

# ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ (БАНК РОССИИ)

УТВЕРЖДЕН

БКМД.62.01.12.545 – ЛУ

## АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБРАБОТКИ ИНЦИДЕНТОВ ФИНЦЕРТ БАНКА РОССИИ

### РУКОВОДСТВО УЧАСТНИКА ПО РАБОТЕ С АСОИ ФИНЦЕРТ

БКМД.62.01.12.545.ИЗ.3

На 120 листах

|               |                |
|---------------|----------------|
| Инов. № подл. | Подпись дата   |
| Взам. инв. №  | Инов. № дубл.  |
| Подпись дата  | Подпись и дата |

2023

### Аннотация

Настоящий документ содержит руководство участника автоматизированной системы обработки инцидентов ФинЦЕРТ Банка России.

Документ разработан в соответствии с ГОСТ 2.105-95 «ЕСКД. Общие требования к текстовым документам».

Данный документ разработан в рамках Договора № ДН3794 от 08.12.2017 г.

Документ доработан в рамках Договора № ДН4181 от 25.12.2018 г.

## Содержание

|        |  |    |
|--------|--|----|
| 1      | Введение.....  | 5  |
| 1.1    | Краткое описание возможностей .....  | 5  |
| 2      | Работа с Личным кабинетом Участника.....   | 7  |
| 2.1    | Первый вход и смена пароля .....   | 7  |
| 2.2    | Работа с меню «Запросы» .....  | 10 |
| 2.3    | Работа с меню «Рассылки центра».....   | 12 |
| 2.4    | Работа с меню «Ваша организация» .....   | 13 |
| 2.5    | Работа с меню «Фиды».....  | 18 |
| 2.6    | Меню «Новый запрос» .....  | 18 |
| 2.6.1  | Создание запроса об инциденте.....   | 20 |
| 2.6.2  | Создание запроса об инциденте с использованием готовых карточек в форматах JSON..... | 22 |
| 2.6.3  | Создание запроса об изменении карточки участника .....                               | 26 |
| 2.6.4  | Создание запроса об угрозе.....  | 31 |
| 2.6.5  | Создание запроса об уязвимости .....   | 34 |
| 2.6.6  | Создание запроса о публикации .....  | 38 |
| 2.6.7  | Регистрация запроса о блокировке корреспондентского счета .....                      | 41 |
| 2.6.8  | Регистрация диспутного запроса .....   | 43 |
| 2.6.9  | Регистрация запроса на анализ ВПО .....  | 44 |
| 2.6.10 | Создание произвольных запросов .....   | 45 |
| 2.6.11 | Электронная форма инцидента .....  | 46 |
| 2.7    | Работа с меню «Управление сертификатом» .....  | 68 |
| 3      | Отправка форм обмена информацией через E-mail.....                                   | 70 |
| 4      | Автоматизированная отправка инцидентов SIEM в АСОИ ФинЦЕРТ .....                     | 71 |
| 4.1    | Вход в "Пользовательский компонент" .....  | 72 |
| 4.2    | Интерфейс.....   | 72 |
| 4.3    | Работа с инцидентами .....   | 73 |
| 4.3.1  | Отправка инцидента.....  | 74 |
| 4.3.2  | Изменение параметров инцидента .....   | 74 |
| 4.3.3  | Скачивание электронной формы инцидента .....   | 75 |
| 4.3.4  | Удаление инцидента .....   | 75 |
| 4.4    | Трансформация инцидентов. Правила трансформации.....                                 | 75 |

|       |   |     |
|-------|---|-----|
| 4.5   | Добавление правила трансформации.....   | 77  |
| 5     | Ошибки .....  | 80  |
| 5.1   | Не открываются страницы приложений АСОИ ФинЦЕРТ .....   | 80  |
| 5.2   | Ошибки в работе веб-интерфейсов приложений АСОИ ФинЦЕРТ .....   | 80  |
| 5.3   | Прочие ошибки и вопросы.....  | 80  |
|       | Приложение А Установка и настройка ПО.....  | 82  |
| A.1   | Общие сведения .....  | 82  |
| A.2   | Требования к АРМ.....   | 82  |
| A.3   | Требования к подключению .....  | 84  |
| A.4   | Установка и настройка TLS-клиента .....   | 84  |
| A.5   | Создание запроса для сертификата Клиента TLS.....   | 95  |
| A.6   | Установка сертификата корневого Центра сертификации .....   | 98  |
| A.7   | Установка сертификата промежуточного Центра сертификации.....   | 103 |
| A.8   | Установка сертификата пользователя Участника.....   | 103 |
| A.9   | Установка сертификата веб-ресурсов АСОИ ФинЦЕРТ .....   | 105 |
| A.10  | Загрузка списков отозванных сертификатов.....   | 106 |
|       | Приложение Б Формат описания правил трансформации .....   | 108 |
|       | Приложение В Описание программного прикладного интерфейса (REST API) работы с<br>электронной подписью ..... | 114 |
| V.1   | Работа с электронной подписью.....  | 114 |
| V.1.1 | Подпись электронной формы.....  | 114 |
| V.1.2 | Проверка подписи электронной формы .....  | 115 |
|       | Приложение Г Типовая форма направления информации об ошибке/сбое/проблеме АСОИ<br>ФинЦЕРТ .....             | 117 |
|       | Перечень принятых сокращений.....   | 119 |

## **1 Введение**

### **1.1 Краткое описание возможностей**

Автоматизированная система обработки инцидентов ФинЦЕРТ Банка России (далее — АСОИ ФинЦЕРТ) предназначена для поддержки бизнес-процессов ФинЦЕРТ и организации непрерывного информационного взаимодействия между ФинЦЕРТ и Участниками информационного обмена (далее — Участник) по вопросам нарушения информационной безопасности.

АСОИ ФинЦЕРТ обеспечивает:

- взаимодействие между ФинЦЕРТ и Участниками в части информирования и реагирования на угрозы и инциденты информационной безопасности;
- повышение уровня информированности Участников об актуальных угрозах информационной безопасности.

АСОИ ФинЦЕРТ обеспечивает взаимодействие между ФинЦЕРТ и Участником в части формирования и реагирования на угрозы и инциденты информационной безопасности.

Обмен информацией между ФинЦЕРТ и Участником осуществляется следующими способами:

- через сообщения в личном кабинете (ЛК), Участник может направить в ФинЦЕРТ сообщение об инциденте, угрозе, уязвимости, публикации, сообщение в сводной форме, или изменении данных в карточке участника, приложив к сообщению соответствующую электронную форму и/или файл. При поступлении первого сообщения от Участника через личный кабинет Участника ФинЦЕРТ формирует запрос. Все последующие сообщения, связанные с исходным, от Участника и ФинЦЕРТ автоматически попадают в этот же запрос. ФинЦЕРТ получает сообщение от Участника, при необходимости формирует рекомендации для противодействия, и направляет их Участнику. Кроме того, Участник может получать бюллетени для своей отрасли, содержащие информацию о наличии или устранении уязвимостей в программном или аппаратном обеспечении (см. п. 2).

- через прикладной программный интерфейс (API) в формате JSON (см. документ «Справочное руководство по REST API»);

Формы обмена информацией в формат JSON можно также отправлять через личный кабинет в виде вложений к сообщениям.

Порядок установки и настройки программного обеспечения, необходимого для работы с АСОИ ФинЦЕРТ, приведен в приложении (Приложение А).

Для организации доступа в Личный кабинет Участника Участнику необходимо реализовать мероприятия, указанные в документах «Регламент подключения участников информационного обмена к АСОИ ФинЦЕРТ» и «Регламент получения ключевой информации».

Более подробно работа с компонентом ФинЦЕРТ: "Личный кабинет Участника" изложена в документе «Руководство участника (Личный кабинет участника)».

## **2 Работа с Личным кабинетом Участника**

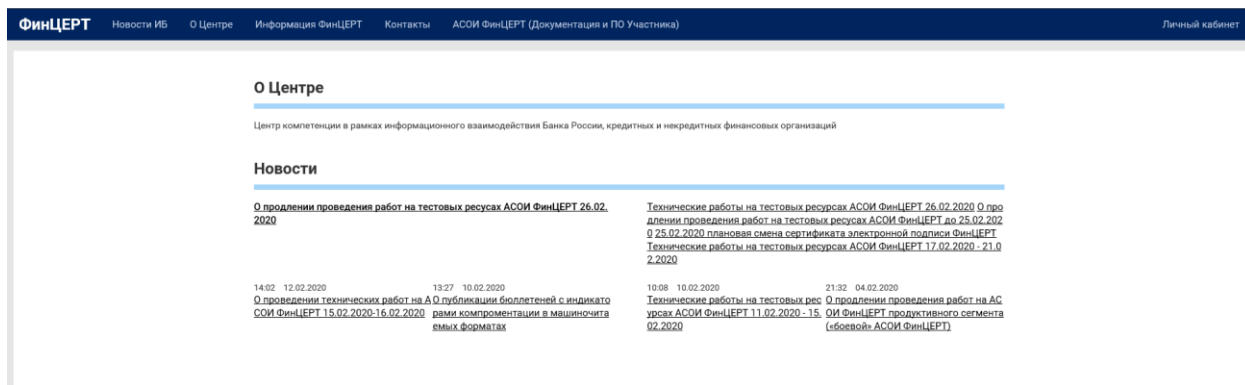
В настоящем разделе рассматривается работа с графическим интерфейсом Личного кабинета Участника АСОИ ФинЦЕРТ. Работа с программным интерфейсом (API) Личного кабинета Участника описана в документ «Справочное руководство по REST API».

Для доступа к АСОИ ФинЦЕРТ необходимо:

- При работе с Континент TLS-клиент:
  - а) запустить Континент TLS-клиент;
  - б) запустить один из поддерживаемых АСОИ ФинЦЕРТ обозревателей:
    - 1) Microsoft Edge;
    - 2) Google Chrome версии не ниже 60;
    - 3) Яндекс.Браузер версии не ниже 22;
    - 4) Опера версии не ниже 83;
    - 5) Chromium-Gost версии не ниже 99.
- При работе с КриптоПро CSP:
  - а) запустить один из поддерживаемых АСОИ ФинЦЕРТ обозревателей:
    - 1) Microsoft Edge;
    - 2) Яндекс.Браузер версии не ниже 22;
    - 3) Опера версии не ниже 83;
    - 4) Chromium-Gost версии не ниже 99 (при использовании КриптоПро CSP 4.0 рекомендуется перейти на КриптоПро CSP 5.0).

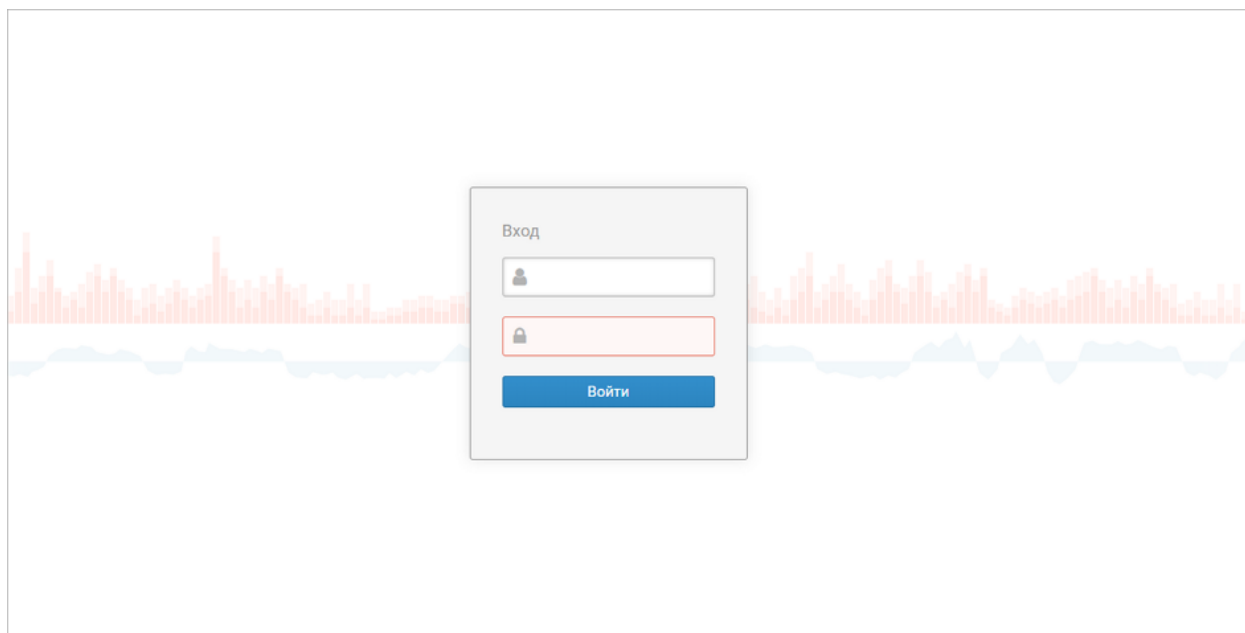
### **2.1 Первый вход и смена пароля**

Для входа в личный кабинет в адресной строке браузера введите адрес:  
<https://portal.fincert.cbr.ru> (Рисунок 1).



**Рисунок 1 – Стартовая страница портала**

В правом верхнем углу страницы нажмите кнопку «Личный кабинет». Откроется страница входа в ФинЦЕРТ (Рисунок 2).

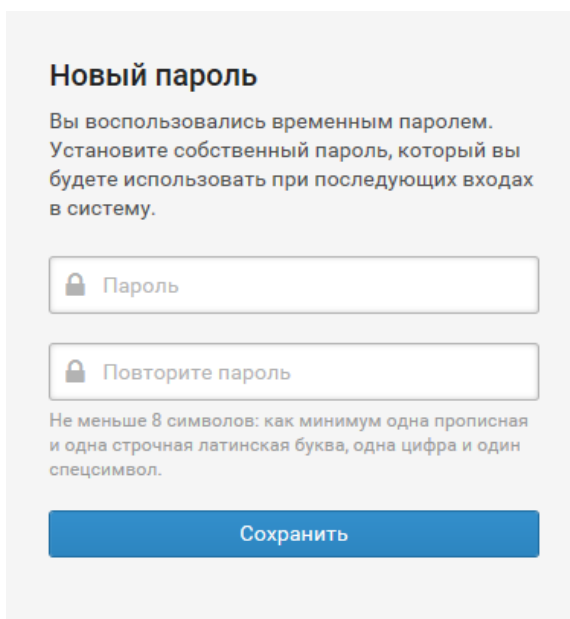


**Рисунок 2 – Вход в личный кабинет Участника**

- 1) В поле Логин введите логин учетной записи.
- 2) В поле Пароль введите пароль вашей учетной записи.
- 3) Нажмите кнопку «Войти».

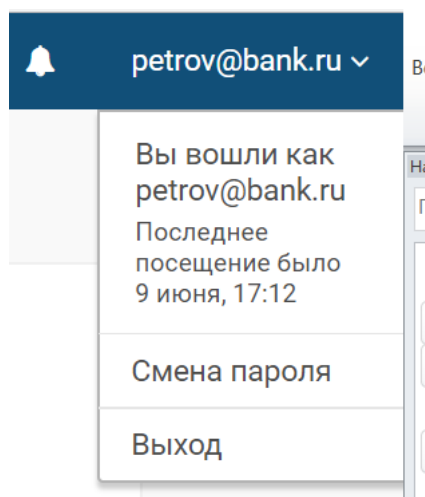
АСОИ ФинЦЕРТ проверяет введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница. Если вы указали неверные данные, отобразится сообщение об ошибке.

При первом входе АСОИ ФинЦЕРТ предложит сменить пароль первого входа (Рисунок 3):



**Рисунок 3 – Окно смены пароля первого входа**

Для смены пароля зайдите на страницу «Смена пароля». Для этого нажмите на иконку в левом верхнем углу, выберите пункт меню «Смена пароля» (Рисунок 4).



**Рисунок 4 – Переход в личный кабинет**

Заполните поля со старым, новым паролем и его подтверждение (Рисунок 5). Нажмите кнопку «Сохранить». Пароль будет изменен.

**Смена пароля**

Текущий пароль

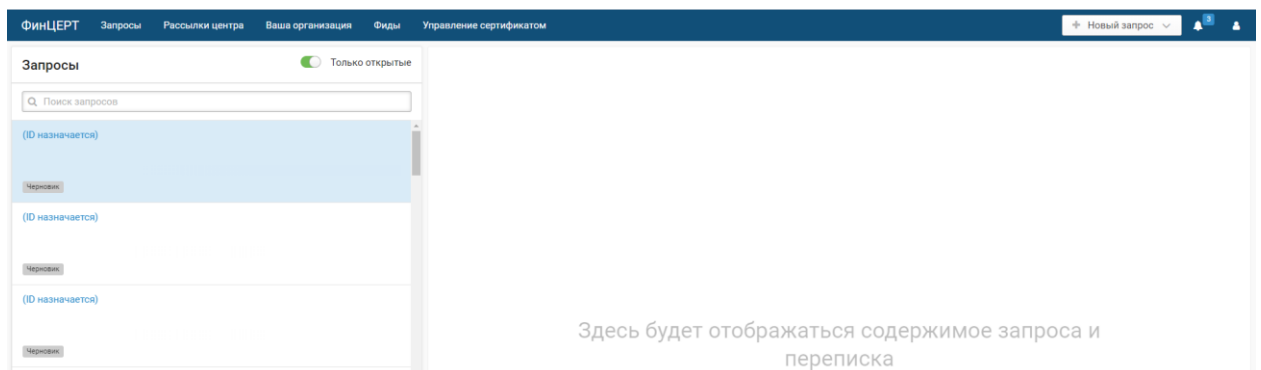
Новый пароль   
Не меньше 8 символов: как минимум одна прописная и одна строчная латинская буква, одна цифра и один спецсимвол.

Повторите новый пароль   
Не меньше 8 символов: как минимум одна прописная и одна строчная латинская буква, одна цифра и один спецсимвол.

**Рисунок 5 – Изменение пароля**

После удачной смены пароля откроется стартовая страница. В открывшемся интерфейсе (Рисунок 6) доступны следующие пункты меню:

- 1) «Запросы»;
- 2) «Рассылки центра»;
- 3) «Ваша организация»;
- 4) «Зарегистрировать запрос».

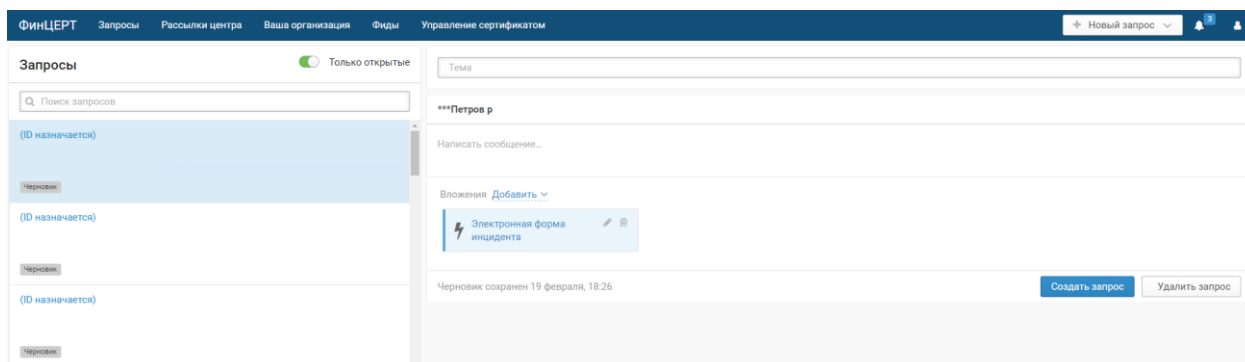


**Рисунок 6 – Интерфейс ЛК Участника**

## 2.2 Работа с меню «Запросы»

Информация о запросах отображается на странице «Запросы».

В открывшейся форме отобразится содержимое запросов (Рисунок 7).



**Рисунок 7 – Информация по запросам**

Рабочая область страницы содержит список запросов. По умолчанию список содержит только открытые запросы и черновики запросов, отсортированные по дате и времени получения запроса (от новых к старым). Вы можете включить отображение закрытых запросов (Рисунок 8).

Запросы Только открытые

**Рисунок 8 – Просмотр только открытых запросов**

Воспользуйтесь строкой поиска, расположенной над списком запросов, чтобы найти интересующий вас запрос. В строке нужно указать идентификатор запроса, его тему или описание (Рисунок 9).

Поиск запросов

**Рисунок 9 – Строка поиска запроса**

Для отображения оставшейся части запросов внизу списка есть кнопка «Загрузить следующие... (всего...)» с указанием общего количества запросов участника (Рисунок 10).

Загрузить следующие 596 (всего - 646)

**Рисунок 10 – Кнопка дозагрузки запросов в списке запросов**

В правой части рабочей области на вкладке «Параметры запроса» отображается основная информация по запросу:

- 1) Статус. Предназначен для отслеживания состояния обработки запроса. В ФинЦЕРТ существуют следующие статусы запроса:
  - а) Открытый — запрос только поступил в ФинЦЕРТ.
  - б) В работе — ведется работа по запросу.
  - в) Ожидает закрытия — ожидается подтверждение от Участника о закрытии запроса.
  - г) Закрыт — запрос успешно обработан и помещен в архив.
  - д) Отклонен — запрос неактуален и отклонен.
- 2) Ожидаемое время ответа. Время реакции на ваше обращение с момента получения от вас запроса до ответа оператора ФинЦЕРТ с описанием дальнейших шагов по решению вашего обращения. Время реакции зависит от приоритета запроса.
- 3) Идентификатор запроса. Идентификатор запроса формируется автоматически.
- 4) Способ получения. Способ отправки запроса.
- 5) Последнее обновление. Дата и время последнего изменения запроса.

На вкладке Переписка отображается вся переписка с ФинЦЕРТ. Вы можете отправить оператору ФинЦЕРТ сообщение и вложить в сообщение файл.

## **2.3 Работа с меню «Рассылки центра»**

Для работы необходимо выполнить переход на вкладку «Рассылки центра».

В открывшейся форме отобразится перечень фильтров, позволяющих упорядочивать содержимое раздела по следующим категориям (Рисунок 11):

- Бюллетени
- Новости
- Уведомления

| ФинЦЕРТ    Запросы    Рассылки центра    Ваша организация    Фиды    Управление сертификатом |                  |                     |                     |              |                 |                         |
|--|------------------|---------------------|---------------------|--------------|-----------------|-------------------------|
| Все<br>Бюллетени<br>Новости<br>Уведомления   | Рассылки центра  |                     |                     |              |                 | FinCERT-2019101-01      |
|  | Опубликован      | Идентификатор       | Заголовок           | Тип рассылки | Подтип рассылки | Краткое описание        |
|  | 22 октября, 2019 | FinCERT-20191022-01 | Тестовый 22.10      | Бюллетень    | Другое          | Тестовый 22.10          |
|  | 22 октября, 2019 | Проверка 2.x        | Проверка 2.x        | Бюллетень    | Другое          | Проверка 2.x            |
|  | 9 октября, 2019  | FinCERT-20191010-01 | FinCERT-2019101-01  | Бюллетень    | Другое          | FinCERT-20191010-01     |
|  | 19 августа, 2019 | FinCERT-20190819-01 | FinCERT-20190819-01 | Бюллетень    | Другое          | FinCERT-20190819-01     |
|  | 6 августа, 2019  | FinCERT-20190806-01 | FinCERT-20190806-01 | Бюллетень    | Другое          | FinCERT-20190802-01 ... |
|  | 2 августа, 2019  | FinCERT-20190802-01 | FinCERT-20190802-01 | Бюллетень    | Другое          | FinCERT-20190802-01 ... |
|  | 26 декабря, 2018 | 26122018-02         | 26122018-02         | Бюллетень    | Другое          | 26122018-02             |
|  | 26 декабря, 2018 | 26122018-01         | 26122018-01         | Бюллетень    | Другое          | 26122018-01             |

Рисунок 11 – Раздел рассылок центра

Информация по каждому из элементов рассылки включает:

- дату опубликования;
- идентификатор;
- заголовок;
- краткое описание;
- тип и подтип рассылки, ее наименование.

Вы можете сортировать значения в столбцах таблицы, нажав на заголовок столбца. Вы можете воспользоваться строкой поиска, расположенной над таблицей бюллетеней, чтобы найти интересующий вас бюллетень. В строке нужно указать идентификатор бюллетеня, его заголовок, описание или имя вложенного файла.

В правой части рабочей области отображается карточка выбранного в таблице бюллетеня. В карточке отображаются основные параметры бюллетеня и ссылка на его скачивание.

## 2.4 Работа с меню «Ваша организация»

Для работы необходимо выполнить переход на вкладку «Ваша организация» (Рисунок 12).

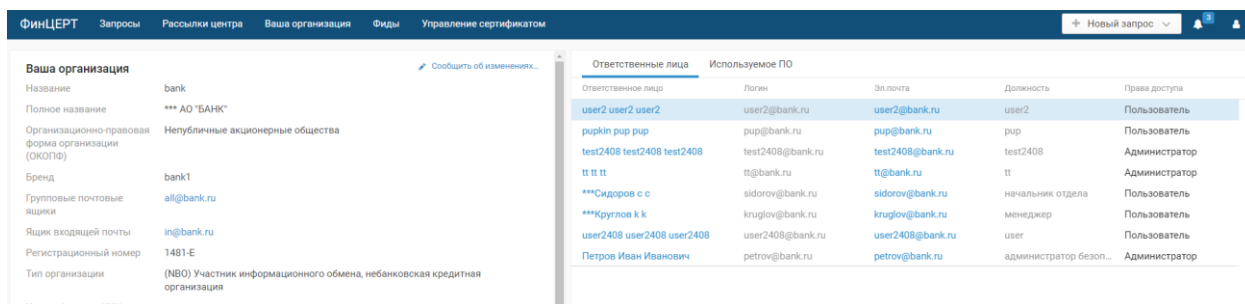


Рисунок 12 – Вкладка «Ваша организация»

Страница «Ваша организация» состоит из двух панелей — информационной и дополнительной.

