Центральный Банк Российской Федерации
(Банк России)

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБРАБОТКИ ИНЦИДЕНТОВ ФИНЦЕРТ БАНКА РОССИИ

Руководство Участника по работе с АСОИ ФинЦЕРТ

На 92 листах

2019

Аннотация

.

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

Содержание

Перечень иллюстраций

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, см. п. 2), 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.
- через сообщение электронной почты с формами обмена информацией:

Формы обмена информацией в формате JSON можно также отправлять через ЛК в виде вложений к сообщениям (см. п. 2.5.2).

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

- реальные данные об инцидентах информационной безопасности в организациях банковской системы РФ – участниках информационного обмена;
- тестовые (имитационные) данные об инцидентах информационной безопасности в организациях банковской системы РФ – участниках информационного обмена. При внесении тестовых данных необходимо помечать их заголовки и темы символом «***». Тестовые (имитационные) данные должны в максимальной мере соответствовать информации, которую предполагается заполнять участнику информационного обмена (по структуре, форматам, наполнению и т.д.). Запросы, содержащие тестовые (имитационные) данные, не обрабатываются операторами ФинЦЕРТ.

Порядок установки и настройки программного обеспечения, необходимого для работы с АСОИ ФинЦЕРТ, приведен в Приложение 1.

2 Работа с Личным кабинетом Участника

Для доступа к АСОИ ФинЦЕРТ необходимо:

- При работе с Континент TLS-клиент:
  - запустить Континент TLS-клиент;
  - запустить один из поддерживаемых АСОИ ФинЦЕРТ обозревателей:
    - Microsoft Edge;
    - Microsoft Internet Explorer версии не ниже 11;
    - Google Chrome версии не ниже 60.
- При работе с КриптоПро CSP
  - запустить обозреватель Microsoft Internet Explorer версии не ниже 11 или Microsoft Edge.

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).

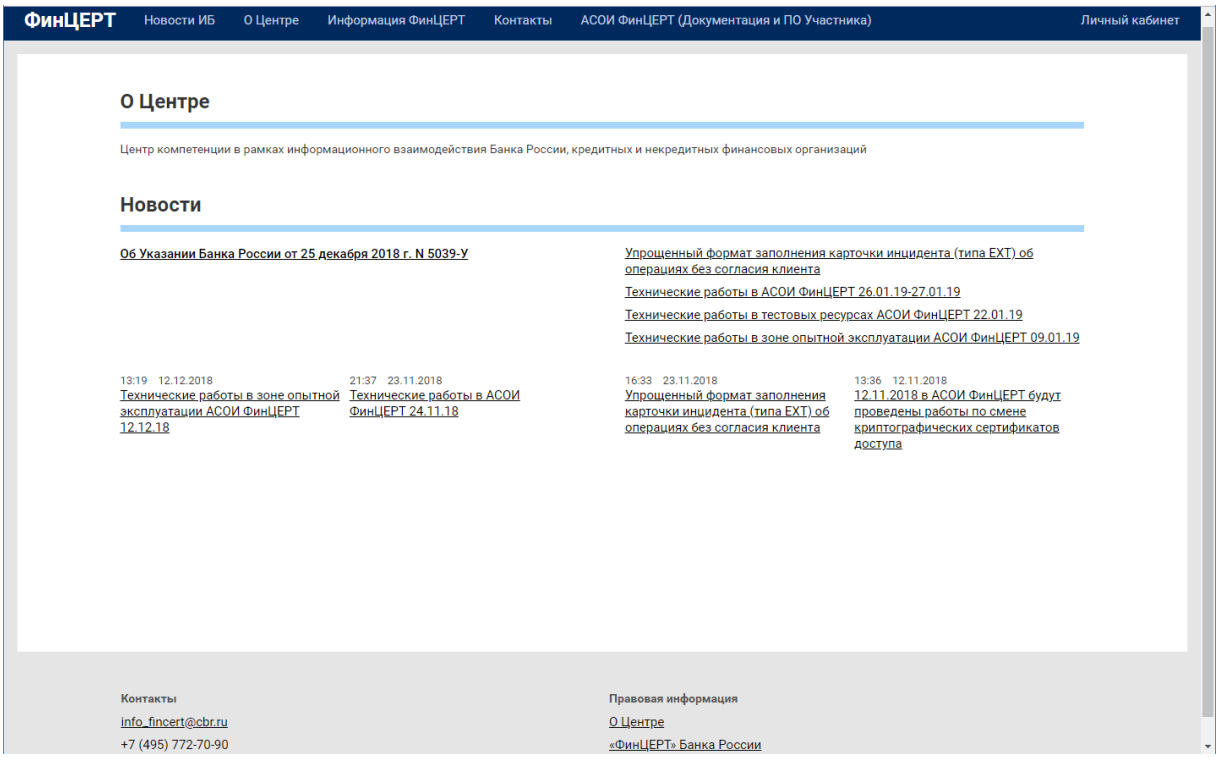


Рисунок 1 – Стартовая страница портала

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

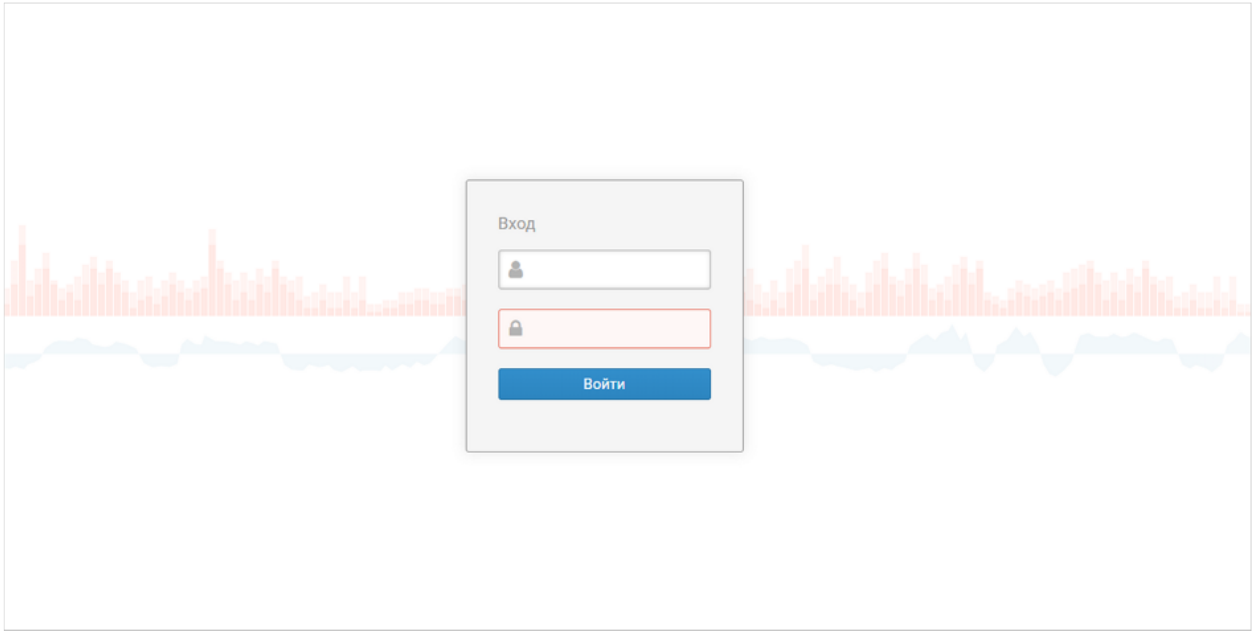


Рисунок 2 – Вход в личный кабинет Участника

- В поле Логин введите логин учетной записи.
- В поле Пароль введите пароль вашей учетной записи.
- 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):

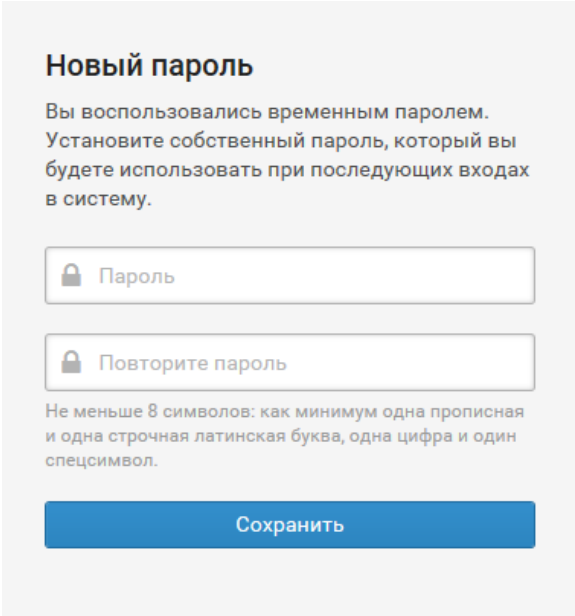


Рисунок 3 – Окно смены пароля первого входа

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

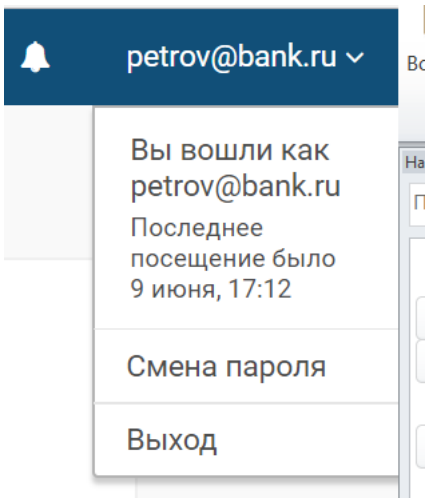


Рисунок 4 - Переход в личный кабинет

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

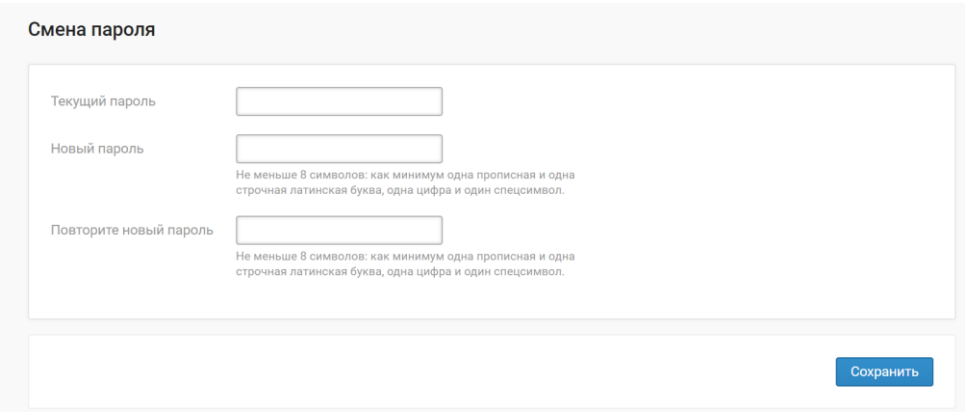


Рисунок 5 - Изменение пароля

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

- «Запросы»;
- «Бюллетени»;
- «Ваша организация»;
- «Зарегистрировать запрос».

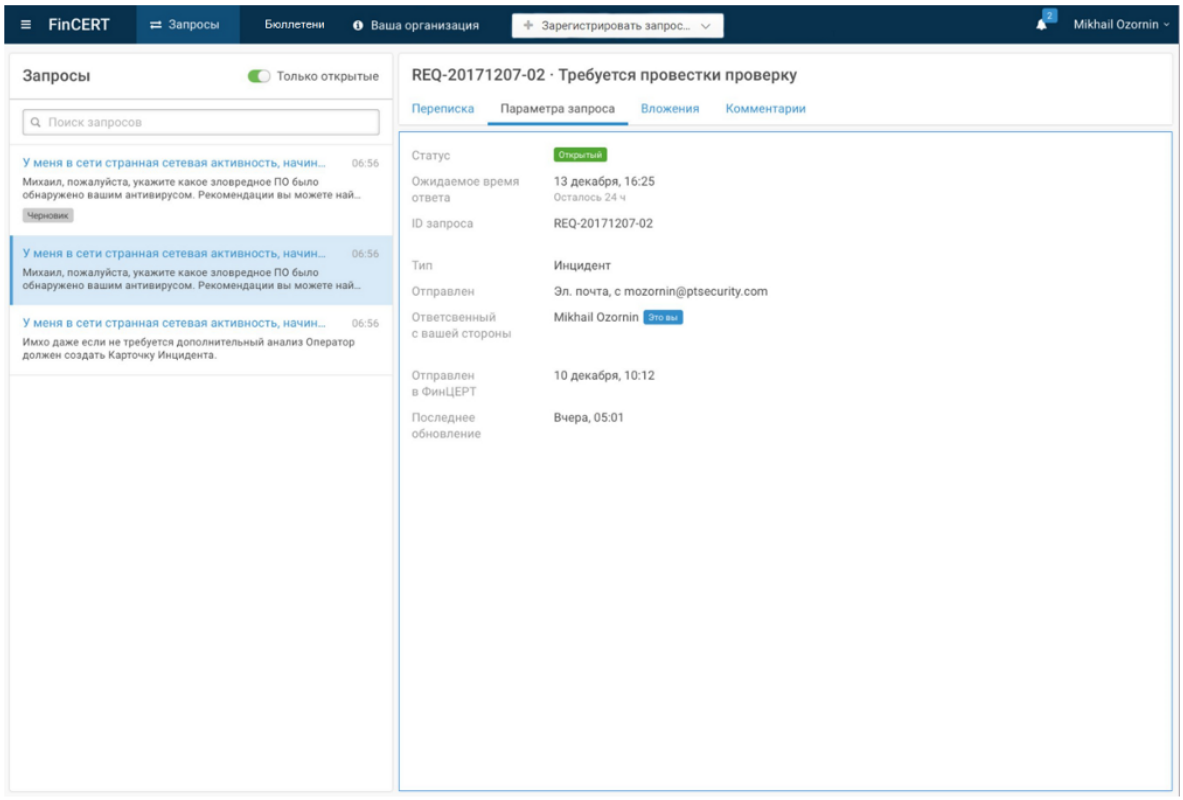


Рисунок 6 – Интерфейс ЛК Участника

2.2 Работа с меню «Запросы»

Информация о запросах отображается на странице «Запросы».

В открывшейся форме отобразится содержимое запросов (Рисунок 7).

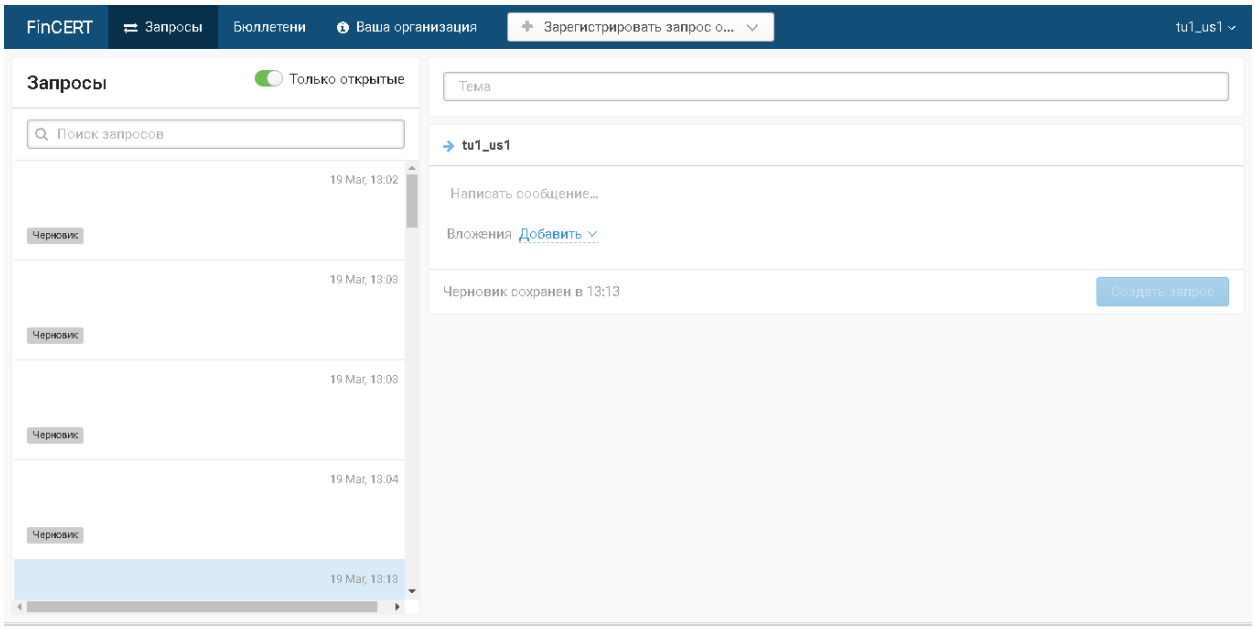


Рисунок 7 – Информация по запросам

Рабочая область страницы содержит список запросов. По умолчанию список содержит только открытые запросы и черновики запросов. Вы можете включить отображение закрытых запросов (Рисунок 8).

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 - Строка поиска запроса

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

- Статус. Предназначен для отслеживания состояния обработки запроса. В ФинЦЕРТ существуют следующие статусы запроса:

- Назначен — запрос только поступил в ФинЦЕРТ и назначен на ответственного оператора.
- В работе — ведется работа по запросу.
- Ожидает закрытия — ожидается подтверждение ФинЦЕРТ о закрытии запроса.
- Закрыт — запрос успешно обработан и помещен в архив.
- Отклонен — запрос неактуален и отклонен.

- 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.
- Идентификатор запроса. Идентификатор запроса формируется автоматически.
- Отправлен. Способ отправки запроса, фамилия и имя пользователя, отправившего запрос.
- Последнее обновление. Дата и время последнего изменения запроса. На вкладке Переписка отображается вся переписка с оператором ФинЦЕРТ. Вы можете отправить оператору сообщение и вложить в сообщение файл.

2.3 Работа с меню «Бюллетени»

Для работы необходимо выполнить переход на вкладку «Бюллетени».

В открывшейся форме отобразится содержимое бюллетеней (Рисунок 10). Детальное описание бюллетеня приведено в правой части экранной формы (Рисунок 10), скачать бюллетень можно по ссылке, приведенной в описании бюллетеня

Информация по бюллетеням включает:

- дату опубликования бюллетеня;
- идентификатор;
- заголовок;
- краткое описание.

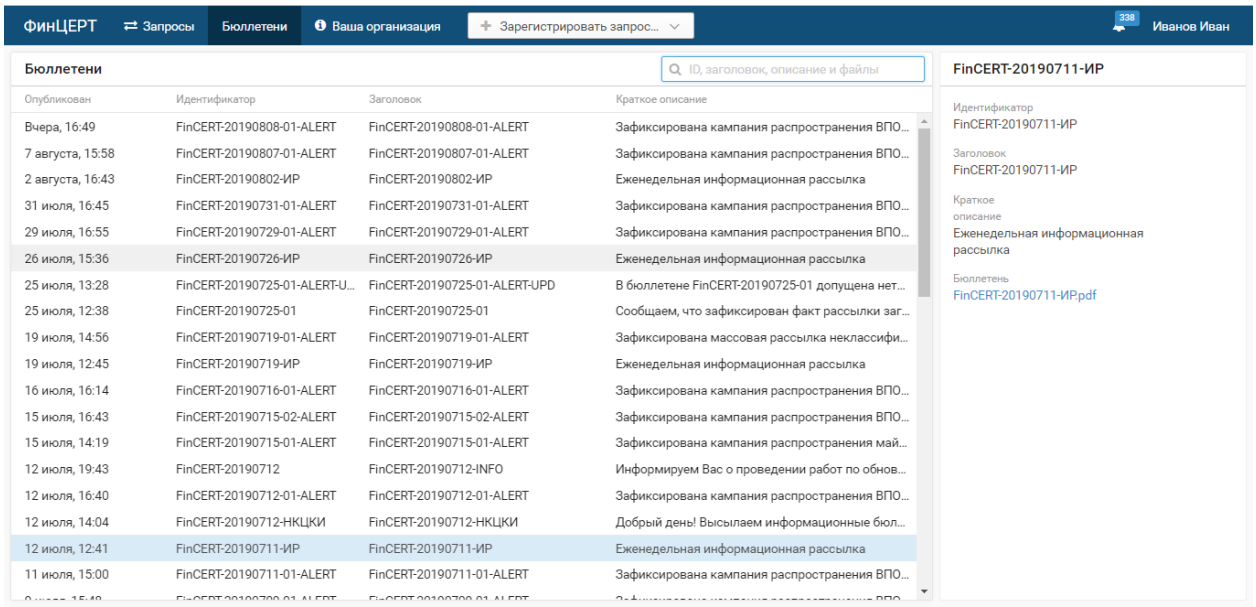


Рисунок 10 – Информация по бюллетеням

Для поиска бюллетеней необходимо внести текст в поле поиска (как показано на рисунке 11), поиск производится по полям: ID, заголовок, описание и файлы

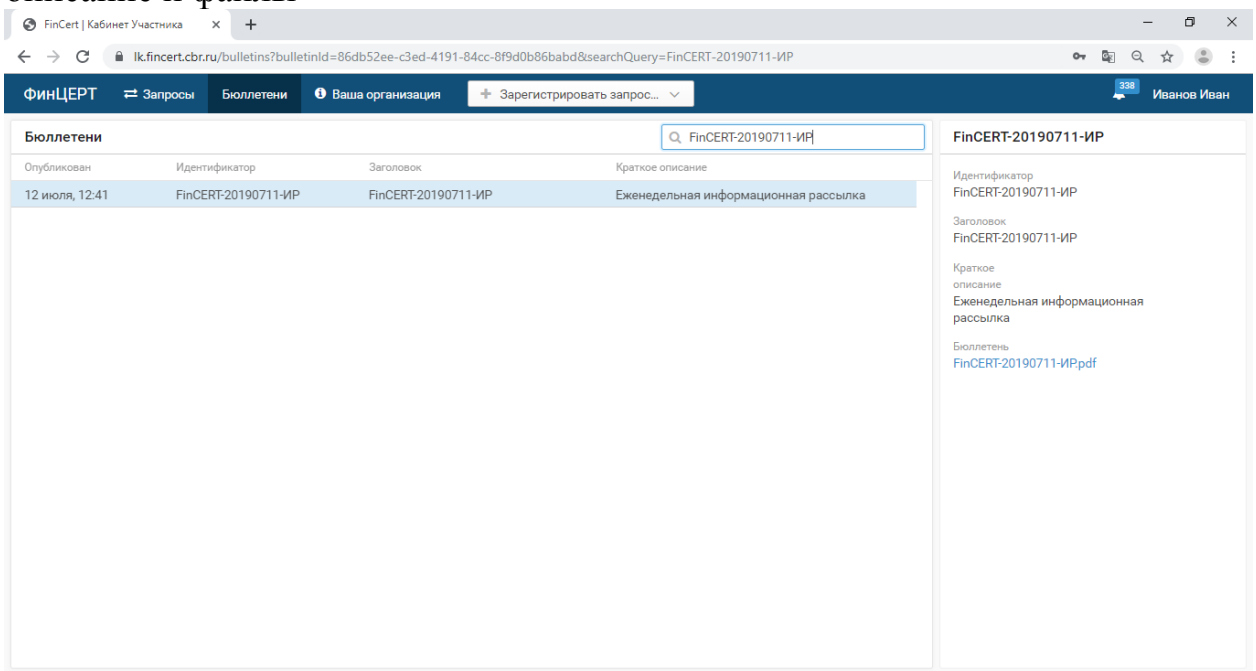


Рисунок 11 – Поиск бюллетеней

2.4 Работа с меню «Ваша организация»

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

Рабочая область страницы Ваша организация содержит следующую информацию об организации:

- Название — краткое название организации;
- Полное название — полное название организации;
- Форма юр. лица;
- Бренд — название, под которым также известна организация;
- Ящик входящей почты – адрес, на который поступают рассылки бюллетеней, уведомления о публикации бюллетеней, регистрации запросов в ФинЦЕРТ, новых сообщений в запросах, изменения статусов запросов, операциях без согласия и т.п. Ящик входящей почты используется по умолчанию для рассылки уведомлений от ФинЦЕРТ.
- Групповые почтовые ящики – адреса, на которые поступают Рассылки информационных бюллетеней.
- Регистрационный номер — номер организации во всероссийском реестре кредитных организаций;
- Тип организации;
- Техническое обеспечение;
- Реквизиты.

Вкладка «Пользователи» содержит таблицу пользователей участника. Основные параметры участников распределены по столбцам таблицы. Вы можете просмотреть полную информацию о пользователе по ссылке с логином пользователя в столбце Пользователь.

