R-Vision

Программный комплекс «Р-Вижн ЭВО»

Руководство пользователя.

Версия 1.01

Настоящий документ является собственностью ООО "Р-Вижн" и защищен законодательством Российской Федерации об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения ООО "Р-Вижн".

Документ может быть изменен без предварительного уведомления.

ОГЛАВЛЕНИЕ

1. Логическая структура и возможности системы «программный комплекс «Р-Вижн ЭВО» 10

2. Начало работы с системой 11
2.1. Авторизация и вход в систему.... 11
2.2. Документация 11
2.3. Интерфейс системы 12
2.4. Выход из системы 12

3. Настройка системы....13
3.1. О разделе Настройки 13
3.2. Подготовка к использованию системы.... 13
3.3. Управление лицензией.... 14
3.4. Настройка организаций 14

3.4.1. Добавление организации 15

3.4.2. Параметры организации для обмена данными с системой ГосСОПКА 17

3.4.3. Описание организации - субъекта КИИ....17

3.4.4. Банковская деятельность....18

3.4.5. Настройка организации для доступа в ФинЦЕРТ....19

3.4.6. Удаление организаций 20

3.4.7. Просмотр организаций 21
3.5. Настройка учетной записи текущего пользователя: мой профиль 21
3.6. Настройка подключения к домену 23
3.7. Установка обновлений системы.... 24
3.8. Обслуживание системы.... 25

4. Коллекторы 28
4.1. Добавление коллектора 28
4.2. Обновление коллектора.... 30
4.3. Управление HTTPS-режимом коллектора.... 30

5. Активы 32
5.1. О модуле активов 32
5.2. Подготовка к работе с активами 32
5.3. Типы активов.... 33

5.3.1. Бизнес-процессы 33

5.3.2. Помещения....36

5.3.3. Информация 37

5.3.4. Оборудование 38

5.3.5. ПО....42

5.3.6. Персонал....44

5.3.7. Подразделение/Организация 46
5.3.8. Сети 48
5.3.9. Пользовательские типы активов 49
5.4. Настройка полей описания активов 51
5.5. Работа со схемой взаимосвязей бизнес-процессов 53
6. Инциденты 55
6.1. О модуле инцидентов 55
6.2. Подготовка к работе с модулем 55
6.3. Создание инцидента 56
6.3.1. Создание инцидента вручную 57
6.3.2. Создание инцидента по шаблону 59
6.3.3. Создание инцидента из уязвимости группы ИТ-активов 60
6.3.4. Создание инцидента в группе 60
6.3.5. Создание инцидента из уязвимости вручную 61
6.3.6. Создание инцидента из меню ПО вручную 62
6.3.7. Создание инцидента из данных по протоколу syslog 63
6.4. Изменение инцидента: особенности 63
6.4.1. Изменение ответственного за инцидент 64
6.4.2. Изменение категории инцидента 64
6.5. Просмотр инцидента 64
6.6. Действия по реагированию на инцидент 65
6.6.1. Просмотр действий по инциденту 66
6.6.2. Просмотр прогресса выполнения действий по инциденту 68
6.6.3. Модификаторы полей-массивов 68
6.7. Настройка доступа к инциденту: рабочая группа 68
6.8. Описание инцидента 70
6.8.1. Описание инцидента: добавление комментариев 71
6.8.2. Описание инцидента: индикаторы 71
6.8.3. Описание инцидента: почтовая переписка 72
6.8.4. Описание инцидента: файлы свидетельств 77
6.8.5. Описание инцидента: причины возникновения 79
6.8.6. Описание инцидента: параметры 040203 79
6.8.7. Описание инцидента: ФинЦЕРТ 80
6.9. Отправка уведомлений в ГосСОПКА 81
7. Уязвимости 83

7.1. Принцип работы с уязвимостями ... 83
7.2. Добавление уязвимостей ... 83
7.2.1. Добавление уязвимости вручную в интерфейсе ... 84
7.3. Просмотр уязвимостей ... 85
7.3.1. Карточка уязвимости ... 85
7.3.2. Связанное оборудование ... 85
7.3.3. Просмотр статистики по уязвимостям ... 86
7.3.4. Фильтрация списка уязвимостей ... 87
7.3.5. Сквозной поиск ... 87
7.4. Действия по уязвимостям ... 88
7.4.1. Открытие уязвимости ... 88
7.4.2. Признание ложным срабатыванием ... 89
7.4.3. Принятие риска ... 89
7.4.4. Закрытие уязвимости ... 90
7.4.5. Создание вручную задачи ... 91
7.4.6. Создание вручную инцидента ... 91
7.5. Статусы уязвимостей ... 92
8. Аудиты ... 93
8.1. О функциональном блоке “Аудиты” ... 93
8.2. Подготовка к работе с разделом Аудит ... 94
8.3. Настройка требований для проведения аудита ... 94
8.3.1. Создание комплекса требований ... 95
8.3.2. Добавление новых требований к комплексу ... 96
8.3.3. Формирование списка контрольных проверок для требования ... 97
8.3.4. Настройка полей требований ... 97
8.3.5. Импорт комплекса требований ... 98
8.4. Настройка аудитов ... 99
8.4.1. Простые аудиты: настройка шкалы оценок ... 99
8.4.2. Простые и сводные аудиты: настройка дополнительных полей ... 100
8.4.3. Простые аудиты: настройка статусов ... 101
8.5. Проведение простых аудитов ... 102
8.5.1. Простой аудит: создание ... 103
8.5.2. Простой аудит: просмотр ... 106
8.5.3. Простой аудит: расширенный режим просмотра оценки ... 106

8.5.4. Простой аудит: рабочая группа 107
8.5.5. Простой аудит: проведение оценки соответствия 107
8.5.6. Простой аудит: расчет показателей оценки соответствия 109
8.5.7. Простой аудит: проведение аудита на основании оценки контрольных проверок 110
8.5.8. Простой аудит: просмотр результатов 111
8.6. Сводная оценка простых аудитов 112
8.6.1. Сводная оценка: просмотр 112
8.6.2. Сводная оценка: создание 114
8.6.3. Сводная оценка: рабочая группа 116
8.6.4. Сводная оценка: настройка методики расчета итогового показателя 117
8.7. Устранение замечаний по аудиту 118
8.7.1. Добавление мероприятия по устранению замечания 119
8.7.2. Изменение статуса мероприятий по устранению 120
8.7.3. Связь мероприятий с активами 121
8.7.4. Связь мероприятий с задачами 121
8.7.5. Связь мероприятий с замечаниями 122
8.7.6. Связь мероприятий с требованиями 122
8.7.7. Связь мероприятий с аудитами 122
9. Риски 124
9.1. О функциональном блоке Риски 124
9.2. Подготовка к работе с рисками 125
9.3. Настройка параметров для работы с рисками 126
9.4. Настройка каталогов угроз 128
9.4.1. Создание нового каталога угроз 128
9.4.2. Копирование каталога угроз 129
9.4.3. Добавление угроз в каталог 130
9.4.4. Добавление источников в каталог 130
9.4.5. Добавление предпосылок в каталог 131
9.5. Управление мерами защиты 131
9.5.1. Добавление меры защиты 131
9.5.2. Меры защиты: режимы отображения 133
9.6. Проведение оценки рисков 133
9.6.1. Этап 1. Создание оценки 134

9.6.2. Этап 2. Идентификация рисков 137
9.6.3. Этап 3. Оценка рисков 139
9.6.4. Этап 4. Обработка рисков 143
9.6.5. Этап 5. Формирование отчетности 148
9.6.6. Этап 6. Журнал 149
9.6.7. Проведение оценки угроз по требованиям ФСТЭК 149
9.7. Просмотр сводной информации по рискам 150
10. Функциональный блок Имитации ИТ-инфраструктуры 152
10.1. Наполнение ловушек 152
10.1.1. Генерация логинов 152
10.1.2. Генерация паролей 153
10.1.3. О наполнении ловушек 154
10.2. Работа с ловушками 154
10.2.1. Добавление ловушек 155
10.2.2. О ловушках 158
10.2.3. Просмотр ловушек 159
10.3. Работа с графиками 159
10.3.1. Об отображении данных 159
10.3.2. Просмотр данных на дашборде 160
10.4. Работа с приманками 160
10.4.1. Добавление приманок 160
10.4.2. О приманках 161
10.4.3. Просмотр и удаление приманок 162
10.4.4. Размещение приманок на пользовательском хосте (Win, MacOS, Linux) 163
10.5. Работа с сетями 164
10.5.1. Добавление сетей 164
10.5.2. О сетях 165
10.5.3. Просмотр информации о сети 165
10.6. Добавление ложных учетных записей 165
10.7. Мониторинг событий 167
10.7.1. Аудит событий 167
10.7.2. Просмотр событий 167
11. Мониторинг и анализ событий безопасности 168
11.1. Интерфейс блока 168

11.1.1. Главное окно 168
11.1.2. Элементы рабочей области 168
11.2. Настройка обнаружения 169
11.2.1. Добавление ноды 169
11.2.2. Добавление сенсора 170
11.2.3. Настройка ротации данных ноды 170
11.2.4. О сенсорах 170
11.3. Индикаторы 171
11.3.1. Мониторинг индикаторов компрометации 171
11.3.2. Настройка правила обогащения 171
11.3.3. Настройка правил обнаружения 172
11.3.4. Об индикаторах компрометации 173
11.3.5. Обогащение индикатора 174
11.3.6. Просмотр списка индикаторов 175
11.3.7. Работа с карточкой индикатора 177
11.4. Угрозы 178
11.4.1. Об угрозах 178
11.4.2. Просмотр, редактирование и удаление угроз 181
11.4.3. Просмотр списка угроз 182
11.5. Аналитические отчеты 186
11.5.1. Автоматизация создания аналитических отчетов 186
11.5.2. Просмотр списка аналитических отчетов 186
11.6. Пользовательские теги 187
12. Поведенческий анализ объектов защиты 188
12.1. Просмотр уведомлений 188
12.2. Просмотр объектов наблюдения 189
12.2.1. Об объектах наблюдения 189
12.2.2. Просмотр информации об объекте 189
12.2.3. Настройка списка объектов наблюдения 193
12.3. Корреляция данных - настройка простых правил 193
12.3.1. Включение и выключение простого правила 193
12.3.2. Добавление правил корреляции 194
12.4. Программные эксперты: обучение и анализ данных 196
12.4.1. Настройка параметров обучения системы 196

12.4.2. Первичное обучение системы 198
12.4.3. Управление экспертами 198
12.5. Просмотр сводных данных 199
12.5.1. Добавление виджета на дашборд 200
12.5.2. Добавление дашборда 202
12.5.3. Просмотр данных на дашбордах 203
13. Защита конечных точек 204
13.1. Работа с компонентом 204
13.1.1. Работа с агентами 204
13.1.2. Настройка сбора данных журналов из файлов, событий Windows и чтения команд. 206
13.1.3. Создание группы агентов 208
13.1.4. Технический аудит агентов 209
13.2. Настройка синхронизации 211
13.2.1. Настройка поиска IoC на хостах с установленными агентами 211

1. ЛОГИЧЕСКАЯ СТРУКТУРА И ВОЗМОЖНОСТИ СИСТЕМЫ «ПРОГРАММНЫЙ КОМПЛЕКС «Р-ВИЖН ЭВО»

Для решения поставленных перед ИБ-подразделением задач структура системы «Программный комплекс «Р-Вижн ЭВО» (далее – ЭВО) логически состоит из функциональных блоков, каждый из которых отвечает за реализацию определенного процесса управления ИБ:

- Блок активов обеспечивает управление активами организации и их взаимосвязями, позволяет проводить сканирование сети с целью контроля за состоянием ИТ-инфраструктуры.
- Блок уязвимостей обеспечивает анализ и управление уязвимостями обнаруженными системой при сканировании оборудования.
- Блок инцидентов обеспечивает централизованный сбор и хранение информации по инцидентам ИБ.
- Блок аудитов обеспечивает деятельность по контролю за соблюдением требований ИБ и позволяет проводить оценку соответствия отраслевым и законодательным требованиям.
- Блок рисков обеспечивает формирование модели угроз и управление рисками информационной безопасности.
- Блок имитации ИТ-инфраструктуры обеспечивает цифровую имитацию объектов ИТ-инфраструктуры для раннего обнаружения злоумышленников, проникших в корпоративную сеть, и предотвращения атак на ранних этапах.
- Блок мониторинга и анализа событий безопасности собирает, обрабатывает и обогащает индикаторы компрометации, получаемые из доступных источников.
- Блок поведенческого анализа объектов защиты детектирует нарушения в состоянии систем, подозрительную активность объектов, осуществляет динамическую оценку угроз и аномалий, а также собирает и хранит события ИБ.
- Блок защиты конечных точек обеспечивает установку агентов на конечные устройства с целью выявления угроз и осуществления реагирования на эти угрозы.

2. НАЧАЛО РАБОТЫ С СИСТЕМОЙ

В этом разделе описаны действия для начала работы с системой.

- Авторизация и вход в систему
- Документация
- Интерфейс системы
- Выход из системы

2.1. Авторизация и вход в систему

После установки и настройки веб-интерфейс системы доступен по ссылке: `http://<ip-адрес виртуальной машины>` или `http://<dns-имя сервера>`, если внесена соответствующая A-запись на DNS-сервере.

После перехода по ссылке в окне браузера отобразится окно авторизации. Для выполнения авторизации и входа в систему укажите логин и пароль учетной записи пользователя и нажмите на кнопку **Войти**.

Если в настройках добавлены сторонние системы для авторизации, то пользователь может войти в систему с помощью своей учетной записи во внешней системе. Доступные варианты входа отображаются в нижней части окна авторизации. Нажатие на кнопку отображает страницу авторизации внешней системы.

Если вход в систему выполнен успешно, то в окне браузера отобразится стартовый раздел системы.

Для первоначальной авторизации в системе используются следующие учетные данные:

- Логин: ***admin***
- Пароль: ***admin***

После первоначальной авторизации рекомендуется сменить пароль учетной записи администратора.

2.2. Документация

Перейдите в раздел **Настройки → Общие → Документация**, чтобы просмотреть Руководство пользователя системы.

2.3. Интерфейс системы

После успешной авторизации в браузере отобразится основное окно системы.

Интерфейс системы отображается в окне браузера.

В левой части окна расположена основная панель системы - панель навигации. Сущности системы логически организованы в разделы панели навигации. В верхней правой части окна отображаются уведомления, название учетной записи текущего пользователя и кнопка выхода из системы ().

В верхней части окна могут располагаться (если предусмотрены или созданы пользователем) другие панели: подразделы, вкладки фильтров, открытые в отдельных вкладках аудиты и инциденты, панели графиков.

Навигация по списку элементов и поиск элементов в списке выполняется с помощью полосы, расположенной в нижней части списка элементов.

Справа от списка расположена полоса с кнопками. Кнопки открывают разделы свойств элемента. Свойства открытого раздела отображаются в правой части окна.

2.4. Выход из системы

Чтобы выйти из системы, нажмите на кнопку  , расположенную справа от имени учетной записи в меню системы. Система завершит сеанс пользователя и на экране отобразится форма ввода логина и пароля. Вы можете осуществить повторный вход в систему с помощью той же или другой учетной записи.

При выходе из системы завершается текущая сессия учетной записи. Завершить все сессии учетной записи можно по кнопке **Выйти из всех сеансов** в разделе **Настройки → Общие → Мой профиль**.

3. НАСТРОЙКА СИСТЕМЫ

Вы можете настроить систему в соответствии с потребностями организации во вкладке **Настройки.** Настраиваемые параметры системы распределены по процессам управления информационной безопасностью.

- О разделе Настройки
- Подготовка к использованию системы
- Управление лицензией
- Настройка организаций
- Настройка учетной записи текущего пользователя: мой профиль
- Настройка подключения к домену
- Установка обновлений системы
- Обслуживание системы

3.1. О разделе Настройки

В разделе **Настройки** можно настроить параметры системы. Он отображает полный список настроек, доступных пользователю в соответствии с его ролью.

Раздел можно открыть, нажав на его название **Настройки системы** внизу панели навигации. В левой части экрана отобразится список настроек, сгруппированных по разделам.

Выше всех в списке находится раздел **Избранное.** Раздел появляется, если в него добавлена хотя бы одна настройка. Он отображает пользовательский список часто используемых настроек для быстрого доступа к ним. Настройки из общего списка можно добавить в **Избранное** по кнопке **Добавить в избранное** (☆) при выделении настройки в списке. Менять расположение настроек в **Избранном** можно, перетаскивая их мышью.

Над списком настроек находится строка поиска по названиям настроек. Развернуть и свернуть все разделы настроек можно, нажав на кнопки  и  рядом с полем поиска.

3.2. Подготовка к использованию системы

Для того, чтобы начать работу с системой, рекомендуется выполнить следующие подготовительные действия:

1. Заполните информацию об организации в разделе **Настройки → Общие → Организации**.

2. Создайте пользователей системы и назначьте им роли в разделе **Настройки → Общие → Пользователи системы → Пользователи.**
3. Задайте настройки почты для отправки уведомлений в разделе **Настройки → Общие → Настройки почты**.

Отредактировать параметры вашей учетной записи вы можете в разделе **Мой профиль**.

Указанный набор действия является минимальным. Остальные параметры настройки системы описаны в разделе **Настройка системы**.

3.3. Управление лицензией

В разделе **Лицензия** отображаются данные о лицензии продукта, функционале, который предоставляется по данной лицензии, и о сроке действия лицензии.

Чтобы загрузить лицензию,выполните следующие действия:

1. В правой части раздела **Настройки → Общие → Лицензия** нажмите на кнопку **Загрузить лицензию.**
2. Укажите путь к файлу лицензии.

Для получения лицензионного файла обратитесь в техническую поддержку по адресу support@rvision.com. Для генерации лицензии потребуется предоставить уникальный код, содержащийся в поле **SERVER-ID**.

3.4. Настройка организаций

В этом разделе вы можете настроить параметры одной или нескольких организаций, с которыми будет работать система. Если в системе существует несколько организаций, этот раздел называется **Организации**.

Вносить изменения в свойства организаций, добавлять и удалять организации могут только пользователи, в свойствах роли которых разрешен доступ к разделу **Сведения об организации** с правами на изменение, а также в свойствах учетной записи установлен флажок **Полный доступ** (доступен в режиме Multi-tenancy).

- Добавление организации
- Параметры организации для обмена данными с системой ГосСОПКА
- Описание организации - субъекта КИИ
- Банковская деятельность
- Настройка организации для доступа в ФинЦЕРТ
- Удаление организаций

- Просмотр организаций

3.4.1. Добавление организации

Вы можете добавить одну или несколько организаций в систему. Если в системе существуют несколько организаций, у всех объектов отображается обязательное свойство **Организация.**

Чтобы указать параметры организации, выполните следующие действия:

1. Перейдите в раздел **Настройки → Общие → Организации.**
2. Создайте организацию:
   a. Если вы хотите создать родительскую организацию: нажмите на кнопку **Создать** над списком. Организация будет корнем новой ветки иерархии.
   b. Если вы хотите создать дочернюю организацию: наведите курсор мыши на родительскую организацию и нажмите на кнопку ⊕. Система назначит выбранную организацию родительской по отношению к новой.
3. Заполните поля карточки:
   a. Полное наименование организации.
   b. Сокращенное наименование организации. Значение, указанное в поле **Сокращенное наименование**, будет использовано системой для упоминания этой организации в других разделах (в режиме Multi-tenancy).

      После создания второй организации все сущности (включая пользователей), существующие в системе, будут отнесены к исходной организации. В свойствах учетной записи пользователя, который создал вторую организацию, автоматически устанавливается флажок **Полный доступ**.

   c. Родительская организация (заполняется автоматически у дочерних организаций). Кнопка **Изменить** открывает окно выбора родительской организации. Кнопка **Изменить** доступна пользователям, которым разрешен доступ ко всем организациям.
   d. Фирменное наименование (бренд).

e. Ссылка на официальный сайт.

f. ИНН организации.

g. КПП организации.

4. Разверните разделы и заполните поля адреса:

   a. **Юридический адрес**.

   b. **Фактический адрес**.

   c. **Почтовый адрес**.

5. В поле **Отрасль экономики** укажите категорию деятельности, осуществляемой организацией. Доступны следующие категории: банковская деятельность, финансовая деятельность (кроме банков), топливно-энергетический комплекс, производственная деятельность, транспорт, государственное управление и оборона, машиностроение, телекоммуникации и связь, здравоохранение.

6. Укажите страну, в которой находится организация.

7. Укажите валюту, в которой будут отображаться денежные значения в интерфейсе.

8. Укажите **часовой пояс** организации. Чтобы применить изменения настроек часового пояса нужно выйти из учетной записи и повторно войти в систему.

9. Укажите фамилию, имя, отчество и должность руководителя организации.

10. Установите флажок **Субъект КИИ**, если вы хотите заполнить описание организации как субъекта КИИ. Над областью редактирования параметров организации отобразится вкладка **КИИ**, на которой вы можете заполнить поля описания.

11. Если организация расположена в Российской Федерации и ее деятельность относится к банковской сфере, отображаются дополнительные группы элементов **Сведения о кредитной организации**, **Сведения об участии в НПС** и **Система отчетности** (ПТК ПСД или KliKO). Задайте значения этих пунктов. Для такой организации доступна вкладка **Доступ в ФинЦЕРТ**, на которой вы можете настроить параметры обмена данными.

3.4.2. Параметры организации для обмена данными с системой ГосСОПКА

Доступность раздела ГосСОПКА определяется лицензией и настройками роли пользователя. Раздел ГосСОПКА доступен пользователям, в свойствах роли которых разрешен доступ к нему (**Настройки → Общие → Роли пользователей: Общее - Доступ к разделу Настройки управления инцидентами - ГосСОПКА**).

Чтобы указать параметры организации для обмена данными с системой ГосСОПКА, выполните следующие действия:

1. Перейдите в раздел **Настройки → Общие → Организации.**
2. Выберите организацию.
3. В свойствах организации перейдите на вкладку **ГосСОПКА**.
4. Укажите, участвует ли организация в обмене данными с ГосСОПКА.
5. Заполните поля:
   a. Токен для подключения к API ГосСОПКА. Установите флажок **Использовать единый токен**, чтобы использовать специальный токен для отправки сообщений. Единый токен можно настроить в разделе **Настройки → Управление инцидентами → ГосСОПКА**.
   b. Сокращенное наименование организации в ЛК ГосСОПКА.

3.4.3. Описание организации - субъекта КИИ

Чтобы заполнить параметры организации как субъекта КИИ, выполните следующие действия:

1. Перейдите в раздел **Настройки → Общие → Организации.**
2. Убедитесь, что в свойствах организации установлен флажок **Субъект КИИ**.
3. Перейдите на вкладку **КИИ**.
4. Заполните параметры. Укажите общие сведения о субъекте КИИ. Эти данные необходимы для формирования отчетных документов.

Таблица **Сводная информация по субъекту КИИ** заполнится автоматически по мере внесения данных о критических процессах и объектах КИИ. В нее попадают:

- Процессы из раздела Активы → Бизнес-процессы, у которых в поле Критичность процесса (КИИ) указано значение Критический.

- Группы ИТ-активов из раздела **Активы → Группы ИТ-активов**, в свойствах которых отмечен флажок **Объект КИИ**.

С помощью кнопки можно перейти в раздел **Активы** для просмотра детальной информации.

В таблице **Применимые показатели критериев значимости** выберите показатели, которые применимы на уровне субъекта КИИ в целом:

1. Нажмите на кнопку **Изменить** в заголовке таблицы. На экране отобразится окно со списком показателей.
2. Выберите показатели, применимые в отношении субъекта КИИ.
3. В отношении неприменимых показателей предложены стандартные формулировки обоснования неприменимости. Чтобы ввести собственное обоснование, дважды нажмите на ячейку и введите текст. Показатели, неприменимые на уровне субъекта КИИ, недоступны при оценке критичности процессов.
4. Нажмите на кнопку **Сохранить**. Применимые показатели отобразятся в таблице.

Настройка списка показателей выполняет следующие функции:

- Исключает неприменимые показатели на всех последующих этапах работы с функционалом КИИ (оценка критичности процессов), категорирования объектов КИИ: неприменимые показатели заблокированы для активов.
- Позволяет указать обоснования неприменимости показателей критериев значимости, одинаковые для всех объектов КИИ в рамках субъекта.

Заполнение таблицы **Применимые показатели критериев значимости** обязательно. Если таблица не заполнена, то оценка критичности процессов КИИ и определение категории значимости объектов КИИ недоступны.

3.4.4. Банковская деятельность

Если организация находится в Российской Федерации и относится к банковскому сектору, нужно указать в системе сведения для предоставления отчетности в ЦБ РФ.

В разделе **Настройки → Общие → Организации** отображаются дополнительные поля: **Сведения о кредитной организации** и **Сведения об участии в НПС**.

Группа элементов **Сведения о кредитной организации** содержит следующие поля:

- регистрационный номер КО;
- номер филиала;
- БИК;
- ОКПО;
- ОКАТО;
- признак вида организации (выбирается из выпадающего списка);
- вид КО (выбирается из выпадающего списка);
- состояние КО (выбирается из выпадающего списка);
- должность и ФИО руководителя;
- должность, ФИО и телефон исполнителя.

Внесите следующую информацию об участии организации в НПС:

- тип отчитывающегося оператора;
- система отчетности;
- вид деятельности, реализуемой организацией в соответствии с 161-ФЗ (отметить соответствующие пункты).

Если вы выбрали пункты, для которых нужно указать дополнительные данные, под разделом **Вид деятельности** отобразятся дополнительные поля для ввода:

- Регистрационный номер ОПС (в случае, если организация является оператором платежной системы). В справочнике **Настройки → Управление инцидентами → Платежные системы** настраивается перечень и коды доступных платежных систем.
- Платежные системы для ОПДС (для организаций, являющихся ОПДС).
- Платежные системы для ОУПИ (для ОЦ / ОУПИ).

Внесенные изменения сохраняются автоматически.

3.4.5. Настройка организации для доступа в ФинЦЕРТ

Чтобы указать параметры для подключения к системе ФинЦЕРТ, выполните следующие действия:

1. Перейдите в раздел **Настройки → Общие → Организации.**
2. Выберите организацию в списке.
3. Убедитесь, что что организация расположена в Российской Федерации и деятельность относится к банковской сфере. В этом случае доступна вкладка **Доступ в ФинЦЕРТ**.

4. Перейдите на вкладку **Доступ в ФинЦЕРТ**.
5. Укажите данные для подключения к ФинЦЕРТ:
    a. Логин.
    b. Пароль.
    c. Укажите тип используемого API.
    d. Если используется прокси сервер, укажите протокол подключения, адрес сервера, порт, параметры авторизации.

3.4.6. Удаление организаций

Чтобы удалить организацию:

1. В разделе **Настройки → Организации** наведите курсор на строку организации в списке.
2. Нажмите на кнопку  для удаления организации. На экране отобразится окно **Удаление организации**.
3. Выберите действия с дочерними организациями (если они есть у удаляемой организации):
    a. Удалить все дочерние организации. Система удалит выбранную организацию и все организации, расположенные ниже в иерархии.
    b. Удалить только выбранную организацию. Система удаляет только выбранную организацию. Все организации, расположенные ниже в иерархии, привязываются к родительской организации с сохранением иерархии.
4. Настройте перенос объектов удаленной организации. На экране отобразится окно со списком элементов удаляемой организации. В списке **Переносимые элементы** перечислены сущности, которые можно перенести в выбранную организацию. В списке **Активы, которые невозможно перенести** перечислены сущности, которые будут удалены при удалении организации.
5. Укажите организацию, к которой будут отнесены эти сущности.
6. Вы можете проверить возможность переноса сущностей в выбранную организацию по кнопке **Проверить**. Кнопка **Удалить с переносом сущностей** позволяет перенести сущности, которые можно перенести, в выбранную организацию. Остальные сущности будут удалены. Кнопка

Удалить без переноса сущностей позволяет удалить организацию без переноса сущностей в другую организацию.

Правом на удаление организации обладают только пользователи, в свойствах учетной записи которых установлен флажок **Полный доступ**.

3.4.7. Просмотр организаций

Чтобы просмотреть организации в системе:

1. Перейдите в раздел **Настройки → Общие →Организации**. В средней части экрана отобразится список организаций.
2. Выберите организацию. В правой части экрана отобразятся параметры организации.

С помощью строки поиска над списком организаций можно искать организации в списке.

Кнопка обновляет список организаций и параметры выбранной организации.

Система обновляет список и параметры выбранной в нем организации:

- Автоматически при внесении изменений в список или параметры организации вручную через интерфейс.
- Вручную по кнопке .

3.5. Настройка учетной записи текущего пользователя: мой профиль

Вы можете изменить параметры своей учетной записи в разделе **Мой профиль**. Для этого выполните следующие действия:

1. Перейдите в раздел **Общие → Мой профиль**.
2. Измените значения полей: **ФИО**, **E-mail**, **Должность**.
3. В поле **Токен API** можно просмотреть токен, если он был сгенерирован для этой учетной записи в разделе **Настройки → Общие → API**.
4. В поле **Организация пользователя** вы можете просмотреть организации, данные которых доступны вашей учетной записи. Организации можно настроить в свойствах пользователя.
5. Настройте часовой пояс. Возможны два варианта настройки часового пояса:

- **Автоматически** - данные о часовом поясе автоматически берутся из параметров браузера.
- **Вручную** – часовой пояс настраивается вручную с помощью выпадающего списка, который появляется при выборе этой опции.

> **Внимание!**
> Чтобы применить изменения настроек часового пояса нужно выйти из учетной записи и повторно войти в систему.

6. Вы можете изменить тему оформления интерфейса с помощью выпадающего списка **Тема оформления**. Внесенные изменения будут применены автоматически.
7. Если вы хотите отключить автоматический выход из системы при отсутствии пользовательской активности, отметьте пункт **Отключить автоматический выход из системы по тайм-ауту**.
8. Чтобы включить отображение всплывающих уведомлений, установите флажок **Включить всплывающие уведомления**.
9. Чтобы сменить пароль, в группе полей **Смена пароля** дважды укажите новый пароль и нажмите на кнопку **Изменить пароль**.
10. Кнопка **Выйти из всех сеансов** завершает все сессии текущей учетной записи.
11. Ниже расположен список **Стартовый раздел,** содержащий разделы и подразделы, отображаемые на панели навигации - стандартные и созданные пользователями. В этом списке вы можете указать раздел, который будет открываться первым при входе в систему.
12. Кнопка **Сбросить настройки интерфейса** позволяет сбросить пользовательские настройки интерфейса.
13. Ниже расположен список фильтров, сохраненных вами в системе. В списке вы можете удалить фильтр из учетной записи. По двойному щелчку на фильтре вы можете перейти в раздел, в котором фильтр был создан. Если поля, использованные при создании фильтра, были удалены, то фильтр помечается восклицательным знаком.

В списках в правой части экрана приведен перечень системных и специальных ролей, назначенных вашей учетной записи.

3.6. Настройка подключения к домену

Если вы хотите включить в состав пользователей системы пользователей домена, настройте подключение к домену. Добавлять учетные записи вручную в систему не потребуется: пользователи получат доступ к системе, используя доменные учетные данные.

Чтобы настроить подключение к домену, выполните следующие действия:

1. Перейдите в раздел **Общие → Пользователи системы → Домены (LDAP).**
2. Нажмите на кнопку  .
3. На вкладке **Основное** укажите следующие данные:
   a. Выберите организацию.

      Выберите тип каталога: **Active Directory** или **FreeIPA**.
   b. Полное имя домена.
   c. IP-адрес LDAP-сервера.
   d. Порт подключения. По умолчанию настроен порт 636.
   e. Зашифрованное подключение к каталогу. По умолчанию флажок подключения установлен.
   f. Base DN.
   g. Логин доступа и пароль.

      > Формат логина доступа **user@DOMAIN** (Значение **DOMAIN** указывается в верхнем регистре).

   h. Коллектор.
   i. Комментарий.
4. Нажмите на кнопку **Проверить настройки**, чтобы проверить корректность настроек.
5. Расписание запуска синхронизации пользователей можно настроить на вкладке **Расписание**. Если вы зададите здесь параметры синхронизации, система будет в указанное время синхронизировать данные пользователей, групп пользователей и их атрибутов.

> Вы можете в любое время синхронизировать данные пользователей, групп пользователей и их атрибутов по нажатию кнопки **Синхронизация пользователей** на вкладке **Основное.** Статус учетной записи обновляется

6. Нажмите на кнопку **Добавить**. Система автоматически интегрируется с Active Directory**.** Добавьте пользователей в систему из Active Directory.

После добавления домена указанная организация, к которой относится домен, автоматически указывается в параметрах:

- Домена, который автоматически создается в разделе **Активы → Домены**.
- Пользователей, которые относятся к этому домену и добавляются через Active Directory в разделе **Настройки → Общие → Пользователи системы**.

3.7. Установка обновлений системы

Чтобы обновить компоненты системы:

1. Скачайте zip-архив с обновлением (rvision-<номер версии>.zip) по ссылке. Чтобы получить ссылку на скачивание zip-архива с обновлением, обратитесь в службу поддержки по адресу support@rvision.ru.
2. Загрузите файл rvision-<номер версии>.zip во временную директорию /tmp на сервер, на котором установлена система. Пример приведен для версии 4.7.0.

   > **Пример**
   > scp ./rvision-4.7.0.-rc1.zip user@rvnserver:/tmp/

3. Подключитесь по протоколу SSH к серверу, на котором установлена система. Для дальнейших действий потребуются права суперпользователя (root).

   ```
   ssh user@rvnserver
   ```

4. Распакуйте файл с обновлением командой

```
unzip -o /tmp/rvision-4.7.0.-rc1.zip -d /tmp/rvn
```

5. Запустите скрипт обновления с помощью одной из следующих команд:

   a. Команда запускает **интерактивный** режим установки. В этом режиме в ходе процесса установки вы отвечаете на вопросы, задаваемые установщиком.

   ```
   /tmp/rvn/install.sh
   ```

   Для подробного вывода информации можно задать переменную VERBOSE.

   Пример
   sudo VERBOSE=yes /tmp/rvn/install.sh

   b. Команда запускает **неинтерактивный** режим установки. В этом режиме по умолчанию считается, что на все вопросы, задаваемые установщиком, введен положительный ответ: yes.

   ```
   NON_INTERACTIVE=yes /tmp/rvn/install.sh
   ```

6. Подтвердите продолжение установки клавишей Enter.
7. Если необходимо, следуйте инструкциям установщика. По окончании установки на экране отобразится сообщение об успешном завершении.
8. Введите учетные данные и нажмите на кнопку **Вход в систему**. В окне браузера отобразится стартовая страница системы.

3.8. Обслуживание системы

Сервисный режим - это режим работы системы, при котором доступ к системе возможен только для пользователей с определенными ролями для внесения изменений в настройки. Выполнить вход в систему в режиме обслуживания могут пользователи, в свойствах системной роли которых установлен флажок **Обслуживание системы** в разделе **Общее**. Эти пользователи могут производить чтение/изменения в настройках системы в соответствии с разрешениями, заданными в их роли.

После перехода в режим обслуживания доступ в систему для пользователей без включенной опции **Обслуживание системы** в свойствах роли не разрешается. При попытке выполнить вход, используя такую учетную запись, отображается

сообщение: **Система находится в режиме обслуживания. Вход в систему не возможен.**

Чтобы настроить правило перехода системы в сервисный режим:

1. Перейдите в раздел **Настройки → Общие → Обслуживание системы**.
2. В правой части экрана отобразится область редактирования правила обслуживания.
3. Укажите наименование.
4. Укажите описание.
5. Задайте дату и время начала и окончания периода.
6. Чтобы отправить письмо с уведомлением о режиме обслуживания всем пользователям системы, у которых указан адрес электронной почты, установите флажок **Отправка уведомления пользователям системы**, задайте срок уведомления, тему письма и текст уведомления.
7. Чтобы вывести окно с предупреждениям о режиме обслуживания пользователям, которые выполнили вход и работают в системе, установите флажок **Предупреждать активных пользователей системы**, задайте срок уведомления и введите текст уведомления.
8. В разделе **Отключить на период обслуживания** установите флажки для отключения текущих процессов системы:
    a. Интеграции с внешними системами - система ожидает завершения работы интеграции. Интеграции отключаются автоматически. Отключенные интеграции автоматически включаются после завершения работы в режиме обслуживания.
    b. Политики инвентаризации - система ожидает завершения работы политики. Политики отключаются автоматически. Отключенные политики автоматически включаются после завершения работы в режиме обслуживания.
    c. Политики автогенерации отчетов - система ожидает завершения работы политики генерации отчетов. Отключенные политики автоматически включаются после завершения работы в режиме обслуживания.
9. Нажмите на кнопку **Сохранить**. Правило будет исполнено в соответствии с настройками. За 24 часа до перехода в режим обслуживания на стартовой странице отображается уведомление с указанием времени, оставшегося до перехода в режим обслуживания.

Вы можете отключить исполнение правила, установив флажок **Отключить правило**. Система не будет переходить в режим обслуживания в соответствии с этим правилом.

4. КОЛЛЕКТОРЫ

В этом разделе приведены рекомендации по настройке и управлению коллекторами.

- Добавление коллектора
- Обновление коллектора
- Управление HTTPS-режимом коллектора

4.1. Добавление коллектора

Если в системе существует одна или несколько организаций, то добавлять коллекторы могут пользователи, у которых есть доступ ко всем организациям: в настройках пользователя установлен флажок **Полный доступ**.

Чтобы добавить коллектор, выполните следующие действия:

1. Перейдите в раздел **Настройки → Общие → Коллекторы**.
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров коллектора.
3. Введите наименование коллектора.
4. Укажите адрес коллектора. Он задается в формате IP-адреса или DNS-имени хоста.
5. Укажите порт коллектора. Связка **IP-адрес + порт коллектора** должна быть уникальной. По умолчанию используется порт 3001.

   Создание коллекторов с дублирующейся связкой **IP-адрес + порт коллектора** запрещено.

   При повторном добавлении одного и того же хоста с коллектором (например, по связкам **IP-адрес + порт коллектора** и **Имя + порт коллектора**) соединение по https станет невозможно.
6. Нажмите на кнопку **Добавить**. Коллектор отобразится в списке, а в свойствах коллектора становится доступен флажок **HTTPS**.
7. Установите флажок **HTTPS** для соединения между сервером R-Vision и коллектором по протоколу https. При этом происходит автоматическая генерация ключевой пары для шифрования трафика. Сервис коллектора перезапускается автоматически.
8. Для настройки созданного коллектора выберите его в списке.

9. В области редактирования коллектора перейдите на вкладку **Организации**.
10. Нажмите на кнопку **Добавить** над списком организаций. На экране отобразится окно выбора организации.
11. Выберите организацию.
12. Нажмите на кнопку **Сохранить**. Организация отобразится в списке организаций коллектора.
13. Задайте тип коллектора для организации:

    a. Вы можете назначить коллектор используемым по умолчанию, установив флажок в столбце **Коллектор по умолчанию.** У организации обязательно должен быть один и только один коллектор по умолчанию. Коллектор по умолчанию помечен в списке значком .Изменить коллектор по умолчанию для организации можно, выбрав эту организацию в настройках другого коллектора.

    b. Если коллектор будет использоваться для работы с коннекторами, установите флажок **Использовать для реагирования**. Коллектор, используемый для реагирования, помечен в списке значком . Количество коллекторов, используемых для реагирования, ограничено лицензией. Если в системе существует несколько организаций, каждая связка **Коллектор + Организация** будет считаться одним коллектором реагирования из лицензии.

    Если коллектор используется в каком либо коннекторе реагирования, снять флажок **Использовать для реагирования** в настройках этого коллектора нельзя.

Рекомендации по расчету нагрузки при сканировании приведены в разделе Расчет нагрузки при инвентаризации оборудования.

Возможные статусы коллекторов (отображаются в таблице со списком существующих коллекторов):

- - Подключено.
- - Ошибка (в случае неуспешного подключения).

Коллектор нельзя удалить, если он:

- является коллектором по умолчанию хотя бы в одной организации.

