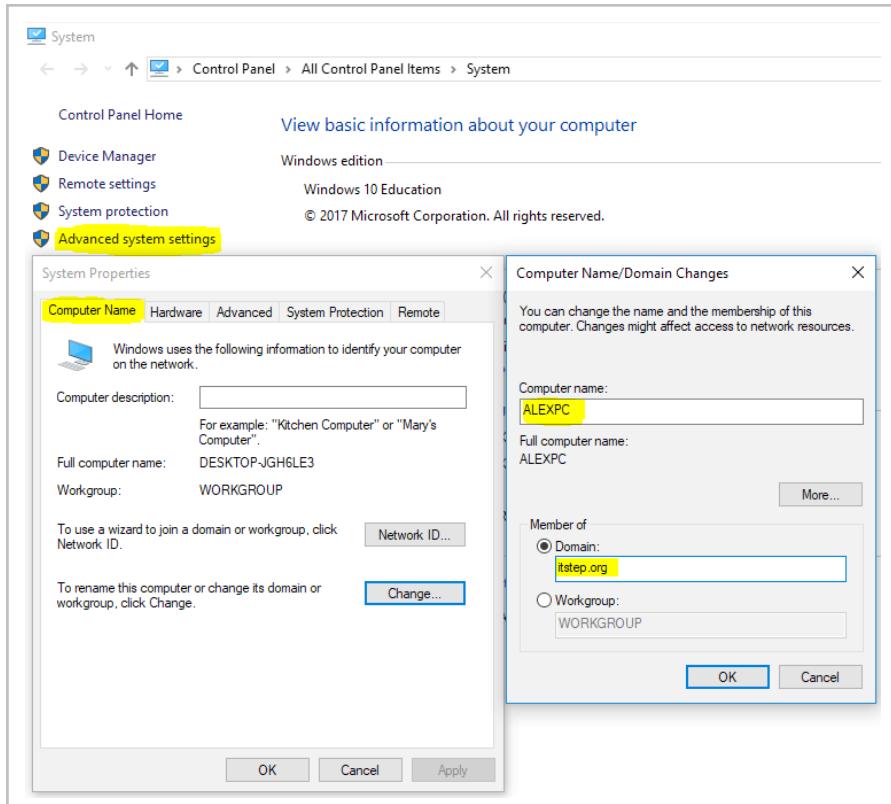


Рисунок 22

Настройка брандмауэра Windows

Брандмауэр Windows, входящий в состав Windows 10, помогает предотвратить сетевой доступ неавторизованных пользователей или вредоносных программ

к вашему компьютеру. Брандмауэр Windows запрещает любой неизвестный трафик, правила прохождения для которого не были определены

Общие сведения о брандмауэре Windows

Для настройки брандмауэра воспользуйтесь одноименным элементом в панели управления. Тут вы можете решить, какие параметры брандмауэра вы хотите установить (как показано на рисунке), например, изменение уведомлений брандмауэра, включение или выключение брандмауэра, восстановление настроек по умолчанию, настройка дополнительных параметров и устранение неполадок.

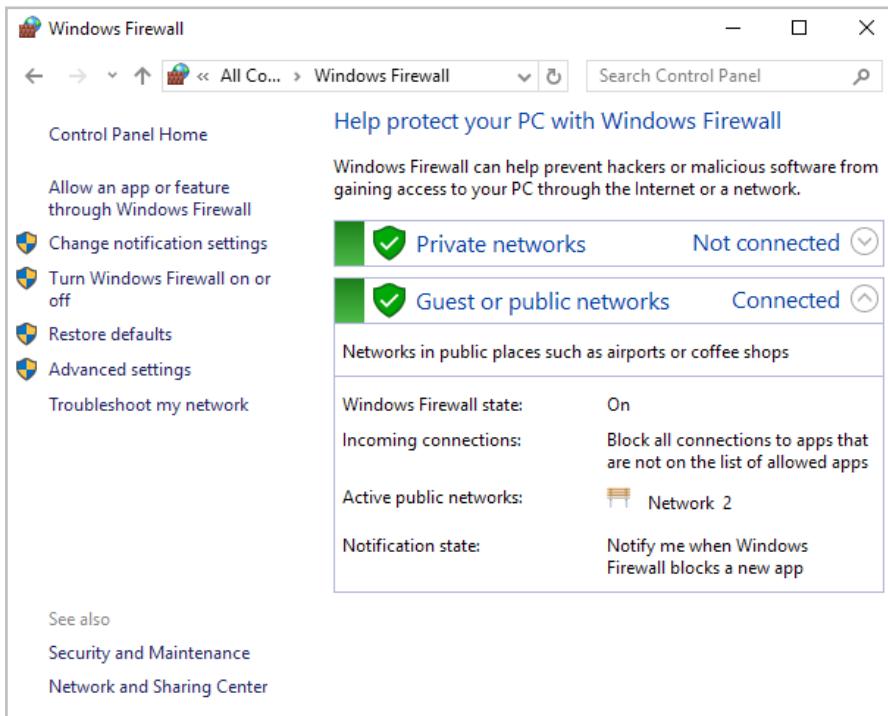


Рисунок 23

Диалоговое окно «Параметры брандмауэра Windows» позволяет включать и выключать брандмауэр Windows для частных и общедоступных сетей. Параметр «Включить» (Turn On) блокирует входящие подключения, а параметр «Отключить» (Turn Off) позволяет разрешить входящие подключения.

Существует также флагок «Блокировать все входящие соединения». Эта функция позволяет подключаться к сетям, которые не защищены. Когда включена блокировка всех входящих подключений, все входящие соединения (даже разрешенные в списке разрешенных приложений) будут заблокированы брандмауэром Windows.

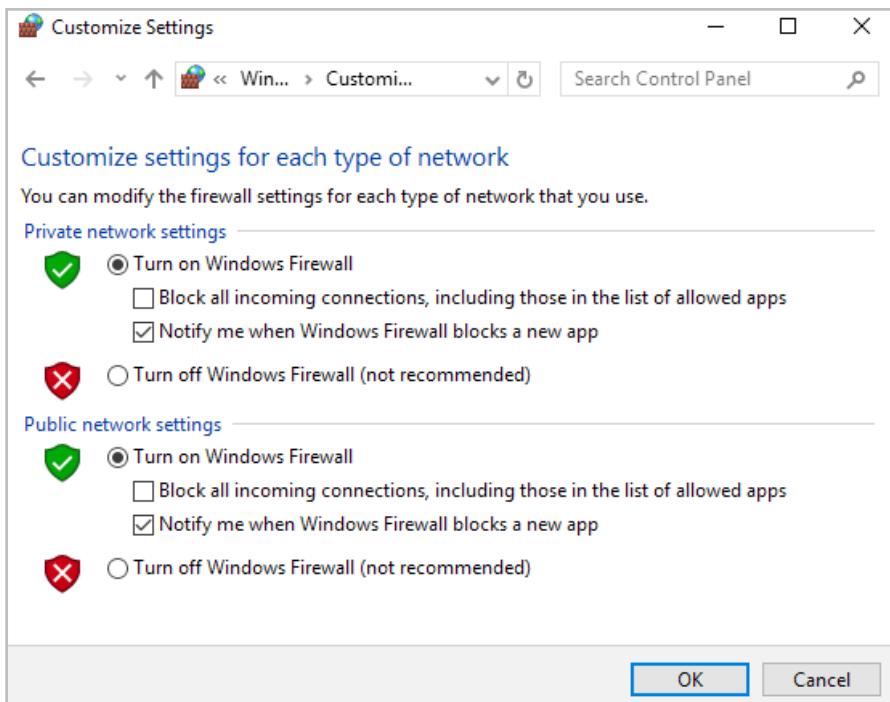


Рисунок 24

Брандмауэр Windows с расширенной безопасностью

Вы можете установить дополнительные параметры, настроив брандмауэр Windows в режиме повышенной безопасности (WFAS). Для этого на главном окне управления брандмауэром выберите пункт «Дополнительные параметры» (Advanced settings). Появится диалоговое окно «Брандмауэр Windows с расширенной безопасностью», как показано на рисунке 25.

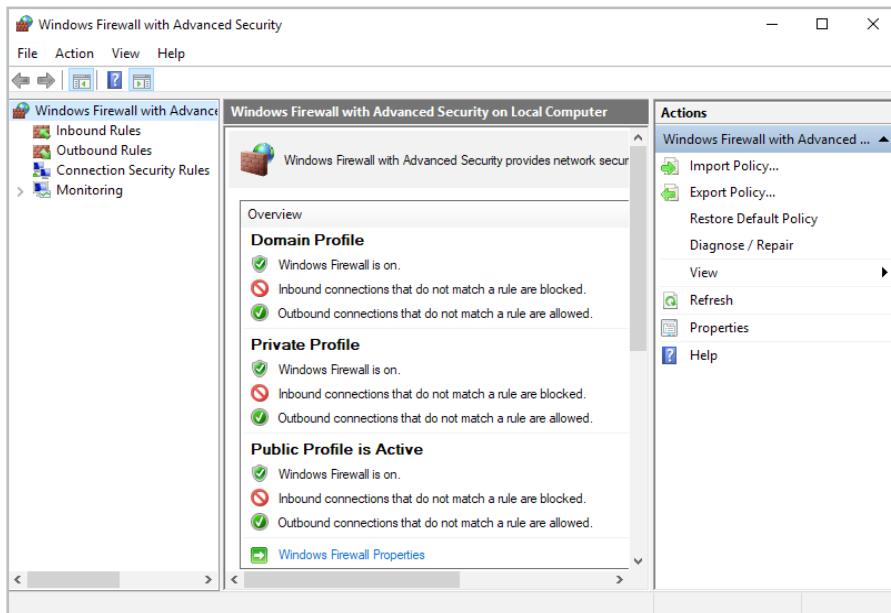


Рисунок 25

Область слева показывает, что вы можете настроить определенные правила входящего и исходящего трафика, правила безопасности подключения и правила мониторинга. Центральная область показывает состояние брандмауэра, когда на левой панели не выбрано правило.

Когда правило выбрано, центральная область показывает настройки правила. На правой панели отображаются те же действия, что и в меню «Действие» вверху. Это просто ярлыки для различных действий, которые могут быть выполнены в брандмауэре Windows. Давайте подробнее рассмотрим некоторые элементы в брандмауэре Windows.

Входящие и исходящие правила

Входящие и исходящие правила состоят из многих предварительно сконфигурированных правил, которые могут быть включены или отключены. Очевидно, что входящие правила (см. Рис. 26) контролируют входящий трафик, а исходящие правила контролируют исходящий трафик. По умолчанию многие из них отключены.

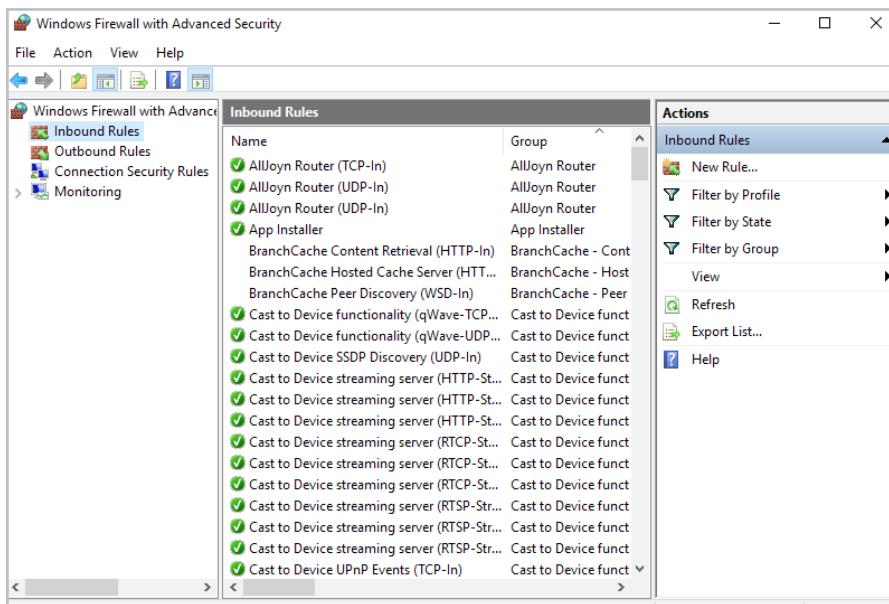


Рисунок 26

При двойном щелчке по правилу открывается диалоговое окно «Свойства» (рис. 27).