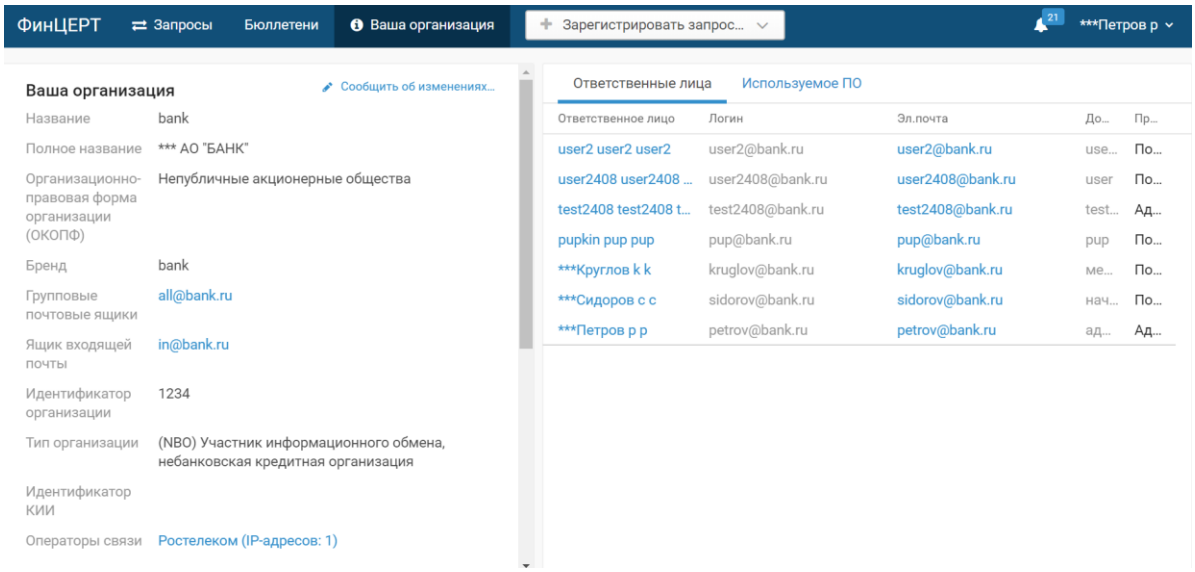


Рисунок 12 – Меню «Ваша организация»

Вкладка Используемое ПО содержит таблицу программного обеспечения участника.

Вы можете отправить запрос на изменение данных организации. Для этого нажмите кнопку «Сообщить об изменениях…» и измените соответствующие сведения о вашей организации (Рисунок 13).

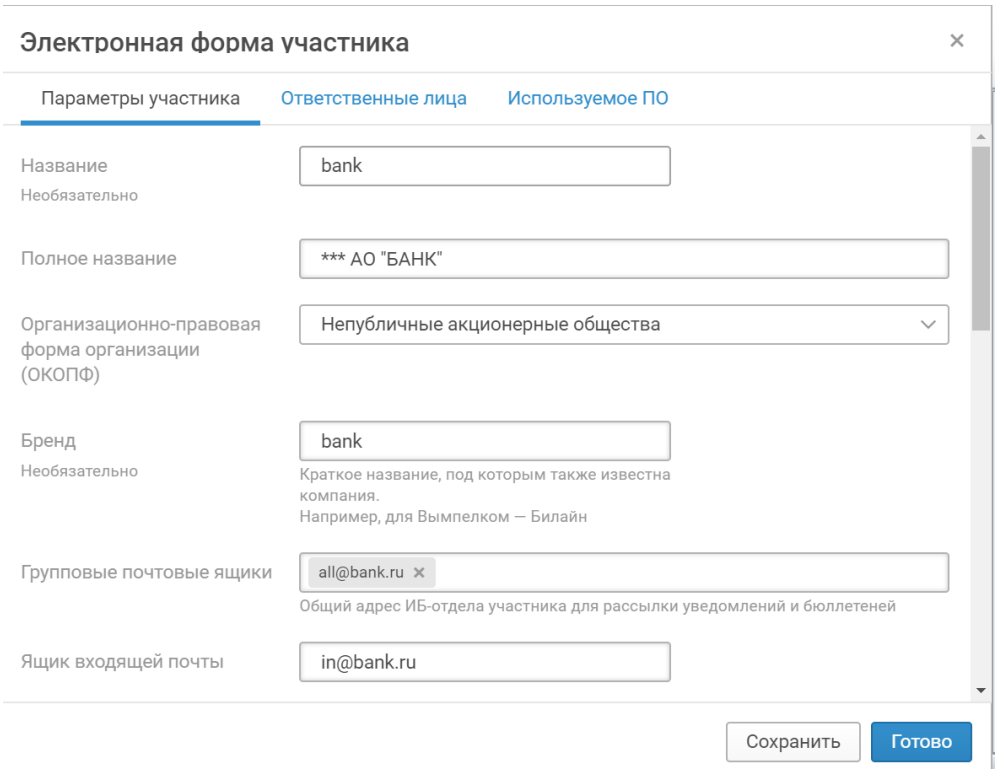


Рисунок 13 – Электронная форма участника

2.5 Меню «Зарегистрировать запрос о…»

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;
- электронную форму угрозы;
- электронную форму уязвимости;
- электронную форму публикации;
- электронную форму участника.

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.

Для работы необходимо выполнить переход на вкладку «Зарегистрировать запрос…» (Рисунок 14).

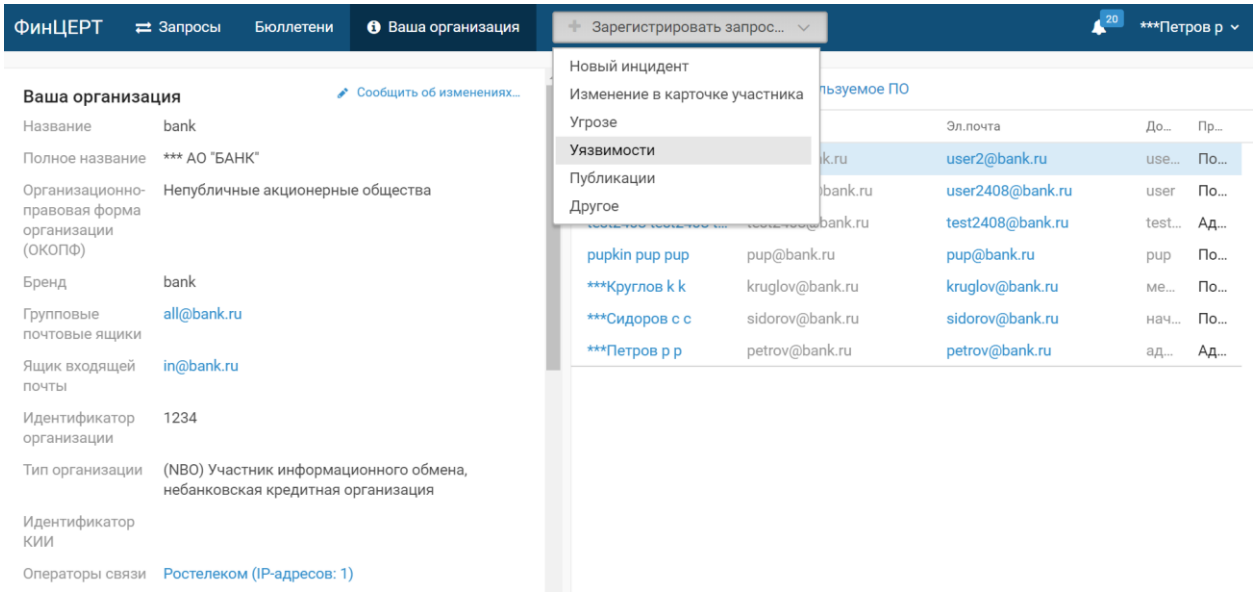


Рисунок 14 – Меню «Зарегистрировать запрос…»

Доступны следующие категории запросов:

- «Новый инцидент»;
- «Изменение в карточке участника»;
- «Угрозе»;
- «Уязвимости»;
- «Публикации»;
- «Другое».

2.5.1 Создание запроса об инциденте

В данном пункте приведена процедура регистрации запроса об инциденте. Детальное описание электронной формы инцидента приведено в п. 2.5.8.

Для регистрации запроса об инциденте:

- В главном меню нажмите кнопку «Зарегистрировать запрос…» и выберите пункт «Новый инцидент» (Рисунок 14). Откроется окно «Электронная форма инцидента» (Рисунок 15).

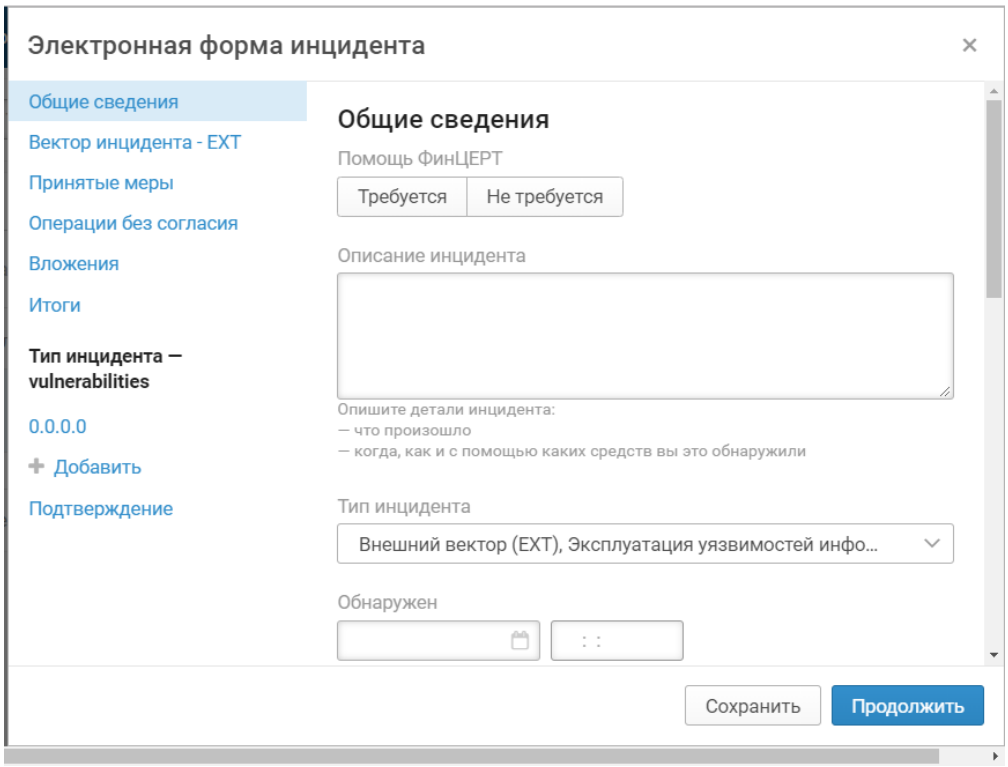


Рисунок 15 - Создание запроса об инциденте

- В открывшейся форме необходимо заполнить (вкладка «Общие сведения» (Рисунок 15)):
  - Помощь ФинЦЕРТ. Укажите, требуется ли консультация или помощь со стороны ФинЦЕРТ. Поле обязательно для заполнения.
  - 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. Поле обязательно для заполнения.
  - в раскрывающемся списке **Тип инцидента** выберите тип инцидента. Поле обязательно для заполнения. (Рисунок 16, Рисунок 17);

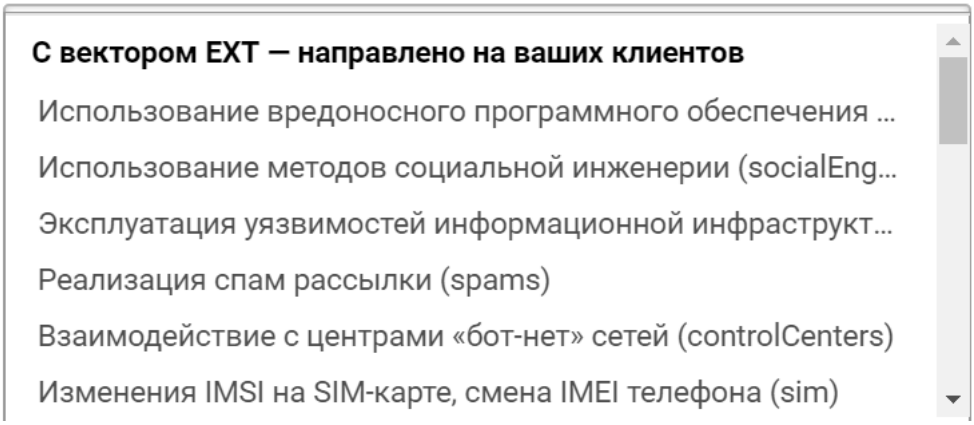


Рисунок 16 – Типы инцидентов с вектором EXT

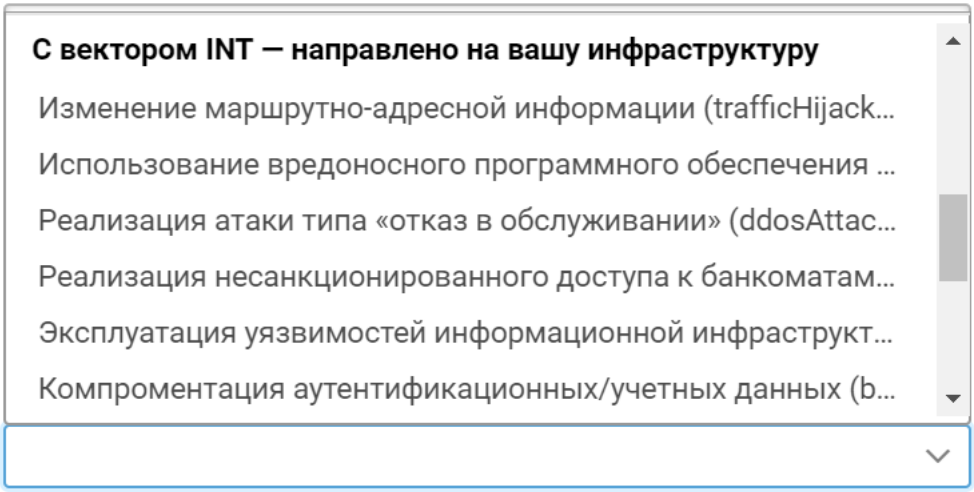


Рисунок 17 – Типы инцидентов с вектором INT

- Обнаружен. Укажите дату и время обнаружения инцидента. Дата указывается в формате ДД.ММ.ГГГГ. Время указывается в формате ЧЧ:ММ. Поле обязательно для заполнения.
- Федеральный округ. Из выпадающего списка выберите значение федеральный округа, на территории которого произошел инцидент. В случае выявления инцидента, связанного с трансграничным переводом денежных средств, место выявления инцидента не указывается. Если инцидент произошел не на территории РФ, выберите пункт «Другой».
- Субъект федерации. Из выпадающего списка выберите значение субъекта федерации, на территории которого произошел инцидент.
- Населенный пункт. Укажите город или иной населенный пункт, в котором произошел инцидент.
- Подразделение. Укажите, атакуемое структурное (организационное) подразделение. Например: департамент информационных технологий. Поле обязательно для заполнения.
- Техническое средство. Укажите, техническое средство, где был зафиксирован инцидент. Поле обязательно для заполнения.
- Атакованные сервисы. Нажмите кнопку «Добавить сервис». В открывшемся окне (Рисунок 18) выберите Тип сервиса и заполните поле Описание сервиса.

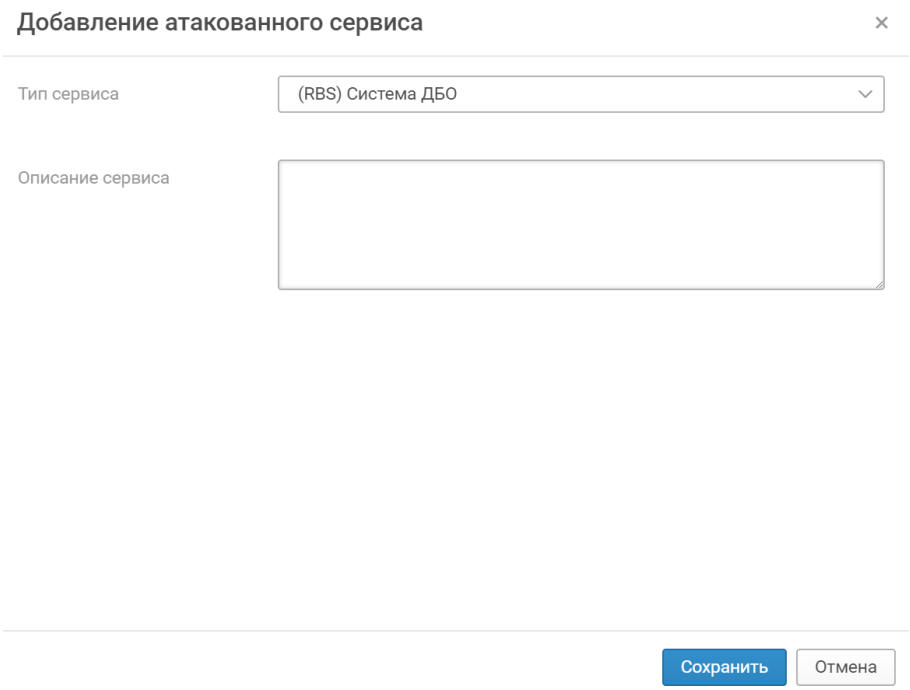


Рисунок 18 – Добавление атакованного сервиса

- Обращение в правоохранительные органы. Поле обязательно для заполнения. Укажите есть ли обращение в правоохранительные органы. В случае наличии, заполните поля:
  - Порядковый номер в книге учета сообщений о преступлениях.
  - Регистрационный номер талона-уведомления.
  - Дата и время принятия заявления.
- нажмите кнопку «Продолжить».

- После выбора (из всплывающего меню) типа инцидента появятся дополнительные группы данных, которые так же необходимо заполнить (Рисунок 19). Подробное описание полей для заполнения приведено в 2.5.8

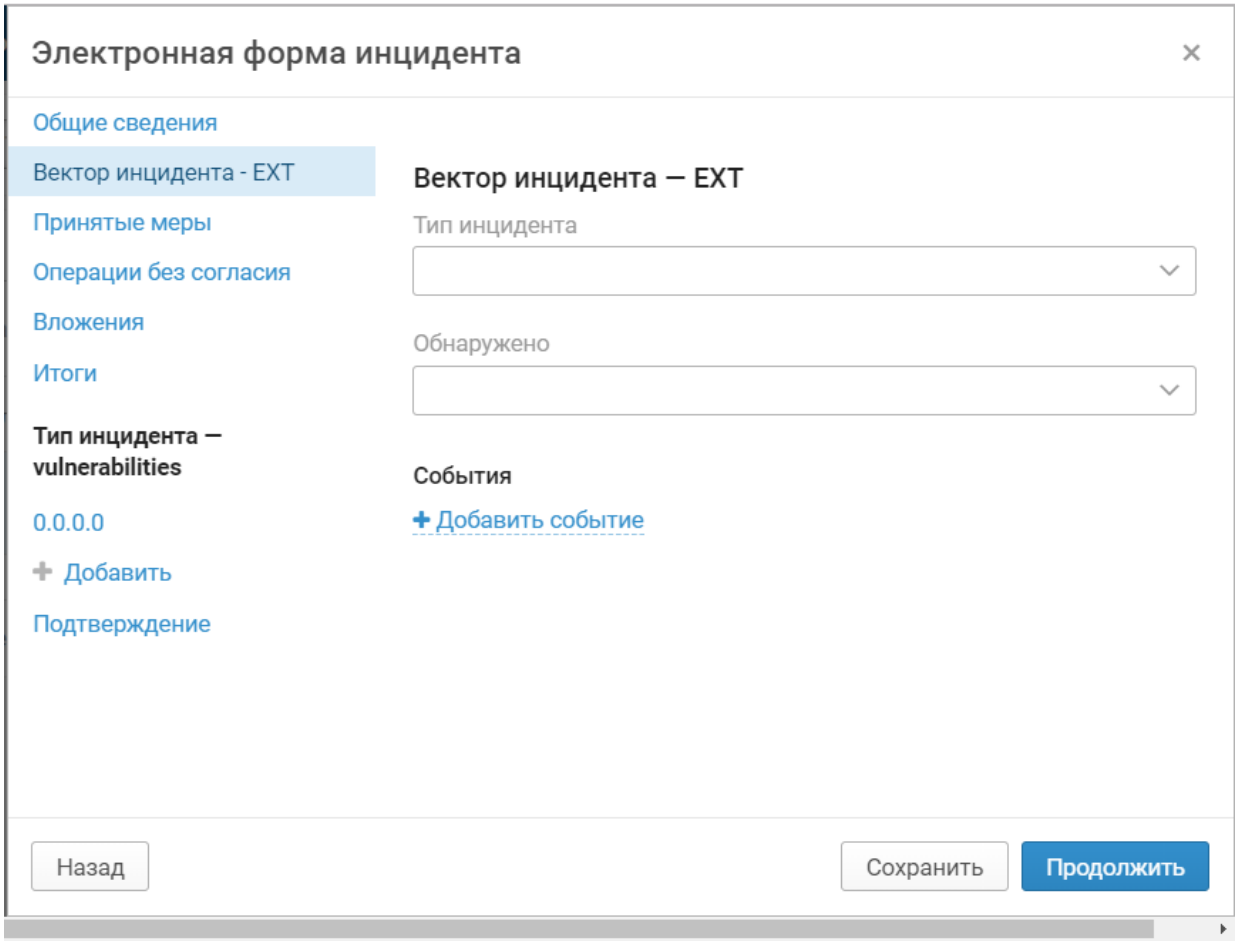


Рисунок 19 - Заполнение дополнительных параметров об инциденте

- Откройте вкладку «Принятые меры». В открывшемся окне (Рисунок 20) опишите принятые меры, нажмите кнопку «Добавить».

