

# **Справочное руководство по подключению к АСОИ ФинЦЕРТ и работе с ключевой информацией**

## **Вопросы и ответы**

г. Москва, 2025

## Перечень вопросов:

1. Какие есть общие рекомендации по подключению к АСОИ ФинЦЕРТ? .....	4
2. Как получить доступ к АСОИ ФинЦЕРТ?.....	4
3. Какие имеются ресурсы АСОИ ФинЦЕРТ? .....	5
4. Как организуется подключение к АСОИ ФинЦЕРТ?.....	6
5. Где взять СКЗИ для подключения к АСОИ ФинЦЕРТ? .....	7
6. Как настроить СКЗИ «Континент TLS-клиент»? .....	8
7. Как настроить СКЗИ «КриптоПро»? .....	9
8. Как убедиться, что доступ к ресурсам АСОИ ФинЦЕРТ настроен? .....	9
9. Для чего нужны пользовательские TLS-сертификаты? .....	10
10. Как организовать TLS-подключение для обмена информацией через API? .....	10
11. Как применять пользовательский TLS-сертификат для организации обмена информацией через API? .....	10
12. Нужны ли отдельные TLS-сертификаты для работы на тестовом API (zoe-api.fincert.cbr.ru) и промышленном API (api.fincert.cbr.ru)?.....	11
13. Все ли пользователи АСОИ ФинЦЕРТ должны получить TLS-сертификаты? .....	11
14. Где получить пользовательский TLS-сертификат?.....	11
15. Какой порядок получения пользовательских TLS-сертификатов? .....	12
16. В какое ТУ БР надо обращаться за получением TLS-сертификата?.....	12
17. К кому следует обращаться в ТУ БР? .....	12
18. Может ли уполномоченный от организации получить комплект ключевой информации (распечатки сертификатов и сами сертификаты) сразу на всех пользователей? .....	13
19. Можно ли указать от организации несколько уполномоченных для получения ключевой информации? .....	13
20. Как сформировать заявку на TLS-сертификат? .....	13
21. Что делать, если в организации не используется Континент TLS-клиент? .....	13
22. Как перевыпустить TLS-сертификат под другой тип криптопровайдера?.....	14

23. В каком виде необходимо сформировать электронную заявку на TLS-сертификат? .....	14
24. Какие еще есть особенности формирования заявки на TLS-сертификат? .....	15
25. Как установить пользовательский TLS-сертификат? .....	16
26. Как убедиться, что доступ к ресурсам АСОИ ФинЦЕРТ с использованием пользовательского сертификата настроен? .....	17
27. Как уведомить Банк России о подключении к АСОИ ФинЦЕРТ?.....	18
28. Не удается настроить доступ к АСОИ ФинЦЕРТ с помощью СКЗИ «Континент TLS-клиент». В чем может быть причина? .....	20
29. Не удается настроить доступ к АСОИ ФинЦЕРТ с помощью СКЗИ «КриптоПро». В чем может быть причина? .....	20
30. Ошибка подключения при использовании браузера Microsoft Edge, как быть?.....	22
31. Не удается подключиться к АСОИ ФинЦЕРТ, в чем причина? .....	23
32. Как определить период действия пользовательского TLS-сертификата? .....	25
33. Можно ли получить TLS-сертификаты без личной явки в территориальное учреждение Банка России? .....	26
34. Кто имеет возможность получить сертификаты без личного присутствия (личной явки) в территориальном учреждении Банка России? .....	26
35. Как и в каком виде оформить доверенность на получение ключевой информации без личного присутствия?.....	27
36. Каким образом можно подписать электронный файл? .....	28
37. Каким образом оформить распечатку TLS-сертификата в электронном виде?.....	30
38. Можно ли обойтись без оформления доверенности? .....	30
39. Что делать если не получается подключиться к АСОИ ФинЦЕРТ?.....	30

## 1. Какие есть общие рекомендации по подключению к АСОИ ФинЦЕРТ?

По требованиям обеспечения информационной безопасности, для подключения к ресурсам Автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России (далее - АСОИ ФинЦЕРТ) требуется настроить шифрованное соединение с использованием отечественной криптографии (на основе криптографических алгоритмов серии 34 ГОСТ Р).

ФинЦЕРТ Банка России не налагает никаких ограничений на использование программного обеспечения (далее – ПО).

Рекомендованным средством криптографической защиты информации (далее – СКЗИ) является ПО «Континент TLS-клиент» производства компании «Код безопасности», доступное участникам информационного обмена с ФинЦЕРТ (далее – Участникам) бесплатно на сайте разработчика ([www.securitycode.ru](http://www.securitycode.ru)).

Порядок подключения к АСОИ ФинЦЕРТ на примере использования ПО «Континент TLS-клиент» описан в документе «Руководство Участника по работе с АСОИ ФинЦЕРТ», размещенном на портале АСОИ ФинЦЕРТ ([https://portal.fincert.cbr.ru/Content/1136/руководство\\_участника.pdf](https://portal.fincert.cbr.ru/Content/1136/руководство_участника.pdf)). Также Участникам настоятельно рекомендуется ознакомиться с документацией производителя на используемое СКЗИ.

Доступ в АСОИ ФинЦЕРТ осуществляется через веб-браузеры в зависимости от установленного СКЗИ.

При работе с СКЗИ «Континент TLS-клиент»:

- Microsoft Edge версии выше 140;
- Google Chrome версии выше 125;
- Яндекс.Браузер версии выше 22;
- Chromium-Gost версии выше 103.

При работе с СКЗИ КриптоПро:

- Google Chrome версии выше 125;
- Яндекс.Браузер версии выше 22;
- Chromium-Gost версии выше 103.

## 2. Как получить доступ к АСОИ ФинЦЕРТ?

После регистрации (подписания соглашения об обмене информацией) Участник получает учетные данные пользователей для работы в АСОИ ФинЦЕРТ (логин и пароль).

Для подключения к системе под выданными учетными данными Участнику необходимо организовать доступ к ресурсам АСОИ ФинЦЕРТ, для чего следует установить на рабочих местах пользователей серверные и пользовательские сертификаты.

В одностороннем режиме аутентификации (только по серверным сертификатам) можно получить доступ к информационным порталам: portal.fincert.cbr.ru (основной ресурс) и zoe-portal.fincert.cbr.ru (тестовый ресурс, не содержит актуальной информации).

Серверные сертификаты размещаются на информационном портале АСОИ ФинЦЕРТ (portal.fincert.cbr.ru) в разделе «АСОИ ФинЦЕРТ (Документация и ПО Участника)». При первоначальном подключении сертификаты направляются дежурной службой ФинЦЕРТ ([info\\_fincert@cbr.ru](mailto:info_fincert@cbr.ru), +7 (495) 772-70-90). При плановой смене сертификатов, в задачу Участника входит своевременное получение (посредством скачивания с портала АСОИ ФинЦЕРТ либо из соответствующего бюллетеня) и установка новых версий сертификатов.

Пользовательские сертификаты выдаются пользователям Участника территориальными учреждениями Банка России. О порядке их получения и применения см. соответствующие разделы данного документа.

## 3. Какие имеются ресурсы АСОИ ФинЦЕРТ?

АСОИ ФинЦЕРТ реализована в виде зоны постоянной эксплуатации (ЗПЭ, «промышленная») и зоны опытной эксплуатации (ЗОЭ, «тестовые ресурсы»).

ЗПЭ АСОИ ФинЦЕРТ содержит следующие ресурсы:

- Личный кабинет Участника (lk.fincert.cbr.ru);
- Сервис API-взаимодействия (api.fincert.cbr.ru);
- Сервис Крипто-API для автоматизированного подписания сообщений электронной подписью (crypto-api.fincert.cbr.ru).

ЗОЭ АСОИ ФинЦЕРТ содержит следующие ресурсы:

- Тестовый личный кабинет Участника (zoe-lk.fincert.cbr.ru);
- Сервис API-взаимодействия (zoe-api.fincert.cbr.ru);

- Сервис Крипто-API для автоматизированного подписания сообщений электронной подписью (zoe-crypto-api.fincert.cbr.ru).

Доступ к перечисленным ресурсам осуществляется по пользовательскому TLS-сертификату (единому для всех ресурсов ЗПЭ и ЗОЭ АСОИ ФинЦЕРТ).

Для получения доступа к информационным порталам ЗПЭ АСОИ ФинЦЕРТ (portal.fincert.cbr.ru) и ЗОЭ АСОИ ФинЦЕРТ (zoe-portal.fincert.cbr.ru) пользовательский TLS-сертификат не требуется.

#### 4. Как организуется подключение к АСОИ ФинЦЕРТ?

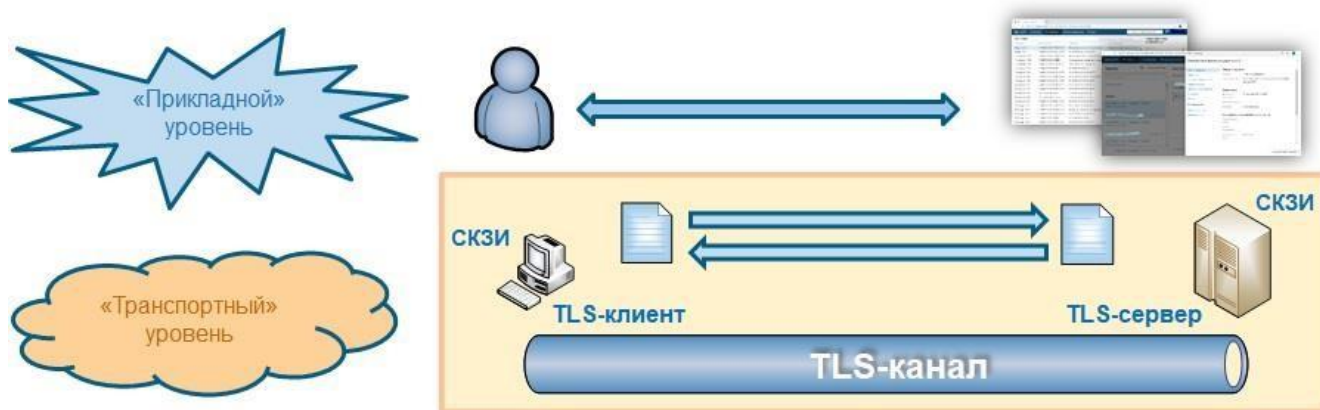


Рисунок 1. Схема организации взаимодействия с АСОИ ФинЦЕРТ

Взаимодействие с АСОИ ФинЦЕРТ организуется на «транспортном» уровне (путем установления зашифрованного канала) и «прикладном» уровне (путем получения логического доступа), см. рисунок 1.

Подключение к системе необходимо начать с организации сетевого подключения в одностороннем режиме аутентификации (для возможности получения доступа к информационному portalу АСОИ ФинЦЕРТ):

- получить серверные сертификаты;
- установить СКЗИ;
- настроить доступ к ресурсам.

Для возможности отправки запросов в АСОИ ФинЦЕРТ и получения информации от ФинЦЕРТ необходимо получить и установить пользовательские сертификаты, см. соответствующие пункты данного документа.

## 5. Где взять СКЗИ для подключения к АСОИ ФинЦЕРТ?

Специальных требований по использованию СКЗИ при подключении к АСОИ ФинЦЕРТ не выдвигается: для этой цели Участники используют доступное «на рынке» ПО.

Для Участников бесплатно на сайте производителя доступно СКЗИ «Континент TLS-клиент» производства компании «Код безопасности» (: [www.securitycode.ru](http://www.securitycode.ru)), см. рисунок 2, которое позволяет работать с разными браузерами и которое также используется при формировании запросов на пользовательские TLS-сертификаты.

Те Участники, которые используют СКЗИ «КриптоПро» могут использовать для подключения к АСОИ ФинЦЕРТ данное ПО.

ФинЦЕРТ не занимается распространением ПО СКЗИ для Участников. Серверные версии ПО, а также специализированные версии ПО Участникам необходимо приобретать, устанавливать и настраивать самостоятельно.

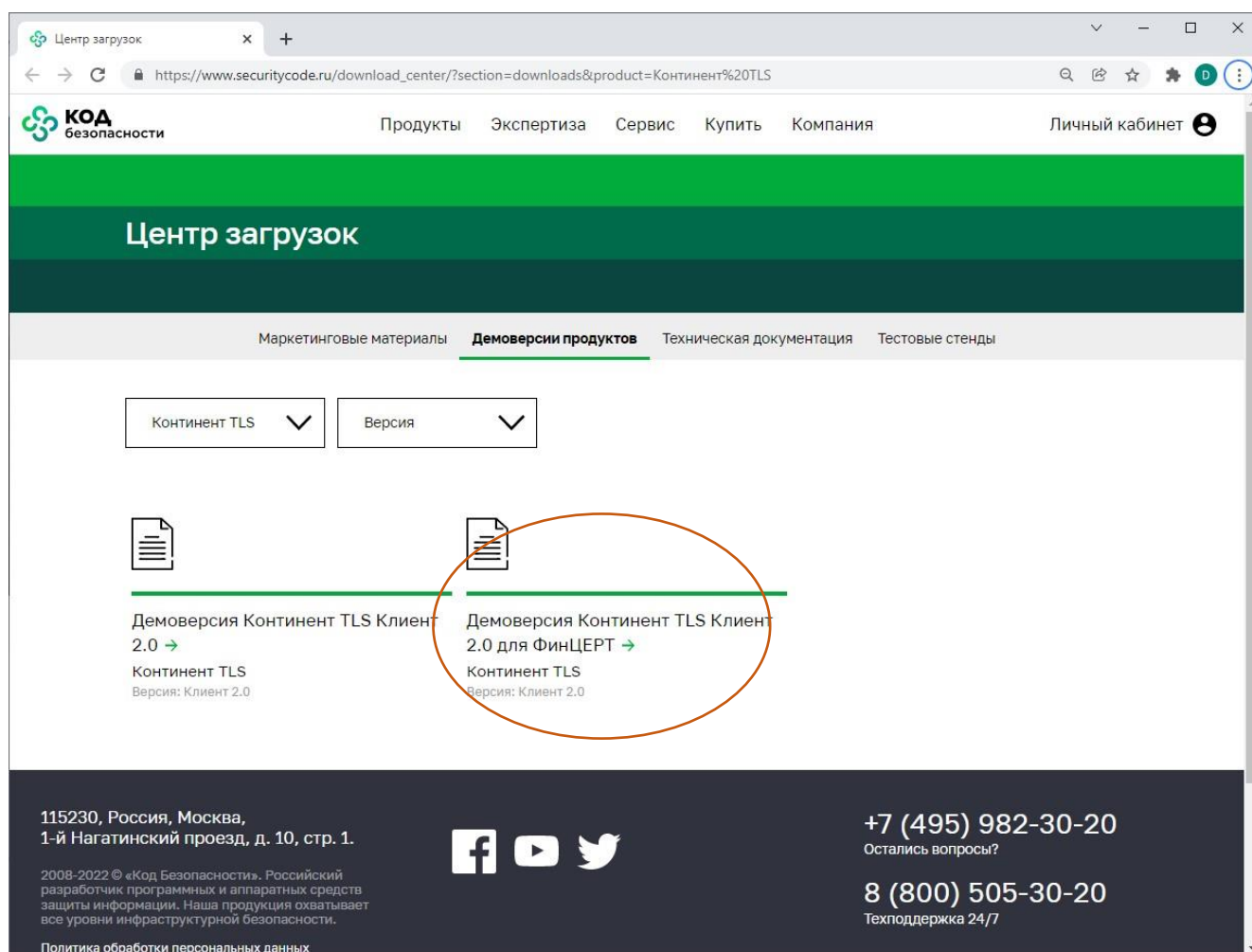


Рисунок 2. Страница сайта [www.securitycode.ru](http://www.securitycode.ru) до момента авторизации для скачивания продукта

## 6. Как настроить СКЗИ «Континент TLS-клиент»?

Детальный порядок действий приведен в документе «Руководство Участника по работе с АСОИ ФинЦЕРТ», размещенном на портале АСОИ ФинЦЕРТ ([https://portal.fincert.cbr.ru/Content/1136/руководство\\_участника.pdf](https://portal.fincert.cbr.ru/Content/1136/руководство_участника.pdf)).

Для доступа к серверным ресурсам необходимо:

- установить корневой сертификат ROOTsvc-CA (имя файла: sacert.cer) в раздел «Доверенные корневые центры сертификации»;
- импортировать серверные сертификаты, в раздел «Доверенные издатели»;
- ■ добавить ресурсы АСОИ ФинЦЕРТ в перечень соединений.

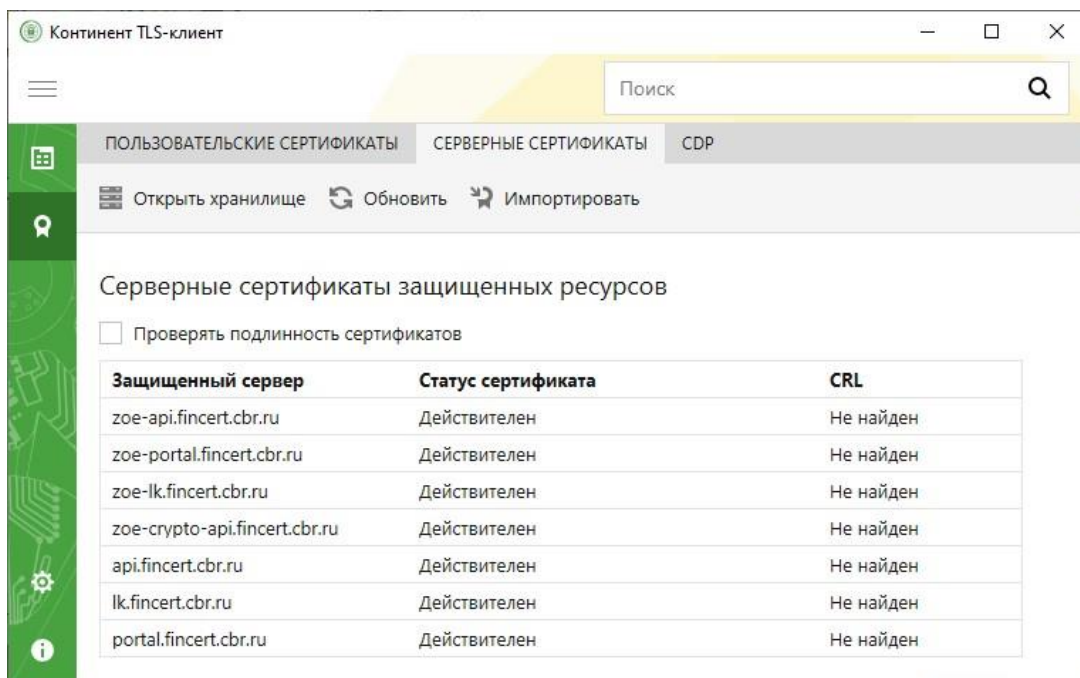


Рисунок 3. Серверные сертификаты АСОИ ФинЦЕРТ

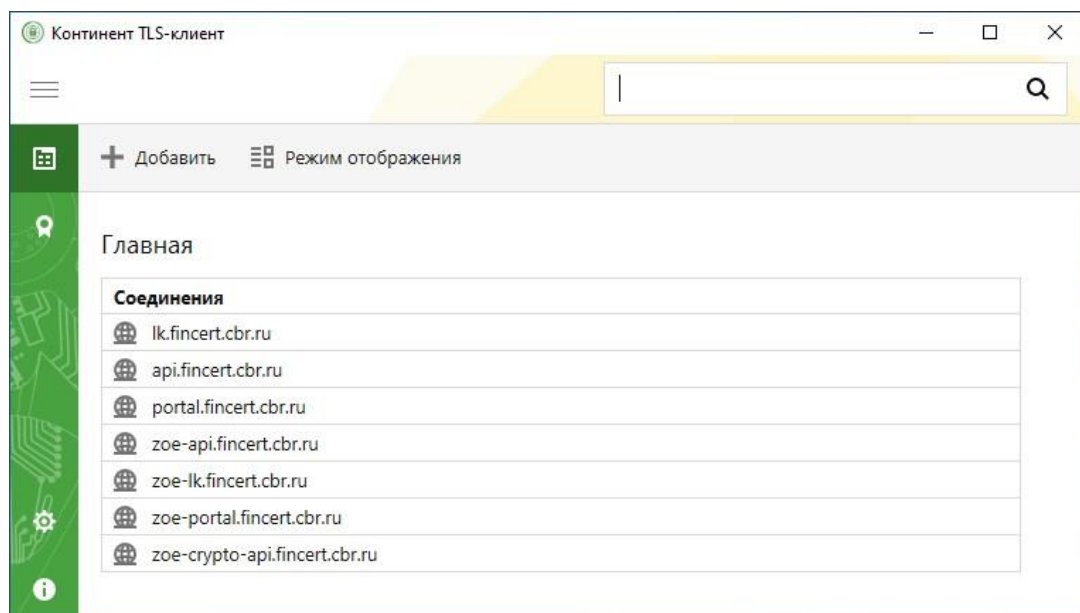


Рисунок 4. Перечень ресурсов АСОИ ФинЦЕРТ

После добавления ресурсов убедиться, что в настройках опция «Проверять сертификаты по CRL» не отмечена.

Для установки пользовательских сертификатов в СКЗИ см. соответствующий раздел данного документа.

## 7. Как настроить СКЗИ «КриптоПро»?

Для доступа к серверным ресурсам необходимо:

- установить корневой сертификат ROOTsvc-CA (имя файла: cacert.cer) в раздел «Доверенные корневые центры сертификации»;
- импортировать серверные сертификаты, выбрать «Другие пользователи».

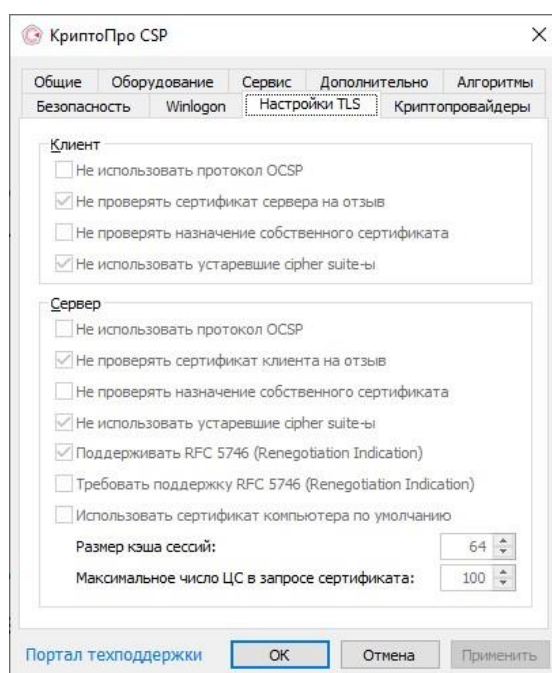


Рисунок 5. Настройки КриптоПро CSP версии 5

После установки сертификатов убедиться в настройках, что в секции клиент выбрана опция «Не проверять сертификат сервера на отзыв».

Для установки пользовательских сертификатов в СКЗИ см. соответствующие разделы данного документа.

## 8. Как убедиться, что доступ к ресурсам АСОИ ФинЦЕРТ настроен?

Если серверные сертификаты установлены корректно и зашифрованное соединение устанавливается, то появляется доступ к информационным порталам АСОИ ФинЦЕРТ: portal.fincert.cbr.ru (основной ресурс) и zoe-portal.fincert.cbr.ru (тестовый ресурс, не содержит

актуальной информации), которые функционируют в режиме односторонней TLS-аутентификации (пользователь Участника доверяет серверным сертификатам).

Если при попытке подключиться к ресурсам информационного обмена (lk.fincert.cbr.ru, zoe-lk.fincert.cbr.ru) браузер предлагает выбрать нужный сертификат для продолжения, то это так же означает, что серверные сертификаты установлены корректно.

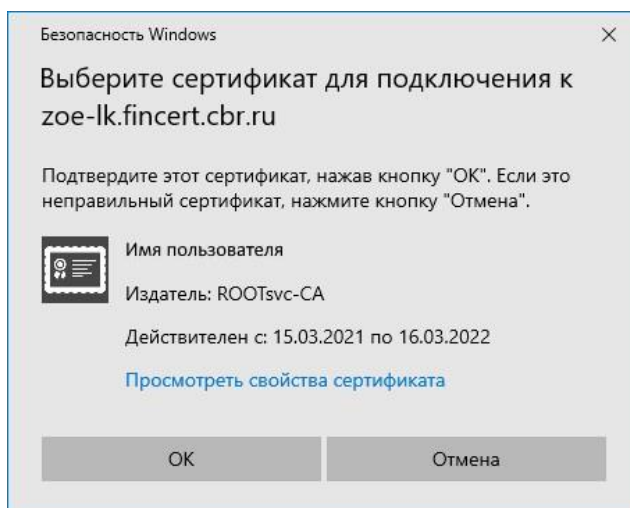


Рисунок 6. Приглашение к выбору пользовательского сертификата

## 9. Для чего нужны пользовательские TLS-сертификаты?

Пользовательские TLS-сертификаты необходимы для организации доверенного канала взаимодействия с АСОИ ФинЦЕРТ, в целях возможности применения функционала электронной подписи в АСОИ ФинЦЕРТ.

## 10. Как организовать TLS-подключение для обмена информацией через API?

Для организации зашифрованного канала с целью последующего обмена посредством прикладного программного интерфейса (API) следует использовать пользовательский TLS-сертификат ответственного за информационное взаимодействие по API.

## 11. Как применять пользовательский TLS-сертификат для организации обмена информацией через API?

Для организации зашифрованного канала подключения к АСОИ ФинЦЕРТ с целью взаимодействия по API следует использовать пользовательский TLS-сертификат ответственного за информационное взаимодействие по API. В части назначения работника Участника на роль ответственного за взаимодействие по API рекомендуется применять следующий порядок.

В карточке Участника (как организации) создаются две учетные записи:

- назначенный на эту роль работник прописывается как пользователь с указанием персонального рабочего адреса электронной почты (который также служит логином для входа в систему), – данная учетная запись используется для доступа пользователя в личный кабинет АСОИ ФинЦЕРТ. Для чего на этого пользователя оформляется пользовательский TLS-сертификат в территориальном учреждении Банка России;
- также на этого работника (с указанием Ф.И.О., должности, подразделения и телефона) заводится другая учетная запись с электронной почтой вида `api_fincert@<доменорганизации.ru>`. Это позволяет использовать тот же пользовательский TLS-сертификат и для организации доступа к АСОИ ФинЦЕРТ посредством API.

В том случае, если в организации Участника происходят штатные изменения (например, в случае увольнения работника), то на роль ответственного за взаимодействие по API можно назначить другого работника, направив соответствующий запрос на изменение учетных данных в АСОИ ФинЦЕРТ (изменение Ф.И.О., должности, номера телефона) для учетной записи, ассоциированной с логином: `api_fincert@<доменорганизации.ru>`.

## 12. Нужны ли отдельные TLS-сертификаты для работы на тестовом API (`zoe-api.fincert.cbr.ru`) и промышленном API (`api.fincert.cbr.ru`)?

Для доступа ко всем ресурсам АСОИ ФинЦЕРТ используется единый пользовательский TLS-сертификат, который обеспечивает создание защищенного канала связи с АСОИ ФинЦЕРТ в целом (как к «продуктивному сегменту», так и к тестовым ресурсам).

## 13. Все ли пользователи АСОИ ФинЦЕРТ должны получить TLS-сертификаты?

Да, поскольку без TLS-сертификатов пользователи не смогут подключиться к АСОИ ФинЦЕРТ и авторизоваться в системе.

## 14. Где получить пользовательский TLS-сертификат?

Пользовательские TLS-сертификаты для работы с АСОИ ФинЦЕРТ выдаются на бесплатной основе в территориальных учреждениях Банка России (ТУ БР).

Обращаться следует в ТУ БР по месту регистрации юридического лица (перечень ТУ БР приведен на сайте ЦБ: [http://www.cbr.ru/about\\_br/tubr/](http://www.cbr.ru/about_br/tubr/)). Организации, имеющие филиалы в разных субъектах Российской Федерации (кроме г. Москвы и Московской области), могут направлять заявки в территориальное учреждение Банка России по месту фактического расположения подразделения (подразделения, расположенные вне г. Москвы, могут направлять соответствующие заявки в ближайшее территориальное учреждение Банка России за подписью руководителя филиала).

## 15. Какой порядок получения пользовательских TLS-сертификатов?

TLS-сертификаты выдаются в ТУ БР в соответствии с документом «Регламент получения ключевой информации», размещенном на информационном портале АСОИ ФинЦЕРТ (<https://portal.fincert.cbr.ru>).

Также на информационном портале приведена другая полезная информация: контактные данные администраторов ключевой системы (АКС) ТУ БР, подборка бюллетеней ФинЦЕРТ по вопросам получения TLS-сертификатов в виде архивного файла: <https://portal.fincert.cbr.ru/Content/1177/дополнительный-комплект-документов.rar>, в составе которого имеются «Диаграмма взаимодействия с АКС ТУ при получении ключевой информации» и презентация «Порядок получения ключевой информации и работа с электронной подписью в АСОИ ФинЦЕРТ».

## 16. В какое ТУ БР надо обращаться за получением TLS-сертификата?

Обращаться следует в ТУ БР по месту регистрации юридического лица (перечень ТУ приведен на сайте Банка России: [http://www.cbr.ru/about\\_br/tubr/](http://www.cbr.ru/about_br/tubr/)). Организации, имеющие филиалы в разных субъектах Российской Федерации (кроме г. Москвы и Московской области), могут направлять заявки в территориальное учреждение Банка России по месту фактического расположения подразделения (подразделения, расположенные вне г. Москвы, могут направлять соответствующие заявки в ближайшее территориальное учреждение Банка России за подписью руководителя филиала).

## 17. К кому следует обращаться в ТУ БР?

Контактные данные администраторов ключевой системы (АКС) в территориальных учреждениях Банка России размещены на информационном портале АСОИ ФинЦЕРТ.

## 18. Может ли уполномоченный от организации получить комплект ключевой информации (распечатки сертификатов и сами сертификаты) сразу на всех пользователей?

Да, поскольку эта открытая информация.

## 19. Можно ли указать от организации несколько уполномоченных для получения ключевой информации?

Да, можно.

## 20. Как сформировать заявку на TLS-сертификат?

Для формирования заявки на TLS-сертификат необходимо использовать СКЗИ Континент TLS-клиент от компании «Код безопасности». Данное ПО позволяет работать с криптопровайдерами от других производителей: см. документ «Руководство по эксплуатации» (поставляется вместе с СКЗИ Континент TLS-клиент), где описаны процедуры подготовки заявок с использованием криптопровайдеров «КриптоПро» и «Код безопасности».

Также рекомендуем ознакомиться с бюллетенем FinCERT-20210406-01-INFO. (Находится в подборке бюллетеней ФинЦЕРТ по вопросам получения TLS-сертификатов в виде архивного файла: <https://portal.fincert.cbr.ru/Content/1177/дополнительный-комплект-документов.rar>).



## 21. Что делать, если в организации не используется Континент TLSклиент?

ПО «Континент TLS-клиент» для ФинЦЕРТ доступно бесплатно на сайте разработчика ([www.securitycode.ru](http://www.securitycode.ru)) и может быть использовано только для формирования запроса на сертификат ключа в электронном виде.

Запрос на сертификат ключа может быть сформирован на отдельно стоящем компьютере (с обязательным использованием криптопровайдера установленного на рабочих местах пользователей).

По вопросу формирования запроса на сертификат ключа в электронном виде рекомендуем ознакомиться с бюллетенем FinCERT-20210406-01-INFO. (Находится в подборке бюллетеней ФинЦЕРТ по вопросам получения TLS-сертификатов в виде архивного файла: <https://portal.fincert.cbr.ru/Content/1177/дополнительный-комплект-документов.rar>).

## 22. Как перевыпустить TLS-сертификат под другой тип криптопровайдера?

Перевыпуск TLS-сертификатов осуществляется в соответствии с порядком, приведенном в разделе 2 «Регламента получения ключевой информации» ПО «Континент TLS-клиент» (далее – Регламент). Оформление заявки следует проводить по формату «Приложения 5» к Регламенту с указанием актуальной причины перевыпуска сертификата(-ов) в свободной форме. Например, указав: «в связи с производственной необходимостью использования другого типа СКЗИ».

Одновременно в данной заявке можно указать необходимость отозвать ранее выданного сертификата(-ов). При этом, поскольку ответственность за правильное использование TLS-сертификатов находится в зоне ответственности Участника, ранее выданный сертификат можно не отзывать. Например, если пользователю Участника требуется иметь доступ к АСОИ ФинЦЕРТ с рабочих мест, имеющих разную программную конфигурацию.

## 23. В каком виде необходимо сформировать электронную заявку на TLS-сертификат?

Электронная заявка на сертификат формируется в виде двух файлов: \*.req и \*.html. Процедура формирования заявки в формате req-файла описана в Приложении А.5 «Руководство участника по работе с АСОИ ФинЦЕРТ» (необходимо выбрать опцию формата файла «двоичные данные»). При формировании заявки поля: СНИЛС, ИНН и ОГРН – заполнять необязательно.

Файл для распечатки «Заявки на получение в удостоверяющем центре сертификата ключа» формируется в виде html-файла. Заявка на получение TLS-сертификата формируется в ПО «Континент TLS-клиент» автоматически и может быть использована «как есть». В этом случае паспортные данные и номер приказа о предоставлении полномочий не указываются, также следует оставить пустыми поля «[Должность] и [ФИО]» в заголовке страницы.

Формируемый печатный экземпляр заявки может быть отредактирован (например, по образцу, приведенному на портале АСОИ ФинЦЕРТ, <https://portal.fincert.cbr.ru>). В этом случае просьба продублировать в заявке адрес электронной почты, который ранее был введен в ПО «Континент TLS-клиент» и который будет являться логином для доступа в АСОИ ФинЦЕРТ.

При направлении заявки, печатный экземпляр подписывает только пользователь (общий направляемый комплект документ оформляется сопроводительным письмом, подписываемым руководителем организации).

## 24. Какие еще есть особенности формирования заявки на TLS-сертификат?

Практика показывает, что информации, представленной на информационном портале АСОИ ФинЦЕРТ, достаточно для получения TLS-сертификатов.

Стоит отметить, что в документах не регламентировано заполнение поля «Описание» в запросе на TLS-сертификат. Это поле является необязательным, его можно не заполнять, либо указать «TLS-сертификат АСОИ ФинЦЕРТ» (рекомендуется). Данное пояснение относится к СКЗИ Континент TLS-клиент версии 2.0.1440.0. На текущий момент актуальная версия СКЗИ на сайте производителя (<https://www.securitycode.ru/>) имеет версию 2.0.1482.0, которая имеет незначительные отличия в параметрах формирования заявки на выпуск сертификата.

Для новой версии СКЗИ Континент TLS-клиент при формировании заявки на TLS-сертификат предварительно предлагается выбрать опции: тип субъекта (по умолчанию – «Произвольный тип») и использование ключей (по умолчанию – «Стандартный набор»). Рекомендуется оставить указанные опции по умолчанию – в этом случае состав полей будет соответствует описанным в документации на АСОИ ФинЦЕРТ (см. рис. 7). Порядок заполнения полей регламентируется документом «Правила заполнения полей и применения ключей проверки ЭП», размещенным на информационном портале АСОИ ФинЦЕРТ. Для поля «Общее имя» следует указать Ф.И.О. полностью – в этом случае на подготовленной в виде HTML-файла поле с именем пользователя будет заполнено корректно.

Использовать расширенный набор ключей шифрования не требуется, так пользовательский TLS-сертификат применяется только для организации зашифрованного канала передачи данных для подключения к АСОИ ФинЦЕРТ.

← Запросить сертификат

Параметры сертификата пользователя

Заполните обязательные поля для выпуска запроса сертификата пользователя.  
В полях должны быть указаны полные официальные названия без сокращений.

Фамилия: Иванов Имя Отчество: Иван Иванович

Общее имя: Иванов Иван Иванович

Организация: Банк

Подразделение: Департамент безопасности

Должность:

Страна: RU Область: Москва

Населенный пункт: Москва

Адрес: Зимняя улица дом 1

Электронная почта: ivanov@bank.ru

ИНН: СНИЛС:

ОГРН:

Далее Отмена

Рисунок 7. Пример заполнения полей запроса на выпуск сертификата

Так же, поскольку заявки на сертификат являются открытой информацией, направлять электронные заявки на TLS-сертификаты можно на одном электронном носителе.

## 25. Как установить пользовательский TLS-сертификат?

Пользовательские сертификаты состоят в цепочке доверия: корневой сертификат > сертификат промежуточного центра сертификации > пользовательский сертификат. Поэтому перед установкой пользовательского сертификата необходимо проверить наличие ранее установленного корневого сертификата ROOTsvc-CA (от него наследуются серверные сертификаты). Затем необходимо установить в раздел «Промежуточные центры сертификации» сертификат ЦСп (промежуточного центра сертификации), см. приложение А.7 «Руководства Участника по работе с АСОИ ФинЦЕРТ».

Далее для установки пользовательского сертификата необходимо выбрать пункт меню «Импортировать» («Континент TLS-клиент») либо «Установить личный сертификат...» («КриптоПро»). Действовать в соответствии с руководствами: вставить USB-носитель

с секретной частью ключа (в случае ПО «Континент TLS-клиент» – папка «topsecretkeys» с одним файлом, в случае ПО «КриптоПро» – папка вида «Ivanov.000» с 6 файлами), ввести ПИН-код.

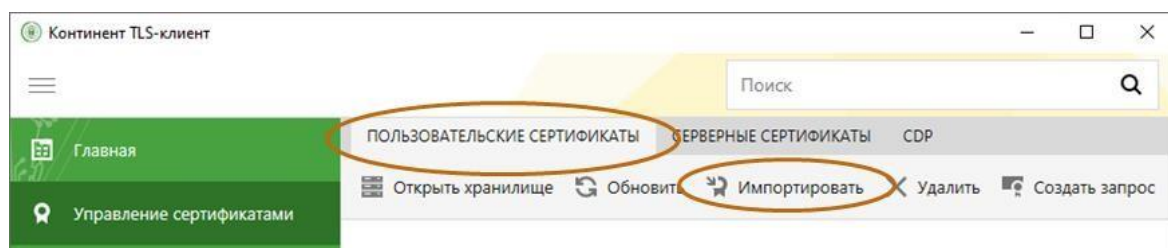


Рисунок 8. Установка TLS-сертификата в "Континент TLS-клиент"

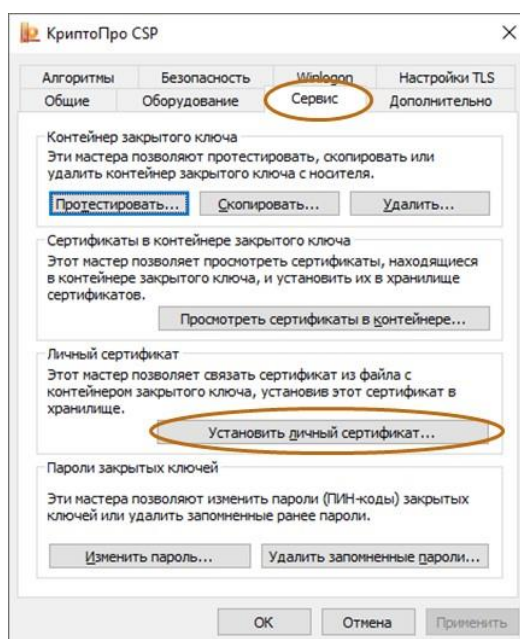


Рисунок 9. Установка TLS-сертификата в "КриптоПро"

После установки сертификата следует убедиться, что в СКЗИ в настройках отключена проверка по CRL (проверка по списку отозванных сертификатов отключена).

## 26. Как убедиться, что доступ к ресурсам АСОИ ФинЦЕРТ с использованием пользовательского сертификата настроен?

Если при подключении к ресурсам информационного обмена (lk.fincert.cbr.ru, zoelk.fincert.cbr.ru) браузер предлагает выбрать пользовательский сертификат и после ввода пинкода отображает приглашение ввести логин-пароль, – это означает, что все сертификаты и СКЗИ настроено корректно.

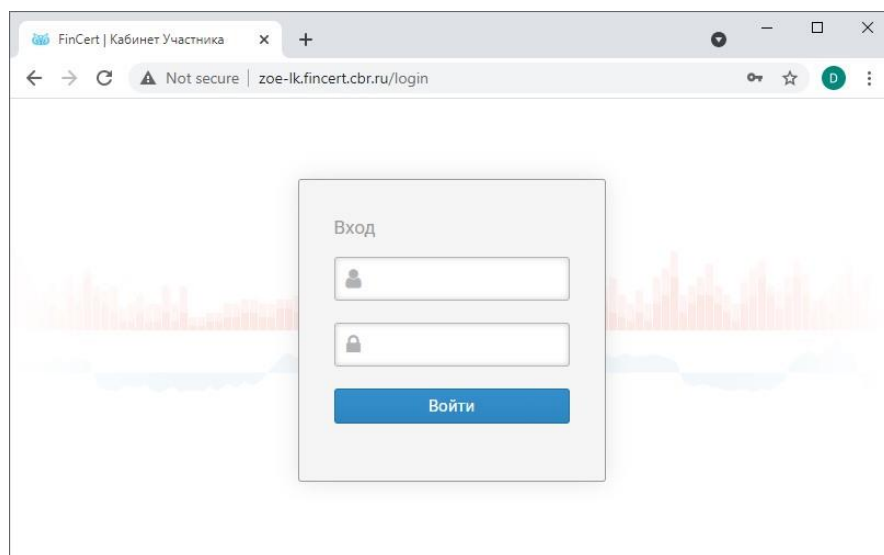


Рисунок 10. Приглашение системы ввести логин/пароль

## 27. Как уведомить Банк России о подключении к АСОИ ФинЦЕРТ?

Для того, чтобы операторы АСОИ ФинЦЕРТ обладали информацией о возможности коммуникации с Участником через сервисы личного кабинета (рекомендуемый тип взаимодействия), после подключения к АСОИ ФинЦЕРТ необходимо (в соответствии с требованиями бюллетеня FinCERT-20210518) направить текстовый запрос в АСОИ ФинЦЕРТ (тип «Другое») об успешном подключении (с заголовком: «\*\*\*Успешное подключение по TLSсертификату») и подтвердить официальным письмом в адрес Департамента информационной безопасности Банка России (ДИБ) (направляется электронным образом через ЛК ЕСПП) готовность взаимодействовать с АСОИ ФинЦЕРТ в режиме двусторонней аутентификации.

Письмо в ДИБ оформляется в произвольном виде. Например, оно может иметь следующий вид:

Директору Департамента информационной  
безопасности Центрального банка  
Российской Федерации  
В.А. Уварову

*О готовности взаимодействия с АСОИ ФинЦЕРТ в  
режиме двусторонней аутентификации*

Уважаемый Вадим Александрович!

Сообщаем об успешном прохождении тестирования подключения к АСОИ ФинЦЕРТ в режиме двусторонней аутентификации по пользовательским TLS-сертификатам и подтверждаем готовность взаимодействовать с АСОИ ФинЦЕРТ в данном режиме аутентификации.

Подпись

## 28. Не удастся настроить доступ к АСОИ ФинЦЕРТ с помощью СКЗИ «Континент TLS-клиент». В чем может быть причина?

Основными причинами, как правило являются:

- в основных настройках активна опция «Проверять сертификаты по CRL»;
- имеются ошибки в соединениях (может устраняться путем перезапуска приложения).

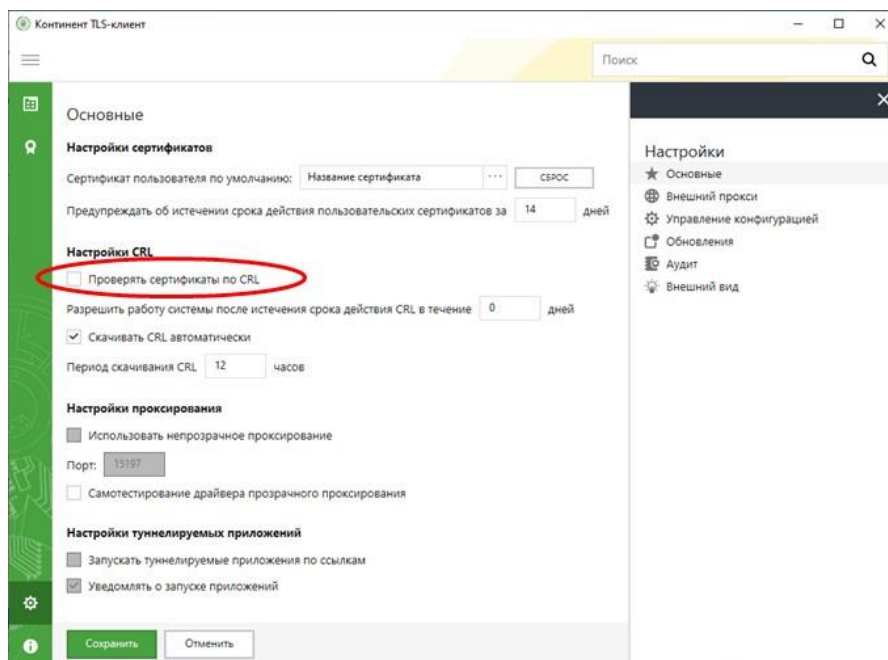


Рисунок 11. Отключение проверки сертификатов на отзыв

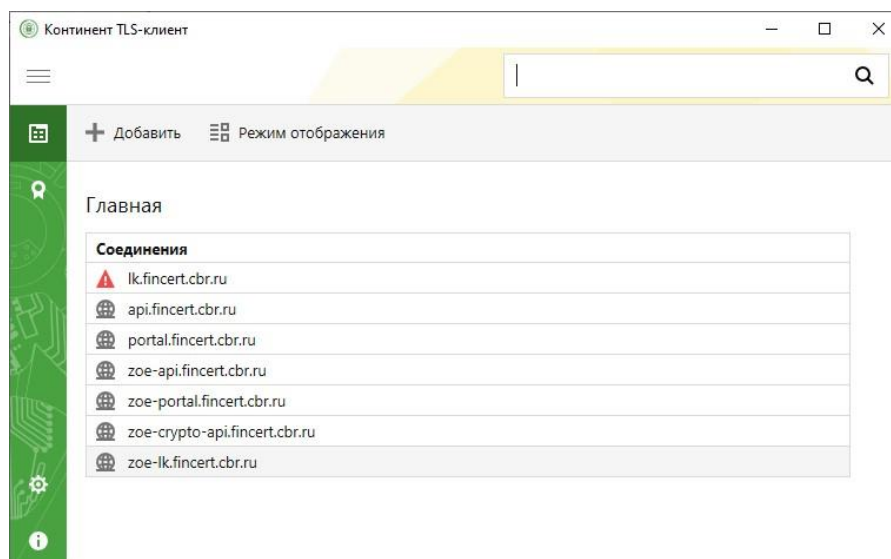


Рисунок 12. Ошибка соединения

## 29. Не удастся настроить доступ к АСОИ ФинЦЕРТ с помощью СКЗИ «КриптоПро». В чем может быть причина?

Основными причинами, как правило являются:

- в настройках TLS, секция «Клиент», не выбрана опция «Не проверять сертификат сервера на отзыв»;
- имеются ошибки в соединениях (сторонние программы: прокси, антивирус, DLP-система пытаются анализировать трафик);
- в настройках Internet Explorer не выбраны TLS 1.1 и TLS 1.2.

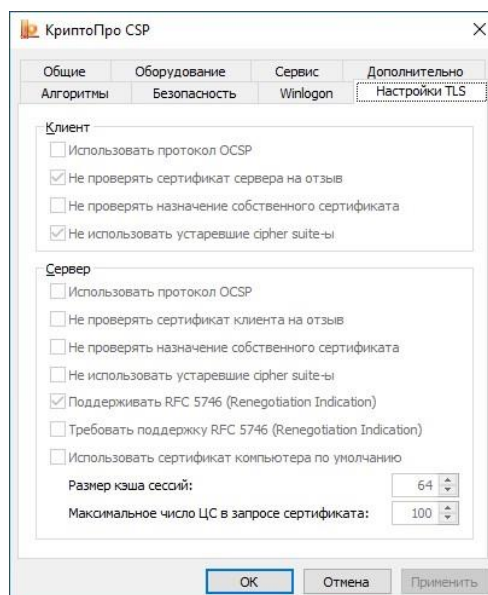


Рисунок 13. Отключение проверки сертификатов на отзыв

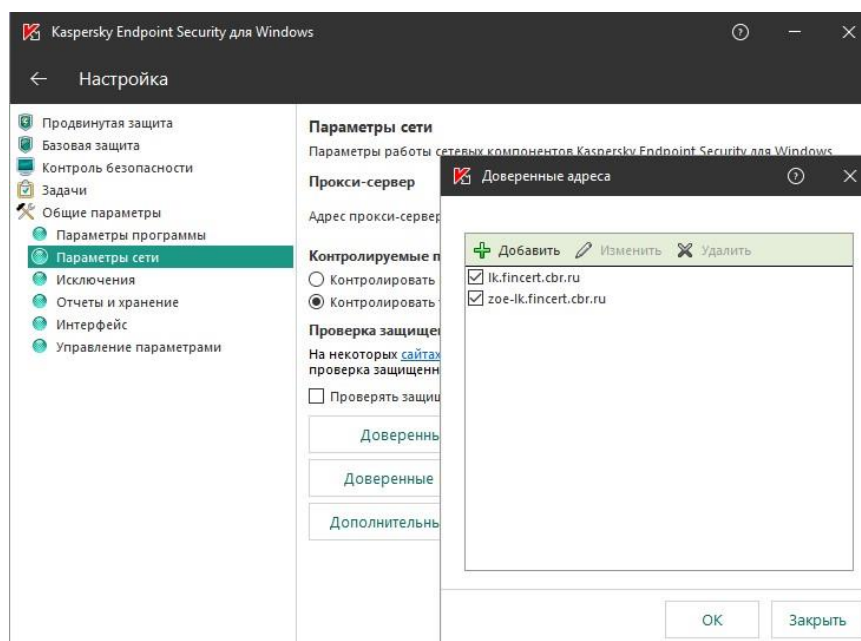


Рисунок 14. Добавить ресурсы АСОИ ФинЦЕРТ в белый список

## 30. Ошибка подключения при использовании браузера Microsoft Edge, как быть?

Если все сертификаты установлены корректно, но тем не менее не удастся подключиться к ресурсам АСОИ ФинЦЕРТ с помощью браузера Microsoft Edge, то рекомендуется провести следующие действия.

В случае применения СКЗИ «Континент TLS-клиент» указать префикс «http://» вместо «https://».

В случае применения СКЗИ КриптоПро перезапустить браузер в режиме совместимости с Internet Explorer. Для этого в параметрах программы разрешить перезапустить браузер в нужном режиме (см. рис. 15).

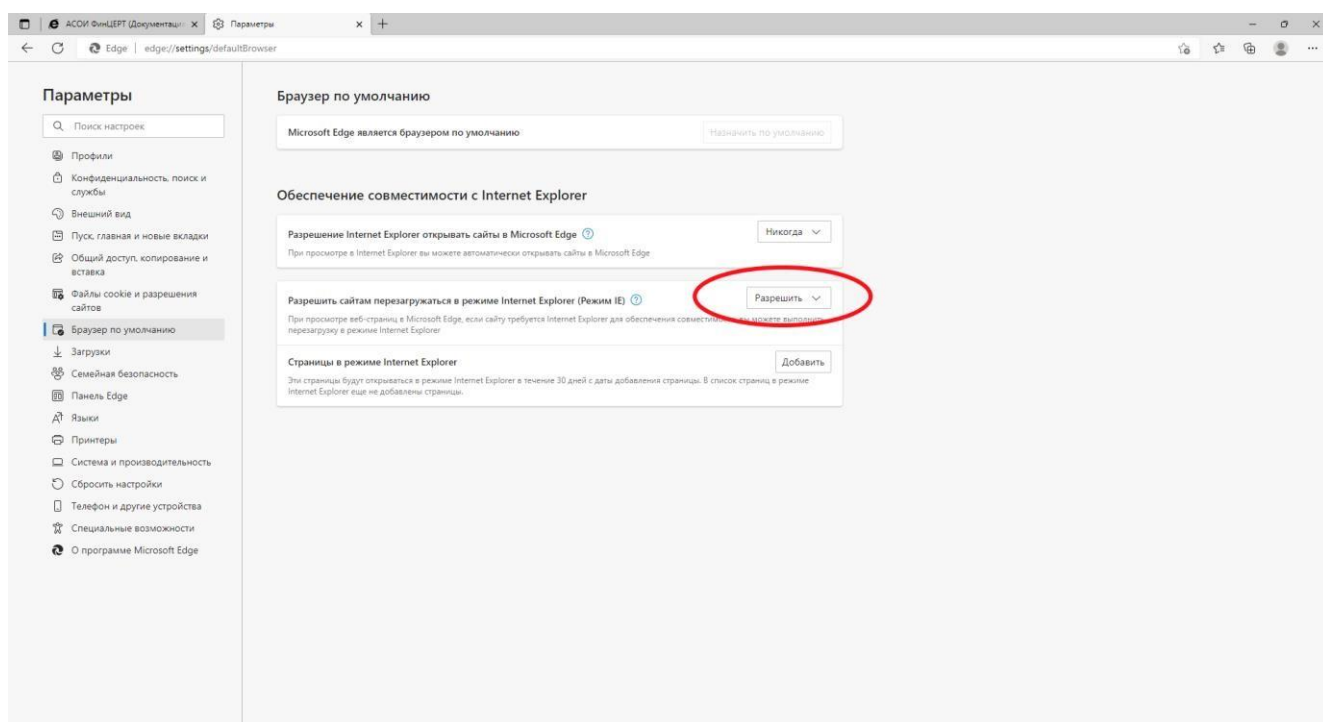


Рисунок 15. Настройка параметров браузера Microsoft Edge.

После чего произвести перезагрузку web-страницы в режиме совместимости браузера Microsoft Internet Explorer (см. рис.16).

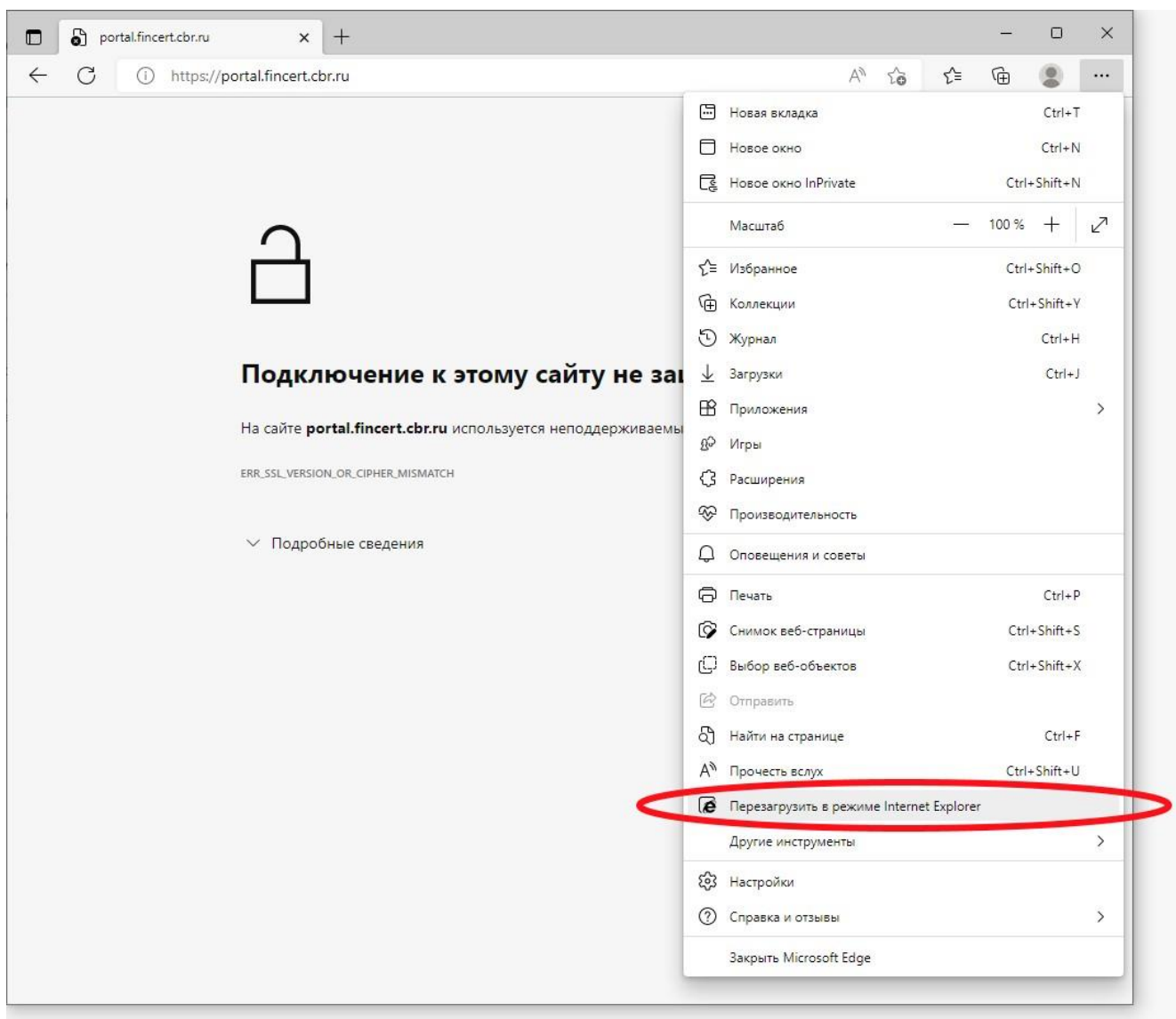


Рисунок 16. Перезапуск браузера в режиме Internet Explorer.

### 31. Не удастся подключиться к АСОИ ФинЦЕРТ, в чем причина?

Даже если ранее взаимодействие с АСОИ ФинЦЕРТ работало, в какой-то момент времени подключение может прерваться.

В случае с СКЗИ «Континент TLS-клиент» первым делом следует убедиться, что в разделе «Главная» перечень соединений отображается без красных иконок. Для восстановления соединений необходимо попробовать выбрать опцию «Сброс соединений» (нажать правой кнопкой мыши на иконке в области состояний (системном трее)), если не помогло – перезапустить приложение.

Также следует проверить что в параметрах сетевого соединения выбраны опции использовать TLS 1.1 и TLS 1.2.

Возможна ситуация, когда из-за вновь установленных программ или обновлений операционной системы СКЗИ перестало работать. В этом случае возможна ситуация, когда СКЗИ не работает по причине нарушения контроля целостности. На примере СКЗИ «Континент TLS-клиент» можно попробовать исправить ситуацию запустив утилиту «Контроль целостности TLS-клиент» и выбрать опцию «Пересчитать контрольные суммы». Если это не помогло, то следует запустить программу «Просмотр событий» (eventvwr.msc) и проверить журналы событий на наличие ошибок. Если имеются ошибки, то попробовать переустановить СКЗИ через панель «Установка и удаление программ». (Для СКЗИ «КриптоПро» дополнительно можно использовать утилиту «cspclean.exe», доступна на официальном сайте компании). Если провести автоматическое удаление ПО в полном объеме не получается (повторная установка происходит с ошибкой), то следует попробовать удалить оставшиеся файлы в ручном режиме. В случае СКЗИ «Континент TLS-клиент» следует очистить ветки реестра:

HKEY\_LOCAL\_MACHINE\SOFTWARE\SecurityCode\TlsClient

HKEY\_LOCAL\_MACHINE\SOFTWARE\SecurityCode\TlsClient\Setup

и каталоги на жестком диске: c:\Program Files\Security

Code\Continent TLS Client

c:\Users\Public\ContinentTLSCClient

Также при возникновении ошибок в подключении к ресурсам АСОИ ФинЦЕРТ следует включить логирование, после чего проанализировать логи на предмет наличия ошибок.

