Positive Technologies Incident Processing Center

Версия 2.7

Руководство оператора

POSITIVE TECHNOLOGIES

Дата редакции документа: 16.04.2020

Версия документа: 1

Содержание

1. Об этом документе

Руководство оператора содержит основные сценарии действий оператора, справочную информацию и инструкции для работы в интерфейсе "Личного кабинета оператора" Positive Technologies Incident Processing Center (далее также — PT Incident Processing Center).

Комплект документации PT Incident Processing Center включает в себя следующие документы:

— Этот документ.

— Руководство администратора — содержит справочную информацию и инструкции по установке, настройке и администрированию продукта.

— Руководство участника (Личный кабинет участника) — содержит описание сценариев работы и инструкции для участника информационного обмена.

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример текста с условным обозначением	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

2. О системе PT Incident Processing Center

Positive Technologies Incident Processing Center (далее также — PT Incident Processing Center) предназначен для поддержки бизнес-процессов национального или отраслевого центра реагирования на инциденты (далее также — центр) и организации непрерывного информационного взаимодействия между центром и участниками информационного обмена по вопросам нарушения режима информационной безопасности.

PT Incident Processing Center обеспечивает:

- взаимодействие между центром и участниками в части формирования и реагирования на угрозы и инциденты информационной безопасности;
- повышение уровня информированности участников об актуальных угрозах информационной безопасности;
- автоматизацию обработки инцидентов, поступающих от участников;
- проверку объектов и файлов, поступающих от участников, на присутствие вредоносного кода, опасной активности, а также на наличие угроз и уязвимостей информационной безопасности;
- взаимодействие с ГосСОПКА для эскалации вопросов информационной безопасности и получения инструкций.

По умолчанию система не подключена к ГосСОПКА. Данные из системы не передаются в ГосСОПКА. Для подключения к ГосСОПКА необходимо заключить соглашение с Национальным координационным центром по компьютерным инцидентам (НКЦКИ) Российской Федерации. После заключения соглашения с НКЦКИ Российской Федерации администратор системы настраивает подключение к ГосСОПКА.

3. Принципы работы PT Incident Processing Center

PT Incident Processing Center обеспечивает взаимодействие между национальным или отраслевым центром реагирования на инциденты (далее также — центр) и участником в части формирования и реагирования на угрозы и инциденты информационной безопасности.

Обмен информацией между центром и участником осуществляется по следующему алгоритму:

1. Участник направляет в центр сообщение об инциденте, угрозе, уязвимости или изменении данных в карточке участника, приложив к сообщению соответствующую электронную форму. При поступлении первого сообщения от участника через "Личный кабинет участника" PT Incident Processing Center формирует запрос. Все последующие сообщения, связанные с исходным, от участника и центра автоматически попадают в этот же запрос.
2. Центр получает сообщение от участника, проводит анализ запроса, проверку вложенных объектов и при необходимости формирует рекомендации для противодействия и направляет их участнику.
3. В сложных случаях, требующих дополнительной и более глубокой экспертизы, центр может перенаправить запрос в ГосСОПКА для дальнейшего расследования и получения рекомендаций.
4. Участник получает рекомендации по своему запросу, а также может получать бюллетени для своей отрасли, содержащие информацию о наличии или устранении уязвимостей в программном или аппаратном обеспечении.
5. Регулярная отраслевая аналитика по информационной безопасности и противодействию инцидентам публикуется Центром компетенции национального или отраслевого центра реагирования на инциденты для всех участников PT Incident Processing Center.

4. Вход в "Личный кабинет оператора"

Сервис управления пользователями и доступом PT MC обеспечивает механизм единого входа (технология single sign-on) в приложения "Позитив Текнолоджиз".

Перед входом в PT Incident Processing Center запросите у администратора PT MC :

— ссылку для входа в интерфейс продукта;

— тип учетной записи (локальная или доменная);

— логин и пароль вашей учетной записи пользователя.

Примечание. Убедитесь, что в браузере разрешены всплывающие окна, а также отключена функция Compatibility view для браузеров Microsoft Edge и Microsoft Internet Explorer.

► Чтобы войти в PT Incident Processing Center:

1. В адресной строке браузера введите ссылку для входа в интерфейс PT Incident Processing Center.

   Откроется страница входа в сервис PT MC.

2. Выполните одно из следующих действий:

   - Если вы выполняете вход под локальной учетной записью, то на вкладке **Локальный** укажите логин учетной записи.
   - Если вы выполняете вход под доменной учетной записью, то на вкладке **LDAP** укажите логин доменной учетной записи.

3. В поле **Пароль** введите пароль вашей учетной записи.

   Примечание. Стандартная сессия пользователя в PT Incident Processing Center длится 12 часов. Вы можете продлить сессию, установив флажок **Запомнить меня**: тогда она завершится только через 7 дней бездействия.

4. Нажмите кнопку **Войти**.

PT MC проверяет введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница с системным дашбордом PT Incident Processing Center. Если вы указали неверные данные, отобразится сообщение об ошибке.

5. Интерфейс "Личного кабинета оператора"

При входе в "Личный кабинет оператора" по умолчанию открывается домашняя страница.

Домашняя страница содержит главное меню и рабочую область.

Главное меню расположено в верхней части страницы и обеспечивает доступ к основным функциям PT Incident Processing Center.

Главное меню содержит следующие элементы:

— разделы для перехода к страницам PT Incident Processing Center;

— кнопку , по которой вы можете переходить из PT Incident Processing Center в сервис управления пользователями и доступом PT Management and Configuration;

— кнопку , по которой вы можете переходить с любой страницы системы на домашнюю страницу для просмотра статистической информации о запросах и инцидентах;

— раскрывающийся список **Новый запрос** для быстрого перехода к следующим электронным формам:

  - нового участника;
  - инцидента;
  - угрозы;
  - уязвимости;
  - сообщения о публикации;
  - диспутного запроса;
  - иного запроса, не подпадающего под категории, приведенные выше;

— кнопку поиска по меткам ;

— значок , отображающий количество непрочитанных уведомлений в системе;

— раздел с данными учетной записи.

Раздел **<Учетная запись>** расположен в правой части главного меню. Название этого раздела содержит имя и фамилию пользователя, который вошел в PT Incident Processing Center. Если раздел объединяет несколько страниц системы, то у него есть меню.

На ряде других страниц интерфейса PT Incident Processing Center также присутствует панель инструментов, которая расположена в верхней части страницы под главным меню и содержит кнопки. С их помощью вы можете выполнять действия с данными, представленными в рабочей области. Рабочая область расположена на странице под панелью инструментов. Состав панели инструментов и содержимое рабочей области зависит от страницы.

В этом разделе

5.1. Представление статистических данных: дашборд и виджеты

Главная страница обеспечивает доступ к статистическим данным системы. Она содержит дашборд **Домашняя страница**.

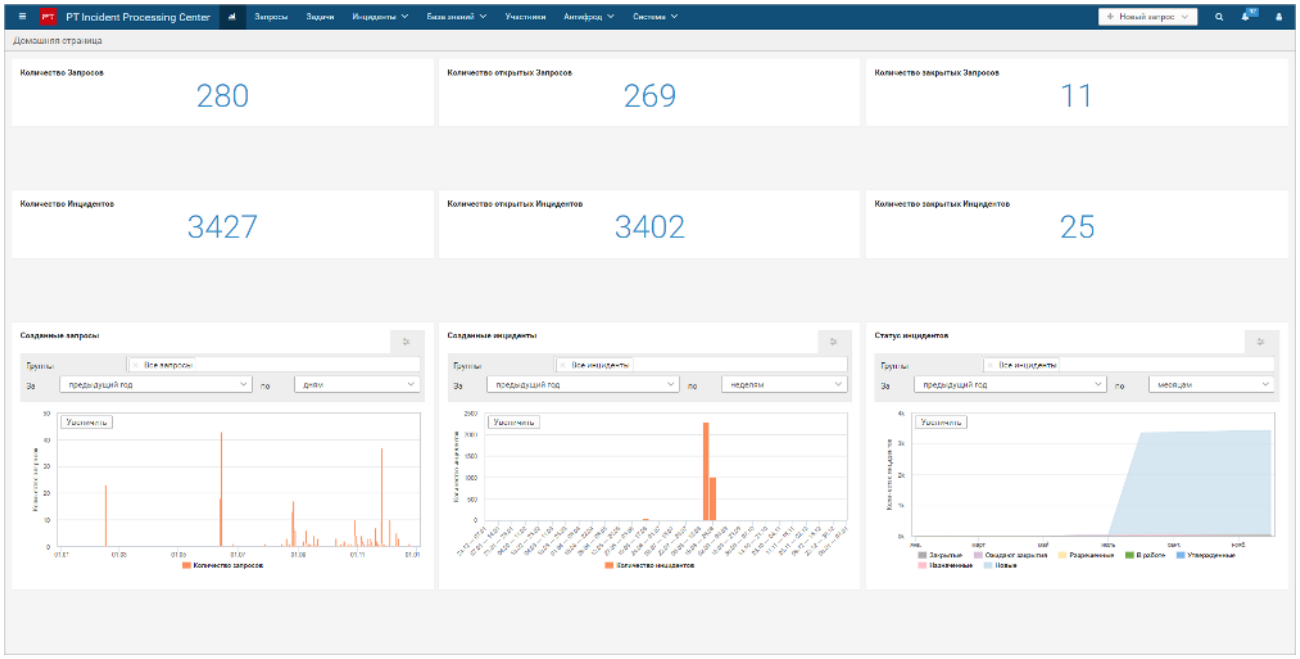

Рисунок 1. Главная страница системы PT Incident Processing Center

Дашборд **Домашняя страница** содержит виджеты. Виджеты отображают информацию о запросах и инцидентах в виде количественного показателя или диаграммы с распределением данных во времени. С помощью кнопок фильтров вы можете включать и отключать данные определенного типа на диаграммах. Подсвеченная кнопка означает, что фильтр включен.

По умолчанию на виджетах отображается информация за последние 30 дней. Информация на виджетах обновляется раз в минуту. Вы не можете изменять состав и расположение виджетов на дашборде.

5.2. Страница Запросы

Информация о зарегистрированных в PT Incident Processing Center запросах отображается на странице **Запросы**.

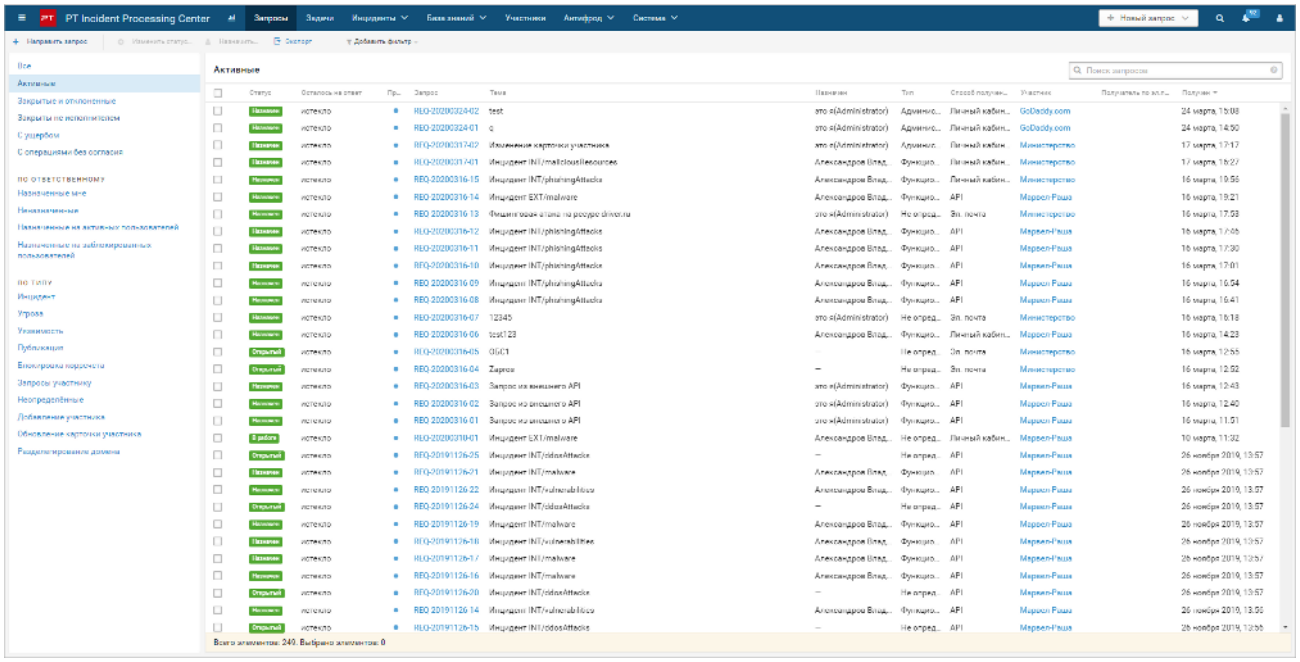

Рисунок 2. Просмотр списка запросов

Рабочая область страницы содержит таблицу запросов и панель фильтрации. По умолчанию таблица запросов отображает все запросы, зарегистрированные в PT Incident Processing Center. Вы можете менять список отображаемых в таблице запросов, используя фильтры в панели фильтрации:

- **Все**. При выборе этого фильтра таблица содержит все запросы, зарегистрированные в PT Incident Processing Center.
- **Активные**. Таблица содержит только активные запросы.
- **Закрытые и отклоненные**. Таблица содержит закрытые и отклоненные оператором запросы.
- **Закрыты не исполнителем**. Таблица содержит запросы, которые были закрыты пользователем, не являющимся исполнителем по запросу на момент его закрытия.
- **С ущербом**. Таблица содержит запросы, в которых сообщается об инцидентах с ущербом (в инциденте выбрано любое значение в раскрывающемся списке Тип ущерба (см. раздел 5.6.2.7)).
- **С операциями без согласия**. Таблица содержит запросы, в которых сообщается об инцидентах, в рамках которых зафиксированы попытки выполнить операции без согласия клиента.

Часть фильтров объединена в группу **По ответственному**:

- **Назначенные мне**. Таблица содержит только те запросы, которые назначены вам.
- **Неназначенные**. Таблица содержит только те запросы, для которых пока не указано лицо, отвечающее за обработку.
- **Назначенные на активных пользователей**. Таблица содержит только те запросы, которые назначены на активных пользователей
- **Назначенные на заблокированных пользователей**. Таблица содержит только те запросы, которые назначены на заблокированных пользователей. Это возможно в случае если пользователь был заблокирован после того, как на него был назначен запрос.

Часть фильтров объединена в группу **По типу**. Вы можете выбрать нужный тип запроса и отфильтровать данные в таблице.

Основные параметры запросов распределены по столбцам таблицы.

Вы можете воспользоваться строкой поиска, расположенной над таблицей запросов, чтобы найти интересующий вас запрос. В строке нужно указать идентификатор запроса, его тему или описание.

Информация на странице **Запросы** обновляется автоматически раз в минуту. Вы можете выключить автоматическое обновление.

Подробную информацию о запросе вы можете просматривать в карточке запроса. Перейти в карточку запроса вы можете по ссылке с идентификатором запроса в столбце **Запрос**.

В системе предусмотрены следующие дополнительные фильтры:

— **Дата появления** — дата первичного добавления запроса участником в личном кабинете участника или оператором в PT Incident Processing Center. По умолчанию создается фильтр на текущую дату. Вы можете скорректировать дату, выбрав фильтр и в открывшемся календаре указав дату или период.

— **Назначенный оператор** — лицо, ответственное за обработку запроса.

— **Участник** — название организации-участника, из заявки или по сообщению от которого запрос зарегистрирован в PT Incident Processing Center. Вы можете воспользоваться строкой поиска.

— **Категория запроса** — категория запроса, указанная в карточке запроса:

  - **Административный** — запрос на добавление участника или изменение карточки участника, зарегистрированный по инициативе участника.
  - **Функциональный** — запрос на расследование инцидента, закрытие уязвимости, устранение угрозы или добавление публикации, зарегистрированный по инициативе участника.
  - **Не определено** — запрос, тип которого не указан.
  - **Запрос участнику** — запрос, зарегистрированный по инициативе оператора PT Incident Processing Center.

— **Статус запроса** — статус запроса, указанный в карточке запроса.

— **Тип вложения** — тип файла, вложенного в запрос.

— **Способ получения** — способ получения запроса в PT Incident Processing Center.

— **Прочитанные**. Вы можете отфильтровать таблицу по прочитанным или непрочитанным запросам.

Примечание. Вы можете добавить несколько дополнительных фильтров. Каждый последующий дополнительный фильтр уточняет результат фильтрации таблицы запросов.

5.3. Карточка запроса

Карточка запроса содержит полную информацию о запросе.

В левой части рабочей области отображается информационная панель. Эта панель содержит основные параметры запроса:

— **Статус**. В PT Incident Processing Center существуют следующие статусы запроса:

  - **Открытый** — запрос только поступил в PT Incident Processing Center.
  - **Назначен** — назначен ответственный за обработку запроса.
  - **В работе** — ведется работа по запросу.
  - **Ожидает закрытия** — ожидается подтверждение от участника о закрытии запроса.

- **Закрыт** — запрос успешно обработан и помещен в архив.
- **Отклонен** — запрос неактуален и отклонен.
  Вы можете изменять статус запроса в раскрывающемся списке.

  Примечание. В системе предусмотрен служебный статус **Новый**: он присваивается всем только поступившим запросам и через несколько секунд меняется на **Открытый**.

— **Приоритет**. В PT Incident Processing Center существуют следующие приоритеты: критический, очень высокий, высокий, средний, низкий. Приоритет определяется набором параметров. Вы можете изменять приоритет запроса в раскрывающемся списке.

— **Назначен** — оператор, ответственный за обработку запроса.

— **Осталось на ответ** — количество дней, часов, минут и секунд, оставшихся на ответ участнику.

— **Тип запроса**. Тип запроса определяется по типу вложенной электронной формы:

- **Административный: Добавление нового участника**;
- **Административный: Обновление карточки участника**;
- **Функциональный: Инцидент**;
- **Функциональный: Уязвимость**;
- **Функциональный: Угроза**;
- **Функциональный: Публикация**;
- **Функциональный: Антифрод**;
- **Не определено**. Запрос содержит несколько электронных форм или не содержит ни одной.

— **Получен в** PT Incident Processing Center — дата и время поступления запроса в PT Incident Processing Center.

— **Способ получения**. Запрос может быть получен по телефону, электронной почте, из личного кабинета участника, по REST API или другим способом.

— **Последнее обновление** — дата и время последнего изменения запроса.

— **Участник** — участник, от которого поступил запрос. Вы можете перейти в карточку участника по ссылке с именем участника.

— **Метки** — ключевые слова для поиска данных.

В панели **Переписка** отображается вся переписка с участником. Вы можете отправлять участнику сообщения и вкладывать в сообщения файлы. Кроме того, вы можете сохранять полезную информацию в информационную карточку.

Вы можете просматривать подробную информацию о сообщении по кнопке ℹ.

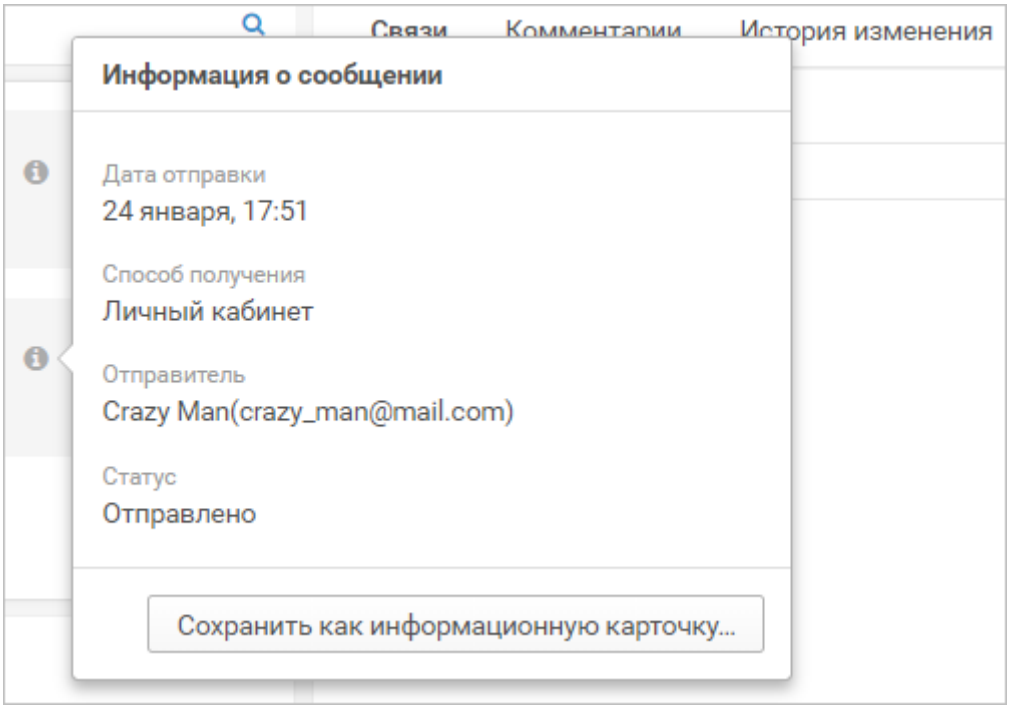

Рисунок 3. Просмотр информации о сообщении

Кроме того, вы можете воспользоваться поиском по сообщениям и пользователям участника по кнопке .

В панели с дополнительной информацией отображаются связи запроса с другими объектами, комментарии (см. раздел 21.3) к запросу и история изменений (см. раздел 21.4) запроса.

См. также

Создание задачи на запрос (см. раздел 10.1)

5.4. Страница Задачи

Информация о задачах приведена на странице **Задачи**.

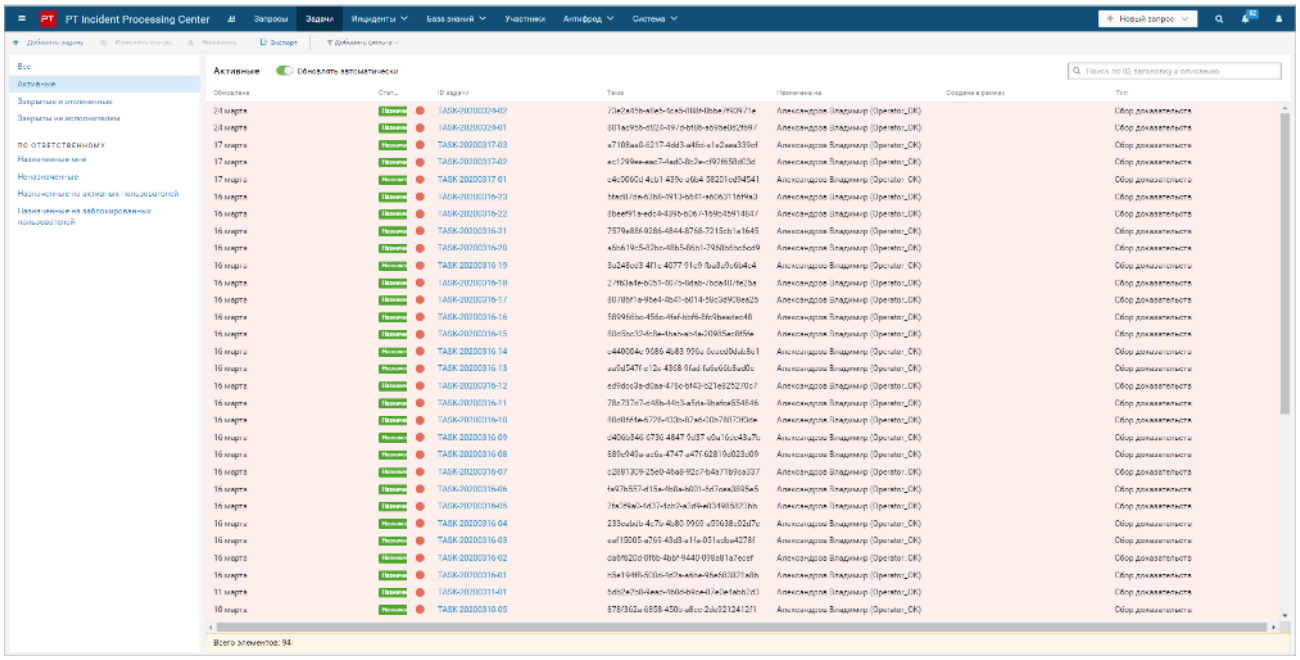

Рисунок 4. Просмотр списка задач

Рабочая область страницы содержит таблицу задач и панель фильтрации. По умолчанию таблица задач отображает все задачи, зарегистрированные в PT Incident Processing Center. Вы можете менять список отображаемых в таблице задач, используя фильтры в панели фильтрации:

— **Все**. При выборе этого фильтра таблица содержит все задачи, зарегистрированные в PT Incident Processing Center.

— **Активные**. При выборе этого фильтра таблица содержит только активные задачи.

— **Закрытые и удаленные**. При выборе этого фильтра таблица содержит закрытые и удаленные оператором задачи.

— **Закрыты не исполнителем**. При выборе этого фильтра таблица содержит задачи, которые были закрыты пользователем, не являющимся исполнителем по задаче на момент ее закрытия.

Часть фильтров объединена в группу **По ответственному**:

— **Назначенные мне**. При выборе этого фильтра таблица содержит только те задачи, ответственным за выполнение которых являетесь вы.

— **Неназначенные**. При выборе этого фильтра таблица содержит только те задачи, для которых пока не указано лицо, отвечающее за обработку.

— **Назначенные на активных пользователей**. При выборе этого фильтра таблица содержит только те задачи, которые назначены на активных пользователей.

— **Назначенные на заблокированных пользователей**. При выборе этого фильтра таблица содержит только те задачи, которые назначены на заблокированных пользователей.

Основные параметры задач распределены по столбцам таблицы.

Вы можете воспользоваться полем поиска, расположенным над таблицей задач, чтобы найти интересующую вас задачу. В поле нужно указать идентификатор задачи, ее заголовок или описание.

Информация на странице **Задачи** обновляется автоматически раз в минуту. Вы можете выключить автоматическое обновление.

Подробную информацию о задаче вы можете просмотреть в карточке задачи. Перейти в карточку задачи вы можете по ссылке с идентификатором в столбце **ID задачи**.

Панель инструментов страницы **Задачи** содержит кнопки добавления задачи, назначения ответственного за выполнение задачи, изменения ее статуса, выпуска отчета и добавления дополнительного фильтра по одному из параметров задачи.

В системе предусмотрены следующие дополнительные фильтры:

— **Дата создания** — дата регистрации задачи в PT Incident Processing Center. По умолчанию создается фильтр на текущую дату. Вы можете скорректировать дату, выбрав фильтр и в открывшемся календаре указав дату или период.

— **Тип задачи**. В PT Incident Processing Center существуют следующие типы задачи:

  - **Расследование** — задачи, которые связаны с анализом инцидентов для выяснения их причин и способов предотвратить повторное возникновение.
  - **Сбор доказательств** — задачи по работе с журналами безопасности и подготовке доказательной базы для передачи в правоохранительные органы.
  - **Восстановление** — задачи, которые связаны с устранением последствий инцидента.

— **Дата последнего обновления** — дата последних изменений задачи. По умолчанию создается фильтр на текущую дату. Вы можете скорректировать дату, выбрав фильтр и в открывшемся календаре указав дату или период.

  Примечание. Вы можете добавить несколько дополнительных фильтров. Каждый последующий дополнительный фильтр уточняет результат фильтрации.

Кнопка **Сбросить фильтр** позволяет удалить все дополнительные фильтры.

5.5. Карточка задачи

В карточке задачи отображается полная информация о задаче.

В левой части рабочей области отображается информационная панель. Эта панель содержит основные параметры задачи:

— **Статус**. В PT Incident Processing Center существуют следующие статусы задачи:

  - **Новая** — задача только создана.
  - **Назначена** — задача назначена на ответственного за ее обработку.
  - **В работе** — ведется работа по задаче.

  - **Закрыта** — задача успешно обработана.
  - **Удалена** — задача неактуальна и удалена.
- **Идентификатор задачи** — уникальный набор символов, позволяющий отличать задачу от других объектов.
- **Крайний срок** — дата, к которой должна быть выполнена задача.
- **Приоритет**. В PT Incident Processing Center существуют следующие приоритеты: критический, очень высокий, высокий, средний, низкий. Приоритет определяется набором параметров.
- **Тип задачи**. В PT Incident Processing Center существуют следующие типы задачи:
  - **Расследование** — выяснение причин инцидента и способов предотвратить его повторное возникновение.
  - **Сбор доказательств** — выявление объектов атаки, сбор и хранение доказательств атаки.
  - **Восстановление** — восстановление работоспособности IT-инфраструктуры организации.
- **Назначена на** — оператор, ответственный за обработку задачи.
- **История обработки** — дата и время создания или изменения задачи.
- **Метки** — ключевые слова для поиска данных.

В центральной панели отображаются описание задачи и вложения, а также итог по задаче. Это поле необходимо заполнить при закрытии задачи.

В панели с дополнительной информацией, расположенной в правой части рабочей области, вы можете:

- просматривать и добавлять связи (см. раздел 21.2.1) задачи с другими объектами;
- просматривать и добавлять комментарии (см. раздел 21.3) к задаче;
- просматривать историю изменений (см. раздел 21.4) задачи.

Панель инструментов карточки задачи содержит кнопку **Редактировать**, по которой можно изменять параметры задачи, а также кнопку **Задачи** для перехода к таблице задач.

5.6. Страница Инциденты

Информация о зарегистрированных инцидентах приведена на странице **Инциденты**.

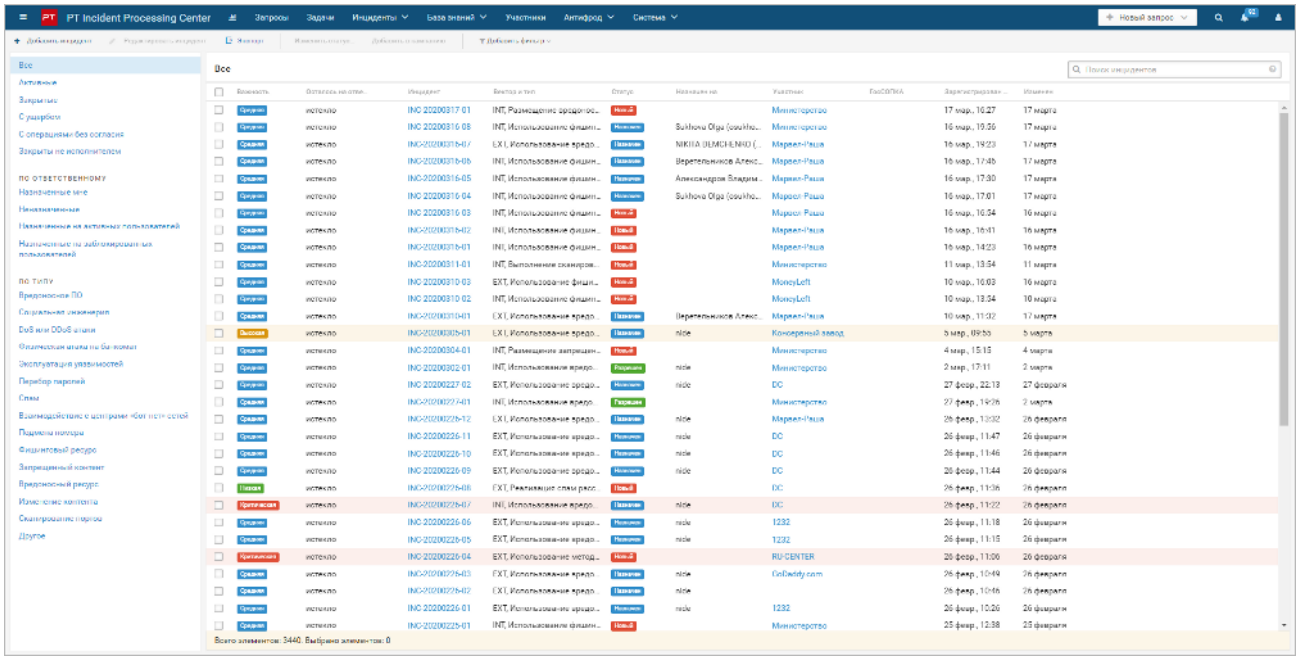

Рисунок 5. Страница **Инциденты**

Рабочая область страницы содержит таблицу инцидентов и панель фильтрации. По умолчанию таблица инцидентов отображает все инциденты, зарегистрированные в PT Incident Processing Center. Вы можете менять список отображаемых в таблице инцидентов, используя фильтры в панели фильтрации:

— **Все**. При выборе этого фильтра таблица содержит все инциденты, зарегистрированные в PT Incident Processing Center.

— **Активные**. При выборе этого фильтра таблица содержит только активные инциденты.

— **Закрытые**. При выборе этого фильтра таблица содержит только закрытые инциденты

— **С ущербом**. При выборе этого фильтра таблица содержит инциденты, в результате которых был нанесен любой тип ущерба (выбрано любое значение в раскрывающемся списке Тип ущерба (см. раздел 5.6.2.7)).

— **С операциями без согласия**. При выборе этого фильтра таблица содержит инциденты, в рамках которых зафиксированы попытки выполнить операции без согласия клиента.

— **Закрытые не исполнителем**. При выборе этого фильтра таблица содержит инциденты, которые были закрыты пользователем, не являющимся исполнителем по инциденту на момент его закрытия.

Часть фильтров объединена в группу **По ответственному**:

— **Назначенные мне**. При выборе этого фильтра таблица содержит только инциденты, ответственным за расследование которых являетесь вы.

— **Неназначенные**. При выборе этого фильтра таблица содержит только инциденты, для которых пока не указано лицо, отвечающее за расследование.

— **Назначенные на активных пользователей**. При выборе этого фильтра таблица содержит только те инциденты, которые назначены на активных пользователей.

— **Назначенные на заблокированных пользователей**. При выборе этого фильтра таблица содержит только те инциденты, которые назначены на заблокированных пользователей. Это возможно в случае если пользователь был заблокирован после того, как на него был назначен инцидент.

Часть фильтров объединена в группу **По типу**. Вы можете выбрать нужный тип инцидента и отфильтровать данные в таблице.

Примечание. Вы можете уточнять результаты фильтрации по отдельным параметрам инцидента.

Основные параметры инцидентов распределены по столбцам таблицы. Вы можете сортировать значения в столбцах таблицы, нажав на заголовок столбца.

Кроме того, вы можете воспользоваться строкой поиска, расположенной над таблицей инцидентов, чтобы найти интересующий вас инцидент. В строке необходимо указать идентификатор инцидента или его описание.

Подробная информация об инциденте отображается в карточке инцидента. Перейти в карточку инцидента вы можете по ссылке с идентификатором инцидента в столбце **Инцидент**.

Панель инструментов страницы **Инциденты** содержит кнопки добавления карточки инцидента, изменения ее параметров, выпуска отчета, изменения статуса и добавления дополнительного фильтра по одному из параметров инцидента.

В системе предусмотрены следующие дополнительные фильтры:

— **Дата создания** — дата первичного добавления инцидента участником в личном кабинете участника или оператором в PT Incident Processing Center. По умолчанию создается фильтр на текущую дату. Вы можете скорректировать дату, выбрав фильтр и в открывшемся календаре указав дату или период.

— **Дата фиксации** — дата регистрации инцидента в PT Incident Processing Center; совпадает с **Датой создания**, если вы регистрируете инцидент самостоятельно, а не добавляете его из заявки участника. По умолчанию создается фильтр на текущую дату. Вы можете скорректировать дату, выбрав фильтр и в открывшемся календаре указав дату или период.

— **Участник** — название организации-участника, из заявки или по сообщению от которого инцидент зарегистрирован в PT Incident Processing Center. Вы можете воспользоваться поиском по имени участника.

— **Исполнитель** — лицо, ответственное за расследование инцидента. Выберите фильтр и в раскрывающемся списке установите флажки для имен ответственных лиц, инциденты по которым вы хотите отобразить в таблице инцидентов.

Примечание. Вы можете добавить несколько дополнительных фильтров. Каждый последующий дополнительный фильтр уточняет результат фильтрации.

Кнопка **Сбросить фильтр** позволяет удалить все дополнительные фильтры.

В этом разделе

См. также

Итоги (см. раздел 5.6.2.7)

5.6.1. Карточка инцидента

Карточка инцидента содержит полную информацию об инциденте.

Карточка инцидента состоит из трех частей. В левой части рабочей области отображается информационная панель, которая содержит основные группы параметров инцидента. В центральной панели отображаются параметры, входящие в выбранную группу. Кроме того, в центральной панели вы можете просматривать, добавлять и изменять метки. Набор вкладок и полей зависит от типа инцидента.

В панели с дополнительной информацией, расположенной в правой части рабочей области, вы можете:

— просматривать и добавлять связи инцидента с другими объектами;

— просматривать похожие инциденты (см. раздел 11.10);

— просматривать и добавлять комментарии (см. раздел 21.3) к инциденту;

— просматривать историю изменений (см. раздел 21.4) инцидента;

— запросить содействие ГосСОПКА (см. раздел 11.8) по расследованию инцидента.

Кроме того, по соответствующей кнопке в панели инструментов вы можете:

— изменять статус инцидента;

— изменять параметры инцидента;

— выпускать справки-отчеты;

— сформировать бюллетень.

См. также

Просмотр похожих инцидентов (см. раздел 11.10)

5.6.2. Параметры инцидента

Набор параметров инцидента зависит от вектора и типа инцидента.

