ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ СЕРВЕРА РАСКРЫТИЯ ИНФОРМАЦИИ «ПРАЙМ» ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Общая информация

Технология электронной подписи (ЭП) реализуется на связке открытого и закрытого ключа.

Закрытый ключ – уникальная последовательность символов, с помощью которой формируется каждая электронная подпись. Закрытый ключ хранится на ключевом носителе (токене) и защищен паролем, который известен только владельцу. Работает закрытый ключ только в паре с открытым ключом.

Открытый ключ – известен всем пользователям системы и необходим для проверки электронной подписи. С его помощью получатель документа устанавливает авторство документа и неизменность документа после подписания.

Токен – это миниатюрное устройство, необходимое для надёжного хранения персональных данных и для авторизации пользователя. Внешне токен напоминает обычную USB-флешку и имеет защищённую память, в которой содержится важнейшая информация: ключи шифрования, пароли, цифровые сертификаты. В основе устройства лежит специальная микросхема с защищённой памятью. Предусмотрено непосредственное подключение к ПК через USB-порт.

Разновидности токенов:

RuToken – это один из наиболее популярных видов ключевых носителей в России. Выглядит как флешка красного либо синего цвета, и при использовании вставляется в USB-порт. Считается одним из наиболее безопасных ключевых носителей и отличается сравнительно невысокой ценой. Разработан и изготавливается на территории России.

eToken – европейский вариант ключевого носителя, средство хранения информации и аутентификации, поддерживающее работу с электронной подписью и цифровыми сертификатами. Наряду с RuToken, является одним из наиболее безопасных ключевых носителей.

Для применения электронной подписи на сервере раскрытия информации ПРАЙМ пользователю необходимо:

Шаг 1. Приобретение пользователем ключа ЭП в удостоверяющем центре.

- Список удостоверяющих центров, авторизованных ЗАО «АЭИ «ПРАЙМ» см. в меню сайта раскрытия информации https://disclosure.1prime.ru/ «Список авторизованных удостоверяющих центров»

- Расширение сертификата пользователя «Улучшенный ключ» (объектный идентификатор 2.5.29.37) должно содержать объектный идентификатор на раскрытие информации **ПРАЙМ - OID 1.2.643.6.42.5.5.5**
- В переходный период с 1 февраля 2017 года по 1 декабря 2017 года Агентство вправе принимать к опубликованию электронные документы, содержащие публичную информацию, подписанные усиленной квалифицированной электронной подписью, которая не содержит объектный идентификатор вида 0.0.000.0.0.00.0.0.0 (Участник, имеющий право на раскрытие информации).

Шаг 2. Установка программного обеспечения к полученному в УЦ ключу ЭП

Для работы с электронной подписью (ЭП) на сайте раскрытия информации https://disclosure.1prime.ru/ пользователю необходимо установить на свой компьютер программное обеспечение к полученному в удостоверяющем центре (УЦ) ключу ЭП. Для этого необходимо обратиться в указанный удостоверяющий центр. Во многих удостоверяющих центрах установка всех компонентов и настройка рабочего места проходит в автоматическом режиме. Т.е. пользователю необходимо зайти на сайт УЦ и следовать пошаговым инструкциям.

Шаг 3. Установка Крипто-плагина

КриптоПро ЭЦП Browser plug-in предназначен для создания и проверки электронной подписи (ЭП) на веб-страницах с использованием СКЗИ "КриптоПро CSP". КриптоПро ЭЦП Browser plug-in легко встраивается и применим в любом из современных браузеров с поддержкой сценариев JavaScript: Internet Explorer; Mozilla Firefox; Opera; Google Chrome; Яндекс.Браузер; Apple Safari.Поддерживаемые операционные системы: Microsoft Windows; Linux; Apple iOS; Apple MacOS.

