2025

SecurityDesk
Инструкция
администратора

# [SECURITYDESK АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ]

Инструкция администратора 1.42

# Оглавление

# Введение

Документ предназначен для администраторов системы управления безопасностью «SecurityDesk». В документе описываются правила установки и настройки системы.

# Принятые сокращения и определения

| | | |
|---|---|---|
| **Инцидент** | - | Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или требуемое состояние безопасности, приводящее к материальному, репутационному или иному виду ущерба. |
| **Документ** | - | Файл, содержащий какую-либо информацию. |
| **Задача** | - | Зарегистрированная работа в системе. |
| **Нормативный документ** | - | Разработанный в рамках функционирующей системы обеспечения безопасности нормативный документ (инструкция, регламент, политика и т.д.). |
| **Администратор** | - | Пользователь системы, входящий в группу/профиль Administrators и имеющий полномочия настройки системы. |
| **Пользователь** | - | Любой пользователь, зарегистрированный в системе. |
| **Суперпользователь** | - | Пользователь системы, которой входит в группу/профиль SuperUsers имеющий доступ ко всем инцидентам, задачам и уязвимостям. |
| **Профиль** | - | Объект системы, наделяющий входящих в нее пользователей определенными привилегиями. |
| **Система** | - | Автоматизированная система управления безопасностью «SecurityDesk». |
| **Уязвимость** | - | Зарегистрированный в системе объект, характеризующий недостаток, с помощью которого возможно нанесение ущерба, вызвать неправильную работу актива. |
| **Актив** | - | Оборудование или персонал, который может служить источником или объектом воздействия событий безопасности. |

# 1. Минимальные системные требования

Для функционирования системы требуется аппаратный или виртуальный сервер со следующими минимальными характеристиками:

- **64-разрядный процессор с тактовой частотой 1 ГГц или выше**
- **4 ГБ оперативной памяти**
- **Свободное место на жестком диске 15 Гб.**
- **Windows Server 2012 и выше**
- **.NET Framework 4.8**
- **IIS 8**
- **SQL Server 2014 (включая Express) и выше**

Для работы с системой необходимо требуется персональный компьютер со следующими характеристиками:

- **Интернет-браузер Google Chrome, Microsoft EDGE**
- **4 ГБ оперативной памяти**

# 2. Установка и настройка

Установка Системы выполняется в следующей последовательности:

## 2.1 Подготовка операционной системы

После установки операционной системы откройте диспетчер серверов, в окне диспетчера нажмите на ссылку «Добавить роли и компоненты» и нажмите на кнопку «Далее» в мастере добавления ролей и компонентов – Рисунок 1.

