

Службы удаленного доступа ИВС МЭИ.

Подключение к ИВС МЭИ с использованием VPN.

Технология VPN.

Технология VPN (Virtual Private Network – виртуальная частная сеть) позволяет обеспечить сетевые соединения поверх другой сети. При этом устанавливается туннель между удаленной рабочей станцией пользователя и сервером ИВС МЭИ. IP адрес полученного соединения относится к внутреннему пространству адресов ИВС МЭИ, что позволяет получить доступ к внутренним сервисам ИВС. Процедура установки соединения строго авторизована, а передаваемые данные зашифрованы. Таким образом, VPN-соединение является доверенным для ИВС МЭИ.

При установленном VPN-соединении удаленная рабочая станция рассматривается как рабочая станция ИВС МЭИ. При этом обеспечивается подключение к внутренним информационным сервисам, доступ к которым из Интернет обычно закрыт. Например, доступ к серверу виртуальных рабочих столов `viewserver.mpei.local` возможен только из внутренней сети МЭИ и с помощью VPN, а не из Интернет. Такое же правило действует и в отношении других серверов и компьютеров, входящих в домен `public.mpei.local`.

Реализация служб удаленного доступа к ИВС МЭИ с использованием VPN отличается несколькими дополнительными чертами:

- Обеспечивается доступ только к внутреннему сегменту ИВС МЭИ. Доступ к Интернет и публичному сегменту ИВС МЭИ использует текущее соединение. Таким образом, обеспечивается высокий уровень защиты соединения.
- Весь трафик VPN-соединения шифруется, что позволяет удаленно работать с конфиденциальными данными.
- Весь трафик VPN-соединения инспектируется, что снижает риск заражения рабочей станции пользователя вредоносным ПО.
- VPN-соединения строго авторизованы, что исключает несанкционированный доступ к информации и внутренним сервисам ИВС МЭИ.

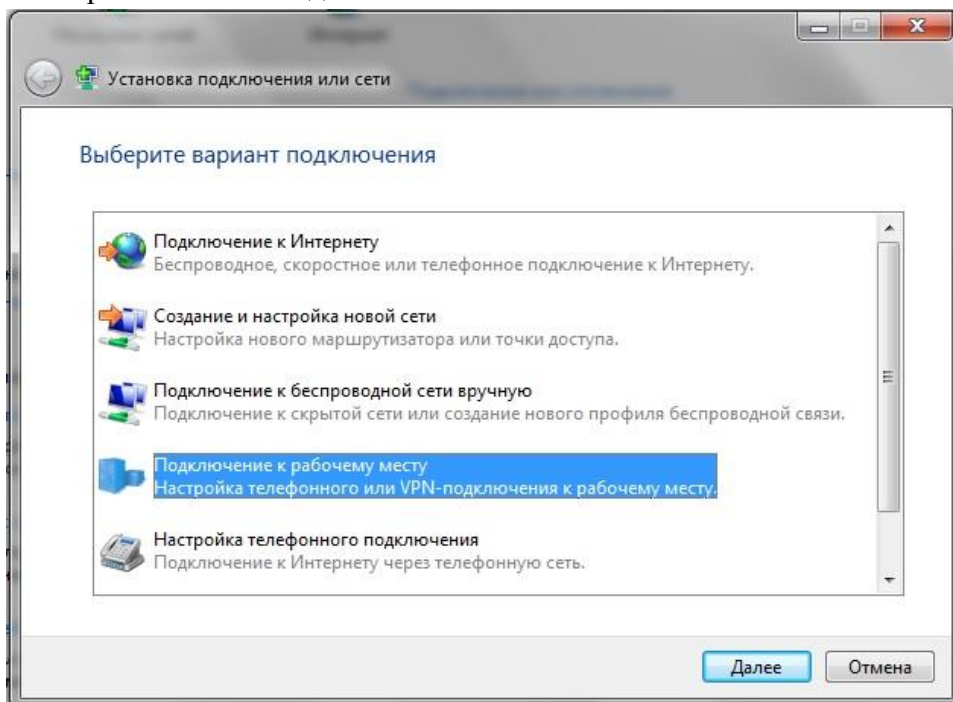
Примеры использования VPN-соединения:

- Доступ из дома к серверу виртуальных рабочих столов `viewserver.mpei.local`.
- Защищенный доступ из дома к системам хранения данных ИВС МЭИ.
- Защищенный полный доступ из дома к электронной почте посредством программ Outlook и др.
- Защищенный доступ к рабочему столу своего компьютера.