Скачать плагин «КриптоПро Browser Plugin» можно по ссылке

https://www.cryptopro.ru/products/cades/plugin

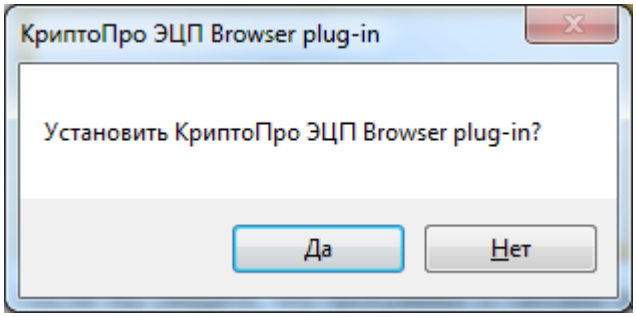
Актуальная версия плагина:

- версия 2.0 для пользователей (автоматическая загрузка версии плагина, соответствующей Вашей ОС)

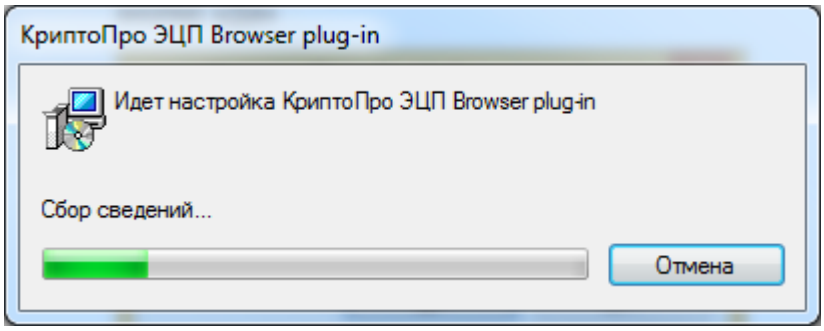
- Актуальная, развивающаяся версия, находится в процессе сертификации.
- Поддерживает работу с алгоритмами ГОСТ Р 34.10/11-2012 (при использовании с КриптоПро CSP 4.0 и выше).
- Для Microsoft Windows совместима с КриптоПро CSP версии 3.6 R4 и выше, для других ОС – с КриптоПро CSP версии 4.0 и выше.
- Компоненты КриптоПро TSP Client 2.0 и КриптоПро OCSP Client 2.0, входящие в данную версию, не принимают лицензию от версий 1.x.
- Минимальная поддерживаемая версия Microsoft Windows – Windows XP.
- Минимальная поддерживаемая версия Internet Explorer – IE9
- Firefox 52.0.2 не поддерживает работу плагина

В зависимости от версии операционной системы Windows, возможно надо будет подтвердить согласие на внесение изменений в компьютер, необходимо дать разрешение кликнув по кнопке «Да».

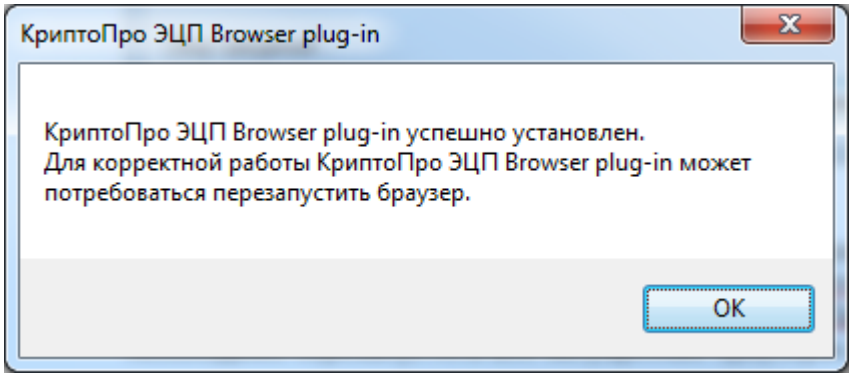
После этого Вы увидите окно с предложением установить плагин, необходимо кликнуть по кнопке «Да»