Информационная панель содержит данные об организации (Рисунок 13):

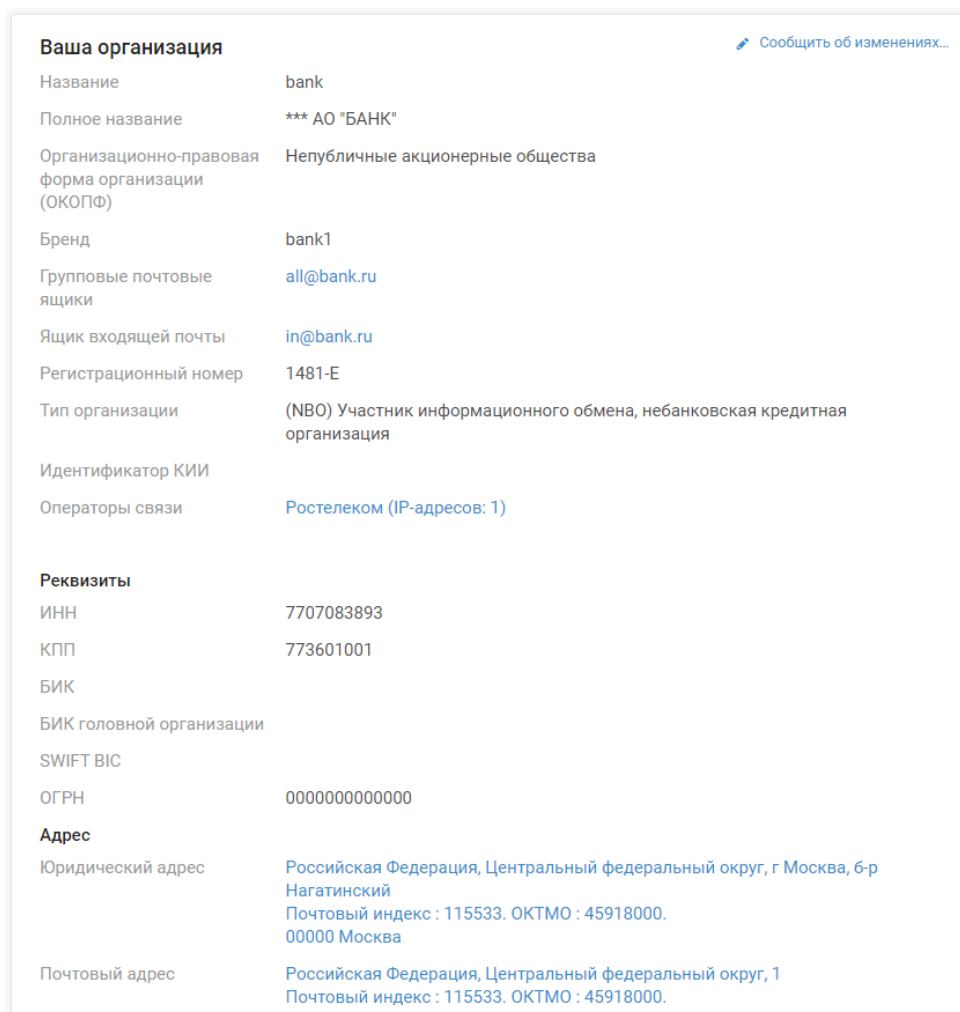


Рисунок 13 – Информационная панель вкладки «Ваша организация»

- Название — краткое название организации;
- Полное название — полное название организации;
- Организационно-правовая форма организации (ОКОПФ) — код ОКОПФ ;
- Бренд — название, под которым также известна организация;
- Групповые почтовые ящики — адреса электронной почты отделов ИБ организации;
- Ящики входящей почты — адреса электронной почты, на которые участнику приходят сообщения, уведомления и бюллетени от "ФинЦЕРТ";
- Регистрационный номер – номер кредитной организации;
- Тип организации;
- Идентификатор КИИ — идентификатор объекта критической информационной инфраструктуры;
- Операторы связи — организации, предоставляющие услуги доступа к интернету;
- Реквизиты;
- Адрес – содержит указание юридического, почтового и фактического адресов организации;
- Дополнительно – содержит информацию о SWIFT-BIK, Acquirer Id, ID в платежной системе (при наличии);
- БИН эмитента
- Тип используемой криптографии – тип используемой криптографии при ведении информационного обмена с ФинЦЕРТ. Возможны варианты GPG и ГОСТ. По умолчанию выставляется ГОСТ.
- Автоматически отправлять инциденты в ГосСОПКА – признак автоматической отправки инцидентов от Участника в ГосСОПКА. Выставляется оператором ФинЦЕРТ.

В панели, содержащей дополнительную информацию, отображается краткая информация об ответственных лицах участника и используемом программном обеспечении.

Полная информация об ответственном лице отображается в карточке ответственного лица (Рисунок 14).

**Петров Иван Иванович**

Активирован

×

|                                   |                                      |
|-----------------------------------|--------------------------------------|
| Идентификатор в ФинЦЕРТ           | 40c91d00-67db-4f8a-b542-2002e60f953a |
| Идентификатор в системе участника | 40c91d00-67db-4f8a-b542-2002e60f953a |
| Должность                         | администратор безопасности           |
| Категория                         | Безопасность                         |
| Логин                             | petrov@bank.ru                       |
| Пароль первого входа              | TJBVGW                               |
| Права доступа                     | Администратор                        |
| Доступ в личный кабинет           | Активирован                          |

**Контакты**

|                   |  |
|-------------------|--|
| Эл.почта          | <a href="mailto:petrov@bank.ru">petrov@bank.ru</a> |
| Городской телефон | 0  |
| Мобильный телефон | 0  |

**Сертификат пользователя**

|                  |  |
|------------------|--|
| Версия           |  |
| Серийный номер   |  |
| Алгоритм подписи |  |
| Поставщик        |  |
| Действителен с   |  |
| Действителен до  |  |
| Субъект          |  |
| Открытый ключ    |  |

**Рисунок 14 – Карточка ответственного лица организации**

Вы можете изменять параметры ответственного лица или заблокировать его. Удалить ответственного лица из системы нельзя. Вы можете отправлять учетные данные ответственному лицу на адрес электронной почты, который указан в карточке.

Вкладка «Используемое ПО» содержит таблицу программного обеспечения участника.

Вы можете отправить запрос на изменение данных организации. Для этого нажмите кнопку «Сообщить об изменениях» и в открывшейся электронной форме участника внесите изменения в соответствующее поле. Возможно внесение изменений в три вкладки: «Параметры участника», «Ответственные лица», «Используемое ПО» (Рисунок 15).

The screenshot shows a web application window titled "Электронная форма участника" (Electronic form of participant). It has three tabs: "Параметры участника" (Participant parameters), "Ответственные лица" (Responsible persons), and "Используемое ПО" (Software used). The "Параметры участника" tab is active. Under the heading "Общие сведения" (General information), there are several input fields and dropdown menus:

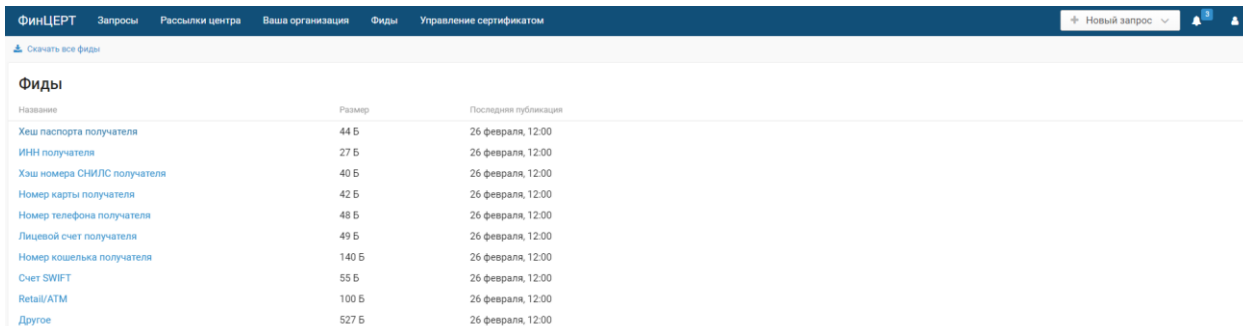
- Тип организации** (Organization type): A dropdown menu with the selected value "(NBO) Участник информационного обмена, небанковская кр..." (NBO Participant of information exchange, non-bank credit...).
- Название** (Name): An input field with the value "bank". Below it, the text "Необязательно" (Optional) is displayed.
- Полное название** (Full name): An input field with the value "\*\*\* АО 'БАНК'" (\*\*\* JSC 'BANK').
- Организационно-правовая форма организации (ОКОПФ)** (Organizational and legal form of the organization (OKOPF)): A dropdown menu with the selected value "Непубличные акционерные общества" (Non-public joint-stock companies).
- Бренд** (Brand): An input field with the value "bank1". Below it, the text "Необязательно" (Optional) is displayed, followed by a description: "Краткое название, под которым также известна компания. Например, для Вымпелком – Билайн" (Short name, under which the company is also known. For example, for Vimpelcom – Beeline).
- Групповые почтовые ящики** (Group mailboxes): An input field with the value "all@bank.ru" and a small 'x' icon. Below it, the text "Адреса эл. почты отделов ИБ участника" (Email addresses of the participant's IT departments) is displayed.
- Ящик входящей почты** (Incoming mailbox): An input field with the value "in@bank.ru" and a small icon. Below it, the text "Адрес эл. почты для получения сообщений, запросов и рассылок от 'ФинЦЕРТ'" (Email address for receiving messages, requests and newsletters from 'FinCERT') is displayed.
- Регистрационный номер** (Registration number): An input field with the value "1481-E". Below it, the text "Номер лицензии выданной Банком России" (License number issued by the Bank of Russia) is displayed.
- Идентификатор КИИ** (KIIC identifier): An empty input field. Below it, the text "Необязательно" (Optional) is displayed.
- Операторы связи** (Communication operators): A section showing "Ростелеком (IP-адресов: 1)" (Rostelecom (IP addresses: 1)) with edit and delete icons. Below it is a link "+ Добавить оператора" (+ Add operator).

At the bottom right of the form, there are two buttons: "Сохранить" (Save) and "Готово" (Done).

Рисунок 15 – Внесение данных в электронную форму участника

## 2.5 Работа с меню «Фиды»

Для работы необходимо выполнить переход на вкладку «Фиды» (Рисунок 16).



| Название                    | Размер | Последняя публикация |
|-----------------------------|--------|----------------------|
| Хеш паспорта получателя     | 44 Б   | 26 февраля, 12:00    |
| ИНН получателя              | 27 Б   | 26 февраля, 12:00    |
| Хэш номера СНИЛС получателя | 40 Б   | 26 февраля, 12:00    |
| Номер карты получателя      | 42 Б   | 26 февраля, 12:00    |
| Номер телефона получателя   | 48 Б   | 26 февраля, 12:00    |
| Лицевой счет получателя     | 49 Б   | 26 февраля, 12:00    |
| Номер кошелька получателя   | 140 Б  | 26 февраля, 12:00    |
| Счет SWIFT                  | 55 Б   | 26 февраля, 12:00    |
| Retail/ATM                  | 100 Б  | 26 февраля, 12:00    |
| Другое                      | 527 Б  | 26 февраля, 12:00    |

**Рисунок 16 – Меню «Фиды»**

Рабочая область страницы «Фиды» содержит следующую информацию о фидах:

- Название – наименование фидов;
- Размер – размер в байтах;
- Последняя публикация – дата и время последней публикации фидов.

Чтобы скачать фиды:

- 1) В главном меню выберите пункт Фиды.
- 2) Откроется страница «Фиды» со списком фидов, доступных для скачивания, и датами последней публикации этих фидов.
- 3) Нажмите название фидов, которые хотите скачать (например, «Номер телефона получателя»).
- 4) В папку для скачивания браузера будет загружен csv-файл с фидами.
- 5) Если необходимо, скачайте zip-архив со всеми последними файлами фидов по кнопке «Скачать все фиды».

Скачивание фидов завершено.

## 2.6 Меню «Новый запрос»

АСОИ ФинЦЕРТ обеспечивает обмен информацией между Центральным банком Российской Федерации и Участниками через сообщения. При поступлении первого сообщения от Участника через личный кабинет Участника ФинЦЕРТ формирует запрос.

Все последующие сообщения, связанные с исходным, автоматически попадают в этот же запрос. Сообщения в запросе могут содержать вложения разных типов:

- файлы, например, скриншоты;
- электронную форму инцидента (векторы INT\EXT);
- электронную форму угрозы;
- электронную форму уязвимости;
- электронную форму публикации;
- электронную форму участника;
- электронную форму запроса на блокировку корреспондентского счета;
- электронную форму диспутного запроса;
- электронную форму запроса на анализ ВПО.

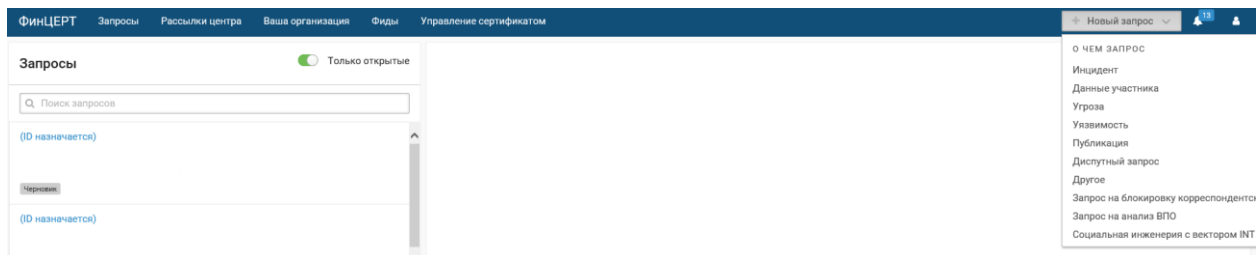
Запрос, формируемый через ЛКУ, может содержать не более десяти электронных форм.

Список запросов отображается на странице «Запросы». Все пользователи Участника могут просматривать все запросы и сообщения в них.

Для удобства поиска запросов в АСОИ ФинЦЕРТ предусмотрено поле поиска.

Работа с запросом ведется в карточке запроса и включает в себя следующие шаги:

- 1) Регистрация запроса.
- 2) Переписка со специалистом Банка России для уточнения информации по запросу.
- 3) Получение рекомендаций по решению запроса от специалиста Банка России.
- 4) Применение рекомендаций, полученных от специалиста Банка России.
- 5) Закрытие запроса.



**Рисунок 17 – Меню «Новый запрос»**

Доступны следующие категории запросов:

- «Инцидент»;
- «Данные участника»;
- «Угроза»;
- «Уязвимость»;
- «Публикация»;
- «Диспутный запрос»;
- «Другое»;
- «Запрос на блокировку корреспондентского счета»;
- «Запрос на анализ ВПО»;
- «Социальная инженерия с вектором INT».

### **2.6.1 Создание запроса об инциденте**

В данном пункте приведена процедура регистрации запроса об инциденте. Детальное описание электронной формы инцидента приведено в п. 2.6.11.

Для регистрации запроса об инциденте:

- В главном меню нажмите кнопку «Новый запрос» и выберите пункт «Инцидент» (Рисунок 17). Откроется окно «Электронная форма инцидента» (Рисунок 18).

Электронная форма инцидента

Общие сведения

Принятые меры

Операции без согласия

Вложения

Итоги

Дополнительно

Подтверждение

Общие сведения

Помощь ФинЦЕРТ

ТребуетсяНе требуется

Описание инцидента

Опишите детали инцидента:  
— что произошло  
— когда, как и с помощью каких средств вы это обнаружили

Тип инцидента

Обнаружен

Географическое местоположение инцидента

Федеральный округ

Субъект федерации

Населенный пункт

Укажите название населенного пункта, в котором произошел инцидент

Локализация инцидента и атакованные сервисы

Подразделение

СохранитьПродолжить

**Рисунок 18 – Создание запроса об инциденте**

- Заполните электронную форму инцидента согласно п. 2.6.11
- Нажмите кнопку «Добавить к запросу».
- Откроется страница «Запросы».
- Добавьте сообщение, сопровождающее запрос.
- Нажмите кнопку «Создать запрос».
- Откроется окно «Добавить цифровую подпись».

- Введите код безопасности, полученный вместе с сертификатом для электронной подписи. Запросить сертификат вы можете самостоятельно на странице «Управление сертификатом» (п. 2.7).

Запрос об инциденте зарегистрирован.

### 2.6.2 Создание запроса об инциденте с использованием готовых карточек в форматах JSON

Для регистрации запроса об инциденте:

- Из списка (Рисунок 17) выберите пункт меню «Другое».
- В появившемся окне нажмите «Вложения» – «Добавить» – «Файл» (Рисунок 19).
- Далее нажмите «Выберите» (или перетащите файл с заполненным инцидентом в формате JSON).



Рисунок 19 – Выбор вложения к запросу

- В открывшемся окне выберите файл и нажмите кнопку «Открыть» (Рисунок 20).

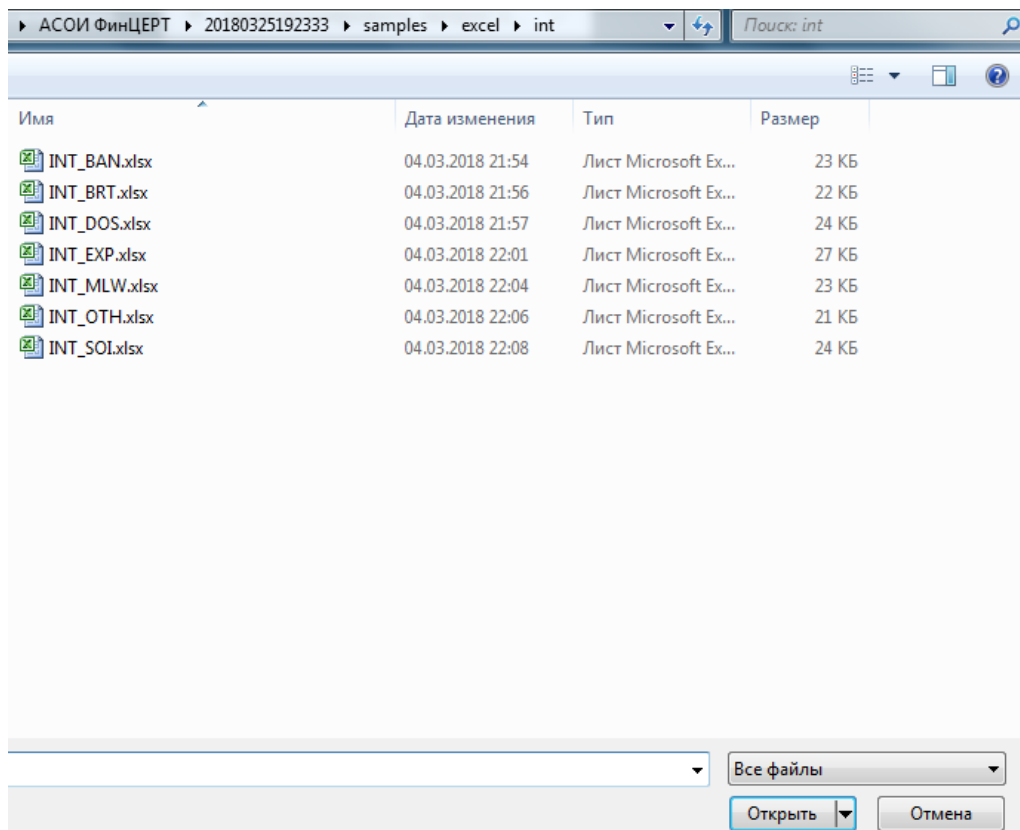
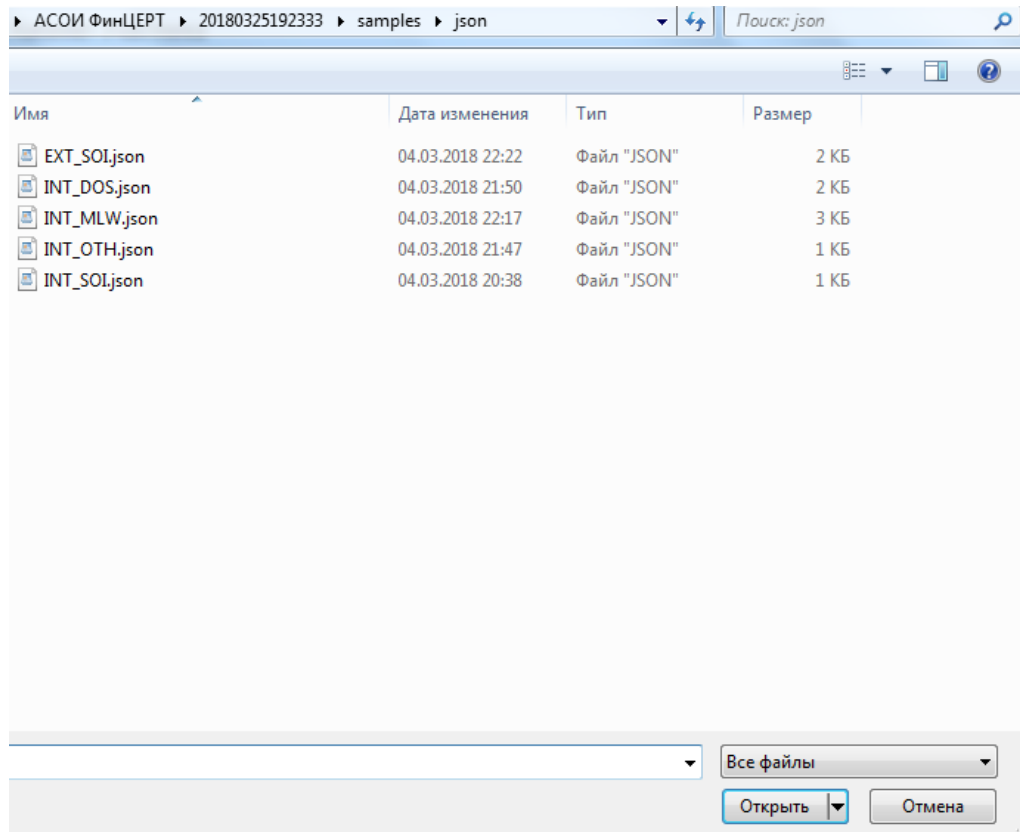
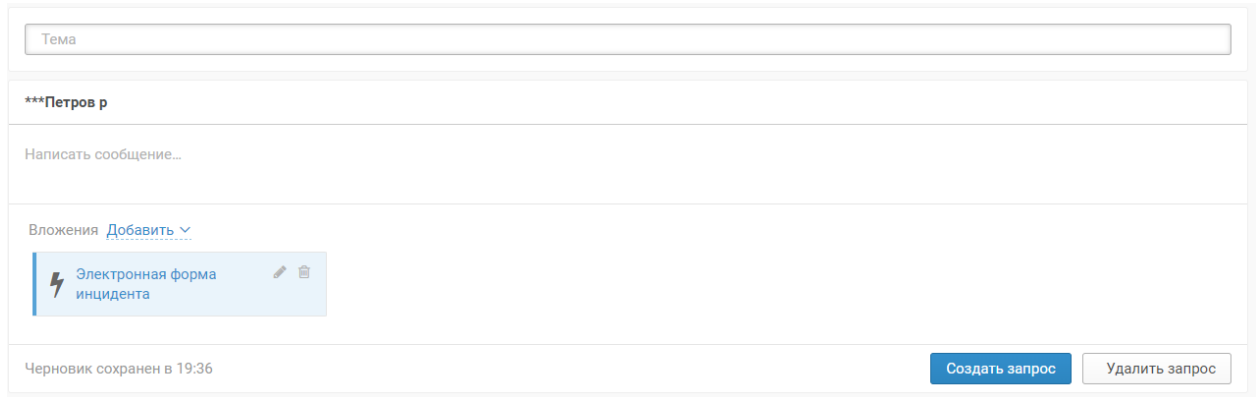


Рисунок 20 – Выбор заполненной карточки инцидента в формате JSON

- После выбора файла в открывшемся окне появится информация о прикрепленном к электронной форме файле, в котором необходимо нажать кнопку «Продолжить» (Рисунок 21).



Тема

\*\*\*Петров р

Написать сообщение...

Вложения [Добавить](#) ▾

Электронная форма инцидента

Черновик сохранен в 19:36

Создать запрос

Удалить запрос

**Рисунок 21 – Карточка инцидента в формате JSON, прикрепленная к запросу**

В форме запроса можно нажать на панель «Электронная форма инцидента» и просмотреть содержание карточки инцидента и приложенного файла в формате JSON (Рисунок 22).

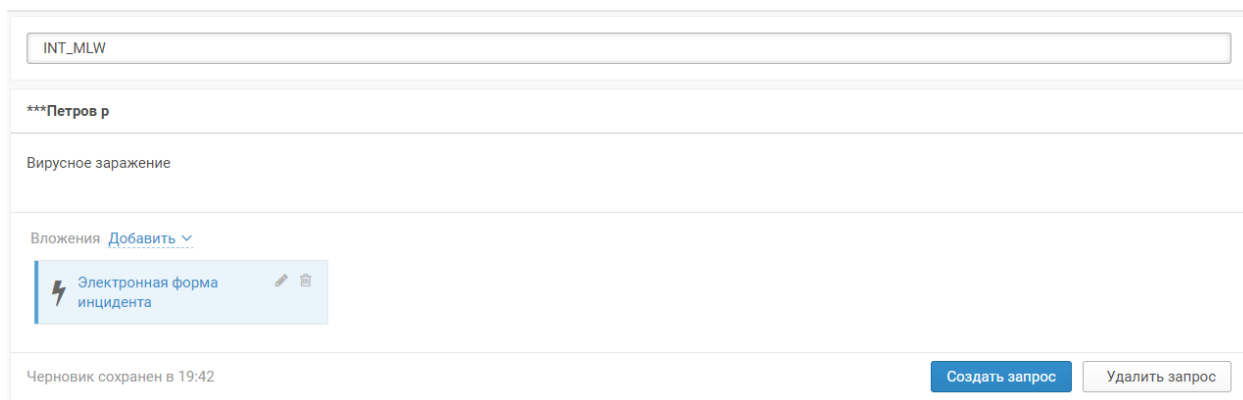
Электронная форма инцидента (v.1) ×

|                            |  |  |
|----------------------------|--|--|
| <b>Общие сведения</b>      | <b>Общие сведения</b>                              |  |
| Описание                   | Помощь   | — Не запрашивалась   |
| Вектор инцидента — INT     | Тип инцидента                                      | Использование вредоносного программного обеспечения (malware), Внутренний вектор (INT) |
| Принятые меры              |  |  |
| Операции без согласия      | <b>Обнаружение</b>                                 |  |
| Вложения                   | Выявлен у участника                                | 13 ноября 2019, 00:00  |
| Итоги                      | Зарегистрирован                                    |  |
| <b>Тип инцидента</b>       | Изменен  | 0 секунд назад   |
| 0.0.0.0                    |  |  |
| Влияние и способ заражения | <b>Географическое местоположение инцидента</b>     |  |
| Образцы вредоносного ПО    | Федеральный округ                                  | Центральный федеральный округ  |
| Вредоносные письма         | Субъект федерации                                  | Московская область   |
| Индикаторы компрометации   | Населенный пункт                                   |  |
| Дополнительно              | <b>Локализация инцидента и атакованные сервисы</b> |  |
|                            | Подразделение                                      | ИТ   |
|                            | Техническое средство                               | Техническое средство клиента   |
|                            | Атакованные сервисы                                |  |
|                            | <b>Обращение в правоохранительные органы</b>       |  |
|                            | Обращение в правоохранительные органы              | Обращения нет  |

[Создать новую версию](#)

**Рисунок 22 – Просмотр содержания инцидента из карточки в формате JSON**

- Для завершения создания запроса и отправки его ФинЦЕРТ необходимо заполнить поле «Тема» и добавить описание, после чего нажать кнопку «Создать запрос» либо нажать «Удалить запрос», если необходимо пересоздать запрос заново или необходимость в нем отпала (Рисунок 23).



