Центральный Банк Российской Федерации
(Банк России)

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБРАБОТКИ ИНЦИДЕНТОВ ФИНЦЕРТ БАНКА РОССИИ

Регламент подключения участников информационного обмена к АСОИ ФинЦЕРТ

На 37 листах

2019

Аннотация

Настоящий документ содержит регламент подключения участников информационного обмена автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России.

Документ разработан в соответствии с РД 50-34.698-90 «Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов» и ГОСТ 2.105-95 «ЕСКД. Общие требования к текстовым документам»

Содержание

1 Общие положения 6
2 Регистрация Участника 9
3 Установка и настройка ПО 10
3.1 Требования к АРМ 10
3.2 Общие требования 11
3.3 Требования к подключению 12
3.4 Установка и настройка TLS-клиента/СКЗИ 12
3.5 Установка сертификатов 26
3.6 Описание и устранение возможных ошибок при подключении к АСОИ ФинЦЕРТ 29
4 Первый вход в АСОИ ФинЦЕРТ 31
5 Подключение нового пользователя зарегистрированного Участника 33
6 Перечень типовых ошибок при подключении и способы их решения 34
6.1 Ошибки при подключении к АСОИ ФинЦЕРТ 34
6.2 Ошибки при регистрации Континент TLS Клиента 34
Перечень принятых сокращений 35
Перечень принятых терминов 36

Перечень иллюстраций

Рисунок 1 – сайт Код Безопасности, на котором можно скачать TLS-клиент 13

Рисунок 2 – сайт Код Безопасности, главная страница, демоверсии программ. 13

Рисунок 3 – сайт Код Безопасности, регистрация. 14

Рисунок 4 – сайт Код Безопасности, регистрация, заполнение полей для создания учетной записи. 14

Рисунок 5 – Лицензионное соглашение 15

Рисунок 6 – Продолжение установки после ознакомления с лицензионным соглашением 15

Рисунок 7 – Завершение установки 16

Рисунок 8 – Накопление энтропии для биологического датчика случайных чисел 17

Рисунок 9 – Согласие о регистрации 17

Рисунок 10 – Начало регистрации 18

Рисунок 11 – Ввод регистрационных данных 18

Рисунок 12 – Загрузка файла конфигурации 19

Рисунок 13 – Выбор файла конфигурации 20

Рисунок 14 – Успешный результат загрузки файла конфигурации 20

Рисунок 15 – Сообщение об отключении проверки CRL 21

Рисунок 16 – Окно «Управление сертификатами» 21

Рисунок 17 – Выбор сертифкатов веб-ресурсов 22

Рисунок 18 – Окно «Управление сертификатами-Серверные сертифкаты» . 22

Рисунок 19 – Окно настройки параметров прокси-сервера в Континент-TLS 23

Рисунок 20 – Окно настройки параметров прокси-сервера в веб-браузере... 24

Рисунок 21 – Окно настройки исключений для прокси-сервера в веб-браузере 24

Рисунок 22 – Главное окно программы «Контроль целостности» 25

Рисунок 23 – Настройка режима работы контроля целостности 26

Рисунок 24 – Окно запуска мастера импорта сертификатов 27

Рисунок 25 – Мастер импорта сертификатов – выбор хранилища сертификатов 27

Рисунок 26 – Мастера импорта сертификатов «Доверенные корневые центры сертифкации»..... 28

Рисунок 27 – Мастер импорта сертификатов «Доверенные корневые центры сертифкации»..... 28

Рисунок 28 – Мастер импорта сертификатов – Завершение мастера импорта сертифкатов 29

Рисунок 29 – Сообщение об успешном импорте сертифката..... 29

Рисунок 30 – Окно смены пароля первого входа..... 31

1 Общие положения

Настоящий Регламент устанавливает порядок подключения Участников к АСОИ ФинЦЕРТ.

Регламент предназначен для Участников, не зарегистрированных в АСОИ ФинЦЕРТ, а также зарегистрированных в АСОИ ФинЦЕРТ.

Не поднадзорным организациям, для подключения к АСОИ ФинЦЕРТ, предварительно необходимо подписать документ «Типовая форма соглашения о взаимодействии Центрального банка Российской Федерации по вопросам противодействия компьютерным атакам» (http://www.cbr.ru/StaticHtml/File/14435/agreement.pdf) и отправить в Центральный банк Российской Федерации в двух экземплярах, подписанных со стороны организации.

Для обеспечения взаимодействия между Участниками и Центром посредством АСОИ ФинЦЕРТ каждый из Участников должен иметь хотя бы одного зарегистрированного пользователя.

Для осуществления информационного взаимодействия посредством АСОИ ФинЦЕРТ Участникам необходимо:

- направить запрос на регистрацию на адрес электронной почты info_fincert@cbr.ru с пометкой «Информационное взаимодействие». К запросу приложить заполненную Форму карточки участника;
- получить от Центра:
  - учетные данные для доступа в АСОИ ФинЦЕРТ;
  - документ «Руководство Участника по работе с АСОИ ФинЦЕРТ»;
  - корневые сертификаты и сертификаты веб-ресурсов.

В период до 15.08.2019 (включительно) для защищенного подключения к АСОИ ФинЦЕРТ используются следующие сертификаты (далее - Сертификаты 1), доступные по ссылке http://cbr.ru/StaticHtml/File/14408/ASOI_docs.zip (в папке «сертификаты»):

- cacert_nuc.cer – корневой сертификат Национального удостоверяющего центра;
- cacert_guc.cer – корневой сертификат Головного удостоверяющего центра;

- lk.fincert.cbr.ru.cer – сертификат ресурса lk.fincert.cbr.ru;
- portal.fincert.cbr.ru.cer – сертификат ресурса portal.fincert.cbr.ru;
- api.fincert.cbr.ru.cer- сертификат ресурса api.fincert.cbr.ru.

Начиная с 16.08.2019 для защищенного подключения к АСОИ ФинЦЕРТ будут использоваться следующие сертификаты (далее - Сертификаты 2), доступные по ссылке http://cbr.ru/StaticHtml/File/14408/ASOI_docs.zip (в папке «сертификаты 2019-2020») и на информационном портале в разделе «АСОИ ФинЦЕРТ (Документация и ПО Участника)» https://portal.fincert.cbr.ru/Content/1069/cert_asoi_2019.rar (доступно для подключенных к АСОИ ФинЦЕРТ Участников с установленной ГОСТ- криптографией):

- cacert.cer – корневой сертификат удостоверяющего центра;
- cacert.crl– список отозванных сертификатов;
- lk.fincert.cbr.ru.cer – сертификат ресурса lk.fincert.cbr.ru;
- portal.fincert.cbr.ru.cer – сертификат ресурса portal.fincert.cbr.ru;
- api.fincert.cbr.ru.cer- сертификат ресурса api.fincert.cbr.ru.

Описание установки сертификатов приведено в п. 3.5.

Далее Участники могут осуществлять работу в АСОИ ФинЦЕРТ в соответствии с документом «Руководство Участника по работе с АСОИ ФинЦЕРТ». Актуальные версии документации для работы с АСОИ ФинЦЕРТ будут размещаться в информационном портале (https://portal.fincert.cbr.ru) в разделе «АСОИ ФинЦЕРТ (Документация и ПО Участника)».

При работе в АСОИ ФинЦЕРТ и формировании запросов в ФинЦЕРТ Участники могут использовать следующие типы данных:

- реальные данные об инцидентах информационной безопасности в организациях банковской системы РФ – участниках информационного обмена;
- тестовые (имитационные) данные об инцидентах информационной безопасности в организациях банковской системы РФ – участниках информационного обмена. При внесении тестовых данных необходимо помечать их заголовки и темы символом «***». Тестовые (имитационные)

данные должны в максимальной мере соответствовать информации, которую предполагается заполнять участнику информационного обмена (по структуре, форматам, наполнению и т.д.). Запросы, содержащие тестовые (имитационные) данные, не обрабатываются операторами ФинЦЕРТ.

2 Регистрация Участника

На основании полученной по электронной почте карточки Участника Центр осуществляет создание не менее одной учетной записи пользователя Участника с правами на управление пользователями в рамках Участника (Ответственный УИО), учетные записи пользователей (Пользователь УИО) и пароли для первичного входа в личный кабинет Участника.

По умолчанию пароль учетной записи создается с требованием его смены при первом входе в АСОИ ФинЦЕРТ.

Созданная учетная запись и первичный пароль передаются Центром на указанные в карточке Участника адрес электронной почты и/или телефон ответственного лица.

Регистрация пользователя Участника осуществляется Центром после получения им запроса на регистрацию от Ответственного УИО. Запрос от Ответственного УИО может быть получен как через Личный кабинет Участника либо посредством электронной почты в рабочем порядке.

3 Установка и настройка ПО

3.1 Требования к АРМ

Для работы с АСОИ ФинЦЕРТ должны использоваться АРМ с характеристиками, не ниже представленных в таблице 1.

Таблица 1 – Системные требования к АРМ для работы с АСОИ ФинЦЕРТ

Оборудование	Рекомендуемые требования
Процессор	не хуже Intel Core i3
ОЗУ	>3072 Мб
Графическая карта	Разрешение не менее 1920x1080 точек, с возможностью вывода изображения на 2 монитора
НЖМД	>80 Гб
Сетевой адаптер	Ethernet 100 Base-T и выше
Монитор	диагональ не менее 19 дюймов разрешение не менее 1920x1080 точек

На АРМ, должно быть установлено следующее программное обеспечение:

- операционная система Microsoft Windows 7/10;
- Adobe Acrobat Reader 11 и выше;
- обозреватель (любой из):
  - Microsoft Edge;
  - Microsoft Internet Explorer версии не ниже 11;
  - Google Chrome версии не ниже 60;
- одно из следующих СКЗИ для установки защищенного соединения с АСОИ ФинЦЕРТ (через браузер Microsoft Internet Explorer):
  - КриптоПро CSP;

- VipNet CSP;
- Lissi CSP;

- средство антивирусной защиты.