- используется хотя бы в одном коннекторе реагирования.

4.2. Обновление коллектора

Чтобы обновить коллектор:

1. Запустите обновление компонентов системы. После запуска скрипта установки обновления install.sh на шаге 5, скрипт отобразит список компонентов, которые можно обновить, и запросит подтверждение.
2. Подтвердите обновление компонентов клавишей Enter.
3. Следуйте инструкциям скрипта установки. По окончанию обновления на экране отобразится сообщение об успешном завершении.

4.3. Управление HTTPS-режимом коллектора

После установки локальный коллектор подключен по ip-адресу сервера в http-режиме.

Для повышения безопасности подключение можно перевести в https-режим. Изменить режим можно только для успешно подключенного коллектора.

Чтобы включить режим HTTPS, установите флажок **HTTPS**.

Если для коллектора включен режим HTTPS, то система автоматически выполняет следующие действия:

1. Создает сертификат с IP-адресом в CN-записи в каталоге dataFiles коллектора `/opt/r-vision/data/collectors/collectorjs/volumes/dataFiles`. Сертификат генерируется при каждом включении режима HTTPS. Срок действия сертификата - один год. Проверить сертификат можно командами:

```
openssl x509 -in /opt/r-
   vision/data/collectors/collectorjs/volumes/dataFiles/cert -
   noout -startdate -enddate
openssl x509 -in /opt/r-
   vision/data/collectors/collectorjs/volumes/dataFiles/cert -
   noout -issuer | sed 's/.*\/CN=\(.*\)/\1/'
```

2. Создает файл is_https. Этот файл является флагом режима. Коллектор автоматически переключится в https-режим через reload:

```
ls -l /opt/r-
   vision/data/collectors/collectorjs/volumes/dataFiles/
```

Со стороны smp в таблице am_collectors у коллектора обновятся поля https и certificate:

```
docker exec $(docker ps -a --filter "name=postgres" --format
'{{.Names}}') sh -c "psql -U rvision -h 127.0.0.1 -c 'select id, address,
https, status, certificate from am_collectors;'"
```

Статус при исправном подключении коллектора должен иметь флаг true: `t`.

Система не может подключить коллектор, который работает корректно, если закрыт порт службы коллектора на брандмауэре, не соответствуют режимы подключения и работы коллектора, просрочен сертификат, указан неверный адрес подключения в CN-записи в сертификате.

Сетевые ошибки можно выявить с помощью утилит, например, tcpdump, nc, telnet, ss.

Для восстановления подключения рекомендуется принудительно перевести коллектор и подключение к нему в режим http.

Чтобы включить режим http:

1. Удалите файл is_https командой

```
rm -f /opt/r-
   vision/data/collectors/collectorjs/volumes/dataFiles/is_http
   s
```

2. Задайте режим подключения к коллектору

```
docker exec $(docker ps -a --filter "name=postgres" --format
   '{{.Names}}') sh -c "psql -U rvision -h 127.0.0.1 -c
   \"UPDATE am_collectors SET https='f' where
   address='ip_address';\""
```

3. Перезапустите контейнер коллектора

```
docker restart $(docker ps -a --filter "name=collector" --
   format '{{.Names}}')
```

Соединение с коллектором восстановится.

5. АКТИВЫ

В этом разделе приведены инструкции по настройке и работе с активами в системе. Сущности **Активы** в системе используются для описания как бизнес-активов организации (информационные активы, бизнес-процессы, персонал), так и ИТ-активов (оборудование, ПО, сети и т.д.).

Добавление и актуализация данных об активах в системе осуществляется либо в ручном режиме пользователями системы, либо в автоматическом режиме посредством сканирования сетевых устройств.

- О модуле активов
- Подготовка к работе с активами
- Типы активов
- Настройка полей описания активов
- Работа с доменами

5.1. О модуле активов

Ключевые возможности:

- Сканирование ИТ-инфраструктуры, выявление оборудования и сбор данных по его характеристикам: основные параметры оборудования, установленное программное обеспечение, пользователи оборудования, применяемые параметры безопасности.
- Учет материальных и нематериальных активов и их взаимосвязей (бизнес-процессы, информационные активы, информационные и автоматизированные системы, сети, оборудование, персонал и пр.).
- Контроль структуры и состава компонентов ИТ-инфраструктуры (появление новых устройств, установка или удаление программного обеспечения, изменение параметров безопасности, появление новых пользователей).
- Визуализация сетевой инфраструктуры в формате географического расположения, сетевых схем, схем физического размещения оборудования в помещениях.
- Формирование необходимых отчетных документов (паспортов сетей, систем и помещений, перечней, сводных отчетов).

5.2. Подготовка к работе с активами

1. Настройте перечень пользовательских типов активов в разделе **Настройки → Управление активами → Типы активов**.

2. Настройте типы категорий бизнес-процессов, типов информационных активов и типов организационных единиц, используемых в организации, в разделе **Настройки → Управление активами → Справочники**.
3. (Опционально) Создайте дополнительные поля описания активов (раздел **Настройки→Управление активами→ Справочники → Поля описания активов**) и добавьте их к типам активов (**Настройки → Управление активами → Справочники → Типы активов**).
4. Внесите данные об активах организации в систему, создав или отредактировав сущности на вкладках раздела **Активы**.
5. Назначьте пользователей ответственными за активы. Для этого заполните поля **Ответственный** в свойствах активов (возможные роли: **Владелец**, **Администратор безопасности**, **Аудитор безопасности**, **Менеджер по контролю соответствия**).
6. Проведите инвентаризацию, если она не была проведена ранее.
7. Через свойства активов установите имеющиеся связи между ними.
8. Настройте политики включения оборудования в Группы ИТ-активов в разделе **Настройки → Управление активами → Политики инвентаризации → Политики назначения**.
9. В разделе **Главное** создайте необходимые панели графиков, карт сетей, схем взаимосвязей

5.3. Типы активов

- Бизнес-процессы
- Помещения
- Информация
- Оборудование
- ПО
- Персонал
- Подразделение/Организация
- Сети
- Пользовательские типы активов

5.3.1. Бизнес-процессы

С помощью активов типа **Бизнес-процессы** вы можете описать бизнес-процессы организации в системе.

Работа с бизнес-процессами (просмотр и изменение) доступна только пользователям, обладающим специальными ролями: **Владелец актива**, **Администратор безопасности**, **Аудитор безопасности** и **Менеджер по контролю соответствия**, а также пользователям, в свойствах системной роли которых отмечен раздел **Бизнес-процессы** на вкладке **Активы**.

Чтобы добавить бизнес-процесс, выполните следующие действия:

1. Перейдите в раздел **Активы → Бизнес-процессы.**
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров актива.

   Вы можете создать дочерний бизнес-процесс для существующего. Дочерним активам автоматически присваиваются роли: **Владелец актива**, **Администратор безопасности**, **Аудитор безопасности** и **Менеджер по контролю соответствия**.
3. Заполните поля.
   - Организация (если в системе создано две и более организаций).
   - Идентификатор.
   - Категория бизнес-процессов. Вы можете добавить категории и названия бизнес-процессов с помощью справочника **Настройки → Управление активами → Справочники → Бизнес-процессы**. При добавлении категории в справочник укажите название категории бизнес-процесса.
   - Наименование процесса.
   - *Критичность* (условный параметр, определяющий степень критичности данного процесса).
   - *Владелец,администратор безопасности, аудитор безопасности, менеджер по контролю соответствия процесса* (в том числе из раздела **Персонал**). Доступны для группового редактирования
   - *Описание.*
   - *Входит в* (для дочерних активов).
4. Если бизнес-процесс входит в организацию, в свойствах которой установлен флажок **Объект КИИ** и заполнена таблица **Применимые показатели критериев значимости**, то в свойствах бизнес-процесса

отображаются параметры КИИ. Заполнение параметров КИИ бизнес-процесса позволяет:

a. Автоматически проставить свойство **Объект КИИ** для всех групп ИТ-активов, связанных с критическими процессами.

b. Исключить неприменимые показатели на этапе категорирования объектов КИИ: неприменимые показателя будут недоступны для групп ИТ-активов.

c. Заполнить обоснование неприменимости показателей критериев значимости, одинаковые для всех объектов КИИ в рамках процесса.

Задайте **Критичность процесса (КИИ)**: укажите показатели, применимые в отношении процесса. Для неприменимых показателей можно использовать стандартные формулировки обоснований или задать собственную формулировку по двойному щелчку на ячейке. Показатели, неприменимые на уровне процесса, будут заблокированы при проведении категорирования связанных объектов КИИ. Если хотя бы один показатель применим в отношении процесса, процесс будет отмечен как критический.

Дата оценки критичности (КИИ) заполняется автоматически после сохранения данных в поле **Критичность процесса (КИИ)**.

> Заполнение таблицы **Критичность процесса КИИ** обязательно для использования функционала по категорированию объектов КИИ. Если таблица не заполнена, то калькулятор категории значимости не доступен.

5. Чтобы в дальнейшем проводить оценку рисков для данного актива, установите флажок **Проводить оценку риска**, выберите схему оценки рисков, установите уровень допустимого риска и определите ценность актива. В свойствах актива отобразится раздел **Атрибуты безопасности** (), в котором можно настроить взаимосвязи атрибутов безопасности активов.
6. Нажмите на кнопку **Добавить**. Бизнес-процесс появится в списке.

При удалении родительского актива типа **Бизнес-процессы**, удаляются также все цепочки активов, дочерних по отношению к данному активу.

5.3.2. Помещения

Работа с помещениями (просмотр и изменение) доступна только пользователям, обладающим специальными ролями: **Владелец актива**, **Администратор безопасности**, а также пользователям, в свойствах системной роли которых отмечен раздел **Помещения** на вкладке **Активы.**

Вы можете добавить в систему помещение и использовать его при визуализации размещения оборудования.

Чтобы добавить помещение, выполните следующие действия:

1. Перейдите в раздел **Активы → Помещения**.
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров помещения.
3. Укажите организацию (если в системе создано две и более организаций).
4. Укажите идентификатор помещения или оставьте поле пустым, чтобы идентификатор сгенерировался автоматически.
5. Укажите тип помещения. Доступны следующие типы помещений: **здание**, **этаж**, **помещение**. Для каждого типа помещений доступен разный набор параметров. Общие для всех типов поля:
    a. Название.
    b. Если помещение входит в другой элемент в разделе **Помещения**, укажите родительский элемент в списке **Входит в**. При удалении родительского актива типа **Помещения**, удаляются также все цепочки активов, дочерних по отношению к данному активу.
    c. Подразделение/Организация.
    d. Администратор безопасности.
    e. Локация.
    f. Описание помещения.
6. Для типов **Помещение** и **Здание** укажите адрес и номер.
7. Вы можете загрузить графический план (схему) помещения в формате **.jpeg или *.png** для типа **Здание, Этаж** или **Помещение**, чтобы

просмотреть оборудование на карте помещения в разделе **Карты и схемы**.

8. Вы можете указать требования при добавлении актива. Требования доступны для группового редактирования.
9. Нажмите на кнопку **Добавить**.

5.3.3. Информация

С помощью активов типа **Информация** вы можете добавлять данные об обрабатываемой информации в организации в систему.

Работа с информационными активами (просмотр и изменение) доступна только пользователям, обладающим специальными ролями: **Владелец актива**, **Администратор безопасности**, **Аудитор безопасности** и **Менеджер по контролю соответствия**, а также пользователям, в свойствах системной роли которых отмечен раздел **Информация** на вкладке **Активы**.

Чтобы добавить информационный актив, выполните следующие действия:

1. Перейдите в раздел **Активы → Информация.**
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров актива.
3. Заполните поля. Параметры, указанные курсивом, доступны для группового редактирования.
   - Организация (если в системе создано две и более организаций).
   - Идентификатор.
   - Категория информационного актива. Категории и типы информационных объектов из справочника используются для описания информационных активов на вкладке **Активы**. Вы можете настроить категории и типы информационных активов с помощью справочника **Настройка → Управление активами → Справочники → Информационные активы**.
   - Тип информационного актива.
   - *Критичность* (условный параметр, определяющий степень критичности данного актива).

- *Владелец информации, Администратор безопасности, Аудитор безопасности, Менеджер по контролю соответствия* (вы можете указать пользователя из раздела **Персонал**).
- *Состав*.

4. Чтобы в дальнейшем проводить оценку рисков для данного актива, установите флажок **Проводить оценку риска**, выберите схему оценки рисков, установите уровень допустимого риска и определите ценность актива. В свойствах актива отобразится раздел **Атрибуты безопасности** (), в котором можно настроить взаимосвязи атрибутов безопасности активов.
5. Нажмите на кнопку **Добавить**. Актив будет добавлен в систему.

5.3.4. Оборудование

В результате сканирования во вкладке **Оборудование** для каждого объекта в правом разделе будет отображена основная информация по устройству, а также поля для внесения данных вручную.

- Внешние и внутренние устройства
- Добавление оборудования
- Оборудование: настройка параметров отображения
- Оборудование: просмотр обновлений ОС Windows

5.3.4.1. Внешние и внутренние устройства

Оборудование делится по IP-адресу на следующие типы: **внутреннее** и **внешнее.**

Узлы с IP-адресом являются **внутренними**:

- Если хотя бы один IP-адрес узла попадает в следующие диапазоны:
  - От 10.0.0.0 до 10.255.255.255 с маской 255.0.0.0 или /8.
  - От 172.16.0.0 до 172.31.255.255 с маской 255.240.0.0 или /12.
  - От 192.168.0.0 до 192.168.255.255 с маской 255.255.0.0 или /16.
  - От 100.64.0.0 до 100.127.255.255 с маской подсети 255.192.0.0 или /10.
- Если узел создан в системе в разделе **Активы** вручную.
- Если узел создан автоматически по данным, полученным из интеграций или путем импорта из файлов Excel.

Внешнее оборудование может создаваться только из инцидентов, если IP-адрес узла не попадает в диапазоны адресов внутренних узлов.

Внешние узлы по умолчанию не отображаются в разделе **Активы → Оборудование**. Вы можете посмотреть перечень внешних узлов, установив флажок **Показать внешнее оборудование** в разделе **Параметры отображения** свойств актива с типом **Оборудование**. Вы можете вручную указать дополнительную информацию в свойствах внешнего узла.

Внешний узел становится внутренним при изменении типа узла вручную в свойствах актива.

5.3.4.2. Добавление оборудования

Вы можете добавить оборудование в систему:

- Вручную в разделе Активы → Оборудование.
- При импорте из Excel файла. При импорте оборудования из файла домен привязывается (если такой домен существует в системе) или создается автоматически в разделе **Активы → Домены**.

  Если в организации есть сети с одинаковой адресацией, то при добавлении оборудования путем импорта из файлов Excel нужно указать приоритетную сеть.
- Автоматически (при инвентаризации).
- Автоматически через интеграции с внешними системами.

Работа с оборудованием (просмотр и изменение) доступна только пользователям, обладающим специальными ролями: **Владелец актива**, **Администратор безопасности**, **Аудитор безопасности** и **Менеджер по контролю соответствия**, а также пользователям, в свойствах системной роли которых отмечен раздел **Оборудование** на вкладке **Активы**

Чтобы добавить оборудование вручную, выполните следующие действия:

1. Перейдите в раздел **Активы → Оборудование.**
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров актива.
3. Заполните поля. Параметры, указанные курсивом, доступны для группового редактирования.
   - Организация (если в системе создано две и более организаций).

- Имя устройства. Если в качестве имени устройства указан IP-адрес, то этот IP-адрес будет автоматически добавлен в список IP- адресов оборудования. Для IP-адреса в списке автоматически указывается MAC-адрес 00:00:00:00:00:00 и маска подсети 255.255.255.0.
- Критичность (условный параметр, определяющий степень критичности данного актива).
- IP-адрес, маска подсети, MAC-адрес.
- Домен/рабочая группа.
- *ОС.*
- *Виртуальная машина.*
- *Тип узла (сервер, рабочая станция, мобильное оборудование и т.д.).*
- *Статус.* Статусы оборудования настраиваются в справочнике **Статусы активов** (**Настройки → Управление активами → Справочники → Статусы активов**). Статусы описывают текущее состояние оборудования, обнаруженного в ходе сканирования. По умолчанию для этого типа актива добавлены три статуса: **Рабочий**, **Тестовый**, **В процессе внедрения**.
- *Группы ИТ-активов.*
- *Владелец актива.*
- *Администратор безопасности.*
- *Аудитор безопасности.*
- *Менеджер по контролю соответствия.*
- *Теги.Теги можно добавить в справочник **Теги** в разделе **Активы → Справочники → Теги**. Теги можно использовать для фильтрации информации при просмотре данных в базе активов, либо при экспорте информации из системы.*
- *Локация. Можно выбрать значение из справочника.*
- *Помещение.*
- *Бизнес-подразделение/организация.*

- *Комментарий.*
- *Дополнительные поля.*

4. Вы можете указать требования при добавлении актива. Требования доступны для группового редактирования.
5. Нажмите на кнопку **Добавить**. Оборудование будет добавлено в список активов.

5.3.4.3. Оборудование: настройка параметров отображения

Параметры отображения влияют на отображение всего списка активов в разделе **Активы → Оборудование**, поэтому вы можете изменять параметры отображения для любого актива из этого раздела или при создании нового актива в этом разделе.

Для изменения параметров отображения списка оборудования выполните следующие действия:

1. Перейдите в раздел **Активы → Оборудование**.
2. Выберите любой актив в списке или создайте новый.
3. Перейдите в раздел **Параметры отображения** с помощью кнопки  .
4. Установите один или несколько флажков:
   - Скрывать устаревшее оборудование (узлы с индикатором **устаревший**);
   - Скрывать нераспознанное оборудование (все узлы с индикаторами **нет доступа** и **нет открытых портов**).
   - Показать внешнее оборудование (все узлы с типом **Внешнее устройство**).

Список активов будет отображаться в соответствии с внесенными изменениями.

Устаревшие учетные записи помечаются в списке значком  .

5.3.4.4. Оборудование: просмотр обновлений ОС Windows

Чтобы просмотреть список обновлений ОС Windows, обнаруженных на Windows-узлах при сканировании:

1. Перейдите в раздел **Активы → Оборудование**.

2. Выберите узел, параметры которого вы хотите просмотреть. Раздел **Обновления** доступен для узлов с ОС Windows, просканированных коллектором R-Vision.

3. Нажмите на кнопку  . В правой части экрана отобразится список обнаруженных на узле обновлений. Кнопка **Показать в списке обновлений Windows** открывает раздел **Уязвимости → Обновления** с фильтром по выбранному узлу.

5.3.5. ПО

Активы типа **Программное обеспечение** позволяют ввести в систему информацию обо всем обнаруженном во время сканирования и установленном на устройствах программном обеспечении.

- Добавление ПО
- Автоматизация обнаружения ПО

5.3.5.1. Добавление ПО

Работа с ПО (просмотр и изменение) доступна только пользователям, обладающим специальными ролями: **Владелец актива**, **Администратор безопасности**, **Аудитор безопасности** и **Менеджер по контролю соответствия**, а также пользователям, в свойствах системной роли которых отмечен раздел **ПО** на вкладке **Активы**

Чтобы добавить ПО, выполните следующие действия:

1. Перейдите в раздел **Активы → ПО.**

2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров актива.

3. Заполните поля. Параметры, указанные курсивом, доступны для группового редактирования.

   a. Организация (если в системе создано две и более организаций).

   b. *Название.*

   c. Версия.

   d. *Группа ПО*. Группировку ПО можно настроить с помощью справочника **Группы ПО**.

e. *Теги*.Теги можно добавить в справочник **Теги** в разделе **Активы → Справочники → Теги**. Теги можно использовать для фильтрации информации при просмотре данных в базе активов, либо при экспорте информации из системы.

f. *Администратор безопасности.*

g. *Комментарии*.

h. *Количество лицензий*.

i. *Срок истечения лицензии*.

j. *Дополнительные поля*.

4. Нажмите на кнопку **Добавить**. Актив будет добавлен в систему.

5.3.5.2. Автоматизация обнаружения ПО

В системе предусмотрена возможность распознавания ПО, которое установлено на узле, при проведении инвентаризации. Раздел доступен пользователям, в свойствах роли которых разрешен доступ к этому разделу с правами на изменение, а также в свойствах учетной записи установлен флажок **Все организации** (доступен в режиме Multi-tenancy).

Если известен только путь к каталогу установки файлов программного обеспечения, для его обнаружения нужно создать политику обнаружения ПО. Согласно политике система будет проверять наличие ПО на узле: существует ли на узле указанный каталог и/или файл (в соответствии с заданным путем).

Чтобы добавить политику обнаружения ПО, выполните следующие действия:

1. Перейдите в раздел **Настройки → Управление активами → Политики инвентаризации → Политики обнаружения ПО**.
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования политики.
3. Заполните поля :
   a. Наименование политики.
   b. Описание политики.
   c. **Тип**. Тип определяет способ обнаружения ПО (в настоящий момент доступен только поиск по заданному пути).

d. **Путь к каталогу установки/файлу приложения**. Параметр используется для указания либо каталога, либо полного пути в файлу, наличие которого на целевой системе будет означать факт наличия искомого ПО.

e. Наименование и версия ПО – эти поля определяют название и версию ПО, которые будет отображаться в списке обнаруженного ПО (**Активы → ПО**).

4. Нажмите на кнопку **Добавить**. Созданная запись появится в списке.

5.3.6. Персонал

Активы типа **Персонал** представляют собой учетные записи пользователей, которые были обнаружены в ходе сканирования. В системе также предусмотрена возможность настройки отображения персонала.

- Добавление персонала
- Настройка параметров отображения персонала

5.3.6.1. Добавление персонала

Работа с персоналом (просмотр и изменение) доступна только пользователям, обладающим специальными ролями: **Владелец актива**, **Администратор безопасности**, **Аудитор безопасности** и **Менеджер по контролю соответствия**, а также пользователям, в свойствах системной роли которых отмечен раздел **Персонал** на вкладке **Активы**

Чтобы добавить персонал, выполните следующие действия:

1. Перейдите в раздел **Активы → Персонал.**
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров актива.
3. Заполните поля, расположенные в правой панели. Параметры, указанные курсивом, доступны для группового редактирования.
   - Организация (если в системе создано две и более организаций).
   - ФИО.
   - *Должность.*
   - Логин.
   - *Домен.*

- E-mail.
- *Телефон.*
- *Подразделение/Организация*.
- *Помещение.*
- *Администратор безопасности* (на эту роль автоматически назначается пользователь, являющийся администратором связанного домена. Пользователей можно назначить вручную).
- *Теги*.Теги можно добавить в справочник **Теги** в разделе **Активы → Справочники → Теги**. Теги можно использовать для фильтрации информации при просмотре данных в базе активов, либо при экспорте информации из системы.
- *Комментарии*.
- Критичность.
- *Дополнительные поля*.

4. Нажмите на кнопку **Добавить**. Актив будет добавлен в систему.

5.3.6.2. Настройка параметров отображения персонала

Параметры отображения влияют на отображение всего списка активов в разделе **Активы → Персонал**, поэтому вы можете изменять параметры отображения для любого актива из этого раздела или при создании нового актива в этом разделе.

Для изменения параметров отображения списка пользователей выполните следующие действия:

1. Перейдите в раздел **Активы → Персонал**.
2. Выберите любой актив в списке или создайте новый.
3. Перейдите в раздел **Параметры отображения** с помощью кнопки .
4. Установите один или несколько флажков:
   - Скрывать устаревшие учетные записи;
   - Скрывать заблокированные учетные записи.

Список активов будет отображаться в соответствии с внесенными изменениями.

Устаревшие учетные записи помечаются в списке значком .

5.3.7. Подразделение/Организация

Активы типа **Подразделение/Организация** описывают в системе единицы штатной структуры организации, сторонних организаций и контрагентов. С помощью активов типа **Подразделение/Организация** вы можете внести в систему информацию об имеющихся филиалах, подразделениях, контрагентах и их взаимосвязях с другими активами организации (информацией, бизнес-процессами, помещениями и т.д.)

В отличие от сущности **Организация**, которая служит для обозначения и разделения доступа между дочерними предприятиями, активы типа **Подразделение/Организация** позволяют реализовать более низкоуровневую привязку, когда нужно встроить актив в организационную структуру на уровне одного дочернего предприятия. Созданная сущность **Организация** автоматически добавляется в раздел **Активы → Подразделение/Организация**. Добавленная организация не может быть дочерней по отношению к другому активу. Удалить организацию можно только в разделе **Настройки → Общие → Организации**.

Работа с организационной единицей (просмотр и изменение) доступна только пользователям, обладающим специальными ролями: **Владелец актива**, **Администратор безопасности**, **Аудитор безопасности** и **Менеджер по контролю соответствия**, а также пользователям, в свойствах системной роли которых отмечен раздел **Подразделение/Организация** на вкладке **Активы**.

5.3.7.1. Настройка типов подразделений

Вы можете настроить типы подразделений с помощью справочника **Настройки → Управление активами → Справочники → Типы подразделений**. Этот справочник содержит описания типов подразделений имеющейся штатной структуры организации, а также (опционально) партнерских организаций и контрагентов.

При добавлении нового типа подразделения в справочник укажите его наименование и описание и сформируйте список полей типа подразделения. Порядок полей в списке определяет порядок следования полей в карточке подразделения. По умолчанию поля отображаются в разделе **Дополнительные сведения** свойств актива. Если вы хотите отобразить поле в разделе **Общие сведения** свойств подразделения, установите флажок **Основное** в таблице **Поля:** раздела **Настройки → Управление активами → Справочники → Типы подразделений.**

Если поле входит в тип актива и в тип подразделения, то настройка поля для типа актива считается приоритетной.

5.3.7.2. Добавление подразделения в список активов

Чтобы добавить подразделение/организацию, выполните следующие действия:

1. Перейдите в раздел **Активы → Подразделение/Организация.**
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров. Вы можете создать организацию как дочернюю по отношению к другой организации. Дочерним активам автоматически присваиваются роли: **Администратор безопасности**, **Аудитор безопасности** и **Менеджер по контролю соответствия**.
3. Заполните поля (набор полей зависит от типа подразделения):
   - Организация (если в системе создано две и более организаций).
   - Идентификатор.
   - Наименование.
   - Тип (подразделение, филиал, контрагент, департамент). Настраивается в справочнике **Типы подразделений** (см. описание выше). Определяет набор полей в карточке подразделения.
   - Входит в (опционально). Это поле указывает родительский актив.
   - Локация. Можно выбрать значение из справочника или указать координаты.
   - Администратор безопасности (в том числе из раздела **Персонал**).
   - Менеджер по контролю соответствия (в том числе из раздела **Персонал**).
   - Аудитор безопасности (в том числе из раздела **Персонал**).
   - Описание.
4. Вы можете указать требования при добавлении актива.
5. Нажмите на кнопку **Добавить**. Организационная единица появится в списке.

5.3.8. Сети

Активы типа **Сети** представляют собой описание в системе сетей организации, добавленных в систему вручную, либо обнаруженных системой в ходе сканирования.

- Добавление сети
- Удаление сети

5.3.8.1. Добавление сети

Работа с персоналом (просмотр и изменение) доступна только пользователям, обладающим специальными ролями: **Владелец актива**, **Администратор безопасности**, а также пользователям, в свойствах системной роли которых отмечен раздел **Сети** на вкладке **Активы**.

Если в структуре организации есть сети с одинаковой адресацией, то для корректной работы системы нужно создать все дублирующиеся сети. Для навигации по сетям используется поле **Наименование**. Наименование сети является уникальным и обязательно для заполнения. Все сети автоматически связываются между собой на основании их адресов. Иерархия сетей отображается в виде дерева. На каждом уровне дерева может быть любое количество дублирующихся сетей.

Чтобы добавить новую сеть, выполните следующие действия:

1. Перейдите в раздел **Активы → Сети.**
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров актива.
3. Укажите организацию (если в системе создано две и более организаций).
4. Заполните следующие поля:
   a. Адрес.
   b. Маска сети.
   c. Коллектор.
   d. Тип сети.
   e. Владелец актива.
   f. Администратор безопасности.

g. Дополнительные поля.

5. Нажмите на кнопку **Добавить**. Указанная сеть появится в списке сетей. Полю **Локация** автоматически присваиваются значения от входящих в сеть узлов.

При создании сети родительская сеть назначается автоматически. При редактировании сети можно изменить родительскую сеть в поле **Входит в:** для выбора доступны подходящие для привязки сети.

Для групповой редактирования доступны следующие поля активов типа **Сети**:

- Коллектор.
- Тип сети.
- Владелец актива.
- Администратор безопасности.
- Теги.
- Комментарий.
- Дополнительные поля.

5.3.8.2. Удаление сети

Удаление сети выполняется аналогично удалению других сущностей. При этом оборудование, входящее в удаленную сеть, автоматически привяжется к сети 0.0.0.0 и не будет удалено из системы.

5.3.9. Пользовательские типы активов

В систему можно добавить произвольный тип активов для гибкого ведения реестра активов на предприятии. Такой тип является пользовательским. Пользовательский тип активов добавляется с помощью справочника **Типы активов**. Раздел доступен пользователям, в свойствах роли которых разрешен доступ к этому разделу.

Можно создать собственные типы как материальных (помещения, ПО, персонал), так и нематериальных активов. В системе определено два класса активов:

- бизнес-активы, к которым относятся, например, информационные активы, персонал, бизнес-процессы и т.д.;
- ИТ-активы, к которым относятся материальные ресурсы, такие как ПО, оборудование, сети и т.д.

Для каждого типа актива можно задать поля, используемые для описания активов в системе.

Пользовательские типы активов отображаются на отдельных панелях в разделе **Активы**.

Для пользовательских активов в системе существует ряд ограничений по функционалу:

- Не поддерживается иерархия пользовательских активов.
- По пользовательским активам нельзя проводить аудиты.
- Пользовательские активы нельзя связывать с инцидентами.
- Для пользовательских активов нет предварительно настроенных полей и связей.

Все поля пользовательских активов, кроме поля **Наименование**, доступны для группового редактирования. При групповом выделении в перечне связанных активов и задач отображаются активы и задачи, связанные с каждым из выбранных пользовательских активов.

Пользовательские активы можно связать с активами типов: Группы ИТ-активов, Информация, Бизнес - процессы, Оборудование, Персонал, Сети. Для пользовательских активов можно создавать задачи (в том числе, при групповом выделении).

Права на доступ к пользовательским типам активов распределяются по тому же принципу, что и к стандартным: доступ к ним будут иметь пользователи, в свойствах системной роли которых отмечен раздел с пользовательским типом актива, и пользователи. назначенные **Владельцем**, **Администратором** или **Аудитором безопасности** этого актива.

> Созданный пользователем тип актива становится доступен пользователю только после того, как пользователь выйдет из учетной записи и снова войдет в систему под своей учетной записью.

5.3.9.1. Добавление пользовательского типа активов

Чтобы добавить пользовательский тип, выполните следующие действия:

1. Перейдите в раздел **Настройки → Управление активами → Типы активов**.
2. Нажмите на кнопку  .
3. Выберите класс актива.
4. Заполните поля:

a. Наименование.

b. Тег.

c. Описание.

5. Выберите иконку для типа актива. Она будет отображаться на схеме взаимосвязей бизнес-процессов при выборе актива этого типа.

   a. В разделе **Иконка** нажмите на кнопку **Изменить**.

   b. В появившемся окне выберите иконку и нажмите **Выбрать**. Вы в любой момент можете вернуть иконку по умолчанию, назначенную типу системой, нажав на кнопку **Иконка по умолчанию**.

6. Сформируйте список полей, описывающих актив в системе, с помощью кнопки **Изменить**. В появившемся окне выберите поля.

   a. Если вы хотите отобразить поле в разделе **Общие сведения** свойств актива, установите флажок **Основное**.

   b. Чтобы использовать значение поля как идентификатор актива, установите флажок **Идентификатор актива**. В этом качестве можно использовать поля следующих типов: текстовое поле, несколько текстовых строк, числовое поле, ip-адрес.

7. Нажмите на кнопку **Сохранить**. Порядок полей в списке определяет порядок следования полей в свойствах актива.

8. Чтобы отключить отображение поля в свойствах актива, в списке активов, в файлах при экспорте и импорте, выделите поле и нажмите на кнопку **Скрыть**. Скрытые поля отображаются в списке серым перечеркнутым шрифтом и отмечены значком  .

   > Если в системе настроена интеграция с базами данных для импорта активов, то при изменении идентификатора актива актуализируйте настройки связывания полей в свойствах интеграции.

9. Для сохранения записи нажмите на кнопку **Добавить.** Вы можете настроить связь активов через атрибуты безопасности.

5.4. Настройка полей описания активов

В разделе **Поля описания активов** можно просмотреть общий перечень возможных типов полей, используемых для описания активов. Для подробного

описания активов можно создавать дополнительные поля, которые пользователь заполнит при внесении в систему записи об активе. В разделе **Типы активов** можно настроить набор полей из общего перечня, которые будут использоваться в описании каждого актива.

Раздел доступен пользователям, в свойствах роли которых разрешен доступ к этому разделу, а также в свойствах учетной записи установлен флажок **Все организации** (доступен в режиме Multi-tenancy).

Чтобы добавить новый тип поля, выполните следующие действия:

1. Перейдите в раздел **Настройки → Управление активами → Поля описания активов.**
2. В правой части вкладки нажмите на кнопку  .
3. Укажите группу поля или создайте новую. Группы полей используются для организации списка полей активов в окне выбора полей в справочниках: **Типы активов**, **Типы групп ИТ-активов**, **Типы подразделений**.
4. Введите наименование и описание.
5. Выберите тип поля. Набор доступных настроек зависит от типа поля.
   a. Для полей типов **Текстовое поле**, **Числовое поле**, **Несколько текстовых строк**, **Числовое поле с денежным символом** вы можете дополнительно указать подсказку для поля.
   b. Для полей типа **Список** установите флажок **Множественный выбор**, чтобы пользователь мог указать несколько значений из списка одновременно. В поле **Справочник** выберите справочник, данные которого будут использоваться как значения списка.
   c. Для полей типа **Текстовое поле** и **IP-адрес/адрес сети** можно указать регулярное выражение для валидации значения. При сохранении изменений в карточке актива, значение этого поля валидируется регулярным выражением. Если значение не проходит валидацию, то система отображает предупреждение и не сохраняет внесенные изменения. Для поля **IP-адрес/адрес сети** регулярное выражение применяется дополнительно после автоматической проверки формата IP-адреса.
   d. Поля типа **Агрегированный список** объединяет возможные значения указанного поля (типа **Выпадающий список**), полученные

из активов, указанных в поле **Источник данных**. Список создается автоматически. В свойствах актива агрегированный список отображается в виде таблицы.

e. Поле типа **Выбор пользователя** позволяет указать в поле пользователя, доступного в списке пользователей системы.

f. Для поля типа **Дата** можно установить флажок **Проверка истечения**, чтобы система автоматически проверяла истечение указанной в поле даты. Поля с истекшей датой помечаются значком ⓘ в списке активов. Список активов можно фильтровать по полям с истекшей датой.

g. Поля типов **Текстовое поле**, **Числовое поле**, **Несколько текстовых строк**, **IP-адрес** можно использовать как идентификатор пользовательского актива. Задать идентификатор актива можно в настройках типа актива.

6. Укажите тег поля. Тег используется для связи полей описания активов с полями отчетов.
7. Для сохранения записи в системе нажмите на кнопку **Добавить**. В результате новая запись появится в списке элементов.

Вы можете указать значения для пользовательских полей, выбрав несколько активов. При выборе нескольких активов пользовательские поля отображаются пустыми, если значения этих полей у выбранных активов не совпадают. Если у всех выбранных активов в поле одинаковое значение, то это значение отображается в поле. При изменении значения в поле, изменение вносится во все активы.

5.5. Работа со схемой взаимосвязей бизнес-процессов

При первом открытии система автоматически создает схему бизнес-процесса на основании существующих связей между активами. Вы можете просматривать объекты, связанные с бизнес-процссом, добавлять и удалять связи и активы на схеме по своему усмотрению.

Чтобы просмотреть схему взаимосвязей:

1. Перейдите в раздел **Активы → Бизнес-процессы**.
2. Выберите бизнес-процесс, для которого вы хотите открыть схему взаимосвязей.

3. Нажмите на кнопку  . На экране отобразится окно, в котором вы можете просмотреть и отредактировать схему, отображающую взаимосвязи между активами в рамках этого бизнес-процесса.

После открытия схемы в панели сверху появляется вкладка этой схемы, что позволяет быстро переключаться между различными схемами взаимосвязей. Система использует следующие правила связей между типами активов для задания направления на схеме:

- Персонал - влияет на Помещения, Подразделения, Группы ИТ-активов, Оборудование.
- Оборудование - влияет на Группы ИТ-активов, Сети.
- Сети - влияют на Группы ИТ-активов.
- Помещение - влияет на Подразделения.
- Группы ИТ-активов - влияет на Подразделения, Бизнес-процессы.
- Информация - влияет на Бизнес-процессы, Подразделения.
- **Пользовательские активы** - влияют на все системные активы, кроме **ПО**.

6. ИНЦИДЕНТЫ

- О модуле инцидентов
- Подготовка к работе с модулем
- Создание инцидента
- Изменение инцидента: особенности
- Просмотр инцидента
- Действия по реагированию на инцидент
- Настройка доступа к инциденту: рабочая группа
- Описание инцидента
- Отправка уведомлений в ГосСОПКА

6.1. О модуле инцидентов

Блок «Инциденты» – компонент, предназначенный для организации процесса управления инцидентами информационной безопасности и анализа информации, относящейся к инциденту.

Ключевыми возможностями модуля «Инциденты» являются:

- Ведение учета и регистрации инцидентов, проведение классификации инцидентов информационной безопасности.
- Реализация полного цикла обработки инцидентов в соответствии с заданными в организации процедурами.
- Организация совместной работы различных групп специалистов и экспертов, участвующих в расследовании инцидентов, хранение всей информации в единой базе данных.
- Оценка уровня ущерба от реализации инцидентов информационной безопасности.
- Формирование необходимых отчетных документов, в том числе в соответствии с требованиями регуляторов.

6.2. Подготовка к работе с модулем

1. Настройте перечень типов инцидентов, используемых в организации, в разделе **Настройки → Управление инцидентами → Типы инцидентов**.
2. Настройте перечень способов реализации, используемых в организации, в разделе **Настройки → Управление инцидентами → Справочники → Способы реализации инцидентов**. В свойствах способов укажите связанные с ними типы инцидентов.

3. Настройте последовательности статусов, отражающие этапы реагирования на инциденты, в разделе **Настройки → Управление инцидентами → Циклы обработки**.
4. Настройте уровни критичности инцидентов, установленные в организации, в разделе **Настройки → Управление инцидентами → Уровни критичности.**
5. Настройте категории инцидентов в разделе **Настройки → Управление инцидентами → Категории инцидентов**. Категории определяют состав полей, используемых для описания инцидентов и цикл обработки для этих инцидентов.

   При создании/редактировании категории укажите:

   - состав и свойства входящих в нее полей (чтобы создать новое поле, перейдите в раздел **Настройки → Управление инцидентами → Поля инцидентов**);
   - используемый цикл обработки;
   - связанные типы инцидентов.
6. Настройте интеграции с внешними системами для автоматического получения данных об инцидентах в разделе **Настройки → Управление инцидентами → Интеграция с внешними системами**.
7. Создайте сценарии для автоматизации процесса обработки инцидентов в разделах **Настройки → Управление инцидентами → Сценарии реагирования** .
8. Настройте удобный для вас набор столбцов, выводимых на экран в разделе **Инциденты**.
9. С помощью фильтров создайте вкладки в разделе **Инциденты** для более быстрого доступа к определенным инцидентам.
10. В разделе **Дашборд** создайте панели графиков, на которых будет отображаться нужная вам информация об инцидентах.

6.3. Создание инцидента

В этом разделе приведены инструкции по созданию инцидента различными способами.