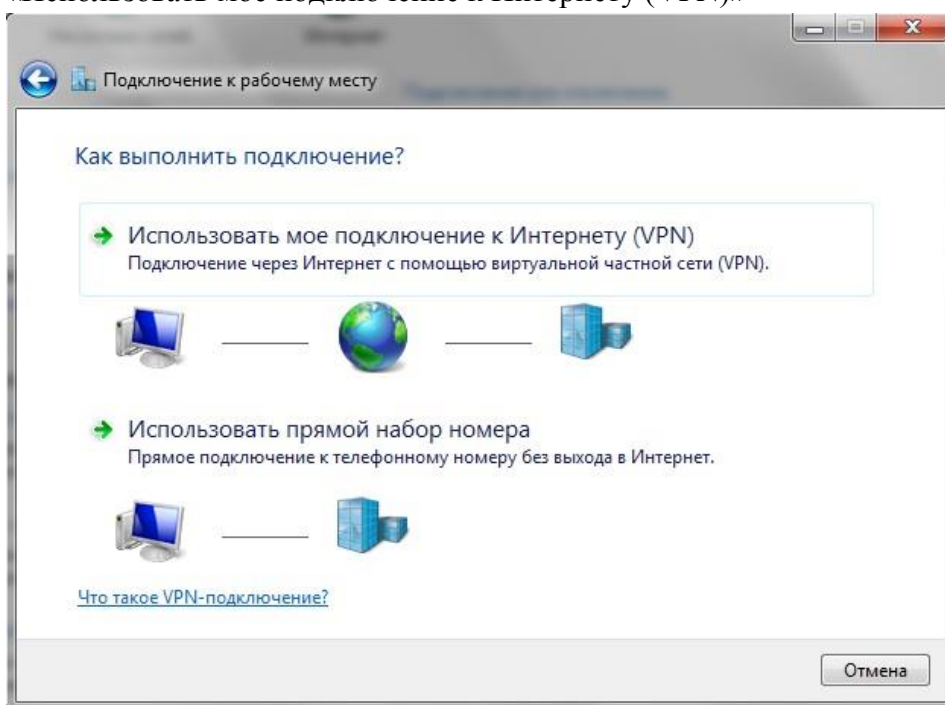
Подключение к ИВС МЭИ по протоколу PPTP с шифрованием MPPE.

Протокол PPTP с шифрованием MPPE является стандартным средством построения VPN в операционных системах семейства Windows. Конфигурация соединения с использованием Windows 7.

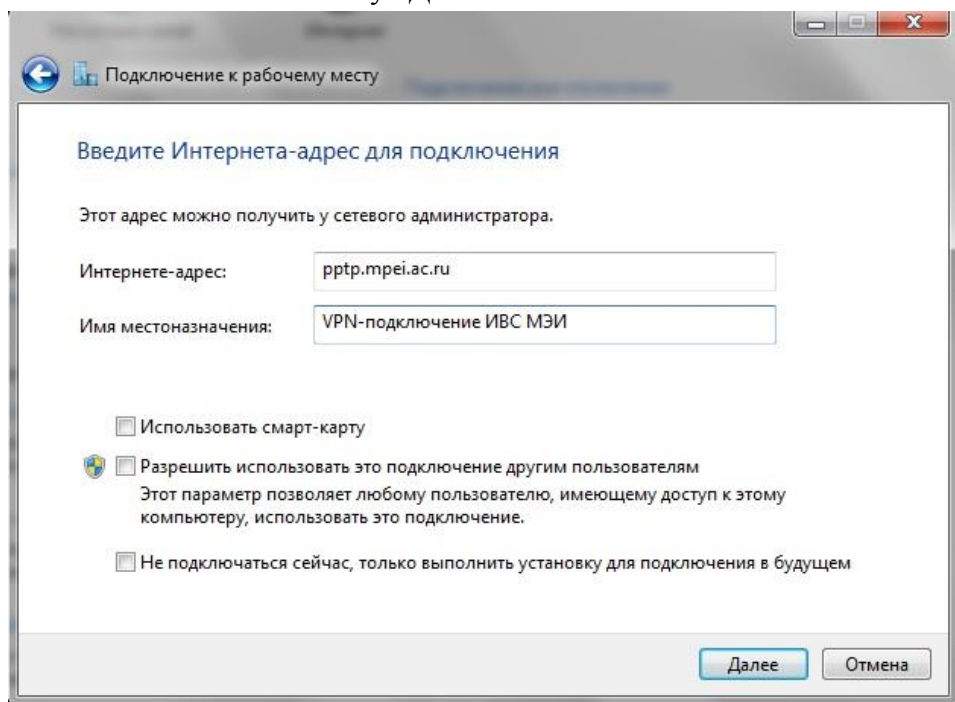
1. Запустим «Центр управления сетями и общим доступом» и выберем пункт «Настройка нового подключения или сети»



