

Инструкция по настройке автоматизированного рабочего места пользователя на базе операционной системы Windows для подключения посредством ViPNet TLS Gateway к СЭД «Диалог» и подписания электронных документов в нем ключом электронной подписи

СЭД «Диалог» является Web-приложением, для доступа к которому на автоматизированном рабочем месте пользователя должны быть установлены браузер и средство криптографической защиты информации (криптопровайдер) с поддержкой российских ГОСТ-алгоритмов, а также специальный плагин для осуществления функции подписания электронных документов ключом электронной подписи.

В настоящей Инструкции представлена схема общего алгоритма настройки автоматизированных рабочих мест на операционной системе Windows для подключения посредством ViPNet TLS Gateway к СЭД «Диалог» и описан процесс установки и настройки сертифицированного средства криптографической защиты информации КриптоПро CSP 4.0, плагина КриптоПро ЭЦП Browser plugin и браузера Chromium ГОСТ.

Для обеспечения подключения к СЭД «Диалог» на автоматизированном рабочем месте пользователя СЭД «Диалог» необходимо:

1) Установить на автоматизированном рабочем месте браузер Chromium GOST, поддерживающий соединение по протоколу TLS. Скачать дистрибутив можно по ссылке:

2) Установить одно из предложенных ниже средств криптографической защиты информации (одно на Ваш выбор):

- КриптоПро CSP;
- ViPNet CSP;
- ViPNet Client .

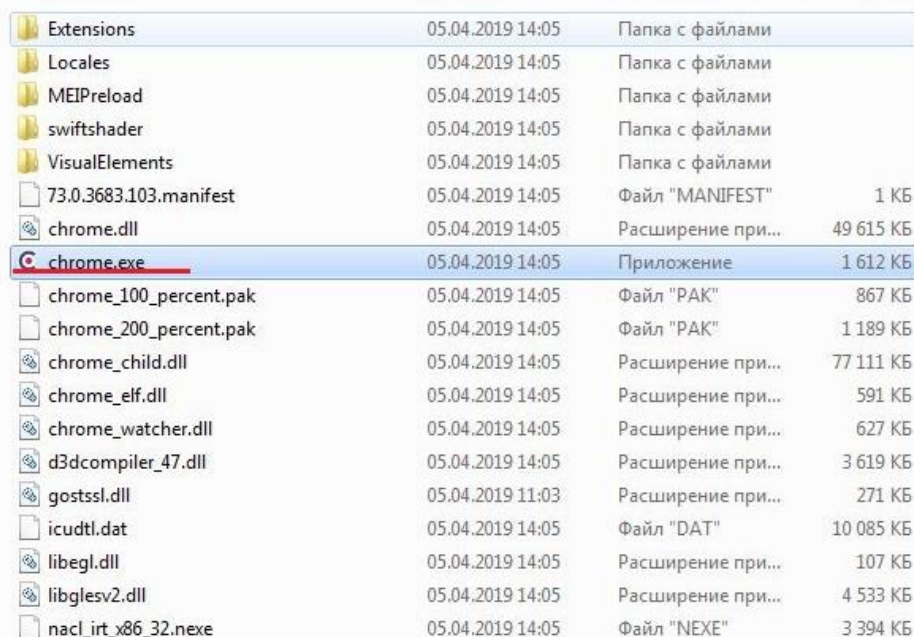
3) Установить корневые сертификаты и списки отозванных сертификатов Головного удостоверяющего центра (Минкомсвязь России) и удостоверяющего центра «ИнфоТекС Интернет Траст».

4) Для работы с ключом электронной подписи дополнительно необходимо установить плагин КриптоПро-ЭЦП-Browser-plugin.

Обращаем Ваше внимание на то, что перед установкой вышеуказанных компонентов на рабочей станции с операционной системой Windows должны быть установлены **все обновления безопасности**.

1. Браузер Chromium GOST.

