



Приложение № 1

УТВЕРЖДЕНА

Приказом АО «Гринатом»

от _____ № _____

**Руководство настройки сертификата ключа проверки
электронной подписи пользователя, выпущенного на
алгоритмах шифрования ГОСТ Р 34.10-2012 для авторизации
на портале государственных услуг, использования ЗКПС**

Москва, 2018



Содержание

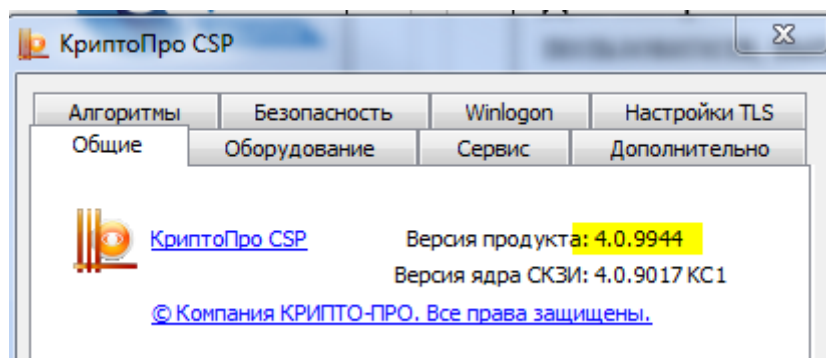
Настройка нового сертификата на АРМ пользователя	3
Установка цепочки сертификатов	5
Настройки браузера для доступа к portalу Госуслуг	6
Настройка защищенной корпоративной почтовой системы (ЗКПС)	9



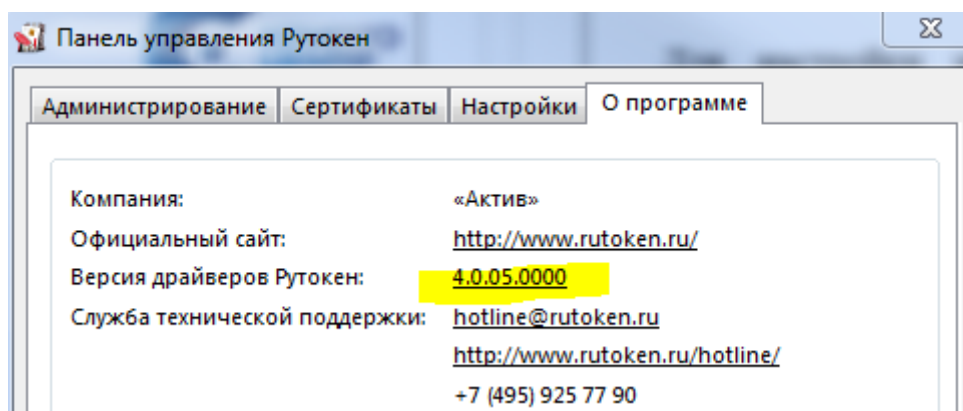
Настройка нового сертификата на АРМ пользователя

Для настройки сертификата ключа проверки электронной подписи пользователя, выпущенного на новых алгоритмах шифрования (ГОСТ Р 34.10-2012) необходимо:

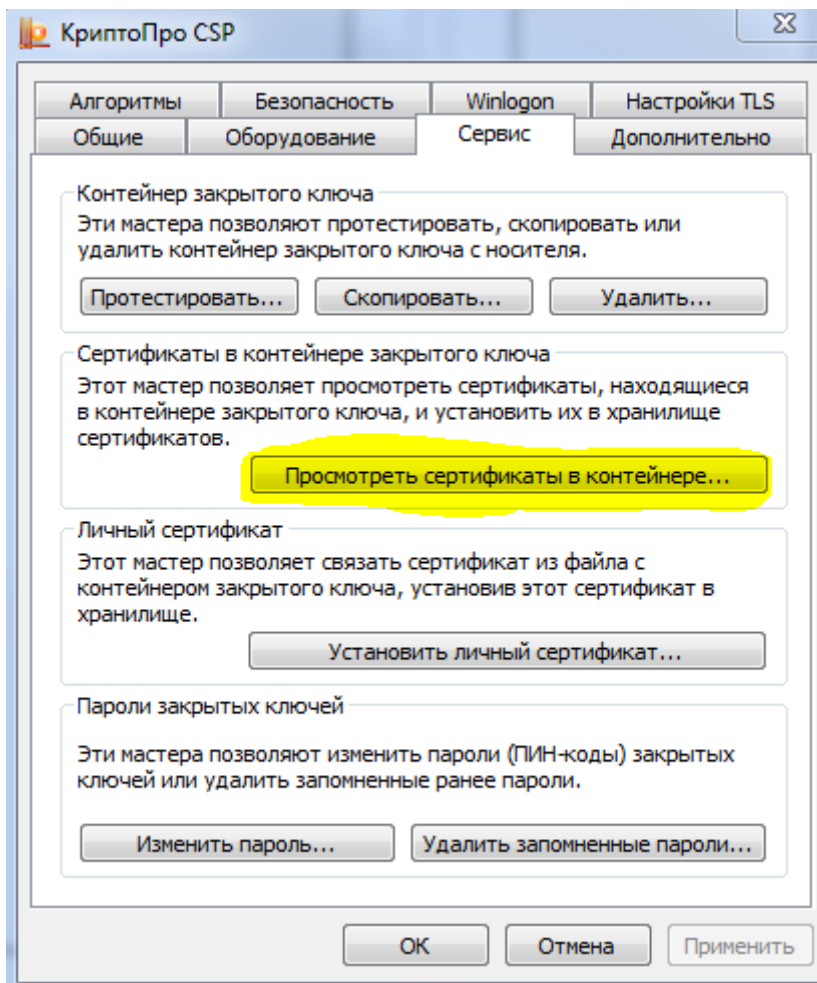
- 1) Убедиться, что установлена актуальная версия криптопровайдера СКЗИ Крипто Про CSP v. 4.0, сборка 9944 (R3). Для этого выполнить следующие действия: нажать «Пуск» в левом нижнем углу рабочего стола, найти программу «КриптоПро CSP», во вкладке «Общие» просмотреть версию продукта.



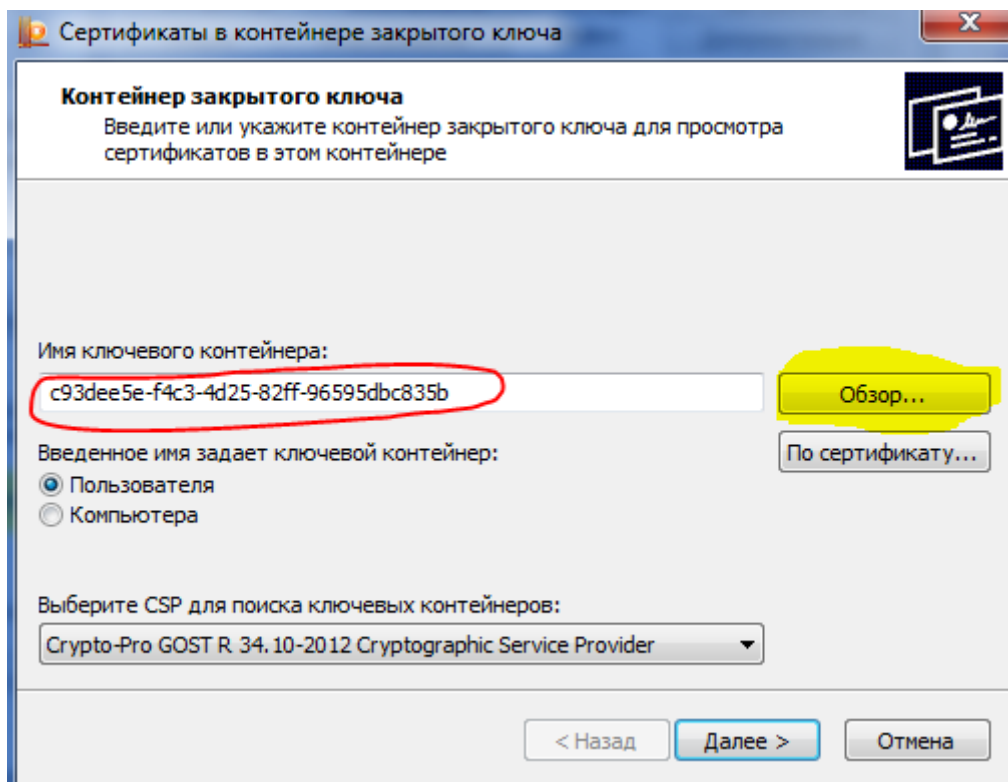
- 2) Убедиться, что установлена актуальная версия драйверов Рутокен (не ниже 4.0.05.0000). Для этого выполнить следующие действия: нажать «Пуск» в левом нижнем углу рабочего стола, найти программу «Панель управления Рутокен», во вкладке «О программе» просмотреть версию продукта.