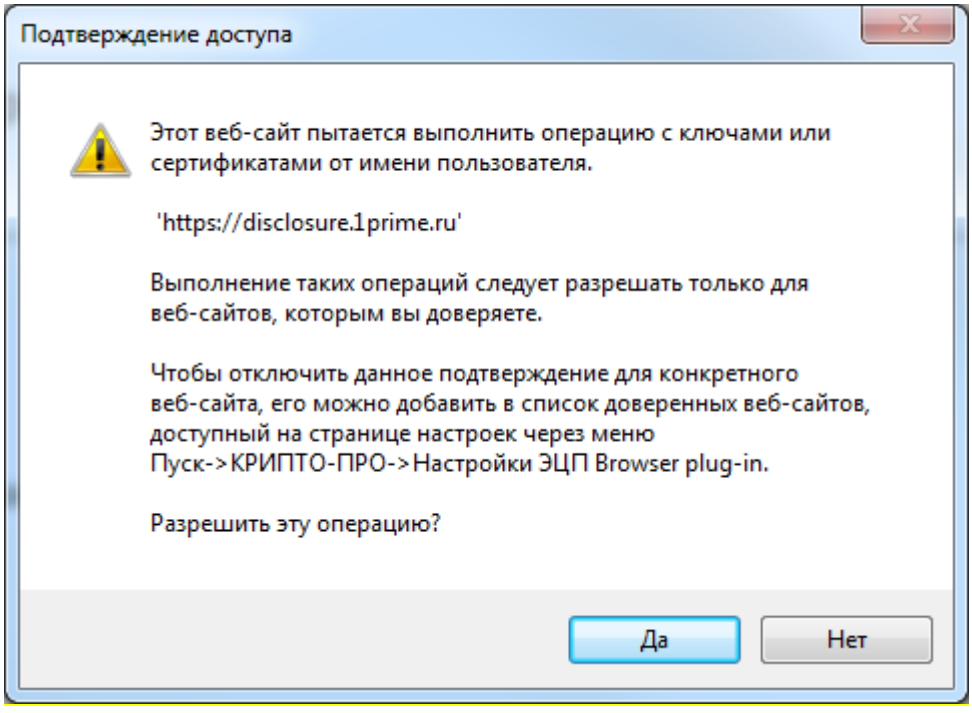
Далее должен начаться процесс установки, который займет немного времени.



По завершении процесса установки, Вы увидите окно с сообщением, что плагин «КриптоПро Browser Plugin» успешно установлен. Для корректной работы плагина, рекомендуется перезапустить все запущенные браузеры.



В некоторых браузерах по умолчанию запрещен запуск плагинов. Необходимо проверить разрешение на запуск «КриптоПро Browser Plugin» в используемом браузере, в случае необходимости разрешить запуск данного плагина (например, в браузере Internet Explorer нажать кнопку «Да». См. скриншот ниже).

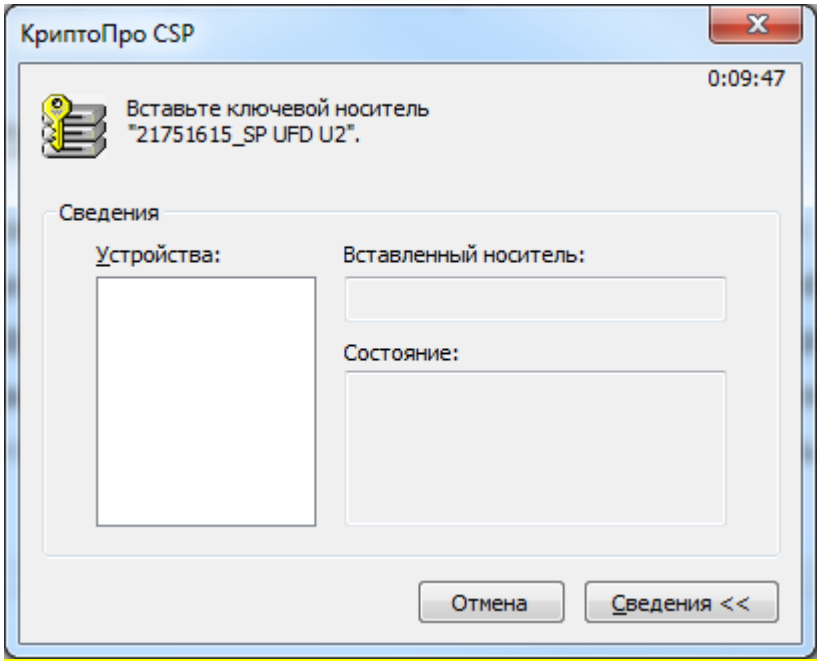


Более подробную инструкцию по установке плагина и тестовой проверке его работы см. http://cpdn.cryptopro.ru/default.asp?url=content/cades/plugin-installation.html

