ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Платформа мониторинга информационной безопасности VISOR

(Версия 1.1)

Руководство оператора

Листов 95

2019 год

АННОТАЦИЯ

Данный документ является руководством оператора для специального программного обеспечения «Платформы мониторинга информационной безопасности VISOR», версия 1.1 (далее по тексту – Visor).

В настоящем документе содержатся назначение, состав, сообщения оператору и указания для корректной работы с программным обеспечением, в том числе:

– требования к техническим средствам, к системному и общему программному обеспечению, необходимых для обеспечения выполнение Visor;

– основные функции оператора и описание методов их выполнения в Visor/

СОДЕРЖАНИЕ

1 Назначение программы ... 6
1.1 Компоненты Visor и их функции ... 6
1.2 Сервер ... 8
1.3 Агент ... 9
1.4 Агент-коллектор ... 9
1.5 Модуль сбора событий из БД ... 10
2 Условия выполнения программы ... 11
2.1 Список поддерживаемых методов сбора данных ... 11
2.2 Требования к аппаратной конфигурации СВТ ... 13
2.3 Требования к программной конфигурации ОПО ... 15
3 Выполнение программы ... 17
3.1 Веб-интерфейс сервера ... 17
4 Сообщения оператору ... 21
4.1 Выполнение функций аналитика ... 21
4.2 Требования к квалификации оператора, выполняющего функции аналитика ... 24
4.3 Контроль выполнения политик обеспечения безопасности информации ... 24
4.4 Управление параметрами аудита ... 26
4.5 Мониторинг событий информационной безопасности ... 27
4.6 Меню «Мониторинг» ... 28
4.6.1 Управление гео-расположениями ... 29
4.6.2 Управление департаментами ... 31
4.6.3 Привязка узлов к гео-расположению ... 32
4.6.4 Просмотр данных по событиям ИБ в привязке к гео-расположению ... 33
4.6.5 Просмотр отчетов в привязке к гео-расположению ... 36
4.7 Меню «Узлы» ... 37
4.7.1 Паспорт узла ... 38
4.7.2 Общие данные по узлу ... 38
4.7.3 Вкладка «Параметра ОС» ... 39
4.7.4 Вкладка «Аппаратное обеспечение» ... 40
4.7.5 Вкладка «Другое» ... 40

4.7.6 Вкладка «Параметра» ... 41
4.7.7 Наборы узлов ... 41
4.7.8 Установка агента, агента-коллектора из меню «Узлы» ... 42
4.7.9 Удаление агента, агента-коллектора из меню «Узлы» ... 42
4.7.10 Удаление узла из списка узлов ... 43
4.8 Меню «Сканер сети» ... 44
4.8.1 Создание задачи сканирования и добавления нового узла ... 44
4.9 Меню «Поиск» ... 47
4.9.1 Контекстный поиск ... 48
4.9.2 Фильтрация поиска событий ... 48
4.9.3 Просмотр полей нормализации ... 49
4.9.4 Привязка событий к инцидентам ИБ ... 51
4.9.5 Управление поисковыми запросами ... 52
4.10 Меню «Отчеты» ... 53
4.11 Меню «Архив» ... 55
4.11.1 Выполнение задач архивирования ... 55
4.11.2 Задание пути для сохранения файла архива ... 58
4.11.3 Поиск данных из архивных файлов ... 58
4.12 Управление правилами фильтрации событий ... 59
4.12.1 Настройка правил фильтрации событий на агенте или агенте-коллекторе 60
4.12.2 Примеры правил фильтрации событий ... 63
4.12.3 Внутренний аудит правил фильтрации событий ... 63
4.13 Управление правилами корреляции событий ... 64
4.13.1 Создание правила корреляции ... 67
4.13.2 Написание кода (логики) правила корреляции ... 69
4.13.3 Пример правила, контролирующего изменение настроек агента ... 69
4.13.4 Пример правила для событий, поступающих с системы обнаружения вторжений, связанных с выявлением сетевой активности вредоносного кода ... 71
4.13.5 Пример правила для событий, поступающих с системы антивирусной защиты 72
4.14 Вспомогательные инструменты для создания правил корреляции ... 74
4.14.1 Подменю «Списки» ... 74

4.14.2 Создание списка 75
4.14.3 Изменение, удаление списка 75
4.14.4 Подменю «Категоризация» 76
4.15 Настройка параметров оповещения о срабатывании правил корреляции событий 79
4.15.1 Вывод оповещений в веб-интерфейсе 79
4.15.2 Автоматическое присвоение событию метки инцидента 80
4.15.3 Направление уведомлений по E-mail адресу 81
4.15.4 Настройка параметров сжатия e-mail сообщений 83
4.15.5 Изменение отключение или удаление правила 85
4.16 Управление инцидентами 86
4.16.1 Общая таблица инцидентов ИБ 86
4.16.2 Просмотр паспорта (карточки) инцидента ИБ 88
4.16.3 Регистрация инцидентов ИБ 90
4.16.4 Редактирование паспорта инцидента ИБ 91
4.16.5 Пакетная обработка нескольких инцидентов ИБ 92
4.16.6 Комментирование инцидентов ИБ 92
4.16.7 Выгрузка данных об инциденте в формате ГосСОПКА 93
4.16.8 Удаление паспорта (карточки) инцидента 94
4.16.9 Настройка автоматической выгрузки инцидентов 94

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

Visor является программным продуктом и предназначен для оперативного информирования оператора о возникновении в узлах сети состояний, представляющих угрозы безопасности обрабатываемых данных или безопасности функционирования узла, а также для сбора, обработки и представления в удобном для оператора виде данных, в том числе справочного характера, позволяющих проводить разбирательства по фактам нарушения информационной безопасности.

Функции выполняются в произвольном порядке в зависимости от задач оператора.

1.1 Компоненты Visor и их функции

Visor состоит из трех взаимодействующих программных компонентов:

– сервер;
– агент;
– агент-коллектор;
– модуль сбора событий из БД.

Сервер включает следующие компоненты:

– веб-приложение;
– syslog-сервер;
– сервис аналитики;
– основной сервис.

Веб-приложение: формирует веб-интерфейс пользователя и предоставляет доступ к обрабатываемой информации. Осуществляет визуальное представление информации и оповещение об инцидентах.

Syslog-сервер: осуществляет сбор, нормализацию и фильтрацию сообщений, поступивших по протоколу syslog.

Сервис аналитики: осуществляет обработку поступающих данных о событиях с контролируемых средств защиты в соответствии с правилами корреляции и выявление инцидентов ИБ.

Основной сервис: обеспечивает получение передаваемых источниками событий ИБ и других дополнительных данных, нормализацию полученных данных и их загрузку в БД Visor; выгрузку данных из БД в архивные файлы; формирование предустановленных

отчетов на основании собранных данных. Обеспечивает взаимодействие компонентов Visor.

Типовая схема взаимодействия компонентов Visor представлена ниже.

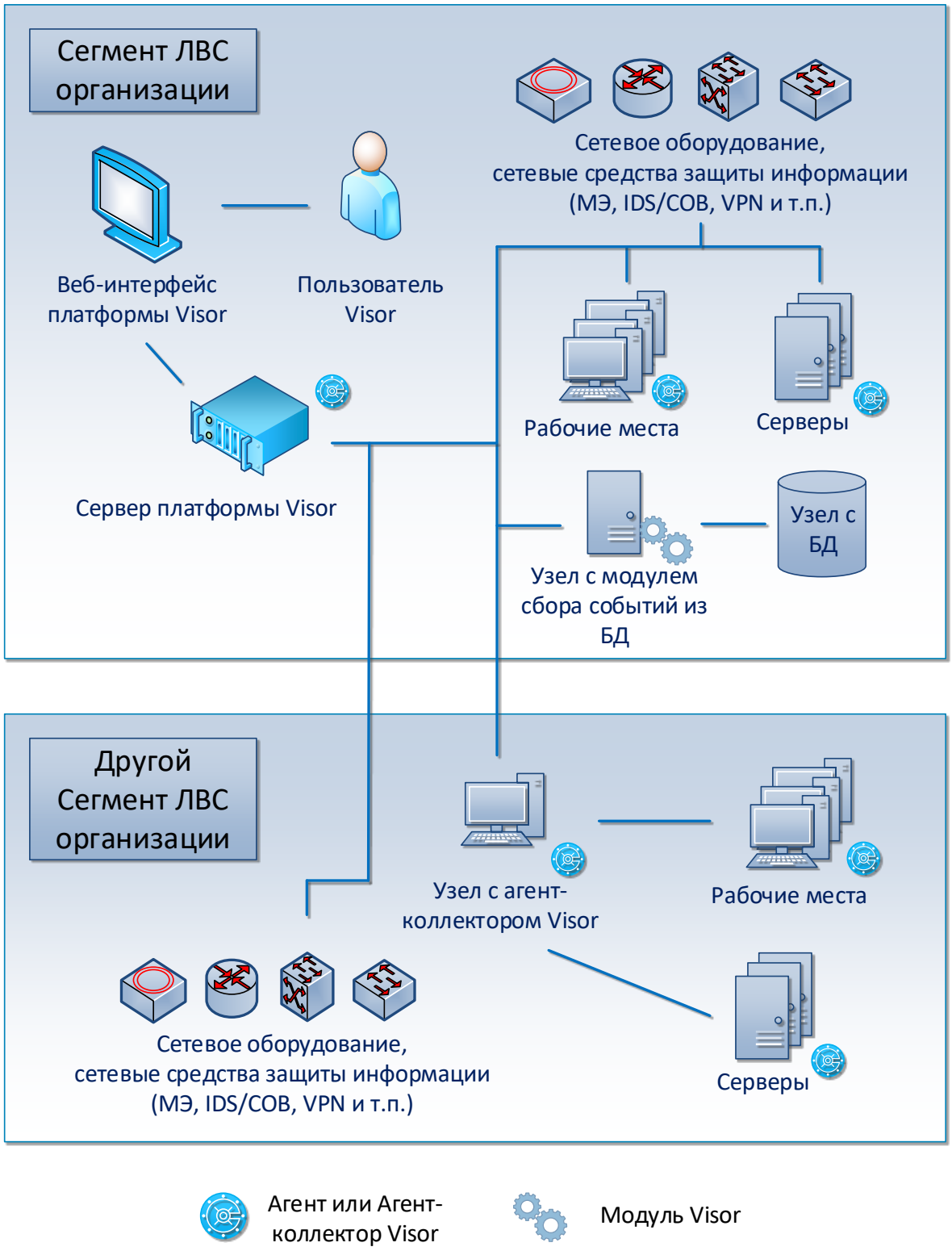


Рисунок 1. Типовая схема взаимодействия компонентов Visor

Сервер располагается в одном из сетевых сегментов ЛВС организации. Для работы с сервером оператор выполняет подключение к веб-интерфейсу сервера посредством введения URL адреса в адресной строке веб-браузера.

Агенты устанавливаются в среду ОС, контролируемых ПЭВМ АРМ и СВТ с программными серверами прикладного назначения. Установленные агенты обеспечивают сбор событий из журналов ОС и программных средств защиты, взаимодействуют по сети с сервером СПО для выполнения передачи на него собранных событий.

Агент-коллектор устанавливается в промежуточный узел (ПЭВМ АРМ, СВТ с программным сервером, входящие в состав контролируемой АС) для обеспечения серверу связи с агентами, расположенными в закрытых для сервера сегментах ЛВС организации.

Модуль сбора событий из БД на сервер Visor либо на отдельный узел (СВТ предназначенное для сбора данных с доступных серверов БД). После настройки модуль начинает выполнять сбор данных из различных БД СУБД и перенаправлять их на сервер Visor.

Для обеспечения сбора данных в Visor должны быть выполнены настройки контролируемого сетевого оборудования и средств защиты, обеспечивающие ведение журналов событий.

1.2 Сервер

Сервер обеспечивает выполнение следующих функций:

– сбор передаваемых агентами, агент-коллекторами и модулем сбора событий из БД, событий и других дополнительных данных, нормализацию полученных данных и их загрузку в БД Visor;

– обработку полученных данных о событиях в соответствии с правилами корреляции и выявление инцидентов ИБ;

– хранение инцидентов ИБ в БД;

– выгрузку данных из БД в архивные файлы;

– выполнение поиска информации в БД и в архивных файлах по заданным критериям;

– формирование предустановленных отчетов на основании собранных данных;

– визуализацию обрабатываемой информации в веб-интерфейсе;

– оповещение в веб-интерфейсе об инцидентах ИБ;

– разграничение доступа пользователей к отображаемой веб-интерфейсе информации;

– дистанционную установку, обновление, удаление агентов и агентов-коллекторов на контролируемых ПЭВМ и СВТ с программными серверами прикладного назначения.

1.3 Агент

Агент устанавливается на контролируемых ПЭВМ и СВТ с программными серверами прикладного назначения (далее – защищаемые активы).

Агент выполняет следующие функции:

– сбор событий из журналов источников (программных средств защиты) на контролируемом активе;

Примечание: список поддерживаемых методов сбора событий агентом, агентом-коллектором представлен в Таблице 1.

– сбор данных об аппаратной конфигурации защищаемого актива, установленных параметрах настройки ОС Windows и подключенных USB-устройствах (состав дополнительных данных приведен в Таблице 2);

– сканирование сегмента сети для обнаружения подключенных сетевых устройств в ЛВС;

– нормализация собранных данных;

– временное хранение собранных данных в собственной локальной БД;

– передача собранных данных серверу или агенту-коллектору;

– получение от управляющего сервера команд на выполнение обновлений версии или конфигурационных настроек агента, на удаление агента;

– получение от управляющего сервера команд на блокировку и разблокировку учетных записей пользователей ОС Windows.

1.4 Агент-коллектор

Агент-коллектор устанавливается на защищаемый актив (на контролируемых ПЭВМ и СВТ с программными серверами прикладного назначения), имеющий сетевой доступ в определенную подсеть ЛВС. Агент-коллектор является прокси-узлом, обеспечивающим передачу серверу данных от агентов, установленных в одной подсети с

агентом-коллектором, при этом выполняет все функции агента, установленного на защищаемый актив.

Примечание: список поддерживаемых методов сбора событий агентом, агентом-коллектором представлен в Таблице 1.

1.5 Модуль сбора событий из БД

Модуль сбора событий из БД устанавливается на сервер Visor либо на отдельный узел (СВТ предназначенное для сбора данных с доступных серверов БД).

Модуль выполняет следующие функции:

– удаленное подключение и сбор данных (событий) из БД (список поддерживаемых методов сбора событий модулем представлен в Таблице 1);

– нормализацию собранных данных;

– временное хранение данных в собственной локальной БД;

– передачу данных серверу Visor;

– получение от управляющего сервера команд на выполнение управляющих команд, связанных с конфигурацией модуля для подключения к контролируемым базам данных и управлением работой модуля.

Модуль сбора событий из БД поддерживает сбор событий из следующих баз данных:

– MySql;

– PostgreSQL;

– SQLite.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Список поддерживаемых методов сбора данных

Visor обеспечивает сбор данных с контролируемых источников методами и в составе данных об аппаратной конфигурации защищаемого актива, которые указаны в таблице 1, таблице 2.

Таблица 1. Список поддерживаемых методов сбора данных с источников событий.

Номер п/п	**Метод сбора данных**	**Область применения**
1.	Сбор данных по протоколу syslog	Применяется для получения событий от источников, поддерживающих передачу данных по протоколу Syslog (например, СОВ «Кречет»).
2.	Сбор данных агентом	Применяется для сбора событий из журналов безопасности ОС Windows, из прикладных журналов Антивируса Касперского, SecretNet, SecurePack и других источников.
3.	Сбор данных модулем сбора событий из БД	Применяется для сбора событий из БД VipNet, MySql, PostgreSQL, SQLite.
4.	Сбор данных из специализированных бинарных файлов	Применяется для сбора событий из бинарных файлов с событиями VipNet и файлов других источников.

Таблица 2. Состав собираемых данных об аппаратной конфигурации защищаемого актива

Номер п/п	**Собираемые данные**	**Описание**
Данные о состоянии актива		
1.	Сетевая доступность актива	Включен или выключен актив.
Данные об аппаратном обеспечении актива		

Номер п/п	Собираемые данные	Описание
2.	Базовая система ввода/вывода	Информация о BIOS: - тип; - производитель; - название; - версия.
3.	Подключенные USB-устройства	Перечень подключенных к активу USB-устройств (за исключением клавиатур и «мышей») и их идентификационных данных: - производитель; - класс; - серийный номер; - имя (если имеется).
4.	Состав аппаратного обеспечения	Перечень характеристик аппаратного обеспечения: - процессор (тип, тактовая частота); - оперативная память (тип, объем); - жесткие диски (количество, объем); - платы расширения (тип, производитель, назначение); - сетевые интерфейсы.
Данные о параметрах настройки ОС		
5.	Настройки ОС	Перечень собираемой информации о настройках ОС должен включать в себя: - перечень параметров политик безопасности; - перечень параметров системных служб.
6.	Установленные обновления ОС	Перечень установленных обновлений ОС Windows: - название обновления; - дата установки.
7.	Учетные записи ОС	Перечень локальных и доменных учетных записей: - тип учетной записи (локальная/доменная); - уровень прав доступа учетной записи;

Номер п/п	Собираемые данные	Описание
		- статус учетной записи (включена/ отключена/ заблокирована/активна). - текущая активная учетная запись в ОС.
8.	Состав ПО	Перечень установленного ПО: - название ПО; - версия ПО; - дата установки.
9.	Лицензии на ОС и прикладное ПО	Перечень лицензий на ПО: - название ПО; - лицензия.

2.2 Требования к аппаратной конфигурации СВТ

СВТ или виртуальная машина, используемые для обеспечения условий выполнения Visor, должны удовлетворять минимальным рекомендуемым требованиям, указанным в таблице 3, таблице 4, таблице 5.

Таблица 3. Рекомендуемые требования к СВТ или виртуальной машины для обеспечения работы сервера.

Количество собираемых событий в секунду	Процессор	ОЗУ	ПЗУ	RAID-массив	Аппаратная платформа
От 500 до 3000 событий в секунду	1 x Intel Xeon-E5 от 6-ти ядер с частотой от 1700 МГц и выше. Доступный	От 16 Гбайт, DDR4	От 10 Тбайт	10	1) Подключение к 2-ум сетевым интерфейсам GbE; 2) Возможность увеличения ОЗУ до 256 Гб; 3) Наличие резервного питания (2x500/700 Вт); 4) Возможность увеличения

	ресурс процессора не менее - 80%.				ПЗУ; 5) Возможность установки дополнительного сетевого интерфейса.
От 4000 до 7500 событий в секунду	2 x Intel Xeon-E5 от 6-ти ядер с частотой от 1700 МГц и выше Доступный ресурс процессоров не менее - 80%.	От 32 Гбайт, DDR4	От 40 Тбайт	10	

Таблица 4. Рекомендуемые требования к СВТ или виртуальной машины для обеспечения работы агента или агента-коллектора.

Процессор	**ОЗУ**	**ПЗУ**	**Аппаратная платформа**
1 x Intel Pentium 4, с частотой от 3 Ghz и выше. Доступный ресурс процессора не менее - 30%.	От 1 Гбайт	От 40 Мб	Наличие сетевого интерфейса (10 Мбит/с и более).

Таблица 5. Рекомендуемые требования к СВТ или виртуальной машины для обеспечения работы модуля сбора событий из БД

Процессор	**ОЗУ**	**ПЗУ**	**Аппаратная платформа**
1 x Intel Core i5 совместимый процессор с тактовой частотой	Минимум 8 Гбайт Минимум 2 Гбайт	Минимум 3 Гб для развёртывания ПО и хранения лог файлов. Минимум 6 Гб для	Наличие сетевого интерфейса (10 Мбит/с и более).

не ниже 2,3 ГГц. Доступный ресурс процессора не менее - 60%.	зарезервированного под сервис модуля	резервного хранения событий.	

2.3 Требования к программной конфигурации ОПО

Для обеспечения функционирования Visor необходима предварительная установка общего программного обеспечения на СВТ, предназначенных для выполнения компонент СПО.

Для обеспечения функционирования сервера требуется предварительная установка:

– ОС Microsoft Windows Server 2008 R2 в редакциях: Windows Server 2008 R2 Foundation, Windows Small Business Server 2008, Windows Server 2008 R2 Standard, Windows Server 2008 R2 Enterprise;

– СУБД PostgreSQL версии 3.6 (32-х или 64-х битные версии);

– .Net Framework версии 4.5.1;

– веб-сервер IIS версии 7.5.

Для обеспечения функционирования агента, агента-коллектора требуется предварительная установка:

– ОС Microsoft Windows 7 (Starter, Home Basic, Home Premium, Professional, Enterprise, Ultimate), Windows 8 (Core, Pro, Enterprise, n, n Pro, n Enterprise), Windows Server 2008 (R2 Foundation, Small Business Server, R2 Standard, R2 Enterprise), Windows Server 2012 Foundation Essentials Standard Datacenter - 32-х или 64-х битные версии;

– программный пакет .Net Framework версии 4.5.1.

Для обеспечения функционирования модуля сбора событий из БД требуется предварительная установка:

– ОС Windows Server 2008 (R2 Foundation, Small Business Server, R2 Standard, R2 Enterprise), Windows Server 2012 Foundation Essentials Standard Datacenter - 32-х или 64-х битные версии или Linux-подобная ОС (Ubuntu 16.04 и выше, Astra Linux).

Для обеспечения сбора событий по протоколу syslog на контролируемом источнике (защищаемом активе) требуется предварительно установить либо настроить:

– клиентский сервис syslogd.

Для обеспечения работы оператора с веб-интерфейсом сервера СПО на ПЭВМ АРМ должен быть установлен любой из указанных ниже веб-браузеров:

– Google Chrome версии 63;
– Mozilla FireFox версии 50;
– Microsoft Internet Explorer версии 11.

Для обеспечения корректного выполнения Visor необходимо соблюдать и обеспечить следующие условия эксплуатации:

– физическую целостность и сохранность работоспособности оборудования, обеспечивающего функционирование компонентов Visor;
– целостность неизменяемых файлов ОПО и Visor;
– защиту ОПО и Visor от вредоносного воздействия вирусов.

3 ВЫПОЛНЕНИЕ ПРОГРАММЫ

Запуск Visor осуществляется в Visor в режиме изолированной программной среды после перезагрузки ОС Microsoft Windows Server 2008 R2 (версии ОС указаны в разделе 2.3) и успешного проведения процедуры идентификации/аутентификации администратора системы.

3.1 Веб-интерфейс сервера

Веб-интерфейс сервера предназначен для отображения обрабатываемой в Visor информации.

Для выполнения входа в веб-интерфейс сервера Visor оператору необходимо на ПЭВМ в веб–браузере ввести адрес сервера:

https://<ip-адрес сервера Visor>

либо назначенное серверу доменное имя

https://<dns имя сервера Visor>

После перехода по ссылке в окне веб-браузера откроется страница приглашения для аутентификации пользователя перед входом в web-приложение Visor.

На данной странице оператор должен ввести учетные свои учетные данные пользователя Visor и нажать кнопку «Войти».

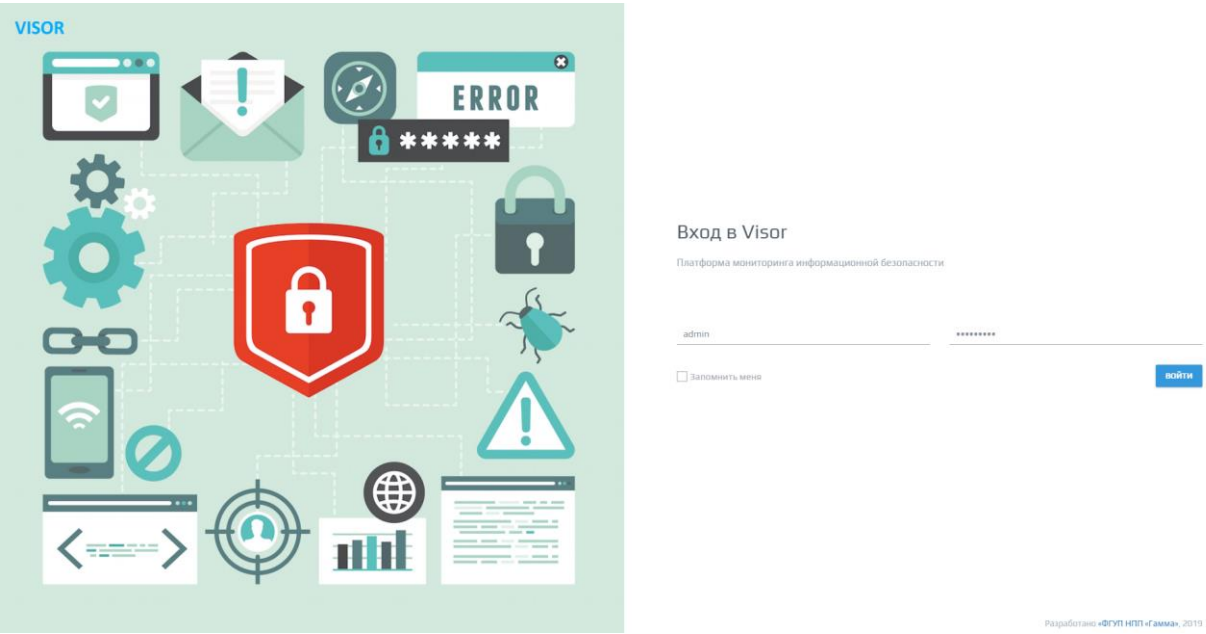


Рисунок 1 - Окно входа в web-приложение Visor

Если учетные данные пользователя Visor введены верно, оператор получит доступ к веб-интерфейсу web-приложения сервера Visor.

Окно веб-интерфейса оператора состоит из следующих основных частей:

– навигационное меню по разделам веб-интерфейса, располагающееся по горизонтали в верхней части экрана и предназначенное для переключения между разделами меню веб-интерфейса Visor (рисунок 3);

– окно выбранного раздела меню, располагающееся по центру экрана и предназначенное для выполнения оператором конкретной задачи в данном разделе меню, вид окна меняется в зависимости от выбранного раздела меню и имеет разное графическое представление данных (рисунок 3);

– окно «Оповещения», располагающееся в верхнем правом углу экрана и предназначенное для отображения оповещений и уведомлений оператору о срабатывании правил корреляции, создании инцидентов и выполнении внутренних задач сервером по установке/обновлению/удалению агентов или агент-коллекторов, созданию архивов и сканирования сетей. По умолчанию окно «Оповещения» всегда свернуто и для его разворачивания необходимо нажать на кнопку, расположенную в крайнем верхнем правом углу экрана (рисунок 4).

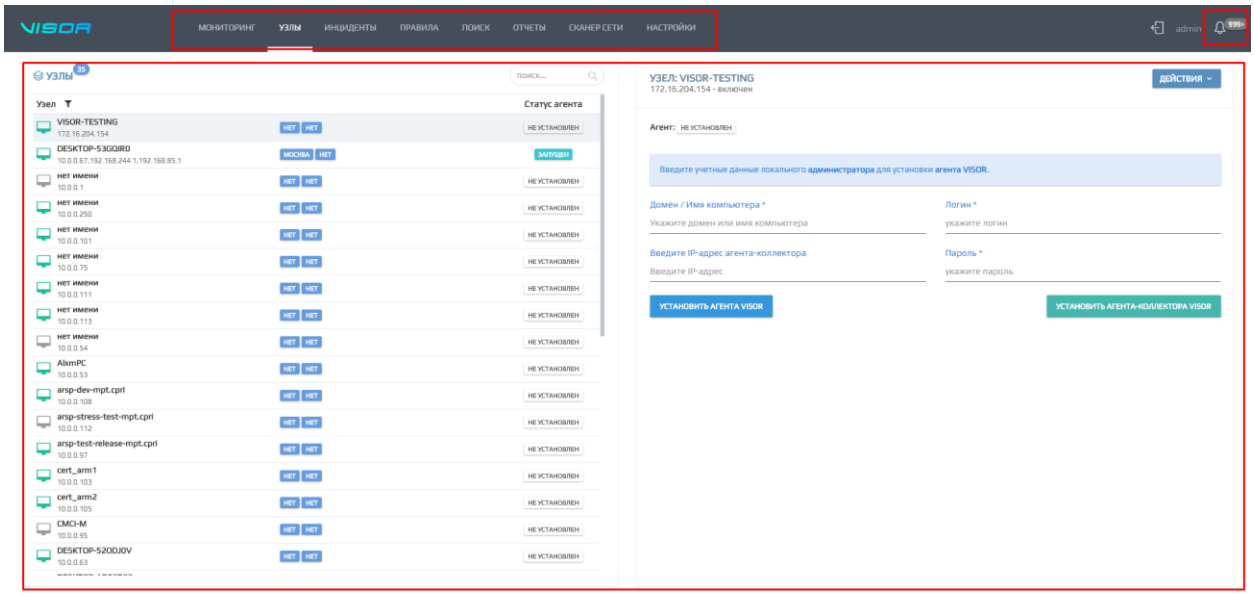


Рисунок 2 – Основные части окна веб-интерфейса оператора

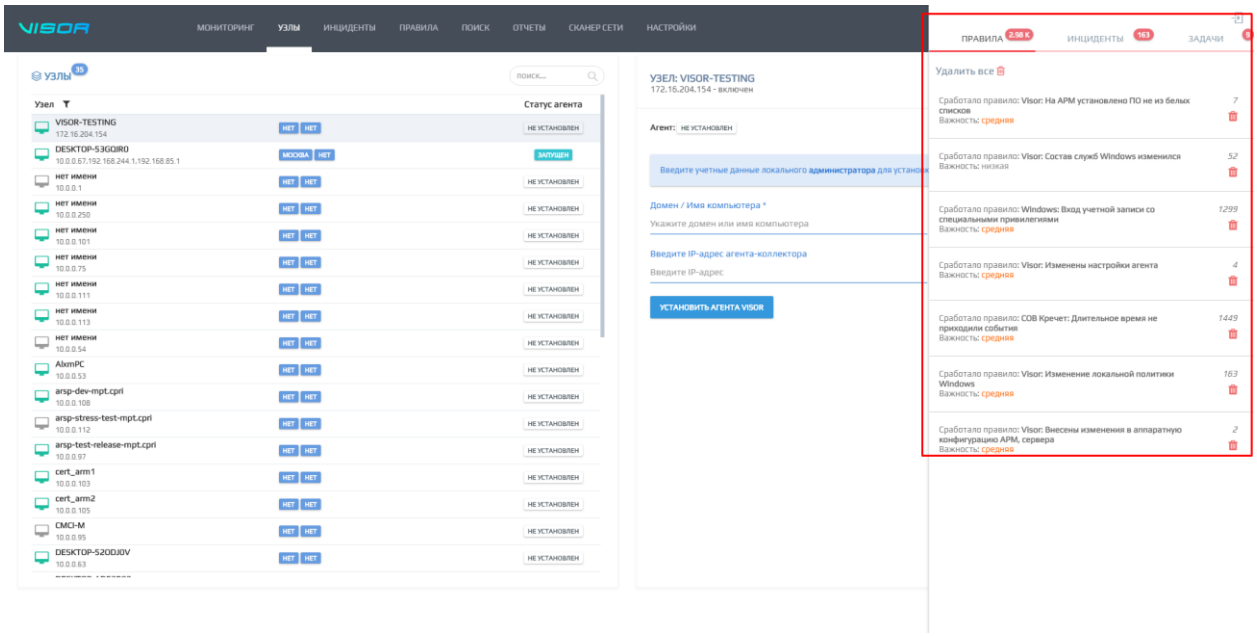


Рисунок 3 - Развернутое окно «Оповещения»

Окно веб-интерфейса оператора состоит из следующих функциональных разделов:

а) Мониторинг;

1)Подменю «Карта»;

б) Узлы;

в) Инциденты;

г) Правила;

1)Подменю «Списки»;

2)Подменю «Категоризация».