- 3) Подсоединить носитель к АРМ пользователя. Установить новый сертификат пользователя с помощью оснастки СКЗИ КриптоПро CSP в личное Хранилище сертификатов. Для этого выполнить следующие действия: нажать «Пуск» в левом нижнем углу рабочего стола, найти программу «КриптоПро CSP», во вкладке «Сервис» просмотреть сертификаты в контейнере.

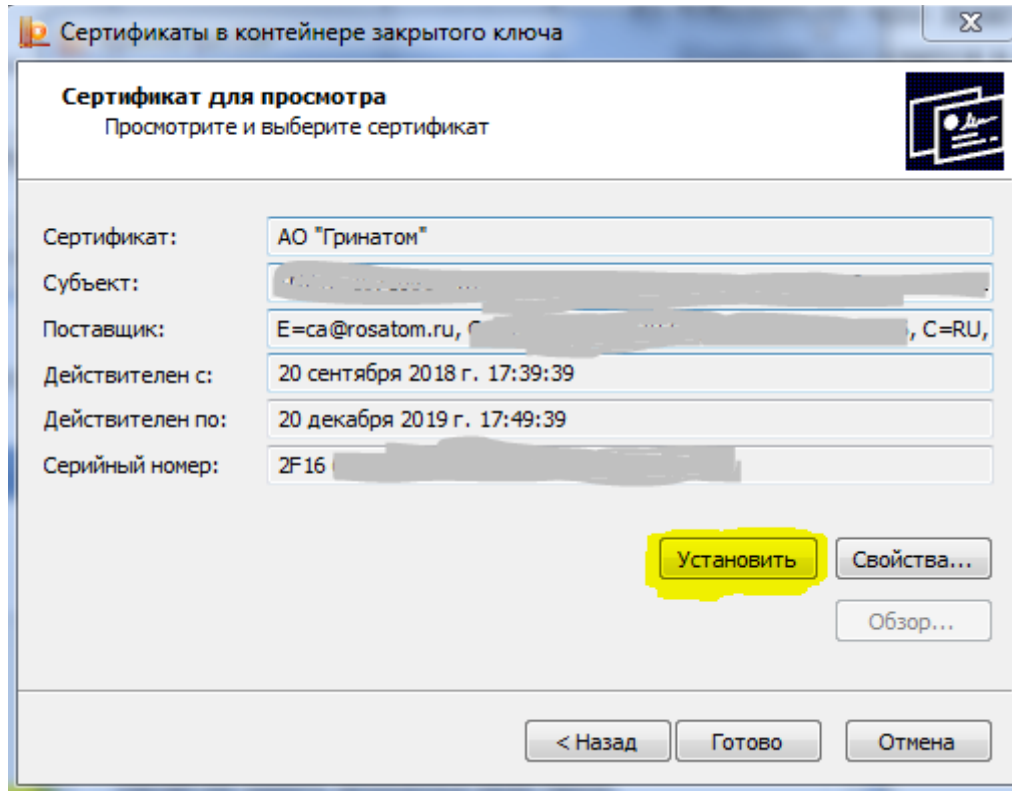


Далее через «Обзор» выбрать нужный ключевой контейнер и нажать «Далее».





Затем «Установить» и «Готово».



Установка цепочки сертификатов

- 4) Произвести установку сертификатов Головного удостоверяющего центра Минкомсвязи на новых алгоритмах шифрования, в соответствии с инструкцией от удостоверяющего центра АО «Гринатом», доступны по ссылке: <https://crypto.rosatom.ru/ca/tseepochka-sertifikatov/>



Целочка сертификатов, СОС

Квалифицированные сертификаты на ГОСТе Р 34.10-2012

Для осуществления доверия к сертификатам, изданным Корпоративным удостоверяющим центром Госкорпорации «Росатом» необходимо установить доверие к сертификатам Головного удостоверяющего центра Минкомсвязи:

- Сертификат "Минкомсвязь России" на ГОСТе 2012" (файл Root_GUC2012.cer) необходимо установить в хранилище "Доверенные корневые центры сертификации".
- Сертификат "Акционерное общество «Гринатом»" (файл Root_Greenatom_2012.cer) необходимо установить в хранилище "Промежуточные центры сертификации".