- Создание инцидента вручную
- Создание инцидента по шаблону

- Создание инцидента из уязвимости группы ИТ-активов
- Создание инцидента в группе
- Создание инцидента из уязвимости вручную
- Создание инцидента из меню ПО вручную
- Создание инцидента из данных по протоколу syslog

Вы можете настроить автоматическое создание инцидента из уязвимостей с помощью политик управления уязвимостями.

6.3.1. Создание инцидента вручную

Вы можете создать новый инцидент вручную с пустыми полями или использовать шаблон. Новый инцидент можно сохранить как шаблон.

Чтобы создать новый инцидент вручную (без использования шаблона), выполните следующие действия:

1. Перейдите в раздел **Инциденты**.
2. Нажмите на кнопку  .
3. В появившемся меню выберите категорию инцидента.
4. Если вы работаете в режиме Multi-tenancy, система предложит вам выбрать организацию.
5. Заполните поля инцидента (список доступных полей зависит от выбранной категории / типа инцидента и настроенного представления):
   a. Тип инцидента.
   b. Способ реализации (если доступно для выбранной категории).
   c. Статус инцидента.
   d. Ответственный (по умолчанию устанавливается пользователь, создающий инцидент). Если пользователь, ответственный за инцидент, назначает ответственным другого пользователя, то он добавляется в рабочую группу инцидента в качестве участника с правами на изменение.
   e. Уровень инцидента.
   f. Плановая дата устранения инцидента.
   g. Количественная (в рублях) и качественная оценка ущерба, нанесенного в результате реализации инцидента.

h. Описание инцидента.

i. Локация. Можно указать несколько локаций из справочника или координаты. Кнопка + добавляет дополнительную строку ввода локации. Кнопка добавляет координаты в справочник. Флажок **Использовать локацию связанных активов** добавляет к локациям инцидента локации связанных активов. Максимальное количество локаций задается в свойствах поля **Локации**. Если задано ограничение на количество локаций, то локации связанных активов не используются.

j. При создании нового инцидента следующие поля заполняются автоматически:

i. Дата создания инцидента (не редактируемо).

ii. Дата выявления инцидента (нельзя очистить).

iii. Дата последнего обновления инцидента.

iv. Счетчик времени.

6. Вы можете включить этот инцидент в отчет по форме 0403203, установив флажок **Включить в отчет 0403203**. Флажок доступен, если в поле **Организация** указана организация со следующими параметрами : Вид деятельности - **Банковская**, Страна нахождения - **Российская Федерация.**

7. Если флажок установлен, то в списке кнопок в свойствах инцидента появится дополнительная кнопка **Параметры (0403203)** ( ).

8. Для организаций из Российской Федерации, связанных с банковской деятельностью, вы можете заполнить параметры инцидента любого типа в соответствии с регламентом ФинЦЕРТ. Для этого установите флажок **Подлежит передаче в ФинЦЕРТ**. Если флажок установлен, то справа отобразится ссылка **Заполнить описание**, и в списке кнопок в свойствах инцидента появится дополнительная кнопка **ФинЦЕРТ** ( ). По ссылке и по кнопке открывается раздел для заполнения параметров инцидента по регламенту ФинЦЕРТ.

9. Нажмите на кнопку **Добавить инцидент**. Инцидент будет сохранен в системе. Пользователь, ответственный за инцидент, получит на электронную почту соответствующее уведомление.

С помощью опции **Сохранить как шаблон** в меню **Добавить инцидент** вы можете сохранить созданный инцидент как шаблон. Шаблон можно использовать в дальнейшем для создания подобных инцидентов.

10. Перейдите к заполнению дополнительных полей инцидента по кнопке  . При добавлении полей инцидентов для каждого поля можно определить, является оно основным и обязательным для заполнения или дополнительным. Поля, указанные как дополнительные, отображаются в разделе **Дополнительные поля** свойств инцидента.
11. При создании инцидента можно указать:
    a. Связанные активы ().
    b. Описание инцидента: файлы свидетельств ().
    c. Описание инцидента: причины возникновения ().

После добавления нового инцидента ИБ созданная запись появится во вкладке **Инциденты** и инциденту будет присвоен уникальный идентификатор. Данный идентификатор также определяет уникальный адрес (URL)

http://<имя сервера R-Vision>/#incidents:<номер инцидента>,

который может быть использован для быстрого доступа к инциденту путем перехода по соответствующей ссылке. Адрес инцидента (URL) всегда отображается в адресной строке браузера при выборе инцидента в общем списке.

6.3.2. Создание инцидента по шаблону

Вы можете ускорить создание инцидентов с помощью шаблонов. Шаблоны позволяют использовать ранее заданные в шаблоне значения полей для создания инцидентов.

Для создания инцидента потребуется шаблон, доступный пользователю, который создает инцидент.

Чтобы создать инцидент с помощью шаблона, уже существующего в системе:

1. Перейдите в раздел **Инциденты**.
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования инцидента.
3. Откройте меню **Добавить инцидент**.

4. Перейдите в меню **По шаблону** и выберите шаблон.
5. В появившемся окне выберите организацию. Инцидент будет создан в системе и доступен для дальнейшего редактирования.

6.3.3. Создание инцидента из уязвимости группы ИТ-активов

Вы можете создать инцидент из уязвимости **Группы ИТ-активов**:

1. Вручную в разделе **Активы →Группы ИТ-активов** (см. инструкцию ниже).
2. Автоматически с помощью политик.

Чтобы создать инцидент, выполните следующие действия:

1. Перейдите в раздел **Активы →Группы ИТ-активов.**
2. По правой клавише мыши откройте контекстное меню актива, для которого вы хотите создать инцидент.
3. Выберите опцию **Создать инцидент по уязвимостям**. На экране отобразится окно создания инцидента.
4. Укажите узлы, для которых вы хотите создать инцидент.
5. Укажите уязвимости. В таблице отображаются уязвимости по выбранным узлам группы.
6. Нажмите на кнопку **Создать инцидент**. В разделе **Инциденты** автоматически создается инцидент с категорией **Событие безопасности** и типом **Обнаружение уязвимостей**. Связанное оборудование инцидента: узлы, выбранные в окне выбора узлов и группа активов, по уязвимостям которой был создан инцидент

В разделе **Свидетельства** свойств инцидента автоматически создается отчет по уязвимостям для инцидента и хостам, с которым они связаны.

Контекстное меню доступно пользователям со следующими правами:

- Администратор безопасности группы ИТ-активов в отношении своих активов.
- Пользователям, в свойствах системной роли разрешен доступ к уязвимостям.

6.3.4. Создание инцидента в группе

В группу можно добавить:

- Инцидент из списка инцидентов в системе.

- Создать новый инцидент, входящий в группу (см. инструкцию ниже).

Чтобы создать новый инцидент, входящий в группу:

1. Перейдите на вкладку **Инциденты**.
2. В списке выберите родительский инцидент группы инцидентов. Родительский инцидент группы отмечен в списке индикатором  .
3. Создайте новый инцидент в группе одним из двух способов:
   a. С помощью опции **Новый инцидент в группе** контекстного меню родительского инцидента.
   b. С помощью опции **Создать новый** в поле **Дочерние инциденты** в карточке родительского инцидента.
4. В правой части экрана отобразится область редактирования свойств инцидента. Заполните поля инцидента.
5. Нажмите на кнопку **Добавить**. Система создаст дочерний инцидент в составе выбранной группы.

6.3.5. Создание инцидента из уязвимости вручную

По факту обнаружения уязвимости можно создать инцидент.

> Можно настроить автоматическое создание инцидентов из уязвимостей с помощью политик.

Чтобы создать инцидент на основании выбранной уязвимости, выполните следующие действия:

1. Перейдите в раздел **Уязвимости → Уязвимости.**
2. Нажмите на кнопку  или откройте контекстное меню уязвимости по правой клавише мыши. Можно выделить группу одинаковых уязвимостей (на разных узлах), чтобы создать инцидент, связанный с этими узлами.
3. В появившемся меню выберите действие **Создать инцидент.** На экране отобразится окно настройки инцидента.
4. Задайте параметры инцидента: краткое описание, ответственный и уровень критичности.
5. Нажмите на кнопку **Создать**. В разделе **Инциденты** создается инцидент со следующими параметрами:

- Категория: **Событие безопасности**.
- Тип: **Обнаружение уязвимостей**.
- Дата выявления: дата обнаружения уязвимости.
- Дата создания: дата создания инцидента.
- Источник информации об инциденте ИБ: источник уязвимости, по которой был создан инцидент.
- Краткое описание: текст, включающий в себя общие сведения об уязвимости (ID, уровень критичности, название), ее описание и решение (при наличии).

В разделе **Свидетельства** свойств инцидента будет автоматически создан отчет по уязвимостям для узлов, связанных с инцидентом.

6.3.6. Создание инцидента из меню ПО вручную

Инцидент можно создать для активов типа ПО из контекстного меню.

Чтобы создать инцидент:

1. Перейдите в раздел **Активы → ПО**.
2. Выберите активов типа ПО.
3. Откройте контекстное меню актива по правой клавише мыши и выберите опцию **Создать инцидент**. На экране отобразится окно создания инцидента.
4. Выберите категорию инцидента.
5. Выберите тип инцидента.
6. Укажите параметры инцидента (набор доступных параметров зависит от типа инцидента).
7. Нажмите на кнопку **Добавить инцидент**. В разделе **Инциденты** создается инцидент с заданными параметрами. Инцидент автоматически связывается с активом, из которого он был создан.

6.3.7. Создание инцидента из данных по протоколу syslog

Система поддерживает обмен данными по протоколу syslog. Эти данные могут использоваться для создания инцидентов в системе. По умолчанию данный сервис выключен.

Чтобы система могла создавать инциденты на основе данных, полученных по syslog, включите этот сервис:

1. Подключитесь по протоколу SSH к серверу, на котором установлена система.

```
ssh user@smpserver
```

2. Перейдите в папку **common:**

```
cd /opt/r-vision/data/smp/volumes/common/
```

3. Добавьте в файл **config** следующие строки:

```
[services.syslog]
start = true
```

4. Перейдите в в папку **smp:**

```
cd /opt/r-vision/app/smp/
```

5. Выполните следующую команду:

```
./command.sh up -d --force-recreate syslog
```

Сервис syslog включен.

6.4. Изменение инцидента: особенности

Изменение параметров инцидента имеет ряд особенностей.

Примечание

Дата и время внесения изменений в инцидент автоматически обновляется после каждого изменения инцидента. Вы можете фильтровать список инцидентов по этому параметру.

6.4.1. Изменение ответственного за инцидент

Ответственного за инцидент можно изменить:

- Вручную в свойствах инцидента.
- Автоматически с помощью действия **Назначение**.

Если пользователь, ответственный за инцидент, назначает ответственным другого пользователя, то он добавляется в рабочую группу инцидента в качестве участника с правами на изменение.

Если пользователь, системная роль которого имеет настройку **Инциденты → Видит все инциденты** меняет ответственного за инцидент, то система направляет ему запрос о дальнейших действиях по отношению к пользователю, с которого сняли роль ответственного: удалить из рабочей группы, оставить в рабочей группе с правом на чтение, или оставить в рабочей группе с правом на изменение

6.4.2. Изменение категории инцидента

При изменении категории и/или типа инцидентов нужно указать, данные каких полей должны быть перенесены путем сопоставления текущих и целевых полей в таблице. По умолчанию данные из полей, для которых не заданы целевые поля в новом типе инцидента, будут удалены. В таблице отображаются только не совпадающие поля (полностью совпадающие поля сохраняют значение). Если у инцидента был указан тип, то при изменении категории, система автоматически присваивает этот тип инциденту, если он есть в новой категории. Если в новой категории такого типа нет – тип не присваивается.

6.5. Просмотр инцидента

Список инцидентов, созданных в системе, отображается в разделе **Инциденты**. В правой части экрана отображается карточка с параметрами выбранного инцидента. Если инцидент не выбран, то карточка по умолчанию свернута. Вы можете свернуть и развернуть карточку с помощью кнопки  .

Инцидент является непросмотренным, пока его карточка не открыта пользователем. Непросмотренные инциденты в списке выделены жирным шрифтом.

Пометить инцидент как просмотренный можно одним из двух способов:

- Выберите инцидент в списке. Инцидент будет помечен как просмотренный.
- Откройте контекстное меню инцидента в списке по правой клавише мыши. Выберите опцию **Отметить как просмотренный** в контекстном меню инцидента.

Пометить инцидент как непросмотренный можно с помощью опции **Отметить как непросмотренный** в контекстном меню инцидента**.**

Можно пометить все инциденты на вкладке как просмотренные или непросмотренные с помощью опций контекстного меню. Контекстное меню открывается по щелчку правой клавишей мыши на заголовке вкладки.

В столбце в левой части формы, отображающей параметры инцидентов**,** вертикально расположены кнопки управления процессом создания записей об инцидентах.

Открыть инцидент из списка в отдельной вкладке можно следующими способами:

- двойным щелчком мыши на строке инцидента в списке.
- нажмите на кнопку в столбце **ID** в списке.
- откройте контекстное меню инцидента по правой клавише мыши и выберите опцию **Открыть в отдельной вкладке**.

6.6. Действия по реагированию на инцидент

Автоматизация действий по реагированию на инцидент в системе выполняется следующими способами:

1. Путем добавления действий по инциденту различных типов в свойствах инцидента.
2. Путем добавления сценариев реагирования, которые представляют собой последовательность действий и срабатывают при выполнении заданных условий.

Если у действия есть результат выполнения, он доступен по нажатию кнопки  . Эта кнопка доступна в записи действия в списке действий инцидента либо в блоке действия на диаграмме сценария.

В этом разделе приведены инструкции по добавлению действий в инцидент, просмотру действий на схеме, просмотру прогресса реагирования на инцидент и работе с переменными.

- Просмотр действий по инциденту
- Просмотр прогресса выполнения действий по инциденту
- Модификаторы полей-массивов

6.6.1. Просмотр действий по инциденту

Действия по инциденту можно просмотреть на диаграмме (предпочтительный способ) либо в списке.

- Диаграмма действий по инциденту
- Список действий по инциденту

6.6.1.1. Диаграмма действий по инциденту

С помощью кнопки **Диаграмма**, которая расположена в заголовке списка действий по инциденту, вы можете просмотреть графическое отображение дерева действий для этого инцидента. Переходы между действиями отмечены стрелками.

Чтобы просмотреть действия по инциденту на схеме, выполните следующие действия:

1. Перейдите в раздел **Инциденты**.
2. Выберите инцидент, для которого вы хотите просмотреть действия. В правой части экрана отобразится область редактирования параметров инцидента.
3. Нажмите на кнопку  . В правой части экрана отобразится список действий по инциденту.
4. Нажмите на кнопку **Диаграмма**. На экране отобразится дерево действий. Слева от дерева отображается хронология выполнения действий: линия с указанием даты и времени выполнения действия.

В правом верхнем углу окна диаграммы расположены кнопки управления:

- Кнопка  разворачивает окно диаграммы.
- Кнопка  закрывает диаграмму.

В каждом блоке диаграммы отображается тип, статус, наименование и описание действия. Вы можете открыть окно свойств действия по двойному щелчку мыши на блоке.

В блоке расположены кнопки управления действием: отображает окно редактирования действия.

- отображает результаты выполнения действия.

В правом нижнем углу окна расположена кнопка , управляющая отображением блоков на схеме. После ее нажатия появляется панель, на которой вы можете включить и отключить отображение запланированных и удаленных действий, развернуть и свернуть все сценарии, а также настроить интервал группировки действий на диаграмме. Действия будут сгруппированы с заданным временным шагом..

Масштаб схемы можно увеличить по двойному щелчку на свободном месте. Вернуться к отображению схемы целиком можно, выполнив двойной щелчок мышью повторно.

Кнопки и позволяют изменять масштаб схемы постепенно. Кнопка отображает схему целиком.

Навигацию по схеме при увеличении масштаба можно выполнять перемещением рамки по мини-карте, расположенной в правом нижнем углу окна.

6.6.1.2. Список действий по инциденту

Чтобы просмотреть действия по инциденту в списке:

1. Перейдите в раздел **Инциденты**.
2. Выберите инцидент, для которого вы хотите просмотреть действия. В правой части экрана отобразится область свойств инцидента.
3. Нажмите на кнопку (**Действия по инциденту**). В области свойств отобразится список действий по инциденту. В таблице показывается наименование действия, наименование сценария реагирования (если действие добавлено в рамках сценария реагирования) или имя пользователя (если действие добавлено вручную), статус действия.

6.6.2. Просмотр прогресса выполнения действий по инциденту

Вы можете просмотреть прогресс реализации действий по реагированию на инцидент в следующих разделах:

- В столбце **Прогресс действий** списка инцидентов в разделе **Инциденты**.
- В разделе **Общие сведения** свойств инцидента. Индикатор отображает процентное отношение количества действий со статусом **Завершено** относительно общего количества действий по инциденту.

6.6.3. Модификаторы полей-массивов

Для работы с полями-массивами доступны следующие модификаторы:

:json - выводит содержимое массива как JSON в одну строку. Используется по умолчанию. Этот модификатор можно опустить.

:json_readable - выводит содержимое массива как JSON с отступами и переносами.

:csv - выполняет ввод или вывод содержимого массива в формате CSV с заданным разделителем (по умолчанию - запятая). Разделитель указывается в конце модификатора (запятую можно не указывать). Например, для вывода CSV в стиле MS Office (разделитель - точка с запятой) используется модификатор :csv; или модификатор :scsv (эквивалент :csv). Ячейки, содержащие символы-разделители, выводятся в двойных кавычках.

:html - выполняет вывод содержимого массива в виде html-таблицы.

Модификаторы можно указать в разделах системы, где выполняется работа с полями-массивами:

- Действия по инциденту: Уведомление, Запуск коннектора, Запрос информации, Циклическое действие.
- Действия в рамках сценария реагирования: **Уведомление**, **Модификация, Запуск коннектора**, **Запрос информации**, **Циклическое действие**. Модификатор вводится через двоеточие после тега поля, которое используется для вывода значений.

При вводе значения модификатор выбирается из выпадающего списка.

6.7. Настройка доступа к инциденту: рабочая группа

Вы можете добавить пользователя или группу пользователей в рабочую группу инцидента одним из двух способов:

- Автоматически. Вы можете создавать сценарии реагирования, в результате выполнения которых пользователи будут назначаться автоматически согласно определенным критериям.
- Вручную в свойствах инцидента.

Чтобы добавить пользователя в рабочую группу вручную, выполните следующие действия:

1. Перейдите в раздел **Инциденты**.
2. Выберите в списке или откройте двойным щелчком мыши инцидент, рабочую группу которого вы хотите определить.
3. Нажмите на кнопку  . В правой части экрана отобразится список участников рабочей группы.
4. Нажмите на кнопку **Добавить**. На экране отобразится окно **Рабочая группа**, в котором вы можете указать членов рабочей группы и определить их права доступа.
5. Сформируйте список пользователей и групп пользователей. В состав рабочей группы могут быть включены пользователи из раздела **Персонал**, даже если их учетная запись не существует в системе (в этом случае система автоматически добавит ее в общий список пользователей). Вы можете добавить пользователя из раздела **Персонал** с помощью кнопки **Добавить пользователя из раздела Персонал**. Если в свойствах инцидента не указан ответственный, любой пользователь с правами на **Изменение** сможет назначить себя на эту роль.
6. Определите права доступа к полям (изменение, чтение) указанных участников рабочей группы. По умолчанию участники имеют права на изменение. Флажок **Только чтение** предоставляет права только на просмотр данных по инциденту. Если для члена рабочей группы установлен флажок **Без ограничений**, ему станут доступны поля со свойством **Ограничение**, при этом возможность чтения и изменения будет определяться установленным уровнем доступа. Пользователь, назначенный ответственным за инцидент, имеет полный доступ к полям инцидента, в том числе и к тем, для которых установлено ограничение на доступ. Уровень доступа пользователя с флажком **Без ограничений** отмечен звездочкой в списке пользователей.
7. Нажмите на кнопку **Сохранить**. Выбранные пользователи и группы будут добавлены в рабочую группу и отобразятся в списке.

В списке участников рабочей группы отображаются права пользователей, указанные для них в момент добавления. Они не всегда соответствуют реальным правам, поскольку пользователи могут состоять в нескольких группах, также включенных в инцидент в качестве участников с различными уровнями доступа. Столбец **Итоговый доступ** отображает результирующие права пользователей (с учетом членства в нескольких группах).

Удалить пользователя или группу пользователей из рабочей группы можно по кнопке  .

Примечание

- Права, указанные для группы пользователей, назначаются всем входящим в группу пользователям.
- Если в группу пользователей добавляется новый пользователь, он получает все связанные с группой специальные роли в отношении соответствующих инцидентов.
- Если группа пользователей удалена в разделе **Настройки → Пользователи**, то она удаляется из рабочей группы. Специальная роль участника инцидента при этом снимается со всех входивших в нее пользователей.
- Если группа удалена из инцидента, все ее члены теряют специальную роль в отношении этого инцидента.
- Если пользователя удаляют из группы, он теряет связанные с группой специальные роли по инцидентам.
- В перечисленных выше случаях пользователь не потеряет специальные роли в отношении инцидентов, если он был добавлен в их рабочую группу напрямую (через режим «пользователи», а не через связь с группой).
- Если несколько групп добавлены в рабочую группу и в каждую из них входит один и тот же пользователь, то он получает максимальный уровень доступа.

6.8. Описание инцидента

- Описание инцидента: добавление комментариев
- Описание инцидента: индикаторы
- Описание инцидента: почтовая переписка
- Описание инцидента: файлы свидетельств
- Описание инцидента: причины возникновения
- Описание инцидента: параметры 040203

- Описание инцидента: ФинЦЕРТ

6.8.1. Описание инцидента: добавление комментариев

Чтобы добавить комментарий, выполните следующие действия:

1. Перейдите в раздел **Инциденты**.
2. Выберите инцидент, для которого вы хотите оставить комментарий.
3. Нажмите на кнопку  . В правой части экрана вы можете просмотреть имеющиеся комментарии и ввести новый.
4. В поле ввода комментариев внизу введите символ "@", чтобы указать получателя комментария. В новом окне отобразится список пользователей. Для каждого пользователя указывается, входит ли пользователь в рабочую группу по инциденту. При отправке комментариев пользователю, не входящему в рабочую группу по инциденту, можно добавить этого пользователя в рабочую группу или только оповестить его.
5. После выбора получателя комментария введите текст в поле ввода и нажмите на клавишу **Enter**. Комментарий будет доступен для автора замечания, ответственного лица и пользователя, у которого есть доступ к разделу, в котором находится элемент, на уровне системной роли.

Комментарий отображается в ленте уведомлений указанного пользователя. При нажатии на ссылку в уведомлении открывается раздел **Комментарии** свойств инцидента.

6.8.2. Описание инцидента: индикаторы

К инциденту вы можете прикрепить индикаторы компрометации - данные, которые могут быть признаками вредоносной активности в инфраструктуре. В этом разделе приведены инструкции по работе с индикаторами, связанными с инцидентом.

Права доступа к разделу **Индикаторы** можно настроить в разделе **Индикаторы** свойств системной роли пользователя.

- Добавление индикатора к инциденту
- Просмотр связанных индикаторов

6.8.2.1. Добавление индикатора к инциденту

Вы можете добавить к инциденту индикаторы компрометации вручную (см. инструкцию ниже) или с помощью запросов API.

Чтобы добавить индикаторы компрометации, выполните следующие действия:

1. Перейдите в раздел **Инциденты**.
2. Выберите в списке или откройте двойным щелчком мыши инцидент, для которого вы хотите добавить индикаторы.
3. Нажмите на кнопку Индикаторы ( ). В правой части экрана отобразится список индикаторов.
4. Нажмите на кнопку **Добавить**. На экране отобразится окно **Связанные индикаторы**.
5. Укажите значение и тип индикатора.
6. Нажмите на кнопку **Добавить**. Индикатор отобразится в списке связанных индикаторов.

6.8.2.2. Просмотр связанных индикаторов

Чтобы просмотреть связанные индикаторы, выполните следующие действия:

1. Перейдите на вкладку **Инциденты**.
2. В списке выберите инцидент и откройте раздел индикаторов по кнопке **Индикаторы** ( ). В области свойств инцидента отобразится список связанных индикаторов.

6.8.3. Описание инцидента: почтовая переписка

Система позволяет вести почтовую переписку по инциденту. В рамках почтовой переписки пользователи системы могут отправлять сообщения по электронной почте, получать ответы, а также вести дальнейшую переписку в рамках своей цепочки писем по инциденту в интерфейсе системы. К входящим и исходящим электронным письмам в переписке могут быть прикреплены файлы произвольного формата.

Почтовая переписка позволяет обмениваться электронными письмами только по уже существующему в системе инциденту. Первое письмо цепочки должно быть отправленным из системы. Входящее письмо добавляется в цепочку, если оно содержит служебный заголовок с тем же идентификатором, что и остальные письма в цепочке.

Переписка в инциденте может быть добавлена к инциденту:

- вручную пользователем
- автоматически в результате запуска на инциденте действия **Запрос информации** в режиме **Начать переписку по инциденту**.

Для корректной работы функции почтовой переписки вам необходимо выполнить настройку почтовых серверов и настроить отображение раздела в настройках представлений.

- Настройка почтовых серверов
- Работа с почтовой перепиской

6.8.3.1. Настройка почтовых серверов

Для корректной работы с почтовыми переписками в инцидентах необходимо настроить почтовые серверы, которые будут обрабатывать входящую и исходящую электронную почту. Для **каждого** адреса электронной почты, который вы собираетесь использовать в почтовой переписке, необходимо настроить **два** почтовых сервера, а именно:

- сервер исходящей почты;
- сервер входящей почты.

Раздел настройки доступен пользователям, в свойствах системной роли которых на вкладке **Общее** разрешен доступ к разделу **Почтовая переписка**.

> Работа почтовой переписки и почтовой интеграции с одним почтовым ящиком в настоящее время не поддерживается.

Для того, чтобы настроить почтовые серверы, выполните следующие действия:

1. Перейдите в раздел **Настройки → Управление инцидентами → Почтовая переписка.**
2. Нажмите на кнопку **Создать.**
3. Укажите адрес электронной почты.
4. Укажите, для каких сообщений будет использоваться сервер - **входящих** или **исходящих**.
5. Выполните настройки сервера (общие для серверов входящей и исходящей почты):

- Выберите почтовый протокол. Если выбран протокол EWS, укажите его версию.
- Укажите данные почтового сервера: IP-адрес/домен сервера, сведения о шифровании и порт.
- Укажите, нужно ли проверять подлинность сертификата (только для протокола IMAP) и использовать прокси-сервер.
- Выберите тип аутентификации.
- Введите логин и пароль.

6. Для сервера входящей почты выполните дополнительные настройки:
   - Установите флажок **Удалять после прочтения**, если вам необходимо удалять прочитанные письма из почтового ящика.
   - Укажите периодичность запуска выгрузки писем из почтового ящика.
7. Для сервера исходящей почты укажите, будет ли эта настройка использоваться по умолчанию.
8. Нажмите на кнопку **Сохранить**. Настройка почтового сервера сохранится в системе.
9. Проверьте правильность устанавливаемого соединения, нажав на кнопку **Проверить**.

6.8.3.1.1 Рекомендации по работе с почтовой перепиской

Если в почтовой переписке карточки инцидента не отправляются или не приходят ответные сообщения, в первую очередь перепроверьте настройки серверов. Если рядом с названием в таблице настроек отображается  , настройка является нерабочей и необходимо проверить ее правильность.

Если вы отправляете письма с помощью функции почтовой переписки карточки инцидента, система выгружает ответы на эти письма и отображает их в карточке инцидента не мгновенно, а согласно расписанию почтового сервера. Это расписание задается в настройках сервера входящей почты.

Ответ на письмо, созданное в почтовой переписке карточки инцидента, не отобразится в переписке, если будет прочитан до того, как система выгрузит его в соответствии с расписанием. Для сохранения ответа в карточке инцидента убедитесь, что оно не будет прочитано в почтовом клиенте - как пользователями, так и автоматически.

6.8.3.2. Работа с почтовой перепиской

6.8.3.2.1 Просмотр переписок

Кнопка  в свойствах инцидента позволяет просмотреть почтовые переписки по инциденту. Система отобразит список доступных переписок в правом окне.

> Для того, чтобы система отобразила переписку в карточке инцидента, необходимо включить раздел **Почтовая переписка** в настройки представлений.

Для переписки отображаются следующие статусы:  - письмо отправлено, но ответ от сервиса переписок еще не получен.  - сервис переписок по каким-либо причинам недоступен (например, при некорректных настройках почтового шлюза).

Кнопка меню в строке переписки позволяет отобразить меню переписки. Доступны следующие команды:

- **Отметить прочитанным** - отметить все входящие сообщения прочитанными.
- **Параметры переписки** - переименовать переписку.

6.8.3.2.2 Просмотр сообщений в переписке

Переписка открывается двойным щелчком мыши. Система отобразит все имеющиеся в переписке сообщения. Если в письме имеется вложение, в правом нижнем углу сообщения показывается иконка скрепки.

Сообщения показываются в сокращенном виде и открываются по двойному щелчку мыши.

Кнопка  в поле сообщения отображает меню сообщения. Доступны следующие команды:

- **Удалить** - удалить письмо из переписки.
- **Копировать текст** - скопировать текст сообщения в буфер.

- **Переслать** - отобразить окно для пересылки сообщения другому адресату.
- **Ответить** - отобразить окно для ответа отправителю сообщения. Отправка ответов в почтовой переписке доступна только пользователям с ролью, у которой в разделе **Инциденты** установлен флажок **Отправка ответов в почтовых переписках**.

Скачать вложение можно двойным щелчком мыши по полю вложения в открытом сообщении.

6.8.3.2.3 Создание нового сообщения и ответ на сообщение

В системе можно создать новое сообщение, открыв им переписку, и ответить на имеющиеся в переписках сообщения.

> Почтовый ящик может использоваться для отправки сообщений только, если для него настроены параметры серверов входящей и исходящей почты.

Создание нового сообщения

1. Нажмите на кнопку **Добавить** в окне **Почтовая переписка**, чтобы начать новую переписку. Отобразится окно для создания первого сообщения в новой переписке.
2. Укажите отправителя.
3. Укажите адресата и тему сообщения.
4. Для отправки копии/скрытой копии сообщения другому адресату нажмите на кнопку **Копия** или **Скрытая копия** и укажите адрес.
5. Вы можете прикрепить к сообщению файл или имеющиеся свидетельства по инциденту. Суммарный размер вложений не должен превышать 20 МБ. Нажмите на кнопку и выберите один из пунктов меню:
   a. **Вставка из свидетельств**.
   b. **Прикрепить файл**.
6. Для отправки сообщения нажмите на кнопку **Отправить**.

Начинать переписку и отправлять ответы могут пользователи, в свойствах системной роли которых на вкладке **Инциденты** разрешена отправка ответов в почтовых переписках.

Ответ на сообщение

1. В системе предусмотрено два способа ответа на сообщение:
   a. Выберите в переписке сообщение, на которое необходимо ответить, и нажмите на кнопку **Ответить** или **Ответить всем** в самом низу панели. Отобразится окно для ответа отправителю выделенного сообщения или всем участникам этой переписки.
   b. Дважды нажмите на сообщение в переписке. Отобразится окно для ответа отправителю этого сообщения. При создании сообщения вам доступны режимы визуального редактора, HTML-кода или обычного текста.
2. Дальнейшие шаги (указание адресата, прикрепление сообщения и отправка) аналогичны шагам для создания нового сообщения.

Для отправки сообщений система всегда будет использовать почтовый ящик, с которого отправлялось первое сообщение в переписке.

6.8.4. Описание инцидента: файлы свидетельств

К зарегистрированному в системе инциденту вы можете прикрепить свидетельства - файлы, содержащие дополнительную информацию, собранную в ходе обработки инцидента.

- Добавление свидетельства к инциденту
- Просмотр файлов свидетельства
- Скачивание файла свидетельства на локальный диск

6.8.4.1. Добавление свидетельства к инциденту

Вы можете добавить к инциденту файлы свидетельств. Объем файла не должен превышать 50 МБ.

Чтобы добавить файлы свидетельств, выполните следующие действия:

1. Перейдите в раздел **Инциденты**.
2. Выберите в списке или откройте двойным щелчком мыши инцидент, для которого вы хотите добавить свидетельства.

3. Нажмите на кнопку . В правой части экрана отобразится список свидетельств.
4. Нажмите на кнопку **Добавить**. На экране отобразится окно выбора файла.
5. Выберите файлы для добавления и нажмите на кнопку **Открыть**.

> Файлы можно также добавить перетаскиванием на выделенную область.

Файлы отобразятся в списке. Система автоматически заполняет наименование свидетельства именем файла. Настроить параметры свидетельства можно по кнопке **Изменить**. При загрузке файлов система автоматически рассчитает контрольную сумму для загруженного файла. Вы можете удалить файл с помощью кнопки **Удалить**.

6.8.4.2. Просмотр файлов свидетельства

Чтобы просмотреть содержимое файлов, загруженных в систему, из веб-интерфейса системы, выполните следующие действия:

1. Перейдите на вкладку **Инциденты**.
2. В списке выберите инцидент и откройте раздел настройки свидетельств с помощью кнопки .
3. Откройте окно просмотра свидетельства двойным щелчком мыши на нужной строке в списке свидетельств.

6.8.4.3. Скачивание файла свидетельства на локальный диск

Чтобы скачать один или все файлы свидетельства на локальный диск, выполните следующие действия:

1. Перейдите в раздел **Инциденты**.
2. Выберите в списке или откройте двойным щелчком мыши инцидент, свидетельства которого вы хотите скачать.
3. Нажмите на кнопку . В правой части экрана отобразится список свидетельств.
4. Скачайте свидетельство одним из двух способов:

a. Наведите курсор мыши на строку свидетельства и нажмите на кнопку в строке свидетельства.

b. Выберите свидетельство, которое вы хотите скачать и нажмите на кнопку **Скачать** и укажите опцию: **Текущий файл** или **Скачать все**.

5. Укажите путь для скачивания. Свидетельство будет загружено по указанному пути.

6.8.5. Описание инцидента: причины возникновения

Настроить причины возникновения, которые доступны в свойствах инцидента, можно в справочнике **Настройки → Управление инцидентами → Справочники → Причины возникновения**.

Чтобы указать причины, выполните следующие действия:

1. Перейдите в раздел **Инциденты**.
2. Выберите в списке или откройте двойным щелчком мыши инцидент.
3. Нажмите на кнопку . В правой части экрана отобразится список причин возникновения. Установите фильтр **Показать все** над списком, чтобы просмотреть полный список причин возникновения. Для просмотра связанных причин выберите опцию **Только связанные**.
4. Укажите причины возникновения инцидента.

6.8.6. Описание инцидента: параметры 040203

Если организация, к которой принадлежит инцидент, занимается банковской деятельностью, и в свойствах инцидента установлен флажок **Включить в отчет 0403203**, то в свойствах инцидента становится доступен раздел **Параметры (0403203)** ( ).

В этом разделе вы можете задать специфические параметры инцидента для включения в отчет 0403203.

Набор доступных типов 0403203 зависит от указанных видов деятельности в разделе **Сведения об участии в НПС** сведений об организации, к которой относится инцидент (**Настройки → Общие сведения → Организация**).

Чтобы задать описание, выполните следующие действия:

1. Перейдите в раздел **Инциденты**.

2. Выберите в списке или откройте двойным щелчком мыши инцидент, параметры которого вы хотите задать.
3. Нажмите на кнопку  . В правой части экрана отобразится список доступных параметров.
4. Укажите тип 0403203 и заполните поля в соответствии с заданным типом. Указанные параметры будут использованы при формировании отчета по форме 0403203.

6.8.7. Описание инцидента: ФинЦЕРТ

Чтобы передать данные об инциденте в ФинЦЕРТ, для инцидента должны выполняться следующие требования:

- Инцидент должен принадлежать к банковской организации, для которой заданы параметры доступа в ФинЦЕРТ.
- В разделе **Общие сведения** свойств инцидента установлен флажок **Подлежит передаче в ФинЦЕРТ.**

Ввести данные для передачи в ФинЦЕРТ можно в окне **Данные для ФинЦЕРТ** (окно открывается по кнопке ).

> Если форма заполнена автоматически сценарием реагирования и содержит вложенные файлы, то изменение данных вручную приведет к удалению вложенных файлов.

Чтобы задать данные, выполните следующие действия:

1. Перейдите в раздел **Инциденты**.
2. Выберите в списке или откройте двойным щелчком мыши инцидент, параметры которого вы хотите задать.
3. Нажмите на кнопку  . На экране отобразится окно для ввода данных.
4. Задайте основные и дополнительные параметры. Список разделов отображен в левой части окна. Кнопка **Сохранить** сохраняет внесенные изменения без отправки данных в ФинЦЕРТ.
5. При добавлении операции без согласия, вы можете упростить заполнение остальных обязательных параметров электронной формы ФинЦЕРТ с помощью кнопки **Заполнить поля**. Эта кнопка позволяет заполнить поля инцидента автоматически, если значения для них не были введены вручную. Список присваиваемых значений отобразится в

появившемся окне. Для присвоения значений нажмите на кнопку **Заполнить**.

6. После заполнения параметров нажмите на кнопку **Передать в ФинЦЕРТ**. В список действий по инциденту будет добавлено действие типа **Отправка данных в ФинЦЕРТ**. В появившемся окне заполните параметры действия и нажмите на кнопку **Добавить**. Данные будут переданы согласно настройкам действия.
7. Заполненную форму можно скачать в виде JSON-файла, выбрав опцию **Скачать файл** (JSON) в меню, доступном по щелчку на кнопке  .

Снятие отметки **Подлежит передаче в ФинЦЕРТ** в свойствах инцидента приведет к удалению ранее заполненной информации в окне свойств ФинЦЕРТ.

6.9. Отправка уведомлений в ГосСОПКА

Отправка уведомлений и чат с ГосСОПКА доступен пользователям с ролью, в свойствах которой установлен флажок **Отправка инцидентов в ГосСОПКА** в разделе **Инциденты → Дополнительные функции**.

Чтобы отправить уведомление в ГосСОПКА:

1. Перейдите в раздел **Инциденты**.
2. Выберите инцидент в списке. В правой части экрана отобразится область редактирования инцидента.
3. Нажмите на кнопку **Экспорт** () и выберите опцию **Отправка данных в ГосСОПКА**. В правой части экрана отобразится вкладка **ГосСОПКА**, которая содержит параметры инцидента для передачи в ГосСОПКА. Кнопка **Инцидент** в верхней части карточки открывает основной раздел свойств инцидента. После отправки инцидента в ГосСОПКА кнопка **Экспорт** для этого инцидента недоступна.
4. В подразделе **Общие сведения** () на вкладке ГосСОПКА заполните параметры инцидента для передачи в ГосСОПКА. В разделе **Ход обработки уведомления** отображается текущий статус обработки уведомления. Уведомлению могут быть присвоены статусы: **Подготовка уведомления**, **Создано**, **Зарегистрировано**, **Требуется дополнение**, **Проверка НКЦКИ**, **Принято решение**, **Отправлено в архив**.

5. В подразделе **Свидетельства** ( ) сформируйте список свидетельств по инциденту для передачи в ГосСОПКА. Вы можете загрузить файлы или выбрать из текущего набора свидетельств по инциденту. Добавить свидетельства можно до отправки уведомления в ГосСОПКА и в статусе уведомления **Требуется дополнение**.

6. В подразделе **Комментарии** ( ) можно оставлять комментарии для оператора в чате ГосСОПКА. При добавлении комментария система автоматически создает действие по инциденту. Подраздел становится доступен только после передачи инцидента в ГосСОПКА.

7. По завершении работы над карточкой инцидента нажмите на кнопку **Отправить** для передачи инцидента в ГосСОПКА. Система автоматически создает действие по отправке уведомления в ГосСОПКА. В статусах **Создано**, **Зарегистрировано**, **Требуется дополнение**, **Проверка НКЦКИ** доступна кнопка **Обновить,** которая добавляет действие по инциденту **Обновление данных ГосСОПКА**. В рамках действия система получает актуальные значения полей и комментарии из ЛК ГосСОПКА.