д) «Поиск»;

е) «Отчеты»;

ж) «Настройки»;

1)Подменю «Управление доступом»;

2)Архив;

3)Подменю «Интеграция»;

4)Подменю «SMTP»;

5)Подменю «Лицензия»;

6)Подменю «Компоненты и серверы»;

7)Подменю «Настройки инцидентов».

Каждый из разделов меню веб-интерфейса предназначен для выполнения определенных функций и задач.

Если оператор впервые выполнил вход в веб-интерфейс под своей учетной записью, то настоятельно рекомендуется выполнить изменение пароля для персональной учетной записи. Для этого необходимо нажать на имени своей учетной записи, расположенного в верхней правой части экрана веб-интерфейса. На открывшейся странице «Мой профиль» выполнить смену пароля для своей учетной записи (рисунок 5).

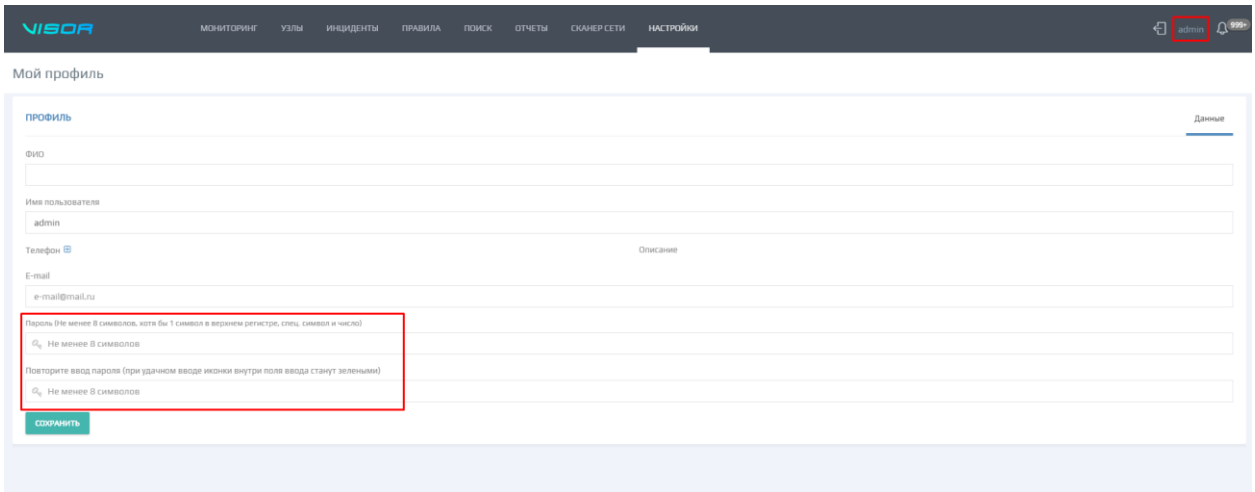


Рисунок 4 – Изменение пароля учетной записи

В дальнейшем рекомендуется выполнять периодическую смену пароля в соответствии с парольной политикой безопасности вашей организации.

4 СООБЩЕНИЯ ОПЕРАТОРУ

4.1 Выполнение функций аналитика

Для выполнения функций аналитика в Visor необходимо наличие в СПО зарегистрированной учетной записи пользователя с ролью Аналитик (Оператор).

Таблица 5 - Функции Аналитика (Оператора)

№	Функция	Назначение	Периодичность	Раздел руководства
1	Управление моделью угроз и нарушителей ИБ	Систематическое определение (оценка), знание, фиксация и пересмотр угроз безопасности информации и методов их реализации в организации.	Непрерывно	См. Раздел 6
2	Управление параметрами аудита для источников событий ИБ	Определение необходимых параметров аудита, которые должны быть настроены на источниках событий ИБ с целью получения необходимых событий ИБ для возможности выявления угроз безопасности информации. Включает в себя отслеживание внесения изменений в настройки аудита и их периодический пересмотр.	Первично при развертывании Visor. Далее выполнять систематический мониторинг настроек с помощью соответствующих правил корреляции. Пересмотр стоит выполнять при подключении новых источников или изменении	См. Раздел 7

№	Функция	Назначение	Периодичность	Раздел руководства
			модели угроз и нарушителей ИБ.	
3	Мониторинг событий ИБ	Систематический просмотр и анализ собираемых событий ИБ от источников и дополнительных данных о защищаемых активах. Определение инцидентов ИБ, подозрительных событий и данных, выявление закономерностей и штатного функционирования защищаемых узлов на основе анализа.	Непрерывно	См. Раздел 8
4	Управление правилами фильтрации событий ИБ	Определение логических условий, запрещающих выполнение сбора определенных событий от источников. Включает в себя периодический пересмотр правил.	Периодически при выявлении событий ИБ, не несущих смысла для определения угроз безопасности. Пересмотр стоит выполнять при подключении новых источников или изменении модели угроз и нарушителей ИБ.	См. Раздел 9

№	Функция	Назначение	Периодичность	Раздел руководства
5	Управление правилами корреляции событий ИБ	Определение логических условий, при которых вероятна компрометация защищаемых активов и реализация угроз безопасности информации, применительно к имеющимся в организации источникам событий ИБ. Включает в себя разработку логических условий на языке EPL (Event Processing Language) и их периодический пересмотр.	Первично при развертывании Visor. Далее выполнять систематический мониторинг их срабатывания. Пересмотр стоит выполнять при подключении новых источников или изменении модели угроз и нарушителей.	См. Раздел 10
6	Управление инцидентами ИБ	Организация регистрации, реагирования, устранения последствий и расследования причин инцидентов ИБ.	Непрерывно	См. Раздел 11
7	Разработка мер предотвращения повторений инцидентов ИБ	Определение мер и средств защиты, необходимых для исключения повторения выявленных инцидентов ИБ в будущем.	После каждого завершения расследования причин и обстоятельств инцидента ИБ	См. Раздел 12

В последующих разделах документа приведено описание и порядок выполнения каждой из функций оператора-аналитика.

Для обеспечения эффективного функционирования Visor недостаточно выполнения функций только оператора, в обеспечении работы Visor важную роль играет пользователь с ролью администратора.

4.2 Требования к квалификации оператора, выполняющего функции аналитика

Для эффективного выполнения функций аналитика рекомендуется, чтобы оператор обладал следующими навыками и знаниями:

– опыт проведения или участия в проведении аудитов ИБ;

– опыт разработки модели угроз и нарушителей ИБ;

– знания стандартов и лучших практик в области информационной безопасности;

– знания и опыт внедрения, эксплуатации средств и систем защиты информации;

– знание принципов штатного функционирования защищаемых информационных систем в организации;

– знание современных методов взлома и использования различных видов угроз информационной безопасности при организации различных типов кибератак;

– базовые знания составления запросов на языке SQL;

– практика мониторинга статистики работы информационных систем и/или пользователей по различным параметрам;

– опыт разработки и согласования нормативных документов в области информационной безопасности.

4.3 Контроль выполнения политик обеспечения безопасности информации

Оператор-аналитик сможет выполнять задачи мониторинга более эффективно, если будет участвовать в систематическом процессе актуализации угроз безопасности информации по отношению к защищаемым активам организации.

На основе знаний об угрозах безопасности, модели угроз и нарушителей, политик обеспечения безопасности информации, обрабатываемой в защищаемых активов оператор сможет:

– определить какие типы источников событий должны быть подключены к Visor, чтобы обеспечить возможность выявления угроз правилами корреляции;

– определить какие именно типы событий от источников будут необходимы для возможности выявления угроз правилами корреляции;

– сформулировать правильные требования для настройки параметров аудита источников событий ИБ, что обеспечить регистрацию необходимых событий в журналах источников событий;

– эффективнее определять приоритет событий ИБ в процессе их мониторинга и выявлять нештатные, подозрительные события ИБ;

– формулировать необходимые правила фильтрации событий ИБ;

– формулировать необходимые правила корреляции событий ИБ;

– эффективнее определять приоритет инцидентов ИБ;

– эффективнее действовать в ходе устранения последствий инцидентов ИБ и их расследований;

– эффективнее разрабатывать меры предотвращения повторений инцидентов ИБ.

Службе безопасности организации рекомендуется до этапа внедрения Visor провести оценку (или переоценку, если это необходимо) угроз безопасности информации по отношению к защищаемым активам.

Желательно, чтобы оператор выполнял свои функции на основе знания следующих систематизированных в организации данных:

– перечень защищаемых и подлежащих мониторингу, активов организации;

– инвентаризационные данные о каждом защищаемом активе;

– данные о приоритетах и уровнях важности одних защищаемых активов по отношению к другим;

– уровни конфиденциальности данных, обрабатываемых на защищаемых активах;

– данные о существующих и возможных угрозах безопасности информации по отношению к защищаемым активам;

– данные о средствах (включая применяемые настройки) и мерах защиты, применяемых в организации к защищаемым активам.

Настройки параметров аудита для источников событий ИБ рекомендуется выполнять с привлечением группы специалистов, выполняющих роли администратора АС, администратора Visor, руководителя службы ИБ.

4.4 Управление параметрами аудита

Настройку источников событий рекомендуется выполнять совместно и по согласованию с Администратором Visor, Администратором АС и руководителем службы ИБ организации.

Visor осуществляет сбор (или получение, в зависимости от протокола или метода получения событий) событий из источников, которыми являются журналы регистрации событий системного, общего и прикладного программного обеспечения, а также программно-аппаратных средств.

Агент и агент-коллектор начинают выполнять сбор событий с даты и времени его установки на защищаемом активе. Сбор событий, записанных в журналы источников событий до момента установки агента или агент-коллектора, не выполняется.

Чтобы в журналах регистрации событий фиксировался необходимый набор событий ИБ, средства аудита системного, общего и прикладного программного обеспечения, программно-аппаратных средств должны быть соответствующим образом настроены. В противном случае события в журналах контролируемых источников событий регистрироваться не будут, при этом они не будут поступать на в Visor и, их обработка в процессах Visor будет невозможной.

Следует всегда поддерживать настройки аудита источников событий ИБ на защищаемых активах в актуальном состоянии и отслеживать внесение изменений в их настройки, чтобы не допустить возможности несанкционированного изменения параметров или отключения аудита в источниках событий ИБ.

Следует учитывать, что параметры настройки аудита для каждого конкретного типа источника зависят от:

- действительной необходимости сбора конкретного типа событий ИБ.
- модели угроз и нарушителей, применимых к защищаемым активам;
- действующие политики обеспечения безопасности информации;
- возможности в тонкости настройки параметров аудита у каждого конкретного типа источника.

4.5 Мониторинг событий информационной безопасности

Одной из основных функций оператора-аналитика является выполнение систематического просмотра и анализа данных о зарегистрированных событиях, поступающих в Visor.

Целью мониторинга является систематическое определение:

– штатных событий и ситуаций на защищаемых активах;

– нештатных, подозрительных и опасных событий и ситуаций на защищаемых активах.

Оператор-аналитик должен на основе своих знаний о защищаемых активах с помощью средств мониторинга Visor отличать закономерные штатные события, которые характеризуют нормальное функционирование и поведение защищаемых активов, от подозрительных и опасных событий, которые могут сообщать о возможных проблемах, ошибках функционирования или потенциальных нарушениях состояния безопасности защищаемых активов и средств защиты.

Оператор-аналитик должен иметь представление о том, какие события возникают при определенных действиях и ситуациях на защищаемых активах. Для этого рекомендуется изучить документацию на источники событий, применяемые в организации, с целью найти перечень всех возможных событий для каждого конкретного источника с их описанием и назначением. Например, оператору-аналитику необходимо знать какова нормальная последовательность и содержание событий в журнале регистрации событий ОС при выполнении входа и выхода пользователя.

После внедрения Visor рекомендуется выделять период первичного мониторинга и анализа (не менее 2-3 рабочих недель) на события для каждого подключаемого типа источника. В этот период оператор-аналитик должен:

– определить и изучить назначение возможных типов событий от данного источника;

– определить последовательность событий при выполнении штатных функций источника событий (например, запуск и выключение) и нормальном функционировании источника событий;

– определить потенциальные для фильтрации, часто повторяющиеся неинформативные события ИБ;

– определить, необходима ли корректировка настройки параметров аудита на источнике событий ИБ.

Например, после подключения системы обнаружения вторжений, применяемой в организации, рекомендуется выделить 2-3 рабочих недели на изучение получаемых событий с целью систематизации знаний о них.

На основании систематического просмотра и анализа событий оператор-аналитик сможет:

– определять и корректировать необходимые для настройки правила фильтрации событий ИБ, чтобы исключить сбор неинформативных данных;

– определять и корректировать правила корреляции необходимые для настройки, чтобы выявлять инциденты ИБ и другие нештатные ситуации;

– выявлять события, которые относятся к инцидентам ИБ.

Для выполнения задач мониторинга оператор-аналитик должен изучить функционал следующих меню окна веб-интерфейса:

– меню «Мониторинг»;

– меню «Узлы»;

– меню «Сканер сети»;

– меню «Поиск»;

– меню «Отчеты»;

– меню «Архив».

Далее будут рассмотрены возможности и назначение каждого из перечисленных меню.

4.6 Меню «Мониторинг»

Меню «Мониторинг» предназначено для отображения двух графических виджетов, отображающих статистику по событиям и узлам:

– Топ-10 категорий событий по источникам;

– Топ 10 узлов по кол-ву событий.

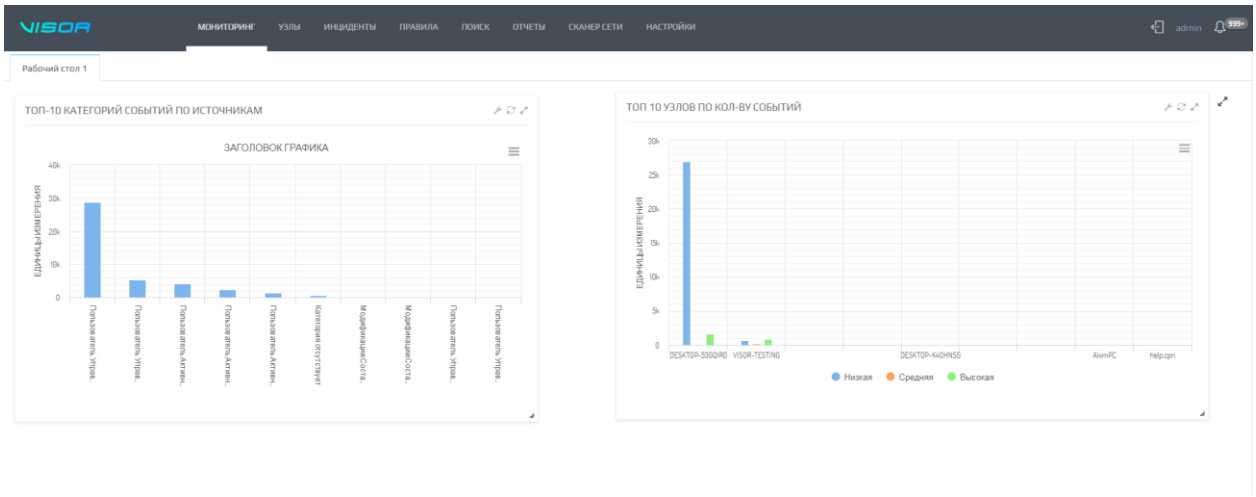


Рисунок 5 – Меню «Мониторинг»

Подменю «Карта» отображает географическую карту мира с расположенными на ней объектами, которые в веб-интерфейсе оператора называются «Гео-расположения».

Отображаемая карта загружается сервером из сети Интернет с веб-сайта проекта - https://www.openstreetmap.org/, поэтому для отображения карты, серверу Visor необходим доступ к данному веб-ресурсу.

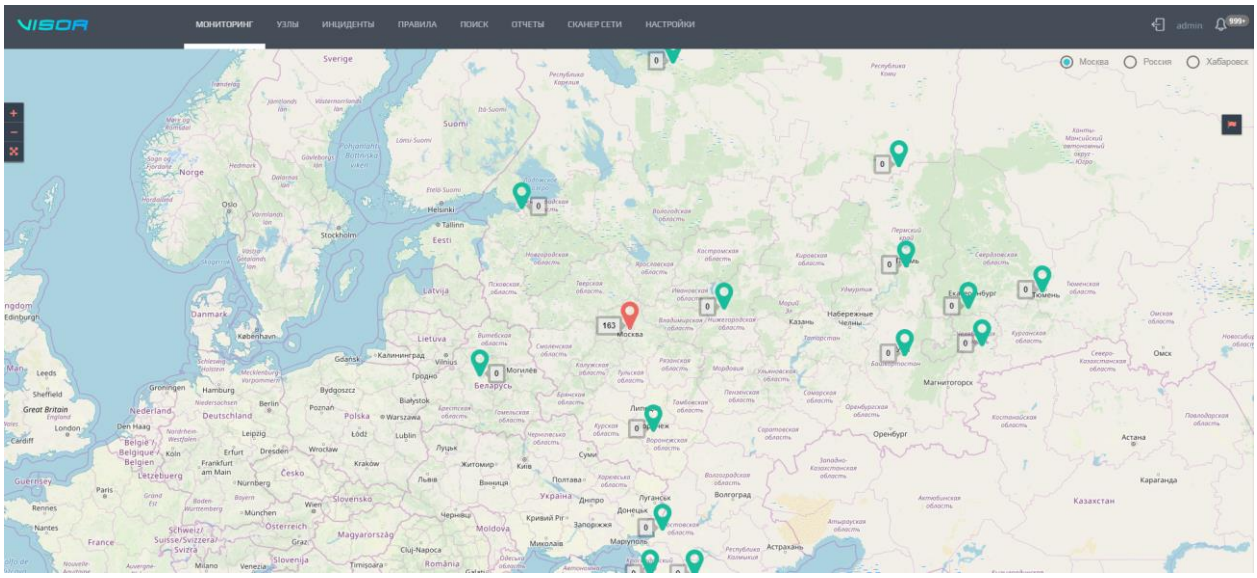


Рисунок 6 – Подменю «Карта»

4.6.1 Управление гео-расположениями

Гео-расположение – это место на карте (с координатами), к которому могут быть привязаны узлы из меню «Узлы».

Для создания гео-расположения кликните в нужном географическом месте на карте правой кнопкой мыши, укажите имя нового гео-расположения и нажмите на кнопку «Сохранить».

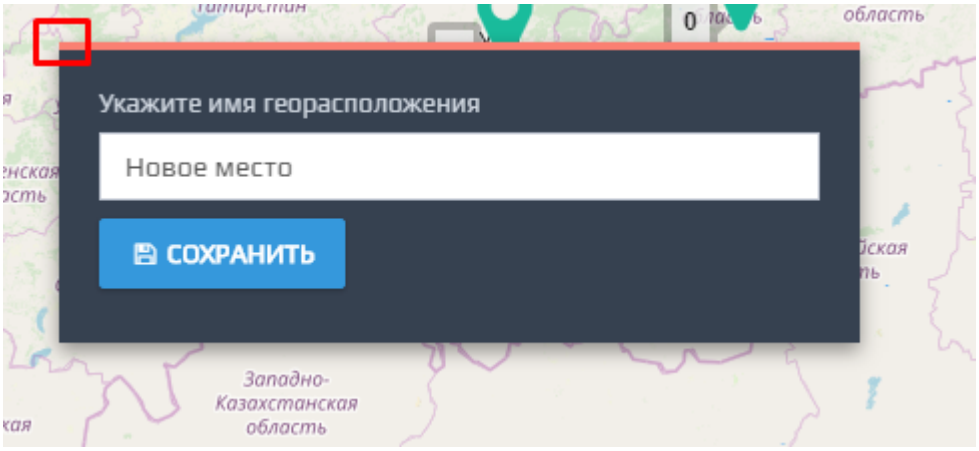


Рисунок 8 – Создание гео-расположения

Вы так же можете создать гео-расположение указав его точные координаты (широту и долготу) нажав на иконке


.

Рисунок 8.1. Иконка

После создания гео-расположения на карте появится соответствующая иконка на карте.

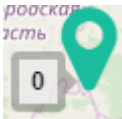


Рисунок 8.2. Иконка на карте.

Цифра «0» рядом с иконкой изображения отображает общее количество инцидентов внутри данного гео-расположения.

Чтобы просмотреть паспорт гео-расположения кликните левой кнопкой мыши на иконке гео-расположения.

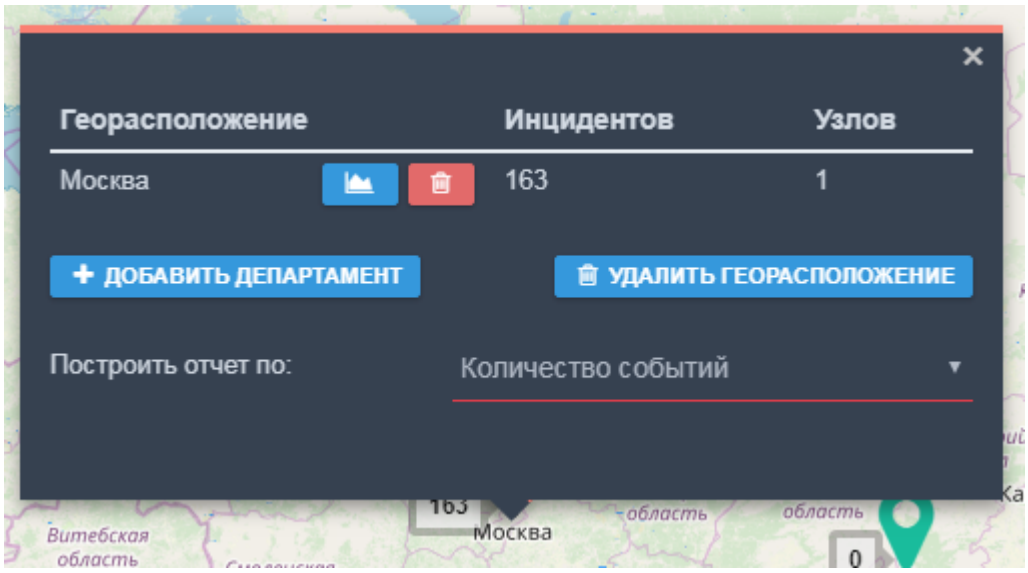


Рисунок 9 – Просмотр гео-расположения

Паспорт гео-расположения содержит следующие элементы:

– Департаменты внутри гео-расположения;

– Количество инцидентов внутри каждого департамента;

– Количество узлов внутри каждого департамента;

– Элементы управления для просмотра отчётов по департаментам;

– Элементы для просмотра диаграммы сетевой доступности между узлами и загруженного изображения карты сети департамента.

Чтобы удалить гео-расположение кликните на кнопке «Удалить гео-расположение» и подтвердите удаление.

4.6.2 Управление департаментами

Внутри каждого гео-расположения может быть несколько «Департаментов». Например, внутри и гео-расположения «Москва» могут быть следующие департаменты: «Здание 1», «Здание 2» и «Здание 3».

По умолчанию, при создании гео-расположения внутри него создаётся один департамент с одноименным названием гео-расположения. Для создания дополнительного департамента внутри гео-расположения нажмите на кнопку «Добавить департамент» и введите имя его имя.

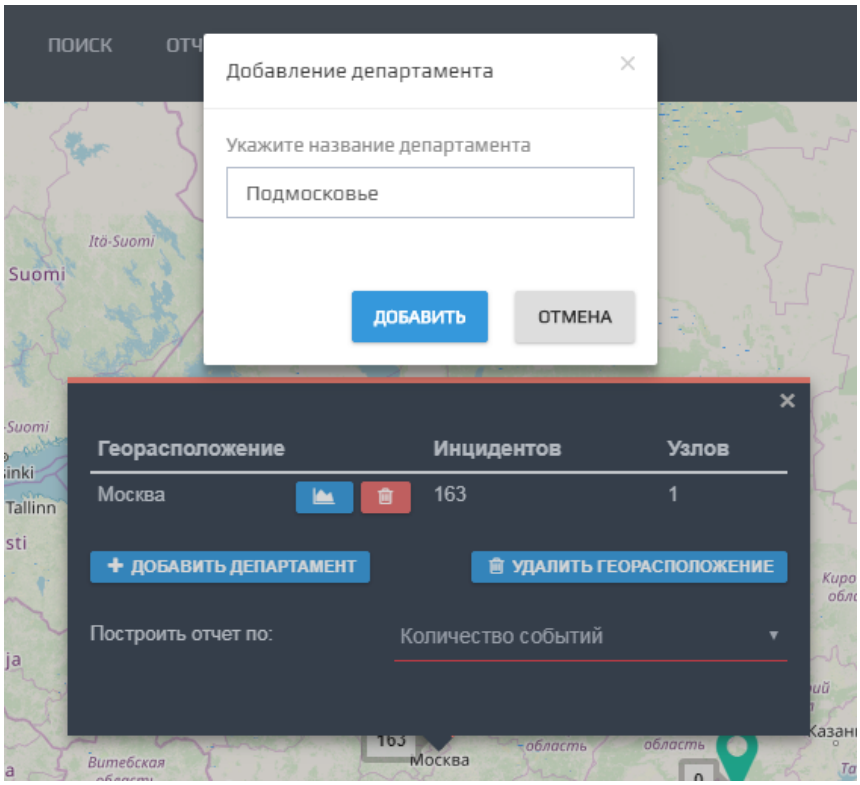


Рисунок 7 – Создание департамента

Для удаления департамента кликните на иконке __, расположенной справа от названия департамента.

4.6.3 Привязка узлов к гео-расположению

После создания гео-расположения их необходимо наполнить узлами. Чтобы привязать узел к конкретному гео-расположению перейдите в меню «Узлы», выберите нужный узел и перейдите на вкладку «Другое» в паспорте узла. Кликните на выпадающем списке «Гео-расположения» и выберите нужное гео-расположение.

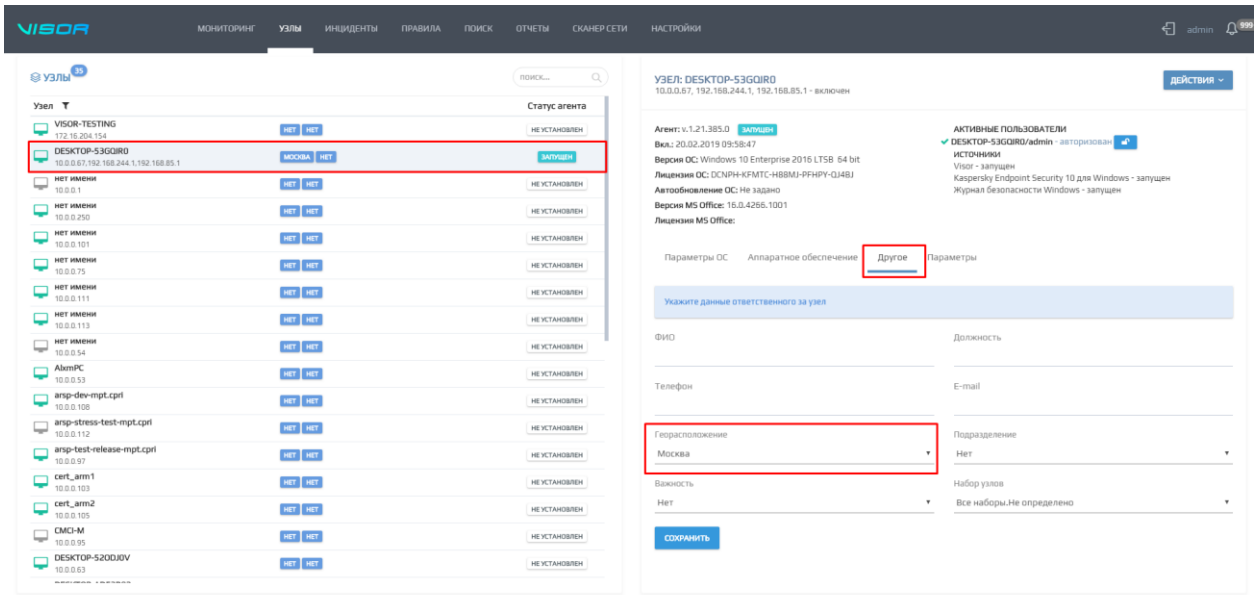


Рисунок 8 – Привязка узла к гео-расположению

После этого в меню «Мониторинг» в данном гео-расположении появится привязанный узел. В будущем, все инциденты содержащие события, полученные от источников с данного узла, будут отображаться в паспорте данного гео-расположения.

4.6.4 Просмотр данных по событиям ИБ в привязке к гео-расположению

В меню «Инциденты» для перехода к инцидентам, которые имеют отношение к конкретному департаменту внутри гео-расположения кликните на соответствующей цифре с количество инцидентов.