Рекомендуем проверить доступность списков отозванных сертификатов Головного удостоверяющего центра Минкомсвязи:

- http://feedst-ru1.ru/cdpl/guc_gost12.cer
- http://company.ru/cdpl/guc_gost12.cer
- http://rostelecom.ru/cdpl/guc_gost12.cer

Квалифицированные 2018

Для осуществления доверия к сертификатам, изданным Корпоративным удостоверяющим центром Госкорпорации «Росатом» необходимо установить доверие к сертификатам Головного удостоверяющего центра Минкомсвязи:

- Сертификат "Головной удостоверяющий центр" (файл GUC.cer) необходимо установить в хранилище "Доверенные корневые центры сертификации".
- Сертификат "АО «Гринатом»" (файл Root_CA_Grinatom.cer) необходимо установить в хранилище "Промежуточные центры сертификации".

Квалифицированные 2017

Для осуществления доверия к сертификатам, изданным Корпоративным удостоверяющим центром Госкорпорации «Росатом» необходимо установить доверие к сертификатам Головного удостоверяющего центра Минкомсвязи:

- Сертификат "Головной удостоверяющий центр" (файл GUC.cer) необходимо установить в хранилище "Доверенные корневые центры сертификации".

Настройки браузера для доступа к portalу Госуслуг

5) Установить под учётной записью пользователя актуальный плагин пользователя систем электронного правительства, доступный по ссылке: <https://ds-plugin.gosuslugi.ru/plugin/upload/Index.spr>

госуслуги

Установка плагина для работы с порталом государственных услуг

Поддерживаемые браузеры:

- Internet Explorer версии 6.0 и выше;
- Safari версии 5.0.6 и выше;
- Mozilla Firefox версии 50.0 и выше;
- Google Chrome версии 29.0 и выше;

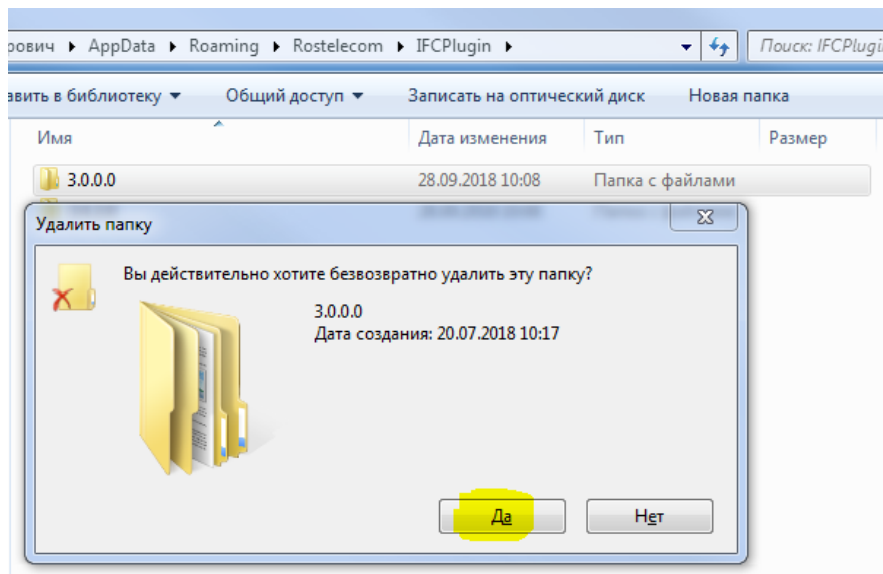
Для вашей системы рекомендуется следующая версия плагина. Загрузка начнется автоматически.

Операционная система	Плагин	Версия
Microsoft Windows 7/8/10, 64-bit	IFCPPlugin-x64.msi	3.0.3.0

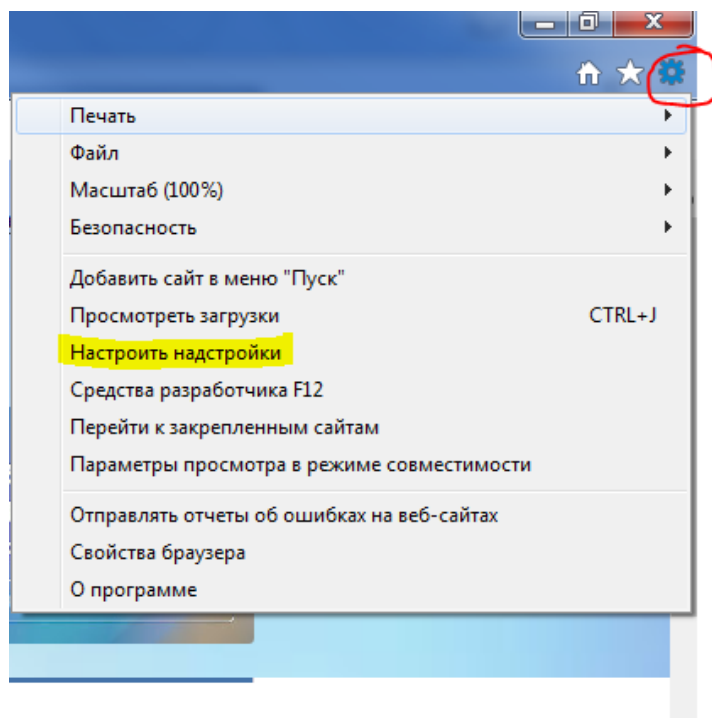
Для корректной работы перед установкой актуальной версии плагина необходимо вручную удалить предыдущие версии плагина через Панель управления, предварительно закрыв все окна браузера(ов) на компьютере, вручную **очистить** папку