Браузер Chromium GOST не нуждается в установке на рабочем месте с операционной системой Windows. Вам необходимо скачать архив по ссылке (<https://github.com/deemru/chromium-gost/releases/latest>) и распаковать его в удобную для Вас папку. После распаковки найдите в ней файл *chrome.exe* и запустите его.



Extensions	05.04.2019 14:05	Папка с файлами	
Locales	05.04.2019 14:05	Папка с файлами	
MEIPreload	05.04.2019 14:05	Папка с файлами	
swiftshader	05.04.2019 14:05	Папка с файлами	
VisualElements	05.04.2019 14:05	Папка с файлами	
73.0.3683.103.manifest	05.04.2019 14:05	Файл "MANIFEST"	1 КБ
chrome.dll	05.04.2019 14:05	Расширение при...	49 615 КБ
chrome.exe	05.04.2019 14:05	Приложение	1 612 КБ
chrome_100_percent.pak	05.04.2019 14:05	Файл "PAK"	867 КБ
chrome_200_percent.pak	05.04.2019 14:05	Файл "PAK"	1 189 КБ
chrome_child.dll	05.04.2019 14:05	Расширение при...	77 111 КБ
chrome_elf.dll	05.04.2019 14:05	Расширение при...	591 КБ
chrome_watcher.dll	05.04.2019 14:05	Расширение при...	627 КБ
d3dcompiler_47.dll	05.04.2019 14:05	Расширение при...	3 619 КБ
gostssl.dll	05.04.2019 11:03	Расширение при...	271 КБ
icudtl.dat	05.04.2019 14:05	Файл "DAT"	10 085 КБ
libegl.dll	05.04.2019 14:05	Расширение при...	107 КБ
libglesv2.dll	05.04.2019 14:05	Расширение при...	4 533 КБ
nacl_irt_x86_32.nexe	05.04.2019 14:05	Файл "NEXE"	3 394 КБ

Для удобства Вы можете создать его ярлык и вывести на Рабочий стол.

2. Установка средства криптографической защиты информации КриптоПро CSP

При отсутствии в Вашей организации дистрибутивов указанных выше средств криптографической защиты информации, Вы можете скачать КриптоПро CSP или ViPNet CSP с официальных сайтов их производителей (ООО «КРИПТО-ПРО», ОАО «ИнфоТеКС») бесплатно, но только для авторизованных пользователей.

- КриптоПро CSP (https://www.cryptopro.ru/products/csp/downloads#latest_csp40r4);
- ViPNet CSP (<https://infotecs.ru/downloads/besplatnye-produkty/vipnet-csp.html>);

3. Установка корневых сертификатов и списков отозванных сертификатов для работы TLS

Необходимо установить корневые сертификаты и списки отозванных сертификатов удостоверяющего центра, выпустившего сертификат ключа проверки электронной подписи, обеспечивающий работу защищенного TLS соединения.

Установка любых сертификатов, в том числе корневых сертификатов, и списков отозванных сертификатов должна выполняться под учетной записью пользователя СЭД «Диалог», чтобы сертификаты поместились в хранилища сертификатов пользователя.