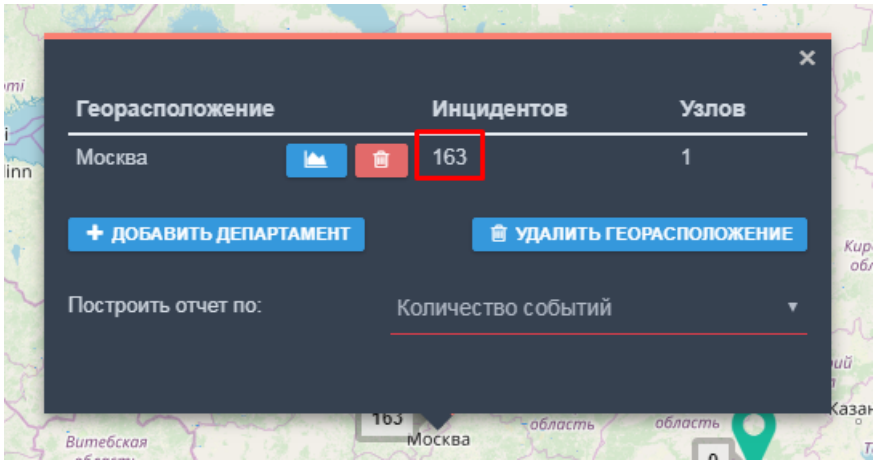


Рисунок 9 – Счётчик количества инцидентов в гео-расположении

Для перехода в меню «Узлы» к узлам, которые имеют отношение к конкретному департаменту внутри гео-расположения кликните на соответствующей цифре с количество узлов.

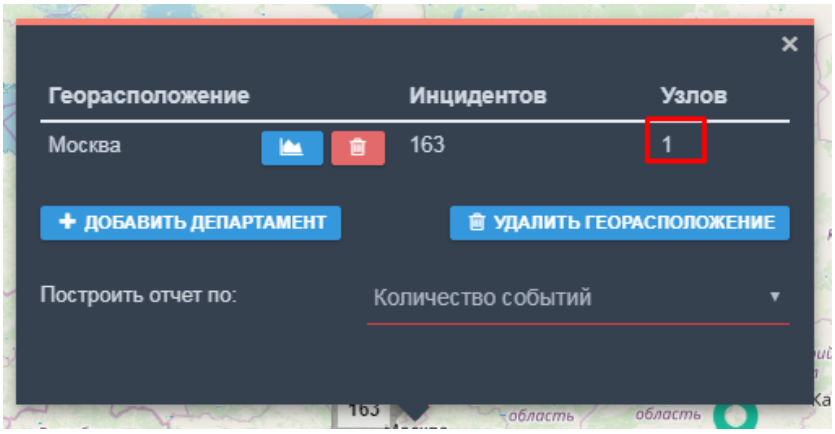


Рисунок 10 – Счётчик количества узлов в гео-расположении

Для просмотра графа сетевой связности узлов внутри гео-расположения кликните на названии соответствующего департамента, справа появится соответствующая схема.

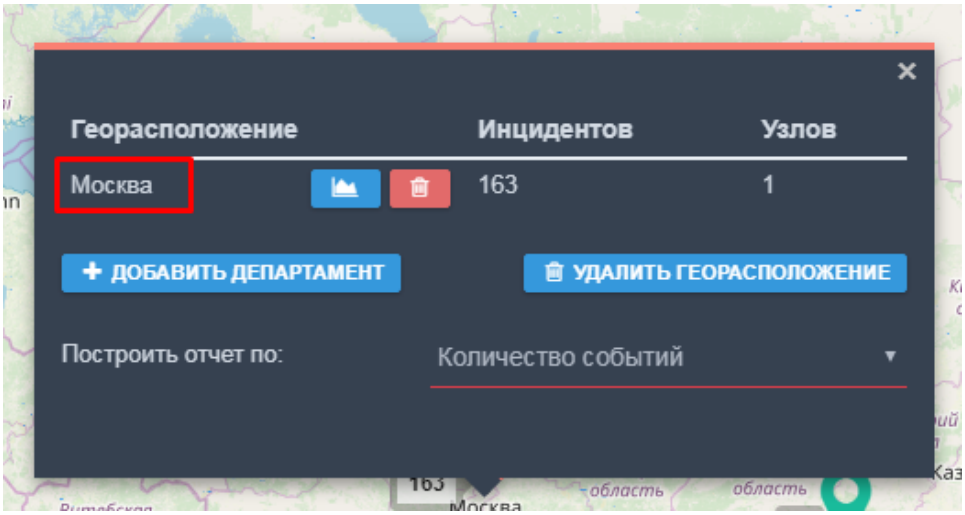


Рисунок 11 – Название департамента внутри гео-расположения для просмотра графа сетевой связности узлов

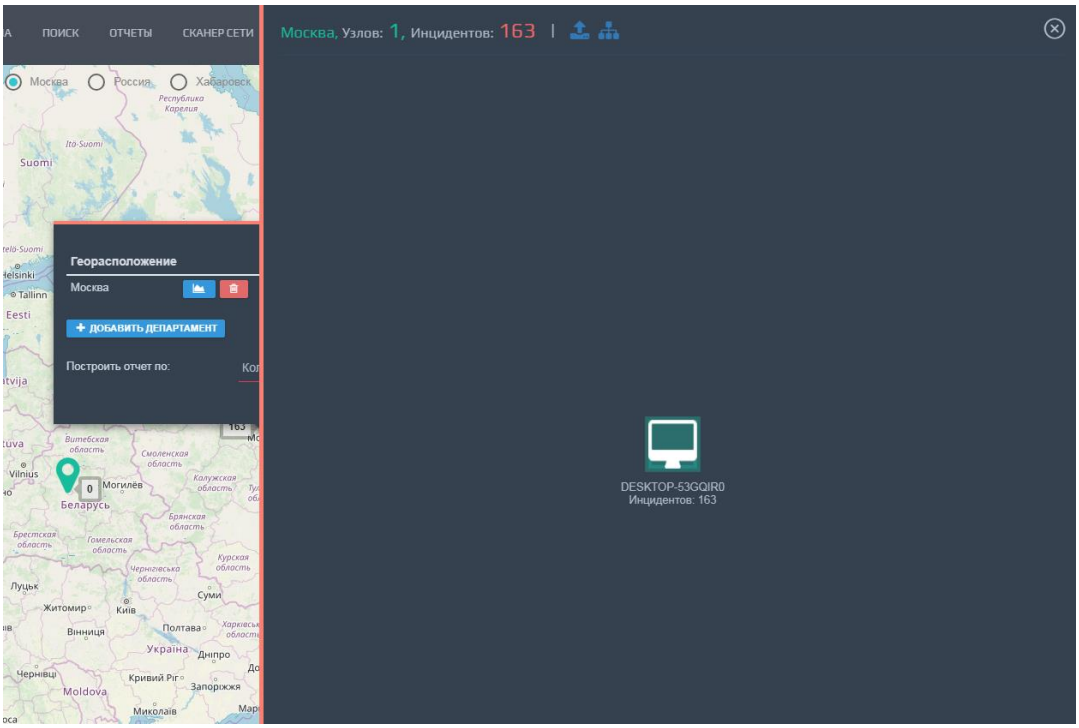


Рисунок 12 – Граф сетевой связности узлов

Для просмотра информации по конкретному узлу кликните правой кнопкой мыши на его изображении.

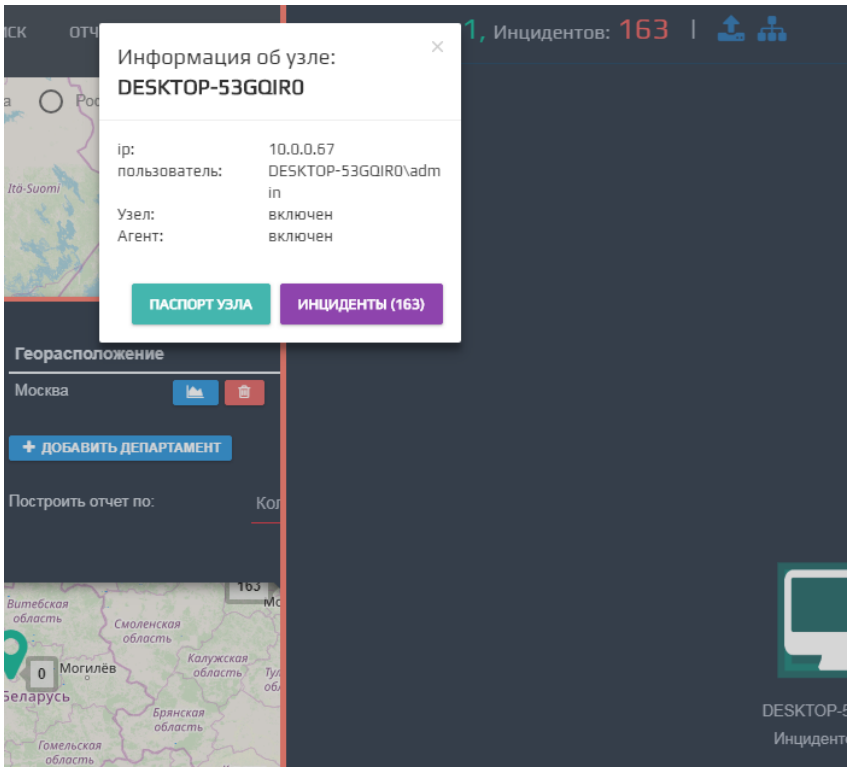


Рисунок 13 – Просмотр информации по узлу на графе

В окне с графом сетевой связности узлов может быть подгружено ваше изображение (например, схема помещения), которое соответствует данному департаменту или гео-расположению. Это сделано для удобства физической локализации места возникновения инцидента. Для этого нажмите на иконке

и выберите соответствующий файл. Для просмотра загруженного изображения нажмите на иконке

 .

4.6.5 Просмотр отчетов в привязке к гео-расположению

В меню «Мониторинг» по каждому гео-расположению можно построить один из преднастроенных отчётов. Для этого откройте паспорт нужного гео-расположения, в нижней части паспорта («Построить отчёт по») выберите отчёт для построения. Далее нажмите на иконку

напротив нужного департамента.

В открывшемся окне задайте параметры отчёта (временной период и частота обновления) и нажмите на кнопку «Готово».

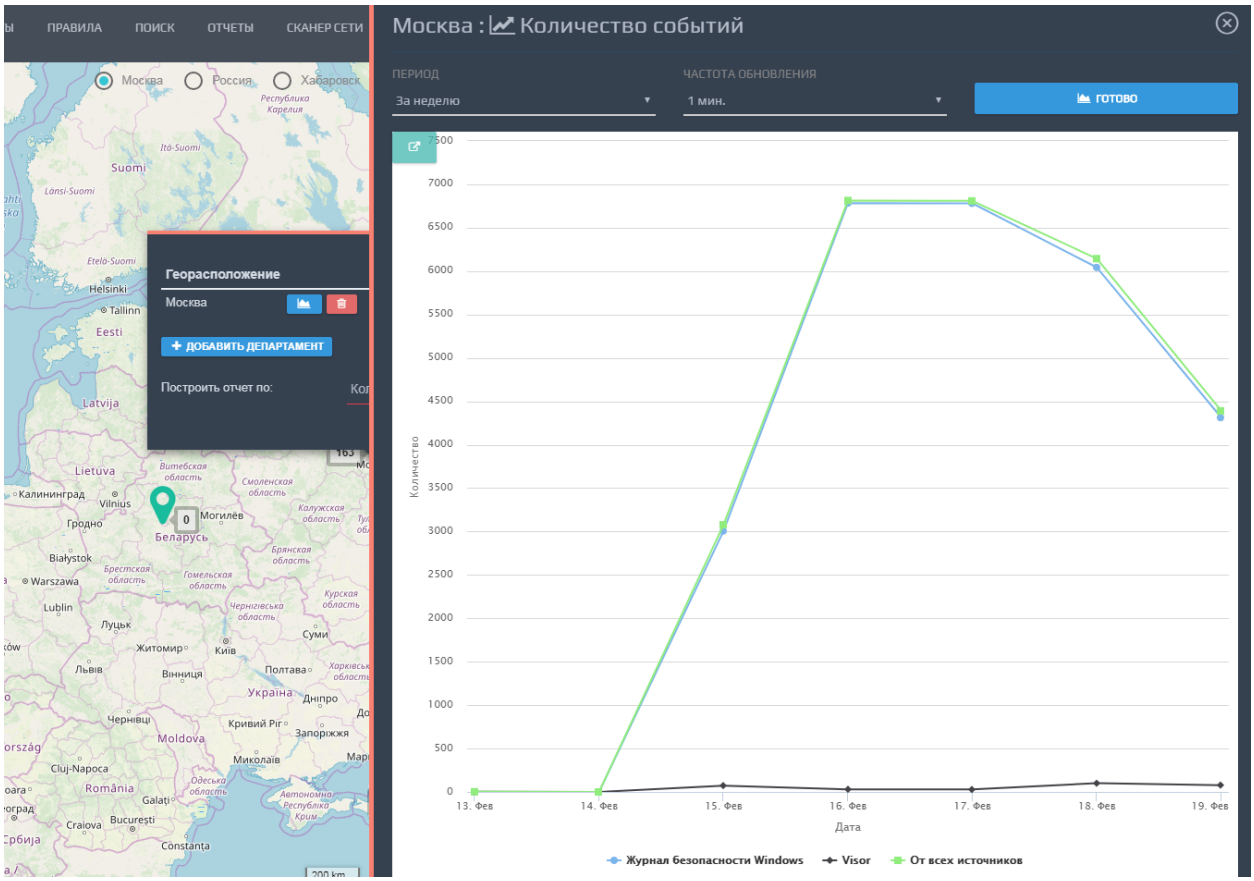


Рисунок 14 – Построение отчёта по гео-расположению

4.7 Меню «Узлы»

Меню «Узлы» отображает перечень сетевых узлов, который представляет собой список защищаемых активов, источников событий ИБ, с установленными или без установленных агентов или агент-коллекторов.

В таблице слева на экране меню «Узлы» отображается перечень узлов, источников, агентов и т.п. В таблице узлов отображается «Гео-расположение», «Подразделение», «Имя узла» «IP-адрес» и «Статус агента» (если агент установлен на узле) для каждого узла в таблице.

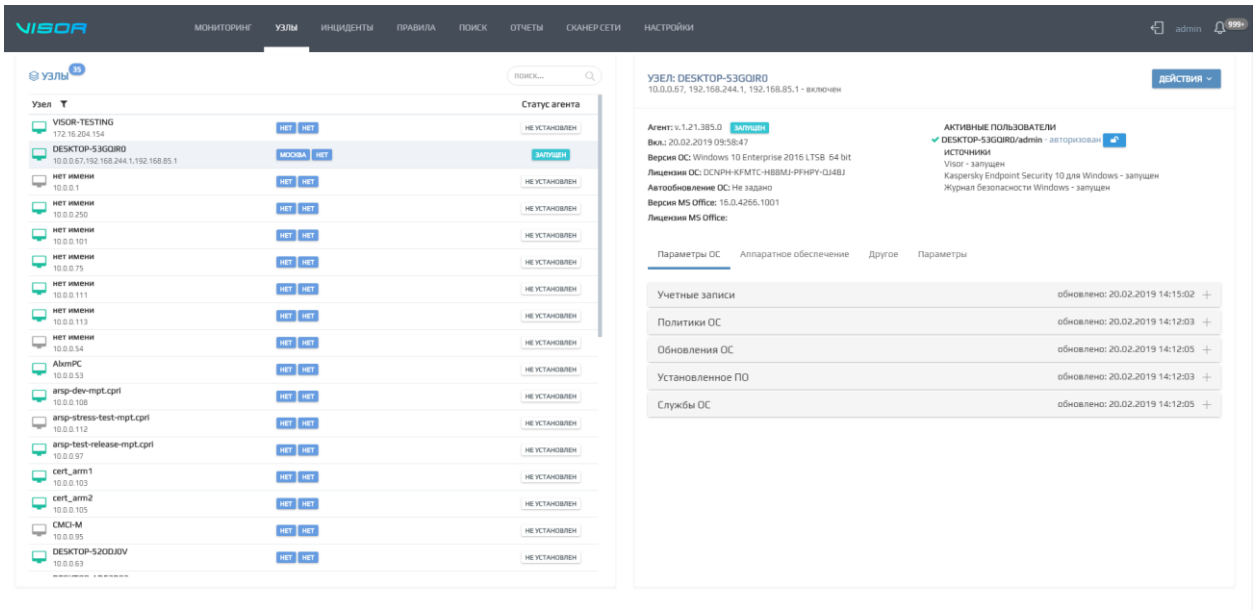


Рисунок 15 – Меню «Узлы»

Для поиска нужного узла по таблице нажмите в поле поиска, расположенного сверху справа над таблицей узлов.

4.7.1 Паспорт узла

Для просмотра информации об узле необходимо выбрать узел в таблице узлов путем нажатия левой клавиши мыши на имени узла.

В правой части экрана отобразится паспорт узла.

Если на защищаемом активе установлен агент или агент-коллектор, то паспорт узла будет содержать следующую информацию:

– «Общие данные»;
– «Параметры ОС»;
– «Аппаратное обеспечение»;
– «Другое»;
– «Параметры».

Если на защищаемом активе не установлен агент или агент-коллектор, то его паспорт будет зависеть от типа узла и источника событий ИБ, расположенных на нём.

4.7.2 Общие данные по узлу

При установленном агенте или агент-коллекторе на защищаемом активе сверху в паспорте узла будут отображаться следующие сведения:

– имя узла;

– IP-адрес узла;

– состояние узла;

– версия установленного агента или агент-коллектора;

– последняя дата включения узла;

– версия ОС;

– лицензия ОС;

– включен ли параметр «Автообновления» для ОС Windows;

– активные пользователи (которые на данный момент работают в ОС Windows на узле). Для каждого пользователя отображается иконка  для немедленной блокировки / разблокировки учетной записи пользователя;

– источники (перечень источников событий ИБ на узле, поддерживаемых агентом или агент-коллектором Visor;

– кнопка «Действия» (позволяет удалять узел из меню «Узлы», устанавливать или удалять агентов на узлы).

4.7.3 Вкладка «Параметра ОС»

На вкладке «Параметры ОС» отображаются дополнительные данные, собранные агентом и агент-коллектором о состоянии ОС. Там представлены следующие сведения по узлу:

– версия ОС;

– лицензия ОС;

– версия Microsoft Office;

– лицензия Microsoft Office;

– учетные записи и их уровень прав;

– политики ОС;

– обновления ОС;

– установленное ПО;

– службы ОС.

4.7.4 Вкладка «Аппаратное обеспечение»

Вкладка «Аппаратное обеспечение» хранит информацию об аппаратном обеспечение узла:

- подключенные USB-устройства класса «Носители данных»;
- процессоры;
- оперативная память;
- жёсткие диски;
- сетевые интерфейсы;
- графические адаптеры;
- параметры BIOS.

4.7.5 Вкладка «Другое»

Вкладка «Другое» отображает информацию об ответственном за узел и другие параметры, которые можно использовать для привязки узла к гео-расположению. Для добавления данных необходимо заполнить все необходимые поля и нажать кнопку «Сохранить». Процедура редактирования аналогична процедуре добавления.

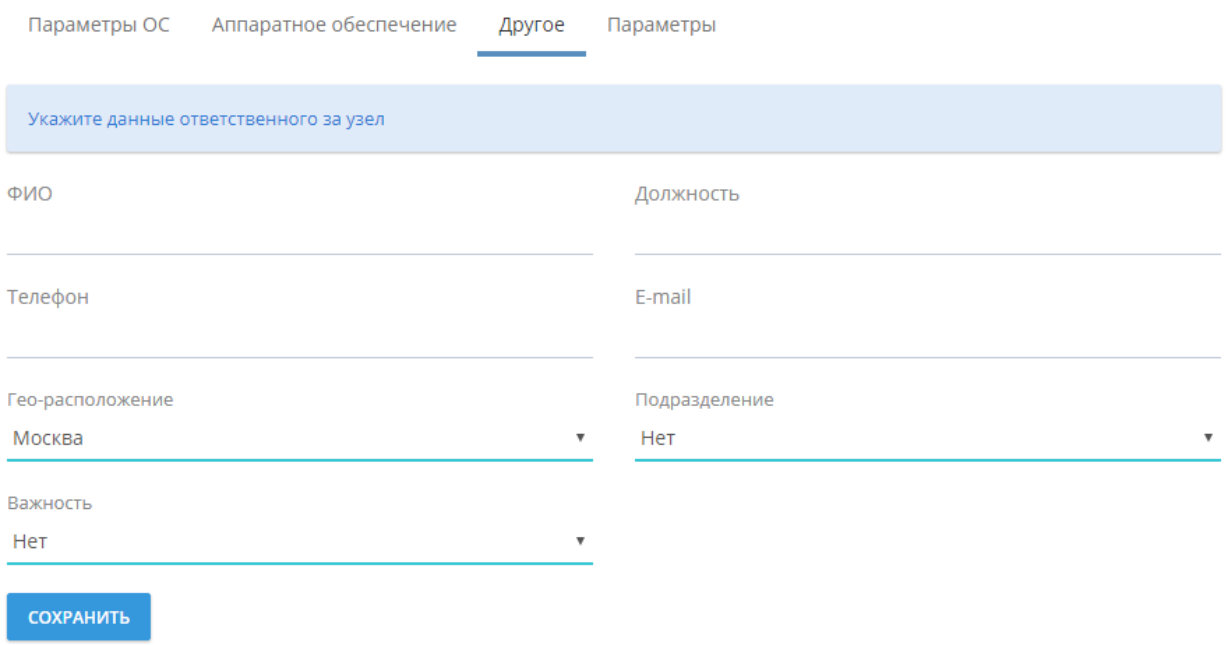


Рисунок 16. Меню «Узлы», вкладка «Другое»

4.7.6 Вкладка «Параметра»

Вкладка «Параметры» позволяет настроить параметры работы агента или агента-коллектора на узле, управлять правилами фильтрации событий источников на данном узле. Для изменения параметров необходимо внести желаемые значения в поля с данными, изменения сразу же будут приняты и отправлены агенту.

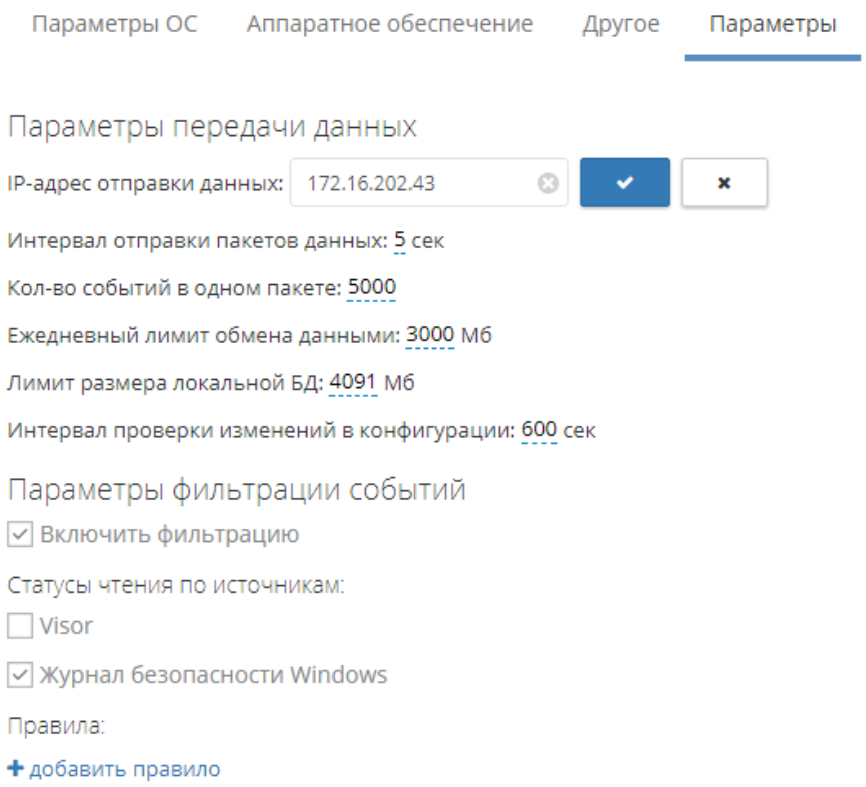


Рисунок 17. Меню «Узлы», вкладка «Параметры»

4.7.7 Наборы узлов

Узлы могут быть сгруппированы в наборы узлов. Наборы узлов предназначены для сортировки узлов по различным признакам. Например, вы можете сгруппировать узлы по их назначению, по департаментам, по гео-расположениям, информационным системам и т.п. Структура наборов узлов имеет древовидное строение и позволяет разграничивать доступ пользователей к каждой ветке дерева.

Сверху над таблицей узлов всегда отображается ветка дерева наборов узлов, содержание которой на данный момент отображается в таблице. Рядом с названием ветки отображается количество узлов в ней.

Для навигации по наборам (веткам) узлов кликните левой кнопкой мыши в название текущей отображаемой ветки над таблицей узлов, выберите нужную и кликните по ней левой кнопкой мыши. В таблице узлов отобразится перечень узлов, входящих в данный набор, ветку.

Для управления наборами (ветками) древовидной структуры кликните правой кнопкой мыши на одной из веток. Чтобы создать внутри данной ветки (набора) дочернюю ветку, кликните «Создать». Чтобы переименовать существующую, кликните «Переименовать». Для удаления набора (ветки), нажмите «Удалить».

4.7.8 Установка агента, агента-коллектора из меню «Узлы»

Если в список узлов был добавлен новый узел из меню «Сканера сети», то на него может быть дистанционно установлен агент или агент-коллектор из меню «Узлы».

Для этого выберите из списка узел, на котором надо установить агента или агент-коллектора, щелкнув на нем левой клавишей мыши. В правой части экрана введите сетевое или доменное имя узла, учетные данные локального администратора и пароль для выбранного узла и нажмите кнопку «Установить агента / агент-коллектора».

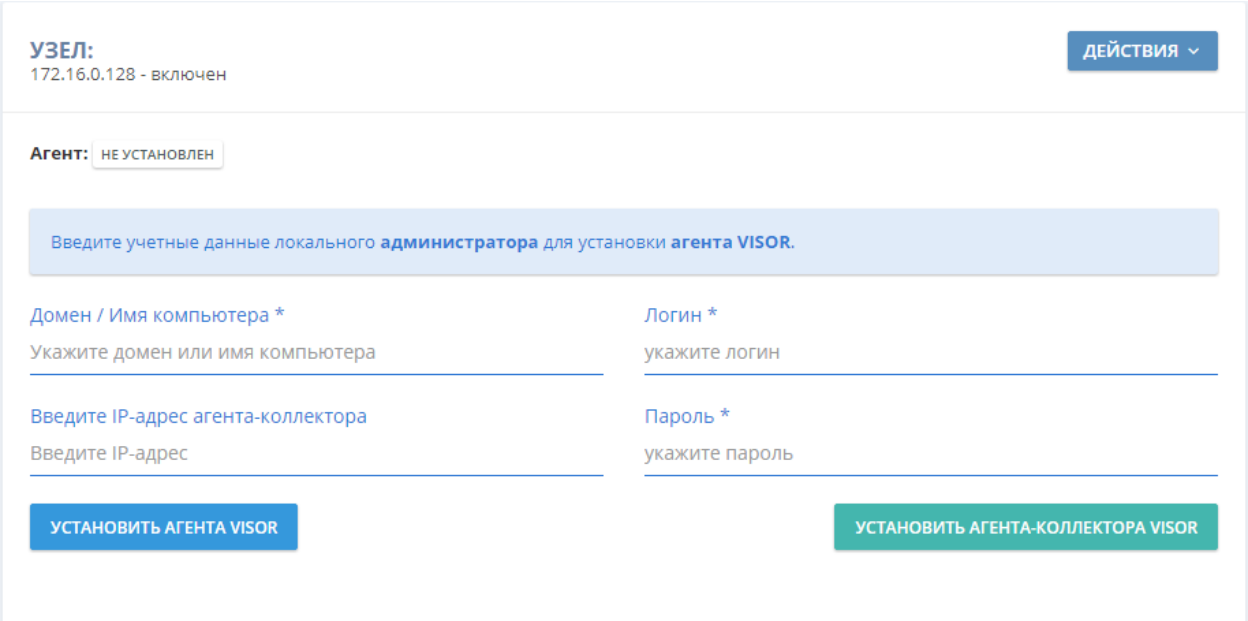


Рисунок 18 - Меню «Узлы», установка агента или агент-коллектора

4.7.9 Удаление агента, агента-коллектора из меню «Узлы»

Выберите из списка узел, щелкнув на нем левой клавишей мыши. В верхней правой части паспорта узла нажмите на кнопку «Действия» -> «Удалить агента».

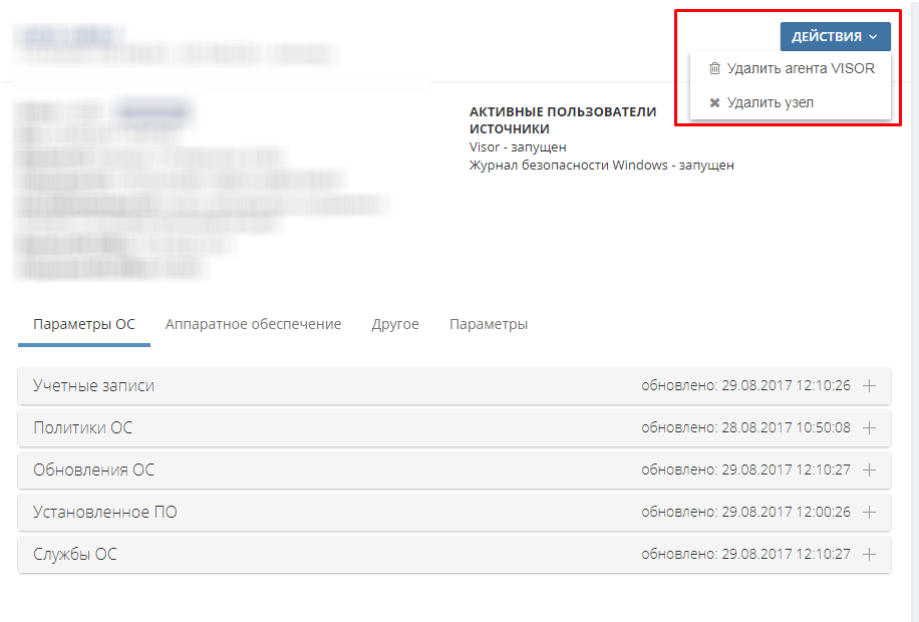


Рисунок 19 - Меню «Узлы», Удаление агента или агент-коллектора

4.7.10 Удаление узла из списка узлов

Выберите из списка узел, щелкнув на нем левой клавишей мыши. В верхней правой части паспорта узла нажмите на кнопку «Действия» -> «Удалить узел». В окне подтверждения нажмите на кнопку «Удалить узел».