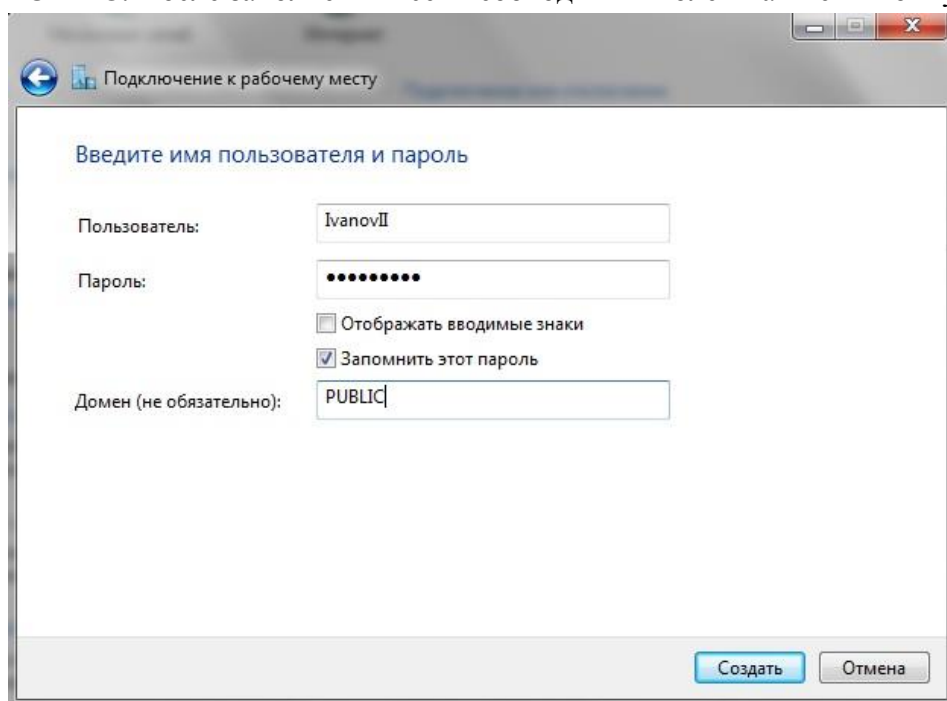
2. Выберем «Подключение к рабочему месту» и нажмем кнопку «Далее». Выберем «Использовать мое подключение к Интернету (VPN)»



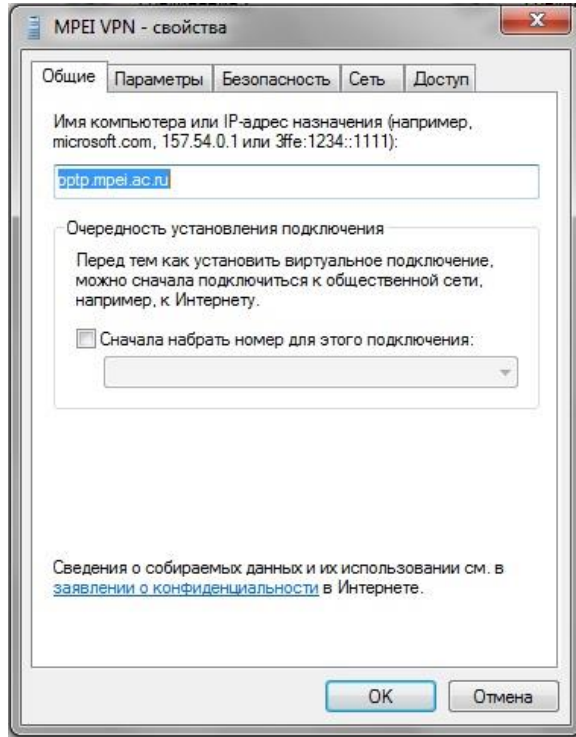
3. В появившемся окне укажем необходимый адрес для подключения, его описание и возможные опции. Желательно поставить галочку в пункте «Не подключаться сейчас, только выполнить настройку для подключения в будущем». После заполнения нажмем кнопку «Далее»



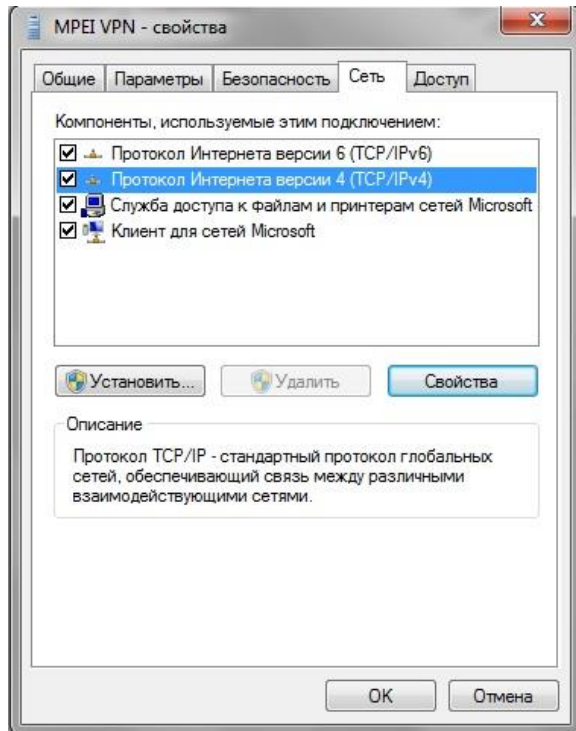
4. Теперь введем наше имя и пароль (те же, что используются для работы с электронной почтой МЭИ). Можно (но не обязательно) указать имя домена – PUBLIC. После заполнения всех необходимых полей нажмем кнопку «Создать».



