Инструкция для настройки L2TP-IPSec для Windows 7-8-10

• Открываем «Панель управления» -> «Сеть и Интернет»



• Открываем «Центр управления сетями и общим доступом»



• Открываем «Настройка нового подключения или сети»



• Выбираем «Подключение к рабочему месту», нажимаем «ДАЛЕЕ»



• Выбираем «Нет, создать новое подключение», нажимаем «ДАЛЕЕ»

🚱 🌆 Подключение к рабочему месту	
Использовать имеющееся подключение?	
Нет, создать новое подключение Да, выбрать существующее подключение	
VPN-подключение 3 WAN Miniport (PPTP)	E
WAN Miniport (PPTP)	
WAN Miniport (L2TP)	-
	Далее Отмена

• Выбираем «Использовать моё подключение к Интернету (VPN)»

🚱 🌆 Подключение к рабочему месту
Как выполнить подключение?
Использовать мое подключение к Интернету (VPN) Подключение через Интернет с помощью виртуальной частной сети (VPN).
🧶 — 🎱 — 🥼
Использовать прямой набор номера Прямое подключение к телефонному номеру без выхода в Интернет.
ing ing ing
<u>Что такое VPN-подключение?</u>
Отмена

• Пишем в поле «Интернет-адрес:» adm2-vpn.dns-shop.ru и в поле «Имя местонахождения:» VPN-ADM. После этого нажимаем «Далее»

Подключение к рабоче	ему месту	
Введите Интернета-	адрес для подключения	
Этот адрес можно получи	ть у сетевого администратора.	
Интернете-адрес:	adm2-vpn.dns-shop.ru	
Имя местоназначения:	VPN-ADM	
 Использовать смар Разрешить исполь Этот параметр позв компьютеру, исполь Не подключаться с 	от-карту зовать это подключение другим пользователям воляет любому пользователю, имеющему доступ к этом льзовать это подключение. :ейчас, только выполнить установку для подключения в	У будущем
	Далее	Отмена

• Указываем параметры вашей учётной записи, а также заполняем поле «Домен» **PARTNER.RU** .

9	Падключение к расоч	ему месту		
	Введите имя пользон	зателя и пароль		
	<u>П</u> ользователь:			
	Паро <u>л</u> ь:			
		Отобра <u>ж</u> ать вводимые знаки		
	До <u>м</u> ен (не обязательно):			
			Подк	л <u>ю</u> чить Отмена

• Нажимаем кнопку «Пропустить»

🌍 🌆 Подключение к рабочему месту	
Установка связи с VPN-подключение 4	
N	
Порт открыт.	
	опустить Отмена

• Нажимаем «Закрыть»

🙆 🗽 Подключение к рабочему месту	
Полключение готово к использованию	
Подключение тотово к использованию	
i i	
Подключиться <u>с</u> ейчас	
\	
	<u>З</u> акрыть

• Открываем «Изменение параметров адаптера»

🕞 📲 « Сеть и Интернет	• Центр управления сетями и общим досту	том 👻 😽 Поиск в панели управления	
Панель управления - домашняя страница Управление беспроводными сетями Изменение параметров	Просмотр основных сведений о Армін-ПК (этот компьютер)	сети и настройка подключений ——— Ф Интернет Сетей Интернет	•
адаптера	Просмотр активных сетей	Подключение или отключение	
Изменить дополнительные параметры общего доступа	Сіясо 5 Домашняя сеть	Тип доступа: Интернет Домашняя группа: Присоединен Подключения: Беспроводное сетевое соединение (Cisco)	
	Неопознанная сеть Общественная сеть	Тип доступа: Без доступа к сети Подключения: VirtualBox Host-Only Network VMware Network Adapter VMnet1 VMware Network Adapter VMnet8	
	Изменение сетевых параметров		
	Настройка нового подключения Настройка беспроводного, шир или же настройка маршрутизате	или сети окополосного, модемного, прямого или VPN-подключения зра или точки доступа.	
См. также	Подключиться к сети Подключение или повторное по сетевому соединению или подкл	дключение к беспроводному, проводному, модемному ючение к VPN.	
Брандмауэр Windows Домашняя группа Свойства борузера	Выбор домашней группы и пара Доступ к файлам и принтерам, р	метров общего доступа асположенным на других сетевых компьютерах, или	

• Находим созданное подключение, нажимаем правой кнопкой мыши на данном значке, выбираем пункт «Свойства»



• Открываем вкладку «Безопасность». Шифрование данных Обязательное.