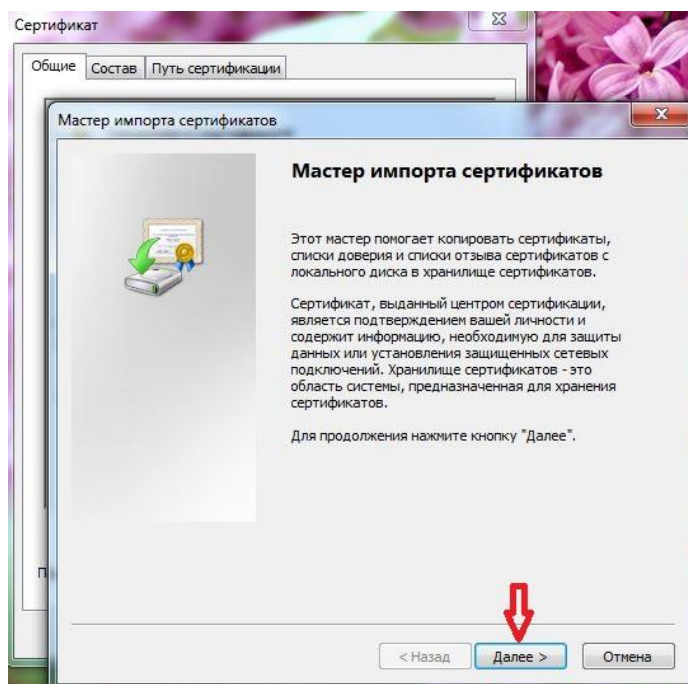
1) Необходимо скачать корневые сертификаты Минкомсвязи России и Удостоверяющего центра ООО «ИИТ», перейдя по следующим ссылкам:

<http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=4BC6DC14D97010C41A26E058AD851F81C842415A>
[http://uc1.iitrust.ru/uc/CA-ИИТ-\(К3\)-2018.cer](http://uc1.iitrust.ru/uc/CA-ИИТ-(К3)-2018.cer)

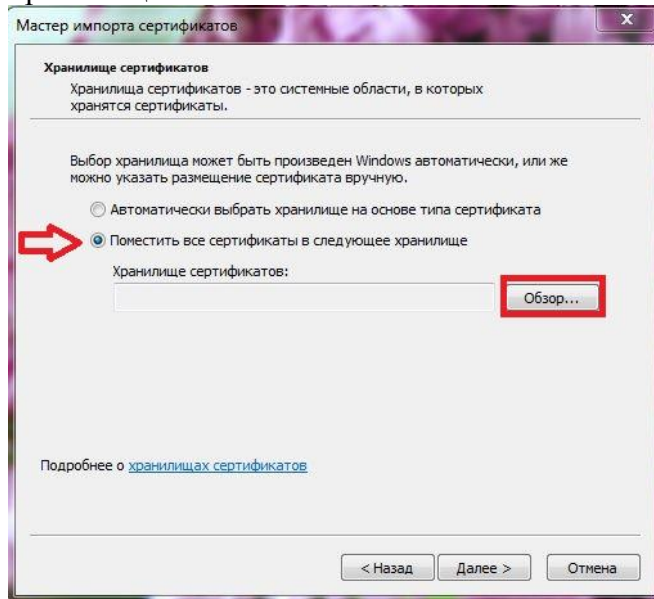
2) Необходимо скачать списки отозванных сертификатов Минкомсвязи России и Удостоверяющего центра ООО «ИИТ», перейдя по следующим ссылкам:

http://reestr-pki.ru/cdp/guc_gost12.crl
[http://uc1.iitrust.ru/uc/CA-ИИТ-\(К3\)-2018.crl](http://uc1.iitrust.ru/uc/CA-ИИТ-(К3)-2018.crl)

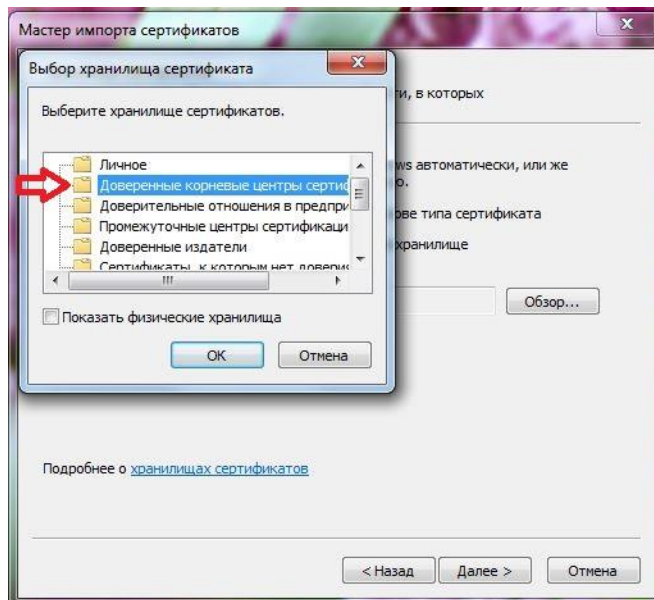
Для установки корневого сертификата необходимо нажать правой кнопкой мыши по файлу корневого сертификата и выбрать пункт меню «Установить сертификат» после чего откроется мастер импорта сертификатов.