INT\_MLW

\*\*\*Петров р

Вирусное заражение

Вложения [Добавить](#) ▾

Электронная форма инцидента

Черновик сохранен в 19:42

Создать запрос Удалить запрос

**Рисунок 23 – Создание запроса в ФинЦЕРТ**

### **2.6.3 Создание запроса об изменении карточки участника**

Запрос об изменении в карточке участника может содержать обновленную информацию об организации, используемом ПО или ответственных лицах.

#### **2.6.3.1 Регистрация запроса об изменении информации об организации**

Чтобы зарегистрировать запрос об изменении основной информации об организации:

- В главном меню нажмите кнопку «Новый запрос» и выберите «Данные участника».
- Откроется окно «Электронная форма участника».
- На вкладке «Параметры участника» внесите необходимые изменения.
- Нажмите кнопку «Готово».
- Откроется страница «Запросы».
- Введите сообщение и тему запроса.
- Нажмите кнопку «Создать запрос» для отправки запроса в ФинЦЕРТ.

Запрос об изменении основной информации об организации зарегистрирован.

#### **2.6.3.2 Регистрация запроса об изменении информации об ответственном лице**

Вы можете изменить информацию об ответственном лице, заблокировать или добавить ответственное лицо. Вы не можете удалить карточку ответственного лица.

Чтобы добавить ответственное лицо:

- В главном меню нажмите кнопку «Новый запрос» и выберите «Данные участника».
- Откроется окно «Электронная форма участника».
- На вкладке «Ответственные лица» нажмите кнопку «Добавить».

Откроется окно «Добавление ответственного лица».

The screenshot shows a web form titled "Добавление ответственного лица" (Add responsible person) with a close button (X) in the top right corner. The form contains the following fields and controls:

- ФИО** (Full Name): Three text input fields for last name, first name, and middle name, each with a small icon on the right.
- Должность** (Position): A single text input field.
- Доступ в личный кабинет** (Access to personal cabinet): Two radio buttons labeled "Активирован" (Activated) and "Не активирован" (Not activated).
- Права доступа** (Access rights): Two buttons labeled "Администратор" (Administrator) and "Пользователь" (User).
- Категория** (Category): A dropdown menu.
- Контакты** (Contacts):
  - Эл.почта** (Email): A text input field with a small icon on the right. Below it is the text "Адрес для отправки уведомлений" (Address for sending notifications).
  - Городской телефон** (City phone): A text input field. Below it is the text "Укажите добавочный номер, если он известен" (Specify extension number if known).
  - Мобильный телефон** (Mobile phone): A text input field with a small icon on the right.

A blue button labeled "Готово" (Ready) is located at the bottom right of the form.

**Рисунок 24 – Добавление ответственного лица**

- В поля «ФИО» введите фамилию, имя и отчество ответственного лица.
- В поле «Должность» введите должность ответственного лица.

## БКМД.62.01.12.545.ИЗ.3

- В поле «Права доступа» выберите набор прав для ответственного лица.
- В поле «Категория» выберите категорию ответственного лица.
- В поле «Эл. почта» введите адрес электронной почты ответственного лица для рассылки уведомлений.
- В поле «Городской телефон» введите номер городского телефона ответственного лица.
- В поле «Мобильный телефон» введите номер мобильного телефона ответственного лица.
- Нажмите кнопку «Готово».

Откроется страница Запросы.

- Введите сообщение и тему запроса.
- Нажмите кнопку «Создать запрос».

Запрос о добавлении ответственного лица зарегистрирован.

Чтобы зарегистрировать запрос об изменении информации об ответственном лице:

- В главном меню нажмите кнопку «Новый запрос» и выберите «Данные участника».

Откроется окно «Электронная форма участника».

- На вкладке «Ответственные лица» выберите пользователя, данные которого необходимо изменить, и нажмите кнопку «Редактировать».

Откроется окно «Редактирование ответственного лица».

- Внесите изменения.
- Нажмите кнопку «Готово».

Откроется страница «Запросы».

- Введите сообщение и тему запроса.
- Нажмите кнопку «Создать запрос».

Запрос об изменении информации об ответственном лице зарегистрирован.

Чтобы зарегистрировать запрос о блокировке доступа ответственного лица к Личному кабинету Участника:

- В главном меню нажмите кнопку «Новый запрос» и выберите «Данные участника».

Откроется окно «Электронная форма участника».

- На вкладке «Ответственные лица» выберите пользователя, доступ которого вы хотите заблокировать, и нажмите кнопку «Заблокировать».
- Нажмите кнопку «Готово».

Откроется страница «Запросы».

- Введите сообщение и тему запроса.
- Нажмите кнопку «Создать запрос».

Запрос о блокировке доступа ответственного лица к Личному кабинету Участника зарегистрирован.

### **2.6.3.3 Регистрация запроса об изменении информации об используемом ПО**

Вы можете добавить, изменить или удалить информацию об используемом ПО.

Чтобы добавить информацию об используемом ПО:

- В главном меню нажмите кнопку «Новый запрос» и выберите «Данные участника».

Откроется окно «Электронная форма участника».

- На вкладке «Используемое ПО» нажмите кнопку «Добавить ПО...».

Откроется окно «Новое программное обеспечение».

## Электронная форма участника

The screenshot shows the 'Электронная форма участника' (Electronic form of the participant) interface. At the top, there are three tabs: 'Параметры участника' (Participant parameters), 'Ответственные лица' (Responsible persons), and 'Используемое ПО' (Used software), with the last one being the active tab. Below the tabs, there are three buttons: '+ Добавить ПО...' (Add software...), 'Изменить' (Edit), and 'Удалить' (Delete). A modal window titled 'Новое программное обеспечение' (New software) is open, containing two input fields: 'Название' (Name) and 'Тип ПО' (Software type), and two buttons at the bottom: 'Создать' (Create) and 'Заккрыть' (Close).

**Рисунок 25 – Добавление информации об используемом ПО**

- В поле «Название» введите название программного обеспечения.
- В поле «Тип ПО» выберите тип программного обеспечения.
- Нажмите кнопку «Создать».

Откроется страница Запросы.

- Введите сообщение и тему запроса.
- Нажмите кнопку «Создать запрос».

Запрос о добавлении информации об используемом ПО зарегистрирован.

Чтобы изменить информацию об используемом ПО:

- В главном меню нажмите кнопку «Новый запрос» и выберите «Данные участника».

Откроется окно «Электронная форма участника».

- На вкладке «Используемое ПО» выберите ПО и нажмите кнопку «Изменить».

Откроется окно «Изменение данных ПО».

- Внесите необходимые изменения.

- Нажмите кнопку «Сохранить».

- Нажмите кнопку «Готово».

Откроется страница «Запросы».

- Введите сообщение и тему запроса.

- Нажмите кнопку «Создать запрос».

Запрос об изменении информации об используемом ПО зарегистрирован.

Чтобы удалить информацию об используемом ПО:

- В главном меню нажмите кнопку «Новый запрос» и выберите «Данные участника».

Откроется окно «Электронная форма участника».

- На вкладке «Используемое ПО» выберите ПО и нажмите кнопку «Удалить».

- Нажмите кнопку «Готово».

Откроется страница «Запросы».

- Введите сообщение и тему запроса.

- Нажмите кнопку «Создать запрос».

Запрос об удалении информации об используемом ПО зарегистрирован.

#### **2.6.3.4 Регистрация запроса о внесении данных о сертификате ЭП пользователя, сгенерированном в меню «Управление сертификатом»**

#### **2.6.4 Создание запроса об угрозе**

Для регистрации запроса об угрозе:

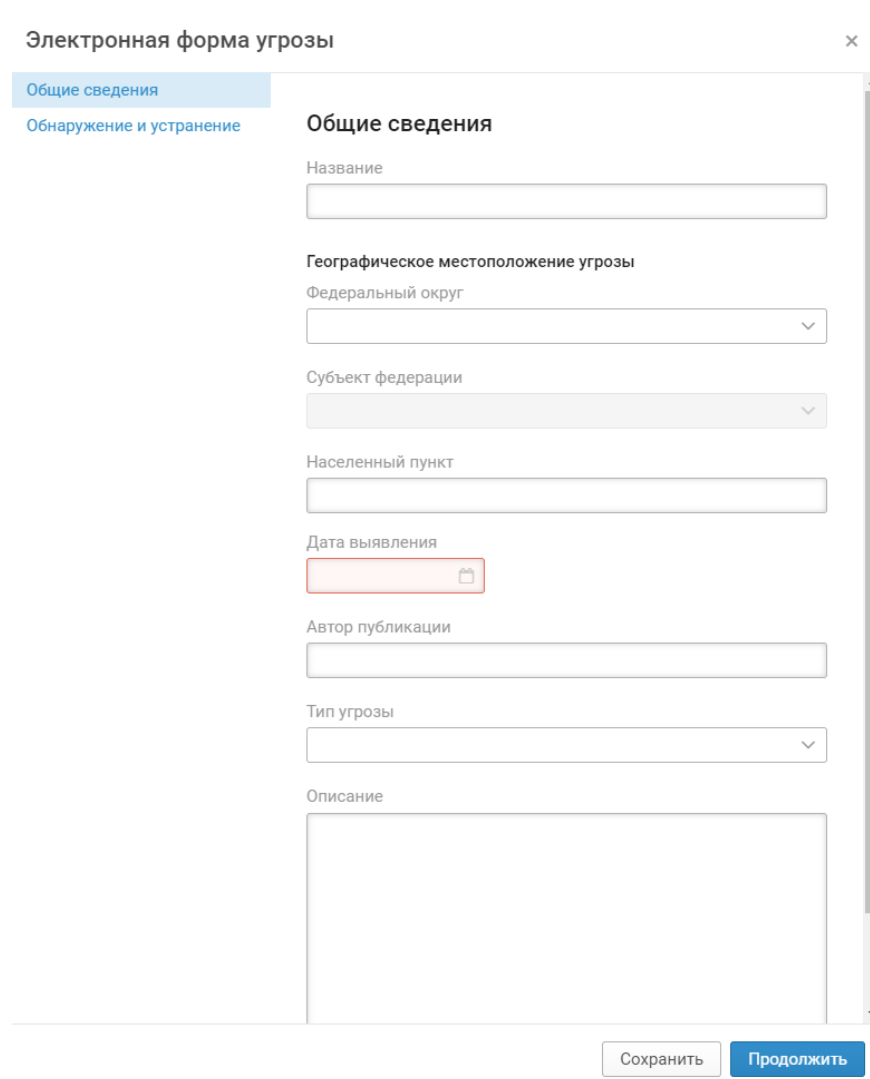
- В главном меню нажмите кнопку «Новый запрос» и выберите «Угроза».

- В открывшейся форме (Рисунок 26) заполните поля:

- а) на вкладке «Общие сведения» в поле «Название» введите название угрозы;

## БКМД.62.01.12.545.ИЗ.3

- б) в поле «Федеральный округ» выберите федеральный округ, на территории которого обнаружена угроза.
- в) в поле «Субъект федерации» выберите субъект Российской Федерации, на территории которого обнаружена угроза.
- г) в поле «Населенный пункт» введите название города или иного населенного пункта, в котором обнаружена угроза.
- д) в поле «Дата выявления» укажите дату выявления угрозы;
- е) в поле «Автор публикации» укажите автора, который обнаружил угрозу;
- ж) в поле «Тип угрозы» из раскрывающегося списка выберите тип угрозы;
- з) в поле «Описание» введите описание угрозы;



Электронная форма угрозы

Общие сведения

Обнаружение и устранение

Общие сведения

Название

Географическое местоположение угрозы

Федеральный округ

Субъект федерации

Населенный пункт

Дата выявления

Автор публикации

Тип угрозы

Описание

Сохранить

Продолжить

Рисунок 26 – Добавление общих сведений об угрозе

- Нажмите кнопку «Продолжить». Откроется вкладка «Обнаружение и устранение». Состав и содержимое вкладок зависит от выбранного типа угрозы. После выбора (из всплывающего меню) типа угрозы появится дополнительный пункт меню с одноимённым названием, которое так же необходимо заполнить (Рисунок 27).

Электронная форма угрозы

Общие сведения

Вредоносное программное обеспечение

Вредоносное программное обеспечение

Обнаружение и устранение

Дата выявления

Автор публикации

Тип угрозы

Вредоносное программное обеспечение

Вредоносное программное обеспечение

Эксплуатация уязвимости

DDoS

ЦУ бот-сети

Фишинг

Вредоносный ресурс

Мошеннический телефонный номер

Продолжить

**Рисунок 27 – Выбор типа угрозы**

- Нажмите кнопку «Продолжить». В форме (Рисунок 28) необходимо заполнить информацию:
  - а) в поле «Автор способа» введите автора способа обнаружения и устранения угрозы;
  - б) в поле «Описание способа» введите описание способа обнаружения и устранения угрозы;
  - в) в поле «Файл с правилами сигнатуры или правила детекта» перетащите или выберите файл;
  - г) в поле «Возможные меры устранения» введите описание неформализованного или формализованного способа определения угрозы;

д) в поле «Прочая информация» введите дополнительную информацию;

**Рисунок 28 – Добавление информации о способах обнаружения и устранения угрозы**

- Нажмите кнопку «Добавить к запросу». Откроется страница «Запросы».
- Введите текст в поле «Написать сообщение...» и в поле «Тема».
- Нажмите кнопку «Создать запрос».

Запрос об угрозе создан.

### **2.6.5 Создание запроса об уязвимости**

Для регистрации запроса об уязвимости:

- В главном меню нажмите кнопку «Новый запрос» и выберите пункт меню «Уязвимость».
- В открывшейся форме (Рисунок 29) заполните:
  - а) на вкладке «Общие сведения» в поле «Название» введите название уязвимости;

## БКМД.62.01.12.545.ИЗ.3

- б) в поле «Идентификаторы других систем описаний уязвимостей» введите один идентификатор или несколько через запятую;
  - в) в поле «Описание уязвимости и способов ее использования» введите описание;
  - г) в блоке «Класс уязвимости» выберите соответствующий пункт;
  - д) в поле «CVSS-вектор» введите CVSS-вектор;
  - е) в поле «Федеральный округ» выберите федеральный округ, на территории которого обнаружена угроза.
  - ж) в поле «Субъект федерации» выберите субъект Российской Федерации, на территории которого обнаружена угроза.
  - з) в поле «Населенный пункт» введите название города или иного населенного пункта, в котором обнаружена угроза.
- Нажмите кнопку «Продолжить». Откроется вкладка «Технические подробности».

Электронная форма уязвимости

Общие сведения

Технические подробности

Возникновение и устранение

**Общие сведения**

Название

Идентификаторы других систем описаний уязвимостей

Через запятую или построчно

Описание уязвимости и способов ее использования

Класс уязвимости

☐ Уязвимость кода (COD)  
Уязвимость, появившаяся при разработке ПО

☐ Уязвимость конфигурации (CFG)  
Уязвимость, появившаяся при настройке ОС, ПО или информационной системы

☐ Уязвимость архитектуры (ARH)  
Уязвимость, появившаяся при проектировании информационной системы

☐ Организационная уязвимость (ORG)  
Уязвимость, появившаяся из-за нарушения или отсутствия организационных мер защиты информации, нарушения правил эксплуатации системы защиты информации, различных требований или регламентов

☐ Многофакторная уязвимость (MULT)  
Уязвимость, появившаяся при наличии нескольких различных недостатков

☐ Не определенная уязвимость (OTH)

CVSS-вектор

Например: AV:N/AC:U/Au:N/C:C/J

Сохранить

Продолжить

**Рисунок 29 – Добавление общих сведений об уязвимости**

- Во вкладке «Технические подробности» (Рисунок 30) необходимо:
- а) в поле «Тип недостатка» выберите из выпадающего списка соответствующее значение типа недостатка.
  - б) в блоке параметров «Программное обеспечение» в поле «Название» введите название программного обеспечения;
  - в) в поле «Версия» введите версию программного обеспечения;
  - г) в поле «Служба или порт, который используется для функционирования ПО» укажите службу или порт;

Электронная форма уязвимости

×

Общие сведения

Технические подробности

Возникновение и устранение

Технические подробности

Тип недостатка

Программное обеспечение

Название

Версия

Служба или порт, который используется для функционирования ПО

Назад

Продолжить

**Рисунок 30 – Добавление технических подробностей об уязвимости**

- Нажмите кнопку «Продолжить». Откроется вкладка «Возникновение и устранение».
- В открывшейся форме (Рисунок 31):
  - а) в поле «Место возникновения или появления уязвимости» из выпадающего списка выберите нужное значение;
  - б) в поле «Операционная система и иное окружение уязвимого ПО» введите название операционной системы и иного окружения уязвимого ПО;
  - в) в поле «Дата выявления» укажите дату выявления уязвимости;
  - г) в поле «Автор, опубликовавший информацию о выявленной уязвимости» укажите организацию, которая обнаружила уязвимость, или ссылку на источник;
  - д) в поле «Способ обнаружения» введите способ обнаружения;

- е) в поле «Автоматизированное правило обнаружения» перетащите или выберите файл;
- ж) в поле «Рекомендации по устранению уязвимости» введите рекомендации по устранению;
- з) в поле «Прочая информация» введите дополнительную информацию;

**Рисунок 31 – Добавление информации по возникновению и устранению уязвимости**

- Нажмите кнопку «Готово». Откроется страница «Запросы».
- Введите текст в поле «Написать сообщение...» и в поле «Тема» Нажмите кнопку «Создать запрос».

Запрос об уязвимости создан.

### **2.6.6 Создание запроса о публикации**

Для регистрации запроса о публикации:

- В главном меню нажмите кнопку «Новый запрос» и выберите пункт меню «Публикация».

Откроется окно «Электронная форма публикации» на вкладке «Общие сведения» (Рисунок 32).

Электронная форма публикации

Общие сведения

Мероприятие

Наименование мероприятия

Описание

Не более 3 000 символов

Наименование организации

Ответственные лица

[+ Добавить ответственное лицо](#)

Дата мероприятия

Географическое местоположение

Федеральный округ

Субъект федерации

Населенный пункт

Сохранить Продолжить

**Рисунок 32 – Электронная форма публикации**

- В поле «Наименование мероприятия» укажите, как называется мероприятие.
- В поле «Описание» приведите краткую информацию о целях и формате мероприятия, о целевой аудитории.
- В поле «Наименование организации» укажите полное название компании, выступающей организатором мероприятия.
- Сформируйте список ответственных за мероприятие лиц. По ссылке «Добавить ответственное лицо» перейдите в окно «Новое ответственное лицо» и введите данные о новом контакте:
  - а) В поле «Имя» введите имя ответственного лица.

- б) В поле «Фамилия» введите фамилию ответственного лица.
- в) В поле «Отчество» введите отчество ответственного лица.
- г) В поле «Должность» введите должность ответственного лица.
- д) В поле «Городской телефон» укажите номер городского телефона ответственного лица.
- е) В поле «Мобильный телефон» укажите номер мобильного телефона ответственного лица.
- ж) В поле «Адрес эл. Почты» укажите адрес электронной почты ответственного лица.
- з) Нажмите кнопку «Сохранить».

Откроется окно «Электронная форма публикации».

- В поле «Дата мероприятия» выберите дату и при необходимости скорректируйте время начала мероприятия. По умолчанию начало мероприятия в 12:00 дня.
- В раскрывающемся списке «Федеральный округ» выберите федеральный округ, на территории которого проводится мероприятие.
- В раскрывающемся списке «Субъект федерации» выберите субъект федерации, на территории которого проводится мероприятие.
- В поле «Населенный пункт» введите город или иной населенный пункт, в котором проводится мероприятие.
- Нажмите кнопку «Продолжить».
- На вкладке «Мероприятия» в раскрывающемся списке «Тип мероприятия» выберите тип, к которому относится ваше мероприятие. Вы можете отнести мероприятие к нескольким типам.
- В поле «Текст мероприятия» введите текст публикации о вашем мероприятии. Поле обязательно для заполнения.
- В поле «Вложение» перетащите или выберите файл публикации о вашем мероприятии.
- Нажмите кнопку «Готово».

Откроется страница «Запросы».

- Добавьте сообщение в область «Написать сообщение...» и нажмите кнопку «Создать запрос».

Запрос о публикации зарегистрирован.

### **2.6.7 Регистрация запроса о блокировке корреспондентского счета**

Чтобы зарегистрировать запрос о блокировке корреспондентского счета:

- В главном меню нажмите кнопку «Новый запрос» и выберите пункт меню «Запрос на блокировку корреспондентского счета».

Откроется окно «Запрос на блокировку корреспондентского счета» (Рисунок 33).

Добавление заявки ×

**Общие сведения**  
Контактное лицо

**Общие сведения**

УИС  
  
Уникальный идентификатор составителя электронного сообщения

Регистрационный номер  
  
Регистрационный номер из книги государственной регистрации кредитных организаций

БИК участника  
  
Банковский идентификационный код – 9 цифр

Операция

Дата исполнения операции

Описание  
  
Необязательно  
Не более 3 000 символов

Вложение  

Перетащите сюда файлы или [выберите](#)

  
Приложите скан подписанного заявления установленного образца. Обязателен

**Рисунок 33 – Создание заявки на блокировку корреспондентского счета**

- В поле «УИС» введите уникальный идентификатор составителя электронного сообщения.
- В поле «Регистрационный номер» введите регистрационный номер организации из книги государственной регистрации кредитных организаций.
- Выберите операцию «Заблокировать».
- В поле «Дата исполнения операции» выберите дату.
- В область загрузки перетащите файл с копией подписанного заявления установленного образца.
- Нажмите кнопку «Сохранить».

- На вкладке «Контактное лицо» автоматически подставляются записи текущего пользователя, при необходимости допускается корректировка значений.
- Нажмите кнопку «Добавить к запросу».
- В панели переписки введите тему и добавьте сообщение.
- Нажмите кнопку «Создать запрос».

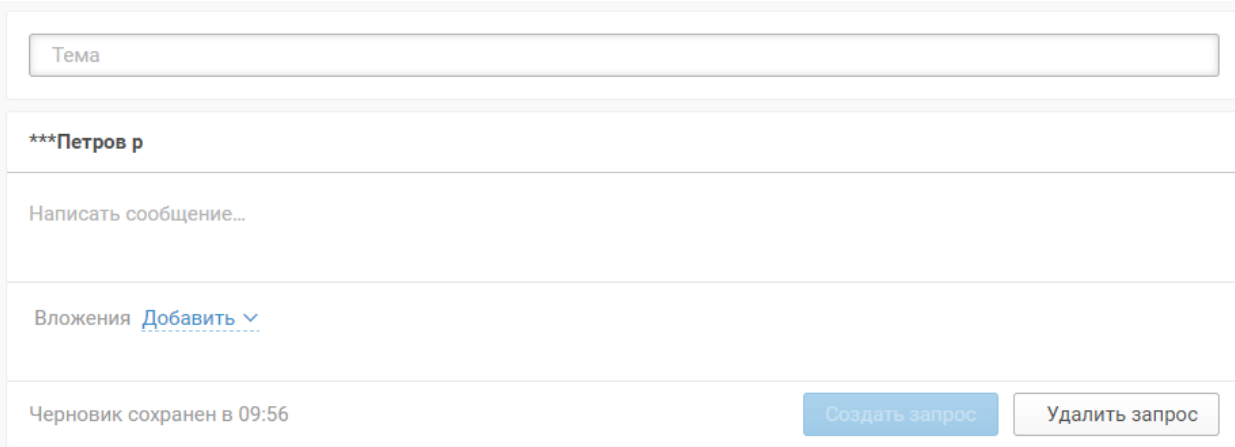
Запрос о блокировке корреспондентского счета организации зарегистрирован в ФинЦЕРТ.

### 2.6.8 Регистрация диспутного запроса

Чтобы зарегистрировать диспутный запрос:

- В главном меню нажмите кнопку «Новый запрос» и выберите пункт меню «Диспутный запрос».

Откроется страница создания запроса.



**Рисунок 34 – Окно создания диспутного запроса**

- В поле «Тема» введите тему запроса.
- Добавьте сообщение, сопровождающее запрос.
- Если требуется, вложите файлы с дополнительной информацией.

Нельзя добавлять в запрос электронные формы, а также исполняемые файлы (файлы с расширениями .exe, .app, .vb и прочими).

- Нажмите кнопку «Создать запрос».

Запрос зарегистрирован и отображается в списке запросов.

### 2.6.9 Регистрация запроса на анализ ВПО

Вы можете отправить в "ФинЦЕРТ" потенциально вредоносный файл для его проверки. Система автоматически проверит этот файл и пришлет вам результат.

Чтобы отправить запрос на анализ ВПО:

- В главном меню нажмите кнопку «Новый запрос» и выберите пункт «Запрос на анализ ВПО».


Откроется окно «Запрос на анализ ВПО».

Запрос на анализ ВПО

Общие сведения

Запрос на анализ ВПО

Файлы с ВПО

 Перетащите сюда файлы или [выберите](#)

Сохранить

Добавить к запросу

Рисунок 35 – Окно «Запрос на анализ ВПО»

- В область загрузки перетащите файл для проверки или выберите его из списка.  
Файлы с образцами вредоносного ПО должны быть помещены в архив RAR.

- Нажмите кнопку «Добавить к запросу».
- В панели переписки введите тему.
- Нажмите кнопку «Создать запрос».