Кнопка **Удалить** удаляет карточку ГосСОПКА: данные полей в разделе **ГосСОПКА** удаляются и раздел **ГосСОПКА** не отображается в свойствах инцидента. Кнопка **Экспорт** ( ) в свойствах инцидента становится доступной (если она доступна в рамках роли и представления).

7. УЯЗВИМОСТИ

В этом разделе приведены рекомендации по работе с уязвимостями, обнаруженными системой при сканировании оборудования.

- Принцип работы с уязвимостями
- Добавление уязвимостей
- Просмотр уязвимостей
- Действия по уязвимостям
- Статусы уязвимостей

7.1. Принцип работы с уязвимостями

Система импортирует устройства из различных сканеров уязвимостей:

- Интеграция со сканером безопасности MaxPatrol / XSpider.
- Интеграция со сканером безопасности RedCheck.
- Интеграция со сканером уязвимостей Rapid7 Nexpose.
- Интеграция со сканером безопасности Qualys.
- Интеграция с SIEM-системой MaxPatrol.
- Интеграция с системой управления безопасностью Skybox.
- Интеграция со сканером безопасности Nessus.
- Интеграция с Kaspersky Security Center.

При первом импорте данных из сканеров уязвимостей система создает оборудование с набором выявленных уязвимостей.

При повторном запуске интеграции система импортирует оборудование из сканера и ищет подходящий хост среди хостов, ранее загруженных в систему. После выявления подходящего устройства, система сравнивает перечень пришедших уязвимостей с перечнем уязвимостей, имеющимся на устройстве. В результате сравнения система выполняет действия:

- Открывает новые уязвимости на найденном устройстве.
- Закрывает существующие уязвимости, которые не обнаружены в новом перечне.

Уязвимости поступают в систему из разных источников (разных сканеров) уязвимостей. Уязвимости из разных источников считаются разными.

7.2. Добавление уязвимостей

Уязвимость можно добавить следующими способами:

- Вручную в интерфейсе системы. Связка **Уязвимость-Хост** задается вручную.
- Вручную путем импорта из пользовательского файла отчета.
- Автоматически путем импорта отчета сканера уязвимостей.
- Автоматически при получении данных из интеграций.

Уязвимости, созданные вручную, получают отметку **Создана вручную** в свойствах уязвимости.

7.2.1. Добавление уязвимости вручную в интерфейсе

Добавлять уязвимость могут пользователи, в свойствах системной роли которых отмечены разделы **Права на добавление** и **Уязвимости** на вкладке **Активы**.

Чтобы добавить уязвимость вручную в интерфейсе системы:

1. Перейдите в раздел **Уязвимости → Уязвимости**.
2. Нажмите на кнопку **Добавить уязвимость** ( ). На экране отобразится область настройки уязвимости.
3. Заполните поля:
   a. Название уязвимости.
   b. Описание.
   c. Решение.
   d. Организация.
   e. Оценка и вектор CVSS V2.
   f. Оценка и вектор CVSS V3.
   g. Тип эксплойта.
   h. Ссылки на информацию об уязвимости.
4. В таблице **Оборудование** по кнопке **Добавить** сформируйте список хостов, на которых обнаружена уязвимость.
5. Выберите хост в списке. Справа от списка отобразятся параметры хоста. Вы можете выбрать несколько хостов для группового редактирования.
6. Для каждого хоста заполните поля:
   a. Порт.

b. Протокол.

c. Статус уязвимости на выбранном хосте: **Открыта** или **Закрыта**.

d. Дата обнаружения.

e. Наименование уязвимого ПО на хосте.

f. Версия уязвимого ПО на хосте.

g. Результат сканера.

7. Нажмите на кнопку **Добавить**. Уязвимость будет добавлена в систему. В карточке уязвимости отобразится пометка **Создана вручную**.

7.3. Просмотр уязвимостей

Уязвимости в системе представляют собой сущности, которые содержат все сведения о собранных сканерами и добавленных вручную актуальных уязвимостях.

Вкладка **Уязвимости** содержит информацию об обнаруженных и устраненных уязвимостях в системе. Информацию по конкретной уязвимости можно просмотреть в карточке уязвимости.

- Карточка уязвимости
- Связанное оборудование
- Просмотр статистики по уязвимостям
- Фильтрация списка уязвимостей
- Сквозной поиск

7.3.1. Карточка уязвимости

В карточке уязвимости можно просмотреть и отредактировать сведения об уязвимости, а также удалить эту уязвимость.

Чтобы открыть карточку уязвимости, нажмите на кнопку  в свойствах уязвимости. Кнопка доступна только для уязвимостей, созданных вручную.

7.3.2. Связанное оборудование

В свойствах уязвимости можно просмотреть информацию об оборудовании, на котором обнаружена уязвимость. Статистическую информацию об узлах, на которых обнаружены уязвимости, можно просмотреть по кнопке **Статистика** ( ).

Чтобы просмотреть параметры оборудования в свойствах уязвимости:

1. Перейдите в раздел **Уязвимости → Уязвимости.**
2. Выберите уязвимость, для которой вы хотите просмотреть связанное оборудование.
3. Нажмите на кнопку . В правой части экрана отобразится перечень параметров уязвимости.
4. Перейдите на вкладку **Оборудование**. В области параметров отобразится информация о связанном оборудовании.

В таблицах **Группы ИТ-активов** и **Бизнес-подразделения/Организации** отображаются группы ИТ-активов и подразделения, связанные с выбранной уязвимостью. Наведите курсор на строку актива и щелкните по кнопке , чтобы просмотреть иерархию.

Если уязвимость обнаружена на нескольких узлах, эта уязвимость в списке дублируется для каждого узла.

7.3.3. Просмотр статистики по уязвимостям

В разделе **Статистика** отображается статистика по уязвимостям, зарегистрированным в системе.

Раздел **Статистика** открывается:

- по умолчанию при переходе в раздел **Уязвимости**.
- вручную по кнопке в свойствах уязвимости.

В верхней части информационной области отображается количество уязвимостей по уровням критичности в виде набора кнопок. По нажатию на кнопку система фильтрует список уязвимостей по указанному уровню критичности.

В таблицах ниже приводится количество уязвимостей:

- По типу оборудования.
- По наличию эксплойта.
- По портам.

Кнопка ⇨ фильтрует список уязвимостей по выбранному критерию.

Если список уязвимостей отфильтрован, то статистика отображается по результатам фильтрации.

7.3.4. Фильтрация списка уязвимостей

Список уязвимостей можно фильтровать с помощью настраиваемых фильтров.

Для настройки фильтра нажмите на кнопку над списком уязвимостей в разделе **Уязвимости**.

В строке фильтра отображаются критерии фильтрации и операторы. Вы можете управлять настройками фильтра:

- Кнопка добавляет критерии фильтрации. Чтобы настроить значение критерия, нажмите на критерий в строке фильтра.

  Для **текстовых полей** можно использовать SQL-операторы ilike (проверка соответствия без учета регистра).

- При добавлении двух и более критериев автоматически добавляются операторы. Чтобы выбрать значение оператора (доступны операторы И и ИЛИ), нажмите на оператор в строке фильтра.
- Удалить критерий можно с помощью значка в блоке критерия. Кнопка очищает строку фильтра.
- Сохранить фильтр можно по кнопке . Кнопка создает отдельную вкладку с настроенным фильтром.

7.3.5. Сквозной поиск

При выполнении сквозного поиска в таблице уязвимостей система добавляет в строку фильтра аналогичный фильтр с названием **Поиск по разделу**. Теперь при создании критериев фильтрации, система будет применять эти критерии к значениям таблицы, отфильтрованным согласно условию фильтра **Поиск по разделу**.

Сквозной поиск осуществляется по следующим полям раздела **Общие сведения** карточки уязвимости:

- ID;
- Название;
- Описание;
- Решение;
- Результат сканера;
- Уязвимое ПО (по названию и по версии);
- Ссылки;

- IP и имя связанного оборудования;
- Операционная система.

7.4. Действия по уязвимостям

- Открытие уязвимости
- Признание ложным срабатыванием
- Принятие риска
- Закрытие уязвимости
- Создание вручную задачи
- Создание вручную инцидента

7.4.1. Открытие уязвимости

Уязвимость, которая была ошибочно признана неактуальной, может быть открыта повторно. Переоткрытой уязвимости присваивается статус **Открыта**.

> Уязвимости в статусе **Риск принят** переоткрываются автоматически, если при присвоении этого статуса задан срок истечения.

Открыть уязвимость вручную можно двумя способами:

- С помощью контекстного меню уязвимости.
- По кнопке **Действия** ( ) в свойствах уязвимости.
  Вы также можете открывать уязвимости, создав политику управления уязвимостями.

Чтобы открыть уязвимость вручную, выполните следующие действия:

1. Перейдите в раздел **Уязвимости → Все уязвимости.**
2. Выберите уязвимость в списке. Можно выделить группу уязвимостей, если они относятся к одной организации.
3. Нажмите на кнопку или откройте контекстное меню уязвимости по правой клавише мыши.
4. В появившемся меню выберите действие **Открыть уязвимость**. На экране отобразится запрос причины.
5. Укажите причину действия.
6. Нажмите на кнопку **ОК**. Статус уязвимости изменится на **Открыта**. Причина действия отображается в разделе **Комментарии** ( ) свойств уязвимости.

7.4.2. Признание ложным срабатыванием

Если по результатам анализа данных уязвимость признана ложным срабатыванием, вы можете пометить уязвимость как **Ложное срабатывание** в системе.

Пометить уязвимость как ложное срабатывание вручную можно двумя способами:

- С помощью контекстного меню уязвимости.
- По кнопке **Действия** ( ) в свойствах уязвимости.

Чтобы выполнить действие из свойств уязвимости:

1. Перейдите в раздел **Уязвимости → Все уязвимости.**
2. Выберите уязвимость в списке. Можно выделить группу уязвимостей с одинаковым статусом.
3. Нажмите на кнопку или откройте контекстное меню уязвимости по правой клавише мыши.
4. В появившемся меню выберите действие **Ложное срабатывание**. На экране отобразится запрос причины.
5. Укажите причину действия.
6. Нажмите на кнопку **ОК**. Статус уязвимости изменится на **Ложное срабатывание**. Причина действия отображается в разделе **Комментарии** ( ) свойств уязвимости.

Если уязвимость была ошибочно признана ложным срабатыванием, то ее можно переоткрыть.

Для изменения статуса уязвимости вы можете использовать политику управления уязвимостями.

7.4.3. Принятие риска

Если уязвимость невозможно устранить, но требуется принять факт существования уязвимости (например, если уязвимость задействует технологию, которая не используется в сети), то можно присвоить такой уязвимости статус **Риск принят**.

Принять риск уязвимости вручную можно двумя способами:

- С помощью контекстного меню уязвимости.

- По кнопке **Действия** ( ) в свойствах уязвимости.

Чтобы принять риск уязвимости:

1. Перейдите в раздел **Уязвимости → Уязвимости.**
2. Выберите уязвимость в списке. Можно выделить группу уязвимостей с одинаковым статусом, если они относятся к одной организации.
3. Нажмите на кнопку или откройте контекстное меню уязвимости по правой клавише мыши.
4. В появившемся меню выберите действие **Принять риск**. На экране отобразится запрос подтверждения.
5. Укажите причину действия.
6. Вы можете принять риск на время и установить дату автоматического открытия уязвимости. Установите флажок **Принять риск на время** и задайте дату истечения. После указанной даты система автоматически присвоит уязвимости статус **Открыта**. Дату истечения можно просмотреть в карточке уязвимости.
7. Нажмите на кнопку **ОК**. Статус уязвимости изменится на **Риск принят**. Причина действия отображается в разделе **Комментарии** ( ) свойств уязвимости. Если риск принят на время и задана дата истечения, то система автоматически откроет уязвимость в указанное время.

Уязвимость в статусе **Риск принят** можно открыть вручную, если период автоматического открытия не задан или еще не истек.

7.4.4. Закрытие уязвимости

Система закрывает уязвимости автоматически, когда проведены работы по устранению уязвимости и при повторном сканировании уязвимость не обнаружена. Вы также можете закрывать уязвимости, создав политику управления уязвимостями или вручную. Закрыть уязвимость вручную, не дожидаясь сканирования, можно, например, если вы убедились, что уязвимость устранена.

> Если закрытая уязвимость повторно поступит в систему из сканера уязвимостей, ей будет автоматически присвоен статус **Открыта**.

Закрыть уязвимость вручную можно двумя способами:

- С помощью контекстного меню уязвимости.

- По кнопке **Действия (**) в свойствах уязвимости.

Чтобы закрыть уязвимость вручную, выполните следующие действия:

1. Перейдите в раздел **Уязвимости → Все уязвимости.**
2. Выберите уязвимость в списке. Можно выделить группу уязвимостей, если они относятся к одной организации.
3. Нажмите на кнопку или откройте контекстное меню уязвимости по правой клавише мыши.
4. В появившемся меню выберите действие **Закрыть уязвимость**. На экране отобразится запрос причины.
5. Укажите причину действия.
6. Нажмите на кнопку **ОК**. Статус уязвимости изменится на **Закрыта**. Причина действия отображается в разделе **Комментарии** (**)** свойств уязвимости.

7.4.5. Создание вручную задачи

Из уязвимости можно создать задачу с помощью контекстного меню уязвимости или по кнопке **Действия** ( ) в свойствах уязвимости.

Прогресс устранения уязвимости отображается в виде полосы прогресса в свойствах задачи с типом **Устранение уязвимости**. Ссылка **Детали** открывает раздел **Уязвимости** с фильтрацией по связанным уязвимостям.

Чтобы просмотреть прогресс устранения, откройте связанную с уязвимостью задачу.

Прогресс устранения уязвимости рассчитывается как изменение (в процентах) количества связок **Уязвимость** (в статусе **Открыта**) - **Порт** - **Протокол** - **Хост**, связанных с задачей. Прогресс увеличивается за счет перевода уязвимостей в статус **Закрыта** или **Ложное срабатывание**.

7.4.6. Создание вручную инцидента

По факту обнаружения уязвимости можно создать инцидент с помощью контекстного меню уязвимости или по кнопке **Действия** ( ) в свойствах уязвимости.

7.5. Статусы уязвимостей

Уязвимостям, которые обнаружены сканером безопасности, могут быть присвоены следующие статусы:

- **Открыта.** Уязвимость актуальна. Присваивается автоматически после проведения сканирования и обнаружения этих уязвимостей на узле, или после открытия уязвимости.
- **Закрыта.** Проведены работы по устранению уязвимости. Присваивается автоматически при повторном сканировании, если уязвимость не обнаружена.
- **Ложное срабатывание**. Уязвимость неактуальна.
- **Риск принят.** Уязвимость невозможно устранить, но факт ее существования принимается и учитывается в работе.

Уязвимости в любом статусе можно присвоить любой другой статус. Статус уязвимости определяется для конкретного узла. Одна уязвимость может иметь разный статус на разных узлах.

Изменить статус уязвимости вы можете с помощью политики управления уязвимостями или вручную.

Таблица изменения статусов уязвимостей по данным из внешних систем:

Текущий статус уязвимости	Уязвимость пришла из сканера	Уязвимость НЕ пришла из сканера
Открыта	Открыта	Закрыта
Закрыта	Открыта	Закрыта
Ложное срабатывание	Ложное срабатывание	Закрыта
Риск принят	Риск принят	Закрыта

8. АУДИТЫ

В этом разделе описан инструмент, позволяющий обеспечить внутренний контроль и оперативное уведомление о наличии проблем и (или) несоответствий с точки зрения выполнения необходимых мероприятий по обеспечению безопасности

- О модуле аудитов
- Подготовка к работе с разделом Аудит
- Настройка требований для проведения аудита
- Настройка аудитов
- Проведение простых аудитов
- Сводная оценка простых аудитов
- Устранение замечаний по аудиту

8.1. О функциональном блоке “Аудиты”

Блок «Аудит» – компонент, предназначенный для автоматизации контроля и оценки соответствия организации требованиям различных нормативных и законодательных документов в области информационной безопасности.

Основными функциональными возможностями модуля являются:

- Обеспечение учета всех мероприятий по информационной безопасности, нормативных документов, замечаний, проводимых аудитов безопасности и пр.
- Организация единой системы оценки состояния информационной безопасности на всех объектах организации.
- Поддержка совместной работы различных групп специалистов (ответственных за информационную безопасность на объектах, аудиторов, контроллеров, руководителей по информационной безопасности).
- Автоматическая оценка выполнения различных нормативных и законодательных требований.
- Формирование пакета отчетных документов по состоянию системы информационной безопасности, а также результатам проводимых оценок соответствия и аудитов информационной безопасности.
- Хранение истории проведенных оценок для отслеживания изменений.

8.2. Подготовка к работе с разделом Аудит

Чтобы приступить к работе с аудитами, выполните следующие подготовительные шаги:

1. Настройте поля аудитов в разделе **Настройки → Аудит и контроль → Справочники → Поля аудитов**.
2. Настройте шкалы оценки, используемые организацией при проведении аудита, в разделе **Настройки → Аудит и контроль → Справочники → Шкалы оценки.**
3. Настройте типы аудитов в разделе **Настройки → Аудит и контроль → Справочники → Типы аудитов.**
4. Задайте набор статусов аудитов в разделе **Настройки → Аудит и контроль → Справочники → Статусы аудитов**.
5. Настройте уровни замечаний аудита в разделе **Настройки → Аудит и контроль → Справочники → Уровни замечаний**.
6. Настройте перечень стандартов, используемых в организации для проведения аудита, в разделе **Настройки → Аудит и контроль → Требования.** При необходимости загрузите перечень требований посредством импорта из Excel.
7. Создайте и заполните комплекс контрольных проверок в **Настройки → Аудит и контроль → Контрольные проверки**.
8. Свяжите контрольные проверки с соответствующими положениями стандартов и, при необходимости, с мерами контроля.
9. В разделах **Активы → Подразделение/Организация**, **Активы → Бизнес-процессы**, **Активы → Группы ИТ-активов, Активы → Оборудование, Активы → Помещения** отметьте у соответствующих активов перечень связанных с ними нормативных требований (раздел свойств **Требования**).

8.3. Настройка требований для проведения аудита

В данном разделе приведены инструкции по созданию нормативных / законодательных требований, контроль выполнения которых проводится с помощью модуля **Аудит**.

Для работы можно использовать готовые комплексы требований или создать собственные.

Пользовательские требования настраиваются в несколько этапов: нужно создать комплекс требований, добавить требования в новый (или существующий) комплекс, добавить контрольные проверки для периодического контроля показателей аудита.

- Создание комплекса требований
- Добавление новых требований к комплексу
- Формирование списка контрольных проверок для требования
- Настройка полей требований
- Импорт комплекса требований

8.3.1. Создание комплекса требований

Новые комплексы требований добавляются либо в рамках обновления системы, либо путем создания пользователем собственных комплексов требований, которыми могут быть, например, собственная корпоративная политика ИБ, внутренние стандарты организации и пр. (если используемая лицензия допускает такое расширение).

Комплекс требований логически объединяет требования, по которым проводится аудит.

Вы можете добавить комплексы требований вручную или путем импорта данных из файла. Шаблон файла для импорта можно скачать в окне импорта в меню кнопки **Выбрать файл**. В окне импорта укажите параметры импортируемого комплекса требований.

Чтобы создать новый комплекс требований, выполните следующие действия:

1. Перейдите в раздел **Настройки → Аудит и контроль → Требования**.
2. В правой части экрана нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров.
3. Введите обозначение и наименование, выберите группу стандартов, к которой относится данный комплекс.
4. Укажите тип аудита.
5. Нажмите на кнопку **Добавить**. Новая запись появится в списке. Перейдите к добавлению требований в комплекс.

8.3.2. Добавление новых требований к комплексу

Новые требования можно добавить в новый или существующий комплекс требований. В рамках проведения аудита оценивается выполнение требований из комплекса.

Чтобы добавить новое требование в комплекс, выполните следующие действия:

1. Перейдите в раздел **Настройки → Аудит и контроль → Требования**.
2. В списке откройте комплекс, в который вы хотите добавить требование.
3. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров требования.
4. В появившейся справа форме укажите идентификатор и из выпадающего списка выберите группу требований или добавьте новую. Группа определяет иерархию требований внутри комплекса. Укажите родительскую группу в поле **Входит в**, чтобы создать дочернюю группу. Иерархия требований доступна только для пользовательских типов аудита.
5. Введите наименование требования.
6. Укажите комментарий (доступно для группового редактирования).
7. Укажите значение коэффициента значимости (доступно для группового редактирования). Коэффициент значимости используется при расчете **Индекса соответствия** показателей внутри аудитов.
8. Выберите форму аудита. Набор доступных форм определяется типом аудита.
9. Вы можете указать значение полей формы, для которых установлен флажок **Предзаполнять при создании требований**. При создании аудита эти поля будут иметь указанное значение, и не будут доступны для редактирования.
10. После заполнения всех полей нажмите на кнопку **Добавить**. Запись появится в комплексе требований. Перетащите элемент списка, чтобы изменить порядок требований и групп внутри комплекса. Вы можете выделить несколько групп или требований, удерживая клавишу CTRL.

Контролировать выполнение требований можно с помощью функционала контрольных проверок. Для этого после завершения настройки требований свяжите требования с контрольными проверками.

Следующие действия внутри комплекса требований:

- Создание новой группы требований.
- Создание нового требования.
- Удаление требования.
- Изменение поля, для которого установлен флажок **Предзаполнять при создании требований** (если такое поле входит в тип аудита).

применяются к новым и к ранее созданным аудитам в разделе **Аудит и контроль → Аудиты** с любым статусом, кроме **Завершен**. Изменения не применяются к аудитам в статусе **Завершен**.

8.3.3. Формирование списка контрольных проверок для требования

Для формирования списка контрольных проверок, с которыми связано требование, выполните следующие действия:

1. Убедитесь, что созданы контрольные проверки для требований, которые вы хотите связать.
2. Перейдите в раздел **Настройки → Аудит и контроль → Требования**.
3. В списке откройте комплекс, для требования которого вы хотите сформировать список контрольных проверок. На экране отобразится список требований, входящих в комплекс.
4. Выберите требование.
5. Нажмите на кнопку  . В правой части экрана отобразится список контрольных проверок, привязанных к этому требованию.
6. С помощью кнопок **Добавить** и **Удалить** сформируйте список связанных контрольных проверок.

8.3.4. Настройка полей требований

Вы можете настроить набор полей, который отображается при оценке выполнения требования.

Для настройки набора полей:

1. Создайте поля, которые будут отображаться при выставлении оценки требования (см. инструкцию ниже).
2. Добавьте поля в формы в рамках типов аудитов.
3. Используйте типы для создания аудитов.

Чтобы настроить набор полей требований:

1. Перейдите в раздел **Настройки → Аудит и контроль → Параметры аудитов → Поля описания аудитов**.
2. Выберите вкладку **Поля требований**. В правой части экрана отобразится область редактирования полей требований.
3. Заполните параметры поля:
   a. Наименование.
   b. Тип поля.
   c. Подсказка, которая отображается при наведении курсора на поле.
   d. Описание поля.
4. Нажмите на кнопку **Добавить**.

Для использования в карточке аудита перейдите к настройке форм в рамках типов аудитов.

8.3.5. Импорт комплекса требований

Вы можете импортировать комплексы требований из файлов в формате Excel.

Чтобы импортировать комплексы требований:

1. Перейдите в раздел **Настройки → Аудит и контроль → Требования**.
2. Нажмите на кнопку  . На экране отобразится окно импорта данных.
3. Выберите группу.
4. Укажите обозначение и наименование комплекса.
5. Выберите тип аудита.
6. Скачайте шаблон импортируемого файла (в формате Excel), нажав на стрелку в кнопке **Загрузить/скачать шаблон** и выбрав команду **Скачать шаблон файла импорта**.
7. Заполните шаблон в соответствии с описанием, заданным в файле шаблона, и сохраните его.
8. Нажмите на кнопку **Загрузить/скачать шаблон.**
9. Укажите путь к заполненному импортируемому файлу.
10. Нажмите на кнопку **Отправить**. Система отобразит окно с данными импорта. Ошибки, допущенные при заполнении шаблона,

подсвечиваются красным. Если в файле имеются ошибки, кнопка **Импортировать** будет недоступна.

11. Нажмите на кнопку **Импортировать**. Комплекс требований будет добавлен в систему.

8.4. Настройка аудитов

В этом разделе описана настройка параметров аудитов.

Тип аудита определяет схему расчета показателей аудита. Для настройки типов аудитов нужно настроить поля аудитов и шкалы оценки. Статусы аудитов используются при работе с аудитом и определяют действия, которые доступны пользователю для работы с аудитом.

- Простые аудиты: настройка шкалы оценок
- Простые и сводные аудиты: настройка дополнительных полей
- Простые аудиты: настройка статусов

8.4.1. Простые аудиты: настройка шкалы оценок

Шкалы задают количество и наименование уровней, которые используются для оценки выполнения требований по информационной безопасности. В набор доступных шкал могут быть по умолчанию включены шкалы, используемые для оценки законодательных или отраслевых требований.

Для добавления новой шкалы оценки соответствия требованиям выполните следующие действия:

1. Перейдите в раздел **Настройки →Аудит и Контроль → Параметры аудитов → Шкалы оценок**.
2. В правой части экрана нажмите на кнопку  .
3. Введите наименование, краткое описание и добавьте элементы шкалы (не менее двух). Если у предыдущего элемента шкалы меняется верхняя граница числового диапазона, то у следующего элемента шкалы нижняя граница числового диапазона автоматически принимает то же значение.
4. Установите флажок **Используется по умолчанию**, чтобы выбранная шкала по умолчанию автоматически устанавливалась у всех создаваемых оценок.
5. Если вы хотите, чтобы при выставлении оценки требования (кроме значений шкалы: максимальное, не оценено, не применимо)

автоматически отображался запрос о создании замечания, установите флажок **Обязательно фиксировать замечания**. Запрос отображается, если в типе стандарта, по которому проводится аудит, есть показатель типа **простая оценка** с идентификатором редактируемого поля типа **Шкала оценки**. Если вы хотите, чтобы при выставлении оценки требования **Не применимо** автоматически отображался запрос о создании замечания, установите флажок **Отдельный учет обоснований неприменимости** и укажите тип замечания.

6. Нажмите на кнопку **Добавить**. В результате в перечне шкал оценок появится новая запись.

Элемент **Не применимо** нельзя удалить. Этот элемент можно скрыть. В этом случае в аудитах, в которых используется эта шкала, требования с оценкой **не применимо** станут не оцененными.

8.4.2. Простые и сводные аудиты: настройка дополнительных полей

Вы можете добавить поля, которые будут показаны в разделе **Дополнительные сведения** свойств простых или сводных аудитов (доступен при выборе аудита в списке в разделе **Аудит и Контроль**). Одно и то же поле можно добавить в простой и в сводный аудит одновременно.

Чтобы создать поле, выполните следующие действия:

1. Перейдите в раздел **Настройки → Аудит и контроль → Параметры аудитов → Поля описания аудитов**.
2. Перейдите на вкладку **Поля аудитов**.
3. Нажмите на кнопку  . В правой части экрана отобразится область настройки параметров поля.
4. Заполните поля:
   a. Наименование.
   b. В зависимости от выбранного типа, укажите дополнительные параметры поля (например, описание и подсказку). Для поля типа **Выпадающий список** сформируйте список значений.
5. Нажмите на кнопку **Добавить**. Поле отобразится в списке.

Перейдите к настройке отображения полей в свойствах простых и сводных аудитов. Вы можете задать набор и порядок полей в разделе **Дополнительные**

сведения свойств простых или сводных аудитов (доступен при выборе аудита в списке в разделе **Аудит и Контроль**).

Чтобы сформировать список полей в карточке аудита:

1. Перейдите в раздел **Настройки → Аудит и контроль → Параметры аудитов → Настройка описания аудитов.**
2. Выберите для какого аудита вы хотите настроить карточку: простого или сводного. В правой части экрана отобразится область настройки карточки.
3. Сформируйте список полей с помощью кнопок **Изменить** и **Удалить**. Порядок следования полей можно изменить перетаскиванием или с помощью кнопок управления в правой части каждой строки.

Поля будут отображаться в заданном порядке:

- В разделе **Дополнительные сведения** свойств аудитов.
- В окне создания аудитов из свойств активов.

8.4.3. Простые аудиты: настройка статусов

Вы можете настроить статусы, которые будут присваиваться аудитам. Статус определяет набор действий, которые пользователь может произвести с аудитом.

Чтобы добавить статусы аудитов, выполните следующие действия:

1. Перейдите в раздел **Настройки → Аудит и контроль → Параметры аудитов → Статусы аудитов**.
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров нового статуса.
3. Введите название и описание статуса.
4. Чтобы ячейки статуса в списках аудитов и сводок в разделе **Аудит и Контроль** обозначались цветом, укажите цвет статуса.
5. Нажмите на кнопку **Добавить**. Статус отобразится в списке.

От статуса зависят следующие действия в системе:

1. **Запланирован** (системный). Пользователь может отредактировать плановую дату проведения, задать срок отправки уведомлений и установить флажок **Заполнить оценку, используя данные из системы контроля**. Аудит не может быть открыт. Флажок **Зафиксировать оценку** отсутствует.

2. **Рабочие статусы** (редактируемые). По умолчанию определен статус **В работе.** Пользователь не может редактировать плановую дату проведения. Есть флажок **Заблокировать изменения в оценке**. Дата начала проведения заполняется автоматически текущей датой при смене статуса с **Запланирован** на первый рабочий статус, но может быть изменена. Аудит может быть открыт для проведения. Если на статусе **Запланирован** был отмечен флажок **Заполнить оценку, используя данные из системы контроля**, то ряд оценочных полей может быть предзаполнен.
3. **Завершен** (системный). Пользователь не может редактировать дату проведения аудита. Содержимое аудита недоступно для редактирования, но оценку можно открыть для просмотра. При попытке вернуть аудит в работу, система предложит обновить данные из системы контроля, если флажок **Заполнить оценку, используя данные из системы контроля** был отмечен на статусе **Запланирован**. При переводе аудита в статус **Завершен** система предложит создать отчет по аудиту, если аудит не входит в сводку и не является последним незавершенным аудитом в ней.

   Установите флажок **Запретить закрывать аудиты при наличии неоцененных требований**, чтобы автоматически выполнять проверку на наличие неоцененных требований при переводе аудита в статус **Завершен**: если есть неоцененные требования, система отображает уведомление и аудит не переводится в статус **Завершен**.

Вы можете изменить порядок следования рабочих статусов, изменив их порядок в списке. Вы не можете переименовать, удалить или изменить порядок следования статусов **Запланирован** и **Завершен**.

8.5. Проведение простых аудитов

В этом разделе описана работа с простыми оценками.

- Простой аудит: создание
- Простой аудит: просмотр
- Простой аудит: расширенный режим просмотра оценки
- Простой аудит: рабочая группа
- Простой аудит: проведение оценки соответствия
- Простой аудит: расчет показателей оценки соответствия
- Простой аудит: проведение аудита на основании оценки контрольных проверок
- Простой аудит: просмотр результатов

8.5.1. Простой аудит: создание

В этом разделе описаны способы создания простого аудита.

Создать аудит можно тремя способами:

- Вручную в разделе **Простые аудиты** - создается аудит с незаполненными полями.
- Из контекстного меню актива - создается аудит для активов типа **Подразделение/организация**, **Бизнес-процессы**, **Группы ИТ-активов**, **Оборудование**, **Помещения.**
- Путем копирования существующей оценки.

Вы можете настроить набор дополнительных полей в карточке аудита.

8.5.1.1. Создание простого аудита с незаполненными полями

Создание оценки проводится экспертом в ручном режиме. Данная оценка изначально не содержит каких-либо сведений.

Чтобы сформировать пустую оценку, выполните следующие действия:

1. Перейдите в раздел **Аудит и контроль → Аудиты → Простые аудиты.**
2. Нажмите на кнопку  .
3. В появившемся меню выберите пункт **Аудит**.
4. Укажите следующие сведения:
   - Организация (если в системе создано две и более организаций).
   - Наименование.
   - Тип аудита (указать комплекс требований, на соответствие которым будет проведен аудит).
   - Менеджер аудита (выбрать из списка пользователей системы или добавить из раздела **Персонал**, по умолчанию им назначается текущий пользователь). Поле доступно для группового редактирования.
   - Плановая дата проведения. Поле доступно для группового редактирования.

- Срок уведомления о проведении аудита (в днях).
- Используемая шкала оценок (если предполагается типом аудита).
- Область оценки. Выберите тип актива и укажите актив. Если в окне добавления актива установить флажок **Назначить менеджеров по контролю соответствия актива ответственными за аудит**, то в поле **Менеджер аудита** отобразятся все пользователи, указанные в свойствах выбранного актива как менеджеры по контролю соответствия. Кнопка  позволяет отобразить список активов в виде дерева.
- Если аудит входит в область оценки сводного аудита, выберите сводный аудит в поле **Входит в**.

5. Нажмите на кнопку **Добавить.** В списке отобразится новый аудит со статусом **Запланирован.**

После добавления оценки нужно сформировать рабочую группу пользователей по этой оценке. Рабочая группа доступна для группового редактирования.

Все новые аудиты создаются со статусом **Запланирован**. Изменить статус аудита могут следующие пользователи:

- пользователь, указанный в поле **Менеджер оценки** создаваемого аудита.
- пользователь, в системной роли которого на вкладке **Аудит** установлен флажок **Аудиты** и задано право на изменение.

Набор рабочих статусов, которые можно выставить для аудита, вы можете задать в разделе **Настройки → Аудит и контроль → Справочники → Статусы аудитов.** Статус доступен для группового редактирования.

Если в свойствах аудита со статусом **Запланирован** установить флажок **Заполнить оценку, используя данные из системы контроля**, то система заполнит значения показателей в соответствии с оценками связанных контрольных проверок при переводе аудита в первый рабочий статус. Оценки выставляются пользователем в разделе **Система контроля** до проведения аудита.

8.5.1.2. Создание простого аудита для активов

Вы можете создать аудит для активов типа **Подразделение/организация**, **Бизнес-процессы**, **Группы ИТ-активов**, **Оборудование**, **Помещения**.

Чтобы создать аудит, выполните следующие действия:

1. Перейдите в раздел **Активы.**
2. По правой клавише мыши откройте контекстное меню актива, для которого вы хотите создать аудит. Чтобы создать аудит, актив должен быть связан с комплексом требований.
3. Выберите опцию **Создать аудит**. На экране отобразится окно создания аудита.
4. Задайте тип оценки: **простой аудит**.
5. Заполните параметры аудита. Если аудит входит в область оценки сводного аудита, выберите сводный аудит в поле **Входит в**.
6. Нажмите на кнопку **Добавить**. На экране отобразятся параметры созданного аудита в разделе **Аудиты**. Если вы выбрали несколько активов, система для каждого актива создаст отдельный аудит, с соответствующим активом в области оценки.

Контекстное меню доступно пользователям со следующими правами:

- Пользователям со специальной ролью **Менеджер контроля соответствия** в отношении своих активов.
- Пользователям со специальной ролью **Аудитор безопасности** в отношении своих активов.
- Пользователям, в свойствах системной роли которых на вкладке **Аудит** разрешен доступ к аудитам с правами на изменение.

Если пользователь выделяет несколько активов, но не ко всем активам имеет право на доступ к контекстному меню, то меню не отображается.

8.5.1.3. Простой аудит: копирование оценки

Чтобы скопировать оценку, выполните следующие действия:

1. Перейдите в раздел **Аудит и контроль → Аудиты → Простые аудиты**.
2. Выберите оценку, которую вы хотите скопировать.
3. Откройте контекстное меню оценки по правой клавише мыши.
4. Выберите пункт **Копировать оценку**. На экране отобразится запрос изменения области оценки.
5. Чтобы скопировать оценку без изменения области оценки, не устанавливайте флажок **Изменить объект оценки**. Если вы хотите изменить область оценки, установите флажок **Изменить объект оценки**,

нажмите на поле **Область оценки** и выберите актив. В окне отображаются активы, связанные со стандартом, по которому выполняется аудит. Копия оценки отобразится в списке.

6. Вы можете добавить новый аудит, в сводку, в которую входит скопированный аудит. Для этого установите флажок **Оставить аудит в сводной оценке**.

8.5.2. Простой аудит: просмотр

Вы можете открыть оценку в списке оценок в разделе **Аудит и контроль → Аудиты → Простые аудиты** одним из двух способов:

- По двойному щелчку на названии оценки в списке.
- С помощью кнопки **Открыть оценку** в свойствах оценки.

8.5.3. Простой аудит: расширенный режим просмотра оценки

При проведении оценки вы можете использовать расширенный режим просмотра.

Для перехода в расширенный режим просмотра выполните следующие действия:

1. Перейдите в раздел **Аудит и контроль → Аудиты → Простые аудиты**.
2. Откройте нужную оценку в отдельной вкладке. В открывшейся вкладке основной части интерфейса будут перечислены требования, а в правой части экрана представлены результаты проведения оценки, как в виде графических диаграмм, так и в форме отчета.
3. Нажмите на кнопку  , расположенную в нижней части области редактирования. Экран будет разделен на три части.
   a. В центральной части отображаются общие сведения.
   b. В правой части отображается выбранный раздел свойств.
   c. В левой части в виде пиктограмм отображаются оценки аудитора.
4. Вы можете использовать кнопку  для перехода к предыдущему просмотренному пункту и  для перехода к следующему неоцененному пункту.
5. Чтобы переключиться в обычный режим, нажмите на кнопку  .

8.5.4. Простой аудит: рабочая группа

Чтобы сформировать рабочую группу аудита, выполните следующие действия:

1. Перейдите в раздел **Аудит и контроль → Аудиты → Простые аудиты**.
2. Выберите аудит, для которого вы хотите сформировать группу.
3. Перейдите в раздел **Рабочая группа** с помощью кнопки  .
4. Нажмите на кнопку **Добавить**.
5. Выберите пользователей и укажите их уровень доступа (только чтение, полный доступ). Пользователи могут назначаться как для всего комплекса требований, так и для отдельных групп показателей. Группы, не включенные в область доступа, не будут отображаться в оценке аудита и ее журнале. Пользователи с правами **только чтение** смогут просматривать всю информацию о соответствующих показателях без возможности ее изменения. Пользователи, обладающие полным доступом, смогут вносить любые изменения в открытые для них группы требований.
6. Если вы хотите предоставить доступ пользователя к аудиту только на указанных этапах, установите флажок **Временный участник** и укажите этапы. Если аудит находится в неразрешенном для пользователя статусе, то в списке участников рабочей группы имя пользователя зачеркнуто, отображается серым шрифтом. Аудит не отображается в списке аудитов в разделе **Аудит и контроль → Аудиты**. Если у пользователя есть специальная роль **Аудитор безопасности** или **Менеджер по контролю соответствия** на активе из области оценки аудита, то аудит будет доступен пользователю на любом статусе.
7. Если вы хотите добавить пользователя из раздела персонал, в выпадающем списке **ФИО** выберите позицию **Добавить пользователя из раздела Персонал** и в появившемся окне укажите домен и логин сотрудника.
8. Нажмите на кнопку **Добавить** в окне создания оценки. В результате новая запись появится на панели **Аудиты.**

Вы можете настроить отправку уведомлений по электронной почте об изменениях свойств аудита, указав получателя в выпадающем списке **Уведомить**.

8.5.5. Простой аудит: проведение оценки соответствия

Чтобы провести оценку соответствия, выполните следующие действия:

1. Перейдите в раздел **Аудит и контроль → Аудиты → Простые аудиты**.
2. Откройте нужную оценку в отдельной вкладке. В открывшейся вкладке основной части интерфейса будут перечислены требования, а в правой части экрана представлены результаты проведения оценки, как в виде графических диаграмм, так и в форме отчета.