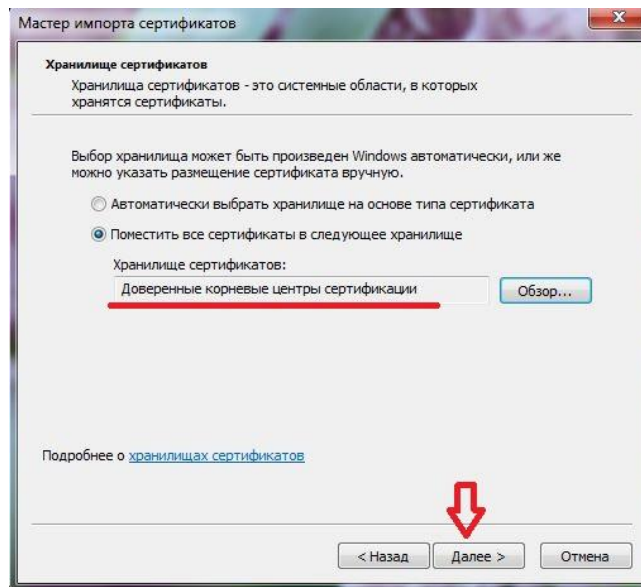
Выберите значение «Поместить все сертификаты в следующее хранилище» и нажмите на кнопку «Обзор» для выбора хранилища.



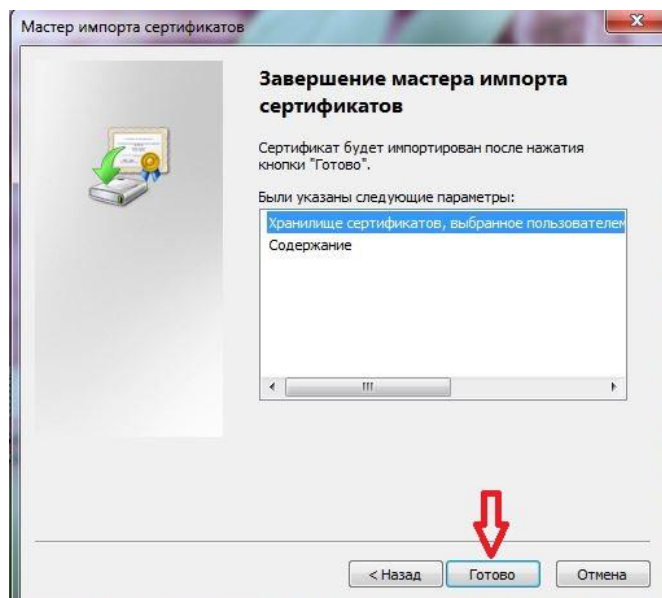
В открывшемся окне выберите хранилище «Доверенные корневые центры сертификации».



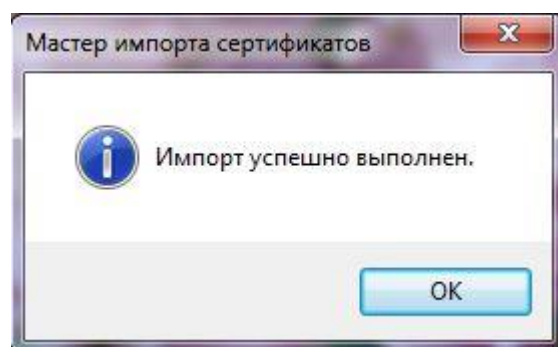
Убедитесь, что выбрали верное хранилище и нажмите на кнопку «Далее».