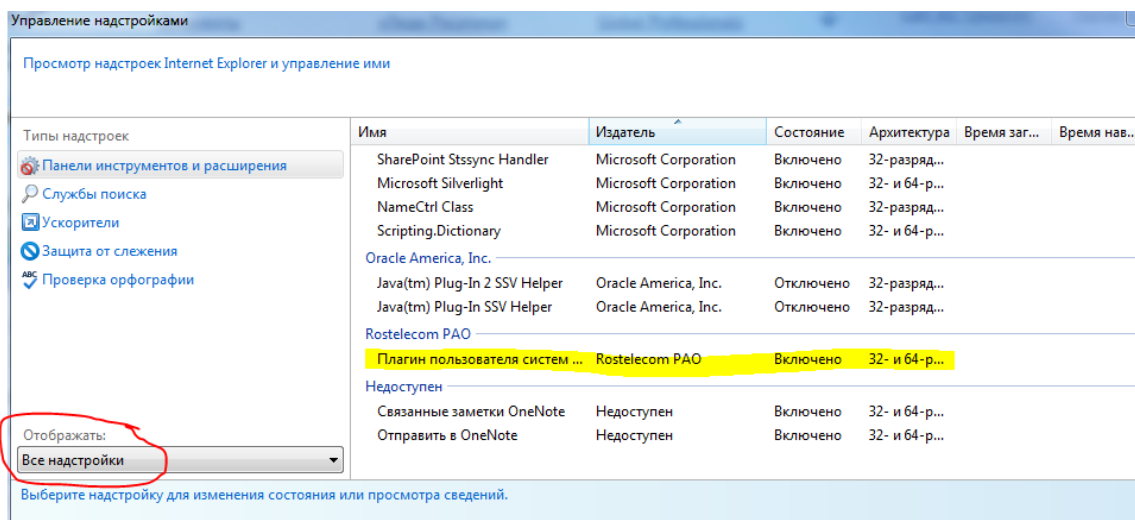
C:\Users\%USERNAME%\AppData\Roaming\Rostelecom\IFCPlugin. Для этого необходимо скопировать путь к папке в адресную строку проводника и удалить ее содержимое.



- б) Убедиться, что плагин Crypto Interface Plugin в надстройках браузера Internet Explorer находится в состоянии «Включено». Для этого в настройках браузера нажать на «Настроить надстройки».



Далее «Отображать – Все надстройки», просмотреть раздел «Rostelecom PAO».



7) В свойствах браузера в разделе «Безопасность» добавить в список надёжных сайтов следующие адреса:

<https://esia.gosuslugi.ru>

<https://gosuslugi.ru>

<https://esia.gosuslugi.ru>

<https://zakupki.gov.ru>

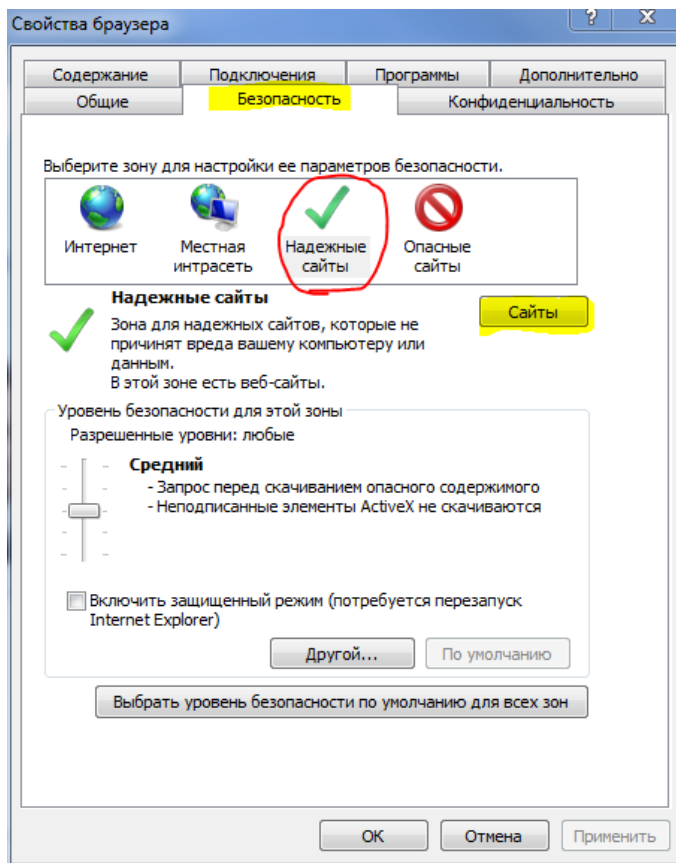
<http://esia.gosuslugi.ru>

<http://gosuslugi.ru>

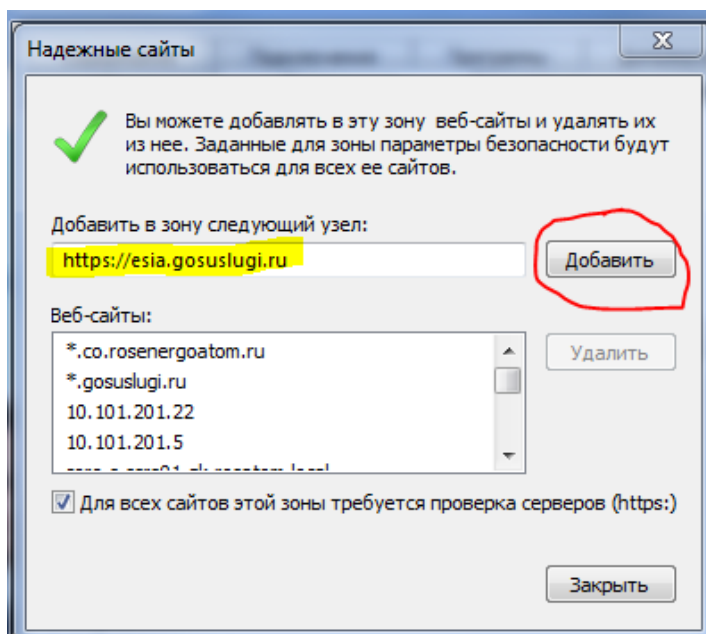
<http://esia.gosuslugi.ru>

<http://zakupki.gov.ru>

Для этого необходимо перейти в свойствах браузера к вкладке «Безопасность», выбрать «Надёжные сайты», нажать на «Сайты».



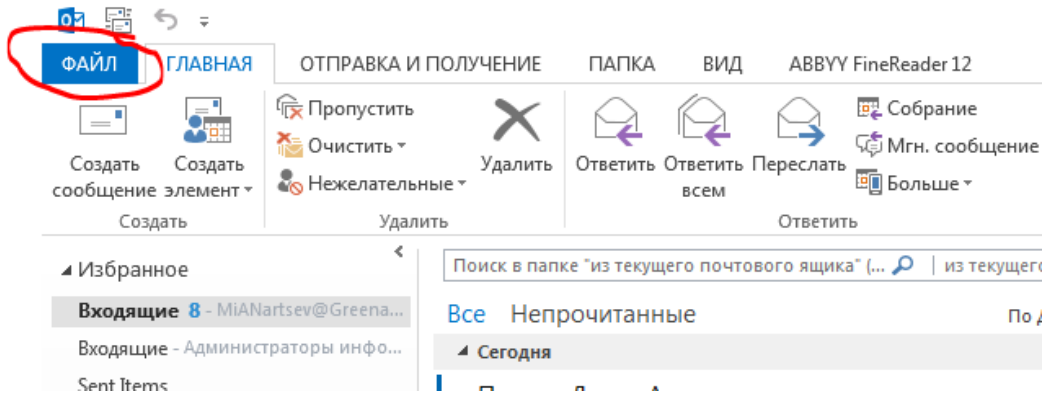
В появившемся меню прописать по очереди и нажать «Добавить» указанные выше адреса, нажать «Закрывать».