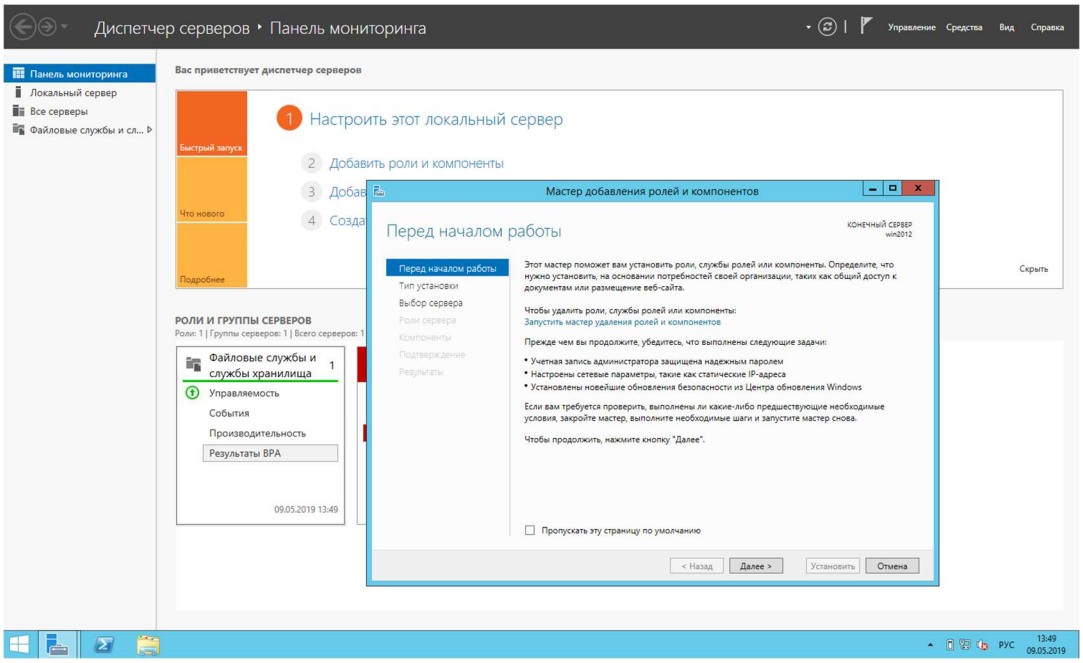


Рисунок 1. Мастер добавления ролей и компонентов.

Перейдя на следующее окно мастера, также нажмите кнопку «Далее» - Рисунок 2.

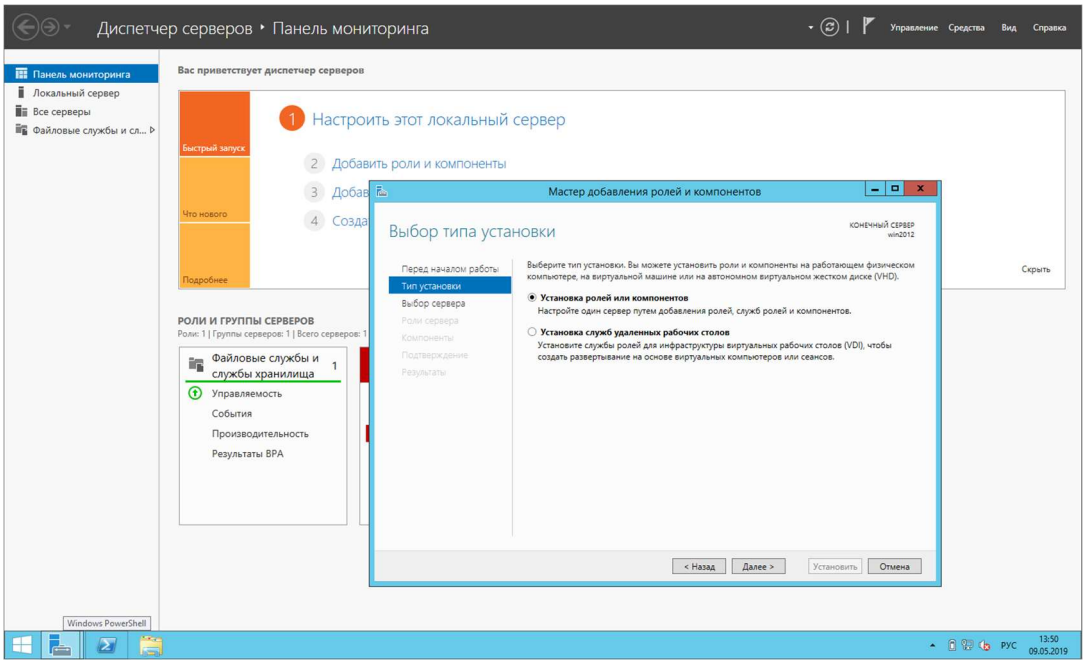


Рисунок 2. Выбор типа установки.

В следующем окне выберите, если это потребуется сервер для установки Системы и нажмите кнопку «Далее» - Рисунок 3.