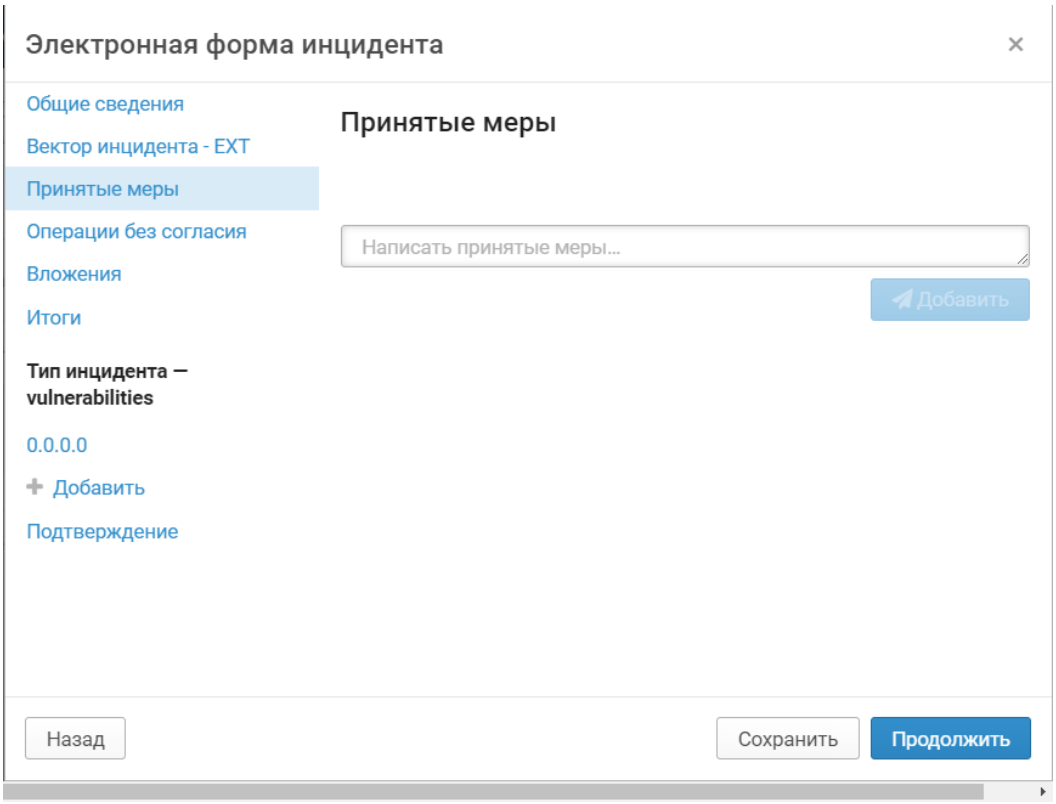


Рисунок 20 – Описание принятых мер

- Откройте вкладку «Операции без согласия» В открывшейся форме (Рисунок 21) необходимо нажать кнопку «+Добавить операцию». Ввод информации производить в соответствии с документом «Руководство Участника Прототипа АС «Фид-Антифрод», размещенным на информационном портале АСОИ ФинЦЕРТ (https://portal.fincert.cbr.ru) в разделе «АСОИ ФинЦЕРТ (Документация и ПО Участника)»

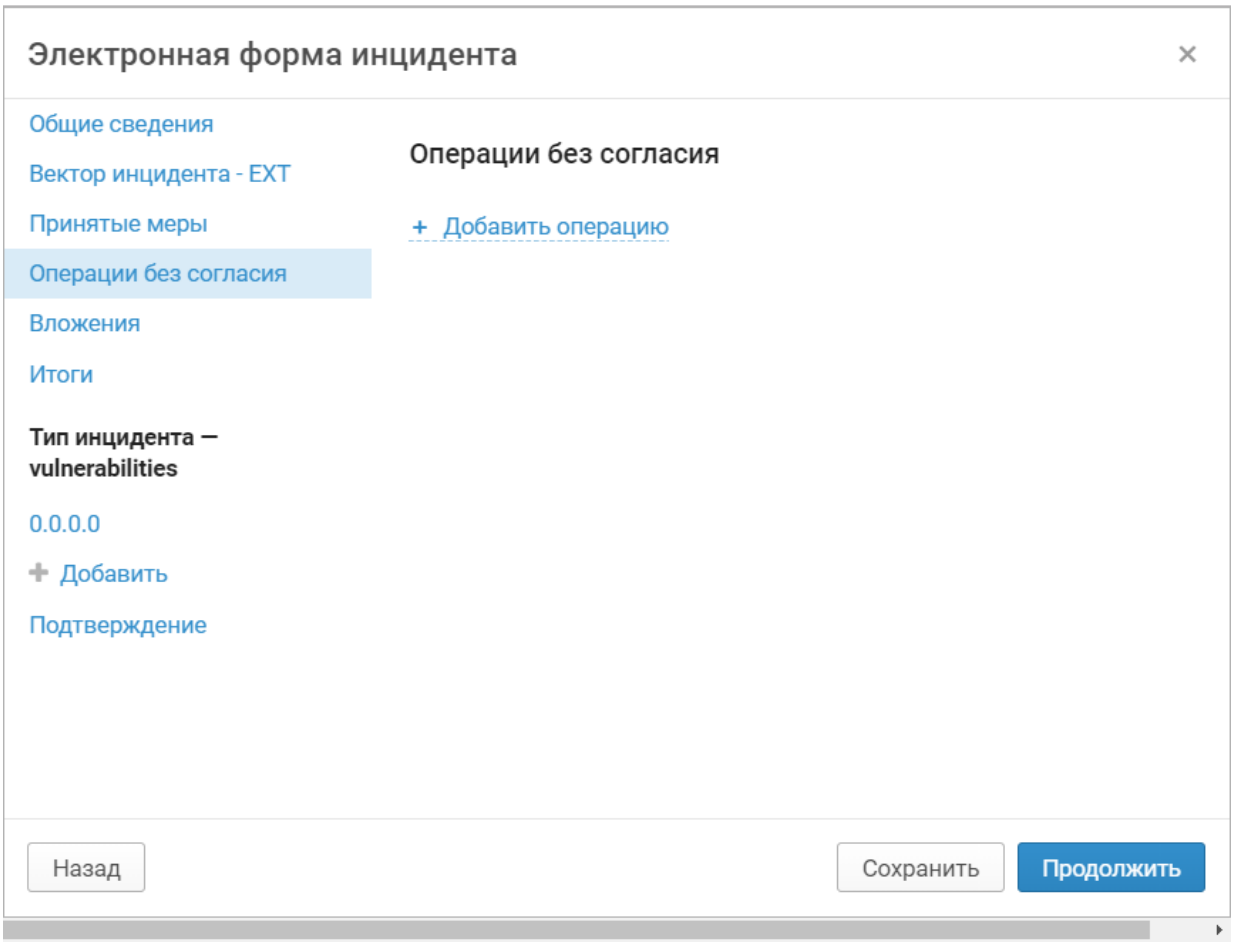


Рисунок 21 – Описание операций без согласия

- Откройте вкладку «Вложения». В открывшейся форме (Рисунок 22) необходимо выбрать файл для загрузки, нажать кнопку в диалоговом окне «Открыть», либо перетащить файл в указанное место и нажать кнопку «Продолжить».

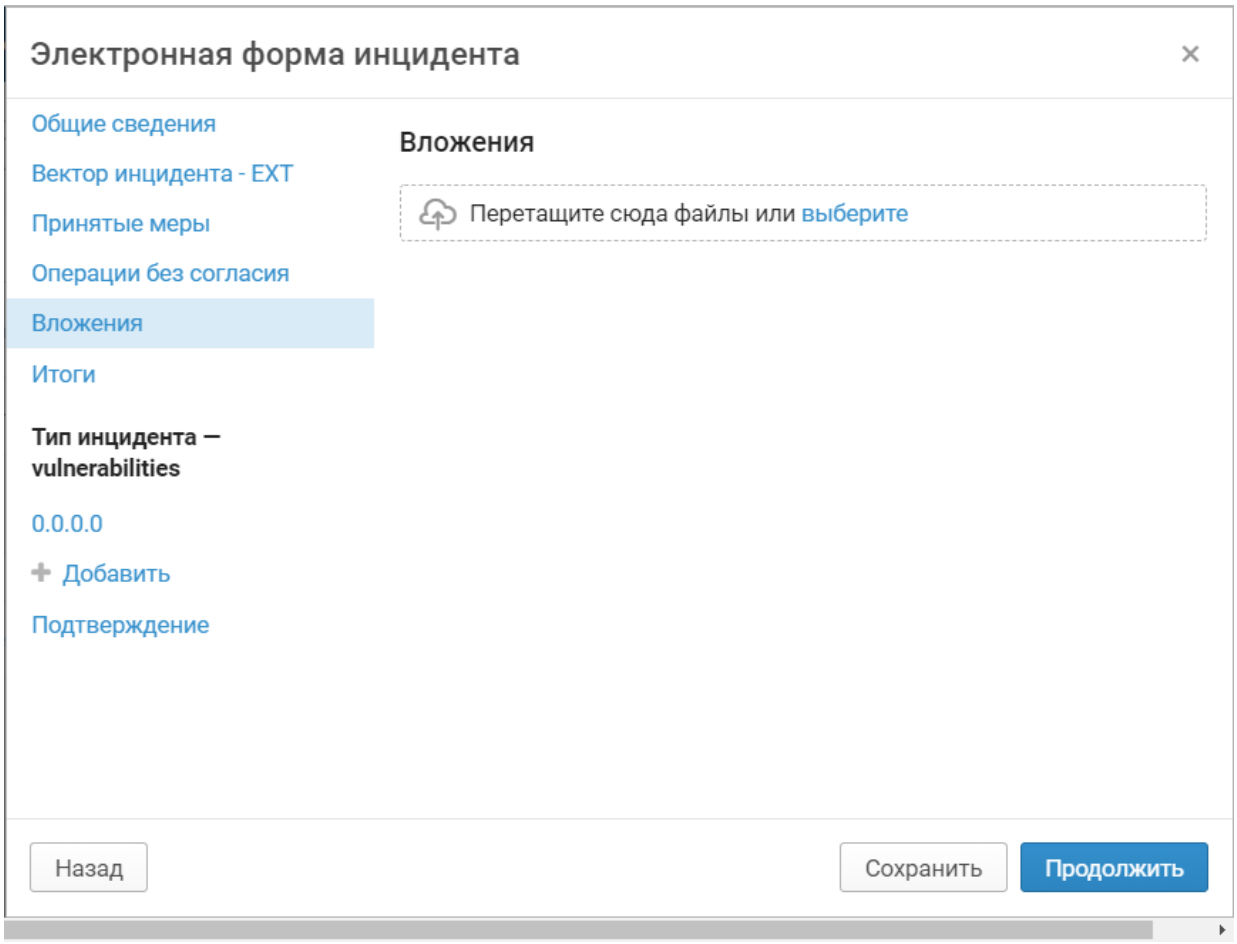


Рисунок 22 – Добавление вложения к описанию инцидента

- Далее откроется вкладка «Итоги». В открывшейся форме (Рисунок 23) необходимо заполнить поля:
  - Ущерб от инцидента. Операционные расходы.
  - Ущерб от инцидента. Относительный масштаб. Выберите из выпадающего списка одно из значений: (MOD) Умеренное влияние, (ESS) Существенное влияние, (CRIT) Критическое влияние.
  - Сигнатуры атаки. Средство обнаружения.
  - Сигнатуры атаки. Идентификатор сигнатуры.
  - Сигнатуры атаки. Источник получения.
  - Сигнатуры атаки. Число срабатываний.

- SNORT-правило обнаружения атак. В открывшемся окне укажите SNORT-правило.
- Итоговый отчёт. Дата закрытия инцидента. Укажите дату.
- Итоговый отчёт. Восстановление функционирования. Выберите из выпадающего списка одно из значений: (Full) Восстановлено полностью, (Not_Full) Восстановлено частично.
- Итоговый отчёт. Описание.
- Итоговый отчёт. Причины возникновения.
- Итоговый отчёт. Принятые меры.

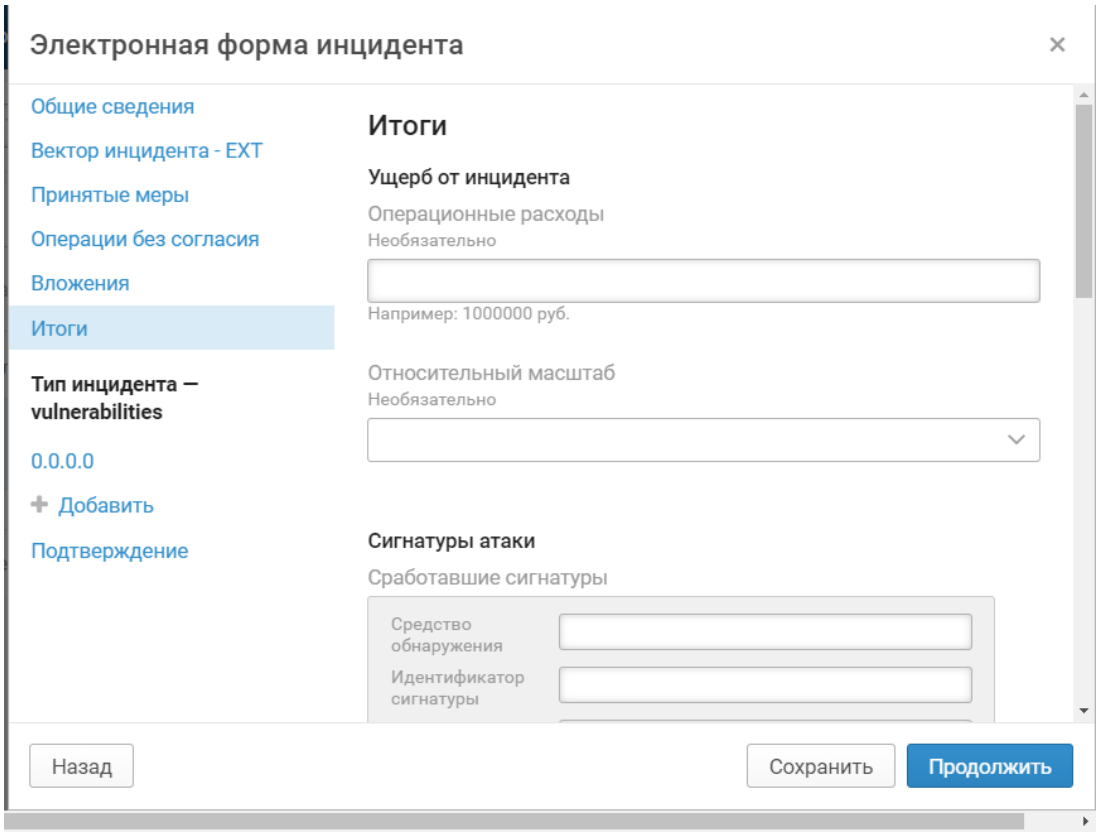


Рисунок 23 – Описание итогов в запросе об инциденте

После заполнения нажмите кнопку «Продолжить».

- Далее откроется вкладка «Подтверждение». В открывшейся форме (Рисунок 24) необходимо проверить введённую информацию об инциденте и нажать кнопку «Добавить к запросу» или «Сохранить».

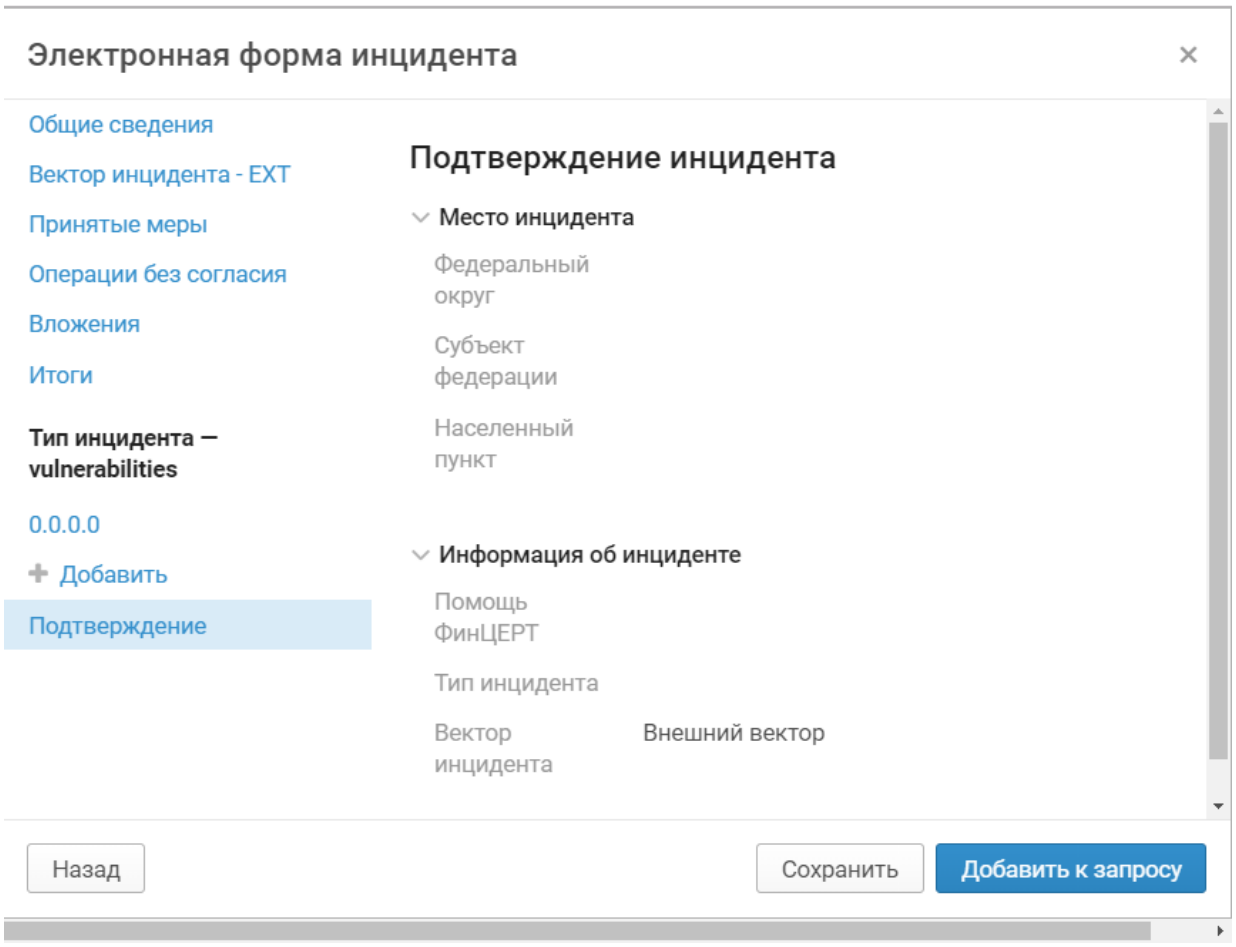


Рисунок 24 – Подтверждение информации об инциденте

- В случае необходимости корректировки введённых данных необходимо нажать кнопку «Назад» и выполнить корректировку информации согласно п.2 и 3.

2.5.2 Создание запроса об инциденте с использование готовых карточек в форматах JSON для регистрации запроса об инциденте:

- Из списка (Рисунок 14) выберите пункт меню «Другое».
- В появившемся окне нажмите «Вложения» – «Добавить»– «Файл». (Рисунок 25).
- Далее нажмите «Выберите» (или перетащите файл с заполненным инцидентом в формате JSON).

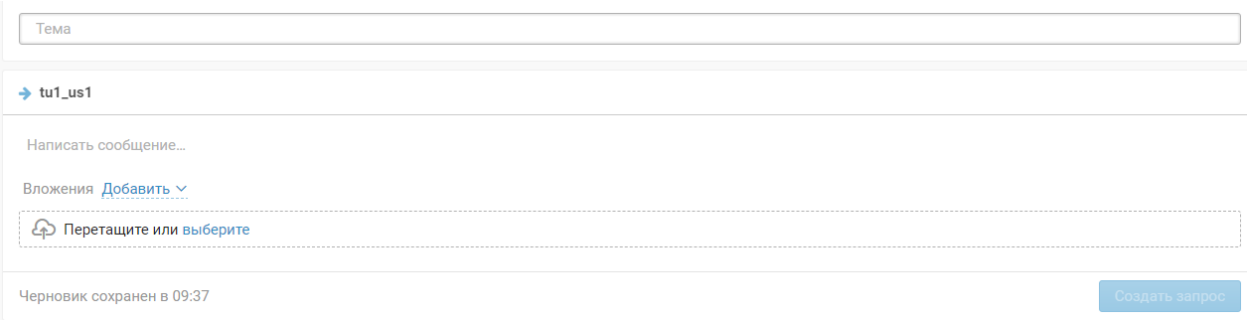


Рисунок 25 – Выбор вложения к запросу

- В открывшемся окне выберите файл и нажмите кнопку «Открыть» (Рисунок 26).

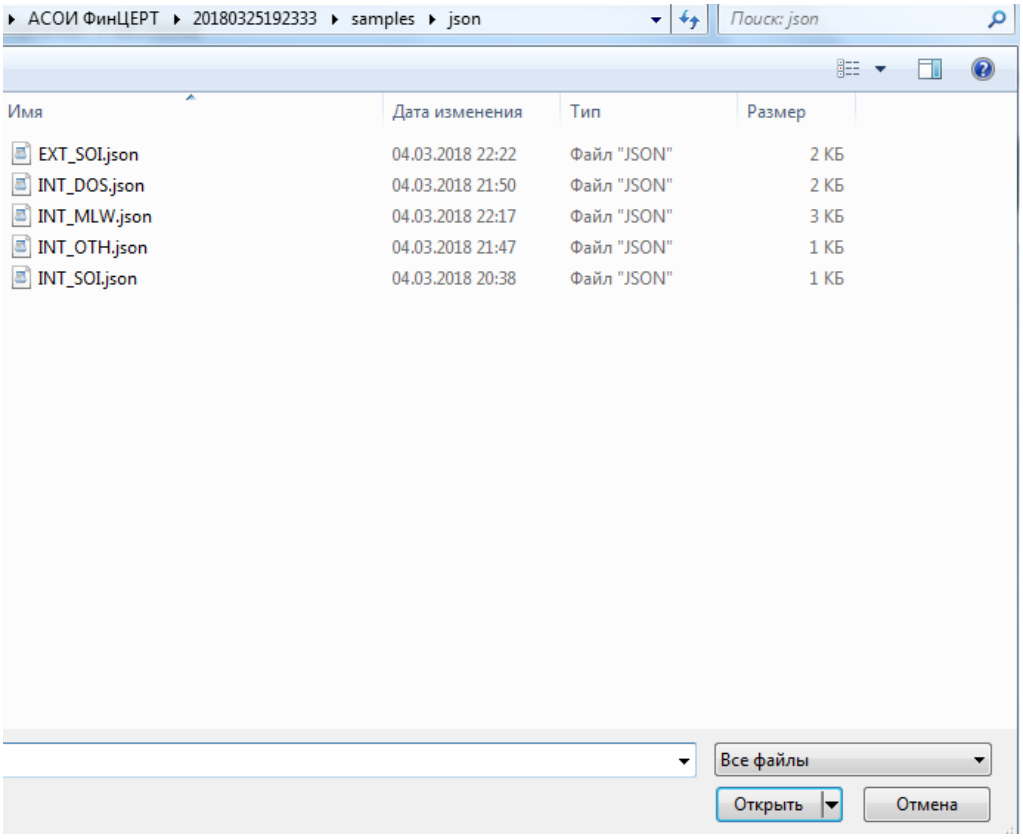


Рисунок 26 – Выбор заполненной карточки инцидента в формате JSON

- После выбора файла в открывшемся окне появится информация о прикрепленном к электронной форме файле (Рисунок 27).

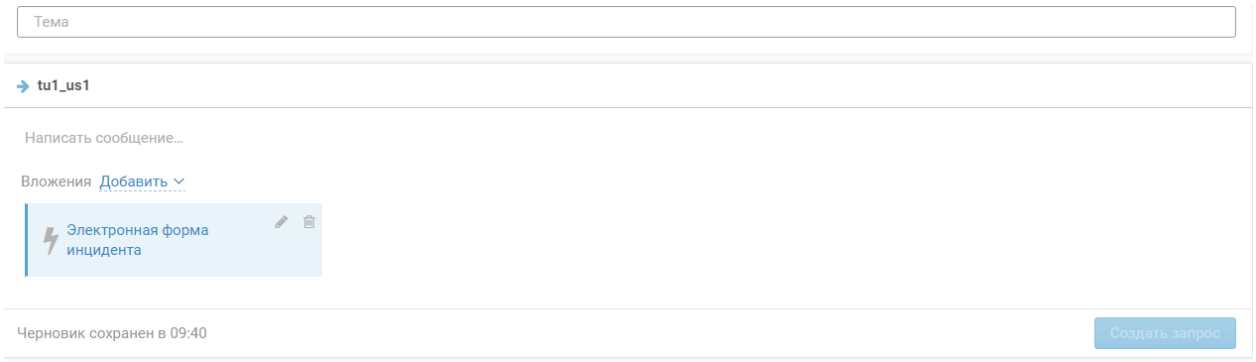
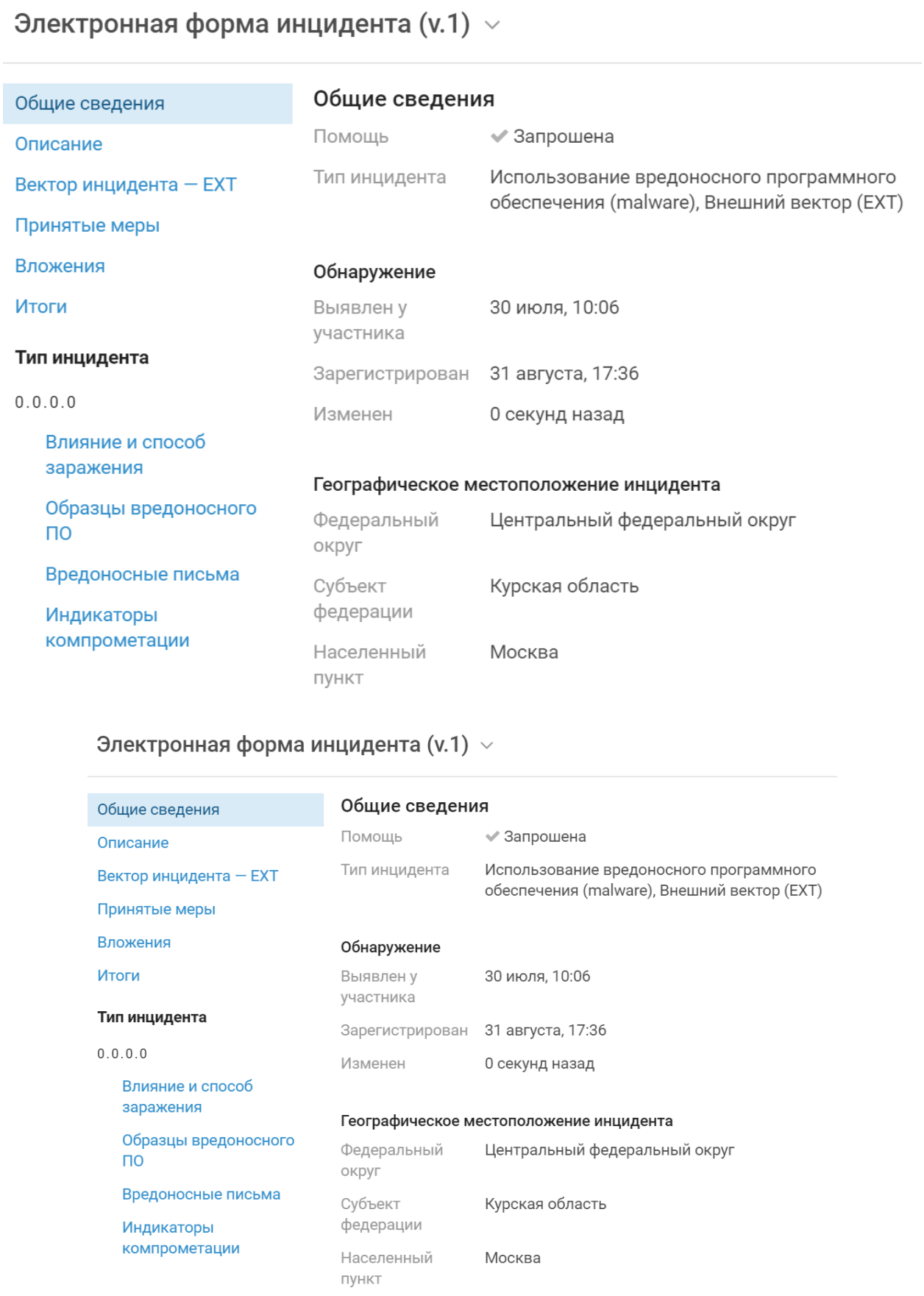


Рисунок 27 – Карточка инцидента в формате JSON, прикрепленная к запросу

В форме запроса можно нажать на панель «Электронная форма инцидента» и просмотреть содержание карточки инцидента и приложенного файла в формате JSON (Рисунок 28).