Шаг 4. Работа в ЛИЧНОМ КАБИНЕТЕ

В личном кабинете пользователя раскрытия информации после установки клиентом плагина при заполнении форм для публикации сообщения в Ленте раскрытия информации или размещении документа в сети Интернет, а также при изменении данных регистрационной карточки появятся дополнительные поля «Электронная подпись документа», где необходимо будет выбрать отображенный в соответствующем служебном поле сертификат ключа подписи и нажать кнопку «Подписать». Таким образом клиент будет подтверждать свои действия по раскрытию информации или внесению изменений в свою регистрационную карточку.

При нажатии кнопки «Подписать» на экране может появиться всплывающее окно с напоминанием, что пользователю необходимо вставить ключевой носитель (токен), если пользователь не сделал предварительно. Электронная подпись без применения ключевого носителя сервером раскрытия информации не принимается.



- После подписания электронной подписью сообщения клиенту необходимо нажать кнопку «Публиковать»
- После подписания электронной подписью документа клиенту необходимо нажать кнопку «Добавить документ».
- После подписания электронной подписью изменений в регкарточке клиенту необходимо нажать кнопку «Отправить идентификационный бланк».

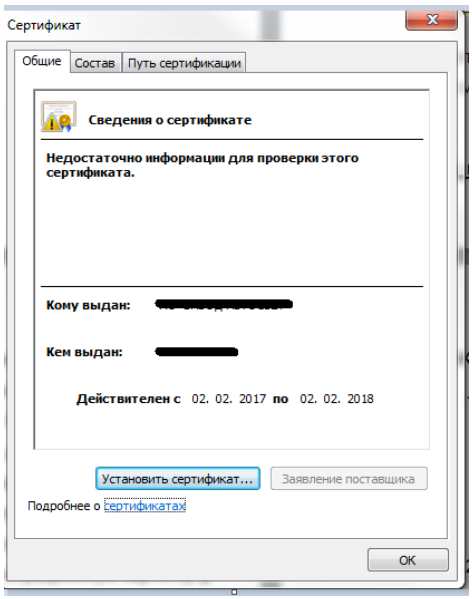
В остальном порядок действий эмитента в личном кабинете на сервере раскрытия информации «ПРАЙМ» не меняется.

КАК УЗНАТЬ подходит ли ключ для раскрытия после 02.12.2017:

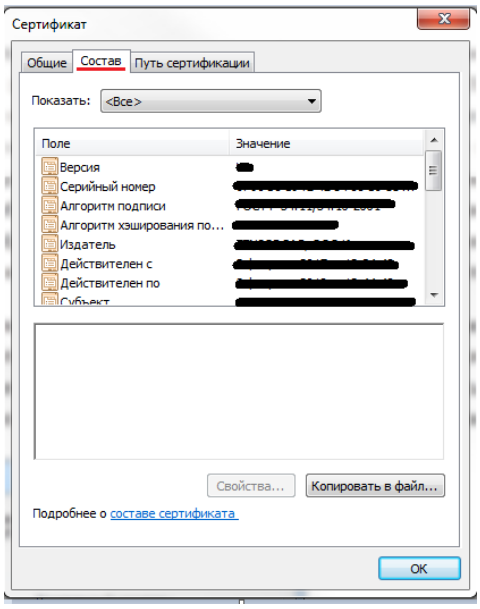
1. Скачайте открытую часть ключа с сайта (необходимо нажать на данный символ  около уже опубликованного сообщения)

1	Раскрытие эмитентом ежеквартального отчета	10.11.2017	10.11.2017	Загрузить
2	Раскрытие в сети Интернет списка аффилированных лиц	02.10.2017	02.10.2017	Загрузить