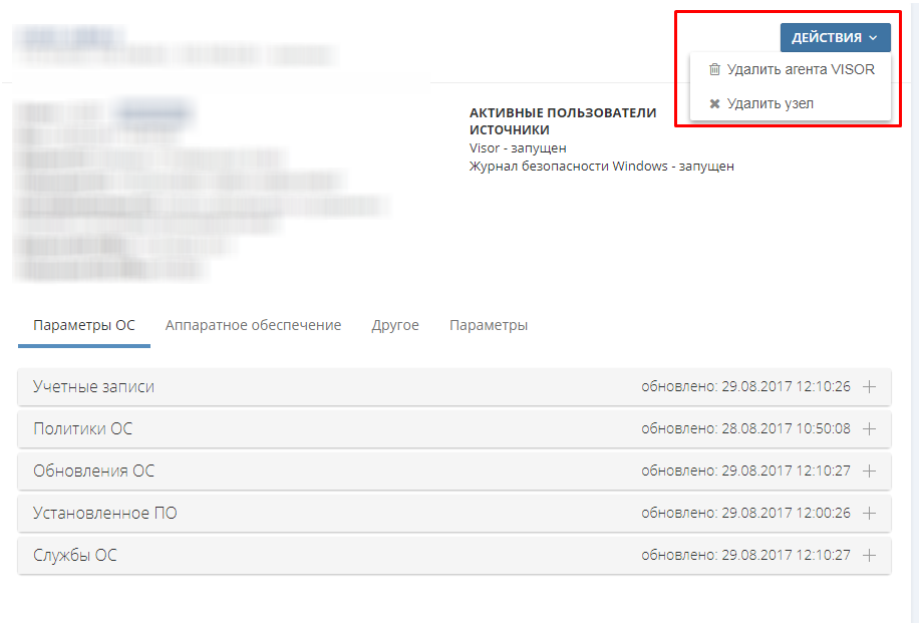


Рисунок 20 - Меню «Узлы», Удаление узла

4.8 Меню «Сканер сети»

Сканер сети позволяет выполнять поиск сетевых узлов, расположенных в одних подсетях с агентами или агент-коллекторами. Для этого в каждый агент или агент-коллектор встроен модуль сканера сети, который позволяет выполнять сканирование сетевого окружения. Сканирование выполняется за счет назначения агентам или агент-коллекторам задач сканирования.

Сканирование сети позволяет выполнять:

– поиск новых узлов для дистанционного распространения на них агентов или агент-коллекторов;

– выявление в подсетях новых, возможно несанкционированных сетевых узлов.

4.8.1 Создание задачи сканирования и добавления нового узла

Для создания задачи сканирования нажмите кнопку «Создать» и укажите параметры задачи:

– название задачи (рекомендовано для удобства в название задачи добавлять сканируемый адрес подсети);

– агент или агент-коллектор, который будет выполнять сканирование доступных ему подсетей (можно использовать фильтр по гео-расположению, чтобы быстро найти необходимый агент или агент-коллектор);

– установите флаг «Начать сканирование сейчас», если хотите, чтобы задача начала выполнять сканирование сразу же после создания; не устанавливайте данный флаг, если у выбранного агента или агент-коллектора имеется несколько сетевых интерфейсов, и вы не хотите выполнять полное сканирование всех доступных им подсетей;

– установите флаг «Находить имена компьютеров для найденных IP-адресов», если хотите, чтобы для всех найденных IP-адресов выполнялось нахождение их DNS-имен;

– установите флаг «Обнаруживать новые сетевые подключения», если хотите, чтобы задача сканирования повторялась циклически сразу же после ее завершения. Циклическое сканирование позволит постоянно выявлять подключение новых узлов в сканируемом сегменте сети.

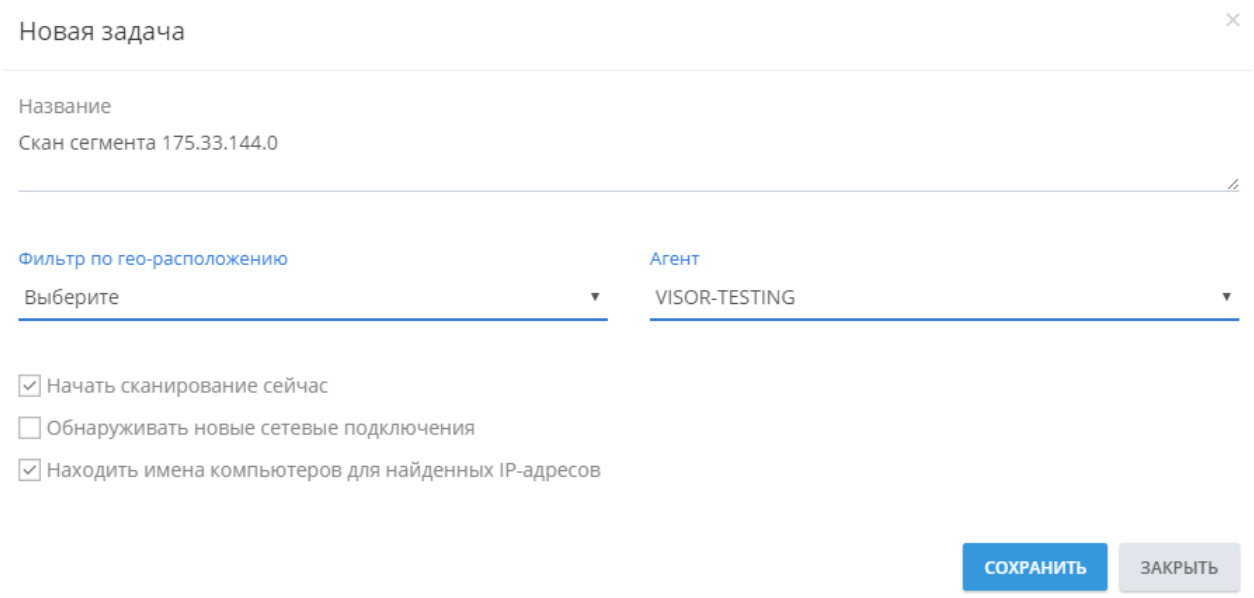


Рисунок 21 - Создание задачи сканирования

Перед запуском задачи сканирования может быть выбран сетевой интерфейс и задан диапазон IP-адресов для проведения сканирования. Для этого откройте паспорт созданной задачи сканирования и нажмите на «IP адреса не указаны. Добавить».

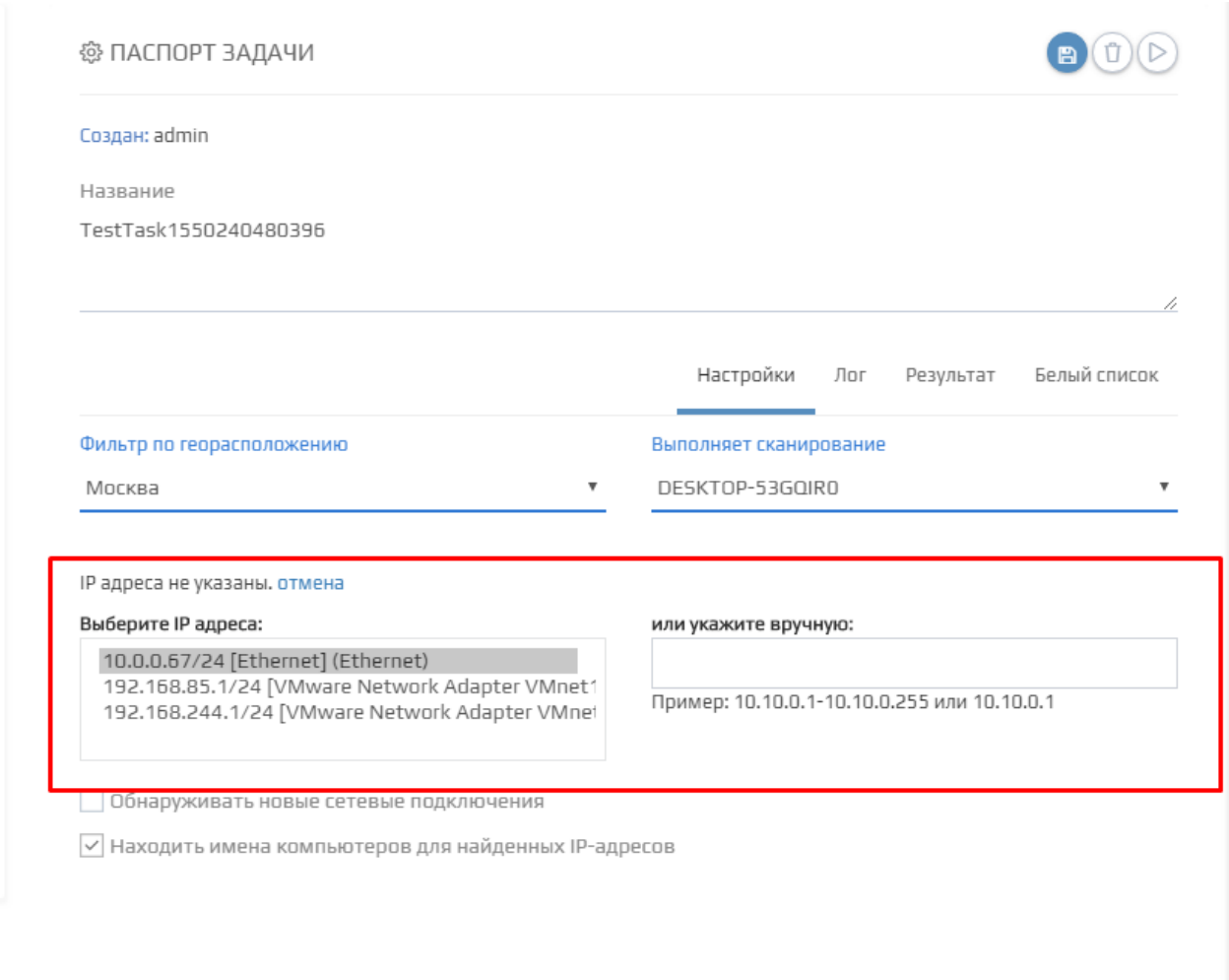


Рисунок 22 – Задание сетевого интерфейса и диапазона сканирования IP-адресов

После запуска задачи вы увидите статус выполнения задачи сканирования в Оповещениях на вкладке Задачи:

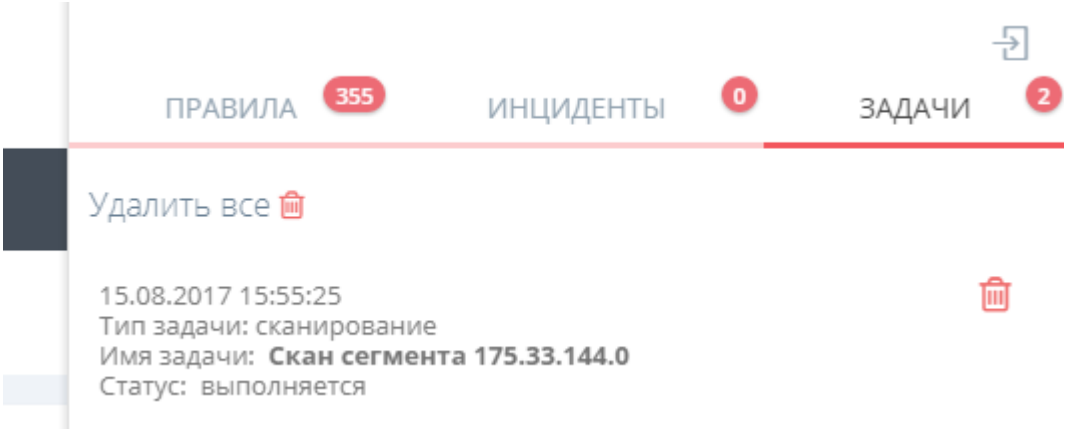


Рисунок 23 - Статус выполнения задачи сканирования

После завершения задачи сканирования, выберите вкладку Результат в паспорте задачи сканирования. В перечне обнаруженных сетевых устройств выберите необходимый актив, на который планируется установить агента или агент-коллектора, после этого нажмите кнопку «Добавить в узлы». Требуемый актив появится в таблице узлов в меню «Узлы».

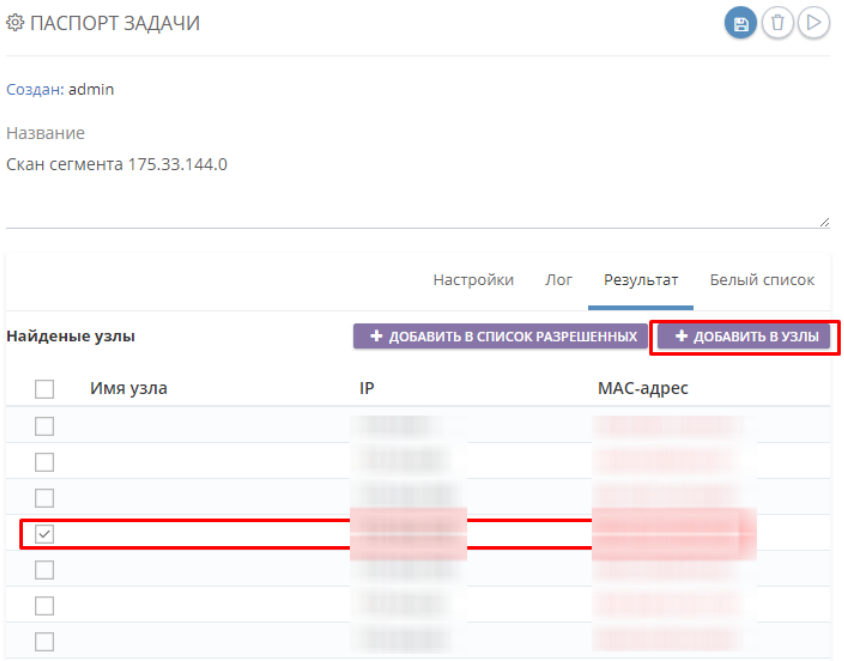


Рисунок 24 - Добавление найденного актива в меню «Узлы»

В результате в меню «Узлы» появится новый узел, для которого будет доступно выполнение дистанционной установки агента или агент-коллектора.

4.9 Меню «Поиск»

Меню «Поиск» является одним из основных инструментов при мониторинге событий ИБ.

Меню «Поиск» позволяет пользователям:

– выполнять поисковые запросы к БД Visor для отображения хранимых в ней событий;

– применять различные фильтры для поиска событий (по времени, по источнику, по узлу и т.п.);

– сохранять и обмениваться Visor поисковыми запросами в виде ссылок;

– просматривать каждое событие в нормализованном виде (в виде значений нормализованных полей).

4.9.1 Контекстный поиск

Для выполнения контекстного поиска в строке поиска введите искомые данные и нажмите кнопку «Найти». По завершению поиска вы увидите результаты поисковой выдачи, соответствующие вашему запросу. Контекстный поиск выполняет поиск введенного значения в каждом поле нормализации каждого события в БД сервера Visor поэтому выдача результата может потребовать некоторого времени.

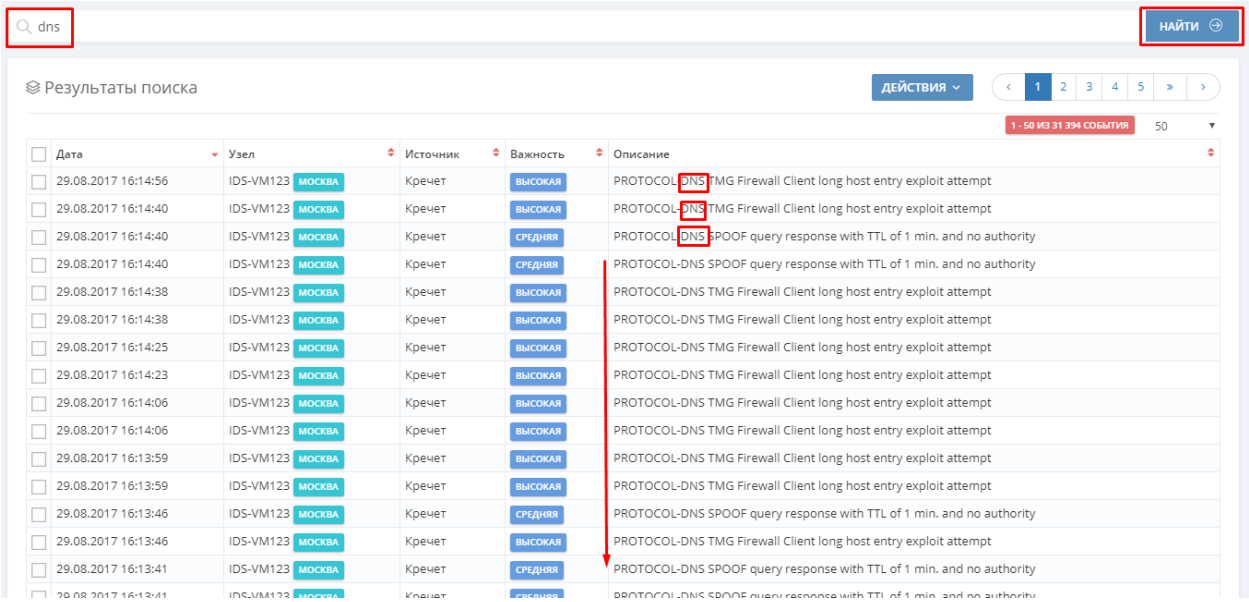


Рисунок 25 - Меню «Поиск», результат поисковой выдачи при контекстном

4.9.2 Фильтрация поиска событий

В дополнение к контекстному поиску доступна фильтрация поисковой выдачи на основе фильтров, отображаемых слева в меню «Поиск».

Фильтрация данных доступна по:

– дате и времени происхождения события (не по дате и времени его записи в БД);

– имени узла;

– гео–расположению узла;

– источнику события;

– категории события;

– важности события;

– подключенному архиву для поиска.

Задав значение для одного из фильтров, возможные значения для остальных фильтров автоматически подстраиваются под выбранное значение.

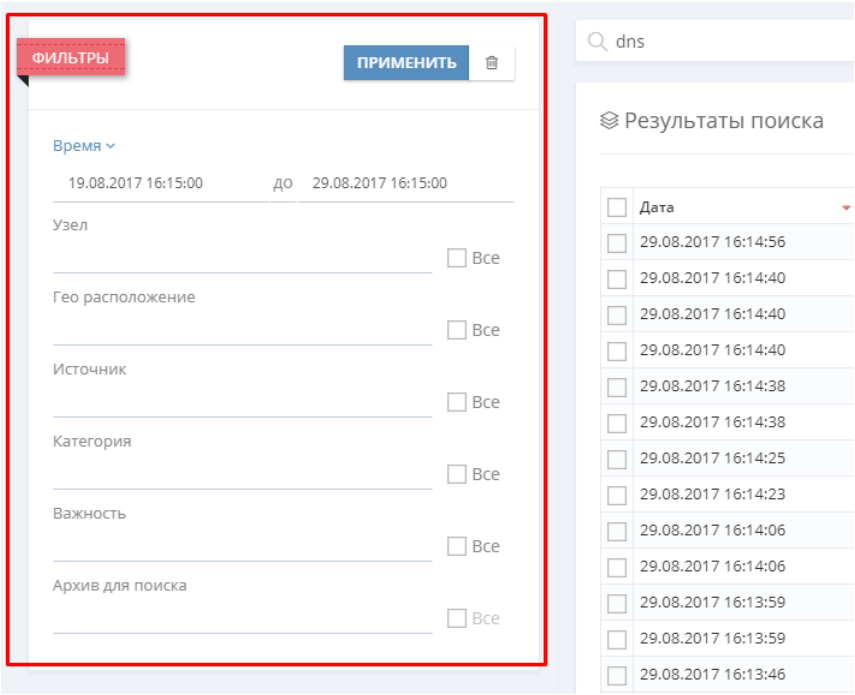


Рисунок 26 - Меню «Поиск», доступные поисковые фильтры

Значения фильтров можно вводить как вручную, так и выбирать из выпадающего списка доступных значений.

4.9.3 Просмотр полей нормализации

В поисковой выдаче по событиям отображаются следующие данные:

– дата и время происхождения события (не дате и время выполнения его записи в БД Visor);

– имя узла, на котором произошло событие;

– гео–расположению узла;

– источник события;

– важность события;

– описание события (в кратком виде).

Для просмотра конкретного события в нормализованном виде выберите в поисковой выдаче необходимое событие и нажмите на его содержимое в столбце «Описание».

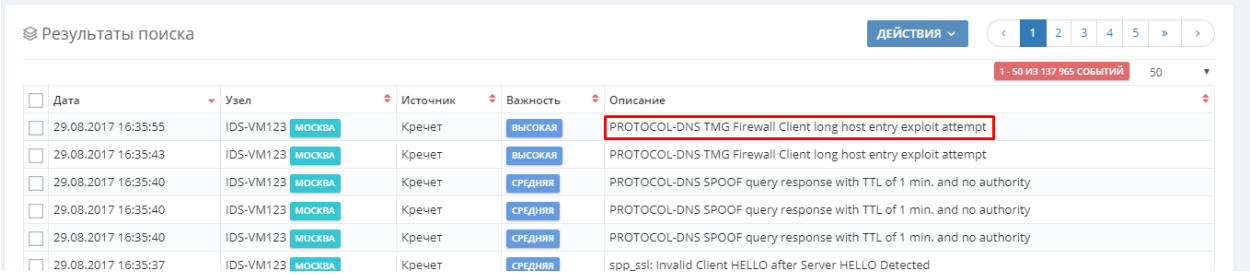
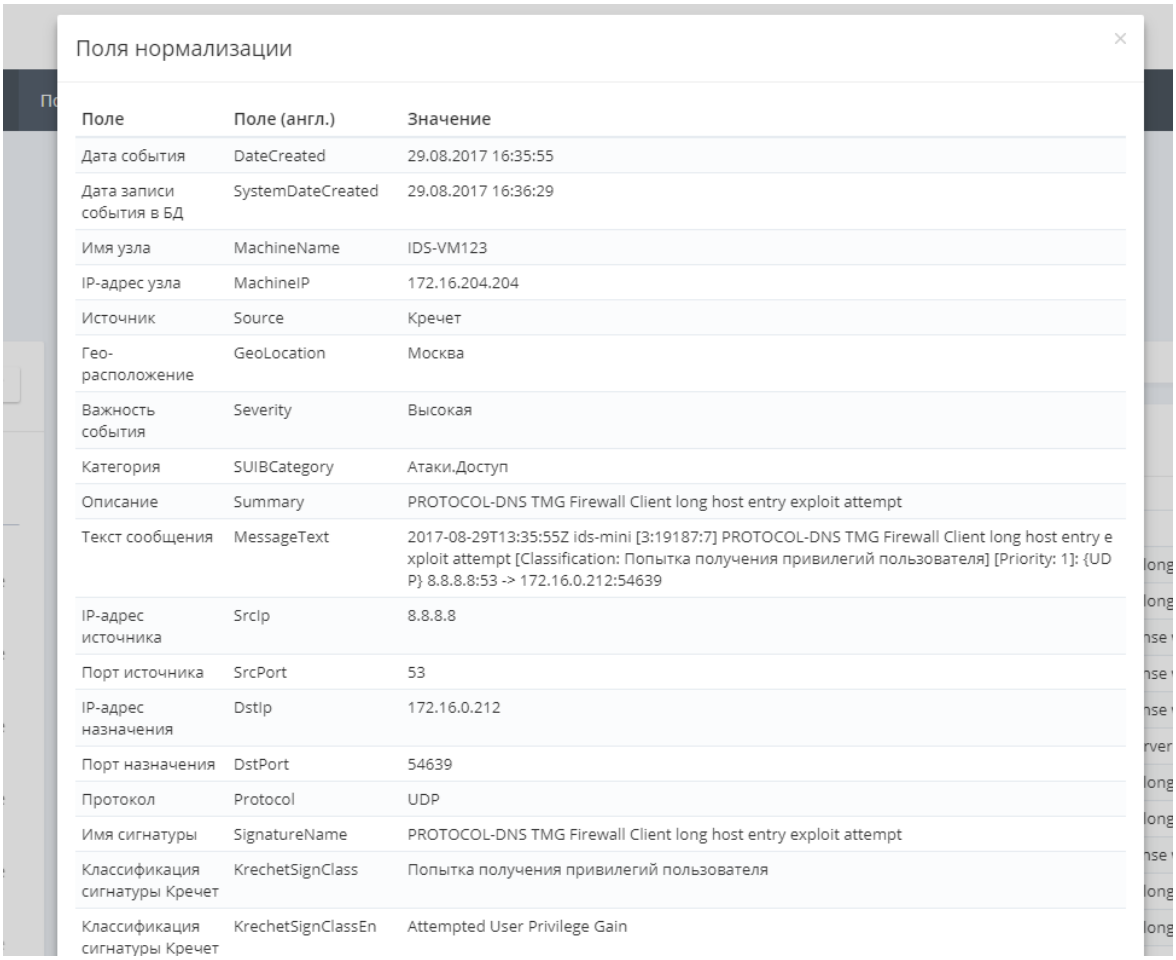


Рисунок 27 - Меню «Поиск», клик по описанию события в поисковой выдаче

После этого откроется форма «поля нормализации» для данного события. В данной форме отображаются все значения полей нормализации для данного конкретного события.



Поля нормализации

Поле	Поле (англ.)	Значение
Дата события	DateCreated	29.08.2017 16:35:55
Дата записи события в БД	SystemDateCreated	29.08.2017 16:36:29
Имя узла	MachineName	IDS-VM123
IP-адрес узла	MachineIP	172.16.204.204
Источник	Source	Кречет
Гео-расположение	GeoLocation	Москва
Важность события	Severity	Высокая
Категория	SUIBCategory	Атаки.Доступ
Описание	Summary	PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt
Текст сообщения	MessageText	2017-08-29T13:35:55Z ids-mini [3:19187:7] PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt [Classification: Попытка получения привилегий пользователя] [Priority: 1]: {UDP} 8.8.8.8:53 -> 172.16.0.212:54639
IP-адрес источника	SrcIp	8.8.8.8
Порт источника	SrcPort	53
IP-адрес назначения	DstIp	172.16.0.212
Порт назначения	DstPort	54639
Протокол	Protocol	UDP
Имя сигнатуры	SignatureName	PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt
Классификация сигнатуры Кречет	KrechetSignClass	Попытка получения привилегий пользователя
Классификация сигнатуры Кречет	KrechetSignClassEn	Attempted User Privilege Gain

Рисунок 28 - Меню «Поиск», поля нормализации для события

4.9.4 Привязка событий к инцидентам ИБ

Если в результате поиска было обнаружено, что найденное событие или события могут иметь отношение к существующему инциденту, они могут быть привязаны к паспорту инцидента. После привязки, выбранные события будут отображаться в паспорте инцидента на вкладке «События».

Для этого установите флаг рядом с необходимыми событиями и нажмите кнопку «Связать с инцидентом».

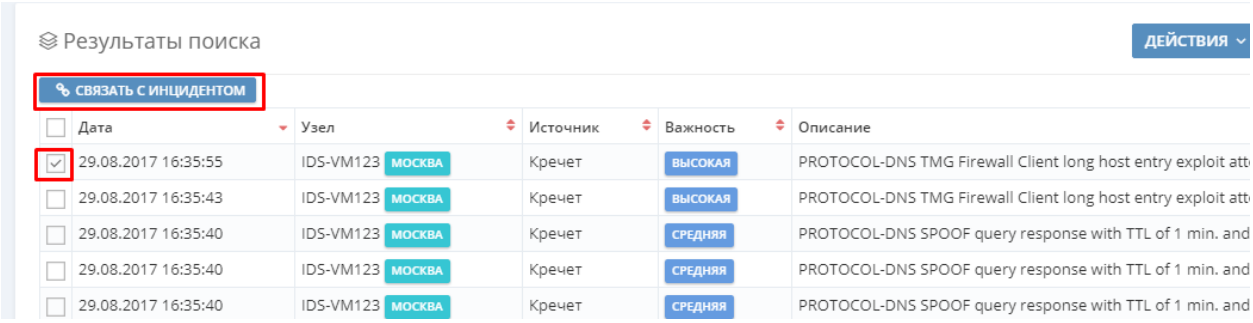


Рисунок 29 - Меню «Поиск», привязка события к инциденту (1)

Откроется окно «Привязка к инциденту». Выберите из раскрывающегося списка инцидент, к которому требуется привязать событий, далее нажмите кнопку «Привязать». Для отмены нажмите кнопку «Закрыть».

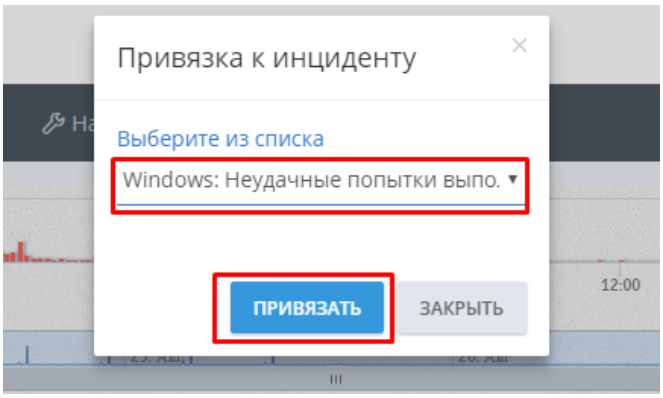


Рисунок 30 - Меню «Поиск», привязка события к инциденту (2)

4.9.5 Управление поисковыми запросами

Пользователи могут сохранять, удалять и обмениваться комбинациями поисковых запросов и фильтров. Эта возможность полезна при совместном мониторинге событий группой операторов или при выполнении часто повторяющихся задач мониторинга.