Электронная форма инцидента (v.1)

Общие сведения
Описание
Вектор инцидента — EXT
Принятые меры
Вложения
Итоги

Тип инцидента

0.0.0.0

Влияние и способ заражения
Образцы вредоносного ПО
Вредоносные письма
Индикаторы компрометации

Общие сведения

Помощь — Запрошена
Тип инцидента — Использование вредоносного программного обеспечения (malware), Внешний вектор (EXT)

Обнаружение

Выявлен у участника — 30 июля, 10:06
Зарегистрирован — 31 августа, 17:36
Изменен — 0 секунд назад

Географическое местоположение инцидента

Федеральный округ — Центральный федеральный округ
Субъект федерации — Курская область
Населенный пункт — Москва

Электронная форма инцидента (v.1)

Общие сведения
Описание
Вектор инцидента — EXT
Принятые меры
Вложения
Итоги

Тип инцидента

0.0.0.0

Влияние и способ заражения
Образцы вредоносного ПО
Вредоносные письма
Индикаторы компрометации

Общие сведения

Помощь — Запрошена
Тип инцидента — Использование вредоносного программного обеспечения (malware), Внешний вектор (EXT)

Обнаружение

Выявлен у участника — 30 июля, 10:06
Зарегистрирован — 31 августа, 17:36
Изменен — 0 секунд назад

Географическое местоположение инцидента

Федеральный округ — Центральный федеральный округ
Субъект федерации — Курская область
Населенный пункт — Москва

Рисунок 28 – 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» (Рисунок 29).

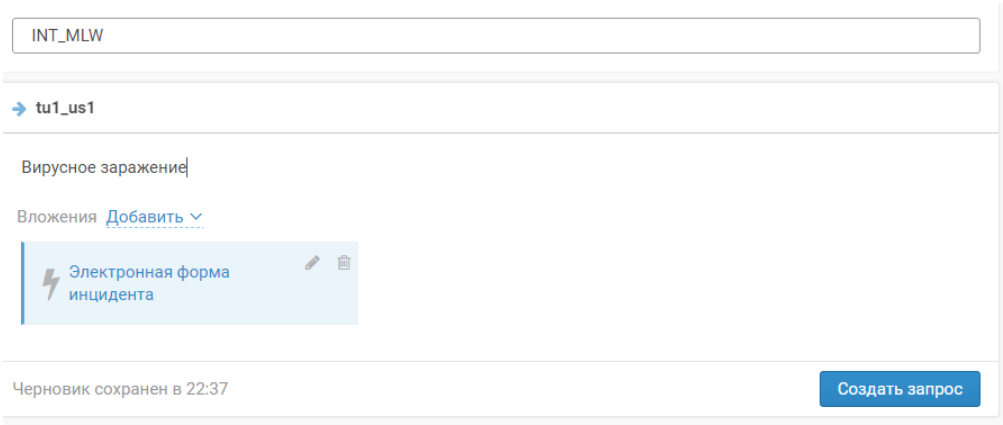


Рисунок 29 – Создание запроса в ФинЦЕРТ

2.5.3 Создание запроса об изменении карточки участника

Для регистрации запроса об изменении в карточке участника необходимо:

- Из списка (Рисунок 14) выбрать пункт меню «Изменении в карточке участника».
- В открывшейся форме (Рисунок 30) внесите изменения в необходимых полях и нажмите кнопку «Готово».

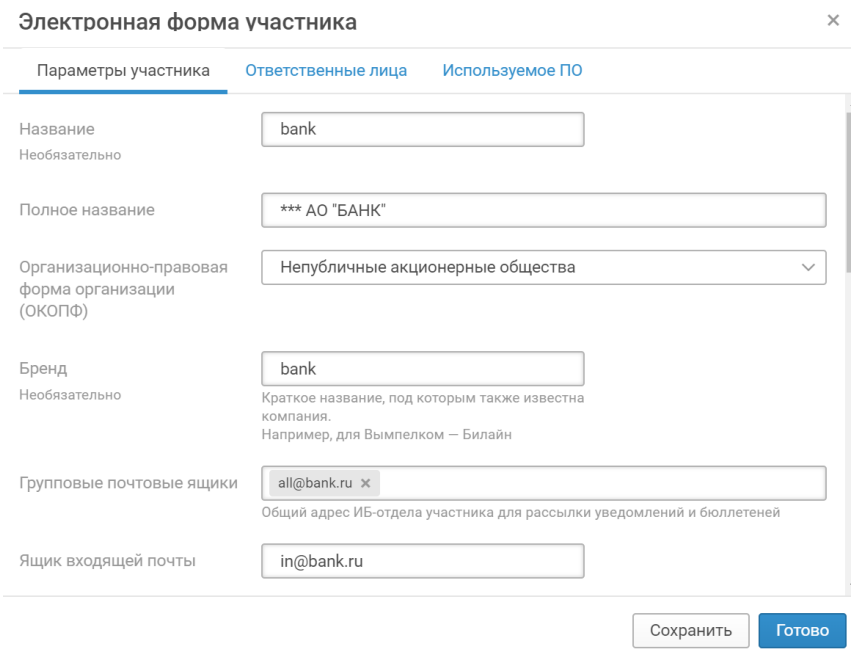


Рисунок 30 – Изменение информации об участнике

- Перейти на вкладку «Ответственные лица» (Рисунок 31).

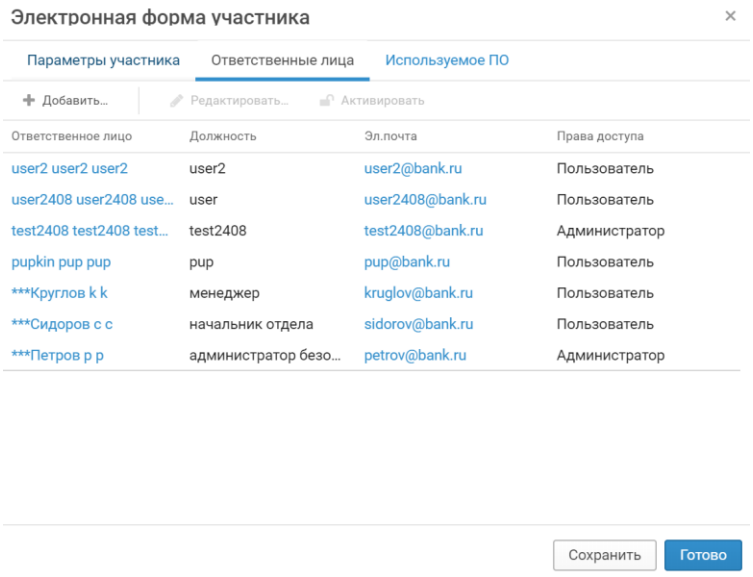


Рисунок 31 – Корректировка пользователей

- Для добавления пользователя необходимо выбрать пункт «Добавить пользователя», заполнить поля формы (Рисунок 32):
  - в поля ФИО ввести фамилию, имя и отчество пользователя;

- в поле «Должность» ввести название должности пользователя. Поле обязательно для заполнения;
- Поле «Доступ в личный кабинет». При необходимости сразу активируйте пользователя;
- Поле «Права доступа». При необходимости дайте пользователю расширенные права Администратора.
- в раскрывающемся списке «Категория» выберите категорию. Поле обязательно для заполнения;
- в поле «Эл. Почта» введите адрес электронной почты пользователя. Поле обязательно для заполнения;
- в поля «Городской телефон» и «Мобильный телефон» введите соответствующие номера телефонов. Поля обязательны для заполнения.

- Нажмите кнопку «Готово» для сохранения измененной формы и ее отправки в ФинЦЕРТ либо кнопку «Сохранить» для сохранения черновика формы для дальнейшего редактирования.

Рисунок 32 – Добавление ответсвеннного лица

- Для редактирования информации о пользователе необходимо выбрать пользователя из списка и нажать кнопку «Редактировать», заполнить все поля формы (Рисунок 33) и нажать кнопку «Готово».

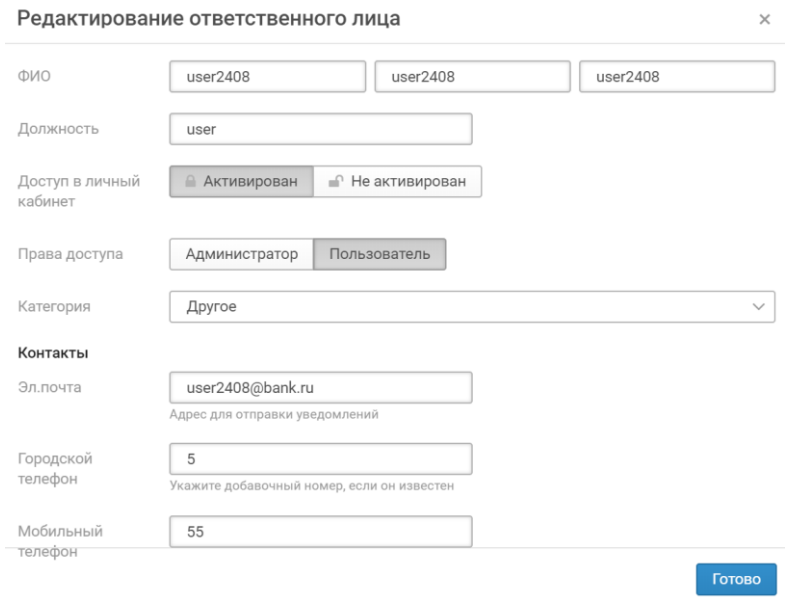


Рисунок 33 – Редактирование ответсвеннного лица

- Для блокировки пользователя необходимо выбрать пользователя из списка и нажать кнопку «Заблокировать».
- Для изменения состава используемого ПО перейдите на вкладку «Используемое ПО» (Рисунок 34).

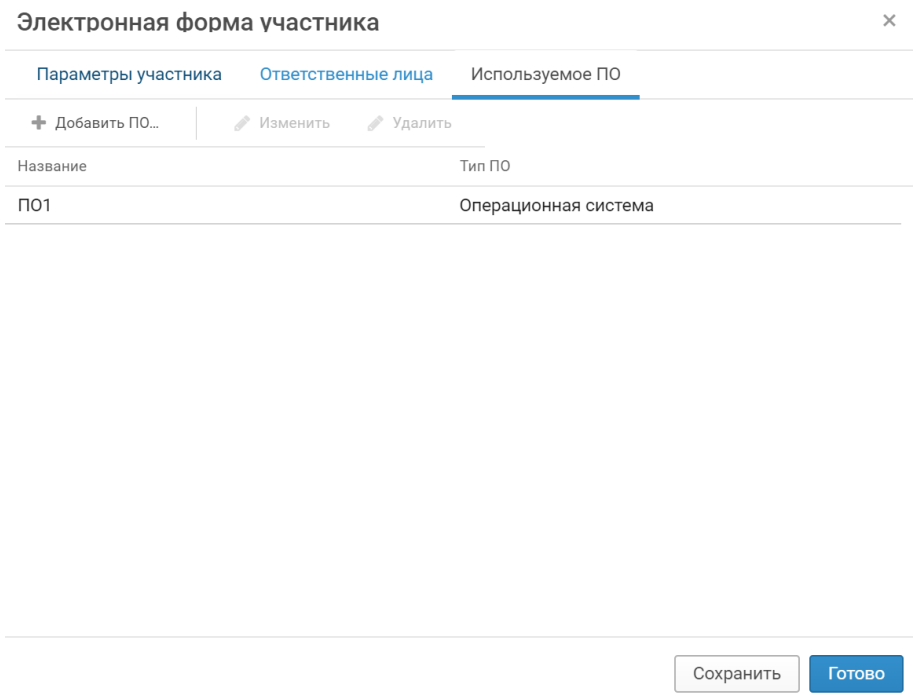
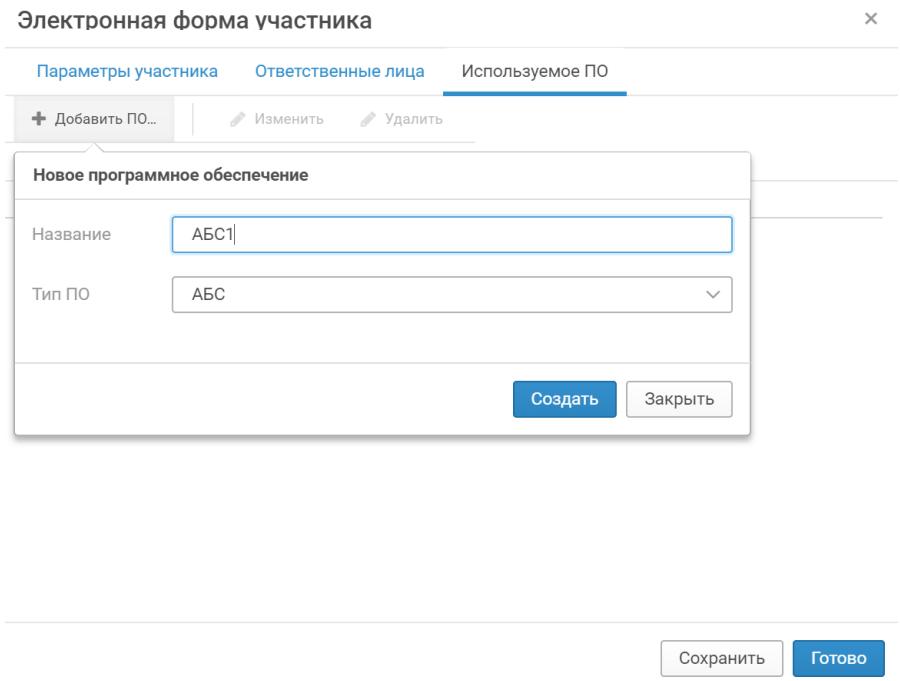


Рисунок 34 – Редактирование используемого ПО

- нажмите кнопку «Добавить ПО…». В окне введите Название и выберите Тип ПО и нажмите кнопку «Создать»



- для удаления ПО выберите соответствующий пункт и нажмите кнопку «Удалить».

Для завершения создания запроса об изменении карточки Участника и отправки его в ФинЦЕРТ необходимо нажать кнопку «Готово». В открывшемся окне заполните поле «Тема», после чего необходимо нажать кнопку «Создать запрос». После подтверждения изменений в ФинЦЕРТ указанные изменения будут внесены в карточку Участника.

2.5.4 Создание запроса об угрозе

Для регистрации запроса об угрозе:

- Из списка (Рисунок 14) выберите пункт меню «Угрозе».
- В открывшейся форме (Рисунок 35) заполните поля:
  - на вкладке «Общие сведения» заполните поля:
  - в поле «Название» введите название угрозы;
  - в поле «Федеральный округ» из раскрывающегося списка выберите требуемое значение;
  - в поле «Субъект федерации» из раскрывающегося списка выберите требуемое значение;
  - в поле «Населенный пункт» введите требуемое значение;
  - в поле «Дата выявления» укажите дату выявления угрозы;
  - в поле «Автор публикации» укажите автора, который обнаружил угрозу;
  - в поле «Тип угрозы» из раскрывающегося списка выберите тип угрозы;
  - в поле «Описание» введите описание угрозы;

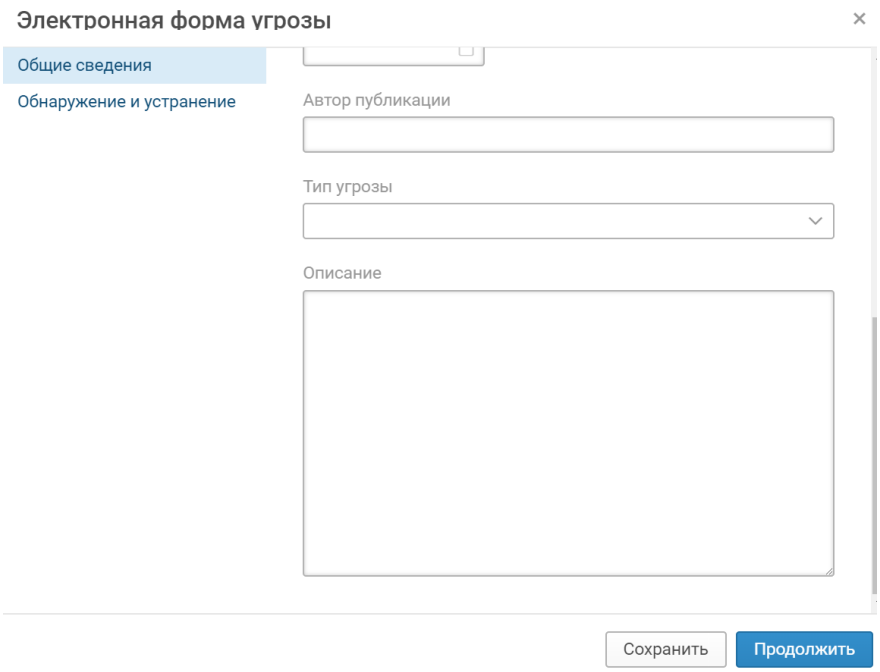


Рисунок 35 – Добавление общих сведений об угрозе

- Нажмите кнопку «Продолжить». Откроется следующая вкладка (Рисунок 36) в зависимости от типа угрозы имеющая разный состав полей:
  - Вредоносное программное обеспечение. В поле «Обнаруживается антивирусными решениями» введите названия антивирусных средств, которыми можно обнаружить вредоносное ПО. В поле «Индикаторы компрометации» введите индикаторы компрометации в формате OpenIOC, Yara, XML и так далее.
  - Эксплуатация уязвимости. В поле «Идентификаторы уязвимости» введите идентификаторы уязвимости (Поле обязательно для заполнения). В поле «Методика эксплуатации» введите метрики эксплуатации (Поле обязательно для заполнения).
  - DDoS. В поле «Атакующие IP-адреса» введите IP-адреса источника атаки (список IP адресов можно загрузить из файла по соответствующей ссылке). В поле «Тип атаки» введите тип атаки (Поле обязательно для заполнения). В поле «Ожидаемая мощность» введите ожидаемую мощность. В поле «Ожидаемое усилие» введите ожидаемое усилие.

- ЦУ бот-сети. В поле «IP-адрес или доменное имя» введите IP-адрес или доменное имя бот-сети (Поле обязательно для заполнения). В поле «Тип и общие сведения о бот-сети» введите тип бот-сети и общие сведения. В поле «Каким образом выявлен» опишите способ обнаружения бот-сети (Поле обязательно для заполнения).
- Фишинг. В поле «IP-адрес или доменное имя» введите IP-адрес или доменное имя ресурса, замаскированного под доверенный аналог (Поле обязательно для заполнения). В поле «Дата обнаружения ресурса» выберите дату обнаружения ресурса, замаскированного под доверенный аналог (Поле обязательно для заполнения). В поле «Текст письма» введите текст письма, полученного от фишингового ресурса. В поле «Технические заголовки письма» введите технические заголовки письма.
- Вредоносный ресурс. В поле «IP-адрес или доменное имя» введите IP-адрес или доменное имя вредоносного ресурса (Поле обязательно для заполнения). В поле «Дата обнаружения ресурса» выберите дату обнаружения ресурса. В поле «Причины, почему ресурс подозревается вредоносным» опишите, почему ресурс подозревается вредоносным (Поле обязательно для заполнения).
- Мошеннический телефонный номер. В поле «Дата и время звонка (смс)» выберите дату и введите время совершения несанкционированного действия. Время указывается в формате ЧЧ:ММ. В поле «Номер телефона» введите номер, с которого было совершено несанкционированное действие (Поле обязательно для заполнения). В поле «Текст SMS» введите текст SMS-сообщения.
- Технические подробности. В поле «Описание» введите описание угрозы. Поле обязательно для заполнения.