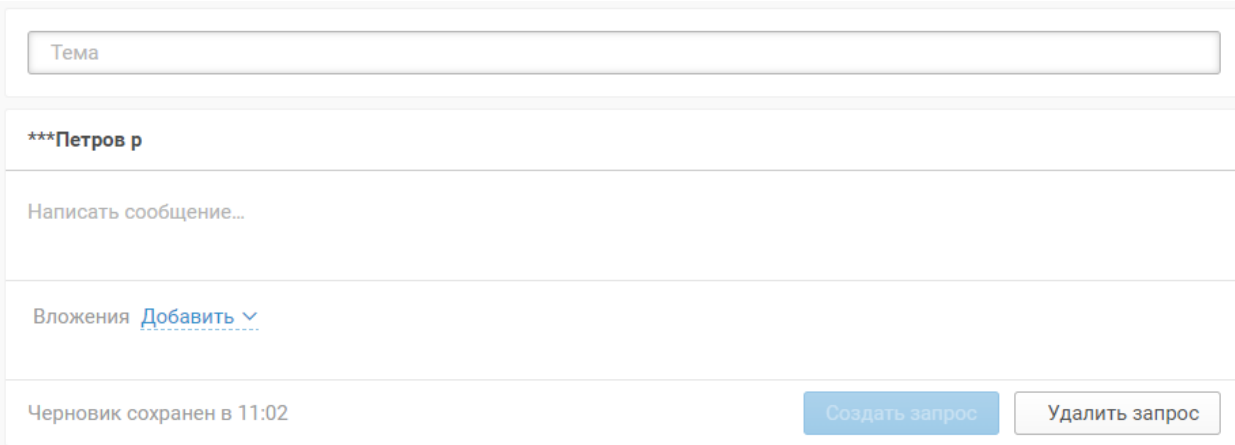
Запрос на анализ ВПО отправлен.

### 2.6.10 Создание произвольных запросов

Для регистрации других (произвольных) запросов:

- В главном меню нажмите кнопку «Новый запрос» и выберите пункт «Другое».

Откроется окно формирования произвольного запроса (Рисунок 36)



Тема

\*\*\*Петров р

Написать сообщение...

Вложения [Добавить](#) ▼

Черновик сохранен в 11:02

Создать запрос

Удалить запрос

**Рисунок 36 – Окно формирования произвольного запроса**

- В открывшейся форме:
  - а) в правой панели в поле «Тема» ввести тему запроса;
  - б) в поле «Написать сообщение» введите сообщение;
  - в) в поле «Вложения» перетащите или выберите файл или по кнопке «Добавить» добавьте информацию об инциденте, участнике, уязвимости, угрозе или публикации;
  - г) нажмите кнопку «Создать запрос».

Запрос создан.

## **2.6.11 Электронная форма инцидента**

Набор вкладок и полей электронной формы инцидента зависит от типа инцидента. Для всех типов инцидентов необходимо указать следующую информацию:

- Блок Общие сведения (Рисунок 37):
  - а) Помощь ФинЦЕРТ. Укажите, требуется ли консультация или помощь со стороны ФинЦЕРТ. Поле обязательно для заполнения.
  - б) Описание инцидента. Укажите, что произошло, когда и с помощью каких средств вы это обнаружили, какие меры были приняты участником для локализации последствий инцидента и предотвращения подобных инцидентов в дальнейшем.
  - в) Тип инцидента. В раскрывающемся списке выберите тип инцидента в одной из групп: с вектором EXТ (2.6.11.1) или с вектором INT (2.6.11.3). Поле обязательно для заполнения.
  - г) Обнаружен. Укажите дату и время обнаружения инцидента. Дата указывается в формате ДДММГГГГ. Время указывается в формате ЧЧ:ММ.

Блок Географическое местоположение инцидента содержит следующие параметры:

- а) Федеральный округ. Укажите федеральный округ, на территории которого произошел инцидент. В случае выявления инцидента, связанного с трансграничным переводом денежных средств, место выявления инцидента не указывается. Поле обязательно для заполнения.
- б) Субъект федерации. Укажите субъект федерации, на территории которого произошел инцидент. Поле обязательно для заполнения.
- в) Населенный пункт. Укажите город или иной населенный пункт, в котором произошел инцидент. Поле обязательно для заполнения.

Блок Локализация инцидента и атакованные сервисы содержит следующие параметры:

- а) Подразделение. Укажите атакуемое структурное (организационное) подразделение. Например: департамент информационных технологий;

## БКМД.62.01.12.545.ИЗ.3

- б) Техническое средство. Укажите техническое средство, где был зафиксирован инцидент;
- в) Атакованные сервисы. Чтобы добавить информацию по атакованным сервисам нажмите «Добавить сервис». Появится окно добавления атакованного сервиса. Из выпадающего списка Тип сервиса выберите подходящее значение, при необходимости укажите дополнительную информацию в поле «Описание сервиса» и нажмите кнопку «Сохранить»;
- г) в выпадающем списке «Обращение в правоохранительные органы» выберите значение;

Электронная форма инцидента

Общие сведения

Принятые меры

Операции без согласия

Вложения

Итоги

Дополнительно

Подтверждение

Общие сведения

Помощь ФинЦЕРТ

Требуется Не требуется

Описание инцидента

Опишите детали инцидента:  
— что произошло  
— когда, как и с помощью каких средств вы это обнаружили

Тип инцидента

Обнаружен

Географическое местоположение инцидента

Федеральный округ

Субъект федерации

Населенный пункт

Укажите название населенного пункта, в котором произошел инцидент

Локализация инцидента и атакованные сервисы

Подразделение

Атакующее структурное (организационное) подразделение. Например: департамент информационных технологий.

Техническое средство

Техническое средство, где был зафиксирован инцидент

Атакованные сервисы + Добавить сервис

Обращение в правоохранительные органы

Обращение в правоохранительные органы

Сохранить Продолжить

**Рисунок 37 – Общие сведения по инциденту**

- Блок «Вектор инцидента — EXT» (Рисунок 38):
- Тип инцидента. В раскрывающемся списке выберите один из предложенных типов.
  - События. Перечислите события, последствия или выявление которых привело к инциденту. По ссылке [Добавить событие](#) перейдите в окно и заполните поля:

## БКМД.62.01.12.545.ИЗ.3

- 1) Событие. В раскрывающемся списке выберите событие, максимально точно описывающее, каким образом зафиксировано несанкционированное действие.
- 2) Тип и способ использования электронного средства платежа для списания денежных средств. В раскрывающемся списке выберите инструментарий, средствами которого произведено несанкционированное списание средств.

**Внимание!** Детальная информация по инциденту указывается на отдельных вкладках. Их состав зависит от выбранного типа инцидента вектора EXT.

**Электронная форма инцидента**

Общие сведения

**Вектор инцидента - EXT**

Принятые меры

Операции без согласия

Вложения

Итоги

**Тип инцидента — malware**

0.0.0.0

Влияние и способ заражения

Образцы вредоносного ПО

Вредоносные письма

Индикаторы компрометации

+ Добавить

Дополнительно

Подтверждение

**Вектор инцидента — EXT**

Тип инцидента

Нарушение требований к обеспечению защиты информац...

**События**

Событие

(MTR\_WC) Получение уведомлений от клиентов – физических и (или) юридических лиц, и (или) индивидуальных предпринимателей и (или) лиц, занимающихся частной практикой о попытках осуществления переводов денежных средств без их согласия

Тип и способ списания

(SMS) SMS банкинг. Технология дистанционного банковского обслуживания, при которой обмен информацией между клиентом и банком осуществляется с применением коротких текстовых сообщений с определенного в договоре банковского счета номера телефона

+ Добавить событие

**Рисунок 38 – Пример параметров инцидента вектора EXT**

- Блок «Вектор инцидента — INT»:

## БКМД.62.01.12.545.ИЗ.3

- а) Тип инцидента. В раскрывающемся списке выберите один из предложенных типов.
- б) События. Перечислите события, последствия или выявление которых привело к инциденту. По ссылке [Добавить событие](#) перейдите в окно и заполните поля:
  - 1) Событие. В раскрывающемся списке выберите событие, максимально точно описывающее, каким образом зафиксировано несанкционированное действие.
  - 2) Тип нарушителя. В раскрывающемся списке выберите один из предложенных вариантов. Поле обязательно для заполнения.

**Внимание!** Детальная информация по инциденту указывается на отдельных вкладках (2.6.11.4). Их состав зависит от выбранного типа инцидента вектора INT.

Электронная форма инцидента

×

Общие сведения

Вектор инцидента - INT

Принятые меры

Операции без согласия

Вложения

Итоги

Тип инцидента – trafficHijackAttacks

Описание по типу

+ Добавить

Дополнительно

Подтверждение

Вектор инцидента – INT

Тип инцидента

Нарушение требований к обеспечению защиты информац... ▾

События

Событие

(EMP-UA) Уменьшение остатка электронных денежных средств, совершенного в результате несанкционированного доступа к объектам информационной инфраструктуры оператора электронных денежных средств

✎ 🗑

Тип нарушителя

(EXT\_ORG) Реализации компьютерных атак или несанкционированного доступа лиц, не обладающих полномочиями доступа к объектам информационной инфраструктуры участников информационного обмена (действия внешнего нарушителя)

+ Добавить событие

**Рисунок 39 – Пример параметров инцидента вектора INT**

- Блок «Принятые меры». В открывшейся форме перечислите действия, которые вы предприняли в контексте обнаруженного инцидента. По кнопке «Добавить» меры будут зафиксированы на вкладке с указанием даты и времени.
- Блок «Вложения»:
  - а) Перетащите или выберите файл. Перетащите или выберите файлы, которые могут быть полезны для расследования инцидента.

Электронная форма инцидента x

---

Общие сведения

Вектор инцидента - INT

Принятые меры

Операции без согласия

**Вложения**

Итоги

Тип инцидента –  
trafficHijackAttacks


Описание по типу

+ Добавить

Дополнительно

Подтверждение

**Вложения**

 Перетащите сюда файлы или [выберите](#)

**Рисунок 40 – Добавление вложения к описанию инцидента**

– Блок «Итоги».

а) Секция «Ущерб от инцидента» содержит следующие параметры:

- 1) Операционные расходы. Оцените размер ущерба и возможные негативные последствия. Если ущерба нанесено не было, отсавтить поле пустым.
- 2) Относительный масштаб. В раскрывающемся списке выберите вариант влияния обнаруженного инцидента.

б) Секция «Сигнатуры атаки» содержит следующие параметры:

- 1) Сработавшие атаки. Перечислите все известные вам в контексте обнаруженного инцидента свойства обнаруженных атак:
  - Средство обнаружения. Укажите средство, с помощью которого обнаружены атаки.
  - Идентификатор сигнатуры. Укажите уникальную последовательность символов, полученных в результате вычисления хеш-функции MD5. Поле обязательно для заполнения.
  - Источник получения. Укажите, из каких источников получены сигнатуры атак.

- Число срабатываний. Укажите, сколько раз сработали сигнатуры атак в рамках описываемого инцидента.

в) Секция «SNORT-правило обнаружения атак». По ссылке «Добавить SNORT-правило» перейдите в окно, где в поле SNORT-правило укажите все атрибуты правила в формате:

*<Действие> <Протокол> <IP-адреса отправителей> <Порты отправителей> <Оператор направления> <IP-адреса получателей> <Порты получателей> (ключ\_1: значение\_1; ключ\_2: значение\_2; ... ключ\_N: значение\_N;)*

- Секция «Итоговый отчет» содержит следующие параметры:
- Дата закрытия инцидента. Укажите дату и время, когда инцидент был закрыт.
- Восстановление функционирования. В раскрывающемся списке выберите Восстановлено полностью, если вам удалось привести систему в состояние до начала атаки, или Восстановлено частично, если в результате устранения последствий инцидента остались невосстановленные объекты или данные.
- Описание. Укажите меры, предпринятые для восстановления системы.
- Причины возникновения. Укажите причины возникновения инцидента.
- Принятые меры. Перечислите все действия, которые были предприняты для устранения инцидента и его последствий.
- Далее откроется вкладка Подтверждение. Проверьте заполненную информацию об инциденте. Если требуется, измените информацию.

Вложите заполненную электронную форму инцидента в запрос по кнопке «Добавить к запросу».

### **2.6.11.1 Типы инцидентов с вектором EXT**

К инцидентам с вектором EXT относятся инциденты, направленные на клиентов организации. Несанкционированная операция может быть осуществлена одним из следующих способов:

- SMS-банкинг — технология дистанционного банковского обслуживания, при которой обмен информацией между клиентом и банком осуществляется с

применением коротких текстовых сообщений с номера телефона, определенного в договоре банковского счета;

- банкомат;
- интернет-банкинг — технология дистанционного банковского обслуживания, при которой обмен информацией между клиентом и банком осуществляется с применением браузера без установки дополнительного программного обеспечения;
- платежи в интернете без предъявления карты;
- платежный терминал;
- приложение для мобильного банка — технология дистанционного банковского обслуживания, при которой обмен информацией между клиентом и банком осуществляется с применением программного обеспечения, разрабатываемого для использования в операционных системах мобильных устройств (например, iOS, Android);
- система "Банкинг-клиент" — технология дистанционного банковского обслуживания, при которой обмен информацией между клиентом и банком осуществляется с персонального компьютера с применением дополнительного программного обеспечения, предоставляемого банком.

Инциденты с вектором EXT бывают следующих типов:

- Вредоносное ПО (MLW) — совершение несанкционированного перевода денежных средств в результате воздействия вредоносного ПО.
- Фишинговый ресурс (P2P) — совершение несанкционированного перевода денежных средств в результате использования фишингового ресурса.
- Социальная инженерия (SOI) — совершение несанкционированного перевода денежных средств в результате обмана или злоупотребления доверием.
- Атака с подменой номера (SIM) — совершение несанкционированного перевода денежных средств в результате изменения IMSI SIM-карты, смена IMEI телефона.

- Утрата электронного средства платежа (LST) — совершение несанкционированного перевода денежных средств в результате утраты электронного средства платежа.
- Другой инцидент с вектором EXT (ОТН) — совершение несанкционированного перевода денежных средств в результате иных причин.

Информацию об инцидентах перечисленных типов необходимо предоставить в течение одного рабочего дня с момента выявления.

### **2.6.11.2 Параметры инцидентов с вектором EXT**

Тип инцидента «Использование вредоносного программного обеспечения (malware)» имеет следующие параметры:

- Вкладка Влияние и способ заражения:
  - а) Внешний IP-адрес узла. Введите IP-адрес зараженного узла.
  - б) Классификаторы. Укажите наименование антивирусной системы и тип вредоносного ПО. Поле может содержать несколько значений.
  - в) Способ заражения. Укажите предполагаемый способ заражения: по каналам электронной почты, с носителя информации, распространение по локальной сети, иной способ. Поле обязательно для заполнения.
- Вкладка Образцы вредоносного ПО:
  - а) Файл. Прикрепите файлы, определенные антивирусным ПО или участником как подозрительные или вредоносные. Файлы с образцами вредоносного ПО должны быть помещены в архив RAR с паролем "infected". Размер файла не должен превышать 5 МБ.
  - б) Хеш-сумма. Укажите контрольную сумму каждого образца вредоносного ПО.
- Вкладка Вредоносные письма:
  - а) Адреса, с которых поступали письма. Укажите адрес электронной почты, с которого пришло письмо, и IP-адрес последнего почтового сервера, через который было передано письмо.

- б) Файл электронного письма. Перетащите или выберите экспортированное из почтовой программы письмо в форматах EML или MSG (письма необходимо упаковать в архив RAR с паролем "infected").
- Вкладка Индикаторы компрометации. Укажите все или часть индикаторов компрометации:
- а) Обращение по IP/URL-адресу. Перечислите скомпрометированные IP-адреса или URL-адреса.
  - б) Модификация текущих сетевых настроек. Поле заполняется в свободной форме.
  - в) Соккрытие следов сетевого взаимодействия. Например, удаление маршрутов или записей журналов сетевых устройств. Поле заполняется в свободной форме.
  - г) Создание файлов. Поле заполняется в свободной форме.
  - д) Изменение файлов. Поле заполняется в свободной форме.
  - е) Удаление файлов. Поле заполняется в свободной форме.
  - ж) Создание записей реестра. Поле заполняется в свободной форме.
  - з) Изменение записей реестра. Сведения заполняются в свободной форме.
  - и) Удаление записей реестра. Поле заполняется в свободной форме.
  - к) Запуск процесса. Сведения заполняются в свободной форме.
  - л) Изменение запущенного процесса. Сведения заполняются в свободной форме.
  - м) Завершение процесса. Сведения заполняются в свободной форме.
  - н) Отчет средств динамического анализа кода ("песочница"). Перетащите или выберите файл из списка.
  - о) Иные индикаторы. Сведения заполняются в свободной форме.

Тип инцидента «Использование методов социальной инженерии (socialEngineering)» имеет следующие параметры:

- Вкладка Описание по типу:

- а) Тип. Выберите метод социальной инженерии: звонок с мобильного телефона, звонок с телефонного номера 8-800, SMS-сообщение, социальная инженерия с использованием социальных сетей, социальная инженерия с использованием средств мгновенных сообщений или иной способ.
- б) Примечание. Опишите инцидент.
- в) Номер телефона. Укажите номер телефона, с которого было совершено несанкционированное действие.
- г) Электронная почта. Укажите адрес электронной почты в формате user@domain.ru, с которого поступала недостоверная информация, вредоносное содержимое или побуждение к несанкционированным действиям.
- д) IP-адрес почтового сервера. Укажите IP-адрес почтового сервера, с которого поступала недостоверная информация, вредоносное содержимое или побуждение к несанкционированным действиям.
- е) Вложение. В случае телефонных звонков приложите запись разговора или описание разговора в свободной форме. В случае SMS-сообщений, использования социальных сетей или средств мгновенных сообщений приложите фотографию сообщения с указанием номера отправителя или укажите любые идентифицирующие признаки в средстве мгновенного сообщения.

Тип инцидента «Эксплуатация уязвимостей информационной инфраструктуры (vulnerabilities)» имеет следующие параметры:

- Вкладка <0.0.0.0>: Внешний адрес пострадавшей системы:
  - а) IP-адрес. Укажите IP-адрес узла, на котором эксплуатировалась уязвимость, в формате XXX.XXX.XXX.XXX.
  - б) Доменное имя. Введите в поле доменное имя пострадавшего узла.
  - в) URL-адрес. Укажите URL-адрес пострадавшего узла в формате www.domain.ru.

- г) Тип сервиса. Перечислите через запятую службы, которые были запущены на пострадавшей системе во время эксплуатации уязвимости. Сведения заполняются в свободной форме.

– Вкладка <0.0.0.0>: Атака:

- а) Источники атаки. Перечислите IP-адреса и URL-адреса систем, с которых производилась эксплуатация уязвимости пострадавшей системы.
- б) Идентификатор уязвимости. Укажите уникальный номер обнаруженной уязвимости согласно классификации ФСТЭК ([bdu.fstec.ru/vul](http://bdu.fstec.ru/vul)).

– Вкладка <0.0.0.0>: Свой идентификатор уязвимости:

- а) Описание. Введите описание уязвимости.
- б) Название ПО. Введите название программного обеспечения, в котором была выявлена уязвимость.
- в) Версия ПО. Введите версию программного обеспечения, в котором была выявлена уязвимость.
- г) Тип уязвимости. Введите название типа уязвимости.
- д) Класс уязвимости. Выберите один из следующих вариантов: Уязвимость кода, Уязвимость архитектуры, Уязвимость многофакторная.
- е) Дата обнаружения. Выберите в календаре дату обнаружения уязвимости. По умолчанию выбрана текущая дата.
- ж) Базовый CVSS. Введите базовый вектор уязвимости.
- з) Опасность. Выберите уровень опасности обнаруженной уязвимости: низкий, средний, высокий или критический.
- и) Меры устранения. Перечислите, какие меры были предприняты.
- к) Статус. Выберите статус уязвимости.
- л) Наличие эксплойта. Укажите наличие эксплойта.
- м) Рекомендации. Введите рекомендации по устранению уязвимости.
- н) Ссылки. Введите ссылки на источники информации об устранении уязвимости.

## БКМД.62.01.12.545.ИЗ.3

- о) Вендор. Введите название производителя программного обеспечения, в котором была обнаружена уязвимость.

Тип инцидента «Реализация спам рассылки (spams)» имеет следующие параметры:

- Вкладка Описание по типу:
  - а) Спам. Дата получения. Выберите дату получения сообщения, содержащего спам.
  - б) Цель атаки. Адрес электронной почты. Введите адрес электронной почты, на который поступил спам.
  - в) Источник атаки. IP-адрес. Введите IP-адрес, с которого был отправлен спам, в формате XXX.XXX.XXX.XXX.
  - г) Источник атаки. Доменное имя. Введите доменное имя источника рассылки спама.
  - д) Источник атаки. Адрес электронной почты. Введите адрес электронной почты, с которого был отправлен спам.

Тип инцидента «Взаимодействие с центрами "бот-нет" сетей (controlCenters)» имеет следующие параметры:

- Вкладка Описание по типу: Адрес пострадавшей системы:
  - а) IP-адрес. Введите IP-адрес пострадавшей системы в формате XXX.XXX.XXX.XXX.
  - б) URL. Введите URL-адрес пострадавшей системы в формате www.domain.ru.
- Вкладка Описание по типу: Информация с ЦУ бот-сети:
  - а) URL с ЦУ. Введите URL-адрес, на котором размещен ЦУ бот-сети.
  - б) IP-адрес злоумышленника. Введите IP-адрес злоумышленника, разместившего ЦУ бот-сети, в формате XXX.XXX.XXX.XXX.
  - в) Действия злоумышленника. Опишите действия злоумышленника, которые удалось выявить.
  - г) Сведения о бот-сети. Введите описание бот-сети.

- д) IP-адреса, обращавшиеся к ЦУ. Введите IP-адреса, обращавшиеся к ЦУ бот-сети, в формате XXX.XXX.XXX.XXX.

Тип инцидента «Использование фишинговых ресурсов (phishingAttacks)» имеет следующие параметры:

- Вкладка <0.0.0.0>: Пострадавшая система:
  - а) IP-адрес. Введите IP-адрес пострадавшей системы в формате XXX.XXX.XXX.XXX.
  - б) Домен. Введите в поле доменное имя пострадавшей системы.
  - в) Добавить фишинговый ресурс. Введите IP-адрес ресурса в формате XXX.XXX.XXX.XXX и URL-адрес ресурса в формате www.domain.ru.
  - д) Дата фиксации. Дата фиксирования фишингового сообщения.

Тип инцидента «Изменение IMSI на SIM-карте, смена IMEI телефона (sim)» имеет следующие параметры:

- Оператор связи. Введите название оператора связи.
- Номер телефона. Введите номер телефона в формате +7(XXX) XXXXXXXX.
- IMSI. Введите уникальный номер sim-карты в формате XXXXXXXXXXXXXXXX.
- Дата смены IMSI. Выберите дату фиксации смены IMSI.

Тип инцидента «Размещение запрещенного контента в сети "Интернет" (maliciousResourcer)» имеет следующие параметры:

- IP-адрес. Введите IP-адрес запрещенного контента в формате XXX.XXX.XXX.XXX.
- Единый указатель ресурса. Введите URL-адрес запрещенного контента в формате www.domain.ru
- Тип контента. Введите тип запрещенного контента.

Тип инцидента «Размещение вредоносного ресурса в сети "Интернет" (prohibitedContents)» имеет следующие параметры:

- IP-адрес. Введите IP-адрес вредоносного ресурса в формате XXX.XXX.XXX.XXX.

- Единый указатель ресурса. Введите URL-адрес вредоносного ресурса в формате `www.domain.ru`
- Описание вредоносной активности. Введите описание вредоносной активности.

Тип инцидента «Иная компьютерная атака (other)» имеет следующие параметры:

- Описание. Опишите произошедшее. Поле заполняется в свободной форме.
- Тип атаки. Введите иной тип атаки.
- IP-адрес. Введите IP-адрес в формате `XXX.XXX.XXX.XXX`.
- Единый указатель ресурса. Введите URL-адрес в формате `www.domain.ru`

### **2.6.11.3 Типы инцидентов с вектором INT**

К инцидентам с вектором INT относятся инциденты, направленные на инфраструктуру организации. Инциденты с вектором INT бывают следующих типов:

- Вредоносное ПО (MLW) — атака вредоносного ПО на любые устройства инфраструктуры (в том числе банкоматы, электронные и платежные терминалы). Атака учитывается при выполнении хотя бы одного из условий:
  - а) выявление вредоносного кода, не определяемого антивирусными ПО или определяемого не более чем пятью антивирусами на Virus Total;
  - б) обнаружение вредоносного или подозрительного ПО на объекте информационной инфраструктуры антивирусными ПО или иными СЗИ и направленного на этот объект информационной инфраструктуры;
  - в) обнаружение подозрительных файлов (процессов), обнаруженных на объекте информационной инфраструктуры, в том числе неисполняемых, не обнаруживаемых антивирусным ПО или хостинг-системами обнаружения вторжений (HIPS). Информацию об инциденте этого типа необходимо предоставить в течение одного рабочего дня с момента выявления инцидента.
- Эксплуатация уязвимостей (EXP) — попытка эксплуатации уязвимостей. К эксплуатации уязвимостей относится, например, использование SQL-инъекций. Попытки эксплуатации могут быть выявлены как средствами IDS / IPS / HIPS, так и специалистами организации либо в результате обращения гражданина в организацию о возможной попытке эксплуатации уязвимости. Информацию об

инциденте этого типа необходимо предоставить в течение одного рабочего дня с момента выявления инцидента.

- DoS или DDoS-атаки (DOS) — DoS / DDoS, сбой в работе оборудования и каналов связи, вызванный внешними причинами. Информацию об инциденте этого типа необходимо предоставить в течение трех часов с момента его окончания.
- Перебор паролей (BRF) — попытка взлома учетных записей (как внутри сети, так и на веб-ресурсах, принадлежащих организации) посредством автоматизированного подбора комбинаций паролей и логинов. Информацию о попытке подбора паролей к АРМ КБР, ДБО, АБС, базам данных, системам процессинга и иным критически важным системам, обеспечивающим функционирование КО и НСД, которая может повлечь финансовые риски, необходимо предоставить в течение трех часов с момента обнаружения. Информацию о попытке подбора паролей пользователей домена необходимо предоставить по завершению внутренней проверки в случае выявления внешнего вмешательства (заражения, проникновения в сеть извне).
- Фишинг (мошенничество) (PHI) — попытка получения доступа к конфиденциальным данным путем маскировки электронного письма или сайта под доверенный аналог. Информацию об инциденте этого типа необходимо предоставить в течение одного рабочего дня с момента выявления инцидента.
- Социальная инженерия (SOI) — использование телефонных номеров и электронных писем для распространения недостоверной информации, вредоносного содержимого и (или) побуждения работника организации к совершению несанкционированных действий путем обмана или злоупотребления доверием (включая письма, содержащие угрозы в адрес организации). Информацию об инциденте этого типа необходимо предоставить в течение одного рабочего дня с момента выявления инцидента.
- Физическая атака на банкомат (BAN) — физическое и (или) логическое воздействие на объекты информационной инфраструктуры. К физическому воздействию относятся установка скиммингового оборудования, несанкционированный доступ к интерфейсам управления (в том числе банкоматов и терминалов), повреждение оборудования с целью установки

сторонних аппаратных устройств или хищения находящихся в устройстве денежных средств. К логическому воздействию относятся внедрение стороннего программного обеспечения либо модификация существующих параметров системного программного обеспечения. Информацию об инциденте этого типа необходимо предоставить в течение одного рабочего дня с момента его выявления.