ВАЖНО! *Установку «Континент TLS-клиент» на АРМ, предназначенный для работы с АСОИ ФинЦЕРТ,* ***не производить*** *в случае, если на АРМ установлено СКЗИ КриптоПро/VipNet CSP/Lissi CSP, поддерживающее с работу с ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012 (с использованием ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012), и планируется использовать только обозреватели Microsoft Internet Explorer.*

Дистрибутивы СКЗИ и эксплуатационная документация доступны для скачивания на официальных сайтах производителей данных средств:

- Континент TLS-клиент: https://www.securitycode.ru/products/demo-versions/ ;
- КриптоПро CSP: https://www.cryptopro.ru/products/csp/downloads ;
- VipNet CSP: https://infotecs.ru/downloads/besplatnye-produkty/vipnet-csp.html ;
- Lissi CSP: http://lissi-crypto.ru/downloads/download_lissi_csp/ .

Установка СКЗИ осуществляется в соответствии с эксплуатационной документацией на них.

В п.3.4 описана установка Континент TLS-клиент как основного средства для доступа к АСОИ ФинЦЕРТ.

3.2 Общие требования

Перед началом работы необходимо получить в Центральном банке Российской Федерации (при первичном подключении участника к АСОИ ФинЦЕРТ) или от ответственного представителя в организации - Участнике уже подключенного к АСОИ ФинЦЕРТ:

- конфигурационный файл для TLS-клиента с настройками подключения к АСОИ ФинЦЕРТ;
- корневые сертификаты удостоверяющих центров;
- сертификаты ресурсов portal.fincert.cbr.ru и lk.fincert.cbr.ru;

- руководство участника по работе с АСОИ ФинЦЕРТ.

Перечисленные выше средства, за исключением TLS-клиента, предаются Центром в виде архива (АСОИ ФинЦЕРТ.zip), содержащего следующие каталоги и файлы:

- conf.json – конфигурационный файл, содержащий параметры подключения к АСОИ ФинЦЕРТ;
- cacert_nuc.cer – корневой сертификат Национального удостоверяющего центра;
- cacert_guc.cer – корневой сертификат Головного удостоверяющего центра;
- portal.fincert.cbr.ru.cer – сертификат ресурса lk.fincert.cbr.ru;
- lk.fincert.cbr.ru.cer – сертификат ресурса portal.fincert.cbr.ru;
- Руководство_участника.pdf – содержит руководство участника по работе с АСОИ ФинЦЕРТ.

3.3 Требования к подключению

Для подключения к АСОИ ФинЦЕРТ на стороне Участника должны быть настроены:

- сетевые правила, разрешающие подключение по порту 443 к адресам:
  - portal.fincert.cbr.ru;
  - lk.fincert.cbr.ru;
- в средстве антивирусной защиты должен быть отключен контроль исходящих соединений на 443 порт при использовании для доступа к АСОИ ФинЦЕРТ ПО Континент TLS-клиент.

3.4 Установка и настройка TLS-клиента/СКЗИ

Для обеспечения защищенного доступа по алгоритмам ГОСТ к АСОИ ФинЦЕРТ на АРМ необходимо установить TLS- клиент.

Для этого:

1 Перейдите на сайт https://www.securitycode.ru. Если есть учетная запись (аккаунт) на данном сайте – необходимо осуществить вход под своими логином и паролем:

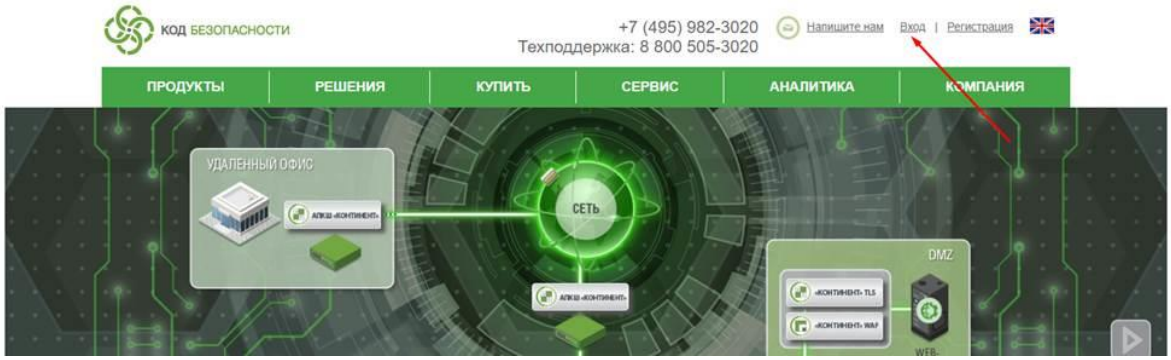

Рисунок 1 – сайт Код Безопасности, на котором можно скачать TLS-клиент

2 Зайдите в раздел демоверсии: https://www.securitycode.ru/products/demo-versions/. Ссылка на этот раздел есть на главной странице сайта:

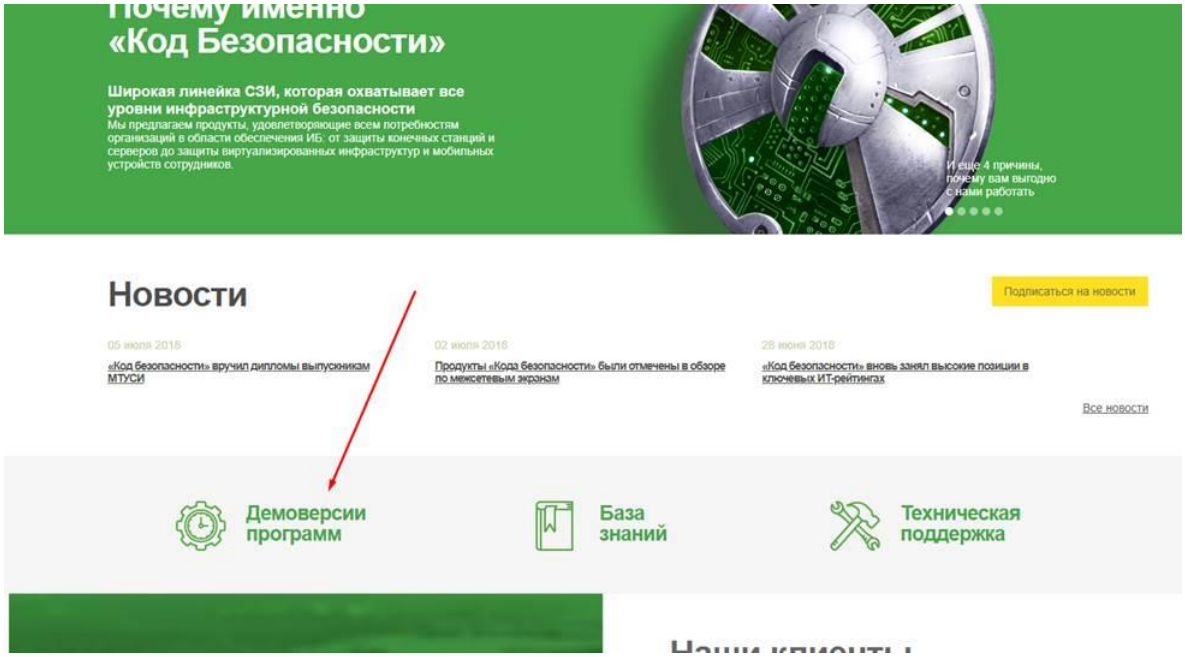

Рисунок 2 – сайт Код Безопасности, главная страница, демоверсии программ.

3 Если аккаунта на указанном сайте нет, то необходимо его создать, нажав кнопку «Регистрация»:

Рисунок 3 – сайт Код Безопасности, регистрация.

В открывшемся окне заполнить форму регистрации:

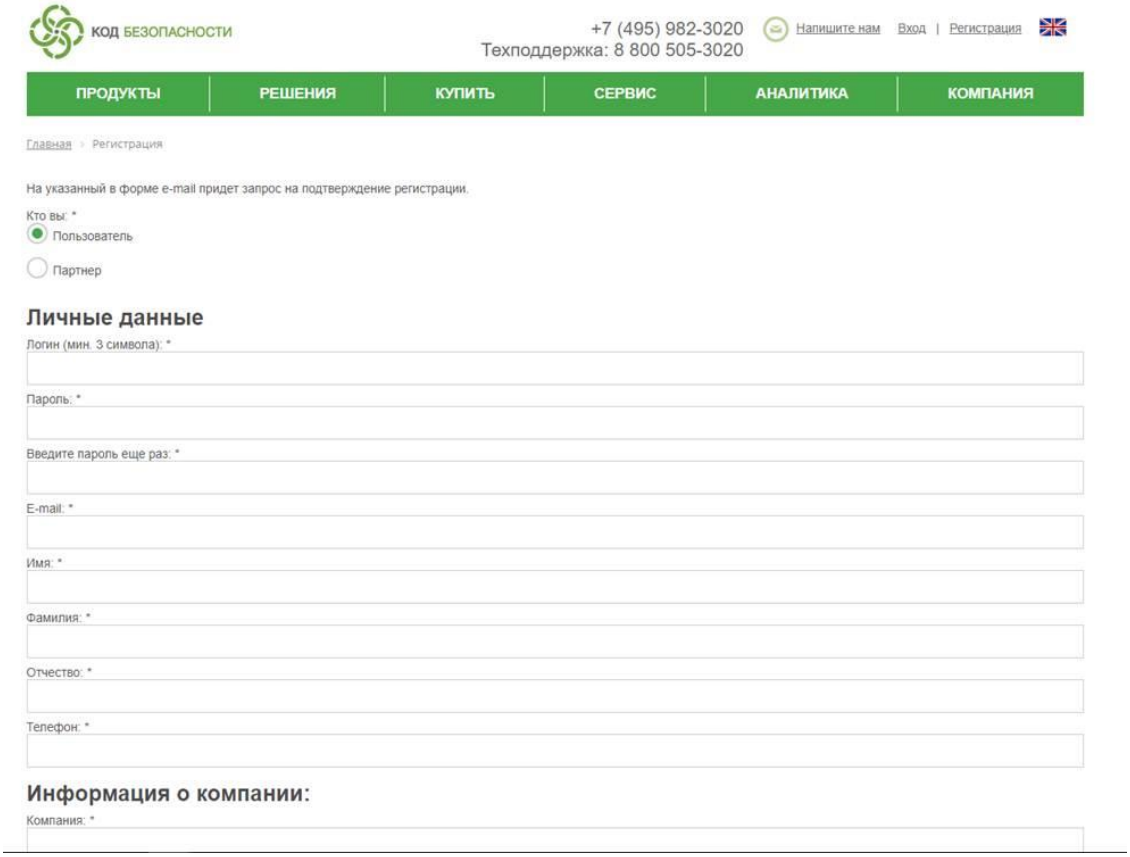

Рисунок 4 – сайт Код Безопасности, регистрация, заполнение полей для создания учетной записи.