В том случае, если при подключении к ресурсам АСОИ ФинЦЕРТ операционная система предлагает выбрать пользовательский сертификат, но не предлагает ввести пин-код, либо возникает ошибка доступа к контейнеру закрытого ключа, то рекомендуется попробовать переустановить пользовательский сертификат, после чего проверить, что цепочка доверительных отношений сертификатов (корневой – промежуточный – личный) выстроена корректно. В этом случае рекомендуется попробовать скопировать закрытую часть ключа на другой носитель (в реестр операционной системы либо наоборот на внешний носитель информации).

В некоторых случаях, например, при ошибках в браузере Internet Explorer удастся подключиться к АСОИ ФинЦЕРТ с использованием альтернативным способом, например, через «Яндекс.Браузер» с включенной опцией «Подключаться к сайтам, использующим шифрование по ГОСТ».

## 32. Как определить период действия пользовательского TLS-сертификата?

В свойствах TLS-сертификата указывается период, в течении которого сертификат является действительным, при этом возможность установления зашифрованного соединения определяется периодом использования закрытого ключа. В зависимости от версии операционной системы это поле может отображаться либо в виде текстового поля, либо в виде числового дампа. В последнем случае необходимо обратить внимание на правый столбец и считать последовательность цифр. На приведенном рисунке справа это дата: 2023-06-15 23:59:00.

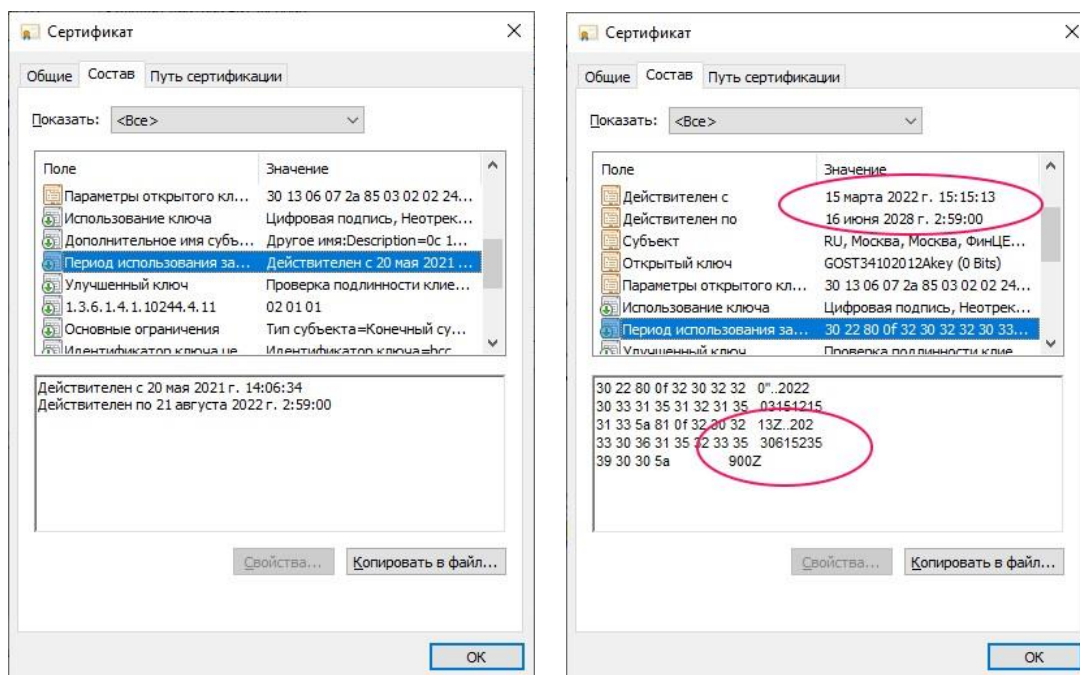


Рисунок 17. Информация о периоде действия TLS-сертификата

Тем не менее, при использовании криптопровайдера от компании КриптоПро имеется особенность. Срок действия сертификата определяется несколькими условиями, в том числе периодом использования закрытого ключа, который отсчитывается с даты формирования контейнера закрытого ключа. На практике это означает, что для в КриптоПро CSP полезный срок использования ограничивается максимально возможным периодом в 1 год и 3 месяца с даты формирования заявки на выпуск TLS-сертификата, что иногда может быть меньше срока действия сертификата, прописанного в удостоверяющем центре при его выпуске.

Для получения информации о сроке действия закрытого ключа рекомендуется на вкладке «Сервис» КриптоПро CSP выбрать команду «Протестировать...», которая для выбранного контейнера предоставит информацию о сроке действия закрытого ключа.

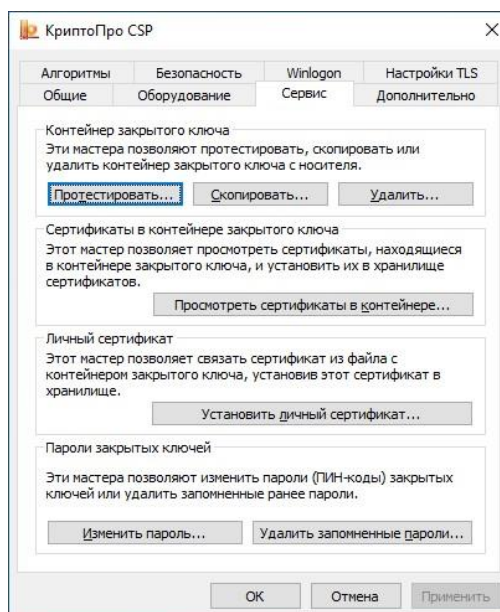


Рисунок 18. Информация о периоде действия TLS-сертификата

### 33. Можно ли получить TLS-сертификаты без личной явки в территориальное учреждение Банка России?

Да, такая возможность появилась в 2023 году, после издания обновленного «Регламента получения ключевой информации». При этом сохранилась так же и возможность получить TLS-сертификат путем личной явки в территориальное учреждение Банка России.

### 34. Кто имеет возможность получить сертификаты без личного присутствия (личной явки) в территориальном учреждении Банка России?

Процедура получения сертификатов без личного присутствия требует подтверждения АКС ТУ правомерности выдачи TLS-сертификата. При оформлении сертификата без личного присутствия в этом случае организуется цепочка доверия к направляемому Участником документу на основе криптографических сертификатов. Для этой цели оформляется доверенность в электронном виде на основании информации о ранее выданном сертификате электронной подписи в Удостоверяющем центре Банка России, которая позволяет доверять произвольному личному сертификату электронной подписи (полученному работником организации в любом аккредитованном удостоверяющем центре).

Таким образом, возможностью получения TLS-сертификата и сертификата электронной подписи АСОИ ФинЦЕРТ (может быть оформлен в личном кабинете Участника АСОИ

ФинЦЕРТ) обладают работники тех организаций, в которых руководители получили сертификаты электронной подписи в Удостоверяющем центре Банка России.

### 35. Как и в каком виде оформить доверенность на получение ключевой информации без личного присутствия?

Доверенность оформляется в виде документа по образцу, приведенном в Приложении И к Регламенту получения ключевой информации.

**ДОВЕРЕННОСТЬ № 1**

**на право обращаться в Банк России по вопросам получения ключевой информации для работы с АСОИ ФинЦЕРТ**

г.Москва <small>(наименование населенного пункта)</small>	«01» апреля 2023 г. <small>(дата, месяц, год)</small>
Настоящей доверенностью,	ООО «Банк Проверочный» <small>(полное наименование организации)</small>
в лице	Председателя Правления, Иванова Ивана Ивановича <small>(должность руководителя, ФИО)</small>
действующего на основании	Приказа №1/2023 от 09.01.2023 <small>(учредительный документ)</small>
подтверждает полномочия	начальника службы ИБ, Петрова Петра Петровича <small>(должность, ФИО)</small>
Сертификат УКЭП работника	40601d006e0f913b4251e2e961cdb777 <small>(серийный номер сертификата УКЭП)</small>

**Настоящая доверенность выдана по «31» декабря 2023 г. без права передоверия.**



Рисунок 19. Пример оформления доверенности

В тексте документа обязательно должны быть указаны: наименование организации, должность и ФИО руководителя, на имя которого в Удостоверяющем центре Банка России был выдан сертификат электронной подписи, должность и ФИО работника и номер его личного

сертификата УКЭП (который может быть получен в любом аккредитованном удостоверяющем центре).

Проставление в документе плашки с визуализацией электронной подписи, содержащей информацию о подписании электронной подписью, с указанием номера, владельца и периода действия сертификата ключа проверки электронной подписи не является обязательным.

Сформированный электронный документ в виде PDF-файла (предпочтительно), либо в виде файла с изображением (в формате Jpeg или PNG) необходимо подписать в виде отсоединенной электронной подписи. Исходный файл (PDF, JPG, PNG) и файл с проставленной электронной подписью (SIG) необходимо направить АКС ТУ.

Аналогичным образом подписываются электронной подписью прочие документы.

### 36. Каким образом можно подписать электронный файл?

Подписание электронного файла необходимо осуществлять любым программным средством, обеспечивающим работу с электронной подписью в виде отсоединенного файла с использованием отечественной криптографии.

Например, можно использовать ПО КриптоАРМ, которое позволяет производить подписание документов в виде отсоединенной подписи, см. рис.20.