В этом разделе

5.6.2.1. Общие сведения

Примечание. В разделе приведены описания параметров для Российской Федерации.

Вкладка **Общие сведения** карточки инцидента содержит следующие параметры:

— **Доступ к инциденту**:
  - **Red** — PT Incident Processing Center, ГосСОПКА и данный участник;
  - **Amber** — PT Incident Processing Center, ГосСОПКА и все участники отрасли;
  - **Green** — PT Incident Processing Center, ГосСОПКА и все участники;
  - **White** — любые организации.

— **Помощь**. Выберите, требуется ли консультация или помощь со стороны PT Incident Processing Center. Поле обязательно для заполнения.

— **Описание инцидента**. Укажите, что произошло, когда и с помощью каких средств был обнаружен инцидент, какие меры были приняты для локализации последствий инцидента и предотвращения подобных инцидентов в дальнейшем.

— **Тип инцидента**. Инциденты с вектором INT — несанкционированные действия злоумышленников, направленные на информационную инфраструктуру участников. Инциденты с вектором EXT — несанкционированные действия злоумышленников, направленные на клиентов участников. Инциденты бывают следующих типов:
  - С вектором EXT. Использование вредоносного программного обеспечения (Malware) — компьютерные атаки, связанные с использованием вредоносного программного обеспечения применительно к объектам информационной инфраструктуры клиентов участников.
  - С вектором EXT. Использование методов социальной инженерии (SocialEngineering) — совершение несанкционированного перевода денежных средств в результате обмана или злоупотребления доверием.

- С вектором EXT. Эксплуатация уязвимостей информационной инфраструктуры (Vulnerabilities) — компьютерные атаки, связанные с эксплуатацией уязвимостей информационной инфраструктуры клиентов участников.
- С вектором EXT. Реализация спам рассылки (Spams) — компьютерные атаки, связанные с реализацией спам рассылки, осуществляемой в отношении клиентов участников.
- С вектором EXT. Взаимодействие с центрами "бот-нет" сетей (ControlCenters) — компьютерные атаки, связанные с выявлением взаимодействия объектов информационной инфраструктуры клиентов участников с командными центрами бот-сетей.
- С вектором EXT. Изменение IMSI на SIM-карте, смена IMEI телефона (Sim) — компьютерные атаки, связанные с изменением (подменой) идентификатора мобильного абонента (IMSI) номера SIM-карты, а также с заменой идентификатор мобильного оборудования (IMEI).
- С вектором EXT. Использование фишинговых ресурсов (PhishingAttacks) — компьютерные атаки, связанные с информацией, вводящей клиентов участников, а также иных лиц, взаимодействующих с ними, в заблуждение относительно принадлежности информации, распространяемой в интернете, вследствие сходства доменных имен, оформления или содержания.
- С вектором EXT. Размещение запрещенного контента в интернете (ProhibitedContents) — компьютерные атаки, связанные с распространением информации, касающейся предоставления на территории страны услуг лицами, не имеющими права их оказывать в соответствии с законодательством.
- С вектором EXT. Размещение вредоносного ресурса в интернете (MaliciousResources) — компьютерные атаки, связанные с размещением в интернете информации, позволяющей осуществить неправомерный доступ к информационным системам клиентов участников при предоставлении или получении финансовых услуг.
- С вектором EXT. Иная компьютерная атака (Other) — иные компьютерные атаки, направленные на объекты информационной инфраструктуры клиентов участников.
- С вектором INT. Изменение маршрутно-адресной информации (TrafficHijackAttacks) — компьютерные атаки, связанные с изменением маршрутно-адресной информации.
- С вектором INT. Использование вредоносного программного обеспечения (Malware) — компьютерные атаки, связанные с использованием вредоносного программного обеспечения применительно к объектам информационной инфраструктуры участников.
- С вектором INT. Реализация атаки типа "отказ в обслуживании" (DdosAttacks) — компьютерные атаки, связанные со сбоем в работе оборудования и каналов связи участника, вызванным внешними причинами.
- С вектором INT. Реализация несанкционированного доступа к банкоматам и платежным терминалам (AtmAttacks) — компьютерные атаки, связанные с реализацией несанкционированного доступа к банкоматам и платежным терминалам участников.

- С вектором INT. Эксплуатация уязвимостей информационной инфраструктуры (Vulnerabilities) — компьютерные атаки, связанные с эксплуатацией уязвимостей информационной инфраструктуры участников.
- С вектором INT. Компрометация аутентификационных / учетных данных (BluteForces) — компьютерные атаки, связанные с подбором учетных данных участника.
- С вектором INT. Реализация спам рассылки (Spams) — компьютерные атаки, связанные с реализацией спам рассылки, осуществляемой в отношении участников.
- С вектором INT. Взаимодействие с центрами "бот-нет" сетей (ControlCenters) — компьютерные атаки, связанные с выявлением взаимодействия объектов информационной инфраструктуры участников с командными центрами бот-сетей.
- С вектором INT. Использование фишинговых ресурсов (PhishingAttacks) — компьютерные атаки, связанные с информацией, вводящей клиентов участников, а также иных лиц, взаимодействующих с ними, в заблуждение относительно принадлежности информации, распространяемой в интернете, вследствие сходства доменных имен, оформления или содержания.
- С вектором INT. Размещение запрещенного контента в интернете (ProhibitedContents) — компьютерные атаки, связанные с распространением информации, касающейся предоставления на территории страны финансовых услуг лицами, не имеющими права их оказывать в соответствии с законодательством.
- С вектором INT. Размещение вредоносного ресурса в сети интернете (MaliciousResources) — компьютерные атаки, связанные с размещением в интернете информации, позволяющей осуществить неправомерный доступ к информационным системам участников при предоставлении или получении финансовых услуг.
- С вектором INT. Выполнение изменения контента (ChangeContent) — компьютерные атаки, связанные с изменением контента информационного ресурса участника.
- С вектором INT. Выполнение сканирования портов (ScanPorts) — компьютерные атаки, связанные со сканированием программных портов объектов информационной инфраструктуры участников информационного обмена лицами, не обладающими соответствующими полномочиями.
- С вектором INT. Иная компьютерная атака (Other) — иные компьютерные атаки, направленные на объекты информационной инфраструктуры участников.

— **Важность**. Выберите значение важности инцидента. По умолчанию выбрано значение **Средняя**.

— **Приоритет**. Оцените приоритет инцидента и выберите значение из списка. По умолчанию выбрано значение **Средний**.

— **Обнаружен**. Укажите дату и время обнаружения инцидента. Дата указывается в формате **ДДММГГГГ**. Время указывается в формате **ЧЧ:ММ**.

— **Ответственный оператор**. Выберите ответственного за расследование инцидента.

— **Ответственный на стороне участника**. Введите имя, фамилию и отчество ответственного лица участника, которое сообщило об инциденте.

- **Федеральный округ**. Укажите федеральный округ, на территории которого произошел инцидент (только для Российской Федерации). В случае выявления инцидента, связанного с трансграничным переводом денежных средств, место выявления инцидента не указывается.
- **Субъект федерации**. Укажите субъект, на территории которого произошел инцидент (только для Российской Федерации).
- **Населенный пункт**. Укажите город или иной населенный пункт, в котором произошел инцидент.
- **Подразделение**. Введите название структурного подразделения, подвергшегося атаке.
- **Техническое средство**. Укажите, каким техническим средством был зафиксирован инцидент. Поле обязательно для заполнения.
- **Атакованные сервисы**. Перечислите сервисы, подвергшиеся атаке в рамках инцидента. Для этого по ссылке **Добавить сервис** перейдите в окно **Добавление атакованного сервиса** и выберите **Тип сервиса**. Типы сервисов конфигурируются в зависимости от специфики организации.
- **Описание сервиса**. Описание атакованного сервиса.
- **Обращение в правоохранительные органы**. Укажите, было ли зафиксировано обращение в правоохранительные органы. Если обращение в правоохранительные органы совершено, укажите следующую информацию:
  - порядковый номер в книге учета сообщений о преступлениях;
  - регистрационный номер талона-уведомления;
  - дату и время принятия заявления. Дата указывается в формате **ДДММГГГГ**. Время указывается в формате **ЧЧ:ММ**.

5.6.2.2. Вектор инцидента — EXT

- **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:
  - **Событие**. В раскрывающемся списке выберите событие, максимально точно описывающее, каким образом зафиксировано несанкционированное действие. Поле обязательно для заполнения.
  - **Тип и способ списания**. В раскрывающемся списке выберите инструментарий, средствами которого произведено несанкционированное списание средств. Поле обязательно для заполнения.
  - **Кем обнаружено**. В раскрывающемся списке выберите, кто обнаружил событие. Поле обязательно для заполнения.

  Внимание! Детальная информация об инциденте указывается на отдельных вкладках. Их состав зависит от выбранного типа инцидента вектора EXT.

5.6.2.3. Вектор инцидента — INT

Вкладка **Вектор инцидента — INT** карточки инцидента содержит следующие параметры:

— **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:

  - **Событие**. В раскрывающемся списке выберите событие, максимально точно описывающее, каким образом зафиксировано несанкционированное действие. Поле обязательно для заполнения.
  - **Тип нарушителя**. В раскрывающемся списке выберите один из предложенных вариантов. Поле обязательно для заполнения.

  Внимание! Детальная информация об инциденте указывается на отдельных вкладках. Их состав зависит от выбранного типа инцидента вектора INT.

5.6.2.4. Принятые меры

Вкладка содержит параметр **Принятые меры** — описание действий, которые были предприняты для устранения инцидента и его последствий.

5.6.2.5. Операции без согласия

Примечание. Сведения об операциях без согласия указывают участники, которым в рамках их деятельности необходимо фиксировать и обрабатывать такую информацию.

Если в рамках обнаруженного инцидента зафиксирована попытка выполнить финансовые операции без согласия клиента, опишите максимально подробно имеющиеся факты на вкладке **Операции без согласия**.

Примечание. В разделе приведены описания параметров для Российской Федерации.

Блок данных **Информация о плательщике** содержит следующие параметры для юридического лица:

— **Тип лица плательщика** — юридическое лицо.

— **Добавить учредителя** — добавление учредителя юридического лица. Добавить информацию о новом учредителе можно после сохранения информации о предыдущем.

— **Учредители** — информация об учредителях юридического лица:

  - **Хеш-сумма номера и серии паспорта** — последовательность символов, полученных в результате хеширования серии и номера паспорта в формате **XX XX YYYYYY**, где **XX XX** — четырехзначная серия паспорта, **YYYYYY** — шестизначный номер паспорта;
  - **Хеш-сумма СНИЛС** — последовательность символов, полученных в результате хеширования страхового номера индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Пенсионного фонда Российской Федерации.

— **ИНН** — индивидуальный номер налогоплательщика. Поле обязательно для заполнения.

Блок данных **Информация о плательщике** содержит следующие параметры для физического лица:

— **Хеш-сумма номера и серии паспорта** — последовательность символов, полученных в результате хеширования серии и номера паспорта в формате **XX XX YYYYYY**, где:

  - **XX XX** — четырехзначная серия паспорта;
  - **YYYYYY** — шестизначный номер паспорта.

— **Хеш-сумма СНИЛС** — последовательность символов, полученных в результате хеширования страхового номера индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Пенсионного фонда Российской Федерации.

— **ИНН** — индивидуальный номер налогоплательщика. Поле обязательно для заполнения.

Блок данных **Информация о переводе** содержит следующие параметры:

— **Обнаружено как**. Выберите способ обнаружения операции без согласия.

— **Статус приостановления перевода** — статус перевода денежных средств, инициированного без согласия клиента.

— **Статус подтверждения перевода** — статус, подтверждающий или опровергающий законность перевода.

— **Способ реализации перевода**. Выберите один из способов, используемых злоумышленниками для инициации перевода:

— Блок параметров **Карта** содержит параметры для ситуации, когда перевод выполнен на карту:

  - **Номер платежной карты**. Укажите номер платежной карты. Номер может содержать от 16 до 18 цифр.
  - **Сумма**. Укажите сумму операции без разделителей. Поле обязательно для заполнения.
  - **Валюта**. Выберите код валюты операции из раскрывающегося списка. Воспользуйтесь поиском нужной валюты в поле **Быстрый поиск**.

- **Дата и время**. Выберите в календаре дату, когда был инициирован перевод. Время по умолчанию — **12:00 AM**. Вручную скорректируйте его по необходимости. Поля обязательны для заполнения.
- **RRN**. Укажите номер операции по переводу денежных средств, формируемый при выполнении ее авторизации в формате **YJJJXXNNNNNN**, где:

  Y — последняя цифра года;

  JJJ — юлианская дата;

  XX — идентификатор, присвоенный узлу банка-эквайера;

  NNNNNN — последовательный шестизначный номер транзакции в течение дня.

— Блок параметров **Телефон** содержит параметры для ситуации, когда несанкционированная операция инициирована через привязанный к счету номер телефона:

- **Номер телефона**. Укажите полный номер телефона с кодом страны и региона, кодом сотового оператора и номером абонента в формате **+ XX (XXX) XXXXXXX**. Как правило, номер телефона указан в договоре, заключенном между банком и клиентом.
- **Сумма**. Укажите сумму операции без разделителей. Поле обязательно для заполнения.
- **Валюта**. Выберите код валюты операции из раскрывающегося списка. Воспользуйтесь поиском нужной валюты в поле **Быстрый поиск**.
- **Дата и время**. Выберите в календаре дату, когда был инициирован перевод. Время по умолчанию — **12:00 AM**. Вручную скорректируйте его по необходимости. Поля обязательны для заполнения.

— Блок параметров **Счет в банке** содержит параметры для ситуации, когда несанкционированный перевод выполнен со счета в банке:

- **Номер банковского счета**. Укажите 20-значный номер лицевого банковского счета клиента, задействованного в несанкционированной операции, в формате **XXXXX XXXXX XXXXX XXXXX**.
- **БИК**. Укажите 8-значный банковский идентификационный код оператора по переводу денежных средств.
- **Сумма**. Укажите сумму операции без разделителей. Поле обязательно для заполнения.
- **Валюта**. Выберите код валюты операции из раскрывающегося списка. Воспользуйтесь поиском нужной валюты в поле **Быстрый поиск**.
- **Дата и время**. Выберите в календаре дату, когда был инициирован перевод. Время по умолчанию — **12:00 AM**. Вручную скорректируйте его по необходимости. Поля обязательны для заполнения.

— Блок параметров **Электронный кошелек** содержит параметры для ситуации, когда несанкционированный перевод выполнялся с электронного кошелька плательщика:

- **Номер электронного кошелька**. Укажите номер электронного кошелька на основании договора, заключенного с оператором по переводу денежных средств. Поле обязательно для заполнения.
- **Название электронной платежной системы**. Введите в поле название платежной системы. Поле обязательно для заполнения.
- **Сумма**. Укажите сумму операции без разделителей. Поле обязательно для заполнения.

- **Валюта**. Выберите код валюты операции из раскрывающегося списка. Воспользуйтесь поиском нужной валюты в поле **Быстрый поиск**.
- **Дата и время**. Выберите в календаре дату, когда был инициирован перевод. Время по умолчанию — **12:00 AM**. Вручную скорректируйте его по необходимости. Поля обязательны для заполнения.

— Блок параметров **Swift** содержит параметры для ситуации, когда несанкционированная операция выполнена с помощью SWIFT:

- **Номер банковского счета**. Укажите номер лицевого банковского счета клиента, задействованного в несанкционированной операции.
- **Swift-код**. Укажите банковский идентификационный код SWIFT. Код может содержать от 8 до 11 знаков.
- **Сумма**. Укажите сумму операции без разделителей. Поле обязательно для заполнения.
- **Валюта**. Выберите код валюты операции из раскрывающегося списка. Воспользуйтесь поиском нужной валюты в поле Быстрый поиск.
- **Дата и время**. Выберите в календаре дату, когда был инициирован перевод. Время по умолчанию — 12:00 AM. Вручную скорректируйте его по необходимости. Поля обязательны для заполнения.

— Блок параметров **Retail/ATM** содержит параметры для ситуации, когда несанкционированная операция выполнена по карте через терминал торгово-сервисного предприятия (сеть retail) или с помощью банкомата:

- **Сумма**. Укажите сумму операции без разделителей. Поле обязательно для заполнения.
- **Валюта**. Выберите код валюты операции из раскрывающегося списка. Воспользуйтесь поиском нужной валюты в поле Быстрый поиск.
- **Дата и время**. Выберите в календаре дату, когда был инициирован перевод. Время по умолчанию — 12:00 AM. Вручную скорректируйте его по необходимости. Поля обязательны для заполнения.
- **BIN эквайера**. Укажите банковский идентификационный номер банка-эквайера. Поле обязательно для заполнения.
- **Мерчант**. Укажите название торгово-сервисного предприятия, если несанкционированная операция совершена через сеть retail. Укажите название банкомата, если несанкционированная операция совершена через банкомат. Поле обязательно для заполнения.
- **MCC**. Укажите четырехзначный код, классифицирующий вид деятельности торгово-сервисного предприятия.

— Блок параметров **Иной идентификатор** содержит параметры для ситуации, когда несанкционированная операция совершена отличным от перечисленных выше способов:

- **Иной номер**. Введите идентификатор средства, с помощью которого выполнена несанкционированная операция.
- **Сумма**. Укажите сумму операции без разделителей. Поле обязательно для заполнения.
- **Валюта**. Выберите код валюты операции из раскрывающегося списка. Воспользуйтесь поиском нужной валюты в поле **Быстрый поиск**.
- **Дата и время**. Выберите в календаре дату, когда был инициирован перевод. Время по умолчанию — **12:00 AM**. Вручную скорректируйте его по необходимости. Поля обязательны для заполнения.

Блок данных **Реквизиты получателя** содержит следующие параметры:

— **Способ реализации перевода**. Выберите один из способов, используемых злоумышленниками для инициации перевода.

— Блок параметров **Карта** содержит параметры для ситуации, когда перевод выполнен на карту:

  - **Номер платежной карты**. Укажите номер платежной карты. Номер может содержать от 16 до 18 цифр.

— Блок параметров **Телефон** содержит параметры для ситуации, когда несанкционированная операция инициирована через привязанный к счету номер телефона:

  - **Номер телефона**. Укажите полный номер телефона с кодом страны и региона, кодом сотового оператора и номером абонента в формате **+ XX (XXX) XXXXXXX**. Как правило, номер телефона указан в договоре, заключенном между банком и клиентом.

— Блок параметров **Счет в банке** содержит параметры для ситуации, когда несанкционированный перевод выполняется со счета в банке:

  - **Номер банковского счета**. Укажите 20-значный номер лицевого банковского счета клиента, задействованного в несанкционированной операции, в формате **XXXXX XXXXX XXXXX XXXXX**.
  - **БИК**. Укажите 8-значный банковский идентификационный код оператора по переводу денежных средств.

— Блок параметров **Электронный кошелек** содержит параметры для ситуации, когда несанкционированный перевод выполнялся на электронный кошелек:
  - **Номер электронного кошелька**. Укажите номер электронного кошелька на основании договора, заключенного с оператором по переводу денежных средств. Поле обязательно для заполнения.
  - **Название электронной платежной системы**. Введите в поле название платежной системы. Поле обязательно для заполнения.

— В блоке параметров **Иной идентификатор** в поле **Иной номер** введите идентификатор средства, с помощью которого выполнена несанкционированная операция. Параметр предназначен для ситуации, когда несанкционированная операция совершена отличным от перечисленных выше способов.

Блок параметров **Идентификаторы устройства** содержит параметры устройства, с использованием которого злоумышленник получил доступ к автоматизированной системе или программному обеспечению для несанкционированного перевода денежных средств без согласия клиента:

— **IP** — IP-адрес устройства.

— **IMSI** — международный идентификатор мобильного абонента, по которому определяется пользователь мобильной связи, использующий стандарты GSM и UMTS, в формате **AA-BBBBBB-CCCCCC-EE**.

— **IMEI** — международный идентификатор мобильного устройства в формате **AA-BBBBBB-CCCCCC-EE**.

— **AIIC** — идентификатор банка-эквайера, выполнявшего операции по переводу денежных средств с использованием платежных карт.

— **CATI** — идентификатор банкомата или электронного терминала, на котором осуществлялась операция по несанкционированному переводу или снятию денежных средств.

— **CAIC** — идентификатор географического местоположения банкомата или электронного терминала, на котором осуществлялась операция по несанкционированному переводу или снятию денежных средств.

Блок данных **Аналитическая форма** содержит следующие параметры:

— **Новый получатель для клиента**. Установите флажок, если клиент впервые перевел денежные средства получателю.

— **Cross country**. Установите флажок, если клиент переводил денежные средства в разных географических точках и при этом время между операциями меньше времени, за которое клиент мог переместиться между этими точками.

— **Время между текущей и предыдущей операциями меньше 5 секунд**. Установите флажок, если между текущей и предыдущей операцией прошло менее 5 секунд.

— **Нетипичное место проведения операции**. Установите флажок, если операция проводилась в месте, нетипичном для клиента.

— **Нетипичная сумма проведения операции**. Установите флажок, если сумма операции нетипична для клиента.

— **Тип карты**. В раскрывающемся списке выберите тип карты, с которой осуществлялась операция:

- кредитная;
- дебетовая;
- предоплаченная.

— **Тип операции**. В раскрывающемся списке выберите тип операции:

- покупка;
- оплата;
- перевод;
- снятие;
- комиссия;
- списание штрафа;
- списание других запросов ГО.

— **Клиент уже совершал переводы этому получателю**. Установите флажок, если клиент ранее переводил денежные средства получателю.

— **Карточный продукт**. В раскрывающемся списке выберите карточный продукт клиента:

- кампусная;
- личная;
- зарплатная;
- корпоративная.

Блок параметров **Критерии легитимности** содержит следующие параметры:

— **Клиент — крупная торговая сеть**. Установите флажок, если получатель платежа — крупная торговая сеть.

— **Клиент регулярно получает подобные операции от этого получателя**. Установите флажок, если клиенту регулярно приходят подобные платежи от этого получателя.

— **Профиль клиента содержит регулярные торговые операции**. Установите флажок, если получатель платежа регулярно совершает торговые операции.

— **Клиент имеет другие счета и вклады в данной КО**. Установите флажок, если получатель платежа имеет другие счета и вклады в данной КО.

Блок данных **Дополнительные статусы** содержит следующие параметры:

— **Идентификатор трансграничности**. Укажите, осуществлялся денежный перевод внутри Российской Федерации или за ее пределами. Поле обязательно для заполнения.

— **Идентификатор дополнительного подтверждения операции**. В раскрывающемся списке выберите один или несколько способов подтверждения транзакции:

- операция подтверждена с использованием 3D Secure;
- реализация технологических мер по использованию раздельных технологий;
- операция без подтверждения;
- подтверждение операции выполнено с применением коротких текстовых сообщений (SMS-сообщений);
- операция выполнена в соответствии со списком доверенных получателей;
- операция подтверждена по телефону;
- иной способ подтверждения.

5.6.2.6. Вложения

Перетащите или выберите файл. Добавьте файлы, которые могут быть полезны для расследования инцидента.

Примечание. Можно прикладывать к инциденту вложения суммарным объемом до 5 ТБ.

5.6.2.7. Итоги

Блок параметров **Ущерб от инцидента** содержит следующие параметры:

— **Тип ущерба**. В раскрывающемся списке выберите **Операционные расходы**, если ущерб был нанесен денежным средствам.

— **Описание ущерба**. Оцените размер ущерба и возможные негативные последствия. Если ущерба нанесено не было, оставьте поле пустым.

— **Относительный масштаб**. В раскрывающемся списке выберите вариант влияния обнаруженного инцидента.

Блок параметров **Сигнатуры атаки** содержит следующие параметры:

— **Сработавшие атаки**. Перечислите все известные вам в контексте обнаруженного инцидента свойства обнаруженных атак:

- **Средство обнаружения**. Укажите средство, с помощью которого обнаружены атаки. Поле обязательно для заполнения.
- **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. Поле обязательно для заполнения.
  - **Число срабатываний**. Укажите, сколько раз сработали сигнатуры атак в рамках описываемого инцидента. Поле обязательно для заполнения.
- **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;)
```

Блок параметров **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.
- **Причины возникновения**. Укажите причины возникновения инцидента.
- **Принятые меры**. Перечислите все действия, которые были предприняты для устранения инцидента и его последствий.

5.6.2.8. Параметры инцидентов с вектором EXT

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

- Вкладка **Влияние и способ заражения**:
  - **Внешний IP-адрес узла**. Введите IP-адрес зараженного узла.
  - **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:

- **Обращение по IP/URL-адресу**. Перечислите скомпрометированные IP-адреса или URL-адреса.
- **Модификация текущих сетевых настроек**. Поле заполняется в свободной форме.
- **Сокрытие следов сетевого взаимодействия**. Например, удаление маршрутов или записей журналов сетевых устройств. Поле заполняется в свободной форме.
- **Создание файлов**. Поле заполняется в свободной форме.
- **Изменение файлов**. Поле заполняется в свободной форме.
- **Удаление файлов**. Поле заполняется в свободной форме.
- **Создание записей реестра**. Поле заполняется в свободной форме.
- **Изменение записей реестра**. Сведения заполняются в свободной форме.
- **Удаление записей реестра**. Поле заполняется в свободной форме.
- **Запуск процесса**. Сведения заполняются в свободной форме.
- **Изменение запущенного процесса**. Сведения заполняются в свободной форме.
- **Завершение процесса**. Сведения заполняются в свободной форме.
- **Отчет средств динамического анализа кода ("песочница")**. Перетащите или выберите файл из списка.
- **Иные индикаторы**. Сведения заполняются в свободной форме.

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

— Вкладка **Описание по типу**:

- **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.
- **Примечание**. Опишите инцидент.
- **Номер телефона**. Укажите номер телефона, с которого было совершено несанкционированное действие.

- **Электронная почта**. Укажите адрес электронной почты в формате user@domain.com, с которого поступала недостоверная информация, вредоносное содержимое или побуждение к несанкционированным действиям.
- **IP-адрес почтового сервера**. Укажите IP-адрес почтового сервера, с которого поступала недостоверная информация, вредоносное содержимое или побуждение к несанкционированным действиям.
- **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**:

- **IP-адрес**. Укажите IP-адрес узла, на котором эксплуатировалась уязвимость, в формате XXX.XXX.XXX.XXX.
- **Доменное имя**. Введите в поле доменное имя пострадавшего узла.
- **URL-адрес**. Укажите URL-адрес пострадавшего узла в формате www.domain.com.
- **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**:

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

— Вкладка **<0.0.0.0>: Свой идентификатор уязвимости**:

- **Описание**. Введите описание уязвимости.
- **Название ПО**. Введите название программного обеспечения, в котором была выявлена уязвимость.
- **Версия ПО**. Введите версию программного обеспечения, в котором была выявлена уязвимость.
- **Тип уязвимости**. Введите название типа уязвимости.
- **Класс уязвимости**. Выберите один из следующих вариантов: **Уязвимость кода**, **Уязвимость архитектуры**, **Уязвимость многофакторная**.
- **Дата обнаружения**. Выберите в календаре дату обнаружения уязвимости. По умолчанию выбрана текущая дата.
- **Базовый CVSS**. Введите базовый вектор уязвимости.

- **Опасность**. Выберите уровень опасности обнаруженной уязвимости: низкий, средний, высокий или критический.
- **Меры устранения**. Перечислите, какие меры были предприняты.
- **Статус**. Выберите статус уязвимости.
- **Наличие эксплойта**. Укажите наличие эксплойта.
- **Рекомендации**. Введите рекомендации по устранению уязвимости.
- **Ссылки**. Введите ссылки на источники информации об устранении уязвимости.
- **Вендор**. Введите название производителя программного обеспечения, в котором была обнаружена уязвимость.

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

— Вкладка **Описание по типу**:

- **Спам. Дата получения. Выберите дату получения сообщения, содержащего спам**.
- **Цель атаки. Адрес электронной почты. Введите адрес электронной почты, на который поступил спам**.
- **Источник атаки. IP-адрес**. Введите IP-адрес, с которого был отправлен спам, в формате XXX.XXX.XXX.XXX.
- **Источник атаки. Доменное имя**. Введите доменное имя источника рассылки спама.
- **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**:

- **IP-адрес**. Введите IP-адрес пострадавшей системы в формате XXX.XXX.XXX.XXX.
- **URL**. Введите URL-адрес пострадавшей системы в формате www.domain.com.

— Вкладка **Описание по типу**: **Информация с ЦУ бот-сети**:

- **URL с ЦУ**. Введите URL-адрес, на котором размещен ЦУ бот-сети.
- **IP-адрес злоумышленника**. Введите IP-адрес злоумышленника, разместившего ЦУ бот-сети, в формате XXX.XXX.XXX.XXX.
- **Действия злоумышленника**. Опишите действия злоумышленника, которые удалось выявить.
- **Сведения о бот-сети**. Введите описание бот-сети.
- **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**:

- **IP-адрес**. Введите IP-адрес пострадавшей системы в формате XXX.XXX.XXX.XXX.
- **Домен**. Введите в поле доменное имя пострадавшей системы.
- **Добавить фишинговый ресурс**. Введите IP-адрес ресурса в формате XXX.XXX.XXX.XXX и URL-адрес ресурса в формате www.domain.com.
- **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) XXXXXXX.

— **IMSI**. Введите уникальный номер sim-карты в формате XXXXXXXXXXXXXXX.

— **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.example.com.

— **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.example.com.

— **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.com

5.6.2.9. Параметры инцидентов с вектором INT

Примечание. Сведения об операциях без согласия указывают участники, которым в рамках их деятельности необходимо фиксировать и обрабатывать такую информацию.

Использование вредоносного программного обеспечения (malware)

— Вкладка **Влияние и способ заражения**:

- **Внешний IP-адрес узла**. Введите IP-адрес зараженного узла.
- **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:

- **Модификация текущих сетевых настроек**. Поле заполняется в свободной форме.
- **Сокрытие следов сетевого взаимодействия**. Например, удаление маршрутов или записей журналов сетевых устройств. Поле заполняется в свободной форме.
- **Изменение файлов**. Поле заполняется в свободной форме.
- **Удаление файлов**. Поле заполняется в свободной форме.
- **Изменение записей реестра**. Сведения заполняются в свободной форме.
- **Запуск процесса**. Сведения заполняются в свободной форме.
- **Изменение запущенного процесса**. Сведения заполняются в свободной форме.
- **Завершение процесса**. Сведения заполняются в свободной форме.
- **Отчет средств динамического анализа кода ("песочница")**. Перетащите или выберите файл из списка.
- **Иные индикаторы**. Сведения заполняются в свободной форме.

Изменение маршрутно-адресной информации (trafficHijackAttacks)

— Вкладка **Описание по типу: Атака на трафик:**

- **Штатный AS-path**. Укажите штатный AS-path.
- **Подставной AS-path**. Укажите измененный AS-path.
- **Ссылка на Looking Glass**. Ввведите ссылку на используемый Looking Glass для проверки AS-path.
- **Штатный prefix**. Укажите штатный prefix.
- **Подставной prefix**. Укажите измененный prefix.

Реализация атаки типа "отказ в обслуживании" (ddosAttacks)

— Вкладка **<0.0.0.0>: Адрес пострадавшей системы**:

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

— Вкладка **<0.0.0.0>: Атака**:

- **IP-адреса источников**. Укажите IP-адреса или загрузите их из файла.
- **Тип атаки**. В раскрывающемся списке выберите тип атаки. Поле обязательно для заполнения.
- **Примечание**. Укажите дополнительную информацию.
- **Начало атаки**. Укажите дату и время начала атаки. Дата указывается в формате **ДДММГГГГ**. Время указывается в формате **ЧЧ:ММ**.
- **Окончание атаки**. Укажите дату и время окончания атаки. Дата указывается в формате **ДДММГГГГ**. Время указывается в формате **ЧЧ:ММ**.
- **Мощность**. **PPS (пакетов в секунду)**. Введите количество пакетов в секунду.
- **Мощность**. **MPS (мегабит в секунду)**. Введите количество мегабит в секунду.
- **Мощность**. **RPS (запросов в секунду)**. Введите количество запросов в секунду
- **Негативное влияние**. В раскрывающемся списке выберите тип негативного влияния: прерывание доступности ресурса, иные негативные последствия, негативного влияния не было.
- **Примечание**. Укажите дополнительную информацию.

Реализация несанкционированного доступа к банковским и платежным терминалам (atmAttacks)

— Вкладка **Описание по типу: Физическая атака на банкомат**:

- **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.
- **Примечание**. Укажите любые данные, которые могут быть полезными при расследовании инцидента.
- **Тип атаки**. В раскрывающемся списке выберите тип атаки: атаки "блэкбокс", атаки "прямой диспенс" и их разновидности, скимминг, иная атака. Поле обязательно для заполнения.
- **Примечание**. Укажите любые данные, которые могут быть полезными при расследовании инцидента.
- **Вложения**. Приложите любые фотографии пострадавшего устройства, позволяющие получить представление о конкретно реализованном способе атаки, либо следов, оставленных злоумышленником.

Эксплуатация уязвимостей информационной инфраструктуры (vulnerabilities)

— Вкладка **<0.0.0.0>: Внешний адрес пострадавшей системы**:

- **IP-адрес**. Укажите IP-адрес узла, на котором эксплуатировалась уязвимость, в формате XXX.XXX.XXX.XXX.
- **Доменное имя**. Введите в поле доменное имя пострадавшего узла.
- **URL-адрес**. Укажите URL-адрес пострадавшего узла в формате www.domain.com.
- **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**:

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

— Вкладка **<0.0.0.0>: Свой идентификатор уязвимости**:

- **Описание**. Введите описание уязвимости.
- **Название ПО**. Введите название программного обеспечения, в котором была выявлена уязвимость.

- **Версия ПО**. Введите версию программного обеспечения, в котором была выявлена уязвимость.
- **Тип уязвимости**. Введите название типа уязвимости.
- **Класс уязвимости**. Выберите один из следующих вариантов: **Уязвимость кода**, **Уязвимость архитектуры**, **Уязвимость многофакторная**.
- **Дата обнаружения**. Выберите в календаре дату обнаружения уязвимости. По умолчанию выбрана текущая дата.
- **Базовый CVSS**. Введите базовый вектор уязвимости.
- **Опасность**. Выберите уровень опасности обнаруженной уязвимости: низкий, средний, высокий или критический.
- **Меры устранения**. Перечислите, какие меры были предприняты.
- **Статус**. Выберите статус уязвимости.
- **Наличие эксплойта**. Укажите наличие эксплойта.
- **Рекомендации**. Введите рекомендации по устранению уязвимости.
- **Ссылки**. Введите ссылки на источники информации об устранении уязвимости.
- **Вендор**. Введите название производителя программного обеспечения, в котором была обнаружена уязвимость.

Компроментация аутентификационных / учетных данных (bruteForces)

— Вкладка **<0.0.0.0>: Адрес пострадавшей системы**:

  - **IP-адрес**. Укажите IP-адрес пострадавшей системы.
  - **URL**. Укажите месторасположение пострадавшей системы.
  - **Атакованная служба**. Введите наименование сервиса, который был атакован.

— Вкладка **<0.0.0.0>: Атака**:

  - **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.

— Вкладка **<0.0.0.0>: Скомпрометированная учетная запись**:

  - **Учетная запись**. Укажите логин и домен учетной записи, которая была атакована.
  - **Привилегии**. Укажите привилегии учетной записи.

Реализация спам рассылки (spams)

— Вкладка **Описание по типу**:

- **Спам. Дата получения**. Выберите дату получения сообщения, содержащего спам.
- **Цель атаки. Адрес электронной почты**. Введите адрес электронной почты, на который поступил спам.
- **Источник атаки. IP-адрес**. Введите IP-адрес, с которого был отправлен спам, в формате XXX.XXX.XXX.XXX.
- **Источник атаки. Доменное имя**. Введите доменное имя источника рассылки спама.
- **Источник атаки. Адрес электронной почты**. Введите адрес электронной почты, с которого был отправлен спам.

Взаимодействие с центрами "бот-нет" сетей (controlCenters)

— Вкладка **Описание по типу**: **Адрес пострадавшей системы**:

- **IP-адрес**. Введите IP-адрес пострадавшей системы в формате XXX.XXX.XXX.XXX.
- **URL**. Введите URL-адрес пострадавшей системы в формате www.domain.com.

— Вкладка **Описание по типу**: **Информация с ЦУ бот-сети**:

- **URL с ЦУ**. Введите URL-адрес, на котором размещен ЦУ бот-сети.
- **IP-адрес злоумышленника**. Введите IP-адрес злоумышленника, разместившего ЦУ бот-сети, в формате XXX.XXX.XXX.XXX.
- **Действия злоумышленника**. Опишите действия злоумышленника, которые удалось выявить.
- **Сведения о бот-сети**. Введите описание бот-сети.
- **IP-адреса, обращавшиеся к ЦУ**. Введите IP-адреса, обращавшиеся к ЦУ бот-сети, в формате XXX.XXX.XXX.XXX.

Использование фишинговых ресурсов (phishingAttacks)

— Вкладка **<0.0.0.0>: Пострадавшая система**:

- **IP-адрес**. Введите IP-адрес пострадавшей системы в формате XXX.XXX.XXX.XXX.
- **Домен**. Введите в поле доменное имя пострадавшей системы.
- **Добавить фишинговый ресурс**. Введите IP-адрес ресурса в формате XXX.XXX.XXX.XXX и URL-адрес ресурса в формате www.domain.com.
- **Дата фиксации**. Дата фиксирования фишингового сообщения.

Размещение запрещенного контента в сети "Интернет" (maliciousResourcer)

— Вкладка **Описание по типу: Запрещенный контент**:

- **IP-адрес**. Введите IP-адрес запрещенного контента в формате XXX.XXX.XXX.XXX.
- **Единый указатель ресурса**. Введите URL-адрес запрещенного контента в формате www.example.com.
- **Тип контента**. Введите тип запрещенного контента.

Размещение вредоносного ресурса в сети "Интернет" (prohibitedContents)

— Вкладка **Описание по типу: Вредоносный ресурс**:

- **IP-адрес**. Введите IP-адрес вредоносного ресурса в формате XXX.XXX.XXX.XXX.
- **Единый указатель ресурса**. Введите URL-адрес вредоносного ресурса в формате www.example.com.
- **Описание вредоносной активности**. Введите описание вредоносной активности.

Выполнение изменения контента (changeContent)

— Вкладка **Описание по типу: Вредоносный ресурс**:

- **IP-адрес**. Введите IP-адрес измененного контента в формате XXX.XXX.XXX.XXX.
- **URL**. Введите URL-адрес измененного контента в формате www.example.com.
- **Тип измененного контента**. Введите тип измененного контента.

Выполнение сканирования портов (scanPorts)

— Вкладка **Описание по типу: Сканирование портов**:

- **Источник сканирования**. Введите IP-адреса источников сканирования в формате XXX.XXX.XXX.XXX.
- **Сканированные порты**. Введите номера портов, которые подверглись сканированию.
- **Метод сканирования**. Опишите метод сканирования портов.
- **Дата и время начала сканирования**. Выберите дату и укажите время начала сканирования портов.
- **Дата и время окончания сканирования**. Выберите дату и укажите время окончания сканирования портов.

Иная компьютерная атака (other)

— Вкладка **Описание по типу**:

- **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.com.

5.6.2.10. Дополнительно

Вкладка **Дополнительно** содержит следующие элементы управления:

— **Дополнительный комментарий** — поле для произвольного комментария к инциденту.

— **Отправить в ГосСОПКА** — флажок, который требуется установить, если вы хотите, чтобы информация об инциденте отправлялась в ГосСОПКА.

5.7. Страница Информационные карточки

Информационная карточка может содержать уведомление о мероприятии по раскрытию информации или другие полезные материалы в свободной форме. Информационная карточка, содержащая уведомление участнику о планируемом мероприятии по раскрытию информации, называется публикацией. Информационная карточка может быть использована в рамках работы над задачами, инцидентами или угрозами.

Информация о доступных в веб-интерфейсе системы информационных карточках отображается на странице **Информационные карточки**.

Рабочая область страницы **Информационные карточки** содержит панель фильтрации и таблицу информационных карточек. По умолчанию таблица отображает только актуальные информационные карточки. Вы можете менять список отображаемых в таблице информационных карточек, используя фильтры в панели фильтрации.

При выборе фильтра **Все** таблица содержит все информационные карточки, зарегистрированные в PT Incident Processing Center.

Часть фильтров объединена в группу **По ответственному**:

— **Назначенные мне**. При выборе этого фильтра таблица содержит только информационные карточки, ответственным за обработку которых являетесь вы.

— **Неназначенные**. При выборе этого фильтра таблица содержит информационные карточки, для которых пока не указано лицо, отвечающее за обработку.

— **Назначенные на активных пользователей**. При выборе этого фильтра таблица содержит только те информационные карточки, которые назначены на активных пользователей.

— **Назначенные на заблокированных пользователей**. При выборе этого фильтра таблица содержит только те информационные карточки, которые назначены на заблокированных пользователей.

Часть фильтров объединена в группу **По типу**:

— **Информационные карты**. При выборе этого фильтра таблица содержит все информационные карты, кроме публикаций.

— **Публикации**. При выборе этого фильтра таблица содержит только публикации.

Примечание. Вы можете уточнять результаты фильтрации, добавляя по кнопке **Добавить фильтр** фильтры по отдельным параметрам информационной карточки.

Вы можете воспользоваться строкой поиска, расположенной над таблицей, чтобы найти интересующую вас информационную карточку. В строке необходимо указать идентификатор информационной карточки или ее описание.

Основные параметры информационных карточек распределены по столбцам таблицы. Вы можете сортировать значения в столбцах таблицы, нажав на заголовок столбца.

Панель инструментов страницы **Информационные карточки** содержит кнопки добавления информационной карточки, изменения ее параметров и добавления дополнительного фильтра по одному из параметров информационной карточки.

В системе предусмотрены следующие дополнительные фильтры:

— **Дата публикации** — дата публикации информационной карточки о мероприятии по раскрытию информации. По умолчанию создается фильтр на текущую дату. Вы можете скорректировать дату, выбрав фильтр и в открывшемся календаре указав дату или период.

— **Дата последнего обновления** — дата последнего изменения информационной карточки. По умолчанию создается фильтр на текущую дату. Вы можете скорректировать дату, выбрав фильтр и в открывшемся календаре указав дату или период.

— **Дата появления** — дата создания информационной карточки в системе. По умолчанию создается фильтр на текущую дату. Вы можете скорректировать дату, выбрав фильтр и в открывшемся календаре указав дату или период.

— **Источник** — название организации, от которой поступила информационная карточка. Источником могут быть участники или оператор PT Incident Processing Center. Вы можете выбрать фильтр и в раскрывающемся списке установить флажки для организаций, информационные карточки по которым вы хотите отобразить в таблице.

— **Тип** — тип информационной карточки: публикация или другие информационные карточки. Вы можете выбрать фильтр и в раскрывающемся списке установить флажки для типов, информационные карточки по которым вы хотите отобразить в таблице.

— **Актуальность** — статус информационной карточки. Вы можете выбрать фильтр и в раскрывающемся списке установить флажок для статуса, информационные карточки по которому вы хотите отобразить в таблице.

Кнопка **Сбросить фильтр** позволяет удалить все дополнительные фильтры.

Примечание. Вы можете добавить несколько дополнительных фильтров. Каждый последующий дополнительный фильтр уточняет результат фильтрации таблицы информационных карточек.

Если информационная карточка устарела и больше не актуальна, вы можете изменить ее статус на **Неактуальна**. Вы не можете удалять информационные карточки из PT Incident Processing Center.

5.8. Информационная карточка

Информационная карточка содержит полную информацию о мероприятии или другие данные.

Информационная карточка состоит из трех частей. В левой части рабочей области отображается информационная панель, которая содержит основные группы параметров информационной карточки. В центральной панели отображаются параметры, входящие в выбранную группу. Кроме того, в центральной панели вы можете просматривать, добавлять и изменять метки. Набор вкладок и полей зависит от типа информационной карточки.

В панели с дополнительной информацией, расположенной в правой части рабочей области, вы можете:

- просматривать и добавлять связи (см. раздел 21.2.1) информационной карточки с другими объектами;
- просматривать и добавлять комментарии (см. раздел 21.3);
- просматривать историю изменений (см. раздел 21.4) информационной карточки.

Панель инструментов информационной карточки содержит кнопку **Редактировать**, по которой вы можете изменять параметры информационной карточки. По кнопке **Информационные карточки** вы можете перейти к таблице информационных карточек.

5.9. Страница Участники

Информация о зарегистрированных в PT Incident Processing Center участниках приведена на странице **Участники**.

Рабочая область страницы содержит таблицу участников и панель фильтрации. По умолчанию таблица участников отображает всех участников, зарегистрированных в PT Incident Processing Center. Вы можете менять список отображаемых в таблице участников, используя фильтры в панели фильтрации:

- **Все участники**. При выборе этого фильтра таблица содержит всех участников, зарегистрированных в PT Incident Processing Center.
- **По статусу**:
  - **Активные**. При выборе этого фильтра таблица содержит только активированных участников.
  - **Деактивированные**. При выборе этого фильтра таблица содержит только заблокированных участников.

— **По важности**:
  - **Высокая**. При выборе этого фильтра таблица содержит только участников с высокой значимостью.
  - **Средняя**. При выборе этого фильтра таблица содержит только участников со средней значимостью.
  - **Низкая**. При выборе этого фильтра таблица содержит только участников с низкой значимостью.
— **По виду**:
  - **Регистраторы**. При выборе этого фильтра таблица содержит только организации, которые регистрируют новые доменные имена и продлевают срок действия уже существующих имен в домене.
  - **Хостинг-провайдеры**. При выборе этого фильтра таблица содержит только организации, которые предоставляют свои ресурсы для размещения информации.

Основные параметры участников распределены по столбцам таблицы.

Вы можете воспользоваться полем поиска, расположенным над таблицей участников, чтобы найти интересующего вас участника. В поле нужно указать название, регистрационный номер или БИК организации участника.

Подробную информацию об участнике вы можете просматривать в карточке участника. Перейти в карточку участника вы можете по ссылке с идентификатором в столбце **Участник**.

Панель инструментов страницы **Участники** содержит следующие кнопки:

— **Добавить участника**. По этой кнопке вы можете зарегистрировать нового участника в PT Incident Processing Center, заполнив карточку участника.

— **Редактировать участника**. По этой кнопке вы можете изменять параметры карточки участника.

— **Заблокировать / Активировать**. По этой кнопке вы можете деактивировать или активировать участника.

— **Добавить фильтр**. По этой кнопке вы можете уточнять результаты фильтрации по отдельным параметрам участника. В системе существуют следующие дополнительные фильтры:
  - **Форма юридического лица**. Вы можете воспользоваться поиском по форме юридического лица.
  - **Отрасль** — отрасль, в которой участник осуществляет свою деятельность.
  - **Тип участника**. Вы можете выбрать один или несколько типов, участников по которым вы хотите отобразить в таблице.
  - **Тип организации**. Вы можете выбрать один или несколько типов организаций, участников по которым вы хотите отобразить в таблице.

- **Вид участника**. Вы можете выбрать один или несколько видов, участников по которым вы хотите отобразить в таблице участников.
- **Статус**. Вы можете отображать в таблице активированных или деактивированных участников.
- **Пользователь**. Вы можете воспользоваться строкой поиска по пользователям. В строке нужно указать имя, фамилию или логин пользователя.

Примечание. Вы можете добавить несколько дополнительных фильтров. Каждый последующий дополнительный фильтр уточняет результат фильтрации таблицы участников.

В этом разделе

5.9.1. Карточка участника

Карточка участника содержит полную информации об организации и ответственных лицах участника.

Карточка участника состоит из двух панелей — информационной и дополнительной. Информационная панель содержит параметры участника. Вы можете изменять параметры участника или заблокировать его. Удалить участника из системы нельзя.

В панели, содержащей дополнительную информацию, отображается информация об ответственных лицах участника и используемом программном обеспечении. Кроме того, вы можете просматривать и настраивать уведомления, добавлять комментарии (см. раздел 21.3) и просматривать историю изменений (см. раздел 21.4).

5.9.2. Параметры участника

Примечание. Параметры участника настраиваются через конфигурирование в зависимости от специфики организации.

Карточка участника содержит следующие параметры:

— **Тип организации**. Выбирается из предложенных системой вариантов.

— **Название** — краткое название организации.

— **Полное название** — полное название организации.

— **Важность** — важность организации.

— **Организационно-правовая форма организации (ОКОПФ)** — наименование организационно-правовой формы организации.

- **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 PT Incident Processing Center.
- **Регистрационный номер** — регистрационный номер организации.
- **Вид**. В системе существуют следующие виды организаций:
  - **ГосСОПКА** — государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак;
  - **Регистратор** — организации, уполномоченные регистрировать новые доменные имена и продлевать срок действия уже существующих доменных имен в домене, для которого установлена обязательная регистрация;
  - **Хостинг-провайдер** — организации, предоставляющие услуги по предоставлению дискового пространства для размещения файлов на своем сервере;
  - **КО** — все кредитные организации, кроме включенных в Реестр кредитных организаций, признанных центром значимыми на рынке платежных услуг;
  - **Значимые** — все кредитные организации, признанные центром значимыми на рынке платежных услуг (кроме СЗКО);
  - **СЗКО** — системно значимые кредитные организации;
  - **ПС** — платежные системы, включенные в Реестр операторов платежных систем;
  - **НКО** — некоммерческие организации, не являются ПС;
  - **Страховые TOP-10** — десять страховых компаний, имеющих наивысший рейтинг;
  - **Страховые не TOP-10** — страховые компании, не вошедшие в топ-10;
  - **МФО, инвестиционные фонды, ломбарды** — микрофинансовые организации, инвестиционные фонды и ломбарды;
  - **Антивирусная лаборатория** — вирусные лаборатории, антивирусные компании, исследовательские лаборатории;

  - **Контрагент информационной безопасности** — организации, предоставляющие информацию об угрозах;
  - **Остальные источники** — другие организации.
- **Тип** — типы участников. В системе существуют следующие типы участников:
  - **Участник информационного обмена** — кредитные организации, значимые и системно значимые кредитные организации, небанковские кредитные организации, платежные системы, страховые компании, микрофинансовые организации, инвестиционные фонды и ломбарды. Взаимодействие осуществляется через "Личный кабинет участника" и электронную почту.
  - **Системный участник** — антивирусные лаборатории, контрагенты информационной безопасности, регистраторы, хостинг-провайдеры и ГосСОПКА. Взаимодействие осуществляется через электронную почту.
  - **Неучаствующая организация** — прочие организации, зарегистрированные в центре. Взаимодействие осуществляется через электронную почту.
- **Поднадзорные организации** — установленный флажок означает, что участник относится к организациям, поднадзорным центру.
- **Регистрационный номер** — номер организации во всероссийском реестре кредитных организаций.
- **Идентификатор КИИ** — идентификатор объекта критической информационной инфраструктуры.
- **Операторы связи** — организации, предоставляющие услуги доступа к интернету.
- **Идентификаторы регистратора в Whois** — идентификаторы регистратора доменного имени в WHOIS.
- **В компетенции PT Incident Processing Center** — установленный флажок означает, что участник находится в зоне влияния PT Incident Processing Center. Такие участники обязаны предпринимать действия, указанные оператором PT Incident Processing Center, например блокировать вредоносный ресурс в интернете.
- **Признак РКН** — установленный флажок означает, что участник является Роскомнадзором.
- **ИНН** — идентификационный номер налогоплательщика организации. Поле должно содержать десять цифр.
- **КПП** — код причины постановки организации на учет. Поле должно содержать девять цифр.
- **БИК** — банковский идентификационный код организации. Заполняется автоматически из справочника "Справочник БИК и SWIFT BIC".
- **БИК головной организации** — банковский идентификационный код головной организации. Заполняется автоматически из справочника "Справочник БИК и SWIFT BIC".

- **SWIFT BIC** — банковский идентификационный код SWIFT. Заполняется автоматически из справочника "Справочник БИК и SWIFT BIC".
- **Платежная система** — платежная система организации.
- **БИН эмитента** — банковский идентификационный номер банка-эмитента организации. Заполняется автоматически из справочника "Таблицы БИН банков-эмитентов".
- **БИН эквайера** — банковский идентификационный номер банка-эквайера организации. Заполняется автоматически из справочника "Таблицы БИН банков-эквайеров".
- **ОГРН** — государственный регистрационный номер организации. Поле должно содержать тринадцать цифр.
- **Юридический адрес** — полный юридический адрес, указанный в учредительных документах организации.
- **Почтовый адрес** — адрес для рассылки корреспонденции.
- **Фактический адрес** — адрес местонахождения организации.
- **Отрасль** — отрасль, в которой организация осуществляет свою деятельность.
- **Типы объектов** — типы объектов, которые использует организация.
- **Типы систем** — типы систем, которыми пользуется организация.

- **Информация на объектах** — типы информации, обрабатываемой на объектах.
- **Информация на системах** — типы информации, обрабатываемой системами.
- **Категория объектов**. В системе существуют следующие категории объектов:
  - **КВО** — критически важный объект;
  - **Объект КИИ** — объект критической информационной инфраструктуры;
  - **Объект КСИИ** — объект ключевой системы информационной инфраструктуры.
- **Категория систем** — категория значимости системы организации.
- **Тип используемой криптографии** — выбор типа шифрования для переписки с участником:
  - **ГОСТ** — используется криптография ГОСТ (вариант по умолчанию для всех участников);
  - **GPG** — используется криптография GPG;
  - **Не используется** — криптография в переписке с участником не используется, письма не шифруются, не применяется электронная подпись.
- **Автоматически отправлять инциденты в ГосСОПКА** — все инциденты участника, в параметрах которого установлен флажок, будут автоматически отправляться в ГосСОПКА.
- **Номер факсимильного аппарата для блокировки корреспондентского счета** — используя факсимильный аппарат с номером, указанным в этом поле, участник может отправить в PT Incident Processing Center запрос на блокировку корреспондентского счета.
- **Веб-сайт** — URL сайта участника.
- **УИС** — уникальный идентификатор составителя электронного документа.
- **Контактные данные ответственного за обмен в ПС БР** — в блоке параметров указываются контактные данные лица, ответственного за обмен электронными сообщениями в платежной системе центра: **Фамилия ответственного лица**, **Имя ответственного лица**, **Отчество ответственного лица**, **Должность**, **Эл. почта**, **Городской телефон**, **Мобильный телефон**.

5.9.3. Карточка ответственного лица

Полная информация об ответственном лице отображается в карточке ответственного лица.

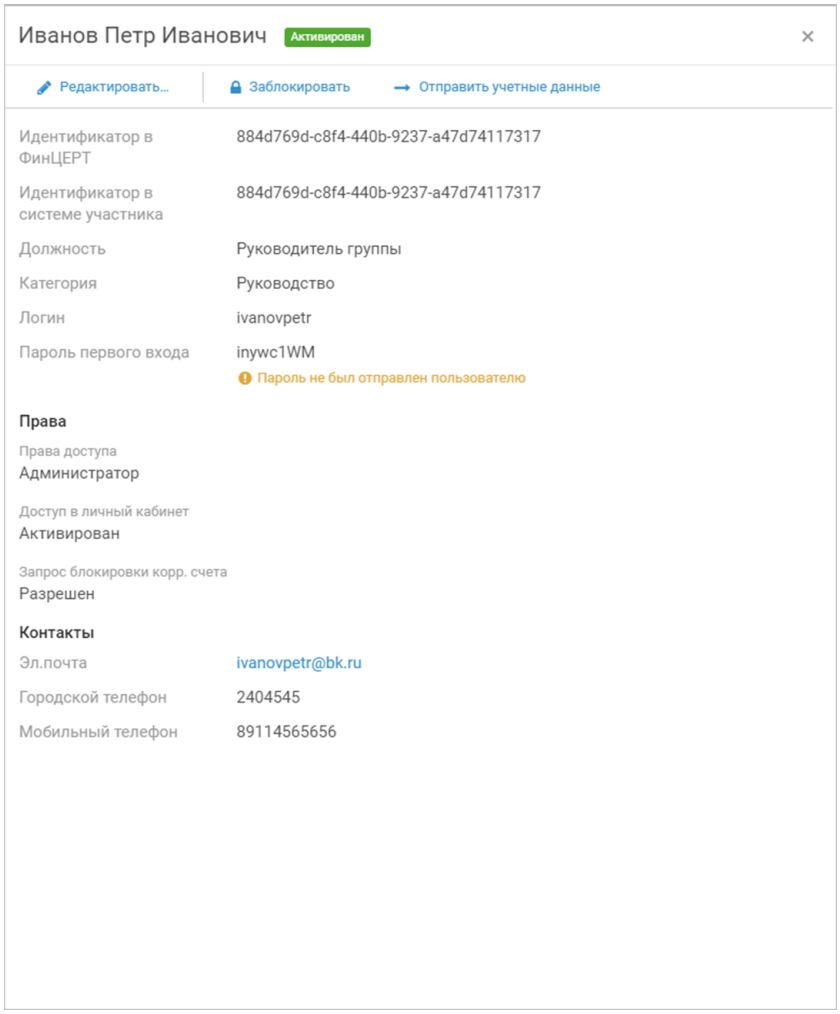

Рисунок 6. Карточка ответственного лица

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

5.9.4. Параметры ответственного лица

Карточка ответственного лица содержит следующие параметры:

- **Идентификатор в** PT Incident Processing Center — идентификатор ответственного лица в PT Incident Processing Center.
- **Идентификатор в системе участника** — идентификатор ответственного лица, который ему присваивает система участника.
- **Должность** — должность ответственного лица.
- **Категория** — категория структурного подразделения ответственного лица.

- **Логин** — логин может содержать только буквы латинского алфавита, цифры, спецсимволы и не может содержать более 64 символов.
- **Пароль первого входа** — пароль первого входа может содержать от шести до восьми символов и может состоять только из букв латинского алфавита, цифр и спецсимволов.
- **Доступ в личный кабинет** — активированные пользователи имеют доступ к "Личному кабинету участника" и получают уведомления.
- **Права доступа** — в системе существуют роли администратора и пользователя.