После успешной регистрации и аутентификации под своими учетными данными, переходим в раздел демоверсии: https://www.securitycode.ru/products/demo-versions/

4 Запустите на исполнение файл Континент TLS-клиент.exe. На экране появится окно установки TLS-клиента с текстом лицензионного соглашения.

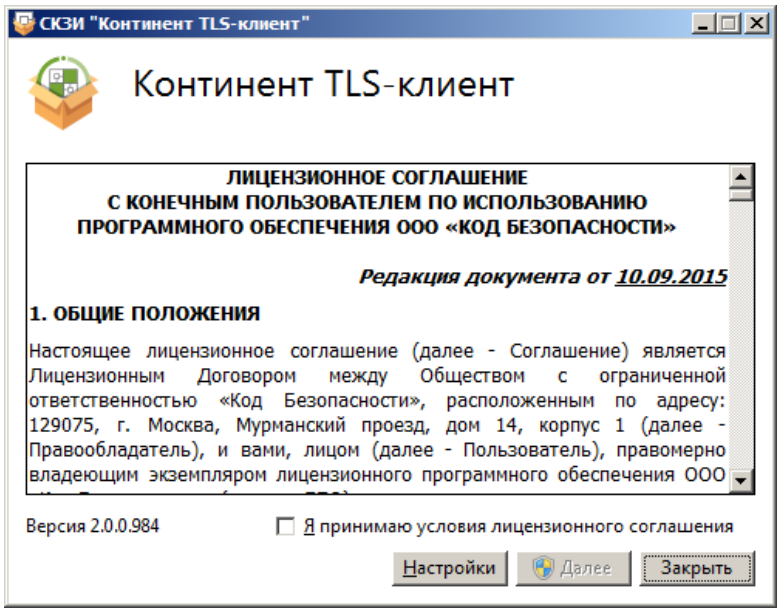

Рисунок 5 – Лицензионное соглашение

Прочтите лицензионное соглашение и, если вы принимаете его условия, поставьте отметку в поле «Я принимаю условия лицензионного соглашения», затем нажмите кнопку «Далее».

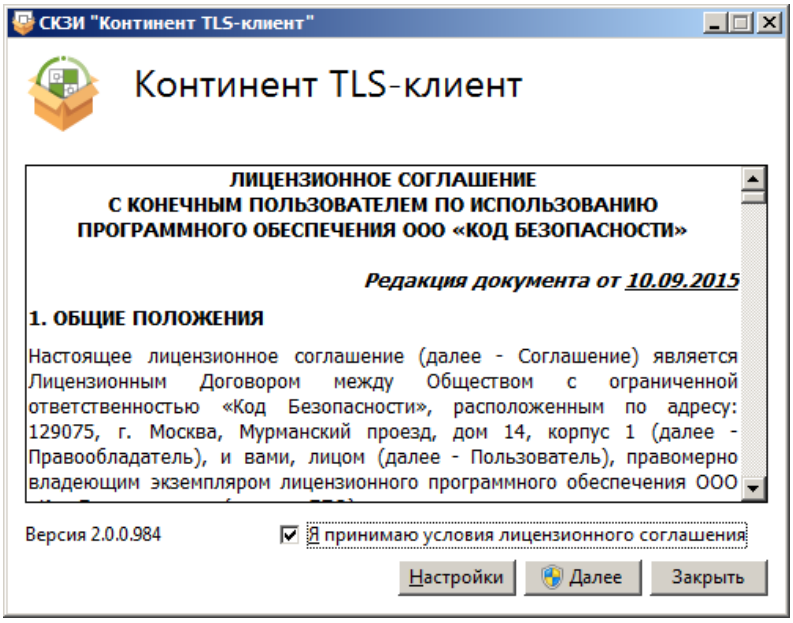

Рисунок 6 – Продолжение установки после ознакомления с лицензионным соглашением

Программа установки выполнит диагностику системы, после чего начнется установка ПО. После ее успешного завершения на экране появится сообщение о необходимости перезагрузки компьютера.

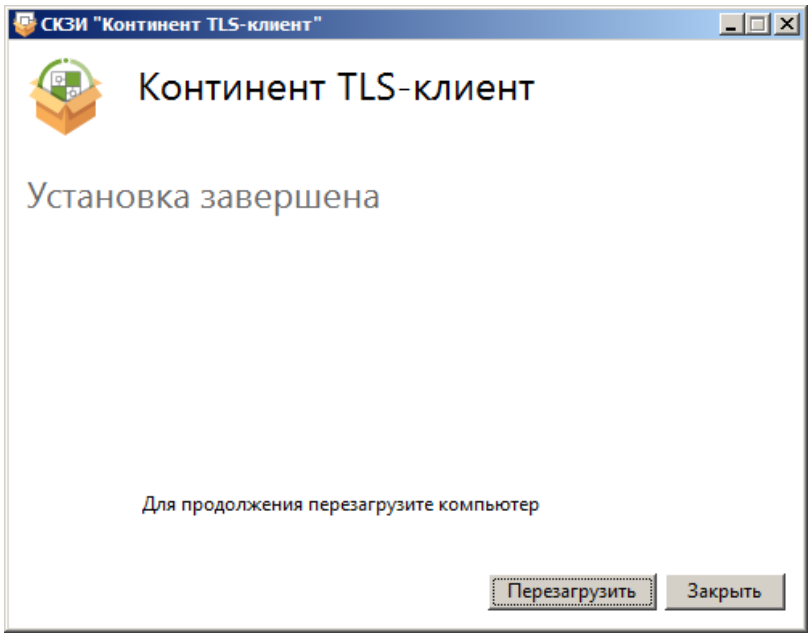

Рисунок 7 – Завершение установки

5 Нажмите кнопку «Перезагрузить» в окне сообщения. Начнется перезагрузка компьютера. После установки TLS-клиента на рабочем столе Windows появится ярлык запуска графического приложения TLS-клиента, а в главном меню Windows появится раздел «Код Безопасности».

При первом запуске TLS-клиента откроется окно с сообщением о накоплении энтропии для биологического датчика случайных чисел. Для выполнения этой процедуры необходимо будет кликать левой кнопкой «мыши» по мишени.

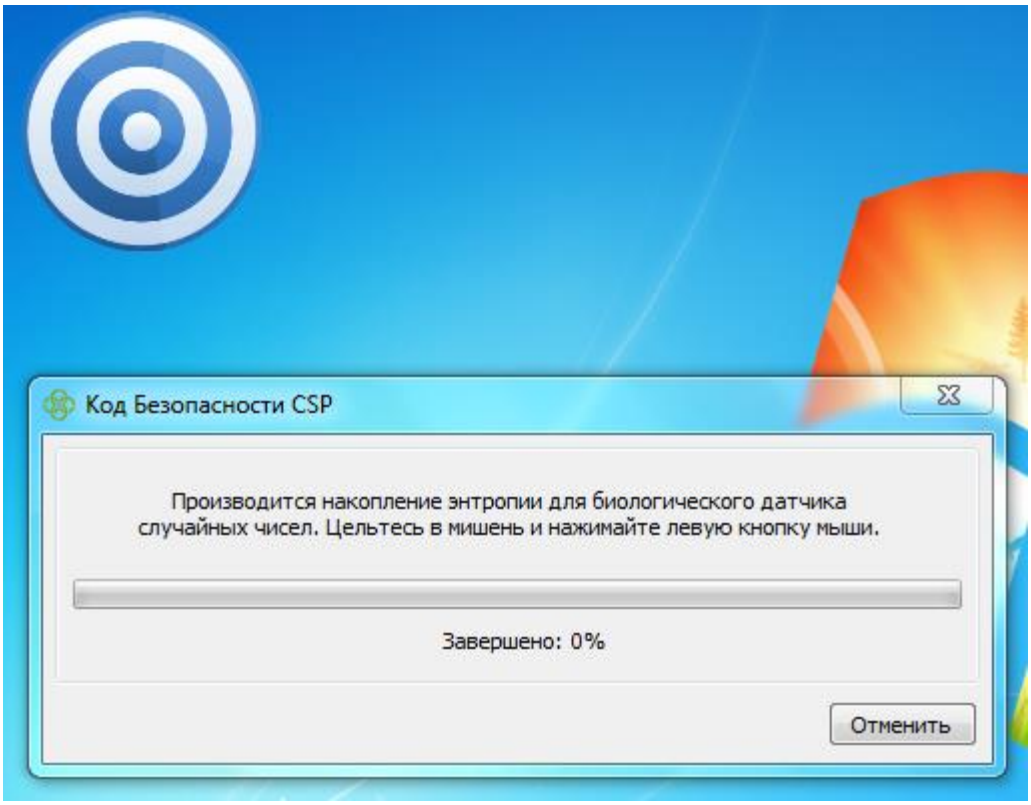

Рисунок 8 – Накопление энтропии для биологического датчика случайных чисел

После завершения установки TLS-клиента необходимо выполнить процедуру его регистрации.

Для регистрации TLS-клиента необходимо выполнить следующие действия:

1 В открывшейся при запуске форме нажать кнопку «Да».