Для сохранения запроса после ввода запроса нажмите на кнопку «Действие». Из раскрывающегося списка выберите «Сохранить запрос».

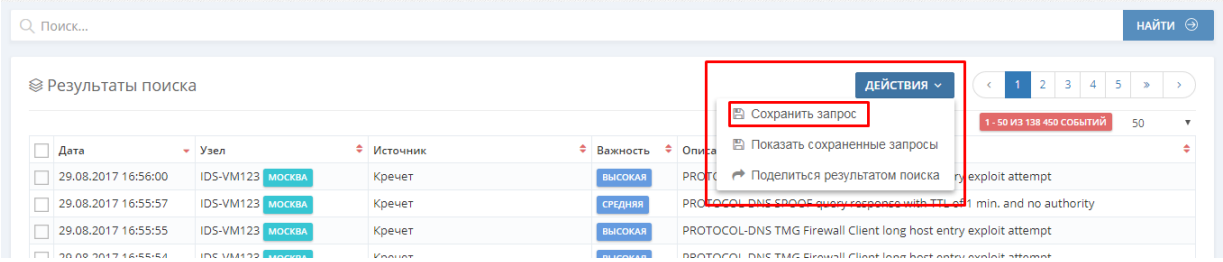


Рисунок 31 - Меню «Поиск», сохранение поисковых запросов (1)

Откроется окно «Запросы». Заполните поле «Название» и нажмите кнопку «Сохранить». Для отмены сохранения нажмите кнопку «Закрыть».

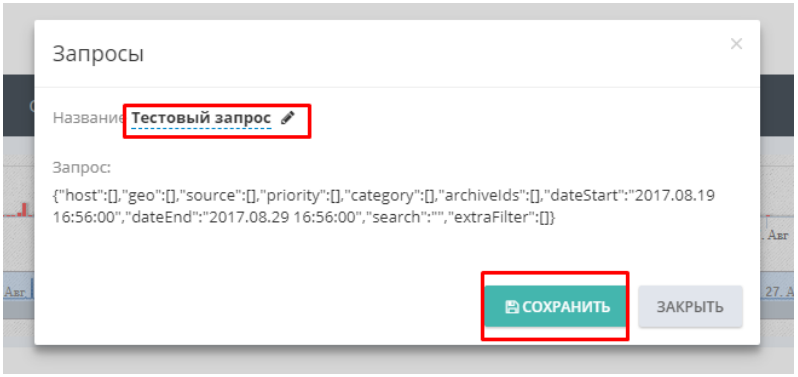


Рисунок 32 - Меню «Поиск», сохранение поисковых запросов (2)

Для просмотра сохраненных ранее поисковых запросов нажмите на кнопку «Действие». Из раскрывающегося списка выберите «Показать сохраненные запросы». Откроется окно «Ваши сохраненные запросы».

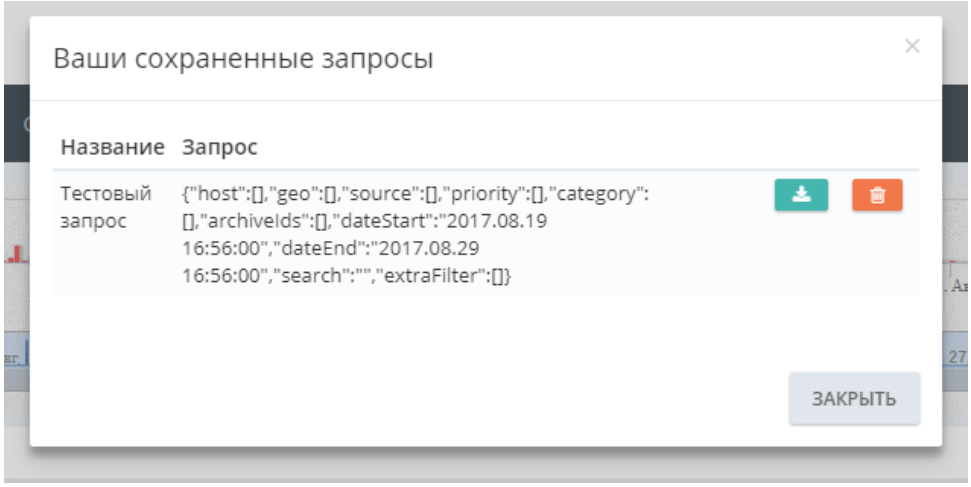


Рисунок 33 - Меню «Поиск», просмотр ранее сохраненных запросов

Для осуществления повторного поиска сохраненного запроса, выберите из списка запрос и нажмите кнопку

 .

Для удаления ранее сохраненных запросов. Выберите из списка запрос и нажмите кнопку

 .

Для копирования ссылки на результат текущего запроса нажмите кнопку «Действие». Из раскрывающегося списка выберите «Поделиться результатом поиска».

4.10 Меню «Отчеты»

Меню «Отчеты» позволяет оператору формировать отчеты по предустановленным шаблонам.

Для формирования отчета выберите тип необходимо отчета в выпадающем списке доступных предустановленных шаблонов:

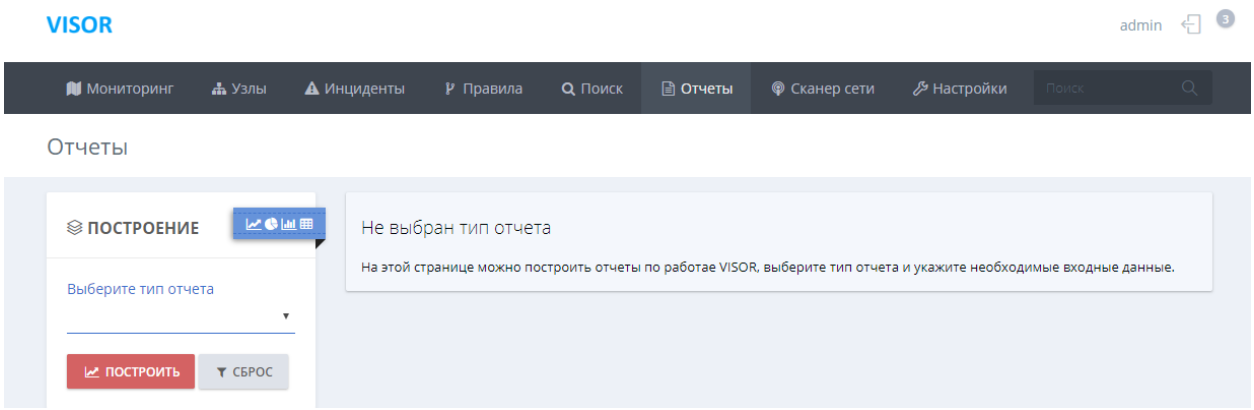


Рисунок 34 - Меню «Отчеты», выбор предустановленного шаблона отчета

После выбора шаблона отчета задайте доступные параметры для построения отчета. После этого нажмите на кнопку «Построить».

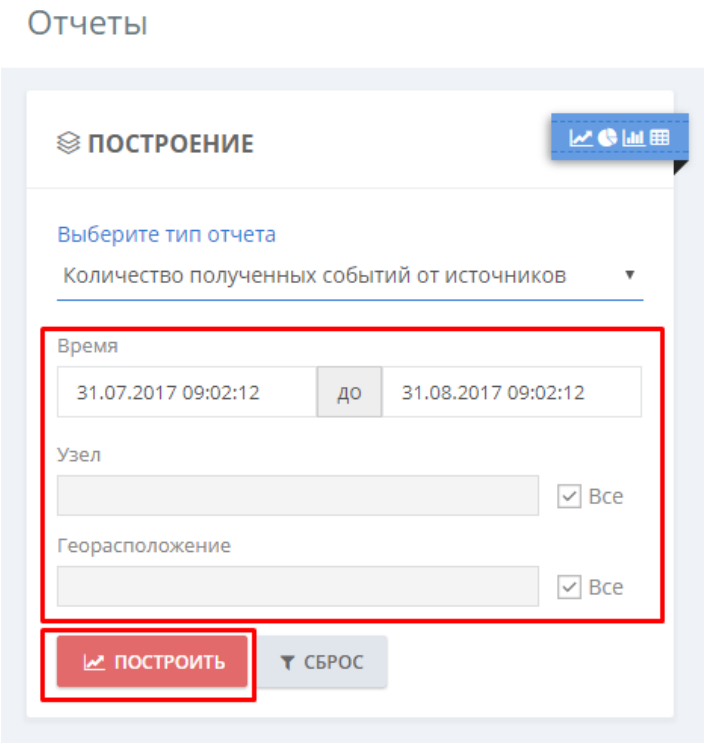


Рисунок 35 - Меню «Отчеты», задание параметров для построения шаблонов отчета

После этого справа от параметров отобразится результат построения отчета.

Рисунок 36 - Меню «Отчеты», отображение построенного отчета

Некоторые отчеты интерактивны и предоставляют возможность кликнуть на изображение точек графика для перехода в другие меню веб-интерфейса для просмотра детальной информации.

4.11 Меню «Архив»

Меню «Архив» позволяет оператору выполнять следующие задачи:

– переносить, вручную или автоматизировано, с определенным периодом времени, во внешние архивные файлы устаревшие события и закрытые инциденты ИБ из основной БД Visor;

– подключать внешние архивные файлы к основной БД Visor для проведения расследований по историческим событиям и инцидентам ИБ в архиве.

Созданные архивные файлы выводятся в виде таблицы. С каждым архивным файлом связана кнопка для его подключения или отключения от БД Visor.

Важно учитывать, что если у подлежащего архивации инцидента ИБ статус отличается от статуса «Закрыт», то данный инцидент и привязанные к нему события не будут помещены в архив.

4.11.1 Выполнение задач архивирования

Для выполнения задач архивирования необходимо перейти в меню «Настройки» -> «Архив».

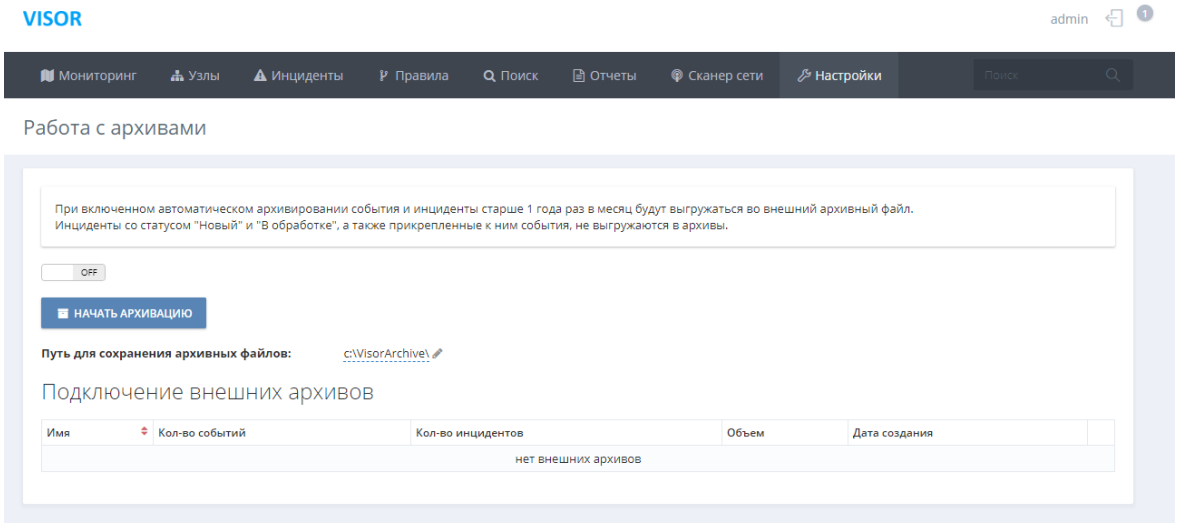


Рисунок 37 - Меню «Архив»

Для включения автоматического архивирования необходимо во вкладке «Архив» установить значение автоматического архивирования в статус «On». Для отключения – в статус «Off.

Учитывайте, что при включении автоматического архивирования операция архивирования будет сразу же запущена.

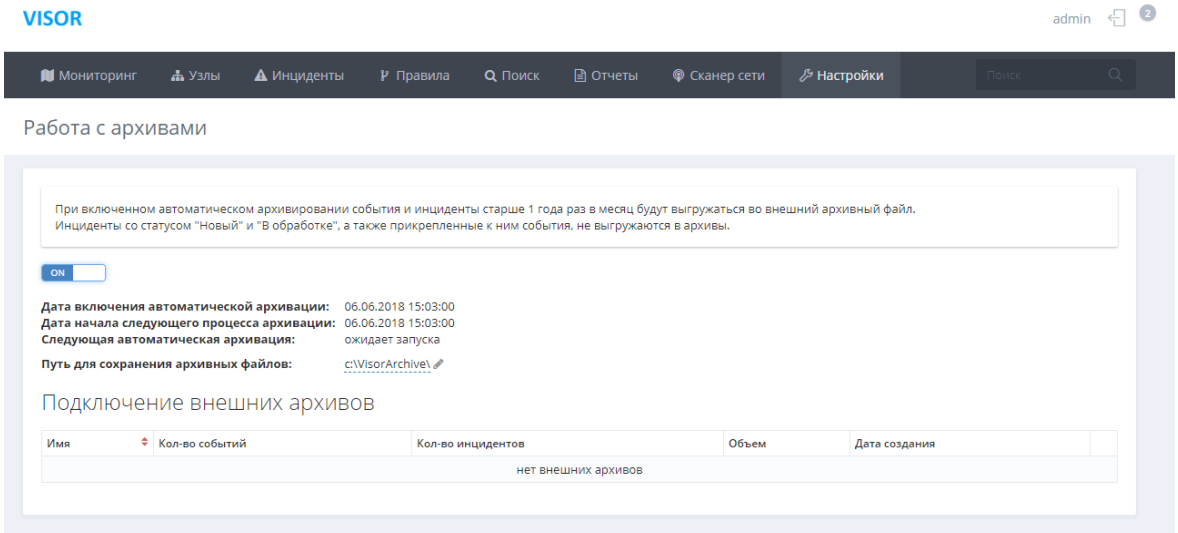


Рисунок 38 - Включение/выключение автоматического архивирования

После этого архив будет автоматически раз в месяц создавать архивные файлы. Все созданные архивные файлы будут отображаться ниже в таблице «Подключение внешних архивов».

Для выполнения задачи архивирования вручную необходимо выключить автоматическую архивацию и нажать на кнопку «Начать». В появившемся окне «Архивация» указать временной период для архивации.

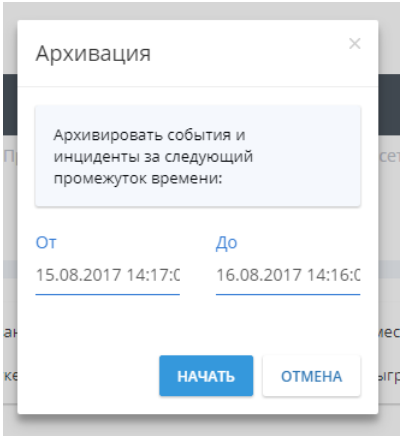


Рисунок 39 - Окно «Архивация» для выполнения ручной архивации

После запуска задачи архивирования как в ручном, так и в автоматическом режиме в правом меню «Оповещения» веб-интерфейса во вкладке «Задачи» появится отображение статуса выполнения текущей задачи архивирования.

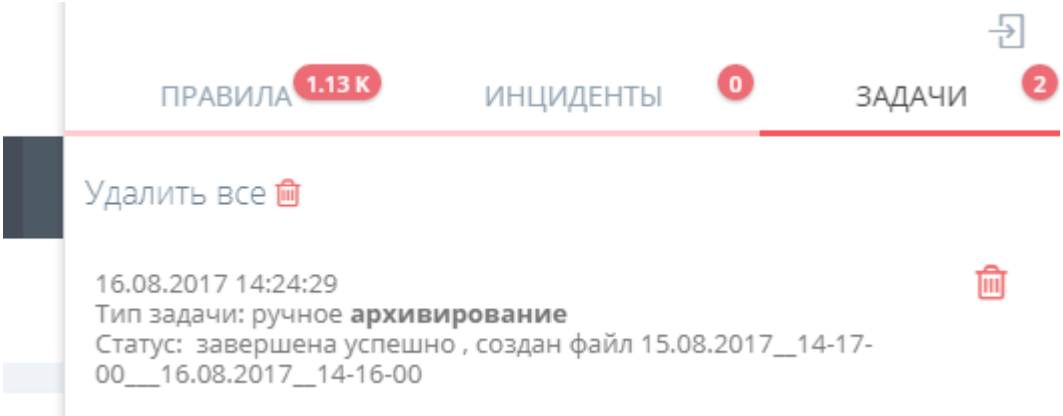


Рисунок 40 - Оповещение о статусе выполнения задачи архивирования

Также во время выполнения задачи архивирования в меню «Архив» появится статус отображения выполнения задачи архивирования.

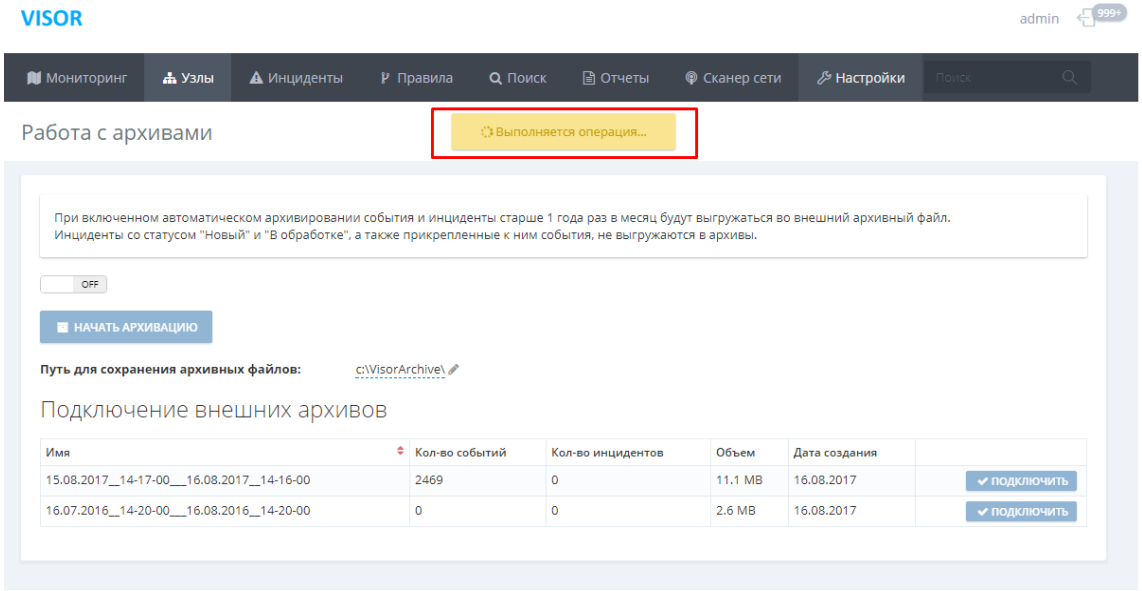


Рисунок 41 - Статус выполнения задачи архивирования в меню «Архив»

4.11.2 Задание пути для сохранения файла архива

В меню «Архив» есть возможность указать путь для сохранения архивных файлов. По умолчанию при установке сервера задается следующий путь для сохранения архивных файлов: «C:\Archive\». Для его изменения необходимо нажать кнопку «Изменить», ввести новый путь и нажать кнопку «Enter».

4.11.3 Поиск данных из архивных файлов

Для того, чтобы выполнить просмотр данных из архивного файла необходимо выполнить подключение архивных файлов к текущей БД. Для этого необходимо нажать кнопку «Подключить» в строке соответствующего архивного файла. Для отключения архивного файла от основной БД необходимо нажать кнопку «Отключить».

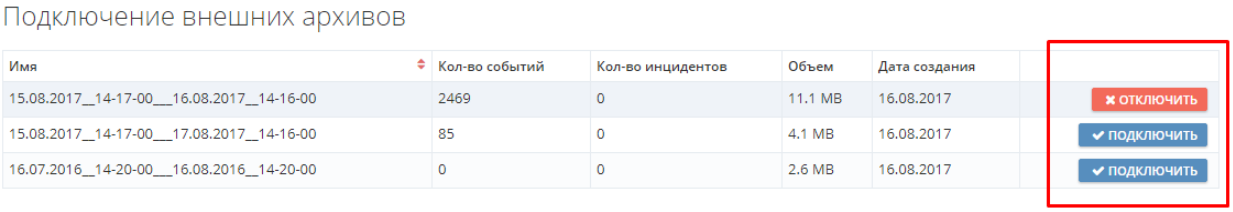


Рисунок 42 - Подключение/Отключение архивных файлов

Для того, чтобы начать поиск по события из архивного файла необходимо после его подключения перейти в меню «Поиск» и в фильтре «Архив для поиска» выбрать соответствующий подключенный архив. После этого можно начинать поиск по временному диапазону архивного файла.

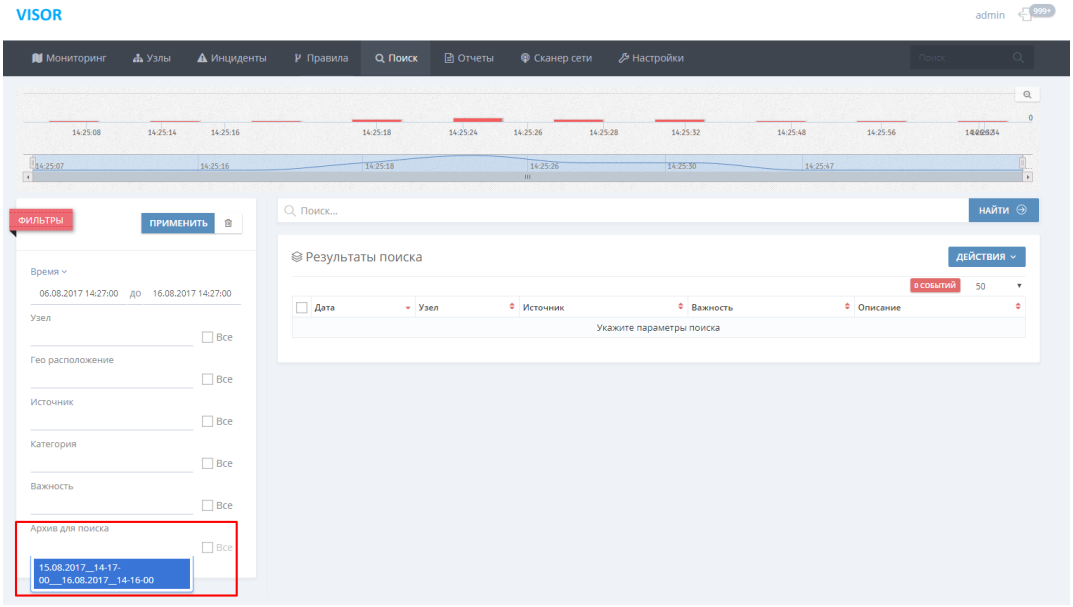


Рисунок 43 - Выбор подключенного архивного файла в меню «Поиск»

После завершения работы в меню «Поиск» с архивным файлом его необходимо отключить в меню «Архив».

Если в архивном файле хранились инциденты ИБ, то соответствующие инциденты будут отображены в меню «Инциденты» веб-интерфейса.

4.12 Управление правилами фильтрации событий

Одной из основных функций оператора-аналитика является определение логических условий, запрещающих выполнение сбора определенных событий от источников.

В процессе мониторинга событий и инцидентов оператор может обнаружить, что некоторые типы событий будут повторяться большое количество раз за короткие промежутки времени (например, 100 одинаковых событий в течение 5-ти секунд). Если данные события, по экспертной оценке оператора-аналитика, не несут информационного смысла для процесса выявления угроз безопасности информации и не будут полезны в будущем при расследовании инцидентов ИБ, то Visor предоставляет функционал для запрета сбора и корреляции таких событий.

Иначе подобные события будут заполнять свободное дисковое пространство в БД сервера и накладывать дополнительную нагрузку при передаче данных (трафика) на ЛВС организации.

Оператору следует всегда с осторожностью настраивать фильтрацию событий ИБ, поскольку определенные типы событий могут быть полезны в будущем при глубинном расследовании и доказательстве различных обстоятельств инцидентов ИБ.

Оператору рекомендуется выполнять периодический пересмотр существующих правил фильтрации событий ИБ при подключении новых источников или изменении модели угроз и нарушителей ИБ.

Фильтрация событий может быть настроена как для всех типов событий.

Visor выполняет аудит любых изменений, внесенных пользователями в правила фильтрации событий ИБ.

4.12.1 Настройка правил фильтрации событий на агенте или агенте-коллекторе

Выполните вход в меню «Узлы», выберите защищаемый актив, для которого необходимо настроить фильтрацию событий, и в его паспорте (справа) перейдите на вкладку «Параметры».

Выберите «Включить фильтрацию»:

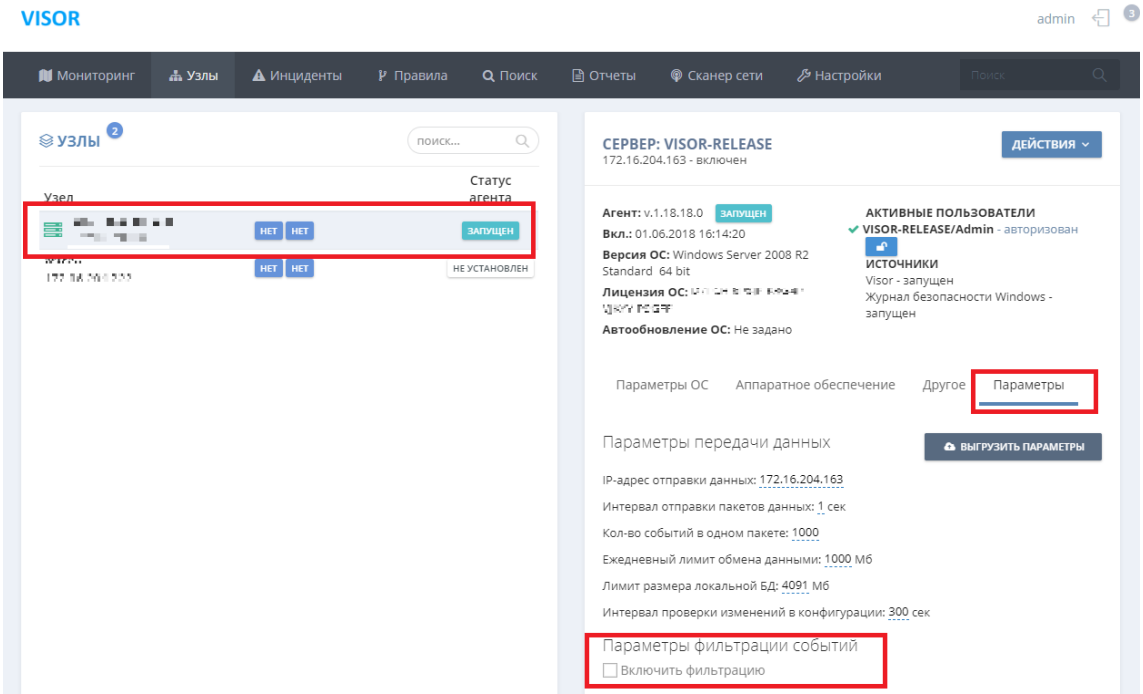


Рисунок 44 - Включение фильтрации на агенте или агент-коллекторе Visor

Для полного отключения сбора событий из определенного источника уберите галочку напротив соответствующего источника, отображаемых в «Статусы чтения по источникам»:

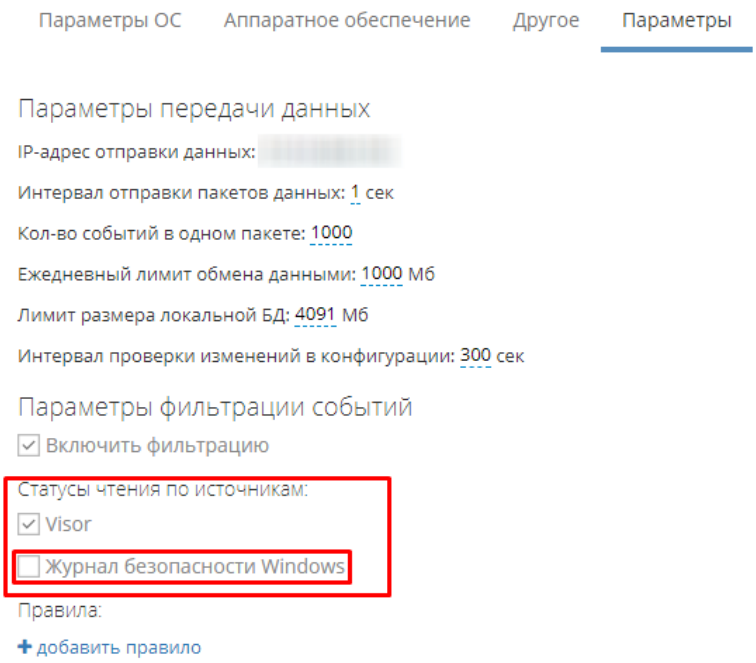


Рисунок 45 - Отключение сбора событий источника

После отключения галочки управляющий сервер выполнит моментальную отправку новых условий фильтрации агенту или агент-коллектору.