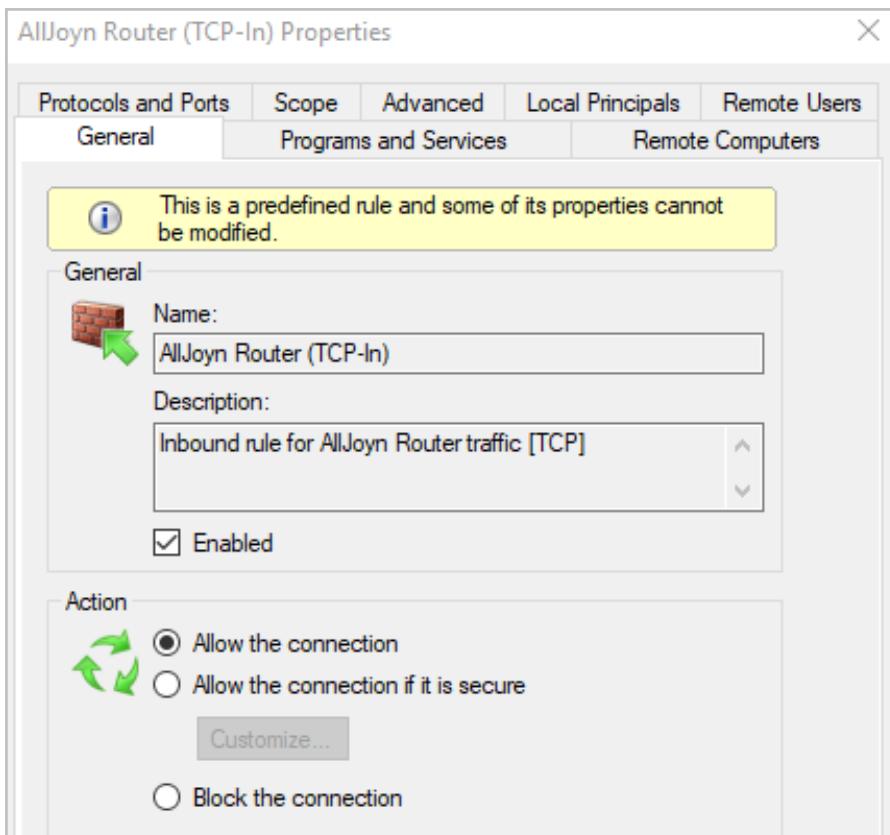


Рисунок 27

Вы можете фильтровать правила, чтобы упростить их просмотр. Фильтрация может быть по профилю, по состоянию, или по группе. Вы можете отфильтровать правило, указав, какой тип фильтра вы хотите использовать в правой панели, или выбрав фильтр в меню «Действия» в верхней части экрана.

Если вы не можете найти правило, соответствующее вашим потребностям, вы можете создать новое правило, выбрав правой кнопкой мыши «Входящие правила» или «Исходящие правила» в области видимости, а затем указав «Новое правило». Будет запущен мастер создания правил для нового входящего (или исходящего) правила, и вас спросят, хотите ли вы создать правило на основе определенной программы, протокола или порта, предопределенной категории или пользовательских настроек.

Когда вы настраиваете правила брандмауэра, вы можете настроить аутентифицированные исключения. Важно понимать, что при настройке этих аутентифицированных исключений вы снижаете безопасность сети. Поэтому убедитесь, что компьютеры, которые добавлены в список исключений, являются доверенными.

Ниже в таблице показаны некоторые из наиболее распространенных номеров портов и номера этих портов.

Порт	Приложение или служба
20	FTP Data
21	FTP Control
22	Secure Shell (SSH)
23	Telnet
25	SMTP
53	DNS
67/68	DHCP/BOOTP
80	HTTP
102	Microsoft Exchange Server
110	POP3
443	HTTPS (HTTP with SSL)

Правила безопасности подключения

Правила безопасности подключения используются для настройки того, как и когда происходит аутентификация. Эти правила сами по себе не разрешают подключения; они работают совместно с правилами для входящих и исходящих подключений. Вы можете настроить следующие правила безопасности подключения:

- **Изоляция (Isolation).** Чтобы ограничить соединение на основе критериев аутентификации
- **Освобождение от аутентификации (Authentication Exemption).** Чтобы указать компьютеры, для которых не требуется аутентификация.
- **Сервер-сервер (Server-to-Server):** проверка подлинности соединений между компьютерами
- **Туннель (Tunnel):** для проверки подлинности соединений между компьютерами, выполняющими роль шлюза.
- **Собственный (Custom).**
- **Мониторинг.**

Раздел «Мониторинг» показывает подробную информацию о настройках брандмауэра для параметров профиля домена, частного профиля и общего профиля. Эти профили сети определяют, какие параметры применяются для частных сетей, общедоступных сетей и сетей, подключенных к домену.

Учетные записи пользователей

При установке Windows 10 автоматически создается несколько учетных записей пользователей. Кроме того, вы можете создавать новые учетные записи пользователей. Как вы уже знаете, учетные записи на компьютерах позволяют пользователю входить в систему и получать доступ к ресурсам.

Вы можете создавать локальные учетные записи пользователей, которые находятся локально на компьютере под управлением Windows 10. Такие учетные записи не могут использоваться для доступа к любым ресурсам, размещенным в сети. Если вы установили Active Directory в облаке (*Azure Active Directory*) или в сети с контроллером домена Windows Server, ваша сеть может иметь учетные записи пользователей домена.

Ниже мы рассмотрим различные типы учетных записей: учетные записи пользователей по умолчанию, создаваемые Windows 10, и рассмотрим различия между локальными и доменными учетными записями пользователей.

Типы учетных записей

Windows 10 поддерживает два основных типа учетных записей пользователей: администратор и стандартный пользователь (см. Рис 28). Каждая из этих учетных записей используется по определенным причинам.

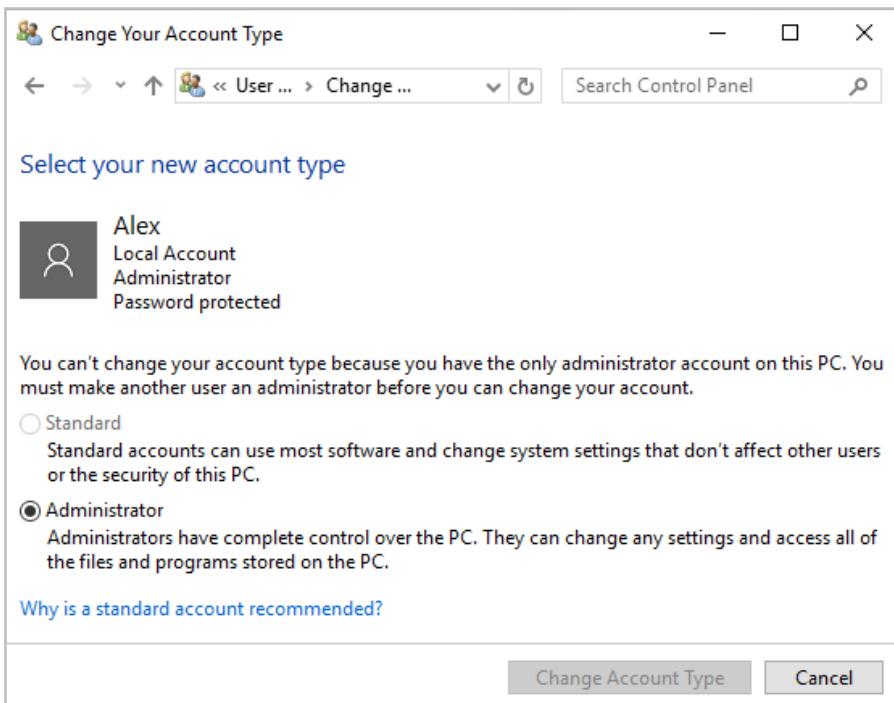


Рисунок 28

Администратор. Тип учетной записи администратора предоставляет неограниченный доступ для выполнения административных задач. В результате учетные записи администратора должны использоваться только для выполнения административных задач и не должны использоваться для решения обычных прикладных и вычислительных задач.

Только из-под учетной записи администратора можно изменить реестр. Когда происходит установка различного ПО на компьютер, реестр изменяется. Поэтому нам нужны права администратора для установки большинства программ.

Стандартный пользователь. Стандартный тип учетной записи пользователя должен назначаться каждому пользователю компьютера. Стандартные учетные записи пользователей могут выполнять большинство повседневных задач, таких как запуск Microsoft Word, доступ к электронной почте, использование Internet Explorer и т.д. Вход в систему в качестве стандартного пользователя повышает безопасность, ограничивая возможность заражения компьютера вирусом или другим вредоносным кодом. Стандартные учетные записи пользователей не могут выполнять общесистемные изменения, что также помогает повысить безопасность.

Когда вы устанавливаете Windows 10, по умолчанию создается несколько учетных записей, называемых встроенными учетными записями.

Встроенные учетные записи

Windows 10 (при условии, что компьютер входит в рабочую группу) имеет три встроенных учетных записи, которые создаются автоматически во время установки операционной системы. На рис. 29 также показаны учетные записи, которые были созданы дополнительно.

Администратор (Administrator). Учетная запись администратора — это специальная учетная запись, которая имеет полный контроль над компьютером. Учетная запись администратора может выполнять все задачи, такие как создание пользователей и групп, управление файловой системой, установка приложений и настройка печати. Обратите внимание, что учетная запись администратора по умолчанию отключена.

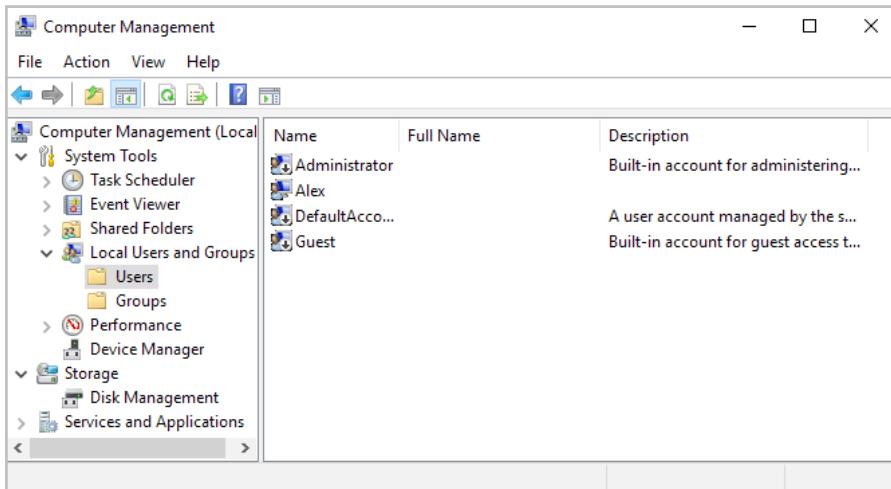


Рисунок 29

DefaultAccount. Это учетная запись пользователя, созданная системой и используемая системой. Эта учетная запись является членом группы **HomeUsers** и группы **System Managed Accounts**.

Гость (Guest). Учетная запись гостя позволяет пользователям получить доступ к компьютеру, даже если у человека нет уникального имени пользователя и пароля. Из-за собственных рисков безопасности, связанных с этим типом пользователя, учетная запись гостя отключена по умолчанию. Когда эта учетная запись включена, она обычно получает очень ограниченные привилегии.

HomeGroupUser\$. Учетная запись **HomeGroupUser\$** создается по умолчанию, чтобы позволить этому компьютеру подключаться к другим в пределах одной сети **HomeGroup**. Эта учетная запись создается по умолчанию,

как только вы настраиваете HomeGroup. Так как домашняя группа в нашем случае еще не создавалась, данная учетная запись отсутствует.

Начальный пользователь (*Initial User*) Учетную запись, которую вы создаете сами во время установки ОС. В нашем случае это учетная запись [Alex](#) По умолчанию начальный пользователь является членом группы «Администраторы».

Все эти пользователи считаются локальными пользователями, и их разрешения содержатся на локальном компьютере. Если учетной записи пользователя требуется доступ к ресурсам на других компьютерах, вы можете подключиться к компьютеру под управлением Windows 10 в качестве удаленного пользователя.

Учетные записи локальных и доменных учетных записей

Windows 10 поддерживает два типа пользователей: локальные пользователи и пользователи домена. Локальные пользователи настраиваются на каждой клиентской системе Windows 10. Windows 10 может быть частью рабочей группы или может быть автономной системой. Компьютер под управлением Windows 10 имеет возможность хранить собственную базу данных учетных записей пользователей. Учетные записи, хранящиеся на локальном компьютере, известны как локальные учетные записи пользователей.

Рабочие группы — это сети, которые имеют пользовательские базы данных на каждом отдельном компьютере. Однако вы можете совместно использовать ресурсы в сети рабочих групп.