- Другой инцидент с вектором INT (OTH) — иные несанкционированные действия, которые могут нарушить безопасность организации.

#### **2.6.11.4 Параметры инцидентов с вектором INT**

Тип инцидента — MLW:

- Вкладка «Влияние и способ заражения»:
  - а) Внешний IP-адрес узла.
  - б) Классификаторы. Укажите наименование антивирусной системы и тип вредоносного ПО. Поле может содержать несколько значений.
  - в) Способ заражения. Укажите предполагаемый способ заражения: по каналам электронной почты, с носителя информации, распространение по локальной сети, иной способ. Поле обязательно для заполнения.
- Вкладка «Образцы вредоносного ПО»:
  - а) Файл. Прикрепите файлы, определенные антивирусным ПО или участником как подозрительные или вредоносные. Файлы с образцами вредоносного ПО должны быть помещены в архив RAR с паролем "infected". Размер файла не должен превышать 5 МБ.
  - б) Хеш-сумма. Укажите контрольную сумму каждого образца вредоносного ПО.
- Вкладка «Вредоносные письма»:
  - а) Адреса, с которых поступали письма. Укажите адрес электронной почты, с которого пришло письмо, и IP-адрес последнего почтового сервера, через который было передано письмо.

## БКМД.62.01.12.545.ИЗ.3

- б) Файл эл. письма. Перетащите или выберите экспортированное из почтовой программы письмо в форматах EML или MSG (письма необходимо упаковать в архив RAR с паролем "infected").
- Вкладка «Индикаторы компрометации». Укажите все или часть индикаторов компрометации:
  - а) Модификация текущих сетевых настроек. Поле заполняется в свободной форме.
  - б) Соккрытие следов сетевого взаимодействия. Например, удаление маршрутов или записей журналов сетевых устройств. Поле заполняется в свободной форме.
  - в) Изменение файлов. Поле заполняется в свободной форме.
  - г) Удаление файлов. Поле заполняется в свободной форме.
  - д) Изменение записей реестра. Сведения заполняются в свободной форме.
  - е) Запуск процесса. Сведения заполняются в свободной форме.
  - ж) Изменение запущенного процесса. Сведения заполняются в свободной форме.
  - з) Завершение процесса. Сведения заполняются в свободной форме.
  - и) Отчет средств динамического анализа кода ("песочница"). Перетащите или выберите файл из списка.
  - к) Иные индикаторы. Сведения заполняются в свободной форме.

Тип инцидента — EXP:

- Блок параметров «Внешний адрес пострадавшей системы»:
  - а) IP-адрес. Укажите внешний адрес атакуемой системы, чья целостность, доступность или конфиденциальность пострадала в результате атаки.
  - б) Доменное имя. Укажите доменное имя пострадавшей системы.
  - в) URL. Укажите месторасположение пострадавшей системы.
  - г) Тип сервиса. Укажите, какие службы были запущены на пострадавшей машине.
- Блок параметров «Атака»:

## БКМД.62.01.12.545.ИЗ.3

- а) Источник атаки. Укажите IP-адрес, с которого была выявлена эксплуатация уязвимости, и URL ресурса, при заходе на который эксплуатировалась уязвимость.
- б) Уязвимость. Если выявлена эксплуатация уязвимости неправильно настроенного сетевого сервиса, укажите его тип и опишите уязвимость. Если выявлена уязвимость ПО, укажите тип уязвимости по классификации ФСТЭК, CVE, MS или другой.
- в) Метрика CVSS. Укажите максимально возможное количество метрик: базовая, временная, контекстная, метрика окружения.
- г) Метрика CVSS (указана участником).

Тип инцидента — DOS:

– Блок параметров «Адрес пострадавшей системы»:

- а) IP-адрес. Укажите внешний адрес атакуемой системы, чья целостность, доступность или конфиденциальность пострадала в результате атаки.
- б) Сеть. Укажите сеть в формате маски подсети XXX.XXX.XXX.XXX/XX.
- в) Доменное имя. Укажите доменное имя пострадавшей системы.
- г) Назначение ресурса. Укажите назначение ресурса.
- д) URL. Укажите месторасположение пострадавшей системы.
- е) Тип сервиса. Укажите, какие службы были запущены на пострадавшей машине.

– Блок параметров «Атака»:

- а) IP-адреса источников. Укажите IP-адреса или загрузите их из файла.
- б) Тип атаки. В раскрывающемся списке выберите тип атаки. Поле обязательно для заполнения.
- в) Примечание. Укажите дополнительную информацию.
- г) Начало атаки. Укажите дату и время начала атаки. Дата указывается в формате ДДММГГГГ. Время указывается в формате ЧЧ:ММ.

## БКМД.62.01.12.545.ИЗ.3

- д) Окончание атаки. Укажите дату и время окончания атаки. Дата указывается в формате ДДММГГГГ. Время указывается в формате ЧЧ:ММ.
- е) Мощность.
- ж) Негативное влияние. В раскрывающемся списке укажите тип негативного влияния: прерывание доступности ресурса, иные негативные последствия, негативного влияния не было.
- з) Примечание. Укажите дополнительную информацию.

Тип инцидента — BRF:

- Блок «Адрес пострадавшей системы»:
  - а) IP-адрес. Укажите IP-адрес пострадавшей системы.
  - б) URL. Укажите месторасположение пострадавшей системы.
  - в) Атакованная служба.
- Блок параметров «Атака»:
  - а) IP-адреса источников. Укажите IP-адреса источников атаки через запятую или построчно или загрузите из файла. Формат файла PLAIN TEXT, по одному IP- адресу на строке.
- Блок параметров «Скомпрометированная учетная запись»:
  - а) Учетная запись. Укажите логин и домен учетной записи, которая была атакована.
  - б) Привилегии.

Тип инцидента — RNI:

- Блок параметров «Пострадавшая система»:
  - а) IP-адрес. Укажите IP-адрес пострадавшей системы.
  - б) Домен. Укажите домен пострадавшей системы.
- Блок параметров «Фишинговый ресурс»:
  - а) IP-адрес ресурса. Укажите IP-адрес ресурса, замаскированного под доверенный аналог.

- б) URL ресурса. Укажите местонахождение ресурса, замаскированного под доверенный аналог.

Тип инцидента — SOI:

– Вкладка «Описание по типу»:

- а) Тип. В раскрывающемся списке выберите тип социальной инженерии: фишинговое письмо, звонок с мобильного телефона, звонок с не мобильного номера, SMS-сообщение, социальная инженерия с использованием социальных сетей, социальная инженерия с использованием средств мгновенных сообщений.
- б) Примечание. Укажите любые данные, которые могут быть полезными при расследовании инцидента.
- в) Номер телефона. Укажите номер телефона, с которого было произведено несанкционированное действие.
- г) Вложения. Перетащите или выберите файл, содержащий фотографию сообщения с указанием номера отправителя, укажите любые идентифицирующие признаки в средстве мгновенного сообщения. В случае фишингово письма необходимо приложить экспортированное из почтовой программы письмо в форматах EML или MSG (письма необходимо упаковать в архив RAR с паролем "infected"). В случае телефонных звонков приложите запись разговора или описание разговора в свободной форме.

Тип инцидента — BAN:

– Вкладка «Описание по типу»:

- а) Тип объекта. В раскрывающемся списке выберите тип объекта, который подвергся воздействию: банкомат, банкомат с возможностью приема наличных денежных средств, банкомат с функцией ресайклинга, POS-терминал, платежный терминал, иной объект. Поле обязательно для заполнения.
- б) Примечание. Укажите любые данные, которые могут быть полезными при расследовании инцидента.

- в) Тип атаки. В раскрывающемся списке выберите тип атаки: атаки "блэкбокс", атаки "прямой диспенс" и их разновидности, скимминг, иная атака. Поле обязательно для заполнения.
- г) Примечание. Укажите любые данные, которые могут быть полезными при расследовании инцидента.
- д) Вложения. Приложите любые фотографии пострадавшего устройства, позволяющие получить представление о конкретно реализованном способе атаки, либо следов, оставленных злоумышленником.
- е) Если обнаружено подозрительное ПО, необходимо заполнить карточку MLW.

Тип инцидента — ОTH:

– Вкладка «Описание по типу»:

- а) Примечание. Опишите, что произошло. Укажите любые данные, которые могут быть полезными при расследовании инцидента. Поле обязательно для заполнения.

## **2.7 Работа с меню «Управление сертификатом»**

Для работы необходимо выполнить переход на вкладку «Управление сертификатом». При переходе открывается страница с описанием свойств текущего сертификата пользователя.

Рабочая область содержит 2 вкладки:

- Текущий сертификат – отображаются сведения о текущем сертификате пользователя, если пользователь ранее формировал запрос на генерацию сертификата и по данному запросу сертификат был издан пользователю (после заполнения полей вкладки «Новый сертификат») либо отображается сообщение «Текущий сертификат отсутствует, необходимо сгенерировать новый сертификат!» в случае, если сертификат пользователя отсутствует или отозван;
- Новый сертификат – отображаются поля для заполнения и кнопка «Сгенерировать».

На вкладке «Текущий сертификат» пользователь может просмотреть данные выданного ему сертификата либо скачать сам сертификат.

## БКМД.62.01.12.545.ИЗ.3

На вкладке «Новый сертификат» пользователь заполняет поля запроса на выдачу сертификата и нажимает кнопку «Сгенерировать», после чего генерируется запрос на сертификат и передается в УЦ АСОИ ФинЦЕРТ для сертификации. Данный сертификат ЭП Участника будет использоваться в информационном обмене. Подробно процедура получения сертификата ЭП Участника описана в документе БКМД.62.01.12.545.ИЗ.9 «Регламент получения ключевой информации».

**Внимание!** При формировании запроса на новый сертификат запрещено редактирование полей «Логин», «ФИО», «Организация».

После формирования сертификата необходимо скачать сгенерированный сертификат и передать его уполномоченному Участнику информационного обмена для формирования запроса на внесение изменений в карточку Участника. Уполномоченный Участник информационного обмена вносит в запрос серийный номер сертификата, а также дату начала и окончания действия сертификата, формирует запрос и отправляет его в ФинЦЕРТ.

При необходимости можно отозвать свой сертификат ЭП. Для этого на вкладке «Текущий сертификат» необходимо нажать кнопку «Отозвать». После отзыва необходимо заново сгенерировать запрос на сертификат в соответствии с вышеописанной процедурой.

### **3 Отправка форм обмена информацией через E-mail**

Заполненную форму в формате JSON необходимо отправить на адрес [fincert@cbr.ru](mailto:fincert@cbr.ru), также ее можно отправить через личный кабинет, приложив ее к запросу (см. п. 2.6.2).

Отправленная по электронной почте форма будет видна в личном кабинете списке запросов (см. п. 2.2). Письма электронной почты, отправляемые на адреса [fincert@cbr.ru](mailto:fincert@cbr.ru) и [info\\_fincert@cbr.ru](mailto:info_fincert@cbr.ru), создаются в виде запросов в АСОИ, и дальнейшая переписка по ним будет попадать в созданный запрос в виде сообщений.

## **4 Автоматизированная отправка инцидентов SIEM в АСОИ ФинЦЕРТ**

Раздел содержит основные сценарии работы с ПО "Пользовательский компонент" АСОИ ФинЦЕРТ. «Пользовательский компонент» обеспечивает автоматизированную отставку в ФинЦЕРТ инцидентов, зарегистрированных системами SIEM участника информационного обмена.

Более подробно работа с компонентом ФинЦЕРТ: "Пользовательский компонент" изложена в документе производителя ПО Positive Technologies «Positive Technologies ФинЦЕРТ: «Пользовательский компонент».

ПО «Пользовательский компонент» разворачивается в инфраструктуре участника информационного обмена. Дистрибутив ПО «Пользовательский компонент» может быть получен с информационного портала АСОИ ФинЦЕРТ (раздел «АСОИ ФинЦЕРТ (Документация и ПО Участника)»).

Как источник данных об инцидентах приложение использует информацию, передаваемую от SIEM (ArcSight, QRadar, PT MaxPatrol SIEM) по протоколу syslog RFC 5424. Полученные данные «Пользовательский компонент» конвертирует в формат JSON, совместимый с ФинЦЕРТ. После преобразования данных приложение отправляет их в ФинЦЕРТ.

«Пользовательский компонент» позволяет:

- отправлять данные инцидентов в ФинЦЕРТ в автоматическом и ручном режиме (по команде пользователя);
- при необходимости вручную изменять параметры инцидента перед отставкой;
- скачивать из приложения электронную форму инцидента в формате JSON для последующей пересылки в ФинЦЕРТ вручную.

«Пользовательский компонент» предоставляет пользователю интерфейс для просмотра инцидента и помогает выявлять и исправлять ошибки, которые могут мешать отставке инцидента в ФинЦЕРТ.

Основной сценарий работы с инцидентами в приложении состоит из следующих этапов:

- Приложение загружает инциденты в хранилище входных данных.
- Приложение конвертирует инциденты в формат, поддерживаемый ФинЦЕРТ, валидирует их и помещает в очередь на отправку.
- Если автоматическая отправка включена, и при конвертации не возникли ошибки, приложение отправляет инциденты в ФинЦЕРТ.
- При возникновении ошибок конвертации приложение отмечает соответствующим статусом инциденты, которые не удалось конвертировать, и помещает их в основное хранилище.
- Если необходимо (например, при возникновении ошибок), пользователь редактирует инциденты в интерфейсе приложения и после повторной автоматической валидации отправляет их в ФинЦЕРТ.
- Работу с успешно отправленными инцидентами можно продолжить в Личном кабинете участника ФинЦЕРТ. Переход в ЛКУ доступен из приложения.

#### 4.1 Вход в "Пользовательский компонент"

Перед входом в "Пользовательский компонент" запросите у администратора ИТ-инфраструктуры, в которой развернут «Пользовательский компонент», ссылку для входа в интерфейс приложения.

Чтобы войти в "Пользовательский компонент", в адресной строке браузера введите ссылку для входа в интерфейс приложения.

Откроется стартовая страница со списком инцидентов.

#### 4.2 Интерфейс

Рабочая область страницы содержит список инцидентов и панели отображения тела выбранного инцидента. По умолчанию в списке отображаются все инциденты, импортированные в "Пользовательский компонент". Вы можете изменять список отображаемых инцидентов, используя фильтры в панели фильтрации:

- **Отправленные.** Список содержит только отправленные в ФинЦЕРТ инциденты.
- **Неотправленные.** Список содержит только неотправленные в ФинЦЕРТ инциденты.

- **Готовые к отправке.** Список содержит только успешно импортированные в "Пользовательский компонент", но еще не отправленные в ФинЦЕРТ инциденты.
- **Все инциденты.** Список содержит все инциденты, импортированные в "Пользовательский компонент".

Для каждого инцидента отображается его идентификатор и статус. В приложении предусмотрены следующие статусы:

- **Готов к отправке** - инцидент успешно импортирован в приложение, но не отправлен в ФинЦЕРТ.
- **Отправляется** - инцидент отправляется в ФинЦЕРТ.
- **Отправлен** - инцидент успешно отправлен в ФинЦЕРТ.
- **Ошибка** - при импорте инцидента произошла ошибка.
- **Ошибка отправки** - при отправке инцидента произошла ошибка.

По умолчанию установлена отправка инцидентов в ФинЦЕРТ вручную. Вы можете установить автоматическую отправку.

Под списком инцидентов находится индикатор состояния "Пользовательского компонента". По кнопке вы можете просматривать информацию о текущем состоянии хранилища и сервисов приложения.

Вы можете изменять параметры неотправленных инцидентов в панели **Инциденты для отправки в ФинЦЕРТ**. Ниже отображается панель ошибок.

Панель **Исходный инцидент** содержит импортированные в приложение параметры инцидента. Эти параметры вы не можете изменять.

### 4.3 Работа с инцидентами

"Пользовательский компонент" обеспечивает отправку в ФинЦЕРТ инцидентов, обнаруженных в IT-инфраструктуре организации. По умолчанию включена отправка инцидентов вручную. Вы можете включить автоматическую отправку инцидентов. В автоматическом режиме приложение отправляет по пять готовых к отправке инцидентов каждые 10 секунд.

Если при импорте инцидента в приложение произошла ошибка, необходимо изменить инцидент в соответствии с сообщением в панели ошибок и отправить инцидент вручную.

Если ошибка произошла при отправке, необходимо проверить состояние работоспособности системы и отправить инцидент повторно.

Вы можете просматривать успешно отправленные инциденты в Личном кабинете Участника по кнопке Открыть в ФинЦЕРТ.

#### **4.3.1 Отправка инцидента**

Вы можете отправлять в ФинЦЕРТ только готовые к отправке инциденты.

Чтобы отправить в ФинЦЕРТ инцидент:

- Выберите инцидент.
- Нажмите кнопку «Отправить в ФинЦЕРТ».

Инцидент отправлен в ФинЦЕРТ.

#### **4.3.2 Изменение параметров инцидента**

Вы можете изменять параметры только неотправленных в ФинЦЕРТ инцидентов.

Чтобы изменить параметры инцидента:

- Выберите инцидент.
- В панели Инциденты для отправки в ФинЦЕРТ измените параметры.

Примечание. Если изменения некорректны, приложение отобразит сообщение в панели ошибок.

- Чтобы сохранить изменения в приложении, нажмите кнопку «Сохранить».
- Чтобы сохранить и отправить инцидент, нажмите кнопки «Сохранить» и «Отправить в ФинЦЕРТ».

Параметры инцидента изменены.

### 4.3.3 Скачивание электронной формы инцидента

Вы можете скачивать электронные формы инцидентов для отправки в ФинЦЕРТ в формате JSON. Такие электронные формы можно отправить в ФинЦЕРТ вручную через Личный кабинет Участника.

Чтобы скачать электронную форму:

- Выберите инцидент.
- Нажмите кнопку «Скачать JSON».

Электронная форма инцидента сохранена в локальную папку, указанную в свойствах браузера.

### 4.3.4 Удаление инцидента

Вы можете удалять инциденты со статусами «Готов к отправке», «Ошибка» и «Ошибка отправки». Инциденты будут удалены только из "Пользовательского компонента" и не будут импортированы повторно.

Чтобы удалить инцидент:

- Выберите инцидент.
- Нажмите кнопку «Удалить».

## 4.4 Трансформация инцидентов. Правила трансформации

Параметры инцидентов, поступающих в «Пользовательский компонент» от МР SIEM и других SIEM-систем по протоколу syslog, необходимо трансформировать в формат, поддерживаемый ФинЦЕРТ.

Трансформация инцидентов в формат ФинЦЕРТ выполняется с помощью правил трансформации. Правила трансформации содержатся в yaml-файлах, расположенных в папке *C:\Program Files\Positive Technologies\UserComponent\Transformation\rules*.

Один файл содержит правила трансформации для одного типа атаки или инцидента.

По умолчанию с «Пользовательским компонентом» поставляются файлы трансформации для следующих типов инцидентов:

- использование вредоносного программного обеспечения (malware) *syslogTOIncidentMalware.yaml*;
- атака типа «отказ в обслуживании» (ddosAttacks) *syslogTOIncidentDDos.yaml*;
- эксплуатация уязвимостей информационной инфраструктуры (vulnerabilities) *syslogTOIncidentVulnerability.yaml*.

Для инцидентов других типов можно создавать пользовательские правила трансформации на основе файлов, поставляемых по умолчанию.

Поддерживаются пользовательские правила трансформации для инцидентов следующих типов:

- изменение маршрутно-адресной информации (trafficHijackAttacks);
- несанкционированный доступ к банкоматам и платежным терминалам (atmAttacks);
- компроментация аутентификационных или учетных данных (bruteForces);
- спам-рассылка (spams);
- взаимодействие с центрами ботнетов (controlCenters);
- использование фишинговых ресурсов (phishingAttacks);
- размещение запрещенного контента в интернете (prohibitedContents);
- размещение вредоносного ресурса в интернете (maliciousResources);
- изменение контента (changeContent);
- сканирование портов (scanPorts);
- изменение IMSI на SIM-карте, смена IMEI телефона (sim);
- использование социальной инженерии (socialEngineering);
- иная компьютерная атака (other).

Описание всех известных системе типов атак и инцидентов содержится в файле *incident.yaml*, расположенном в папке *C:\Program Files\Positive Technologies\UserComponent\Transformation\rules\schemas\*.

После создания нового правила трансформации инцидента необходимо с помощью консольной утилиты JSONmake.exe создать инцидент нового типа и проверить работу

правила. Если правило написано верно, в интерфейсе приложения рядом с исходным инцидентом syslog будет показан результат трансформации — json-форма инцидента в формате АСОИ ФинЦЕРТ. С json-формой можно выполнять дальнейшие действия: редактировать, сохранять, отправлять в АСОИ ФинЦЕРТ.

Формат описания правил трансформации приведен в Приложении Б.

#### 4.5 Добавление правила трансформации

Чтобы добавить правило трансформации:

- Откройте файл C:\Program Files\Positive Technologies\UserComponent\Web\trasformation.json.
- Добавьте новый тип инцидента:

```
"<Значение параметра type, поступающее на порт syslog>":  
"<Наименование правила трансформации>"
```

Например, "atmAttacks: syslogToIncidentatmAttacks"

- Откройте папку C:\Program Files\Positive Technologies\UserComponent\Trasformation\rules.
- Скопируйте один из файлов по умолчанию (например, syslogToIncidentVulnerability.yaml), чтобы использовать его в качестве шаблона.
- Переименуйте файл в соответствии с названием типа инцидента.
- Например, syslogToIncidentatmAttacks.yaml
- Примечание. Имя файла может отличаться от наименования правила трансформации.
- Откройте созданный файл.
- Измените значение параметра description в соответствии с названием типа инцидента.
- Например, Правило трансформации syslog в инцидент FINCERT atmAttacks
- Для параметра name укажите наименование правила трансформации.
- Значение параметра name должно быть одинаковым со значением <Наименование правила трансформации>, заданным в файле trasformation.json.

## БКМД.62.01.12.545.ИЗ.3

- В блоке Полезная информация от syslog'a измените первый шаг в соответствии со структурой:

```
step: "Массив sources для <Название типа инцидента>"
```

```
operations:
```

```
- name: select
```

```
  args:
```

```
path: '$input.src'
```

```
- name: eval
```

```
  args:
```

```
command: "[{0}] if isinstance({0}, str) else {0}"
```

```
- name: eval
```

```
  args:
```

```
command: "[{{'ip': x}} for x in {0}]"
```

```
- name: insert
```

```
  args:
```

```
path: '$output.<Название типа инцидента>.sources'
```

- Измените все последующие шаги в блоке Полезная информация от syslog'a в соответствии со структурой:

```
- step: "Target для vulnerability (ip)"
```

```
- operations:
```

```
- - name: select
```

```
-   args:
```

```
-   path: "$input.dst"
```

```
- - name: insert
```

```
-   args:
```

```
-   path: '$output.vulnerability.target.ip'
```

Где:

**\$input.dst** имя поля, которое "Пользовательский компонент" ожидает получить посредством протокола syslog;

**\$output.vulnerability.target.ip** имя поля, в которое будет подставлено значение полученное в предыдущем поле.

Полный список всех доступных полей для каждого из типов атаки находится в файле *C:\Program Files\Positive Technologies\UserComponent\Transformation\rules\schemas\incident.yaml*.

Таким образом устанавливается связь между полями, поступающими посредством протокола syslog, и их преобразование в форматеJSON ФинЦЕРТ.

**Примечание.** Для корректной работы системы рекомендуется не изменять правила, описанные в блоке # Автозаполнение обязательных полей для создания инцидента # Общее для всех.

- В блоке Для <Наименование типа инцидента> измените значение параметра **value**.
- Параметр **value** должен содержать значение параметра type, поступающее на порт syslog.
- Сохраните файл.
- Перезапустите сервис PT.SP.UC.Transformation.

## **5 Ошибки**

### **5.1 Не открываются страницы приложений АСОИ ФинЦЕРТ**

В случае если приложения АСОИ ФинЦЕРТ не открываются в веб-браузере, выполните следующие действия:

- запустите отладчик браузера и активируйте запись сетевых запросов (клавиша F12, вкладка «Сеть») и выполните запрос к приложению. Зафиксируйте код ответа в столбце «Заголовок/Ответ»;
- направьте результаты, полученные на предыдущем шаге, на адрес электронной почты [svc\\_fincert\\_support@cbr.ru](mailto:svc_fincert_support@cbr.ru).

### **5.2 Ошибки в работе веб-интерфейсов приложений АСОИ ФинЦЕРТ**

К возможным ошибкам веб-интерфейсов приложений АСОИ ФинЦЕРТ относятся следующие ситуации:

- не работает переход между вкладками веб-приложения;
- не закрываются выпадающие или перекрывающие окна веб-интерфейса;
- пустые выпадающие списки или окна веб-интерфейса;
- не сохраняются вводимые значения в полях веб-интерфейсов;
- интерфейс не реагирует на действие пользователя.

В случае возникновения ошибок в работе веб-интерфейсов приложений АСОИ ФинЦЕРТ выполните перезагрузку страницы (F5) и повторите требуемые действия. Если данная ошибка возникает периодически, подготовьте максимально возможное описание (версия браузера, адрес страницы, описание ошибки) и направьте на адрес электронной почты [svc\\_fincert\\_support@cbr.ru](mailto:svc_fincert_support@cbr.ru).

### **5.3 Прочие ошибки и вопросы**

В случае возникновения иных ошибок или вопросов по работе АСОИ ФинЦЕРТ необходимо заполнить Типовую форму направления информации об

ошибке/сбое/проблеме АСОИ ФинЦЕРТ (Приложение Г) и направить ее на адрес электронной почты [svc\\_fincert\\_support@cbr.ru](mailto:svc_fincert_support@cbr.ru).