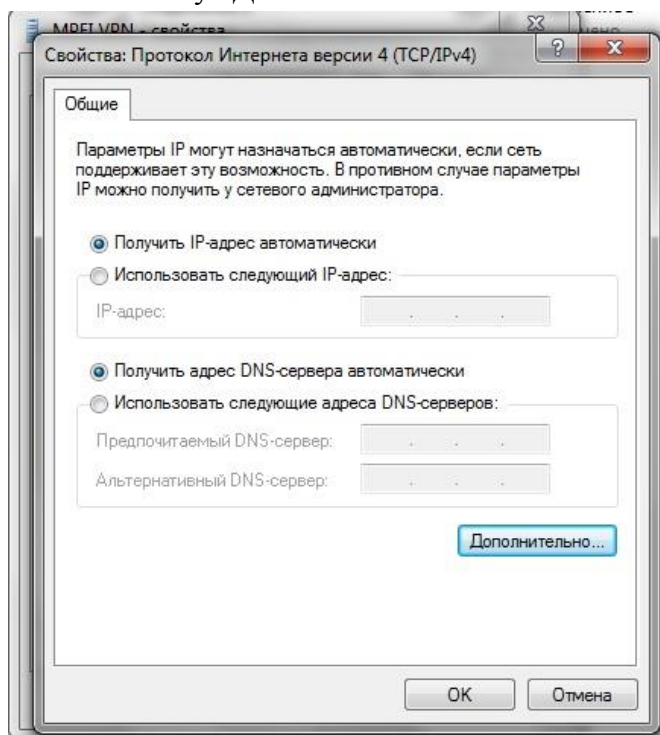
5. Теперь в списке сетевых подключений у вас появилось VPN-подключение. Теперь нужно задать ему некоторые свойства. Выделим вновь созданное VPN-подключение и выберем пункт «Свойства» из меню, выпадающего по нажатию правой кнопки мыши.



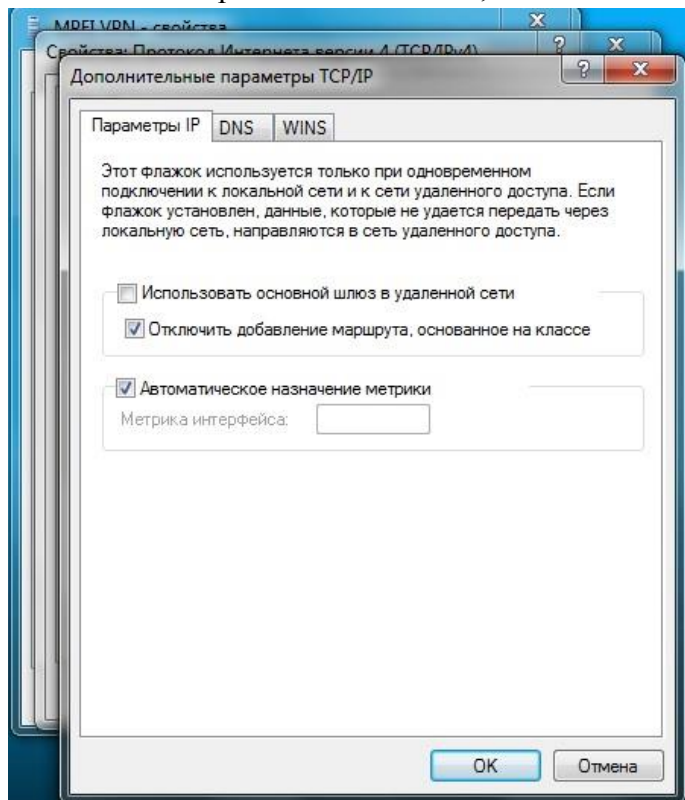
6. В появившемся окне свойств VPN-соединения выберем вкладку «Сеть», выделим пункт «Протокол Интернета версии 4 (TCP/IPv4)» и нажмем кнопку «Свойства».



7. В появившемся окне «Свойства: Протокол Интернета версии 4 (TCP/IPv4)» нужно нажать кнопку «Дополнительно».