📱 VPN-подключение - свойства 🛛 🗙
Общие Параметры Безопасность Сеть Доступ
<u>I</u> ил VPN:
Автоматически
Дополнит <u>е</u> льные параметры
шифрование данных.
обязательное (отключиться, если нет шифрования) 💽
Проверка подлинности
О Протокол расширенной проверки подлинности (ЕАР)
_
• Разрешить следующие протоколы
Для VPN типа IKE v2 будет использован EAP-MSCHAPv2. Для других типов VPN выберите любые из этих протоколов.
<u>Н</u> езашифрованный пароль (РАР)
Протокол проверки пароля (СНАР)
✓ Протокол Microsoft <u>CHAP</u> версии 2 (MS-CHAP v2)
Использовать автоматически имя входа и пароль Windows (и имя домена, если существует)
ОК Отмена

Выбираем «Тип VPN» - L2TP IPSec VPN.

🚦 VPN-подключение - свойства 🗙
Общие Параметры Безопасность Сеть Доступ Тип VPN:
Автоматически
Автоматически Тилиод и и и претекол точка-точка (РРТР)
ISOTT (Secure Society Tunneling Protocol)
Проверка подлинности
О Протокол расширенной проверки подлинности (ЕАР)
Разрешить следующие протоколы
Для VPN типа IKEv2 будет использован EAP-MSCHAPv2. Для других типов VPN выберите любые из этих протоколов.
<u>Н</u> езашифрованный пароль (РАР)
Протокол проверки пароля (СНАР)
✓ Протокол Microsoft <u>C</u> HAP версии 2 (MS-CHAP v2)
Использовать автоматически имя входа и пароль Windows (и имя домена, если существует)
ОК. Отмена

 Нажимаем кнопку «Дополнительные параметры», выбираем «Для проверки подлинности использовать предварительный ключ», заполняем поле «Ключ» данным значением 109086613.
 Нажимаем «ОК» в окне «Дополнительные свойства»

🌀 🌖 🖉 🔻 Панель управления 🔻 Сеть и Интернет 👻 Сете	вые подключения 👻 😴 🛃	Поиск: Сетевые подключения	
Упорядочить • Запуск подключения Переименование по	ключения Удаление подключения Настройка параметров подключения	<u>8</u> : -	
VPN-подключение Подключ	е 😫 VPN-подключение - свойства 📉		
WAN Miniport (KEv2)	СТ Общие Паранитры Безопасность Сеть Доступ		
	In VPN:		
	L2TP IPsec VPN		
	Дополнит ульные параметры		
	Шифрование данных		
	аблазательное (отключиться, если нет шифрования) Дополнительные свойства	×	
	Проверка подличности L2TP		
	 Протокол расширенной проверки подличности (с. 		
	• Для проверки подличности использов-	ать предварительный ключ	
	Paspeшims следующие протоколы Ключ: 109086613		
	Проверить атрибуты имени и испол	пьзования у сертификата	
	E Hanamatorenan di savona (PAP)		
	Протокол проверхи пароля (CHAP)		
	P Протокол Microsoft QHAP версии 2 (MS-CHAP v		
	Использовать автоматически имя входа и		
	napone Windows (и иня домена, если сишествият)	OK OTHEHS	
	OK Orivetiva		

• Далее открываем вкладку «Сеть», выбираем «Протокол Интернета версии 4», щелкаем «Свойства»:



• В новом окне щелкаем на пункт «Дополнительно», снимаем галочку с пункта «Использовать основной шлюз удаленной сети:

До	полнительные параметры ТСР/ІР
1	Параметры IP DNS WINS
	Этот флажок используется только при одновременном подключении к локальной сети и к сети удаленного доступа. Если флажок установлен, данные, которые не удается передать через локальную сеть, направляются в сеть удаленного доступа.
	Использовать основной шлюз в удаленной сети Отключить добавление маршрута, основанное на классе
	И Автоматическое назначение метрики
	Метрика интерфейса:

Нажимаем на всех открытых окнах настроек «Ок»

На этом настройка завершена. Само подключение активируется двойным щелчком в общем списке подключений: