ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Платформа мониторинга информационной безопасности VISOR

(Версия 1.1)

Руководство системного программиста

Листов 74

2019 год

АННОТАЦИЯ

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

В настоящем документе содержатся назначение, состав, сообщения системному программисту 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 системного программиста и описание методов их выполнения в Visor.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

Visor является программным продуктом и предназначен для оперативного информирования 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 Сведения о технических и программах средствах, обеспечивающих выполнение программы

1.1.1 Требования к аппаратной конфигурации СВТ

СВТ или виртуальная машина, используемые для обеспечения условий выполнения Visor, должны удовлетворять минимальным рекомендуемым требованиям, указанным в таблице 1, таблице 2, таблице 3.

Таблица 1. 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 ресурс процессора не менее - 80%.	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 ПЗУ; 5) Возможность установки

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	дополнительного сетевого интерфейса.

Таблица 2. 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 3. 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 не ниже 2,3 Ггц. Доступный ресурс процессора не менее - 60%.	Минимум 8 Гбайт Минимум 2 Гбайт зарезервированного под сервис модуля	Минимум 3 Гб для развёртывания ПО и хранения лог файлов. Минимум 6 Гб для резервного хранения событий.	Наличие сетевого интерфейса (10 Мбит/с и более).

1.1.2 Требования к программной конфигурации ОПО

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

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 9.6 (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 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.

2 СТРУКТУРА ПРОГРАММЫ

2.1 Структура программы и ее составные части

Visor состоит из четырех взаимодействующих программных компонентов:

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

2.2 Связи между составными частями программы

Сервер состоит из компонент:

– 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 взаимодействие компонентов Visor, 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.

Основной сервис получает запросы на подключение от агентов и агентов-коллекторов сразу после выполнения их установки на контролируемом узле, сервис создает соответствующие каждому подключенному агенту и агент-коллектору таблицы в БД сервера Visor. В данных таблицах сохраняются все получаемые данные от агентов и

агент-коллекторов. Все поступающие от источников данные дополнительно нормализуются (добавляются дополнительные поля нормализации) и сохраняются в БД сервера Visor. Вместе с тем, основной сервис обеспечивает возможность выгружать события и инциденты ИБ из БД сервера Visor во внешние архивные файлы вручную или автоматически. Перенос событий и инцидентов из БД в архивные файлы осуществляется при ручном или автоматическом запуске специальной задачи архивирования данных. При этом из БД сервера Visor выгружается соответствующий заданному временному периоду объем данных в созданный архивный файл. Выгруженные данные удаляются из БД сервера Visor. Архивные файлы сохраняются на носители СХД и могут быть подключены к БД сервера Visor в ручном режиме. После подключения архивного файла к серверу Visor хранящиеся в нем данные становятся доступными и могут обрабатываться наравне с данными, хранящимися в БД сервера, в том числе они будут отображаться в веб-интерфейсе сервера Visor. Основной сервис по команде пользователя может создавать управляющие задачи на сканирование агентами сегментов сети, удаленную установку, обновление агентов и агент-коллекторов или их удаление.

Сервис аналитики: обеспечивает обработку потока данных от источников последовательного, в порядке их поступления, либо параллельно с процессами обработки данных, подгружаемых выборочно из БД сервера Visor и применяет для анализа данных логические условия, которые выражены правилами корреляции. Правила корреляции описываются на языке EPL (Event Processing Language). Правила корреляции хранятся в БД сервера Visor и могут определяться и корректироваться пользователями в веб-интерфейсе сервера. При выполнении логических условий, описанных в одном из правил корреляции, сервис анализа, в зависимости от настройки реакции на выполнение правила корреляции, создает инцидент ИБ или команду на оповещение пользователя о срабатывании правила корреляции. Инциденты ИБ и оповещения о срабатывании правила корреляции фиксируются в БД сервера Visor. При выполнении анализа событий ИБ в ручном режиме, «подозрительная» последовательность событий ИБ может быть отмечена пользователем как инцидент ИБ, т.е. инцидент может быть создан вручную, без помощи правила корреляции.

Через интерфейсы веб-приложения пользователям Visor предоставляется доступ к обрабатываемой информации. Доступ пользователей к веб-интерфейсу сервера Visor осуществляется через функционирующую на сервере службу IIS. Информация об учетных

записях пользователей Visor храниться в БД сервера. Создание, изменение и удаление учетных записей пользователей выполняется администратором (системным программистом) через веб-интерфейс сервера Visor. Кроме того, через веб-интерфейс пользователи системы Visor: получают оповещения и визуальную информацию о выявленных событиях и инцидентах информационной безопасности; могут формировать по запросу статистические отчеты по любому из предустановленных шаблонов отчетов. При формировании отчета выполняется соответствующий запрос к БД сервера для извлечения запрошенных данных.

Агенты устанавливаются на защищаемые активы (рабочие станции и серверы) организации. После установки агент выполняет процедуру подключения к серверу Visor и далее постоянно выполняет сбор событий ИБ из журналов источников и дополнительных данных. Агент осуществляет сбор данных о событиях ИБ из журналов источников, произошедших после установки агента. Собранные данные частично нормализуются и хранятся в локальной БД агента на узле, где установлен агент.

Агент может выполнять поступающие от сервера Visor управляющие задачи:

- выполнение сканирования сети;
- блокировка и разблокировка учетных записей пользователей ОС;
- обновление версии агента;
- удаление агента.

Результаты выполнения данных операций фиксируются в локальной БД агента.

С заданной периодичностью агент передает данные из локальной БД серверу Visor или агент-коллектору. Частота и объем передачи данных, IP-адрес назначения для передачи и другие параметры функционирования агентов или агентов-коллекторов задаются в их конфигурационных файлах. Конфигурационные файлы агентов создаются при настройке Visor. В конфигурационных файлах могут быть заданы индивидуальные параметры для каждого агента или агент-коллектора.

Агент-коллектор устанавливается на промежуточные узлы организации, имеющие доступ в подсети с установленными агентами, к которым не имеет доступа сервер. По сравнению с агентом, структура агент-коллектора дополнена модулем, осуществляющем трансляцию данных и управляющих задач от сервера Visor к агентам, недоступным для сервера.

Агент-коллектор выполняет переадресацию данных в обе стороны в случае сетевой доступности адресата. В случае отсутствия связи передача данных выполняется при восстановлении сетевой доступности.

Ограничения, установленные в конфигурационном файле агент-коллектора на объем и частоту передаваемых данных, распространяются только на передачу данных агент-коллектором и не влияют на передачу данных другими агентами.

Модуль сбора событий из БД устанавливается на ЭВМ (сервер Visor, ЭВМ с функциями сервера, ПЭВМ, виртуальную машину) в организации. После установки модуль выполняет процедуру подключения к серверу Visor и далее ожидает управляющих действий со стороны сервера.

На сервере Visor через веб-интерфейс создаются конфигурации с параметрами подключения к различным базам данных. Модуль получив конфигурацию от сервера начинает выполнять периодическое подключение и сбор к внешней базе данных в соответствии с параметрами, полученными от сервера. Модуль осуществляет сбор данных из БД, произошедших после установки агента. Собранные данные хранятся в локальной БД модуля на узле, где установлен агент.

Модуль может выполнять полученные от сервера Visor следующие управляющие задачи:

– создание, запуск, редактирование, проверка соединения, отключение и удаление конфигураций;

– включение, выключение, перезапуск и удаление (из веб-интерфейса) модуля.

2.3 Связи с другими программами

Visor взаимодействует с:

– веб-сервером IIS в части приёма HTTP-запросов от пользователей и обеспечения жизненного цикла ПО;

– СУБД PostgreSQL в части хранения и получения информации, используемой в работе;

– веб-браузером пользователя в части выдачи инструкций отображения пользовательского интерфейса и реакции на пользовательские команды.

3 НАСТРОЙКА ПРОГРАММЫ

Развертывание компонента сервер Visor может выполняться двумя способами:

а) Путем установки файла дистрибутива сервера Visor. Этот этап включает в себя:

1) настройка системного времени;
2) настройка параметров установки обновлений ОС Windows и другого ПО, при необходимости осуществляется установка обновлений компонент ОС;
3) установка и настройка системного и прикладного ПО;
4) установка средств защиты, применяемых в организации;
5) настройка межсетевых экранов;
6) установка файла дистрибутива сервера Visor.

б) Путем развертывания виртуальной машины с сервером Visor. Этот этап включает в себя следующие этапы:

1) Получение виртуальной машины с сервером Visor и учетных данных для входа от производителя;
2) Запуск виртуальной машины в среде Vmware;
3) Настройка системного времени;
4) Настройка параметров установки обновлений ОС Windows и другого ПО. Выполнение установки обновлений при необходимости;
5) Установка средств защиты, применяемых в организации;
6) Настройка межсетевых экранов;
7) Запуск сервисов и процессов сервера Visor.

Далее будут более подробно описаны этапы каждого из способов развертывания сервера платформы Visor.

3.1 Установка и настройка ОПО

3.1.1 Установка ОС

Перед развертыванием из файла дистрибутива сервера Visor, должны быть выполнены следующие подготовительные действия на аппаратном или виртуальном сервере, где будет выполняться установка сервера Visor:

– настройка системного времени;

– настройка параметров установки обновлений ОС Windows и другого ПО, при необходимости осуществляется установка обновлений компонент ОС;

Установка и настройка системного и прикладного ПО:

– установка Microsoft .NET Framework;

– установка PostgreSQL;

– установка и настройка средств защиты (средства защиты применяются в соответствии с политиками безопасности организации);

– настройка межсетевых экранов.

Только после выполнения подготовительных действий следует перейти к развертыванию сервера Visor из файла дистрибутива.

Далее будут описаны каждый из этапов подготовки сервера перед развертывание дистрибутива Visor.

3.1.2 Настройка системного времени

До установки сервера Visor необходимо выполнить проверку настройки системного времени в ОС Windows. Оно должно быть синхронизировано с используемым в ЛВС организации NTP-сервером, заданное время должно соответствовать текущему времени в текущем гео-расположении.

В противном случае, записи в журналах источников событий и БД Visor будут иметь некорректное время и в таком виде будут храниться и отображаться в веб-интерфейсе Visor. Некорректное время происхождения событий сильно затрудняет или делает невозможным процесс расследования и обнаружения инцидентов ИБ.

Следует всегда поддерживать настройки системного времени на сервере Visor и защищаемых активах в актуальном состоянии и отслеживать внесение изменений, с целью не допустить несанкционированного изменения системного времени.

3.1.3 Настройка параметров обновлений установки обновлений в ОС

До установки сервера Visor необходимо выполнить настройку установки обновлений ОС Windows и другого ПО. Настройки должны соответствовать принятым в организации политикам установки обновлений.

После настройки необходимо выполнить установку необходимых обновлений ОС и другого ПО.

Все компоненты Visor не предъявляют никаких ограничений к установки каких-либо обновлений в рамках поддерживаемых версий.

3.1.4 Установка Microsoft .NET Framework

Для установки Microsoft .NET Framework 4.5.1 необходимо скачать с официального сайта Microsoft соответствующий дистрибутив и запустить установщик от имени администратора.

3.1.5 Установка PostgreSQL

Установка PostgreSQL должна выполняться на том же сервере, где будет расположен сервер Visor.

Для установки PostgreSQL необходимо загрузить дистрибутив PostgreSQL версии 9.6 с официального сайта и запустить установщик от имени администратора. Далее следовать инструкциям на экране.

После успешной установки необходимо выполнить перезагрузку.

Установка и настройка PostgreSQL производится в соответствии с программно-эксплуатационной документацией PostgreSQL 9.6, расположенной на официальном сайте PostgreSQL

При выполнении установки сервера Visor из файла дистрибутива потребуется ввести имя или IP-адрес и данные учетной записи пользователя, от имени которой мастер установки Visor выполнить создание базы данные сервера Visor. Учетной записи данного пользователя должна быть назначена роль «sysadmin».

3.1.6 Установка и настройка средств защиты, применяемых в организации

На сервере Visor должны быть установлены и настроены средства защиты информации, применяемые в организации в соответствии с ее политиками безопасности.

При настройке антивирусных средств защиты рекомендуется исключить из периодического сканирования:

а) БД Visor;

б) Процессы Visor:

1) AgentService.exe;
2) AgentUninstaller.exe;
3) MonitoringService.exe;

4) Analytics.Host.exe;
5) Syslog.Server.Host.exe.

3.1.7 Настройка межсетевых экранов

Если на сервере Visor должен быть включен какой-либо межсетевой экран (VipNet, модуль Антивируса Касперского, Брандмауэр ОС Windows и т.п.), то в его настройках необходимо открыть входящие и исходящие соединения:

для процесса «AgentService.exe» по TCP-порту 22234 с подсетями, где располагаются защищаемые активы;

для процесса «AgentUninstaller.exe» по TCP-порту 22235, с подсетями, где располагаются защищаемые активы.

3.2 Установка сервера Visor

Для установки необходимо использовать соответствующий установочный файл дистрибутива.

Скопируйте и запустите установочный файл дистрибутива на локальном жестком диске сервера Visor. Вы должны увидеть приветственное окно мастера установки:

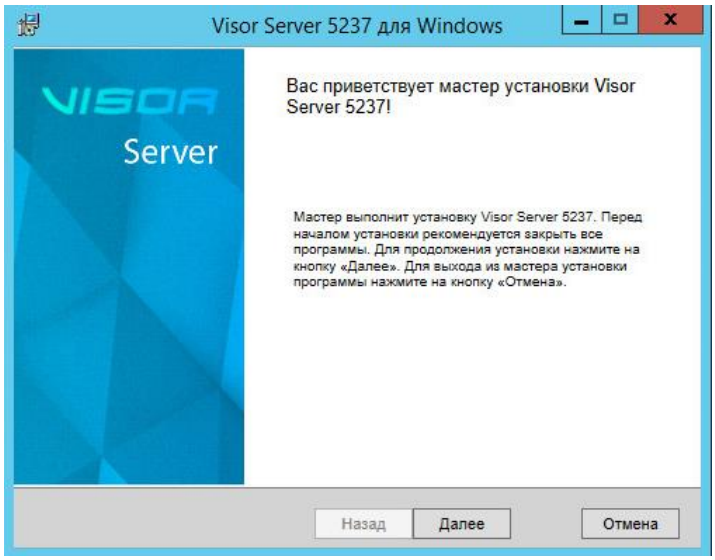

Рисунок 1 - Приветственное окно мастера установки сервера Visor

Для продолжения установки нажмите кнопку Далее.

В следующем окне прочтите условия лицензионного соглашения использования ПО Visor, установите флажок «Я принимаю условия лицензионного соглашения», если вы с ним согласны и нажмите кнопку Далее.

На следующем этапе мастер установки Visor выведет результаты проверки соответствия аппаратной конфигурации сервера минимальным рекомендуемым требованиям.

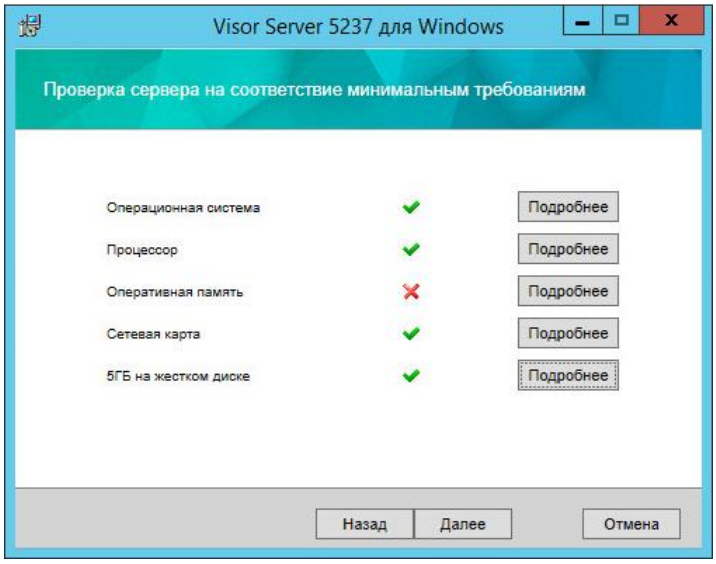

Рисунок 2 - Окно проверки на соответствия минимальным требованиям

На следующем окне вы должны задать папку, в которую будет выполнена установка сервера Visor:

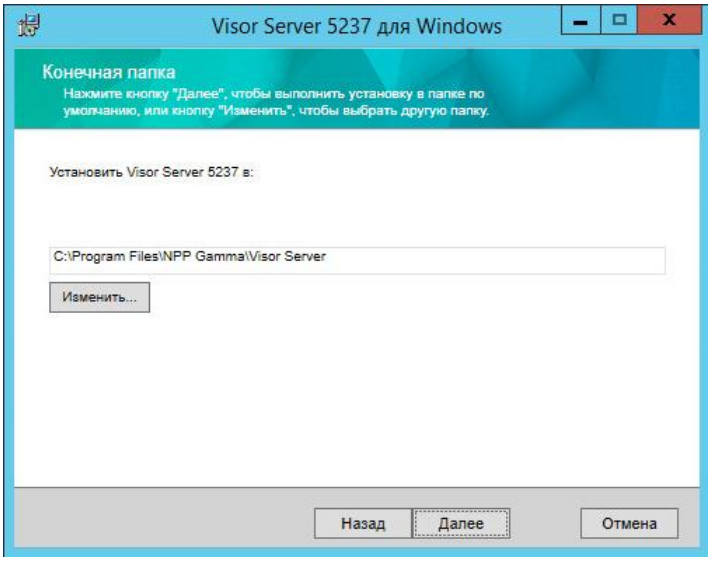

Рисунок 3 - Окно выбора расположения установки сервера Visor

В следующем окне требуется указать параметры для подключения к базе данных для создания мастером установки БД сервера Visor:

– имя или IP-адрес сервера баз данных;

– тип аутентификации при подключении;

– имя пользователя (учетной записи пользователя должна быть назначена роль «sysadmin»);

– пароль пользователя.

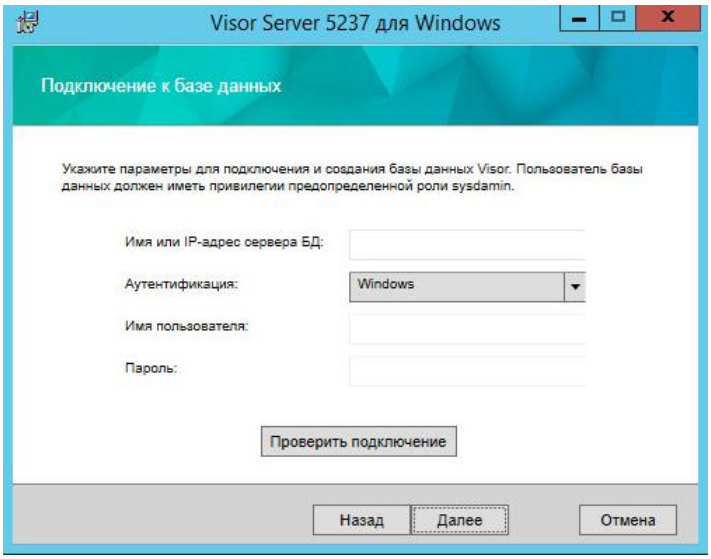

Рисунок 4 - Окно подключения к базе данных

На следующем этапе укажите учетные данные пользователя, который будет использоваться Администратором Visor для входа в веб-интерфейс сервера Visor. Пароль должен быть задан в соответствии с выставленными требованиями к его сложности.

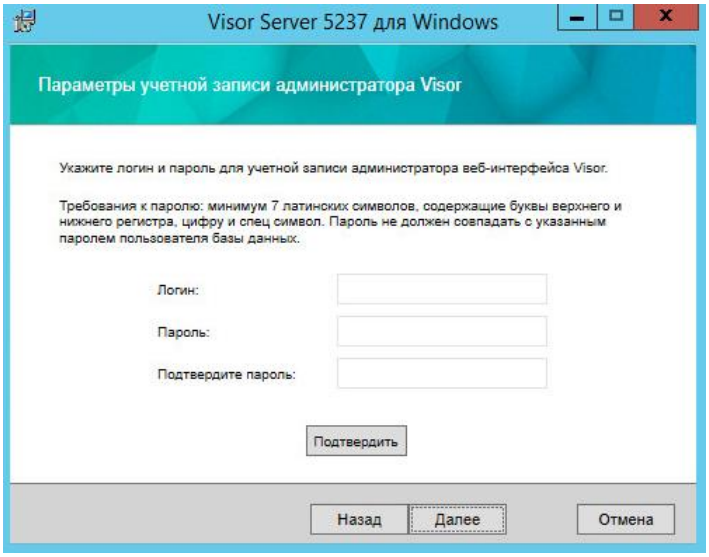

Рисунок 5 - Окно задания параметров учетной записи

Администратора веб-интерфейса Visor

Для продолжения установки нажмите кнопку «Установить». Мастер установки приступит к развертыванию файлов в указанное ранее расположение папки.

В ходе установки сервера Visor будут включены или установлены необходимые компоненты ОС Windows Server.

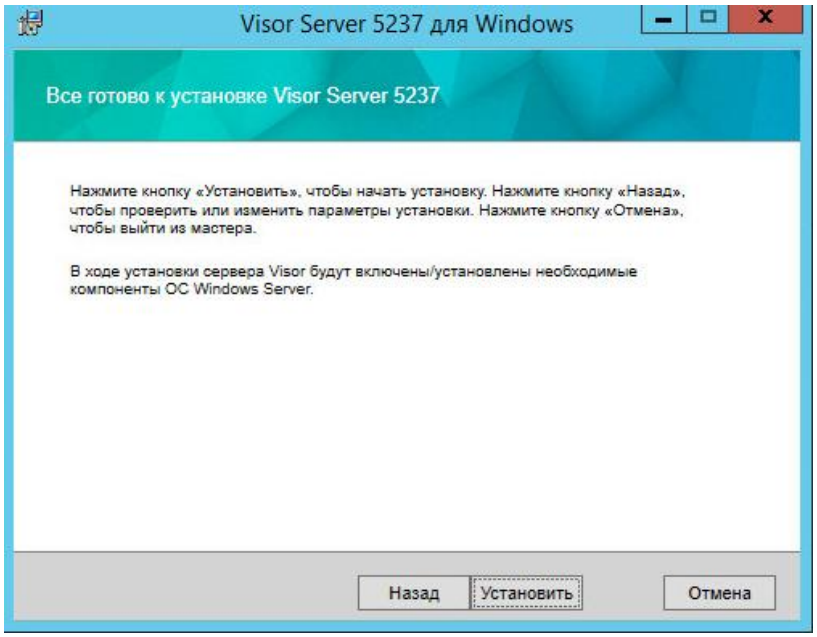

Рисунок 6 - Окно подготовки к установке сервера Visor

На следующем окне будет отображаться процесс выполнения этапов установки дистрибутива.

В следующем окне нажмите кнопку «Готово», чтобы завершить установку сервера Visor.

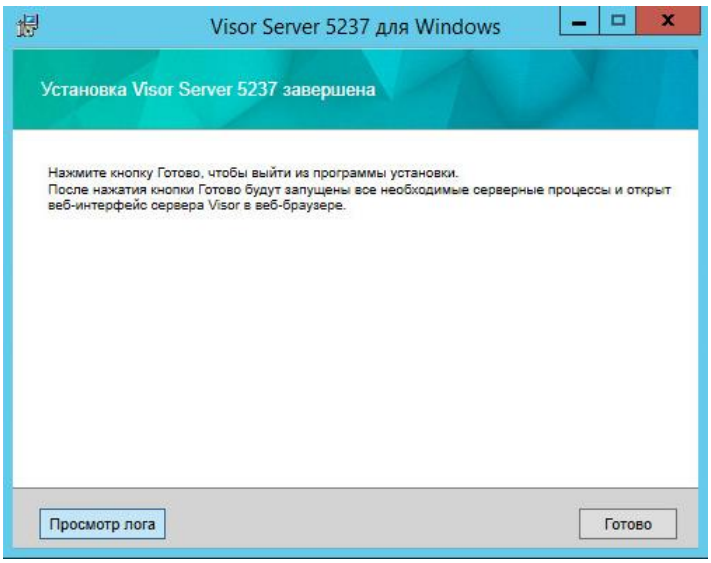

Рисунок 7 - Окно завершения установки сервера Visor

После завершения установка автоматически запустится служба «Visor Server Watcher», которая автоматически запустит следующие консольные приложения:

– серверное приложение Visor – «MonitoringService.exe»;

– приложение модуля анализа Visor – «Analytics.Host.exe»;

– приложение syslog-сервера Visor – «Syslog.Server.Host.exe».

– Чтобы убедиться, что установка сервера Visor прошла успешно, после выполнения установки можно проверить:

– все консольные приложения запущены;

– работает ли служба «Server Watcher»;

– вход в веб-интерфейс Visor от имени учетной записи Администратора Visor (созданной в ходе установки) выполняется успешно.

3.3 Установка виртуальной машины на ЭВМ в составе АС

3.3.1 Развертывание виртуальной машины с сервером Visor

Сервер Visor может быть быстро развернут посредством предоставляемой производителем виртуальной машины, содержащей предварительно установленный и настроенный сервер Visor.

Развертывание виртуальной машины включает в себя следующие этапы:

Получение виртуальной машины с сервером Visor и учетных данных для входа от производителя;

Запуск виртуальной машины в среде Vmware;

Настройка системного времени;

Настройка параметров установки обновлений ОС Windows и другого ПО. Выполнение установки обновлений при необходимости;

Установка средств защиты, применяемых в организации;

Настройка межсетевых экранов;

Запуск сервисов и процессов сервера Visor

3.3.2 Получение виртуальной машины с сервером Visor

Для получения виртуальной машины с сервером Visor и учетных данных для входа в нее обратитесь к официальному представителю производителя Visor.

3.3.3 Запуск виртуальной машины в виртуальной среде Vmware

Для запуска виртуальной машины сервера Visor необходимо выполнить следующие действия:

1. Выполните установку ПО VMware Workstation Player:

http://www.vmware.com/products/player/playerpro-evaluation.html

2. Запустите ПО VMware Workstation Player:

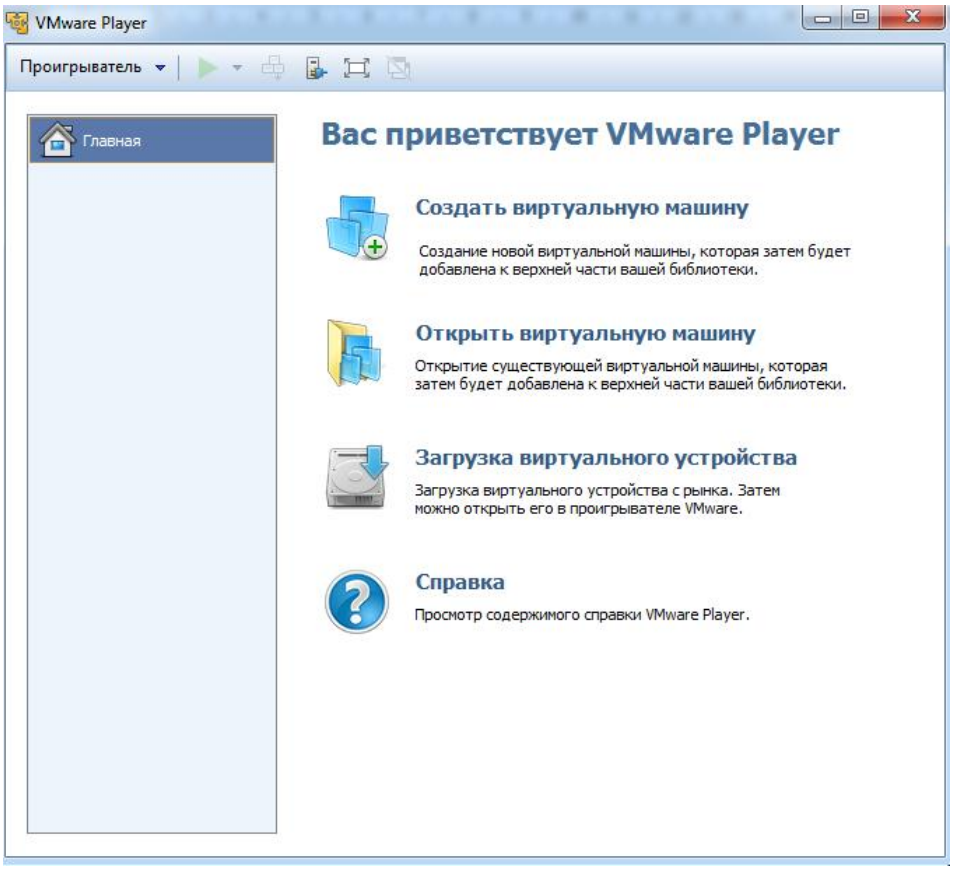

Рисунок 8 - Запуск ПО VMware Workstation Player

3. Откройте файл с предоставленной виртуальной машиной:

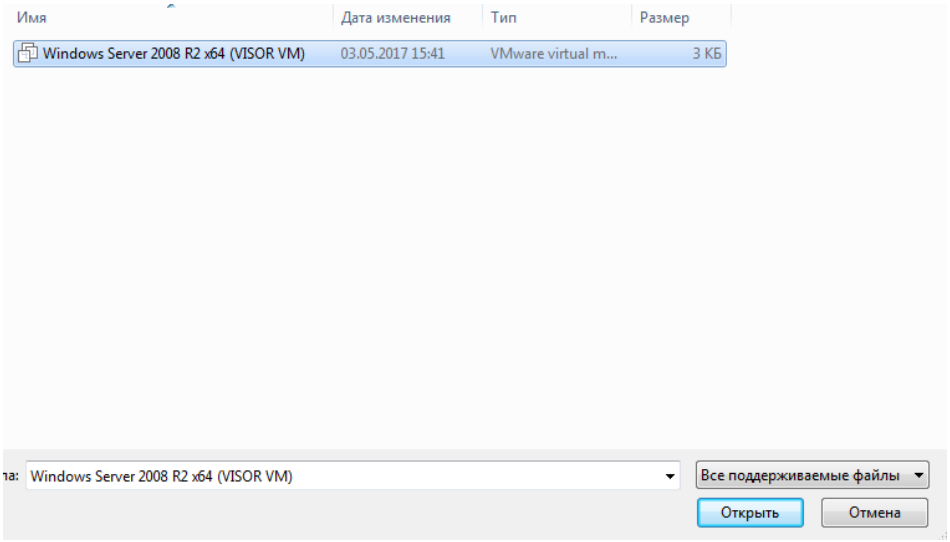

Рисунок 9 - Открытие файла с виртуальной машиной

3. Перед запуском виртуальной машины убедитесь, что настройки сетевого адаптера виртуальной машины соответствуют конфигурации сети, в которой развертывается сервер Visor.

4. Выполните запуск виртуальной машины Visor:

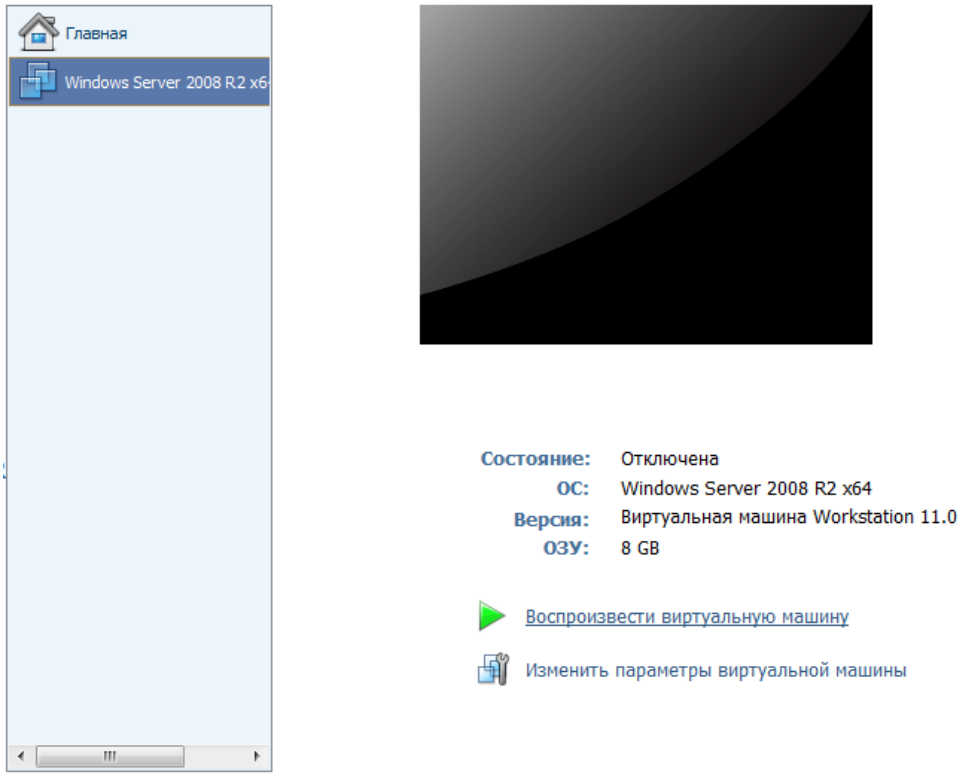

Рисунок 10 - Запуск виртуальной машины Visor

Для входа на виртуальной машине в ОС Windows и в веб-интерфейс Visor используйте данные от учетных записей, предоставленных производителем при передаче виртуальной машины.

3.3.4 Настройка системного времени

До запуска сервера Visor необходимо выполнить проверку настройки системного времени в ОС Windows. Оно должно быть синхронизировано с используемым в ЛВС организации NTP-сервером, заданное время должно соответствовать текущему времени в текущем гео-расположении.

В противном случае, записи в журналах источников событий и БД Visor будут иметь некорректное время и в таком виде будут храниться и отображаться в веб-интерфейсе

Visor. Некорректное время происхождения событий сильно затрудняет или делает невозможным процесс расследования и обнаружения инцидентов ИБ.

Следует всегда поддерживать настройки системного времени на сервере Visor и защищаемых активах в актуальном состоянии и отслеживать внесение изменений, с целью не допустить несанкционированного изменения системного времени.

3.3.5 Настройка параметров установки обновлений ОС Windows и другого ПО

До установки сервера Visor необходимо выполнить настройку установки обновлений ОС Windows и другого ПО. Настройки должны соответствовать принятым в организации политикам установки обновлений.

После настройки необходимо выполнить установку необходимых обновлений ОС и другого ПО.

Все компоненты Visor не предъявляют никаких ограничений к установки каких-либо обновлений в рамках поддерживаемых версий.

3.3.6 Установка и настройка средств защиты, применяемых в организации

На виртуальной машине с сервером Visor должны быть установлены и настроены средства защиты информации, применяемые в организации в соответствии с ее политиками безопасности.

При настройке антивирусных средств защиты рекомендуется исключить из периодического сканирования:

а) БД Visor;

б) Процессы Visor:

1) AgentService.exe;
2) AgentUninstaller.exe;
3) MonitoringService.exe;
4) Analytics.Host.exe;
5) Syslog.Server.Host.exe.

3.3.7 Настройка межсетевых экранов

Если на сервере Visor должен быть включен какой-либо межсетевой экран (VipNet, модуль Антивируса Касперского, Брандмауэр ОС Windows и т.п.), то в его настройках необходимо открыть входящие и исходящие соединения:

для процесса «AgentService.exe» по TCP-порту 22234 с подсетями, где располагаются защищаемые активы;

для процесса «AgentUninstaller.exe» по TCP-порту 22235, с подсетями, где располагаются защищаемые активы.

3.3.8 Запуск сервисов и консольных приложений сервера Visor

После включения виртуальной машины с сервером VISOR необходимо вручную запустить сервисы Visor. Порядок выполнения запуска сервисов Visor описан в разделе 4.1.3 «Порядок включения, выключения и перезагрузки сервера Visor».

3.3.9 Порядок включения, выключения и перезагрузки сервера Visor

Для включения компонентов сервера Visor необходимо:

а) Включить питание сервера, на котором была выполнена установка сервера Visor;

б) Загрузить ОС Windows Server;

в) После запуска ОС Windows Server должна автоматически запуститься служба «Visor Server Watcher», которая автоматически запустит следующие консольные приложения:

1) серверное приложение «MonitoringService.exe»;
2) приложение модуля анализа «Analytics.Host.exe»;
3) приложение syslog-сервера «Syslog.Server.Host.exe»;

г) Если служба «Visor Server Watcher» автоматически не запустилась, выполнить ее запуск вручную в меню служб ОС Windows Server.

д) Для вызова веб-интерфейса Visor перейти в веб-браузере по URL с IP-адресом сервера Visor;

е) Ввести имя учетной записи Visor и пароль для входа в веб-интерфейс Visor.

ж) Для остановки работы сервера Visor нужно остановить работу службы «Visor Server Watcher» затем закрыть консольные приложения в любой последовательности:

1) MonitoringService.exe;
2) Analytics.Host.exe;
3) Syslog.Server.Host.exe.

Для перезагрузки сервера Visor необходимо остановить работу службы «Visor Server Watcher» затем закрыть консольные приложения в любой последовательности:

– MonitoringService.exe;
– Analytics.Host.exe;
– Syslog.Server.Host.exe.

После этого заново включить службу «Visor Server Watcher».

3.4 Настройка соединения сервера Visor с SMTP-серверами

Сервер Visor может рассылать оповещения почтовым адресатам по e-mail при срабатывании правил корреляции, если данная реакция включена в правилах корреляции.

Для этого серверу Visor необходимо настроить конфигурацию подключения к SMTP-серверу, используемому в организации. Необходимо создать специализированную почтовую запись (почтовый ящик) на SMTP-сервере от имени которого платформа Visor будет рассылать e-mail оповещения.

После создания учетной записи на SMTP-сервере, используемом в вашей организации, выполните вход в меню «Настройки» -> «SMTP» и нажмите кнопку «Создать конфигурацию».

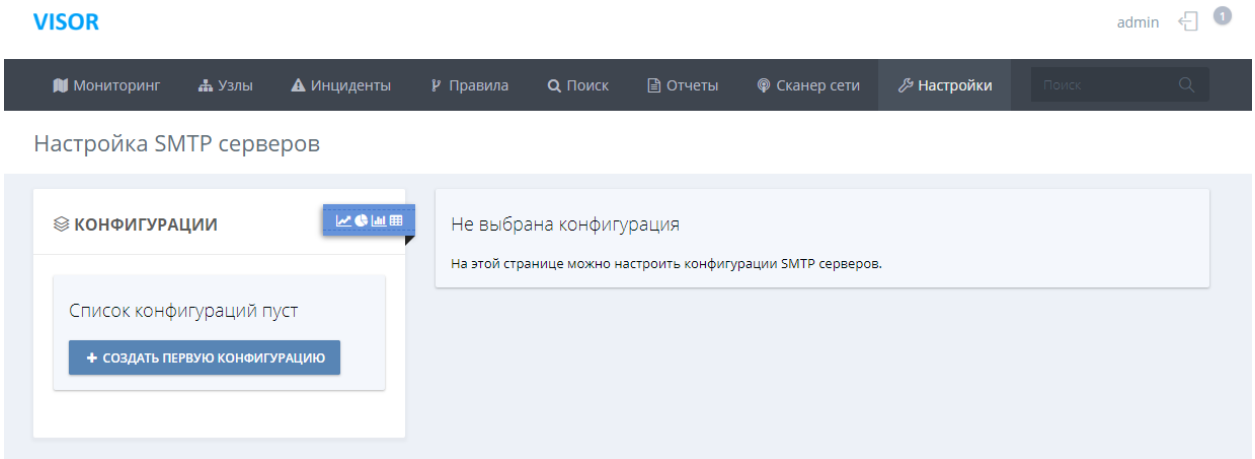

Рисунок 11 - Создание SMTP-конфигурации (1)

В появившемся справа паспорте конфигурации укажите параметры подключения к SMTP-серверу вашей организации, на котором была создана почтовая учетная запись для платформы Visor.

Нажмите кнопку «Сохранить» и сервер Visor выполнит проверку подключения к SMTP-серверу, в случае успешного соединения конфигурация сохранится.

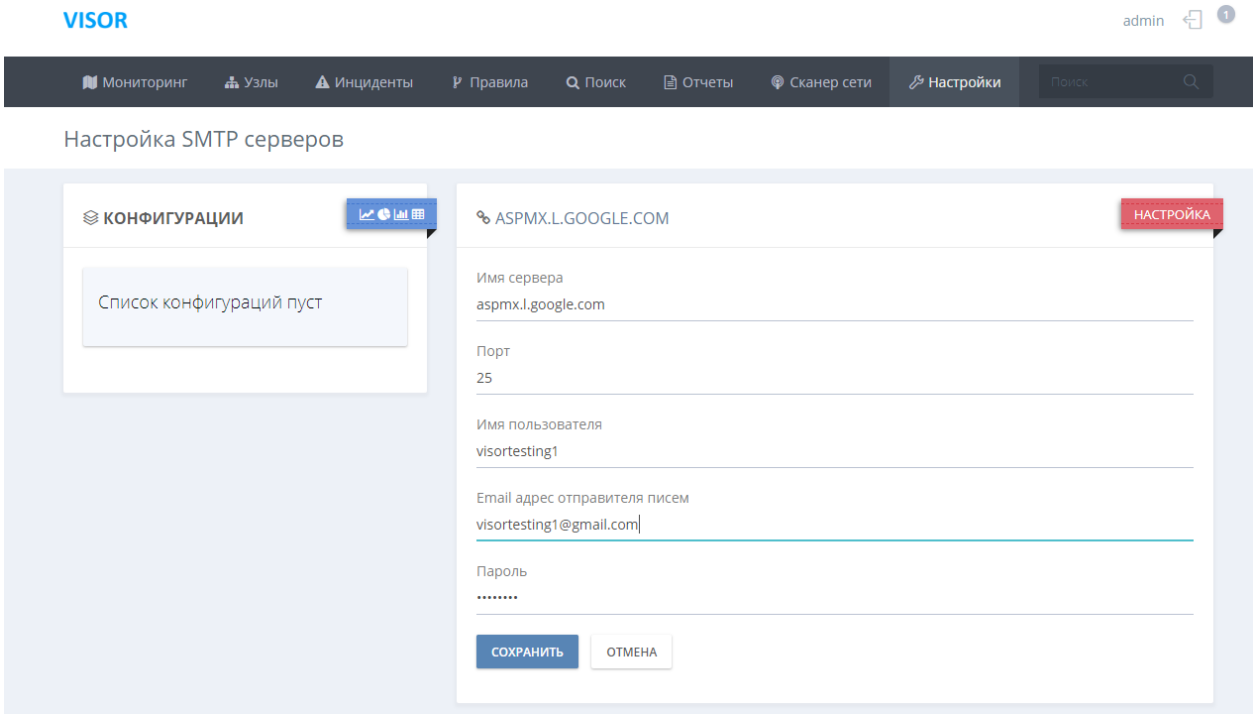

Рисунок 12 - Создание SMTP-конфигурации (2)

После этого Аналитик (Оператор) Visor может включать и настраивать реакцию оповещения по e-mail для правил корреляции.

3.5 Установка агентов и агентов-коллекторов

Установка компонентов агент или агент-коллектор Visor осуществляется в три последовательно выполняемых этапа:

1) настройка источников событий ИБ на защищаемых активах;
2) подготовка защищаемого актива к установке агента или агента-коллектора;
3) распространение агентов или агент-коллекторов Visor на защищаемые активы.

Первые два этапа: настройка источников событий ИБ и подготовка защищаемого актива к установке агента или агент-коллектора Visor, производится на каждом активе либо непосредственно, либо дистанционно, если это позволяют технические возможности, настройки средств защиты информации и политики безопасности организации.

Третий этап может выполняться либо непосредственно на каждом защищаемом активе, либо дистанционно с сервера Visor также в отношении каждого актива. Так же

распространение дистрибутива агентов или агент-коллекторов Visor может быть выполнено посредством доменных политик Active Directory.

Установленный на защищаемом активе агент или агент-коллектор автоматически запускается в фоновом режиме службой AgentService после загрузки ОС Windows.

Далее будут подробно описаны каждый из этапов установки.

3.6 Установка агента, агента-коллектора в ручном режиме

Подготовка защищаемого актива к установке агента или агент-коллектора включает в себя:

- установку на защищаемом активе ПО Microsoft .NET Framework 4.5.1 или выше;
- настройка системного времени ОС Windows;
- настройку межсетевого экрана на активе.

3.6.1 Установка Microsoft .NET Framework

Для работы агента или агент-коллектора Visor требуется наличие ПО Microsoft .NET Framework 4.5.1 или выше.

Для установки Microsoft .NET Framework 4.5.1 необходимо скачать с официального сайта Microsoft соответствующий дистрибутив и запустить установщик от имени администратора.

После успешной установки возможно потребуется выполнить перезагрузку защищаемого актива.

3.6.2 Настройка системного времени ОС Windows

До установки агента или агент-коллектора необходимо выполнить проверку настройки системного времени в ОС Windows. Оно должно быть синхронизировано с используемым в ЛВС организации NTP-сервером, заданное время должно соответствовать текущему времени в текущем гео-расположении.

В противном случае, записи в журналах источников событий будут иметь некорректное время и в таком виде будут храниться и отображаться в веб-интерфейсе Visor. Некорректное время происхождения событий сильно затрудняет или делает невозможным процесс расследования и обнаружения инцидентов ИБ.

Следует всегда поддерживать настройки системного времени на защищаемых активах в актуальном состоянии и отслеживать внесение изменений, с целью не допустить несанкционированного изменения системного времени.

3.6.3 Требования к настройке межсетевого экрана на защищаемом активе

Если на защищаемом активе включен какой-либо межсетевой экран (VipNet, модуль Антивируса Касперского, Брандмауэр ОС Windows и т.п.), то в его настройках необходимо открыть входящие и исходящие соединения:

для процесса «AgentService.exe» по TCP-порту 22234;

для процесса «AgentUninstaller.exe» по TCP-порту 22235.

3.6.4 Установка агента или агент-коллектора Visor

Развертывание агента или агент-коллектора Visor на защищаемом активе может быть выполнено одним из 3-х способов:

– вручную на защищаемом активе;
– дистанционно, при помощи веб-интерфейса Visor;
– дистанционно, при помощи доменных политик Active Directory.

Во всех случаях в ходе установки потребуется указать следующие параметры для установки:

а) путь для установки файлов дистрибутива;

б) IP-адрес сервера Visor (если защищаемый актив имеет сетевой доступ к серверу Visor) или агент-коллектора (если защищаемый актив расположен за прокси-узлом и не имеет сетевого доступа к серверу Visor);

в) параметры конфигурационного файла агента или агент-коллектора Visor. Конфигурационный файл определяет следующие параметры функционирования:

1) максимальный размер локальной БД агента или агент-коллектора для хранения событий;

2) ежедневный лимит обмена трафиком с сервером в Мбайтах;

3) временной интервал между отправками пакетов данных серверу Visor;

4) количество событий, отправляемых в одном пакете;

5) временной интервал между отправками дополнительных данных серверу Visor об аппаратной конфигурации защищаемого актива, установленных параметрах настройки ОС Windows и других данных о защищаемом активе.

3.6.5 Установка агента или агент-коллектора вручную на защищаемом активе

Для установки необходимо использовать соответствующий установочный файл дистрибутива.

Скопируйте и запустите установочный файл дистрибутива на локальном жестком диске защищаемого актива. Вы должны увидеть приветственное окно мастера установки:

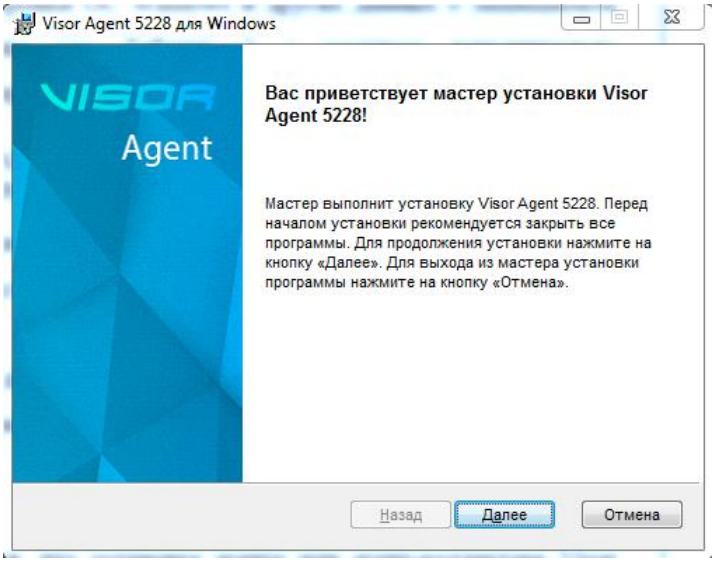

Рисунок 13 - Приветственное окно мастера установки

Для продолжения установки нажмите кнопку Далее.

В следующем окне прочтите условия лицензионного соглашения использования ПО Visor, установите флажок «Я принимаю условия лицензионного соглашения», если вы с ним согласны и нажмите кнопку Далее.

В следующем окне вы должны задать папку, в которую будет выполнена установка агента или агент-коллектора Visor:

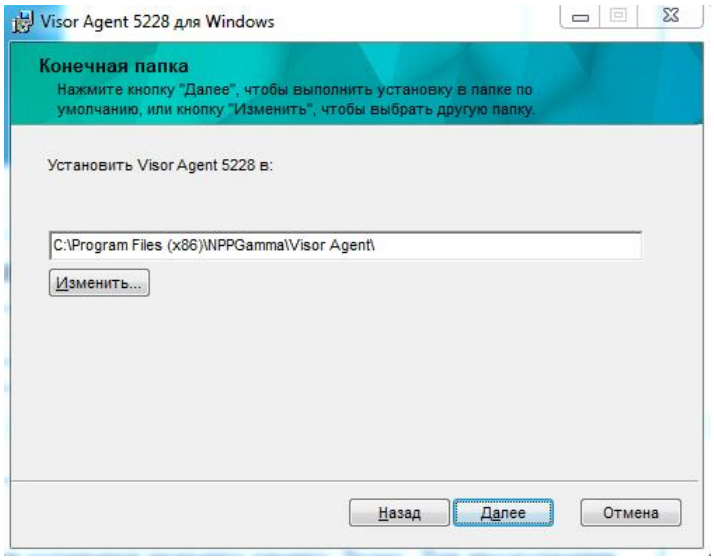

Рисунок 14 - Окно выбора расположения установки

В следующем окне требуется указать IP-адрес и порт сервера или агент-коллектора (если защищаемый актив находится за прокси-узлом). На данный IP-адрес и порт агент будет отправлять собираемые события ИБ и дополнительные данные о защищаемом активе. По умолчанию всегда используется TCP-порт 22235, вы можете не указывать порт, если вы не используете иной номер порта.

В этом же окне укажите тип устанавливаемого агента: агент или агент-коллектор.

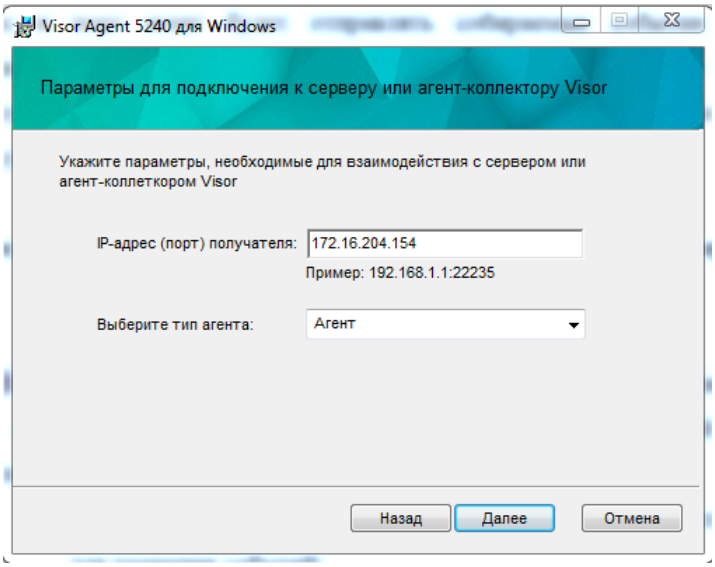

Рисунок 15 - Окно задания IP-адрес сервера или агент-коллектора для отправки событий ИБ, выбор типа устанавливаемого агента

В следующем окне требуется указать параметры конфигурационного файла агента или агент-коллектора Visor. Конфигурационный файл определяет следующие параметры функционирования:

– временной интервал между отправками пакетов данных серверу Visor;

– количество событий, отправляемых в одном пакете;

– ежедневный лимит обмена трафиком с сервером в Мбайтах;

– максимальный размер локальной БД агента или агент-коллектора для хранения событий;

– временной интервал между отправками дополнительных данных серверу Visor о конфигурации защищаемого актива.

Вы можете оставить значения параметров по умолчанию и внести изменения в конфигурационный файл позже, после завершения установки.

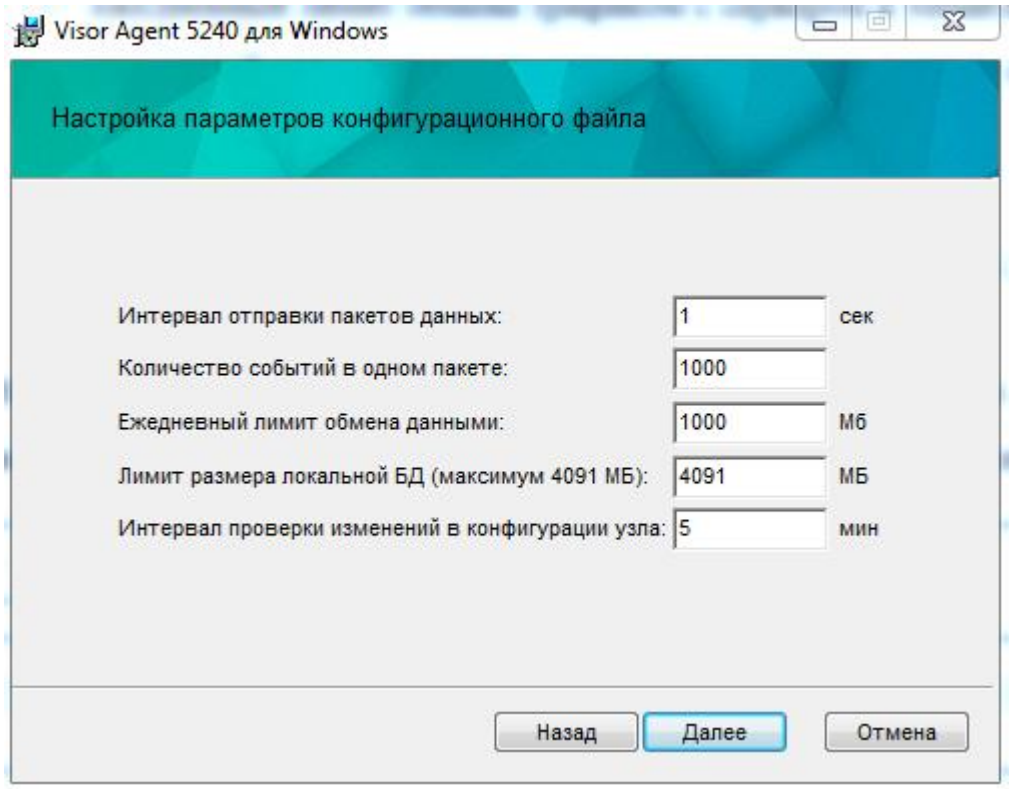

Рисунок 16 - Указание параметров конфигурационного файла агента или агент-коллектора

Для продолжения установки нажмите кнопку «Установить». Мастер установки приступит к развертыванию файлов в указанное ранее расположение папки.

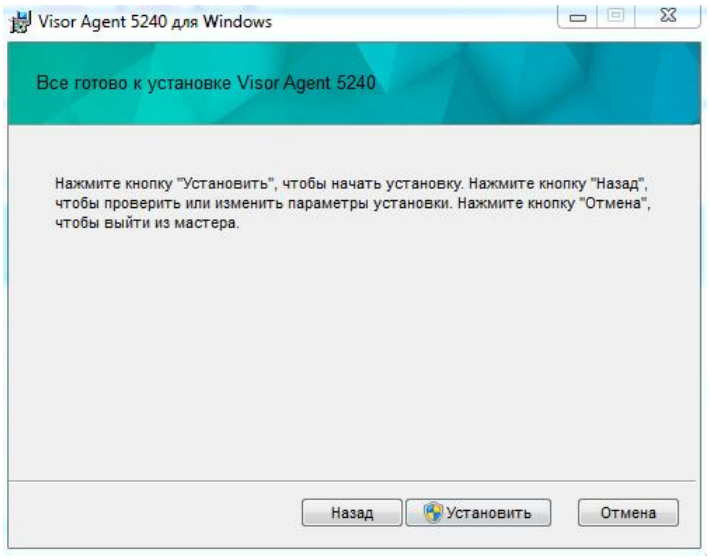

Рисунок 17 - Окно подготовки к установке

На следующем окне будет отображаться процесс выполнения этапов установки дистрибутива.

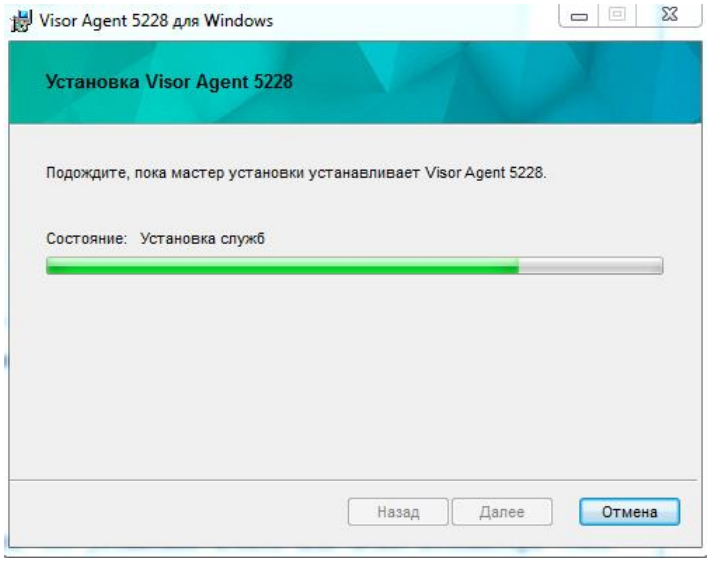

Рисунок 18 - Окно отображения этапов установки

В следующем окне нажмите кнопку «Готово», чтобы завершить установку агента или агент-коллектора Visor.

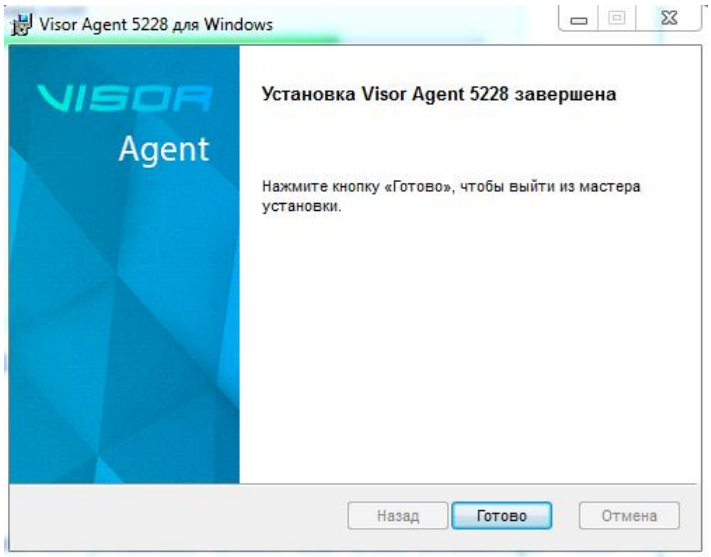

Рисунок 19 - Окно завершения установки

После успешной установки агента или агент-коллектора необходимо выполнить проверку его подключения к серверу Visor. Для этого выполните подключение к веб-интерфейсу сервера Visor.

В веб-интерфейсе в меню «Узлы» через некоторое время (при наличии стабильной сетевой связи и отсутствии проблем, в течение 1-2-х минут) должны появиться данные, собранные подключаемым агентом или агент-коллектором о защищаемом активе.

В меню «Поиск» при просмотре и фильтрации событий по данному активу должны быть доступны собранные события источников ИБ с данного защищаемом актива (с момента времени установки агента или агент-коллектора).

3.7 Установка агента, агента-коллектора через веб-интерфейс сервера Visor

Для дистанционной установки, при помощи веб-интерфейса Visor, будет использован дистрибутив, расположенный в папке «C:\Program Files (x86)\NPPGamma\ Visor Server\agent_bin» на жестком диске сервера платформы Visor. Данная папка создается автоматически, в ходе установки сервера Visor из дистрибутива и содержит дистрибутивы агентов и агент-коллекторов для распространения на защищаемые активы.

В процедуре удаленной установки агента или агент-коллектора участвует два узла. На первом узле – находится агент-установщик. Второй - целевой узел, куда будет установлен агент. Необходимо, чтобы на узле с агентом-установщиком была возможность создавать сетевой диск к целевому узлу. Только в этом случае будет работать удаленная

установка агента. Узел с агентом-установщиком выбирается случайным образом из тех узлов, которые удовлетворяют условиям, описанным выше.

Так же, на узле, на котором будет выполняться удаленная установка агента необходимо установить следующие параметры в реестре ОС Windows (групповых политиках):

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"LocalAccountTokenFilterPolicy"=dword:00000001

и

gpedit.msc - Конфигурация компьютера\Конфигурация Windows\Параметры Безопасности\Сетевая безопасность: уровень проверки подлинности LAN Manager

"Отправлять LM и NTLM ответы"

Для установки агента или агент-коллектора через веб-интерфейс Visor необходимо выполнить следующие действия:

Выполнить вход в веб-интерфейс Visor;

Выполнить вход в меню «Сканер сети»;

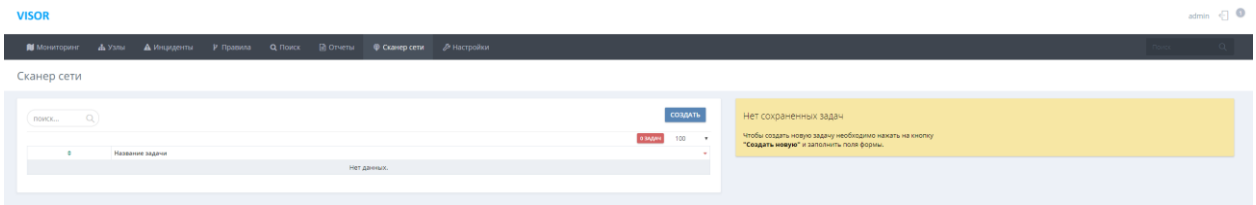

Рисунок 20 - Меню «Сканер сети»

Создать задачу сканирования.

Для того, чтобы Visor мог выполнить дистанционную установку агента или агент-коллектора на защищаемый актив, ему необходимо знать о присутствии данного актива в сети. Для этого в агент и агент-коллектор Visor встроен модуль Сканера сети, который позволяет выполнять сканирование сетевого окружения. Сканирование выполняется за счет назначения агентам или агент-коллекторам задач сканирования.

Для создания задачи 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 чекбокс «Начать сканирование сейчас», если хотите, чтобы задача начала выполнять сканирование сразу же после создания. Не устанавливайте данный чекбокс, если у выбранного агента или агент-коллектора имеется несколько сетевых интерфейсов, и вы не хотите выполнять полное сканирование всех доступных ему подсетей;

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

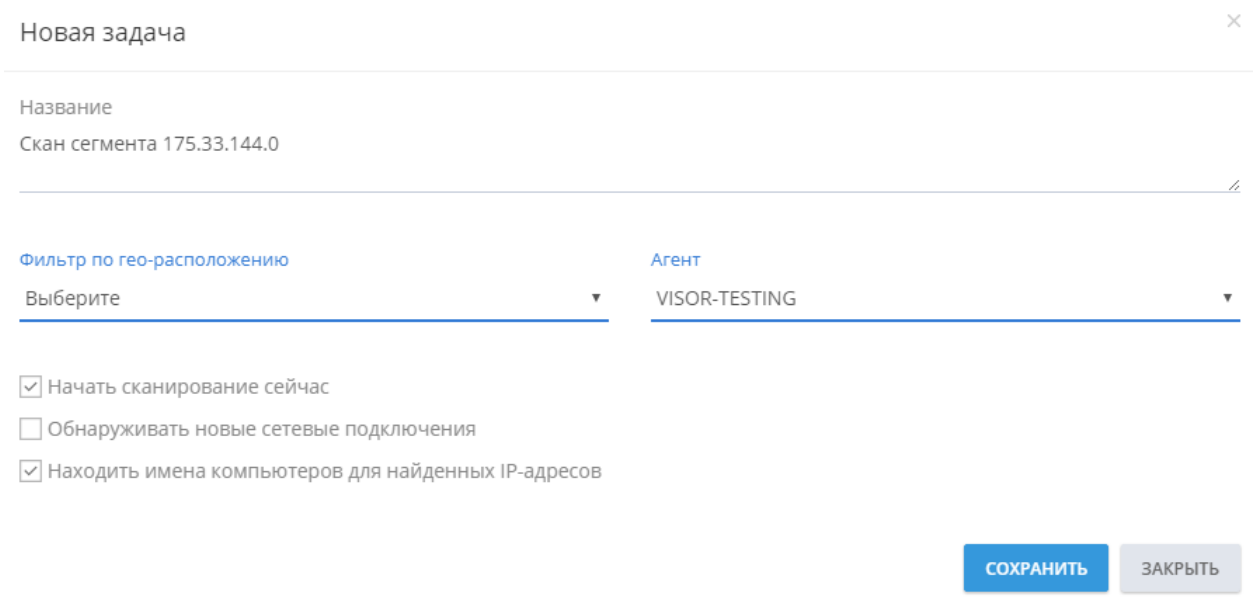

Рисунок 21 - Создание задачи сканирования

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

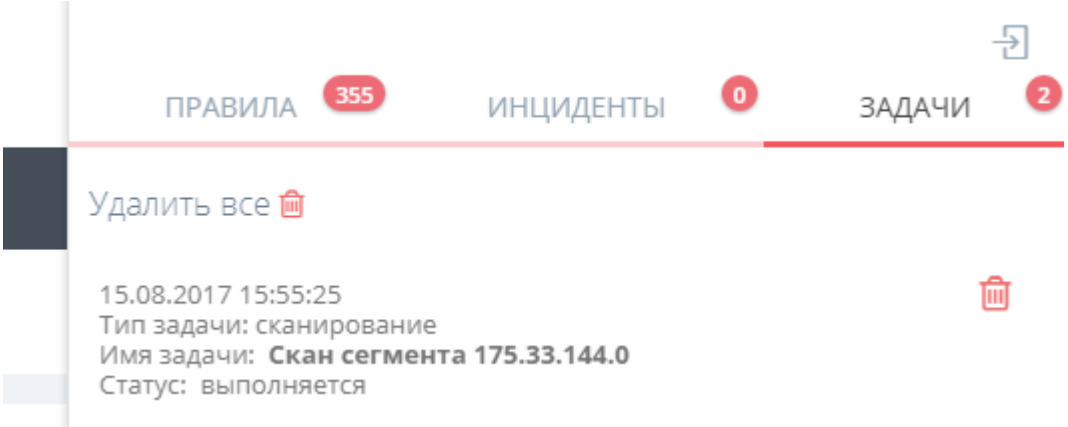

Рисунок 22 - Статус выполнения задачи сканирования

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 Visor, после этого нажмите кнопку «Добавить в узлы». Требуемый актив появится в таблице узлов в меню «Узлы».

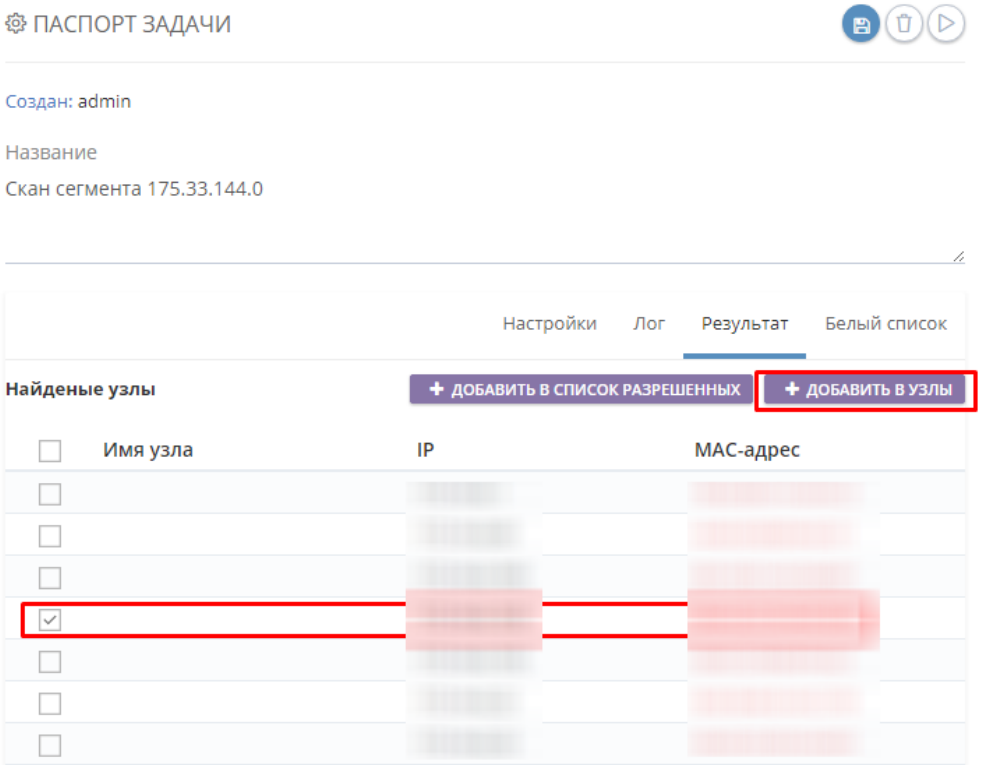

Рисунок 23 - Добавление найденного актива в меню «Узлы»

Войдите в меню «Узлы» и выберите слева в списке узлов только что добавленный актив.

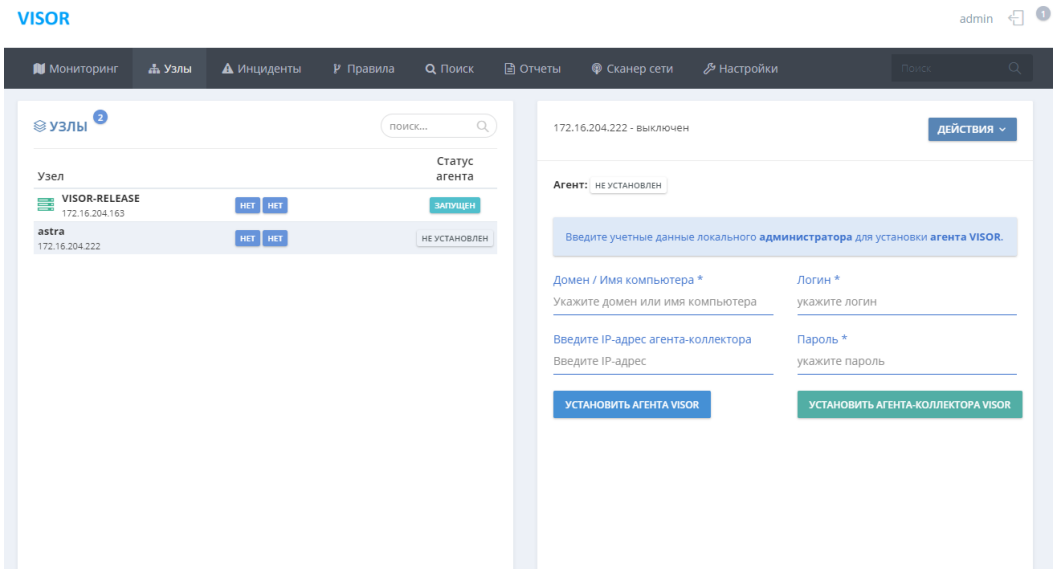

Рисунок 24 - Введение параметров для установки агента или агент-коллектора в паспорте

Справа, в паспорте выбранного актива введите:

данные учетной записи локального администратора для данного защищаемого актива;

введите IP-адрес агент-коллектора при необходимости (если вы устанавливаете агент на актив, расположенный за прокси-узлом);

Далее нажмите кнопку «Установить агента Visor» или «Установить агент-коллектора Visor» в зависимости от необходимости.

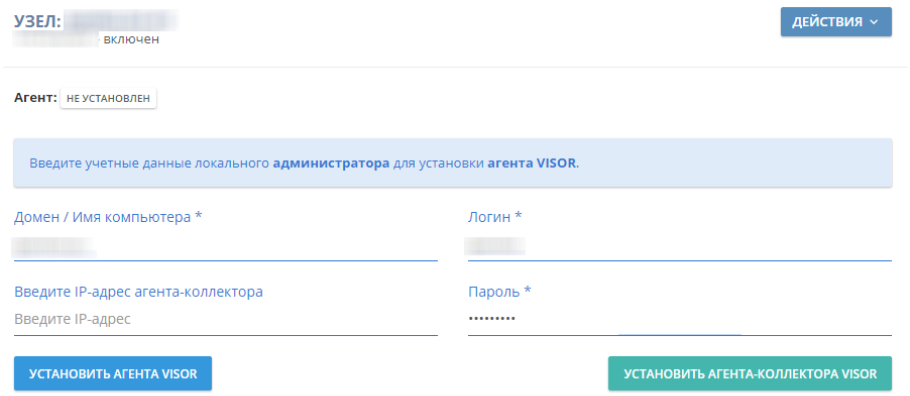

Рисунок 25 - Введение параметров для установки агента или агент-коллектора в паспорте

Далее будет отображен процесс установки агента или агент-коллектора на защищаемый актив. Так же будет отображен статус выполнения установки в Оповещениях на вкладке Задачи:

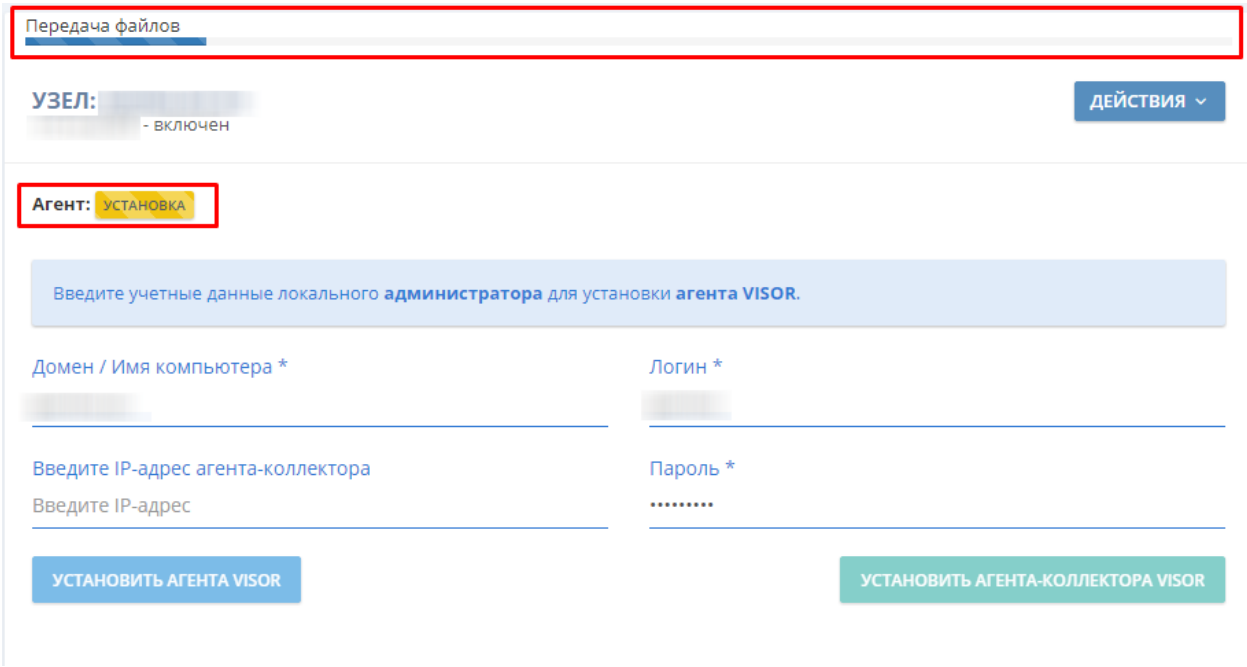

Рисунок 26 - Отображение статуса установки агента

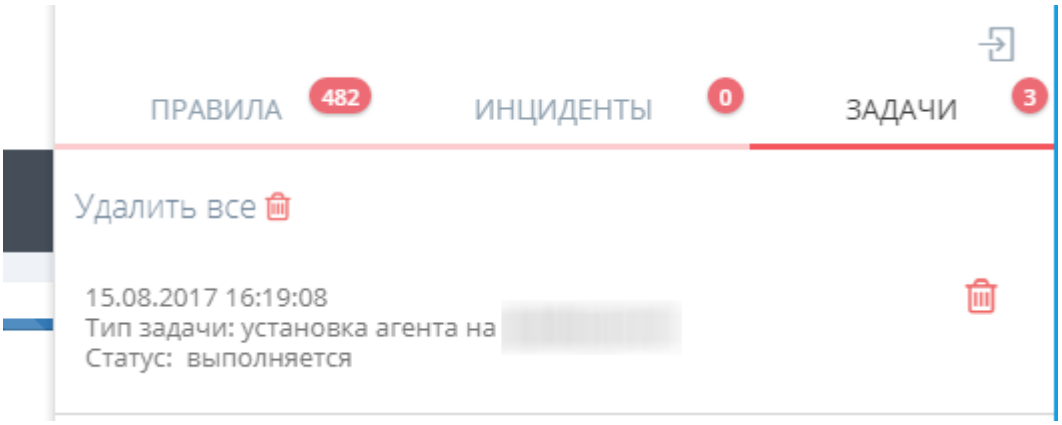

Рисунок 27 - Отображение статуса установки агента в Оповещениях на вкладке Задачи

После завершения установки в паспорте актива будет отображена собранная по активу информация. В Оповещениях на вкладке Задаче будет отображен статус завершения установки.