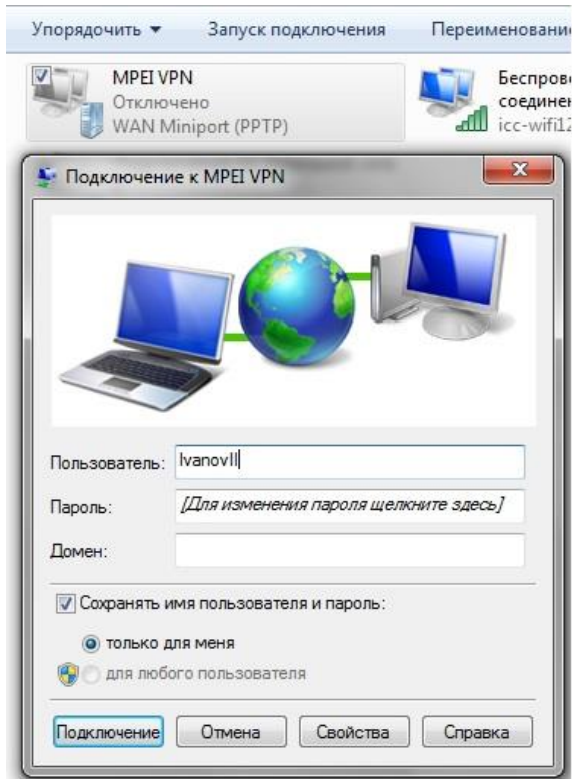


8. В окне «Дополнительные параметры TCP/IP» снимаем отметку в поле «Использовать основной шлюз в удаленной сети» и ставим отметки в полях «Отключить добавление маршрута, основанное на классе» и «Автоматическое назначение метрики». После этого, нажимаем кнопку «ОК».

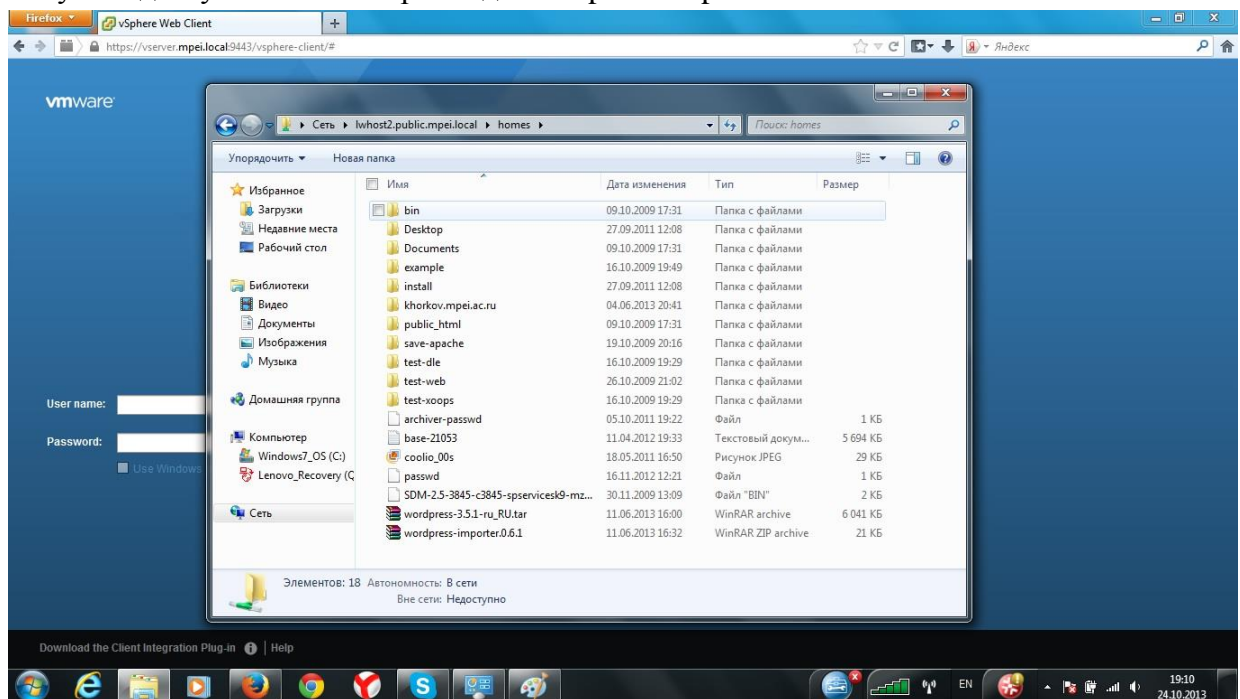


Если этого не сделать, то при работе нашего VPN-подключения не будет работать доступ к Интернет.

9. Во всех открытых окнах нажимаем кнопку «ОК». Наше VPN-подключение настроено, оно появилось в списке «Сетевые подключения» Панели управления и теперь мы сможем им воспользоваться.