Домены — это сети, где имеется централизованная база данных безопасности (*Active Directory*), и вы можете контролировать всех своих пользователей и группы из одного центра.

Active Directory — это служба каталогов, которая хранит информацию в центральной базе данных, которая позволяет пользователям иметь одну учетную запись пользователя для сети. Учетные записи пользователей, хранящиеся в центральной базе данных Active Directory, называются учетными записями пользователей домена.

Вы можете выполнить локальный вход на компьютер под управлением Windows 10, используя локально сохраненную учетную запись пользователя, или вы можете войти в домен, используя учетную запись Active Directory. Когда вы устанавливаете Windows 10 на компьютере, вы указываете, что компьютер будет частью рабочей группы, что подразумевает локальный вход в систему или что он будет частью домена, что подразумевает вход в домен.

Работа с учетными записями пользователей

Чтобы настроить и управлять локальными учетными записями пользователей, используется оснастка «[Локальные пользователи и группы](#)» или утилита «[Учетные записи пользователей](#)» на панели управления. С помощью любого из предложенных вариантов вы можете создавать, отключать, удалять и переименовывать учетные записи пользователей, а также изменять пароли пользователей.

Windows 10 включает в себя контроль учетных записей пользователей (UAC), который обеспечивает дополнительный уровень безопасности, ограничивая уровень доступа,

который пользователи имеют при выполнении обычных повседневных задач. При необходимости пользователи могут получить повышение уровня доступа для решения конкретных административных задач.

Использование оснастки «Локальные пользователи и группы»

Существует два распространенных метода доступа к утилите «Локальные пользователи и группы»:

- Запуск оснастки «Локальные пользователи и группы» в качестве оснастки ММС.
- Запуск оснастки «Локальные пользователи и группы» с помощью оснастки «Управление компьютером».

Самый быстрый способ доступа к оснастке «Локальные пользователи и группы» — через «Управление компьютером».

Использование утилиты «Учетные записи пользователей» в панели управления

Альтернативный способ управления локальными пользователями — с помощью одноименной утилиты панели управления, которая обеспечивает возможность управления учетными записями пользователей в дополнение к настройке родительского контроля. Чтобы открыть утилиту — откройте панель управления и выберите элемент «Учетные записи пользователей».

Создание новых пользователей

Чтобы создать пользователей на компьютере под управлением Windows 10, вы должны войти в систему

как пользователь с разрешением на создание нового пользователя, что означает, что ваша учетная запись должна быть членом группы «Администраторы».

Когда вы создаете нового пользователя, существует множество параметров, которые вы должны настроить. Более подробно процесс создания учетных записей несколькими способами (включая использование консольной команды net user) будет рассмотрен в лабораторной работе.

Правила и соглашения, используемые при создании нового пользователя.

Единственное реальное требование для создания нового пользователя — предоставить действительное имя пользователя. Чтобы быть действительным, имя должно соответствовать правилам Windows 10 для имен пользователей. Тем не менее, также неплохо иметь свои собственные правила для формирования имен пользователей.

Ниже приведены правила Windows 10 для имен пользователей:

- Имя пользователя должно быть от 1 до 20 символов.
- Имя пользователя должно быть уникальным среди всех других имен пользователей и групп, хранящихся на компьютере.
- Имя пользователя не может содержать ни один из следующих символов: / \ [] ; | =, +? <> "@"
- Имя пользователя не может состоять исключительно из пробелов.

Соблюдая правила Windows 10, вы должны выбрать соглашение об именах (согласованный формат именования) для вашей компании. Например, ваше соглашение об именах

может состоять в том, чтобы использовать имя и первую букву фамилии, поэтому для пользователя с именем Vasya Pupkin имя пользователя будет VasP или VasyaP. В другом соглашении об именах может использоваться первая буква имени и фамилия, тогда получаем VPupkin. Это соглашение об именах, которому следуют многие средние и крупные организации. Вы можете использовать имена пользователей в соглашении об именах, которое ваша компания определила для имен электронной почты, чтобы имя входа и имя в адресе электронной почты совпадали.

Вы также должны предоставить механизм, который будет предусматривать создание похожих имен. Например, если у вас есть пользователь по имени Vasya Pupkin и пользователь Vitya Pupkin, вы можете использовать первую букву отчества для формирования имени пользователей, таких как VA Pupkin и VB Pupkin. Также хорошей практикой является придумать соглашение об именах для групп, принтеров и компьютеров.

При создании пользователей важно убедиться, что ваши пароли имеют высокий уровень сложности. Причина, по которой вам нужна надежная защита, заключается в том, что когда пользователь входит в систему, учетные данные пользователя помещаются в память процесса подсистемы локальной безопасности (LSASS) компьютера. Это делается для того, чтобы учетные данные могли использоваться данным пользователем во время сеанса работы.

Учетные данные также будут храниться в авторитетных базах данных Windows 10, таких как база данных SAM и в базе данных, которая используется доменными службами Active Directory (AD DS).

Идентификаторы безопасности

Когда вы создаете новую учетную запись пользователя, для неё автоматически создается идентификатор безопасности (SID). Имя пользователя является исходными данными для формирования SID. Например, SID пользователя может выглядеть так:

S-1-5-21-823518204-746137067-120266-629-500.

Очевидно, что использование SID для идентификации пользователя сделало бы администрирование кошмаром. К счастью, для ваших административных задач вы видите и используете имя пользователя вместо SID.

У SID есть несколько преимуществ. Поскольку Windows 10 использует SID как основной идентификатор пользователя, вы можете легко переименовать пользователя, сохраняя все его свойства. Все настройки безопасности связаны с SID, а не с учетной записью пользователя. Каждый раз, когда вы создаете нового пользователя, создается новый уникальный SID. Это гарантирует, что если вы удалите и заново создадите учетную запись пользователя с тем же именем пользователя, новая учетная запись не будет иметь никаких свойств старой учетной записи, поскольку она основана на новом уникальном SID. Даже если имя пользователя совпадает с ранее удаленной учетной записью, система все равно будет считать ее новым пользователем.

Поскольку каждая учетная запись пользователя получает уникальный номер SID, рекомендуется отключать, а не удалять учетные записи пользователей, которые покидают компанию или длительно отсутствуют. Если

вам вдруг понадобится доступ к отключенной учетной записи, у вас есть возможность сделать это.

Отключение учетных записей пользователей

Если учетная запись пользователя больше не нужна, она должна быть отключена или удалена. После того, как вы отключили учетную запись, вы можете впоследствии ее повторно использовать, чтобы восстановить ее со всеми связанными с ней свойствами пользователя. Однако удаляемая учетная запись никогда не может быть восстановлена, если вы не выполните восстановление из ранее сделанной резервной копии.

Вы можете отключить учетную запись, потому что пользователь не будет использовать ее в течение определенного периода времени, возможно, потому, что этот сотрудник отправляется в отпуск или длительную командировку. Другой причиной отключения учетной записи является то, что вы планируете использовать другого пользователя на этой должности и хотите повторно использовать эту учетную запись.

Отключение учетных записей также обеспечивает механизм безопасности для особых ситуаций. Например, если ваша компания увольняет группу людей, в качестве меры безопасности вы можете отключить их учетные записи одновременно с выдачей уведомлений об увольнении. Это помешает этим пользователям нанести ущерб файлам компании после получения уведомления об увольнении.

Когда пользователь покинул компанию на длительный период времени, и вы знаете, что вам больше не нужна учетная запись этого пользователя, вы можете ее

удалить. Давайте посмотрим, как удалить учетные записи пользователей.

Удаление учетных записей пользователей

Как отмечено в предыдущем разделе, вы должны отключить учетную запись пользователя, если нет уверенности в том, что она точно не понадобится. Но если учетная запись была отключена, и вы знаете, что она никогда не понадобится снова, вы можете удалить учетную запись.

Чтобы удалить пользователя, откройте оснастку «Локальные пользователи и группы», выделите учетную запись пользователя, которую вы хотите удалить, откройте контекстное меню, показанное на рисунке, и выберите «Удалить» (Delete). Вы также можете удалить учетную запись, выделив учетную запись и нажав клавишу «Удалить» (Delete) на клавиатуре.

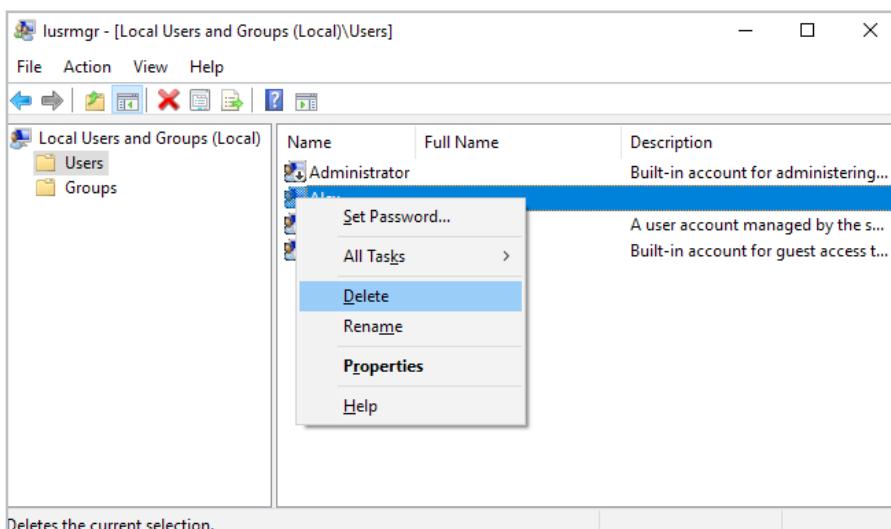


Рисунок 30

Поскольку удаление учетной записи является необратимым действием, вы увидите диалоговое окно, показанное на рисунке, с просьбой подтвердить, что вы действительно хотите удалить учетную запись. После нажатия кнопки «Да», вы не сможете повторно пересоздать или повторно получить доступ к этой учетной записи (если вы не восстановите базу данных локальных учетных записей пользователей из резервной копии).

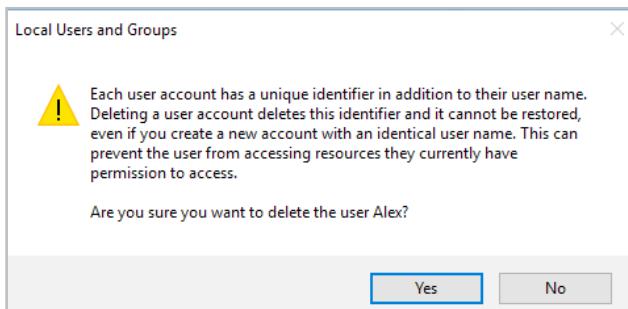


Рисунок 31

Переименование учетных записей пользователей

После создания учетной записи вы можете переименовать ее в любое время. Переименование учетной записи пользователя позволяет учетной записи сохранять все связанные с ней свойства пользователя, такие как членство в группах и назначенные разрешения, даже если имя пользователя изменяется.

Возможно, вы захотите переименовать учетную запись пользователя, потому что имя или фамилия пользователя изменились (например, пользователь выходит замуж) или потому, что имя было написано неправильно. Кроме того, как объясняется в разделе «[Отключение учетных записей](#)

пользователей», вы можете переименовать существующую учетную запись пользователя для нового пользователя, например, кого-то, нанятого на должность бывшего сотрудника, если вы хотите, чтобы новый пользователь имел те же свойства.

Изменение пароля пользователя

Что делать, если пользователь забудет свой пароль и не сможет войти в систему? В качестве администратора вы можете изменить пароль пользователя на любой другой, который они смогут использовать.

Очень важно, что ИТ-менеджеры и ИТ-администраторы обучаются наших пользователей надлежащим мерам безопасности, которые сочетаются с защитой пароля. Как вам, вероятно, доводилось видеть раньше, некоторые пользователи записывают свой пароль на стикер, который приклеивается к монитору или на бумажку, которая прячется под клавиатуру. Одна из наиболее важных наших задач, как ИТ-специалистов — научить наших пользователей надлежащей безопасности.

Управление пользовательскими свойствами

Для дополнительного контроля над учетными записями пользователей вы можете настроить свойства пользователя. В диалоговом окне «Свойства пользователя» вы можете изменить параметры исходного пароля, добавить пользователя в существующие группы и указать информацию о профиле пользователя.

Чтобы открыть диалоговое окно «Свойства пользователя», откройте оснастку «Локальные пользователи и группы»,

откройте папку «Пользователи» и откройте контекстное меню учетной записи пользователя. В диалоговом окне «Свойства пользователя» есть вкладки для трех основных категорий свойств: «Общие», «Членство» и «Профиль».