- **Ответственный за обмен в ПС БР** — лицо, которое имеет полномочия подписывать заявления на блокировку корреспондентских счетов. Ответственные за обмен электронными сообщениями с платежной системой центра отмечены в системе цветом.
- **Эл. почта** — адрес электронной почты ответственного лица для отправки уведомлений.
- **Городской телефон** — номер стационарного рабочего телефона ответственного лица.
- **Мобильный телефон** — номер мобильного телефона ответственного лица.
- **Сертификат открытого ключа** — блок параметров, содержащий подробную информацию об активном сертификате открытого ключа, выданном ответственному лицу.

5.10. Страница Операции без согласия

Примечание. Сведения об операциях без согласия указывают участники, которым в рамках их деятельности необходимо фиксировать и обрабатывать такую информацию.

Информация о зарегистрированных в PT Incident Processing Center денежных операциях, выполненных без согласия клиентов участников, отображается на странице **Операции без согласия**.

Рабочая область страницы содержит таблицу операций и панель фильтрации по актуальности с группами **Все**, **Актуальные**, **Неактуальные**, **Требуют ручного контроля**. По умолчанию таблица содержит все операции, зарегистрированные в PT Incident Processing Center.

Основные параметры операций распределены по столбцам таблицы. Вы можете сортировать значения в столбцах таблицы, нажав на заголовок столбца.

Кроме того, вы можете воспользоваться строкой поиска, расположенной над таблицей, чтобы найти интересующую вас операцию. В строке необходимо указать идентификатор операции или информацию о плательщике.

Подробная информация об операции отображается в карточке операции. Перейти в карточку операции вы можете по ссылке с идентификатором в столбце **ID Операции**.

Панель инструментов страницы **Операции без Согласия** содержит кнопки для групповых действий с операциями без согласия, выбранными в списке, а также кнопку **Добавить фильтр**.

По кнопке **Добавить фильтр** вы можете последовательно добавить несколько дополнительных фильтров для параметров операции без согласия. Каждый дополнительный фильтр уточняет результат фильтрации таблицы операций.

При фильтрации по строчному параметру (например, по названию электронной платежной системы получателя платежа) фильтр работает по следующим правилам:

— не учитывается регистр введенных символов: например, фильтры "БАнк01" и "банк01" возвращают одинаковые результаты;

— если значение в фильтре заключено в кавычки, фильтр возвращает результаты с полным совпадением;

— если значение в фильтре не заключено в кавычки, фильтр возвращает результаты с частичным совпадением.

5.11. Карточка операции без согласия

Карточка операции без согласия содержит полную информацию о денежной операции, выполненной без согласия клиента участника. Карточка операции без согласия формируется в PT Incident Processing Center автоматически из карточки инцидента.

Карточка операции без согласия состоит из трех панелей. В левой части рабочей области отображается информационная панель, которая содержит основные группы параметров операции (см. раздел 5.6.2.5). В центральной панели отображаются параметры, входящие в выбранную группу.

Удалить карточку операции без согласия из системы нельзя, но вы можете изменить актуальность операции. Информация по неактуальным операциям без согласия не отображается в фидах.

В правой части рабочей области вы можете просматривать и добавлять связи операции с другими объектами. Связи с инцидентом и запросом, из которых поступила операция без согласия, создаются автоматически.

5.12. Страница Рассылки центра

Вы можете информировать участников о наличии уязвимостей в программном или аппаратном обеспечении, новых возможностях, изменениях формата электронных форм, о технических работах и других событиях. Эта информация отображается на странице **Рассылки центра**.

Исходящие сообщения делятся на типы:

— **Бюллетени** — сообщения о наличии или устранении уязвимостей в программном или аппаратном обеспечении. Такие сообщения могут описывать способы исправления уязвимостей и содержать другие сведения, важные с точки зрения информационной безопасности.

— **Новости** — сообщения общего характера, например об изменениях формата электронных форм.

— **Уведомления** — сообщения о технических работах, об изменениях регламентов взаимодействия.

Рабочая область страницы содержит таблицу рассылки и панель фильтрации. По умолчанию таблица рассылки отображает сообщения всех типов, добавленные в PT Incident Processing Center. Основные параметры рассылки отображаются в столбцах таблицы. Вы можете сортировать значения в таблице, нажав на заголовок столбца. Вы можете изменять список отображаемых сообщений, используя фильтры в панели фильтрации:

- **Все**. При выборе этого фильтра таблица содержит все виды рассылки, добавленные в PT Incident Processing Center.
- **Черновики**. При выборе этого фильтра таблица содержит только неопубликованные рассылки.
- **Опубликованные**. При выборе этого фильтра таблица содержит только опубликованную рассылку.

Вы можете воспользоваться строкой поиска, расположенной над таблицей, чтобы найти интересующую вас рассылку. В строке нужно указать идентификатор рассылки, ее заголовок, описание или имя вложенного файла.

Подробная информация о рассылке отображается в карточке рассылки. Перейти в нее вы можете по ссылке с идентификатором рассылки в столбце **ID рассылки**.

Панель инструментов страницы **Рассылки центра** содержит следующие кнопки:

- **Добавить рассылку**. По этой кнопке вы можете создать рассылку.
- **Создать копию**. По этой кнопке вы можете создать рассылку на основе уже существующей.
- **Редактировать**. По этой кнопке вы можете изменять параметры неопубликованных рассылок.
- **Удалить**. По этой кнопке вы можете удалять неопубликованные рассылки.
- **Скачать публикуемый файл**. По этой кнопке вы можете скачивать публикуемые файлы рассылки в локальную папку.
- **Опубликовать**. По этой кнопке вы можете публиковать черновики. После публикации вы можете добавить новых получателей рассылки.
- **Добавить получателей**. По этой кнопке вы можете отправить опубликованную рассылку новым получателям.
- **Добавить фильтр**. По этой кнопке вы можете уточнять результаты фильтрации по отдельным параметрам рассылки. В системе существуют следующие дополнительные фильтры:
  - **Дата обновления** — дата последнего изменения рассылки. По умолчанию создается фильтр на текущую дату, который можно скорректировать, выбрав фильтр и в открывшемся календаре указав дату или период.
  - **Дата публикации** — дата публикации рассылки. По умолчанию создается фильтр на текущую дату, который можно скорректировать, выбрав фильтр и в открывшемся календаре указав дату или период.

- **Участник** — участник, для которого была опубликована рассылка. Вы можете воспользоваться поиском по имени участника.
- **Группа рассылки** — группа, для которой была опубликована рассылка. Вы можете воспользоваться поиском по имени участника.
- **Статус** — статус рассылки. Вы можете воспользоваться поиском по статусу рассылки.

5.13. Карточка рассылки

Карточка рассылки состоит из трех частей. В левой части рабочей области отображается информационная панель, которая содержит основные группы параметров рассылки и кнопку **Рассылки центра** для перехода к таблице рассылки. В центральной панели отображаются параметры, входящие в выбранную группу.

Рассылка содержит следующие общие сведения:

— **Статус**. В PT Incident Processing Center существуют следующие статусы рассылки:
  - **Опубликован** — рассылка опубликована.
  - **Черновик** — рассылка не опубликована.

— **Краткое описание** — краткое содержание рассылки.

— **Тип рассылки** — бюллетень, новость или уведомление.

— **Подтип рассылки** — подтипы рассылки настраиваются администратором при установке PT Incident Processing Center.

— **Исходный файл** — этот файл можно изменять. Исходный файл создается при формировании рассылки из инцидента или угрозы. При публикации этот файл не будет отправлен участникам.

— **Публикуемый файл** — этот файл содержит информацию исходного файла. При публикации этот файл рассылается участникам.

— **Дополнительные публикуемые файлы** — при публикации эти файлы рассылаются участникам. Вы можете вложить в рассылку до пяти дополнительных файлов.

  Примечание. Рекомендуется добавлять публикуемые и дополнительные публикуемые файлы размером не более 5 МБ. Большие файлы будут доступны в «Личном кабинете участника», но могут не дойти на электронную почту получателей из-за параметров серверов.

— **Создан** — дата создания рассылки.

— **Дата изменения** — дата последнего изменения рассылки.

— **Дата публикации** — дата публикации рассылки.

— **Метки** — ключевые слова для поиска данных.

На вкладке **Получатели рассылки** отображается следующая информация:

— **Участники** — организации, которым была отправлена рассылка.

— **Группы рассылки** — группы участников, которым была отправлена рассылка.

— **Опубликовано** — оператор, опубликовавший рассылку.

В панели с дополнительной информацией, расположенной в правой части рабочей области, вы можете:

— просматривать и добавлять связи рассылки (см. раздел 21.2.1) с другими объектами;

— просматривать и добавлять комментарии (см. раздел 21.3);

— просматривать историю изменений (см. раздел 21.4) рассылки.

Кроме того, по соответствующей кнопке в панели инструментов вы можете:

— создать копию рассылки;

— изменить рассылку;

— удалить рассылку;

— добавить получателей и настроить группы рассылки.

5.14. Страница Справочники

Справочники предназначены для хранения значений классифицируемых параметров описания субъектов, объектов и мероприятий, а также общих параметров.

► Чтобы просмотреть информацию о доступных в веб-интерфейсе продукта справочниках,

в главном меню в разделе **База данных** выберите пункт **Справочники**.

Страница **Справочники** состоит из трех частей. В левой части представлены группы сущностей, к которым привязаны справочники:

— субъекты:

- отраслевая и другая принадлежность;

— объекты:

- категории объектов;
- типы объектов;
- виды услуг;
- типы обрабатываемой информации;

— общие:

- форма юридического лица;
- категории ответственных лиц;
- ответственные лица;

- страны;
- адреса.

Центральная часть страницы представляет список параметров, входящих в выбранную группу. В правой части отображается подробная информация о выбранном параметре.

Существуют системные и пользовательские справочники. К пользовательским справочникам относятся справочники **Ответственные лица** и **Адреса**. Вы можете редактировать пользовательские справочники. К системным справочникам относятся все остальные справочники. Такие справочники поставляются вместе с PT Incident Processing Center. Вы не можете редактировать системные справочники.

5.15. Страница Угрозы

Информация об угрозах отображается на странице **Угрозы**.

Рабочая область страницы содержит таблицу угроз и панель фильтрации. По умолчанию таблица отображает все угрозы, добавленные в PT Incident Processing Center. Вы можете менять список отображаемых в таблице угроз, используя фильтры в панели фильтрации:

— **Все**. При выборе этого фильтра таблица содержит все угрозы, зарегистрированные в PT Incident Processing Center.

— **Активные**. При выборе этого фильтра таблица содержит все активные угрозы.

— **Обработанные**. При выборе этого фильтра таблица содержит обработанные оператором угрозы.

Часть фильтров объединена в группу **По ответственному**:

— **Назначенные мне**. При выборе этого фильтра таблица содержит только те угрозы, ответственным за обработку которых являетесь вы.

— **Неназначенные**. При выборе этого фильтра таблица содержит только те угрозы, для которых пока не указано лицо, отвечающее за обработку.

— **Назначенные на активных пользователей**. При выборе этого фильтра таблица содержит только те угрозы, которые назначены на активных пользователей.

— **Назначенные на заблокированных пользователей**. При выборе этого фильтра таблица содержит угрозы, которые назначены на заблокированных пользователей. Это возможно в случае если пользователь был заблокирован после того, как на него была назначена угроза.

Основные параметры угроз распределены по столбцам таблицы. Вы можете сортировать значения в столбцах таблицы, нажав на заголовок столбца.

Кроме того, вы можете воспользоваться строкой поиска, расположенной над таблицей угроз, чтобы найти интересующую вас угрозу. В строке нужно указать идентификатор угрозы, ее заголовок или описание.

Подробная информация об угрозе отображается в карточке угрозы. Перейти в карточку угрозы вы можете по ссылке с идентификатором в столбце **Угроза**.

Панель инструментов страницы **Угрозы** содержит следующие кнопки:

- **Добавить угрозу**. По этой кнопке вы можете добавить угрозу в систему.
- **Редактировать угрозу**. По этой кнопке вы можете изменять параметры угроз.
- **Изменить статус**. По этой кнопке вы можете изменять статус обработки угрозы.
- **Назначить**. По этой кнопке вы можете назначить ответственного за обработку угрозы.
- **Выпустить отчет**. По этой кнопке вы можете выпускать отчеты об угрозах по времени или типу.
- **Добавить фильтр**. По этой кнопке вы можете уточнять результаты фильтрации по отдельным параметрам угрозы. В системе существует дополнительный фильтр **Дата создания**. По умолчанию создается фильтр на текущую дату, который можно скорректировать, указав дату или период в календаре.

5.16. Карточка угрозы

Карточка угрозы содержит полную информацию об угрозе.

Карточка угрозы состоит из трех частей. В левой части рабочей области отображается информационная панель, которая содержит кнопку **Угрозы** для перехода к таблице угроз и основные группы параметров угрозы. В центральной панели отображаются параметры, входящие в выбранную группу. Кроме того, в центральной панели вы можете просматривать, добавлять и изменять метки. Набор вкладок и полей зависит от типа угрозы.

В панели с дополнительной информацией, расположенной в правой части рабочей области, вы можете:

- просматривать и добавлять связи угрозы с другими объектами;
- просматривать и добавлять комментарии;
- просматривать историю изменений карточки угрозы.

Кроме того, по соответствующей кнопке в панели инструментов вы можете:

- изменять статус угрозы;
- изменять параметры угрозы;
- назначить ответственного за обработку угрозы.

5.17. Страница Уязвимости

Информация об уязвимостях отображается на странице **Уязвимости**.

Рабочая область страницы содержит таблицу уязвимостей и панель фильтрации. По умолчанию таблица отображает все уязвимости, добавленные в PT Incident Processing Center. Вы можете менять список отображаемых в таблице уязвимостей, используя фильтры в панели фильтрации:

- **Все**. При выборе этого фильтра таблица содержит все уязвимости, зарегистрированные в PT Incident Processing Center.
- **Активные**. При выборе этого фильтра таблица содержит все активные уязвимости.
- **Обработанные**. При выборе этого фильтра таблица содержит обработанные оператором уязвимости.

Часть фильтров объединена в группу **По ответственному**:

- **Назначенные мне**. При выборе этого фильтра таблица содержит только те уязвимости, ответственным за обработку которых являетесь вы.
- **Неназначенные**. При выборе этого фильтра таблица содержит только те уязвимости, для которых пока не указано лицо, отвечающее за обработку.
- **Назначенные на активных пользователей**. При выборе этого фильтра таблица содержит только те уязвимости, которые назначены на активных пользователей.
- **Назначенные на заблокированных пользователей**. При выборе этого фильтра таблица содержит только те уязвимости, которые назначены на заблокированных пользователей. Это возможно в случае если пользователь был заблокирован после того, как на него был назначена уязвимость.

Основные параметры уязвимостей отображены в таблице уязвимостей. Вы можете сортировать значения в столбцах таблицы, нажав на заголовок столбца. Чтобы найти интересующую вас уязвимость, вы можете воспользоваться строкой поиска, расположенной над таблицей уязвимостей. В строке можно указать:

- идентификатор уязвимости;
- наименование уязвимости;
- содержимое следующих полей из карточки уязвимости: **Идентификаторы других систем описаний уязвимостей**, **Краткое описание**, **Прочая информация**, **Описание**.

В карточке уязвимости отображается подробная информация об уязвимости. Перейти в карточку уязвимости вы можете по ссылке с идентификатором в столбце **Уязвимость**.

Панель инструментов страницы **Уязвимости** содержит следующие кнопки:

- **Добавить уязвимость**. По этой кнопке вы можете добавить уязвимость в систему.
- **Редактировать**. По этой кнопке вы можете изменять параметры уязвимости.
- **Изменить статус**. По этой кнопке вы можете изменять статус обработки уязвимости.
- **Назначить**. По этой кнопке вы можете назначить ответственного за обработку уязвимости.

— **Выпустить отчет**. По этой кнопке вы можете выпускать отчеты об уязвимостях по времени, классу и участнику.

— **Добавить фильтр**. Вы можете добавлять фильтр по отдельным параметрам уязвимости, выбрав критерий и атрибут фильтра в раскрывающемся списке кнопки:

- **Назначенный оператор** — оператор, ответственный за обработку уязвимости.
- **Дата выявления** — дата, когда была обнаружена уязвимость. По умолчанию создается фильтр на текущую дату, который можно изменить, указав дату или период в календаре.
- **Класс** — характеристика уязвимости, определяющая причину ее возникновения.
- **Статус** — статус обработки уязвимости.

Примечание. Вы можете одновременно применять нескольких фильтров и условие поиска. Критерии фильтрации объединяются по правилам логического "И". Атрибуты фильтрации внутри одного критерия объединяются по правилам логического "ИЛИ".

В этом разделе

5.17.1. Карточка уязвимости

Карточка уязвимости содержит всю имеющуюся в системе информацию об уязвимости.

Карточка уязвимости состоит из трех частей. В левой части рабочей области отображается информационная панель, которая содержит ссылку **Уязвимости** для перехода к таблице уязвимостей и группы параметров уязвимости.

В центральной панели отображаются параметры, входящие в выбранную группу. Набор вкладок и параметров зависит от типа уязвимости. По кнопкам в панели инструментов вы можете:

— изменять статус уязвимости;

— изменять параметры уязвимости;

— назначить ответственного за обработку уязвимости.

В блоке параметров **Метки** вы можете просматривать, изменять и добавлять метки (см. раздел 21.1).

В панели с дополнительной информацией, расположенной в правой части рабочей области, вы можете:

— просматривать и добавлять связи уязвимости с другими объектами;

— просматривать и добавлять комментарии;

— просматривать историю изменений карточки уязвимости.

5.17.2. Параметры уязвимости

Параметры уязвимости отображаются в карточке уязвимости.

Примечание. В разделе приведены описания параметров для Российской Федерации.

Вкладка **Общие сведения** в карточке уязвимости содержит следующие параметры уязвимости:

- **Название**. Название, отражающее суть уязвимости.
- **Статус**. Статус обработки уязвимости. По умолчанию создаваемой уязвимости система назначает статус **Новая**.
- **Назначена**. Ответственный за обработку уязвимости.
- **Дата выявления**. Дата и время выявления уязвимости. Дата указывается в формате **ДДММГГГГ**. Время указывается в формате **ЧЧ:ММ**.
- **Участник**. Имя зарегистрированного в системе участника, от которого поступила информация об уязвимости.
- **Автор**. Имя сотрудника организации-участника, который обнаружил уязвимость, или ссылка на ресурс в интернете.
- **Идентификаторы других систем описаний уязвимостей**. Один идентификатор или несколько через запятую.
- **Критерии опасности уязвимости**. Вектор метрик уязвимости в формате системы оценки уязвимостей CVSS версии 3. О системе CVSS см. сайт проекта Forum of Incident Response and Security Teams.

  Например, `CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N`.
- **Класс**. Класс уязвимости:
  - **Уязвимость кода (COD)**. Уязвимость, появившаяся в процессе разработки программного обеспечения.
  - **Уязвимость конфигурации (CFG)**. Уязвимость, появившаяся в процессе настройки программного обеспечения и технических средств информационной системы.
  - **Уязвимость архитектуры (ARH)**. Уязвимость, появившаяся в процессе проектирования информационной системы.
  - **Организационная уязвимость (ORG)**. Уязвимость, появившаяся в связи с отсутствием или недостатком организационных мер защиты информации в информационной системе и (или) несоблюдением правил эксплуатации системы защиты информационной системы и требований организационно-распорядительных документов по защите информации и (или) несвоевременным выполнением соответствующих действий должностным лицом (работником) или подразделением, ответственными за защиту информации.
  - **Многофакторная уязвимость (MULT)**. Уязвимость, появившаяся в результате наличия нескольких недостатков различных типов.
  - **Не задан (OTH)**.

- **Краткое описание**. Описание уязвимости.
- **Федеральный округ**. Федеральный округ, на территории которого обнаружена уязвимость.
- **Субъект федерации**. Субъект Российской Федерации, на территории которого обнаружена уязвимость.
- **Населенный пункт**. Название населенного пункта, в котором обнаружена уязвимость.
- **Прочая информация**. Дополнительная информация.

Вкладка **Программное обеспечение** в карточке уязвимости содержит следующие параметры уязвимости:

- **Наименование ПО**. Название ПО, в котором обнаружена уязвимость.
- **Версия ПО**. Версия ПО, в котором обнаружена уязвимость.
- **Служба (порт), которую используют для функционирования программного обеспечения**. Название службы (системной или сетевой), номер сетевого порта и название сетевого протокола, которые использует в работе ПО с обнаруженной уязвимостью.
- **Тип недостатка**. Предполагаемая причина уязвимости.
- **Место возникновения или появления уязвимости**. Класс программного обеспечения или технического оборудования, в котором обнаружена уязвимость.
- **Операционная система и иное окружение уязвимого ПО**. Информация об операционной системе или другая информация об окружении ПО с обнаруженной уязвимостью.

Вкладка **Программное обеспечение** в карточке уязвимости содержит следующие параметры уязвимости:

- **Описание**. Информация о том, как была обнаружена уязвимость.
- **Вложение**. Файл с дополнительной информацией об обнаружении уязвимости.

Вкладка **Меры по устранению** в карточке уязвимости содержит параметр уязвимости **Возможные меры по устранению уязвимости** — описание возможных мер для устранения уязвимости.

5.18. Страница Поиск

На странице **Поиск** вы можете осуществлять полнотекстовый поиск. PT Incident Processing Center выполняет поиск по инцидентам, запросам, задачам, информационным карточкам, бюллетеням, угрозам, уязвимостям и участникам. Найденная информация отображается в рабочей области страницы.

6. Экспорт данных

В PT Incident Processing Center есть возможность выгрузить в файл данные на страницах **Запросы**, **Инциденты**, **Операции без согласия**, **Задачи**, **Информационные карточки**, **Бюллетени**, **Новости**, **Угрозы**, **Уязвимости**, **Участники** и **Кампании**. Вы можете экспортировать выбранные строки в файл формата CSV или выпустить отчет по всем данным. Если данные предварительно были отфильтрованы, в отчет будут выгружены данные, удовлетворяющие выбранным фильтрам. Вы можете выгрузить не более 10 000 строк.

Для операций без согласия дополнительно возможна выгрузка данных в формат JSON (не более 1000 строк).

► Чтобы выпустить отчет:

1. На странице с нужными данными (например, на странице **Инциденты**), в главном меню нажмите кнопку **Экспорт**.

   Откроется окно **Экспорт**.

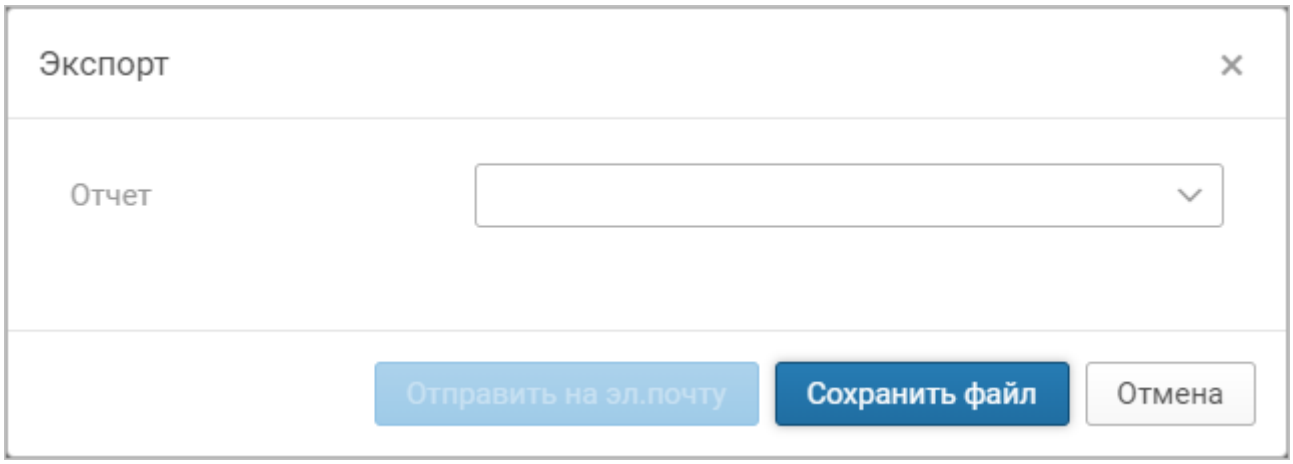

Рисунок 7. Окно **Экспорт отчета**

2. В раскрывающемся списке **Отчет** выберите вид отчета.
3. Выберите формат отчета.
4. В раскрывающемся списке **Период** выберите период, за который вы хотите сформировать отчет.
5. Нажмите кнопку **Сохранить в файл**.

Отчет выпущен.

Также вы можете отправить отчет на почту с помощью кнопки **Отправить на эл. почту**.

7. Электронные формы

Электронная форма — это файл формата JSON, формально описывающий атрибуты какого-либо объекта. Например, электронная форма инцидента описывает случившийся у участника инцидент и нужна для максимально точной и формализованной передачи этой информации в PT Incident Processing Center.

В системе существуют следующие типы электронных форм: электронная форма участника, инцидента, угрозы, уязвимости, публикации, запроса на анализ вредоносного ПО, запроса на блокировку корреспондентского счета, отчета о блокировке корреспондентского счета, запроса по операции без согласия, уведомления по операции без согласия, отчета о приостановлении операции без согласия. Администратор системы может создавать новые типы электронных форм с помощью конфигурационных файлов.

Создать электронную форму в системе вы можете заполнив электронную форму при регистрации запроса в интерфейсе "Личного кабинета оператора". Кроме того, вы можете вложить заполненную электронную форму как JSON-файл, используя тип вложения **Электронная форма из JSON-файла** в "Личном кабинете оператора". Описание JSON-структуры приводится в разделе "Схемы электронных форм" в Справочном руководстве по REST API.

Система автоматически создает и обновляет следующие объекты:

— инциденты — если электронную форму инцидента отправил участник;

— операции без согласия — если инцидент, в рамках которого была зафиксирована операция без согласия, был успешно создан.

Администраторы системы могут настраивать критерии автоматического создания и обновления инцидентов и операций без согласия с помощью конфигурационных файлов. В остальных случаях (если отправлен другой тип электронной формы или если электронная форма инцидента была создана в "Личном кабинете оператора" без указания участника), требуется вручную создать или обновить объект (см. раздел 8.2).

8. Работа с запросами

PT Incident Processing Center обеспечивает обмен информацией между центром и участниками через сообщения. При поступлении первого сообщения от участника через "Личный кабинет участника" система формирует запрос. Если первое сообщение от участника приходит по электронной почте, система валидирует электронный адрес отправителя, формирует запрос и отправляет участнику по электронной почте сообщение о регистрации запроса. При отправке сообщений участникам по электронной почте PT Incident Processing Center использует электронную подпись. Все последующие сообщения, связанные с исходным, автоматически попадают в тот же запрос.

Все поступившие в систему запросы от участников отображаются на странице **Запросы**. Работа с запросом ведется в карточке запроса и включает в себя следующие этапы:

1. Назначение ответственного за обработку запроса.
2. Добавление в систему информации из вложенной электронной формы.
3. Составление рекомендаций по решению запроса и предоставление их участнику.
4. Закрытие запроса.

Статус запроса отображает, на каком этапе работы находится запрос в текущий момент. При переходе от одного этапа к следующему необходимо изменять статус.

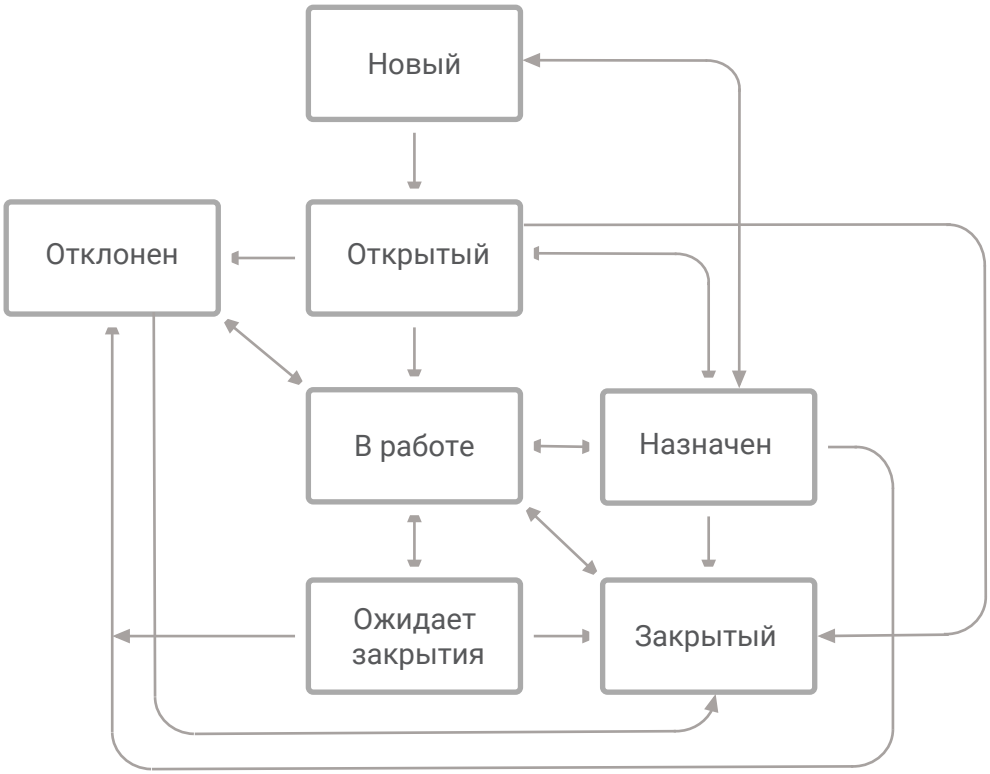

Рисунок 8. Статусы запроса

Система подсвечивает запросы, в рамках которых появились изменения или новые сообщения.

Вы можете создавать задачи в процессе обработки запроса и назначать ответственных за их выполнение. Полезную информацию можно сохранять в информационные карточки. Созданные карточки используются для расследования инцидентов и угроз. Кроме того, можно связывать запрос с другими объектами и оставлять комментарии к запросу.

Сообщения в запросе могут содержать вложения разных типов: электронную форму инцидента, угрозы, уязвимости, участника, публикации или файл, например, скриншот.

Вы можете скачивать файлы, вложенные в запрос, или электронные формы. PT MS сканирует файлы на наличие угроз. При попытке скачать потенциально опасный файл система запрашивает подтверждение.

Участники могут также прикладывать к запросу журналы веб-серверов. Анализ журналов с помощью продукта Web Application Firewall позволит обнаружить уязвимости и дать участникам рекомендации для устранения причин инцидентов. Подробную информацию см. в документации Web Application Firewall.

В этом разделе

См. также

Типовые действия с объектами системы (см. раздел 21)

8.1. Назначение ответственного за обработку запроса вручную

Примечание. При назначении объекта в системе на пользователя для выбора доступны только пользователи, учетные записи которых в системе активны. Нельзя назначить объект на пользователя, учетная запись которого заблокирована.

► Чтобы назначить ответственного за обработку запроса вручную:

1. В главном меню выберите раздел **Запросы**.

   Откроется страница с таблицей запросов.

2. Выберите запрос, для которого вы хотите назначить ответственного.
3. В панели инструментов нажмите кнопку **Назначить** и в раскрывшемся меню выберите ответственного:

   - Если требуется назначить запрос на себя, выберите **Взять себе**.
   - Если требуется отменить ответственного, выберите **Не назначено**.

   Информация о назначении ответственного будет отображена в таблице запросов.

Ответственный за обработку запроса назначен.

8.2. Создание карточки объекта на основе электронной формы объекта

► Чтобы создать карточку объекта на основе электронной формы объекта, добавленной к запросу:

1. В главном меню выберите раздел **Запросы**.

   Откроется страница с таблицей запросов.

2. По ссылке с идентификатором запроса перейдите в карточку запроса.
3. Откройте вложенную электронную форму объекта.

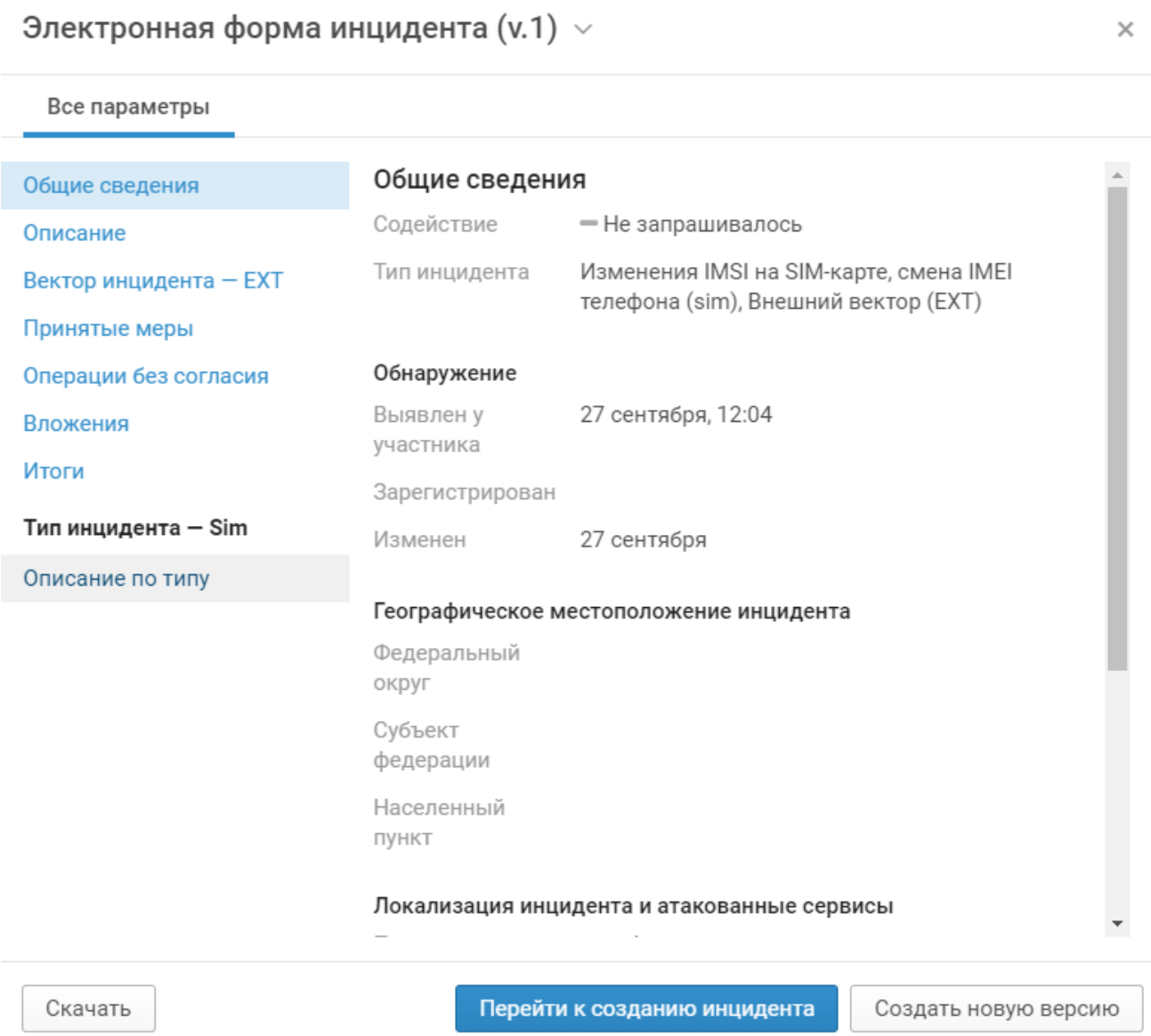

Рисунок 9. Просмотр электронной формы инцидента

4. Нажмите кнопку **Перейти к созданию <Объект>**.

   Откроется карточка объекта.

5. Проверьте информацию на всех вкладках и нажмите кнопку **Создать**.

Карточка объекта создана.

8.3. Создание запроса

Вы можете создавать запросы любого типа, указав в качестве получателей одного или нескольких участников или группы рассылки. Запросы, в которых указано несколько получателей, называются массовыми запросами.

► Чтобы создать запрос:

1. В главном меню выберите раздел **Запросы**.

   Откроется страница с таблицей запросов.

2. Нажмите кнопку **Направить запрос**.

   Откроется страница **Новый запрос**.

3. Добавьте тему запроса.

4. В поле **Участники** выберите одного или нескольких участников, зарегистрированных в системе.

   Вы можете выбрать группы рассылки, которым адресован запрос, в поле **Группы рассылки**.

   Примечание. Вы можете выбирать статические и динамические группы рассылки (см. раздел 19.3), в которые участники попадают автоматически в соответствии с правилами группы.

5. В раскрывающемся списке выберите тип запроса.

6. В центральной панели введите текст запроса.

   Вы можете использовать шаблоны и добавлять к запросу вложения. Вы можете прикладывать к запросу JSON-файлы с электронными формами. Для этого необходимо использовать вложение с типом **Электронная форма из JSON-файла**.

7. Нажмите кнопку **Зарегистрировать запрос**.

Запрос зарегистрирован.

После сохранения запроса выполняется переход на страницу случайного запроса из списка созданных. Система выполняет следующие действия:

— Если получателем выбран один или несколько участников — формирует и направляет запрос каждому участнику.

— Если выбрана статическая группа рассылок — формирует письмо с запросом и отправляет его на каждый адрес из группы. Каждое письмо содержит только того получателя, которому оно отправлено.

— Если выбрана динамическая группа — формирует и направляет запрос для каждого активного участника, соответствующего правилу включения в группу.

8.4. Создание запросов из переписки по инциденту

Вы можете создавать запросы по инциденту к участникам непосредственно из карточки инцидента. В рамках каждого созданного запроса можно вести переписку с участником.

Созданные запросы и переписка по ним отображаются в карточке инцидента на вкладке **Запросы**.

► Чтобы создать запрос по инциденту и просмотреть переписку по ранее созданным запросам:

1. В главном меню выберите раздел **Инциденты**.

   Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.

3. Выберите вкладку **Запросы**.

   В левой части вкладки **Запросы** отображаются запросы, ранее созданные по инциденту. Запросы можно выбирать. В правой части вкладки содержится переписка с участником, которую вели в рамках выбранного запроса. Если по инциденту еще не создавали запросы, на вкладке **Запросы** содержится только кнопка **Добавить запрос**.

4. Нажмите кнопку **Добавить запрос**.

   Откроется страница создания запроса. На ней можно выбрать тему запроса, указать участника, написать сообщение для участника и прикрепить вложение. Вы можете выбрать нескольких участников. Черновики запросов сохраняются автоматически. Можно вернуться к неотправленному запросу, внести в него изменения и отправить позднее.

5. Нажмите кнопку **Зарегистрировать запрос**.

Сохраненный запрос отобразится на вкладке **Запросы**. Между запросом и инцидентом будет создана связь типа "Ссылка".

В созданном запросе можно начать переписку с участником. Переписку с участниками можно просматривать и продолжать и в запросах, созданных для инцидента ранее. Продолжать переписку нельзя только в запросах в статусе **Закрыт**.

8.5. Регистрация диспутного запроса

Диспутный запрос применяется в случаях, когда необходимо оспорить включение реквизитов клиента в фиды, или наоборот — потребовать добавить в фиды реквизиты клиента.

► Чтобы зарегистрировать диспутный запрос:

1. В главном меню нажмите кнопку **Новый запрос** и в раскрывшемся меню выберите **Диспутный запрос**.

   Откроется страница **Новый запрос**.

2. В поле **Тема обращения** введите тему запроса.

3. В раскрывающемся списке **Способ получения** выберите способ получения запроса.

4. Введите ответ.

5. Если требуется, вложите файлы с дополнительной информацией.

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