Для фильтрации конкретных событий необходимо создать соответствующее правило фильтрации, для этого нажмите на «+ добавить правило»:

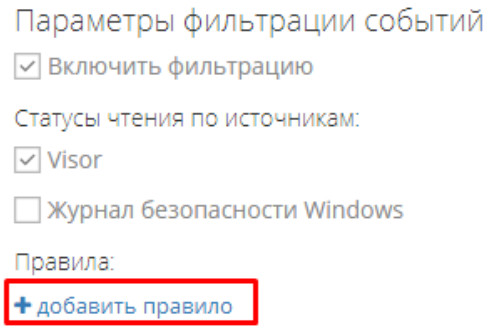


Рисунок 46 - Добавление правила фильтрации (1)

После этого необходимо ввести имя и код правила:

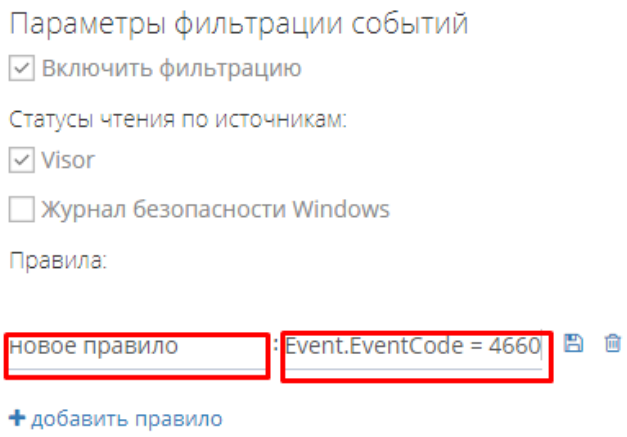


Рисунок 47 - Задание имени и кода для правила фильтрации событий

Для задания условий фильтрации в коде правила используется стандартный язык логических условий (AND, OR, =, >, <, скобки и т.п.) и названия полей нормализации событий на английском языке.

В приведенном выше примере правило фильтрации запрещает выполнять сбор событий, у которых поле нормализации «EventCode» имеет значение 4660.

Следует учитывать, что при добавлении нескольких правил фильтрации с помощью кнопки «+ Добавить правило» между ними будет применяться логическое ИЛИ (OR).

В начале каждого правила необходимо писать слово «Event», затем через точку добавлять английское название поля нормализации «Event.<поле нормализации>».

Между полем нормализации, логическим оператором и значением обязательно всегда ставить пробелы иначе правило будет невозможно сохранить из-за нарушения синтаксиса.

Необходимые названия и значения полей нормализации для событий, претендующих на фильтрацию, могут быть найдены в процессе выполнения анализа событий в меню «Поиск»:

Поля нормализации

Поле	Поле (англ.)	Значение
Дата события	DateCreated	
Дата записи события в БД	SystemDateCreated	
Имя узла	MachineName	
IP-адрес узла	MachineIP	
Источник	Source	Visor
Гео-расположение	GeoLocation	Москва
Важность события	Severity	Низкая
Категория	SUIBCategory	Пользователь.Активность.Вход.Успешно
Описание	Summary	Пользователь 'admin' вошел в систему
Текст сообщения	MessageText	Пользователь 'admin' вошел в систему
АРМ, Сервер	Host	
Объект	Object	

Показать пустые поля

ЗАКРЫТЬ

Рисунок 48 - Поля нормализации событий, отображаемые в меню «Поиск»

Ниже в разделе «Примеры правил фильтрации событий ИБ» описаны дополнительные полезные примеры написания правил фильтрации.

4.12.2 Примеры правил фильтрации событий

Примеры фильтрации событий на агенте (агенте-коллекторе):

Пример №1: «Event.Source = vipnet AND Event.EventCode = 123» - правило запрещает сбор событий от источника vipnet, у которых поле нормализации «EventCode» имеет значение «123».

Пример №2: «Event.MessageText LIKE 'error 14432'» - правило запрещает сбор событий, у которых в поле нормализации «MessageText» встречается текст совпадающим с «error 14432».

4.12.3 Внутренний аудит правил фильтрации событий

Visor выполняет аудит любых изменений, внесенных пользователями в правила фильтрации событий. При этом в меню «Поиск» для агента или агента-коллектора, на котором были внесены изменения в правила фильтрации, регистрируется событие с описанием «Изменены настройки агента»:

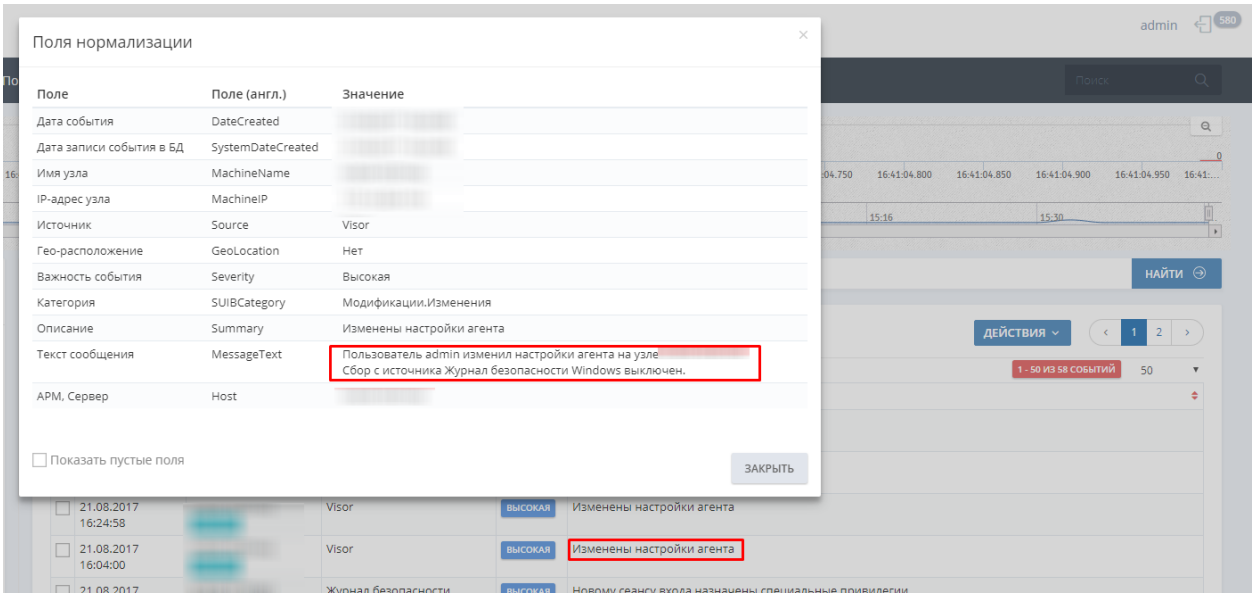


Рисунок 49 - Регистрация события аудита об изменении правил фильтрации на агенте, агенте-коллекторе

Для выявления данных действий в меню «Правила» правило корреляции «Visor: Изменены настройки агента». Данное правило срабатывает при изменении настроек конфигурационного файла и правил фильтрации агента или агент-коллектора.

4.13 Управление правилами корреляции событий

Одной из основных функций оператора является определение логических условий, при которых вероятна компрометация защищаемых активов и реализация угроз безопасности информации, применительно к имеющимся в организации источникам событий ИБ и защищаемым активам.

Каждое собранное событие от каждого источника направляется в модуль аналитики Visor. Модуль аналитики пропускает каждое поступающее ему событие через каждое правило корреляции.

Меню «Правила» предназначено для управления правилами корреляции.

Все правила корреляции в меню «Правила» выводятся в виде таблицы слева. Доступно поле поиска, позволяющее фильтровать правила по ключевым словам.

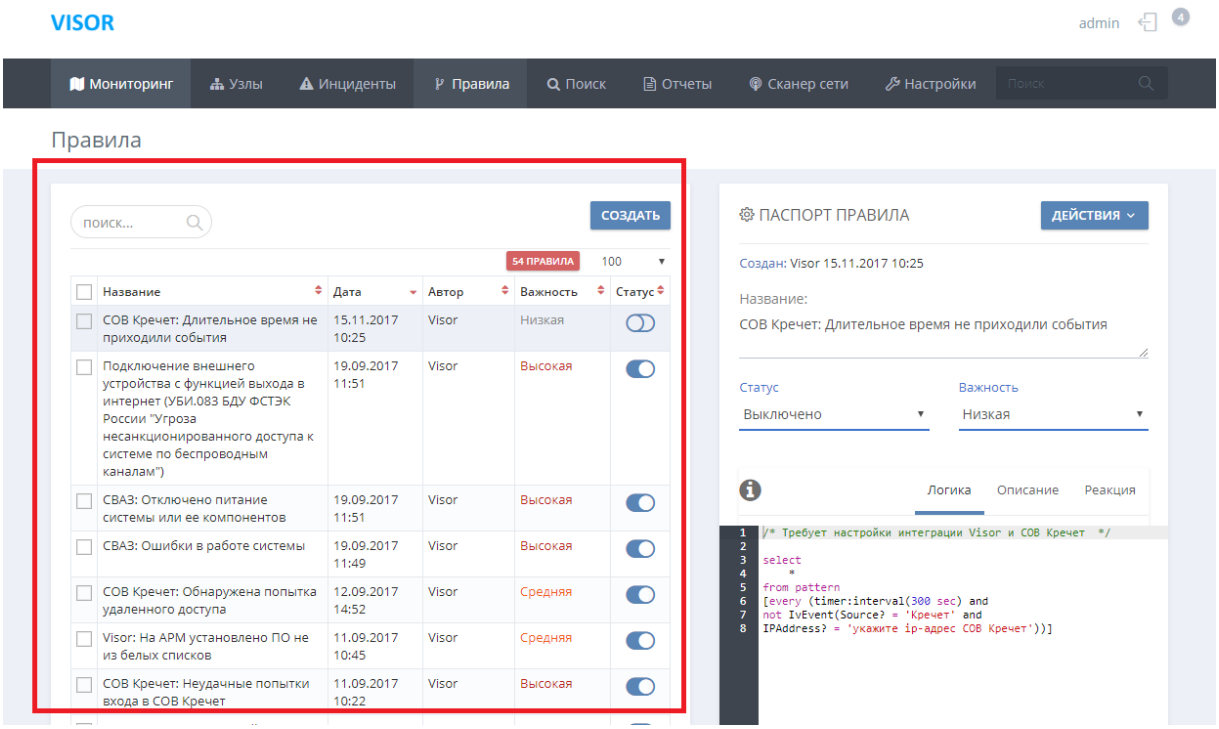


Рисунок 50 - Меню «Правила», перечень правил корреляции

При выборе правила в таблице, справа выводится паспорт данного правила. В паспорте правила отображаются все включенные в него логические условия, а также реакции при выполнении правила. Любое правило может быть включено или выключено.

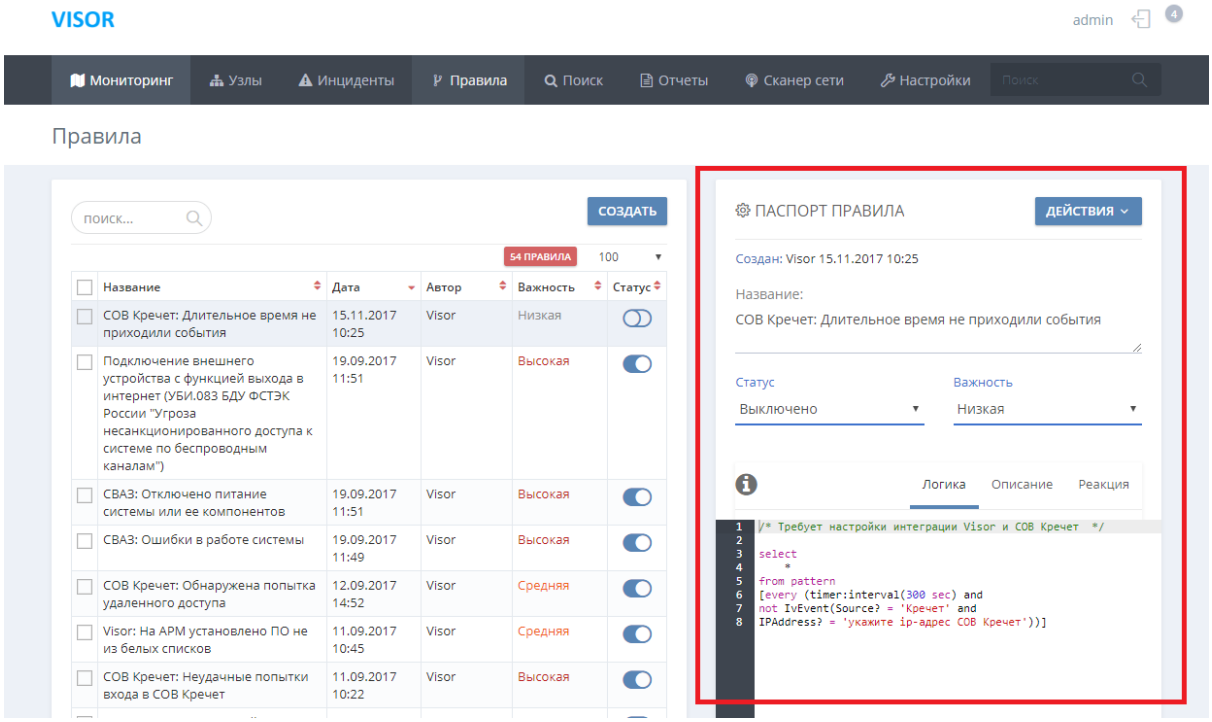


Рисунок 51 - Меню «Правила», паспорт правила корреляции

Каждое правило корреляции представляют собой совокупность логических условий и реакций. Правило корреляции определяет условие (например, «событие А произойдет 10 раз в течение 5 минут, затем произойдет событие Б в течение 1 одной минуты») и реакцию при его выполнении.

Возможны следующие виды реакции модуля аналитики при срабатывании условий правила:

– отображение уведомления в окне «Оповещений» в веб-интерфейсе;

– автоматическое создание инцидента в меню «Инциденты» (при этом модуль аналитики указывает название правила в качестве названия инцидента и привязывает к созданному инциденту события, вызвавшие срабатывание правила корреляции);

– отправка почтового сообщения по SMTP-протоколу заданному списку адресатов, в заданной форме.

Таким образом, при создании правила корреляции должны быть указаны как логические условия, так и реакции.

Написание логических условий правил корреляции в меню «Правила» осуществляется с помощью использования специального SQL-подобного языка – EPL (Event Processing Language). Ниже будет описан синтаксис и примеры написания правил корреляции с помощью языка EPL.

Visor поставляется с набором предустановленных правил корреляции, которые могут использоваться сразу же после развертывания СПО в информационной системе организации и подключения к СПО источников событий. Следует учитывать, что для срабатывания предустановленных правил корреляции необходимо, чтобы в Visor поступали определенные события от источников (защищаемых активов). Каждое предустановленное правило имеет вкладку «Описание», в котором содержится описание его назначения.

Оператор должен выполнять систематический пересмотр правил корреляции в ходе мониторинга событий, в особенности при подключении новых источников событий или изменении модели угроз и нарушителей ИБ.

4.13.1 Создание правила корреляции

Чтобы создать рабочее правило корреляции, оператор должен действовать по следующему общему алгоритму:

– ознакомиться с моделью угроз и нарушителей ИБ организации;
– подключить необходимые типы источников к Visor в соответствии с моделью угроз и нарушителей ИБ организации;
– выполнить мониторинг поступающих событий от источников;
– разработать новое правило;
– наблюдать работу разработанного правила;
– внести корректировку в правило, если это необходимо;
– настроить реакцию правила;
– реагировать при срабатывании правила;
– приступить к разработке нового правила.

Рекомендуется сначала выполнять разработку простых правил корреляции, использующих события только от одного из подключенных типов источников. Завершив разработку простых правил для одного типа источника перейти к разработки простых правил для следующего типа. И так последовательно для всех остальных типов источников.

После подключения всех типов источников и разработки простых правил для них, приступить к разработке сложных правил, которые коррелируют события от двух и более типов источников.

Процесс создания, разработки и тестирования собственных правил корреляции следует выполнять по научному методу проверки гипотез. Разработав и включив новое правило корреляции следует выделить время на наблюдение за его работой. При первичном наблюдении работы правила рекомендуется включать только реакцию «Выводить оповещение в интерфейсе» для того, чтобы не создавались фиктивные инциденты в меню «Инциденты» или не отправлялись не информативные E-mail уведомления. Таким образом можно отслеживать частоту и корректность условий срабатывания нового правила. После периода наблюдения вы можете внести изменения в логические условия правила и его реакцию, если это необходимо и проверить новую гипотезу новыми наблюдениям. Если в ходе наблюдения работы установлено, что гипотеза

логических условий в правиле корректна, то разработка правила завершена. В результате разработки, проверки гипотезы и корректировки правило должно выполнять необходимую задачу:

– выявлять определенные события и их последовательности;

– создавать инциденты в тех случаях, которые принимаются организацией за реальные инциденты;

– оповещать по электронной почте заинтересованный круг лиц о срабатывании и создании инцидентов.

Следует учитывать, что наблюдение и проверка гипотезы работы некоторых правил корреляции может занимать от нескольких секунд до нескольких недель и даже месяцев. Это связано с тем, что для проверки требуется, чтобы в модуль аналитики поступили определенные события от источников (или последовательность событий). Такие события не всегда могут быть специально сгенерированы или могут происходить только при определенных условиях и ситуациях в информационной системе организации, которые затруднительно предсказать или запланировать. Поэтому наблюдение работы и проверка гипотезы нового правила корреляции, в некоторых случаях, может требовать значительного периода времени.

Чтобы создать новое правило нажмите на кнопку «Создать», расположенную сверху справа над таблицей правил корреляции. В окне «Новое правило» внесите данные в поля:

– название правила;

– статус включено/выключено (выберет статус из раскрывающегося списка);

– важность правила (выберете важность из раскрывающегося списка);

– описание (текстовое пояснение для описания назначения правила);

– логические условия правила на языке EPL (см. раздел ниже);

– реакцию правила при срабатывании.

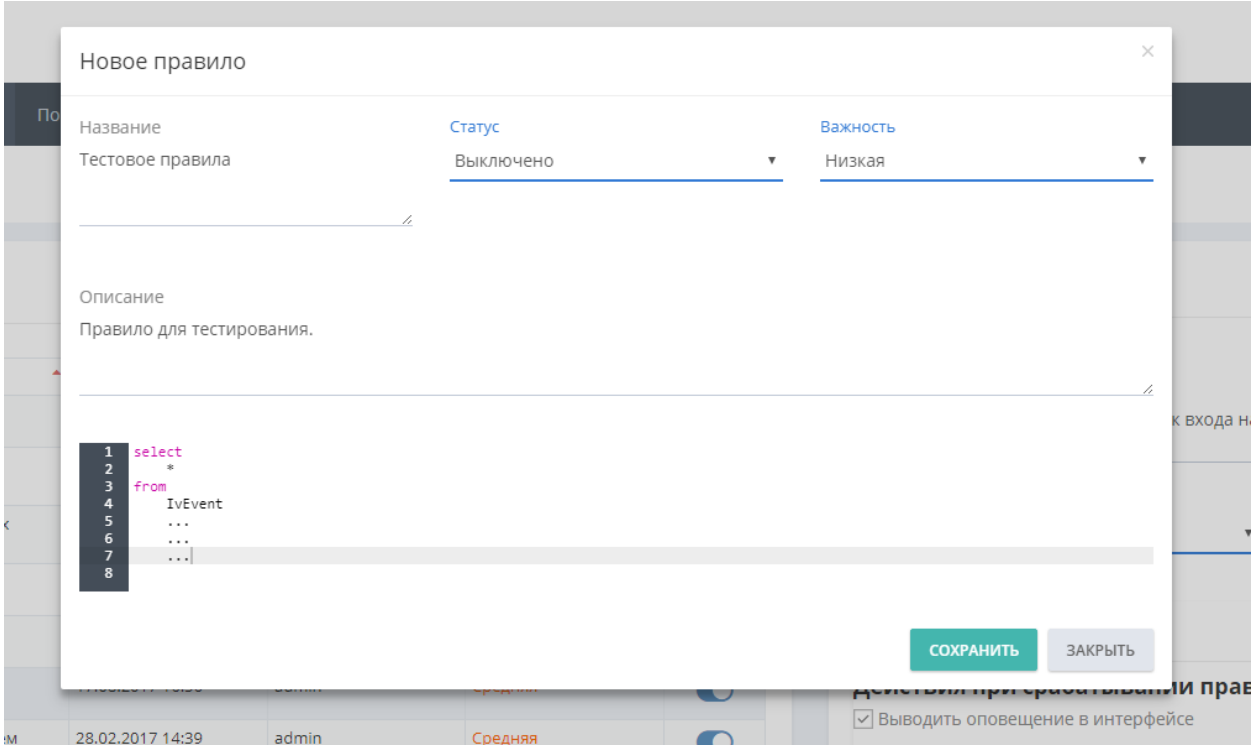


Рисунок 52 - Меню «Правила», окно создания нового правила

Нажмите кнопку «Сохранить». Для отмены создания нажмите кнопку «Закрыть».

4.13.2 Написание кода (логики) правила корреляции

Модуль аналитики платформы Visor использует в качестве движка технологию Nesper for .NET версии 5.

Синтаксис кода правил корреляции описывается на языке EPL (Event Processing Language), который схож с языком SQL (Structured Query Language), но отличается логикой работы и другими особенностями.

Чтобы быстро научиться создавать правила корреляции оператор должен обладать базовыми знаниями языка SQL и уметь формулировать простейшие SQL-запросы. Далее подразумевается, что оператор обладает данной квалификацией.

4.13.3 Пример правила, контролирующего изменение настроек агента

Рассмотрим структуру типичного правила корреляции на простом примере (в предустановленных правилах называется «Visor: Изменены настройки агента»):

```
1 select
2     *
3 from
4     IvEvent e
5 where
6     e.Source? = 'Visor' and
7     e.Summary? = 'Изменены настройки агента'
```

Рисунок 53 - Пример правила корреляции (1)

Каждое правило корреляции по сути является запросом, который обращается к потоку получаемых платформой Visor событий в реальном времени. На подобии запросов к таблицам баз данных в SQL языке, выражения EPL языка (которыми по сути являются правила корреляции) обращаются к потокам. Основной поток событий Visor называется **IvEvent**. Практически все правила корреляции будут обращаться к потоку **IvEvent**.

Выражение:

«Select * from IvEvent e»

выбирает все события из потока **IvEvent** и присваивает им псевдоним «e». Псевдоним «e» используется для удобства краткости применения и обращения к псевдониму далее по тексту кода правила. Псевдоним может иметь любое другое значение, которое вы зададите, это не будет влиять на логику работы правила. Мы рекомендуем использовать псевдонимы для потоков, хотя правила будут работать и без них.

С пятой строки описывается уточнение:

«where

e.Source? = ‘Visor’ and

e.Summary? = ‘Изменены настройки агента’»

«e.Source? = ‘Visor’» – означает, что правило выбирает из потока события, где поле нормализации Source имеет значение ‘Visor’. Т.е. данное правило корреляции применяется только к событиям, получаемым от источника Visor.

При указании имени любого поля нормализации в любом месте правила следует всегда ставить знак «?» после его имени (например, «Source?»).

«e.Summary? = ‘Изменены настройки агента» - означает, что правило выбирает из потока события, где поле нормализации Summary имеет значение ‘Изменены настройки агента’. Т.е. данное правило срабатывает на конкретное событие ‘Изменены настройки агента’ от источника Visor.

Т.е. данное правило позволяет выявлять факты внесения изменений в настройки агентов или агент-коллекторов Visor, что может являться предпосылкой к инциденту ИБ.

4.13.4 Пример правила для событий, поступающих с системы обнаружения вторжений, связанных с выявлением сетевой активности вредоносного кода

Рассмотрим другой пример правила (в предустановленных правилах называется «СОВ Кречет: Обнаружена сетевая активность вредоносного кода»):

```
1  /* Требует настройки интеграции Visor и СОВ Кречет  */
2
3  select
4      *
5  from
6      IvEvent e
7  where
8      e.Source? = 'Кречет'  and
9      (cast(e.SignatureName?,string) like '%MALWARE%' or
10     cast(e.SignatureName?,string) like '%EXPLOIT%' or
11     cast(e.SignatureName?,string) like '%BLACKLIST%' or
12     cast(e.SignatureName?,string) like '%SHELLCODE%')
```

Рисунок 54 - Пример правила корреляции (2)

На первой строке написан комментарий к правилу корреляции. Он означает, что для работы данного правила необходимо предварительно настроить интеграцию между Visor и источником событий СОВ Кречет. Иногда полезно оставлять поясняющие комментарии к коду правил корреляции, чтобы описать особенности его работы и логических условий. Чтобы оставить комментарий поместите его между звездочками в данному выражении **/* Ваш комментарий */**, тогда модуль аналитики не будет реагировать на данный текст при исполнении своего кода.

Далее перейдем к строке 7 и разберем выражение:

«where

e.Source? = ‘Кречет’ and

(cast(e.SignatureName?,string) like '%MALWARE%' or

cast(e.SignatureName?,string) like '%EXPLOIT%' or

cast(e.SignatureName?,string) like '%BLACKLIST%' or

cast(e.SignatureName?,string) like '%SHELLCODE%')»

«e.Source? = ‘Кречет’» – означает, что правило выбирает из потока события, где поле нормализации Source имеет значение ‘Кречет’. Т.е. данное правило корреляции

применяется только к событиям, получаемым от источника ‘Кречет. СОВ Кречет – является системой обнаружения вторжений, разработанной компанией ФГУП «НПП «Гамма».

«cast(e.SignatureName?,string) like '%MALWARE%'» – данное выражение означает, что правило корреляции должно срабатывать, если в тексте поля нормализации ‘SignatureName’ (или по-русски – «Имя сигнатуры»), содержится текст ‘MALWARE’. Выражение «cast(e.SignatureName?,string)» - применяет функцию cast языка EPL. Данная функция присваивает полю нормализации SignatureName тип переменной string (строковый). Это необходимо выполнять всегда, когда необходимо применить к полю нормализации любой строковый оператор (например, ‘like’). Т.е. данное правило будет срабатывать при получении событий о срабатывании системы обнаружения вторжений «Кречет», в которых указано срабатывание сигнатуры, содержащей текст ‘MALWARE’. Такие сигнатуры свидетельствуют о наличии сетевой активности вредоносного кода.

Далее в тексте правила используются такие же выражения, которые реагируют на другие типа сигнатур:

«(cast(e.SignatureName?,string) like '%MALWARE%' or
cast(e.SignatureName?,string) like '%EXPLOIT%' or
cast(e.SignatureName?,string) like '%BLACKLIST%' or
cast(e.SignatureName?,string) like '%SHELLCODE%')»

Между данными выражениями применяется логическое ‘OR’, которое позволяет срабатывать правилу на любой вид сигнатуры.

4.13.5 Пример правила для событий, поступающих с системы антивирусной защиты

Рассмотрим следующий пример правила (в предустановленных правилах называется «Касперский: Распространение определенного вредоносного объекта»):

```
1  select
2      window(*)
3  from
4      IvEvent(Source? = 'Антивирус Касперского' and
5      cast(Summary?,string) like '%Обнаружен вредоносный объект%')
6      .std:groupwin(ResultName?)
7      .win:length_batch(5)
8      .win:time(600 sec)
9  having count(distinct MachineName?) > 1
```

Рисунок 55 - Пример правила корреляции (3)

Выражение:

«select

Window(*)

From

IvEvent(Source? = ‘Антивирус Касперского’ and

…»

«Window(*)» – означает, что далее в правиле будут применяться операторы и функции использующие временное окно, а события потока IvEvent будут помещаться во временное окно. Следует учитывать, что правила корреляции, использующие временные окна повышают нагрузку на модуль аналитики и аппаратные ресурсы сервера платформы Visor, поэтому следует осторожно относиться к таким правилам при их тестировании и проверки.

Далее следует выражение:

«cast(Summary?,string) like '%Обнаружен вредоносный объект%')

.std:groupwin(ResultName?)

.win:length_batch(5)

.win:time(600 sec)

having count(distinct MachineName?) > 1»

«.std:groupwin(ResultName?)» – данное выражение означает, что события во временном окне должны иметь одинаковое значение поля нормализации ‘ResultName’.

«.win:length_batch(5)» – означает, что события во временном окне должны повториться ровно 5 раз.

«.win:time(600 sec)» – означает, что эти 5 событий должны произойти в течение 600 секунд. Т.е. этот параметр задает размер временного окна.

«having count(distinct MachineName?) > 1» – означает, что во всех событиях, выбранных из потока, поле нормализации ‘MachineName’ должно иметь больше 1 одного уникального значения. Оператор ‘Distinct’ является стандартным SQL-оператором для удаления дубликатов из результирующего запроса (т.е. оставляет только уникальные значения). Оператор ’having count’ позволяет подсчитать количество уникальных значения.

Обратите внимание, что все параметры временного окна применяются к выражению «(cast(Summary?,string) like '%Обнаружен вредоносный объект%')», т.е. они будут применены только к событиям, у которых в поле нормализации Summary присутствует текст ‘Обнаружен вредоносный объект’.

Таким образом данное правило корреляции срабатывает, когда происходит более 5 обнаружений (выражение – «.win:length_batch(5)») конкретного вредоносного объекта (выражение – «.std:groupwin(ResultName?)») в течение 10 минут (выражение – «.win:time(600 sec)») на разных узлах (выражение – «having count(distinct MachineName?) > 1»).

4.14 Вспомогательные инструменты для создания правил корреляции

4.14.1 Подменю «Списки»

Подменю «Списки», расположенное в меню «Правила» является вспомогательным инструментом при создании правил корреляции упрощающее управление списками сущностей, к которым могут применяться некоторые из правил корреляции.

Представим, что вам необходимо создать правило корреляции, которое будет срабатывать при установке хотя бы одного ПО из определенного перечня, запрещенного для установки на защищаемых активах, например, Skype, ICQ, BitTorrent или любые другие (правила такого типа есть в предустановленных правилах и одно из них называется «Visor: На АРМ установлено ПО не из белых списков»). Для этого будет необходимо перечислить в правиле название каждого ПО, которое требуется отслеживать. Чтобы каждый раз не перечислять списки сущностей в логике правил корреляции вы можете применить один или несколько списков в подменю «Списки». Каждый список будет содержать перечень определенных сущностей (например, перечни имен узлов, пользователей, ip-адресов или подсетей, названий ПО).

Платформа Visor поставляется с набором предустановленных списков. Следует учитывать, что для корректной работы некоторых предустановленных правил корреляции требуется заполнить используемые ими предустановленные списки. В списки должны быть внесены данные, характерные для конкретной информационной системы организации.