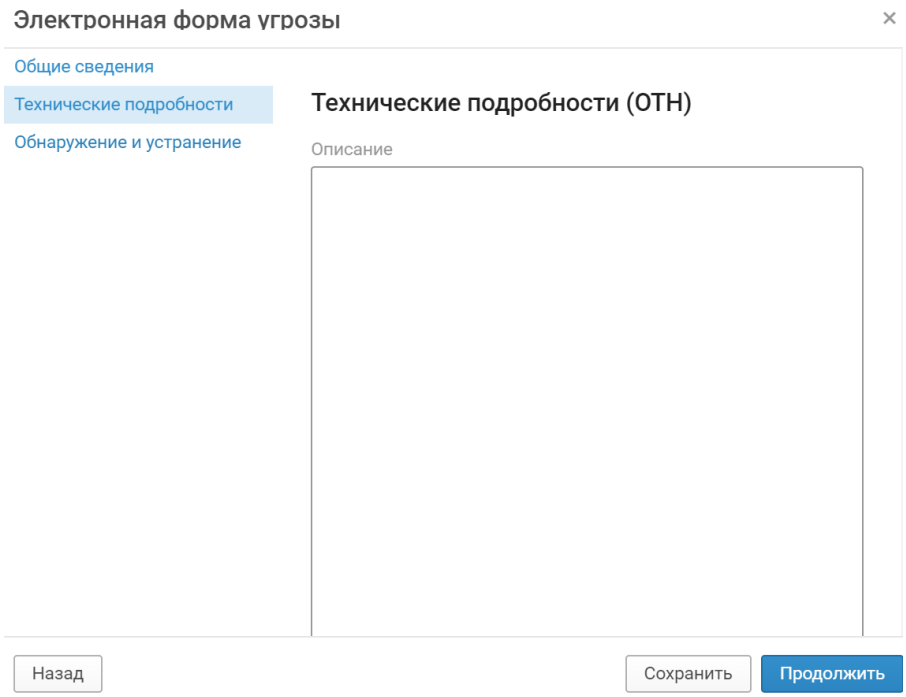


Рисунок 36 – Пример описания различных типов угроз

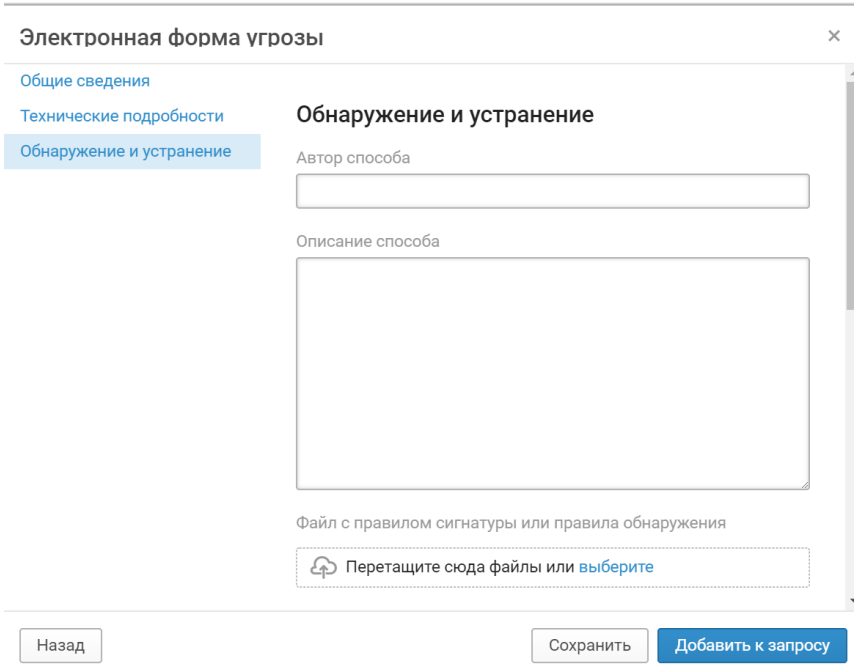


Рисунок 37 – Обнаружение и устранение

- Нажмите кнопку «Продолжить». В форме «Обнаружение и устранение» (Рисунок 38) необходимо заполнить информацию:

- в поле «Автор способа» введите автора способа обнаружения и устранения угрозы (поле обязательно для заполнения);
- в поле «Описание способа» введите описание способа обнаружения и устранения угрозы;
- в поле «Файл с правилами сигнатуры или правила обнаружения» перетащите или выберите файл;
- в поле «Возможные меры устранения» введите описание неформализованного или формализованного способа определения угрозы;
- в поле «Прочая информация» введите дополнительную информацию;

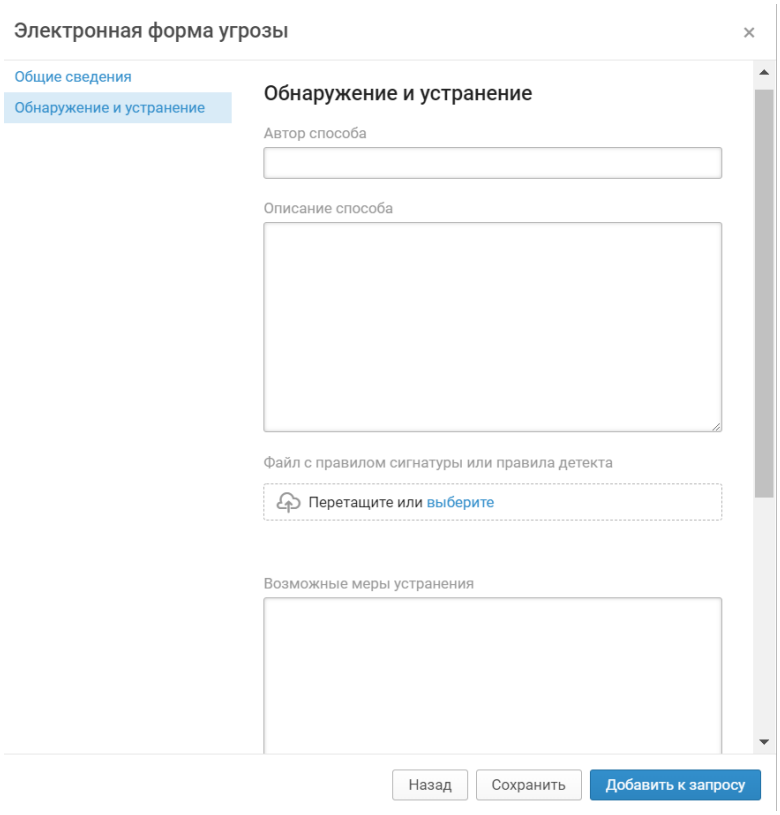


Рисунок 38 – Добавление информации о способах обнаружения и устранения угрозы

- Нажмите кнопку «Добавить к запросу». Откроется страница «Запросы».
- Заполните поля «Тема» и «Написать сообщение…» при необходимости.
- Нажмите кнопку «Создать запрос» и в открывшемся окне «Заполнить и зарегистрировать запрос».

- Запрос об угрозе создан.

2.5.5 Создание запроса об уязвимости

Для регистрации запроса об угрозе:

- Из списка (Рисунок 14) выберите пункт меню «Уязвимости».
- В открывшейся форме (Рисунок 39) заполните:
  - на вкладке «Общие сведения» в поле «Название» введите название уязвимости (поле обязательно для заполнения);
  - в поле «Идентификаторы других систем описаний уязвимостей» введите один идентификатор или несколько через запятую;
  - в поле «Описание уязвимости и способов ее использования» введите описание;
  - в блоке «Класс уязвимости» выберите соответствующий пункт (поле обязательно для заполнения);
  - в поле «CVSS-вектор» введите CVSS-вектор (поле обязательно для заполнения);
  - в поле «Федеральный округ» из раскрывающегося списка выберите требуемое значение;
  - в поле «Субъект федерации» из раскрывающегося списка выберите требуемое значение;
  - в поле «Населенный пункт» введите требуемое значение;

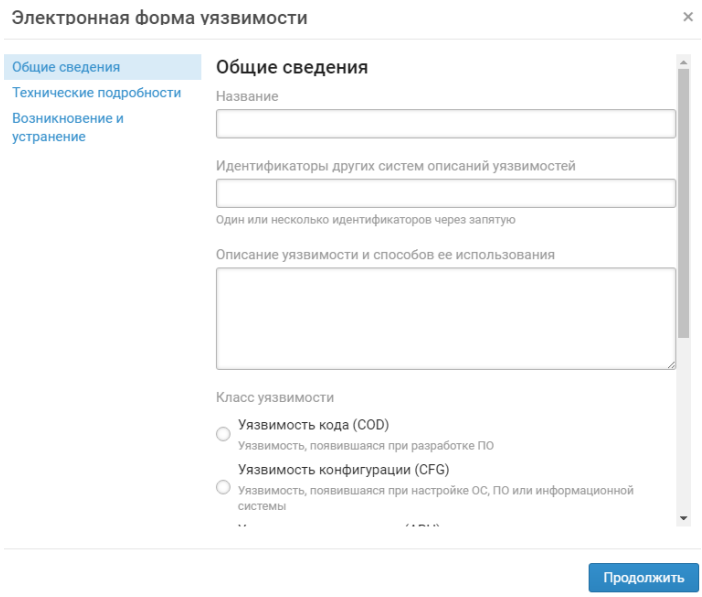


Рисунок 39 – Добавление общих сведений об уязвимости

- Нажмите кнопку «Продолжить». Откроется вкладка «Технические подробности».
- Во вкладке «Технические подробности» (Рисунок 40) необходимо:
  - в поле «Тип недостатка» выберите из выпадающего списка соответствующее значение типа недостатка.
  - в блоке параметров «Программное обеспечение» в поле «Название» введите название программного обеспечения;
  - в поле «Версия» введите версию программного обеспечения;
  - в поле «Служба или порт, который используется для функционирования ПО» укажите службу или порт;

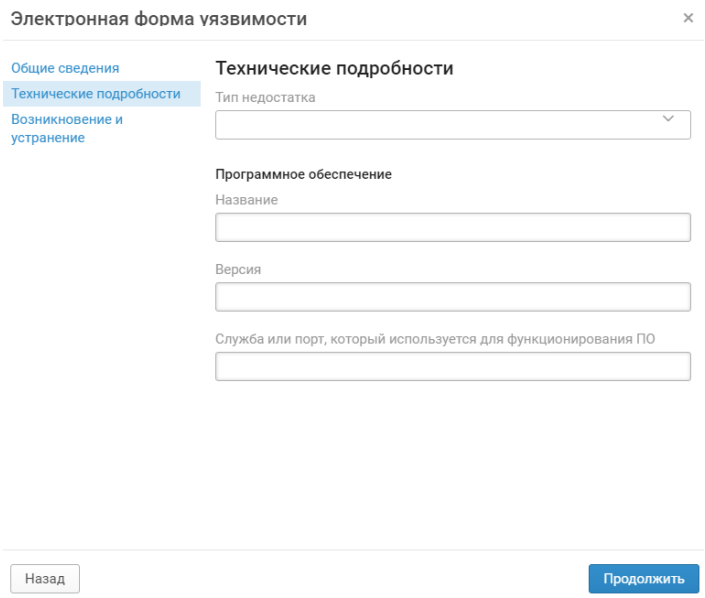


Рисунок 40 – Добавление технических подробностей об уязвимости

- Нажмите кнопку «Продолжить». Откроется вкладка «Возникновение и устранение». В открывшейся форме (Рисунок 41):
  - в поле «Место возникновения или появления уязвимости» из выпадающего списка выберите нужное значение;
  - в поле «Операционная система и иное окружение уязвимого ПО» введите название операционной системы и иного окружения уязвимого ПО;
  - в поле «Дата выявления» укажите дату выявления уязвимости (поле обязательно для заполнения);
  - в поле «Автор, опубликовавший информацию о выявленной уязвимости» укажите организацию, которая обнаружила уязвимость, или ссылку на источник;
  - в поле «Способ обнаружения» введите способ обнаружения;
  - в поле «Автоматизированное правило обнаружения» перетащите или выберите файл;
  - в поле «Рекомендации по устранению уязвимости» введите рекомендации по устранению;
  - в поле «Прочая информация» введите дополнительную информацию;

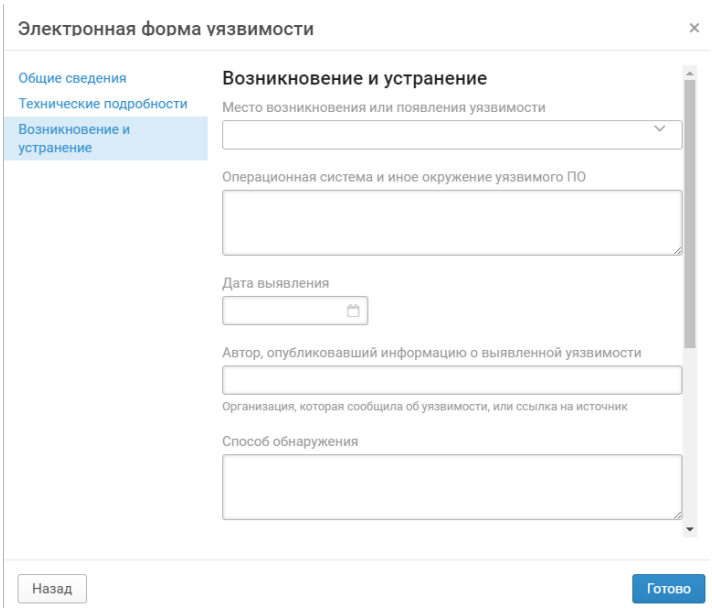


Рисунок 41 – Добавление информации по возникновению и устранению уязвимости

- Заполните поля «Тема» и «Написать сообщение…» при необходимости.
- Нажмите кнопку «Создать запрос» и в открывшемся окне «Заполнить и зарегистрировать запрос».
- Запрос об уязвимости создан.

2.5.6 Создание запроса о публикации

Для регистрации запроса о публикации:

- Из списка (Рисунок 14) выберите пункт меню «Публикации». В открывшейся форме, во вкладке «общие сведения» (Рисунок 43):
  - в поле «Наименование мероприятия» введите наименование мероприятия (Поле обязательно для заполнения);
  - в поле «Описание» введите описание мероприятия (Поле обязательно для заполнения);
  - в поле «Наименование организации» введите название организации (Поле обязательно для заполнения);

- для добавления информации по контактному лицу к публикации необходимо нажать кнопку «Добавить ответственное лицо» (Поле обязательно для заполнения) (Рисунок 43), заполнить данные для создаваемого контакта (Рисунок 42):

- в поле «Имя» введите имя (Поле обязательно для заполнения) ;
- в поле «Фамилия» введите фамилию (Поле обязательно для заполнения);
- в поле «Отчество» введите отчество (Поле обязательно для заполнения);
- в поле «Должность» введите должность (Поле обязательно для заполнения);
- в поле «Городской телефон» введите название города (Поле обязательно для заполнения);
- в поле «Мобильный телефон» введите номер телефона (Поле обязательно для заполнения);
- в поле «Адрес эл. Почты» укажите адрес электронной почты (Поле обязательно для заполнения);
- нажмите кнопку «Готово».

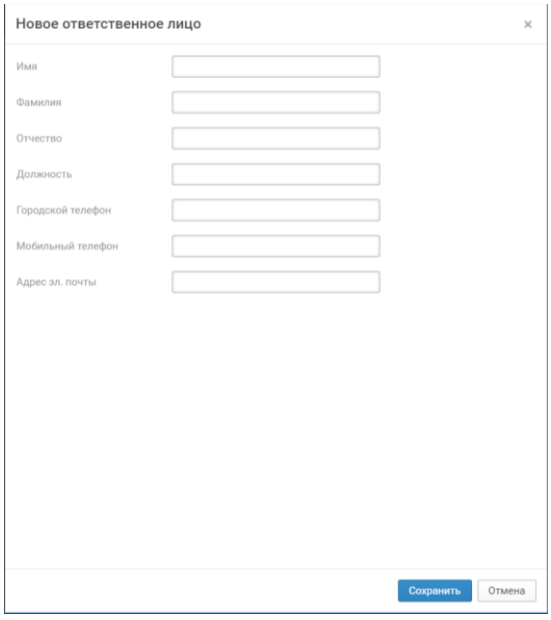


Рисунок 42 – Добавление контактного лица

- в поле «Дата мероприятия» выберите дату и время;
- в поле «Федеральный округ» из раскрывающегося списка выберите требуемое значение (Поле обязательно для заполнения);
- в поле «Субъект федерации» из раскрывающегося списка выберите требуемое значение (Поле обязательно для заполнения);
- в поле «Населенный пункт» введите требуемое значение (Поле обязательно для заполнения);

Нажмите кнопку «Продолжить». Откроется вкладка «Мероприятие». В открывшейся форме

- в раскрывающемся списке «Тип мероприятия» выберите соответствующее значение типа мероприятия;
- в поле «Текст мероприятия» введите Текст мероприятия (Поле обязательно для заполнения);
- так же можно загрузить файл с текстом мероприятия
- нажмите кнопку «Готово».

- Откроется страница Запросы.
- Заполните поля «Тема» и «Написать сообщение…» при необходимости.
- Нажмите кнопку «Создать запрос» и в открывшемся окне «Заполнить и зарегистрировать запрос».
- Запрос о публикации создан.

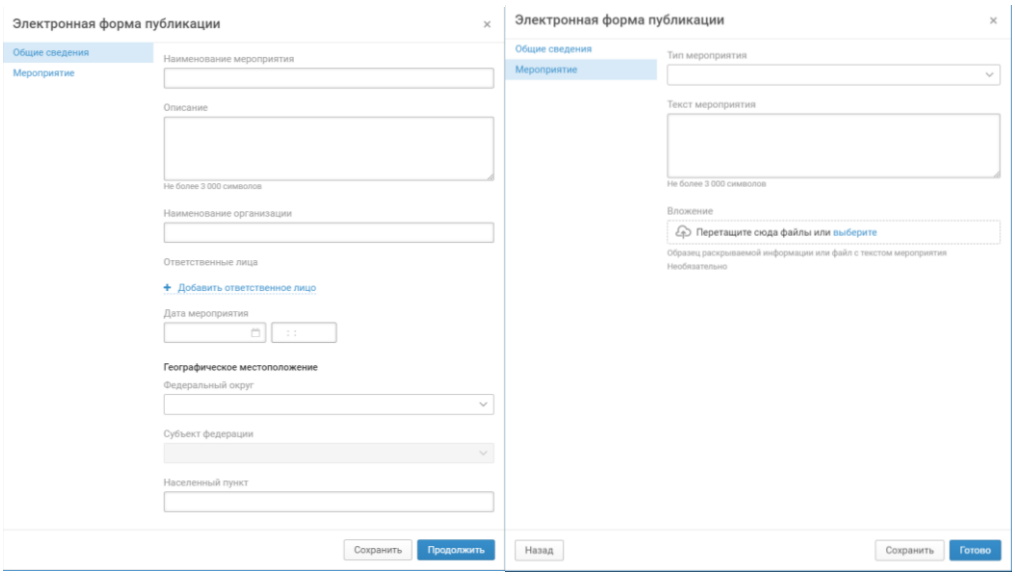


Рисунок 43 – Добавление информации публикации

2.5.7 Создание произвольных запросов

Для регистрации других (произвольных) запросов:

- Из списка (Рисунок 14) выберите пункт меню «Другое».
- В открывшейся форме (Рисунок 44):
  - в правой панели в поле «Тема» ввести тему запроса;
  - в поле «Написать сообщение» введите сообщение;
  - в поле «Вложения» перетащите или выберите файл, или по кнопке «Добавить» добавьте информацию об инциденте, участнике, уязвимости, угрозе или публикации;
  - нажмите кнопку «Создать запрос».
- Запрос создан.

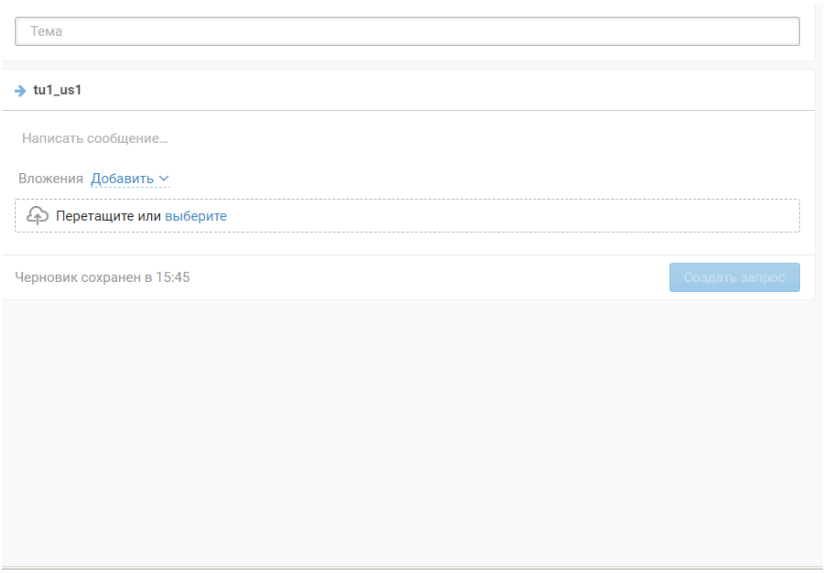


Рисунок 44 – Формирование других запросов

2.5.8 Электронная форма инцидента

Набор вкладок и полей электронной формы инцидента зависит от типа инцидента. Для определения типа инцидента в раскрывающемся списке (см. Рисунок 15) выберите тип инцидента в одной из групп: с вектором EXT (2.5.8.1) или с вектором INT (2.5.8.2). Поле обязательно для заполнения.

После выбора появиться вкладка «Вектор инцидента — EXT» или «Вектор инцидента — INT» в поле «Тип инцидента» (общая) выберите требуемое значение из выпадающего списка. Для типов «Вектор инцидента — EXT» и «Вектор инцидента — INT» значения общие:

- Нарушение требований к обеспечению защиты информации, при осуществлении банковской деятельности
- Нарушение требований к обеспечению защиты информации, при осуществлении деятельности в сфере финансовых рынков
- Неоказание или несвоевременное оказание услуг по переводу денежных средств
- Неоказание или несвоевременное оказание финансовых услуг

В поле «События» нажмите кнопку «Добавить событие». Далее в открывшемся окне (Рисунок 45) добавьте информацию по зарегистрированному событию:

- выберите в поле «Событие» требуемое тип зарегистрированного события;
- выберите в поле «Тип нарушителя» требуемое значение;
- нажмите кнопку «Сохранить»;

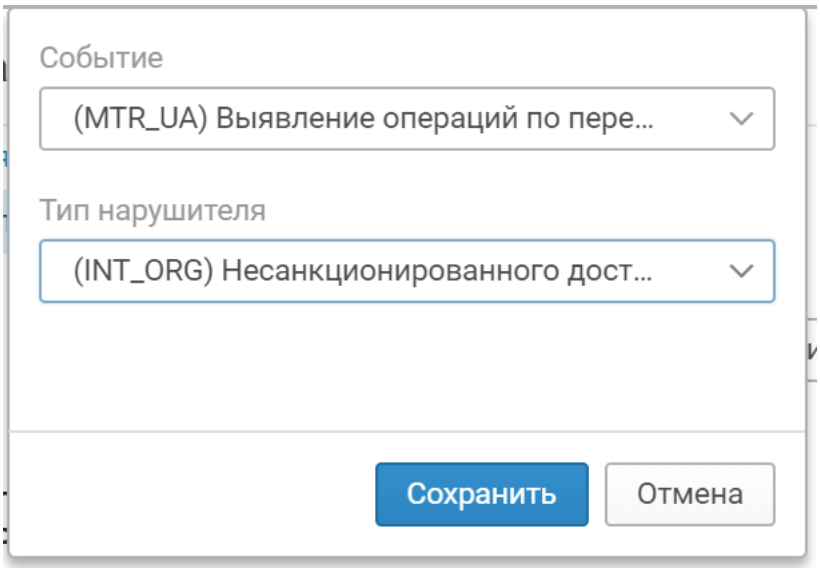


Рисунок 45 – Добавление события

Внимание! Детальная информация по инциденту указывается на отдельных вкладках (2.5.8.2). Их состав зависит от выбранного типа инцидента.

2.5.8.1 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:

- Использование вредоносного программного обеспечения (malware);
- Использование методов социальной инженерии (socialEngineering);
- Эксплуатация уязвимостей информационной инфраструктуры (vulnerabilities);
- Реализация спам рассылки (spams);
- Взаимодействие с центрами «бот-нет» сетей (controlCenters);
- Изменения IMSI на SIM-карте, смена IMEI телефона (sim);
- Использование фишинговых ресурсов (phishingAttacks);
- Размещение запрещенного контента в сети «Интернет» (prohibitedContents);
- Размещение вредоносного ресурса в сети «Интернет» (maliciousResources);
- Иная компьютерная атака (other).

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

2.5.8.2 Параметры инцидентов с вектором EXT

Тип инцидента — Использование вредоносного программного обеспечения (malware):

- Вкладка «Влияние и способ заражения»:

- Внешний IP-адрес узла.
- Блок параметров Адрес, с которого загружено вредоносное ПО. Укажите Доменное имя, IP-адрес и URL.
- Взаимодействие с узлами. В случае выявления взаимодействия зараженной ЭВМ с каким-либо ресурсом, который может являться вредоносным, укажите Доменное имя, IP-адрес и URL этого ресурс.
- Классификаторы. Укажите наименование антивирусной системы и тип вредоносного ПО. Поле может содержать несколько значений.
- 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»:
  - 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.
  - Хеш-сумма. Укажите контрольную сумму каждого образца вредоносного ПО.
- Вкладка «Вредоносные письма»:
  - Адреса, с которых поступали письма. Укажите адрес электронной почты, с которого пришло письмо, и IP-адрес последнего почтового сервера, через который было передано письмо.
  - 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, выбрав из выпадающего списка:
  - Сетевые индикаторы. Обращение по IP/URL-адресу
  - Сетевые индикаторы. Модификация текущих сетевых параметров
  - Сетевые индикаторы. Сокрытие следов сетевого взаимодействия

- Файловые индикаторы. Создание файлов
- Файловые индикаторы. Изменение файлов
- Файловые индикаторы. Удаление файлов
- Индикаторы реестра ОС Windows. Создание записей реестра
- Индикаторы реестра ОС Windows. Изменение записей реестра
- Индикаторы реестра ОС Windows. Удаление записей реестра
- Индикаторы, связанные с процессами. Запуск процесса
- Индикаторы, связанные с процессами. Изменение запущенного процесса
- Индикаторы, связанные с процессами. Завершение процесса
- Иные индикаторы. Создание
- Иные индикаторы. Изменение
- Иные индикаторы. Удаление

Тип инцидента — socialEngineering:

- Вкладка «Описание по типу»:
  - Тип. Укажите метод социальной инженерии: звонок с мобильного телефона, звонок с немобильного номера, SMS-сообщение, социальная инженерия с использованием социальных сетей, социальная инженерия с использованием средств мгновенных сообщений.
  - Примечание. Опишите инцидент.
  - Добавьте Источники социальной инженерии: номер телефона, электронная почта, IP-адрес почтового сервера
  - 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 — vulnerabilities:

Внешний адрес пострадавшей системы

- IP-адрес;
- Доменное имя;
- URL-адрес;
- Тип сервиса. Какие службы были запущены на пострадавшей машине.

Атака

- Источники атак: IP-адрес источника или URL источника, если есть;
- Идентификатор уязвимости;
- Метрика CVSS;

Свой идентификатор уязвимости

- Описание;
- Название ПО;
- Версия ПО;
- Тип уязвимости;
- Класс уязвимости;
- Дата обнаружения;
- Базовый CVSS;
- Опасность;
- Меры устранения;
- Статус;
- Наличие эксплойта;
- Рекомендации;
- Ссылки;
- Вендор.