   Для выбранной оценки на вкладке **Результаты** в правой части экрана доступна кнопка **Рассчитать**. При нажатии этой кнопки система рассчитывает значения групповых и комплексных показателей для оценки. Оценки положений (как обычная, так и комплексная) считаются автоматически при каждой оценке того или иного требования.
3. Выберите требование из списка. В правой части экрана появится область редактирования параметров требования. В области редактирования параметров отображаются: поля оценки требования и дополнительные информационные поля, заданные в настройках для стандарта. Вы можете изменить набор полей оценки требования. При проведении оценки вы можете использовать расширенный режим просмотра.

   > Вы можете редактировать несколько требований одновременно, удерживая клавишу CTRL при выделении.
   > Одновременно можно оценить несколько требований, у которых совпадает форма. При оценке нескольких требований можно выбрать одно из двух значений шкалы: **Выполняется полностью** (значение, у которого верхняя граница равна единице) или **Не применимо**.
4. Оцените степень выполнения выбранного требования.

   на вкладке **Результаты** в правой части экрана доступна кнопка **Рассчитать**. При нажатии этой кнопки система рассчитывает значения групповых и комплексных показателей для текущей оценки требований. Оценки положений (как обычная, так и комплексная) считаются автоматически при каждом заполнении оценки требований.
5. Повторите шаги 3 и 4 для всех требований, которые вы хотите оценить.

   Вы можете использовать кнопку  для перехода к предыдущему просмотренному пункту и  для перехода к следующему неоцененному пункту.
6. Вы можете заполнить дополнительные поля аудита. Для перехода к дополнительным полям нажмите на кнопку  .

7. По завершении оценки система автоматически рассчитает основные показатели и предоставит результаты оценки соответствия, в том числе и в графическом виде. Вы можете создать отчеты с помощью кнопки .

8.5.6. Простой аудит: расчет показателей оценки соответствия

По умолчанию основными показателями оценки являются:

- **Индекс соответствия (сумма)** - сумма индексов соответствия всех требований оценки;
- **Индекс соответствия (среднее)** – среднее значение индексов соответствия всех требований оценки.

В графическом виде вы можете посмотреть как значение показателя, рассчитанное системой автоматически, так и распределение оценок по уровням и по группам требований.

Вы можете настроить методику оценки в разделе **Настройки → Аудит и контроль → Справочники → Типы аудитов.**

При использовании стандартной методики R-Vision, предлагаемой по умолчанию, в свойствах каждого требования будет отображено значение показателя **Индекс соответствия**. Индекс соответствия рассчитывается автоматически на основании коэффициента соответствия, указанного в свойствах требования, и выбранной шкалы оценки. Значение коэффициента умножается на правую границу диапазона значения, выбранного в поле **Оценка**, а затем еще раз умножается на 100.

Примечание

- В случае проведения оценки на соответствие требованиям СТО БР ИББС и 382-П пользователю необходимо для каждого частного показателя указать степень определения и/или выполнения в организации БС РФ (в зависимости от категории проверки).
- Индекс соответствия не рассчитывается для оценок на соответствие требованиям СТО БР ИББС и 382-П .
- При создании оценок по 382-П часть показателей будет автоматически отмечена как **н/о** с учетом свойств организации, указанных в разделе **Настройки → Организации**.

Пример
Показатель 4.1 имеет коэффициент соответствия 0,95 (был указан вручную в разделе **Настройки → Аудит и контроль → Требования)**. Аудит проводится по **Типовой шкале оценки**. В аудите в поле **Оценка** показателю было присвоено значение **Выполняется частично**. В разделе **Настройки → Аудит и контроль → Шкалы оценок** указано, что данное значение имеет числовой диапазон (0,2; 0,95]. Таким образом, индекс соответствия будет рассчитан как:
0,95×0,95×100=90,25

8.5.7. Простой аудит: проведение аудита на основании оценки контрольных проверок

Система позволяет создавать оценки аудита, используя значения контрольных проверок из раздела **Система контроля**. Если при создании оценки вы установили флажок **Заполнить оценку, используя данные из системы контроля**, расчет показателей будет проводиться по следующему принципу:

- Для оценки степени соответствия в системе применяются **Шкалы оценок**, включающие в себя качественные уровни (**Не выполняется**, **Частично**, **Выполняется** и т.д). Каждому уровню соответствует определенный диапазон числовых значений.
- Шкалы оценки могут применяться как для оценки показателей в рамках комплекса требований, так и для оценки контрольных проверок, связанных с этими требованиями. При оценке контрольной проверки системой выбирается верхнее значение диапазона заданного уровня (например, «0,95» для уровня **Выполняется частично** в примере).
- При привязке контрольной проверки к отдельным показателям комплексов требований каждой связи назначается коэффициент, равный «1» по умолчанию.
- При конечном расчете оценки показателя, система умножает значение каждой связанной контрольной проверки на коэффициент связи, а затем подсчитывает среднее арифметическое полученных значений. Итоговому результату назначается качественное значение (название уровня) в соответствии со шкалой, выбранной для оценки аудита.

Пример
С показателем комплекса требований связаны две контрольные проверки. В разделе **Система контроля** одна проверка оценена как «Не

выполняется», другая как «Выполняется» по **Шкале оценки контрольных проверок**. По умолчанию выбранные уровни данной шкалы имеют следующие числовые диапазоны:

- Не выполняется: (0; 0,2];
- Выполняется: (0,95; 1]

Контрольные проверки получают значения «0,2» и «1» соответственно. Коэффициент связи по умолчанию равен «1». Таким образом, расчет итогового значения показателя будет осуществлен следующим образом:
1*(0,2 + 1)/2 = 0,6
При создании оценки аудита пользователем была выбрана **Типовая шкала оценки**. Значение «0,6» попадает в числовой диапазон (0,2; 0,95], соответствующий уровню «Выполняется частично». Этот уровень и будет присвоен рассматриваемому показателю после создания оценки.

8.5.8. Простой аудит: просмотр результатов

Результаты аудита отображаются в разделе **Обзор** свойств аудита (кнопка ). Результаты представлены на следующих вкладках:

- **По уровням**. На вкладке отображается график распределения аудитов по уровням оценки.
- **По группам**. На вкладке отображается график распределения аудитов по группам требований и уровням оценки.
- **Итог (требования)**. На графике отображается распределение аудитов по требованиям и уровням оценки.
- **Итог (показатели)**. На графике отображаются числовые комплексные показатели, входящие в тип этого аудита. Показатели можно выбрать с помощью опции **Настроить показатели** в меню настройки графика (кнопка  на графике).

Скачать график в формате .png можно с помощью опции **Скачать график** в меню настройки графика (кнопка  на графике).

Под графиком расположен ряд вкладок с общей информацией об аудите:

- На вкладке **Результаты** отображаются показатели аудита. Переключатель **Комплексные/Групповые** позволяет изменить тип отображаемых показателей. Кнопка  открывает окно с детальной информацией о расчете группового показателя: группы, для которых рассчитался групповой показатель, и значения показателя для каждой группы.

- На вкладке **Фильтры** можно отфильтровать результаты оценки по заданным условиям.
- На вкладке **Замечания** отображаются замечания, связанные с оценкой. По кнопке **Все замечания** можно перейти в раздел **Замечания** с фильтром по этому аудиту.

8.6. Сводная оценка простых аудитов

Сводная оценка аудита объединяет несколько простых аудитов в единый процесс, охватывающий этапы проведения оценки выполнения требований, обработки замечаний и формирования плана мероприятий по их устранению.

Сводная оценка включает все требования из входящих в нее аудитов.

> Значения параметров простого аудита в составе сводного аудита синхронизируются со значениями параметров этого аудита в разделе **Простые аудиты**.

Права доступа к сводным оценкам имеют:

- Пользователи, в свойствах системной роли которых разрешен доступ на **изменение** к разделу **Аудит и контроль → Аудит**: могут просматривать все сводки, вносить изменения в свойства сводки и комментировать требования.
- Пользователи, в свойствах системной роли которых разрешен доступ на **чтение** к разделу **Аудит и контроль → Аудит**: могут просматривать сводки и комментировать требования.
- Пользователи с системной ролью **Менеджер аудита**: могут менять информацию по своей сводке, просматривать и комментировать требования.
- Сводная оценка: просмотр
- Сводная оценка: создание
- Сводная оценка: рабочая группа
- Сводная оценка: настройка методики расчета итогового показателя

8.6.1. Сводная оценка: просмотр

Вы можете открыть сводную оценку в списке оценок в разделе **Аудит и контроль → Аудиты → Сводки** одним из двух способов:

- По двойному щелчку на названии оценки в списке.
- С помощью кнопки **Открыть оценку** в свойствах оценки.

На экране отобразится окно сводки. Окно разделено на три части:

- В левой части экрана отображается список простых аудитов, которые входят в состав сводки. Для каждого аудита отображается название, стандарт, статус и плановая дата проведения. Аудиты сгруппированы по активам, по которым они созданы. В списке можно управлять статусом аудитов, просматривать связанные активы и управлять рабочей группой.
- В средней части экрана приведен список требований, которые входят в выбранный аудит в составе сводки. В списке можно выбирать требования для просмотра и оценки.
- В правой части экрана отображается информация о выбранном простом аудите или требованиях в составе аудита. Вы можете просмотреть и изменить оценки требований, связанные документы и замечания, добавлять комментарии и создавать отчеты.

  Если выбран простой аудит, на вкладке **Результаты** в правой части экрана доступна кнопка **Рассчитать**. При нажатии этой кнопки система рассчитывает значения групповых и комплексных показателей для оценки. Оценки положений (как обычная, так и комплексная) считаются автоматически при каждой оценке того или иного требования.

Над окном сводки расположена панель с идентификатором сводки. На панели отображается список этапов проведения сводного аудита:

- **Оценки**: отображает требования, которые входят в аудиты в составе сводки. Открывается по умолчанию.
- **Замечания**: отображает замечания по входящим в сводку аудитам. Вы можете редактировать свойства замечания. Замечания также отображаются на вкладке **Замечания** в разделе **Обзор** свойств аудита.
- **Мероприятия по устранению**: отображает мероприятия, созданные из свойств замечаний по входящим в сводку аудитам. Вы можете редактировать свойства мероприятия.
- **Итог**: отображает итоговые показатели сводной оценки.
- **Общая сводка**: отображает общий список требований, которые входят в аудиты в составе сводки.

При добавлении в сводку нового аудита в свойствах сводки (в разделах **Замечания** и **Мероприятия**) отображаются связанные с ним замечания и мероприятия. При удалении аудита из сводной оценки удаляются связанные с этим аудитом сущности из разделов **Замечания** и **Мероприятия**. Сущности не удаляются из разделов **Аудит и контроль → Замечания** и **Аудит и контроль → План мероприятий**.

8.6.2. Сводная оценка: создание

В этом разделе описаны способы создания сводного аудита.

Создать сводный аудит можно тремя способами:

- Вручную в разделе **Сводки** - создается сводный аудит с незаполненными полями.
- Из контекстного меню актива - создается сводный аудит для активов типа **Подразделение/организация**, **Бизнес-процессы**, **Группы ИТ-активов**, **Оборудование**, **Помещения.**
- Путем копирования существующей оценки.

Вы можете настроить набор дополнительных полей в карточке аудита.

8.6.2.1. Сводная оценка: копирование

Чтобы скопировать сводную оценку, выполните следующие действия:

1. Перейдите в раздел **Аудит и контроль → Аудиты →Сводки**.
2. По правой клавише мыши откройте контекстное меню для оценки, которую вы хотите скопировать.
3. Выберите пункт **Копировать оценку**. На экране отобразится запрос изменения параметров сводной оценки.
4. Чтобы задать другой объект оценки, установите флажок **Изменить объект оценки** и выберите объект оценки в поле.
5. Выберите статус, который будет присвоен аудитам в составе скопированной сводной оценки.
6. Нажмите на кнопку **Копировать**. При копировании сводной оценки будут скопированы входящие в нее аудиты. Копируются связи с замечаниями и мероприятиями.

При изменении целевого актива сводной оценки поле **Целевой актив** в связанных замечаниях и мероприятиях не меняется.

8.6.2.2. Сводная оценка: добавление

Чтобы создать сводную оценку, выполните следующие действия:

1. Перейдите в раздел **Аудит и контроль → Аудиты.**
2. Нажмите на кнопку  .

3. В появившемся меню выберите пункт **Сводная оценка**. Откроется вкладка **Сводки**. В правой части вкладки отобразится область редактирования.
4. Укажите организацию.
5. Укажите следующие сведения:
   a. Наименование.
   b. Менеджер аудита.
   c. Описание.
6. Укажите **Объект оценки**: актив, к которому можно отнести сводную оценку. Поле представляет собой метку, которую можно использовать для поиска аудитов и для автоматического поиска похожих замечаний при создании мероприятия по устранению замечания.
7. Сформируйте область оценки с помощью кнопок **Добавить** и **Удалить**. Вы можете перейти к аудитам из области оценки сводки по двойному щелчку на строке аудита.
8. Укажите плановую дату проведения. Поле доступно для редактирования, если сводка находится в статусе **Запланировано**.
9. Статус сводки определяется автоматически: сводке присваивается наименьший статус аудитов, входящих в область оценки сводки.
10. Срок уведомления о проведении аудита (в днях). Поле доступно, если сводка находится статусе **Запланировано**.
11. Нажмите на кнопку **Добавить**. Сводная оценка отобразится в списке на вкладке **Сводки**. В свойствах аудитов, входящих в область оценки, отобразится поле **Входит в**, в котором указано наименование сводной оценки. У сводки появляется набор недоступных для редактирования полей **Период проведения**. Поля автоматически заполняются крайними датами проведения из свойств входящих в сводку аудитов.

Сформируйте рабочую группу пользователей для просмотра сводной оценки.

8.6.2.3. Создание сводного аудита для активов

Вы можете создать аудит для активов типа **Подразделение/организация**, **Бизнес-процессы**, **Группы ИТ-активов**, **Оборудование**, **Помещения**.

Чтобы создать сводный аудит, выполните следующие действия:

1. Перейдите в раздел **Активы.**

2. По правой клавише мыши откройте контекстное меню актива, для которого вы хотите создать сводный аудит. Чтобы создать аудит, актив должен быть связан с комплексом требований.
3. Выберите опцию **Создать аудит**. На экране отобразится окно создания аудита.
4. Укажите тип оценки: **сводный аудит**.
5. Укажите наименование.
6. Укажите системы, для которых будут созданы аудиты, в списке **Создать аудиты для**. Это поле определяет количество создаваемых дочерних аудитов:
    a. **Только для выбранного актива**: создается по одному аудиту для каждого выбранного типа аудита. У созданных аудитов актив входит в область оценки.
    b. **Для дочерних** активов: аудиты создаются для дочерних элементов следующего уровня иерархии. Если стандарт, указанный в поле **Тип аудита**, выбран в разделе **Требования** свойств дочернего актива, то аудит создается.
    c. **Для связанных** активов: аудиты создаются для связанных активов. Если стандарт, указанный в поле **Тип аудита**, выбран в разделе **Требования** свойств связанного актива, то аудит создается.
7. Чтобы включить актив в область оценки сводки, установите флажок **Включить текущий актив в область оценки**.
8. Выберите типы аудитов, которые будут созданы в рамках сводки. Это поле указывает, по каким стандартам создаются дочерние аудиты.
9. Заполните параметры сводки и нажмите на кнопку **Добавить**. На экране отобразится запрос перехода в раздел **Аудит и Контроль → Аудиты → Сводки**.

Для сводки автоматически создаются дочерние аудиты. У сводки и у дочерних аудитов совпадают значения полей: менеджер аудита, статус аудита, плановая дата проведения, срок уведомления, шкала оценки.

8.6.3. Сводная оценка: рабочая группа

Чтобы сформировать рабочую группу сводки, выполните следующие действия:

1. Перейдите в раздел **Аудит и контроль → Аудиты → Сводки**.

2. Выберите сводку, для которого вы хотите сформировать группу.
3. Перейдите в раздел **Рабочая группа** с помощью кнопки  .
4. Нажмите на кнопку **Добавить**.
5. В появившемся меню выберите один из трех вариантов:
   a. **Из списка пользователей системы**. Выберите пользователей, которые войдут в состав рабочей группы и нажмите на кнопку **Выбрать**.
   b. **Добавить менеджеров входящих аудитов**: включить в рабочую группу пользователей, указанных в поле **Менеджер аудита** входящих в сводку аудитов.
   c. **Добавить менеджеров по контролю соответствия активов**: включить в рабочую группу пользователей, указанных в поле **Менеджер по контролю соответствия** активов, входящих в область оценки.

Пользователь из рабочей группы получает доступ на чтение к сводной оценке, и может оставлять комментарии к требованиям, входящим в сводную оценку.

Вы можете настроить отправку уведомлений по электронной почте об изменениях свойств сводной оценки, указав получателя в выпадающем списке **Уведомить**.

Вы можете настроить рабочую группу простого аудита в составе сводки.

8.6.4. Сводная оценка: настройка методики расчета итогового показателя

В системе можно рассчитать итоговый показатель по результатам проведения сводной оценки аудита. Итоговый показатель можно использовать, например, для создания отчетов и графиков.

Чтобы настроить методику расчета показателей для сводного аудита:

1. Перейдите в раздел **Настройки → Аудит и контроль → Параметры аудитов → Типы сводных аудитов**.
2. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров.
3. Введите наименование и описание методики.

4. В таблице **Показатели соответствия** нажмите на кнопку **Добавить**. На экране отобразится окно настройки показателя.
5. Укажите идентификатор и наименование показателя. Задайте тип показателя: **качественный** или **количественный**, и укажите формат возможных значений:
   a. **Формула** - укажите формулу, по которой вычисляется показатель. Список доступных переменных вы можете просмотреть по кнопке **Просмотр доступных переменных**. В качестве аргументов для формул используются идентификаторы простых аудитов.
   b. **Список** - добавьте значения списка (не менее двух). С помощью кнопки **Определить критерии оценки** укажите условия присвоения значений создаваемому комплексному параметру.
6. Нажмите на кнопку **Создать**, чтобы сохранить настроенный показатель. Повторите шаги 4-6 для всех показателей, которые нужно создать.
7. В таблице **Показатели соответствия** установите флажок **Итоговый** у одного показателя, который будет определять итоговый уровень соответствия.
8. Установите флажок **Используется по умолчанию**, чтобы использовать методику для вычисления показателей по умолчанию.
9. Нажмите на кнопку **Добавить**. Новая методика будет доступна в разделе **Результаты** свойств сводных аудитов.

Список операторов, доступных для использования в формулах:

- `sum` - вычисляет сумму матрицы или списка значений.
- `if` - возвращает второй аргумент, если первый ИСТИНА, иначе третий.
- `bitAnd` - побитовое И двух значений, x & y.
- `bitNot` - побитовое значение НЕ, ~x.
- `bitOr` - побитовое ИЛИ двух значений, x | y.
- `PI` – константа, число Пи.
- `count` - вычисляет количество элементов списка со значениями.
- `avg` - вычисляет среднее значение.

8.7. Устранение замечаний по аудиту

Планирование действий по устранению замечаний, созданных в ходе аудита, осуществляется с помощью мероприятий по устранению. Детализация действий

по устранению и управление работой исполнителей осуществляется с помощью задач.

В этом разделе приведены инструкции по настройке и работе с мероприятиями по устранению замечаний, созданных в ходе аудита.

- Добавление мероприятия по устранению замечания
- Изменение статуса мероприятий по устранению
- Связь мероприятий с активами
- Связь мероприятий с задачами
- Связь мероприятий с замечаниями
- Связь мероприятий с требованиями
- Связь мероприятий с аудитами

8.7.1. Добавление мероприятия по устранению замечания

Мероприятие можно создать:

- Вручную в разделе План мероприятий (см. инструкцию ниже).
- Вручную или по шаблону в свойствах замечания.
- Вручную или по шаблону в свойствах замечания внутри сводного аудита (этап **Замечания**).

Чтобы добавить мероприятие, выполните следующие действия:

1. Перейдите в раздел **Аудит и Контроль → Мероприятия по устранению**.
2. Нажмите на кнопку  .
3. В меню выберите организацию.
4. Выберите тип мероприятия. В правой части отобразится карточка мероприятия выбранного типа.
5. Заполните поля:
   a. Тип связанной задачи: тип задачи, которая автоматически создается в разделе **Задачи** при создании мероприятия. Если для связанной задачи выбран тип, участвующий в интеграции, то эта связанная задача передается во внешнюю систему.
   b. Наименование.
   c. Описание.
   d. Целевой актив: актив, к которому можно отнести мероприятие. Поле представляет собой метку, которую можно использовать для

поиска мероприятий и для автоматического поиска похожих элементов.

e. Ответственный (укажите одного или нескольких пользователей). Пользователям присваивается специальная роль **Ответственный за мероприятие по устранению**.

f. Настройка важности мероприятий по устранению мероприятия.

g. Срок исполнения.

6. Нажмите на кнопку **Добавить**. Мероприятие будет добавлено в список.

Пользователю, создавшему мероприятие, автоматически присваивается специальная роль **Постановщик мероприятия по устранению**. При создании мероприятия автоматически создается связанная с ним задача в разделе **Задачи**. Созданная задача синхронизируется с мероприятием по полям: **Ответственный**, **Срок исполнения**, **Статус**.

8.7.2. Изменение статуса мероприятий по устранению

В процессе управления жизненным циклом мероприятия предусмотрено несколько статусов. Если мероприятие не связано ни с одной задачей, созданной дополнительно из свойств мероприятия, значение поля **Статус** можно переключить вручную (**Запланировано, Выполняется, На проверке, Завершено**). Значение поля **статус** влияет на статус связанных задач и замечаний.

Если мероприятие связано с задачами, которые были созданы в разделе **Задачи** свойств мероприятия, то поле **статус** блокируется и его изменение производится автоматически на основании статусов подзадач.

Чтобы изменить статус мероприятия, выполните следующие действия:

1. Перейдите в раздел **Аудит и контроль → Мероприятия по устранению**.
2. Выберите мероприятие, статус которого вы хотите изменить. В правой части экрана отобразится область редактирования параметров.
3. Текущий статус мероприятия отображается в поле **Статус**. С помощью кнопок  и  , расположенных справа от поля **Статус**, выберите статус мероприятия.

В свойствах мероприятия нельзя установить статусы **Отложено**, **Отменено** и **В архиве**. Эти статусы присваиваются автоматически, если в них перевели связанную с мероприятием автоматически созданную задачу.

Если связанная с мероприятием задача передана во внешнюю систему в рамках интеграции, то статус мероприятия нельзя изменить вручную. Можно изменить статус только у мероприятий с текущим статусом **На проверке**.

8.7.3. Связь мероприятий с активами

В раздел **Связанные активы** (кнопка ) свойств мероприятия автоматически добавляются активы, которые указаны в свойствах замечаний, связанных с мероприятием.

Чтобы добавить к мероприятию связанные активы вручную, выполните следующие действия:

1. Перейдите в раздел **Аудит и Контроль → Мероприятия по устранению**.
2. Выберите мероприятие, для которого нужно добавить активы.
3. Нажмите на кнопку  . В правой части экрана отобразится перечень активов из связанных с мероприятием замечаний. Типы активов переключаются кнопками в верхней части списка.
4. Отредактируйте список связанных активов с помощью кнопок **Добавить** и **Удалить**.

8.7.4. Связь мероприятий с задачами

Связанные задачи позволяют управлять работой исполнителей в рамках мероприятия по устранению замечания.

Чтобы добавить к мероприятию связанные задачи, выполните следующие действия:

1. Перейдите в раздел **Аудит и Контроль → Мероприятия по устранению**.
2. Выберите мероприятие, для которого нужно добавить задачу.
3. Нажмите на кнопку  . В правой части экрана отобразится перечень задач.
4. Добавьте связанные задачи с помощью кнопки **Добавить**. Задача добавляется как дочерняя по отношению к задаче, созданной автоматически при создании мероприятия. Кнопка **Все задачи** осуществляет переход в раздел **Задачи**.

8.7.5. Связь мероприятий с замечаниями

Чтобы добавить к мероприятию связанные замечания, выполните следующие действия:

1. Перейдите в раздел **Аудит и Контроль → Мероприятия по устранению**.
2. Выберите мероприятие, для которого нужно добавить замечание.
3. Нажмите на кнопку  . В правой части экрана отобразится перечень замечаний.
4. Добавьте связанные замечания с помощью кнопки **Добавить**. По двойному щелчку на строке вы можете просмотреть выбранное замечание в разделе **Замечания**. Кнопка **Все замечания** осуществляет переход в раздел **Замечания**.

8.7.6. Связь мероприятий с требованиями

При связывании мероприятия с замечанием, в раздел **Требования** свойств мероприятия (кнопка ) автоматически добавляются требования, связанные с замечанием.

Чтобы добавить к мероприятию связанные требования, выполните следующие действия:

1. Перейдите в раздел **Аудит и Контроль → Мероприятия по устранению**.
2. Выберите мероприятие, для которого нужно добавить требования.
3. Нажмите на кнопку  . В правой части экрана отобразится перечень требований.
4. Отредактируйте список связанных требований с помощью кнопок **Добавить** и **Удалить**.

8.7.7. Связь мероприятий с аудитами

Чтобы просмотреть связанные сводки и аудиты, выполните следующие действия:

1. Перейдите в раздел **Аудит и Контроль → Мероприятия по устранению**.
2. Выберите мероприятие.

3. Нажмите на кнопку  . В правой части экрана отобразится перечень сводок и аудитов, связанных с замечаниями, с которыми связано мероприятие.

9. РИСКИ

В этом разделе приведены инструкции по работе с рисками. Функционал позволяет решать задачи по управлению рисками в организации, в частности:

- Сформировать модель угроз;
- Провести оценку рисков, в том числе и производных рисков (в случае если риски одного актива влияют на возможность реализации рисков для другого актива);
- Подготовить и отслеживать реализацию плана обработки рисков;
- Оценить экономический эффект и обосновать бюджет на ИБ.

Также в разделе приведены инструкции по работе с защитными мерами, применяемыми для предотвращения реализации рисков.

- О модуле рисков
- Подготовка к работе с рисками
- Настройка параметров для работы с рисками
- Настройка каталогов угроз
- Управление мерами защиты
- Проведение оценки рисков
- Просмотр сводной информации по рискам

9.1. О функциональном блоке Риски

Блок «Риски» — компонент, предназначенный для оценки и управления рисками информационной безопасности в соответствии с требованиями и рекомендациями российских и международных стандартов. Основными функциональными возможностями модуля являются:

- Формирование модели угроз и модели нарушителя благодаря наличию в системе различных баз угроз (БДУ ФСТЭК, ISO и т.д.).
- Составление перечня активов, входящих в область оценки рисков, и определение их ценности.
- Оценка степени вероятности реализации угроз ИБ и тяжести последствий с прогнозированием возможного ущерба.
- Гибкая схема оценки рисков, которая может быть адаптирована под конкретную модель, используемую в организации.
- Возможность проведения оценки рисков информационной безопасности разного масштаба (для отдельных проектов, активов, прикладных систем).

- Составление плана мероприятий по обработке рисков и сопоставление с имеющимся бюджетом по информационной безопасности.
- Подготовка документов, фиксирующих результаты оценки рисков.

9.2. Подготовка к работе с рисками

Перед началом работы с рисками рекомендуется выполнить следующие подготовительные действия:

1. Если вы хотите добавить защитные меры или изменить существующие, настройте каталоги защитных мер в разделе **Настройки → Система защиты → Каталоги защитных мер**.
2. Если вы хотите использовать настройки, отличные от настроек по умолчанию, настройте уровни эффективности защитных мер и потенциал источников угроз в разделе **Настройки → Управление рисками → Справочники.**
3. При необходимости настройте уровни оценки ценности активов в разделе **Настройки → Управление рисками → Справочники → Уровни оценки ценности**. Выделите уровень и нажмите **Задать критерии**, чтобы установить или отключить связь качественных и количественных уровней ценности и ввести их описание.
4. Настройте каталоги угроз, которые будут использоваться организацией при проведении оценок рисков, в разделе **Настройки → Управление рисками → Каталоги угроз**. Для этого:
    - Создайте или выберите каталог угроз.
    - Заполните вкладку **Источники** перечнем возможных нарушителей, источников рисков.
    - Заполните вкладку **Предпосылки** перечнем возможных уязвимостей, которые могут привести к реализации рисков.
    - Заполните вкладку **Угрозы** перечнем возможных угроз безопасности. В свойствах каждой угрозы укажите следующие параметры:
        - способ реализации;
        - нарушаемый атрибут безопасности;
        - связанные источники с указанием потенциала;

- связанные предпосылки с указанием достаточности;
- связанные защитные меры с указанием эффективности.

5. (Опционально) Настройте схемы оценки, используемые для расчета уровней рисков, в разделе **Настройки → Управление рисками → Схемы оценки**.
6. При необходимости свяжите угрозы из каталогов со способами реализации инцидентов в разделе **Настройки → Управление инцидентами → Справочники → Способы реализации**. При возникновении соответствующего инцидента, связанного с активом, он автоматически отобразится в перечне инцидентов при проведении оценки рисков этого актива.
7. Перейдите в раздел **Настройки → Управление активами → Типы активов**, выделите тип **Группа ИТ-активов**, **Информация** или **Бизнес-процессы** и настройте его:
   - Укажите применяемые каталоги угроз.
   - Укажите применяемые каталоги защитных мер.
   - Укажите схему оценки, применяемую по умолчанию.
   - Задайте связи атрибутов безопасности в разделе свойств **Связанные активы**.
8. В разделе **Активы** перейдите во вкладку **Группа ИТ-активов**, **Информация** или **Бизнес-процессы**. Выберите активы, для которых необходимо провести оценку риска. В их свойствах:
   - Отметьте флажок **Проводить оценку риска**.
   - Установите допустимые уровни риска.
   - Проведите оценку ценности актива.
9. При необходимости задайте перечень защитных мер, внедренных в отношении актива, в разделе **Система защиты → Каталоги защитных мер** и свяжите их с активом в разделе **Меры защиты.**
10. Перейдите к оценке рисков.

9.3. Настройка параметров для работы с рисками

Настроить значения параметров, используемых для составления модели угроз / нарушителя и проведения оценки рисков ИБ, можно с помощью справочников.

В системе имеются следующие справочники:

- **Уровни эффективности**. Справочник определяет уровни эффективности защитных мер в отношении рисков.
- **Уровни оценки ценности**. Справочник определяет уровень ценности того или иного актива.
- **Потенциал источников угроз**. Справочник определяет значимость и потенциал реализации того или иного источника угрозы.

В существующий справочник можно добавлять новые элементы.

Раздел доступен пользователям, в свойствах роли которых разрешен доступ к этому разделу с правами на изменение, а также в свойствах учетной записи установлен флажок **Все организации** (доступен в режиме Multi-tenancy).

Чтобы добавить элемент в справочник, выполните следующие действия:

1. Перейдите в раздел **Настройки** → **Управление рисками** → **Справочники**.
2. Выберите справочник, в который вы хотите добавить элемент. В правой части вкладки отобразится область редактирования параметров справочника. Доступны следующие справочники:
   a. Уровни эффективности.
   b. Уровни оценки ценности.
   c. Потенциал источников угроз.
3. Нажмите на кнопку  .
4. Введите параметры справочника:
   a. Для справочника **Потенциал источников угроз** укажите следующие параметры: **Наименование**, **Описание** и **Коэффициент** (от 0 до 1).
   b. Для справочника **Уровни оценки ценности** укажите следующие параметры: **Наименование**, **Описание** и **Индикатор уровня**. После добавления справочника задайте критерии уровней оценки.
   c. Для справочника **Уровни эффективности** укажите: **Наименование**, **Описание** и **Коэффициент эффективности** (от 0 до 1).
5. Нажмите на кнопку **Добавить**. Новый элемент будет добавлен в справочник.

9.4. Настройка каталогов угроз

Каталоги угроз содержат имеющиеся базы угроз ИБ.

Порядок настройки каталогов:

1. Добавьте каталог угроз любым из двух способов:
   a. создать новый каталог угроз;
   b. скопировать существующий каталог и отредактировать его параметры.
2. Добавьте в каталог угрозы.
3. Свяжите угрозы с источниками, предпосылками и защитными мерами.

Раздел доступен пользователям, в свойствах роли которых разрешен доступ к этому разделу с правами на изменение, а также в свойствах учетной записи установлен флажок **Все организации** (доступен в режиме Multi-tenancy).

- Создание нового каталога угроз
- Копирование каталога угроз
- Добавление угроз в каталог
- Добавление источников в каталог
- Добавление предпосылок в каталог

9.4.1. Создание нового каталога угроз

Вы можете создать каталог угроз двумя способами:

- Создать каталог вручную (см. инструкцию ниже).
- Скопировать существующий каталог и отредактировать его.

Чтобы добавить новый каталог угроз вручную, выполните следующие действия:

1. Перейдите в раздел **Настройки → Управление рисками → Каталоги угроз.**
2. В правой части экрана нажмите на кнопку  .
3. Введите наименование и описание.
4. Укажите идентификатор.
5. Нажмите на кнопку **Добавить**. В результате новая запись появится в перечне каталогов угроз.

6. Для разработки модели угроз в соответствии с требованиями ФСТЭК России в настройках добавленной базы угроз рекомендуется установить флажок **Определение типов угроз по требованиям ФСТЭК**.
7. После создания каталога наполните его данными: добавьте угрозы, источники, предпосылки.

9.4.2. Копирование каталога угроз

Вы можете создать каталог угроз двумя способами:

- Создать каталог вручную.
- Скопировать существующий каталог и отредактировать его (см. инструкцию ниже).

Чтобы создать каталог угроз на основе существующего, выполните следующие действия:

1. Перейдите в раздел **Настройки → Управление рисками → Каталоги угроз**.
2. Выберите в списке в основной панели каталог и нажмите на нем правой клавишей мыши.
3. Выберите опцию **Копировать**.
4. В появившемся окне укажите наименование, идентификатор и описание копии каталога угроз.
5. Нажмите на кнопку **Добавить**. В результате новая запись появится в перечне каталогов угроз.

Примечание
При копировании каталога (недоступно для Банка данных угроз ФСТЭК) сохраняются следующие данные:

- Установлен ли флажок Определение типов угроз по требованиям ФСТЭК.
- Списки угроз, источников, предпосылок (с сохранением описаний), их распределение по группам
- Связка угроз с источниками (с сохранением потенциала источника).
- Связка угроз с предпосылками (с сохранением достаточности).
- Связка угроз с защитными мерами (с сохранением эффективности).
- Все свойства угроз, включая нарушаемые атрибуты безопасности и тип угрозы (если установлен флажок **Определение типов угроз по требованиям ФСТЭК**).

9.4.3. Добавление угроз в каталог

Чтобы добавить новую угрозу, выполните следующие действия:

1. Перейдите в раздел **Настройки → Управление рисками → Каталоги угроз**.
2. Откройте каталог угроз, в который вы хотите добавить угрозу.
3. Перейдите на панель **Угрозы**.
4. Нажмите на кнопку  . В правой части вкладки отобразится область редактирования параметров
5. Укажите категорию угрозы: новую или уже существующую. При выборе пункта **Добавить новую** в появившемся окне введите наименование категории и нажмите на кнопку **Добавить**. Новая категория будет добавлена в систему.
6. При добавлении угрозы в уже существующую категорию укажите следующие сведения:
   - способ реализации угрозы;
   - описание;
   - нарушаемые атрибуты безопасности;
   - тип угрозы (первый, второй или третий) - в случае, если установлен флажок **Определение типов угроз по требованиям ФСТЭК**.
7. Нажмите на кнопку **Добавить**. В результате новая угроза появится в каталоге.

После добавления записи с помощью кнопок  ,  и  свяжите угрозу с источниками, предпосылками и защитными мерами.

Под типами угроз понимаются типы, определенные Постановлением Правительства РФ № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

9.4.4. Добавление источников в каталог

Вы можете добавить источники угроз вручную в любой из имеющихся каталогов. Для этого необходимо выполнить следующие действия:

1. Перейдите в раздел **Настройки → Управление рисками → Каталоги угроз.**
2. Откройте каталог, в который вы хотите добавить источник, и перейдите на панель **Источники**.
3. Нажмите на кнопку  . На экране отобразится область редактирования параметров источника.
4. В списка **Тип**: выберите тип источника, либо добавьте новый, укажите наименование и описание источника.
5. Нажмите на кнопку **Добавить**. Новая запись появится в каталоге.

9.4.5. Добавление предпосылок в каталог

Чтобы добавить новую предпосылку в каталог, выполните следующие действия:

1. Перейдите в раздел **Настройки → Управление рисками → Каталоги угроз**.
2. Откройте каталог угроз, в который вы хотите добавить предпосылку.
3. Перейдите на панель **Предпосылки**.
4. Нажмите на кнопку  . В правой части вкладки отобразится область редактирования параметров
5. Укажите тип предпосылки или добавьте новый.
6. Введите наименование предпосылки.
7. Нажмите на кнопку **Добавить.** Новая запись появится в каталоге.

9.5. Управление мерами защиты

В этом разделе описаны действия с защитными мерами в системе.

- Добавление меры защиты
- Меры защиты: режимы отображения

9.5.1. Добавление меры защиты

Вкладка **Меры защиты** содержит основные сведения о защитных мерах, применяемых в компании.

Перед добавлением защитной меры настройте каталоги защитных мер.

Раздел **Меры защиты** доступен пользователю в следующих случаях:

- В свойствах системной роли пользователя разрешен доступ к разделу **Меры защиты** (установлен флажок **Риски → Защитные меры**).
- Пользователю присвоена специальная роль **Владелец / Администратор безопасности / Менеджер по контролю соответствия** в отношении актива.

Защитные меры связываются с активами следующих типов:

- Группы ИТ - активов.
- Бизнес-процессы.
- Информация.

Чтобы добавить защитную меру для актива, выполните следующие действия:

1. Перейдите в раздел **Меры защиты.**
2. Убедитесь, что установлен режим отображения окна **Активы → Защитные меры** (в этом режиме в левой части окна отображаются активы).
3. В левой части экрана выберите организацию.
4. Выберите тип актива. Ниже в левой части экрана отобразится список активов.
5. Выберите актив из списка.
6. Нажмите на кнопку  . На экране отобразится окно **Добавление защитных мер**.
7. Выберите каталог и укажите защитные меры, которые могут быть использованы для обеспечения безопасности актива.
8. Нажмите на кнопку **Добавить**. Защитные меры отобразятся в списке.
9. Задайте параметры защитной меры:
    a. Описание.
    b. Администратор безопасности.
    c. Статус.
    d. Стоимость внедрения.
    e. Стоимость поддержки.
    f. Ожидаемый период применения.

g. Амортизированная годовая стоимость.

h. Комментарий.

Если защитная мера была добавлена в рамках обработки риска, то эта мера отобразится в списке в разделе **Меры защиты**.

9.5.2. Меры защиты: режимы отображения

У вкладки **Меры защиты** два режима отображения:

- **Активы → Меры защиты:** в левой части экрана приведен список активов. В средней части экрана отображаются защитные меры для указанных активов. В этом режиме можно добавить защитную меру для актива.
- **Меры защиты → Активы:** в левой части экрана приведен список защитных мер. В средней части экрана отображаются активы для выбранных защитных мер. В этом режиме добавление защитных мер недоступно.

  В режиме **Меры защиты → Активы** в списке перечислены только защитные меры, привязанные хотя бы к одному активу в рамках выбранной организации.

  Кнопка  в правой части переключает режим отображения вкладки **Меры защиты**.

9.6. Проведение оценки рисков

В общем случае процесс проведения оценки рисков с помощью системы включает в себя следующие этапы:

1. Создание новой оценки рисков с указанием области оценки и состава рабочей группы;
2. Определение источников возникновения угроз, предпосылок, имеющихся защитных мер с целью идентификации рисков;
3. Оценка рисков;
4. Формирование плана обработки рисков;
5. Формирование отчетности по результатам проведения оценки рисков;
6. Фиксация результатов оценки рисков.

В разделе приведена информация по особенностям проведения оценки рисков в соответствии с требованиями ФСТЭК.