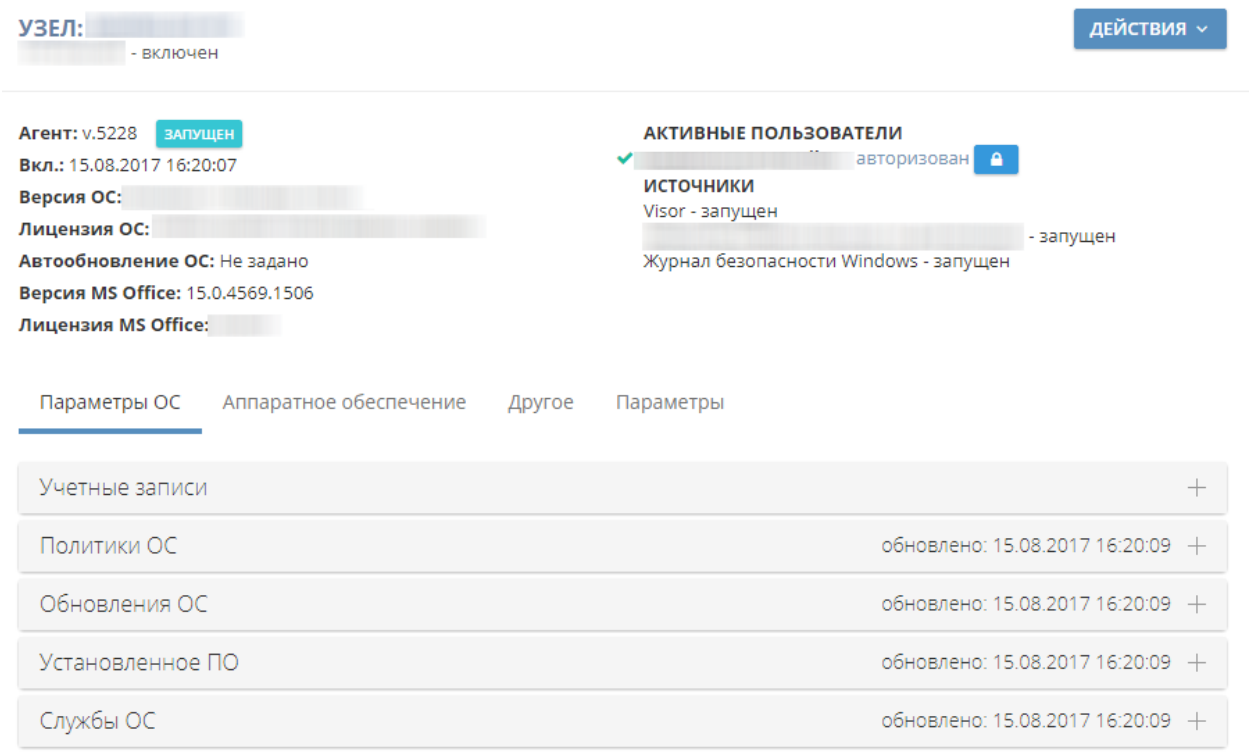

Рисунок 28 - Отображение собранных данных после завершения установки агента

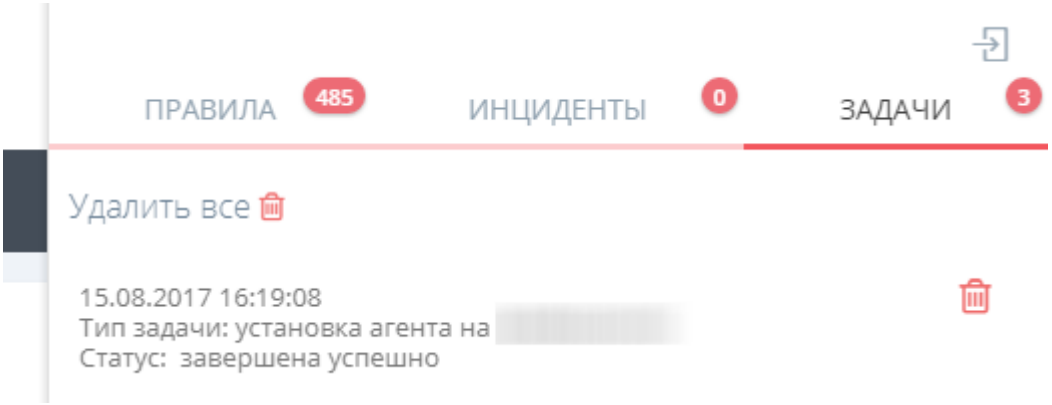

Рисунок 29 - Отображение статуса завершения установки в Оповещениях на вкладке Задачи

В результате этих действий на защищаемом активе будет установлен дистрибутив из папки «C:\Program Files (x86)\NPPGamma\ Visor Server\agent_bin\» с сервера Visor.

3.8 Установка агента, агента-коллектора с использованием доменных политик Active Directory

Для дистанционной установки, при помощи доменных политик Active Directory, необходимо использовать соответствующий установочный msi-пакет дистрибутива платформы Visor.

Вы можете использовать следующие установочные параметры для тихой установки msi-пакета при распространении агентов или агент-коллекторов:

«ENDPOINTADDRESS=net.tcp://xxx.xxx.xxx.xxx:22235/monitoringservice4200» - адрес (порт) службы получателя данных (сервера или агент-коллектора) (обязательное значение).

«IPADDRESSSERVER=xxx.xxx.xxx.xxx:22235» - IP-адрес (порт) получателя данных (сервера или агент-коллектора).

«AGENT_TYPE=Агент» - тип устанавливаемого агента, возможные значения: "Агент", "Агент-коллектор".

«SENDBUFFERSIZEVALUE=1000» - количество событий, передаваемых в одном пакете, по умолчанию 1000 (опциональное значение).

«DAYTRAFFICLIMITVALUE=1000» - ежедневный лимит обмена данными, значение указывается в Мб, по умолчанию 1000 Мб (опциональное значение).

«LOCALSTORAGEMAXSIZEVALUE=4091» - лимит размера локальной БД агент или агент-коллектора (допустимый максимальный размер 4091 МБ), по умолчанию 4091 МБ (опциональное значение).

«SYSTEMINFOGETINTERVALVALUE=5» - интервал проверки изменений в конфигурации защищаемого актива (узла) (в минутах), по умолчанию 5 минут (опциональное значение).

«SENDINTERVALVALUE=1000» - интервал отправки пакетов данных, значение в миллисекундах, по умолчанию 1000 мс (опциональное значение).

Пример команды для тихой установки msi-пакета:

> msiexec /i F:\Directory\VISOR-Agent-5240-x86-64bit-setup.msi /quiet /qn /norestart /log F:\Directory\silent_install.log ENDPOINTADDRESS=net.tcp://1.1.1.1:22235/monitoringservice4200 IPADDRESSSERVER=1.1.1.1 AGENT_TYPE=Агент SENDBUFFERSIZEVALUE=1000 DAYTRAFFICLIMITVALUE=1000 SENDINTERVALVALUE=1000

3.9 Внесение изменений в настройки конфигурационного файла агента, агента-коллектора

Внести изменения в конфигурационный файл агента или агент-коллектора после его установки можно двумя способами:

а) дистанционно, при помощи веб-интерфейса Visor;

б) вручную, локально на защищаемом активе.

Для дистанционного внесения изменений, необходимо зайти в меню «Узлы» выбрать нужный защищаемый актив и в его паспорте перейти на вкладку «Параметры». Выберите необходимый параметр для изменения, внесите новое значение, и оно сразу же будет изменено в конфигурационном файле на защищаемом активе при наличии сетевого соединения, либо оно будет передано агенту при ближайшем сеансе связи.

Параметры в разделе «Параметры передачи данных» хранятся локально в папке с установленным агентом на узле в файле «AgentService.exe.config».

Параметры в разделе «Параметры фильтрации событий» хранятся на сервера платформы Visor.

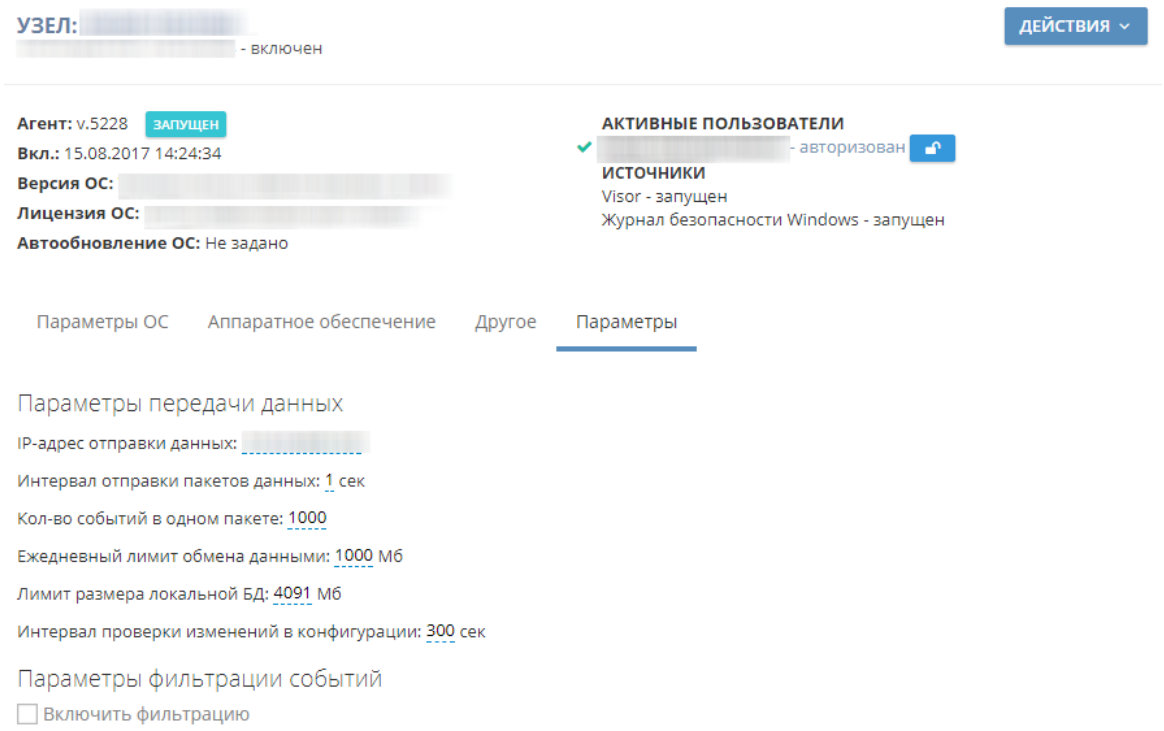

Рисунок 30 - Дистанционное внесение изменений в конфигурационный файл агента в веб-интерфейсе Visor

Для ручного внесения изменений (например, при временном отсутствии связи сервера с агентом), необходимо сначала внести нужные изменения в веб-интерфейсе Visor. После этого выгрузить конфигурационный файл из веб-интерфейса Visor в паспорте узла на вкладке «Параметры».

Далее необходимо выполнить вход в ОС на защищаемом активе, с которым отсутствует связь и где необходимо внести изменения в конфигурационный файл. Выполнить вход в папку с установленным агентом (по умолчанию это папка – C:\Program Files (x86)\NPPGamma\ Visor Agent\) и заменить существующий конфигурационный файл новым (тем, который был получен из веб-интерфейса Visor). Имя заменяемого конфигурационного файла «AgentService.exe.config».

После замены файла требуется обязательно выполнить перезагрузку службы агента или агент-коллектора Visor, чтобы внесенные изменения вступили в силу.

3.10 Управление ролевой моделью доступа

Одной из основных функций Администратора Visor является управление разграничением доступа пользователей к веб-интерфейсу Visor путем управления учетными записями (профилями), ролями, рабочими группами пользователей Visor и доступа к наборам узлов. Управление этими элементами доступа осуществляется в меню «Настройки» -> «Управление доступом».

Меню «Управление доступом» имеет следующие вкладки:

- Пользователи;
- Роли;
- Рабочие группы;
- Наборы узлов.

Прежде чем приступить к созданию пользователей, ролей и рабочих групп в платформе Visor, рекомендуется определить структуру и порядок координации деятельности сотрудников на стадиях обработки инцидентов ИБ в вашей организации. Исходя из этого определить необходимые наборы функций, которые потребуется выполнять сотрудникам (пользователям) в веб-интерфейсе Visor. Определив наборы

функций для возможных типов пользователей – приступить непосредственно к созданию пользователей, ролей и рабочих групп в платформе Visor.

Для получения общего представления о том, что представляет собой производственный процесс управления инцидентами ИБ и как он должен быть организован рекомендуется ознакомиться со стандартом ГОСТ Р ИСО/МЭК ТО 18044-2007 «Менеджмент инцидентов информационной безопасности».

3.10.1 Управление учетными записями (профилями) пользователей

Для каждого пользователя Администратором Visor, включая самого Администратора Visor, должна быть создана отдельная учетная запись (профиль) пользователя в меню «Настройки» -> «Управление доступом» на вкладке «Пользователи».

Встроенная учетная запись Администратора Visor – «admin», создается на этапе развертывания сервера Visor. Данная учетная запись является системной в Visor и не может быть удалена другими пользователями Visor, даже имеющими роль Администратора Visor. Данную учетную запись следует использовать только в экстренных случаях.

Поэтому всегда первая создаваемая учетная запись в платформе Visor должна быть учетная запись для сотрудника, выполняющего функции Администратора Visor.

Пароль от встроенной учетной записи Администратора Visor рекомендуется хранить у Руководителем службы ИБ организации и его заместителя, осуществляющего эксплуатацию платформы Visor в защищенном месте (например, сейфе).

Для создания учетной записи перейти в меню «Настройки» -> «Управление доступом» -> вкладка «Пользователи», далее нажмите кнопку «Создать».

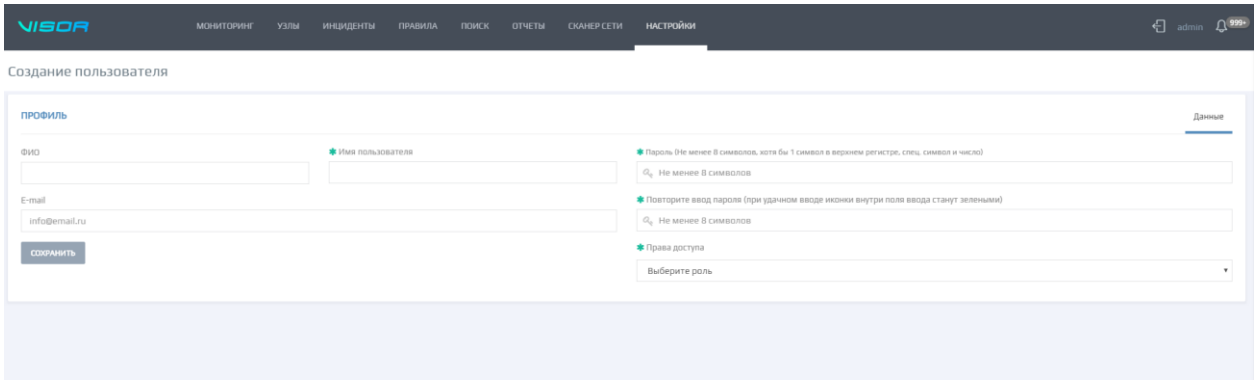

Рисунок 31. Создание профиля пользователя Visor

Учетная запись (профиль) пользователя содержит следующие поля:

а) имя учетной записи пользователя (используется для входа в веб-интерфейс Visor) (поле обязательно для заполнения);

б) роль (или роли) пользователя (поле обязательно для заполнения); одному пользователю могут быть присвоены несколько ролей, в таком случае права доступа пользователя «суммируются»; если у одной роли будет запрещен доступ к разделу меню, а у другой разрешен к этому же разделу меню, то в результате у пользователя будет разрешен доступ к данному разделу меню;

в) данные для аутентификации – имя учетной записи и пароль (поля обязательные для заполнения).

Примечание: в платформе Visor действует минимальная политика безопасности паролей, которая требует:

- длину пароля не менее 8 символов;
- наличие одного символа в верхнем регистре;
- наличие одного специального символа;
- наличие одной цифры.

г) ФИО пользователя;

д) E-mail пользователя.

Заполнив все обязательные поля нажмите кнопку «Сохранить». После этого в таблице пользователей появится только что созданный пользователь.

Для того, чтобы пользователь мог войти в веб-интерфейс Администратор Visor должен передать пользователю данные для аутентификации – имя учетной записи, пароль и адрес веб-сервера Visor для подключения через веб-браузер.

Администратор Visor должен использовать только защищенные и доверенные каналы связи при передачи данных аутентификации пользователю. При первом же входе в веб-интерфейс Visor пользователь должен сменить выданный ему пароль и далее выполнять периодическую смену пароля в соответствии с парольной политикой безопасности вашей организации.

Для редактирования или удаления существующей учетной записи (профиля) необходимо в общей таблице напротив пользователя, нажать кнопку <_>. В открывшемся окне «Редактирование пользователя» внести необходимые изменения в соответствующие

поля и нажать кнопку «Сохранить». Для удаления профиля пользователя следует выбрать пользователя и нажать кнопку и подтвердить удаление пользователя.

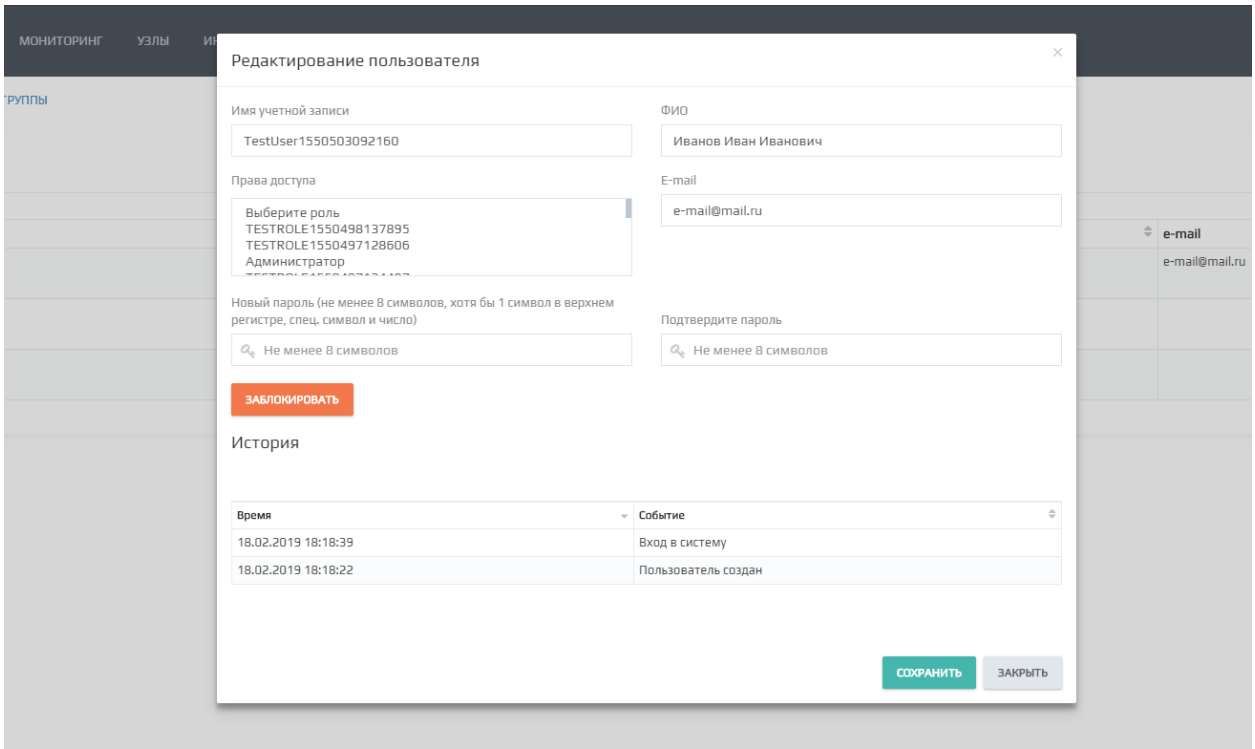

Рисунок 32. Редактирование профилей пользователей

3.10.2 Управление ролями пользователей

В платформе Visor реализована ролевая модель управления доступом, в которой каждому пользователю присваивается одна или несколько ролей. Каждая роль обладает набором прав доступа к различным меню и функциям веб-интерфейса Visor.