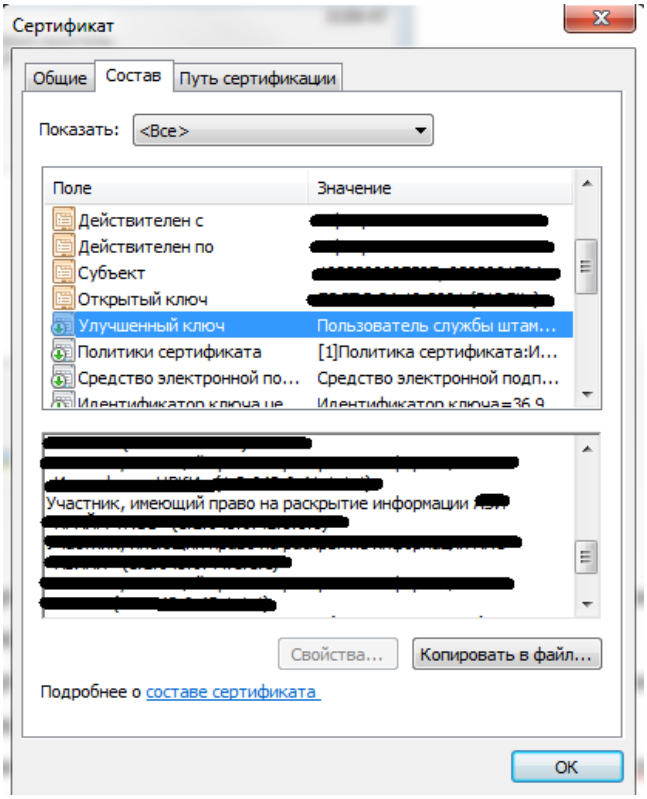
2. Откройте скачанный сертификат.



3. Выберете вкладку «Состав»



4. Необходимо выбрать поле «Улучшенный ключ», и в информации по данному полю найти информацию со словосочетанием «раскрытие информации»