- Этап 1. Создание оценки
- Этап 2. Идентификация рисков
- Этап 3. Оценка рисков
- Этап 4. Обработка рисков
- Этап 5. Формирование отчетности
- Этап 6. Журнал
- Проведение оценки угроз по требованиям ФСТЭК

9.6.1. Этап 1. Создание оценки

Начальным этапом проведения оценки рисков ИБ является создание оценки.

Чтобы создать оценку, выполните следующие действия:

1. Перейдите на панель **Риски → Оценки**.
2. Нажмите на кнопку  .
3. В форме создания оценки заполните следующие поля:
   - Организация (если в системе существует две и более организаций).
   - Наименование и описание оценки.
   - Риск-менеджер (выберите из выпадающего списка пользователей системы. Автоматически риск-менеджером назначается пользователь, от имени которого была создана оценка).
   - Флажок **Оценка актуальности угроз ФСТЭК** позволяет выполнить оценку угроз в соответствии с требованиями ФСТЭК и обеспечивает возможность генерации **Модели угроз ФСТЭК** . Все данные для создания оценки берутся из **Банка данных угроз безопасности информации (ФСТЭК)**. Флажок доступен только при создании оценки и не может быть снят или отмечен после ее добавления в систему. Если флажок **Оценка актуальности угроз ФСТЭК** установлен, то для выбора в область оценки доступны только группы ИТ-активов, в свойствах которых (раздел **Активы → Группы ИТ-активов)** указана **Схема оценки угроз ФСТЭК**.
   - Область оценки рисков (укажите активы организации). Вы можете сформировать список активов с помощью кнопок **Добавить** и **Удалить**. В область оценки вы можете добавить только те активы,

для которых установлена отметка **Проводить оценку рисков**. Если установлен флажок **Оценка актуальности угроз ФСТЭК**, то для выбора доступны только группы ИТ-активов, в свойствах которых указана схема оценки угроз ФСТЭК.

При указании области оценки вы можете указать активы, имеющие связи с другими активами организации. В этом случае система выдаст предупреждение: *Выбранные активы имеют взаимосвязи с другими активами, которые не были включены в область оценки. Хотите добавить в область оценки все связанные активы?* Для продолжения укажите, включать ли связанные активы в область.

4. Нажмите на кнопку **Добавить**. Оценка будет добавлена.
5. Настройте состав участников рабочей группы. Выберите созданную оценку в списке.
6. Нажмите на кнопку  , в панели справа нажмите на кнопку **Добавить** и воспользуйтесь выпадающим списком, чтобы сформировать список пользователей с указанием их роли при проведении оценки (**Участник, Наблюдатель**). Пользователь с ролью **Участник** может вносить изменения в состав предпосылок, источников, защитных мер и мероприятий по обработке рисков, пользователь с ролью **Наблюдатель** может просматривать результаты оценки без права внесения каких-либо изменений. Ни **Участники**, ни **Наблюдатели** не обладают правами на проведение непосредственной оценки рисков.

   a. Чтобы добавить участников рабочей группы из списка пользователей системы, в выпадающем списке выберите опцию **Из списка пользователей системы** и в появившемся окне укажите имя пользователя и его роль.

   b. Чтобы добавить всех владельцев активов одновременно, в выпадающем списке выберите опцию **Добавить всех текущих владельцев активов**: все владельцы активов, включенных в область оценки, автоматически получат роль **Участник** в текущей оценке.

   c. Вы можете включить пользователей из раздела **Персонал** в состав рабочей группы, даже если их учетная запись не существует в системе (в этом случае система автоматически добавит ее в общий список пользователей). Чтобы добавить пользователя из раздела

Персонал, в выпадающем списке выберите опцию **Нового пользователя из раздела Персонал** и в появившемся окне укажите имя или логин пользователя и его роль.

7. Чтобы удалить участника рабочей группы, выделите его в панели справа и нажмите **Удалить**.
8. Нажмите на кнопку  .
9. Нажмите на кнопку **Открыть оценку**, либо откройте оценку двойным щелчком мыши по записи в общем перечне, чтобы выполнить идентификацию рисков.

Пользователи могут видеть только те оценки риска, в отношении которых являются риск-менеджерами или участниками рабочей группы. Правом на доступ ко всем оценкам обладают пользователи с ролями **Менеджер по управлению рисками** и **Аналитик по управлению рисками**.

9.6.1.1. Просмотр оценки рисков

Пользователи могут видеть только те оценки риска, в отношении которых являются риск-менеджерами или участниками рабочей группы. Правом на доступ ко всем оценкам обладают пользователи с ролями, которым разрешен доступ к разделу **Риски → Оценки.**

Для просмотра оценки рисков, выполните следующие действия:

1. Перейдите на панель **Риски → Оценка**.
2. Выберите запись из общего перечня оценок. В правой части экрана отобразится область редактирования параметров оценки.
3. Нажмите на кнопку **Открыть оценку**, либо откройте оценку двойным щелчком мыши по записи в общем перечне, чтобы выполнить идентификацию рисков. Оценка откроется в отдельной вкладке, содержащей следующие разделы:
   - **Идентификация** - раздел предназначен для указания источников угроз, предпосылок возникновения рисков, внедренных мер защиты;
   - **Оценка** - раздел предназначен для отображения списка выявленных рисков и их оценки в соответствии с заданной схемой;

- **План обработки рисков** - раздел содержит итоговый план обработки рисков, содержащий в себе перечень мероприятий, направленных на снижение, устранение или уход от рисков.
- **Отчеты** - раздел содержит функционал создания отчетов по управлению рисками ИБ.
- **Журнал** - раздел отображает полные сведения о действиях пользователей в процессе проведения данной оценки.
- **Назначить экспертов** - предоставляет функционал выбора пользователей (экспертов) для оценки рисков.
- **Зафиксировать** - кнопка для сохранения результатов оценки в общую базу рисков.

9.6.1.2. Просмотр связи между прямыми и производными рисками

Список рисков может отображаться двумя способами:

- Список. Риски отображаются в виде перечня.
- Дерево. Риски и их взаимосвязи отображаются в виде древовидной структуры.

Чтобы переключить режим отображения списка, выполните следующие действия:

1. Перейдите на панель **Риски → Оценки**.
2. Откройте нужную оценку.
3. Выберите раздел **Оценка**.
4. Нажмите на кнопку переключения режима отображения перечня  в нижней правой части вкладки. Список рисков отобразится в виде дерева. Вы можете перейти к отображению в виде списка, нажав на кнопку  .

9.6.2. Этап 2. Идентификация рисков

На втором этапе нужно указать источники угроз, предпосылок и реализованные защитные меры для каждого актива, входящего в область оценки. Вы можете определить риски на панели **Идентификация**.

Чтобы определить риски, выполните следующие действия:

1. Перейдите на панель **Риски → Оценка**.
2. Откройте оценку, для которой вы хотите идентифицировать риски.
3. Перейдите на панель **Идентификация**. Панель **Идентификация** визуально разделена на несколько областей. В левой части экрана расположена информационная область, содержащая перечень активов, входящих в область оценки рисков. Справа от нее располагается область, в которой вы можете указать следующие параметры рисков:
   - **Источники** - в данной вкладке для каждого актива укажите возможные источники возникновения угроз. Если при создании оценки вы установили флажок **Оценка актуальности угроз ФСТЭК**, выбор источников посредством прямого выбора из списка становится недоступным.
   - **Предпосылки** - в данной вкладке для каждого актива укажите возможные предпосылки (организационные и технические) реализации угроз безопасности.
   - **Защитные меры** - в данной вкладке укажите меры защиты (организационные и технические), которые уже реализованы для защиты соответствующего актива. Раздел недоступен, если для оценки риска установлен флажок **Оценка актуальности угроз ФСТЭК**.
   - **Риски** - в данной вкладке система для каждого актива отобразит возможные риски с указанием их типа (прямой, производный) и последствий.
4. Укажите параметры рисков. При снятии флажка какого-либо элемента появится окно, запрашивающее подтверждение действия.
5. После проведения идентификации имеющихся рисков перейдите на панель **Оценка** для продолжения.

- В случае если для актива во вкладке **Система защиты → Защитные меры** уже указаны меры защиты, внедренные в организации, система автоматически учтет их при проведении оценки риска для данного актива.
- Если для заданного набора источников, предпосылок и защитных мер системой не были выявлены соответствующие риски, во

вкладке **Риски** пользователь увидит следующее сообщение: *Для указанных источников и предпосылок не выявлено ни одного потенциального риска*.

9.6.3. Этап 3. Оценка рисков

Вы можете выполнить оценку риска двумя способами:

- Оценка риска без привлечения экспертов
- Оценка рисков с привлечением экспертов

Следующим этапом является формирование плана обработки рисков.

9.6.3.1. Оценка риска без привлечения экспертов

Оценка рисков без привлечения экспертов выполняется по умолчанию автоматически на панели **Оценка**. Вы можете внести изменения в параметры оценки вручную. Измененные вручную параметры будут отмечены символом *****. Их значения не будут изменены при автоматическом пересчете уровней риска.

Примечание: правом на оценку рисков подобным образом обладают только пользователи со специальной ролью **Риск-менеджер** и пользователи с ролями, которым разрешен доступ к разделу **Риски → Оценки**.

Чтобы выполнить автоматическую оценку риска, выполните следующие действия:

1. Перейдите на панель **Риски → Оценки**.
2. Откройте оценку, для которой вы хотите продолжить оценку рисков.
3. Перейдите на панель **Оценка**. На панели **Оценка** отобразятся результаты автоматической оценки риска. В основной части панели **Оценка** содержится перечень всех возможных рисков с указанием текущего и целевого уровня. Риски в данном разделе расположены по убыванию уровня (от самого высокого уровня риска к низкому). Запись, подсвеченная красным цветом, означает, что текущий уровень риска превышает допустимый уровень, установленный для актива, с которым связан данный риск.
4. После выбора конкретного риска из общего перечня вы можете перейти к разделам с подробной информацией о риске (**Источники,**

Предпосылки, Защитные меры, Инциденты, **План обработки**). Вы сможете просмотреть основные сведения о риске:

- Категория и способ реализации риска;
- Актив и нарушаемый атрибут безопасности;
- Объект воздействия (для угроз из базы ФСТЭК);
- Негативные последствия от реализации риска;
- Тип риска;
- Описание (для угроз из базы ФСТЭК)
- Параметры риска - текущий и целевой уровень ценности актива, эффективность защитных мер, потенциал источника угроз и другие значения, указанные в выбранной схеме оценки риска.

5. Если для оценки по схеме вы хотите задать ряд параметров вручную, нажмите на кнопку **Оценка рисков**, расположенную под таблицей со списком параметров риска в разделе **Общие сведения**. На экране отобразится окно, в котором вы можете выполнить оценку параметров рисков, где:

   - **Текущее значение** – значение текущего уровня риска информационной безопасности для соответствующего способа реализации риска;
   - **Целевое значение** – значение уровня риска информационной безопасности для соответствующего способа реализации, который будет достигнут в случае реализации всех запланированных мероприятий по обработке риска. Если целевое значение соответствует текущему, то это означает, что в отношении данного способа реализации риска не запланировано никаких мероприятий по обработке риска, либо все запланированные мероприятия выполнены.

   Для качественных параметров типа «уровень» отобразится модальное окно, где с помощью ползунка нужно установить подходящее значение.

6. Нажмите на кнопку **Сохранить**. Нажатие на кнопку **Отмена** вернет все несохраненные параметры риска к их первоначальным значениям, рассчитанным автоматически. Кнопка **Рассчитать по схеме** сбрасывает

пользовательские изменения и пересчитывает уровни риска в соответствии с выбранной схемой оценки.

9.6.3.2. Оценка рисков с привлечением экспертов

Оценку рисков с привлечением экспертов можно выполнить тремя способами:

- Эксперты выполняют оценку вручную.
- Эксперт выполняет оценку автоматически.
- Эксперт копирует оценку другого эксперта и вносит изменения.

9.6.3.2.1 Оценка рисков с привлечением экспертов вручную

Чтобы провести оценку рисков с привлечением экспертов вручную, выполните следующие действия:

1. Перейдите на панель **Риски → Оценка**.
2. Откройте оценку, для которой вы хотите продолжить оценку рисков.
3. Перейдите на панель **Оценка**.
4. Выберите риск.
5. Нажмите на кнопку **Назначить экспертов**, расположенную в верхнем правом углу интерфейса. На экране отобразится окно выбора экспертов.
6. Выберите экспертов из состава рабочей группы проведения оценки с ролью **Участник**.

   > Пользователи с ролью **Участник**, назначенные **Экспертами**, теряют возможность просматривать все риски актива и получают доступ только к рискам, определенным для них риск-менеджером.

7. Нажмите на кнопку **Добавить**.
8. Укажите метод обобщения результатов, где:
   - **Максимальная оценка** означает, что итоговая оценка будет определена как максимальное значение среди тех оценок, которые были даны экспертами.
   - **Средняя оценка** означает, что итоговым результатом станет среднее значение по всем оценкам экспертов.
9. Для каждого эксперта назначьте риски для оценки.

Риск-менеджер или пользователь с системной ролью, которой разрешен доступ к разделу **Оценки,** назначающий экспертов, автоматически становится экспертом в отношении выбранного риска.
При удалении всех назначенных на риск экспертов параметры риска пересчитываются автоматически в состояние, которое было до назначения на риск эксперта.
Если оценке риска не назначен ни один эксперт, параметры риска будут рассчитаны системой на основании правил (формул и взаимосвязей), определенных схемой оценки рисков.

10. Далее каждый эксперт должен на панели **Оценка** выделить назначенный ему риск, в форме справа нажать на кнопку **Оценка риска** и во вкладке **Моя оценка** оценить параметры риска. При необходимости к выставленной оценке можно оставить комментарий, который затем будет виден другим экспертам во вкладках **Моя оценка** и **Оценки экспертов**.
11. Нажмите на кнопку **Сохранить оценку**. После того, как эксперты проведут оценку рисков (Вкладка **Оценки экспертов)**, система автоматически обобщит результат в соответствии с выбранным методом (максимальная оценка, средняя оценка, оценка риск-менеджера).
12. Результат оценки параметров риска будет представлен во вкладке **Итоговая оценка**.

9.6.3.2.2 Автоматическая оценка риска с привлечением экспертов

Для удобства пользователей предусмотрен режим автоматической оценки параметров рисков.

Чтобы провести оценку рисков с привлечением экспертов автоматически, эксперту необходимо выполнить следующие действия:

1. Перейдите на панель **Риски → Оценка**.
2. Откройте риск, для которого вы хотите продолжить оценку рисков.
3. Перейдите на панель **Оценка**.
4. Нажмите на кнопку **Оценка риска**. На экране отобразится окно **Оценка параметров рисков**.
5. Во вкладке **Моя оценка** нажмите на кнопку  в правом верхнем углу окна. По нажатию на кнопку откроется меню.
6. В меню вы можете выбрать один из вариантов:

- **Скопировать итоговую оценку** - при выборе этого варианта в оценку эксперта копируются текущие значения итоговой оценки.
- **Скопировать оценку эксперта** - при выборе этого варианта в меню раскрывается список экспертов для данного риска, и после выбора эксперта его оценка копируется в оценку текущего эксперта. Вы можете изменить скопированную оценку.
- **Рассчитать оценку по схеме** - при указании этого варианта параметры риска рассчитываются, исходя из схемы оценки риска, заданной для активa.

7. Нажмите на кнопку **Сохранить оценку**. Оценка будет сохранена в системе.

9.6.3.2.3 Копирование оценки другого эксперта

Чтобы провести оценку рисков с помощью копирования оценки другого эксперта, эксперту необходимо выполнить следующие действия:

1. Перейдите на панель **Риски → Оценка**.
2. Откройте риск, для которого вы хотите продолжить оценку рисков.
3. Перейдите на панель **Оценка**.
4. Нажмите на кнопку **Оценка риска**. На экране отобразится окно **Оценка параметров рисков**.
5. Во вкладке **Моя оценка** нажмите на кнопку  в правом верхнем углу окна. По нажатию на кнопку откроется меню.
6. В меню выберите опцию **Скопировать оценку эксперта**. При выборе этого варианта в меню раскрывается список экспертов для данного риска, и после выбора эксперта его оценка копируется в оценку текущего эксперта. Вы можете изменить скопированную оценку.
7. Нажмите на кнопку **Сохранить оценку**. Оценка будет сохранена в системе.

9.6.4. Этап 4. Обработка рисков

На этом этапе нужно создать план обработки рисков (этап недоступен для оценки актуальности угроз ФСТЭК). Каждый из рисков может быть обработан: для каждого риска может быть составлен план мероприятий по снижению, уходу и/или передаче риска. После обработки оценка фиксируется. Реализованное мероприятие по обработке риска может быть перенесено в архив.

- Добавление мероприятия по обработке риска
- Просмотр списка рисков, на которые направлено мероприятие
- Просмотр схемы обработки рисков по активу
- Архивирование мероприятия
- Сохранение результатов оценки в базу рисков: фиксация рисков

9.6.4.1. Добавление мероприятия по обработке риска

Вы можете добавить мероприятие по обработке риска одним из двух способов:

- С помощью кнопки **План обработки** () в свойствах риска на панели **Оценка** внутри оценки. В рамках этого способа вы можете изменить только параметр **Эффективность**.
- С помощью кнопки **Добавить** () на панели **План обработки рисков** внутри оценки. Вы можете изменить все параметры мероприятия с помощью кнопки  .

9.6.4.1.1 Добавление мероприятия по обработке риска из свойств риска

Чтобы добавить мероприятие по обработке рисков из свойств конкретного риска, выполните следующие действия:

1. Перейдите на панель **Риски → Оценки**.
2. Откройте оценку, для которой вы хотите добавить мероприятие.
3. Перейдите на панель **Оценка**.
4. Нажмите на кнопку  .
5. Нажмите на кнопку **Добавить** и выберите один из представленных типов мероприятия по обработке рисков.
6. В зависимости от выбранного типа мероприятия укажите дополнительные параметры:
   - Для типов **Внедрение защитной меры** и **Совершенствование защитной меры** укажите защитную меру.
   - Для мероприятий типа **Уход от риска** и **Передача риска** выберите риск и укажите эффективность снижения риска: на панели **План обработки риска** укажите добавленное мероприятие, нажмите на кнопку  , нажмите на кнопку **Добавить**, расположенную на

верхней панели раздела, выберите нужный риск и выбрать значение уровня эффективности (в соответствии со справочником).

7. Мероприятие будет добавлено в план по обработке рисков, представленный на панели **План обработки рисков**.

9.6.4.1.2 Добавление мероприятия по обработке риска на панели План обработки риска

Чтобы добавить мероприятие на панели План обработки риска, выполните следующие действия:

1. Перейдите в раздел **Риски → Оценки**.
2. Откройте оценку, для которой вы хотите добавить мероприятие.
3. Перейдите на панель **План обработки рисков**.
4. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров мероприятия.
5. Укажите название и краткое описание мероприятия.
6. Выберите тип мероприятия.
7. Укажите актив.
8. Укажите ответственного за выполнение мероприятия
9. Укажите дату начала реализации мероприятия и дату завершения.
10. Укажите финансовые параметры мероприятия.
11. Нажмите на кнопку **Добавить**. Мероприятие будет добавлено в план обработки.Вы можете исключить мероприятие с помощью флажка **Исключить из плана обработки рисков**. Уровни риска будут автоматически пересчитаны без учета исключенного мероприятия. При фиксации оценки все исключенные мероприятия удаляются из плана обработки рисков этой оценки.

9.6.4.2. Просмотр списка рисков, на которые направлено мероприятие

Чтобы просмотреть список рисков, выполните следующие действия:

1. Перейдите на панель **Риски → Оценки**.
2. Откройте оценку, для которой вы хотите просмотреть риски.
3. Перейдите на панель **План обработки рисков**.

4. В списке укажите мероприятие, по которому вы хотите просмотреть информацию.
5. Нажмите на кнопку  . В правой части вкладки отобразится список рисков.

9.6.4.3. Просмотр схемы обработки рисков по активу

Для просмотра качественной или количественной схемы обработки рисков по активу в виде диаграммы, выполните следующие действия:

1. Перейдите на панель **Риски → Оценки**.
2. Откройте оценку.
3. Перейдите на панель **План обработки рисков**.
4. Нажмите на кнопку  .
5. Укажите тип оценки: качественный или количественный.
6. Выберите актив, для которого будет построена диаграмма. Диаграмма будет построена автоматически. Вы можете изменить параметры диаграммы, а затем обновить ее с помощью кнопки  .

9.6.4.4. Архивирование мероприятия

Вы можете перевести мероприятие со статусом **Реализовано** в архив. Мероприятия со статусом **В архиве** по умолчанию не отображаются в списке мероприятий на вкладке **План обработки**. Эти мероприятия недоступны для редактирования и удаления, не используются при создании оценки рисков актива.

Чтобы просмотреть мероприятия в архиве, в списке мероприятий нужно выполнить фильтрацию по параметру **В архиве**.

> Архивирование необратимо. Вы не сможете изменить статус мероприятий, переведенных в архив.

Вы можете выполнить архивирование мероприятия двумя способами: в свойствах мероприятия или с помощью контекстного меню.

Для просмотра мероприятий, переведенных в архив, в столбце **Статус** установите фильтр **В архиве**.

Чтобы перенести мероприятие в архив в свойствах мероприятия, выполните следующие действия:

1. Перейдите на панель **Риски → План обработки**.
2. В списке выберите мероприятие со статусом **Реализовано** для архивирования. В правой части экрана отобразится раздел свойств мероприятия.
3. Нажмите на кнопку **В архив**. Мероприятие будет перенесено в архив.

Чтобы перенести мероприятие в архив с помощью контекстного меню, выполните следующие действия:

1. Перейдите на панель **Риски → План обработки**.
2. В списке нажмите правой клавишей мыши на задачу со статусом **Реализовано** для архивирования. Для выбранного мероприятия отобразится контекстное меню.
3. Выберите опцию **В архив**. Мероприятие будет перенесено в архив.

Мероприятия типа **Внедрение защитной меры** со статусом **Реализовано** не попадают в новую оценку риска, созданную для актива. После фиксации новой оценки риска такие мероприятия приобретают статус **В архиве** и скрываются в общем плане обработки.

9.6.4.5. Сохранение результатов оценки в базу рисков: фиксация рисков

Когда все расчеты по оценке закончены и план обработки окончательно сформирован, менеджер оценки может принять решение, что на текущий момент окончательный перечень рисков для данной организации. В этом случае нужно зафиксировать оценку.

Это действие является необратимым. После фиксации оценки никакие данные оценки не могут быть изменены.

Чтобы сохранить результаты оценки в базу рисков, выполните следующие действия:

1. Перейдите на панель **Риски → Оценки**.
2. Откройте оценку.
3. Нажмите на кнопку **Зафиксировать**. Оценка будет сохранена в базу. Все зафиксированные в оценке сведения будут доступны на панели **Карта**

рисков. Сведения об оценке можно просмотреть, нажав кнопку  и выбрав оценку в списке **Источник данных по текущей оценке риска**.

9.6.5. Этап 5. Формирование отчетности

По итогам проведения оценки рисков вы можете сформировать следующие отчеты:

- **План обработки рисков** – перечень запланированных мероприятий по обработке рисков. Этот отчет недоступен для оценок, создаваемых в соответствии с требованиями ФСТЭК.
- **Сводный реестр рисков** – обобщенный список выявленных рисков информационной безопасности.
- **Детализированный реестр рисков** – детализированный перечень выявленных рисков информационной безопасности, включающий в себя описание всех параметров по каждому из рисков (способы реализации, источники, предпосылки, активы, подвергающиеся риску, защитные меры и проч.).
- **Модель угроз ФСТЭК** – отчет представляет собой документ «Модель угроз», разработанный в соответствии с требованиями ФСТЭК. Для создания отчета необходимо выбрать актив. Для создания модели угроз доступны группы ИТ-активов, для которых в системе существует оценка риска с установленным флажком **Оценка актуальности угроз ФСТЭК**.

Правом на создание отчетов обладают пользователи с ролями: **Риск-менеджер**, **Менеджер по управлению рисками**, **Аналитик по управлению рисками**.

Чтобы сформировать отчет, выполните следующие действия:

1. Перейдите на панель **Риски→Оценки**.
2. Откройте оценку, для которой надо сформировать отчет.
3. Перейдите на панель **Отчеты**.
4. В правой части экрана в списке **Тип отчета** выберите необходимый тип.
5. Нажмите на кнопку **Сформировать отчет**. Для отчетов типа **Детализированный реестр рисков** в появившемся окне укажите активы или установите флажок **Все активы**. В результате новая запись появится в списке элементов. Вы можете удалить отчет с помощью кнопки  .

Вы можете сохранить отчет в формате DOCX и PDF с помощью кнопок  или  , соответственно.

9.6.6. Этап 6. Журнал

Все изменения, связанные с проведением оценки рисков, включая добавление/удаление новых источников угроз, предпосылок, защитных мер и т.д., фиксируются на панели **Журнал**.

Чтобы просмотреть журнал, выполните следующие действия:

1. Перейдите на панель **Риски→Оценки**.
2. Откройте оценку, для которой вы хотите просмотреть журнал.
3. Перейдите на панель **Журнал**. На экране отобразится список изменений по оценке.

9.6.7. Проведение оценки угроз по требованиям ФСТЭК

В этом разделе описаны подробности и отличия выполнения оценки угроз по требованиям ФСТЭК. Оценка угроз по требованиям ФСТЭК проводится в два этапа:

- Создание оценки актуальности угроз ФСТЭК
- Оценка актуальности угроз по требованиям ФСТЭК

9.6.7.1. Создание оценки актуальности угроз ФСТЭК

Для проведения оценки угроз безопасности в соответствии с документом ФСТЭК "Методика определения угроз безопасности информации в информационных системах" (2015 г.). и генерации **Модели угроз ФСТЭК** на этапе создания оценки рисков в разделе **Риски → Оценки** необходимо установить флажок **Оценка актуальности угроз ФСТЭК**. Флажок доступен только при создании оценки и не может быть снят или отмечен после ее добавления в систему.

Если флажок **Оценка актуальности угроз ФСТЭК** установлен, то для выбора в область оценки доступны только группы ИТ-активов, в свойствах которых (раздел **Активы → Группы ИТ-активов)** указана **Схема оценки угроз ФСТЭК**.

9.6.7.2. Оценка актуальности угроз по требованиям ФСТЭК

После создания оценки актуальности угроз ФСТЭК пользователю будет доступен интерфейс, частично отличающийся от типового представления оценок риска.

Оценка актуальности угроз ФСТЭК содержит только разделы, необходимые для генерации **Модели угроз ФСТЭК**. Основные различия:

- Отсутствует раздел **Идентификация → Защитные меры** – данный тип оценки рисков не учитывает влияние внедренных защитных мер.
- Отсутствует вкладка **План обработки** и возможность добавлять мероприятия по обработке из свойств риска – данный тип оценки не предполагает формирование плана обработки рисков.
- Вы не можете выбрать источники из списка. Укажите источники с помощью кнопки **Выбрать согласно требованиям ФСТЭК.** При нажатии на эту кнопку отображается окно, в котором вы можете указать цели нарушителей. В зависимости от выбранных целей в окне автоматически отмечаются связанные с ними источники. Для нарушителей типа **Специальные службы иностранных государств (блоков государств)**, **Террористические, экстремистские группировки** и **Преступные группы (криминальные структуры)** доступна возможность указания сговора с другими нарушителями. Если нарушитель указывается в столбце **Сговор**, он автоматически отмечается как актуальный.

После выбора предпосылок на вкладке **Идентификация → Предпосылки** риски из **Банка данных угроз ФСТЭК** автоматически появятся на вкладке **Оценка**. Параметры **Уровень защищенности** и **Потенциал источника** вычисляются автоматически на основании свойств актива и данных из каталога угроз. При выборе риска учитываются:

- Атрибуты безопасности, указанные в свойствах актива (**Настройки → Управление активами → Справочники → Типы активов**) и в свойствах угрозы в каталоге;
- Объекты воздействия, указанные в свойствах актива (**Активы → Группы ИТ-активов →** иконка **ФСТЭК →** раздел **Компоненты**) и в свойствах угрозы в каталоге;
- Отмеченные источники;
- Отмеченные предпосылки.

Расчет уровня рисков доступен в автоматическом режиме и при помощи экспертов.

9.7. Просмотр сводной информации по рискам

Сводная информация по актуальным рискам в организации отображается в разделе **Риски → Карта рисков**.

Панель **Карта рисков** содержит данные только из зафиксированных оценок. Риски (включая источники угроз и предпосылки), попавшие в общую базу, автоматически переносятся во все новые оценки, созданные для соответствующих активов. Если в ходе мероприятий по обработке какие-либо риски были полностью устранены, они перестанут отображаться в сводке, но не будут удалены из базы: подобный механизм позволяет отслеживать историю изменений уровня риска в случае его повторного возникновения.

Для просмотра сведений по конкретному риску, выполните следующие действия:

1. Перейдите на панель **Риски → Карта рисков**.
2. Выберите запись из общего перечня рисков. В правой части экрана отобразится область редактирования параметров риска.
3. Выберите раздел для просмотра с помощью следующих кнопок: - **Общие сведения**, содержащий основную информацию о выбранном риске (категория риска, способ реализации, тип, текущий и целевой уровень, владелец и актив). - **Параметры риска**, в котором отражен источник данных по текущей оценке выбранного риска, а также график, отображающий изменения по оценке в количественной и качественной шкале. - **Источники**, содержащий перечень источников возникновения выбранного риска. - **Предпосылки**, отражающий текущие предпосылки реализации выбранного риска. - **Защитные меры**, в котором перечислены защитные меры, реализованные в организации в отношении выбранного риска. - **Инциденты**, где представлены все зарегистрированные в системе инциденты, относящиеся к выбранному риску. - **План обработки**, где представлены все текущие мероприятия по обработке выбранного риска.

10. ФУНКЦИОНАЛЬНЫЙ БЛОК ИМИТАЦИИ ИТ-ИНФРАСТРУКТУРЫ

Компонент имитации ИТ-инфраструктуры представляет собой комплекс технологий для раннего обнаружения злоумышленников, проникших в корпоративную сеть, и предотвращения атак на ранних этапах.

С помощью набора программных ловушек и приманок компонент обнаруживает присутствие злоумышленника, замедляет его продвижение внутри сети, запутывая среди ложных объектов, и дает возможность ИБ-специалистам остановить развитие атаки до того, как она приведет к значимому ущербу.

Блок решает следующие задачи:

- Выявляет постоянные серьезные угрозы (APT) и уязвимости нулевого дня (zero-day) на ранних стадиях.
- Собирает данные о злоумышленнике.
- Затрудняет и замедляет продвижение атакующего внутри сети.

Преимущества от использования блока:

- Обнаружение злоумышленников, сумевших обойти классические средства защиты и мониторинга.
- Снижение скорости продвижения атакующего внутри сети, искажение периметра ложными элементами инфраструктуры.
- Возможность предотвращения атак на ранних стадиях.
- Понимание инструментов и действий злоумышленника в отношении конкретной инфраструктуры организации, выявление слабых мест в защите.
- Низкий процент ложных срабатываний.

10.1. Наполнение ловушек

В этом разделе приведены рекомендации по настройке автоматического наполнения ловушек данными.

10.1.1. Генерация логинов

Вы можете настроить автоматическую генерацию логинов пользователей для использования при создании ловушек. Сгенерированные данные должны быть как можно более похожи на данные в реальной инфраструктуре: иметь схожие паттерны и именование.

Чтобы настроить автоматическую генерацию логинов:

1. Перейдите в раздел **Настройки системы → Наполнение ловушек → Генератор логинов**.
2. В разделе **Словари, содержащие Ф.И.О.**, задайте процент фамилий из разных словарей.
3. По кнопке **Добавить словарь** вы можете настроить собственный словарь. Предварительно ознакомьтесь с требованиями к записям в словаре.

   Словарь представляет собой набор имен, фамилий и отчеств (опционально) пользователей в файле формата CSV. Инструкция по наполнению файла приведена в окне. Вы можете скачать шаблон словаря по ссылке в окне.

   Чтобы настроить пользовательский словарь:

   a. Укажите название словаря.

   b. Загрузите файл словаря.

   c. Нажмите на кнопку **Добавить**.

   d. Укажите процент фамилий из пользовательского словаря.

   e. Сохраните изменения по кнопке **Сохранить**.
4. Задайте паттерн генерации логина. Паттерн определяет структуру логина, которая заполняется данными из словаря. Паттерн нужно задавать на примере имени Boris Petrovich Sidorov. В примере паттерна используйте латинские буквы и точку (.) или подчерк (_) в качестве разделителя. Разделитель может отсутствовать. Регистр не важен.

   Пример
   Некоторые примеры заполнения поля **Паттерн**: bpsidorov, b.sidorov, boris_petrovich_sidorov.

Генерация логинов при создании ловушек будет выполняться по новым правилам.

10.1.2. Генерация паролей

Чтобы настроить автоматическую генерацию паролей:

1. Перейдите в раздел **Настройки системы → Наполнение ловушек → Генератор паролей**.
2. Выберите тип генерации паролей:
   a. **Использовать базу популярных паролей** - пароли генерируются с использованием базы популярных паролей.
   b. **Задать параметры вручную** - пароли генерируются на основании заданных критериев. Задайте правила генерации паролей:
      i. Укажите минимальное и максимальное количество символов в пароле.
      ii. Установите флажки для типов символов, которые будут использоваться в паролях.
3. Сохраните изменения по кнопке **Сохранить**. Пароли будут генерироваться по заданным правилам.

10.1.3. О наполнении ловушек

Вы можете настроить автоматическую генерацию данных для использования при создании ловушек. Сгенерированные данные должны быть как можно более похожи на данные в реальной инфраструктуре: иметь схожие паттерны и именование.

Платформа наполняет автоматически созданные ловушки сгенерированными данными.

Платформа может автоматически генерировать:

- Логины и пароли пользовательских учетных записей.
- Имена серверов.
- FTP баннеры.

Для генерации данных вы можете использовать встроенные словари и можете создавать свои словари в соответствии с требованиями, описанными в соответствующих разделах. При загрузке пользовательского словаря система производит валидацию загруженных данных и уведомляет о результате.

10.2. Работа с ловушками

В этом разделе описаны действия по управлению ловушками.

10.2.1. Добавление ловушек

Чтобы добавить ловушку:

1. Перейдите в раздел **Ловушки**.
2. Нажмите на кнопку **Создать**. На экране отобразится окно создания ловушки.
3. Выберите способ создания ловушек:
   a. **Создать ловушку вручную**: введите все данные ловушки для ее создания.
   b. **Создать ловушки автоматически**: создайте несколько ловушек в автоматическом режиме на основе выбранных типов и количества ловушек.
4. Нажмите на кнопку **Далее**. Следующие шаги зависят от выбранного способа создания ловушек.

10.2.1.1. Создание ловушки вручную

1. Выберите размещение ловушки:
   a. **Trap Manager**: выберите развернутый сервер Trap Manager из выпадающего списка.
   b. **Сеть**: выберите виртуальную сеть установленного Trap Manager для размещения ловушки.
2. Выберите тип ловушки:
   a. **FTP**: FTP-сервер.
   b. **ОС Windows**: ловушка типа FullOS, имитирующая компьютер с ОС Windows.
   c. **ОС Linux**: ловушка типа FullOS, имитирующая компьютер с ОС Linux.
   d. **SMB / SMB FS**: SMB-сервер или доступ к его файловой системе.
   e. **SSH**: SSH-сервер.
   f. **HTTP(S)**: имитация страницы ввода логина и пароля с авторизацией по введенной паре.
   g. **АСУ ТП**: имитация ПЛК семейства Siemens SIMATIC.

h. **PostgreSQL**: имитация сервера баз данных PostgreSQL.

i. **MySQL:** имитация сервера баз данных MySQL

j. **DeceptivePorts**: имитация открытых TCP/UDP портов.

3. Название ловушки заполняется автоматически. Для его изменения введите новое имя ловушки в поле **Название**.
4. Добавьте теги для ловушки.
5. Набор параметров, настраиваемый на третьем шаге, зависит от выбранного типа ловушки:

   a. **FTP**: укажите параметры FTP-сервера и данные аутентификации.

   b. **ОС Windows / ОС Linux**: выберите образ, укажите объем ОЗУ и количество процессоров на виртуальной машине. Подробная информация о работе с ловушками типа FullOS приведена в разделе Добавление ловушки типа FullOS.

   c. **SMB / SMB FS**: укажите параметры протокола SMB и параметры ресурсов. Список ресурсов отобразится в таблице в нижней части окна.

   d. **SSH**: укажите параметры протокола SSH, тип аутентификации (учетная запись пользователя или случайная).

   e. **HTTP(S)**: укажите имитируемое серверное ПО, порт и шаблон страницы авторизации, затем добавьте пары логинов и паролей для авторизации.

   f. **АСУ ТП**: выберите модель эмулируемого устройства (**Siemens SIMATIC S7-200** или **Siemens SIMATIC S7-300**). Для выбранного устройства отобразится таблица с портами для соответствующих сетевых протоколов.

   g. **PostgreSQL и MySQL**: укажите используемый порт (по умолчанию 3306) и параметры подключения.

   h. **DeceptivePorts**: укажите требуемые открытые TCP и UDP порты.

6. Для перехода на следующий шаг нажмите на кнопку **Далее**.
7. На четвертом шаге в окне отобразятся настроенные параметры. Убедитесь, что параметры заданы верно, и нажмите на кнопку **Создать**.

Если при настройке допущена ошибка, вернитесь на предыдущий шаг по кнопке **Назад**.

10.2.1.2. Автоматическое создание ловушек

1. Выберите метод создания ловушек:
   a. На основе данных об инфраструктуре.
   b. На основе выбранных типов и количества.

10.2.1.2.1 Создание ловушек на основе данных об инфраструктуре

1. При создании ловушек на основе данных об инфраструктуре загрузите файл данных об инфраструктуре. Нажмите на кнопку **Далее**.
2. На следующем шаге отобразятся доступные к размещению ловушки в виде древа. Для создания ловушек откройте нужную сеть, выберите ловушки и введите их количество. Нажмите на кнопку **Далее**.
3. На следующем шаге отобразится окно с выбранными ловушками и их количествами.
4. Выберите опцию размещения:
   a. **Разместить ловушки сразу**: выбранные ловушки размещаются в сетях одновременно сразу после нажатия кнопки **Создать**.
   b. **Выбрать график размещения**: установите период, в течение которого выбранные ловушки будут размещаться в сетях. При выборе этой опции будет имитироваться размещение реальных ресурсов в рабочее время: с 10:00 до 17:00 в будние дни.
5. Убедитесь, что все параметры заданы верно, и нажмите на кнопку **Создать**. Ловушки будут добавлены в список ловушек.

10.2.1.2.2 Создание ловушек на основе выбранных типов и количества ловушек

1. При создании ловушек на основе выбранных типов и количества ловушек система отобразит доступные серверы Trap Manager и связанные с ними сети в виде древа. Для создания ловушек откройте нужную сеть, выберите создаваемые ловушки и введите их количество.
2. На следующем шаге отобразится окно с выбранными ловушками и их количествами.

   Выберите опцию размещения:

a. **Разместить ловушки сразу**: выбранные ловушки размещаются в сетях одновременно сразу после нажатия кнопки **Создать**.

b. **Выбрать график размещения**: задайте период, в течение которого выбранные ловушки будут размещаться в сетях. При выборе этой опции будет имитироваться размещение реальных ресурсов в рабочее время: с 10:00 до 17:00 в будние дни.

3. Убедитесь, что все параметры заданы верно, и нажмите на кнопку **Создать**. При автоматическом добавлении ловушки система автоматически наполняет ее данными. Данные генерируются согласно заданным правилам.

10.2.2. О ловушках

Ловушка (Trap) — это любой сервер/docker контейнер, с помощью которого можно собрать информацию о злоумышленнике и его действиях. Ловушки размещаются на серверах управления ловушками (Trap Manager).