Вкладка «Общие» содержит информацию, предоставленную вами при настройке новой учетной записи пользователя, включая полное имя и описание, выбранные параметры пароля и отключен ли учетная запись. Если вы хотите изменить любое из этих свойств после создания пользователя, просто откройте диалоговое окно «Свойства пользователя» и внесите изменения на вкладке «Общие» (рис. 32).

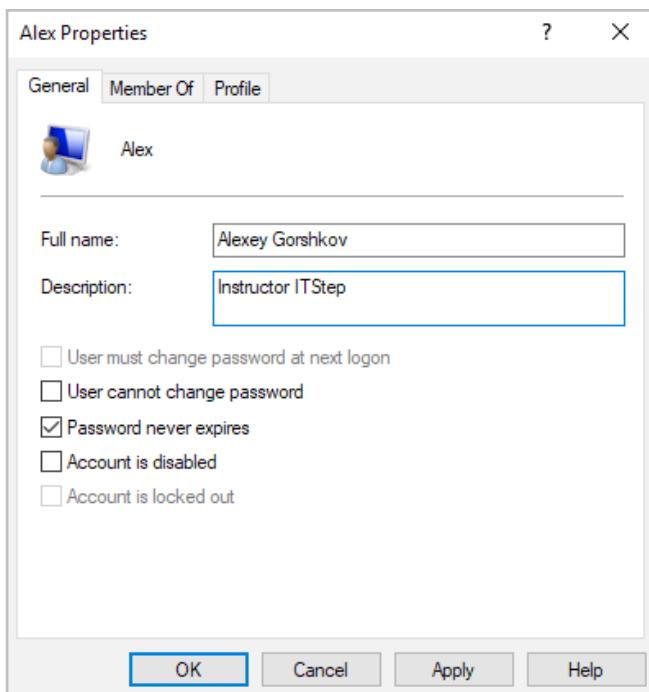


Рисунок 32

Вы можете использовать вкладку «Членство в группах» для управления членством пользователя в группах, а вкладка «Профиль» позволяет вам устанавливать свойства для настройки среды пользователя.

Управление членством в пользовательской группе

Вкладка «Членство...» диалогового окна «Свойства пользователя» отображает все группы, к которым принадлежит пользователь, как показано на рисунке. На этой вкладке вы можете добавить пользователя в существующую группу или удалить пользователя из группы. Чтобы добавить пользователя в группу, нажмите кнопку «Добавить» и выберите группу, к которой должен принадлежать пользователь. Если вы хотите удалить пользователя из группы, выделите группу и нажмите кнопку «Удалить».

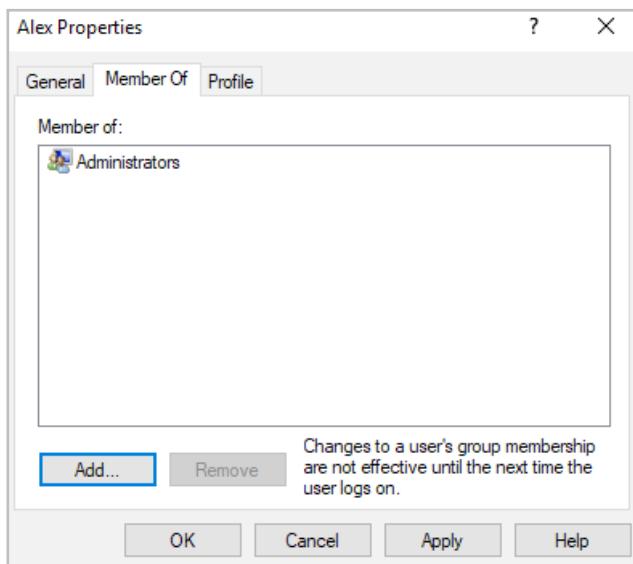


Рисунок 33

Настройка профилей пользователей, сценариев входа и домашних папок

Вкладка «Профиль» диалогового окна «Свойства пользователя», показанная на рис., позволяет настраивать среду пользователя. Здесь вы можете указать следующие элементы для пользователя:

- Путь к профилю пользователя.
- Сценарий входа в систему.
- Домашняя папка.

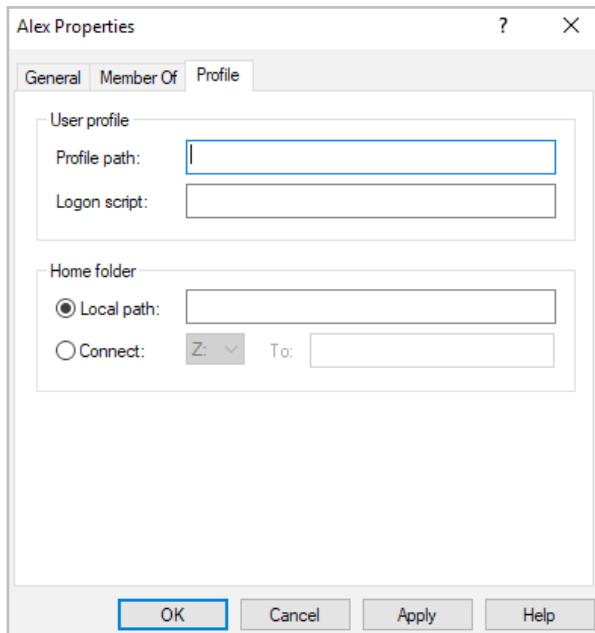


Рисунок 34

Настройка пути профиля пользователя

Профили пользователей содержат информацию о среде Windows 10 для конкретного пользователя. Например,

параметры профиля включают расположение рабочего стола, группы программ и цвета экрана, которые пользователь видит при входе в систему.

При каждом входе в систему на компьютере под управлением Windows 10 система проверяет наличие локального профиля пользователя в папке «Пользователи», которая была создана в загрузочном разделе при установке Windows 10. При первом входе в систему пользователи получают профиль пользователя по умолчанию. Папка, соответствующая имени входа пользователя, создается для пользователя в папке «Пользователи». Созданная папка профиля пользователя содержит файл NTUSER.DAT, а также вложенные папки, которые содержат ссылки каталога на пользовательские элементы рабочего стола.

Недостатком локальных профилей пользователей является то, что они доступны только на том компьютере, на котором они были созданы. Чтобы пользователи могли получать доступ к их профилю с любого компьютера, на котором они вошли в систему, вам нужно использовать перемещаемые профили; однако для этого требуется использование сетевого сервера, поскольку они не могут быть сохранены на локальном компьютере под управлением Windows 10.

Использование перемещаемых профилей

Перемещаемый профиль хранится на сетевом сервере и позволяет пользователю получать доступ к своему профилю независимо от клиентского компьютера, за которым он начал работать. Перемещаемые профили обеспечивают

постоянный рабочий стол для пользователей, которые работают за различными компьютерами, независимо от того, за каким компьютером они находятся. Даже если сервер, который хранит перемещаемый профиль, недоступен, пользователь все равно может войти в систему, используя локальный профиль.

Если вы используете перемещаемые профили, содержимое папки `userdirect` пользователя: `\Users\UserName` будет скопировано на локальный компьютер при каждом обращении к перемещаемому профилю. Если вы храните большие файлы в любых подпапках вашей папки профиля пользователя, вы можете заметить значительную задержку при удаленном доступе к своему профилю, а не локально. Если эта проблема возникает, вы можете уменьшить время загрузки перемещаемого профиля, перемещая подпапку в другое место, например домашний каталог пользователя, или вы можете использовать объекты групповой политики в Active Directory, чтобы указать, что определенные папки должны исключаться при загрузке перемещаемого профиля.

Использование обязательных профилей

Обязательный профиль — это профиль, который не может быть изменен пользователем. Только члены группы «Администраторы» могут управлять обязательными профилями. Вы можете создавать обязательные профили для одного пользователя или группы пользователей. Вы можете подумать о создании обязательных профилей для пользователей, которые должны поддерживать согласованные рабочие столы.

Например, предположим, что у вас есть группа из 20 продавцов, которые достаточно хорошо знают о конфигурации системы, чтобы внести изменения, но недостаточно, чтобы исправить любые проблемы, которые они создают. Для удобства поддержки вы можете использовать обязательные профили. Таким образом, все продавцы всегда будут иметь одинаковый профиль, который они не смогут изменить.

Обязательный профиль хранится в файле NTUSER.MAN. Чтобы создать обязательный профиль, вы просто изменяете расширение перемещаемого профиля пользователя на **.man**, и профиль станет обязательным. Пользователь с обязательным профилем может устанавливать разные настройки рабочего стола во время входа в систему, но эти настройки не будут сохранены при выходе пользователя из системы.

Существуют две папки, в которых хранятся профили. Это **Username** и **Username.v2**. Разница в том, что если вы используете Windows XP, профиль помещается в папку **Username**. Если пользователи используют Windows Vista, Windows 7/8/8.1, Windows 10 или Windows Server 2008/2016, профиль пользователя помещается в папку **Username.v2**.

Использование супер-обязательных профилей

Супер-обязательный профиль является обязательным профилем пользователя с дополнительным уровнем безопасности. С обязательными профилями создается временный профиль, если обязательный профиль недоступен, когда пользователь входит в систему. Однако

при настройке супер-обязательных профилей временные профили не создаются, если обязательный профиль недоступен по сети, пользователь не может войти в систему на компьютере.

Процесс создания супер-обязательных профилей аналогичен процессу создания обязательных профилей, за исключением того, что вместо переименования пользовательской папки **Username.v2**, как и для обязательного профиля, вы указываете папку **Username.man**. Профили пользователей становятся супер-обязательными, когда имя папки пути профиля заканчивается на **.man**, например — **\server\share\Alex.man**. Только системные администраторы могут вносить изменения в обязательные профили пользователей.

Использование сценариев входа в систему

Другим настраиваемым элементом на вкладке «Профиль» свойств пользователя являются файлы сценариев входа в систему, которые запускаются каждый раз, когда пользователь входит в систему. Обычно это пакетные файлы, но они могут быть любым типом исполняемого файла. Сценарии входа либо создаются администратором, либо просто копируются из Интернета. Создание этих сценариев выходит за рамки этого урока.

Чтобы применить сценарий входа в систему для пользователя, введите имя сценария в текстовое поле «**Сценарий входа**» на вкладке «Профиль» диалогового окна «**Свойства пользователя**».

Также на этой вкладке вы можете указать расположение домашней папки в качестве локальной папки или

сетевой папки. Основная причина, по которой вы предоставляете своим пользователям домашнюю папку на сервере, заключается в том, что серверы обычно являются единственными компьютерами, которые используют резервное копирование. Большинство компаний не создают резервные копии отдельных компьютеров пользователей. Если пользователь поместит все свои важные документы в свою домашнюю папку на сервере, эти документы будут скопированы как часть резервной копии.

Чтобы указать локальную папку, выберите параметр «Локальный путь» и введите путь в текстовое поле рядом с этим параметром. Чтобы указать сетевой путь к папке, выберите параметр «Подключиться» и укажите сетевой путь, используя путь UNC. Путь UNC состоит из имени компьютера и общего ресурса, созданного на компьютере. При подключении к имени UNC сетевая папка, к которой вы подключаетесь, должна быть создана и предоставлена в общий доступ. Если домашняя папка, которую вы указываете, не существует, Windows 10 попытается создать ее. Вы также можете использовать переменную %username% вместо имени конкретного пользователя.

Устранение неполадок с учетной записью учетной записи пользователя

Когда пользователь пытается войти в систему и не может быть аутентифицирован, вам нужно будет найти причину проблемы.

Если у локального пользователя возникают проблемы при входе в систему, проблема может быть связана с именем пользователя, паролем или самой учетной записью

пользователя. Ниже приводятся некоторые общие причины ошибок локального входа:

Неправильное имя пользователя. Вы можете проверить правильность имени пользователя, используя оснастку «Локальные пользователи и группы». Убедитесь, что имя написано правильно.

Неверный пароль. Помните, что пароли чувствительны к регистру. Включен ли *Caps Lock*? Если вы видите сообщения, относящиеся к просроченному паролю или заблокированной учетной записи, причина проблемы очевидна. При необходимости вы можете назначить новый пароль.

Запрещающие правила для пользователя. Имеет ли пользователь разрешение на вход в систему локально на компьютере? По умолчанию пользовательское право *Log On Locally* предоставляется группе *Users*, поэтому все пользователи могут подключаться к компьютерам с Windows 10.