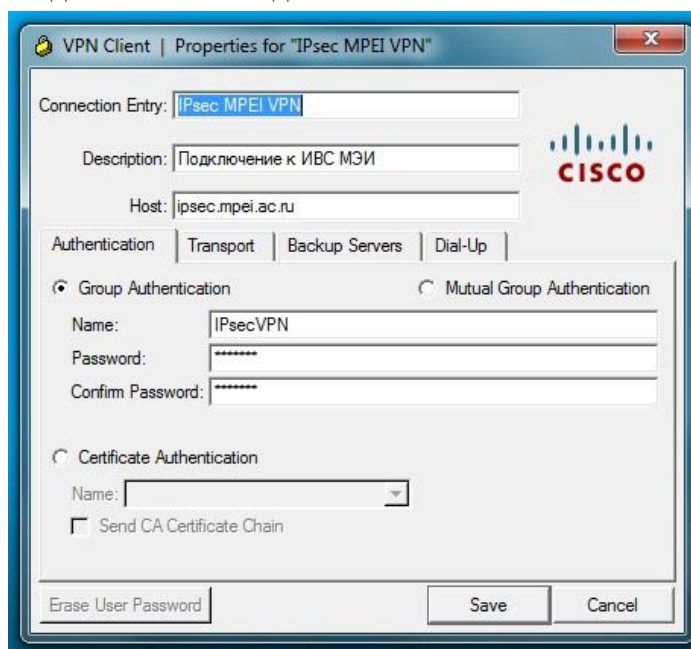
10. Нажимаем кнопку «Подключение» и, после проверки, наше соединение запускается. Теперь мы можем работать с внутренними сервисами ИВС МЭИ, получать доступ к компьютерам в домене public.mpei.local.



Подключение к ИВС МЭИ с использованием IPsec туннеля.

IPsec использует другой тип шифрования – AES. Кроме того, ключи регулярно меняются. IPsec туннель считается более защищенным. Для подключения по этому типу VPN потребуется установить программу Cisco VPN Client версии 5. IPsec VPN может использоваться не только на операционных системах семейства Windows, но и на платформе Android. Скачать Cisco VPN Client для установки в Windows можно [здесь \(32 битная версия\)](#) и [здесь \(64-битная версия\)](#). Кроме Cisco VPN client можно использовать и другое ПО – ShrewSoft VPN Client, узнать о котором подробнее можно на сайте производителя www.shrew.net.

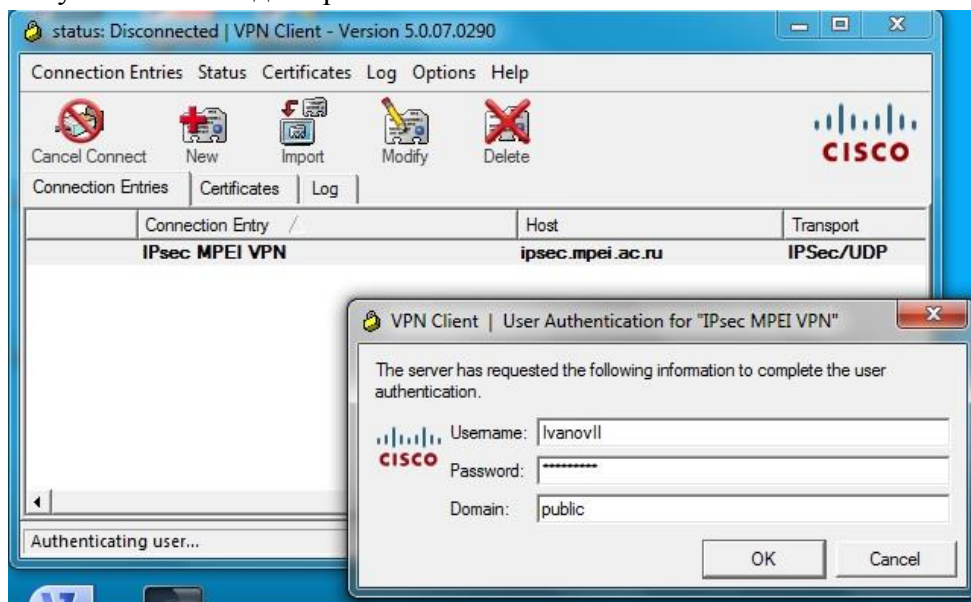
1. После установки запустите Cisco VPN Client и выберите иконку «New» для создания нового подключения.



Введите необходимые данные: Название и описание VPN-соединения, имя или IP адрес сервера и имя и пароль групповой аутентификации. В качестве сервера нужно указать ipsec.mpei.ac.ru.

Группа определяет уровень и тип шифрования. В качестве имени группы укажите IPsecVPN, а пароль для нее – mpeinet

2. После того как все эти параметры указаны, в основном окне Cisco VPN Client появится новое VPN-соединение. Выбрав его и нажав кнопку «Connect» мы получим окно ввода пароля.

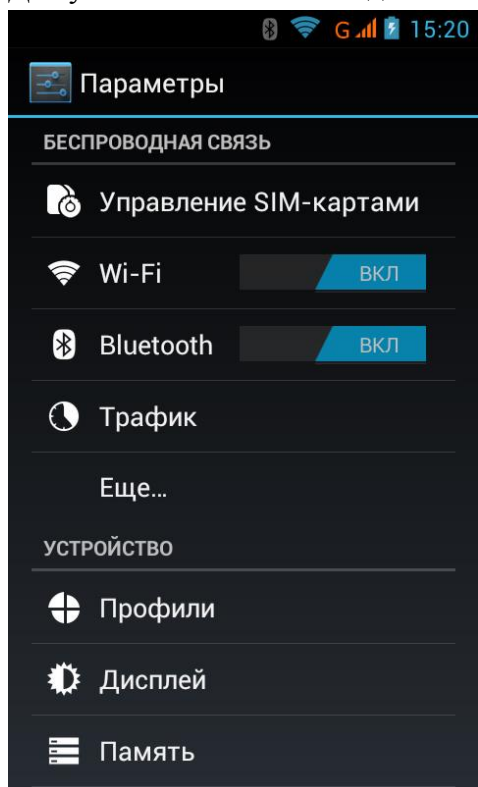


Вводим имя и пароль, которые используются для работы с электронной почтой МЭИ. Имя домена указывать необязательно. Нажимаем «OK» и процедура установления соединения запускается.