Существует две категории ловушек:

1. **FullOS**: полноценная ОС Windows или Linux, настроенная для максимальной схожести с реальной системой. Такие ловушки отслеживают любое нелегитимное воздействие.
2. **Эмуляции устройств**: контейнеризованное сервис-приложение, настроенное для схожести с реальным приложением. Есть несколько типов эмулятивных устройств:

   a. **Высокоинтерактивные (High-Interaction)**: Docker-контейнер с полноценным модернизированным приложением. Ловушка отслеживает и фиксирует все происходящие события.

   b. **Среднеинтерактивные (Medium-Interaction)**: Docker-контейнер с приложением, эмулирующим сервис файловой системы. К такому приложению можно подключиться для взаимодействия, но реалистичность ограничена полнотой проработки эмуляции.

   c. **Низкоинтерактивные (Low-Interaction)**: Docker-контейнер с приложением, создающим видимость работы реального приложения и не предполагающим прямого взаимодействия злоумышленника с ловушкой.

10.2.3. Просмотр ловушек

Информация о ловушках отображается в разделе **Ловушки**.

Просмотреть подробную информацию о ловушке можно по нажатию на строку в списке ловушек. В правой части экрана отобразится карточка ловушки. Кнопка **Подробнее** отображает карточку в расширенном режиме.

В карточке представлена информация о ловушке (набор данных зависит от типа ловушки):

- Название.
- Статус. Ловушку можно отключить с помощью переключателя в верхней части карточки.
- Тип.
- Сетевые параметры.
- Сервер Trap Manager.
- Дата создания и обновления.
- Параметры протокола или виртуальной машины (в зависимости от типа ловушки).

Вы можете выбрать несколько ловушек в списке с помощью флажка в левой части списка.

В карточке и в списке отображается статус ловушки:

- **Активна**: ловушка работает.
- **Выключена**: ловушка отключена. Вы можете включить ловушку с помощью переключателя в карточке ловушки.
- **Ошибка**: ловушка может быть настроена неверно. Проверьте настройки.
- **Перезапуск**: автоматическая перезагрузка ловушки при возникновении ошибки.

10.3. Работа с графиками

В этом разделе приведено описание работы с графиками в системе.

10.3.1. Об отображении данных

Дашборд отображает сводные данные о работе системы. На дашборде отображаются показатели работы системы, например, статистика ловушек и событий.

Данные обновляются автоматически.

10.3.2. Просмотр данных на дашборде

Чтобы просмотреть данные, перейдите в раздел **Дашборд**.

Для просмотра подробной информации наведите курсор мыши на сегмент графика.

Изменить размер виджета можно, потянув за нижний правый угол.

10.4. Работа с приманками

В этом разделе описаны действия по управлению приманками.

10.4.1. Добавление приманок

Чтобы добавить приманку:

1. Перейдите в раздел **Приманки**.
2. Нажмите на кнопку **Создать**. На экране отобразится окно **Создание приманок**.
3. На первом шаге выберите способ создания приманок:
   a. **Создать приманку вручную**: ввести необходимые данные для создания приманки.
   b. **Создать приманки на основе ловушек**: создать приманки на основе ловушек.
4. Нажмите **Далее**. Последующие шаги зависят от выбранного метода создания.

10.4.1.1. Создание приманки вручную

1. Выберите тип ловушки:
   a. **FTP**: FTP-сервер.
   b. **ОС Windows**: операционная система в сети.
   c. **SMB / SMB FS**: SMB-сервер или доступ к его файловой системе.
   d. **SSH**: SSH-сервер.
   e. **HTTP(S)**: имитация страницы авторизации с логином и паролем.

f. **АСУ ТП**: имитация ПЛК Siemens SIMATIC.

2. Выберите созданную ловушку для новой приманки.
3. Выберите тип операционной системы: **Linux**, **MacOS** или **Windows**.
4. Выберите тип приманки.
5. Имя приманки генерируется автоматически. Для изменения имени введите его в поле **Название приманки**.
6. Для перехода на следующий шаг нажмите на кнопку **Далее**.
7. На третьем шаге введите информацию в зависимости от типа ловушки: IP-адрес, доменное имя, учетные данные, пути к файлам.
8. Нажмите на кнопку **Далее**.
9. Убедитесь, что параметры заданы верно и нажмите на кнопку **Создать**. Если при настройке допущена ошибка, вернитесь на предыдущий шаг по кнопке **Назад**.

10.4.1.2. Создание приманок на основе ловушек

1. Выберите ловушки для создания приманок. Вы можете отфильтровать ловушки по типу или найти определенные ловушки при помощи поискового поля.
2. Нажмите на кнопку **Далее**.
3. На третьем шаге вы увидите доступные типы приманок в виде дерева. Выберите необходимые типы приманок. Нажмите на кнопку **Далее**.
4. На следующем шаге вы увидите выбранные приманки и их количество. Убедитесь, что параметры заданы верно и нажмите на кнопку **Создать**. Если при настройке допущена ошибка, вернитесь на предыдущий шаг по кнопке **Назад**.

10.4.2. О приманках

Приманка (Lure) — это ресурс на конечном хосте сети, который указывает на ловушку (Trap), размещенную в инфраструктуре.

Компонент поддерживает следующие типы приманок:

- Файл HOSTS.
- PuTTY-реестр или его ярлык.
- WinSCP-реестр или его ярлык FTP/SSH.
- FileZilla.

- Реестр Windows Remote Desktop.
- Учетные данные, сохраненные браузером: Я.браузер, Microsoft Edge (актуальная и legacy-версия), Google Chrome, Internet Explorer.
- Текстовый файл с учетными данными.
- Credential Manager (Windows, generic) .
- Файлы сессий и реестров Windows Remote Desktop (.rdp).
- SMB-диск или его ярлык.
- OpenSSH ключи.

10.4.3. Просмотр и удаление приманок

Информация о приманках отображается в разделе **Приманки**.

Просмотреть подробную информацию о приманке можно по нажатию на строку в списке приманок. В правой части экрана отобразится карточка приманки. Кнопка **Подробнее** отображает карточку в расширенном режиме.

В карточке представлена информация о приманке в зависимости от типа приманки:

- Название.
- Тип.
- Дата создания.
- Дата обновления.
- Хост.
- Логин.
- Пароль.
- Порт.
- Имя сессии.
- Имя файла.

Вы можете выбрать несколько приманок при помощи флажков в левой части списка.

Нажмите на кнопку  для импорта информации о размещенных ловушках из файла JSON.

10.4.4. Размещение приманок на пользовательском хосте (Win, MacOS, Linux)

10.4.4.1. Размещение на хосте под управлением ОС Windows

Для размещения приманки в вашем окружении на хосте под управлением Windows:

1. Перейдите в раздел **Приманки**.
2. Выберите одну или несколько приманок с помощью флажка слева от их названия.
3. Нажмите на кнопку **Разместить (**  **)**.

   Система предложит выбрать способ размещения приманок.
4. Выберите способ **Скачать средство размещения приманок.**
5. Чтобы разместить часть приманок на хосте случайным образом, установите флажок **Разместить часть приманок случайным образом**. В этом случае от 70% до 90% приманок будут случайно распределены на вашем целевом хосте.
6. Скачайте архив по кнопке **Скачать**.

   В архиве **hoster-windows.zip** содержится файл **.yml** с параметрами созданных ловушек и исполняемый файл **hoster-win.exe**.
7. Разархивируйте файлы для размещения созданных ловушек.
8. Запустите **hoster-win.exe** на вашем хосте. По окончании размещения приманки этот файл удалит все побочные файлы кроме файла отчета **results.json**.
9. Если между платформой и хостом есть связность, в разделе **Узлы сети** система автоматически добавит новые узлы, соответствующие размещенным приманкам.

10.4.4.2. Размещение на хосте под управлением ОС MacOS и Linux

Для размещения приманки в вашем окружении на хосте под управлением MacOS и Linux:

1. Выполните шаги 1-5 из инструкции по размещению приманок на хосте, приведенной выше в этом разделе
2. Скачайте архив по кнопке **Скачать**.

В архиве **hoster-macos.zip** (или **hoster-linux.zip**) содержится файл **.yml** с параметрами созданных ловушек и исполняемый файл **hoster-mac** (или **hoster-linux**).

3. Разархивируйте файлы для размещения созданных ловушек.
4. Убедитесь, что у исполняемого файла есть разрешение на его выполнение.
5. Запустите исполняемый файл на вашем хосте. По окончании размещения приманки этот файл удалит все побочные файлы кроме файла отчета **results.json**.
6. Если между платформой и хостом есть связность, в разделе **Узлы сети** система автоматически добавит новые узлы, соответствующие размещенным приманкам.

10.4.4.3. Ручная загрузка информации о размещении приманок при отсутствии сетевой связности между конечным хостом и Control center

После запуска **hoster.exe** будет создан файл отчета **results.json**.

Чтобы загрузить информацию о размещении приманок вручную:

1. На странице **Приманки** нажмите кнопку  .
2. В открывшемся окне нажмите на кнопку **Выбрать файл** и укажите путь к созданному файлу отчета.
3. Загрузите файл отчета в систему с помощью кнопки **Загрузить**.

   В разделе **Узлы сети** появятся узлы, соответствующие размещенным приманкам.

10.5. Работа с сетями

В этом разделе приведены инструкции по работе с сетями для размещения ловушек.

10.5.1. Добавление сетей

Чтобы добавить сеть:

1. Перейдите в раздел **Настройки системы → Сети**.
2. Нажмите на кнопку **Добавить**. На экране отобразится окно **Добавление сети**.

3. На первом шаге выберите Trap Manager и его сетевой интерфейс. Компонент проверяет название сети на уникальность.

   Сетевые параметры будут добавлены автоматически.

4. Для перехода на следующий шаг нажмите на кнопку **Далее**.
5. На втором шаге настройте диапазон доступных IP-адресов сети. Для этого введите один или несколько диапазонов.
6. Нажмите на кнопку **Добавить сеть**. Сеть отобразится в списке в разделе **Настройки системы → Сети**.

10.5.2. О сетях

Сеть (Network) — это сущность, отражающая конфигурацию сети для размещения в ней ловушек. В системе каждая сеть уникальна благодаря IP-адресу и маске сети. Сеть можно привязать к нескольким сетевым интерфейсам разных серверов управления ловушками (Сервер Trap Manager). Доступ к сети осуществляется через интерфейсы на Control Center или сервере Trap Manager.

10.5.3. Просмотр информации о сети

Информация о сетях отображается в разделе **Настройки системы → Сети**.

Просмотреть подробную информацию о сети можно по нажатию на строку в списке сетей. В правой части экрана отобразится карточка сети.

В карточке представлена информация о сети:

- Название сети. Название можно изменить по кнопке **Изменить**.
- Статус активности.
- Сетевые интерфейсы и серверы Trap Manager.
- Адрес сети и VLAN ID.
- Информация о шлюзе и DNS-сервере.
- Количество свободных IP-адресов.
- Количество ловушек в сети: активных и общее.
- Диапазон доступных IP-адресов для ловушек.

Вы можете выбрать несколько сетей в списке с помощью флажка в левой части списка.

10.6. Добавление ложных учетных записей

Для добавления слоя ложных учетных записей:

1. Перейдите в раздел **Deceptive LDAP**.
2. Нажмите на кнопку **Настройки**.
3. Выберите домен из выпадающего списка.
4. Выберите Organizational Units (OU) для настройки ложных учетных записей. В левой колонке выделите OU для создания ложных учетных записей необходимых категорий. Затем нажмите на кнопку **+**, чтобы добавить выделенные компоненты. Они будут отображены в колонке справа.
5. Выберите процент ложных учетных записей для OU, указанных на предыдущем шаге. Процент ложных учетных записей определяет количество ложных учетных записей по отношению к реальным. Вы можете выбрать единый процент для всех OU, или отдельные значения для каждого из выбранных OU.
6. Выберите эталонную учетную запись для определения групп, где будут состоять созданные пользователи ActiveDirectory. Вы можете выбрать единую эталонную учетную запись для всех OU, или различные учетные записи для каждого OU.
7. На последнем шаге выводится информация о создаваемых ложных учетных записях.

   При необходимости, вернитесь на предыдущие шаги для изменения параметров.

После добавления слоя ложных учетных записей, выполните следующие действия:

- Выберите добавленный домен в древе **Domains**.
- Выделите добавленные учетные записи и нажмите на кнопку **Внести изменения**.
- Система отобразит окно с запросом на загрузку средства для внесения изменений. Подтвердите загрузку.
- Загрузите средство внесения изменений и распакуйте архив на домене ActiveDirectory с правами администратора.
- Запустите файл `hoster.exe`, чтобы автоматически разместить учетные записи в инфраструктуре.
- По окончании операции система создаст файл отчета `results.json`.
- В верхней части окна нажмите на кнопку **Импорт отчета**,(), чтобы загрузить отчет о размещенных учетных записях. Статус каждой учетной

записи будет отображен в колонке **Статус**. Статус **Размещена** показывает, что учетная запись активна и готова к работе.

- Для экспорта созданных учетных записей во внешнюю SIEM, нажмите на кнопку **Экспорт отчета**. При экспорте записей создается csv-файл.

10.7. Мониторинг событий

В этом разделе приведены инструкции по работе с журналом событий.

10.7.1. Аудит событий

Журнал системы находится в разделе **Настройки системы → Аудит событий**. Раздел доступен пользователям с ролью **Администратор**.

В журнале хранится информация о действиях всех пользователей в системе.

10.7.2. Просмотр событий

Раздел **События** содержит список событий, связанных с регистрацией действий на ловушке.

10.7.2.1. Карточка события

По щелчку на событии в списке открывается карточка события.

В карточке приводятся данные о событии и текст сообщения. Скопировать сообщение в буфер обмена можно по кнопке **Скопировать**.

Под областью сообщения расположена область комментариев к событию. Кнопка **Добавить комментарий** открывает поле ввода комментария. Комментарии отображаются снизу вверх.

Комментарии текущего пользователя снабжаются кнопками **Редактировать** и **Удалить**.

11. МОНИТОРИНГ И АНАЛИЗ СОБЫТИЙ БЕЗОПАСНОСТИ

Функциональный блок мониторинга и анализа событий безопасности:

- Получает индикаторы компрометации от поставщиков данных для анализа угроз.
- Проверяет данные по отдельным индикаторам во внешних источниках. Обработанные данные напрямую передаются на внутренние средства защиты, тем самым снижая количество ложных срабатываний, которые возникают при использовании сырых данных, полученных из фидов.

Преимущества использования блока:

- Упрощает работу с данными TI, непрерывно получая, обрабатывая и сохраняя данные из различных источников в единой базе.
- Облегчает выявление скрытых угроз, обеспечивая автоматический мониторинг индикаторов в SIEM.
- Ускоряет процессы ИБ за счет быстрого поиска информации в доступных источниках и автоматизации ключевых сценариев.
- Позволяет вовремя блокировать угрозы и минимизировать возможный ущерб, благодаря автоматической выгрузке обработанных данных напрямую на СЗИ.

11.1. Интерфейс блока

В этом разделе описаны основные элементы интерфейса.

Вы можете изменить язык интерфейса в разделе **Настройки → Система**.

11.1.1. Главное окно

Главное окно содержит следующие элементы:

- Основное меню системы: обеспечивает навигацию по функциям системы. В нижней части меню отображается текущая учетная запись. Вы можете свернуть меню.
- Рабочая область: отображает информацию и обеспечивает работу с системой. Вид рабочей области зависит от выбранного пункта меню.

11.1.2. Элементы рабочей области

В рабочей области отображаются элементы, с которыми работает пользователь: например, карточки индикаторов, правила обработки. Набор доступных элементов управления зависит от выбранного раздела.

Для элемента доступно меню **Действия**, в котором перечислены действия с элементом: например, редактировать, удалить, выключить.

В правом верхнем углу рабочей области расположена кнопка создания нового элемента.

Если рабочая область содержит список элементов, то доступны действия по управлению списком, например, поиск по элементам и фильтр.

Переключатель в карточке элемента управляет работой элемента. Переключатель имеет два состояния:

- - включено.
- -отключено.

Список можно сортировать по нажатию на заголовок столбца. Повторные нажатия изменяют направление сортировки.

Над списком располагаются инструменты управления (набор инструментов зависит от раздела):

- Строка поиска.
- **Настройки**: управляет отображением столбцов и строк списка.
- **Фильтры**: настраивает критерии фильтрации списка.
- **Экспорт в файл**: экспортирует список в файл.

11.2. Настройка обнаружения

В этом разделе приведены рекомендации по настройке обнаружения индикаторов компрометации в потоках данных внешних систем.

11.2.1. Добавление ноды

Добавьте ноду:

1. Перейдите в раздел **Настройки → Обнаружение**.
2. Нажмите на кнопку **Добавить**. Система отобразит окно редактирования ноды.
3. Введите имя ноды.
4. Вы можете включить ротацию данных, чтобы система при поступлении новых данных автоматически удаляла события, у которых истек срок хранения. Если ротация включена, задайте срок (в днях), по истечении которого система удалит события, полученные из ноды.

5. Вы можете ограничить срок действия ключа авторизации ноды в системе с помощью опции **Ограничить срок действия ключа**. Если переключатель активирован, задайте дату истечения срока действия ключа.
6. Нажмите на кнопку **Сохранить**. В разделе **Обнаружение** отобразится вкладка с именем ноды. Перейдите на вкладку, чтобы добавить интеграции для ноды.

11.2.2. Добавление сенсора

Добавьте интеграцию с SIEM системой, для этого обратитесь за консультатцией в support@rvision.ru и сообщите данные о лицензии.

11.2.3. Настройка ротации данных ноды

В системе можно включить ротацию данных ноды. Если настроена ротация данных, то система при поступлении новых данных автоматически удаляет события, у которых истек срок хранения.

Чтобы отредактировать параметры ноды:

1. Перейдите в раздел **Настройки → Обнаружение**.
2. С помощью меню **Действия** () выберите опцию **Редактировать ноду** ().
3. В новом окне отредактируйте параметры ротации данных: статус (включена/выключена) и срок хранения данных.
4. Нажмите на кнопку **Сохранить**.

11.2.4. О сенсорах

Сенсор — это программный компонент, который осуществляет поиск индикаторов компрометации в различных информационных системах.

Полученные события сохраняются в локальное хранилище системы, что обеспечивает возможность ретроспективного поиска индикаторов.

Сенсоры не могут блокировать трафик, они предназначены для обнаружения и последующего оповещения о фактах нахождения индикаторов компрометации.

Сенсоры входят в состав нод. Ноды — это отчуждаемые программные модули. Ноды передают оповещения о фактах нахождения индикаторов компрометации

в платформу и получают конфигурационные данные для настройки сенсоров и параметры правил обнаружения. Ноды устанавливаются отдельно.

На ноде можно настроить несколько сенсоров любого типа. Сенсоры не требуют отдельной установки. Для получения данных необходимо настроить ноды и сенсоры в интерфейсе платформы.

11.3. Индикаторы

В этом разделе приведена информация по работе с индикаторами: просмотр списка индикаторов, карточки индикатора и обогащение индикатора.

11.3.1. Мониторинг индикаторов компрометации

Обнаружение — это событие, при котором сенсор обнаруживает индикатор компрометации в целевой системе (SIEM).

В разделе **Обнаружения** отображаются все события обнаружения индикаторов компрометации, которые произошли согласно правилам, настроенным в разделе **Автоматизация → Обнаружение**.

Для отображения обнаружений:

- Убедитесь, что настроены поставщики данных.
- Настройте сенсоры.
- Настройте правила обнаружений.

11.3.2. Настройка правила обогащения

Правила обогащения отображаются в разделе **Автоматизация → Обогащение**.

Чтобы добавить правило обогащения:

1. Нажмите на кнопку **Добавить правило**. На экране отобразится окно редактирования параметров правила.
2. Укажите имя и описание правила.
3. Настройте фильтр индикаторов. Индикаторы, для которых выполняются критерии фильтрации, будут автоматически обогащаться с помощью сервиса обогащения.
    a. Укажите источники данных.
    b. Укажите типы индикаторов.

c. Добавьте фильтры индикаторов. Для фильтра укажите критерий, оператор и значения параметра.

4. Выберите сервисы обогащения.
5. Задайте периодичность повторного обогащения индикаторов. В соответствии с заданной периодичностью автоматически повторится обогащение существующих индикаторов компрометации, по которым изменились данные обогащения.
6. Нажмите на кнопку **Сохранить**. Карточка созданного правила отобразится в разделе. Система отображает в карточке правила количество индикаторов, которые подпадают под действие правила.

Можно настроить правило интеграции, чтобы создать инцидент во внешней системе при автоматическом или ручном обогащении индикатора.

Вы можете отключить правило с помощью переключателя в карточке правила. Если правило включено, то переключатель отобразится в зеленом цвете.

11.3.3. Настройка правил обнаружения

Правила обнаружения отображаются в разделе **Автоматизация → Обнаружение**. Карточка правила обнаружения содержит краткую информацию о параметрах правила: название, описание, сенсоры, статистика работы правила.

Чтобы добавить правило обнаружения:

1. Нажмите на кнопку **Добавить правило**. На экране отобразится окно редактирования параметров правила.
2. Укажите имя и описание правила.
3. Настройте фильтр индикаторов. Индикаторы, для которых выполняются критерии фильтрации, будут переданы в сенсор для поиска в инфраструктуре.

   a. Укажите источники данных.

   b. Укажите типы индикаторов.

   c. Добавьте фильтры индикаторов. Для каждого фильтра укажите критерий, оператор и значения параметра.

4. Выберите сенсор SIEM: в списке отображаются ноды и интеграции из раздела **Настройки → Обнаружение**.

5. Нажмите на кнопку **Сохранить**. Карточка созданного правила отобразится в разделе. Система отображает в карточке правила количество индикаторов, которые подпадают под действие правила.

Вы можете отключить правило с помощью переключателя в карточке правила. Если правило включено, то переключатель отобразится в зеленом цвете.

11.3.4. Об индикаторах компрометации

Индикаторы компрометации — это данные, которые могут быть признаками вредоносной активности в инфраструктуре. Индикаторы компрометации используются для:

- выявления подозрительных объектов, процессов, сетевых соединений, рабочих станций и серверов.
- противодействия злоумышленнику, например, хэши вредоносных файлов можно использовать для настройки антивирусного ПО.

Платформа получает данные об индикаторах от поставщиков данных, настроенных в системе. Пользователь может добавить индикаторы вручную или задать правила их формирования.

Платформа не получает данные об индикаторах с IP-адресов, принадлежащих к частным диапазонам, поскольку идентифицирует эти индикаторы как исключения.
К частным диапазонам относятся следующие:
`10.0.0.0 - 10.255.255.255 (префикс 10/8)`
`172.16.0.0 - 172.31.255.255 (префикс 172.16/12)`
`192.168.0.0 - 192.168.255.255 (префикс 192.168/16)`

У индикатора может быть указан рейтинг — оценка влияния индикатора на безопасность системы либо уровень вредоносности объекта, который описывается индикатором компрометации.

При использовании модуля совместно с R-Vision SOAR индикатор компрометации хранит типы активности, связанные с указанным в нем инцидентом.

У индикатора может быть определен статус устаревания:

- **Активный**: индикатор актуален.
- **Неактивный**: индикатор считается неактуальным. Неактивные индикаторы вне зависимости от фильтров не участвуют в правилах обнаружения. В остальных правилах автоматизации нужно применять

фильтр по статусу индикаторов для отсева неактивных. Неактивные индикаторы по умолчанию не отображаются в списке индикаторов.

Данные об устаревании индикатора предоставляет поставщик. Настроить логику устаревания можно в карточке поставщика.

Каждый канал поставщика предоставляет собственные данные об устаревании индикатора. Индикатору присваивается статус **Активный**, если как минимум один канал считает его таковым.

Данные в карточке индикатора можно редактировать. Если пользователь редактирует индикатор, полученный от поставщика, то в системе создается новый индикатор, у которого в качестве источника указан этот пользователь.

Индикаторы, созданные или отредактированные пользователями, можно удалить. Индикаторы, полученные от поставщика, можно удалить при удалении канала или поставщика данных.

Рейтинг рассчитывается с помощью внутреннего механизма для всех индикаторов компрометации, полученных из источников данных. Для индикаторов, созданных пользователями, рейтинг не рассчитывается. Рейтинг можно использовать для принятия решения о дальнейшей работе с обнаруженными угрозами, например, о блокировке потенциально опасных ip-адресов.

Для отображения индикаторов в системе настройте поставщиков данных.

11.3.5. Обогащение индикатора

Для обогащения индикатора:

1. Откройте карточку индикатора.
2. В блоке **Обогащение** выберите внешнюю систему для запроса. В блоке отобразится сообщение о статусе обогащения.
3. Нажмите на кнопку **Запросить обогащение**  . Если запрос выполнен успешно, то в блоке отобразится информация, полученная по запросу. Если запрос не выполнен, то в блоке отобразится сообщение об ошибке.

> По умолчанию индикатор обогащается вручную, по нажатию на кнопку **Обновить**. Это позволяет сократить количество запросов в сервис, количество которых может быть ограничено. Автоматически (при переходе на вкладку) выполняются запросы

к сервисам MaxMind, Sypex. Эти сервисы используют локальные базы, поэтому запрос к ним быстрый и бесплатный.
Информация, полученная от всех внешних сервисов, кэшируется в системе.

11.3.6. Просмотр списка индикаторов

В разделе **Индикаторы** приведен список индикаторов, полученных от поставщиков данных.

В столбцах списка приведена информация о полученных индикаторах:

- **Источники**: потоки данных, в которых обнаружен индикатор. Если индикатор обнаружен в нескольких каналах, то в столбце отображается количество каналов, в которых обнаружен индикатор. При наведении курсора на число каналов отображается перечень каналов.
- **Значение**: значение индикатора.
- Тип индикатора.
- **Рейтинг индикатора**.
- Рейтинг индикатора от поставщика.
- **Страна:** данные о стране индикатора, определяется автоматически для компрометации типа **IP**. Для использования этой функции, нужно создать правило обогащения для индикаторов типа IP и одного из сервисов: MaxMind или Sypex.
- **Отрасли**: данные об отрасли индикатора.
- **Теги:** пользовательские теги, присвоенные этому индикатору.
- **Инциденты**: инциденты, связанные с этим индикатором.
- **Вид сущности**: тип сущности.
- **Тактики MITRE ATT&CK**: значение тактики поставщика данных MITRE ATT&CK для индикатора.
- **Связанные тактики MITRE ATT&CK**: значение связанной тактики поставщика данных MITRE ATT&CK для индикатора.
- **Первое появление:** дата и время первого обнаружения по данным поставщика.
- **Последнее появление**: дата и время последнего обнаружения по данным поставщика.
- **Получен**: дата и время попадания индикатора в базу данных платформы.
- **Создан**: дата и время создания по данным поставщика.

- **Изменен**: дата и время изменения информации об индикаторе в базе данных платформы.
- **Связанные уязвимости**: связанные угрозы типа **Уязвимости**.
- Связанное вредоносное ПО: связанные угрозы типа Вредоносное ПО.
- Связанные личности: связанные угрозы типа Личности.
- **Типы активности**: типы вредоносной активности.
- **Автономная система**: номер автономной системы (Autonomous System Number).
- **Владелец автономной системы**: сведения о владельце автономной системы.
- Категория.
- **Регистратор**: регистратор доменного имени.
- **Virustotal detections**: количество обнаружений VirusTotal.
- **Статус**: статус индикатора.

Кнопка **Добавить** открывает окно добавления индикатора вручную.

Вы можете использовать строку поиска для поиска значения индикатора в списке. Поиск может работать по точному и неполному значению, а также по маскам. Последний критерий используется для поиска индикаторов типа mask. При поиске система учитывает логику формирования маскированных значений, поэтому при поиске конкретных значений будут учитываться и релевантные маскированные * индикаторы.

> Исключение - тип маски 22. Этот тип при поиске не учитывается.

Кнопка **Настройки** () открывает настройки столбцов в списке. Вы можете задать набор столбцов в списке, порядок столбцов и высоту строк.

Для столбцов доступна фильтрация (кнопка **Фильтры** ) и сортировка. Направление сортировки изменяется по щелчку на заголовке столбца.

Кнопка **Экспорт в файл** () экспортирует индикаторы.

Чтобы выделить индикаторы в списке, установите флажок в левой колонке. Чтобы выделить все индикаторы в списке, установите флажок в заголовке левой колонки. Выделенные индикаторы можно редактировать () и удалить ().

11.3.7. Работа с карточкой индикатора

Карточка индикатора представляет собой выделенный экран с набором блоков, которые логически группируют данные об индикаторе компрометации и его контексте.

Откройте карточку индикатора двойным щелчком на строке индикатора в списке в разделе **Индикаторы**. Кнопка **К списку индикаторов** закрывает карточку индикатора.

Краткая информация о деталях индикатора доступна по одинарному щелчку в строке таблицы **Индикаторы**.

Выберите индикаторы с помощью флажка в левой колонке таблицы. При выборе одного или нескольких индикаторов становятся доступны кнопки **Редактировать** () и **Удалить** (). Кнопка **Редактировать** открывает окно редактирования карточки индикатора (доступно в полной карточке пользователям с ролью **Администратор** или **Аналитик**).

> Если пользователь редактирует индикатор, полученный от поставщика, то в системе создается новый индикатор, у которого в качестве источника указан этот пользователь.

Карточка индикатора содержит следующие блоки:

- **Детали индикатора**: источник; статус, значение; тип; вид сущности; тактики из справочника базы MITRE ATT&CK (поле отображается при наличии добавленных тактик), дата и время первого получения данных об индикаторе платформой, рейтинг, пользовательские теги (если заданы). Для индикатора типа Mask отображается тип маски.
  Если индикатор компрометации связан с вредоносным ПО, имеющим атрибут Тактика, в блоке отображается поле **Связанные тактики MITRE ATT&CK**, содержащее теги, связанные с вредоносным ПО, по которому есть данные от поставщика MITRE ATT&CK.
  В этом блоке информация представлена в виде агрегатных значений по набору всех поставщиков, которые предоставляли информацию об индикаторе. Нажав на тип можно отфильтровать список индикаторов по этому типу. Пользователь с ролью **Администратор** или **Аналитик** может редактировать теги в окне редактирования индикатора.
- **Источники**: статус, вид сущности, дата и время получения данных об индикаторе источником (т.е. когда индикатор появился у этого поставщика) и уровень доверия к источнику. Уровень доверия

рассчитывается на основании условного качества фидов. Изменить его нельзя. Вы можете повлиять на расчет уровня доверия при выборе способа расчета рейтинга при ранжировании угроз.
Система получает данные о сущностях из следующих источников:

- Поставщики данных;
- Пользователи;
- Внешние системы.

- **Взаимосвязи**: данные о связи индикатора с другими сущностями системы. Просмотреть взаимосвязи на графе можно по кнопке **Показать связи**  .
- **Обогащение**: данные от подключенных к системе сервисов обогащения.
- **Обнаружения**: количество обнаружений индикатора сенсорами платформы. По кнопке **Подробнее** доступна подробная информация об обнаружении.
- **Жизненный цикл индикатора**: история изменения данных индикатора. Хранение истории индикатора можно настроить в разделе **Настройки → Система**.

Пустые поля в карточке не отображаются.

11.4. Угрозы

В этом разделе приведены инструкции по работе с угрозами.

11.4.1. Об угрозах

Система работает с набором представлений данных об угрозах.

11.4.1.1. Отчеты

Отчеты представляют собой структурированные документы, которые содержат описание угрозы с различной степенью детализации; уязвимости, способы реализации, тактики и действия злоумышленника (TTP), которые могут привести или приводят к реализации той или иной угрозы. Отчеты — это контекст для индикаторов компрометации, который позволяет улучшить понимание угрозы и принять решение о компенсирующих мерах, выработать приоритет действий.

Информация, предоставляемая в отчетах исследователей угроз, отображается в разделе **Отчеты**. Способы формирования отчетов и их содержимого:

- Предоставляются подключенными и сконфигурированными поставщиками данных: в таком случае наличие отчетов зависит от конкретного поставщика данных, потому что не у всех поставщиков есть отчеты.
- Могут быть созданы вручную пользователями.

Отчет может быть связан с индикаторами компрометации, объектами наблюдения, уязвимостями, вредоносным ПО. Взаимосвязи позволяют проследить картину и масштаб угрозы, причинно-следственную связь.

Пользовательскому отчету может быть присвоен один из следующих статусов:

- **Черновик**: работа над отчетом не закончена.
- **Опубликован**: работа над отчетом завершена. Отчету присваивается дата публикации.

Изменить статус можно при редактировании отчета.

11.4.1.2. Вредоносное ПО

Раздел **Вредоносное ПО** содержит информацию о наименованиях вредоносного ПО, которое было обнаружено исследователями при анализе угроз и / или уязвимостей. Наименования вредоносного ПО позволяют лучше понимать контекст угрозы: тактику, технику, цели, мотивацию атакующего. Информацию о вредоносном ПО предоставляют подключенные и сконфигурированные поставщики данных.

Вредоносное ПО может быть связано с индикаторами компрометации, объектами наблюдения, уязвимостями, отчетами. Взаимосвязи позволяют проследить картину и масштаб угрозы, проследить причинно-следственную связь.

11.4.1.3. Уязвимости

Раздел **Уязвимости** содержит информацию об известных уязвимостях. Информация об уязвимостях является полезным контекстом для понимания картины угрозы: будучи привязанной к индикаторам компрометации, объектам наблюдения, отчетам, вредоносному ПО, уязвимость повествует о том, какими средствами, при каких обстоятельствам она может быть проэксплуатирована. Этот контекст помогает сформировать адекватные защитные меры и определить верный приоритет в процессе управления уязвимостями в собственной инфраструктуре. Информацию об уязвимостях предоставляют подключенные и сконфигурированные поставщики данных.

Уязвимость может быть связана с индикаторами компрометации, объектами наблюдения, отчетами, вредоносным ПО. Взаимосвязи позволяют проследить картину и масштаб угрозы, проследить причинно-следственную связь.

11.4.1.4. Кампании

Раздел **Кампании** содержит информацию о вредоносных кампаниях. Кампания представляет собой вредоносную активность, включающую набор действий или атак, которые выполняются в течение определенного периода времени против ряда целей. Наименования кампаний предоставляют полезный контекст угрозы: цели, набор действий и субъект атаки.

Кампания может быть связана с вредоносным ПО, жертвами, индикаторами компрометации.

11.4.1.5. Жертвы

Раздел **Жертвы** содержит информацию о жертвах атаки. Жертва представляет собой объект (человек или организация), на который направлена атака. Информация о жертвах позволяет лучше понимать цели и мотивацию атакующего.

Жертва может быть связана с вредоносным ПО, кампаниями, индикаторами компрометации.

11.4.1.6. Субъекты угроз

Раздел **Субъекты угроз** содержит информацию о лицах или организациях, которые осуществляют злонамеренные действия. Информация об субъектах угрозы позволяет лучше понимать навыки атакующего, его мотивацию и цели.

Субъект угрозы может быть связан с вредоносным ПО, жертвами, индикаторами компрометации.

11.4.1.7. Личности

Раздел **Личности** содержит основную информацию о личности, совершающей злонамеренные действия. Информация о личностях позволяет идентифицировать атакующего и предположить источники данных.

11.4.1.8. Техники

Раздел **Техники** содержит информацию о том, какими методами лица, которые осуществляют злонамеренные действия, достигают тактической цели, а также

описывают, каких целей они при этом достигают. Техники сгруппированы по тактическим категориям.

Каждая техника может выступать в роли вспомогательной техники для другой техники, т.е. будет сабтехникой для этой техники, детально описывая способы выполнения техники, направленные на достижение цели.

Информацию о техниках предоставляет только поставщик данных MITRE ATT&CK. Таким образом, для работы с этой сущностью необходимо убедиться, что данный поставщик подключен к системе. Эта информация доступна только для чтения.

11.4.2. Просмотр, редактирование и удаление угроз

11.4.2.1. Просмотр карточки угрозы

Карточка угрозы представляет собой выделенный экран с набором блоков, которые логически группируют данные об угрозе, полученные от поставщика.

Выберите подраздел раздела **Угрозы** и откройте карточку, нажав на элемент.

- Карточка **отчета** содержит описание и подробную информацию об отчете.
- В карточке **Вредоносного ПО** отображается информация об обнаруженном вредоносном ПО (ВПО) и его взаимосвязях с другими сущностями системы.
  Если данные по ВПО предоставляются поставщиком данных **MITRE Attack** и ВПО связано с Техникой, относящейся к определенной Тактике, в карточке ВПО отображается поле **Тактики MITRE ATT&CK** с названием Тактики, связанной с этой Техникой. При нажатии на название определенной Тактики в списке тактик в этом поле система отображает описание Тактики в отдельном окне.
- В карточке **Уязвимости** отображаются данные об оценке уязвимостей (если доступны).
- В карточке **Кампании** отображается информация о кампании и ее взаимосвязях с другими сущностями системы.
- В карточке **Техники** отображается информация о технике и ее взаимосвязях с другими сущностями, полученными от поставщика данных MITRE Attack.
- В карточке **Субъекты угроз** отображается информация о субъектах угроз, полученных от поставщиков данных.
  Если данные по субъектам угроз предоставляются поставщиком данных **MITRE Attack** и субъект угроз связан с Техникой, относящейся к определенной Тактике, в карточке субъекта угроз отображается поле

Тактики MITRE ATT&CK с названием Тактики, связанной с этой Техникой. При нажатии на название определенной Тактики в списке тактик в этом поле система отображает описание Тактики в отдельном окне.

Просмотреть взаимосвязи на графе можно по кнопке **Показать связи** ().

11.4.2.2. Редактирование карточки угрозы

Пользователь с ролью **Аналитик** или **Администратор** может редактировать:

- Теги в карточках отчетов, вредоносного ПО и кампаний.
- Параметры в карточке уязвимости по кнопке  .
- Параметры отчета в списке отчетов. Пользователь может редактировать свои отчеты, добавленные вручную. Редактирование отчета доступно по кнопке  в карточке отчета.

11.4.2.3. Удаление отчета

Чтобы удалить один или несколько отчетов:

1. Перейдите в раздел **Угрозы → Отчеты**.
2. Выберите отчеты с помощью флажков в левой части списка.
3. Нажмите на кнопку **Удалить** () над списком. На экране отобразится предупреждение об удалении.
4. Чтобы удалить отчеты, нажмите на кнопку **Удалить**. Кнопка **Отменить** отменяет удаление.

11.4.3. Просмотр списка угроз

В подразделах раздела **Угрозы** приведены списки угроз.

В разделе **Угрозы → Отчеты** приведен список отчетов об угрозах, атаках, техниках, тактиках и процедурах, полученных от поставщиков данных.

В столбцах списка приведена информация о полученных отчетах:

- **Имя**: название отчета.
- **Источники**: поток данных, из которого получен отчет. Если отчет получен из нескольких каналов, то в столбце отображается список каналов, в которых обнаружен отчет.
- **Страны**: страны, упомянутые в отчете.

- **Отрасли**: затронутые сектора экономики.
- **Теги.**
- **Создан**: дата и время создания отчета по данным поставщика.
- **Изменен**: дата и время изменения информации об отчете по данным поставщика.

В разделе **Угрозы → Вредоносное ПО** приведен список вредоносных программ, полученных от поставщиков данных.

В столбцах списка приведена информация о полученном вредоносном ПО и соответствующих датах:

- **Источники**: поток данных, из которого получен отчет.
- **Имя**: название вредоносного ПО.
- Теги.
- **Получен:** дата получения информации.
- **Обновлен:** дата обновления информации.
- **Тактики MITRE ATT&CK:** список Тактик (если данные по ВПО предоставляются поставщиком данных MITRE ATT&CK и ВПО связано с Техникой, относящейся к определенной Тактике).

В разделе **Угрозы → Уязвимости** приведен список уязвимостей, полученных от поставщиков данных.