Каждый предустановленный список имеет вкладку «Описание», в котором содержится описание его назначения.

4.14.2 Создание списка

Для создания списка перейдите в подменю «Списки» меню «Правила». Нажмите на кнопку «Создать». В окне «Новый список» заполните поля: Название, Описание, Состав. Затем нажмите кнопку «Сохранить». Для отмены нажмите кнопку «Закрыть».

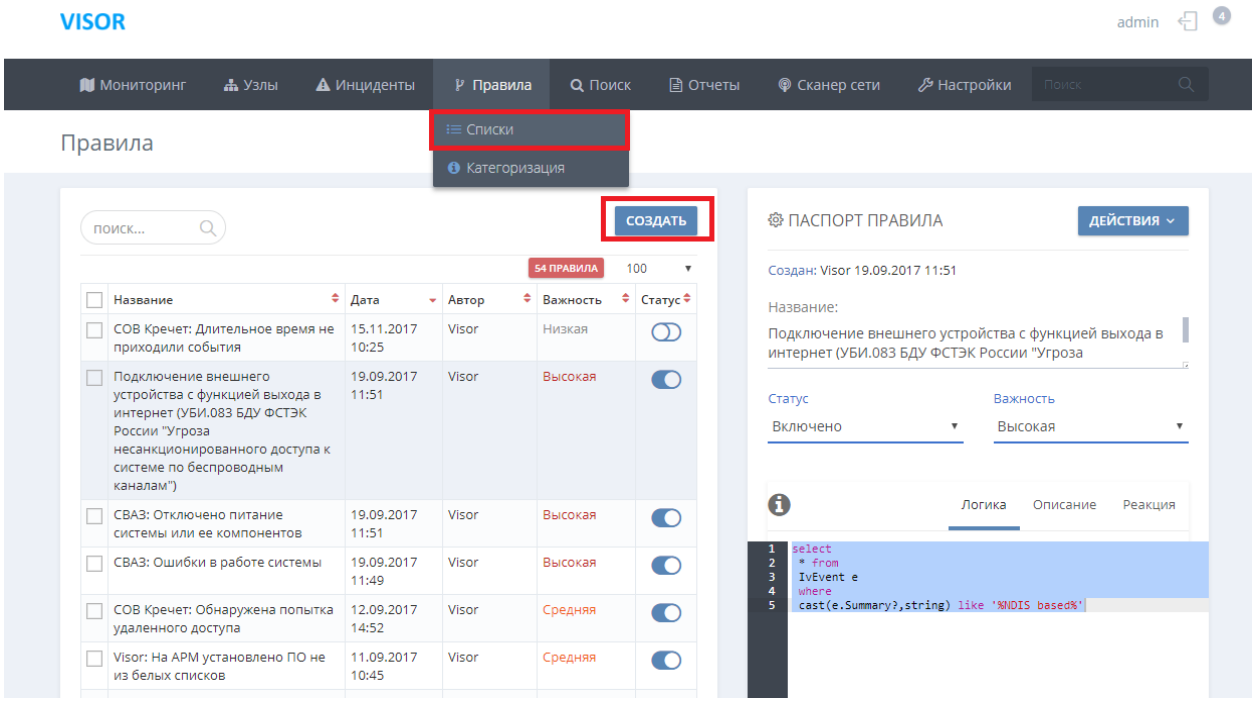


Рисунок 56 - Создание списка

Заполняя состав списка следует учитывать следующее:

– каждое новое значение списка надо размещать на новой строке;

– правила корреляции применяют значения в составе списка без учета регистра (т.е. значения «icq» и «ICQ» являются равнозначными, поэтому если вы просто напишите «icq» в списке, то правило сработает на любой вариант написания названия этого ПО).

4.14.3 Изменение, удаление списка

Выберите необходимый список, щелкнув на нем левой клавишей мыши. В паспорте списка внесите изменения и нажмите кнопку «Действие» -> «Сохранить» в правой верхней части паспорта списка.

Для того, чтобы удалить списков нажмите кнопку «Действие» -> «Удалить» в правой верхней части паспорта списка.

Выберите необходимый список, щелкнув на нем левой клавишей мыши. В паспорте списка внесите изменения и нажмите кнопку «Действие» -> «Сохранить» в правой верхней части паспорта списка.

Для того, чтобы удалить списков нажмите кнопку «Действие» -> «Удалить» в правой верхней части паспорта списка.

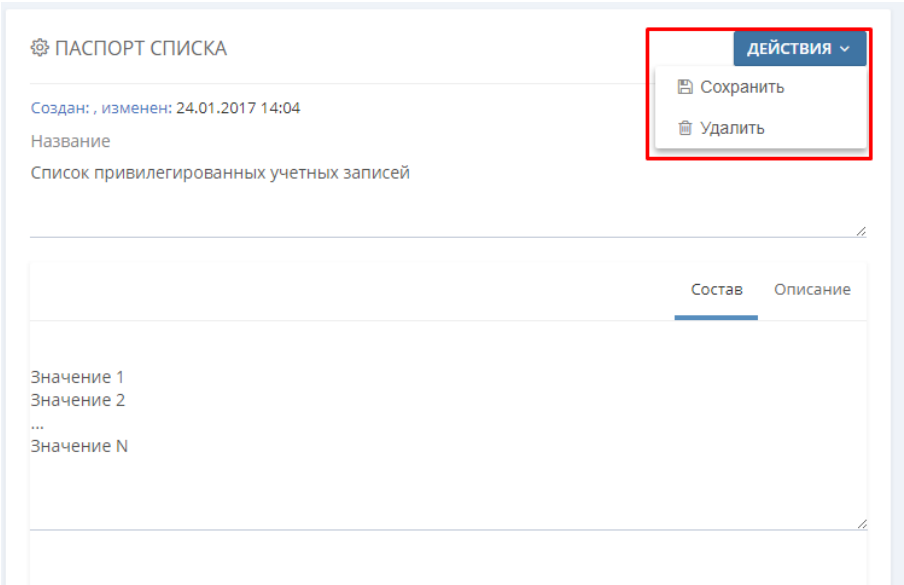


Рисунок 57 - Изменение и удаление списка

4.14.4 Подменю «Категоризация»

В Visor содержится собственный перечень категорий, которые присваиваются событиям источников. В процессе нормализации каждому поступающему в БД событию Visor присваивает определенную категорию, которая соответствует информационному смыслу события. Присваивание категорий событиям происходит на основании заданного списка соответствия, разработанного экспертами-аналитиками и разработчиками Visor.

Примечание: к примеру, всем событиям от любых типов источников, которые сообщают об успешном выполнении входа пользователя, присваивается категория «Пользователь.Активность.Вход.Успешно».

Применение категорий при разработке правил корреляции позволяет настроить срабатывание правила на все похожие по информационному смыслу события от различных типов источников. Такой подход позволяет создавать более универсальные и широкие по

назначению правила корреляции, что облегчает выполнение задач мониторинга событий ИБ.

При просмотре событий в меню «Поиск» вы можете увидеть категорию, присвоенную событию в поле нормализации «Категория».

Поля нормализации

Поле	Поле (англ.)	Значение
Дата события	DateCreated	01.09.2017 07:43:28
Дата записи события в БД	SystemDateCreated	01.09.2017 07:43:35
Имя узла	MachineName	VISOR-TESTING
IP-адрес узла	MachineIP	172.16.204.154
Источник	Source	Журнал безопасности Windows
Гео-расположение	GeoLocation	Москва
Важность события	Severity	Низкая
Категория	SUIBCategory	Пользователь.Активность.Вход
Описание	Summary	Выполнена попытка входа в систему с явным указанием учетных данных.
Текст сообщения	MessageText	Выполнена попытка входа в систему с явным указанием учетных данных. Субъект: ИД безопасности: -\Никто Имя учетной записи: - Домен учетной записи: - Код входа: 0x950f GUID входа: {00000000-0000-0000-0000-000000000000} Были использованы учетные данные следующей учетной записи: Имя учетной записи: svt_adm Домен учетной записи: ARM-S GUID входа: {00000000-0000-0000-0000-000000000000} Целевой сервер: Имя целевого сервера: ARM-S.csdis.dit.nppgamma.ru Дополнительные сведения: ARM-S.csdis.dit.nppgamma.ru Сведения о процессе: Идентификатор процесса: 0x4 Имя процесса: Сведения о сети: Сетевой адрес: - Порт: - Данное событие возникает, когда процесс пытается выполнить вход с учетной записью, явно указав ее учетные данные. Это обычно происходит при использовании конфигураций пакет ного типа, например, назначенных задач, или выполнении команды RUNAS.

Рисунок 58 - Отображение категории Visor в полях нормализации событий

Если необходимо отфильтровать в меню «Поиск» события по своему информационному значению (например, все события о каких-либо ошибках), то для этого удобней всего будет использовать фильтр по категории.

Подменю «Категоризация» меню «Правила» позволяет узнать какие категории присваиваются возможным типам событий для каждого типа источника, поддерживаемого Visor.

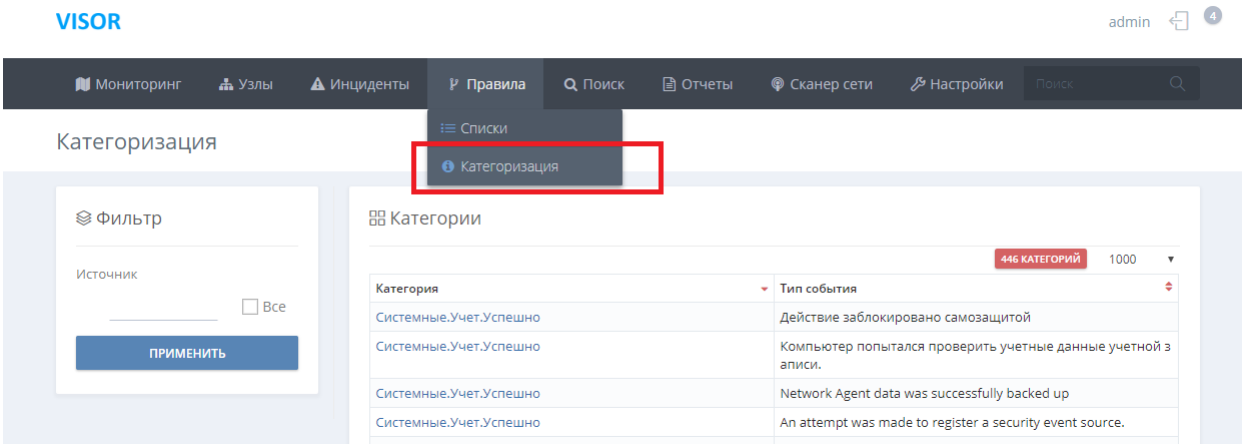


Рисунок 59 - Подменю «Категоризация»

Для просмотра категорий, присваиваемых всем возможным типам событий источника, выберите определенный тип источника в выпадающем окне «Источник» и нажмите «Применить».

Справа от фильтра отобразится список примеров всех возможных типов событий и присваиваемых им категорий.

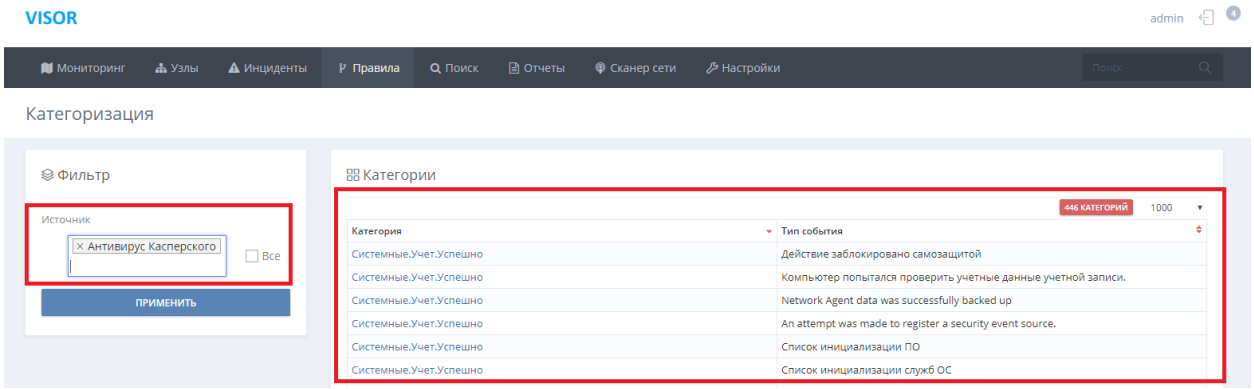


Рисунок 60 - Фильтрация по источнику и просмотр категорий событий

4.15 Настройка параметров оповещения о срабатывании правил корреляции событий

4.15.1 Вывод оповещений в веб-интерфейсе

Для того, чтобы при каждом срабатывании правила корреляции выводилось оповещение в веб-интерфейсе, необходимо установить флаг «Выводить оповещение в интерфейсе» на вкладке «Реакция» в паспорте правила.

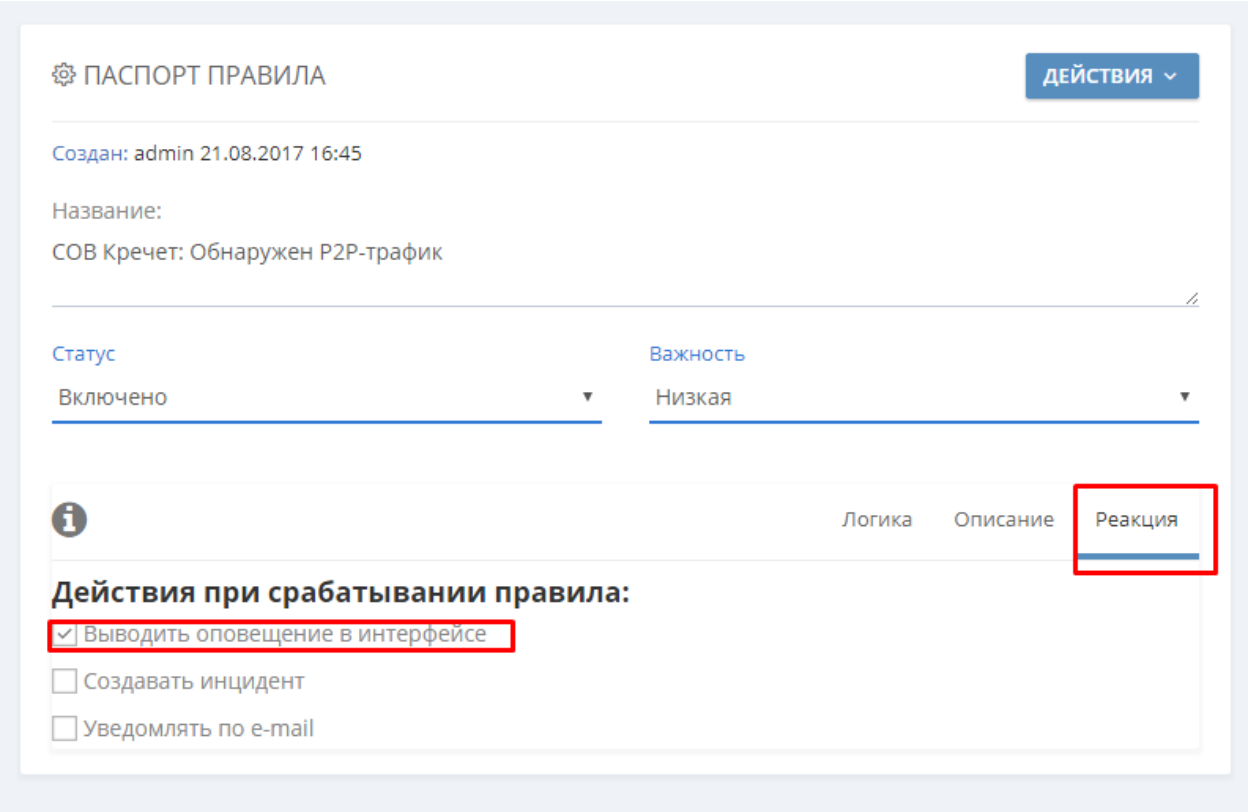


Рисунок 61 - Меню «Правила», настройка реакции правила

После этого в окне «Оповещений» будет выводиться информация о каждом срабатывании правила.

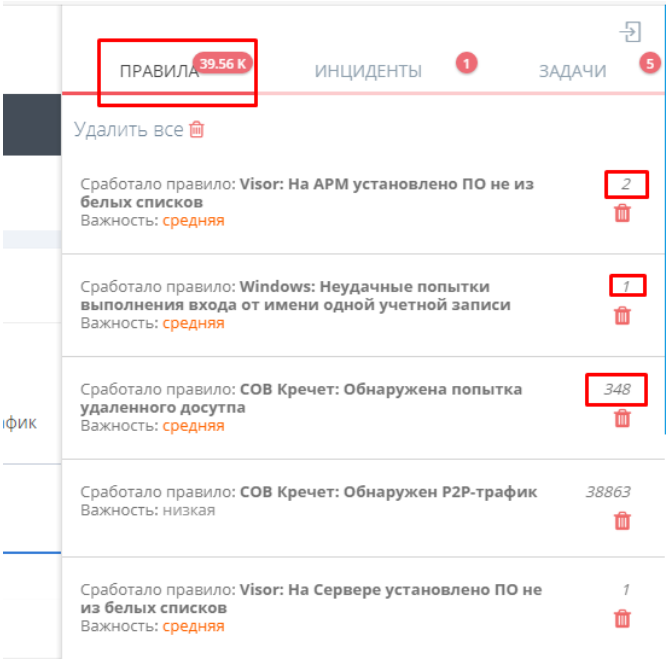


Рисунок 62 - Окно «Оповещения», отображение срабатываний правил

4.15.2 Автоматическое присвоение событию метки инцидента

Если срабатывание правила является для организации реальным инцидентом ИБ, то для данного правила должна быть установлена реакция в виде автоматического создания инцидента в меню «Инциденты».

Для этого необходимо установить флаг «Создать инцидент» на вкладке «Реакция» в паспорте правила. В поле под флагом «Создать инцидент» укажите название рабочей группы, на которую должны назначаться инциденты, автоматически создаваемые данным правилом.

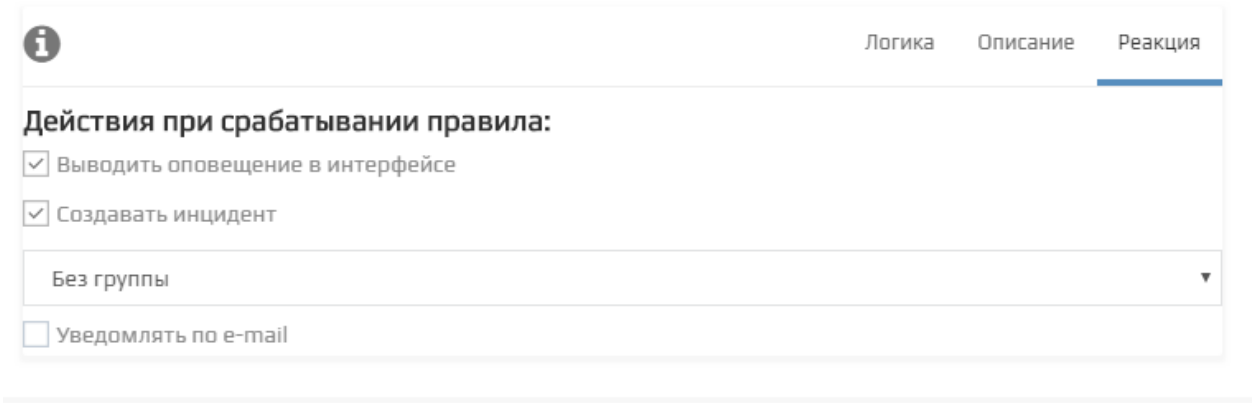


Рисунок 63 - Меню «Правила», настройка реакции правила

Для некоторых предустановленных правил корреляции реакция «Создавать инцидент» установлена по умолчанию. Вы можете ее отключить, если в вашей организации данные условия не являются признаками инцидента ИБ,

Примечание: в правилах Visor разработчиком предустановлен флаг «Создать инцидент» исходя из накопленного практического опыта.

4.15.3 Направление уведомлений по E-mail адресу

Оператор может настроить отправку почтовых сообщений указанному перечню адресатов в заданном формате.

Для этого необходимо установить флаг «Уведомлять по E-mail» на вкладке «Реакция» в паспорте правила.

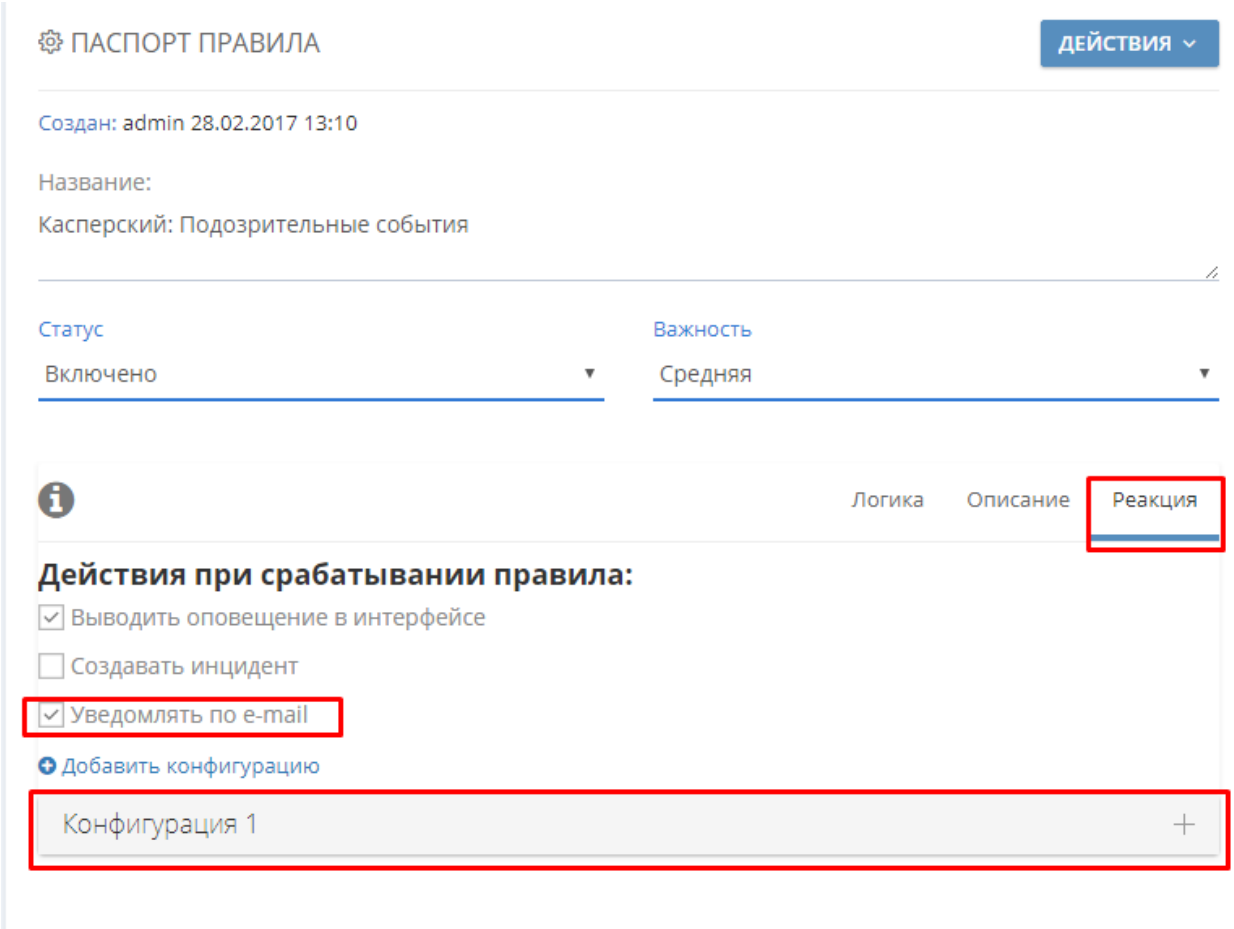


Рисунок 64 - Меню «Правила», настройка реакции правила

При включении реакции «Уведомлять по E-mail» автоматически создается конфигурация для отправки почтовых сообщений. Оператор может добавить несколько

конфигураций нажав на кнопку «Добавить конфигурацию» для того, чтобы отправлять уведомление разным перечням адресатов в разном формате. Например, оператор может отправить группе администраторов письмо с темой и поясняющим текстом письма в одном формате, а группе ответственных руководителей организации в другом.

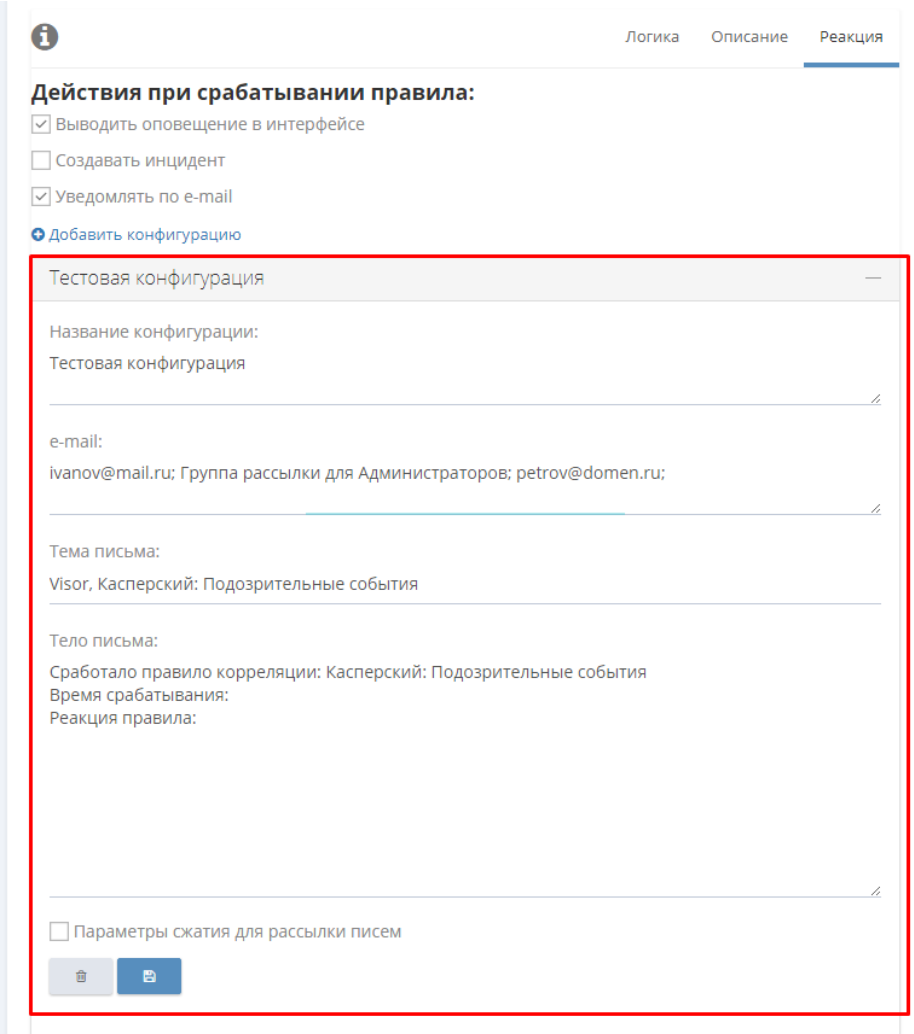


Рисунок 65 - Меню «Правила», настройка конфигурации для уведомления по e-mail

Для настройки конфигурации введите значения следующих полей:

– название конфигурации;

– e-mail (указание перечня e-mail адресов на которые отправятся уведомления. Адреса должны быть перечислены через точку с запятой);

– тема e-mail письма (по умолчанию всегда соответствует имени правила корреляции);

– текст e-mail письма (по умолчанию в теле письма указывается имя сработавшего правила, время его срабатывания и все виды реакций).

При указании перечня e-mail адресов можно использовать имена списков из меню «Списки». Например, оператор может создать список в меню «Списки», который содержит e-mail адреса всех администраторов ИТ в организации, и присвоить ему имя «Группа рассылки для Администраторов». После этого для рассылки сообщений оператору потребуется только указывать имя этого списка, вместо списка e-mail адресов, которым необходимо рассылать сообщение.

4.15.4 Настройка параметров сжатия e-mail сообщений

При настройке отправки уведомлений по e-mail адресу оператор может настроить параметры сжатия рассылаемых писем. Данная функция может быть применена в ситуации, при которой происходит частое срабатывание правила корреляции, к примеру 1000 раз в 1 секунду, при этом для срабатывающего правила настроена отправка уведомление по e-mail адресам.

Примечание: частое срабатывание правила может происходить из-за большого количества событий от источников, вызывающих срабатывание настроенного правила; если в Visor в 1 секунду поступит 1000 событий, вызывающих срабатывание правила, то сервер Visor в свою очередь выполнить рассылку 1000 писем в течение 1 секунды.

Для того, чтобы исключить рассылки чрезмерного количества писем за короткий период времени необходимо включить флаг «Параметры сжатия для рассылки писем».