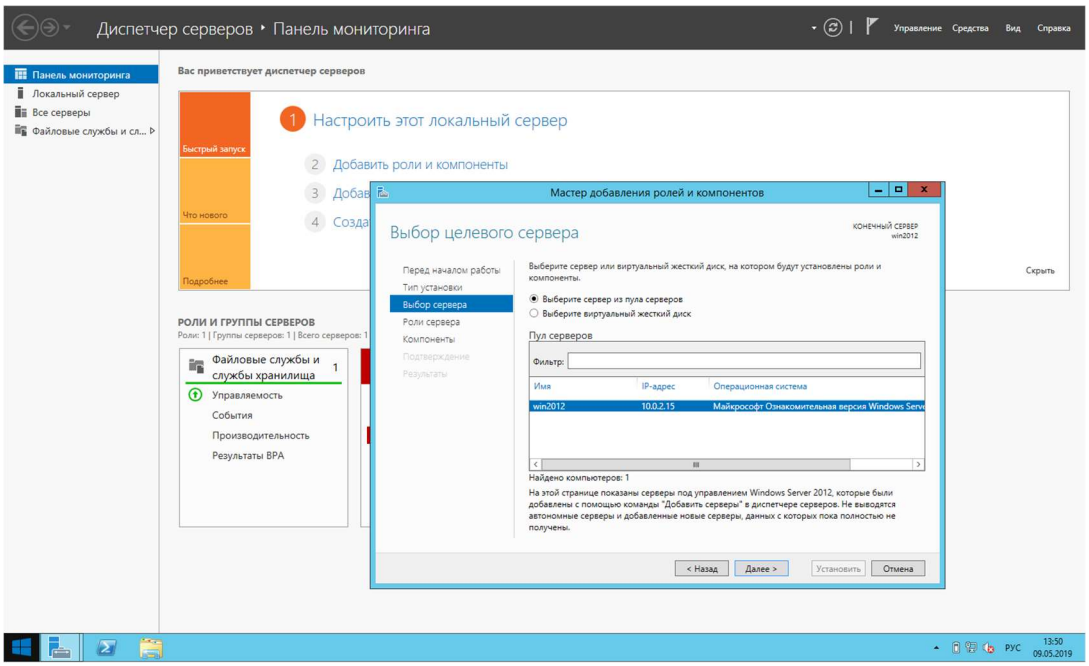


Рисунок 3. Выбор сервера для установки.

В открывшемся окне выбора ролей сервера отметьте галочкой пункт «Веб-сервер (IIS)», в отрывшемся дополнительном окне нажмите кнопку «Добавить компоненты» - Рисунок 4 и кнопку «Далее» на окне выбора ролей сервера – Рисунок 5.