Однако, если это правило было изменено, вы увидите сообщение об ошибке, указывающее, что локальная политика этого компьютера не разрешает интерактивный вход в систему. Термины интерактивного входа и локального входа являются синонимами и означают, что пользователь входит в систему на компьютере, где учетная запись пользователя хранится в локальной базе данных компьютера.

Отключенная или удаленная учетная запись. Вы можете проверить, была ли отключена учетная запись, проверяя свойства учетной записи с помощью оснастки

«Локальные пользователи и группы». Если учетной записи больше нет в базе данных, она скорее всего была удалена.

Управление группами

Группы являются важной частью сетевого управления. Администраторы могут выполнять большинство своих управлений задач с помощью групп; они редко назначают разрешения отдельным пользователям.

Windows 10 включает в себя встроенные локальные группы (такие как администраторы и операторы резервного копирования), которые уже имеют все разрешения, необходимые для выполнения определенных задач. Windows 10 также использует встроенные специальные группы, в которые пользователи добавляются автоматически, когда они отвечают определенным критериям.

Вы можете создавать и управлять локальными группами (но не специальными группами) с помощью оснастки «Локальные пользователи и группы». С помощью этой оснастки вы можете добавлять группы, изменять членство в группах, переименовывать группы и удалять группы.

Использование встроенных групп

На компьютере под управлением Windows 10 уже созданы встроенные локальные группы и назначены все необходимые разрешения для выполнения основных задач. Кроме того, есть встроенные специальные группы, такие как группа [Все \(Everyone\)](#), группа [Система \(System\)](#), группа [Прошедшие аутентификацию \(Authenticated Users\)](#) и т.д.

На скриншоте ниже показаны встроенные группы, которые были созданы на этапе установки ОС.

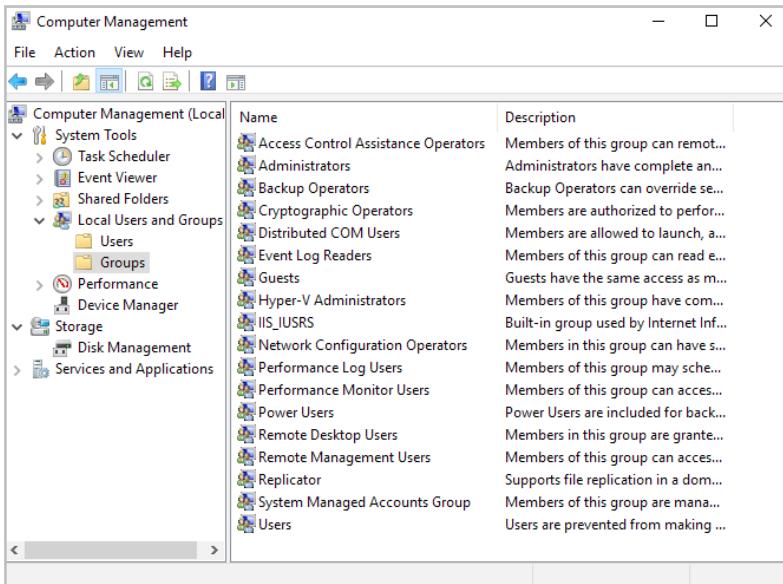


Рисунок 35

Создание групп

Чтобы создать группу, вы должны войти в систему с правами группы «[Администраторы](#)». Группа «[Администраторы](#)» имеет полные разрешения для управления пользователями и группами.

Соглашения об именах при назначении имен для групп, аналогичные тем, которые используются при выборе имени пользователя. Обратите внимание на следующие рекомендации:

- Имя группы должно быть описательным; например, «Пользователи учетных данных».
- Имя группы должно быть уникальным для компьютера и отличаться от всех других имен групп и имен пользователей, существующих на этом компьютере.

- Имена групп могут содержать до 256 символов. Для удобства администрирования лучше использовать буквенно-цифровые символы. Символ обратной косой черты (\) не допускается.

Создание групп аналогично созданию пользователей, и это довольно простой процесс. После того, как вы добавили оснастку «Локальные пользователи и группы» или оснастку «Управление компьютером», разверните ее, чтобы получить доступ к папкам «Пользователи» и «Группы». В контекстном меню папки «Группы» и выберите пункт «Новая группа». Появится диалоговое окно «Новая группа», показанное на рисунке 36.

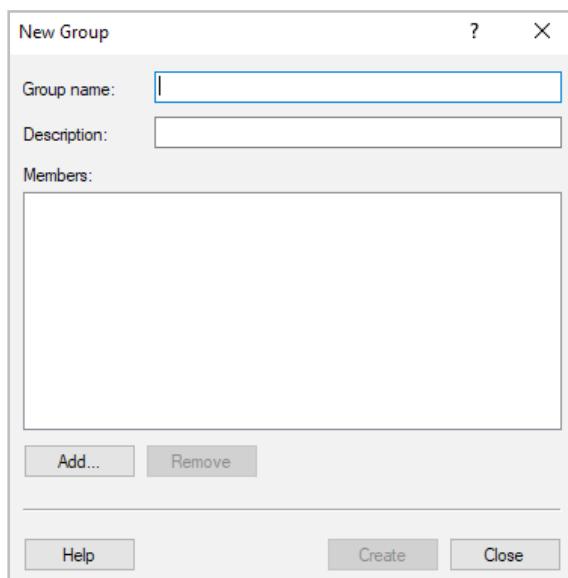


Рисунок 36

Единственной обязательной записью в диалоговом окне «Новая группа» является имя группы. Если необходимо,

вы можете ввести описание для группы, и вы можете добавить (или удалить) членов группы. Когда вы заполните поля и выполните все необходимые действия, нажмите кнопку «Создать».

Управление членством в группах

После того, как создана группа, вы можете добавить к ней участников. Как упоминалось ранее, вы можете поместить одного и того же пользователя в несколько групп. Вы можете легко добавлять и удалять пользователей через диалоговое окно «Свойства» группы, показанное на рисунке. Чтобы получить доступ к диалоговому окну «Свойства группы» в папке «Группы» откройте контекстное меню на имени группы, свойства которой хотите изменить.

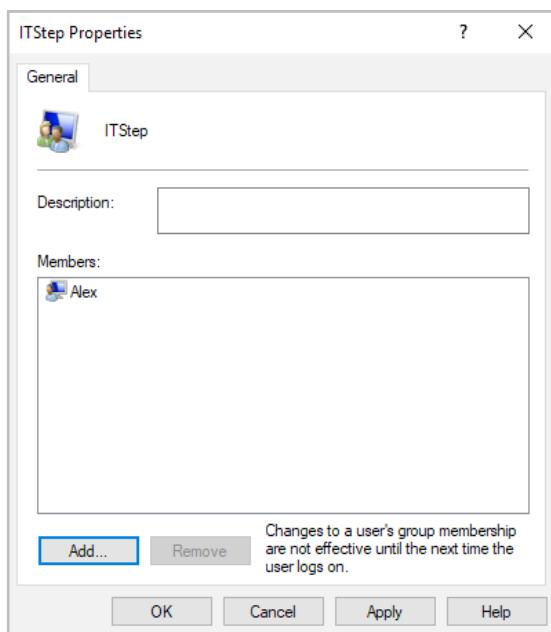


Рисунок 37

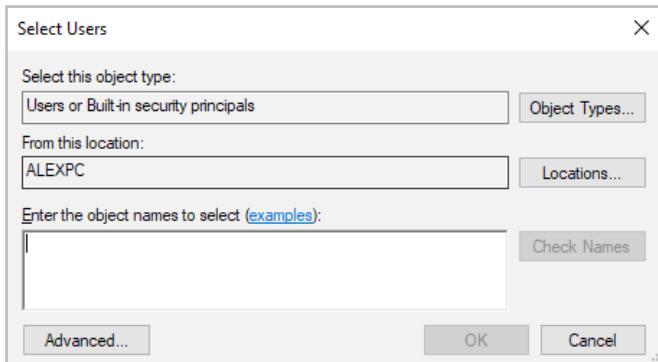


Рисунок 38

В диалоговом окне «Свойства» группы вы можете изменить описание группы и добавить или удалить членов группы. Когда вы нажимаете кнопку «Добавить» для добавления членов, появляется диалоговое окно «Выбрать пользователей» (рисунок). В диалоговом окне «Выбор пользователей» вы вводите имена объектов для пользователей, которые хотите добавить. Вы можете использовать кнопку «Проверить имена», чтобы проверить наличие пользователей в базе данных. Выберите учетные записи пользователей, которые вы хотите добавить, и нажмите «Добавить». Нажмите кнопку «OK», чтобы добавить выбранных пользователей в группу.

Чтобы удалить участника из группы, выберите его имя в списке «Члены группы» диалогового окна «Свойства» и нажмите кнопку «Удалить».

Удаление групп

Если вы уверены, что больше никогда не захотите использовать определенную группу, вы можете удалить ее. Когда группа удаляется, вы теряете все назначения

разрешений, которые были указаны для группы. Чтобы удалить группу, откройте контекстное меню для этой группы и выберите «Удалить». Вы увидите предупреждение о том, что после удаления группы она исчезнет. Нажмите кнопку «Да», если вы уверены, что хотите удалить группу.

Если вы удалите группу и дадите другой группе то же имя, новая группа не будет обладать теми же свойствами, что и удаленная группа, потому что, подобно пользователям, группы получают уникальные идентификаторы SID, назначаемые в момент создания.

Управление безопасностью с использованием локальной политики безопасности

Политика безопасности — это набор параметров, которые регулируют безопасность компьютера и управляются с помощью локального объекта GPO. Настраивать данные политики можно при помощи оснастки «Редактор локальной групповой политики» или оснастки «Локальная политика безопасности». Оснастка «Локальная политика безопасности» используется для изменения политики учетных записей и локальной политики на локальном компьютере, а политики учетных записей, привязанных к домену Active Directory можно настраивать при помощи оснастки «Редактор управления групповыми политиками».

Например, вы можете использовать политики для управления учетными записями пользователей. Правила, устанавливаемые для учетной записи, управляют средой входа в систему для компьютера, например, сложностью пароля и ограничениями по количеству неправильных попыток ввода пароля. Локальные политики определяют, что пользователи могут делать после входа в систему и позволяют включить аудит, определить права пользователя и параметры безопасности. Вы также можете управлять критическими функциями безопасности через Центр безопасности Windows.

Конфигурирование политик безопасности

Политики, которые были назначены через Active Directory, по умолчанию будут иметь приоритет перед любыми установленными политиками локальных групп. Политики локальных групп обычно применяются к компьютерам, которые не являются частью сети, или находятся в сети, у которой нет контроллера домена, и поэтому не используют базу Active Directory.

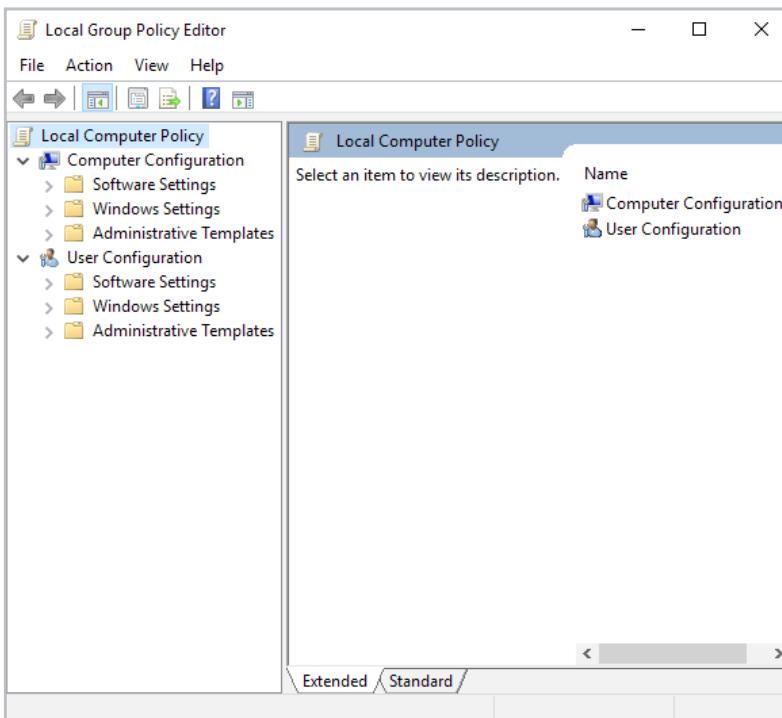


Рисунок 39

Политики локального компьютера — включают настройки компьютера и пользователя; другие политики содержат только пользовательские настройки. Применяемые

здесь настройки будут применяться ко всем пользователям компьютера.