Тип инцидента — spams:

Спам

- Дата получения (Необязательно);

  Цель атаки

- Адреса электронной почты (Необязательно);

  Источник атаки (Необязательно);

- IP-адрес;
- Доменное имя;
- Адрес электронной почты;

Тип инцидента — controlCenters:

- IP-адрес пострадавшей системы;
- URL-адрес пострадавшей системы;
- Информация с ЦУ бот-сети. URL с ЦУ;
- IP-адрес злоумышленника;
- Действия злоумышленника. Опишите, что предшествовало инциденту, какие действия злоумышленника удалось выявить;
- Сведения о бот-сети. Сведения о бот-сети, которые удалось выяснить;
- IP-адреса, обращавшиеся к ЦУ.

Тип инцидента — sim:

- Оператор связи (Необязательно);
- Номер телефона (Необязательно);
- IMSI (Необязательно);
- Дата смены IMSI (Необязательно);

Тип инцидента — Использование фишинговых ресурсов (phishingAttacks):

- Пострадавшая система. IP-адрес;
- Пострадавшая система. Домен;
- Фишинговый ресурс. Добавьте IP-адрес ресурса или URL-адрес ресурса;
- Дата фиксации.

Тип инцидента — prohibitedContents:

- IP-адрес запрещённого ресурса (Необязательно);
- Единый указатель ресурса (Необязательно);
- Тип контента (Необязательно).

Тип инцидента — maliciousResources:

- IP-адрес вредоносного ресурса;
- URL-адрес вредоносного ресурса;
- Описание вредоносной активности (Необязательно).

Тип инцидента — other:

- Описание (Необязательно)
- Тип атаки (Необязательно)
- Цель атаки. IP-адрес (Необязательно)

  Цель атаки. Единый указатель ресурса (Необязательно)

2.5.8.3 Типы инцидентов с вектором INT

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

- Изменение маршрутно-адресной информации (trafficHijackAttacks);
- Использование вредоносного программного обеспечения (malware);
- Реализация атаки типа «отказ в обслуживании» (ddosAttacks);
- Реализация несанкционированного доступа к банкоматам и платежным терминалам (atmAttacks);
- Эксплуатация уязвимостей информационной инфраструктуры (vulnerabilities);
- Компроментация аутентификационных/учетных данных (bruteForces);
- Реализация спам рассылки (spams);
- Взаимодействие с центрами «бот-нет» сетей (controlCenters);
- Использование фишинговых ресурсов (phishingAttacks);
- Размещение запрещенного контента в сети «Интернет» (prohibitedContents);

- Размещение вредоносного ресурса в сети «Интернет» (maliciousResources);
- Выполнение изменение контента (changeContent);
- Выполнение сканирования портов (scanPorts);
- Иная компьютерная атака (other).

2.5.8.4 Параметры инцидентов с вектором INT

Тип инцидента — trafficHijackAttacks:

- Штатный AS-path Необязательно
- Подставной AS-path (Необязательно)
- Ссылка на Looking Glass (Необязательно)
- Штатный prefix (Необязательно)
- Подставной prefix (Необязательно)

Тип инцидента — malware:

- Вкладка «Влияние и способ заражения»:
  - Внешний IP-адрес узла.
  - Блок параметров Адрес, с которого загружено вредоносное ПО. Укажите Доменное имя, IP-адрес и URL.
  - Взаимодействие с узлами. В случае выявления взаимодействия зараженной ЭВМ с каким-либо ресурсом, который может являться вредоносным, укажите Доменное имя, IP-адрес и URL этого ресурс.
  - Классификаторы. Укажите наименование антивирусной системы и тип вредоносного ПО. Поле может содержать несколько значений.
  - 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»:
  - 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.

- Хеш-сумма. Укажите контрольную сумму каждого образца вредоносного ПО.

- Вкладка «Вредоносные письма»:
  - Адреса, с которых поступали письма. Укажите адрес электронной почты, с которого пришло письмо, и IP-адрес последнего почтового сервера, через который было передано письмо.
  - 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, выбрав из выпадающего списка:
  - Сетевые индикаторы. Обращение по IP/URL-адресу
  - Сетевые индикаторы. Модификация текущих сетевых параметров
  - Сетевые индикаторы. Сокрытие следов сетевого взаимодействия
  - Файловые индикаторы. Создание файлов
  - Файловые индикаторы. Изменение файлов
  - Файловые индикаторы. Удаление файлов
  - Индикаторы реестра ОС Windows. Создание записей реестра
  - Индикаторы реестра ОС Windows. Изменение записей реестра
  - Индикаторы реестра ОС Windows. Удаление записей реестра
  - Индикаторы, связанные с процессами. Запуск процесса
  - Индикаторы, связанные с процессами. Изменение запущенного процесса
  - Индикаторы, связанные с процессами. Завершение процесса
  - Иные индикаторы. Создание
  - Иные индикаторы. Изменение

- Иные индикаторы. Удаление

Тип инцидента — ddosAttacks:

- Адрес пострадавшей системы. IP-адрес
- Адрес пострадавшей системы. Сеть. В формате маски подсети
- Адрес пострадавшей системы. Доменное имя
- Адрес пострадавшей системы. Назначение ресурса
- Адрес пострадавшей системы. URL-адрес
- Адрес пострадавшей системы. Тип сервиса. Какие службы были запущены на пострадавшей машине
- Атака. IP-адреса источников. Не более 100 IP-адресов. Можно добавить IP-адреса вручную, загрузить из файла (формат plain text) или скопировать. Разделители — запятая, точка с запятой, пробел, перевод строки.
- Атака. Тип атаки. Детали можно указать в примечаниях
- Атака. Примечание
- Начало атаки
- Окончание атаки
- Мощность PPS (пакетов в секунду)
- Мощность RPS (запросов в секунду)
- Негативное влияние. Тип и Примечание

Тип инцидента — atmAttacks:

- Пострадавший объект. Тип объекта. Детали можно указать в примечаниях;
- Пострадавший объект. Примечание;
- Атака. Тип атаки. Детали можно указать в примечаниях;
- Атака. Примечание;
- Вложения.

Тип инцидента — vulnerabilities:

Внешний адрес пострадавшей системы

- IP-адрес;
- Доменное имя;
- URL-адрес;
- Тип сервиса. Какие службы были запущены на пострадавшей машине.

Атака

- Источники атак: IP-адрес источника или URL источника, если есть;
- Идентификатор уязвимости;
- Метрика CVSS;

Свой идентификатор уязвимости

- Описание;
- Название ПО;
- Версия ПО;
- Тип уязвимости;
- Класс уязвимости;
- Дата обнаружения;
- Базовый CVSS;
- Опасность;
- Меры устранения;
- Статус;
- Наличие эксплойта;
- Рекомендации;
- Ссылки;
- Вендор.

Тип инцидента — bruteForces:

- Адрес пострадавшей системы. IP-адрес;
- Адрес пострадавшей системы. URL-адрес;

- Атакованная служба;
- Атака. IP-адреса источников. Не более 100 IP-адресов. Можно добавить IP-адреса вручную, загрузить из файла (формат plain text) или скопировать. Разделители — запятая, точка с запятой, пробел, перевод строки.
- Скомпрометированная учетная запись. Учетная запись;
- Скомпрометированная учетная запись. Логин;
- Скомпрометированная учетная запись. Привилегии. Через запятую или построчно.

Тип инцидента — spams:

Спам

- Дата получения (Необязательно);

Цель атаки

- Адреса электронной почты (Необязательно);

Источник атаки (Необязательно);

- IP-адрес;
- Доменное имя;
- Адрес электронной почты;

Тип инцидента — controlCenters:

- IP-адрес пострадавшей системы;
- URL-адрес пострадавшей системы;
- Информация с ЦУ бот-сети. URL с ЦУ;
- IP-адрес злоумышленника;
- Действия злоумышленника. Опишите, что предшествовало инциденту, какие действия злоумышленника удалось выявить;
- Сведения о бот-сети. Сведения о бот-сети, которые удалось выяснить;
- IP-адреса, обращавшиеся к ЦУ.

Тип инцидента — Использование фишинговых ресурсов (phishingAttacks):

- Пострадавшая система. IP-адрес;
- Пострадавшая система. Домен;
- Фишинговый ресурс. Добавьте IP-адрес ресурса или URL-адрес ресурса;
- Дата фиксации.

Тип инцидента — prohibitedContents:

- IP-адрес запрещённого ресурса (Необязательно);
- Единый указатель ресурса (Необязательно);
- Тип контента (Необязательно).

Тип инцидента — maliciousResources:

- IP-адрес вредоносного ресурса;
- URL-адрес вредоносного ресурса;
- Описание вредоносной активности (Необязательно).

Тип инцидента — changeContent:

- Изменённый ресурс. IP-адрес (Необязательно);
- Изменённый ресурс. URL-адрес (Необязательно);
- Тип изменённого контента.

Тип инцидента — scanPorts:

- Источники сканирования. Не более 100 IP-адресов. Можно добавить IP-адреса вручную, загрузить из файла (формат plain text) или скопировать. Разделители — запятая, точка с запятой, пробел, перевод строки.
- Сканированные порты;
- Метод сканирования;
- Дата и время начала сканирования;
- Дата и время окончания сканирования.

Тип инцидента — other:

- Описание (Необязательно);
- Тип атаки (Необязательно);

- Цель атаки. IP-адрес (Необязательно);
- Цель атаки. Единый указатель ресурса (Необязательно).

3 Отправка информации по резервным каналам передачи данных

Информация о запланированных работах публикуется на информационном портале (http://portal.fincert.cbr.ru) в разделе «Новости» а также в виде информационного бюллетеня. В период технических работ на АСОИ ФинЦЕРТ для передачи информации в ФинЦЕРТ требуется использовать электронную почту fincert@cbr.ru а также передавать информацию по телефону 8 (495) 772-70-90.

4 Ошибки

4.1 Ошибки при установке защищенного соединения при использовании TLS-клиента

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

- Не работает подключение TLS клиента через прокси сервер.
- Не осуществляется регистрация ПО

При появлении данных ошибок необходимо:

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

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

4.2 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.

4.3 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.

4.4 Прочие ошибки и вопросы

В случае возникновения иных ошибок или вопросов по работе АСОИ ФинЦЕРТ просьба направлять обращения на адрес электронной почты svc_fincert_support@cbr.ru.

Приложение 1 Установка и настройка ПО

Перед началом работы необходимо получить в Центральном банке Российской Федерации (по ссылке http://cbr.ru/StaticHtml/File/14408/ASOI_docs.zip):

- конфигурационный файл для TLS-клиента с настройками подключения к АСОИ ФинЦЕРТ;
- корневые сертификаты Национального и Головного удостоверяющих центров;
- сертификаты ресурсов portal.fincert.cbr.ru, lk.fincert.cbr.ru;
- сертификаты ресурсов среды тестирования zoe-portal.fincert.cbr.ru, zoe-lk.fincert.cbr.ru, zoe-api.fincert.cbr.ru;
- руководство участника по работе с АСОИ ФинЦЕРТ;
- регламент подключения Участников к АСОИ финЦЕРТ.

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

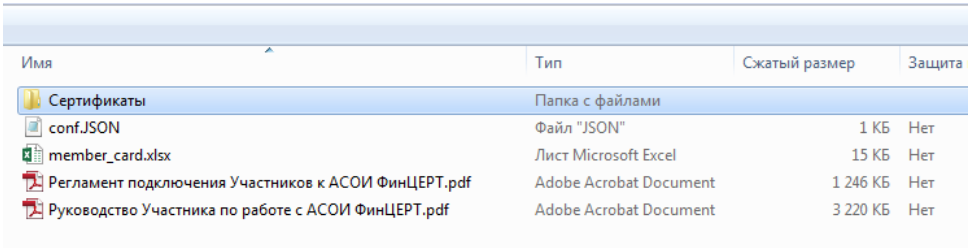


Рисунок 46 – Состав архива АСОИ ФинЦЕРТ

- Сертификаты – каталог, содержащий:

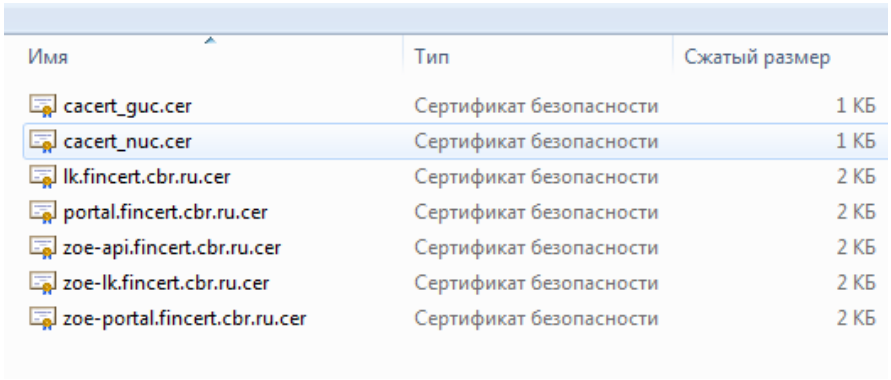


Рисунок 47 – Содержание каталога Континент TLS-client

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

1.1 Требования к АРМ

Для работы с АСОИ ФинЕРТ должны использоваться АРМ с характеристиками, не хуже представленными 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 разрешение не менее 1920x1080 точек

На АРМ, должно быть установлено следующее программное обеспечение:

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

- Lissi CSP;
- Континент TLS-клиент (поддерживается работа и в других браузерах. Участникам предоставляется безвозмездно);

- средство антивирусной защиты.

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

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

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

Установка СКЗИ осуществляется в соответствии с эксплуатационной документацией на них.

В п. 1.3 описана установка Континент TLS-клиент как основного средства для доступа к АСОИ ФинЦЕРТ.

1.2 Требования к подключению

Для подключения к АСОИ ФинЦЕРТ на стороне Участника должно быть реализованы следующие настройки:

- сетевые правила, разрешающие подключение по порту 443 к адресам:
  - portal.fincert.cbr.ru;
  - lk.fincert.cbr.ru.
- в средстве антивирусной защиты должен быть отключен контроль исходящих соединений на 443 порт при использовании для доступа к АСОИ ФинЦЕРТ ПО Континент TLS-клиент;
- установлено СКЗИ для работы с АСОИ с ФинЦЕРТ, соответствующее следующим требованиям:
  - поддержка реализации протокола TLS с ГОСТ 2001/2012;
  - работа с браузерами, поддерживаемыми системой.

1.3 Установка и настройка TLS-клиента

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

Для этого:

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

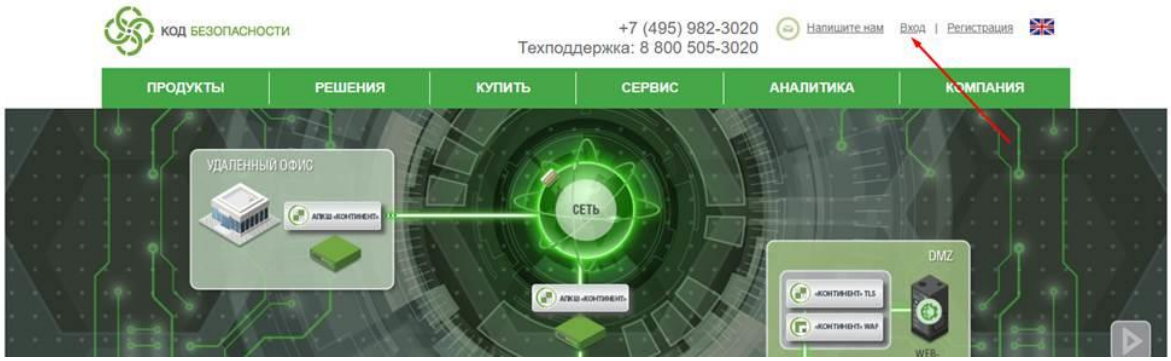


Рисунок 48 – сайт Код Безопасности, на котором можно скачать TLS-клиент

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

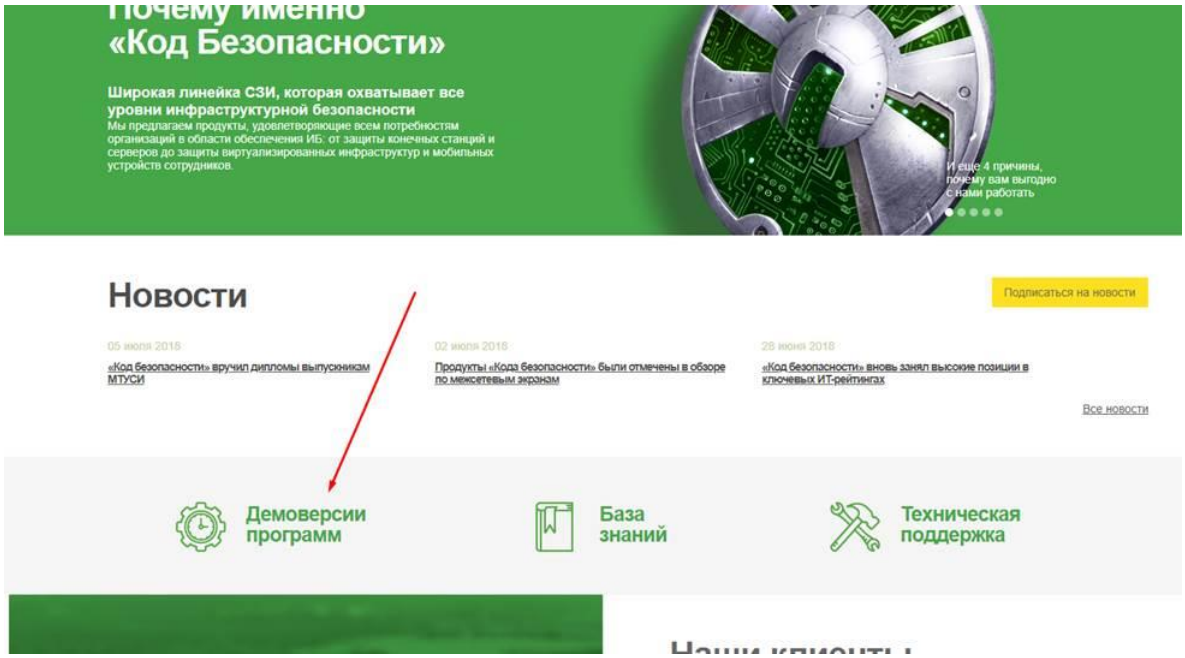


Рисунок 49 – сайт Код Безопасности, главная страница, демоверсии программ

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

Рисунок 50 – сайт Код Безопасности, регистрация

В открывшемся окне заполнить форму регистрации:

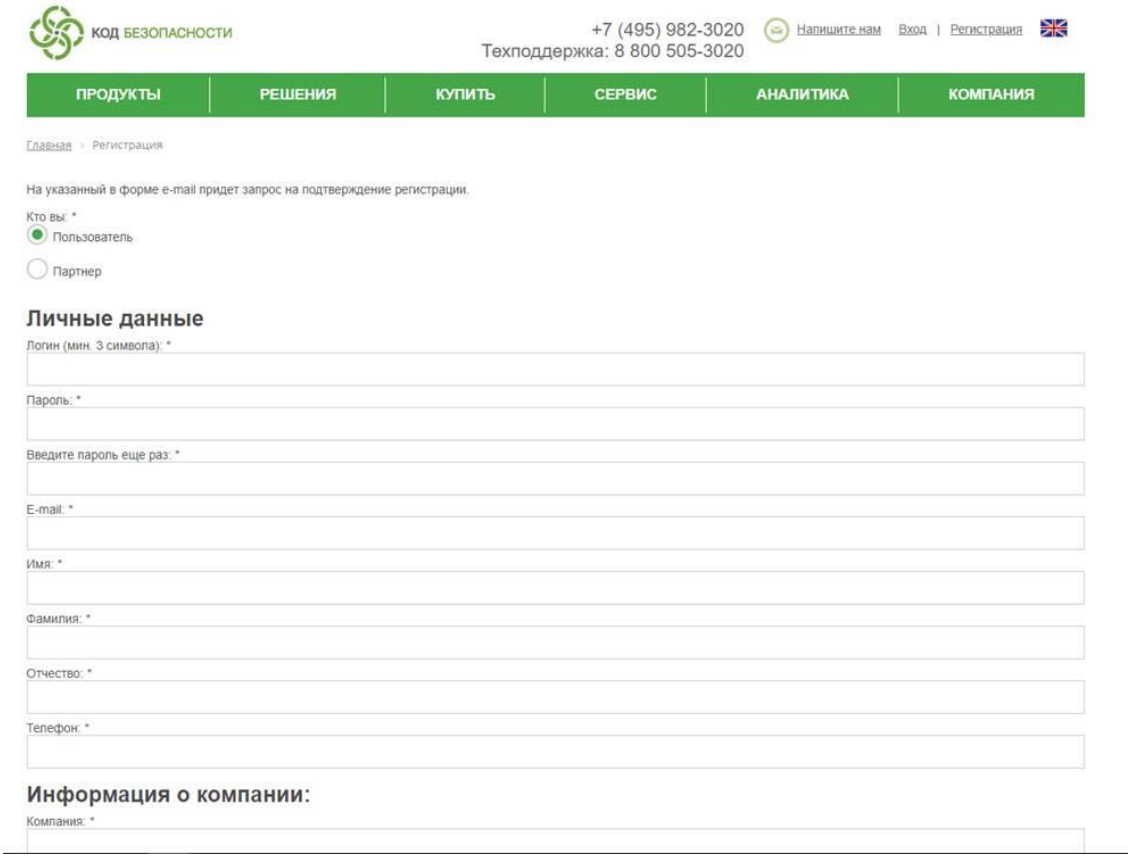


Рисунок 51 – сайт Код Безопасности, регистрация, заполнение полей для создания учетной записи.

- После успешной регистрации и аутентификации под своими учетными данными, переходим в раздел демоверсии: https://www.securitycode.ru/products/demo-versions/Запустите на исполнение файл Континент TLS-клиент.exe. На экране появится окно установки TLS-клиента с текстом лицензионного соглашения (Рисунок 52).

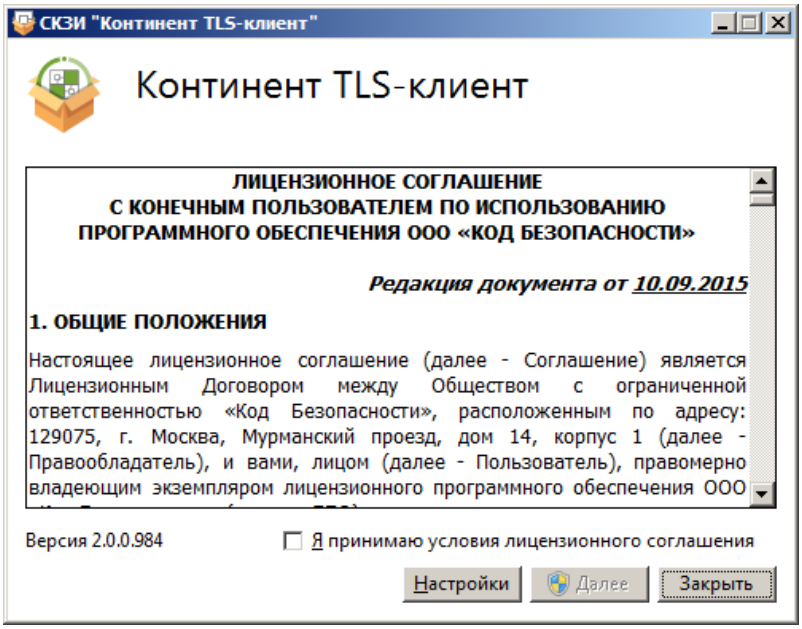


Рисунок 52 – Лицензионное соглашение

- Прочтите лицензионное соглашение и, если вы принимаете его условия, поставьте отметку в поле «Я принимаю условия лицензионного соглашения», затем нажмите кнопку «Далее» (Рисунок 53).