Пользователям, у которых должен быть одинаковый набор прав доступа к веб-интерфейсу Visor, Администратор Visor присваивает соответствующую роль (или набор ролей).

Для создания роли перейти в меню «Настройки» -> «Управление доступом» -> вкладка «Роли», далее нажмите кнопку «Создать роль».

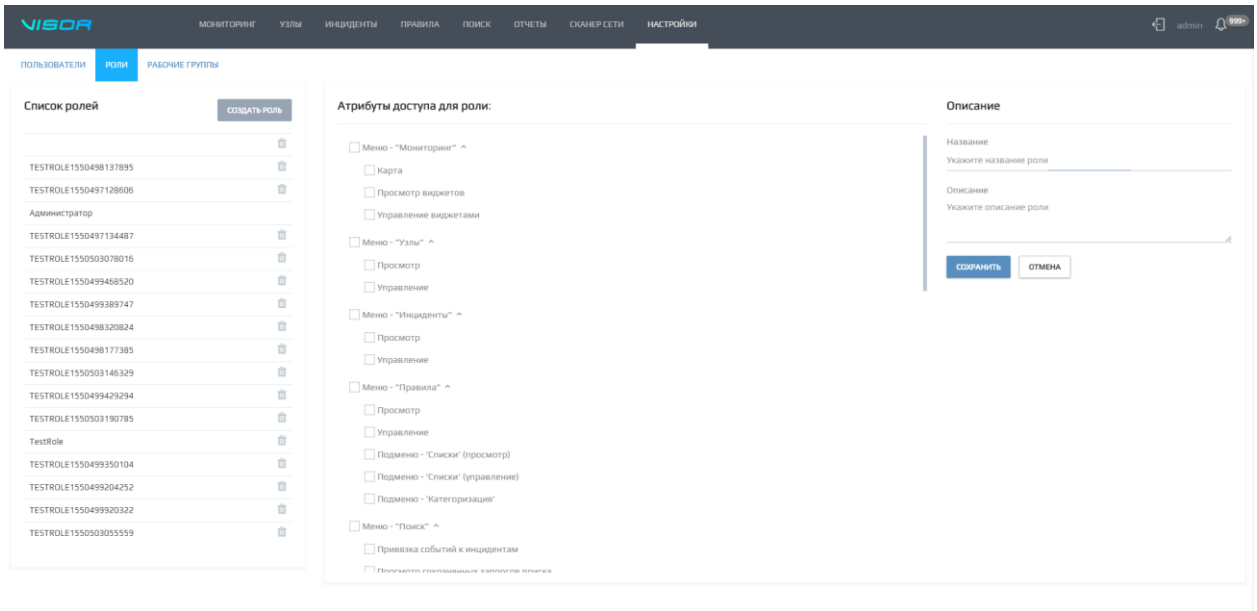

Рисунок 33. Создание роли

Роль содержит следующие поля:

а) Название (поле обязательно для заполнения);

б) Описание;

в) Дерево атрибутов доступа для роли (по центру экрана) (обязательно для заполнения).

В дереве атрибутов доступа предоставляются права к меню и подменю веб-интерфейса Visor. К большинству меню может быть предоставлен доступ на:

а) Просмотр – даёт право на просмотр элементов данного меню, без возможности управления (элементы интерфейса будут заблокированы для редактирования);

б) Управление – даёт право на управление элементами меню (создание, редактирование, удаление элементов).

Для некоторых меню возможно разграничение доступа к выполнению некоторых специфических функций в данном меню.

Заполнив все обязательные поля нажмите кнопку «Сохранить». После этого в таблице ролей (в правой части экрана) появится только что созданная роль.

Теперь все пользователи, которым будет присвоена данная роль будут обладать набором прав доступа характерным для данной роли. Меню, к которым отсутствует доступ у роли, не будут отображаться у пользователей при входе в веб-интерфейс Visor.

Для редактирования или удаления существующей роли необходимо в общей таблице ролей нажать на соответствующую роль и внести необходимые изменения в поля и нажать кнопку «Сохранить». Для удаления роли следует нажать на кнопку <_> и подтвердить удаление роли. Перед удалением роли убедитесь, что она не присвоена ни одному из пользователей.

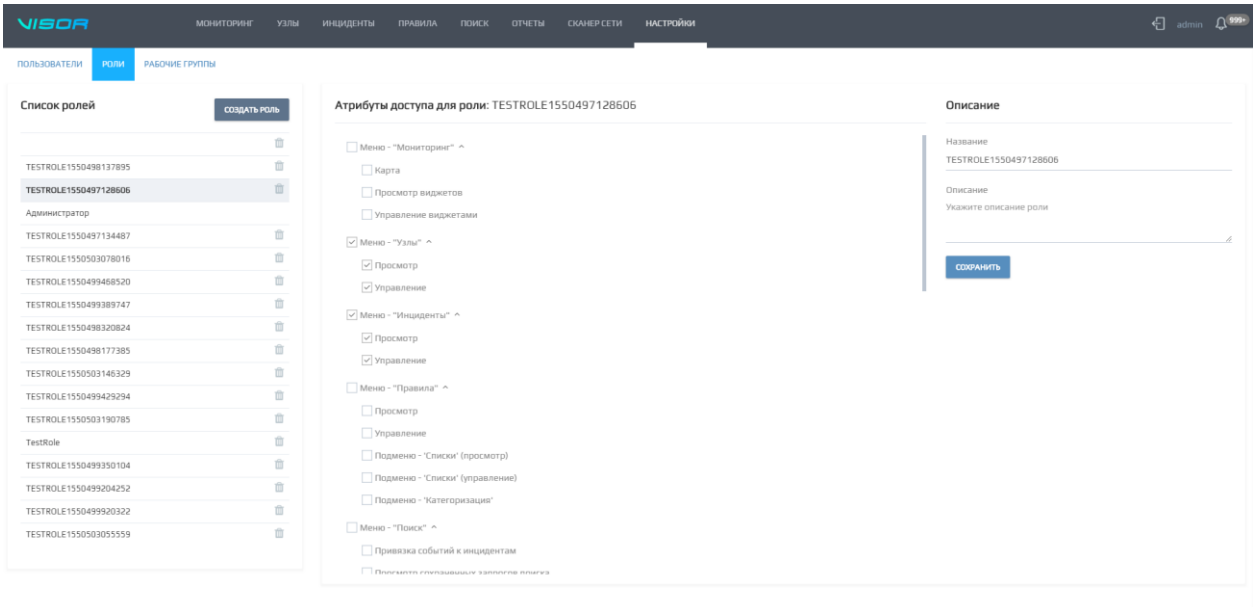

Рисунок 34. Редактирование роли

Стоит учитывать, что, если в атрибуты доступа роли были внесены и сохранены изменения прямо во время того, как пользователи с данной ролью работают в веб-интерфейсе Visor, то у этих пользователей моментально применятся внесенные изменения в атрибуты доступа, но для полной актуализации внешнего вида веб-интерфейса пользователям необходимо перезайти в веб-интерфейс Visor.

Встроенная роль Администратора Visor – «Администратор», создается на этапе развертывания сервера Visor. Данная роль является системной в Visor, не может быть удалена и включает в себя полный набор всех прав доступа.

3.10.3 Управление рабочими группами пользователей

Рабочие группы в Visor предназначены для управления рабочим процессом обработки инцидентов ИБ пользователями в меню «Инциденты». Рабочие группы позволяют:

– задать порядок обработки и обмена инцидентами между рабочими группами пользователей,

– дать права пользователям на просмотр или изменение инцидентов для конкретных рабочих групп,

– дать права пользователям на выполнение различных действий над инцидентами ИБ.

Администратор Visor должен выполнять настройку рабочих групп совместно с руководителем Аналитиков Visor и Руководителем службы ИБ организации.

Процесс настройки рабочих групп состоит из следующих этапов:

1) Определение структуры и порядка координации деятельности сотрудников на стадиях обработки инцидентов ИБ в вашей организации;

2) Создание рабочих групп в таблице «Управление рабочими группами», необходимых для организации структуры;

3) Присвоение каждому пользователю рабочей группы в таблице «Управление рабочим процессом», в соответствии с их функциональными обязанностями на этапах обработки инцидентов;

4) Назначение каждому пользователю прав в таблице «Управление рабочим процессом» по обработке инцидентов, в соответствии с принятым в организации рабочим процессом.

3.10.4 Создание, редактирование, удаление рабочих групп

Для создания рабочей группы перейти в меню «Настройки» -> «Управление доступом» -> вкладка «Рабочие группы», далее нажмите кнопку «Добавить группу» в разделе «Управление рабочими группами».

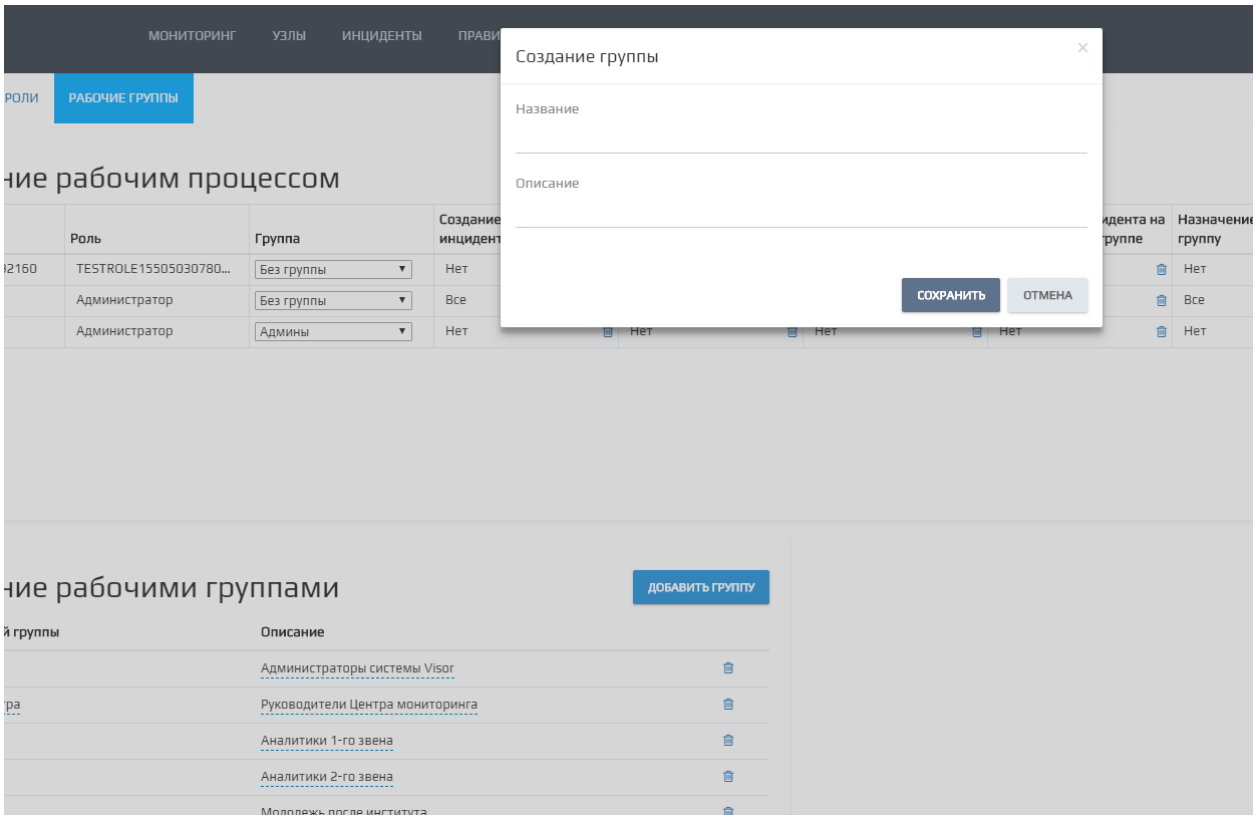

Рисунок 35. Добавление рабочей группы

Рабочая группа содержит следующие поля:

а) Название (поле обязательно для заполнения);

б) Описание.

Заполнив все обязательные поля нажмите кнопку «Сохранить». После этого в таблице рабочих групп появится только что созданная рабочая группа.

Для редактирования или удаления существующей рабочей группы необходимо в общей таблице нажать на соответствующую рабочую группу и внести необходимые изменения в поля и нажать кнопку «Сохранить». Для удаления рабочей группы следует нажать на кнопку <_> и подтвердить удаление. Перед удалением рабочей группы убедитесь, что она не присвоена ни одному из пользователей.

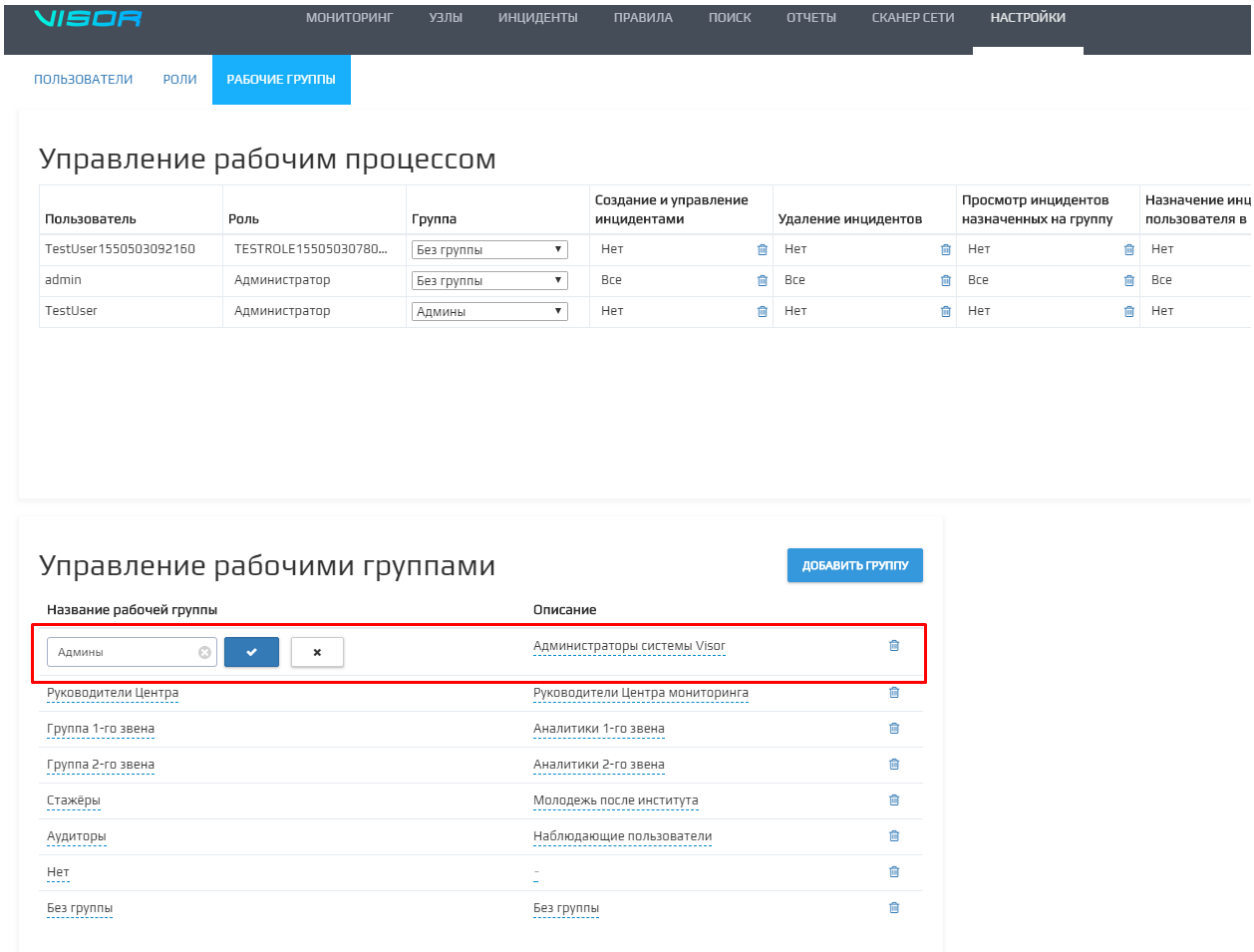

Рисунок 36. Редактирование рабочей группы

3.11 Управление рабочим процессом

После создания необходимых рабочих групп, каждому пользователю нужно присвоить ту рабочую группу, к которой он принадлежит. Каждому пользователю можно присвоить только одну рабочую группу.

Для этого в таблице «Управление рабочим процессом» найдите нужного пользователя и в столбце «Группа» присвойте нужную ему группу, значение сохранится сразу же после его выбора.

После этого каждому пользователю необходимо назначить права обработки инцидентов. В таблице «Управление рабочим процессом» вы можете предоставить каждому пользователю следующие права:

Таблица 4 - Назначение прав доступа в таблице «Управление рабочим процессом»

Название права доступа	Назначение
Создание и управление инцидентами	Даст право создавать и редактировать инциденты, назначенные на соответствующие рабочие группы.
Удаление инцидентов	Даст право удалять инциденты, назначенные на соответствующие рабочие группы.
Просмотр инцидентов, назначенных на группу	Даст право просматривать инциденты, назначенные на соответствующие рабочие группы.
Назначение инцидента на пользователя в группе	Даст право назначать инциденты на соответствующие рабочие группы (поле «Назначен на группу» в паспорте инцидента), с возможностью назначения на конкретного пользователя в данной группе.
Назначение инцидента на группу	Даст право назначать инциденты на соответствующие рабочие группы (поле «Назначен на группу» в паспорте инцидента), без возможности назначения на конкретного пользователя в данной группе.
Комментарии к инцидентам	Даст право оставлять комментарии и прикладывать файлы к комментариям для инцидентов, назначенных на соответствующие рабочие группы.
Выгрузка инцидентов в файлы	Даст право выгружать инциденты в файлы, назначенные на соответствующие рабочие группы.

Для назначения любого из перечисленных права пользователю в таблице необходимо выбрать те рабочие группы, в которых пользователь сможет выполнять это действие. При выборе значения «Все» - выберутся все рабочие группы.

Существует встроенная рабочая группа под названием – «Без группы», она используется в случаях, когда инциденты не нужно назначать на одну из групп. На данную группу по умолчанию назначаются все автоматически создаваемые инциденты правилами корреляции.

3.11.1 Настройка рабочих групп для автоматически создаваемых инцидентов

Для инцидентов, создаваемых автоматически при срабатывании каждого отдельного правила корреляции может быть настроена определенная рабочая группа, на которую будут назначаться такие инциденты.

Для этого перейти в меню «Правила», выбрать конкретное правило корреляции, затем перейти в паспорте правила на вкладку «Реакция», установить галочку «Создание инцидентов» и задать значение «Назначать на группу».