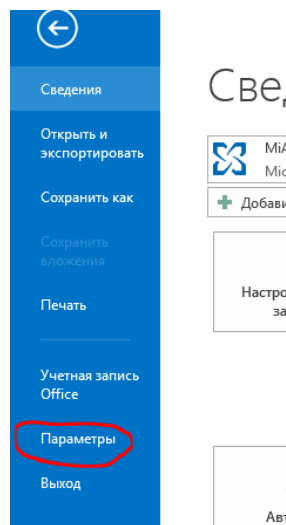
Настройка защищенной корпоративной почтовой системы (ЗКПС)

8) Настройка защищенной корпоративной почтовой системы (ЗКПС)

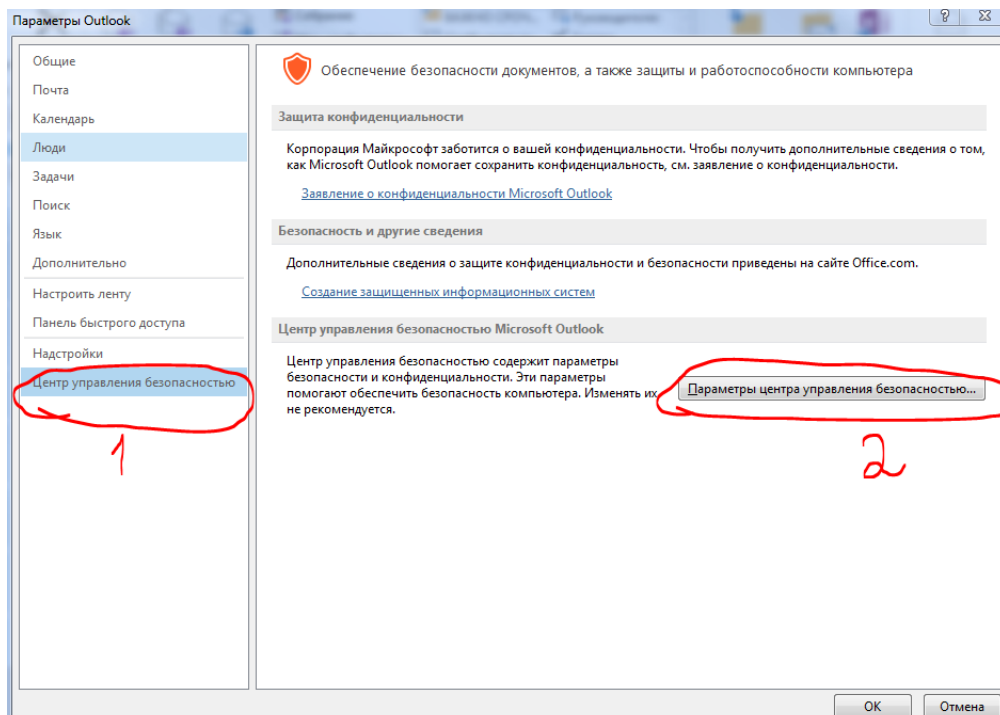
Для настройки ЗКПС необходимо запустить MS Outlook, далее в главном меню открыть подменю «Файл»




Далее «Параметры»