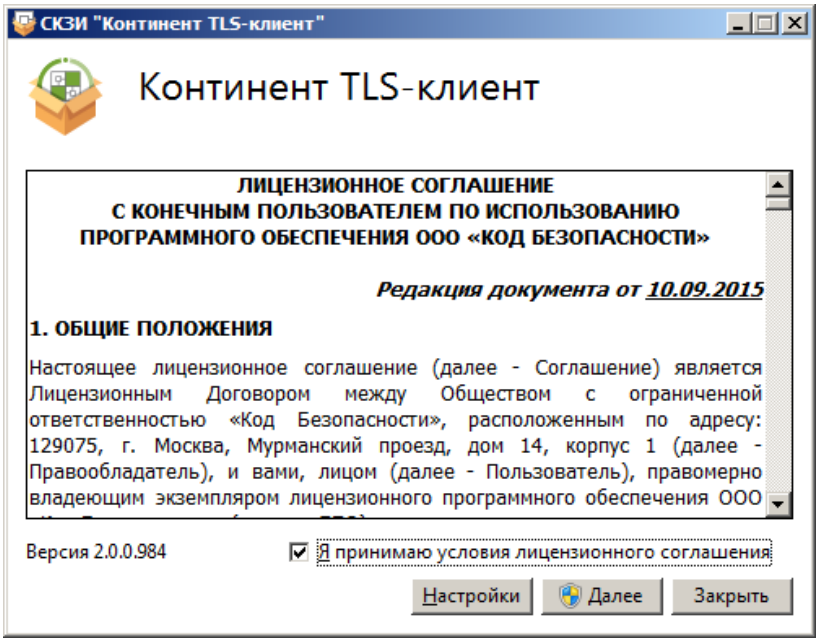


Рисунок 53 – Продолжение установки после ознакомления с лицензионным соглашением

- Программа установки выполнит диагностику системы, после чего начнется установка ПО. После ее успешного завершения на экране появится сообщение о необходимости перезагрузки компьютера (Рисунок 54).

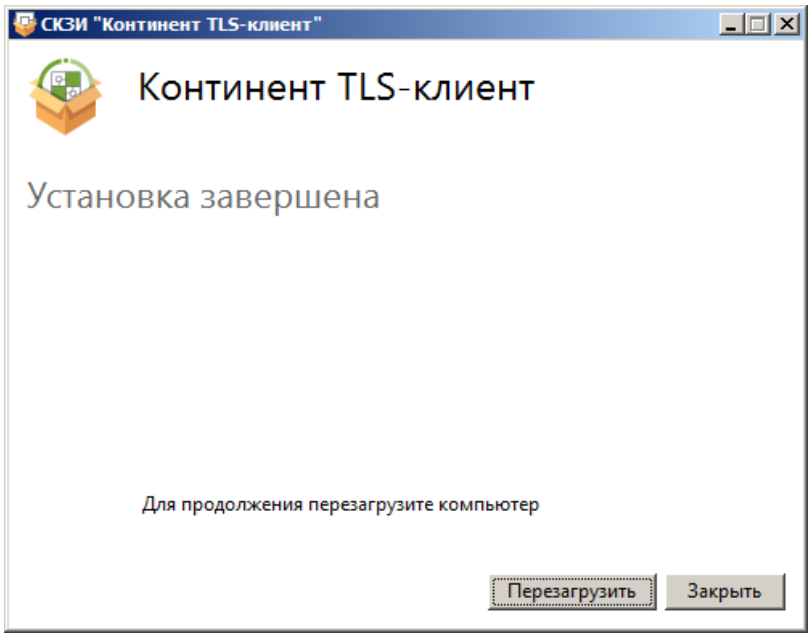


Рисунок 54 – Завершение установки

- Нажмите кнопку «Перезагрузить» в окне сообщения. Начнется перезагрузка компьютера. После установки TLS-клиента на рабочем столе Windows появится ярлык запуска графического приложения TLS-клиента, а в главном меню Windows появится раздел «Код Безопасности».
- При первом запуске TLS-клиента откроется окно с сообщением о накоплении энтропии для биологического датчика случайных чисел. Для выполнения этой процедуры необходимо будет кликать левой кнопкой «мыши» по мишени (Рисунок 55).

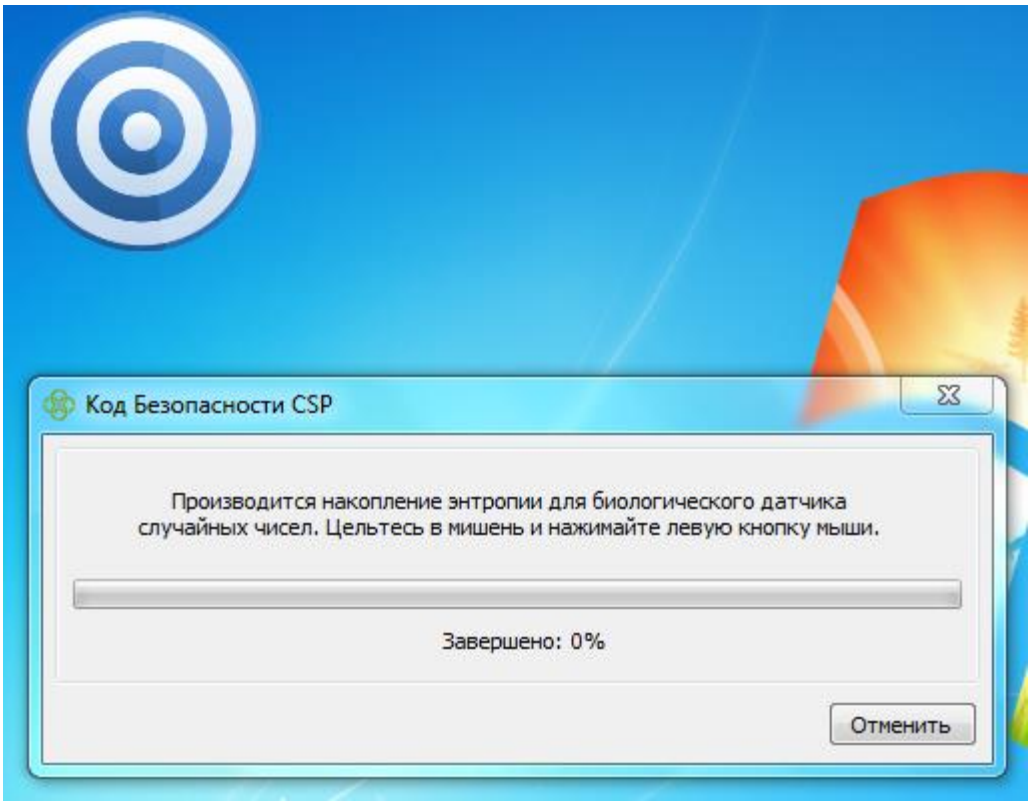


Рисунок 55 – Накопление энтропии для биологического датчика случайных чисел

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

Для регистрации TLS-клиента необходимо выполнить следующие действия:

- В открывшейся при запуске форме (Рисунок 56) нажать кнопку «Да».

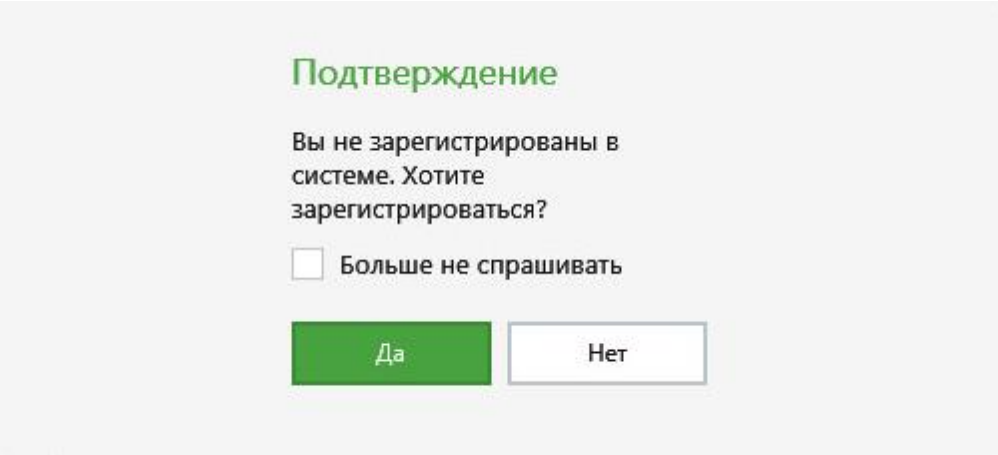


Рисунок 56 – Согласие о регистрации

- В случае отмены автоматического отображения окна регистрации при запуске TLS-клиента выберите в меню настроек TLS-клиента пункт «Регистрация» и нажмите кнопку «Начать» (Рисунок 57).

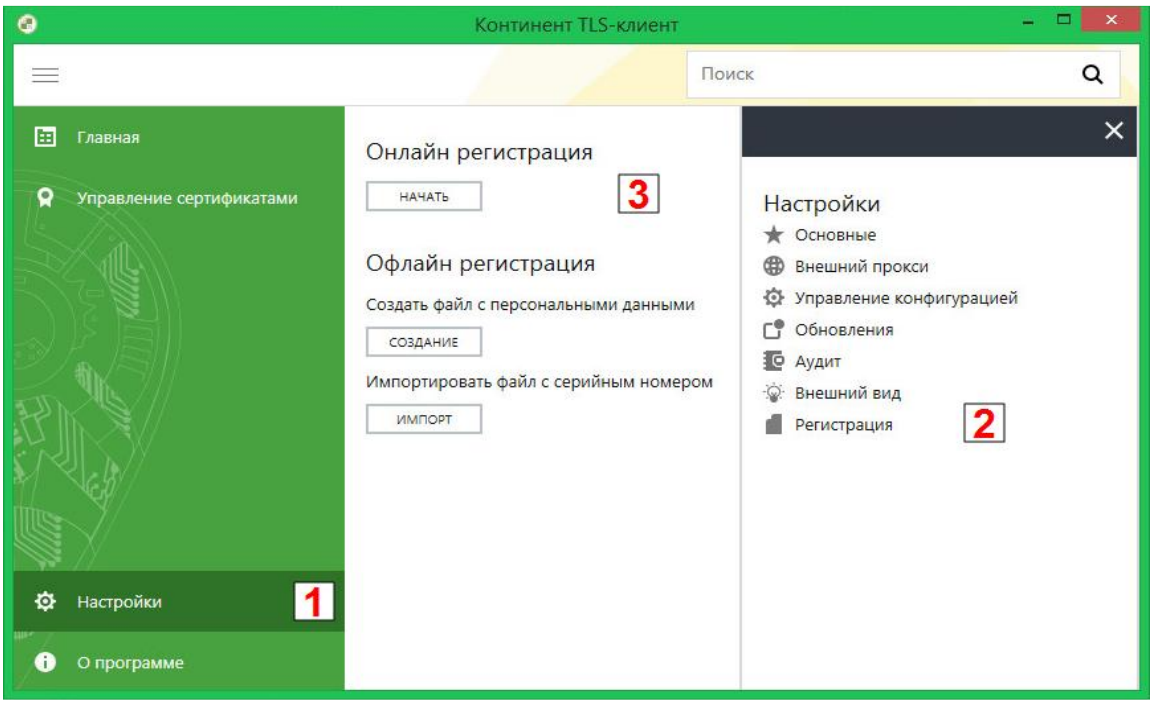


Рисунок 57 – Начало регистрации

- На экране появится диалоговое окно регистрации (Рисунок 58).

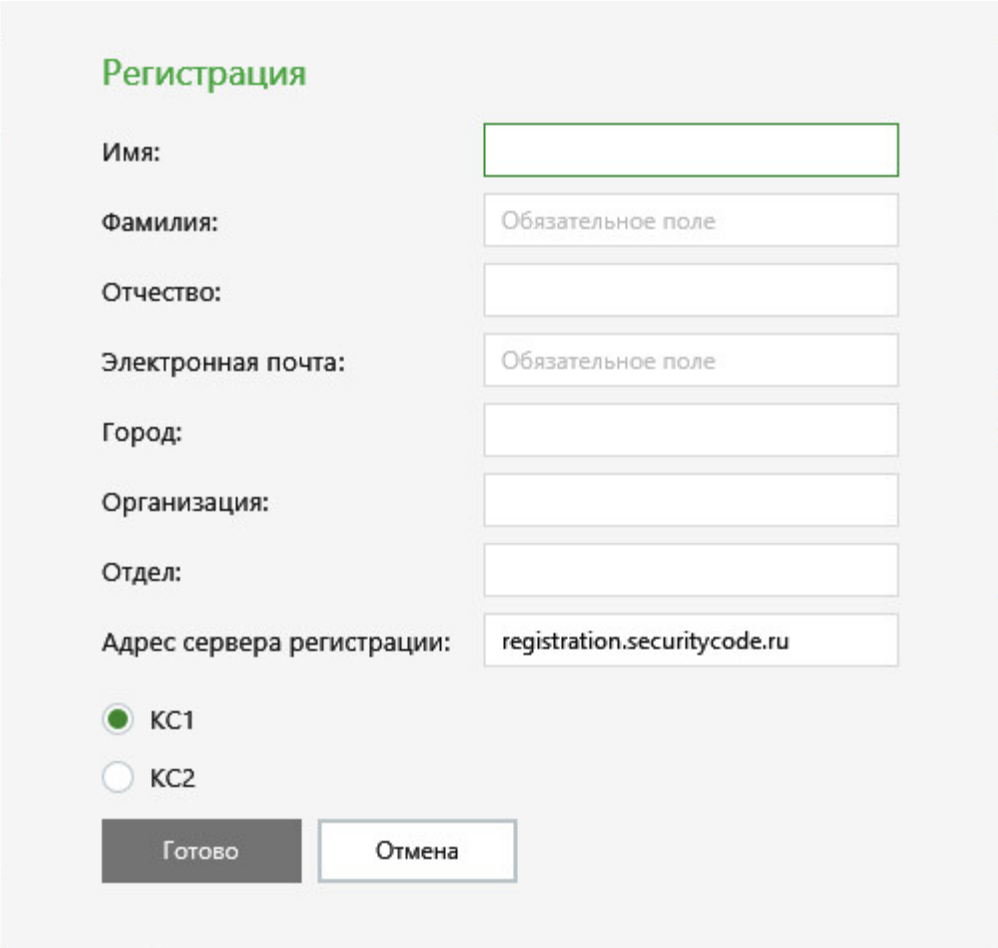


Рисунок 58 – Ввод регистрационных данных

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

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

После установки и регистрации TLS-клиента необходимо:

- Импортировать конфигурационный файл TLS-клиента conf.json, для этого необходимо:
  - запустить TLS-клиент на АРМ;
  - выбрать пункт «Настройки» - «Управление конфигурацией» (Рисунок 59);

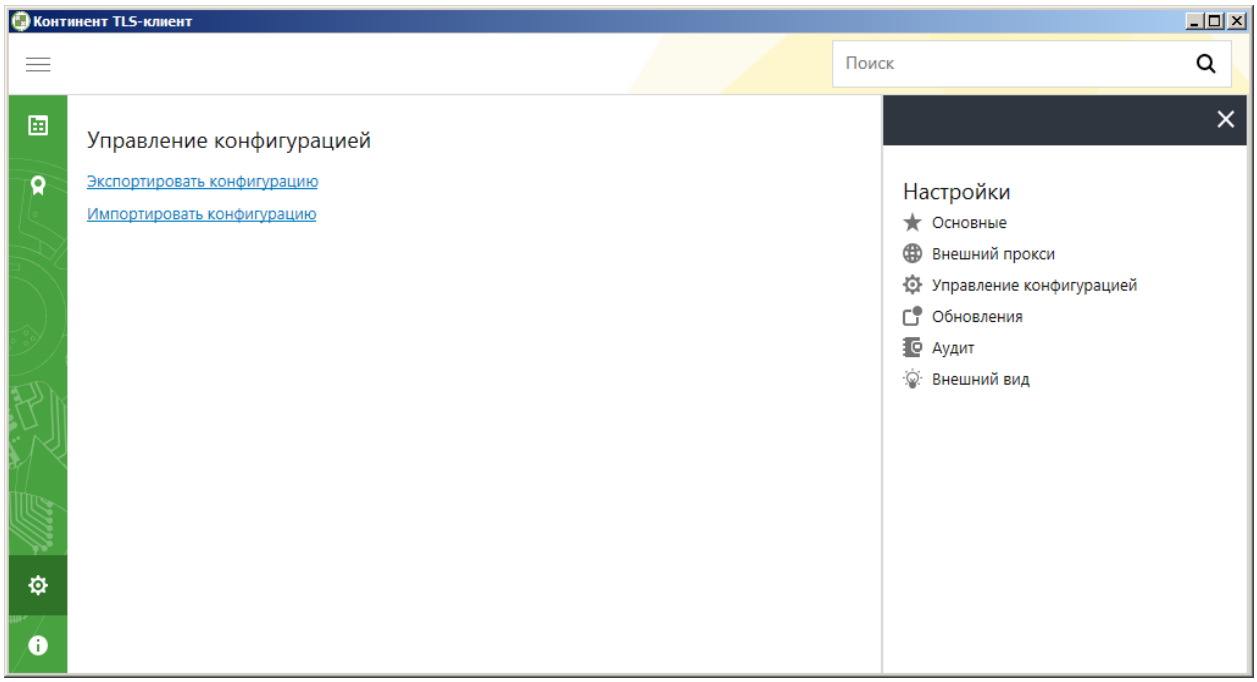
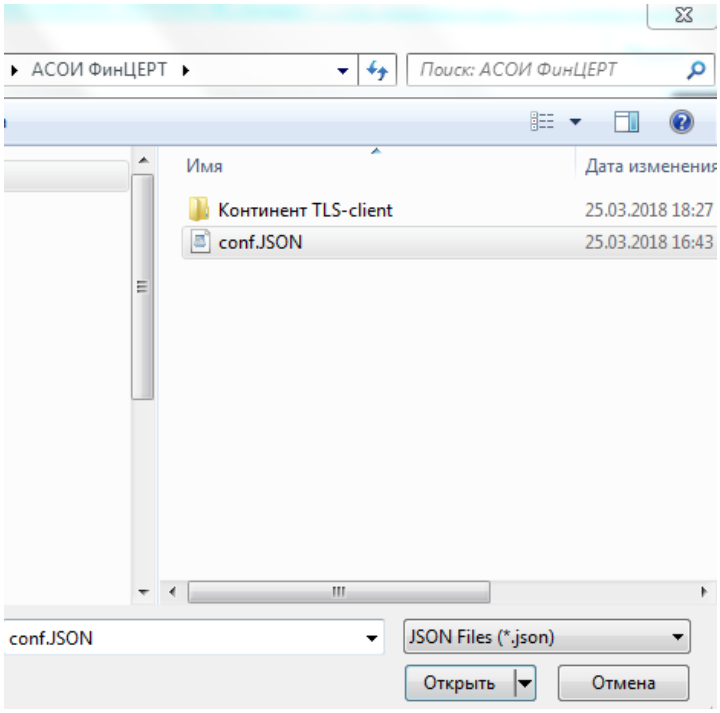


Рисунок 59 – Загрузка файла конфигурации

- в левой части выбрать пункт «Импортировать конфигурацию».



- осуществить загрузку файла конфигурации.
- в случае успешной загрузки появится сообщение (Рисунок 60).

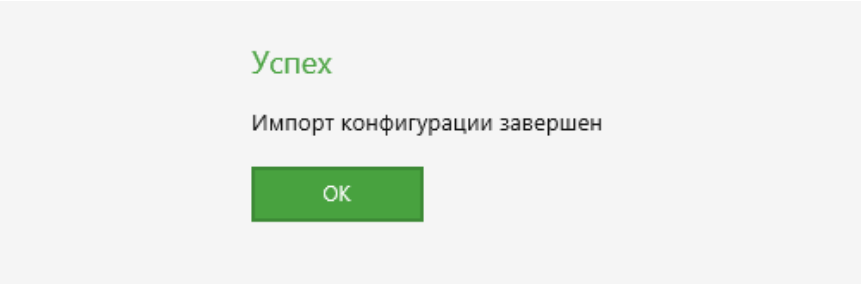


Рисунок 60 – Успешный результат загрузки файла конфигурации

- после нажатия кнопки «ОК» появится сообщение (Рисунок 61);
- подтвердить отключение проверки CRL, нажав кнопку «Да»

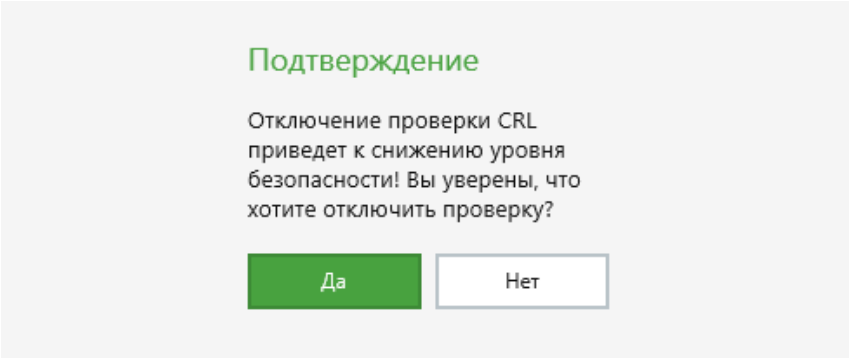


Рисунок 61. Сообщение об отключение проверки CRL

- Добавить сертификаты веб-ресурсов, для этого необходимо:
  - в главном окне программы перейти на вкладку «Управление сертификатами» и выбрать «Импортировать» (Рисунок 62);

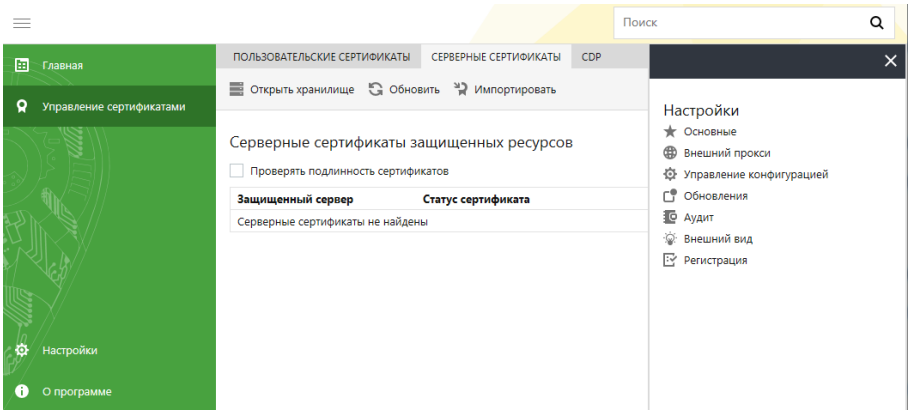


Рисунок 62 – Окно «Управление сертификатами»

- в открывшемся окне выбора файлов выбрать по очереди файлы lk_cert.cer и portal_cert.cer и нажать кнопку «Открыть» (Рисунок 63);

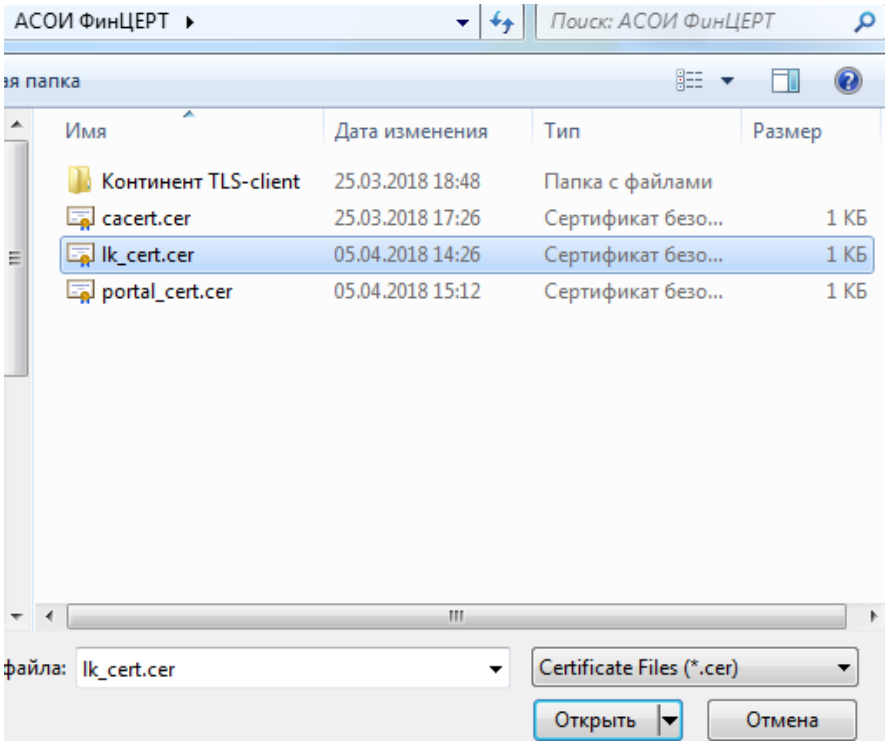


Рисунок 63 – Выбор сертифкатов веб-ресурсов

- добавленные сертификаты будут отображены в списке «Серверные сертификаты» (Рисунок 64).