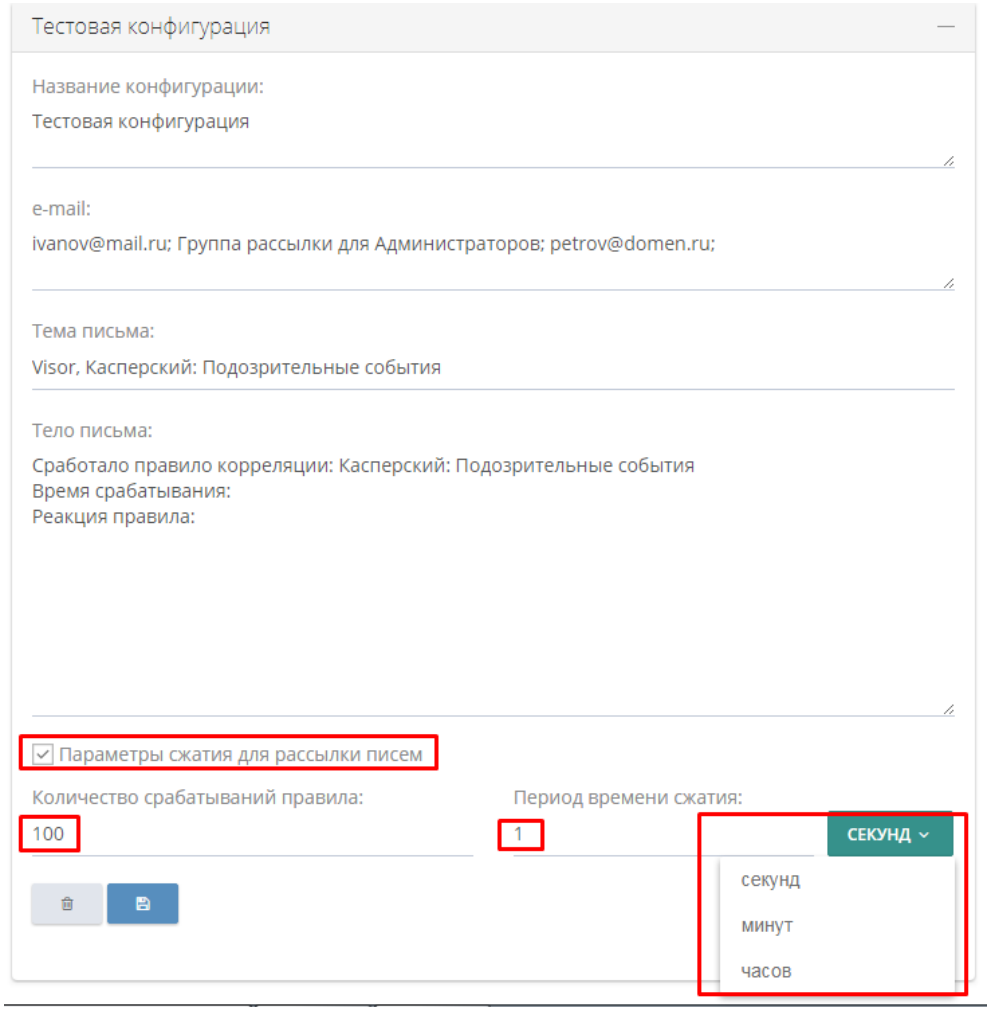


Рисунок 66 - Меню «Правила», настройка параметров сжатия для рассылки писем

Для настройки сжатия необходимо указать два параметра:

– количество срабатываний правила (данное количество срабатываний правила будет сжиматься в одно письмо);

– период времени сжатия (временной период за который указанное количество срабатываний правила должно произойти. В выпадающем меню вы можете задать временной период в секундах, минутах и часах).

Например, вы установили значение в количестве 100 срабатываний в течение 1 секунды. Это означает, что если произойдет 1014 событий в течение 1 секунды, то Visor отправит 11 e-mail сообщений и в них укажет, что произошло 1014 срабатываний, 10 писем будут содержать информацию о 1000 срабатываний, а в 1 письме будет информация о 14 срабатываниях.

4.15.5 Изменение отключение или удаление правила

Выберите из списка правило, щелкнув на нем левой клавишей мыши. В правой части экрана внесите в поля необходимые изменения и нажмите кнопку «Действие» (сверху справа в паспорте правила) -> «Сохранить».

Для удаления правила в этом же меню нажмите кнопку «Действие» -> «Удалить».

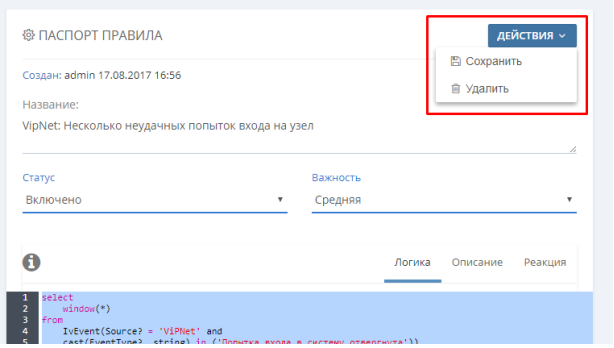


Рисунок 67 - Меню «Правила», сохранение изменений и удаление в правиле

Если правило может быть полезно в будущем, но на текущий момент его работа не требуется, вы можете выполнить его временное отключение и включить в нужный момент. Для этого выберите в выпадающей вкладке «Статус» -> «Выключено» или отключите правило путем изменения положения слайдера в таблице правил.

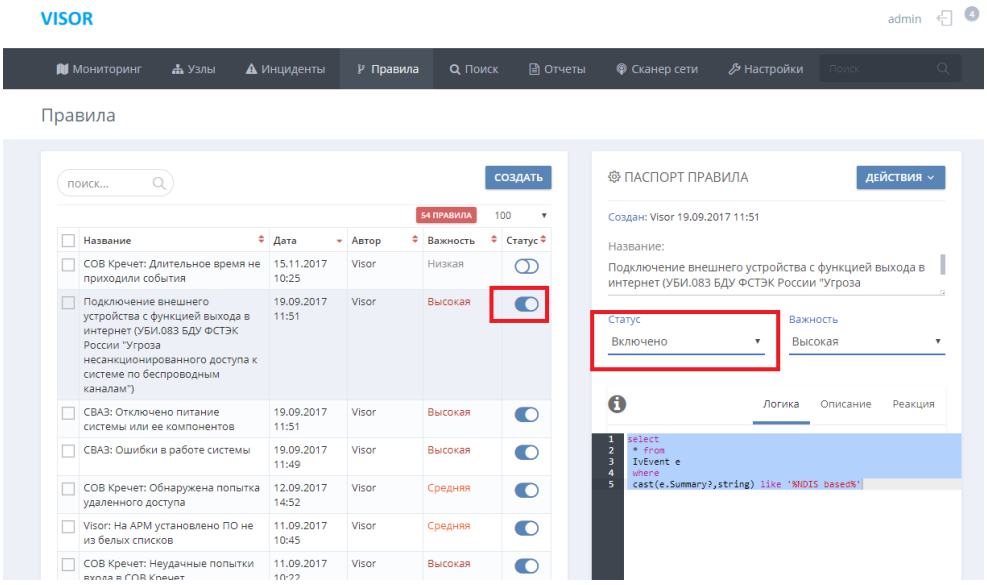


Рисунок 68 - Включение / отключение правил корреляции

4.16 Управление инцидентами

Одной из основных функций оператора является осуществление регистрации, реагирования, устранения последствий и расследование причин инцидентов ИБ.

Основная обработка событий, связанных с инцидентами осуществляется в меню «Инциденты». Настройка прав доступа оператору к выполнению операций с инцидентами ИБ выполняется администратором Visor.

Перечень доступных инцидентов ИБ в общей таблице меню «Инциденты», а также доступные оператору операции с инцидентами ИБ (создание, назначение рабочей группе или пользователю, редактирование, комментирование, выгрузка, удаление и другие операции) зависят от назначенных ему администратором прав.

Настройка прав доступа должна выполняться в соответствии с принятой структурой и порядком координации деятельности сотрудников на стадиях обработки инцидентов ИБ в вашей организации.

4.16.1 Общая таблица инцидентов ИБ

Основную часть экрана меню «Инциденты» занимает общая таблица в которой выводятся доступные пользователю инциденты ИБ, где каждая строка является отдельным инцидентом ИБ.

Над общей таблицей инцидентов ИБ отображаются элементы управления, позволяющие выполнять различные операции с инцидентами ИБ и изменять внешний вид общей таблицы.

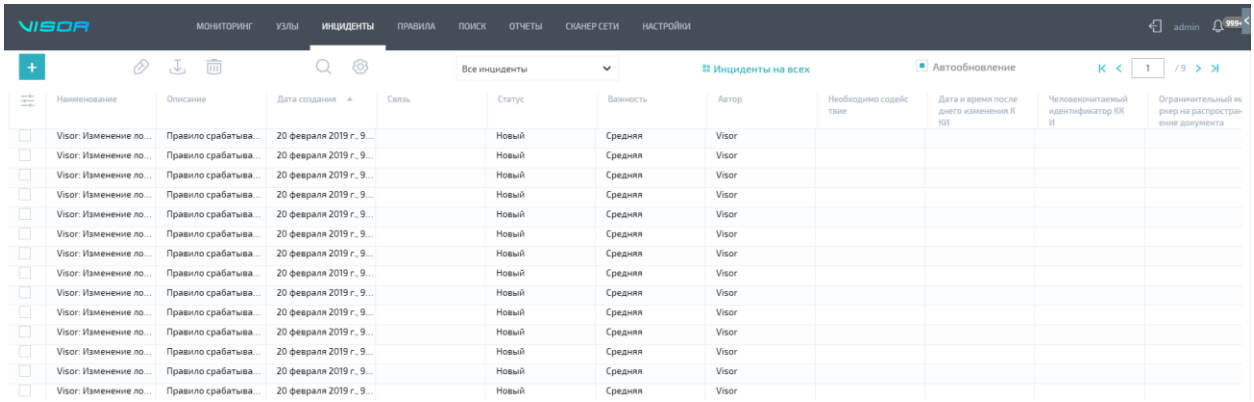


Рисунок 69 – Общая таблица инцидентов

Чтобы изменить отображаемые столбцы в общей таблице нажмите на иконке ,

расположенной сверху в левом углу общей таблицы. Далее выберите столбцы, которые должны быть отображены в общей таблице.

Чтобы изменить порядок отображения столбцов в общей таблице, нажмите и удерживайте на названии одного из столбцов и перетащите его.

Чтобы изменить порядок сортировки общей таблицы инцидентов ИБ кликните на одном из столбцов, чтобы инвертировать порядок сортировки кликните на столбце ещё раз.

Чтобы выполнить переключение между страницами инцидентов ИБ в общей таблице, используйте набор элементов для навигации, расположенный сверху справа над общей таблицей.

На одной странице пагинации отображается 20 инцидентов ИБ. При скроллинге инцидентов ИБ по общей таблице, через каждые 20 строк отображается горизонтальный разделитель страниц пагинации.

Чтобы найти инцидент в общей таблице, нажмите на иконке ,

расположенной над общей таблицей и введите поисковой запрос. При формулировании поискового запроса учитывайте, что поиск выполняет проверку всех полей по каждому инциденту ИБ в общей таблице.

Чтобы включить автоматическое обновление общей таблицы инцидентов ИБ, включите функцию «Автообновление» (по умолчанию включена).

По умолчанию в общей таблице инцидентов отображаются все доступные пользователю инциденты. Чтобы отфильтровать инциденты ИБ, которые назначены лично на пользователя или на рабочую группу, в которой он состоит, используйте соответствующий фильтр.

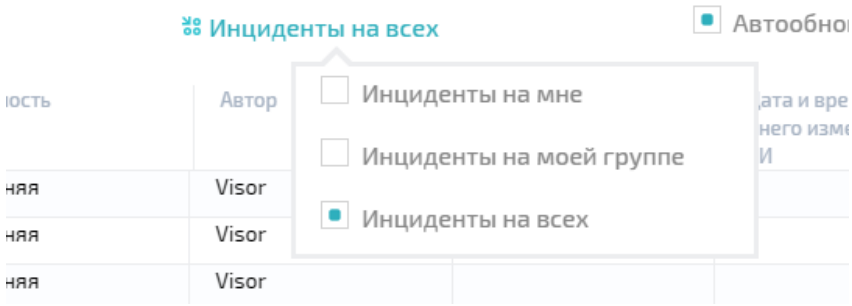


Рисунок 70 – Фильтр инцидентов ИБ по назначению

Чтобы отфильтровать инциденты ИБ в общей таблице по времени воспользуйтесь соответствующим фильтром и задайте требуемый временной период. Или выберите один из доступных быстрых временных периодов.

Чтобы перейти в меню «Настройка» -> «Настройка инцидентов» кликните по иконке

.

Подменю «Настройка инцидентов» позволяет управлять полями, которые отображаются в паспортах инцидентов ИБ, ограничивать допустимый размер вложений к комментариям и настраивать другие функции. Подробное описание применения указанного подменю см. ниже.

Любые настройки внешнего отображения столбцов являются индивидуальными для каждого пользователя Visor и не влияют на внешний вид общей таблицы у других пользователей.

4.16.2 Просмотр паспорта (карточки) инцидента ИБ

Для быстрого просмотра полной информации по инциденту ИБ кликните один раз на одном из инцидентов в общей таблице, справа появится отображение его паспорта (карточки).

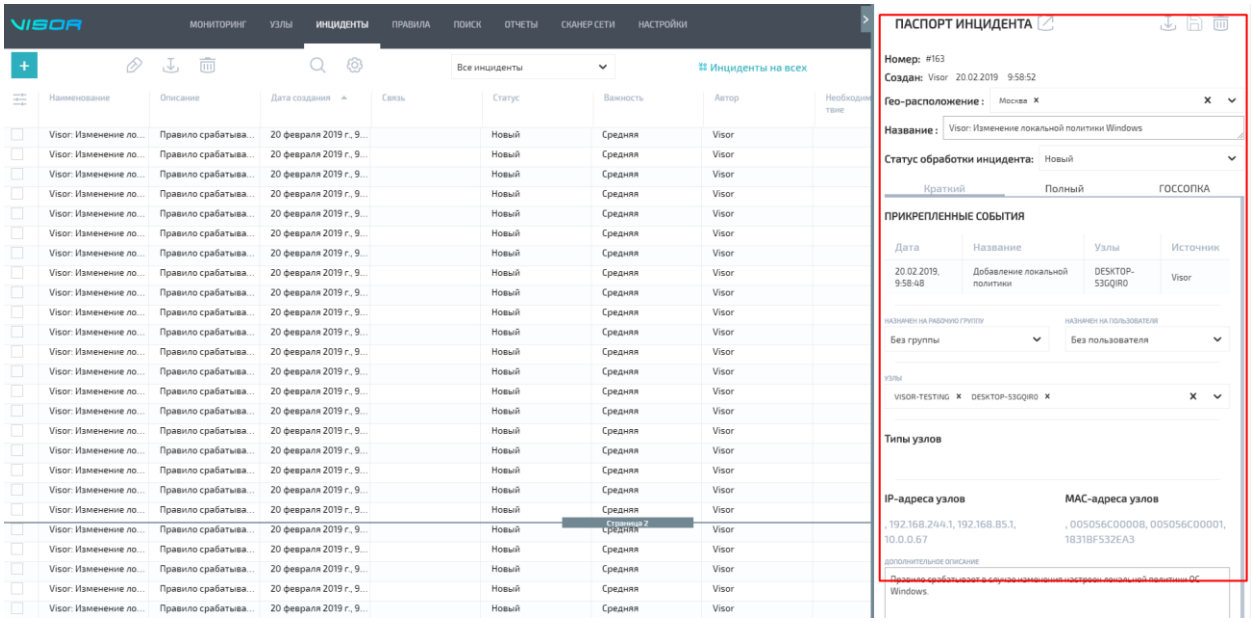


Рисунок 71 – Отображение паспорта инцидента

При двойном клике на инциденте ИБ в общей таблице, появится развернутое отображение его паспорта (карточки) в отдельном окне.

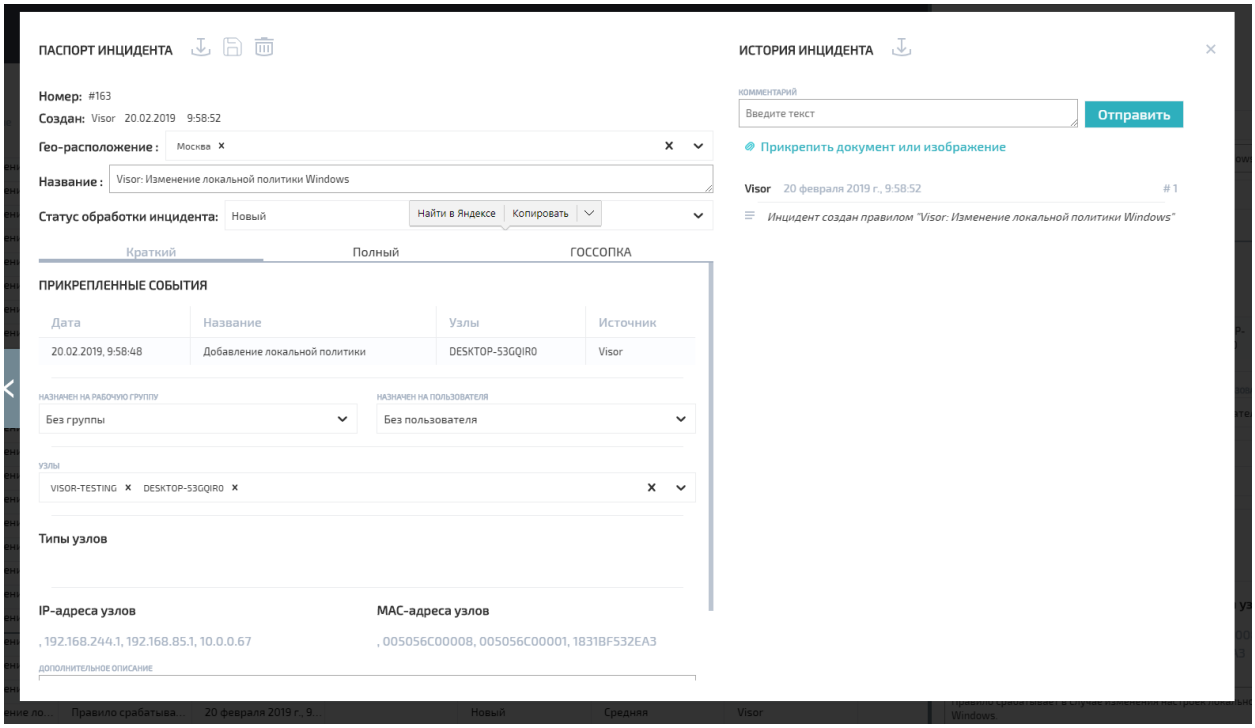


Рисунок 72 – Отображение полной карточки инцидента

Стрелки влево и вправо, расположенные по бокам развёрнутого окна паспорта инцидента ИБ позволяют переходит к предыдущему или следующему по дате создания инциденту ИБ в общей таблице инцидентов.

В левой части окна паспорта (карточки) инцидента ИБ отображаются поля, содержащие основную информацию по инциденту.

Поля паспорта инцидента ИБ имеют следующие представления:

– «Краткий» - в этой версии паспорта отображаются основные поля по инциденту ИБ;

– «Полный» - это представление отображает все доступные поля Visor по инциденту ИБ;

– «ГосСОПКА» - отображает все доступные поля Visor по инциденту ИБ и дополнительно все поля, в соответствии с требованиями ГосСОПКА, которые может иметь инцидент при предоставлении информации о нём в Центр ГосСОПКА.

На правой части окна паспорта (карточки) инцидента ИБ отображается история всех изменений и комментариев пользователей по нему.

4.16.3 Регистрация инцидентов ИБ

Инцидент ИБ в меню «Инциденты» может быть создан:

– автоматически при срабатывании правила корреляции, у которого установлена реакция «Создавать инцидент» (см. соответствующий раздел документации);

– вручную пользователем Visor в любой момент времени.

При создании нового инцидента ИБ, как автоматически, так и вручную, в окне «Оповещения» на вкладке «Инциденты» всегда отображается оповещение о созданном инциденте.

Чтобы создать инцидент ИБ вручную нажмите на иконку  .

Создание инцидента» заполните все необходимые поля.

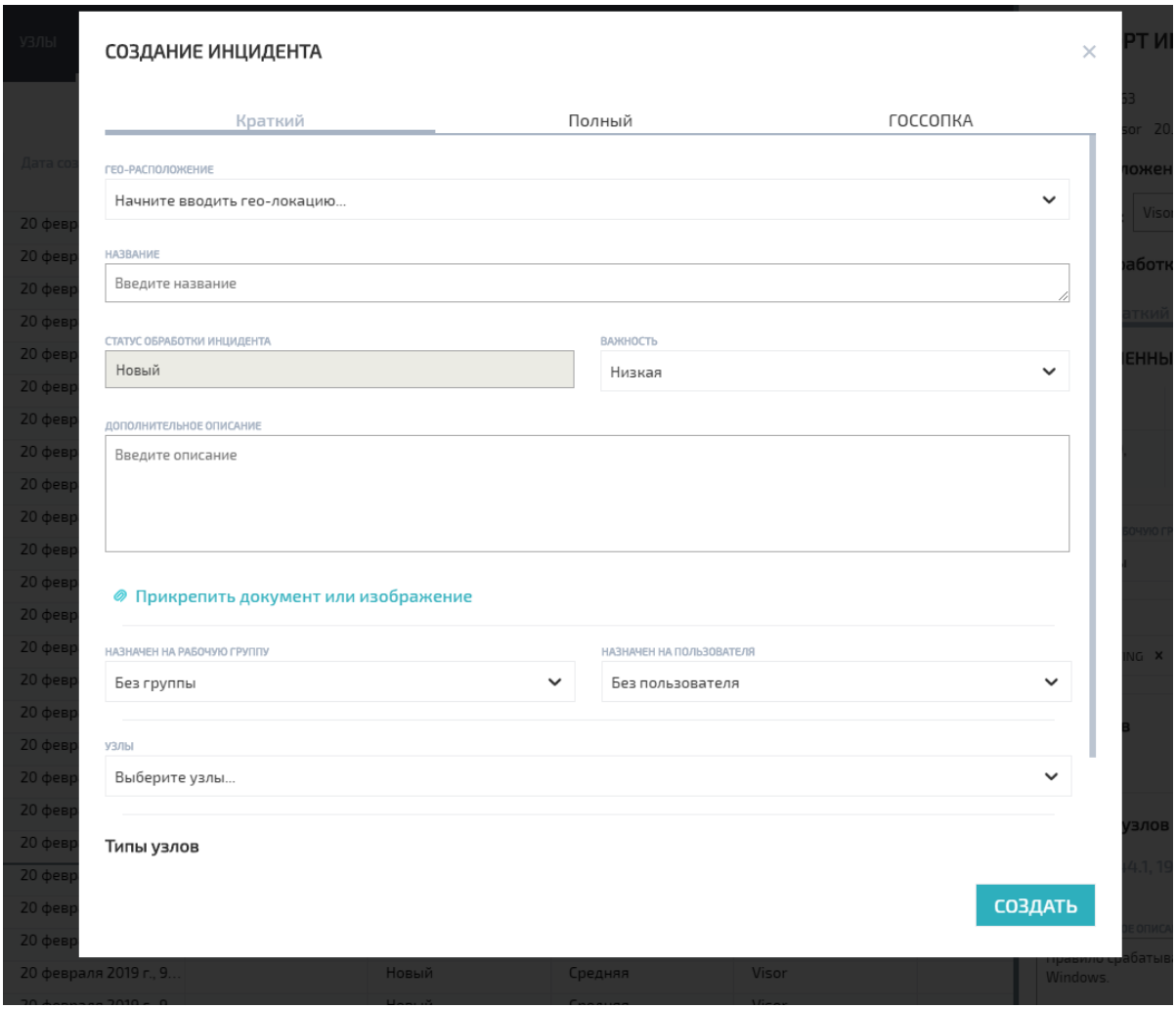


Рисунок 73 – Окно создания инцидента

После этого нажмите кнопку «Сохранить». Для отмены создания нажмите на иконку ✕ .

4.16.4 Редактирование паспорта инцидента ИБ

Чтобы внести изменения в поле паспорта инцидента ИБ, выберите нужный инцидент ИБ в общей таблице, откройте его паспорт, найдите соответствующее поле и внесите в него требуемое значение. После этого нажмите на иконку , чтобы сохранить внесенное изменение.

При внесении любого изменения в правой части ока паспорта (карточки) инцидента ИБ – «История инцидента», появится соответствующая запись о внесенном изменении.

К любому инциденту ИБ могут быть привязаны события, полученные от источников и отображаемые в меню «Поиск». Это позволяет хранить вместе с инцидентом ИБ те события, которые прямо или косвенно относятся к нему. Подробнее о как это сделать написано в разделе про меню «Поиск».

Если инцидент ИБ был создан автоматически при срабатывании правила корреляции, то события, вызвавшие срабатывание этого правила, будут автоматически привязаны к созданному инциденту. Автоматически созданным инцидентам ИБ в поле «Создан» будет проставлено значение «Visor» в качестве создатели. Название у таких инцидентов ИБ будет идентично названию правила корреляции, которое его создало.

4.16.5 Пакетная обработка нескольких инцидентов ИБ

Чтобы внести изменения одновременно в несколько инцидентов ИБ, выберите несколько инцидентов в общей таблице кликнув в начале строки каждого инцидента ИБ. Затем нажмите на иконку


,

расположенную над общей таблицей, появится окно «Пакетная обработка».

В тех полях, где значения не совпадают для выбранной группы инцидентов (например, выбрано два инцидента и у первого поле «Важность» имеет значение «Высокая», а у второго – «Низкая»), будут отображаться значения «*». Если значения совпадают, то будет отображаться это общее значение.

Внесите необходимые изменения, и нажмите кнопку «Сохранить».

4.16.6 Комментирование инцидентов ИБ

В правой части окна паспорта (карточки) инцидента ИБ расположена «История инцидента». В ней отображаются все изменения и комментарии по инциденту. Сверху всегда отображаются самые свежие изменения или комментарии.

Чтобы оставить комментарий по инциденту ИБ откройте его паспорт (карточку) и в «Истории инцидента» введите нужный комментарий в поле «Комментарий».

К комментарию может быть прикреплен внешний файл. Ограничение на максимально допустимый размер прикрепляемых файлов задаётся в меню «Настройка» -> «Настройки инцидентов».

Для сохранения комментария нажмите на кнопке «Отправить».

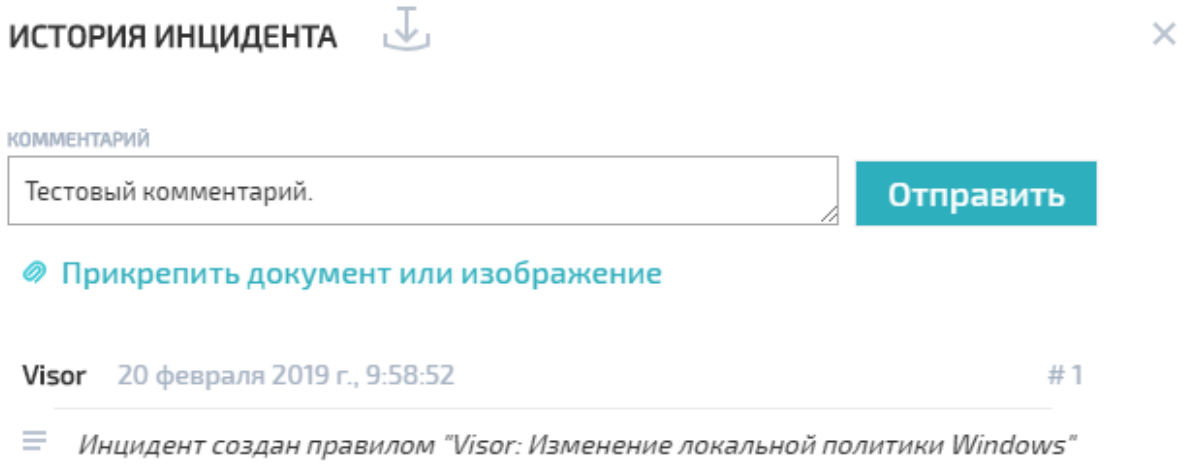


Рисунок 74 – Комментирование инцидентов

При наличии соответствующих прав, можно редактировать и удалять содержание комментариев. Для этого наведите мышью на нужный комментарий и нажмите на иконке

для редактирования. После этого введите изменения в комментарий и нажмите кнопку «Отправить».

Для удаления комментария нажмите на иконке

.

Вся «История инцидента» может быть выгружена в отдельный файл. Для этого нажмите на иконке

справа от надписи – «История инцидента» и сохраните файл на жёсткий диск.

4.16.7 Выгрузка данных об инциденте в формате ГосСОПКА

Для выгрузки инцидента ИБ во внешний json-файл в формате ГосСОПКА откройте паспорт (карточку) инцидента ИБ и нажмите на иконке

справа от надписи «Паспорт инцидента». Далее выберите директорию на жёстком диске для сохранения json-файла

Для выгрузки группы инцидентов ИБ одновременно во внешние json-файлы в формате ГосСОПКА, выберите несколько инцидентов в общей таблице кликнув в начале строки каждого инцидента ИБ. Затем нажмите на иконку

 ,

расположенную над общей таблицей. Далее выберите директорию на жёстком диске для сохранения json-файла.

Следует учитывать, что при выгрузке инцидентов ИБ во внешний файл в формате ГосСОПКА, «История инцидента» не выгружается в этот файл, при необходимости, её необходимо выгружать отдельно.

4.16.8 Удаление паспорта (карточки) инцидента

Для удаления паспорта (карточки) инцидента ИБ откройте паспорт (карточку) инцидента ИБ и нажмите на иконку

 .

Для удаления группы паспортов (карточек) инцидентов ИБ выберите несколько инцидентов в общей таблице кликнув в начале строки каждого инцидента ИБ. Затем нажмите на иконку

 ,

расположенную над общей таблицей.

При удалении инцидентов ИБ, все события, прикрепленные к удаляемым инцидентам ИБ, не удаляются и остаются в базе данных Visor и доступны для просмотра в меню «Поиск».

4.16.9 Настройка автоматической выгрузки инцидентов

Выполните вход в меню «Настройка» -> «Настройка инцидентов».

Подменю «Настройка инцидентов» позволяет:

– ограничивать максимально допустимый размер файла для приложения к комментариям инцидентов ИБ;

– настраивать параметры экспорта инцидентов в другие системы с Visor;

– настраивать автоматическую выгрузку инцидентов в файлы;

– настраивать выгрузку инцидентов по API в ГосСОПКА (в формате НКЦКИ).

Перечень принятых сокращений

АРМ – автоматизированное рабочее место

АС – автоматизированная система

БД – база данных

ИБ – информационная безопасность

ЛВС – локальная вычислительная сеть

НКЦКИ – Национальный координационный центр по компьютерным инцидентам

ОС – операционная система

ПО – программное обеспечение

ОПО – общесистемное программное обеспечение

СПО – специальное программное обеспечение

СОВ – система обнаружения вторжений