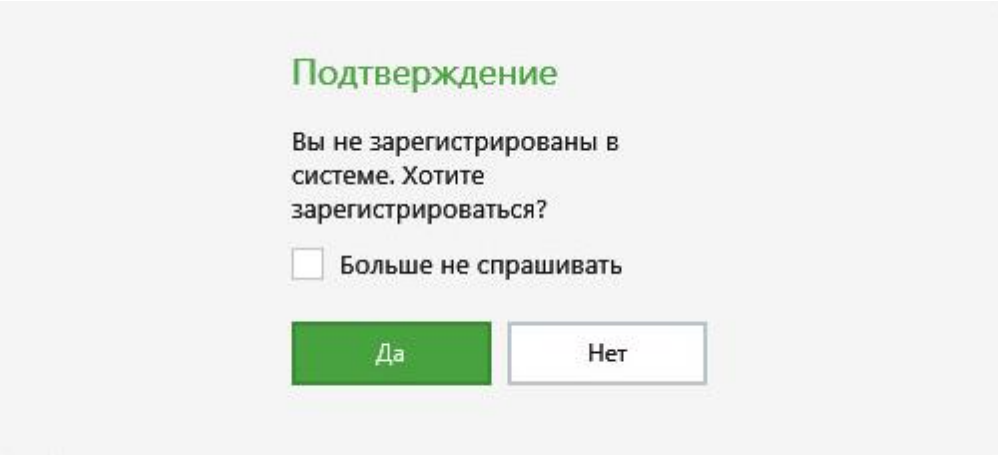

Рисунок 9 – Согласие о регистрации

2 В случае отмены автоматического отображения окна регистрации при запуске TLS-клиента выберите в меню настроек TLS-клиента пункт «Регистрация» и нажмите кнопку «Начать».

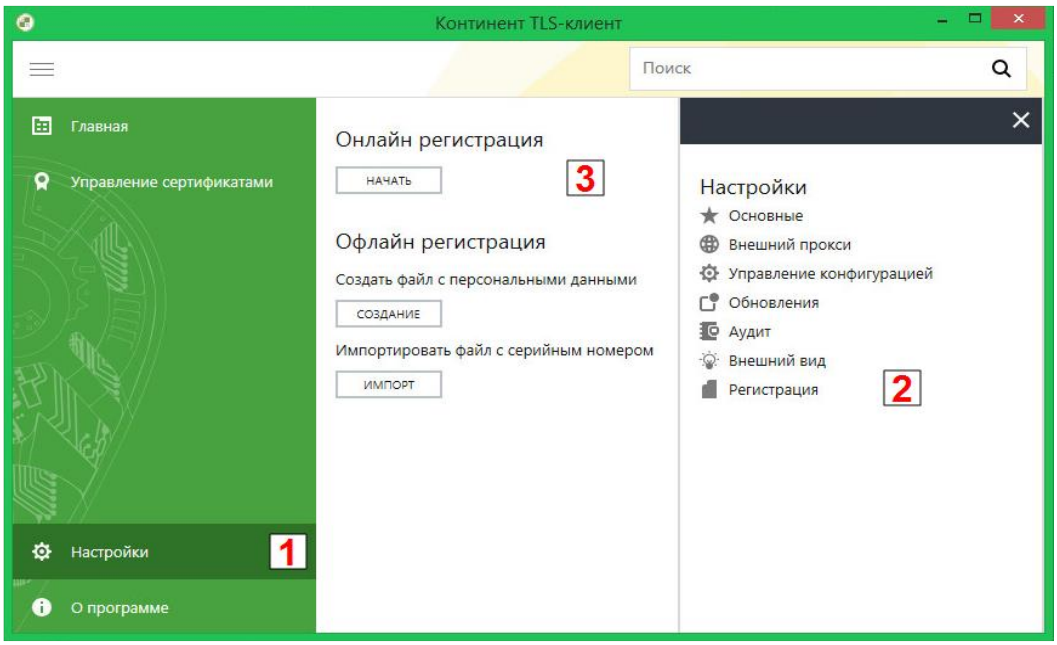

Рисунок 10 – Начало регистрации

На экране появится диалоговое окно регистрации.

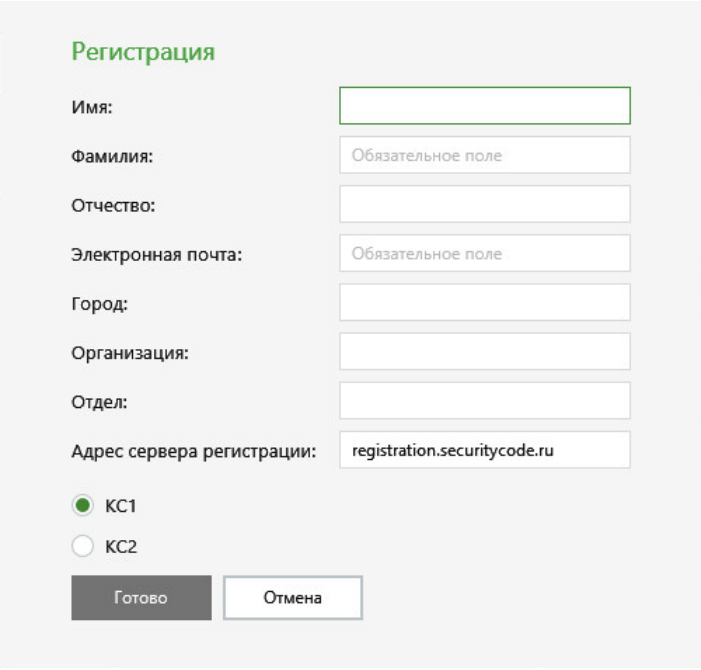

Рисунок 11 – Ввод регистрационных данных

Введите требуемые параметры и нажмите кнопку «Готово». Адрес сервера регистрации и выбор «КС1» **не изменять.**

Начнется процесс регистрации и подключения к указанному серверу. При его успешном завершении на экране появится соответствующее информационное окно.

После установки и регистрации TLS-клиента необходимо:

1 Импортировать конфигурационный файл TLS-клиента conf.json, для этого необходимо:

- запустить TLS-клиент на АРМ;
- выбрать пункт «Настройки» - «Управление конфигурацией»;

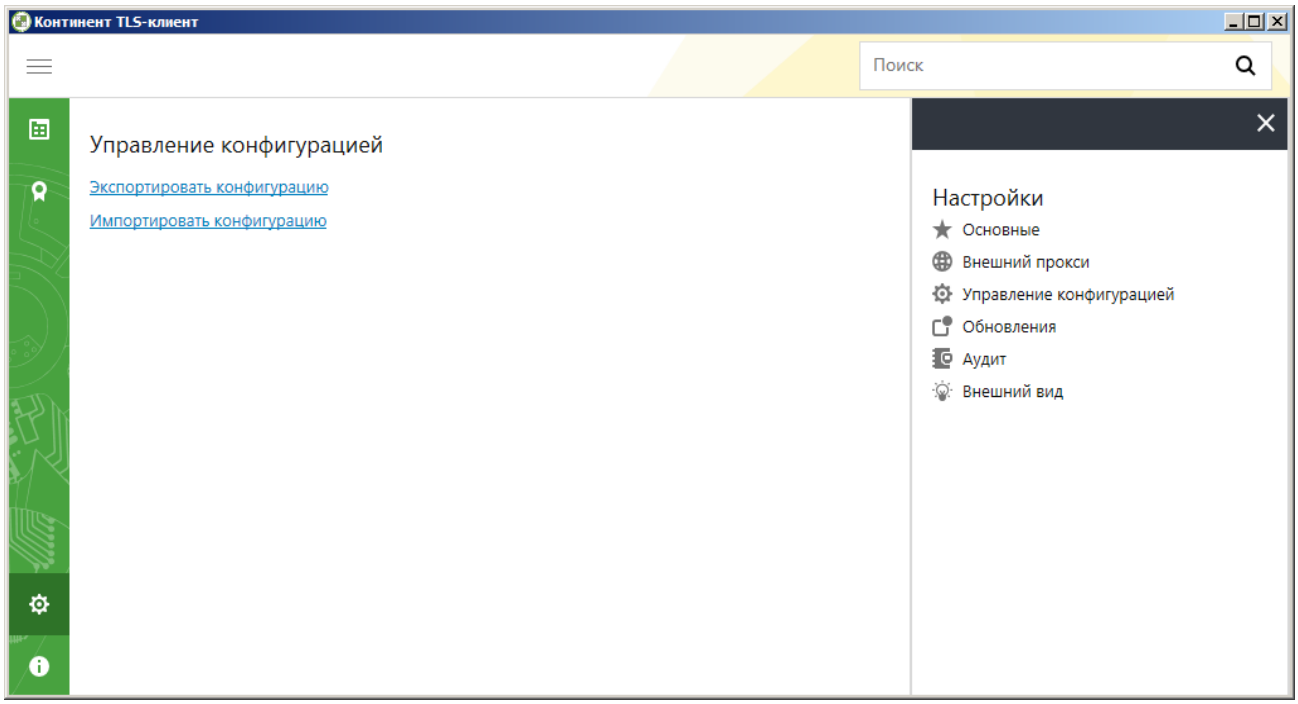

Рисунок 12 – Загрузка файла конфигурации

- в левой части выбрать пункт «Импортировать конфигурацию».