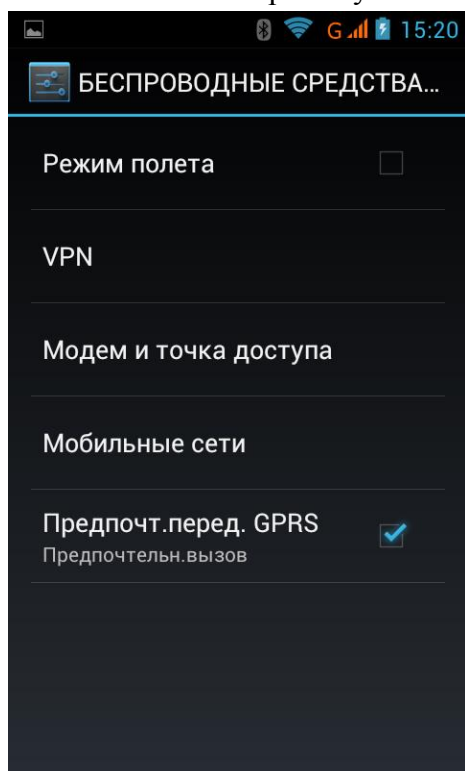
После установления соединения мы получаем доступ ко внутренним ресурсам ИВС МЭИ.

Подключение Android.

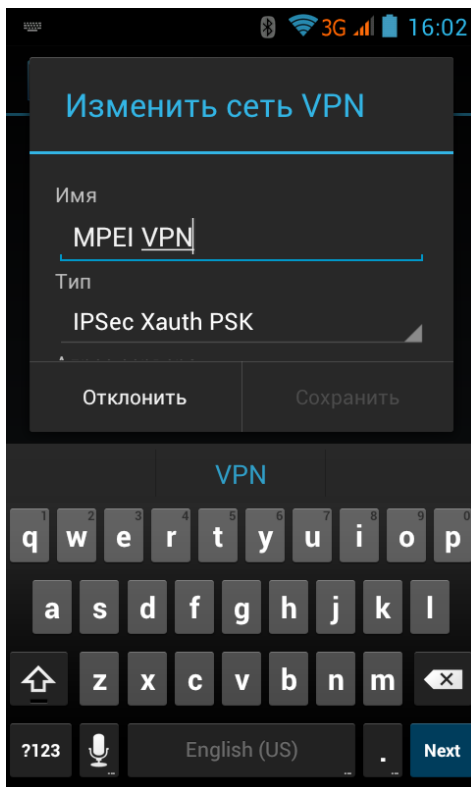
Для установления VPN подключения нужно выбрать «Настройки» и «Еще»



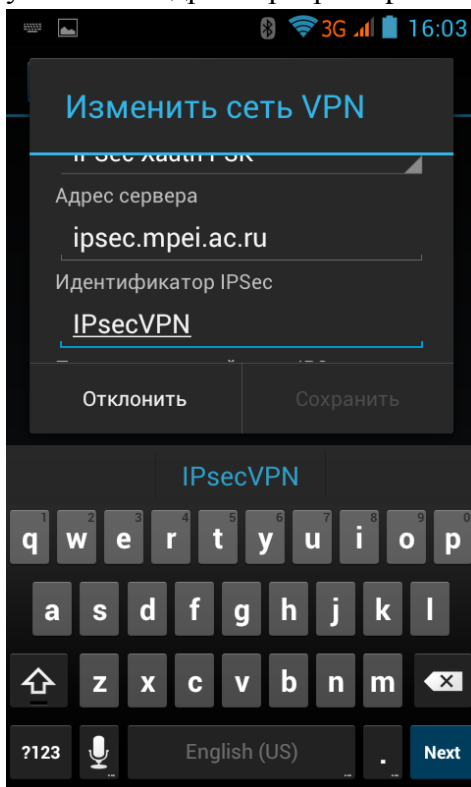
В появившемся меню выбрать пункт «VPN»