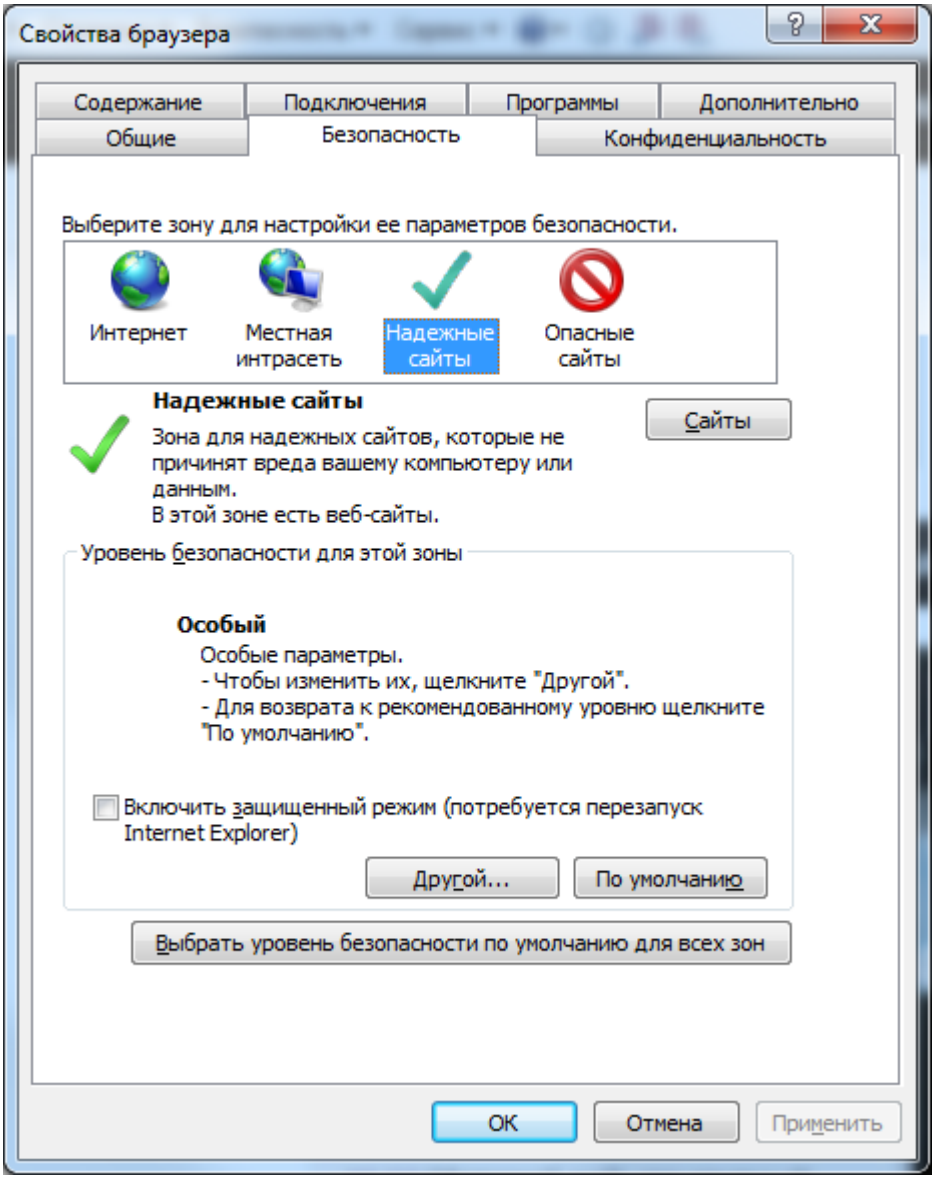

Сертификат
Общие
Состав
Путь сертификации
Показать:
<Все>
Поле
Значение
Действителен с
Действителен по
Субъект
Открытый ключ
Улучшенный ключ
Пользователь службы штам...
Политики сертификата
[1]Политика сертификата:И...
Средство электронной по...
Средство электронной подп...
Участник, имеющий право на раскрытие информации
Свойства...
Копировать в файл...
Подробнее о составе сертификата
OK

ЧАСТО ВОЗНИКАЮЩИЕ ВОПРОСЫ:

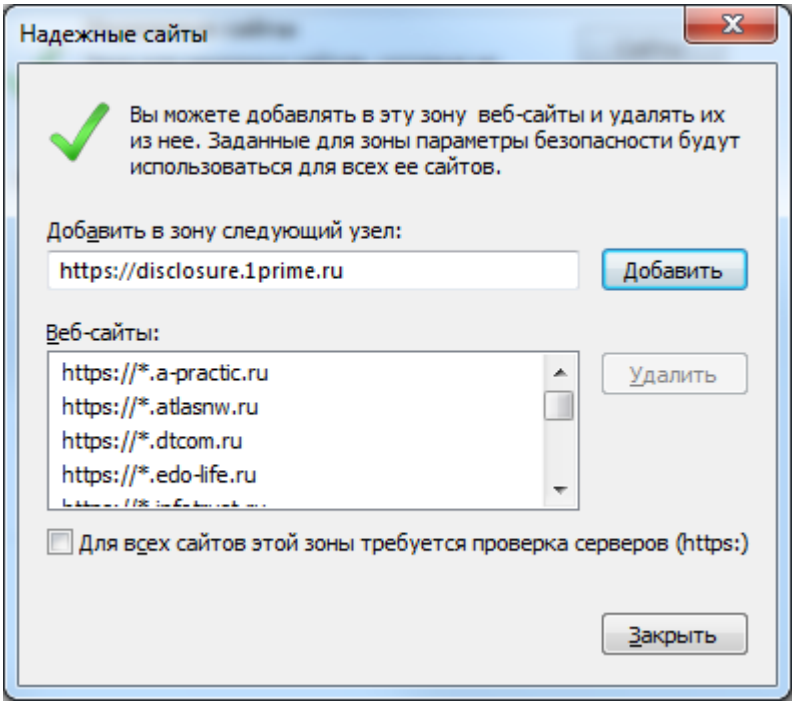
ЕСЛИ КРИПТО-ПЛАГИН ЗАГРУЖЕН, НО ДАННЫЕ ЭЛЕКТРОННОЙ ПОДПИСИ НЕ ВИДНЫ В КОНТЕЙНЕРЕ, ТО НЕОБХОДИМО:

1. Проверить корректность отражения подписи на сайте CryptoPro по ссылке: https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_file.html

   Если ключ не отражается по данной ссылке, то необходимо обратиться в УЦ выдавший ключ.
2. Проверить отображение электронной подписи во всех браузерах, которые установлены на компьютере (по причине настроек безопасности), либо внести сайт раскрытия информации «ПРАЙМ» https://disclosure.1prime.ru/ в список доверенных сайтов используемого браузера. Для этого необходимо в окне браузера (например, Internet Explorer) нажать кнопку «Сервис» на панели инструментов и выбрать пункт меню «Свойства браузера». Далее в окне «Свойства браузера» перейти на вкладку «Безопасность», выбрать зону «Надежные сайты» в списке зон для настройки безопасности и нажать кнопку «Сайты»



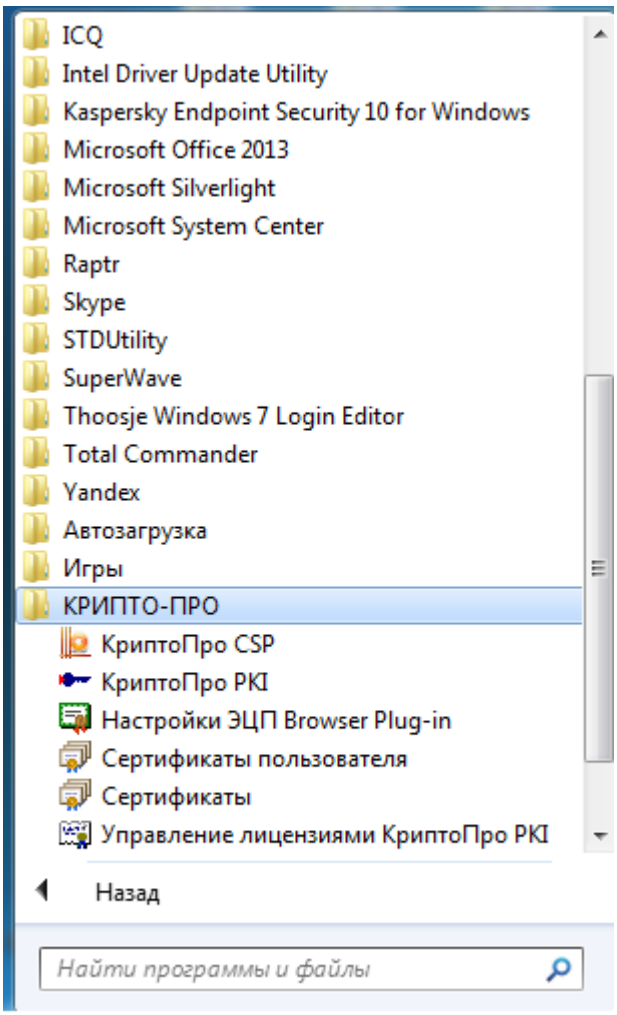
В окне «Надежные сайты» ввести адрес «https://disclosure.1prime.ru/» и нажать кнопку «Добавить», чтобы добавить указанный сайт в список надежных сайтов.