6. Нажмите кнопку **Зарегистрировать запрос**.

Запрос зарегистрирован и отображается в списке запросов.

Для быстрого просмотра всех диспутных запросов на странице **Запросы** доступен фильтр **Диспутные запросы**. Вы можете изменять статус и приоритет диспутного запроса, а также назначать его на оператора.

8.6. Обновление карточки объекта на основе электронной формы объекта

► Чтобы обновить карточку объекта на основе электронной формы объекта, добавленной в запрос:

1. В главном меню выберите раздел **Запросы**.

   Откроется страница с таблицей запросов.

2. По ссылке с идентификатором запроса перейдите в карточку запроса.
3. Откройте вложенную электронную форму объекта.

   На вкладке **Измененные параметры** отобразятся изменения, которые внес участник. О характере изменения говорит цветовое выделение слева от названий параметров объекта:

- Зеленый цвет означает, что в новой версии электронной формы добавлено значение параметра.
- Красный цвет означает, что в новой версии электронной формы удалено значение параметра.
- Оранжевый цвет означает, что в новой версии электронной формы изменено значение параметра.

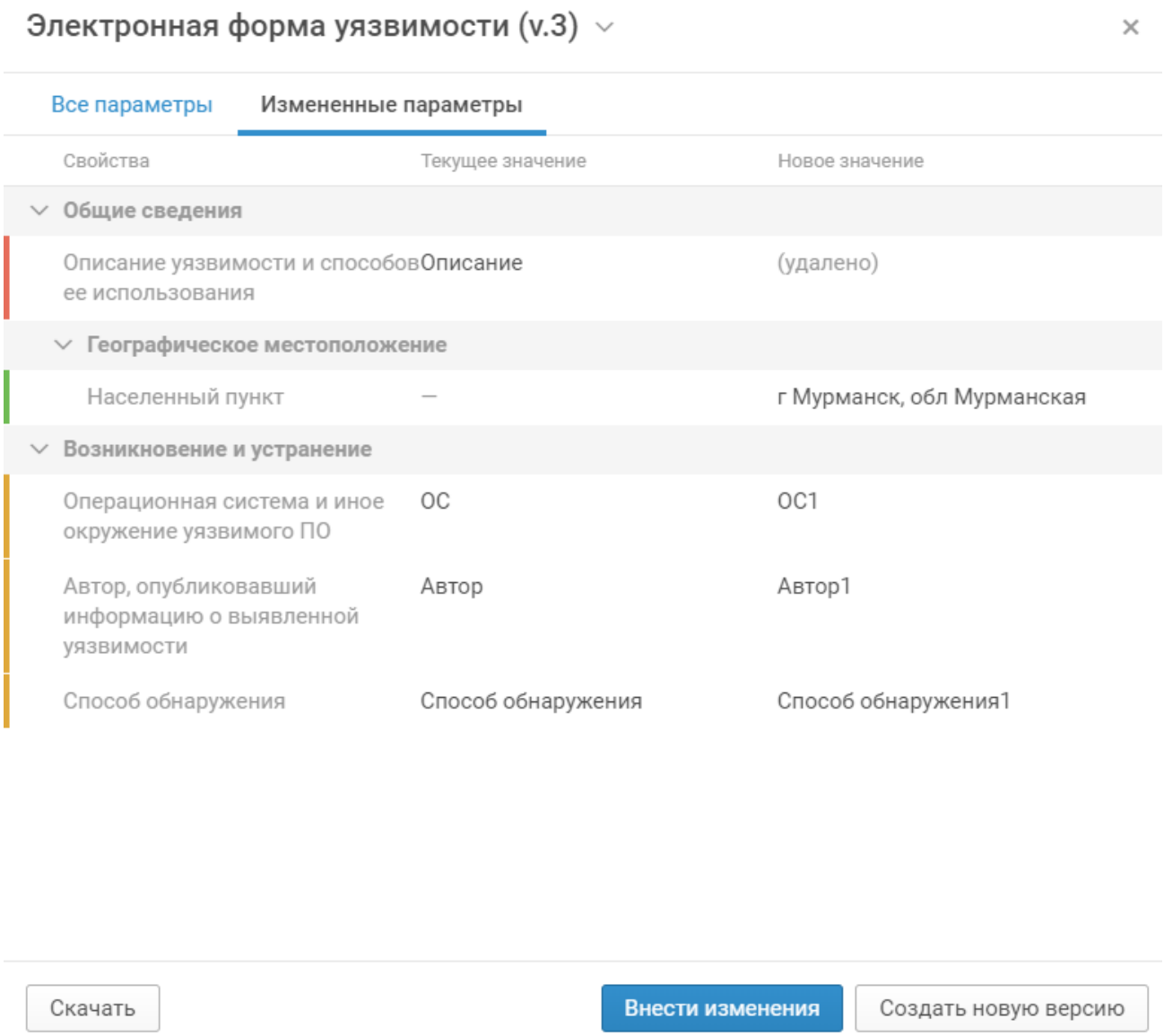

Рисунок 10. Измененные параметры в электронной форме уязвимости

4. Нажмите кнопку **Внести изменения**.

   Откроется обновленная карточка объекта в режиме изменения.

Внимание! Если вы обновляете карточку участника и добавляете в нее новое ответственное лицо, отправьте ответственному лицу его учетные данные.

8.7. Изменение электронной формы объекта с уведомлением участника

Если электронная форма объекта содержит неполную информацию, вы можете дополнить электронную форму и отправить ее копию участнику для подтверждения информации.

► Чтобы изменить параметры электронной формы объекта и отправить ее участнику:

1. В главном меню выберите раздел **Запросы**.

   Откроется страница с таблицей запросов.

2. По ссылке с идентификатором запроса перейдите в карточку запроса.
3. Откройте вложенную электронную форму объекта.
4. Нажмите кнопку **Редактировать**.
5. Измените необходимую информацию.
6. Нажмите кнопку **Добавить к запросу**.

   Измененная электронная форма объекта будет вложена в сообщение.

7. В панели **Переписка** введите пояснение к изменениям и нажмите кнопку **Отправить**.

Измененная электронная форма отправлена участнику.

После подтверждения информации от участника вам нужно обновить карточку объекта в системе (см. раздел 8.6).

8.8. Изменение статуса запроса

► Чтобы изменить статус запроса:

1. В главном меню выберите раздел **Запросы**.

   Откроется страница с таблицей запросов.

2. Выберите запрос, статус которого вы хотите изменить.

   Примечание. Вы можете выбрать несколько запросов.

3. В панели инструментов нажмите кнопку **Изменить статус** и в раскрывшемся меню выберите статус.

Статус запроса изменен.

8.9. Обработка запроса о блокировке корреспондентского счета

Корреспондентский счет — счет кредитной организации в Банке России, предназначенный для расчетов между кредитными организациями.

Если с корреспондентского счета организации было совершено или может быть совершено хищение денежных средств, участник может зарегистрировать в PT Incident Processing Center запрос о блокировке корреспондентского счета организации.

► Чтобы обработать запрос о блокировке корреспондентского счета:

1. В главном меню выберите раздел **Запросы**.

Откроется страница с таблицей запросов.

2. По ссылке с идентификатором запроса о блокировке корреспондентского счета откройте карточку запроса.
3. Откройте вложенную электронную форму блокировки корреспондентского счета.
4. Проверьте данные в заявке.
5. Проведите комплекс мероприятий по блокировке корреспондентского счета в соответствии с установленным в организации регламентом.
6. Нажмите кнопку **Создать отчет о блокировке**.

   Откроется окно **Электронная форма отчета о блокировке**.
7. В поле с наименованием заявки нажмите .

   Откроется окно **Редактирование заявки**.
8. В поле **Статус заявки** выберите статус заявки.
9. Нажмите кнопку **Сохранить**.
10. Нажмите кнопку **Добавить к запросу**.
11. Добавьте сообщение и нажмите кнопку **Отправить**.

    Отчет о блокировке корреспондентского счета будет отправлен участнику.

8.10. Проверка потенциально вредоносного файла

В PT Incident Processing Center предусмотрена возможность проверять файлы на наличие ВПО.

► Чтобы проверить файл на наличие ВПО:

1. В главном меню нажмите кнопку **Новый запрос** и выберите **Запрос на анализ ВПО**.

   Откроется окно **Запрос на анализ ВПО**.
2. В область загрузки перетащите файл для проверки или выберите его из списка.
3. Нажмите кнопку **Добавить к запросу**.
4. В поле **Тема сообщения** введите тему.
5. В панели переписки введите сообщение.
6. Нажмите кнопку **Зарегистрировать запрос**.

   Система выполнит проверку файла и сформирует отчет.

8.11. Работа с запросами на разделегирование домена

Примечание. В разделе приведены описания параметров для Российской Федерации.

Запрос на разделегирование домена применяется в случаях, когда необходимо заблокировать вредоносный домен.

Примечание. Перед началом работы с запросами на разделегирование домена в системе необходимо зарегистрировать участника "Роскомнадзор".

В общем случае работа с запросами на разделегирование домена состоит из следующих шагов:

1. Участник информационного обмена в личном кабинете регистрирует инцидент с типом, для которого доступны параметры **Домен** и (или) **URL** (например **Размещение вредоносного ресурса в сети "Интернет"** или **Использование фишинговых ресурсов**), и указывает эти параметры.
2. Оператор в личном кабинете на основе инцидента создает запрос на разделегирование домена и отправляет запрос регистратору домена.
3. Регистратор домена:
   - На своей стороне блокирует вредоносный ресурс и отправляет сообщение о блокировке. Сообщение отображается в карточке запроса.
   - Не отвечает на запрос о разделегировании домена или отказывает в его блокировке.
4. Если регистратор домена заблокировал вредоносный ресурс, оператор отправляет сообщение о блокировке участнику, приславшему запрос с инцидентом.
5. Если регистратор домена не заблокировал вредоносный ресурс или не ответил на запрос, но оператор считает, что ресурс должен быть заблокирован, он отправляет запрос в Роскомнадзор на внесение домена в реестр запрещенных на территории Российской Федерации.
6. Роскомнадзор блокирует домен, оператор отправляет участнику, приславшему запрос с инцидентом, сообщение о внесении домена в реестр Роскомнадзора.

В этом разделе

8.11.1. Регистрация запроса на разделегирование домена

► Чтобы создать запрос на разделегирование домена:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.
2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. На вкладке **Описание по типу** нажмите кнопку с доменным именем или URL.

В правой части страницы отобразится панель с дополнительной информацией о домене. Дополнительная информация содержит WHOIS- и DNS-записи, полученные от Cybsi.

4. Нажмите кнопку **Запросить разделегирование**.

   Откроется страница **Новый запрос**. В панели переписки отобразится шаблон сообщения о разделегировании домена для отправки регистратору доменного имени.

5. Если требуется, в раскрывающемся списке **Участник** измените регистратора домена.
6. Если требуется, в поле **Тема обращения** измените текст сообщения.
7. Если требуется, вложите файлы с дополнительной информацией.

   Примечание. Вы не можете добавлять в запрос электронные формы, а также исполняемые файлы (в частности, файлы с расширениями .exe, .app, .vb).

8. Нажмите кнопку **Зарегистрировать запрос**.

Запрос создан и отображается в списке запросов.

8.11.2. Регистрация запроса на внесение домена в реестр Роскомнадзора

Если регистратор домена не отвечает на запрос о разделегировании домена или отказывает в его блокировке, вы можете отправить запрос в Роскомнадзор на внесение домена в реестр запрещенных.

► Чтобы отправить запрос в Роскомнадзор:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. На вкладке **Описание по типу** нажмите кнопку с доменным именем или URL.

   В правой части страницы отобразится панель с дополнительной информацией о домене. Дополнительная информация содержит WHOIS- и DNS-записи, полученные от Cybsi.

4. Нажмите кнопку **Запросить внесение в реестр РКН**.

   Откроется страница **Новый запрос**. В панели переписки отобразится шаблон сообщения о внесении домена в реестр запрещенных.

5. Если требуется, в поле **Тема обращения** измените текст сообщения.
6. Если требуется, вложите файлы с дополнительной информацией.

Примечание. Вы не можете добавлять в запрос электронные формы, а также исполняемые файлы (в частности, файлы с расширениями .exe, .app, .vb).

7. Нажмите кнопку **Зарегистрировать запрос**.

Запрос отправлен в Роскомнадзор. После отправки PT Incident Processing Center автоматически закрывает этот запрос.

8.11.3. Проверка доступности веб-ресурсов

Вы можете периодически проверять доступность веб-ресурсов (например, вредоносных или мошеннических), для которых вы создали запросы на разделегирование домена.

► Чтобы проверить доступность веб-ресурса:

1. В главном меню выберите раздел **Инциденты**.

   Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. В карточке инцидента нажмите доменное имя или URL веб-ресурса.

   Откроется окно **<Имя ресурса>**.

4. Выберите вкладку **availability**.
5. На вкладке отображается доступность веб-ресурса по HTTP, HTTPS, ICMP: доступен (**yes**) или недоступен (**no**).

   Если необходимо, вы можете вручную обновить информацию о доступности веб-ресурса по ссылке **Обновить**, или просмотреть историю обновлений по ссылке **История**.

8.11.4. Скачивание архива с сайтом

Система позволяет скачивать и сохранять в виде архива веб-сайт целиком. Эта функция может быть полезна, например, при расследовании инцидентов, связанных с вредоносным веб-сайтом.

Максимальный размер скачиваемого архива с веб-сайтом — 1 ГБ. При превышении этого размера скачивание файлов сайта прекращается. Уже скачанные файлы сохраняются в архиве.

► Чтобы скачать веб-сайт:

1. В главном меню выберите раздел **Инциденты**.

   Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. В карточке инцидента нажмите URL или доменное имя веб-сайта.

   Откроется окно **<Имя веб-сайта>**.

4. Выберите вкладку **downloader**.
5. Нажмите кнопку **Обновить**.

   На вкладке отобразится ссылка для скачивания архива с веб-сайтом.
6. Скопируйте ссылку и вставьте ее в адресную строку в новой вкладке браузера.

   Начнется скачивание архива с веб-сайтом на жесткий диск вашего компьютера.

Сайт скачивается целиком, без исполнения скриптов, со структурой папок до третьего уровня вложенности включительно.

8.12. Приоритетная сортировка запросов

На странице **Запросы** в предустановленном фильтре по умолчанию **Активные** используется приоритетная сортировка запросов. Когда выбран фильтр **Активные**, запросы на странице отображаются в следующем порядке:

- запросы с непрочитанными сообщениями;
- запросы с типом "Блокировка корр.счета";
- запросы с типом "Инцидент", у которых в первой ЭФ инцидента поле **Операционные расходы** заполнено;
- запросы с типом "Инцидент", у которых в первой ЭФ инцидента в поле **Требуется помощь** PT Incident Processing Center выбрано значение **Требуется**;
- остальные запросы.

Приоритетная сортировка запросов имеет ряд ограничений.

Для запросов с типом "Инцидент" сортировка выполняется по данным ЭФ инцидента, полученной в первом сообщении в запросе. Если к другим сообщениям в этом же запросе приложены версии этой ЭФ, то сортировка выполняется по данным наибольшей версии. Например, запрос, в котором к первому сообщению приложена ЭФ инцидента с заполненным полем **Операционные расходы**, отобразится в верхней части списка запросов.

Сортировка по ЭФ инцидента не выполняется, если к первому сообщению в запросе приложены:

- несколько ЭФ инцидента;
- несколько ЭФ разных типов в том числе ЭФ инцидента (например, ЭФ инцидента и ЭФ угрозы);
- ЭФ инцидента и файлы, не являющиеся ЭФ.

Например, если к первому сообщению в запросе приложена ЭФ инцидента с заполненным полем **Операционные расходы** и текстовый документ, запрос не отобразится в верхней части списка.

Сортировка не выполняется по данным ЭФ, приложенных к сообщениям в запросе, отличным от первого, или по новым версиям этих ЭФ. Например, получен запрос, в первом сообщении которого нет ЭФ. В этот запрос участник или оператор добавил сообщение с ЭФ инцидента с заполненным полем **Операционные расходы**. Запрос не отобразится в верхней части списка.

При сортировке не учитываются новые версии ЭФ, если они получены в сообщениях с несколькими вложениями. Например, получен запрос, в котором к первому сообщению приложена ЭФ инцидента с заполненным полем **Операционные расходы**. Запрос отобразится в верхней части списка. Если оператор или участник добавит в этот запрос сообщение с новой версией ЭФ инцидента с незаполненным полем **Операционные расходы** и любым другим вложением, запрос останется в верхней части списка.

9. Электронная подпись

В PT Incident Processing Center реализована возможность подписания электронных форм электронной подписью. Электронная подпись служит для подтверждения подлинности электронного документа. Участники подписывают электронной подписью электронные формы инцидента, уведомления об операции без согласия.

На странице просмотра запроса на электронных формах, приложенных к запросу, отображается результат проверки электронной подписи:

— подпись проверяется;

— подпись действительна;

— подпись недействительна.

Отсутствие индикатора проверки подписи означает, что электронная форма не подписана электронной подписью.

Вы можете запросить повторную проверку подлинности электронной подписи с помощью кнопки .

Проверка подлинности происходит автоматически в процессе регистрации запроса с электронной формой. Пользователь с правами администратора может настраивать сценарии обработки электронных форм в зависимости от статуса проверки подлинности электронной подписи.

10. Работа с задачами

С помощью задач можно назначать операторам системы работу с запросами и инцидентами, а также другие работы. Оператор, которому назначена задача, является ответственным за ее выполнение. Ответственный может просматривать описание задачи и оставлять комментарии в карточке задачи.

> **Примечание.** При назначении объекта в системе на пользователя для выбора доступны только пользователи, учетные записи которых в системе активны. Нельзя назначить объект на пользователя, учетная запись которого заблокирована.

Существуют следующие статусы задачи:

— **Новая** — задача создана и ожидает назначения ответственного за ее выполнение;

— **В работе** — задача назначена на ответственного и по ней идет работа;

— **Завершена** — задача выполнена;

— **Удалена** — задача создана по ошибке или неактуальна.

Новую задачу без ответственного нельзя взять в работу (присвоить статус **В работе**). Такую задачу можно только удалить (присвоить статус **Удалена**).

Задачи на работу с инцидентами и запросами нужно создавать в их карточках. Задачи на другие работы, не привязанные к инциденту или запросу, нужно создавать на странице **Задачи**.

Страница **Задачи** содержит все задачи, созданные в системе. В центральной части страницы отображается список задач в соответствии с выбранным фильтром. Вы можете фильтровать задачи по ответственному, приоритету, типу и статусу, дате создания и обновления.

Задачи, в которых больше 90 календарных дней не было изменений (не изменялась информация в карточке задачи, статус, ответственный, итог) автоматически переносятся в архив. Срок переноса задачи в архив (90 дней) установлен по умолчанию и может быть изменен при конфигурировании системы. Изменение срока в интерфейсе недоступно.

Архивные задачи не отображаются в общем списке задач. При попытке перейти к архивной задаче (например, из связанного с ней объекта) отображается страница **Задача в архиве** с номером задачи и датой перенесения задачи в архив. Никакие действия с архивной задачей невозможны. Вы можете удалять связи других объектов с задачей, помещенной в архив.

В этом разделе

Закрытие задачи (см. раздел 10.6)

Назначение задачи оператору (см. раздел 10.7)

См. также

Типовые действия с объектами системы (см. раздел 21)

10.1. Создание задачи на запрос

► Чтобы создать задачу на запрос:

1. В главном меню выберите раздел **Запросы**.

   Откроется страница, содержащая список запросов.

2. По ссылке с идентификатором запроса откройте карточку запроса.

3. В панели справа нажмите кнопку **Добавить** и в раскрывшемся меню выберите **Задачу**.

   Откроется страница **Создание задачи**.

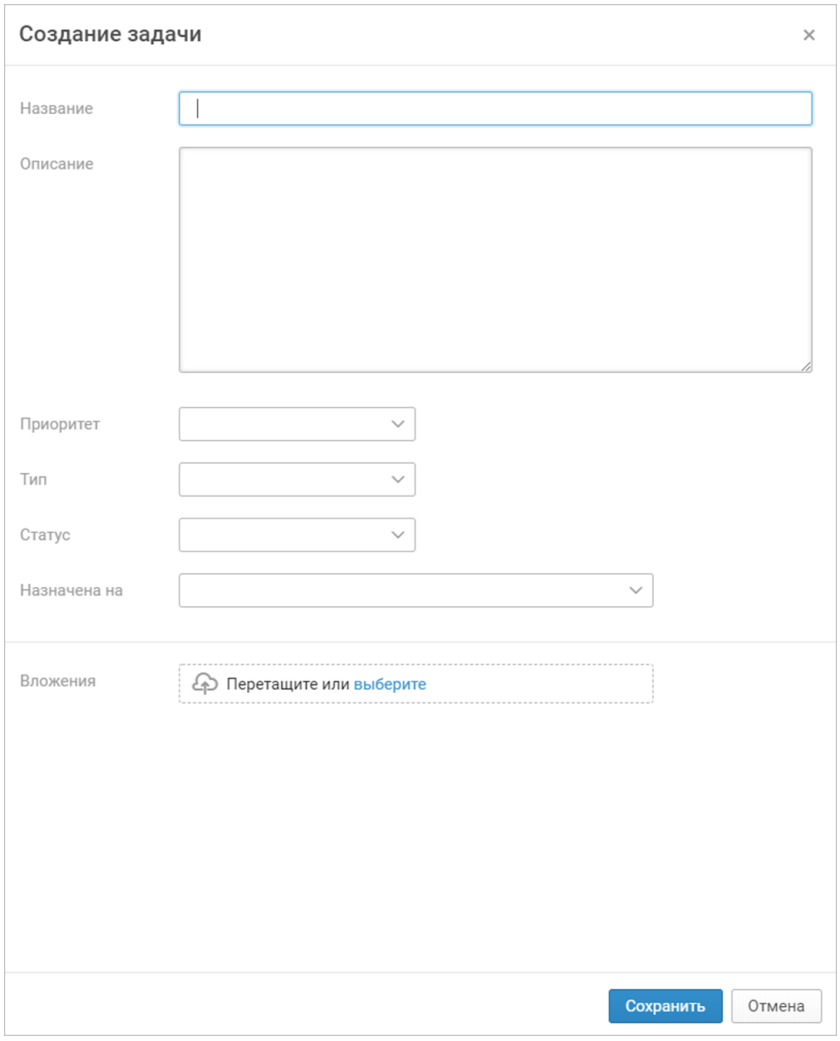

Рисунок 11. Создание задачи

4. В поле **Название** введите название, описывающее задачу.
5. В поле **Описание** введите, что нужно выполнить в рамках задачи.
6. В раскрывающемся списке **Приоритет** выберите приоритет задачи.

   Примечание. Приоритет задачи должен соответствовать запросу в рамках которого создается задача.
7. В поле **Тип** выберите тип задачи:
   - **Расследование** — выявление причин инцидента и способов предотвратить его повторное возникновение;
   - **Сбор доказательств** — выявление объектов атаки, сбор и хранение доказательств атаки;
   - **Восстановление** — восстановление работоспособности IT-инфраструктуры сети.
8. В поле **Дедлайн** укажите дату, к которой должна быть выполнена задача.

9. В поле **Ответственный** укажите ответственного за выполнение задачи.
10. Нажмите кнопку **Сохранить**.

Задача на запрос создана.

10.2. Создание задачи на инцидент

► Чтобы создать задачу на инцидент:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.
2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. В панели **Инцидент связан с** нажмите кнопку **Добавить** и в раскрывшемся меню выберите **Задачу**.

   Откроется страница **Создание задачи**.

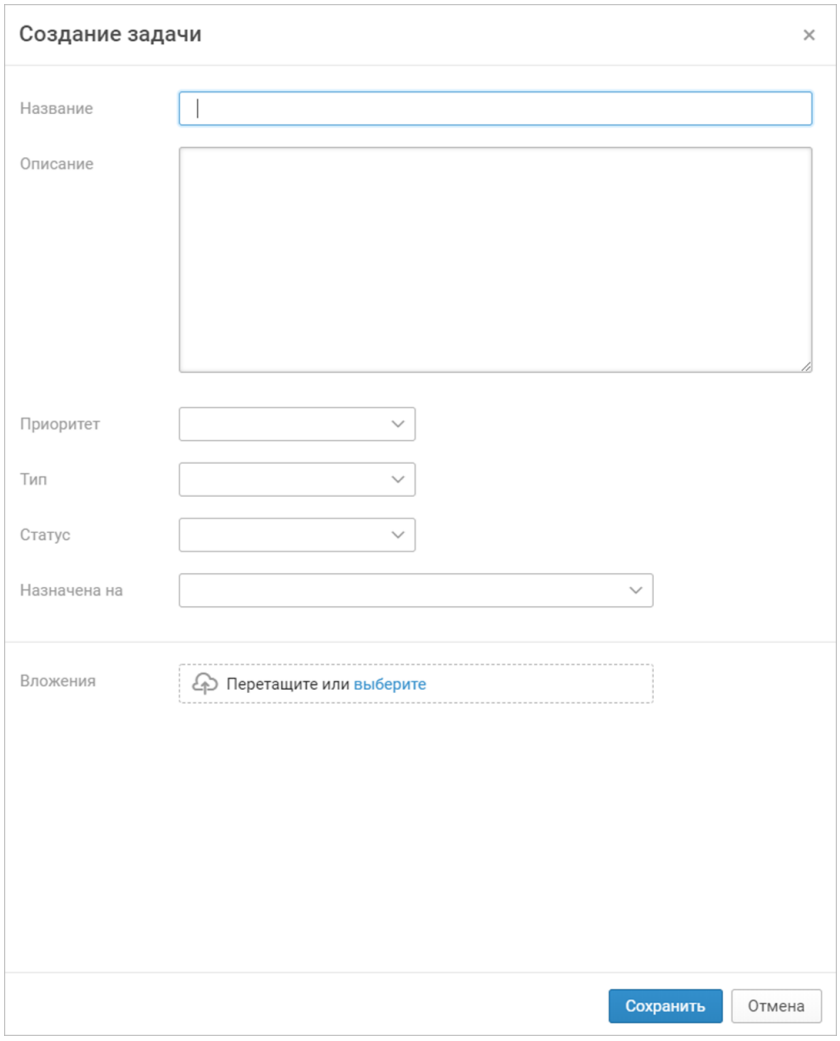

Рисунок 12. Создание задачи

4. В верхнем поле введите название задачи.
5. В следующем поле введите описание задачи.
6. В поле **Тип** укажите тип задачи:
   - **Расследование** — выявление причин инцидента и способов предотвратить его повторное возникновение;
   - **Сбор доказательств** — выявление объектов атаки, сбор и хранение доказательств атаки;
   - **Восстановление** — восстановление работоспособности IT-инфраструктуры сети.
7. В поле **Дедлайн** укажите дату, к которой должна быть выполнена задача.
8. В поле **Ответственный** укажите ответственного за выполнение задачи.
9. Нажмите кнопку **Сохранить**.

Задача на инцидент создана.

10.3. Создание задачи без привязки к запросу или инциденту

Вы можете создавать задачи, не связанные с запросом или инцидентом.

► Чтобы создать задачу без привязки к запросу или инциденту:

1. В главном меню выберите раздел **Задачи**.

   Откроется страница со списком задач.

2. В панели инструментов нажмите кнопку **Добавить**.

   Откроется форма заполнения карточки задачи.

3. В поле **Название** введите название задачи.
4. В поле **Тип** укажите тип задачи:
   - **Расследование** — выявление причин инцидента и способов предотвратить его повторное возникновение;
   - **Сбор доказательств** — выявление объектов атаки, сбор и хранение доказательств атаки;
   - **Восстановление** — восстановление работоспособности IT-инфраструктуры сети.
5. В поле **Дедлайн** укажите срок выполнения задачи.
6. В поле **Ответственный** укажите исполнителя.
7. В поле **Описание** введите описание задачи.
8. Нажмите кнопку **Сохранить**.

Задача, не связанная с запросом или инцидентом, создана.

10.4. Изменение статуса задачи

► Чтобы изменить статус задачи:

1. В главном меню выберите раздел **Задачи**.

   Откроется страница со списком задач.

2. В панели инструментов нажмите кнопку **Изменить статус** и в раскрывшемся меню выберите статус.

   Если вы измените статус новой задачи, не назначив предварительно ответственного по кнопке **Назначить** в панели инструментов, задача будет автоматически назначена вам.

   Примечание. Чтобы перевести задачу в статус **Завершена** или **Удалена**, заполните поле **Итог задачи** в карточке задачи.

Статус задачи изменен.

10.5. Изменение сроков выполнения задачи

► Чтобы изменить сроки выполнения задачи:

1. В главном меню выберите раздел **Задачи**.

   Откроется страница со списком задач.

2. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется страница **<Задачи / Название задачи>**.

3. В блоке **Параметры** в поле **Дедлайн** укажите срок выполнения задачи.
4. Нажмите кнопку **Сохранить**.

Срок выполнения задачи изменен.

10.6. Закрытие задачи

► Чтобы закрыть задачу:

1. В главном меню выберите раздел **Задачи**.

   Откроется страница со списком задач.

2. Перейдите в карточку задачи по ссылке с идентификатором задачи.
3. В рабочей области нажмите кнопку **Редактировать итог**.

   Примечание. Изменить итог задачи может только оператор, ответственный за выполнение задачи.

4. В поле **Итог задачи** введите описание результата выполнения задачи.
5. Нажмите кнопку **Сохранить**.
6. Нажмите кнопку **Редактировать**.

   Откроется окно **Редактирование задачи**.

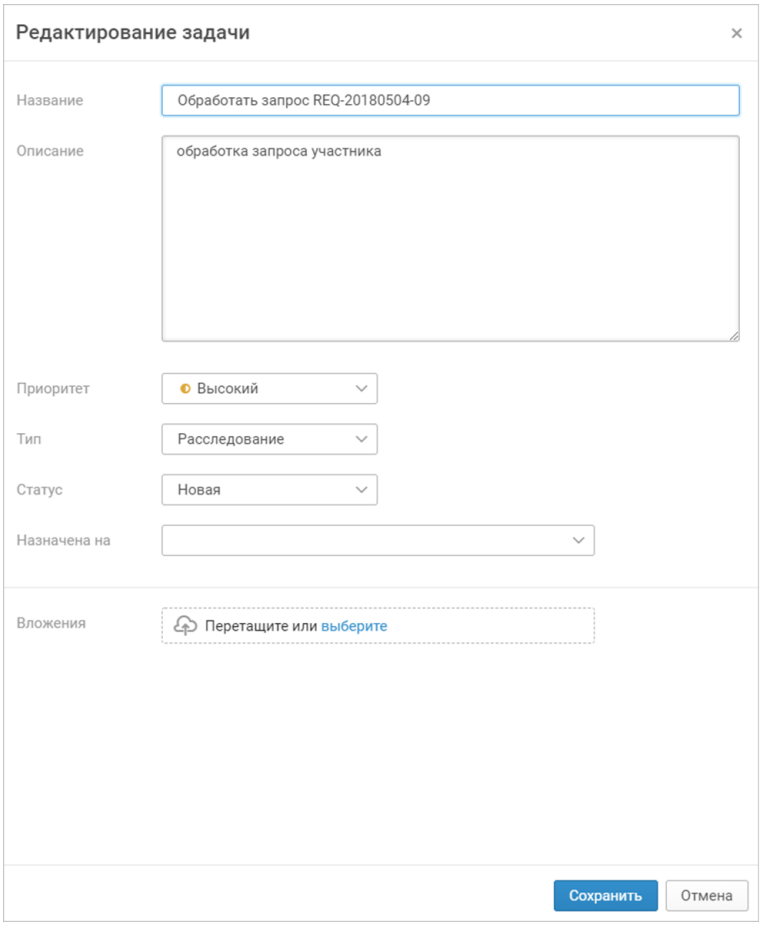

Рисунок 13. Изменение карточки задачи

7. В поле **Статус** выберите **Закрыта**.
8. Нажмите кнопку **Сохранить**.

Задача закрыта.

10.7. Назначение задачи оператору

► Чтобы назначить задачу оператору:

1. В главном меню выберите раздел **Задачи**.

   Откроется страница со списком задач.
2. Выберите задачу.
3. Нажмите **Назначить** в панели инструментов и в раскрывшемся меню выберите ответственного за назначаемую задачу.

Задача назначена оператору.

Примечание. При переводе задачи с одного оператора на другого руководителям операторов приходит уведомление на электронную почту о переназначении задачи.

11. Работа с инцидентами

Инцидент — одно или несколько нежелательных или неожиданных событий, которые могут нарушить информационную безопасность 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.

Все поступившие в систему инциденты отображаются на странице **Инциденты**. Работа с инцидентом ведется в карточке инцидента и включает в себя следующие этапы:

1. Назначение ответственного за расследование инцидента.
2. Расследование инцидента и составление рекомендаций по его устранению.
3. Закрытие инцидента.

   Примечание. При назначении объекта в системе на пользователя для выбора доступны только пользователи, учетные записи которых в системе активны. Нельзя назначить объект на пользователя, учетная запись которого заблокирована.

Статус инцидента отображает, на каком этапе работы находится инцидент в текущий момент. При переходе от одного этапа к следующему необходимо изменять статус.

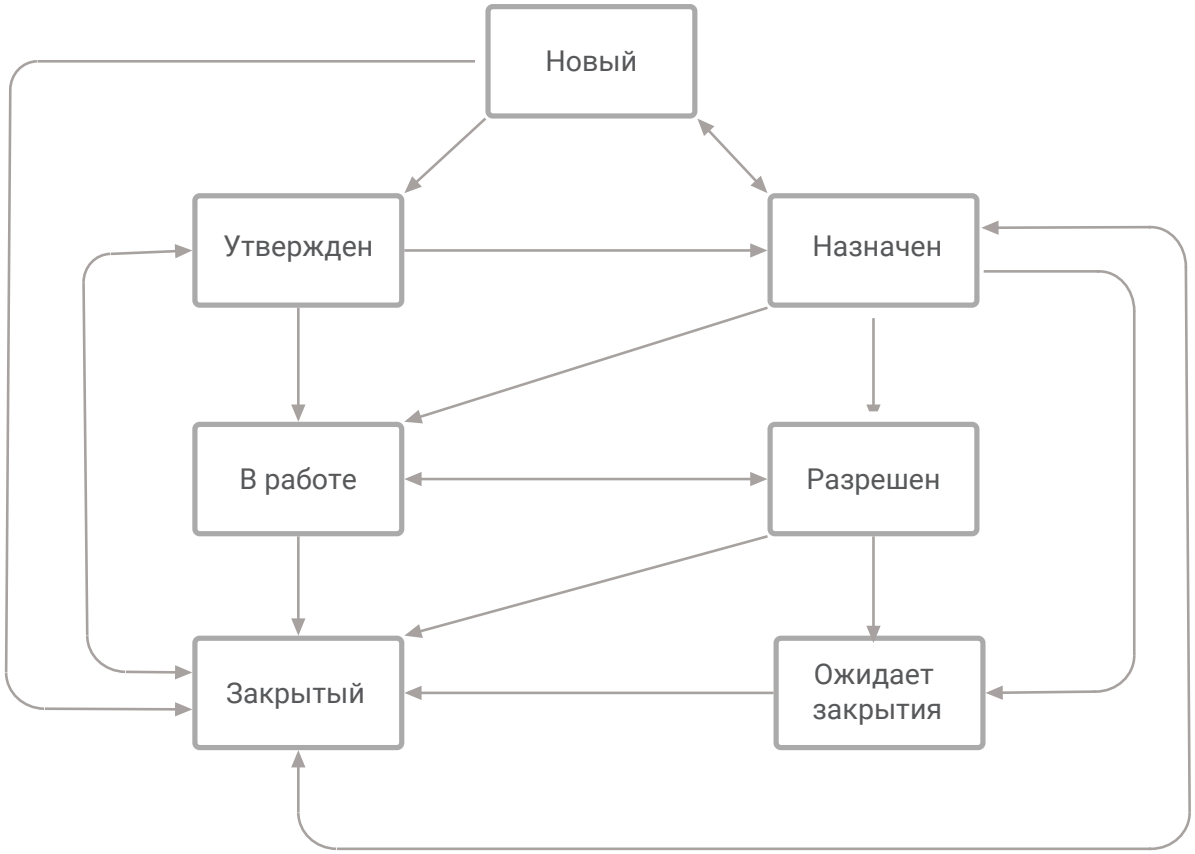

Рисунок 14. Статусы инцидента

Вы можете создавать задачи в процессе расследования инцидента и назначать ответственных за их выполнение.

При необходимости вы можете запросить содействия в расследовании у ГосСОПКА.

Кроме того, вы можете связывать инцидент с другими объектами и оставлять комментарии к инциденту.

Вы можете редактировать закрытые инциденты и задачи. Права на редактирование закрытых задач есть по умолчанию. Права на редактирование закрытых инцидентов предоставляет администратор системы.

В этом разделе

См. также

11.1. Добавление инцидента

► Чтобы добавить в PT Incident Processing Center новый инцидент:

На странице **Инциденты** нажмите кнопку **Добавить инцидент**.

Откроется окно **Создание инцидента**.

Набор вкладок и полей карточки инцидента зависит от типа инцидента: с вектором EXT или с вектором INT.

1. Заполните вкладку **Общие сведения**:

- В блоке параметров **Доступ к инциденту** выберите один из вариантов:
  Red — PT Incident Processing Center, ГосСОПКА и данный участник;
  Amber — PT Incident Processing Center, ГосСОПКА и все участники отрасли;
  Green — PT Incident Processing Center, ГосСОПКА и все участники;
  White — любые организации.
- В блоке параметров **Помощь** PT Incident Processing Center выберите, требуется ли помощь специалистов центра для расследования инцидента.
- В раскрывающемся списке **Участник** выберите участника, у которого произошел инцидент.
- В раскрывающемся списке **Федеральный округ** выберите федеральный округ, на территории которого произошел инцидент.

  Примечание. В случае выявления инцидента, связанного с трансграничным переводом денежных средств, место выявления инцидента не указывается. Поле обязательно для заполнения.
- В раскрывающемся списке **Субъект федерации** выберите субъект федерации, на территории которого произошел инцидент.

  Примечание. Поле обязательно для заполнения.
- В поле **Населенный пункт** введите город или иной населенный пункт, в котором произошел инцидент.

Примечание. Поле обязательно для заполнения.

- В поле **Описание произошедшего** введите, 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 раскрывающемся списке **Тип инцидента** выберите тип инцидента.

  Примечание. Если инцидент не подходит ни под один из предложенных типов, укажите **Другой инцидент**. Поле обязательно для заполнения.
- Оцените важность инцидента и в раскрывающемся списке **Важность** выберите значение: **Низкая**, **Средняя**, **Высокая**, **Критическая**.
- Оцените приоритет инцидента и в раскрывающемся списке **Приоритет** выберите значение: **Критический**, **Очень высокий**, **Высокий**, **Средний**, **Низкий**.
- В блоке параметров **Обнаружен** введите дату и время обнаружения инцидента.

  Примечание. Дата указывается в формате **ДДММГГГГ**. Время указывается в формате **ЧЧ:ММ**. Поле обязательно для заполнения.

  В поле **Ущерб** введите, был ли причинен ущерб организации или ее клиентам в результате инцидента. Оцените размер ущерба и возможные негативные последствия. **Примечание.** Если ущерба нанесено не было, оставьте поле пустым.
- В раскрывающемся списке **Ответственный оператор** выберите ответственного за расследование инцидента.
- В поле **Ответственный на стороне участника** введите имя, фамилию и отчество ответственного на стороне участника, который сообщил об инциденте.

2. Если инцидент направлен на ваших клиентов, заполните вкладку **Вектор инцидента — EXT**:

- В раскрывающемся списке **Способ осуществления** выберите один из способов осуществления несанкционированной операции.

  Примечание. Поле обязательно для заполнения.

  В раскрывающемся списке **Способ перевода** выберите способ перевода денежных средств: **Перевод по номеру карты**, **Перевод по номеру счета**, **Иное**.
  Примечание. Поле обязательно для заполнения.
- В блоке параметров **Трансграничность** выберите, осуществлялся денежный перевод внутри Российской Федерации или за ее пределами. Поле обязательно для заполнения.

  Примечание. Поле обязательно для заполнения.

  В раскрывающемся списке **Подтверждение операции** выберите способ подтверждения транзакции: **Транзакция без подтверждения**, **Транзакция подтверждена с использованием 3D Secure**, **Иной способ подтверждения**.
  Примечание. Поле обязательно для заполнения.
- В раскрывающемся списке **Обращение в полицию** выберите, обращались ли вы в правоохранительные органы.

Примечание. Поле обязательно для заполнения.

3. Если инцидент направлен на организацию, заполните вкладку **Вектор инцидента — INT**:

- В поле **Средство обнаружения** введите средство обнаружения сигнатуры.

  Примечание. Поле обязательно для заполнения.

  . В поле **ID сигнатуры** введите идентификатор сигнатуры. Поле обязательно для заполнения.

  Примечание. Поле обязательно для заполнения.

- В поле **Источник получения** введите источник получения.

  Примечание. Поле обязательно для заполнения.

- В поле **Срабатываний** введите количество срабатываний сигнатуры.

  Примечание. Поле обязательно для заполнения.

4. На вкладке **Вложения** в поле **Перетащите или выберите файл** перетащите или выберите файлы, которые могут быть полезны для расследования инцидента.
5. На вкладке **Подтверждение** проверьте заполненную информацию об инциденте. Если требуется, измените информацию.
6. Чтобы создать карточку инцидента, нажмите кнопку **Создать инцидент**.

11.2. Выпуск справки-отчета об инциденте

Справка-отчет содержит краткую информацию об инциденте и историю изменений.

► Чтобы выпустить справку-отчет об инциденте:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. В панели инструментов нажмите кнопку **Выпустить справку-отчет**.

   Откроется окно **Выпустить справку-отчет**.

4. Если требуется отправить сравку-отчет по электронной почте:

- В поле **Эл. почта получателя** введите электронный адрес.
- Нажмите кнопку **Отправить на эл. почту**.

5. Если требуется сохранить справку-отчет в локальную папку, указанную в свойствах браузера, нажмите кнопку **Сохранить файл**.

11.3. Смена статуса инцидента

► Чтобы изменить статус инцидента:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
2. В таблице инцидентов выберите инцидент, статус которого вы хотите изменить.

   Примечание. Вы можете выбрать несколько инцидентов.
3. В панели инструментов нажмите кнопку **Изменить статус**.

   Откроется окно **Сменить статус инцидента "<идентификатор инцидента>"**.

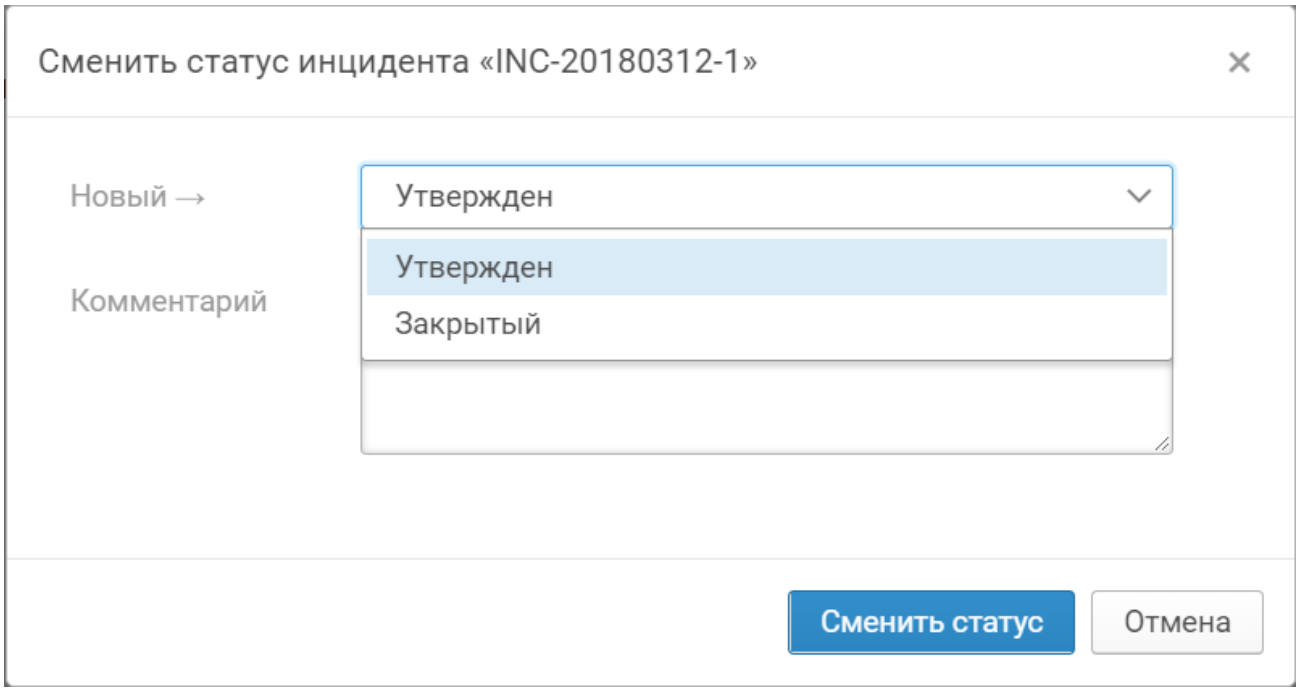

Рисунок 15. Смена статуса инцидента

4. В раскрывающемся списке **<Текущий статус инцидента>** выберите новый статус:
   - **Утвержден**. Выберите этот статус, если в результате расследования инцидент был подтвержден.
   - **Закрытый**. Выберите этот статус, если работы по инциденту завершены.
5. Если требуется, в поле **Комментарий** укажите причину смены статуса.
6. Нажмите кнопку **Сменить статус**.

Обновленный статус инцидента отображается в таблице инцидентов и в карточке инцидента.

11.4. Просмотр информации о связанных с инцидентами IP-адресах, URL и доменах

Вы можете просматривать информацию об IP-адресах, URL и доменах, связанных с инцидентами. Эта информация включает в себя регистрационные данные о владельцах доменных имен и IP-адресов, а также уровни опасности доменных имен, IP-адресов и URL. PT Incident Processing Center получает эти данные от Cybsi.

Примечание. Возможность доступна для инцидентов с типами "Вредоносное ПО", "Эксплуатация уязвимостей", "DoS или DDo-атаки", "Перебор паролей", "Фишинг" и "Фишинговый ресурс".

► Чтобы просмотреть информацию об IP-адресе, URL и домене:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.

3. На вкладке **Влияние и способ заражения** (при просмотре инцидента типа "Вредоносное ПО") или **<IP-адрес>** (при просмотре инцидента другого типа) нажмите на кнопку с IP-адресом, доменным именем или URL.

   Откроется панель, содержащая общие сведения, регистрационные данные и сведения об уровне опасности.

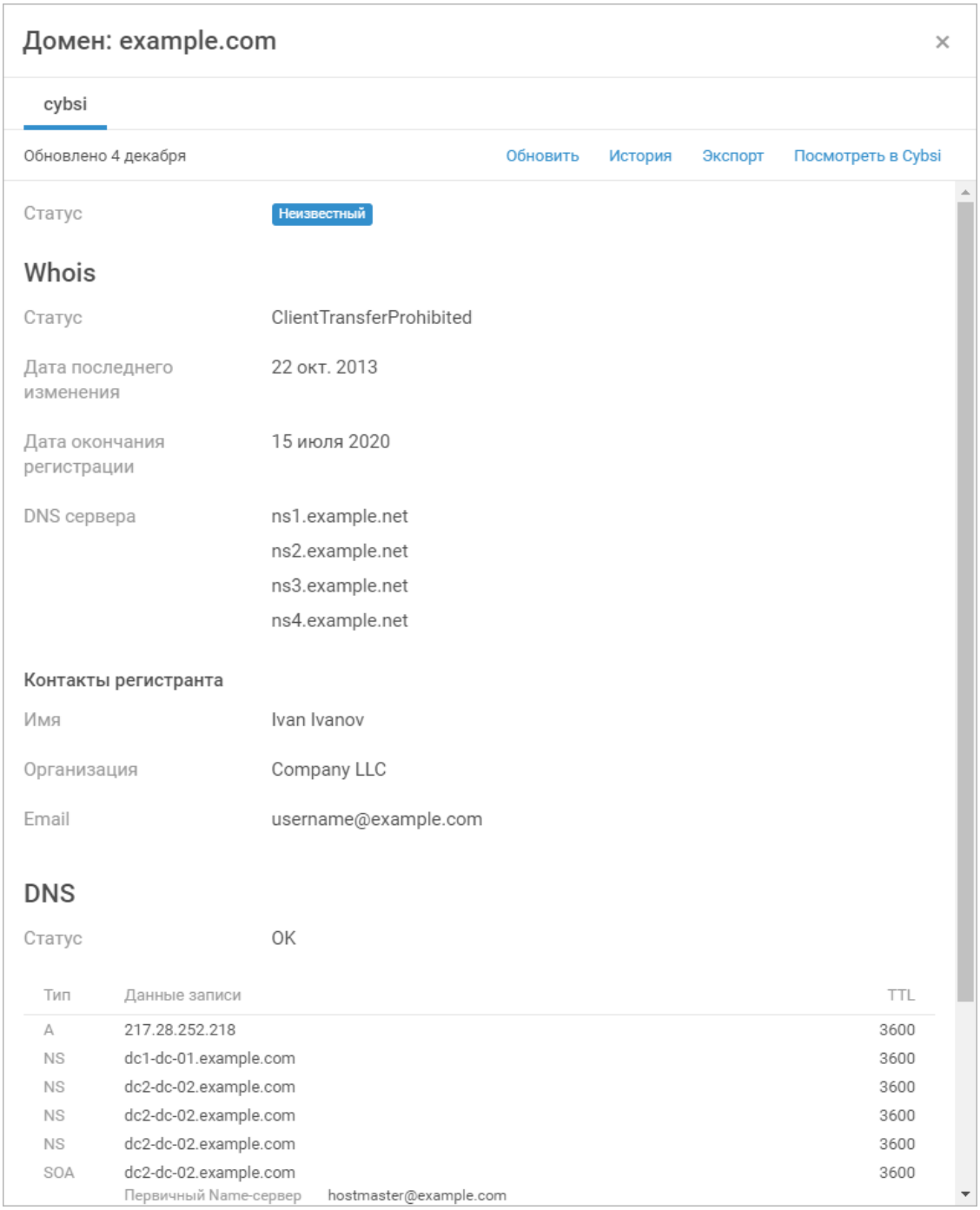

Рисунок 16. Просмотр информации о домене

4. Если вам нужно обновить информацию, нажмите кнопку **Обновить**.

   Примечание. Вы можете просматривать время, когда были получены или обновлены данные от Cybsi, по кнопке **История**. При выборе времени в открывшемся раскрывающемся списке отображается информация, полученная в это время.

5. Если вам нужно просмотреть подробную информацию в Cybsi, нажмите кнопку **Посмотреть в Cybsi**.

См. также

Передача URL и доменных имен в антивирусную лабораторию (см. раздел 21.5)

11.5. Просмотр оператора связи телефона, указанного в инциденте

PT Incident Processing Center позволяет обогащать номер телефона, связанный с инцидентом: получать информацию об операторе связи, обслуживающем номер. Название оператора связи поступает из Cybsi.

Обогащение номера телефона доступно в электронных формах операций без согласия со способом перевода "с номера телефона на номер телефона". Обогащение номера также доступно для инцидентов с типом "Использование социальной инженерии", в которых источником социальной инженерии указан номер телефона.

По умолчанию обогащение номера телефона выполняется вручную из электронной формы операции без согласия. При необходимости администратор может настроить систему так, чтобы обогащение выполнялось автоматически при создании и изменении инцидента.

► Чтобы просмотреть оператора связи:

1. В карточке инцидента выберите вкладку **Операции без согласия**.
2. В открывшейся электронной форме операции без согласия выберите вкладку **Информация о переводе**.

   Номер телефона, доступный для обогащения, отображается в виде ссылки.
3. Нажмите на номер телефона.

   Откроется боковая панель результата обогащения с названием оператора связи.

   Примечание. Вы можете просматривать время, когда были получены или обновлены данные от Cybsi, по кнопке **История**. При выборе времени в открывшемся раскрывающемся списке отображается информация, полученная в это время.
4. Если вам нужно просмотреть подробную информацию в Cybsi, нажмите кнопку **Посмотреть в Cybsi**.

11.6. Анализ трафика атаки типа "отказ в обслуживании"

При отправке заявки на регистрацию инцидента типа "DoS или DDoS-атаки" (ddosAttacks) участник информационного обмена может приложить к электронной форме дампы сетевого трафика. Приложенные дампы могут помочь вам в расследовании инцидента. Чтобы вы могли получить больше вводных данных для анализа инцидента, PT Incident Processing Center может отправлять дампы в Cybsi, который использует PT NAD для их обогащения. Обогащенные дампы включают в себя информацию о сессиях, индикаторах компрометации, переданных файлах, IP-адресах, URL и доменных именах.

► Чтобы проанализировать трафик атаки:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. На вкладке **Реализация атаки типа "отказ в обслуживании" <IP-адрес>** в блоке **Дампы сетевого трафика** нажмите на интересующий вас дамп трафика.

   Откроется окно с подробной информацией о трафике атаки.

4. Если информации нет или вам нужно ее обновить, нажмите кнопку **Обновить**.

   Примечание. Вы можете просматривать время, когда были получены или обновлены данные от Cybsi, по кнопке **История**. При выборе времени в открывшемся раскрывающемся списке отображается информация, полученная в это время.