В столбцах списка приведена информация о полученных уязвимостях:

- **Источники**: поток данных, из которого получена уязвимость. Если уязвимость получена из нескольких каналов, то в столбце отображается список каналов, в которых обнаружена уязвимость.
- **CWE**: классификация уязвимости в перечне CWE.
- **Бюллетени**: наличие уязвимости в бюллетени.
- **Имя**: название уязвимости.
- **CVE**: идентификатор уязвимости в базе данных общеизвестных уязвимостей информационной безопасности CVE.
- Вендоры.
- Базовая оценка уязвимости по стандарту CVSS v2.
- Базовая оценка уязвимости по стандарту CVSS v3.
- Теги.
- Наличие патча.
- Дата и время создания, изменения и публикации.

В разделе **Угрозы → Кампании** приведен список вредоносных кампаний, полученных от поставщиков данных.

В столбцах списка приведена информация о полученных кампаниях:

- **Источники**: поток данных, из которого получена информация о кампании. Если кампания получена из нескольких каналов, то в столбце отображается список каналов, в которых обнаружена кампания.
- **Имя**: название кампании.
- Теги.
- Дата и время первого появления.
- Дата и время последнего появления.
- Дата и время получения, обновления, создания и изменения кампании.

В разделе **Угрозы → Жертвы** приведен список жертв атаки, полученных от поставщиков данных.

В столбцах списка приведена информация о полученных жертвах:

- **Источники**: поток данных, из которого получена информация о жертвах атаки. Если информация о жертвах получена из нескольких каналов, то в столбце отображается список каналов, в которых обнаружена информация.
- **Имя**: название жертвы.
- Теги.
- Дата и время получения, обновления, создания и изменения жертвы.

В разделе **Угрозы → Субъекты угроз** приведен список субъектов угроз, полученных от поставщиков данных.

В столбцах списка приведена информация о полученных субъектах угроз:

- **Источники**: поток данных, из которого получена информация о субъектах угроз. Если информация получена из нескольких каналов, то в столбце отображается список каналов, в которых обнаружена информация.
- **Имя**: название субъекта угроз.
- Теги.
- Страны.
- Синонимы.
- Мотивация.
- Цели.
- Дата и время получения, обновления, создания и изменения.
- **Тактики MITRE Attack:** список Тактик (если данные по ВПО предоставляются поставщиком данных MITRE Attack и субъект угроз связан с Техникой, относящейся к определенной Тактике).

В разделе **Угрозы → Личности** приведен список личностей, полученных от поставщиков данных.

В столбцах списка приведена информация о полученных личностях:

- **Источники**: поток данных, из которого получена информация о личностях. Если информация получена из нескольких каналов, то в столбце отображается список каналов, в которых обнаружена информация.
- **Имя**: название личности.
- **Класс**: тип объекта, который описывается данными личности.
- Теги.
- **Страна**: страна, связанная с личностью.
- Первое и последнее появление.
- Дата и время получения, обновления, создания и изменения информации о личности.

В разделе **Угрозы → Техники** приведен список техник и сабтехник от поставщика данных **MITRE Attack**.

В столбцах списка приведена информация о полученных техниках:

- **Название**: техника, описывающая, как противник достигает тактической цели.
- **Является сабтехникой**: индикатор, показывающий, является ли эта техника сабтехникой у другой техники.
- Дата и время создания.
- Дата и время последнего изменения.
- **Тактики**: название тактики, к которой относится данная техника.
- Среда функционирования.
- Обход защиты.
- Обнаружение.

Вы можете использовать строку поиска для поиска угрозы в списке. Поиск работает по точному и неполному значению, в том числе с использованием символов *. В разделе **Угрозы → Уязвимости** можно указать несколько значений CVE уязвимостей в строке поиска.

Для столбцов доступна фильтрация и сортировка. Направление сортировки изменяется по нажатию на заголовке столбца.

11.5. Аналитические отчеты

Аналитические отчеты предоставляют аналитические срезы количественных и качественных данных по поставщикам индикаторов компрометации и событиям обнаружений. Аналитические отчеты помогают экспертам составить представление об актуальности, релевантности и достоверности данных об угрозах.

В системе существует фиксированный набор типов отчетов. Отчеты можно вручную экспортировать в формат pdf и отправлять на адрес e-mail.

Создавать и отправлять отчеты по расписанию на e-mail адрес можно автоматически с помощью правил.

11.5.1. Автоматизация создания аналитических отчетов

Добавлять и редактировать правила создания отчетов могут пользователи с ролями **Администратор** или **Аналитик**.

Чтобы добавить правило создания отчетов:

1. Убедитесь, что в системе настроен почтовый сервер.
2. Перейдите в раздел **Аналитика → Настройка расписания**.
3. Нажмите **Добавить**. Система отобразит окно создания правила.
4. Укажите имя правила.
5. Выберите категорию отчета и заполните поля (набор полей зависит от категории отчета).
6. Укажите каналы данных, используемых для создания отчета.
7. Чтобы создать правило, активируйте переключатель **Автоматическое создание**.
8. Задайте периодичность создания отчетов.
9. Нажмите на кнопку **Сохранить**. Правило отобразится в списке на вкладке **Настройка расписания**. На указанный e-mail платформа будет отправлять отчеты с заданной периодичностью. Отчеты, созданные в результате срабатывания правила, отображаются в списке на вкладке **Аналитика → Все отчеты** и помечаются значком  .

11.5.2. Просмотр списка аналитических отчетов

Список аналитических отчетов отображается на вкладках в разделе **Аналитика**:

- **Все отчеты**: содержит список созданных отчетов. Отчеты, созданные в результате срабатывания правила, помечаются значком  .
- **Настройка расписания**: содержит список правил создания отчетов.

В столбцах списка приведена информация об отчетах.

По кнопке **Фильтры** можно настроить фильтрацию списка отчетов или правил. Вы можете использовать строку поиска для поиска отчета или правила в списке.

11.6. Пользовательские теги

Для маркировки, фильтрации и поиска сущностей в системе можно использовать пользовательские теги.

Редактировать теги могут только пользователи с ролью **Аналитик**.

Теги можно указать в свойствах следующих сущностей: индикаторы, отчеты, вредоносное ПО, уязвимости.

Теги можно использовать в следующих операциях:

1. Поиск и фильтрация в разделе **Индикаторы**.
2. В качестве фильтра в настройках правил в разделах:
   a. **Автоматизация → Обогащение**.
   b. **Автоматизация → Обнаружение**.
   c. **Автоматизация → Экспорт**.

В свойствах сущности можно указать один или несколько тегов.

12. ПОВЕДЕНЧЕСКИЙ АНАЛИЗ ОБЪЕКТОВ ЗАЩИТЫ

Функциональный блок поведенческого анализа объектов защиты (далее компонент) детектирует нарушения в состоянии систем, подозрительную активность объектов и осуществляет динамическую оценку угроз и аномалий.

Аналитические возможности компонента повышают эффективность работы SOC: в потоке подозрительных событий и инцидентов выявляют признаки начинающейся атаки и назначают приоритеты угрозам.

Компонент непрерывно отслеживает события безопасности, анализируя данные из различных источников: систем лог-менеджмента, SIEM-систем и других. Платформа анализирует события, связанные с конкретными объектами, например, пользователями, узлами, файлами, сервисами.

Изучая поведение объектов, компонент формирует профили нормального поведения и фиксирует подозрительную активность при обнаружении отклонений. Система динамической оценки угроз и аномалий рассчитывает рейтинг опасности контролируемых объектов. При обнаружении подозрительной активности рейтинг (скор) объекта увеличивается, и в случае превышения допустимого уровня аналитик получит оповещение.

Компонент автоматически совершенствует встроенную аналитику по выявлению аномалий. При появлении новых источников и моделей данных простые правила и программные эксперты адаптируются в автоматическом режиме и не требуют донастройки. Для анализа данных платформа использует универсальный формат, что позволяет реализовать гибкие алгоритмы детектирования отклонений.

Компонент собирает и хранит события ИБ и предоставляет возможность корреляции и анализ действительно больших объемов данных в реальном времени с использованием сложных алгоритмов и правил. Это позволяет выявлять сложные связи между различными событиями и атаками, а также улучшать проактивность и автоматизировать процессы обнаружения и реагирования на инциденты.

12.1. Просмотр уведомлений

Компонент отображает уведомления о следующих событиях:

- оповещения системы;
- системные ошибки;
- уведомления о состоянии системы.

Просмотреть список уведомлений можно по кнопке  в верхней части экрана.

В списке отображается название, дата и время произошедшего события.

События можно удалить:

- По одному по кнопке **Удалить** () в списке.
- Удалить все события: по кнопке **Очистить** () над списком.

Вы можете отключить уведомления по кнопке **Не беспокоить** над списком. Уведомления будут отключены. Нажмите повторно для того, чтобы вновь активировать уведомления.

12.2. Просмотр объектов наблюдения

В этом разделе приведена инструкция по просмотру данных об объектах наблюдения.

- Об объектах наблюдения
- Просмотр информации об объекте
- Настройка списка объектов наблюдения

12.2.1. Об объектах наблюдения

Объекты наблюдения — это объекты инфраструктуры организации (например, учетные записи пользователей, оборудование в сети организации), данные по которым отслеживает система. Система получает данные по объектам наблюдения и связанным с ними событиям из журналов SIEM систем и Microsoft Active Directory.

Система использует простые правила и программные эксперты для обнаружения аномалий. Связанные аномалии и события сохраняются в виде таймлайна объекта. На таймлайне выстраивается последовательность событий и контекст.

Обнаруженные аномалии повышают оценку риска объекта (скор). Система может оповещать аналитиков об изменении скора объекта и отображать информацию об изменении скора на дашборде.

12.2.2. Просмотр информации об объекте

Чтобы просмотреть информацию об объекте наблюдения:

1. Перейдите в раздел **Объекты наблюдения**.

2. Выберите пункт меню, соответствующий типу объекта: **Пользователи**, **Учетные записи** или **Оборудование**.
3. Выберите объект.

> - Для удобства поиска нужных объектов используйте фильтр и строку поиска в правой верхней части экрана.
> - Вы можете задать, какие данные должны выводиться в списке объектов - для этого воспользуйтесь кнопкой **Настройки** над списком.

4. В правой части экрана отобразится **карточка объекта**. В нижней части карточки объекта находится кнопка **Смотреть таймлайн**, при нажатии на которую отображается хронология событий, связанных с объектом наблюдения. Для объектов **Пользователи** кнопка **Смотреть таймлайн** находится в нижней части вкладки **Основное**.

12.2.2.1. Пользователи

По умолчанию система отображает **Синхронизированных** пользователей (т. е. полученных из Active Directory). Чтобы просмотреть пользователей, созданных в системе вручную, переключитесь на вкладку **Созданные** над списком объектов.

Карточка пользователя содержит вкладки со следующей информацией:

- Основное:
  - **информация о пользователе** (ФИО, контакты, статус и т. д.);
  - **персональные устройства**, с которых пользователь заходил в систему;
  - **пять последних оповещений**, связанных с поведением пользователем (кнопка **Перейти** открывает карточку оповещения);
  - **график работы** - типичное и нетипичное время работы пользователя в системе, полученное на основе работы программных экспертов.
- Аналитика:
  - **рейтинг** - суточный показатель уровня отклонений от нормального поведения пользователя; включает график в виде временной шкалы, где показано распределение аномалий за последние сутки;

- **аномалии** - суточная выборка из пяти наиболее частых аномалий с наивысшим суммарным рейтингом;
- **задействованные устройства** - суточная выборка из пяти устройств, на которые пользователь заходил чаще всего;
- **внешние ресурсы** - суточная выборка из пяти программ/приложений, которые пользователь использовал чаще всего;
- **зоны** - суточная выборка из пяти доменных зон, в которых пользователь работал чаще всего.

> Для объектов аналитики, частота использования которых отображается в процентах, первый пункт в списке принимается за эталон (100%), частота использования остальных объектов рассчитывается относительно него.

- **Учетные записи** пользователя в системе.

> В карточке пользователя можно управлять его учетными записями в системе.
>
> - Воспользуйтесь кнопкой **Добавить**, чтобы добавить одну или несколько учетных записей.
> - Воспользуйтесь кнопкой с тремя точками справа от учетной записи, чтобы изменить или удалить запись.

- История.

  Для каждого события в истории выводится следующая информация:
  - Дата;
  - Время;
  - Тип события;
  - Пользователь, инициировавший событие.

> Если пользователь имеет имя вида `xService` (например, `PersonAccountsService`), это означает, что действие было совершено системным процессом.

- Для события **Изменения в данных** отображаются детали изменений в виде двух столбцов: слева показывается предыдущая версия данных, справа - актуальная версия.

Пользователей, созданных вручную, можно редактировать.

12.2.2.2. Учетные записи

Карточка учетной записи содержит следующие данные:

- **общая информация** об учетной записи (название, тип, система);
- **рейтинг** - показатель уровня отклонений от нормального поведения учетной записи за все время наблюдения;
- **количество оповещений** о состоянии или поведении учетной записи за выбранный интервал;
- **количество аномалий** за выбранный интервал;
- **тренд по рейтингу** - график в виде временной шкалы, где показано распределение аномалий в поведении учетной записи на временном отрезке в последние 2 недели.

12.2.2.3. Оборудование

Карточка оборудования (хоста) содержит следующие данные:

- **Информация** - название оборудования и ОС.
- Аналитика за сутки:
  - **рейтинг** - суточный показатель уровня отклонений от нормального поведения хоста; включает график в виде временной шкалы, где показано распределение аномалий за последние сутки;
  - **IP-адреса подключений** - суточная выборка из пяти адресов, с которых наиболее часто подключались к хосту;
  - **пять последних оповещений**, связанных с поведением хоста (кнопка **Перейти** открывает карточку оповещения);
  - **аномалии** - суточная выборка из пяти наиболее частых аномалий с наивысшим суммарным рейтингом;
  - **постоянные пользователи** - выборка из пяти пользователей, которые наиболее часто используют хост за все время наблюдения;

- **пользователи** - суточная выборка из пяти пользователей, которые наиболее часто использовали хост под своей учетной записью;
- **зоны** - суточная выборка из пяти доменных зон, к которым наиболее часто подключался хост.

12.2.3. Настройка списка объектов наблюдения

В разделе **Объекты наблюдения** можно настроить вид списка объектов:

1. Откройте нужный список (**Пользователи**, **Учетные записи** или **Оборудование**).
2. В правом нижнем углу списка нажмите на кнопку **Настройки таблицы** (). Откроется карточка настроек таблицы, которые включают:
   - набор отображаемых колонок,
   - высоту строк в списке.

Чтобы вернуться к первоначальным настройкам, нажмите кнопку **Сбросить**.

12.3. Корреляция данных - настройка простых правил

При создании простого правила пользователь задает набор критериев. События, удовлетворяющие набору критериев простого правила, помечаются индикатором правила и получают рейтинг.

Обнаруженные события формируют рейтинг объекта и отображаются в таймлайне.

НравитсяСтаньте первыми кому понравится это

12.3.1. Включение и выключение простого правила

Чтобы переключить состояние правила:

1. Откройте список правил в разделе **Настройки системы → Простые правила**.
2. В строке правила переключите состояние правила с помощью переключателя:
   a. Переключатель в правом положении: правило активно и используется.
   b. Переключатель в левом положении: правило неактивно.

Неактивные правила в списке отображаются после активных.

Если правило отключено, то оно не присваивает рейтинг событиям. При повторном включении правила система предлагает провести ретроспективный анализ данных для поиска аномалий, пропущенных за период неактивности правила. Если ретроспективный анализ отключен при включении правила, то пропущенные аномалии будут утеряны.
Чтобы восстановить пропущенные аномалии:

1. В окне запроса включите ретроспективный анализ и задайте дату начала пересмотра данных.
2. Нажмите на кнопку **Включить простое правило**. Система проведет ретроспективный анализ данных.

12.3.2. Добавление правил корреляции

Чтобы добавить простое правило:

1. Перейдите в раздел **Настройки системы → Простые правила**.
2. Нажмите **Добавить**. В правой части экрана отобразится форма **Добавить правило**.
3. Заполните поля:
   - Имя.
   - Описание.
   - Уровень угрозы. Уровень угрозы информирует аналитика о значении рейтинга, который присваивает правило. Значение задается произвольно. Для быстрого ввода значения используйте набор ссылок на значения под полем.
   - Теги. С помощью тегов можно пометить правило.
   - Ограничение уведомлений - максимальное количество уведомлений в минуту, которое отобразит система при обнаружении аномалий. Если количество уведомлений превысит заданное значение, обнаружения сверх этого значения будут регистрироваться в системе без уведомлений.
   - С помощью переключателя **Создать оповещение** можно включить автоматическое создание оповещения при срабатывании правила. При включении этой опции появится выпадающий список с настроенными интеграциями.

4. В разделе **Конструктор правила** нажмите на кнопку **Создать**. На экране отобразится окно конструктора правила.
5. В списке в верхнем углу окна выберите тип правила. В таблице отобразится предварительная информация о событии, которое удовлетворяет набору условий срабатывания правила. Справа над таблицей отображается число совпадений — это число событий, зарегистрированных в системе, которые удовлетворяют условиям правила. Ячейки таблицы и число событий будут автоматически обновляться по мере настройки условий срабатывания правила.
6. С помощью кнопки **Добавить условие** создайте набор условий срабатывания простого правила.

   Условия суммируются по логике И.

7. Для каждого условия укажите:
   - Параметр, в котором система ищет аномалию.
   - Условие для значения параметра. В системе есть следующие варианты условий:
     - **один из**, **не один из**: включить или исключить указанные значения параметра.
     - **Расписание**: день недели и время для параметров типа **Дата**.
   - Значение параметра. Значение можно выбрать из списка или ввести вручную. Значения для параметров типа **Дата** задаются через **Расписание**.

     Значения параметров можно задавать с использованием регулярных выражений.

8. Нажмите на кнопку **Сохранить**. Информация о созданной логике отобразится в разделе **Конструктор правила**. Кнопка **Изменить** () открывает окно конструктора правила.
9. Нажмите на кнопку **Добавить правило**. Правило отобразится в списке.

12.4. Программные эксперты: обучение и анализ данных

Программные эксперты — это программы в составе системы для поиска аномалий в наборе данных. Программные эксперты анализируют журналы объектов наблюдения для поиска аномалий.

Перед началом анализа данных журналов систему нужно обучить. В процессе обучения программные эксперты собирают данные о нормальном состоянии системы.

Данные о нормальном состоянии системы служат основой для поиска аномалий в режиме анализа данных. Отклонения от нормального состояния будут рассматриваться как аномалии.

Система использует обнаруженные аномалии при расчете рейтинга объекта наблюдения, т. е. показателя уровня отклонений от нормального поведения. Рейтинг рассчитывается постоянно по всем полученным индикаторам. При обнаружении подозрительной активности рейтинг объекта увеличивается, и в случае превышения допустимого уровня аналитик получит оповещение.

12.4.1. Настройка параметров обучения системы

Если эксперты обучены ранее, вы можете изменить периодичность автоматического обучения:

- Дообучение - дополнение существующего контекста новыми данными.
- Переобучение - повторное обучение с удалением старых данных и заменой их на новые.

Чтобы настроить обучение системы:

1. Перейдите в раздел **Настройки системы → Обучение системы.** На экране отображается информация о статусе обучения и список обученных программных экспертов.
2. Нажмите на кнопку **Изменить параметры обучения**. На экране отобразится окно настройки обучения.
3. В поле **Интервал дообучения** укажите интервал времени, через который система повторяет наблюдение за объектами для дообучения программных экспертов. Программные эксперты обогащаются дополнительным контекстом. Данные обучения не удаляются. Дообучение экспертов уменьшает число ложных срабатываний.

4. В поле **Интервал переобучения** задайте интервал времени, по истечении которого система удаляет неактуальные данные и обучает экспертов заново. Переобучение экспертов используется при сильном изменении поведения объектов наблюдения.

   - Рекомендуемый срок обучения - один месяц. Минимальный срок обучения для корректной работы системы - две недели.
   - Рекомендуется повторять обучение системы раз в два месяца, но не реже, чем раз в шесть месяцев.
   - При переобучении экспертов анализ поведения объектов наблюдения не прекращается. Наблюдение продолжается на основе уже накопленных данных, которые заменяются на новые при окончании переобучения.
   - Для каждого эксперта в системе задан минимальный срок обучения (как правило, две недели). Интервал дообучения или переобучения не может быть меньше минимального срока обучения эксперта. Поэтому если вы задали интервал дообучения 1 день, но в таблице со статусами экспертов видно, что реальные даты дообучения соответствуют более продолжительному сроку, это означает, что ваш интервал слишком мал, и система выставила интервал дообучения равным минимальному сроку обучения эксперта.
   - Интервал дообучения всегда должен быть меньше, чем интервал переобучения.

5. Нажмите на кнопку **Применить**. Система будет выполнять дообучение и переобучение периодически с заданными интервалами. Интервалы дообучения и переобучения изменятся начиная со следующего интервала.

6. Система начнет обучение, которое будет продолжаться до даты начала анализа. Если система перешла в режим анализа, то она будет анализировать данные до наступления даты дообучения.

Эксперты в таблице **Обученные эксперты** могут иметь следующие статусы:

- **В работе** - эксперт доступен и выполняет мониторинг объектов наблюдения.

- **Отключен** - эксперт недоступен, мониторинг объектов наблюдения не ведется.
- **Нет данных** - мониторинг объектов наблюдения не ведется, так как отсутствуют данные для его обучения.
- **Ошибка** - эксперт недоступен.

Подробнее просмотреть свойства каждого эксперта можно в разделе **Управление экспертами**.

12.4.2. Первичное обучение системы

Для начала анализа данных и поиска аномалий нужно запустить обучение экспертов.

Чтобы запустить первичное обучение:

1. Перейдите в раздел **Настройки системы → Обучение системы.**
2. Задайте параметры обучения системы в разделе **Основные настройки**: укажите даты начала обучения и начала анализа.

   Запустить обучение можно, только если в системе включен хотя бы один эксперт. Проверить доступность экспертов можно в разделе **Эксперты**.

3. В разделе **Дополнительные настройки** вы можете настроить периодичность автоматического дообучения и переобучения. Периодичность можно будет также настроить после завершения обучения.
4. Нажмите на кнопку **Применить**. Система начнет обучение экспертов. По завершении обучения система отобразит статус и информацию об обученных экспертах.

12.4.3. Управление экспертами

Просмотреть список экспертов можно в разделе **Настройки системы → Эксперты**.

Чтобы просмотреть свойства эксперта, откройте карточку эксперта по клику на строке эксперта. В правой части экрана отобразится информация об эксперте.

12.4.3.1. Редактирование аномалий

Чтобы отредактировать аномалии, с которыми работает эксперт:

1. Откройте список экспертов в разделе **Настройки системы → Эксперты**.

По умолчанию в начале выводятся эксперты в состоянии Доступен, затем - недоступные эксперты. Вы можете отсортировать экспертов по алфавиту без учета их состояния с помощью выпадающего меню **Сортировать**, расположенного над списком.

2. Выберите эксперта по клику на строке. В правой части экрана отобразится информация об эксперте.
3. В разделе **Аномалии** в карточке эксперта нажмите на кнопку **Редактировать список**. На экране отобразится перечень аномалий, с которыми работает эксперт.
4. Вы можете указать теги для аномалий в колонке **Теги** напротив названия аномалии. Теги используются в качестве меток. Теги отображаются в информации об аномалии в таймлайне.
5. Настройте уровень угрозы. Уровень угрозы используется для расчета рейтинга.
6. Сохраните изменения по кнопке **Сохранить**.

12.4.3.2. Включение и выключение эксперта

Слева от названия эксперта отображается переключатель состояния. Эксперт в состоянии **Доступен** анализирует данные. Эксперт в состоянии **Недоступен** не используется для анализа данных.

Чтобы изменить состояние эксперта:

1. Откройте список экспертов в разделе **Настройки системы → Эксперты**.
2. В строке эксперта измените состояние с помощью переключателя:
   a. Переключатель в правом положении: эксперт **Доступен** и используется.
   b. Переключатель в левом положении: эксперт **Недоступен** (отключен).

12.5. Просмотр сводных данных

Дашборд отображает сводные данные о работе системы. С помощью виджетов на дашборде отображаются показатели работы системы, например, список основных аномальных учетных записей, статистика событий и другое.

Количество дашбордов и набор виджетов на дашборде можно настроить. Каждый пользователь видит только свои дашборды.

Количество дашбордов и виджетов не ограничено.

Данные виджетов обновляются автоматически за указанный период отображения либо по прошествии отдельно настроенного периода времени, например, каждые 15 минут.

12.5.1. Добавление виджета на дашборд

Виджеты отображают на дашборде информацию о показателях системы.

Чтобы добавить виджет:

1. Перейдите в раздел **Дашборд**.
2. Откройте дашборд, на который вы хотите добавить виджет. Вы можете создавать новые дашборды.
3. Нажмите на кнопку **Добавить виджет**. Вы увидите окно **Добавить виджет**.
4. Выберите тип виджета:
    a. **Средний поток событий**: график, отображающий среднее количество событий в системе за единицу времени.
    b. **Метрики**: системные метрики сервисов.
    c. **Угрозы**: круговая диаграмма с распределением возникших угроз по их количеству.
    d. **События**: статистика событий системы.
    e. **Объекты**: статистика по отслеживаемым объектам системы.
    f. **Пользователи**: диаграмма, отображающая общее количество пользователей и количество аномальных среди них.
    g. **Учетные записи**: диаграмма, отображающая общее количество учетных записей и количество аномальных среди них.
    h. **Оборудование**: диаграмма, отображающая общее количество единиц оборудования и количество аномальных среди них.
    i. **Эксперты**: диаграмма, отображающая общее и активное количество экспертов.

j. **Простые правила**: диаграмма, отображающая общее и активное количество простых правил.

k. **Топ аномальных пользователей**: список аномальных пользователей с максимальным изменением рейтинга за указанный период.

l. **Топ аномальных учетных записей**: список аномальных учетных записей с максимальным изменением рейтинга за указанный период.

m. **Топ учетных записей по ошибкам входа**: список учетных записей с максимальным количеством ошибок входа за указанный период.

n. **Топ аномального оборудования**: список аномального оборудования с максимальным изменением рейтинга за указанный период.

o. **Топ аномалий экспертов**: список наиболее часто встречающихся аномалий за указанный период.

p. **Типы аномалий по экспертам**: список типов наиболее часто встречающихся аномалий за указанный период.

q. **Топ простых правил**: список простых правил с максимальным количеством срабатываний за указанный период.

r. **Лист наблюдения**: настраиваемый список объектов наблюдения, за которыми пользователь может следить в течение определенного периода времени.

- В листе наблюдения для каждого объекта показывается рейтинг за тот день из выбранного периода, когда рейтинг был максимальным.
- Объекты в листе наблюдения сортируются по рейтингу: вверху списка - объект с максимальным рейтингом за выбранный период.
- В лист наблюдения можно включать только один тип объектов наблюдения (например, только Пользователей или только Оборудование).
- В лист наблюдения можно добавить не более 100 объектов.

5. Для определенных типов виджетов нужно задать дополнительные данные:
   - для типов виджетов **k - p** укажите отображаемое количество объектов в списке;
   - для виджета **Лист наблюдения** выберите тип объекта наблюдения.

     Для листа наблюдения можно также задать период автоматического удаления - время, по истечении которого виджет будет удален с дашборда.
6. Задайте произвольное название виджета.
7. Установите переключатель **Включить автообновление**, чтобы задать период автоматического обновления данных виджета. В этом случае данные виджета будут обновляться в течение периода, указанного в разделе **Обновлять каждые**. Если этот переключатель не установлен, данные обновляются в течение периода, заданного в выпадающем списке **Период времени**.
8. Нажмите на кнопку **Добавить виджет**. Виджет отобразится на дашборде.

У добавленного виджета есть меню **Действия** ( ), через которое виджет можно отредактировать или удалить.

12.5.2. Добавление дашборда

Вы можете добавить несколько дашбордов для размещения виджетов.

Чтобы добавить дашборд:

1. Перейдите в раздел **Дашборд**.
2. Нажмите на кнопку **Добавить дашборд**. В правой части экрана отобразится область настройки дашборда.
3. Укажите название дашборда. Чтобы переименовать дашборд, нажмите на кнопку справа от его названия.
4. Нажмите на кнопку **Добавить дашборд**. На экране отобразится пустой дашборд. Для отображения информации, добавьте виджеты.

12.5.3. Просмотр данных на дашбордах

Чтобы просмотреть сводные данные:

1. Перейдите в раздел **Дашборд**.
2. По нажатию на название дашборда в верхней части экрана откройте список дашбордов.
3. В списке выберите дашборд для просмотра. На экране отобразится выбранный дашборд с набором виджетов.

Изменить размер виджета можно, потянув за нижний правый угол.

Переместить виджет на дашборде можно перетаскиванием мышью за заголовок виджета.

С помощью кнопки  (в верхней панели с кнопками управления дашбордом) можно растянуть дашборд на весь экран.

Если на виджете представлены объекты наблюдения, то при нажатии на объект отображается окно с информацией. Кнопка **Смотреть таймлайн** открывает карточку объекта с его таймлайном.

13. ЗАЩИТА КОНЕЧНЫХ ТОЧЕК

Функциональный блок защиты конечных точек (далее компонент) состоит из сервера и управляемых им агентов. Агенты устанавливаются на конечные устройства для выявления угроз и осуществления реагирования на эти угрозы.

Агенты позволяют осуществлять сетевую изоляцию устройства и производить сбор следующих данных:

- Инвентаризационная информация;
- Сведения об уязвимом ПО;
- Телеметрия;
- События.

В результате актуализируется состояние внутренней сети, упрощается реагирование на угрозы, а смежные системы обогащаются дополнительной информацией.

13.1. Работа с компонентом

На стартовой странице функционального блока доступны вкладки **Агенты** и **Политика Агентов**, а также левая панель с настройками системы.

13.1.1. Работа с агентами

На вкладке **Агенты** показывается таблица с данными обо всех имеющихся агентах:

- Имя и статус;
- Группа, в которую включен агент;
- IP-адрес;
- Данные об активности;
- ОС, под которой работает агент;
- Версия агента.

На вкладке доступен поиск по имени агента. Начните вводить запрос в поле поиска в правой верхней части экрана (как минимум два символа). Система отобразит в таблице только имена агентов, включающие данное сочетание символов.

При нажатии на строку агента система отображает в правой части экрана карточку со сведениями об агенте.

13.1.1.1. Действия на агенте

Если на вкладке **Агенты** вы выбрали одного или нескольких агентов и нажали на кнопку  над списком агентов, система отображает окно **Действия на агенте**, где можно выбрать действие, которое нужно произвести над агентом:

1. **Поиск IoC** - поиск индикаторов компрометации IoC на хостах, где установлены агенты.
2. **Удалить файл** - удаление файла или директории на хосте.
3. **Самоизоляция хоста -** изоляция хоста от агента.
4. **Снятие самоизоляции хоста** - отмена предыдущего действия.
5. **Остановка процесса** - остановка выполнения указанного процесса на выбранном агенте.
6. **Отправка файла** - отправка файла на указанный URL.

В зависимости от выбранного действия система отображает в окне параметры, которые нужно указать.

13.1.1.2. Команды агента

Вы можете выполнить в отношении агентов ряд команд:

1. Выделите строку или строки агентов в таблице, установив флажок слева от имени. В панели над таблицей система отобразит иконки следующих команд:
   -  - перезапуск агента;
   -  - обновление версии агента;
   -  - удаление агента из системы.
   -  - меню действий на агенте. При нажатии на эту кнопку система отображает окно, где можно выбрать действие над выбранными агентами.
2. Выберите требуемую команду и при необходимости укажите параметры команды. Действие будет выполнено.

13.1.2. Настройка сбора данных журналов из файлов, событий Windows и чтения команд.

Значимые события (например, ошибки при работе приложений) записываются системой, под которой работает агент, в специальные журналы событий. Также данные можно собирать из файлов в системе агента и с помощью специальных команд.

При настройке политики группы агентов укажите каким способом и по какому пути агенты текущей группы должны собирать данные.

1. В разделе **Чтение файлов/выполнение команд** нажмите на значок редактирования.

   Система отобразит окно редактирования конфигурации.

2. Нажмите на кнопку **Добавить**. Появится строка с набором полей для настройки типа журнала.

3. Нажмите на стрелку в поле **Тип журнала** и выберите требуемый тип из списка.

   Для каждого типа журнала нужно указать **Путь**, используемый системой при сборе данных на агенте.

   - **audit** - используется для событий из инструмента Linux Audit Daemon (auditd). Объединяет последовательные журналы с одинаковым идентификатором в одно событие.

   - **command** - используется для чтения вывода команды, запущенной пользователем root и указанной в теге команды. Каждая строка вывода обрабатывается как отдельный журнал.

     - **Частота** - частота использования команды.

     - **Команда** - текст команды Linux. Например, команда **last -n 5** отобразит список последних 5 терминальных сессий.

   - **djb-multilog** - используется для чтения файлов в формате, созданном сервисным регистратором с несколькими журналами в daemon-tools.

   - **eventchannel** - используется для журналов событий Windows, получает события в формате JSON, контролирует все каналы, указанные в файле конфигурации, и показывает все включенные в

них поля. Может использоваться для мониторинга стандартных журналов событий Windows и журналов приложений и служб.

- **Фильтр** - запрос на языке XPath, позволяющий указать критерии, по которым будут отфильтрованы собираемые данные.

  Например, запрос вида **Event/System[EventID != 5145 and EventID != 5156]** позволит собрать из папки **event/system** в системе, где установлен агент, все события за исключением событий с идентификаторами 5145 и 5156.

- **eventlog** - используется для классического формата журнала событий Windows.
- **full_command** - используется для чтения вывода команды, запущенной пользователем root и указанной в теге команды. Весь вывод будет рассматриваться как один элемент журнала.
  - **Частота** - частота использования команды.
  - **Команда** - текст команды.
- **iis** - используется для IIS (веб-сервер Windows).
- **json** - используется для однострочных файлов JSON и позволяет добавлять настраиваемые метки к событиям JSON.
- **macos** - используется для журналов системы логирования macOS ULS и получает журналы в формате системного журнала.
- **mysql_log** - используется для журналов MySQL, однако, это значение не поддерживает многострочный журнал.
- **nmapg** - используется для мониторинга файлов, соответствующих выводу данных в grepable формате при использовании утилиты nmap.
- **postgresql_log** - используется для журналов PostgreSQL, однако, это значение не поддерживает многострочный журнал.
- **snort-full** - используется для формата полного вывода системы обнаружения вторжений Snort.
- **squid** - используется для журналов программного пакета squid.

- **syslog** - используется для простых текстовых файлов в формате, подобном системному журналу.

4. После добавления всех необходимых типов журналов нажмите **Сохранить**. Система сохранит настройки сбора данных с агентов в рамках данной политики.

Чтобы удалить строку настройки типа журнала, нажмите  справа от этой строки.

13.1.3. Создание группы агентов

Группу агентов можно создать на вкладке **Агенты**.

Чтобы создать группу агентов с выбранными агентами:

1. Перейдите на вкладку **Агенты.**
2. Выберите из списка агенты для включения в группу.
3. Нажмите на кнопку **Создать группу.**Система отобразит выпадающий список с пунктами меню.
4. Выберите команду **С выбранными агентами**.
5. Укажите имя группы и нажмите на кнопку **Создать.**Система создаст группу с указанным именем и выбранными агентами.

Чтобы создать пустую группу:

1. Перейдите на вкладку **Агенты.**
2. Нажмите на кнопку **Создать группу.**Система отобразит выпадающий список с пунктами меню.
3. Выберите команду **Пустую группу**.
4. Укажите имя группы и нажмите на кнопку **Создать.** Система создаст группу с указанным именем**.**

Чтобы добавить агенты в созданную группу:

1. Перейдите на вкладку **Агенты.**
2. В левой панели выберите созданную группу.
3. Выберите агенты для включения в эту группу.
4. Выберите команду **Добавить выбранные агенты в существующую группу.**

5. В новом окне выберите группу, в которую необходимо включить агенты.
6. Нажмите на кнопку **Перенести**.

   Система добавит агенты в выбранную группу.

13.1.4. Технический аудит агентов

Контрольные показатели, разработанные некоммерческой организацией Center for Internet Security (CIS), являются международными стандартами безопасности для защиты ИТ-систем и данных от кибератак. Рекомендации CIS доступны в виде специальных политик и могут применяться для оценочного тестирования существующих развертываний и проверки их безопасности.

Система позволяет получить ряд преимуществ в области кибербезопасности, проведя технический аудит агентов, установленных на конечных устройствах.

В ходе аудита анализируются следующие сущности системы:

- Файл;
- Папка;
- Процесс;
- Команда;
- Реестр (только для Windows).

По итогам аудита система отобразит конкретные рекомендации по настройке безопасной конфигурации ваших ИТ-систем.

13.1.4.1. Просмотр результатов аудита

Результаты аудита для агента можно просмотреть на вкладке **Агенты**. Необходимо выбрать агента, требуемую политику, а затем проанализировать список проверок в этой политике.

13.1.4.1.1 Просмотр политик агента

1. На стартовой странице модуля перейдите на вкладку **Агенты.**
2. Нажмите на строку агента, информацию о котором необходимо просмотреть. Система отобразит справа панель с карточкой агента.

В верхней части карточки показана информация об агенте:

a. Имя агента.

b. ОС, группа и IP-адрес.

c. Статус и версия.

Ниже в карточке находится список политик, в рамках которых проводился аудит агента, в формате:

- название политики;
- статистика.

Для каждой политики система показывает количество и результаты проверок в составе политики.

Под списком политик отображается история обновлений агента.

13.1.4.1.2 Список проверок

Для просмотра списка проверок в рамках выбранной политики нажмите на стрелку справа от названия политики.

Система отобразит информацию по статистике проверок, дату и время последнего сканирования, а также таблицу со списком проверок.

Для быстрого поиска данных в списке проверок используйте поле поиска и кнопку фильтра.

Данные списка проверок можно выгрузить в файл формата .csv. Для навигации по страницам таблицы и настройки отображения количества записей на странице используйте поля внизу таблицы.

Чтобы отфильтровать проверки по статусу, нажмите на количество проверок, имеющих данный статус.

13.1.4.1.3 Просмотр проверок

Для просмотра проверок в рамках выбранной политики нажмите на стрелку справа от индикатора статуса в строке выбранной проверки. Система отобразит подробную информацию о выбранной проверке:

- описание;
- проблема;
- рекомендации по устранению проблемы;
- данные по проверке и соответствию.

13.2. Настройка синхронизации

13.2.1. Настройка поиска IoC на хостах с установленными агентами

Для настройки поиска индикаторов компрометации (IoC) на хостах с установленными агентами необходимо создать в R-Vision SOAR специальное поле инцидента типа **Массив** и добавить это поле в категорию **Событие безопасности**.

Чтобы создать поле инцидента и добавить его в категорию:

1. Войдите в систему R-Vision SOAR.
2. Перейдите в раздел **Настройки → Управление инцидентами → Поля.** Раздел доступен пользователям, в свойствах роли которых разрешен доступ к этому разделу с правами на изменение, а также в свойствах учетной записи установлен флажок **Полный доступ** (доступен в режиме Multi-tenancy).
3. Нажмите на кнопку  . В правой части экрана отобразится область редактирования параметров поля.
4. Выберите тип поля инцидента **Массив**.
5. Укажите наименование.

   Например, **Обнаружения IoC на хостах после сканирования**.
6. Сформируйте список столбцов: выберите тип, укажите наименование и тег. Массив должен содержать столбцы типа **Текстовое поле** со следующими данными:

   a. наименование: **Хост;** тег: **findhost.**

   b. наименование: **Путь**; тег: **findpath**.
7. Нажмите на кнопку **Добавить**.

   Поле будет добавлено в систему.
8. Перейдите в раздел **Настройки → Управление инцидентами → Категории**.
9. Выберите категорию **Событие безопасности**.
10. В правой панели в разделе **Поля** нажмите на кнопку **Изменить**.

    Система отобразит таблицу выбора полей.

11. Выберите созданное поле и раздел свойств инцидента, в котором будет отображаться поле (**Общие сведения** или **Дополнительные поля**).
12. Нажмите на кнопку **Сохранить**.

    Система добавит поле в категорию **Событие безопасности**.