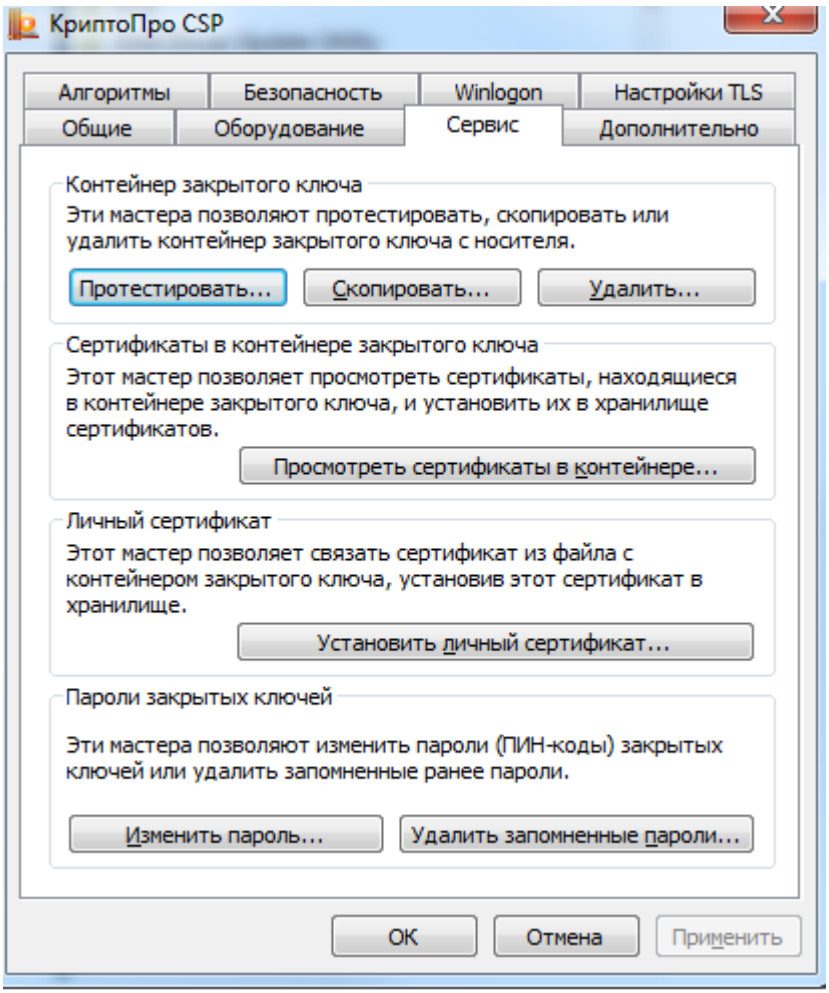


После добавления сайта https://disclosure.1prime.ru/ в список надежных нажать кнопку «Закрыть». После этого необходимо перезагрузить браузер.

3. Обратиться в удостоверяющий центр, где был приобретен ключ ЭП. На сайтах большинства УЦ есть сервисы по проверке ключа ЭП или настройке необходимого программного обеспечения. Если такого сервиса нет, то необходимо позвонить в службу технической поддержки удостоверяющего центра.

   Либо проверить наличие программного обеспечения к ключу ЭП или действительность сертификата ЭП на своем компьютере через кнопку «Пуск» (Пуск\Панель управления\КриптоПРО CSP\Сервис\Протестировать - по сертификату....).


ICQ
Intel Driver Update Utility
Kaspersky Endpoint Security 10 for Windows
Microsoft Office 2013
Microsoft Silverlight
Microsoft System Center
Raptr
Skype
STDUtility
SuperWave
Thoosje Windows 7 Login Editor
Total Commander
Yandex
Автозагрузка
Игры
КРИПТО-ПРО
КриптоПро CSP
КриптоПро PKI
Настройки ЭЦП Browser Plug-in
Сертификаты пользователя
Сертификаты
Управление лицензиями КриптоПро PKI
Назад
Найти программы и файлы


КриптоПро CSP
Алгоритмы
Безопасность
Winlogon
Настройки TLS
Общие
Оборудование
Сервис
Дополнительно
Контейнер закрытого ключа
Эти мастера позволяют протестировать, скопировать или удалить контейнер закрытого ключа с носителя.
Протестировать...
Скопировать...
Удалить...
Сертификаты в контейнере закрытого ключа
Этот мастер позволяет просмотреть сертификаты, находящиеся в контейнере закрытого ключа, и установить их в хранилище сертификатов.
Просмотреть сертификаты в контейнере...
Личный сертификат
Этот мастер позволяет связать сертификат из файла с контейнером закрытого ключа, установив этот сертификат в хранилище.
Установить личный сертификат...
Пароли закрытых ключей
Эти мастера позволяют изменить пароли (ПИН-коды) закрытых ключей или удалить запомненные ранее пароли.
Изменить пароль...
Удалить запомненные пароли...
OK
Отмена
Применить