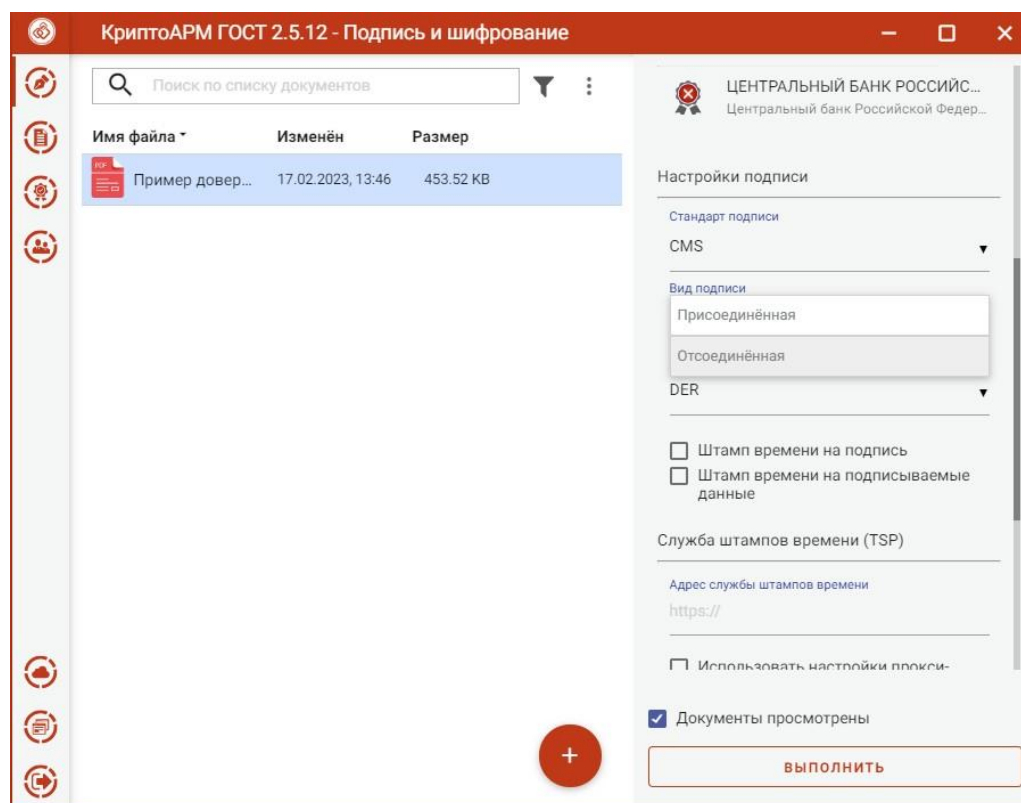


Рисунок 20. Пример выбора вида подписи в ПО КриптоАРМ

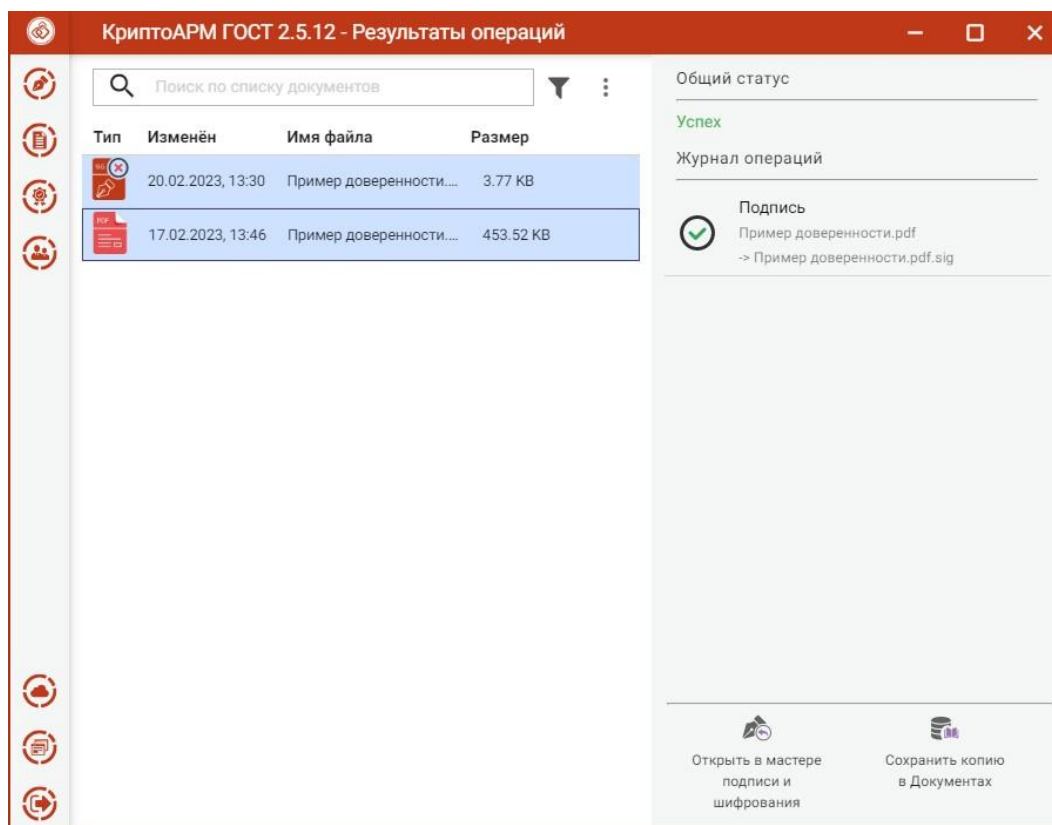


Рисунок 21. Интерфейс ПО КриптоАРМ

Аналогичным образом можно использовать программную компоненту «Инструменты КриптоПро» (CryptoPro Tools, cptools), из состава ПО КриптоПро CSP версии 5, см. рис.22.

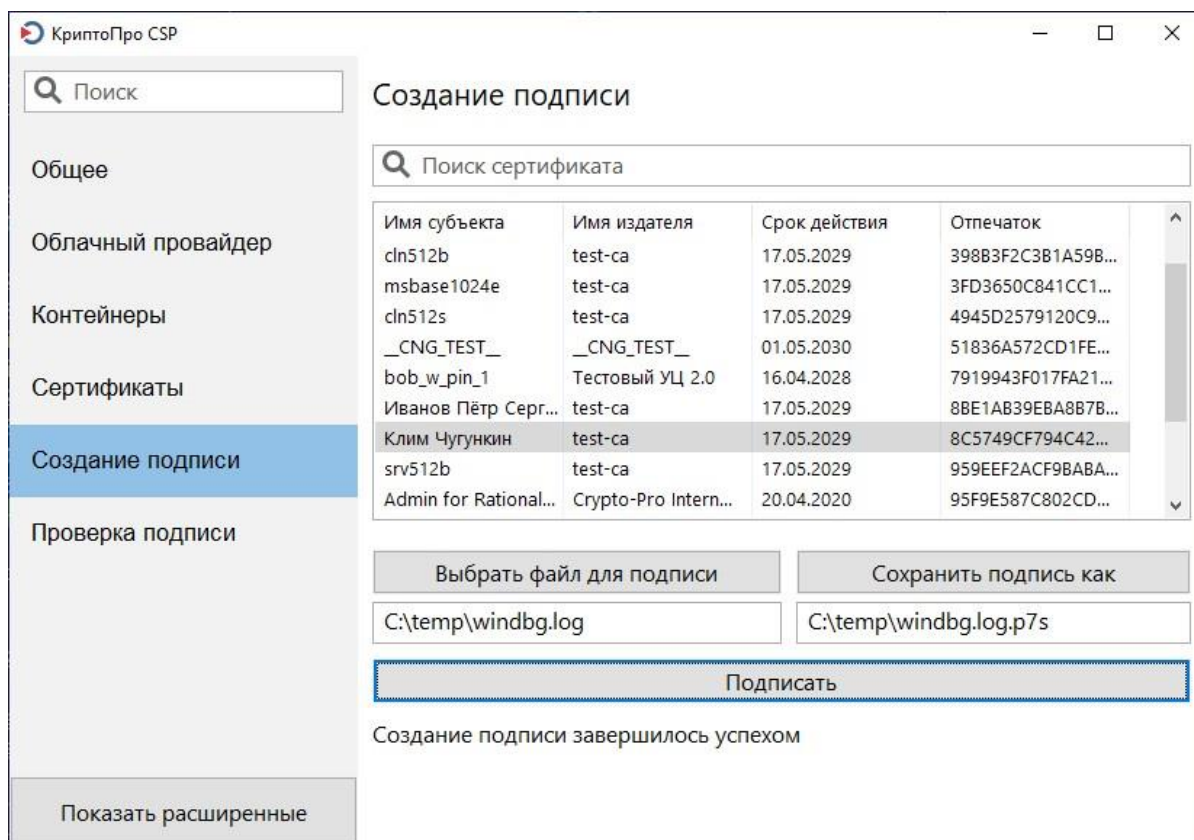


Рисунок 22. Интерфейс ПО «Инструменты КриптоПро» (картинка взята с сайта [www.cryptopro.ru](http://www.cryptopro.ru))

### 37. Каким образом оформить распечатку TLS-сертификата в электронном виде?

АКС ТУ БР направляет распечатку TLS-сертификата в электронном виде. Пользователь Участника должен распечатать и собственноручно расписаться в распечатке. После чего отсканированное изображение распечатки (в формате PDF (рекомендуется) или в виде файла изображения (в формате Jpeg или PNG) уполномоченный представитель Участника подписывает отсоединенной электронной подписью и направляет по электронной почте АКС ТУ БР. При этом номер сертификата электронной подписи уполномоченного представителя Участника должен соответствовать номеру, указанному в доверенности на право получения ключевой информации.

### 38. Можно ли обойтись без оформления доверенности?

Регламент получения ключевой информации позволяет не оформлять доверенность на уполномоченного представителя Участника, если файлы будут подписаны УКЭП лица, имеющего право действовать от имени Участника без доверенности.

Обращаем внимание, что в этом случае Участник все равно обязан сообщить контакты уполномоченного представителя Участника для решения возникающих вопросов в рабочем порядке.

### 39. Что делать если не получается подключиться к АСОИ ФинЦЕРТ?

Представленного в данном документе материала достаточно для проведения успешного подключения к АСОИ ФинЦЕРТ. При этом следует иметь ввиду, что вопросы настройки СКЗИ относятся к зоне ответственности пользователей Участника.

В случае возникновения вопросов, связанных с подключением к АСОИ ФинЦЕРТ, и не описанных в настоящем документе, просьба направлять их на адрес электронной почты: [svc\\_fincert\\_support@cbr.ru](mailto:svc_fincert_support@cbr.ru).

После подключения к АСОИ ФинЦЕРТ, все вопросы по работе в системе необходимо направлять через личный кабинет Участника, с приложением необходимых материалов, см. бюллетень: FinCERT-20220113-INFO «О направлении вопросов по работе в АСОИ ФинЦЕРТ».