## **Приложение А**

### **Установка и настройка ПО**

#### **А.1 Общие сведения**

Перед началом работы необходимо:

- скачать дистрибутив «Средство криптографической защиты информации «Континент TLS-клиент. Версия 2» (далее — TLS-клиент) с сайта производителя ПО – ООО «Код Безопасности».
- получить от Центра:
  - а) учетные данные для доступа в АСОИ ФинЦЕРТ;
  - б) конфигурационный файл для TLS-клиента с настройками подключения к АСОИ ФинЦЕРТ;
  - в) документ БКМД.62.01.12.545.ИЗ.3. «Руководство Участника по работе с АСОИ ФинЦЕРТ»;
  - г) документ БКМД.62.01.12.545.ИЗ.9. «Регламент получения ключевой информации».
- присоединиться к Регламенту получения ключевой информации и получить в соответствии с ним в территориальном учреждении Банка России (ТУ БР) ключевую информацию, необходимую для работы с АСОИ ФинЦЕРТ.

#### **А.2 Требования к АРМ**

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

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<br>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):
  - а) Microsoft Edge;
  - б) Google Chrome версии не ниже 60;
  - в) Яндекс.Браузер версии не ниже 22;
  - г) Опера версии не ниже 83;
  - д) Chromium-Gost версии не ниже 99.
- одно из следующих СКЗИ для установки защищенного соединения с АСОИ ФинЦЕРТ (через браузер Опера версии не ниже 83, либо Яндекс.Браузер версии не ниже 22, либо Chromium-Gost версии не ниже 99):
  - а) КриптоПро CSP (при использовании браузера Chromium-Gost версии не ниже 99 и КриптоПро CSP 4.0 рекомендуется перейти на КриптоПро CSP 5.0);
  - б) VipNet CSP;
  - в) 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 34.10-2012 (с

использованием ГОСТ Р 34.11-2012), и планируется использовать только один из обозревателей: Opera версии не ниже 83, либо Яндекс.Браузер версии не ниже 22, либо Chromium-Gost версии не ниже 99.

### **A.3 Требования к подключению**

Для подключения к АСОИ ФинЦЕРТ на стороне Участника должно быть настроено:

- сетевые правила, разрешающие подключение по порту 443 к адресам:
  - а) portal.fincert.cbr.ru;
  - б) 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»;
- установлено СКЗИ для работы с АСОИ с ФИНЦЕРТ, соответствующее следующим требованиям:
  - а) поддержка реализации протокола TLS с ГОСТ 2012;
  - б) работа с браузерами, поддерживаемыми системой.

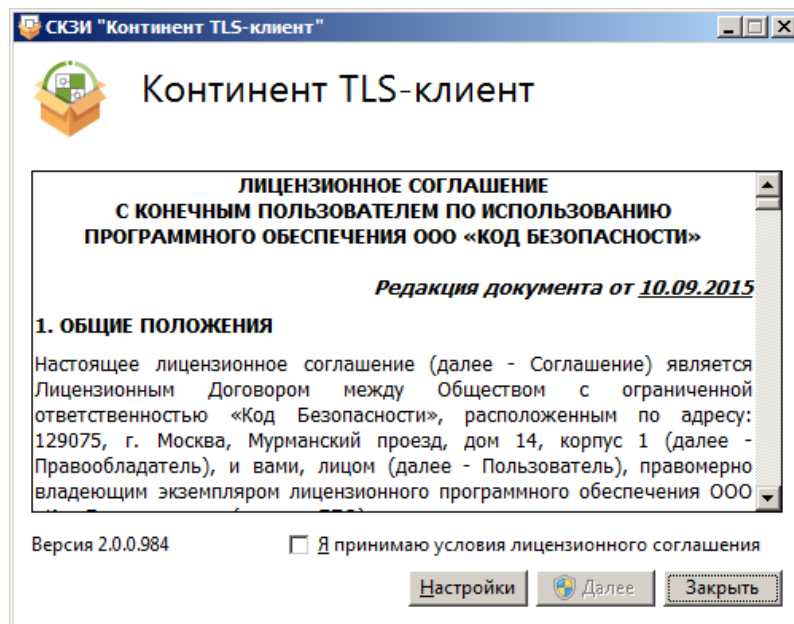
### **A.4 Установка и настройка TLS-клиента**

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

Для этого:

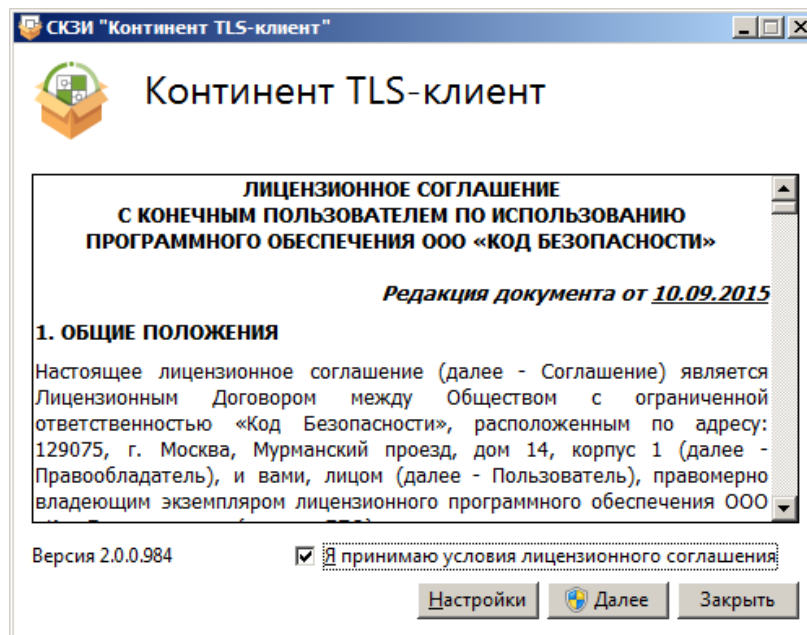
- 1) Перейдите на сайт <https://www.securitycode.ru>. Если есть учетная запись (аккаунт) на данном сайте – необходимо осуществить вход под своими логином и паролем.
- 2) Зайдите в раздел демоверсии: <https://www.securitycode.ru/products/demo-versions/>. Ссылка на этот раздел есть на главной странице сайта.
- 3) Если аккаунта на указанном сайте нет, то необходимо его создать, нажав кнопку «Регистрация».
- 4) В открывшемся окне заполнить форму регистрации.

- 5) После успешной регистрации и аутентификации под своими учетными данными, переходим в раздел демоверсии:  
<https://www.securitycode.ru/products/demo-versions/>
- 6) Запустите на исполнение файл Континент TLS-клиент.exe. На экране появится окно установки TLS-клиента с текстом лицензионного соглашения (Рисунок 41).



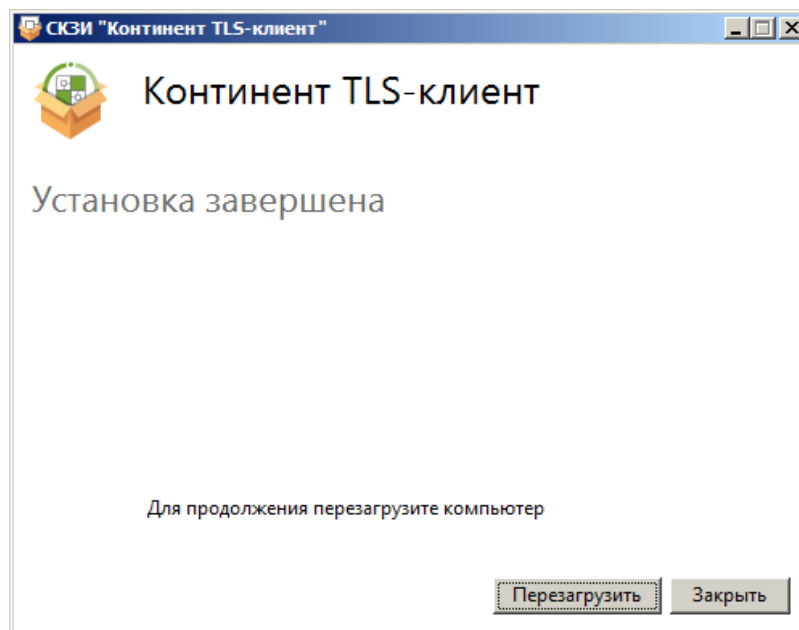
**Рисунок 41 – Лицензионное соглашение**

- 7) Прочтите лицензионное соглашение и, если вы принимаете его условия, поставьте отметку в поле «Я принимаю условия лицензионного соглашения», затем нажмите кнопку «Далее» (Рисунок 42).



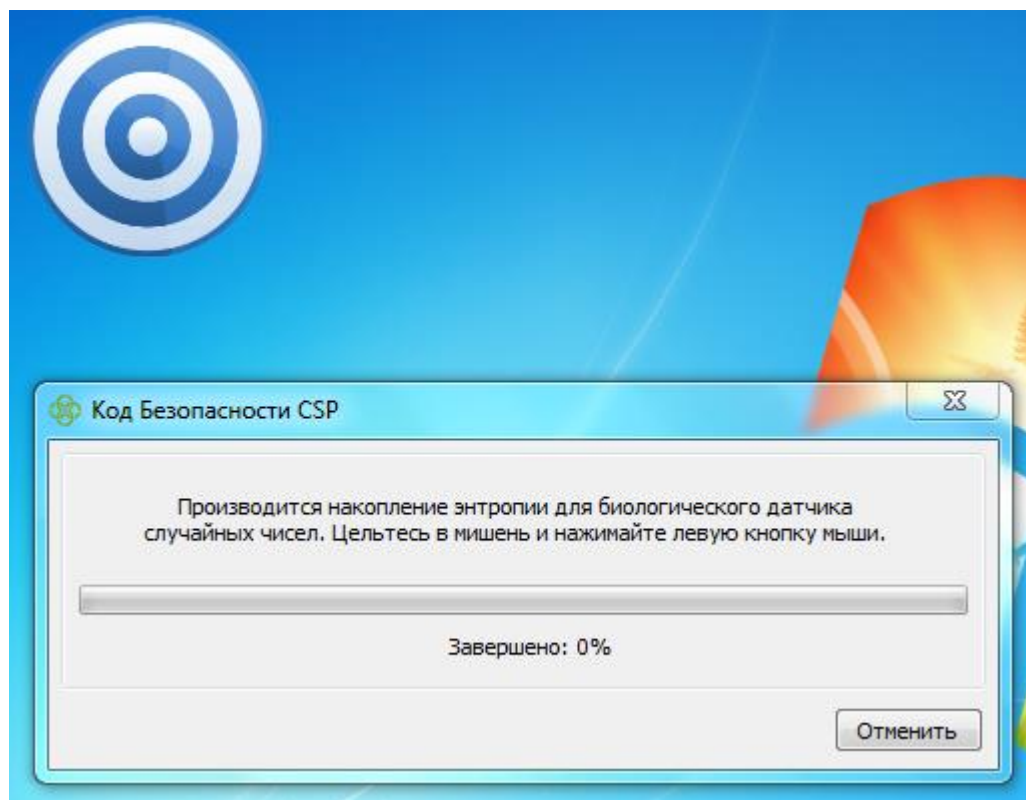
**Рисунок 42 – Продолжение установки после ознакомления с лицензионным соглашением**

- 8) Программа установки выполнит диагностику системы, после чего начнется установка ПО. После ее успешного завершения на экране появится сообщение о необходимости перезагрузки компьютера (Рисунок 43).



**Рисунок 43 – Завершение установки**

- 9) 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».
- 10) 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 44 **Ошибка! Источник ссылки не найден.**).

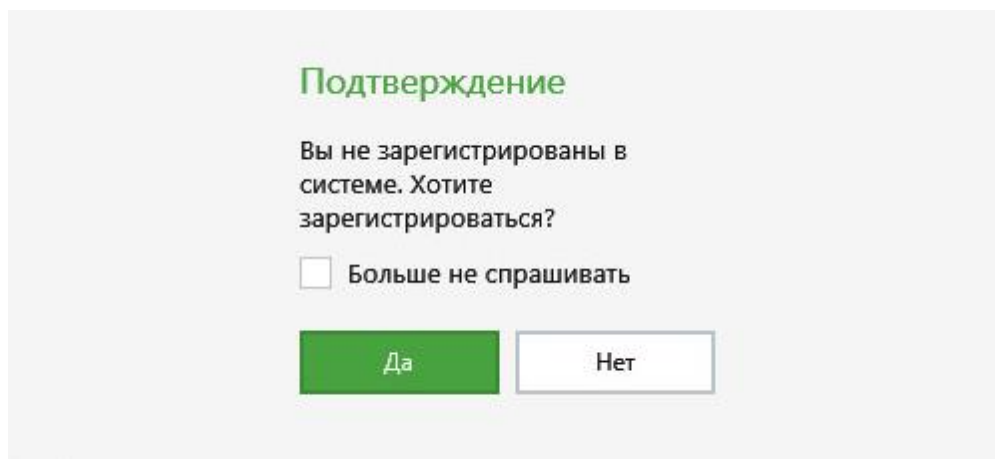


**Рисунок 44 – Накопление энтропии для биологического датчика случайных чисел**

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

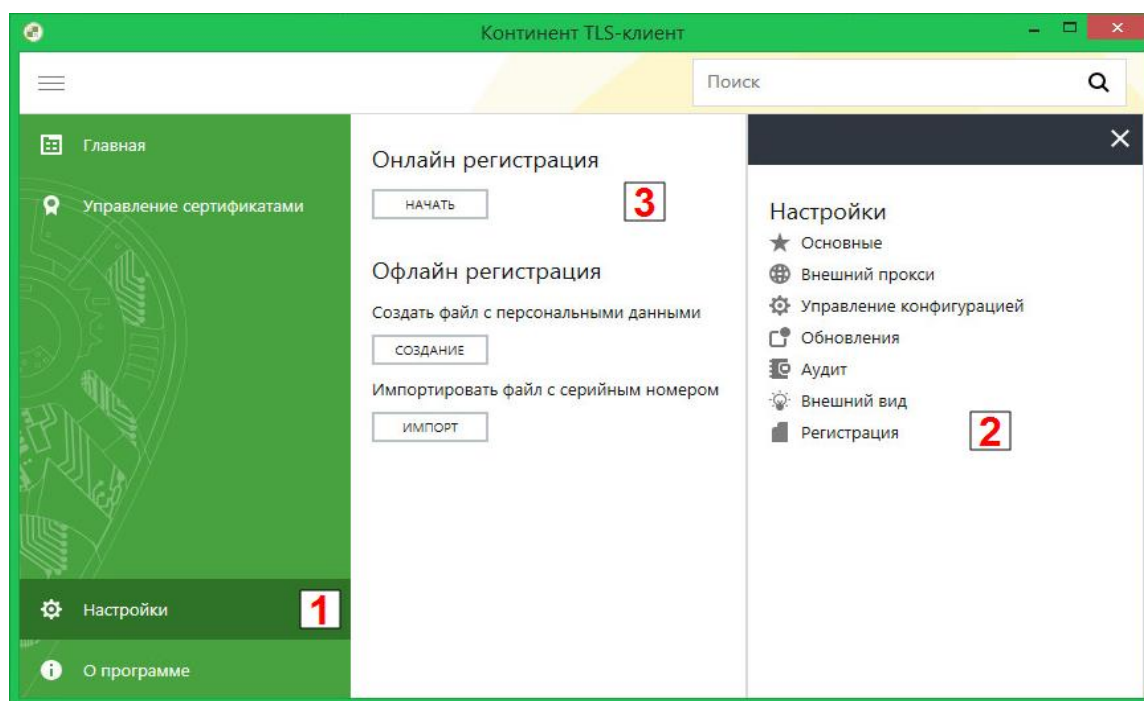
Для регистрации TLS-клиента необходимо выполнить следующие действия:

- 1) В открывшейся при запуске форме (Рисунок 45 **Ошибка! Источник ссылки не найден.**) нажать кнопку «Да».



**Рисунок 45 – 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 46).



**Рисунок 46 – Начало регистрации**

- 3) На экране появится диалоговое окно регистрации (Рисунок 47).

The screenshot shows a registration form with the following fields and options:

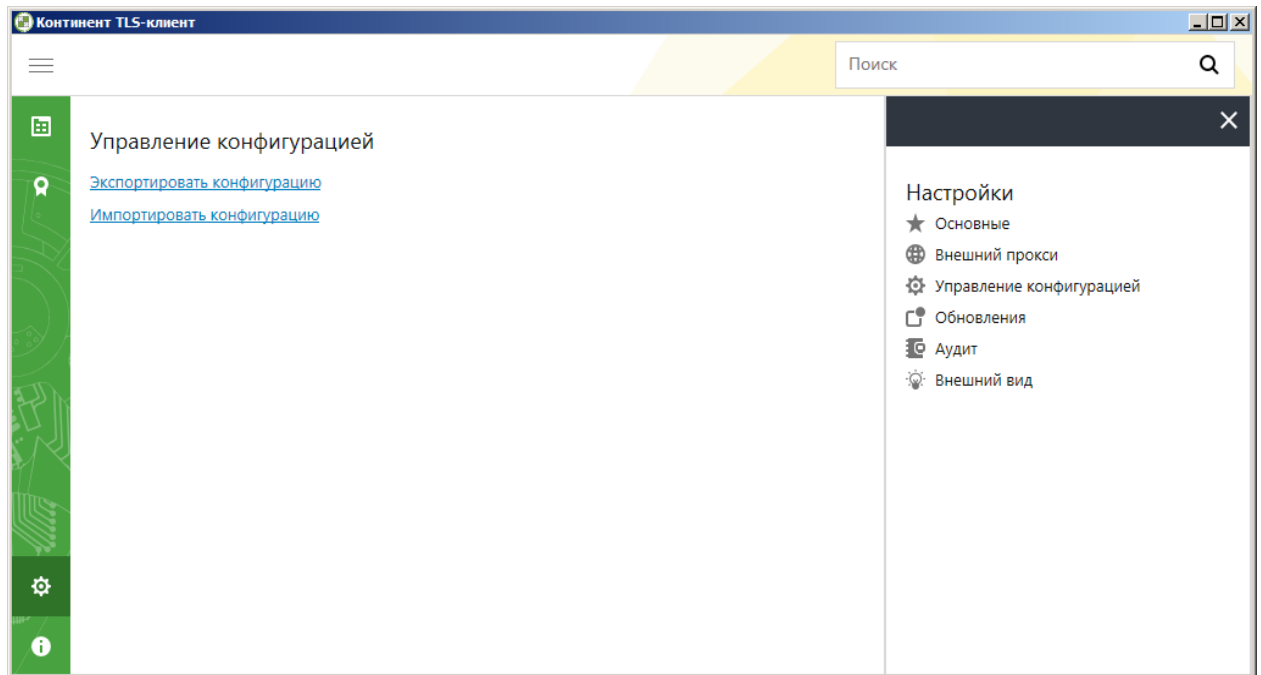
- Имя:** Text input field.
- Фамилия:** Text input field with placeholder text "Обязательное поле".
- Отчество:** Text input field.
- Электронная почта:** Text input field with placeholder text "Обязательное поле".
- Город:** Text input field.
- Организация:** Text input field.
- Отдел:** Text input field.
- Адрес сервера регистрации:** Text input field containing the value "registration.securitycode.ru".
- Radio buttons:** Two options, "КС1" (selected) and "КС2".
- Buttons:** "Готово" (dark grey) and "Отмена" (light grey).

**Рисунок 47 – Ввод регистрационных данных**

- 4) Введите требуемые параметры и нажмите кнопку «Готово». Адрес сервера регистрации и выбор «КС1» **не изменять**.
- 5) Начнется процесс регистрации и подключения к указанному серверу. При его успешном завершении на экране появится соответствующее информационное окно.

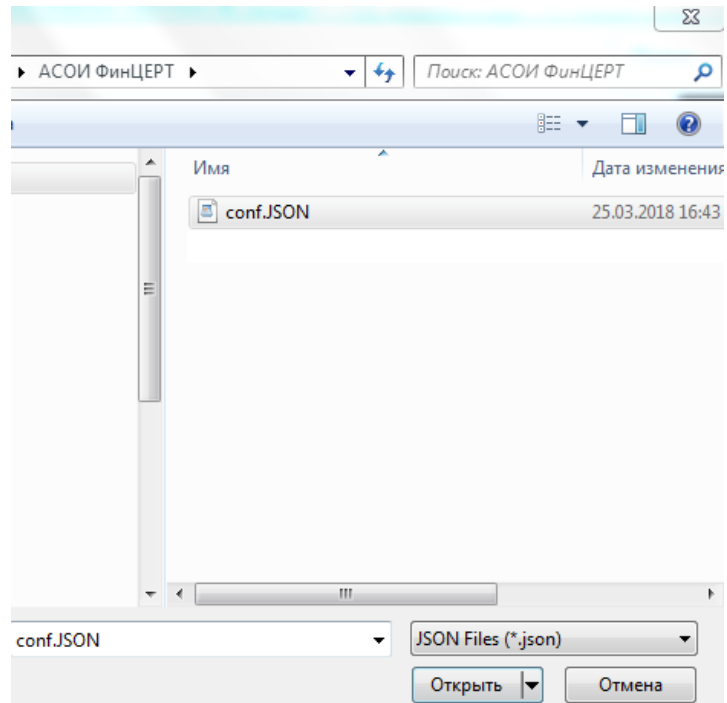
После установки и регистрации TLS-клиента необходимо:

- 1) Импортировать конфигурационный файл TLS-клиента `conf.json`, для этого необходимо:
  - а) запустить TLS-клиент на APM;
  - б) выбрать пункт «Настройки» - «Управление конфигурацией» (Рисунок 48);



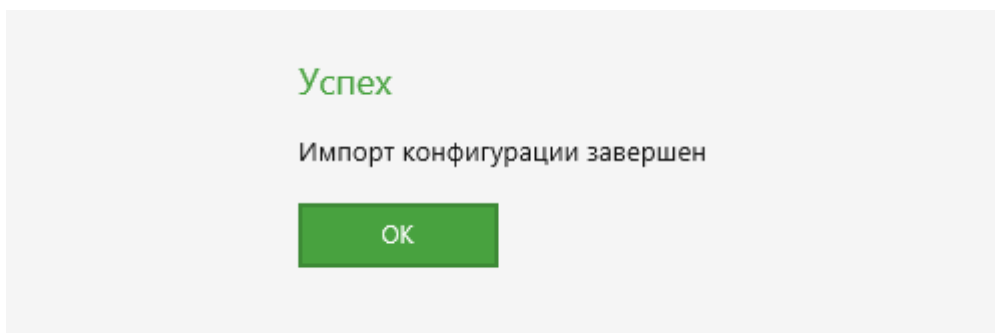
**Рисунок 48 – Загрузка файла конфигурации**

в) в левой части выбрать пункт «Импортировать конфигурацию».



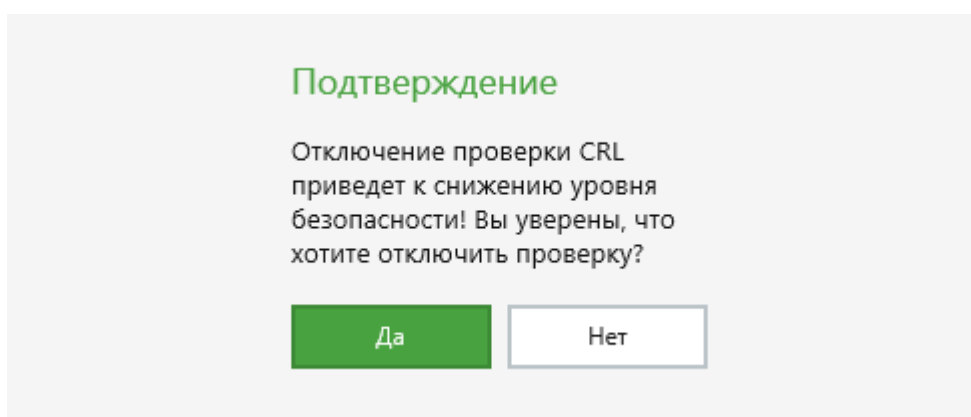
**Рисунок 49 – Выбор файла конфигурации**

- г) осуществить загрузку файла конфигурации.
- д) в случае успешной загрузки появится сообщение (Рисунок 50).




**Рисунок 50 – Успешный результат загрузки файла конфигурации**

- е) после нажатия кнопки «ОК» появится сообщение (Рисунок 51)



**Рисунок 51 – Сообщение об отключении проверки CRL**

- ж) подтвердить отключение проверки CRL, нажав кнопку «Да»
- 2) Если для доступа к сети Интернет используется прокси сервер, необходимо провести настройки программы для корректной работы с прокси сервером:
- а) в основном окне выберите пункт вызова настроек  и выберите в меню настроек пункт «Внешний прокси», после чего появится окно настроек (Рисунок 52 **Ошибка! Источник ссылки не найден.**), в котором

необходимо выбрать «Использовать внешний прокси-сервер», указать настройки для работы с прокси сервером и нажать кнопку «Сохранить».

Внешний прокси

☒ Использовать внешний прокси-сервер

Адрес:

Порт:

Исключения (адреса разделяются ";"):

Аутентификация:

**Рисунок 52 – Окно настройки параметров прокси-сервера в Континент-TLS**

- б) в веб-браузере укажите явные настройки прокси-сервера и добавьте в исключения адреса `portal.fincert.cbr.ru` и `lk.fincert.cbr.ru`, как показано на Рисунок 53 и Рисунок 54:

**Автоматическая настройка**  
 Чтобы использовать установленные вручную параметры, отключите автоматическую настройку.

☐ Автоматическое определение параметров

☐ Использовать сценарий автоматической настройки

Адрес:

**Прокси-сервер**

☒ Использовать прокси-сервер для локальных подключений (не применяется для коммутируемых или VPN-подключений).

Адрес:  Порт:

☐ Не использовать прокси-сервер для локальных адресов

Рисунок 53 – Окно настройки параметров прокси-сервера в веб-браузере

**Серверы**

| Тип        | Адрес прокси-сервера                      | Порт                            |
|------------|---|---------------------------------|
| 1. HTTP:   | <input type="text" value="адрес прокси"/> | <input type="text" value="80"/> |
| 2. Secure: | <input type="text" value="адрес прокси"/> | <input type="text" value="80"/> |
| 3. FTP:    | <input type="text" value="адрес прокси"/> | <input type="text" value="80"/> |
| 4. Socks:  | <input type="text"/>                      | <input type="text"/>            |

☒ Один прокси-сервер для всех протоколов

**Исключения**

☒ Не использовать прокси-сервер для адресов, начинающихся с:

Адреса разделяются точкой с запятой (;).