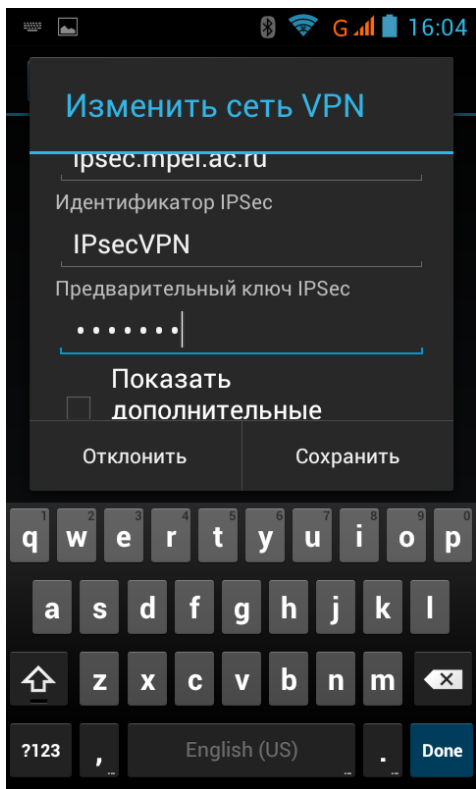
И «Добавить VPN-сеть». При этом запускается мастер настройки VPN-подключения.



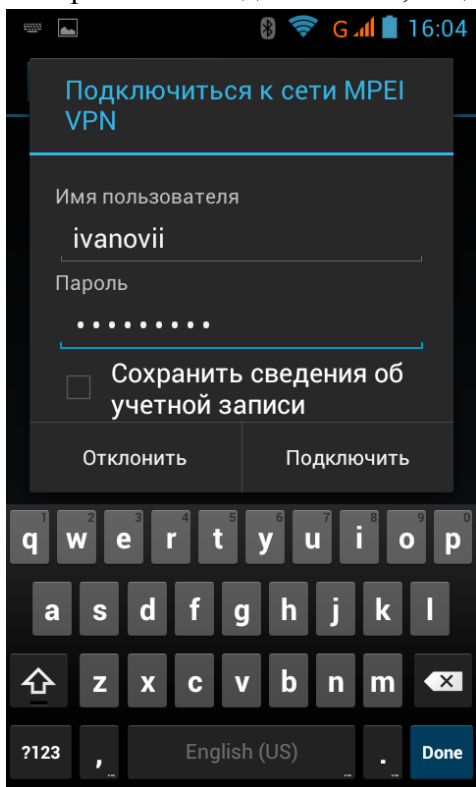
Указываем имя VPN-подключения и его тип – «IPSec Xauth PSK». Далее указываем адрес сервера – ipsec.mpei.ac.ru и идентификатор IPSec – IPsecVPN



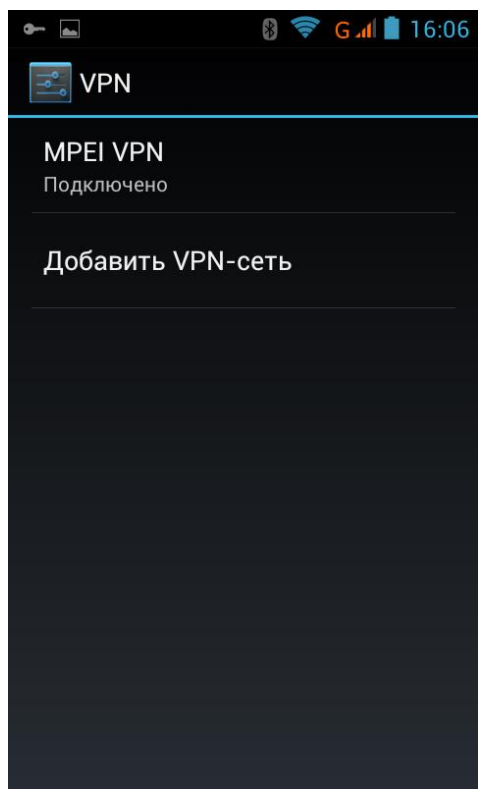
Затем указываем предварительный ключ – mpeinet и сохраняем настройки.



Теперь можно подключаться, вводя нужное имя и пароль:



Для автоматического сохранения имени и пароля нужно установить галочку в пункте «Сохранить сведения об этой учетной записи». После подключения мы увидим, что в списке VPN-подключений появилось новое подключение и его статус установлен в «Подключено».



Наше устройство на базе Android подключено к ИВС МЭИ. В качестве такого устройства может выступать смартфон или планшетный компьютер.

Безопасность VPN-подключений.

Безопасность подключений с использованием VPN обеспечивается следующими механизмами:

- шифрованием передаваемых данных, что затрудняет их перехват по модели атаки man-in-the-middle.
- строгой авторизацией доступа с регистрацией событий на всех этапах этого процесса.
- настройкой маршрутов соединения с ИВС МЭИ – VPN подключение используется только для ИВС МЭИ, доступ в Интернет не затрагивается.
- проверкой передаваемых и принимаемых данных на соответствие спецификациям используемых протоколов.

Техническая поддержка.

Техническую поддержку служб удаленного доступа осуществляет ИВЦ МЭИ. Тел: (495) 362-73-22