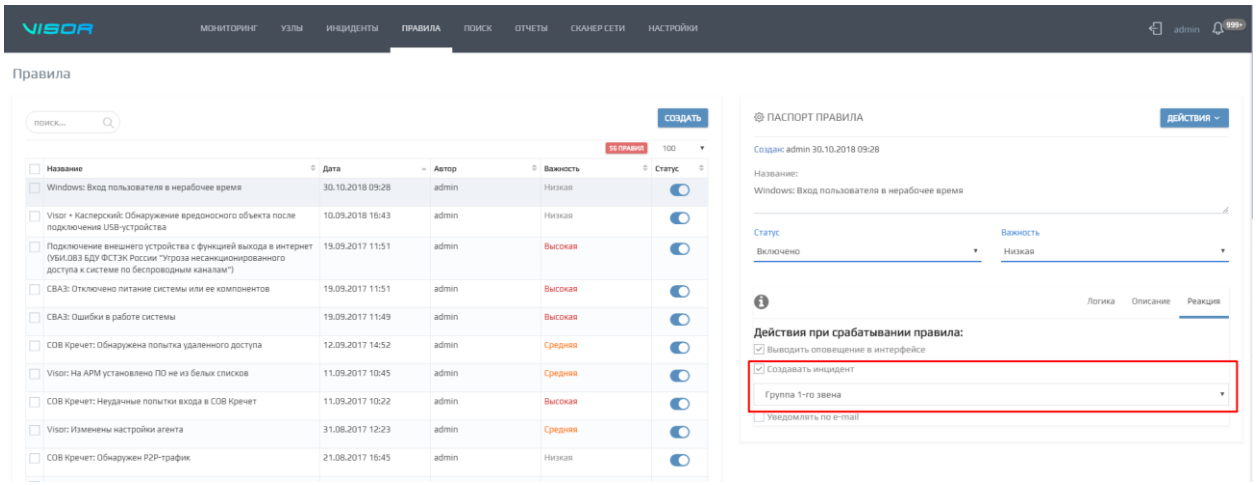

Рисунок 37. Выбор рабочей группы для назначения автоматически создаваемых инцидентов правилом корреляции

3.11.2 Управление доступом к наборам узлов

Наборы узлов предназначены для сортировки узлов по различным признакам в меню «Узлы». Структура наборов узлов имеет древовидное строение и позволяет разграничивать доступ пользователей Visor к каждой ветке дерева.

Чтобы предоставить пользователю Visor к какому-либо набору узлов, перейдите в меню «Настройки» - подменю «Наборы узлов». Выберите нужного пользователя и предоставьте ему доступ, проставив галочку напротив соответствующего набора узлов

Далее пользователю необходимо перезайти в веб-интерфейс Visor, после чего в меню «Узлы» ему станет доступен соответствующий набор узлов, а также просмотр событий ИБ в меню «Поиск» по узлам из этого набора, получение оповещений, просмотр инцидентов и т.п.

4 ПРОВЕРКА ПРОГРАММЫ

4.1 Проверка установки агента, агента-коллектора

Чтобы убедиться, что установка агента или агент-коллектора Visor прошла успешно, после выполнения установки можно проверить:

наличие процесса AgentService.exe в запущенных Процессах ОС Windows;

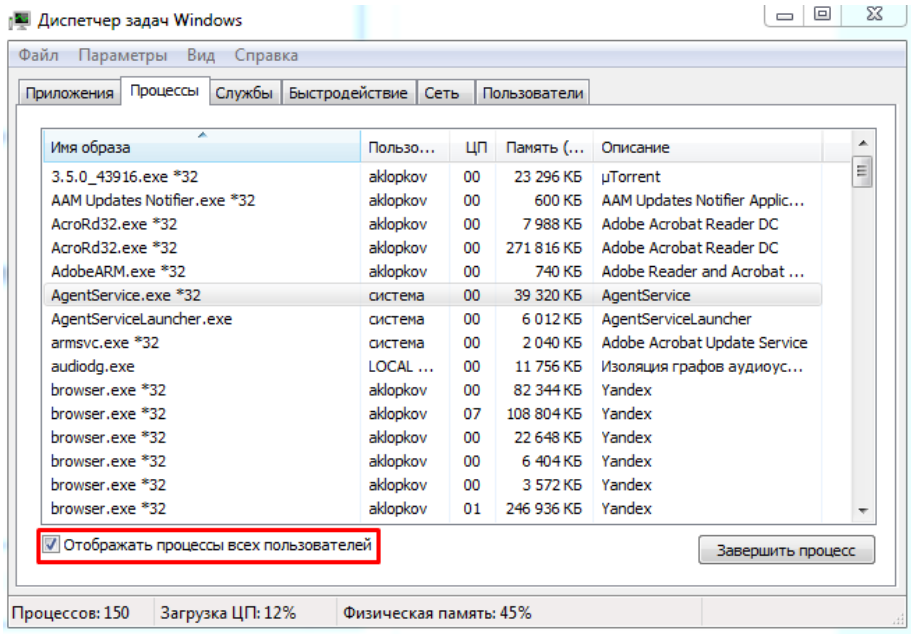

Рисунок 38 - Наличие процесса AgentService.exe в запущенных процессах ОС Windows

наличие службы AgentService в Службах ОС Windows и статус ее работы - «Работает» (Running).

4.2 Устранение проблемы при установке агента или агент-коллектора

Если при установке агента или агент-коллектора подключаемый к Visor защищенный актив не появляется в веб-интерфейсе Visor в меню «Узлы», то в этом случае на защищаемом активе необходимо скопировать журнал событий агента или агент-коллектора Visor, расположенного в папке: «C:\Program Files (x86)\NPPGamma\ Visor Agent\logs\». Копию этого журнала следует предоставить разработчикам Visor для анализа.

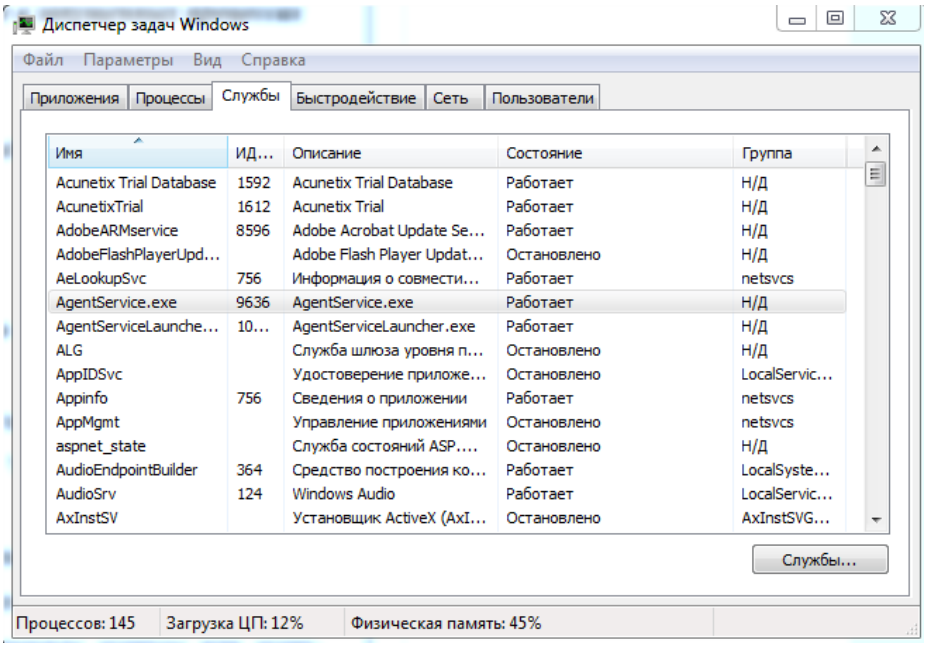

Рисунок 39 - Наличие службы «agentservice» в службах ОС Windows и статус ее работы

5 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

5.1 Мониторинг и анализ статуса функционирования Visor

Одной из основных функций Администратора Visor является выполнение периодического мониторинга внутренних событий и журналов регистрации событий платформы Visor для определения статуса корректности и режимов работы ее компонентов.

Просмотр внутренних событий Visor доступен в меню «Поиск» веб-интерфейса Visor. Для открытия внутренних событий необходимо в меню «Поиск» установить фильтр по источнику «Visor».

Сообщения об ошибках и внутренних событиях Администратору Visor так же отображаются в меню «Поиск» веб-интерфейса Visor при использовании фильтра «Visor» по источнику.

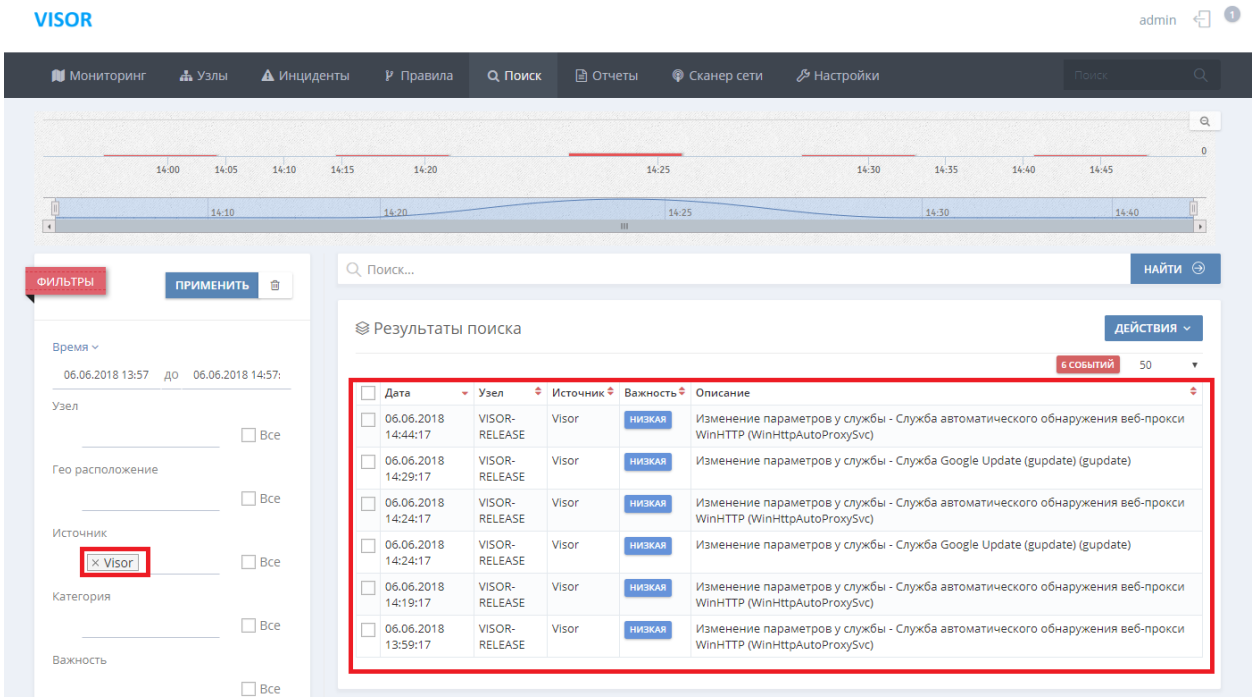

Рисунок 40 - События от источника Visor в меню «Поиск»

Сообщения о создании инцидентов, срабатывании правил корреляции и статусе выполнения различных внутренних задач Visor (выполнение задач сканирования сети, архивирования, установки и удаления агентов и т.п.) отображаются в меню «Оповещения» в веб-интерфейсе Visor.

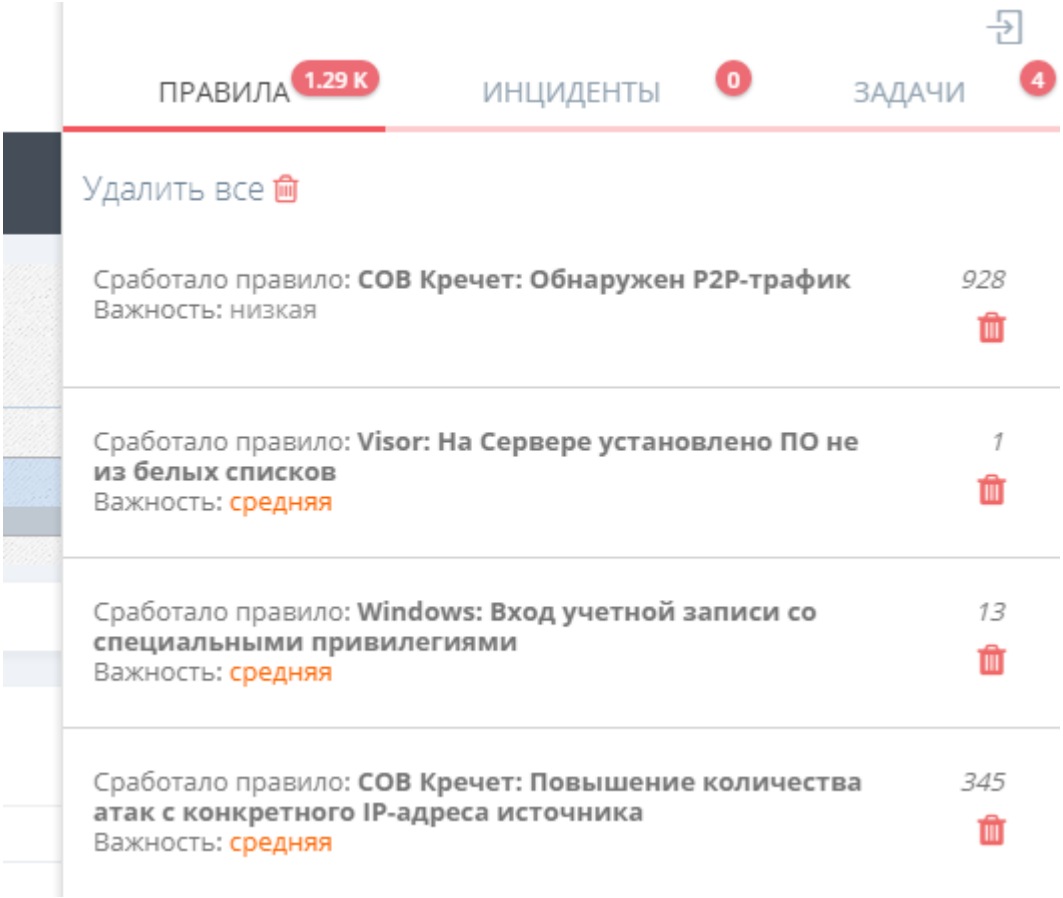

Рисунок 41 - Оповещения о создании инцидентов и срабатывании правил Visor в веб-интерфейсе

5.2 Типы регистрируемых внутренних событий аудита

Платформа Visor регистрирует следующие собственных типы внутренних событий аудита:

– статус сетевой доступности защищаемых активов;

– статус соединения сервера Visor с агентом или агент-коллектором Visor;

– статус работы службы агента или агент-коллектора Visor;

– выполнение задач инициализации агентом или агент-коллектором Visor (инициализация выполняется агентом при первичной установке на защищаемый актив, включает в себя сбор первичной информации об активе);

– изменение настроек конфигурационного файла и параметров фильтрации событий для агентов или агент-коллекторов Visor;

– превышение ограничения по сетевому трафику для агентов и агент-коллекторов Visor;

– изменение различных настроек на защищаемом активе (изменение работы служб ОС, политик безопасности ОС, установленного ПО, установленных обновлений ОС, состава и параметров учетных записей ОС, состава аппаратного обеспечения актива);

– подключение и отключение USB-устройств на защищаемом активе;

– вход, выход пользователей в веб-интерфейс Visor;

– неудачные попытки входа пользователя Visor;

– создание, изменение и удаление профилей пользователей Visor;

– статус выполнения задач архивирования;

– статус выполнения задач сканирования сети и обнаружение новых сетевых устройств.

При этом для каждого регистрируемого события в параметрах регистрации указываются:

– дата и время;

– субъект доступа (если это уместно);

– объект доступа (если это уместно);

– результат выполнения операции.

5.3 Управление архивом

Одной из основных функций Администратора Visor является выполнение периодической или ручной выгрузки исторических событий и инцидентов ИБ во внешние архивные файлы для последующего хранения на внешних носителях данных.

Меню «Настройки» -> «Архив» предоставляет инструментарий для выгрузки событий и инцидентов ИБ из БД Visor во внешний архивный файл, это позволяет высвобождать свободное пространство на сервере в БД Visor для сохранения новых событий.

В меню «Архив» могут быть заданы параметры автоматической или ручной архивации. Автоматическая архивация запускается один раз в месяц и выгружает в архивный файл все события старше одного года. При ручной архивации указывается период времени, за который следует архивировать данные.

Также имеется возможность обратной загрузки информации из внешних файлов в базу Visor при необходимости проведения расследований инцидентов ИБ и выполнения поиска событий по архивным данным.

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

При создании внешних архивных файлов размер дискового пространства БД Visor не уменьшается. Это связанно с тем, что данные выгружаются из БД Visor и очищают лишь ее содержимое, но размер БД Visor при этом остается таким же, как и был до выгрузки. При этом вновь поступающие события будут заполнять очищенное пространство внутри БД Visor.

5.3.1 Выполнение задач архивирования

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

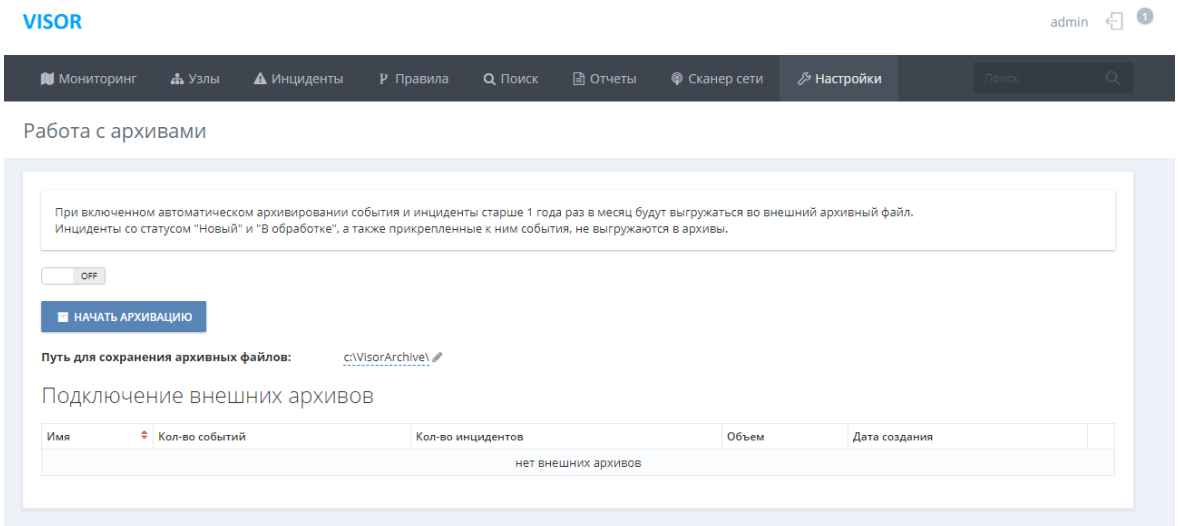

Рисунок 42 - Меню «Архив»

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.

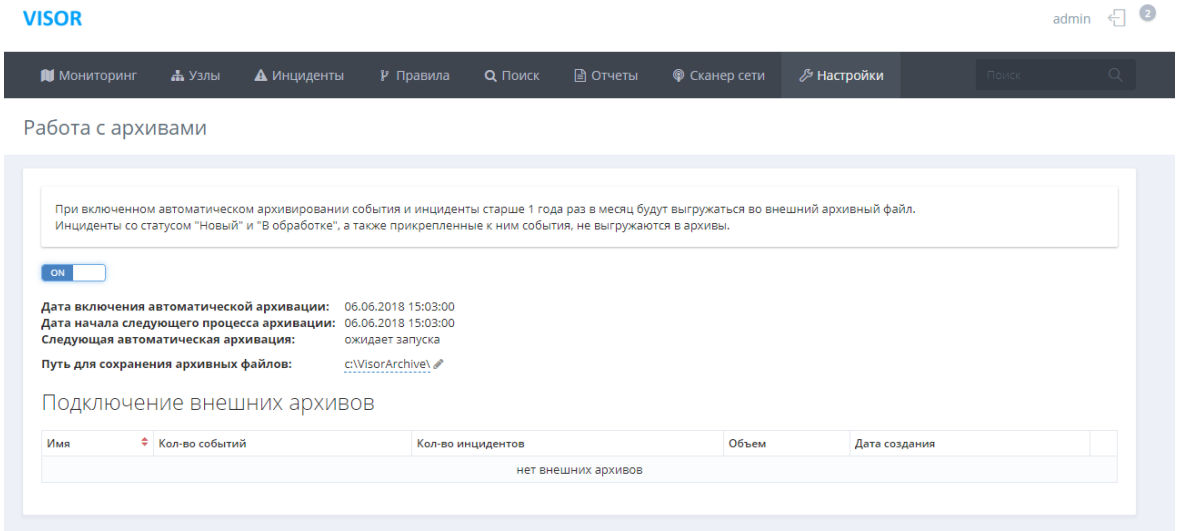

Рисунок 43 - Включение/выключение автоматического архивирования

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.