Рисунок 54 – Окно настройки исключений для прокси-сервера в веб-браузере

3) Настройте режим работы контроля целостности:

- а) запустите программу «Контроль целостности», для этого выберите в главном меню Windows пункт «Все приложения| Код Безопасности |Контроль целостности» (Рисунок 55);

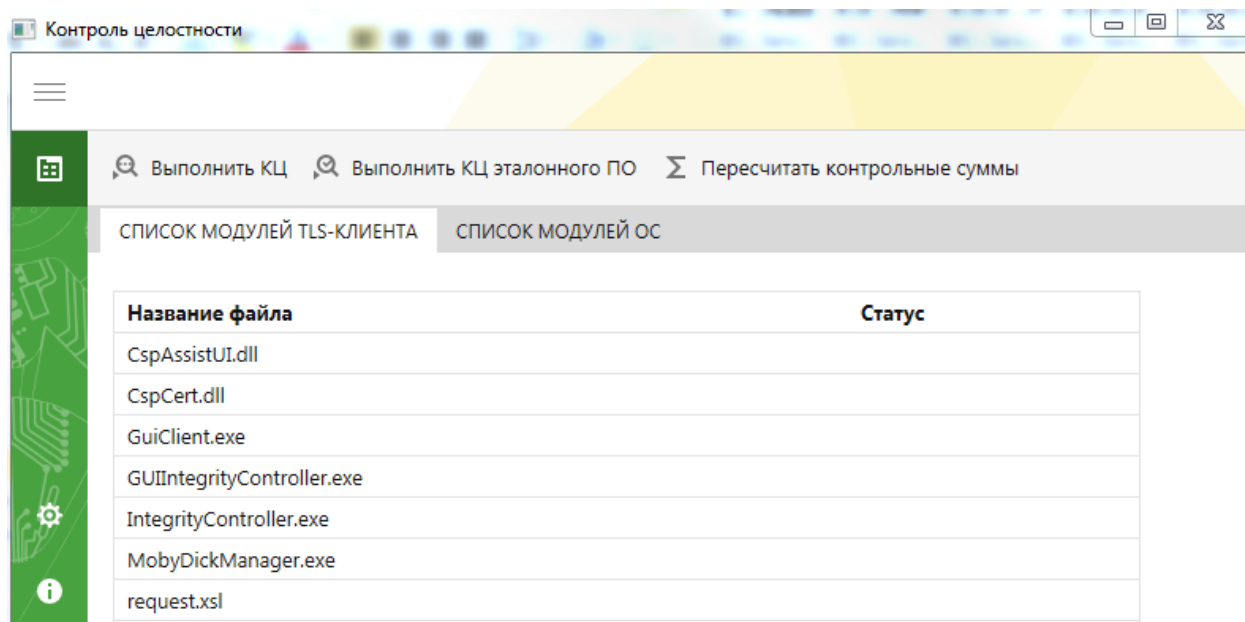



Рисунок 55 – Главное окно программы «Контроль целостности»

- б) в основном окне выберите пункт вызова настроек . На экране появится текущее расписание регламентных проверок (Рисунок 56 **Ошибка! Источник ссылки не найден.**). В открывшемся окне выберите «Разрешить работу при повреждении системных файлов», выбор данной настройки необходим для корректной работы при обновлении операционной системы.

Расписание проверок контроля целостности

Начало в  ч.  мин.

Дни недели:

☐ Пн ☐ Вт ☐ Ср ☐ Чт ☐ Пт ☐ Сб ☒ Вс

Режим работы

☒ Разрешить работу при повреждении системных файлов

**Рисунок 56 – Настройка режима работы контроля целостности**


## **А.5 Создание запроса для сертификата Клиента TLS**

Пользователь с помощью ПО «Код Безопасности Client TLS» формирует запрос на сертификат Клиента TLS. В момент формирования запроса создается контейнер с закрытым ключом, который помещается на защищенный носитель, затем сформированный запрос передается на ПК ЦС ключевой системы СКАД «Сигнатура» - ИАС Территориального Учреждения ЦБ РФ.

Для создания запроса с помощью ПО «Код Безопасности Client TLS»:

- 1) В главном меню TLS-клиента необходимо выбрать пункт «Управление сертификатами».
- 2) В области отображения информации появится раздел пользовательских сертификатов.
- 3) Нажмите на вкладке пользовательских сертификатов кнопку «Создать запрос». На экране появится диалог для ввода параметров запроса.

×

←  Запросить сертификат

### Параметры сертификата пользователя

Заполните обязательные поля для выпуска запроса сертификата пользователя.  
В полях "Область, край" и "Город" должны быть указаны полные официальные названия без сокращений.

Полное имя:

Описание:

Электронная почта:

Организация:

Подразделение:

Снилс:

ИНН:

ОГРН:

Город:

Область, край:

Страна, регион:

**Рисунок 57 – Формирование запроса на сертификат**

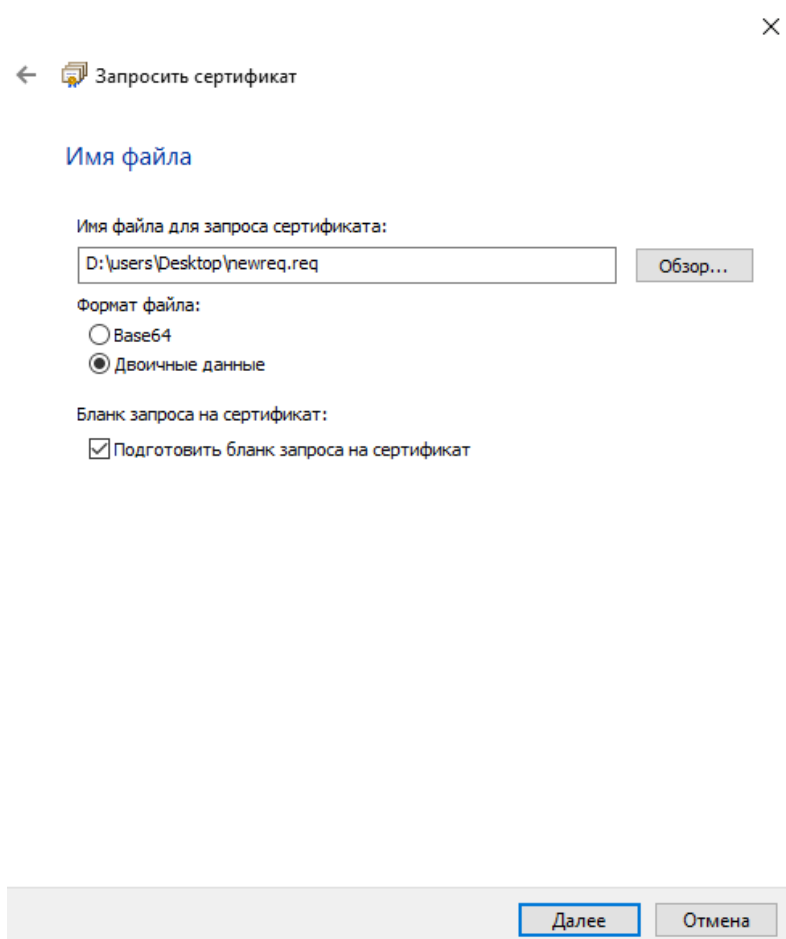
- 4) Заполните параметры запроса в соответствии с документом «Правила заполнения полей и применения ключей проверки ЭП» и нажмите кнопку «Далее». Обязательные поля должны быть заполнены в соответствии со следующей таблицей:

Таблица 2 - Заполнение обязательных полей

| Значение          | Длина поля в символах,<br>не более |
|-------------------|------------------------------------|
| Полное имя        | 64                                 |
| Электронная почта | 128                                |
| Организация       | 64                                 |
| Подразделение     | 64                                 |

|   |     |
|---|-----|
| Город   | 128 |
| Область, край                                     | 128 |
| Страна/Регион (задается двумя латинскими буквами) | 2   |

- 5) В открывшемся окне настроек свойств поставщика служб шифрования оставьте параметры, предлагаемые по умолчанию, и нажмите кнопку «Далее».
- 6) В окне настроек имени файла укажите требуемое место сохранения запроса (путем нажатия кнопки «Обзор...»), выберите двоичный формат файла (запрос будет создан в DER-кодировке).



**Рисунок 58 - Задание параметров для сохранения запроса на сертификат**

На экране появится завершающий диалог мастера запроса сертификата.

- 1) Проверьте корректность введенных параметров и нажмите кнопку «Готово».

- 2) Далее для создания запроса потребуется генерация набора случайных чисел. Если используется датчик ПАК «Соболь», набор энтропии выполняется автоматически и на экране не отображается. Перейдите к п.12.
- 3) В противном случае на экране появится окно, предназначенное для накопления энтропии.
- 4) Следуйте указаниям инструкции на экране и дождитесь завершения набора энтропии. По окончании этой процедуры на экране появится диалог запроса пароля на доступ к контейнеру.
- 5) Дважды введите пароль, с помощью которого будет защищен доступ к закрытому ключу, хранящемуся в создаваемом контейнере, и нажмите кнопку «ОК».

На экране появится окно выбора ключевого носителя.

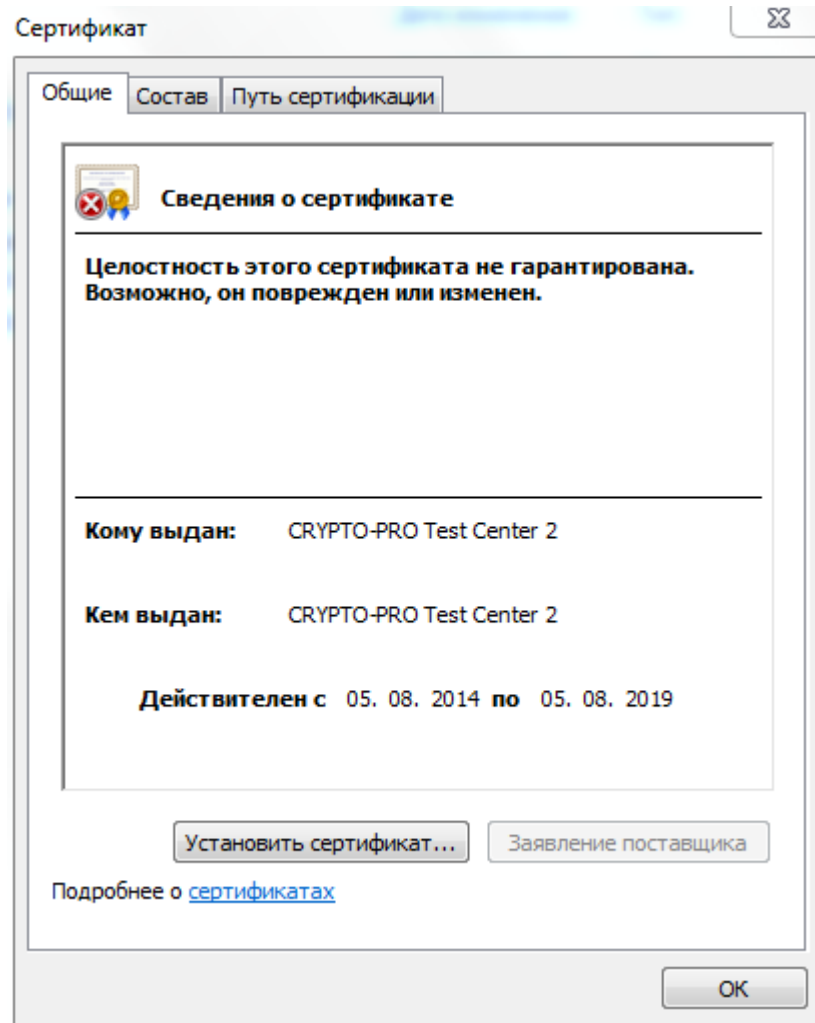
- 1) Выберите нужный ключевой носитель (по умолчанию указывается «Реестр Windows») и нажмите кнопку «ОК».
- 2) Начнется создание запроса и криптографического контейнера. После успешного завершения операции на экране появится соответствующее информационное сообщение.

Нажмите кнопку «ОК» и извлеките носитель.

Установка полученного от ТУ БР сертификата Клиента TLS осуществляется в соответствии с разделом А.8.

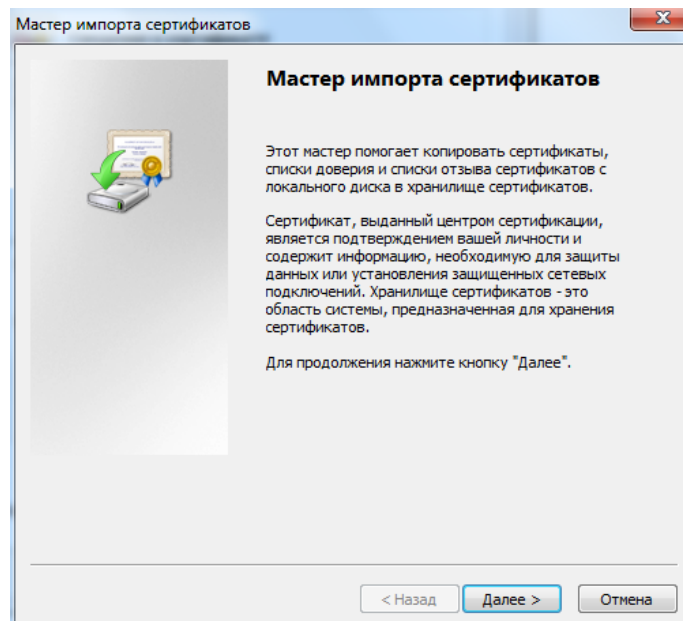
## **А.6 Установка сертификата корневого Центра сертификации**

Для установки сертификата корневого Центра сертификации (ЦСк) необходимо открыть файл сертификата ЦСк, полученный ранее от ТУ БР в составе комплекта ключевой информации и в открывшемся окне нажать кнопку «Установить сертификат» (Рисунок 59).



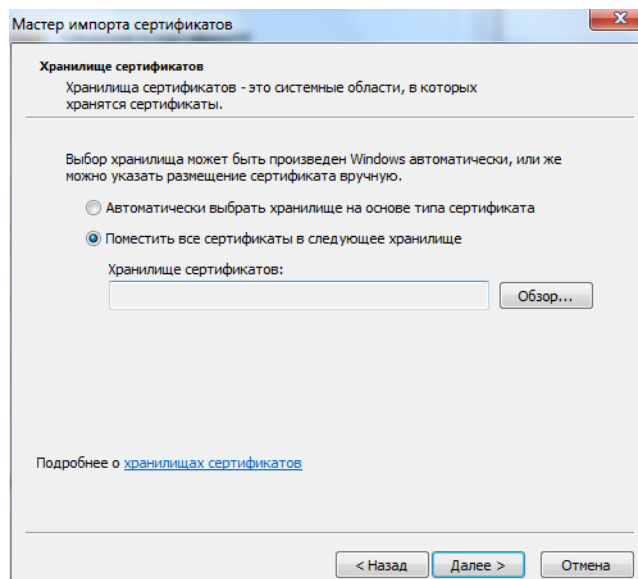
**Рисунок 59 – Успешный результат открытия файла с корневым сертификатом удостоверяющего центра**

В открывшемся окне мастера импорта сертификатов нажать кнопку «Далее» (Рисунок 60).



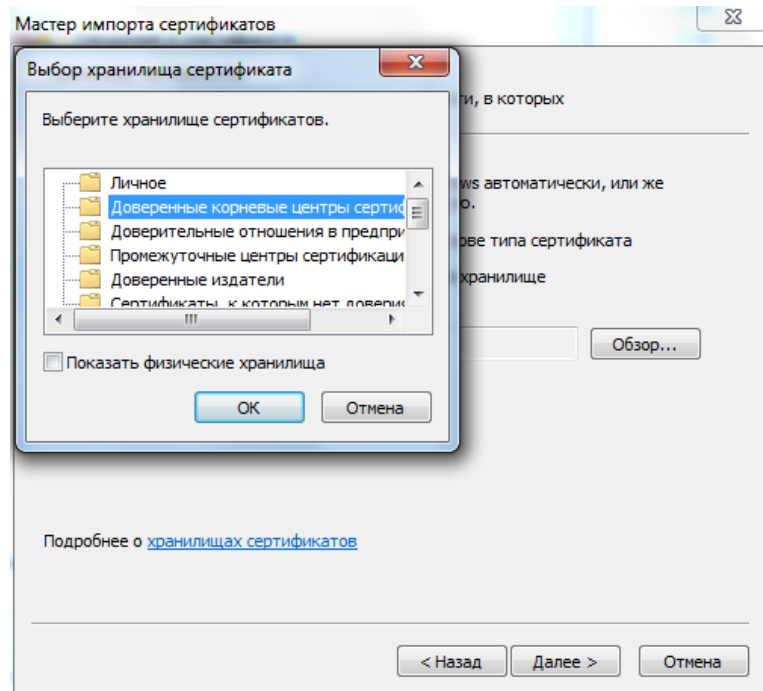
**Рисунок 60 – Окно запуска мастера импорта сертификатов**

В открывшемся окне необходимо выбрать пункт «Поместить все сертификаты в выбранное хранилище» и нажать кнопку «Обзор» (Рисунок 61).



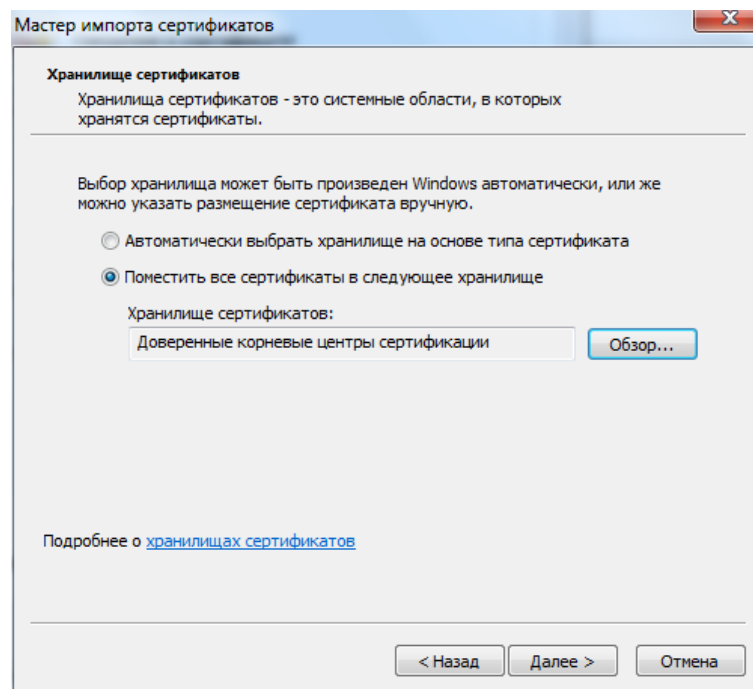
**Рисунок 61 – Мастер импорта сертификатов – выбор хранилища сертификатов**

В открывшемся окне необходимо выбрать пункт «Доверенные корневые центры сертификации» и нажать кнопку «ОК» (Рисунок 62).



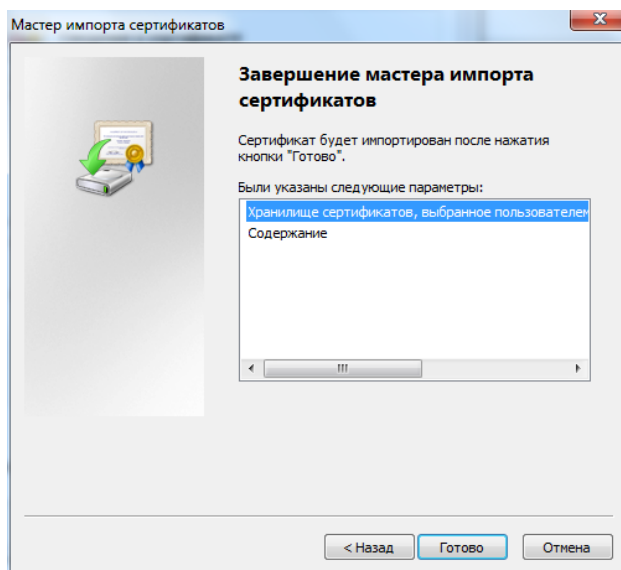
**Рисунок 62 – Мастера импорта сертификатов «Доверенные корневые центры сертификации»**

В появившемся окне необходимо нажать кнопку «Далее» (Рисунок 63).



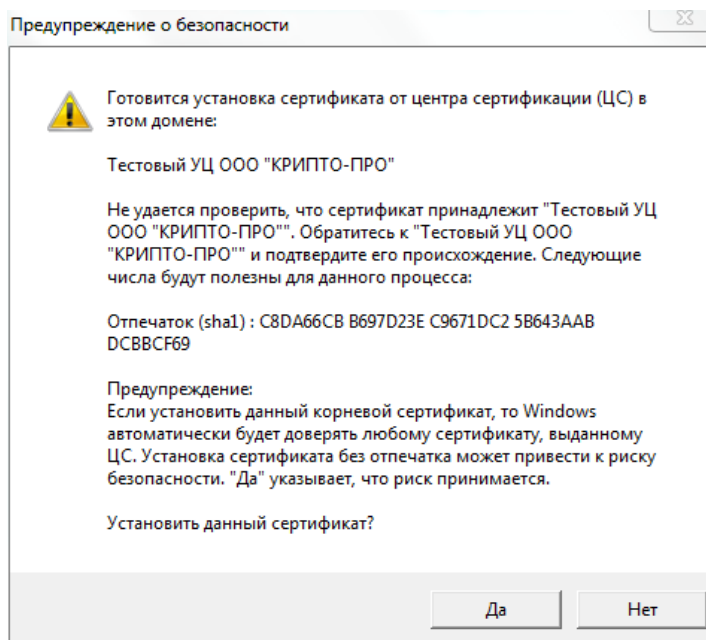
**Рисунок 63 – Мастер импорта сертификатов «Доверенные корневые центры сертификации»**

В появившемся окне необходимо нажать кнопку «Далее» (Рисунок 64).



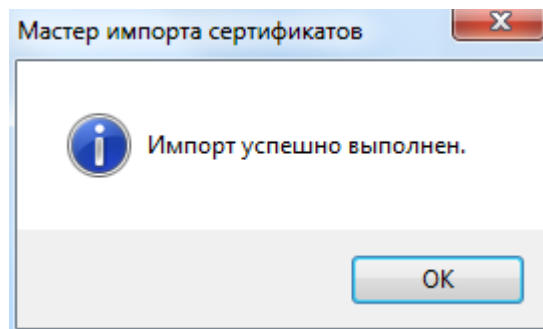
**Рисунок 64 – Мастер импорта сертификатов – Завершение мастера импорта сертификатов**

В появившемся окне необходимо нажать кнопку «Готово», после чего должно появиться сообщение, в котором необходимо нажать кнопку «Да» (Рисунок 65).



**Рисунок 65 – Предупреждение при установке сертификата**

При успешном импорте сертификата появится окно, в котором необходимо нажать кнопку «ОК» (Рисунок 66).



**Рисунок 66 – Сообщение об успешном импорте сертификата**

## **А.7 Установка сертификата промежуточного Центра сертификации**

Для установки сертификата промежуточного Центра сертификации (ЦСП) необходимо открыть файл сертификата ЦСП, полученный ранее от ТУ БР в составе комплекта ключевой информации и в открывшемся окне нажать кнопку «Установить сертификат».

Процедура установки ЦСП аналогична процедуре установки ЦСК, за исключением того, что при выборе хранилища сертификатов необходимо выбрать пункт «Промежуточные центры сертификации».

## **А.8 Установка сертификата пользователя Участника**

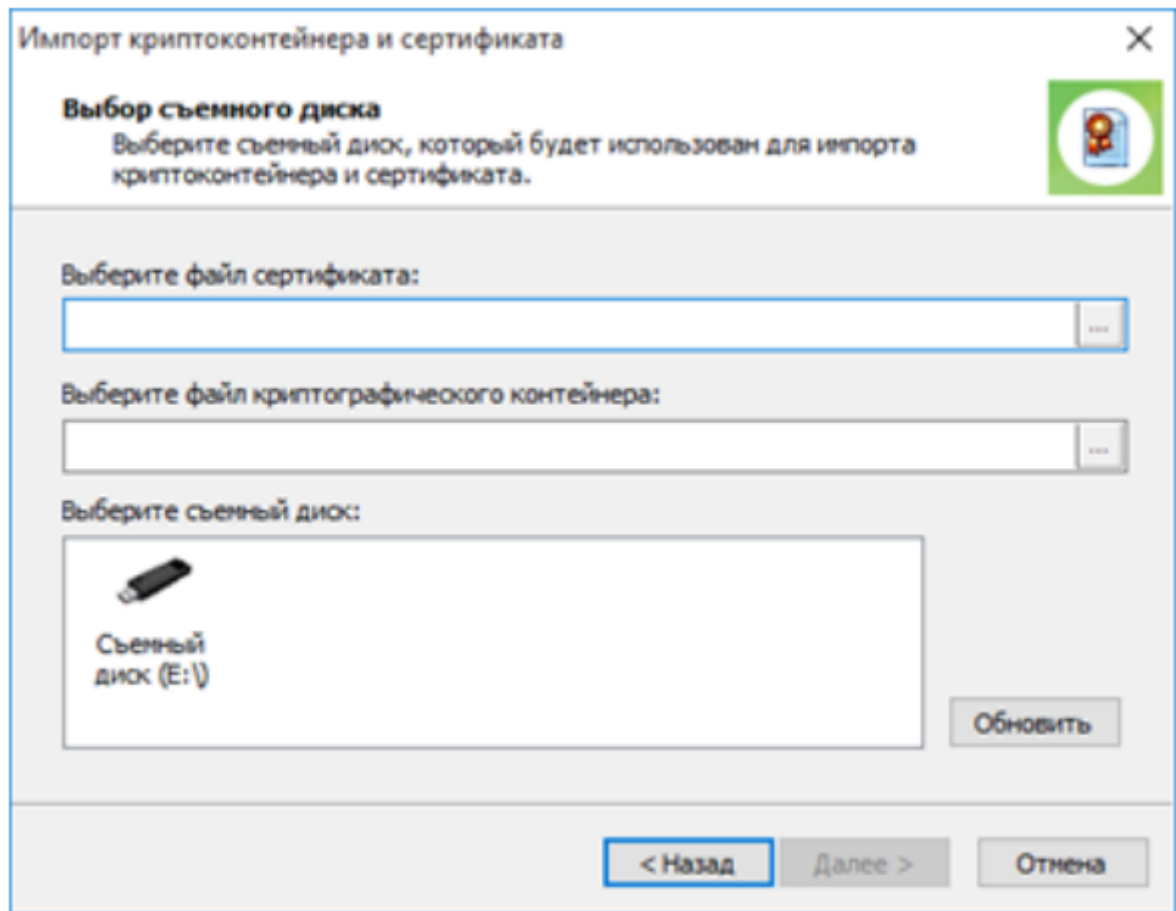
Для установки сертификата TLS-клиента, полученного от ТУ БР по сформированному ранее запросу, выполните следующие действия:

- 1) Вставьте USB-флеш-накопитель с записанным на нем сертификатом пользователя Участника TLS-клиента в свободный USB-разъем.
- 2) В основном окне программы нажмите кнопку «Импортировать...».