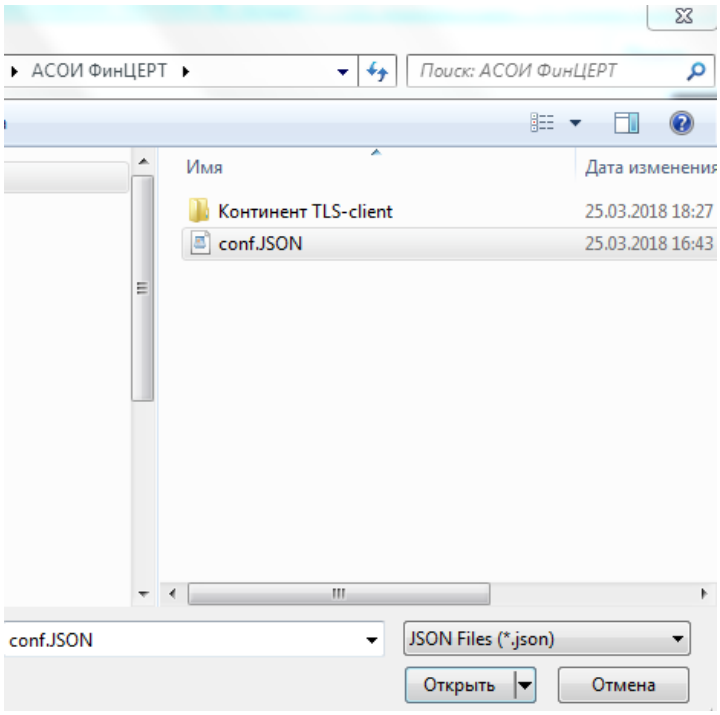

Рисунок 13 – Выбор файла конфигурации

- осуществить загрузку файла конфигурации.
- в случае успешной загрузки появится сообщение.

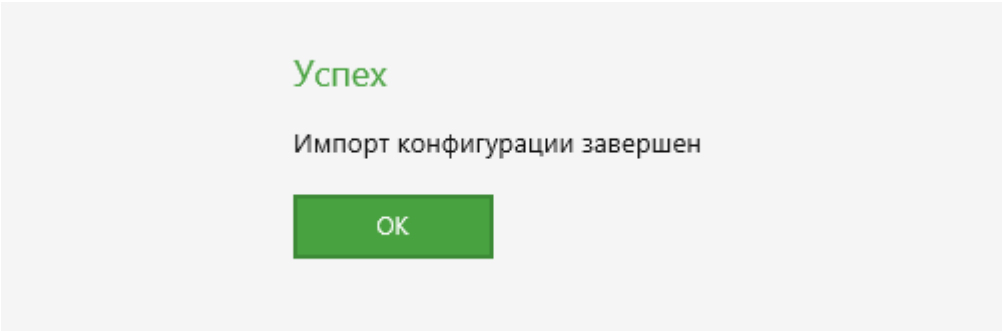

Рисунок 14 – Успешный результат загрузки файла конфигурации

- после нажатия кнопки «ОК» появится сообщение

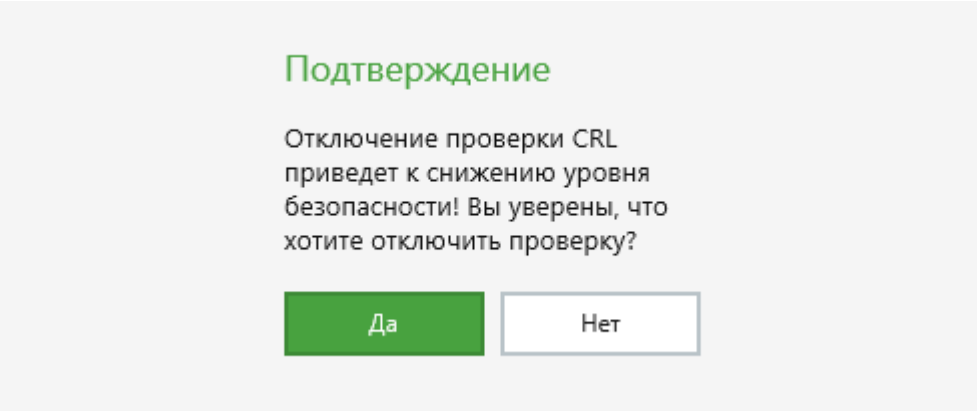

Рисунок 15 – Сообщение об отключении проверки CRL

- подтвердить отключение проверки CRL, нажав кнопку «Да»

2 Добавить сертификаты веб-ресурсов, для этого необходимо:

- в главном окне программы перейти на вкладку «Управление сертификатами» и выбрать «Импортировать»;

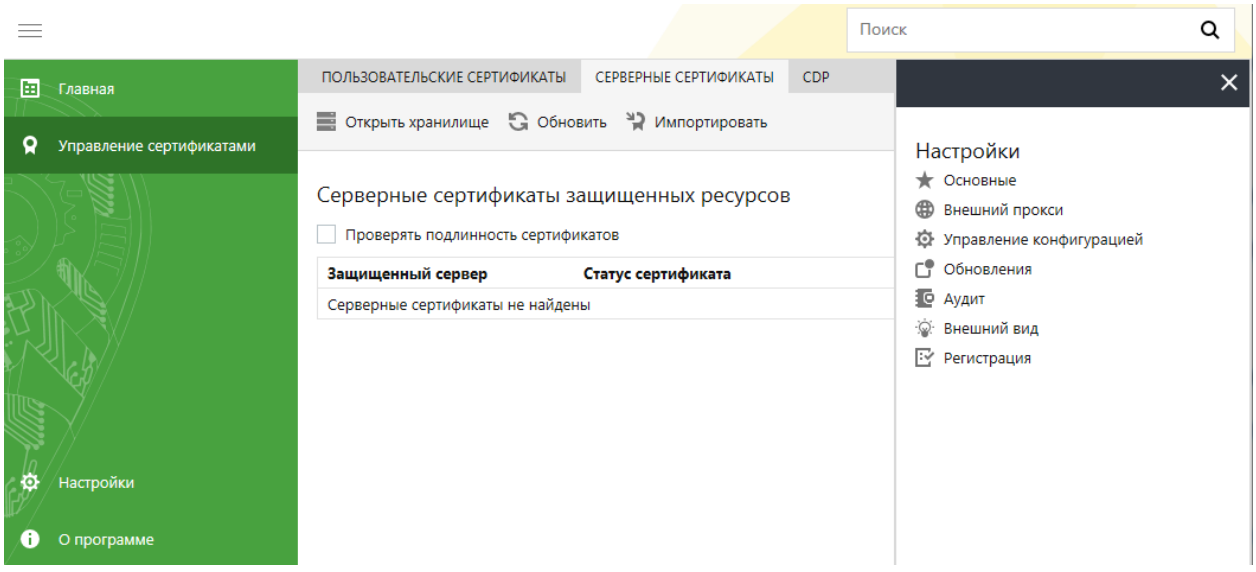

Рисунок 16 – Окно «Управление сертификатами»

- в открывшемся окне выбора файлов выбрать по очереди файлы lk_cert.cer и portal_cert.cer и нажать кнопку «Открыть»;

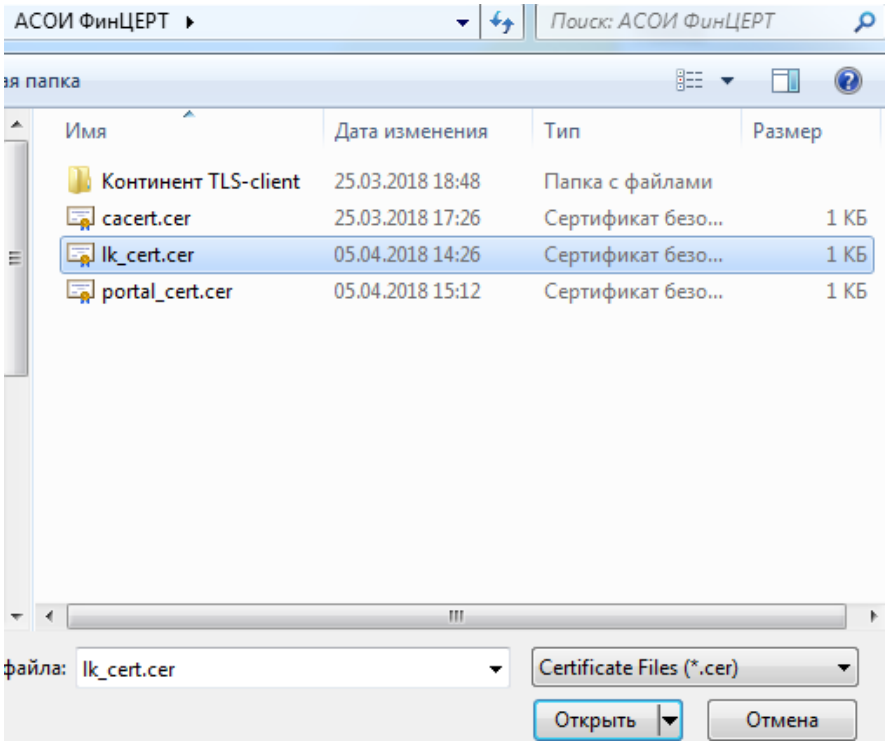

Рисунок 17 – Выбор сертифкатов веб-ресурсов

- добавленные сертификаты будут отображены в списке «Серверные сертификаты».