5. Если вам нужно просмотреть подробную информацию в Cybsi, нажмите кнопку **Посмотреть в Cybsi**.

11.7. Просмотр информации об уязвимости

Система позволяет собирать, актуализировать и хранить информацию об уязвимостях информационной инфраструктуры. На основе полученной информации вы можете формировать для участников рекомендации по устранению уязвимостей.

► Чтобы просмотреть информацию об уязвимости:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента с типом «Эксплуатация уязвимостей информационной инфраструктуры» откройте карточку инцидента.
3. Выберите вкладку **<IP-адрес>**.
4. Из поля **Идентификатор уязвимости** по ссылке откройте окно **Уязвимость: <Идентификатор>**.

   Отобразится информация об уязвимости. Рекомендации по устранению уязвимости содержатся в поле **Локализация** и бюллетенях.

11.8. Взаимодействие с ГосСОПКА

PT Incident Processing Center обеспечивает обмен данными с ГосСОПКА. Это позволяет отправлять в ГосСОПКА информацию об инцидентах и получать содействие в их расследовании.

Информация об инцидентах автоматически отправляется в ГосСОПКА при выполнении как минимум одного из условий:

- Инцидент имеет вектор INT и тип TrafficHijackAttacks, Malware, DdosAttacks, Vulnerabilities, BruteForces, Spams, ControlCenters, PhishingAttacks, ProhibitedContents, MaliciousResources или ChangeContent.
- В карточке участника (см. раздел 5.9.2) на вкладке **Дополнительно** установлен флажок **Автоматически отправлять инциденты в ГосСОПКА**.
- В электронной форме инцидента на вкладке **Дополнительно** установлен флажок **Отправить в ГосСОПКА**.

Сведения о дальнейших изменениях параметров инцидентов, по которым ведется взаимодействие, также отправляются в ГосСОПКА автоматически.

Правила автоматической отправки информации об инцидентах в ГосСОПКА задаются в конфигурационном файле `scenarios.yaml` (настройка правила описана в Справочном руководстве по конфигурированию системы).

Если инцидент не был отправлен в ГосСОПКА автоматически (например, из-за проблем с сетевым соединением или потому что не подошел под указанные условия), вы можете отправить его вручную.

Обмен данными с ГосСОПКА осуществляется в карточке инцидента на вкладке **Взаимодействие с ГосСОПКА**. Вы можете отправлять сообщения в ГосСОПКА, просматривать переписку и статус обработки информации об инциденте в ГосСОПКА. Также по ссылке **Инцидент** на этой вкладке вы можете просматривать, какие именно данные из карточки инцидента были отправлены в ГосСОПКА. О поступлении сообщения от специалиста ГосСОПКА информирует Центр уведомлений.

В случаях, когда для расследования инцидента требуется дополнительная экспертиза, вы можете запросить содействие ГосСОПКА в расследовании. Специалисты ГосСОПКА направят вам рекомендации по расследованию инцидента.

В этом разделе

11.8.1. Отправка инцидента в ГосСОПКА вручную

Если инцидент не был отправлен в ГосСОПКА автоматически, вы можете отправить его вручную.

► Чтобы отправить инцидент в ГосСОПКА:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. Выберите вкладку **Взаимодействие с ГосСОПКА**.

   Примечание. В ГосСОПКА отправляются не все данные, указанные в карточке инцидента. Вы можете просмотреть информацию, которая будет отправлена, по ссылке **Инцидент**.

4. Если требуется содействие ГосСОПКА в расследовании инцидента, установите флажок **Запросить содействие**.
5. Нажмите кнопку **Отправить**.

Инцидент отправлен в ГосСОПКА.

11.8.2. Отправка сообщения в ГосСОПКА

► Чтобы отправить сообщение в ГосСОПКА:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. Выберите вкладку **Взаимодействие с ГосСОПКА**.
4. Нажмите кнопку **Сообщение** и в раскрывшемся меню выберите тип сообщения.
5. Введите сообщение.
6. Нажмите кнопку **Отправить**.

Сообщение отправлено в ГосСОПКА.

11.8.3. Запрос содействия ГосСОПКА в расследовании инцидента

Если вы не только информируете ГосСОПКА об инциденте, но и хотите получить информацию в ответ (например, описание мер, принятых в связи с инцидентом, или рекомендации по устранению последствий), вы можете запросить содействие ГосСОПКА.

► Чтобы запросить содействие ГосСОПКА в расследовании:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. Выберите вкладку **Взаимодействие с ГосСОПКА**.

4. Установите флажок **Запросить содействие**.
5. Нажмите кнопку **Отправить**.

Запрос о содействии в расследовании инцидента отправлен в ГосСОПКА.

11.9. Обновление электронной формы инцидента путем создания новой версии

Электронную форму (ЭФ) инцидента, полученную от участника, можно обновить путем создания новой версии. Для обновления доступны поля (в том числе атрибуты операции без согласия), которые не были заполнены в предыдущей версии электронной формы.

► Чтобы обновить ЭФ инцидента путем создания новой версии:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.
2. В таблице инцидентов выберите инцидент, ЭФ которого вы хотите изменить.
3. На вкладке **Связи** нажмите ссылку с запросом об инциденте.

   Откроется страница **Запросы**.
4. Откройте ЭФ инцидента на вкладке **Переписка**.
5. В окне ЭФ инцидента нажмите кнопку **Создать новую версию**.

   Поля ЭФ, доступные для изменения, станут активны.
6. Укажите в ЭФ значения атрибутов, которые не были заполнены ранее.
7. Нажмите кнопку **Сохранить**.

   Сохраненный черновик ЭФ с новой информацией отобразится в нижней части страницы.
8. Нажмите кнопку **Отправить**.

Новая версия ЭФ инцидента добавлена.

11.10. Просмотр похожих инцидентов

Участники могут сообщать в центр о похожих инцидентах. Это могут быть действия злоумышленников в рамках одной вредоносной кампании или просто похожие инциденты, на которые оператор одинаково реагирует, сокращая время на обработку инцидента.

Степень схожести инцидентов вычисляется автоматически. Вы можете просматривать похожие инциденты в Личном кабинете оператора.

► Чтобы просмотреть похожие инциденты:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

Откроется страница со списком инцидентов.

2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. В правой части страницы выберите вкладку **Похожие**.

   Отобразится список инцидентов (от наиболее похожим к наименее похожим). Вы можете отсортировать инциденты по параметрам в раскрывающемся списке **Сортировка**.

4. Если требуется, создайте связь (см. раздел 21.2.1) текущего инцидента с похожим инцидентом по кнопке **Создать связь**.

12. Кампании. Работа с кампаниями

Кампания — это совокупность нескольких нарушений ИБ (атак), направленных на достижение конкретной цели (например, доступ к конфиденциальной информации) и происходящих в течение определенного времени.

Кампания может характеризоваться следующими признаками:

— целями (люди или информационные ресурсы);

— инцидентами, которые происходят во время кампании;

— инструментами и ресурсами, которые злоумышленники используют для достижения цели кампании (например, вредоносное ПО, методы социальной инженерии).

Кампания в PT Incident Processing Center— это несколько инцидентов, сгруппированных по общим признакам. Объединение инцидентов в кампании позволяет обрабатывать инциденты проще и быстрее.

В PT Incident Processing Center вы можете добавлять кампании и включать в них инциденты.

Созданные кампании можно изменять: добавлять и изменять правила, добавлять вручную в кампанию инциденты и связи с другими объектами в системе.

Автоматическое (на основе правил) и ручное включение инцидентов в состав кампании дополняют друг друга. При необходимости вы можете вручную добавлять в кампанию любые инциденты. Даже если добавленные вручную инциденты не соответствуют правилам автоматического включения в кампанию, система все равно оставит их в кампании.

Кампания может иметь статусы **Новая**, **В работе**, или **Закрыта**. Закрытые кампании можно повторно переводить в статус **В работе**. Статусы кампаний и инцидентов в их составе не зависят друг от друга. Например, в кампанию со статусом **Новая** или **В работе** могут входить закрытые инциденты и наоборот.

В интерфейсе системы список добавленных кампаний содержится на странице **Инциденты** → **Кампании**.

Этот раздел содержит инструкции по работе с кампаниями.

В этом разделе

12.1. Как добавить кампанию

► Чтобы добавить кампанию:

1. В главном меню в разделе **Инциденты** выберите пункт **Кампании**.

Откроется страница со списком кампаний.

2. В панели инструментов нажмите кнопку **Добавить кампанию**.

   Откроется страница добавления кампании.

3. Укажите название кампании, отображаемое в системе, и ее краткое описание.
4. Если необходимо, назначьте кампанию оператору.
5. Настройте правила автоматического включения инцидентов в кампанию.

   Система включает инцидент в кампанию, если для него выполняются все критерии, объединенные оператором "И".

   Для правил с условиями "равно", "не равно" можно указывать значения через запятую. Условия "больше", "больше или равно", "меньше", "меньше или равно" можно использовать только для значений с числом или датой. Условие "содержит" можно использовать для атрибутов инцидента, представляющих собой строку или набор строк. Для правил с условием "содержит" можно указывать несколько значений через запятую. В этом случае в кампанию будут включены все инциденты, атрибуты которых содержат хотя бы одно из указанных значений.

   Примечание. Создавать и настраивать правила сразу не обязательно. Вы можете сохранить кампанию и вернуться к настройке правил позже, или добавить в сохраненную кампанию инциденты вручную из списка инцидентов.

6. Нажмите кнопку **Сохранить**.

Кампания добавлена. Новая кампания отобразится на странице со списком кампаний.

После сохранения новой кампании система проверяет все инциденты на соответствие правилам включения в кампанию и включает в кампанию подходящие инциденты. Аналогичная проверка выполняется при изменении инцидентов или правил включения в кампанию. Принадлежность инцидента к одной или нескольким кампаниям отображается в карточке инцидента в разделе **Общие сведения**.

12.2. Как вручную добавить инциденты в существующую кампанию

При необходимости вы можете вручную добавлять в кампанию любые инциденты.

► Чтобы добавить инциденты в кампанию:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.

   Откроется страница со списком инцидентов.

2. Выберите один или несколько инцидентов, которые нужно включить в кампанию.
3. В панели инструментов нажмите кнопку **Добавить в кампанию**.
4. В открывшемся меню с полем поиска найдите и выберите кампанию, в которую нужно добавить выбранные инциденты.

С помощью пункта меню **Добавить новую** вы также можете на основе выбранных инцидентов добавить новую кампанию. Новая кампания будет содержать только выбранные инциденты.

Инциденты добавлены в существующую кампанию.

12.3. Как посмотреть участников, атакованных в ходе кампании

Вы можете быстро просмотреть список участников, которые подверглись атакам в ходе кампании.

► Чтобы посмотреть участников, атакованных в ходе кампании:

1. В главном меню в разделе **Инциденты** выберите пункт **Кампании**.

   Откроется страница со списком кампаний.

2. Двойным щелчком мыши по идентификатору нужной вам кампании откройте ее карточку.

3. В левой части карточки нажмите **Атакованные участники**.

Отобразится список участников, атакованных в ходе кампании. В списке содержатся участники, которые сообщили хотя бы об одном инциденте, включенном в кампанию.

13. Работа с угрозами

Угроза — это совокупность факторов и условий, которые могут привести к нарушению информационной безопасности организации и способны вызвать негативные последствия для организации.

Примечание. В разделе приведены описания параметров для Российской Федерации.

В этом разделе

См. также

Типовые действия с объектами системы (см. раздел 21)

13.1. Добавление угрозы "Вредоносное программное обеспечение"

Угроза "Вредоносное программное обеспечение" — это угроза несанкционированного перевода денежных средств в результате воздействия вредоносного ПО.

► Чтобы добавить в продукт угрозу "Вредоносное программное обеспечение":

1. В главном меню в разделе **База знаний** выберите пункт **Угрозы**.

   Откроется страница со списком угроз.

2. В панели инструментов нажмите кнопку **Добавить угрозу**.

   Откроется окно **Добавление новой угрозы**.

3. На вкладке **Общие сведения** в поле **Название** введите название угрозы.

   Название должно описывать суть содержания карточки угрозы.

   Примечание. Поле обязательно для заполнения.

4. В поле **Федеральный округ** выберите федеральный округ, на территории которого обнаружена угроза.
5. В поле **Субъект федерации** выберите субъект Федерации, на территории которого обнаружена угроза.
6. В поле **Населенный пункт** введите название города или иного населенного пункта, в котором обнаружена угроза.
7. В поле **Дата выявления** укажите дату выявления угрозы.

   Примечание. Дата указывается в формате **ДДММГГГГ**.
8. В поле **Автор публикации** укажите автора информации об угрозе, например название участника. Вы также можете ввести ссылку на ресурс в интернете.
9. В раскрывающемся списке **Тип угрозы** выберите **Вредоносное программное обеспечение**.
10. В поле **Описание** введите описание угрозы.

    Примечание. Поле обязательно для заполнения.
11. На вкладке **Вредоносное программное обеспечение** в поле **Обнаруживается антивирусными решениями** введите названия антивирусных средств, которыми можно обнаружить вредоносное ПО.

    Примечание. Поле обязательно для заполнения.
12. В поле **Индикаторы компрометации** введите индикаторы компрометации в формате OpenIOC, Yara, XML и так далее.

    Примечание. Поле обязательно для заполнения.
13. На вкладке **Обнаружение и устранение** в поле **Автор способа** укажите автора способа обнаружения угрозы, например название участника.

    Примечание. Поле обязательно для заполнения.
14. В поле **Описание способа** введите описание способа обнаружения угрозы.
15. В поле **Файл с правилом сигнатуры или правила детекта** перетащите или выберите соответствующий файл.
16. В поле **Возможные меры устранения** введите описание возможных мер устранения угрозы.
17. В поле **Прочая информация** введите дополнительную информацию.
18. Нажмите кнопку **Создать**.

Угроза "Вредоносное программное обеспечение" добавлена.

13.2. Добавление угрозы "Эксплуатация уязвимости"

Угроза "Эксплуатация уязвимости" — это угроза использования недостатка программного или аппаратного компонента организации, что может оказать негативное воздействие на конфиденциальность, целостность или доступность данных.

► Чтобы добавить в продукт угрозу "Эксплуатация уязвимости":

1. В главном меню в разделе **База знаний** выберите пункт **Угрозы**.

   Откроется страница со списком угроз.

2. В панели инструментов нажмите кнопку **Добавить угрозу**.

   Откроется окно **Добавление новой угрозы**.

3. На вкладке **Общие сведения** в поле **Название** введите название угрозы.

   Название должно описывать суть содержания карточки угрозы.

   Примечание. Поле обязательно для заполнения.

4. В поле **Федеральный округ** выберите федеральный округ, на территории которого обнаружена угроза.

5. В поле **Субъект федерации** выберите субъект Федерации, на территории которого обнаружена угроза.

6. В поле **Населенный пункт** введите название города или иного населенного пункта, в котором обнаружена угроза.

7. В поле **Дата выявления** укажите дату выявления угрозы.

   Примечание. Дата указывается в формате **ДДММГГГГ**.

8. В поле **Автор публикации** укажите автора информации об угрозе, например название участника. Вы также можете ввести ссылку на ресурс в интернете.

9. В раскрывающемся списке **Тип угрозы** выберите **Эксплуатация уязвимости**.

10. В поле **Описание** введите описание угрозы.

    Примечание. Поле обязательно для заполнения.

11. На вкладке **Эксплуатация уязвимости** в поле **Идентификаторы уязвимости** введите идентификаторы уязвимости.

    Примечание. Поле обязательно для заполнения.

12. В поле **Методики эксплуатации** введите метрики эксплуатации.

    Примечание. Поле обязательно для заполнения.

13. На вкладке **Обнаружение и устранение** в поле **Автор способа** укажите автора способа обнаружения угрозы, например название участника.

    Примечание. Поле обязательно для заполнения.

14. В поле **Описание способа** введите описание способа обнаружения угрозы.

15. В поле **Файл с правилом сигнатуры или правила детекта** перетащите или выберите соответствующий файл.
16. В поле **Возможные меры устранения** введите описание возможных мер устранения угрозы.
17. В поле **Прочая информация** введите дополнительную информацию.
18. Нажмите кнопку **Создать**.

Угроза "Эксплуатация уязвимостей" добавлена.

13.3. Добавление угрозы DDoS

Угроза DDoS — это угроза сбоя в работе оборудования и каналов связи, вызванного внешними причинами.

► Чтобы добавить в продукт угрозу DDoS:

1. В главном меню в разделе **База знаний** выберите пункт **Угрозы**.

   Откроется страница со списком угроз.
2. В панели инструментов нажмите кнопку **Добавить угрозу**.

   Откроется окно **Добавление новой угрозы**.
3. На вкладке **Общие сведения** в поле **Название** введите название угрозы.

   Название должно описывать суть содержания карточки угрозы.

   Примечание. Поле обязательно для заполнения.
4. В поле **Федеральный округ** выберите федеральный округ, на территории которого обнаружена угроза.
5. В поле **Субъект федерации** выберите субъект Федерации, на территории которого обнаружена угроза.
6. В поле **Населенный пункт** введите название города или иного населенного пункта, в котором обнаружена угроза.
7. В поле **Дата выявления** укажите дату выявления угрозы.

   Примечание. Дата указывается в формате **ДДММГГГГ**.
8. В поле **Автор публикации** укажите автора информации об угрозе, например название участника. Вы также можете ввести ссылку на ресурс в интернете.
9. В раскрывающемся списке **Тип угрозы** выберите **DDoS**.
10. В поле **Описание** введите описание угрозы.

    Примечание. Поле обязательно для заполнения.
11. На вкладке **DDoS** в поле **Атакующие IP-адреса** введите IP-адреса источника атаки.
12. В поле **Тип атаки** введите тип атаки.

Примечание. Поле обязательно для заполнения.

13. **Ожидаемая мощность** введите ожидаемую мощность.
14. **Ожидаемое усилие** введите ожидаемое усилие.
15. На вкладке **Обнаружение и устранение** в поле **Автор способа** укажите автора способа обнаружения угрозы, например название участника.

    Примечание. Поле обязательно для заполнения.
16. В поле **Описание способа** введите описание способа обнаружения угрозы.
17. В поле **Файл с правилом сигнатуры или правила детекта** перетащите или выберите соответствующий файл.
18. В поле **Возможные меры устранения** введите описание возможных мер устранения угрозы.
19. В поле **Прочая информация** введите дополнительную информацию.
20. Нажмите кнопку **Создать**.

Угроза DDoS добавлена.

13.4. Добавление угрозы "ЦУ бот-сети"

Угроза "ЦУ бот-сети" — это угроза использования центра управления бот-сетью для распространения вредоносного кода.

► Чтобы добавить в продукт угрозу "ЦУ бот-сети":

1. В главном меню в разделе **База знаний** выберите пункт **Угрозы**.

   Откроется страница со списком угроз.
2. В панели инструментов нажмите кнопку **Добавить угрозу**.

   Откроется окно **Добавление новой угрозы**.
3. На вкладке **Общие сведения** в поле **Название** введите название угрозы.

   Название должно описывать суть содержания карточки угрозы.

   Примечание. Поле обязательно для заполнения.
4. В поле **Дата выявления** укажите дату выявления угрозы.

   Примечание. Дата указывается в формате **ДДММГГГГ**.
5. В поле **Федеральный округ** выберите федеральный округ, на территории которого обнаружена угроза.
6. В поле **Субъект федерации** выберите субъект Федерации, на территории которого обнаружена угроза.
7. В поле **Населенный пункт** введите название города или иного населенного пункта, в котором обнаружена угроза.

8. В поле **Автор публикации** укажите автора информации об угрозе, например название участника. Вы также можете ввести ссылку на ресурс в интернете.
9. В раскрывающемся списке **Тип угрозы** выберите **ЦУ бот-сети**.
10. В поле **Описание** введите описание угрозы.

    Примечание. Поле обязательно для заполнения.
11. На вкладке **ЦУ бот-сети** в поле **IP-адрес или доменное имя** введите IP-адрес или доменное имя бот-сети.

    Примечание. Поле обязательно для заполнения.
12. В поле **Тип и общие сведения о ботнет** введите тип бот-сети и общие сведения.
13. В поле **Каким образом выявлен** опишите способ обнаружения бот-сети.

    Примечание. Поле обязательно для заполнения.
14. На вкладке **Обнаружение и устранение** в поле **Автор способа** укажите автора способа обнаружения угрозы, например название участника.

    Примечание. Поле обязательно для заполнения.
15. В поле **Описание способа** введите описание способа обнаружения угрозы.
16. В поле **Файл с правилом сигнатуры или правила детекта** перетащите или выберите соответствующий файл.
17. В поле **Возможные меры устранения** введите описание возможных мер устранения угрозы.
18. В поле **Прочая информация** введите дополнительную информацию.
19. Нажмите кнопку **Создать**.

Угроза "ЦУ бот-сети" добавлена.

13.5. Добавление угрозы "Фишинг"

Угроза "Фишинг" — это угроза совершения несанкционированного перевода денежных средств в результате использования фишингового ресурса.

► Чтобы добавить в продукт угрозу "Фишинг":

1. В главном меню в разделе **База знаний** выберите пункт **Угрозы**.

   Откроется страница со списком угроз.
2. В панели инструментов нажмите кнопку **Добавить угрозу**.

   Откроется окно **Добавление новой угрозы**.
3. На вкладке **Общие сведения** в поле **Название** введите название угрозы.

   Название должно описывать суть содержания карточки угрозы.

   Примечание. Поле обязательно для заполнения.

4. В поле **Федеральный округ** выберите федеральный округ, на территории которого обнаружена угроза.
5. В поле **Субъект федерации** выберите субъект Федерации, на территории которого обнаружена угроза.
6. В поле **Населенный пункт** введите название города или иного населенного пункта, в котором обнаружена угроза.
7. В поле **Дата выявления** укажите дату выявления угрозы.

   Примечание. Дата указывается в формате **ДДММГГГГ**.
8. В поле **Автор публикации** укажите автора информации об угрозе, например название участника. Вы также можете ввести ссылку на ресурс в интернете.
9. В раскрывающемся списке **Тип угрозы** выберите **Фишинг**.
10. В поле **Описание** введите описание угрозы.

    Примечание. Поле обязательно для заполнения.
11. На вкладке **Фишинг** в поле **IP-адрес или доменное имя** введите IP-адрес или доменное имя ресурса, замаскированного под доверенный аналог.

    Примечание. Поле обязательно для заполнения.
12. В поле **Дата обнаружения ресурса** выберите дату обнаружения ресурса, замаскированного под доверенный аналог.

    Примечание. Поле обязательно для заполнения.
13. В поле **Текст письма** введите текст письма, полученного от фишингового ресурса.
14. В поле **Технические заголовки письма** введите технические заголовки письма.
15. На вкладке **Обнаружение и устранение** в поле **Автор способа** укажите автора способа обнаружения угрозы, например название участника.

    Примечание. Поле обязательно для заполнения.
16. В поле **Описание способа** введите описание способа обнаружения угрозы.
17. В поле **Файл с правилом сигнатуры или правила детекта** перетащите или выберите соответствующий файл.
18. В поле **Возможные меры устранения** введите описание возможных мер устранения угрозы.
19. В поле **Прочая информация** введите дополнительную информацию.
20. Нажмите кнопку **Создать**.

Угроза "Фишинг" добавлена.

13.6. Добавление угрозы "Вредоносный ресурс"

Угроза "Вредоносный ресурс" — это угроза использования ресурса в интернете для распространения противоправного контента или недоставерной информации.

► Чтобы добавить в продукт угрозу "Вредоносный ресурс":

1. В главном меню в разделе **База знаний** выберите пункт **Угрозы**.

   Откроется страница со списком угроз.

2. В панели инструментов нажмите кнопку **Добавить угрозу**.

   Откроется окно **Добавление новой угрозы**.

3. На вкладке **Общие сведения** в поле **Название** введите название угрозы.

   Название должно описывать суть содержания карточки угрозы.

   Примечание. Поле обязательно для заполнения.

4. В поле **Федеральный округ** выберите федеральный округ, на территории которого обнаружена угроза.
5. В поле **Субъект федерации** выберите субъект Федерации, на территории которого обнаружена угроза.
6. В поле **Населенный пункт** введите название города или иного населенного пункта, в котором обнаружена угроза.
7. В поле **Дата выявления** укажите дату выявления угрозы.

   Примечание. Дата указывается в формате **ДДММГГГГ**.

8. В поле **Автор публикации** укажите автора информации об угрозе, например название участника. Вы также можете ввести ссылку на ресурс в интернете.
9. В раскрывающемся списке **Тип угрозы** выберите **Вредоносный ресурс**.
10. В поле **Описание** введите описание угрозы.

    Примечание. Поле обязательно для заполнения.

11. На вкладке **Вредоносный ресурс** в поле **IP-адрес или доменное имя** введите IP-адрес или доменное имя вредоносного ресурса.

    Примечание. Поле обязательно для заполнения.

12. В поле **Дата обнаружения ресурса** выберите дату обнаружения ресурса.
13. В поле **Причины, почему ресурс подозревается вредоносным** опишите, почему ресурс подозревается вредоносным.

    Примечание. Поле обязательно для заполнения.

14. На вкладке **Обнаружение и устранение** в поле **Автор способа** укажите автора способа обнаружения угрозы, например название участника.

    Примечание. Поле обязательно для заполнения.

15. В поле **Описание способа** введите описание способа обнаружения угрозы.
16. В поле **Файл с правилом сигнатуры или правила детекта** перетащите или выберите соответствующий файл.
17. В поле **Возможные меры устранения** введите описание возможных мер устранения угрозы.
18. В поле **Прочая информация** введите дополнительную информацию.
19. Нажмите кнопку **Создать**.

Угроза "Вредоносный ресурс" добавлена.

13.7. Добавление угрозы "Мошеннический телефонный номер"

Угроза "Мошеннический телефонный номер" — это угроза использования 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).

► Чтобы добавить в продукт угрозу "Мошеннический телефонный номер":

1. В главном меню в разделе **База знаний** выберите пункт **Угрозы**.

   Откроется страница со списком угроз.

2. В панели инструментов нажмите кнопку **Добавить угрозу**.

   Откроется окно **Добавление новой угрозы**.

3. На вкладке **Общие сведения** в поле **Название** введите название угрозы.

   Название должно описывать суть содержания карточки угрозы.

   Примечание. Поле обязательно для заполнения.

4. В поле **Федеральный округ** выберите федеральный округ, на территории которого обнаружена угроза.
5. В поле **Субъект федерации** выберите субъект Федерации, на территории которого обнаружена угроза.
6. В поле **Населенный пункт** введите название города или иного населенного пункта, в котором обнаружена угроза.
7. В поле **Дата выявления** укажите дату выявления угрозы.

   Примечание. Дата указывается в формате **ДДММГГГГ**.

8. В поле **Автор публикации** укажите автора информации об угрозе, например название участника. Вы также можете ввести ссылку на ресурс в интернете.
9. В раскрывающемся списке **Тип угрозы** выберите **Мошеннический телефонный номер**.

10. В поле **Описание** введите описание угрозы.

    Примечание. Поле обязательно для заполнения.

11. На вкладке **Мошеннический телефонный номер** в поле **Дата и время звонка (смс)** выберите дату и введите время совершения несанкционированного действия.

    Время указывается в формате **ЧЧ:ММ**.

12. В поле **Номер телефона** введите номер, с которого было совершено несанкционированное действие.

    Примечание. Поле обязательно для заполнения.

13. В поле **Текст SMS** введите текст SMS-сообщения.

14. На вкладке **Обнаружение и устранение** в поле **Автор способа** укажите автора способа обнаружения угрозы, например название участника.

    Примечание. Поле обязательно для заполнения.

15. В поле **Описание способа** введите описание способа обнаружения угрозы.

16. В поле **Файл с правилом сигнатуры или правила детекта** перетащите или выберите соответствующий файл.

17. В поле **Возможные меры устранения** введите описание возможных мер устранения угрозы.

18. В поле **Прочая информация** введите дополнительную информацию.

19. Нажмите кнопку **Создать**.

Угроза "Мошеннический телефонный номер" добавлена.

13.8. Добавление угрозы "Технические подробности"

Угроза "Технические подробности" — это угроза, которую нельзя отнести ни к одному из других типов угроз.

► Чтобы добавить в продукт угрозу "Технические подробности":

1. В главном меню в разделе **База знаний** выберите пункт **Угрозы**.

   Откроется страница со списком угроз.

2. В панели инструментов нажмите кнопку **Добавить угрозу**.

   Откроется окно **Добавление новой угрозы**.

3. На вкладке **Общие сведения** в поле **Название** введите название угрозы.

   Название должно описывать суть содержания карточки угрозы.

   Примечание. Поле обязательно для заполнения.

4. В поле **Федеральный округ** выберите федеральный округ, на территории которого обнаружена угроза.

5. В поле **Субъект федерации** выберите субъект Федерации, на территории которого обнаружена угроза.
6. В поле **Населенный пункт** введите название города или иного населенного пункта, в котором обнаружена угроза.
7. В поле **Дата выявления** укажите дату выявления угрозы.

   Примечание. Дата указывается в формате **ДДММГГГГ**.
8. В поле **Автор публикации** укажите автора информации об угрозе, например название участника. Вы также можете ввести ссылку на ресурс в интернете.
9. В раскрывающемся списке **Тип угрозы** выберите **Технические подробности**.
10. В поле **Описание** введите описание угрозы.

    Примечание. Поле обязательно для заполнения.
11. На вкладке **Технические подробности** в поле **Описание** введите описание угрозы.

    Примечание. Поле обязательно для заполнения.
12. На вкладке **Обнаружение и устранение** в поле **Автор способа** укажите автора способа обнаружения угрозы, например название участника.

    Примечание. Поле обязательно для заполнения.
13. В поле **Описание способа** введите описание способа обнаружения угрозы.
14. В поле **Файл с правилом сигнатуры или правила детекта** перетащите или выберите соответствующий файл.
15. В поле **Возможные меры устранения** введите описание возможных мер устранения угрозы.
16. В поле **Прочая информация** введите дополнительную информацию.
17. Нажмите кнопку **Создать**.

Угроза "Технические подробности" добавлена.

13.9. Просмотр информации о связанных с угрозами IP-адресах, URL и доменах

Вы можете просматривать информацию об IP-адресах, URL и доменах, связанных с угрозами. Эта информация включает в себя регистрационные данные о владельцах доменных имен и IP-адресов, а также указания на уровень опасности доменных имен, IP-адресов и URL. PT Incident Processing Center получает эти данные от Cybsi.

Примечание. Возможность доступна для угроз с типами "Вредоносный ресурс", "ЦУ бот-сети", "DDoS" и "Фишинг".

► Чтобы просмотреть информацию об IP-адресе, URL и домене:

1. В главном меню в разделе **База знаний** выберите пункт **Угрозы**.

Откроется страница со списком угроз.

2. На вкладке **<Тип угрозы>** нажмите на кнопку с IP-адресом, доменным именем или URL ресурса.

   Откроется панель, содержащая общие сведения, регистрационные данные и сведения об уровне опасности.

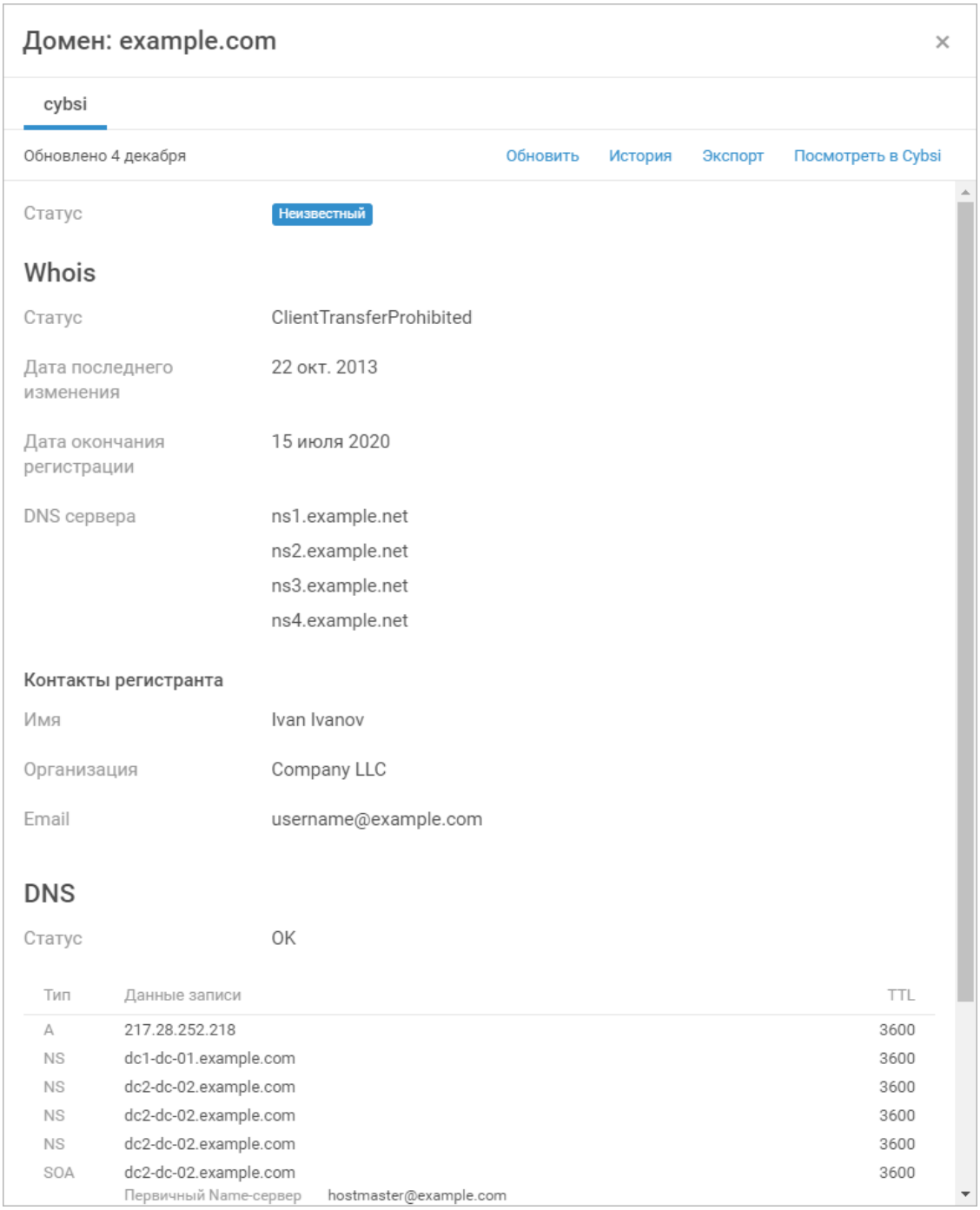

Рисунок 17. Просмотр информации о домене

3. Если вам нужно обновить информацию, нажмите кнопку **Обновить**.

   Примечание. Вы можете просматривать время, когда были получены или обновлены данные от Cybsi, по кнопке **История**. При выборе времени в открывшемся раскрывающемся списке отображается информация, полученная в это время.

4. Если вам нужно просмотреть подробную информацию в Cybsi, нажмите кнопку **Посмотреть в Cybsi**.

13.10. Просмотр описания уязвимости в PT KB

Для угроз Эксплуатация уязвимости вы можете просматривать описание уязвимостей в PT KB.

► Чтобы перейти к описанию уязвимости в PT KB из карточки угрозы:

1. В главном меню в разделе **База знаний** выберите пункт **Угрозы**.

   Откроется страница со списком угроз.

2. По ссылке с идентификатором угрозы Эксплуатация уязвимости перейдите в карточку угрозы.

3. Перейдите на вкладку **Эксплуатация уязвимости**.

4. Из поля **Идентификаторы уязвимости** по ссылке с идентификатором перейдите в PT KB.

   Откроется страница **Уязвимости**.

14. Работа с уязвимостями

Уязвимость — недостаток вычислительной логики (например, в коде), обнаруженный в программном или аппаратном компоненте (например, в прошивке), использование которого может оказать негативное воздействие на конфиденциальность, целостность или доступность данных.

В этом разделе описаны действия, которые вы можете выполнять с уязвимостью:

— Добавить в систему карточку уязвимости, в которой будет храниться информация о найденной уязвимости. Если информацию об уязвимости передает участник в электронной форме в запросе, вы можете добавить в систему карточку уязвимости на основе электронной формы.

— Назначить ответственного за обработку уязвимости во время заполнения карточки уязвимости или отдельно после добавления карточки уязвимости в систему.

— Изменить статус уязвимости на **Назначена**, если назначен ответственный за ее обработку, или **Обработана**, если все работы по уязвимости выполнены.

  Примечание. Сразу после добавления в систему карточки уязвимости уязвимость имеет статус по умолчанию **Новая**.

— Типовые действия, позволяющие ускорить и упростить работу с уязвимостями.

В этом разделе

См. также

Типовые действия с объектами системы (см. раздел 21)

14.1. Добавление карточки уязвимости

Вы можете добавить в систему карточку с информацией об уязвимости следующими способами:

— на странице со списком уязвимостей;

— на основе электронной формы уязвимости, добавленной к запросу (см. раздел 8.2).

► Чтобы добавить карточку уязвимости на странице со списком уязвимостей:

1. В главном меню в разделе **База знаний** выберите пункт **Уязвимости**.

   Откроется страница со списком уязвимостей.

2. В панели инструментов нажмите кнопку **Добавить уязвимость**.

Откроется страница **Добавление уязвимости**.

3. На вкладке **Общие сведения** в раскрывающемся списке **Класс** выберите класс уязвимости.
4. На вкладке **Программное обеспечение** в поле **Наименование ПО** введите название ПО, в котором обнаружена уязвимость.
5. В поле **Версия ПО** введите версию ПО, в котором обнаружена уязвимость.
6. На вкладке **Меры по устранению** нажмите кнопку **Сохранить**.

Добавлена карточка уязвимости со статусом **Новая**.

См. также

Параметры уязвимости (см. раздел 5.17.2)

14.2. Назначение ответственного за обработку уязвимости

Примечание. При назначении объекта в системе на пользователя для выбора доступны только пользователи, учетные записи которых в системе активны. Нельзя назначить объект на пользователя, учетная запись которого заблокирована.

► Чтобы назначить ответственного за обработку уязвимости:

1. В главном меню в разделе **База знаний** выберите пункт **Уязвимости**.

   Откроется страница со списком уязвимостей.
2. Выберите уязвимость, для которой вы хотите назначить ответственного.
3. В панели инструментов нажмите кнопку **Назначить** и в раскрывшемся меню выберите ответственного.

Ответственный за обработку уязвимости назначен.

14.3. Изменение статуса уязвимости

► Чтобы изменить статус уязвимости:

1. В главном меню в разделе **База знаний** выберите пункт **Уязвимости**.

   Откроется страница **Уязвимости**.
2. Выберите уязвимость, статус которой вы хотите изменить.
3. В панели инструментов нажмите кнопку **Изменить статус** и в раскрывшемся меню выберите статус.

Статус уязвимости изменен.

15. Работа с информационными карточками и публикациями

Информационная карточка позволяет оператору сохранять в системе полезные материалы в свободной форме. Информационные карточки можно связывать с другими объектами системы (например, с инцидентами или угрозами) и использовать при работе с ними.

Информационная карточка может содержать уведомление о мероприятии по раскрытию информации или другие полезные материалы в свободной форме. Информационная карточка, содержащая уведомление участника о планируемом мероприятии по раскрытию информации, называется публикацией.

В этом разделе содержатся инструкции по работе с информационными карточками и публикациями.

В этом разделе

См. также

Типовые действия с объектами системы (см. раздел 21)

15.1. Добавление информационной карточки

Примечание. При назначении объекта в системе на пользователя для выбора доступны только пользователи, учетные записи которых в системе активны. Нельзя назначить объект на пользователя, учетная запись которого заблокирована.

► Чтобы добавить информационную карточку в систему:

1. В главном меню в разделе **База знаний** выберите пункт **Информационные карточки**.

   Откроется страница **Информационные карточки**.

2. В панели инструментов нажмите кнопку **Добавить инф. карточку**.

   Откроется страница **Добавление информационной карточки**.

3. На вкладке **Общие сведения** в поле **Тип** выберите **Инф. карточка**.
4. Если требуется, в поле **Назначен** выберите ответственного за обработку информационной карточки.
5. В поле **Статус** выберите статус обработки информационной карточки.

   Примечание. Поле обязательно для заполнения.

6. В поле **Заголовок** введите название информационной карточки.

Примечание. Поле обязательно для заполнения.

7. В поле **Описание** введите описание информационной карточки.

   Примечание. Описание не должно превышать 3000 символов. Поле обязательно для заполнения.

8. Если требуется, в поле **Ссылка** введите ссылку на источник информации.
9. Если требуется, в поле **Вложение** перетащите или выберите файл.

   Примечание. Используйте вложения для сохранения в карточке больших объемов информации, например, статей.

10. Нажмите кнопку **Сохранить**.

Информационная карточка добавлена в систему.

15.2. Добавление публикации

► Чтобы добавить публикацию в систему:

1. В главном меню в разделе **База знаний** выберите пункт **Информационные карточки**.

   Откроется страница **Информационные карточки**.

2. В панели инструментов нажмите кнопку **Добавить инф. карточку**.

   Откроется страница **Добавление информационной карточки**.

3. На вкладке **Общие сведения** в поле **Тип** выберите **Публикация**.
4. Если требуется, в поле **Назначен** выберите ответственного за обработку публикации.
5. В поле **Статус** выберите статус обработки публикации.
6. В поле **Наименование мероприятия** введите название мероприятия.
7. В поле **Описание** введите описание публикации.

   Примечание. Описание не должно превышать 3000 символов. Поле обязательно для заполнения.

8. В поле **Организация** введите наименование организации, которая проводит мероприятие.
9. В поле **Ответственные лица** добавьте ответственных за проведение мероприятия.
10. В поле **Дата мероприятия** выберите дату и время проведения мероприятия.
11. Если требуется, в поле **Географическое местоположение** укажите федеральный округ, субъект федерации и населенный пункт, в котором будет проходить мероприятие.
12. Нажмите кнопку **Продолжить**.
13. На вкладке **Мероприятие** в поле **Тип мероприятия** выберите тип мероприятия.
14. В поле **Тема и содержание мероприятия** введите тему и программу мероприятия.

15. Если требуется, в поле **Вложение** перетащите или выберите файл.

    Примечание. Используйте вложения для сохранения в карточке больших объемов информации, например, статей.

16. Нажмите кнопку **Продолжить**.
17. Если требуется, на вкладке **Калькулятор рейтинга публикации** рассчитайте рейтинг публикации.
18. Нажмите кнопку **Сохранить**.

Публикация добавлена в систему.

15.3. Расчет рейтинга публикации

При получении от участника публикации с информацией о мероприятии оператору нужно оценить, нужно ли оповещать пресс-службу о готовящемся мероприятии.

Система помогает оператору решить эту задачу с помощью расчета рейтинга публикации. Мероприятия с высоким рейтингом (>1) с большой вероятностью вызовут интерес со стороны прессы, которая начнет отправлять запросы в пресс-службу. Рейтинг публикации позволяет своевременно оповестить пресс-службу о возможных запросах прессы и подготовиться к ним.

► Чтобы рассчитать рейтинг публикации:

1. Откройте на просмотр электронную форму публикации, полученную от участника в запросе.
2. По кнопке **Перейти к созданию публикации** перейдите к созданию информационной карточки публикации.
3. На вкладках **Общие сведения** и **Мероприятие** заполните необходимые поля.
4. На вкладке **Калькулятор рейтинга публикации** выберите параметры для расчета индекса публикации:
   - **Критичность публикации для устойчивости финансового состояния субъекта** (после публикации).
   - **Коммерческая организация признана значимой на рынке платежных услуг**: если участник является значимой или системно-значимой кредитной организацией (в карточке участника в параметре **Вид** выбрано **Значимые** или **СЗКО**), по умолчанию выбрано **Да**.
   - **Атака приобретает массовый характер**.
   - **Планируется публикация**: кредитная организация публикует или планирует публиковать информацию об атаке (по умолчанию выбрано **Да**).
   - **Дата мероприятия**: учет влияния на временного фактора (день недели, 4-й квартал) и других значимых событий.

Примечание. Значимыми событиями являются, например, выборы, крупные экономические, банковские форумы и другие массовые публичные мероприятия.

В нижней части страницы отобразится рейтинг. Если рейтинг превышает 1, нужно сообщить о мероприятии пресс-службу.

5. Нажмите кнопку **Сохранить**.

Рассчитанный рейтинг отобразится в строке публикации в общем списке публикаций.

16. Работа с участниками

Участник — это юридическое лицо, зарегистрированное в системе PT Incident Processing Center.

Участники могут быть следующих типов:

- Участники информационного обмена —подчиненные, подведомственные или дочерние организации, зарегистрированные в PT Incident Processing Center. Взаимодействие осуществляется через "Личный кабинет участника" и электронную почту.
- Системные участники — антивирусные лаборатории, контрагенты информационной безопасности, регистраторы, хостинг-провайдеры и ГосСОПКА. Взаимодействие осуществляется через электронную почту.
- Неучаствующие организации — прочие организации, зарегистрированные в центре. Взаимодействие осуществляется через электронную почту.

Вы можете добавить участника в систему из электронной формы в запросе или вручную, заполнив карточку участника. Набор обязательных полей карточки участника зависит от типа участника.

Вы можете заблокировать или активировать участника. Удалить участника из системы невозможно.

Карточка участника может содержать информацию об ответственных лицах организации. Вы можете добавлять ответственных лиц из электронной формы в запросе или вручную, заполнив карточку ответственного лица. Если требуется запретить ответственному лицу доступ к системе, вы можете его заблокировать. Удалить ответственное лицо из системы невозможно.

Система автоматически отправляет уведомления на групповые и входящие адреса электронной почты участников, а также на адреса электронной почты ответственных лиц. Эти уведомления могут содержать данные об изменении в запросе, о публикации бюллетеня или подтверждение, например о доставке сообщения. Подтверждения не отправляются системным участникам и неучаствующим организациям.

Для всех адресов электронной почты новых участников по умолчанию устанавливаются рекомендованные параметры уведомлений. Вы можете изменять параметры по умолчанию. Для всех новых адресов уже зарегистрированного в системе участника устанавливаются параметры уведомлений по умолчанию. Вы можете настраивать уведомления для каждого адреса отдельно.

В этом разделе

16.1. Добавление участника информационного обмена

► Чтобы добавить участника информационного обмена в систему:

1. В главном меню выберите раздел **Участники**.

   Откроется страница со списком участников.

2. В панели инструментов нажмите кнопку **Добавить участника**.

   Откроется страница **Новый участник**.

3. В раскрывающемся списке **Категория** выберите **Участник информационного обмена**.
4. В поле **Полное название** введите название организации.
5. В раскрывающемся списке **Важность** выберите важность участника.
6. В раскрывающемся списке **Организационно-правовая форма организации (ОКОПФ)** выберите организационно-правовую форму организации.
7. В поле **Групповые почтовые ящики** введите адреса электронной почты отделов информационной безопасности.
8. В поле **Ящик входящей почты** введите адреса электронной почты организации для получения сообщений от PT Incident Processing Center.
9. В раскрывающемся списке **Вид** выберите вид организации.
10. В раскрывающемся списке **Тип организации** выберите тип организации.
11. В поле **Регистрационный номер** введите регистрационный номер организации.
12. По ссылке **Добавить оператора** откройте окно **Добавление оператора связи**.
13. В поле **Название** введите название оператора связи или выберите название в списке.
14. В поле **IP-адреса** введите IP-адреса.
15. Нажмите кнопку **Сохранить**.
16. В поле **ИНН** введите идентификационный номер налогоплательщика.
17. В поле **КПП** введите код причины поставки на учет.
18. В поле **ОГРН** введите основной государственный регистрационный номер.
19. В поле **Юридический адрес** по ссылке **Указать адрес** откройте окно **Юридический адрес в формате ФИАС**.

20. В раскрывающемся списке **Страна** выберите страну юридического адреса организации.
21. Нажмите кнопку **Сохранить**.
22. В поле **Почтовый адрес** по ссылке **Указать адрес** откройте окно **Почтовый адрес в формате ФИАС**.
23. В раскрывающемся списке **Страна** выберите страну почтового адреса организации.
24. В поле **Фактический адрес** по ссылке **Указать адрес** откройте окно **Фактический адрес в формате ФИАС**.
25. В раскрывающемся списке **Страна** выберите страну фактического адреса организации.
26. Нажмите кнопку **Сохранить**.
27. В раскрывающемся списке **Отрасль** выберите отрасль организации.
28. В раскрывающемся списке **Тип используемой криптографии** выберите тип шифрования для переписки с участником (**ГОСТ** — по умолчанию, **GPG**, **Не используется**).
29. Если требуется, введите дополнительную информацию (см. раздел 5.9.2).
30. Нажмите кнопку **Сохранить**.

Участник информационного обмена добавлен в систему.

См. также

Параметры участника (см. раздел 5.9.2)

16.2. Добавление системного участника

► Чтобы добавить системного участника в систему:

1. В главном меню выберите раздел **Участники**.

   Откроется страница со списком участников.
2. В панели инструментов нажмите кнопку **Добавить участника**.

   Откроется страница **Новый участник**.
3. В поле **Категория** выберите **Системный участник**.
4. В поле **Полное название** введите название организации.
5. В раскрывающемся списке **Важность** выберите важность участника.
6. В поле **Групповые почтовые ящики** введите адреса электронной почты отделов информационной безопасности.
7. В поле **Ящик входящей почты** введите адреса электронной почты организации для получения сообщений от PT Incident Processing Center.

8. В раскрывающемся списке **Вид** выберите вид организации.
9. В раскрывающемся списке **Тип используемой криптографии** выберите тип шифрования для переписки с участником (**ГОСТ** — по умолчанию, **GPG**, **Не используется**).
10. Если требуется, введите дополнительную информацию (см. раздел 5.9.2).
11. Нажмите кнопку **Сохранить**.

Системный участник добавлен в систему.

16.3. Добавление неучаствующей организации

► Чтобы добавить неучаствующую организацию в систему:

1. В главном меню выберите раздел **Участники**.

   Откроется страница со списком участников.
2. В панели инструментов нажмите кнопку **Добавить участника**.

   Откроется страница **Новый участник**.
3. В поле **Категория** выберите **Неучаствующая организация**.
4. В поле **Полное название** введите название организации.
5. В раскрывающемся списке **Важность** выберите важность участника.
6. В поле **Групповые почтовые ящики** введите адреса электронной почты отделов информационной безопасности.
7. В поле **Ящик входящей почты** введите адреса электронной почты организации для получения сообщений от PT Incident Processing Center.
8. В раскрывающемся списке **Вид** выберите вид организации.
9. Если требуется, введите дополнительную информацию (см. раздел 5.9.2).
10. Нажмите кнопку **Сохранить**.

Неучаствующая организация добавлена в систему.

16.4. Добавление ответственного лица

► Чтобы добавить ответственное лицо в систему:

1. В главном меню выберите раздел **Участники**.

   Откроется страница со списком участников.
2. По ссылке с названием участника, для которого вы хотите добавить ответственное лицо, откройте карточку участника.
3. На вкладке **Ответственные лица** в панели инструментов нажмите кнопку **Добавить**.

Откроется окно **Добавление ответственного лица**.

4. В блоке параметров **ФИО** введите фамилию, имя и отчество ответственного лица.
5. В поле **Должность** введите должность ответственного лица.
6. В раскрывающемся списке **Категория** выберите категорию ответственного лица.

   Вы можете выбрать несколько категорий для одного ответственного лица.
7. В поле **Логин** введите логин ответственного лица.

   Примечание. После добавления ответственного лица в систему вы не сможете изменить логин ответственного лица.
8. По кнопке **Сгенерировать** сгенерируйте пароль для первого входа в "Личный кабинет участника".
9. Если требуется, в блоке параметров **Права** измените права ответственного лица.
10. В поле **Эл. почта** введите адрес электронной почты ответственного лица.
11. В поле **Городской телефон** введите номер городского телефона ответственного лица.
12. В поле **Мобильный телефон** введите номер мобильного телефона ответственного лица.
13. Нажмите кнопку **Сохранить**.

Ответственное лицо добавлено в систему.

Если вы предоставили ответственному лицу доступ к "Личному кабинету участника", необходимо отправить ему учетные данные для входа.

16.5. Отправка учетных данных ответственному лицу

► Чтобы отправить ответственному лицу учетные данные для входа в "Личный кабинет участника":

1. В главном меню выберите раздел **Участники**.

   Откроется страница со списком участников.
2. По ссылке с названием участника откройте карточку участника.
3. На вкладке **Ответственные лица** выберите ответственное лицо.
4. В панели инструментов нажмите кнопку **Отправить учетные данные** и подтвердите отправку.

Учетные данные отправлены на адрес электронной почты, указанный в карточке ответственного лица.

16.6. Настройка уведомлений по умолчанию

Примечание. Рекомендуется использовать рекомендованные параметры уведомлений.

► Чтобы настроить уведомления по умолчанию:

1. В главном меню выберите раздел **Участники**.

   Откроется страница со списком участников.

2. По ссылке с названием участника откройте карточку участника, для которого вы хотите настроить уведомления по умолчанию.

3. На вкладке **Уведомления** в панели инструментов нажмите кнопку **Настройки по умолчанию**.

   Откроется окно **Настройки по умолчанию**.

4. Измените необходимые параметры.

5. Нажмите кнопку **Сохранить**.

Уведомления по умолчанию настроены.

Измененные параметры уведомлений будут установлены только для новых адресов участника.

16.7. Установка рекомендованных параметров уведомлений

Если параметры уведомлений по умолчанию были изменены, вы можете установить рекомендованные параметры.

► Чтобы установить рекомендованные параметры уведомлений:

1. В главном меню выберите раздел **Участники**.

   Откроется страница со списком участников.

2. По ссылке с названием участника откройте карточку участника, для которого вы хотите установить рекомендованные параметры уведомлений.

3. На вкладке **Уведомления** в панели инструментов нажмите кнопку **Настройки по умолчанию**.

   Откроется окно **Настройки по умолчанию**.

4. Нажмите кнопку **Установить рекомендованные значения**.

5. Нажмите кнопку **Сохранить**.

Рекомендованные параметры уведомлений установлены.

Рекомендованные параметры уведомлений будут установлены только для новых адресов участника.

16.8. Настройка уведомлений для адреса

Вы можете настраивать уведомления для любого адреса электронной почты участника.

► Чтобы настроить уведомления для адреса электронной почты:

1. В главном меню выберите раздел **Участники**.

   Откроется страница со списком участников.

2. По ссылке с названием участника откройте карточку участника, для адреса которого вы хотите настроить уведомления.
3. Выберите вкладку **Уведомления**.
4. Выберите адрес электронной почты.
5. Нажмите кнопку **Редактировать**.

   Откроется окно **Редактирование настроек эл. почты**.

6. Измените необходимые параметры:
   - **Уведомления об изменениях**;
   - **Уведомления-подтверждения**;
   - **Полное содержимое**: включает в почтовые уведомления полный текст сообщений и файлы рассылок.

     Вариант **Только бюллетени** включает полный текст (например, описание) только в уведомления о публикации бюллетеня.

   - **Уведомления о публикации фидов**.
7. Нажмите кнопку **Сохранить**.

Уведомления для адреса настроены.

► Чтобы сбросить параметры уведомлений адреса электронной почты до параметров по умолчанию:

1. В таблице адресов электронной почты выберите адрес.
2. Нажмите кнопку **Сбросить настройки эл. почты** и подтвердите операцию.

Параметры уведомлений для адреса электронной почты сброшены до параметров по умолчанию.

Примечание. Администратор участника в "Личном кабинете участника" может настраивать уведомления для почтовых ящиков участника. Изменения, сделанные администратором участника, отобразятся в карточке участника.

16.9. Шифрование переписки

PT Incident Processing Center поддерживает шифрование сообщений электронной почты между участниками и центром по стандартам ГОСТ (российская криптография) и по стандарту GPG. Использование стандарта GPG позволяет зарубежным участникам поддерживать защищенную переписку с центром. Для одного участника может быть выбран один тип криптографии: ГОСТ или GPG.

Тип криптографии для переписки с участником выбирает оператор в центре.

Выбрать тип криптографии для переписки с участником можно в карточке участника, в раскрывающемся списке **Тип используемой криптографии**. Если не предполагается использовать шифрование сообщений, в списке должен быть выбран вариант **Не используется**. В этом случае сообщения между участником и центром отправляются без электронной подписи и не шифруются.

По умолчанию для всех участников выбран тип криптографии ГОСТ.

Для использования криптографии GPG предварительно должны быть выполнены следующие действия:

— Участник создает пару ключей GPG-шифрования (публичный и закрытый) и предоставляет публичный ключ в центр.

— Администратор в центре создает пару ключей GPG-шифрования (публичный и закрытый), настраивает в системе закрытый ключ для шифрования сообщений и передает открытый ключ участнику.

  Создание GPG-ключей и обмен публичными ключами между центром и участником по умолчанию выполняется вне системы, с использованием внешних средств и ресурсов.

17. Работа с антифродом

Примечание. Сведения об операциях без согласия указывают участники, которым в рамках их деятельности необходимо фиксировать и обрабатывать такую информацию.

Примечание. Функция скачивания фидов доступна при наличии модуля "Фид-Антифрод". Модуль используется для организаций финансовой отрасли, которым необходима эта функция.

Антифрод — компонент PT Incident Processing Center, предназначенный для создания прототипа централизованной базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента и обеспечения возможности получения кредитными организациями информации из этой базы данных.

Работа с антифродом состоит из следующих шагов:

1. Кредитная организация, у клиента которой был осуществлен перевод денежных средств без его согласия (далее также — КО-заявитель), регистрирует запрос об операции без согласия в PT Incident Processing Center.
2. PT Incident Processing Center формирует карточку операции без согласия и направляет запрос кредитной организации, клиенту которой был осуществлен перевод (далее также — КО-получатель), о предоставлении данных получателя. Эти операции осуществляются автоматически.
3. КО-получатель, получив запрос о предоставлении данных получателя, заполняет электронную форму уведомления об операции и отправляет ее в PT Incident Processing Center.
   КО-заявителю автоматически отправляется электронная форма отчета о приостановлении зачисления средств.
4. КО-получатель, получив запрос о предоставлении данных получателя, заполняет электронную форму уведомления об операции и отправляет ее в PT Incident Processing Center.
5. PT Incident Processing Center автоматически дополняет карточку операции без согласия информацией о получателе из электронной формы, полученной от КО-получателя.

PT Incident Processing Center позволяет выгружать файлы с фидам. Фид — это обновляемые данные о получателях денежных средств. Фиды могут содержать следующие данные:

— хеш-суммы номеров и серий паспортов;

— хеш-суммы СНИЛС;

— ИНН;

— номера телефонов;

— номера счетов;

— номера платежных карт;

— номера электронных кошельков;

— счет SWIFT;

— Retail/ATM;

— другое.

В фиды поступают данные получателей денежных средств только из актуальных обработанных операций. При этом количество денежных переводов от разных плательщиков одному получателю должно быть не менее количества, указанного в конфигурационном файле (по умолчанию — два).

В фиды не поступают данные получателей, которые вернули денежные средства или если КО-получатель подтвердила законность перевода. Также в фиды не поступают данные, добавленные в белые списки.

Правила попадания данных получателей в фиды может быть изменено администратором системы в конфигурационном файле. Если правило для типа или атрибута фида не задано, то валидация не выполняется.

При выгрузке фидов в файл система валидирует их согласно правилам, указанным в конфигурационном файле. Если хотя бы один атрибут фида содержит невалидное значение, то фид не попадает в файл. Если правило для типа или атрибута фида не задано, то валидация не выполняется.

В этом разделе

17.1. Обновление фидов

Система автоматически обновляет фиды по заданному расписанию. Изменение расписания публикации фидов доступно только администратору системы.

Вы можете обновлять фиды вручную, например, перед публикацией.

► Чтобы обновить фиды:

1. В главном меню в разделе **Антифрод** выберите **Операции без согласия**.

   Откроется страница со списком операций без согласия.

2. В панели инструментов нажмите кнопку **Информация о фидах**.

Откроется окно **Информация о фидах**.

3. Нажмите кнопку **Перезалить фиды**.

Фиды обновлены.

17.2. Публикация фидов

Вы можете публиковать фиды, чтобы распространить информацию о злоумышленниках участникам.

► Чтобы опубликовать фиды:

1. В главном меню в разделе **Антифрод** выберите **Операции без согласия**.

   Откроется страница со списком операций без согласия.

2. В панели инструментов нажмите кнопку **Информация о фидах**.

   Откроется окно **Информация о фидах**.

3. Нажмите кнопку **Опубликовать**.

Фиды опубликованы.

17.3. Запрос информации об актуальности операции без согласия

Система позволяет запросить информацию об актуальности операции без согласия у кредитных организаций (КО) плательщика и получателя платежа:

— у КО получателя — критерии легитимности получателя;

— у КО плательщика — аналитическую форму операции.

Можно запрашивать информацию об операциях с любой актуальностью, но наиболее полезна эта функция для операций с актуальностью **Требует ручного контроля**. На основе информации, полученной от кредитной организации, система автоматически пересчитывает актуальность операции.

► Чтобы запросить информацию об актуальности операции без согласия:

1. В списке установите флажки напротив операций, с которыми нужно выполнить действие.

2. В панели инструментов нажмите кнопку с раскрывающимся списком **Запросить информацию** и выберите вариант запроса в кредитную организацию:

   - **получателя и плательщика**;
   - **получателя**;

- **плательщика**.

Запрос об актуальности отправлен. Отображается всплывающее сообщение об отправке запроса. Статус операции в списке изменяется на **Ожидает ответа**.

Операторы кредитных организаций, указанных в запросе, получают электронную форму запроса по операции. Если по каким-либо критериям операции без согласия передавали информацию раньше, поля этих критериев в форме заполнены. Операторы добавляют данные в форму и отправляют ее обратно.

На основе полученных критериев система пересчитывает актуальность операции и обновляет ее. Если актуальность опять спорная, операция остается в статусе **Требует ручного контроля**. В этом случае вы можете либо самостоятельно принять решение об актуальности и изменить актуальность вручную, либо запросить информацию повторно. Количество запросов не ограничено.

17.4. Групповые действия с операциями без согласия: повторная обработка, изменение статуса, экспорт

Система позволяет выполнять групповые действия с операциями без согласия:

— изменять актуальность (например, для операций с актуальностью **Требует ручного контроля**);

— повторно обрабатывать операции со статусом **Ошибка**, после внесения каких-либо изменений в системе, затрагивающих их обработку (например, обработку операций без согласия после указания БИК и БИН).

— экспортировать список выбранных операций в json-файл.

► Чтобы изменить актуальность операций:

1. В главном меню в разделе **Антифрод** выберите пункт **Операции без согласия**.

   Откроется страница со списком операций.

2. В списке установите флажки напротив операций, с которыми нужно выполнить действие.

3. По кнопке **Сменить актуальность** в панели инструментов измените актуальность выбранных операций.

   Отобразится всплывающее уведомление об изменении актуальности.

Актуальность изменена.

► Чтобы повторно обработать операции со статусом **Ошибка**:

1. В списке установите флажки напротив операций, с которыми нужно выполнить действие.

2. В панели инструментов нажмите кнопку **Повторно обработать**.

Система попытается обработать операции.

Если обработка завершена успешно, статус операций в списке изменится с **Ошибка** на **Обработано**.

► Чтобы экспортировать операции в json-файл:

1. В списке установите флажки напротив операций, с которыми нужно выполнить действие.
2. В панели инструментов нажмите кнопку **Экспорт**.
3. Система экспортирует json-файл со значениями из электронных форм выбранных операций в папку для загрузки вашего браузера.

   Операции содержатся в том порядке, в каком они были выбраны в списке.

Экспорт операций завершен.

17.5. Уведомление участников о публикации новой версии фидов

Вы можете включать и выключать уведомление для участников о публикации новой версии фидов. Если уведомление включено, при публикации участник по почте и в "Личном кабинете участника" получает уведомление с текстом "Опубликована новая версия фидов".

► Чтобы включить уведомление о публикации новой версии фидов для участника:

1. В главном меню выберите раздел **Участники**.

   Откроется страница со списком участников.
2. По ссылке с названием участника откройте карточку участника, для которого вы хотите включить уведомление.
3. На вкладке **Уведомления** в панели инструментов нажмите кнопку **Настройки по умолчанию**.

   Откроется окно **Настройки по умолчанию**.
4. В полях **Отправлять уведомления о публикации новой версии фидов** и **Отправлять ответственным лицам уведомления о публикации новой версии фидов** нажмите кнопку **Отправлять**.
5. Нажмите кнопку **Сохранить**.

Уведомление включено.

18. Работа со справочниками

На странице **Справочники** представлены названия сущностей, к которым привязаны справочники. Например, **Отраслевая и другая принадлежность**.

В рабочей области отображается список значений, относящихся к выбранной сущности, и подробная информация о выбранном значении.

При необходимости панели можно скрывать и отображать.

С помощью кнопок **Добавить**, **Редактировать** и **Удалить** вы можете дополнять и изменять содержимое справочников.

> **Примечание.** Для некоторых справочников изменение недоступно. Например, для справочника **Категории ответственных лиц**.

В этом разделе

18.1. Справочник Адреса

Справочник **Адреса** содержит адреса субъектов и реквизиты документов. Справочник **Адреса** позволяет автоматически определять адрес организации по ее реквизитам при добавлении субъекта. Для использования этого справочника требуется загрузить базу данных федеральной информационной адресной системы (ФИАС).

> **Примечание.** При первом входе в PT Incident Processing Center справочник **Адреса** пуст.

18.2. Справочник Операторы связи

Справочник **Операторы связи** содержит названия операторов связи.

Система предлагает названия из справочника, если вы добавляете оператора связи в карточке участника или электронной форме участника.

18.3. Работа с шаблонами сообщений

Шаблоны сообщений — это типовые тексты, которые вы можете использовать для написания сообщений в запросах (см. раздел 8), например чтобы не вводить повторяющуюся информацию вручную. В шаблонах вы можете использовать переменные (см. раздел 18.3.3), которые в тексте сообщения будут заменены на данные из запроса.

В этом разделе

18.3.1. Создание шаблона сообщения

Для создания шаблонов требуются права на изменение справочников.

► Чтобы создать шаблон:

1. В главном меню в разделе **Система** выберите пункт **Справочники**.
2. В меню слева выберите **Шаблоны сообщений** → **Запросы**.
3. Нажмите кнопку **Добавить**.
4. В раскрывающемся списке **Тип запроса** выберите тип запроса, шаблон для которого вы хотите добавить.

   Указание типа требуется для возможности фильтровать шаблоны при их поиске в запросах и не влияет на то, в каком запросе можно использовать шаблон.
5. В поле **Название** введите название шаблона.
6. В поле **Сообщение** введите текст шаблона.

   Вы можете использовать переменные (см. раздел 18.3.3).
7. Нажмите кнопку **Сохранить**.

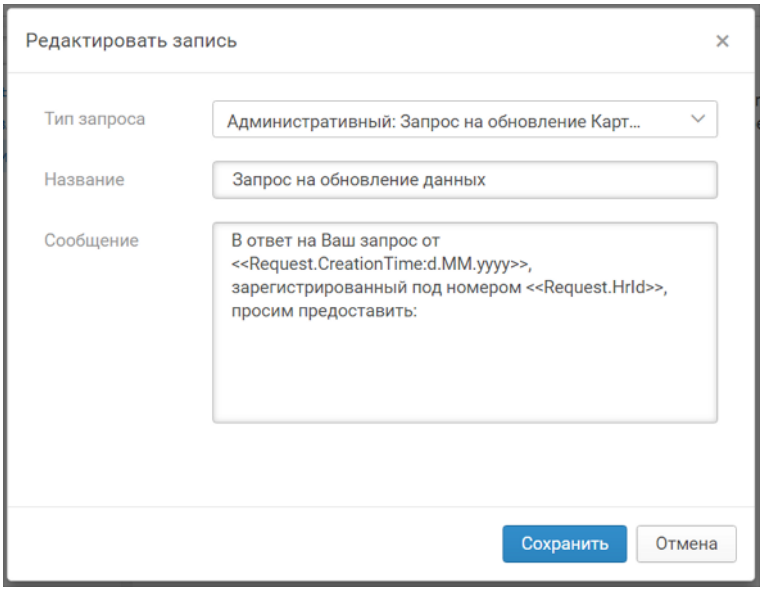

Рисунок 18. Добавление шаблона сообщения

18.3.2. Использование шаблонов сообщений в запросах

Вы можете использовать шаблоны сообщений при создании или изменении запроса.

► Чтобы использовать шаблон сообщений в запросе:

1. На странице **Запросы** выберите запрос.
2. В открывшейся карточке запроса нажмите кнопку **Шаблоны**.
3. В открывшемся окне **Шаблоны сообщений** выберите шаблон и нажмите кнопку **Использовать шаблон**.

Шаблон вставлен в текст сообщения запроса.

Если вы используете несколько шаблонов в запросе, то их текст вставляется в сообщение поочередно сверху вниз.

18.3.3. Переменные в шаблонах сообщений

При создании шаблонов вы можете использовать переменные (см. таблицу ниже), которые в тексте сообщения будут заменены на данные из запроса. Переменная обрамляется двойными треугольными скобками, например `<<Request.ParticipantId>>`. Переменные являются регистрозависимыми. Если переменная введена неверно, то при использовании в тексте сообщения вместо нее не будет выводиться ничего.

Если вы создаете новый запрос, а не отвечаете на сообщение в рамках существующего запроса, то значения некоторых переменных (например, `Request.HrId`) недоступны, так как они могут присваиваться только после создания запроса.

Для переменных, в которых указывается время (`Request.CreationTime`, `Request.LastModified`, `Request.ResponseDeadline`), вы можете через двоеточие задать формат времени, например `Request.LastModified:YYYY.MM.dd`.

Пример шаблона с использованием переменных:

```
В ответ на ваш запрос от <<Request.CreationTime:dd.MM.yyyy>>, зарегистрированный под
номером <<Request.HrId>>, просим предоставить следующую информацию.
```

Пример сообщения в запросе, в котором использован этот шаблон:

```
В ответ на ваш запрос от 13.12.2019, зарегистрированный под номером REQ-20191213-06,
просим предоставить следующую информацию.
```

Таблица 2. Переменные в шаблонах сообщений

Переменная	Значение	Значение доступно при создании запроса
`Request.Id`	Внутренний идентификатор запроса	+
`Request.HrId`	Идентификатор запроса	–

Переменная	Значение	Значение доступно при создании запроса
`Request.ParticipantId`	Идентификатор участника (если участник выбран)	+
`Request.Category`	Категория запроса	+
`Request.Type`	Тип запроса	При создании запроса вместо переменной будет подставлен тип запроса. При ответе на существующий запрос — JSON-объект `Value: <Тип>`
`Request.Type.Value`	Тип запроса	+
`Request.Transport`	Способ получения	+
`Request.CreationTime`	Время получения	+
`Request.AssignedTo`	Логин пользователя, на которого назначен запрос (если назначен)	–
`Request.Status`	Статус	+
`Request.Priority`	Приоритет	+
`Request.ResponseDeadline`	Крайний срок ответа на запрос	–
`Request.Subject`	Название запроса (тип и идентификатор)	+
`Request.LastModified`	Время последнего обновления запроса	+
`Request.InitialMessage.CreatorId`	Идентификатор пользователя, создавшего первое сообщение в запросе	–
`Request.Messages[<Порядковый номер сообщения, начиная с 0>].CreatorId`	Идентификатор пользователя, создавшего выбранное сообщение	+
`Request.InitialMessage.Body`	Содержимое первого сообщения	–
`Request.Messages[<Порядковый номер сообщения, начиная с 0>].Body`	Содержимое выбранного сообщения	+
`Request.InitialMessage.Attachments.AttachmentType`	Тип вложения первого сообщения	–

Переменная	Значение	Значение доступно при создании запроса
`Request. Messages[<Порядковый номер сообщения, начиная с 0>].Attachments.AttachmentType`	Тип вложения выбранного сообщения	+

19. Работа с рассылкой центра

Вы можете формировать рассылку из карточек инцидентов или угроз, а также создавать новую рассылку. Новая рассылка может быть создана на основе любой существующей рассылки и быть ее копией или отличаться от нее.
Вы можете изменять или удалять неопубликованные рассылки. Опубликованную рассылку невозможно изменить, удалить или отозвать.

Для быстрого поиска рассылки вы можете добавить ей метку (см. раздел 21.1.1).

Существуют несколько способов рассылки.

Рассылка всем участникам

Рассылка отправляется всем участникам на адреса электронной почты, указанные в поле **Ящик входящей почты** карточки участника. Ответственные лица участников информационного обмена получают рассылку на адреса электронной почты, указанные в карточке ответственного лица и в "Личном кабинете участника". Кроме того, ответственные лица получают уведомления о поступлении новой рассылки в "Личном кабинете участника".

Рассылка выбранным участникам

Рассылка отправляется только выбранным участникам на адреса электронной почты, указанные в поле **Ящик входящей почты** карточки участника. Ответственные лица выбранных участников получают рассылку на адреса электронной почты, указанные в карточке ответственного лица, и в "Личном кабинете участника". Кроме того, ответственные лица получают уведомления о поступлении новой рассылки в "Личном кабинете участника".

Рассылка группе участников

Группы рассылок бывают статические (созданный вручную набор участников) и динамические (в группу попадают участники, соответствующие определенному признаку). Система поддерживает динамические группы рассылок по виду и типу организации, например, всем организациям, относящимся к типу "Оператор по переводу денежных средств".

Рассылка отправляется добавленным в группу участникам на адреса электронной почты, указанные в поле **Ящик входящей почты** карточки участника, и на адреса электронной почты отдельно указанных лиц. Ответственные лица добавленных в группу участников получают рассылку на адреса электронной почты, указанные в карточке ответственного лица, и в "Личном кабинете участника". Кроме того, ответственные лица получают уведомления о поступлении новой рассылки в "Личном кабинете участника".

При создании рассылки можно комбинировать указанные способы: например, добавлять к получателям рассылки и группы пользователей, и отдельных пользователей, указанных вручную.

Примечание. Рассылка отправляется только участникам информационного обмена, ответственным лицам и на адреса электронной почты отдельно указанных лиц. Рассылка не будет отправлена системным участникам, неучаствующим организациям и заблокированным ответственным лицам.

Вы можете настраивать группы рассылки (см. раздел 19.3).

В этом разделе

19.1. Создание рассылки

► Чтобы создать рассылку:

1. В главном меню в разделе **База знаний** выберите пункт **Рассылки центра**.

   Откроется страница со списком рассылок.

2. В панели инструментов нажмите кнопку **Добавить рассылку**.

   Откроется окно **Создание новой рассылки**.

3. В поле **Заголовок** введите наименование рассылки.
4. В поле **ID рассылки** введите идентификатор рассылки.
5. В поле **Краткое описание** введите краткое содержание рассылки.
6. В раскрывающемся списке **Тип рассылки** выберите тип рассылки.
7. В раскрывающемся списке **Подтип рассылки** выберите подтип рассылки.
8. В раскрывающемся списке **Шаблон** выберите название шаблона, на основании которого должен быть создан рассылаемый документ.

   В поле **Исходный файл** появится ссылка на файл, сгенерированный при помощи выбранного шаблона.

9. Скачайте файл по ссылке в поле **Исходный файл** и при необходимости измените его содержимое.
10. В поле **Публикуемый файл** перетащите или выберите рассылаемый вариант исходного файла.

    Вы также можете приложить к рассылаемому документу дополнительные материалы, выбрав их в поле **Дополнительные публикуемые файлы**.

11. В блоке **Получатели рассылки** выберите получателей рассылки.
12. Нажмите кнопку **Сохранить**.

Рассылка создана.

19.2. Формирование рассылки на основе инцидента или угрозы

► Чтобы сформировать рассылку на основе инцидента или угрозы:

1. Откройте карточку объекта.
2. В панели инструментов нажмите кнопку **Сформировать рассылку**.

   Откроется окно **Создание новой рассылки**.
3. Если требуется, измените данные рассылки.
4. Нажмите кнопку **Сохранить**.

Рассылка создана.

19.3. Добавление группы рассылки

► Чтобы добавить группу рассылки:

1. В главном меню в разделе **База знаний** выберите пункт **Рассылки центра**.

   Откроется страница **Рассылки центра**.
2. В панели инструментов нажмите кнопку **Добавить получателей**.

   Откроется окно **Добавить получателей рассылки**.

   По ссылке **Редактировать группы рассылки** откройте окно **Группы рассылки**.
3. В панели инструментов нажмите кнопку **Добавить группу**.

   Откроется окно **Новая группа рассылки**.
4. В поле **Название группы** введите название группы.
5. Укажите получателей рассылки.

   Если в поле **Тип** выбран тип группы **Статическая**, в полях **Участники** и **Другие адресаты** следует указать получателей, которые войдут в создаваемую статическую группу рассылки.

   Если выбран тип группы **Динамическая**, в блоке параметров **Кого включать в группу** следует указать типы и (или) виды организаций, которые войдут в создаваемую динамическую группу и будут иметь доступ к рассылке.
6. Нажмите кнопку **Сохранить**.

Группа рассылки добавлена.

При публикации рассылки для определенной динамической группы все активные участники с типами и видами организации, соответствующими группе, получают уведомление и доступ к рассылке. Новые или измененные участники (изменился тип, вид или статус участника) имеют доступ к ранее опубликованной рассылке, если их тип или вид равен указанным в рассылке, и они являются активными.

19.4. Публикация рассылки

Внимание! Опубликованную рассылку нельзя изменить или отозвать.

► Чтобы опубликовать рассылку:

1. В главном меню в разделе **База знаний** выберите пункт **Рассылки центра**.

   Откроется страница **Рассылки центра**.

2. В таблице рассылок выберите неопубликованную рассылку и в панели инструментов нажмите кнопку **Опубликовать**.

   Откроется окно **Публикация рассылки**.

3. Проверьте данные и нажмите кнопку **Опубликовать**.

Рассылка опубликована.

Вы не можете повторно опубликовать рассылку, но вы можете отправить опубликованную рассылку новым получателям.

► Чтобы отправить опубликованную рассылку новым получателям:

1. В главном меню в разделе **База знаний** выберите пункт **Рассылки центра**.

   Откроется страница **Рассылки центра**.

2. В таблице рассылок выберите опубликованную рассылку и в панели инструментов нажмите кнопку **Добавить получателей**.

   Откроется окно **Добавить получателей рассылки**.

3. Добавьте получателей рассылки.
4. Нажмите кнопку **Опубликовать**.

Рассылка отправлена только новым получателям.

20. Работа с Центром уведомлений

Центр уведомлений информирует о событиях в работе системы. Вы можете просматривать краткую информацию о последних событиях в Центре уведомлений по нажатию на значок в главном меню.

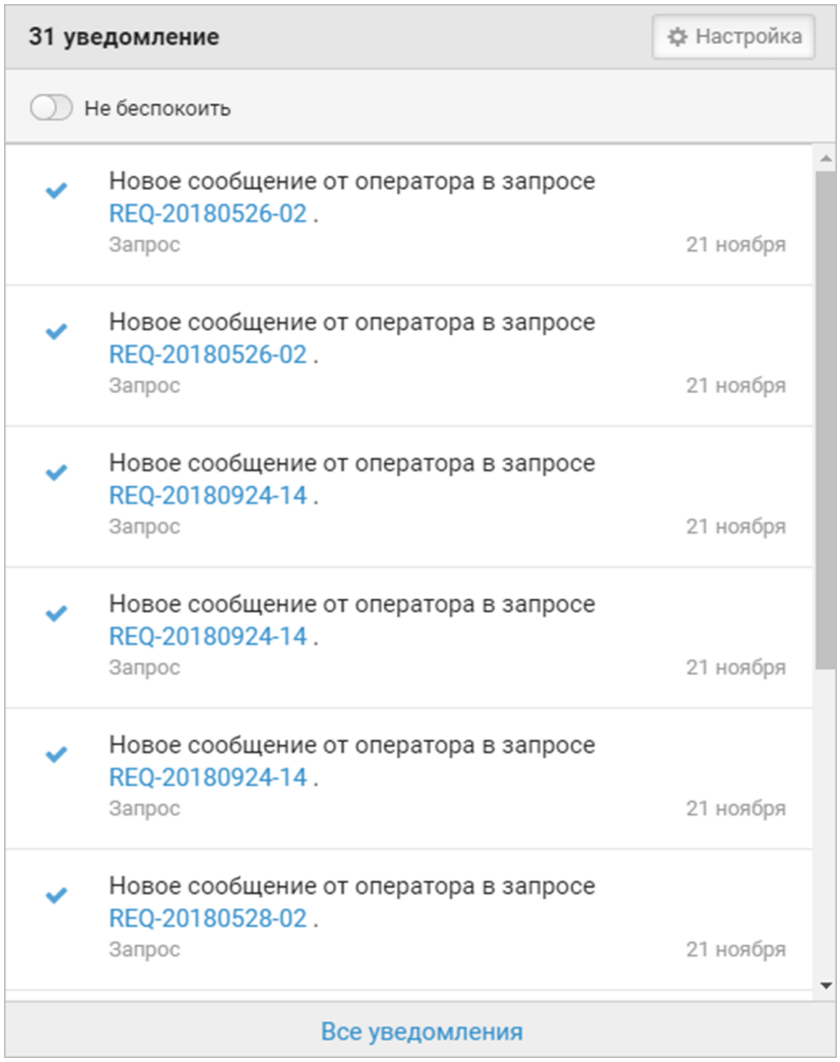

Рисунок 19. Центр уведомлений

Вы можете перейти в карточку объекта по ссылке с идентификатором объекта.

Кроме того, вы можете открыть страницу со списком всех уведомлений по ссылке **Все уведомления**.

На странице со списком всех уведомлений вы можете:

— просматривать подробную информацию о событии;

— переходить в карточку объекта;

— фильтровать события;

- отмечать уведомления как прочитанные;
- удалять уведомления.

21. Типовые действия с объектами системы

Для большинства объектов системы предусмотрены типовые действия, позволяющие упростить и ускорить работу с объектами. К таким действиям относятся:

— добавление метки;

— просмотр истории изменений;

— добавление комментария;

— добавление связи с другим объектом;

— назначение объекта на пользователя.

Примечание. При назначении объекта в системе на пользователя для выбора доступны только пользователи, учетные записи которых в системе активны. Нельзя назначить объект на пользователя, учетная запись которого заблокирована.

Вы можете выполнять типовые действия с объектом в панели с дополнительной информацией, расположенной в правой части рабочей области страницы объекта.

В этом разделе

21.1. Работа с метками

Вы можете присваивать объектам ключевые слова для быстрого поиска данных — метки.

Метка может содержать буквы русского или английского алфавитов, цифры и спецсимволы. Длина метки не должна превышать 255 символов. Метка не зависит от регистра символов.

Вы можете добавлять метки следующим объектам: запросам, инцидентам, задачам, бюллетеням, угрозам, уязвимостям, информационным карточкам.

В этом разделе

21.1.1. Добавление метки

► Чтобы добавить метку:

1. Откройте карточку объекта, которому вы хотите добавить метку.
2. По ссылке **Редактировать метки** откройте окно **Метки**.

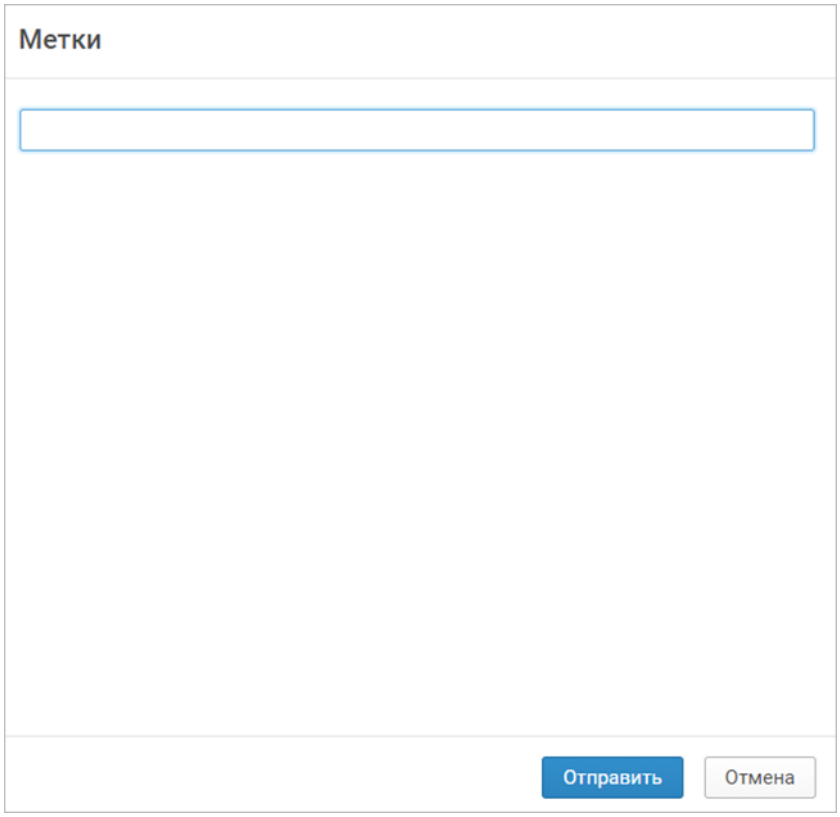

Рисунок 20. Добавление метки

3. Введите метку.
4. Нажмите кнопку **Создать <Метка>**.

   Примечание. Вы можете добавить несколько меток.
5. Нажмите кнопку **Отправить**.

Метка добавлена.

21.1.2. Поиск объектов по меткам

► Чтобы найти объекты по меткам:

1. В главном меню нажмите .

Откроется поле поиска по меткам.

2. Введите одну или несколько меток и нажмите Enter.

   На странице **Поиск по меткам** отобразится список объектов, содержащих введенные метки.

21.2. Работа со связями

При создании объекта из карточки другого объекта система автоматически формирует связь. Например, если из карточки запроса в систему был добавлен (на основе электронной формы) инцидент, то система автоматически свяжет этот инцидент с запросом. Связь будет добавлена в карточки обоих объектов. Автоматически сформированную связь удалить нельзя.

В системе предусмотрена возможность создавать дополнительные связи между объектами вручную. Такие связи можно создавать для всех объектов, кроме операций без согласия. Дополнительную связь можно удалить.

Система отображает связи в виде дерева. Такая структура позволяет просматривать связи всех представленных на вкладке **Связи** объектов, не переходя в карточки объектов.

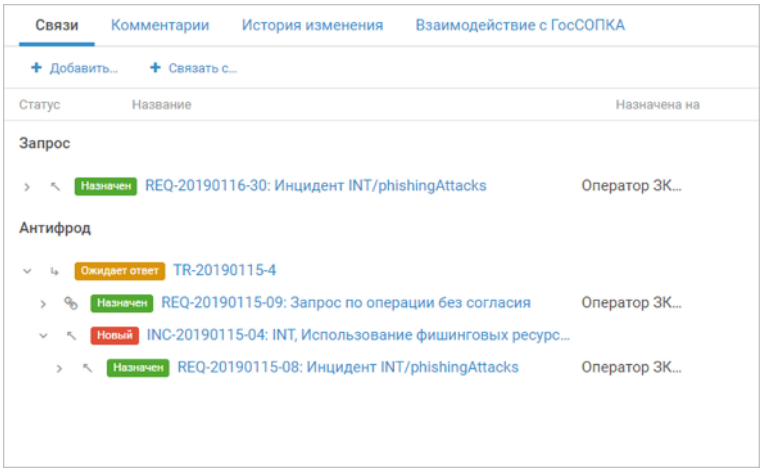

Рисунок 21. Вкладка **Связи**

В этом разделе

21.2.1. Добавление связи между объектами

► Чтобы добавить связь между объектами:

1. В главном меню выберите раздел, в котором содержится объект, который вы хотите связать с другим объектом системы.

Откроется страница со списком объектов.

2. По ссылке с идентификатором объекта откройте карточку объекта.
3. В панели с дополнительной информацией, расположенной в правой части рабочей области, нажмите кнопку **Связать с**.

   Откроется окно **Связать с другим объектом**.
4. В поле поиска введите идентификатор, название или описание объекта.
5. В раскрывающемся списке выберите тип объекта.

   PT Incident Processing Center сформирует таблицу объектов, удовлетворяющих параметрам поиска.
6. Выберите объект в таблице и нажмите кнопку **Добавить связь**.

Связь между объектами добавлена.

21.2.2. Удаление связи между объектами

Вы можете удалять только дополнительные связи, которые были добавлены вручную.

► Чтобы удалить связь между объектами:

1. В главном меню выберите раздел, в котором содержится объект, у которого вы хотите удалить связь с другим объектом.

   Откроется страница со списком объектов.
2. По ссылке с идентификатором объекта откройте карточку объекта.
3. В панели с дополнительной информацией, расположенной в правой части рабочей области, на вкладке **Связи** скопируйте идентификатор объекта, связь с которым вы хотите удалить.
4. Нажмите кнопку **Связать с**.

   Откроется окно **Связать с другим объектом**.
5. В поле поиска вставьте идентификатор объекта.
6. В раскрывающемся списке выберите тип объекта, связь с которым вы хотите удалить.

   PT Incident Processing Center осуществит поиск по указанным вами параметрам и отобразит найденный объект.
7. Нажмите кнопку **Удалить связь**.

Связь между объектами удалена.

21.3. Добавление комментария к объекту

Вы можете добавлять комментарии в карточке следующих объектов:

- запросы;
- задачи;
- инциденты;
- информационные карточки;
- бюллетени;
- угрозы;
- уязвимости;
- участники.

► Чтобы добавить комментарий к объекту:

1. В главном меню выберите раздел, в котором содержится объект, к которому вы хотите добавить комментарий.

   Откроется страница со списком объектов.

2. По ссылке с идентификатором объекта откройте карточку объекта.
3. В панели с дополнительной информацией, расположенной в правой части рабочей области, на вкладке **Комментарии** в поле **Написать комментарий** введите комментарий к объекту.
4. Нажмите кнопку **Добавить**.

Комментарий к объекту добавлен в карточку объекта.

21.4. Просмотр истории изменений объекта

Вы можете просматривать историю изменения следующих объектов:

- запросы;
- задачи;
- инциденты;
- информационные карточки;
- бюллетени;
- угрозы;
- уязвимости;
- участники.

► Чтобы просмотреть историю изменения объекта:

1. В главном меню выберите раздел, в котором содержится объект, историю изменения которого вы хотите просмотреть.

   Откроется страница со списком объектов.

2. По ссылке с идентификатором объекта откройте карточку объекта.
3. В панели с дополнительной информацией, расположенной в правой части рабочей области, откройте вкладку **История изменения**.

   Откроется страница с историей изменения объекта.

21.5. Передача URL и доменных имен в антивирусную лабораторию

Вы можете получить подробную информацию о любом URL или доменном имени (см. раздел 11.4) и проанализировать ее. Если по итогам анализа вы решите, что URL или домен являются вредоносными, вы можете передать их в антивирусную лабораторию, которая включит его в свои базы.

► Чтобы передать URL или доменное имя в антивирусную лабораторию:

1. В карточке объекта нажмите кнопку с URL или доменным именем.

   Откроется окно, содержащее общие сведения, регистрационные данные и сведения об уровне опасности.

2. Нажмите кнопку **Еще** и в раскрывшемся меню выберите пункт **Сообщить участнику**.

   Откроется форма регистрации нового запроса с типом "Передача URL в антивирусные лаборатории". URL или доменное имя будут записаны в текстовый файл и запакованы в зашифрованный архив.

   Примечание. Вы можете узнать пароль архива у администратора PT Incident Processing Center.

3. В раскрывающемся списке **Участник** выберите название антивирусной лаборатории, в которую нужно отправить URL или доменное имя.
4. В раскрывающемся списке **Способ получения** выберите **Другое**.
5. Если вам нужно передать дополнительную информацию о URL или доменном имени, заполните остальные поля формы.
6. Нажмите кнопку **Зарегистрировать запрос**.

   Запрос зарегистрирован. Вы можете его закрыть (см. раздел 8.8).

21.6. Просмотр связей артефакта с объектами Cybsi

Вы можете просматривать связи артефакта в объекте PT Incident Processing Center (например, URL) с объектами в Cybsi. Такое обогащение артефакта выполняет компонент cybsilinker. Администратор системы настраивает cybsilinker во время интеграции системы с Cybsi. Ниже приведена инструкция по просмотру связей на примере инцидента.

► Чтобы просмотреть связи артефакта с объектами Cybsi:

1. В главном меню в разделе **Инциденты** выберите пункт **Инциденты**.
2. По ссылке с идентификатором инцидента откройте карточку инцидента.
3. В карточке инцидента нажмите артефакт (например, URL или IP-адрес), для которого хотите просмотреть связи в Cybsi.

   Откроется окно **<Имя артефакта>**.
4. Выберите вкладку **cybsilinker**.

На вкладке в виде ссылок отобразятся обнаруженные связи артефакта с объектами Cybsi. Вы можете перейти по ссылкам в Cybsi и просмотреть информацию об обнаруженных объектах.

21.7. Публикация новостей для операторов

Вы можете публиковать общие новости, доступные всем операторам центра, а также адресные новости, которые доступны выбранным операторам.

► Чтобы опубликовать новость:

1. В главном меню выберите раздел **Новости**.
2. Откроется страница **Добавить новость**.
3. В поле **Заголовок** укажите заголовок новости.
4. В поле **Получатели** выберите операторов, которым адресована новость.
5. В поле **Ссылки на объекты системы** добавьте ссылки на объекты, относящиеся к новости.
6. В поле **Текст новости** введите текст.
7. Нажмите кнопку **Опубликовать новость**.

Новость опубликована.

Операторы-получатели новости увидят ее в уведомлениях системы. Система также отправляет новость на электронную почту получателя.

21.8. Добавление правил YARA и Snort в бюллетени

PT Incident Processing Center позволяет уведомлять участников информационного обмена об обнаружении опасного артефакта (URL, IP-адреса, доменного имени, файла и т. п.). При этом вы можете написать правило в формате YARA или Snort с упоминанием этого артефакта в коде правила и разослать его участникам информационного обмена в виде бюллетеня. Участники могут использовать полученное правило для автоматической блокировки вредоносной активности. В PT Incident Processing Center существует возможность автоматической генерации подобных правил из шаблонов. После настройки шаблонов данные о том или ином артефакте будут автоматически добавляться в код правил. Вы можете копировать правила из окна информации об артефакте.

► Чтобы добавить правило YARA или Snort в бюллетень:

1. В карточке объекта выберите артефакт, для которого вы хотите добавить правило в бюллетень.

   Откроется окно артефакта.

2. В открывшемся окне выберите вкладку **rules**.

3. Нажмите кнопку .

   Правило для выбранного артефакта будет скопировано в буфер обмена.

4. Добавьте это правило в бюллетень для рассылки (см. раздел 19.1).

22. SLA для действий с сущностями в системе

SLA (Service Level Agreement) в общем случае — это соглашение об уровне сервиса. SLA содержит список оказываемых услуг и значения метрик качества оказания этих услуг.

С помощью SLA в PT Incident Processing Center можно настраивать требования к действиям пользователя в системе, важным для бизнес-процессов. Такими действиями, например, могут быть:

— расследование инцидента;

— ответ на сообщение от участника информационного обмена;

— проверка приложенного файла на наличие вредоносного ПО.

В PT Incident Processing Center метрикой качества является время выполнения пользователями этих действий. Поэтому SLA для каждого действия содержит максимальное время, за которое пользователь должен выполнить это действие.

Система считает SLA выполненным, если пользователь завершил действие за время, не превышающее указанное в SLA.

Для каждого действия с сущностью можно указать несколько значений времени в зависимости от атрибута сущности. Например, на предоставление рекомендаций по инциденту со средним уровнем опасности может быть выделено 2 дня, с высоким уровнем опасности — 2 часа.

Администратор системы может настраивать правила SLA: добавлять новые, изменять и удалять ранее добавленные правила. Изменение или удаление правил не влияют на те SLA, которые в момент изменения была назначены. Эти SLA должны быть выполнены с предыдущими значениями времени.

SLA связанных действий

Некоторые действия с сущностями в системе не может выполнить только один пользователь. Такие действия могут быть назначены на других пользователей, а также порождать другие действия со своими SLA.

Связанные действия могут выполнять одновременно разные пользователи, или один пользователь не сможет выполнить действие до тех пор, пока связанное действие не выполнит другой пользователь. В последнем случае время выполнения связанного действия не должно влиять на время выполнения основного действия.

Например, аналитик ИБ должен расследовать инцидент с высокой опасностью за 2 часа.

Через 1 час после начала расследования аналитик выясняет, что данных, предоставленных участником информационного обмена, недостаточно. Аналитик создает связанную с инцидентом задачу на получение данных у участника и назначает ее на сотрудника первой линии поддержки. Расследование инцидента приостанавливается до тех пор, пока не будет выполнена эта задача.

Для задач на получение данных установлено SLA в 4 часа. Сотрудник первой линии за это время связывается с участником и получает необходимые данные, добавляет данные в инцидент и отмечает задачу как выполненную.

Аналитик ИБ возвращается к расследованию инцидента. У него остается 1 час для принятия решения.

SLA действий, выполняемых одновременно

Пользователь одновременно может выполнять с сущностью разные действия, для которых в SLA определено разное время выполнения.

Например, расследование инцидента с типом "Использование вредоносного ПО" должно быть выполнено за 1 день. В ходе расследования аналитик ИБ должен выполнить следующие действия:

- Проверить приложенный к инциденту файл на наличие вредоносного ПО. Время выполнения SLA — 2 часа.
- Если проверка покажет, что файл содержит вредоносное ПО, то заблокировать ресурс, рассылающий такие файлы. Время выполнения SLA — 4 часа.
- При любом результате проверки предоставить решение по инциденту. Время выполнения SLA — 1 час.

История расследования этого инцидента может выглядеть так:

1. 8:00 — инцидент назначен на аналитика ИБ. Аналитик приступает к расследованию. На инцидент назначены 2 SLA: расследование инцидента и проверка на наличие вредоносного ПО.
2. 9:00 — аналитик проверил файл и обнаружил в нем вредоносное ПО. На инцидент назначены 2 SLA: расследование инцидента и блокировка ресурса, рассылающего вредоносное ПО.
3. 11:00 — аналитик заблокировал ресурс. На инцидент назначены 2 SLA: расследование инцидента и предоставление решения по инциденту.
4. 11:30 — аналитик предоставил решение по инциденту. Все SLA выполнены.

Время выполнения SLA

Временем начала действия пользователя с сущностью является время назначения SLA на сущность.

Временем завершения действия пользователя с сущностью является время, когда система присваивает SLA состояние "Выполнено".

Время, когда SLA находился в состоянии "Приостановлено", не учитывается во времени выполнения действия.

Уведомление о скором истечении времени выполнения SLA

Система позволяет настраивать сценарии уведомления пользователей:

— операторов, на которых назначены сущности с истекающим SLA.

— менеджеров о скором истечении SLA для сущностей.

Уведомления могут отправляться по электронной форме и SMS, а также отображаться в интерфейсе.

Сортировка сущностей по состояниям SLA

Сущности можно сортировать в интерфейсе по состояниям SLA.

Сначала отображаются сущности, для которых SLA находится в состоянии "Выполняется" (то есть действие, для которого определено SLA, находится в процессе выполнения). Такие сущности отсортированы по уменьшению разницы между фактическим временем выполнения действия и временем выполнения SLA.

Пример отсортированного списка таких сущностей:

— Инцидент 1: время выполнения действия 5 часов, время выполнения SLA — 2 часа.

— Инцидент 2: время выполнения действия 5 часов, время выполнения SLA — 6 часов.

— Инцидент 3: время выполнения действия 5 часов, время выполнения SLA — 10 часов.

Затем отображаются сущности, для которых SLA находится в состоянии "Выполнено" или "Приостановлено".

Если для сущности назначено несколько SLA, то для сортировки используется SLA в состоянии "Выполняется" с максимальной разницей между фактическим временем выполнения действия и временем выполнения SLA.

Приложение А. Приоритеты запросов и инцидентов

Приоритет запроса зависит от вида организации, типа инцидента, нанесенного ущерба и необходимости помощи PT Incident Processing Center.

В PT Incident Processing Center существуют следующие приоритеты:

🔴 — критический;

🟡 — очень высокий;

🔵 — высокий;

🔵 — средний;

🔵 — низкий.

Таблица 3. Выбор приоритета запроса или инцидента для участников информационного обмена

Вид инцидента	Ущерб, негативное воздействие	Помощь PT Incident Processing Center	КО	Значимые	СЗКО	ПС	НКО	Страховые TOP-10	Страховые не TOP-10	МФО, инвестиционные фонды ломбарды	Остальные источники
Инциденты с вектором INT											
Вредоносное ПО (MLW)	есть	требуется	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔵	🔵
	есть	не требуется	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔵	🔵

Вид инцидента	Ущерб, негативное воздействие	Помощь РТ Incident Processing Center	КО	Значимые	СЗКО	ПС	НКО	Страховые ТОР-10	Страховые не ТОР-10	МФО, инвестиционные фонды ломбарды	Остальные источники
	нет	требуется	🟡	🟡	🟡	🟡	🔵	🔵	🔵	🔵	⚪
	нет	не требуется	⚪	⚪	⚪	⚪	⚪	⚪	⚪	⚪	⚪
DoS или DDo-атаки (DOS)	есть	требуется	🔴	🔴	🔴	🔴	🔵	🔵	🔵	🔵	🔵
	есть	не требуется	🟡	🟡	🟡	🟡	⚪	⚪	⚪	⚪	⚪
	нет	требуется	🔵	🔵	🔵	🔴	⚪	⚪	⚪	⚪	⚪
	нет	не требуется	⚪	⚪	⚪	⚪	⚪	⚪	⚪	⚪	⚪
Физическая атака на банкомат (BAN)	есть	требуется	🔵	🔵	🔵	-	🔵	🔵	🔵	🔵	-
	есть	не требуется	🔵	🔵	🔵	-	🔵	🔵	🔵	🔵	-
	нет	требуется	🔵	🔵	🔵	-	🔵	🔵	🔵	🔵	-
	нет	не требуется	⚪	⚪	⚪	-	⚪	⚪	⚪	⚪	-

Вид инцидента	Ущерб, негативное воздействие	Помощь РТ Incident Processing Center	КО	Значимые	СЗКО	ПС	НКО	Страховые TOP-10	Страховые не TOP-10	МФО, инвестиционные фонды ломбарды	Остальные источники
Фишинг (мошенничество) (PHI)	есть	требуется	🔵	🔴	🔴	🔴	🔵	🟡	🔵	🔵	•
	есть	не требуется	🔵	🟡	🔴	🔴	🔵	🟡	🔵	🔵	•
	нет	требуется	🔵	🟡	🔴	🔴	🔵	🟡	🔵	🔵	•
	нет	не требуется	•	•	•	🔵	🔵	🔵	•	•	•
Социальная инженерия (SOI)	есть	требуется	•	🟡	🟡	🟡	🟡	🟡	🟡	•	•
	есть	не требуется	•	🟡	🟡	🟡	🟡	🟡	🟡	•	•
	нет	требуется	🔵	🟡	🔴	🔴	🔵	🟡	🔵	🔵	🔵
	нет	не требуется	•	•	•	🔵	🔵	🔵	•	•	•
Эксплуатация уязвимостей (EXP)	есть	требуется	🟡	🟡	🟡	🔵	🔵	🔵	🟡	•	◦
	есть	не требуется	🔵	🔵	🔵	🔵	🔵	🔵	🔵	◦	◦
	нет	требуется	•	•	•	•	•	•	•	◦	◦

Вид инцидента	Ущерб, негативное воздействие	Помощь РТ Incident Processing Center	КО	Значимые	СЗКО	ПС	НКО	Страховые TOP-10	Страховые не TOP-10	МФО, инвестиционные фонды ломбарды	Остальные источники
	нет	не требуется	●	●	●	●	●	●	●	●	●
Перебор паролей (BRF)	есть	требуется	●	●	●	●	●	●	●	●	●
	есть	не требуется	●	●	●	●	●	●	●	●	●
	нет	требуется	●	●	●	●	●	●	●	●	●
	нет	не требуется	●	●	●	●	●	●	●	●	●
INT-SCN Выявление попыток сканирования портов для взлома сети	есть	требуется	●	●	●	●	●	●	●	●	●
	есть	не требуется	●	●	●	●	●	●	●	●	●
	нет	требуется	●	●	●	●	●	●	●	●	●
	нет	не требуется	●	●	●	●	●	●	●	●	●

Вид инцидента	Ущерб, негативное воздействие	Помощь PT Incident Processing Center	КО	Значимые	СЗКО	ПС	НКО	Страховые TOP-10	Страховые не TOP-10	МФО, инвестиционные фонды ломбарды	Остальные источники
Другой инцидент с вектором INT (OTH)	есть	требуется	🔵	🔵	🔵	🔵	🔵	🔵	🔵	⚪	⚪
	есть	не требуется	🔵	🔵	🔵	🔵	🔵	🔵	🔵	⚪	⚪
	нет	требуется	⚪	⚪	⚪	⚪	⚪	⚪	⚪	⚪	⚪
	нет	не требуется	⚪	⚪	⚪	⚪	⚪	⚪	⚪	⚪	⚪
Инциденты с вектором EXT											
Атака с подменой номера (SIM)	есть	требуется	🔵	🔴	🔴	🔴	🔵	🟡	🔵	🔵	🔵
	есть	не требуется	🔵	🟡	🔴	🔴	🔵	🟡	🔵	🔵	🔵
	нет	требуется	🔵	🟡	🔴	🔴	🔵	🟡	🔵	🔵	🔵
	нет	не требуется	🔵	🔵	🔵	🔵	🔵	🔵	🔵	🔵	⚪
Утрата электронного	есть	требуется	🔵	🔴	🔴	🔴	🔵	🟡	🔵	🔵	🔵
	есть	не требуется	🔵	🟡	🔴	🔴	🔵	🟡	🔵	🔵	🔵
	нет	требуется	🔵	🟡	🔴	🔴	🔵	🟡	🔵	🔵	🔵

Вид инцидента	Ущерб, негативное воздействие	Помощь РТ Incident Processing Center	КО	Значимые	СЗКО	ПС	НКО	Страховые TOP-10	Страховые не TOP-10	МФО, инвестиционные фонды ломбарды	Остальные источники
средства платежа (LST)	нет	не требуется	🔵	🔵	🔵	🔵	🔵	🔵	🔵	🔵	🔹
Вредоносное ПО (MLW)	есть	требуется	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔵	🔵
	есть	не требуется	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🔵	🔵
	нет	требуется	🟡	🟡	🟡	🟡	🔵	🔵	🔵	🔵	🔹
	нет	не требуется	🔹	🔹	🔹	🔹	🔹	🔹	🔹	🔹	🔹
Социальная инженерия (SOI)	есть	требуется	🔵	🔴	🔴	🔴	🔵	🟡	🔵	🔵	🔵
	есть	не требуется	🔵	🔵	🔵	🔵	🔵	🔵	🔵	🔵	🔹
	нет	требуется	🔵	🟡	🔴	🔴	🔵	🟡	🔵	🔵	🔵
	нет	не требуется	🔵	🔵	🔵	🔵	🔵	🔵	🔵	🔵	🔹

Вид инцидента	Ущерб, негативное воздействие	Помощь PT Incident Processing Center	КО	Значимые	СЗКО	ПС	НКО	Страховые TOP-10	Страховые не TOP-10	МФО, инвестиционные фонды ломбарды	Остальные источники
Фишинговый ресурс (P2P)	есть	требуется	🔵	🔴	🔴	🔴	🔵	🟡	🔵	🔵	🔹
	есть	не требуется	🔹	🔵	🟡	🟡	🔹	🔵	🔹	🔹	⚪
	нет	требуется	🔵	🟡	🔴	🔴	🔵	🟡	🔵	🔵	🔹
	нет	не требуется	🔹	🔹	🔹	🔵	🔵	🔵	🔹	🔹	⚪
Другой инцидент с вектором EXT (OTH)	есть	требуется	🔵	🔴	🔴	🔴	🔵	🟡	🔵	🔵	🔹
	есть	не требуется	🔹	🔵	🔵	🔵	🔹	🔵	🔹	🔹	⚪
	нет	требуется	🔵	🟡	🔴	🔴	🔵	🟡	🔵	🔵	🔹
	нет	не требуется	⚪	⚪	⚪	⚪	⚪	⚪	⚪	⚪	⚪
Другое											
PUB информация о планируемых ме-	-	-	-	🔹	🔵	🟡	🟡	🔵	🔹	⚪	⚪

Вид инцидента	Ущерб, негативное воздействие	Помощь РТ Incident Processing Center	КО	Значимые	СЗКО	ПС	НКО	Страховые TOP-10	Страховые не TOP-10	МФО, инвестиционные фонды ломбарды	Остальные источники
роприятиях по раскрытию информации об инцидентах, связанных с нарушением требований защиты информации при переводах ДС											

Таблица 4. Выбор приоритета запроса или инцидента для системных участников

Организация	Помощь PT Incident Processing Center	Приоритет для всех типов запросов
ГосСОПКА	-	🔴
CERT (Россия)	-	🟡
Антивирусная лаборатория	-	🟡
Контрагенты информационной безопасности	-	🟡
Международные сообщества (EAST EGAF, FIRST)	-	🔵
Регистраторы	-	🔵
Информационные объекты, относящиеся к другим информационным объектам / инцидентам	требуется	на один уровень ниже приоритета первичного объекта / инцидента
Информационные объекты, относящиеся к другим информационным объектам / инцидентам	не требуется	соответствует уровню приоритета первичного объекта / инцидента
Разработчики автоматизированных банковских систем	-	🔵

О компании

"Позитив Текнолоджиз" — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения "Позитив Текнолоджиз" для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты "Позитив Текнолоджиз" заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com