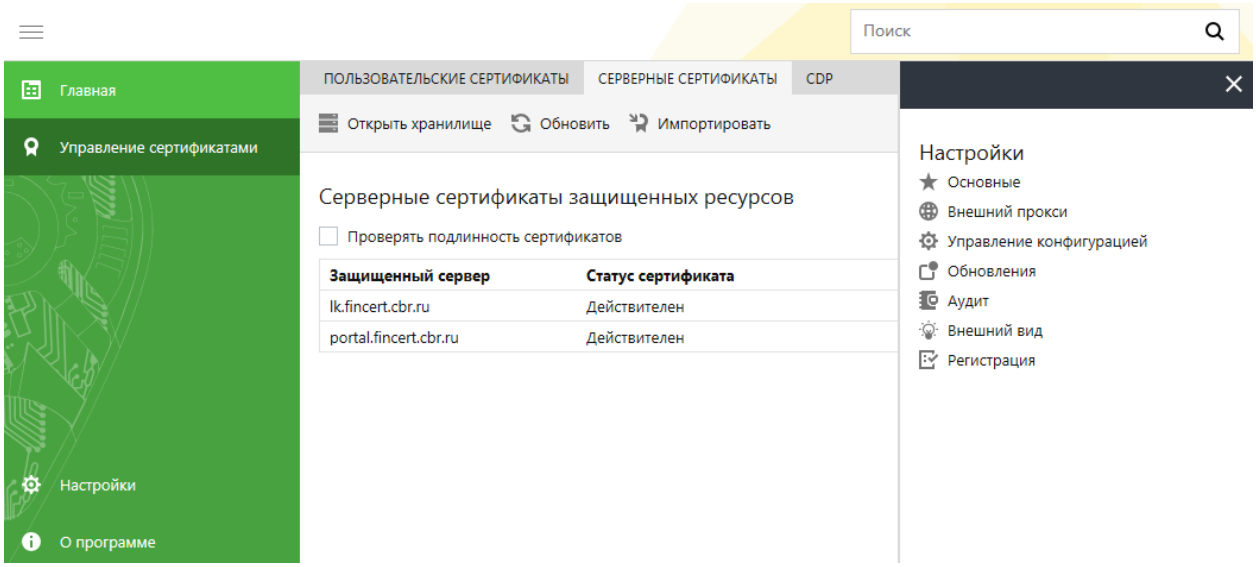


Рисунок 64 – Окно «Управление сертификатами-Серверные сертифкаты»

- Если для доступа к сети Интернет используется прокси сервер необходимо провести настройки программы для корректной работы с прокси сервером:
  - в основном окне выберите пункт вызова настроек  и выберите в меню настроек пункт «Внешний прокси», после чего появится окно настроек (Рисунок 65), в котором необходимо выбрать «Использовать внешний прокси-сервер», указать настройки для работы с прокси-сервером и нажать кнопку «Сохранить».

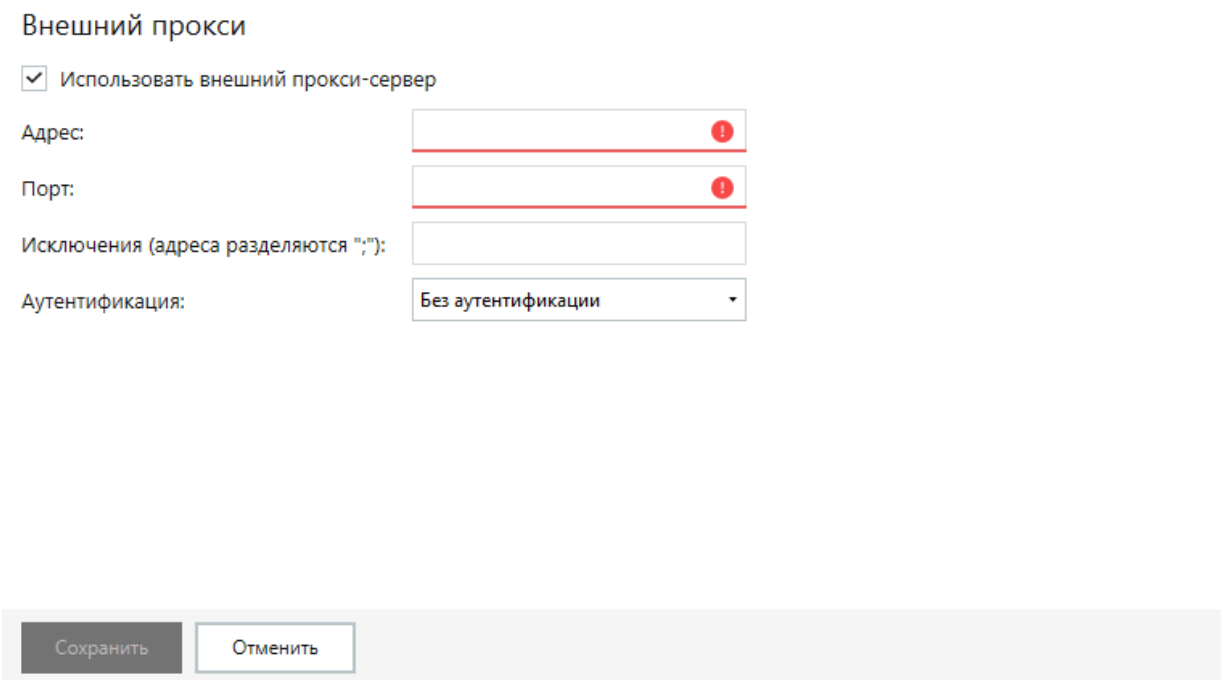


Рисунок 65 – Окно настройки параметров прокси-сервера в Континент TLS

- в вэб-браузере укажите явные настройки прокси-сервера и добавьте в исключения адреса portal.fincert.cbr.ru и lk.fincert.cbr.ru, как показано на Рисунок 66 и Рисунок 67:

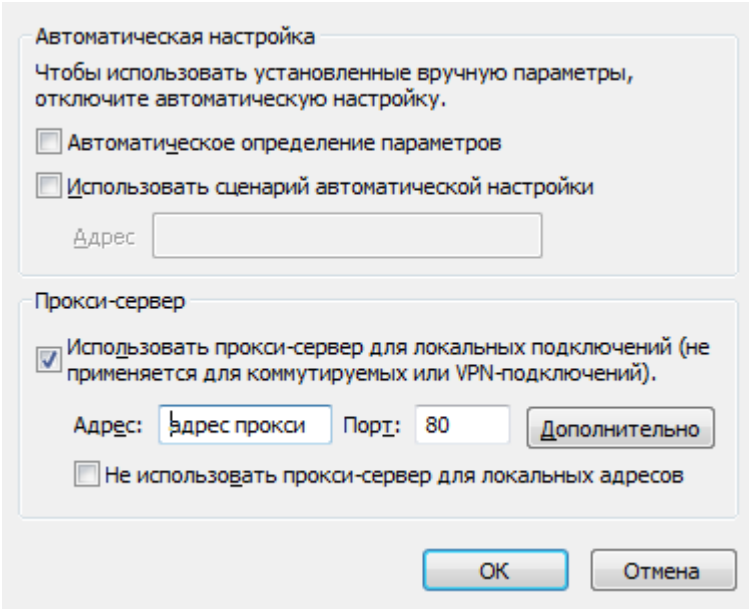


Рисунок 66 – Окно настройки параметров прокси-сервера в веб-браузере

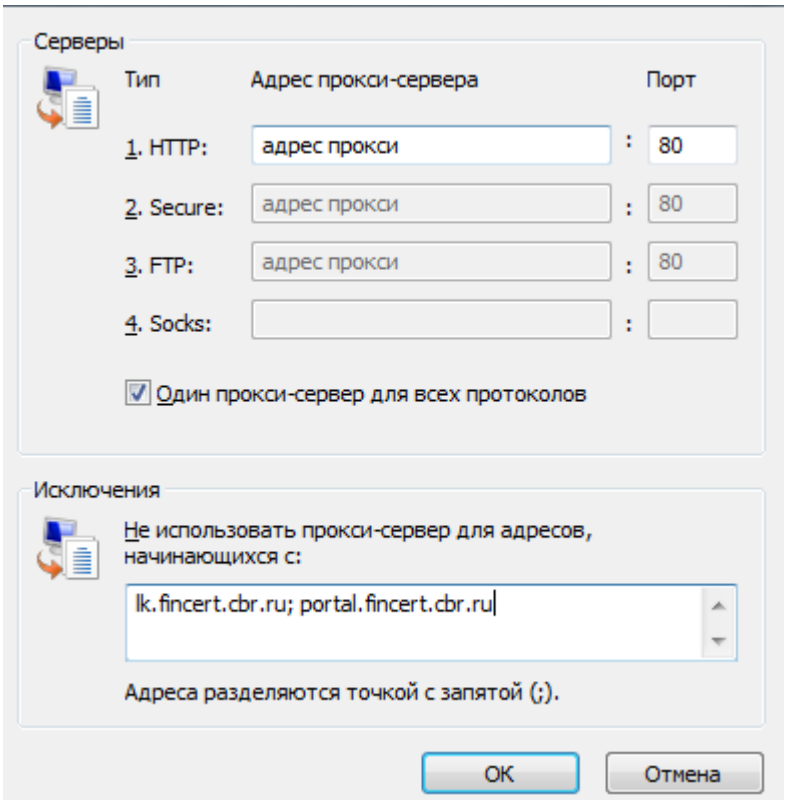


Рисунок 67 – Окно настройки исключений для прокси-сервера в веб-браузере

- Настройте режим работы контроля целостности:
  - запустите программу «Контроль целостности», для этого выберите в главном меню Windows пункт «Все приложения| Код Безопасности |Контроль целостности» (Рисунок 68);

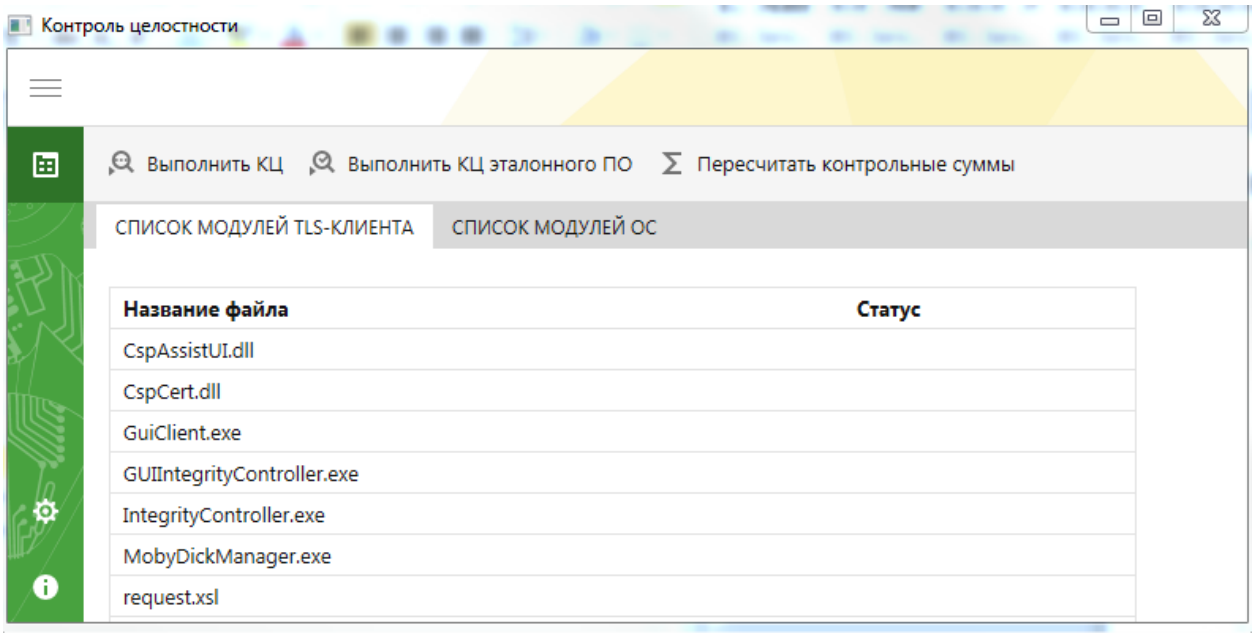


Рисунок 68 – Главное окно программы «Контроль целостности»

- в основном окне выберите пункт вызова настроек  . На экране появится текущее расписание регламентных проверок (Рисунок 69). В открывшемся окне выберите «Разрешить работу при повреждении системных файлов», выбор данной настройки необходим для корректной работы при обновлении операционной системы;

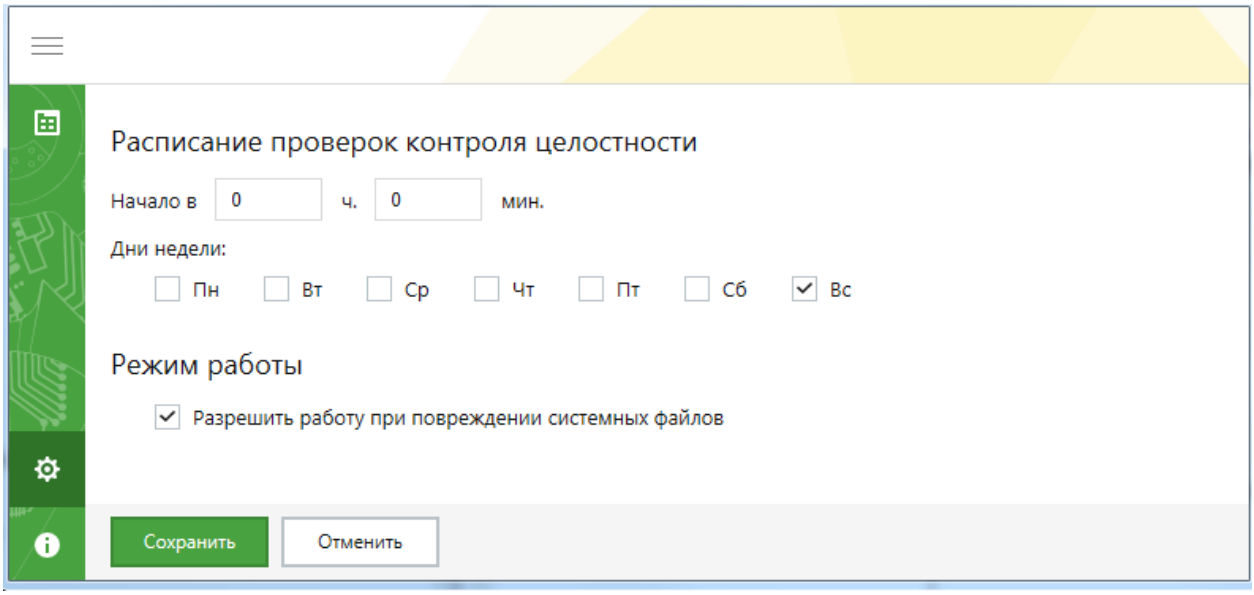


Рисунок 69 – Настройка режима работы контроля целостности

1.4 Установка корневых сертификатов удостоверяющего центра

Для установки корневых сертификатов Головного и Национального удостоверяющих центров, необходимо открыть файл с сертификатом cacert_nuc.cer (последовательность действий, описанных в п.1.4 повторить для файла с сертификатом cacert_guc.cer) и в открывшемся окне нажать кнопку «Установить сертификат». В открывшемся окне мастера импорта сертификатов нажать кнопку «Далее» (Рисунок 70).

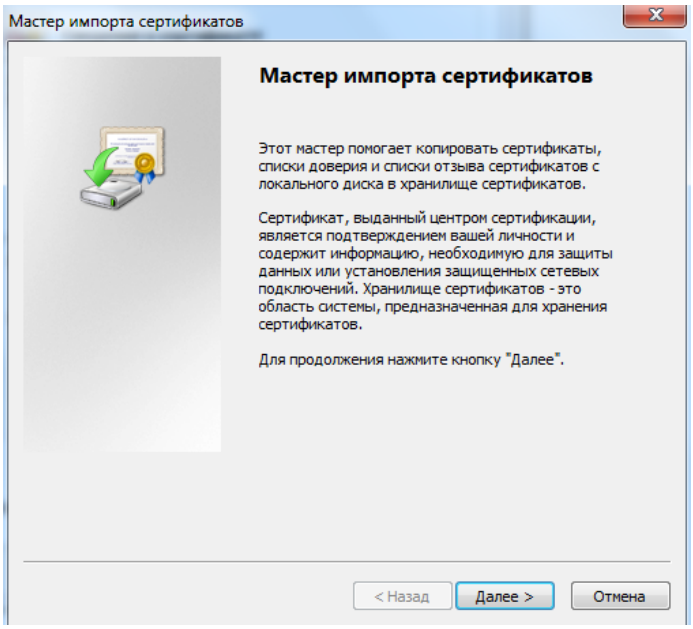


Рисунок 70 – Окно запуска мастера импорта сертификатов

В открывшемся окне необходимо выбрать «Поместить все сертификаты в выбранное хранилище» и нажать кнопку «Обзор» (Рисунок 71).

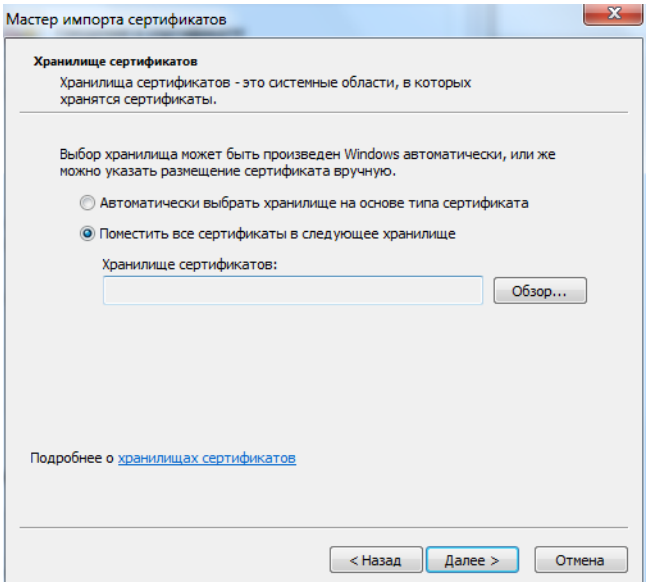


Рисунок 71 – Мастер импорта сертификатов – выбор хранилища сертификатов

В открывшемся окне необходимо выбрать «Доверенные корневые центры сертификации» и нажать кнопку «ОК» (Рисунок 72).

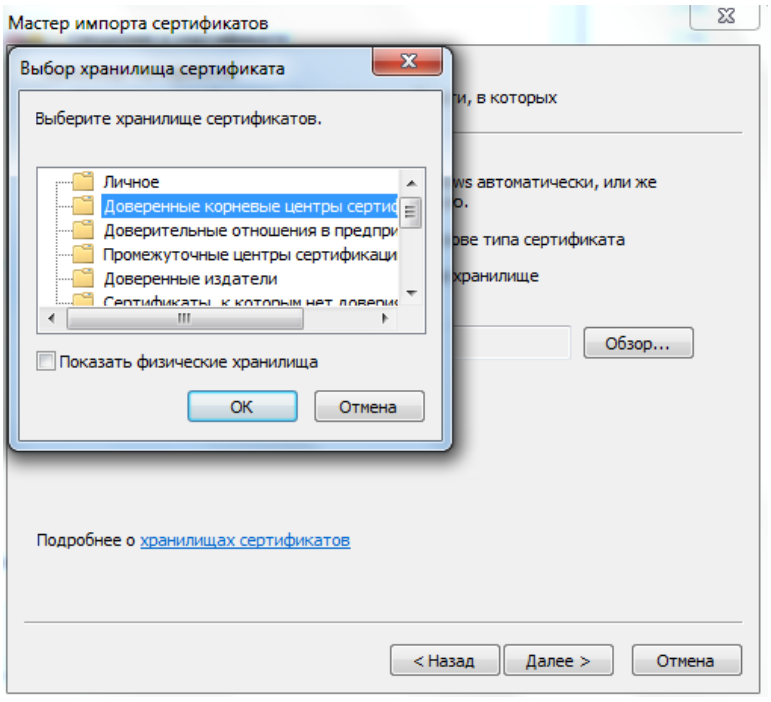


Рисунок 72 – Мастер импорта сертификатов «Доверенные корневые центры сертификации»

В появившемся окне необходимо нажать кнопку «Далее» (Рисунок 73).

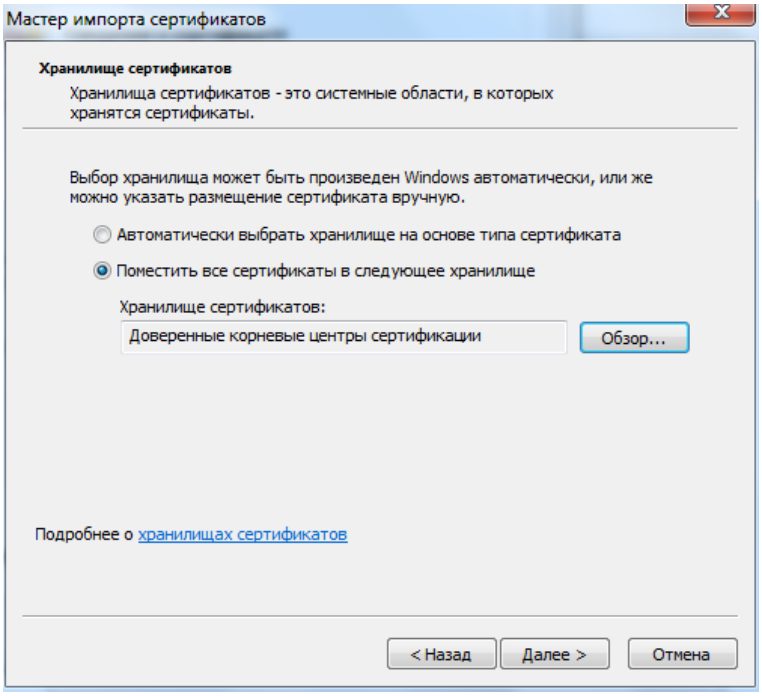


Рисунок 73 – Мастер импорта сертификатов «Доверенные корневые центры сертификации»

В появившемся окне необходимо нажать кнопку «Далее» (Рисунок 74).

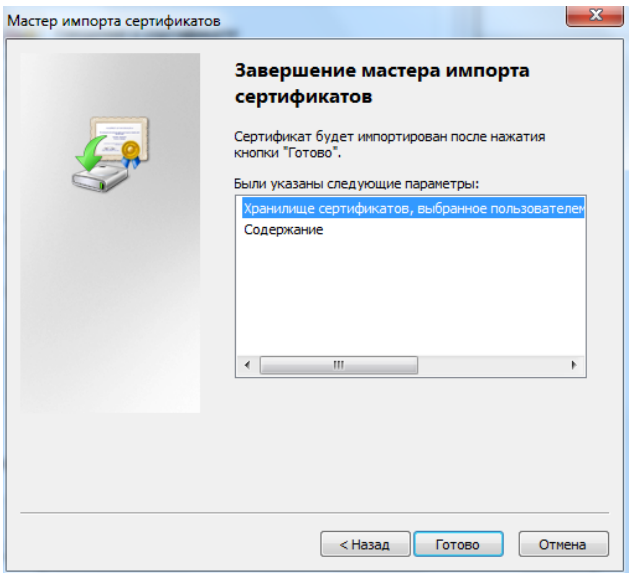


Рисунок 74 – Мастер импорта сертификатов – Завершение мастера импорта сертифкатов

В появившемся окне необходимо нажать кнопку «Готово», после чего должно появиться сообщение, в котором необходимо нажать кнопку «Да». При успешном импорте сертификата появится окно (Рисунок 75), в котором необходимо нажать кнопку «ОК»

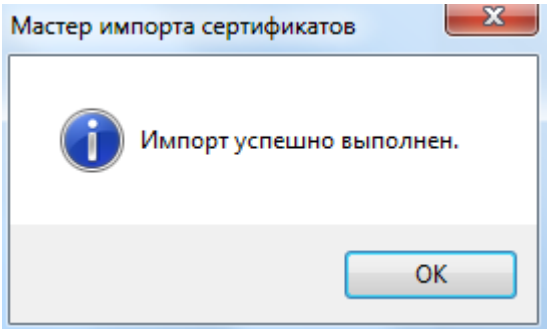


Рисунок 75 – Сообщение о успешном импорте сертифката

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 Главного управления безопасности и защиты информации Банка России