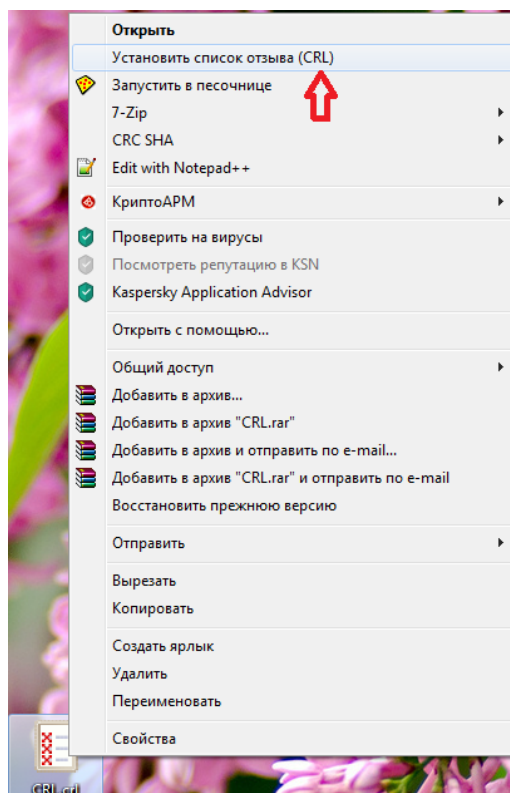
Нажмите на кнопку «Готово».



Дождитесь подтверждения завершения операции импорта сертификата.



Для установки **списков отозванных сертификатов** на рабочее место Вам необходимо вызвать контекстное меню списка отозванных сертификатов путем клика правой кнопкой мыши и выбрать в нем «Установить список отзыва (CRL)».



После этого у вас запустится Мастер импорта сертификатов и дальнейшая установка происходит по аналогии с установкой корневого сертификата.

4. Установка плагина КриптоПро-ЭЦП-Browser-plugin

Для работы с ключом электронной подписи необходимо установить плагин КриптоПро-ЭЦП-Browser-plugin. Для этого необходимо скачать его с сайта КриптоПро <https://www.cryptopro.ru/> (только для авторизованных пользователей), пройдя по пунктам меню:

Загрузка / КриптоПро CSP / КриптоПро ЭЦП Browser plug-in / [КриптоПро ЭЦП Browser plug-in 2.0](#) и скачать версию для ОС вашей рабочей станции.

Запустите установку установку плагина КриптоПро-ЭЦП-Browser-plugin двойным щелчком левой кнопки мыши.

На этом настройка автоматизированного рабочего места завершена.

Пользователь может осуществлять вход в СЭД «Диалог» через браузер Chromium GOST по TLS-каналу.

После сохранения карточки документа для подписания электронного документа ключом электронной подписи необходимо дополнительно установить корневые сертификаты и списки отозванных сертификатов удостоверяющего центра, выдавшего Вам сертификат ключа проверки электронной подписи, и в СЭД «Диалог» в карточке документа нажать на кнопку «Подписать», выбрать пункт выпадающего меню «Квалифицированная электронная подпись», разрешить КриптоПро CSP выполнить операцию с ключами и сертификатами от имени пользователя и выбрать в выпадающем пункте меню ключ электронной подписи, которым пользователь хочет подписать электронный документ (в СЭД «Диалог» в качестве идентификатора ключа указывается отпечаток сертификата ключа проверки электронной подписи).