Политики для администраторов применяются к пользователям, входящим в состав группы локальных администраторов. Как вы могли догадаться, для не-администраторов политики применяются к пользователям, которые не являются членами локальной группы администраторов. Поскольку каждый пользователь компьютера может быть классифицирован как администратор или не-администратор, применяется либо одна политика, либо другая.

На рисунке 39 показана оснастка «Редактора объектов локальной групповой политики» в ММС.

Настройка локальных политик безопасности

С помощью политики локального компьютера вы можете установить широкий диапазон параметров безопасности в разделе «Конфигурация компьютера\Параметры Windows\Параметры безопасности» (Computer Configuration\Windows Settings\Security Settings).

Эта часть политики локального компьютера также известна как **Локальная политика безопасности** (*Local Security Policy*). Ниже рассматриваются элементы, входящие в ее состав. Отдельно запустить оснастку локальной политики безопасности можно при помощи команды `Secpol.msc`, либо по пути **Панель управления-Администрирование-Локальные политики безопасности**.

Политики учетной записи (*Account Policies*). Правила для учетных записей используются для настройки функций блокировки пароля и учетной записи. Некоторые из этих настроек включают историю паролей, максимальный

возраст пароля, минимальный возраст пароля, минимальную длину пароля, сложность пароля, продолжительность блокировки учетной записи, порог блокировки учетной записи и необходимость сброса счетчика блокировки учетной записи.

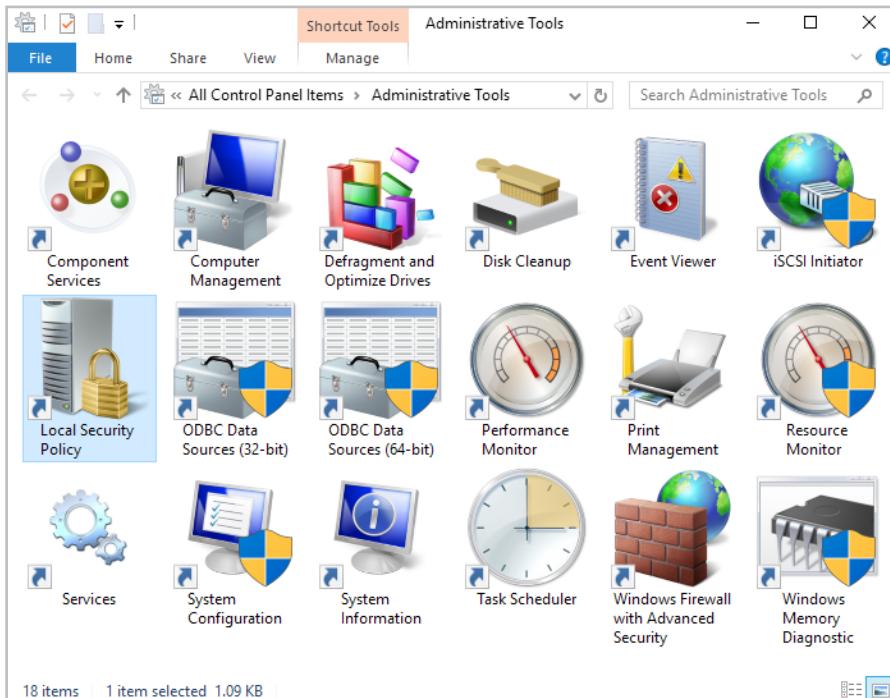


Рисунок 40

Локальные политики (Local Policies). Локальные политики используются для настройки аудита, прав пользователей и параметров безопасности.

Брандмаэр Windows с повышенной безопасностью (Windows Firewall with Advanced Security). Брандмаэр Windows с расширенной безопасностью обеспечивает

сетевую безопасность для компьютеров Windows. С помощью этой LGPO вы можете настроить доменные, частные и общедоступные профили. Вы также можете настроить эту LGPO для аутентификации сообщений между компьютерами и правила для входящих/исходящих сообщений.

Политики диспетчера списка сетей (*Network List Manager Policies*). В этом разделе вы можете указать политики сетевого имени, значка и расположения групповых политик. Администраторы могут устанавливать неопознанные сети, идентифицируемые сети и все сети.

Политики открытого ключа (*Public Key Policies*). Параметры политики открытого ключа, для указания, как управлять сертификатами и жизненными циклами сертификатов.

Политики ограниченного использования программ. (*Software Restriction Policies*). Настройки в этом разделе позволяют идентифицировать вредоносное программное обеспечение и управлять возможностями этого программного обеспечения на компьютере под управлением Windows 10. Эти политики позволяют администратору защищать операционную систему от угроз безопасности, таких как вирусы трояны и т.д.

Политики управления приложениями (*Application Control Policies*). В этом разделе вы можете использовать AppLocker для настройки списка запрещенных и списка разрешенных приложений». Приложения, указанные в списке «Запрет», не будут запускаться в системе, а приложения из списка «Разрешено» будут работать.

Политики IP-безопасности на локальном компьютере (*IP Security Policies on Local Computer*). В этом разделе вы можете настроить политики IPSec.

Конфигурация расширенной политики аудита (*Advanced Audit Policy Configuration*). Используется для обеспечения детального контроля над политиками аудита. В этом разделе вы также можете настроить аудит, чтобы отслеживать успешные или неудачные атаки в своей сети.

Использование политик учетной записи

Политики учетной записи используются для определения свойств учетной записи пользователя, от имени которой произведен вход в систему. Они позволяют настраивать параметры безопасности компьютера для паролей и параметров блокировки учетной записи.

Если параметры безопасности не важны, возможно, потому, что вы используете свой компьютер под управлением Windows 10 дома, тогда вам не нужно беспокоиться о политике учетной записи. Если, с другой стороны, безопасность важна, например, потому что ваш компьютер содержит конфиденциальную рабочую информацию — тогда вы должны установить очень жесткие политики для учетных записей.

Настройка паролей

Политики паролей обеспечивают соблюдение требований безопасности на компьютере. Важно понимать, что политики паролей устанавливаются для всего компьютера; они не могут быть настроены для определенных пользователей.

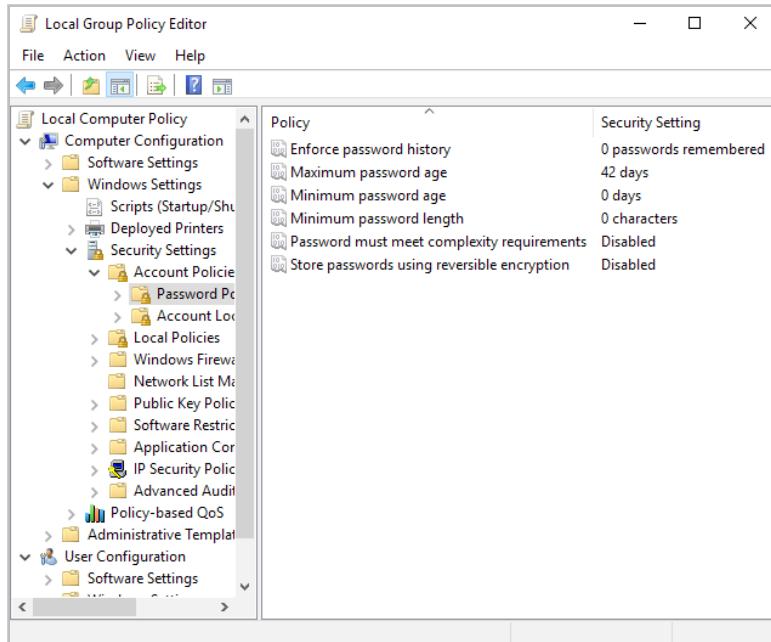


Рисунок 41

Настройка политик блокировки учетной записи

В политике блокировки учетной записи указывается, сколько недопустимых попыток входа в систему может быть. Вы настраиваете политики блокировки учетной записи таким образом, чтобы после того, как после X неудачных попыток входа в течение у минут, учетная запись будет заблокирована в течение определенного времени или до тех пор, пока администратор не разблокирует ее.

Политики блокировки учетной записи похожи на механизмы банка для обеспечения безопасности доступа к ATM. У вас есть определенное количество шансов ввести правильный PIN-код. Таким образом, любой, кто крадет вашу карточку, не может просто угадать ваш код доступа.

Как правило, после трех неудачных попыток банкомат блокирует карту и вам нужно обращаться в банк, чтобы они её разблокировали. На рис. показаны политики блокировки учетной записи.

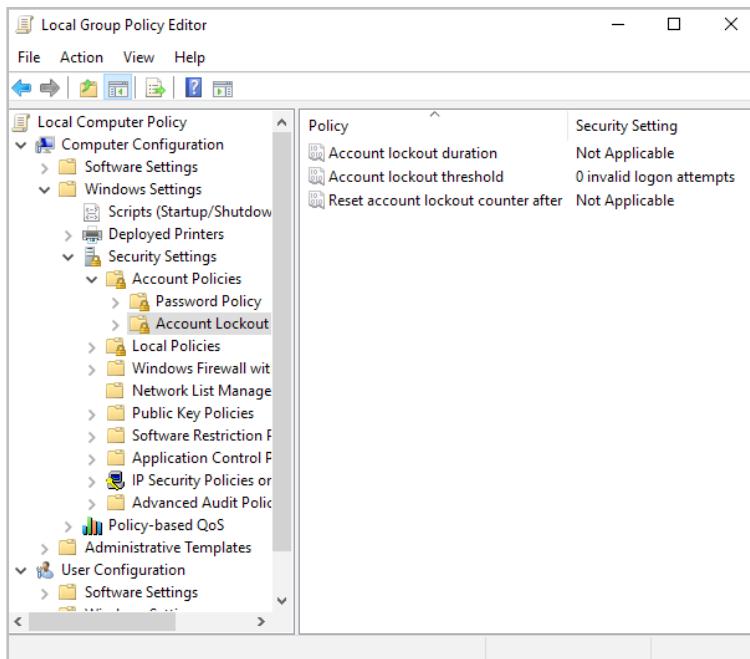


Рисунок 42

Использование локальных политик

Как вы узнали в предыдущем разделе, политики учетной записи используются для управления процедурами входа в систему. Когда вы хотите контролировать то, что пользователь может делать после входа в систему, вы используете локальные политики. С помощью локальных политик вы можете реализовать аудит, указать права пользователя и установить параметры безопасности.

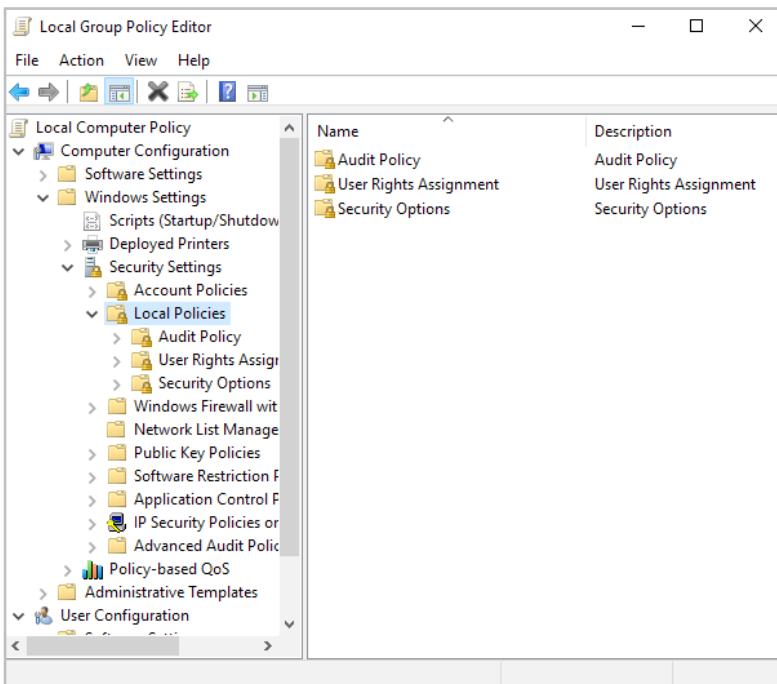


Рисунок 43

Настройка политики аудита

Политики аудита могут быть реализованы для отслеживания успеха или отказа определенных действий пользователя. Вы проверяете события, относящиеся к управлению пользователями, посредством политики аудита. Отслеживая определенные события, вы можете создать историю выполнения определенных задач, таких как создание пользователей, успешные или неудачные попытки входа в систему. Вы также можете определить нарушения безопасности, которые возникают, когда пользователи пытаются получить доступ к задачам системного управления, для которых у них нет разрешения.

Когда вы определяете политику аудита, вы можете выбрать аудит успеха или отказа для определенных событий. Успех события означает, что задача была успешно выполнена. Отказ события означает, что задача не была успешно выполнена.

По умолчанию аудит не включен, и его необходимо настроить вручную. После настройки аудита вы можете увидеть результаты аудита в журнале безопасности с помощью оснастки «Просмотр событий».

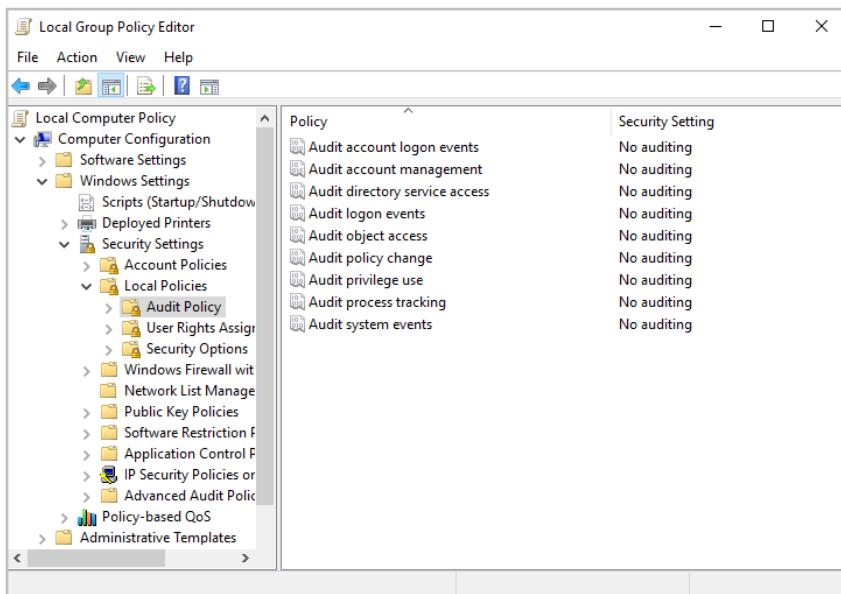


Рисунок 44

После включения политики аудита доступа к объектам, для включения работы аудита, в свойствах объекта необходимо включить аудит в настройках безопасности NTFS. Для включения аудита воспользуйтесь настройками безопасности принтера.

Назначение прав пользователей

Политики прав пользователя определяют, какие права пользователь или группа имеют на компьютере. Права пользователя, также называемые привилегиями, применяются к системе. Они не совпадают с разрешениями, которые применяются к определенному объекту. Примером права пользователя является резервное копирование файлов и каталогов. Это право позволяет пользователю создавать резервные копии файлов и папок, даже если у пользователя нет разрешений, определенных с помощью разрешений файловой системы NTFS.

Другие права пользователя аналогичны, поскольку они касаются доступа к системе, а не доступа к ресурсам.

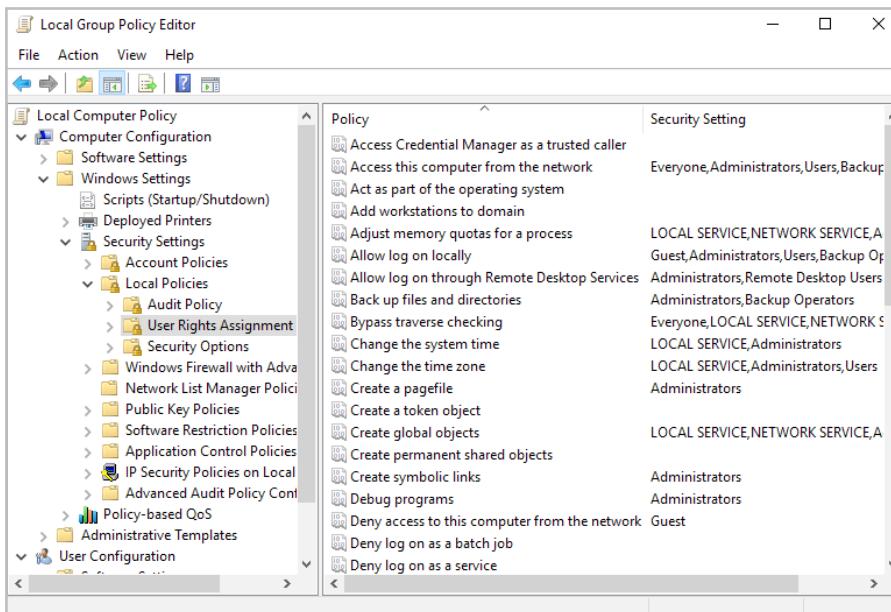


Рисунок 45

Настройка контроля учетных записей пользователей

Большинство администраторов вынуждены были выбирать между безопасностью и возможностью корректного запуска приложений. Раньше некоторые приложения просто не запускались корректно под Windows, если только пользователь, запускающий приложение, не был локальным администратором.

К сожалению, предоставление разрешений локального администратора для пользователя также позволяет пользователю устанавливать программное и аппаратное обеспечение, изменять настройки конфигурации, изменять локальные учетные записи пользователей и удалять критические файлы. Еще более тревожным является тот факт, что вредоносное ПО, заражающее компьютер во время входа администратора, способно выполнять административные функции.

Проблема в том, что многие приложения требуют, чтобы пользователи имели права на запись в защищенные папки и в реестр. Решение, применяемое в Windows 10 — это Контроль учетных записей (UAC). UAC позволяет пользователям, не являющимся администраторами, выполнять стандартные задачи, такие как установка принтера, настройка VPN или беспроводного соединения и установка обновлений, а также предотвращение ими выполнения административных задач, таких как установка приложений.

Повышение привилегий

UAC защищает компьютеры, требуя повышения привилегий для всех пользователей, даже для пользователей, входящих в группу локальных администраторов. Как вы,

без сомнения, уже заметили, UAC предложит вам дополнительно получить разрешение при выполнении задачи, требующей повышения привилегий. Это предотвращает запуск вредоносных программ без вашего ведома.

Для любого действия, напротив которого указан значок щита, требуется повышение привилегий.

Повышение привилегий для пользователей

Все пользователи работают с правами стандартного пользователя. Когда пользователь пытается выполнить действие, требующее административных полномочий, например, создает новую учетную запись, его полномочия должны быть повышенены до прав локального администратора. Это действие и называется повышением полномочий. Основная функция UAC — контролировать процесс повышения полномочий. Он гарантирует, что доступ к административным правам не будет предоставлен без ведома пользователя.

Когда стандартные пользователи пытаются выполнить задачу, требующую повышения привилегий, им предлагается ввести пароль учетной записи пользователя, имеющей административные привилегии. Вы не можете настроить UAC таким образом, чтобы стандартные пользователи могли выполнять административные задачи. Если вы не хотите, чтобы у стандартных пользователей вообще запрашивались учетные данные администратора при попытке выполнить административные задачи, вы изменяете значение параметра UAC для стандартных пользователей автоматически отклонять запросы на повышение.

UAC не влияет на встроенную учетную запись администратора, хотя она по умолчанию отключена. UAC не будет запрашивать встроенную учетную запись администратора для повышения привилегий. Таким образом, важно использовать обычную учетную запись пользователя, когда это возможно, и использовать встроенную учетную запись администратора только тогда, когда это абсолютно необходимо.

Повышенные привилегии для исполняемых файлов

Вы также можете запустить на выполнение исполняемый файл с повышенными привилегиями. Для этого в контекстном меню ярлыка или самого исполняемого файла необходимо выбрать «Запуск от имени администратора». Повышение применится только к этой сессии.

Что делать, если вам нужно на постоянной основе настроить приложение для работы с повышенными привилегиями, но запускаемое от имени стандартного пользователя? Для этого войдите в систему как администратор, откройте контекстное меню ярлыка или исполняемого файла и выберите «Свойства». На вкладке «Совместимость» установите флажок «Запускать эту программу от имени администратора». Если флажок недоступен, программа заблокирована от постоянной работы от имени администратора, либо потому что программе не нужны административные привилегии или вы не вошли в систему как администратор.

Реестр и виртуализация файлов

Многие приложения, установленные на компьютере под управлением Windows 10, должны иметь доступ к реестру. По умолчанию Windows 10 защищает реестр от учетных

записей, отличных от администратора, но функция под названием «Реестр и виртуализация файлов» позволяет пользователям, не являющимся администраторами, запускать приложения, которые ранее требовали прав администратора для корректной работы. Как обсуждалось ранее, некоторые приложения записывают свои данные в реестр и в защищенные папки, такие как [C:\Windows](#) и [C:\Program Files](#). Для пользователей, не являющихся администраторами, Windows 10 перенаправляет любые попытки записи в защищенные местоположения в области, доступные для данного пользователя. Таким образом, Windows 10 позволяет пользователям успешно использовать приложение, защищая критические области системы.

Настройка удаленного управления

Поддержка конечных пользователей является очень важной задачей и требует много времени для большинства ИТ-отделов. Базовая поддержка по телефону или чату помогает во многих случаях, но использование удаленного помощника и удаленного рабочего стола значительно упрощает процесс поиска и устранения неисправностей.

Удаленный помощник в Windows имеет множество улучшений по сравнению с предыдущими версиями, включая улучшения безопасности, производительности и удобства использования. В Windows 10 добавлен инструмент [Easy Connect](#), который помогает начинающим пользователям запрашивать помощь у опытных пользователей. Существует функция командной строки (это

означает, что вы можете добавлять скрипты), оптимизацию полосы пропускания, протоколирование и т.д.

Remote Desktop — это инструмент, который позволяет вам управлять клавиатурой, видео и мышью удаленного компьютера. Этот инструмент не требует, чтобы кто-то сотрудничал с вами на удаленном компьютере. Удаленный рабочий стол используется для доступа к приложениям удаленных компьютеров и устранения неполадок, а также для тех случаев, когда вы хотите получить полный контроль над удаленной машиной.

Удаленный помощник

Удаленный помощник использует для запроса помощи службы мгновенных сообщений, электронную почту, файл или теперь функцию **Easy Connect**. Чтобы использовать удаленный помощник, компьютер, запрашивающий справку или помочь, должен поддерживать функции удаленного помощника и оба компьютера должны иметь сетевое подключение (они должны иметь возможность взаимодействовать друг с другом по сети).

Удаленный помощник предназначен для того, чтобы опытный пользователь (помощник) оказывал помощь начинающему пользователю (просящему помочь). Помогая новичку, эксперт может использовать текстовый чат, встроенный в **Remote Assistance**. Эксперт также может взять под свой контроль рабочий стол новичка (с разрешения, конечно). Вот два распространенных примера использования удаленного помощника:

- Диагностика проблем, которые трудно объяснить или воспроизвести. Удаленный помощник может позволить

эксперту удаленно просматривать компьютер, а пользователь-новичок может показать эксперту ошибку или проблему.

- Помощь начинающему пользователю при выполнения сложного набора действий. Эксперт также может взять под свой контроль компьютер и при необходимости выполнить задачи.

Easy Connect

Метод Easy Connect для получения удаленной помощи является новым для Windows 10. Easy Connect использует протокол разрешения имен псевдонимов (PNRP) для настройки прямой одноранговой передачи с использованием центрального сервера в Интернете для установления соединения. PNRP использует туннелирование IPv6 и Teredo для регистрации машины как глобально уникальной.

Чтобы установить сеанс удаленного помощника с пользователем при помощи Easy Connect, новичкам следует открыть экран «Удаленная помощь Windows», щелкнув правой кнопкой мыши «Пуск». Вы также можете запустить экран удаленной помощи Windows, набрав `msra` в интегрированном окне поиска рядом с меню «Пуск».

Удаленный помощник также может быть включен в групповую политику в корпоративной среде, если пользователь-эксперт настроен как помощник для пользователей на предприятии (по домену или подразделению). После настройки в качестве помощника эксперт может инициировать сеанс удаленного помощника, выдав комманду `msra/offerra`.

Эксперт также может включать в себя IP-адрес или имя компьютера новичка в качестве опции для переключателя offerRA, чтобы инициировать сеанс удаленного помощника за одну остановку (например, msra / offerpa ipaddress | имя_компьютера).

Вне зависимости от того, каким образом начинающий или эксперт запускает эту функцию, откроется экран удаленной помощи Windows (см. Рис.). Чтобы начать использовать Easy Connect, пользователь новичок выберет «Пригласить того, кому вы доверяете, для оказания помощи».

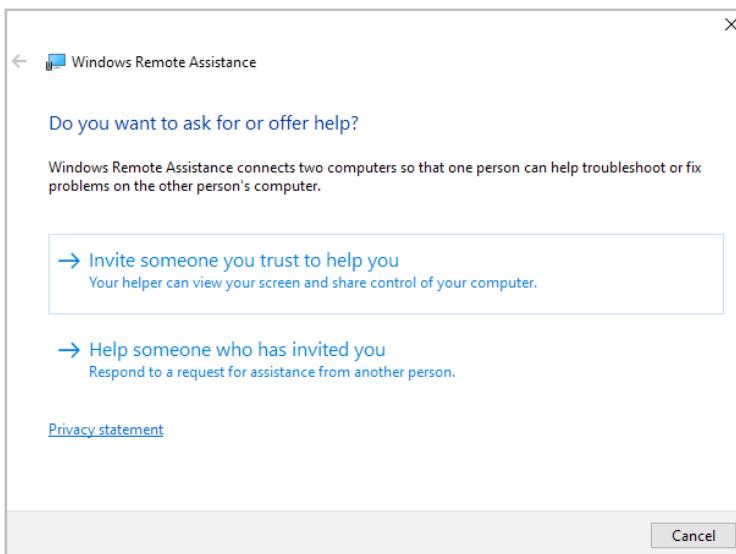


Рисунок 46

Одна из полезных особенностей Easy Connect заключается в том, что если пользователь-новичок установил сеанс Easy Connect ранее с экспертом, экран после выбора Use Easy Connect предложит новичку возможность подключиться к тому же эксперту. Новичок может также

пригласить кого-то нового и/или удалить старый контакт. У пользователя-специалиста будет такой же вариант после выбора **Use Easy Connect** с устройства, используемого для предыдущего сеанса **Easy Connect**.

Пользователь-эксперт должен запустить сеанс удаленного помощника так же, как новичок сделал на рисунке, но эксперт выберет «**Помочь тому, кто вас пригласил**» на экране «**Удаленный помощник Windows**».

Пользователю-эксперту будет представлено диалоговое окно для использования файла приглашения, а затем после выбора файла им будет предложено ввести пароль (рисунок) для подключения к сеансу удаленного помощника.

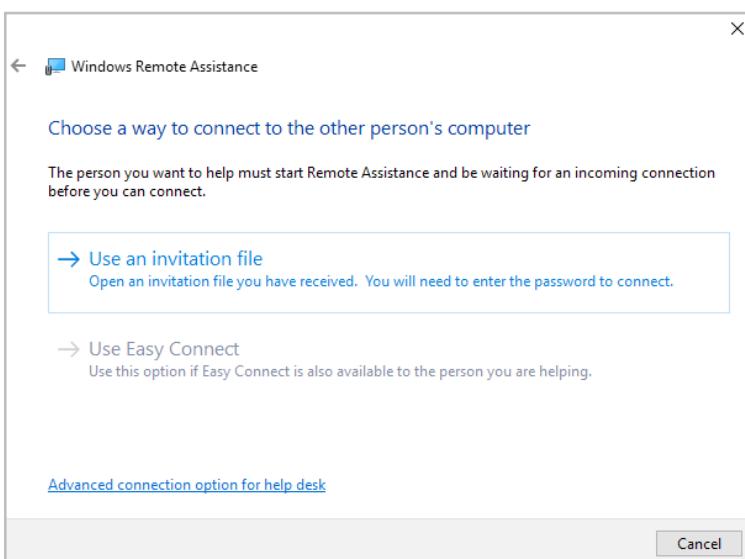


Рисунок 47

После нескольких минут ожидания и поиска информации о соединении, **Remote Assistance** предоставляет

пользователю окно подтверждения, о том, что пользователь хочет получить помощь эксперта.

Затем у пользователя-новичка откроется панель управления экране, указывающая, что сеанс удаленного помощника активен. С этой панели управления новичок может инициировать сеанс чата с экспертом и изменить некоторые общие настройки сеанса (пропускная способность, протоколирование, обмен контактной информацией и управление совместным доступом).

Пользователю-специалисту будет показан рабочий стол пользователя новичка в отдельном окне удаленного помощника. Пользователь-эксперт также будет иметь некоторые общие возможности настройки конфигурации, а также возможность запросить управление рабочим столом новичка. Новичкам, конечно же, будет предложено принять или отклонить запрос эксперта.

Теперь у эксперта и начинающего пользователя есть интерактивный сеанс, в рамках которого может быть оказана необходимая помощь. Этот метод помощи действительно устраняет проблемы между двумя пользователями: «Можете ли вы рассказать мне, что вы видите на экране». Одним из обязательных условий использования функции Easy Connect заключается в том, что оба пользователя должны использовать Windows 10.

Удаленный рабочий стол

Remote Desktop — это инструмент в Windows 10, который позволяет вам управлять клавиатурой, видео и мышью удаленного компьютера. Этот инструмент не требует, чтобы кто-то был доступен для совместной работы

с вами на удаленном компьютере. Пока происходит удаленное подключение, локально компьютер будет заблокированным, и любые действия, которые выполняются удаленно, не будут выводиться на монитор, который подключен к удаленному компьютеру.

Windows 10 Remote Desktop — это еще одна расширенная версия удаленного рабочего стола, которая использовалась во многих предыдущих версиях Windows, как в клиентских, так и в серверных операционных системах. Удаленный рабочий стол использует протокол удаленного рабочего стола (RDP) для обмена данными между хостом и клиентской машиной.

Существует много применений для удаленного рабочего стола, но чаще всего он используется администратором, который пытается выполнить задачу на компьютере конечного пользователя (или на сервере).

Другое вариант использования — конечный пользователь, подключающийся к компьютеру из своего дома или находясь в дороге. Одна из основных целей улучшения удаленного рабочего стола — сделать работу пользователя максимально комфортной и плавной.

Параметры подключения удаленного рабочего стола

При подключении к хосту удаленного рабочего стола доступно несколько параметров для улучшения клиентского сеанса. Доступны к настройке общие параметры, режимы отображения, доступ к локальным ресурсам, программы, которые будут выполняться при запуске, пользовательский интерфейс и расширенные параметры

безопасности и доступа к шлюзу удаленного рабочего стола. На рисунке 48 показано окно параметров.

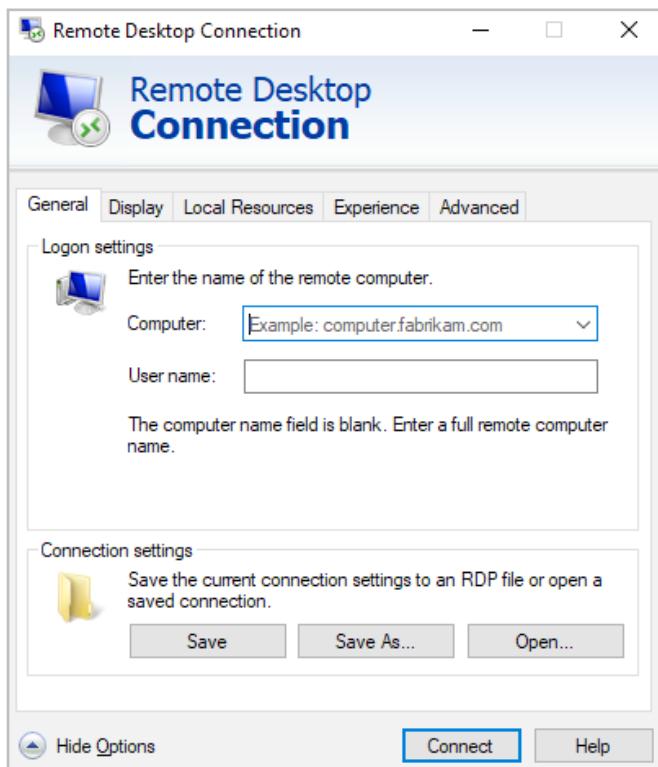


Рисунок 48

На вкладке «Общие» вы можете выбрать целевой удаленный компьютер и имя пользователя. Вы также можете сохранить учетные данные пользователя на этой вкладке. Вы можете сохранить настройки подключения в файл или открыть существующий файл RDP на вкладке «Общие».

На вкладке «Экран» вы можете выбрать размер экрана, вариант использования нескольких мониторов для удаленного сеанса, глубину цвета и опция отображения

панели подключений при использовании полноэкранного режима.

На вкладке «Локальные ресурсы» вы можете указать параметры звука удаленного рабочего стола, настройки клавиатуры и выбрать устройства и ресурсы, которые вы хотите использовать во время удаленного сеанса.

Вкладка «Программы» для параметров «Удаленный рабочий стол» позволяет выбрать программу для запуска при подключении. Указать имя и путь к программе, а также, при необходимости, папку.

На вкладке «Взаимодействие» можно выбрать скорость соединения с сетью для достижения оптимального быстродействия.

Параметры безопасности настраиваются на вкладке «Дополнительно» диалогового окна «Параметры удаленного рабочего стола». Вкладка «Дополнительно» также поддерживает настройку шлюза удаленного рабочего стола, позволяющего устанавливать подключения к удаленному рабочему столу из любого интернет-местоположения через SSL. Пользователь все равно должен быть авторизован, и клиент удаленного рабочего стола должен быть доступен.

Настройка VPN-подключения

Виртуальная частная сеть — это способ установления соединения между клиентской машиной (VPN-клиентом) и сервером (VPN-сервером). VPN дает вам возможность подключаться к серверу с использованием Интернета или удаленного доступа, как правило, с целью доступа к ресурсам, которые доступны в сети, где находится

VPN-сервер. VPN-сервер действует как мост для внешнего пользователя, подключающегося из Интернета или для других внешних подключений, к внутренней сети. В двух словах VPN позволяет вам подключаться к частной сети из общедоступной сети.

VPN-соединения могут быть защищены с использованием различных протоколов. В следующем списке показаны некоторые протоколы туннелирования, которые можно использовать при подключении компьютера Windows 10 к удаленному серверу:

Internet Key Exchange версии 2 (IKEv2). Windows 10 может подключаться к VPN-серверу Windows Server с использованием протокола туннелирования VPN для Internet Key Exchange версии 2 (IKEv2). Протокол IKEv2 VPN является новейшим протоколом VPN из всех существующих протоколов и может использоваться с Windows Server 2012/2012 R2 и Windows Server 2016. Основным преимуществом использования протокола IKEv2 VPN является то, что он позволяет прерывать подключение к сети. IKEv2 автоматически восстановит VPN-соединение после восстановления сетевого соединения. Эта функция называется VPN Reconnect, и она автоматически встроена в протокол IKEv2.

Протокол туннелирования защищенного сокета
Протокол туннелирования защищенных сокетов (SSTP) был выпущен с Windows Server 2008 и является одним из протоколов туннелирования, доступным на серверах Windows Server 2008/2008 R2 и Windows 7. SSTP работает, разрешая инкапсулированные пакеты протокола

«точка-точка» (PPP) для передачи по HTTPS-соединению. Из-за этого брандмауэры или устройства преобразования сетевых адресов (NAT) позволяют более легко установить соединения VPN SSTP. SSTP — лучший выбор для обеспечения VPN-соединения.

Протокол туннелирования «точка-точка» (PPTP)
Является одним из предшественников SSTP. PPTP инкапсулирует кадры PPP в IP и использует TCP для управления PPTP.

Протокол туннелирования 2 уровня (L2TP) — Протокол туннелирования, который не имеет шифрования, включенного в протокол. L2TP использует протокол IPSec для обеспечения безопасности. L2TP с IPSec является гораздо более безопасным туннелированием, чем PPTP.

Для настройки VPN-соединения в Windows 10, используйте [«Центр управления сетями и общим доступом»](#).

Более детально настройка подключения к удаленному рабочему столу и создание VPN подключения будут рассмотрены в лабораторной работе.



Урок №4

Конфигурирование сети в Windows 10

Все права на охраняемые авторским правом фото-, аудио- и видеопрограммные средства, фрагменты которых использованы в материале, принадлежат их законным владельцам. Фрагменты произведений используются в иллюстративных целях в объеме, оправданном поставленной задачей, в рамках учебного процесса и в учебных целях, в соответствии со ст. 1274 ч. 4 ГК РФ и ст. 21 и 23 Закона Украины «Про авторське право і суміжні права». Объем и способ цитируемых произведений соответствует принятым нормам, не наносит ущерба нормальному использованию объектов авторского права и не ущемляет законные интересы автора и правообладателей. Цитируемые фрагменты произведений на момент использования не могут быть заменены альтернативными, не охраняемыми авторским правом аналогами, и как таковые соответствуют критериям добросовестного использования и честного использования.

Все права защищены. Полное или частичное копирование материалов запрещено. Согласование использования произведений или их фрагментов производится с авторами и правообладателями. Согласованное использование материалов возможно только при указании источника.

Ответственность за несанкционированное копирование и коммерческое использование материалов определяется действующим законодательством Украины.