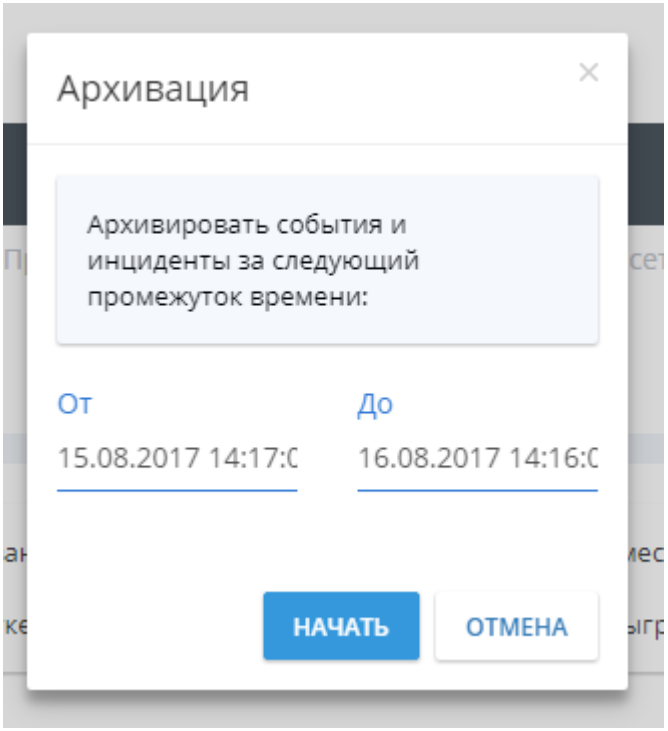

Рисунок 44 - Окно «Архивация» для выполнения ручной архивации

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

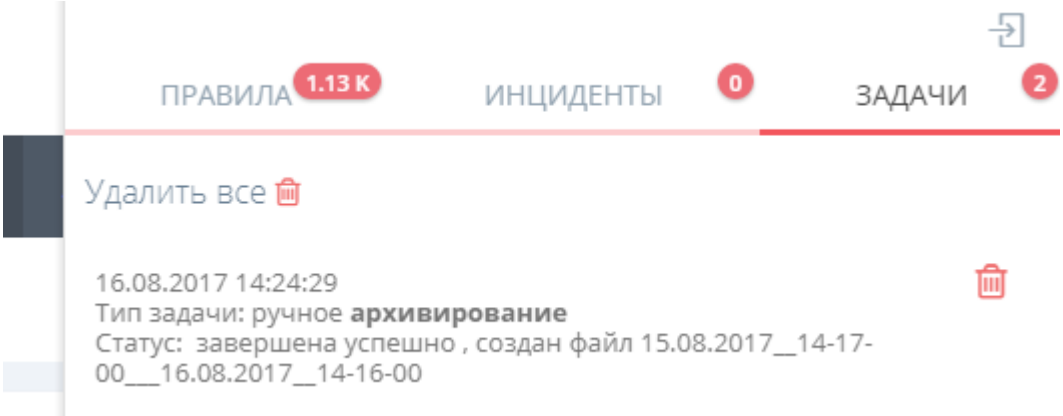

Рисунок 45 - Оповещение о статусе выполнения задачи архивирования

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

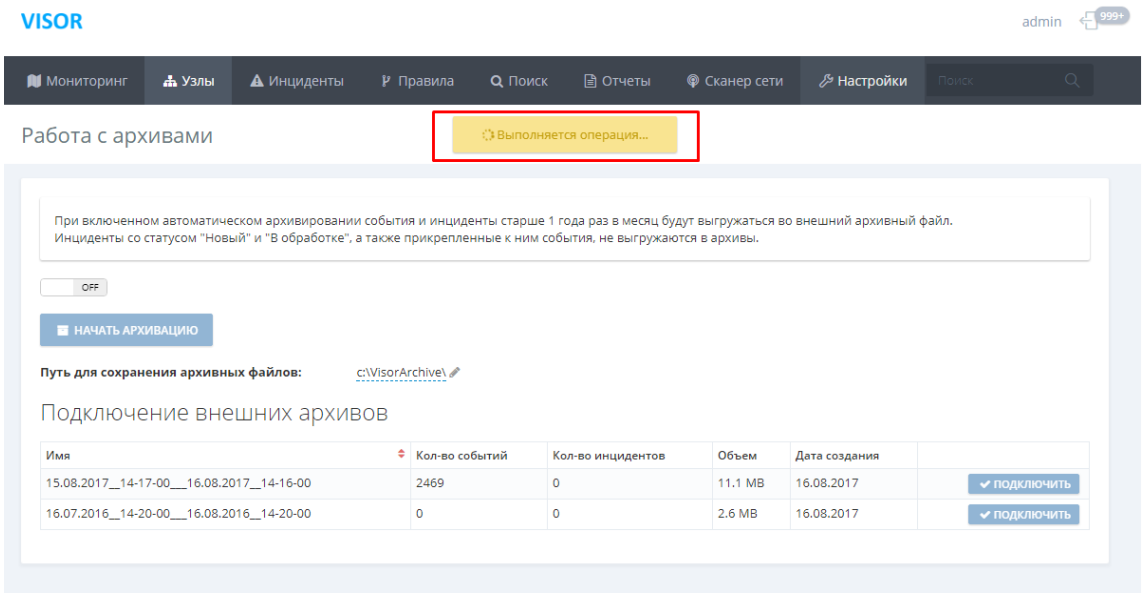

Рисунок 46 - Статус выполнения задачи архивирования в меню «Архив»

5.3.2 Задание пути для сохранения архивных файлов

В меню «Архив» есть возможность указать путь для сохранения архивных файлов. По умолчанию при установке сервера Visor задается следующий путь для сохранения

архивных файлов: «C:\ Visor Archive\». Для его изменения необходимо нажать кнопку «Изменить», ввести новый путь и нажать кнопку «Enter».

5.3.3 Поиск по данным из архивных файлов

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

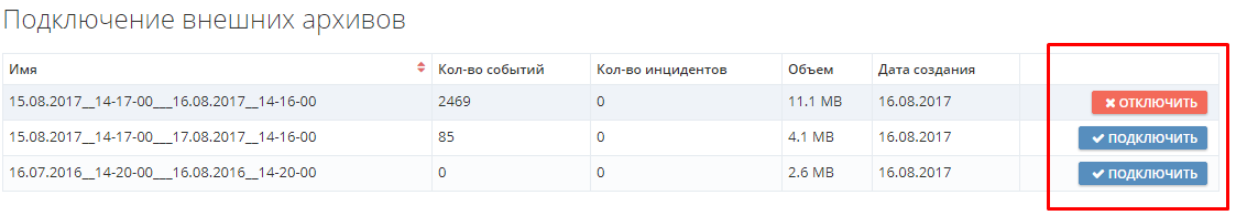

Рисунок 47 - Подключение/Отключение архивных файлов

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 по временному диапазону архивного файла.

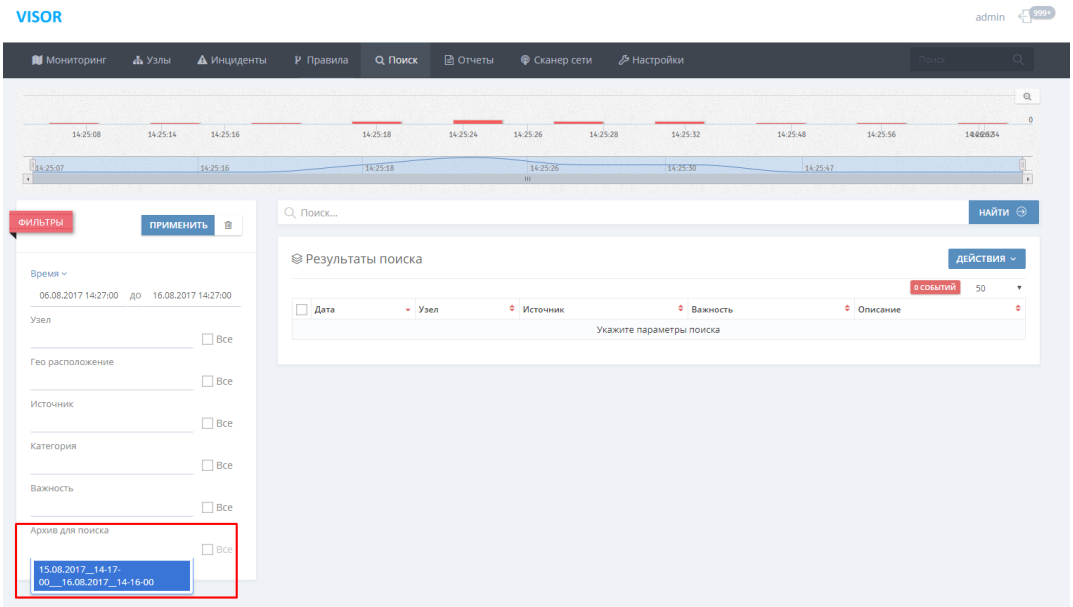

Рисунок 48 - Выбор подключенного архивного файла в меню «Поиск»

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 Visor.

5.4 Резервное копирование и восстановление сервера Visor

Одной из основных функций Администратора Visor является периодическое создание резервных копий критических файлов и БД Visor для возможности восстановления работы платформы Visor после сбоев.

Наличие работающих резервных копий файлов и БД Visor позволяет выполнить оперативное восстановление работоспособности сервера Visor после сбоев и нарушения работы его компонентов.

Периодичность создания резервных копий зависит от принятых политик безопасности в организации.

Рекомендуется проводить регулярные проверки созданных резервных копий. В ходе проверки Администратор Visor должен установить, что из имеющейся резервной копии удается успешно восстановить работоспособность сервера Visor в случае необходимости.

5.5 Управление лицензией

Одной из основных функций Администратора Visor является хранение и загрузка через веб-интерфейс лицензии на платформу Visor, а также своевременное оповещение руководства организации о необходимости продления действия лицензии на платформу Visor при приближении срока окончания её действия (рекомендуется инициировать процедуру продления за 2-3 месяца до даты её окончания).

При приобретении платформы Visor производитель (поставщик) должен поставить вместе с дистрибутивом файл лицензии.

Действующий файл лицензии предоставляет:

- официальное право на использование платформы Visor;
- право на получение обновлений для платформы Visor;
- право на получение технической поддержки от производителя.

Для загрузки файла лицензии перейдите в меню «Настройки» -> «Лицензия» в веб-интерфейсе Visor и нажмите кнопку «Добавить файл лицензии».

В окне проводника выберите предоставленный производителем файл лицензии с расширением *.lic.

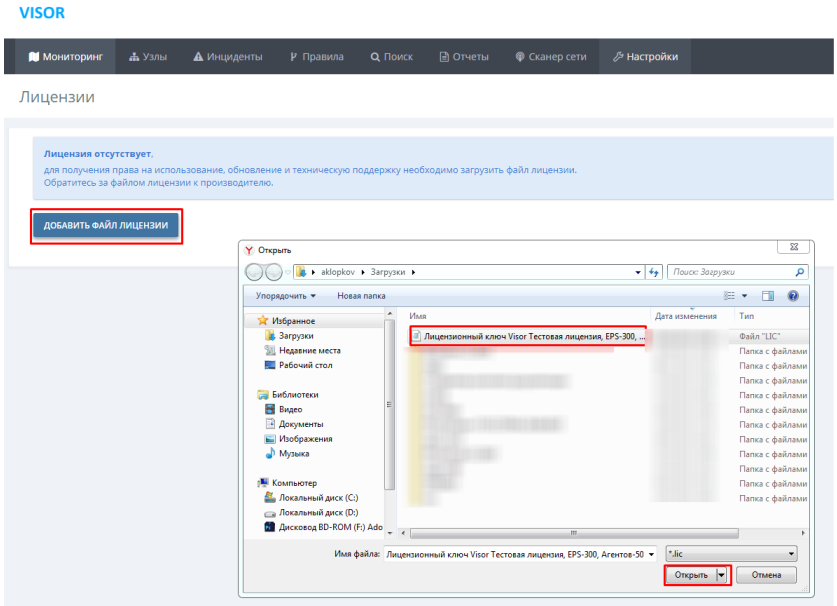

Рисунок 49 - Загрузка файла лицензии

После загрузки файла лицензии в меню «Лицензия» будет отображен статус и другая информация по лицензии.

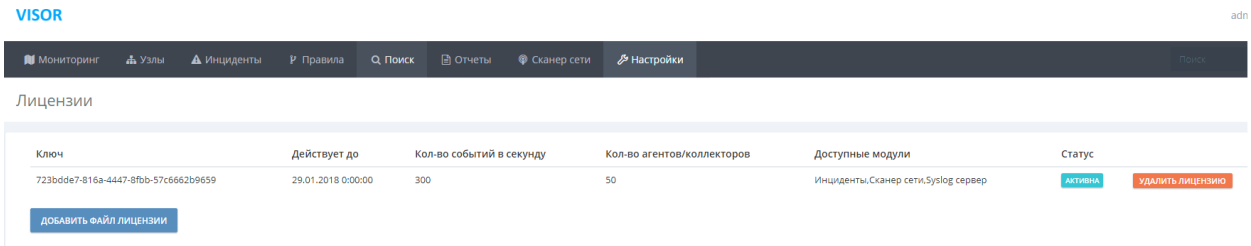

Рисунок 50 - Отображение информации по лицензии

Администратор Visor должен своевременно информировать руководство организации о необходимости продления действия лицензии на платформу Visor.

6 СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

6.1 Основные функции системного программиста (администратора Visor)

Для обеспечения эффективного функционирования платформы Visor необходимо наличие пользователя системы с ролью Администратора. Администратора Visor должен уметь выполнять следующие функции со следующей периодичностью:

Таблица 5. Функции Администратора Visor

№	Функция	Назначение	Периодичность	Раздел руководства
1	Развертывание платформы Visor	Выполнение установки и настройки компонентов платформы Visor – сервера и распространение агентов и агент-коллекторов на защищаемые активы.	Сервер - во время первичного развертывания платформы Visor. Агенты – по мере необходимости их установки. Подключение источников – периодически по мере необходимости их подключения.	См. Раздел 4
2	Управление ролевой моделью доступа	Создание, редактирование и удаление учетных записей пользователей, ролей, рабочих групп для разграничения доступа к	Периодически при необходимости добавления пользователей	См. Раздел 5

№	Функция	Назначение	Периодичность	Раздел руководства
		веб-интерфейсу Visor. Разграничение доступа к наборам узлов.	Visor.	
3	Подключение источников событий	Настройка источников событий ИБ и компонентов Visor для успешного сбора, корреляции и хранения событий от этих источников в БД Visor.	Периодически при необходимости подключения конкретного источника.	См. Раздел 6
4	Мониторинг и анализ статуса функционирования платформы Visor	Периодический мониторинг внутренних событий и журналов регистрации событий платформы Visor для определения статуса корректности работы ее компонентов.	Рекомендуется не реже 1 раза в неделю.	См. Раздел 7
5	Управление лицензией на платформу Visor	Хранение, загрузка в веб-интерфейс и своевременное продление действия лицензии на платформу Visor.	-	См. Раздел 10
6	Обращение в техническую поддержку	Формирование запросов и общение с представителями технической поддержки производителя платформы Visor для решений	По мере возникновения проблем и вопросов.	См. Раздел 11

№	Функция	Назначение	Периодичность	Раздел руководства
		проблем и вопросов, возникающих в ходе эксплуатации Visor.		
7	Хранение дистрибутива и эксплуатационной документации Visor	1. Документация содержит необходимую информацию для обеспечения функционирования и обслуживания платформы Visor. 2. При проведении различного рода аудитов и проверок регуляторами в области ИБ, потребуется предъявить документацию на Visor и копию используемого дистрибутива.	Постоянно в физически защищенном хранилище (сейф и т.п.).	-

В последующих разделах документа приведено описание и порядок выполнения каждой из функций Администратора Visor.

6.2 Требования к квалификации специалиста

Для эффективного выполнения своих функций рекомендуется, чтобы Администратор Visor обладал следующими навыками и знаниями:

– знание основных принципов обеспечения информационной безопасности;

– знания и опыт внедрения, настройки, администрирования средств и систем защиты информации;

– знание принципов штатного функционирования защищаемых информационных систем в организации;

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

– опыт настройки и администрирования баз данных, веб-серверов и серверов приложений.

6.3 Подключение источников событий

Одной из основных функций Администратора Visor является подключение по мере необходимости внешних источников событий ИБ к платформе Visor.

Подключение внешних источников необходимо для обнаружения инцидентов ИБ в полученных событиях. Различные типы и производители источников регистрируют события в своих журналах регистрации событий в собственных форматах, а также хранят и передают их различными методами.

Поэтому подключение каждого источника зависит от его конкретного типа. Для различных типов источников разработаны и описаны инструкции их подключения в соответствующей дополнительной документации к платформе Visor.

Настройку и подключение источников событий ИБ рекомендуется выполнять совместно и по согласованию с пользователем Visor выполняющим роль Аналитика Visor, а также с Администратором и Руководителем службы ИБ организации.

6.4 Настройка источников событий ИБ

Настройку источников событий ИБ рекомендуется выполнять совместно и по согласованию с пользователем Visor выполняющим роль Аналитика Visor, а также с Администратором и Руководителем службы ИБ организации.

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

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

Чтобы в журналах регистрации событий ИБ фиксировался необходимый набор событий ИБ, средства аудита системного, общего и прикладного программного обеспечения, а также программно-аппаратных средств должны быть соответствующим образом настроены. В противном случае в журналах источников события не будут регистрироваться. Соответственно не будут собираться платформой Visor. Это сделает не возможным выполнение процесса мониторинга и обнаружения инцидентов ИБ с помощью платформы Visor.

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. Чрезмерно подробное включение параметров аудита (например, в ОС Windows) спровоцирует большое количество регистрации «шумовых» событий, которые не будут нести информационного смысла для процесса выявления инцидентов; будут заполнять свободное дисковое пространство в БД сервера Visor; накладывать дополнительную нагрузку при передаче данных (трафика) на ЛВС организации. Однако, такие события могут быть полезны при глубинном расследовании различных обстоятельств инцидентов. И наоборот, слишком «легкая» настройка параметров аудита возможно будет способствовать пропуску в регистрации важных при расследовании и обнаружении событий ИБ;

– модели угроз и нарушителей, применимых к защищаемым активам;

– возможностей в тонкости настройки параметров аудита у каждого конкретного типа источника.

6.5 Обращение в техническую поддержку

Одной из основных функций Администратора Visor является формирование запросов и общение со специалистами технической поддержки производителя платформы Visor.

Если в процессе развертывания, эксплуатации и работы платформы Visor возникли проблемы или вопросы по ее функционированию или настройке, необходимо обратиться в техническую поддержку.

После покупки платформы Visor, компания-пользователь автоматически получает стандартную техническую поддержку сроком на 1 год с даты выдачи лицензии (порядок, сроки и условия качества оказания технической поддержки указываются в лицензионном договоре). Далее для обращения в техническую поддержку производителя, компания-пользователь должна продлевать лицензию на оказание технической поддержки платформы Visor.

Предприятие-изготовитель –ФГУП «НПП «Гамма».

Контактная информация:

117393, г. Москва, ул. Профсоюзная д.78;

тел. 8 (495) 663-16-84, доб. 1419

факс: +7 (495) 330-33-88;

Перечень принятых сокращений

АРМ – автоматизированное рабочее место

БД – база данных

ИБ – информационная безопасность

ЛВС – локальная вычислительная сеть

ОС – операционная система

ПО – программное обеспечение

СВТ – средство вычислительной техники

ОПО – общесистемное программное обеспечение

СОВ – система обнаружения вторжений