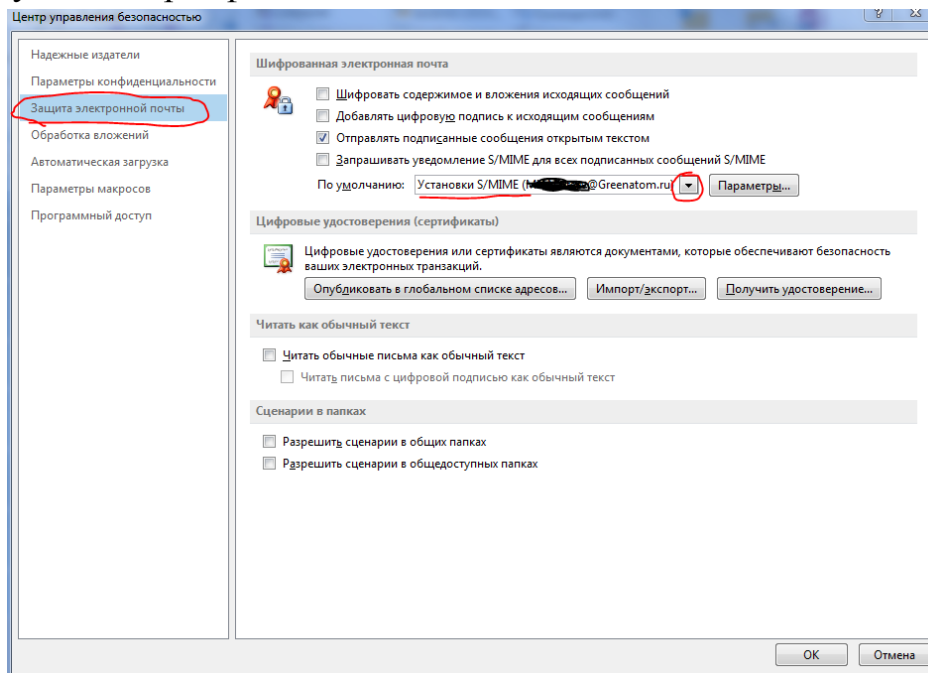


«Центр управления безопасностью», затем «Параметры центра управления безопасностью»

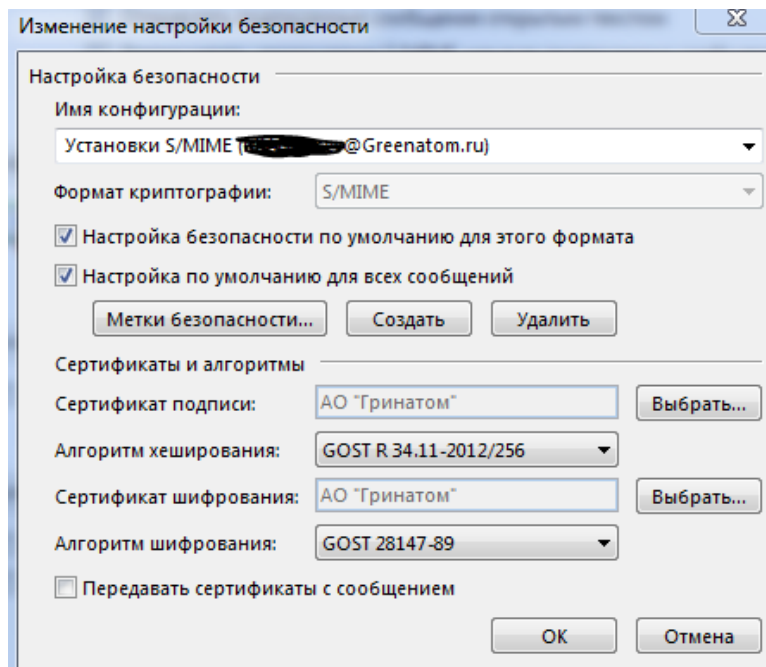




Далее подпункт «Защита электронной почты», затем стрелочку вниз  и выбираем нужный сертификат

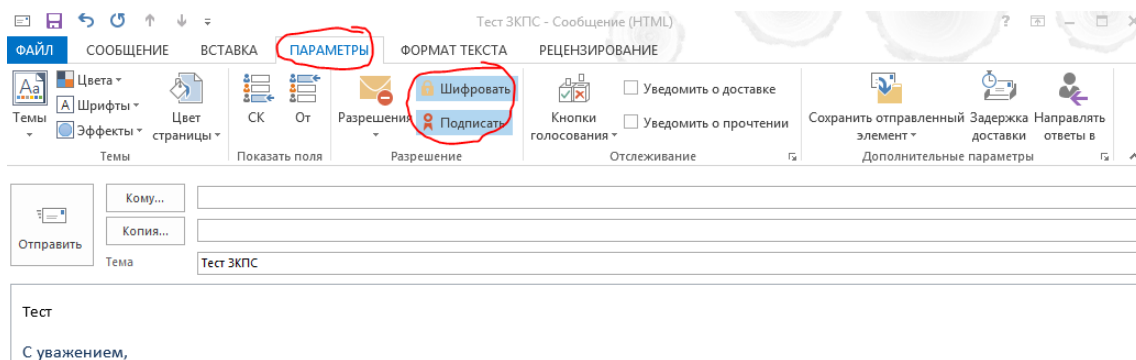


Заходим в «Параметры», проверяем установки сертификата:



Затем «Ок», закрываем все вспомогательные меню.

Для проверки работоспособности создаем новое сообщение в адрес пользователя, имеющего сертификат ключа проверки электронной подписи, во вкладке «Параметры» выбираем функцию «Шифровать» и «Подписать», отправляем сообщение.



9) Протестировать доступ на рабочем месте с пользователем, убедиться в работоспособности всех настроенных систем.