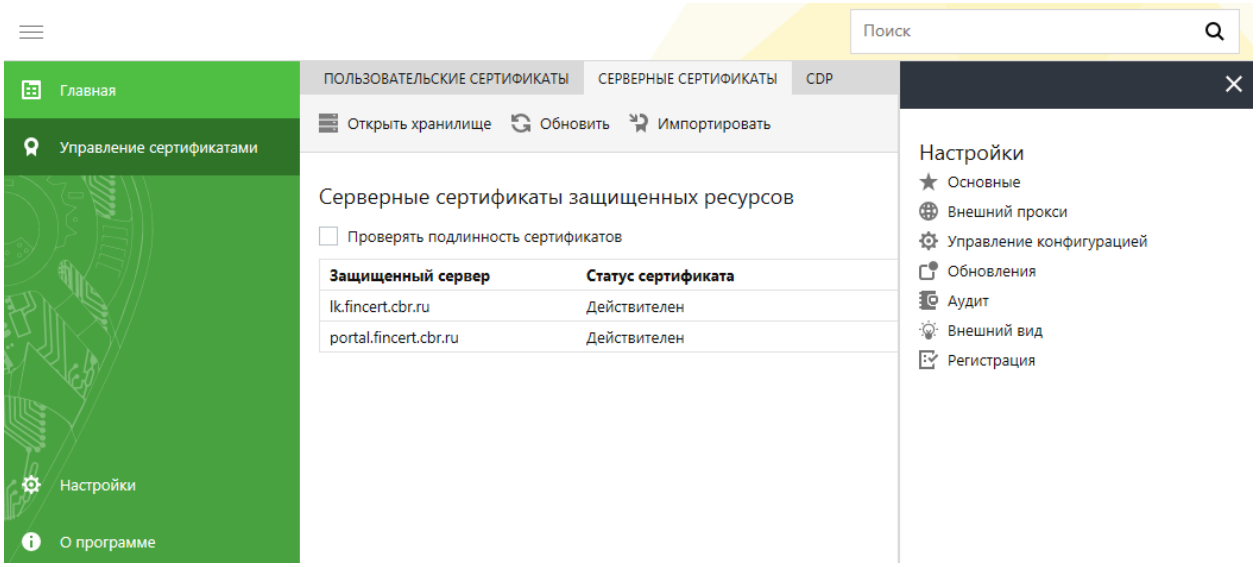

Рисунок 18 – Окно «Управление сертификатами-Серверные сертифкаты»

3 Если для доступа к сети Интернет используется прокси сервер, необходимо провести настройки программы для корректной работы с прокси сервером:

- в основном окне выберите пункт вызова настроек  и выберите в меню настроек пункт «Внешний прокси», после чего появится окно настроек, в котором необходимо выбрать «Использовать внешний прокси-сервер», указать настройки для работы с прокси сервером и нажать кнопку «сохранить».

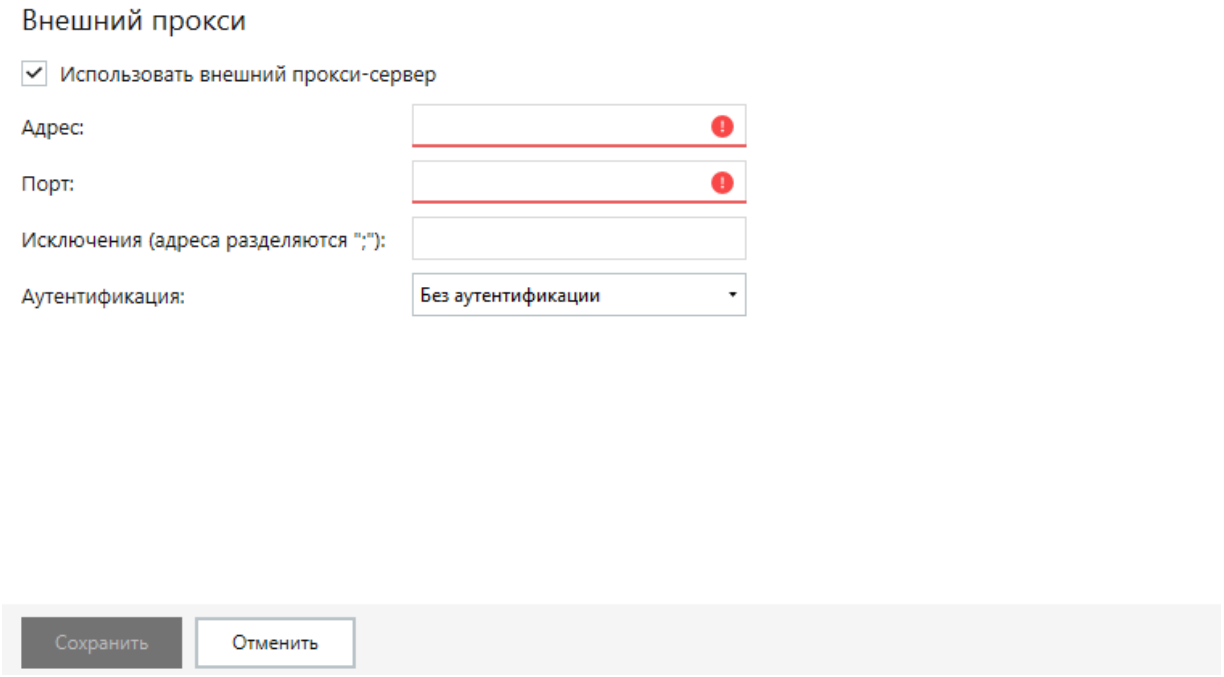

Рисунок 19 – Окно настройки параметров прокси-сервера в Континент-TLS

- в вэб-браузере укажите явные настройки прокси-сервера и добавьте в исключения адреса portal.fincert.cbr.ru и lk.fincert.cbr.ru:

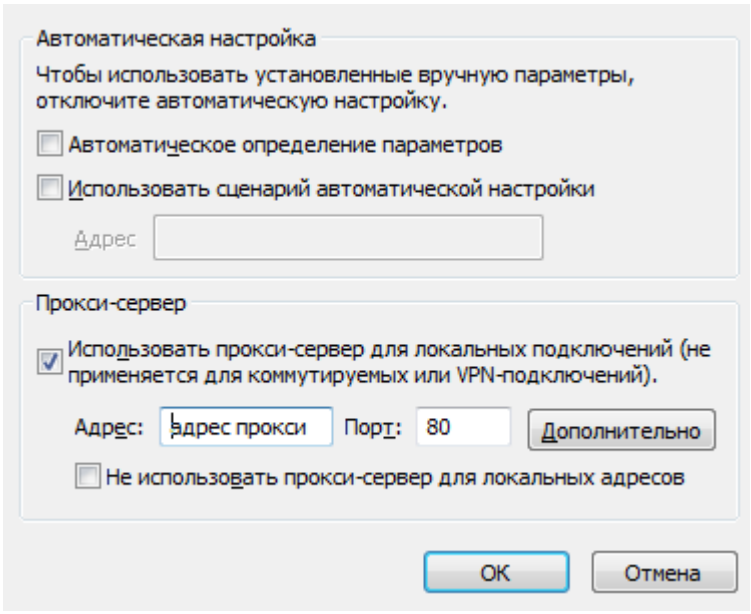

Рисунок 20 – Окно настройки параметров прокси-сервера в веб-браузере

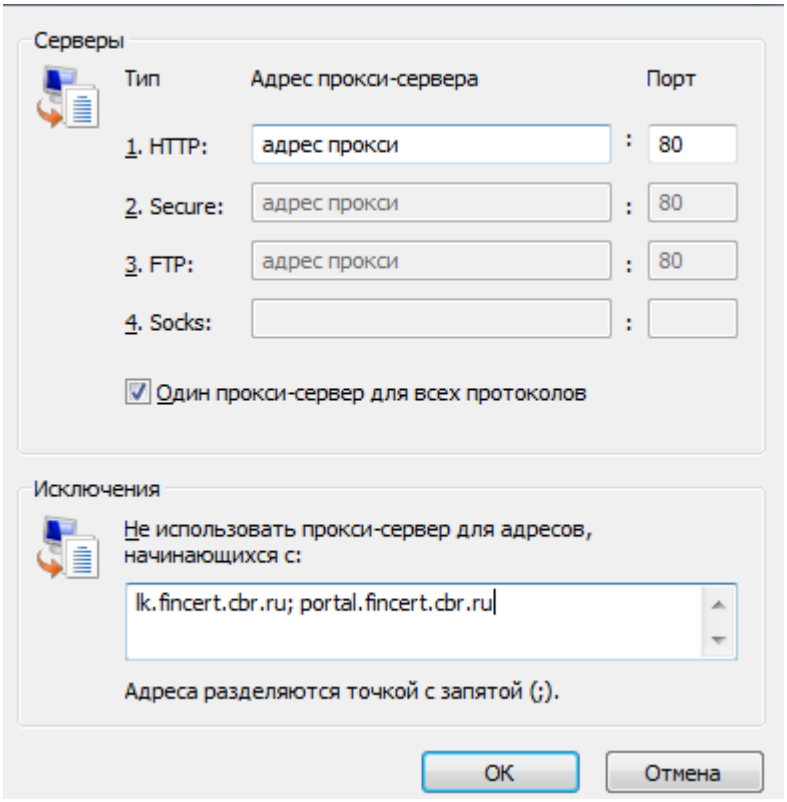

Рисунок 21 – Окно настройки исключений для прокси-сервера в веб-браузере

4 Настройте режим работы контроля целостности:

- запустите программу «Контроль целостности», для этого выберите в главном меню Windows пункт «Все приложения| Код Безопасности |Контроль целостности»;

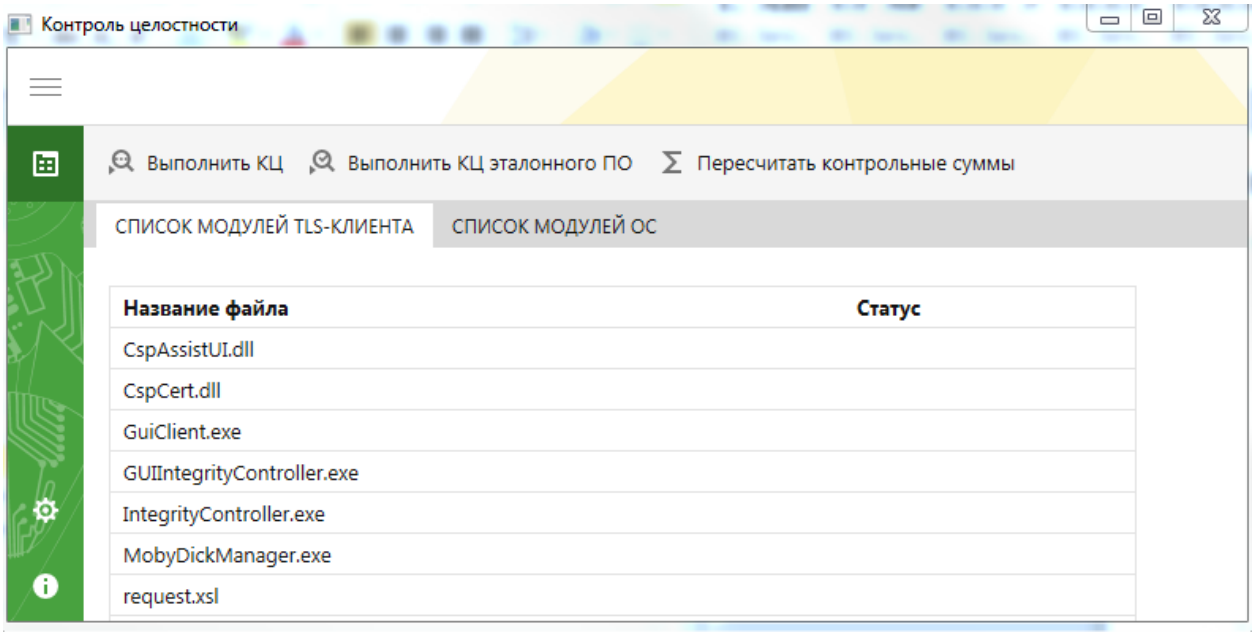

Рисунок 22 – Главное окно программы «Контроль целостности»

- в основном окне выберите пункт вызова настроек . На экране появится текущее расписание регламентных проверок. В открывшемся окне выберите «Разрешить работу при повреждении системных файлов», выбор данной настройки необходим для корректной работы при обновлении операционной системы.