ВАЖНЫЕ НЬЮАНСЫ

Настройка работы ViPNet CSP И КРИПТОПРО CSP на одной рабочей станции

СКЗИ ViPNet CSP может быть установлена на одном компьютере с СКЗИ КриптоПро CSP. Однако при этом необходимо соблюдать следующие условия:

- Если для выполнения криптографических операций в поддерживаемых приложениях требуется использовать криптопровайдер ViPNet CSP:
 - Убедитесь, что компонент ПО КриптоПро CSP «Совместимость с продуктами Microsoft» не был ранее установлен на компьютере.
 - В программе ViPNet CSP в разделе «Дополнительно» установите флажок Поддержка работы ViPNet CSP через Microsoft CryptoAPI
- Если для выполнения криптографических операций в поддерживаемых приложениях требуется использовать криптопровайдер КриптоПро CSP:
 - В программе ViPNet CSP в разделе Дополнительно уберите флажок Поддержка работы ViPNet CSP через Microsoft CryptoAPI.
 - Убедитесь, что компонент ПО КриптоПро CSP «Совместимость с продуктами Microsoft» установлен на компьютере.
 - Для заверения электронной подписью документов Microsoft Office необходимо дополнительно установить программу КриптоПро Office Signature.

Внимание! Не следует устанавливать на компьютер компонент СКЗИ КриптоПро CSP «Совместимость с продуктами Microsoft», если в ViPNet CSP установлен флажок Поддержка работы ViPNet CSP через Microsoft CryptoAPI.

Несоблюдение вышеуказанной рекомендации может привести к нестабильной работе отдельных программ или операционной системы в целом (вплоть до невозможности её загрузки). Также рекомендуем удостовериться в наличии контрольной точки восстановления системы, а в случае её отсутствия – создать её.

По умолчанию после установки СКЗИ ViPNet CSP на компьютер с уже установленным СКЗИ КриптоПро CSP флажок Поддержка работы ViPNet CSP через Microsoft CryptoAPI снят. В этом случае непосредственно после установки криптографические операции продолжают выполняться с помощью СКЗИ КриптоПро CSP.

Если на вашем компьютере установлены СКЗИ ViPNet CSP и СКЗИ КриптоПро CSP и вы хотите удалить СКЗИ ViPNet CSP, то во избежание потери работоспособности ОС выполните следующие действия:

1. Удалите ViPNet CSP и не перезагружайте компьютер.
2. Запустите установочный файл КриптоПро CSP и восстановите компоненты ПО.
3. Перезагрузите компьютер.

Если на вашем компьютере установлены СКЗИ ViPNet CSP и СКЗИ КриптоПро CSP и вы хотите удалить ПО КриптоПро CSP, то во избежание потери работоспособности ОС выполните следующие действия:

1. Удалите КриптоПро CSP и не перезагружайте компьютер.
2. Запустите установочный файл ViPNet CSP и восстановите компоненты программы.
3. Перезагрузите компьютер.

Возможные ошибки

1) Убедитесь, что вводите адрес <https://tls.krtech.ru>. Подключение по <http://tls.krtech.ru> невозможно.

2) В случае, если у Вас на рабочем месте установлена операционная система Windows 7, может возникнуть **ошибка соединения с сервером**. В этом случае вам понадобится либо установить обновление операционной системы по ссылке (<https://support.microsoft.com/en-za/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi>), либо добавить в реестр компьютера следующие папки и файлы:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client

DisabledByDefault dword:00000000

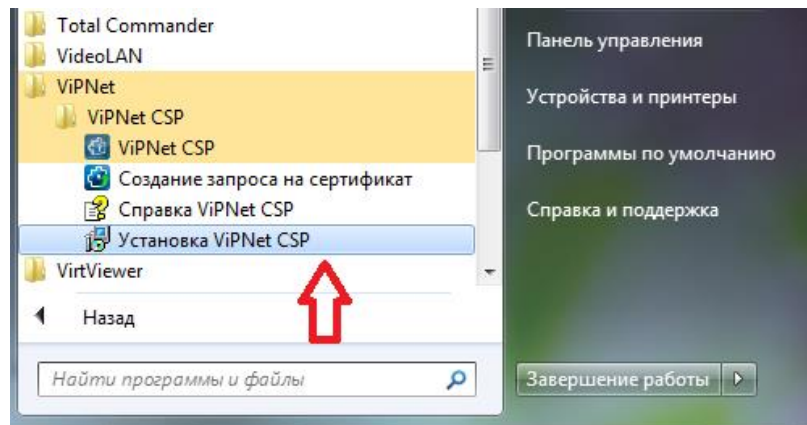
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client