На экране появится стартовый диалог программы-мастера.

- 3) Нажмите кнопку «Далее».

На экране появится диалог для ввода параметров запроса (Рисунок 67):



**Рисунок 67 - Окно диалог для ввода параметров запроса**

4) Укажите местонахождение имеющихся файлов:

- а) в поле «Выберите файл сертификата» - полный путь к файлу с расширением .cer, содержащему сертификат пользователя;
- б) в поле «Выберите файл криптографического контейнера» —полный путь к файлу с расширением .p15 (или .p15\_backup для резервной копии), содержащему закрытый ключ данного сертификата пользователя.

5) Нажмите кнопку «Далее».

На экране появится диалог для ввода пароля.

6) Введите пароль доступа к выбранному криптографическому контейнеру и нажмите кнопку «Далее».

Будет выполнена проверка соответствия друг другу выбранных файлов сертификата и криптографического контейнера. Если указан неверный пароль или

криптографический контейнер не соответствует сертификату, на экране появится сообщение об этом.

При успешном завершении проверки начнется импорт сертификата. По окончании этой процедуры на экране появится диалог с перечнем выполненных действий.

- 7) Извлеките носитель из USB-разъема и нажмите кнопку "Готово".

## А.9 Установка сертификата веб-ресурсов АСОИ ФинЦЕРТ

Для получения доступа к веб-ресурсам АСОИ ФинЦЕРТ необходимо добавить полученный ранее от ТУ БР в составе комплекта ключевой информации сертификат веб-ресурсов. Для этого необходимо:

- 1) в главном окне программы перейти на вкладку «Управление сертификатами» и выбрать «Импортировать» (Рисунок 68 **Ошибка! Источник ссылки не найден.**);

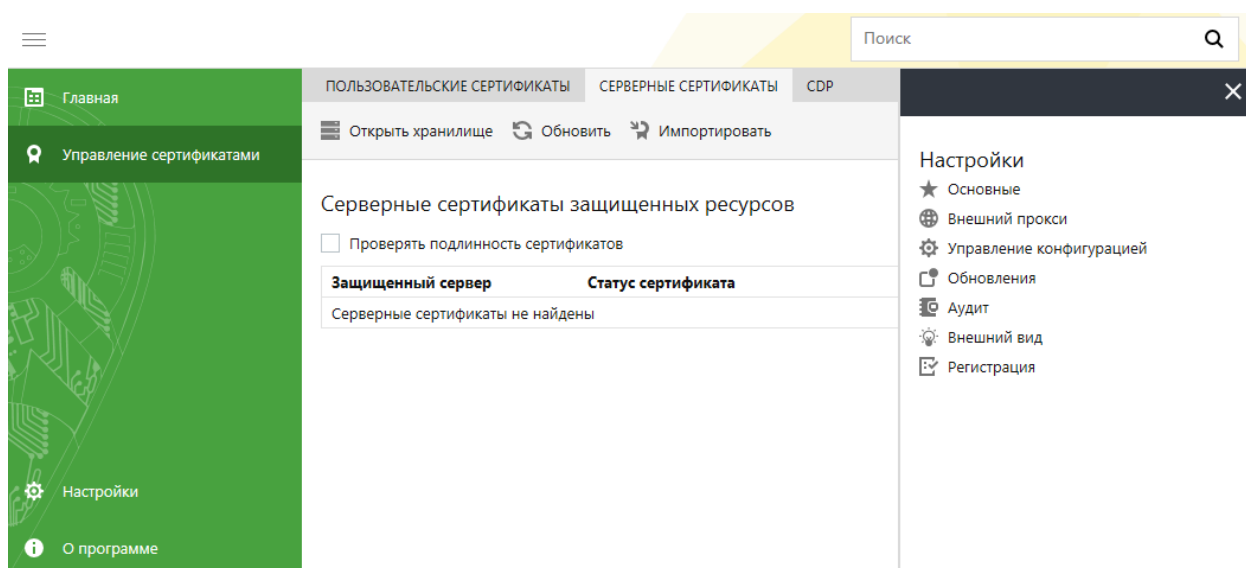


Рисунок 68 – Окно «Управление сертификатами»

- 2) в открывшемся окне выбора файлов выбрать файл сертификата веб-ресурса и нажать кнопку «Открыть»;
- 3) добавленный сертификат будет отображен в списке «Серверные сертификаты» (Рисунок 69 **Ошибка! Источник ссылки не найден.**).

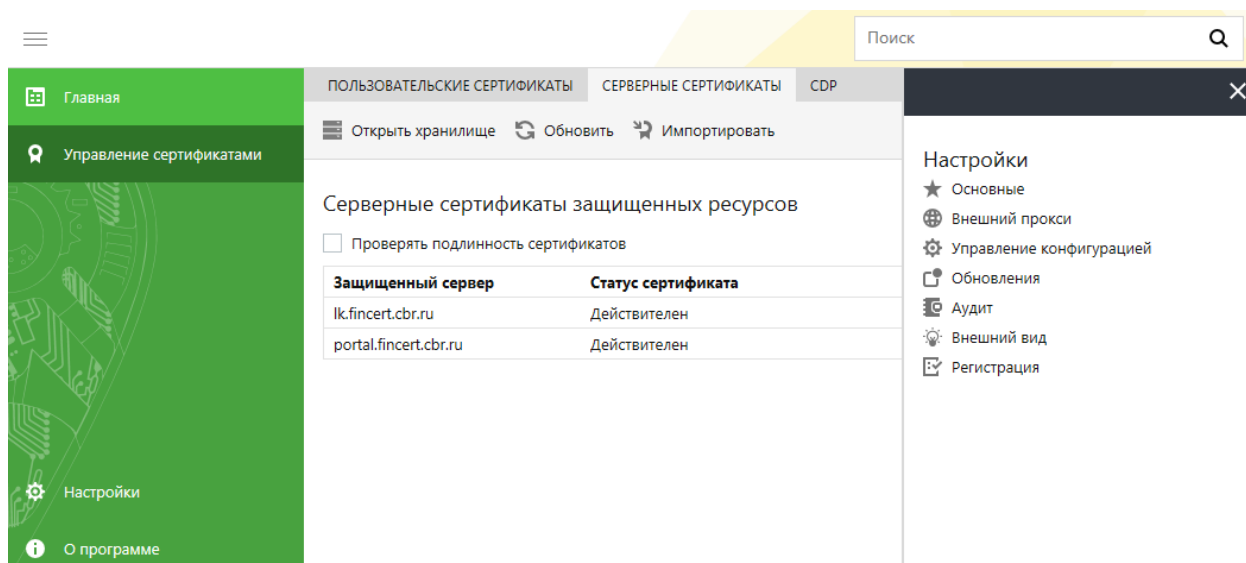


Рисунок 69 – Окно «Управление сертификатами-Серверные сертификаты»

## А.10 Загрузка списков отозванных сертификатов

Т.к. ЦС Банка России не имеют внешних точек распространения СОС, СОС Клиента TLS передаются из ТУ БР и требуют ручной загрузки в хранилище Клиента TLS.

Для установки СОС в СКЗИ «Континент TLS-клиент» необходимо выполнить следующие действия:

- 1) в главном окне программы перейти на вкладку «Управление сертификатами» и выбрать «CDP» (Рисунок 70);

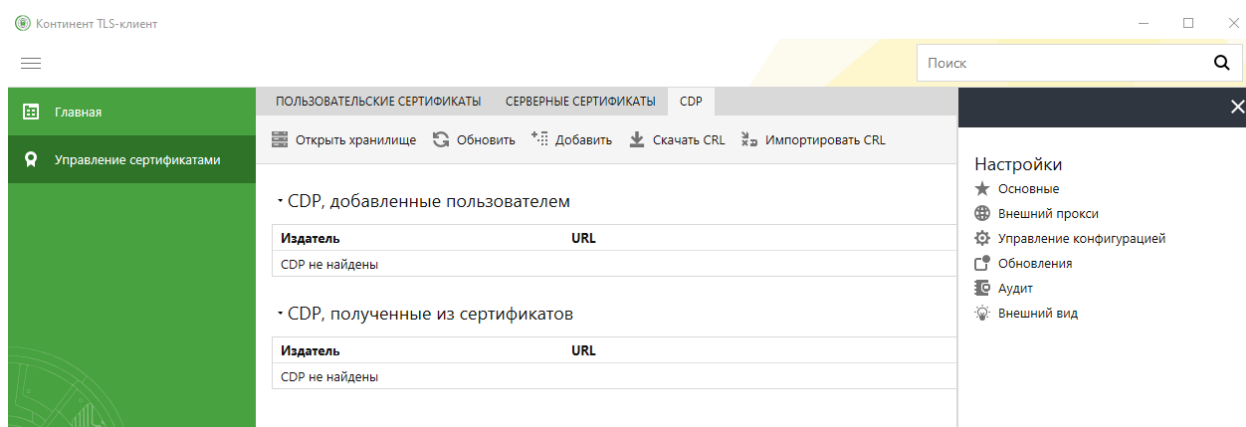
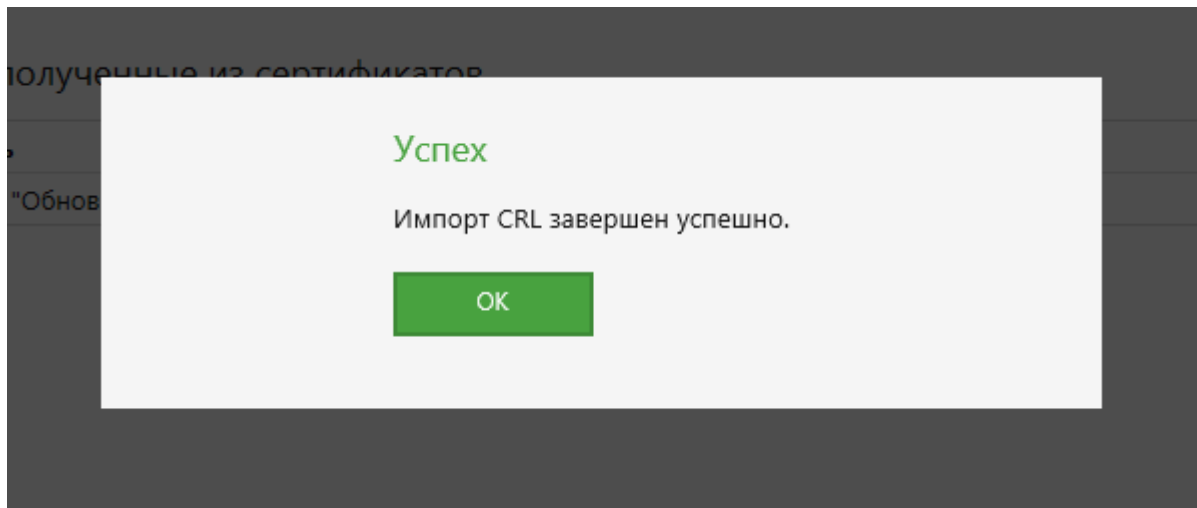


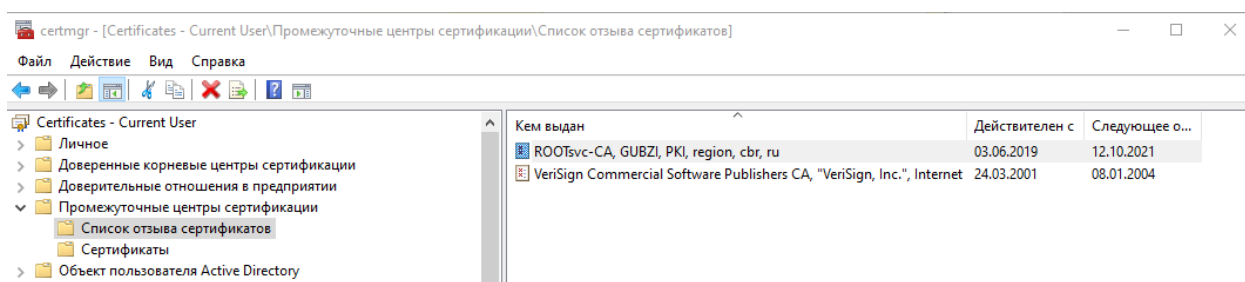
Рисунок 70 - Окно "CDP"

- 2) в открывшемся окне выбора файлов выбрать «Импортировать CRL» и выбрать файл СОС, полученный ранее от ТУ БР. будет сообщено об успешном импорте СОС (Рисунок 71);



**Рисунок 71 - Результат импорта СОС**

- 3) добавленный сертификат будет отображен в списке «Список отзыва сертификатов» при нажатии на кнопку «Открыть хранилище» в интерфейсе СКЗИ «Континент TLS-клиент» (Рисунок 72).



**Рисунок 72 - Список «Список отзыва сертификатов»**

## Приложение Б

### Формат описания правил трансформации

Правила трансформации позволяют конвертировать параметры инцидентов, которые поступают от SIEM, в формат, поддерживаемый ФинЦЕРТ.

Правила трансформации расположены в папке C:\Program Files\Positive Technologies\UserComponent\Transformation\rules. Каждому типу инцидентов соответствует отдельный файл, содержащий правила трансформации.

Таблица 3 – Формат описания правил трансформации

| Элемент структуры |         | Описание и значение  |
|-------------------|---------|--|
| description:      |         | <Описание правила трансформации>   |
| name:             |         | <"Наименование правила трансформации"><br><br>Значение этого параметра должно соответствовать значению в файле C:\Program Files\Positive Technologies\UserComponent\Web\trasformation.json |
| input:            |         |  |
|                   | type:   | deserialiser   |
|                   | name:   | json   |
| output:           |         |  |
|                   | type:   | serialiser   |
|                   | name:   | json   |
|                   | type:   | validator  |
|                   | name:   | json   |
|                   | schema: | incident.yaml  |

|  |                                  |  |
|--|----------------------------------|--|
|  | definitions:                     | definitions.IncidentPayload  |
|  | transformations:                 | Правила трансформации  |
|  | #Полезная информация от syslog'a | Этот блок содержит правила трансформации для необязательных параметров инцидента. Необходимо указать все параметры типа инцидента, которые содержатся в файле C:\Program Files\PositiveTechnologies\UserComponent\Transformation\rules\schemas\incident.yaml |
|  | step:                            | "Массив sources для <Название типа инцидента>"   |
|  | operations:                      |  |
|  | name:                            | select   |
|  | args:                            |  |
|  | path:                            | '\$input.src'  |
|  | name:                            | eval   |
|  | args:                            |  |
|  | command:                         | "[{{ 'ip': x }} for x in {0}]"   |
|  | name:                            | insert   |
|  | args:                            |  |
|  | path:                            | '\$output.<Наименование типа инцидента>.sources'   |
|  | step:                            | <"Наименование шага"><br><br>Количество шагов зависит от количества параметров типа инцидента. Каждому параметру должен соответствовать отдельный шаг  |

|  |        |  |
|--|--------|--|
| operations:  |        |  |
|  | name:  | select   |
|  | args:  |  |
|  | path:  | '\$input.<Наименование исходного параметра, поступающего от SIEM>'   |
|  | name:  | insert   |
|  | args:  |  |
|  | path:  | '\$output.<Наименование параметра ФинЦЕРТ>'<br><br>Наименование параметра ФинЦЕРТ должно соответствовать наименованию, указанному в файле<br><br>C:\Program Files\PositiveTechnologies\UserComponent\Transformation\rules\schemas \incident.yaml |
| # Автозаполнение обязательных полей для создания инцидента<br><br># Общее для всех |        | Этот блок содержит правила трансформации для обязательных параметров инцидентов. Для корректной работы системы рекомендуется не изменять эти правила   |
| step:  |        | "Registration (department). Структурное подразделение прописывается здесь, в поле value."  |
| operations:  |        |  |
|  | name:  | insert   |
|  | args:  |  |
|  | path:  | "\$output.registration.department"   |
|  | Value: | 'department'   |

|             |        |  |
|-------------|--------|--|
| step:       |        | "Damage"                                 |
| operations: |        |  |
|             | name:  | insert                                   |
|             | args:  |  |
|             | path:  | "\$output.lawEnforcementRequest.request" |
|             | value  | "UNKW"                                   |
| step:       |        | "ServiceType"                            |
| operations: |        |  |
|             | name:  | insert                                   |
|             | args:  |  |
|             | path:  | "\$output.serviceType"                   |
|             | value: | []                                       |
| step:       |        | "Description"                            |
| operations: |        |  |
|             | name:  | insert                                   |
|             | args:  |  |
|             | path:  | "\$output.description"                   |
|             | value  | "This incident created by UC (syslog)"   |
| step:       |        | "Location"                               |
| operations: |        |  |
|             | name:  | insert                                   |

|             |       |  |
|-------------|-------|--|
|             | args: |  |
|             | path: | "\$output.location"                            |
| step:       |       | "Assistance"                                   |
| operations: |       |  |
|             | name: | insert   |
|             | args: |  |
|             | path: | "\$output.assistance"                          |
|             | value | "NND"  |
| step:       |       | "VectorCode"                                   |
| operations: |       |  |
|             | name: | insert   |
|             | args: |  |
|             | path: | "\$output.vectorCode"                          |
|             | value | "INT"  |
| step:       |       | "Classification typeOfIncident (захардкожено)" |
| operations: |       |  |
|             | name: | insert   |
|             | args: |  |
|             | path: | "\$output.classification.typeOfIncident"       |
|             | value | "MTR"  |
| step:       |       | "Classification INT(захардкожено)"             |

|                                 |        |   |
|---------------------------------|--------|---|
| operations:                     |        |   |
|                                 | name:  | insert  |
|                                 | args:  |   |
|                                 | path:  | "\$output.classification.INT"                         |
|                                 | value  | []  |
|                                 | name:  | append  |
|                                 | args:  |   |
|                                 | path:  | "\$output.classification.INT"                         |
|                                 | value  | {"events": "MTR-UA", "typeOfIntruder": "INT_ORG"}     |
| # Для <Название типа инцидента> |        |   |
| step:                           |        | "Type"  |
| operations:                     |        |   |
|                                 | name:  | insert  |
|                                 | args:  |   |
|                                 | path:  | "\$output.typeOfAttack"                               |
|                                 | Value: | "Значение параметра type, поступающее на порт syslog" |

## Приложение В

### Описание программного прикладного интерфейса (REST API) работы с электронной подписью

#### В.1 Работа с электронной подписью

Для работы с электронной подписью электронных форм необходимо обращаться по адресу:

- <https://crypto-api.fincert.cbr.ru> – для работы с API ЭП ЗПЭ;
- <https://zoe-crypto-api.fincert.cbr.ru> – для работы с API ЭП ЗОЭ.

##### В.1.1 Подпись электронной формы

###### - HEADERS

a) 'Authorization'

###### - REQUEST

```
POST /api/dss/sign HTTP/1.1

Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryO9ByYds3HRdmsuWz

Content-Length: 339

-----WebKitFormBoundaryO9ByYds3HRdmsuWz

Content-Disposition: form-data; name="file1"; filename="test.json"

Файл на подпись

-----WebKitFormBoundaryO9ByYds3HRdmsuWz

Content-Disposition: form-data; name="file2"; filename="test_2.json"

Файл на подпись

-----WebKitFormBoundaryO9ByYds3HRdmsuWz

Content-Disposition: form-data; name="info";

{"login":"Ivanov_i_i","pincode":"pincode"}

-----WebKitFormBoundaryO9ByYds3HRdmsuWz--
```

###### - REQUEST PARAMS

a) Данные json:

1) login – логин пользователя dss

2) pincode – пин-код

б) Данные о файлах:

1) name – должно содержать порядковый номер файла вложения и иметь формат «fileN»; для json-объекта, содержащего информацию о подписанте name="info";

2) filename – должно содержать имя файла с указанием расширения.

#### – RESPONSE

```
HTTP/1.0 200 OK

{"filename1": " test.json.sig",
 "file1": " MIIJlQYJKoZIhvcNAQcCoIIJEjCCCQ4CAQEhD...MBgGCCqFAwOBawEBEGwwMDc3MDIy",
 "filename2": " test_2.json.sig",
 "file2": "
3k7zTG7z0SS+5o/dil6T3eSQybLiuZVgcE991...fYXEuF4DxVC8W3sX9if1IHVug3XjjZUoH60"}
```

#### – RESPONSE PARAM

а) filename – имя подписанного файла;

б) fileN – содержимое подписанного файла в кодировке Base64.

#### – ERRORS

```
HTTP/1.0 400 BAD REQUEST

{
  "Message": "invalid_pin"
}
```

## **В.1.2 Проверка подписи электронной формы**

#### – HEADERS

а) 'Authorization'

#### – REQUEST

```
POST /api/dss/verify HTTP/1.1

Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryO9ByYds3HRdmsuWz

Content-Length: 339

-----WebKitFormBoundaryO9ByYds3HRdmsuWz

Content-Disposition: form-data; name="file1"; filename="test.json.sig"
```

## БКМД.62.01.12.545.ИЗ.3

Файл на проверку

-----WebKitFormBoundaryO9ByYds3HRdmsuWz

Content-Disposition: form-data; name="file2"; filename="test\_2.json.sig"

Файл на проверку

-----WebKitFormBoundaryO9ByYds3HRdmsuWz--

## – REQUEST PARAMS

### а) Данные о файлах:

- 1) name – должно содержать порядковый номер файла и иметь формат «fileN»;
- 2) filename – должно содержать имя файла с указанием расширений.

## – RESPONSE

HTTP/1.0 200 OK

{"file1":

"2AgEBAgEAMB0GA1UdJQQWMBQGCCsGAQUFB...MCBggrBgEFBQcDBDAnBgkrBgEEAYI3FQoEGjAYMAo

GCCsGAQUFBwMCMAoGCCsGAQUFBwM"} }

## – RESPONSE PARAM

### а) fileN – результат проверки файла N;

## – ERRORS

HTTP/1.0 400 BAD REQUEST

{"Error": "Файл подписи имеет неверный формат. Убедитесь, что данные в файле

имеют кодировку Base64 (с/без заголовками) или переданы бинарные данные.

Ошибка: [Встречено неверное значение тега ASN1]. Код: [0x8009310b]. "}

## Приложение Г

### Типовая форма направления информации об ошибке/сбое/проблеме АСОИ ФинЦЕРТ

| Описание ошибки/проблемы/сбоя | Дата фиксации<br>(ГГГГ-ММ-ДД) | Время<br>(ЧЧ:ММ) |
|-------------------------------|-------------------------------|------------------|
|                               |                               |                  |

|  |                    |                         |
|--|--------------------|-------------------------|
| <b>Место возникновения (выделить знаком «+» или «V»)<br/>(обязательное поле)</b> |                    |                         |
| <b>Прод (ЗПЭ, рабочий ресурс)</b>  |                    |                         |
| <b>ЛКУ</b>   | <b>инф. портал</b> | <b>Другой компонент</b> |
|  |                    |                         |
| <b>Тест (ЗОЭ, тестовый ресурс)</b>   |                    |                         |
| <b>ЛКУ</b>   | <b>инф. портал</b> | <b>Другой компонент</b> |
|  |                    |                         |

| <b>Контактные данные лица обнаружившего ошибку</b> |  |
|--|--|
| Организация  |  |
| ФИО  |  |
| e-mail   |  |
| тел.   |  |

| <b>Описание ошибки/проблемы/сбоя</b>                            |   |
|---|---|
| <b>Как проявляется ошибка?<br/>(обязательное поле)</b>          | <i>Какие возникают сообщения об ошибке, какой функционал недоступен, какое действие не получается выполнить...</i>  |
| <b>Скриншоты ошибки<br/>(обязательное поле)</b>                 | <i>Приложить скриншоты (снимки) с интерфейса программы с возникшей ошибкой.</i>   |
| <b>Дополнительные сведения</b>                                  | <i>REQ-_____ - _____<br/>Номер запроса в АСОИ ФинЦЕРТ, сообщение об ошибке, фрагмент лога и т.п.</i>  |
| <b>Какие действия пользователя/оператора приводят к ошибке?</b> | <i>Описать последовательность действий для возможности повторения ошибки, либо сообщить о нерегулярном характере проявления ошибки и указать в этом случае сопутствующие условия...</i> |
| <b>Действия оператора ФинЦЕРТ по проверке ошибки</b>            | <i>Участником обмена не заполняется</i>   |

| Параметры рабочего компьютера            |                                     |                         |             |
|--|-------------------------------------|-------------------------|-------------|
| Тип операционной системы                 | Наименование и версия браузера      | Наименование (тип) СКЗИ | Версия СКЗИ |
| <i>Microsoft Windows 10 Professional</i> | <i>Google Chrome, 70.0.3538.110</i> | <i>Континент TLS</i>    | <i>56.2</i> |

| Дополнительная информация об ошибке/проблеме/сбое  |
|--|
| <p><i>В это поле включается вся дополнительная информация, которую участник считает необходимым сообщить по данной ошибке/проблеме/сбое</i></p> <ul style="list-style-type: none"><li><i>- прикладываются файлы любого формата, касающиеся ошибки/проблемы/сбоа, в том числе из e-mail</i></li><li><i>- в случае проблемы, связанной с почтовой рассылкой от имени АСОИ ФинЦЕРТ, необходимо приложить историю переписки и <u>обязательно</u> исходные письма в формате *.msg</i></li><li><i>- описывается дополнительная информация, не вошедшая в вышеописанные поля</i></li><li><i>-</i></li></ul> |

## Перечень принятых сокращений

| Сокращение     | Полное наименование  |
|----------------|--|
| TLS            | Transport Layer Security   |
| CVSS           | Common Vulnerability Scoring System  |
| АРМ            | Автоматизированное рабочее место   |
| АС             | Автоматизированная система   |
| АСОИ           | Автоматизированная система обработки инцидентов  |
| ПО             | Программное обеспечение  |
| ФинЦЕРТ, Центр | Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Департамента информационной безопасности Банка России |

[illegible]