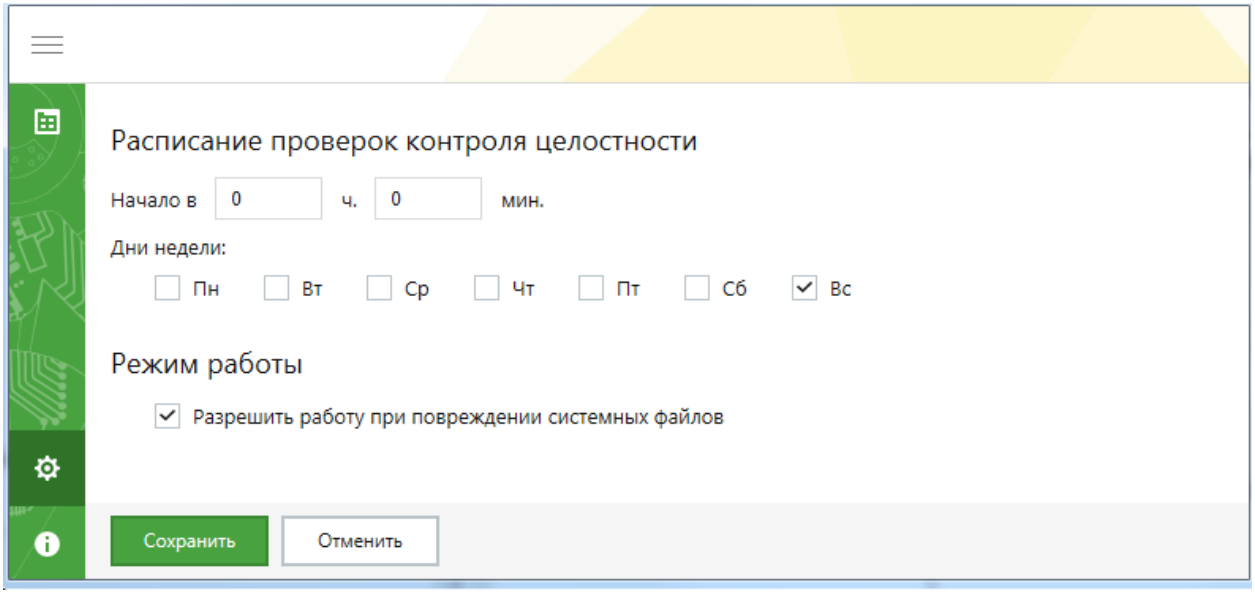

Рисунок 23 – Настройка режима работы контроля целостности

3.5 Установка сертификатов

Для установки корневых сертификатов удостоверяющих центров необходимо последовательно открыть файлы с сертификатами:

- cacert_nuc.cer;
- cacert_guc.cer.

Для каждого сертификата в открывшемся окне нажать кнопку «Установить сертификат». В открывшемся окне мастера импорта сертификатов нажать кнопку «Далее».

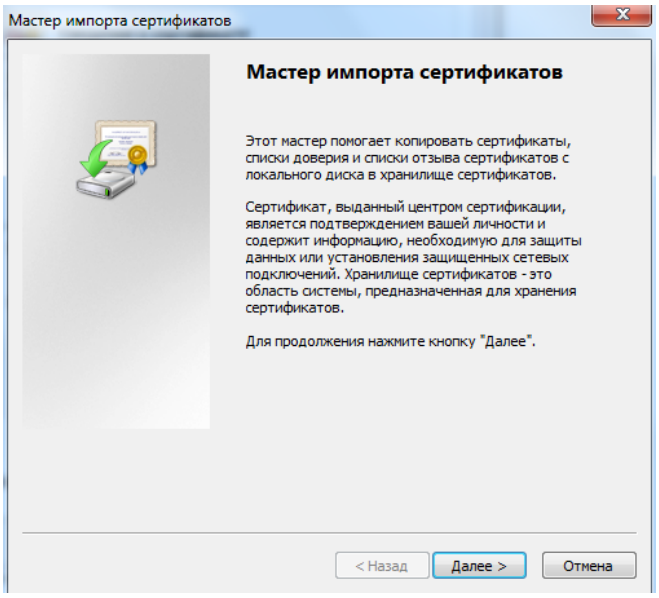

Рисунок 24 – Окно запуска мастера импорта сертификатов

В открывшемся окне необходимо выбрать пункт «Поместить все сертификаты в выбранное хранилище» и нажать кнопку «Обзор».

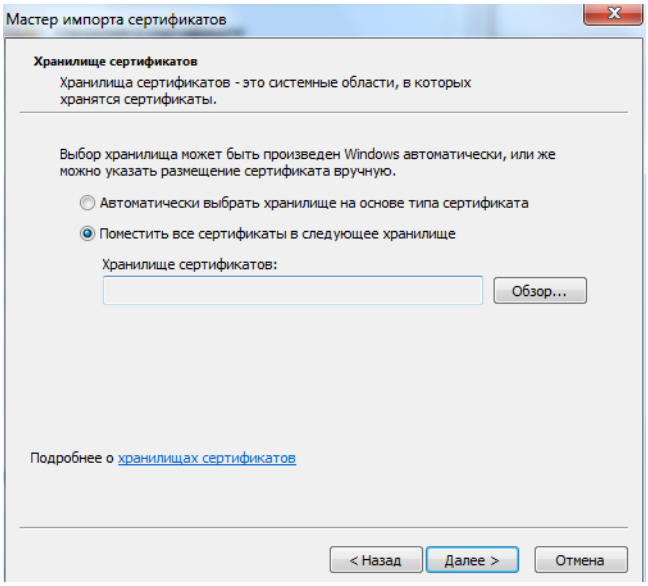

Рисунок 25 – Мастер импорта сертификатов – выбор хранилища сертификатов

В открывшемся окне необходимо выбрать пункт «Доверенные корневые центры сертификации» и нажать кнопку «ОК».

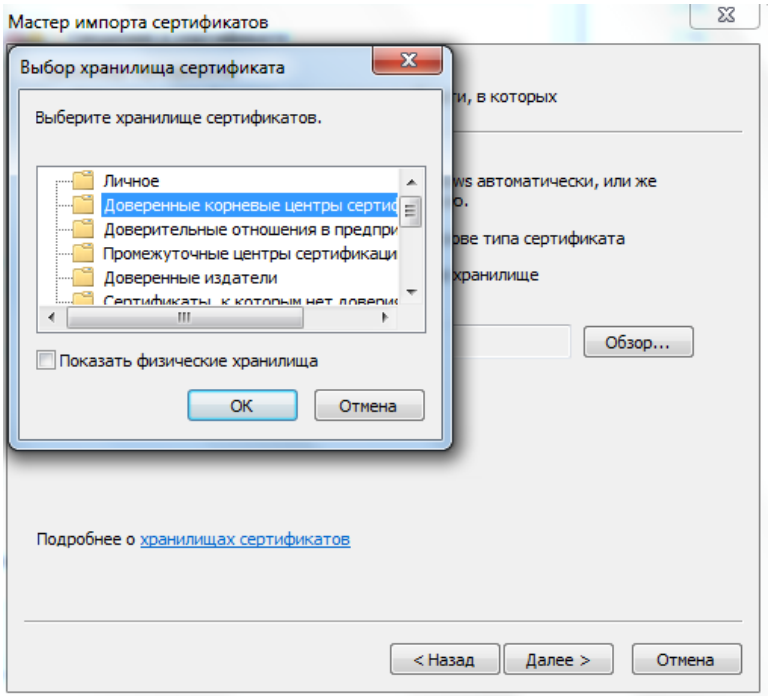

Рисунок 26 – Мастера импорта сертификатов «Доверенные корневые центры сертифкации»

В появившемся окне необходимо нажать кнопку «Далее».

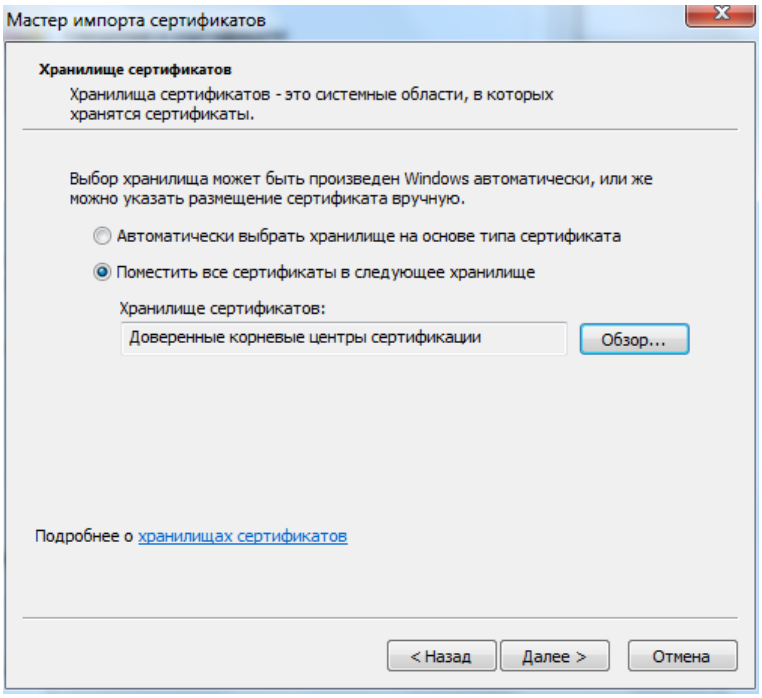

Рисунок 27 – Мастер импорта сертификатов «Доверенные корневые центры сертифкации»

В появившемся окне необходимо нажать кнопку «Далее».