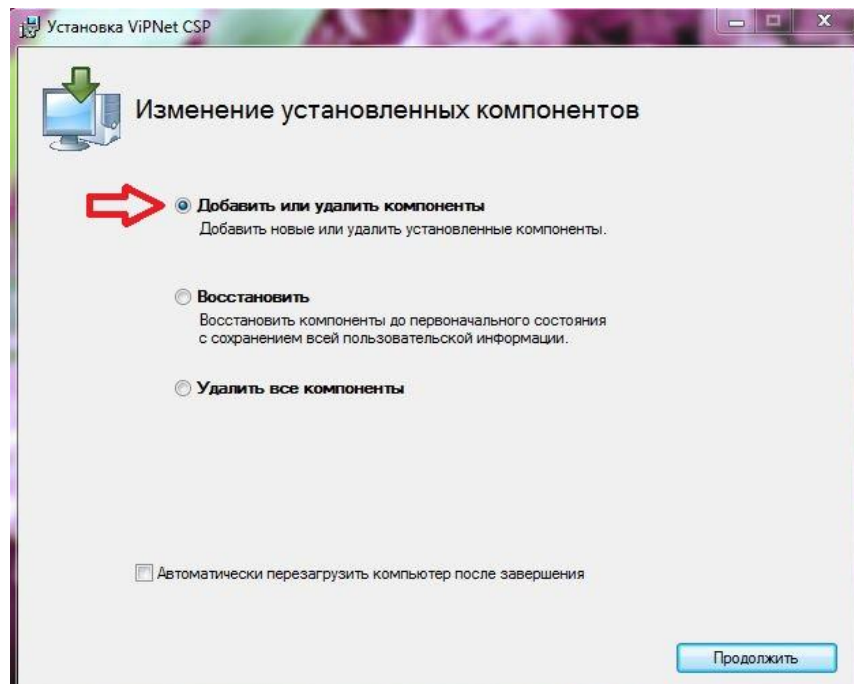
DisabledByDefault=dword:00000000

3) При установке ViPNet CSP на компьютер, работающий под управлением ОС Windows 10 или Windows Server 2016, а также при установке программы ViPNet CSP в составе ПО ViPNet Client, поддержка протокола TLS/SSL **отключена**.

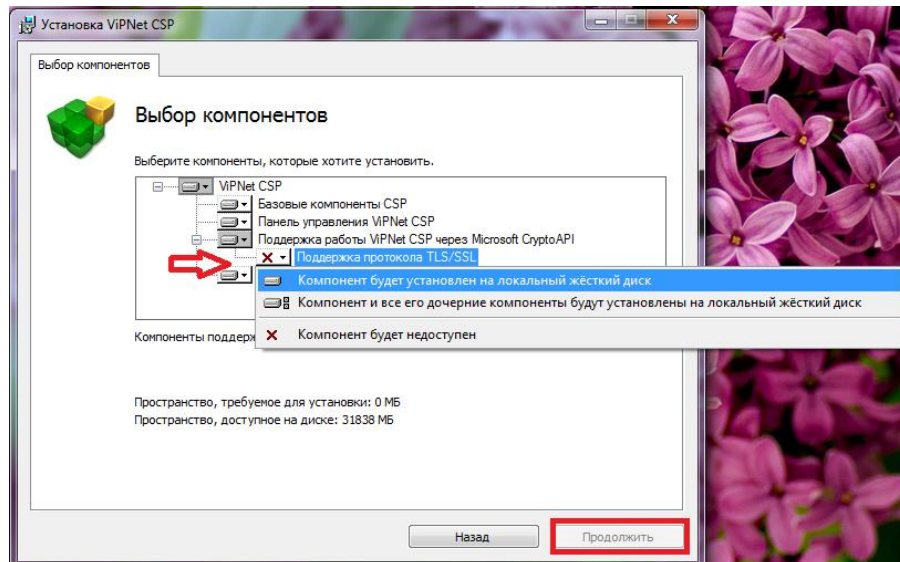
Чтобы включить поддержку протокола, в меню Пуск выберите Все программы > ViPNet > ViPNet CSP, щелкните Установка ViPNet CSP.