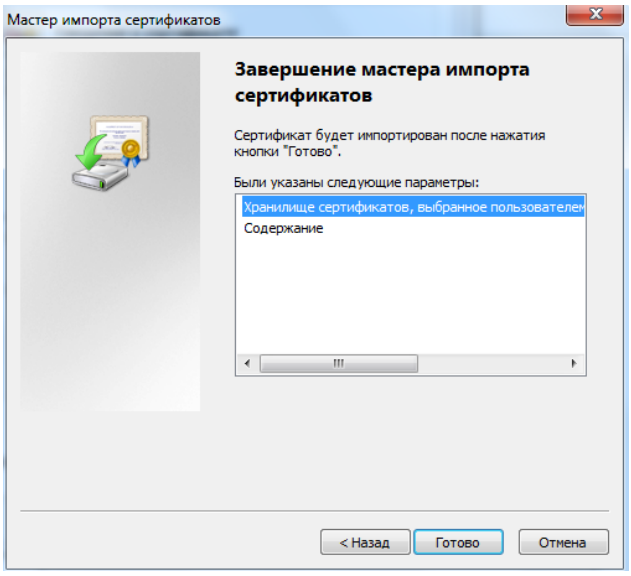

Рисунок 28 – Мастер импорта сертификатов – Завершение мастера импорта сертифкатов

В появившемся окне необходимо нажать кнопку «Готово», после чего должно появиться сообщение, в котором необходимо нажать кнопку «Да». При успешном импорте сертификата появится окно, в котором необходимо нажать кнопку «ОК».

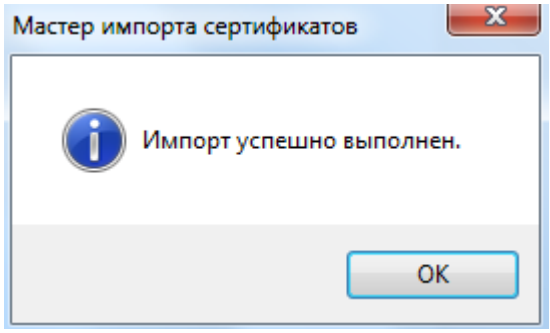

Рисунок 29 – Сообщение об успешном импорте сертифката

3.6 Описание и устранение возможных ошибок при подключении к АСОИ ФинЦЕРТ

При установке защищенного соединения при помощи TLS-клиента могут появляться следующие ошибки:

- Не работает подключение TLS клиента через прокси сервер.

- Не осуществляется регистрация ПО

При появлении данных ошибок необходимо:

- убедиться, что используется версия TLS-клиента не ниже 2.0.0.1151;
- отключить в настройках антивируса контроль порта 443\tcp;
- установить СКЗИ Крипто ПРО CSP 4.0 и проверить работоспособность соединения в браузере Internet Explorer;
- в случае возникновения ошибки подключения повторить процедуру установку TLS-клиента в соответствии с п. 1.3 Приложения 1 к настоящему Руководству.

В случае повторного возникновения ошибок необходимо подготовьте максимально возможное описание (версия ОС, версия браузера, версия СКЗИ, описание ошибки, снимки экрана, на которых видна ошибка) и направьте на адрес электронной почты svc_fincert_support@cbr.ru.

4 Первый вход в АСОИ ФинЦЕРТ

Доступ к личному кабинету Участника осуществляется путем перехода с информационного портала АСОИ ФинЦЕРТ, доступного по адресу https://portal.fincert.cbr.ru .

При первом входе в ЛК пользователь Участника должен:

1 сменить пароль для входа в АСОИ ФинЦЕРТ:

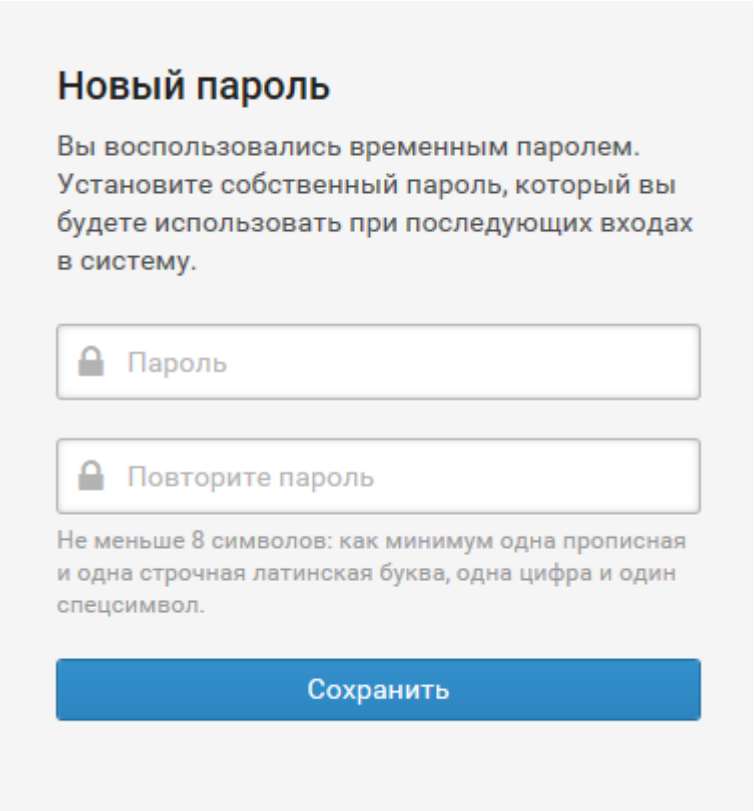

Рисунок 30 – Окно смены пароля первого входа

2 пользователь с правами «Ответственный УИО»:

- проверить и при необходимости уточнить данные в карточке Участника, сформировать запрос на их изменение в случае необходимости;
- сформировать запрос на создание новых пользователей Участника (Пользователей УИО).
- начать работу в соответствии с документом «Руководство Участника по работе с АСОИ ФинЦЕРТ»;

3 пользователь с правами «Пользователь УИО»:

- начать работу в соответствии с документом «Руководство Участника по работе с АСОИ ФинЦЕРТ».

5 Подключение нового пользователя зарегистрированного Участника

Для подключения нового пользователя зарегистрированного Участника необходимо:

- скачать актуальную версию документа «Руководство Участника по работе с АСОИ ФинЦЕРТ» и комплекта программного обеспечения с сайта https://portal.fincert.cbr.ru;
- пользователю с правами «Ответственный УИО» войти в АСОИ ФинЦЕРТ и сделать запрос на добавление нового пользователя участника в соответствии с документом «Руководство Участника по работе с АСОИ ФинЦЕРТ»;
- получить уведомление о создании новой учетной записи пользователя участника;
- осуществить установку необходимо ПО на АРМ пользователя.

6 Перечень типовых ошибок при подключении и способы их решения

6.1 Ошибки при подключении к АСОИ ФинЦЕРТ

П р и м е ч а н и е. Если на компьютере установлено несколько криптопровайдеров, то стабильное подключение к порталам не гарантируется.

АСОИ ФинЦЕРТ поддерживает следующие криптопровайдеры:

- VipNet CSP не ниже версии 4.2.10.51612 beta (не сертифицированная версия);
- КриптоПро CSP не ниже версии 4.0.9944 (R3 - сертифицированная версия);
- Код безопасности CSP (в составе Континент TLS-клиента). Криптопровайдер Код безопасности CSP обеспечивает работу только Континент TLS-клиента.

Работа с АСОИ ФинЦЕРТ с использованием других криптопровайдеров не поддерживается.

6.2 Ошибки при регистрации Континент TLS Клиента

В исключениях прокси-сервера должен быть добавлен адрес регистрации registration.securitycode.ru

Перечень принятых сокращений

Сокращение	Полное наименование
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
АСОИ	Автоматизированная система обработки инцидентов
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
Центр, ФинЦЕРТ	Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России.
УИО	Участник информационного обмена
ФСБ России	Федеральная служба безопасности Российской Федерации

Перечень принятых терминов

Сокращение	Полное наименование
Информационный обмен	Обмен информацией о компьютерных атаках между Участниками и Центром с целью предупреждения, выявления и создания условий для пресечения правонарушений на финансовом рынке Российской Федерации, в национальной платежной системе и повышение уровня информационной безопасности
Участник	1 Поднадзорная Центральному банку Российской Федерации организация: - кредитные организации; - профессиональные участники рынка ценных бумаг; - микрофинансовые организации; - кредитные потребительские кооперативы; - страховые организации; - страховые брокеры; - общества взаимного страхования; - организаторы торговли; - клиринговые организации; - негосударственные пенсионные фонды; - управляющие компании инвестиционного фонда; - управляющие компании паевого инвестиционного фонда; - управляющие компании негосударственного пенсионного фонда; - специализированные депозитарии инвестиционного фонда; - специализированные депозитарии паевого инвестиционного фонда; - специализированные депозитарии негосударственного пенсионного фонда; - ломбарды.

Сокращение	Полное наименование
	2 Не поднадзорная Центральному банку Российской Федерации организация - юридическое лицо, подписавшее соглашение о взаимодействии с Центральным банком Российской Федерации по вопросам противодействия компьютерным атакам