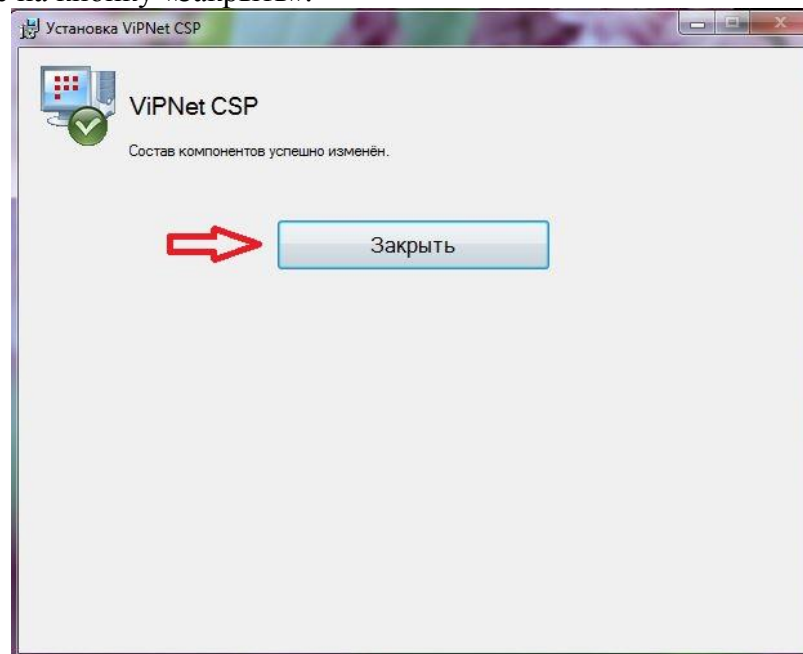
В открывшемся окне выберите «Добавить или удалить компоненты» и нажмите на кнопку «Продолжить».



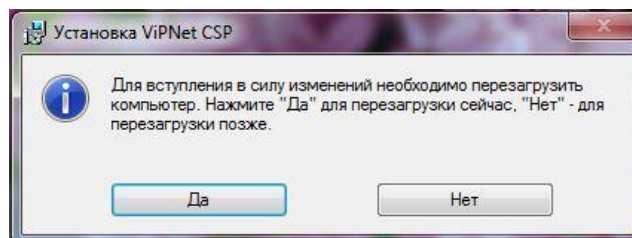
В следующем окне раскройте список Поддержка работы ViPNet CSP через MS Crypto API и добавьте компонент Поддержка протокола TLS/SSL.



После выбора компонента кнопка «Продолжить» станет активной. Нажмите на нее и дождитесь завершения установки компонента. После появления уведомления об изменении состава компонентов, нажмите на кнопку «Закреть».



После этого программа предложит перезагрузить компьютер.



После перезагрузки повторите попытку подключения к tls.krtech.ru.

В случае, если на Windows не установлены все обновления безопасности, могут возникать различного рода ошибки, например, выявляться отсутствие **алгоритма хэширования SHA-256**.

Для решения данной проблемы необходимо скачать и установить пакет обновления Windows **KB4474419**

<https://www.catalog.update.microsoft.com/Search.aspx?q=4474419>

В случае с ошибками аналогичного характера – решение то же – найти и скачать недостающий пакет обновления безопасности Windows.