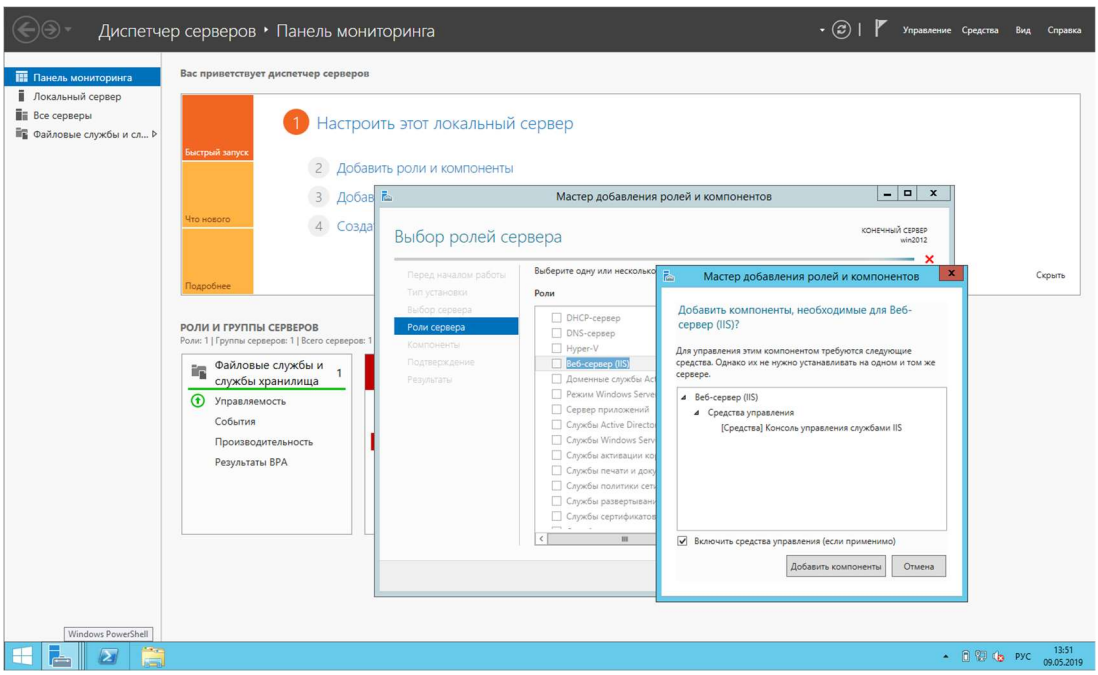


Рисунок 4. Добавление компонентов к роли сервера.

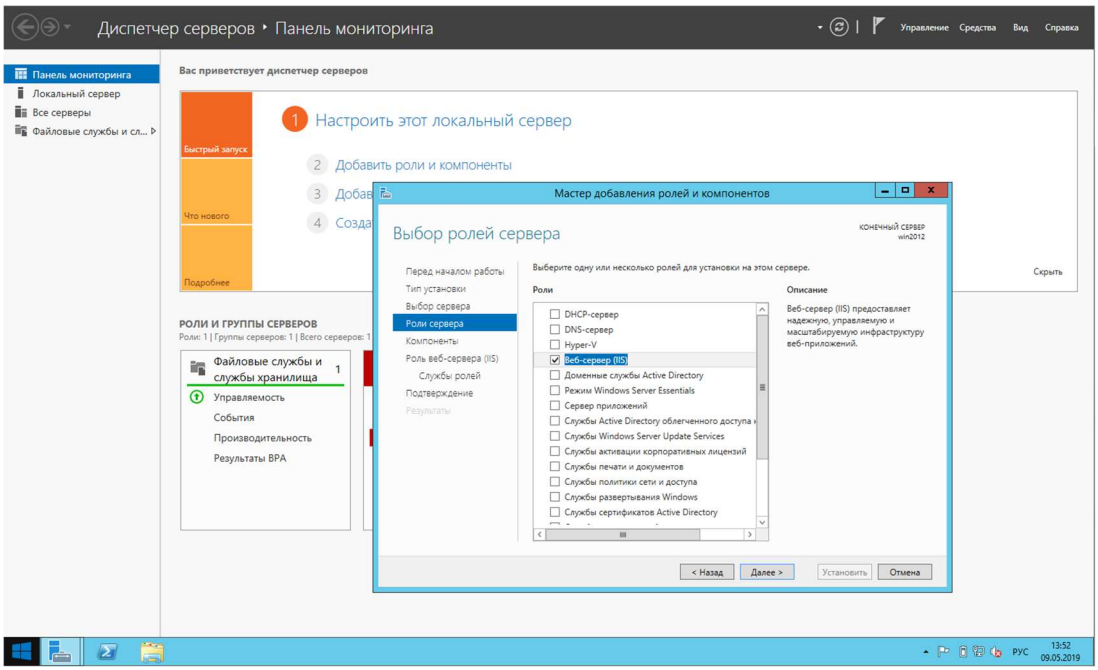


Рисунок 5. Выбор ролей сервера.

На открывшемся окне выбора компонентов сервера установите галочки как показано на рисунке (Рисунок 6) и нажмите кнопку «Далее».

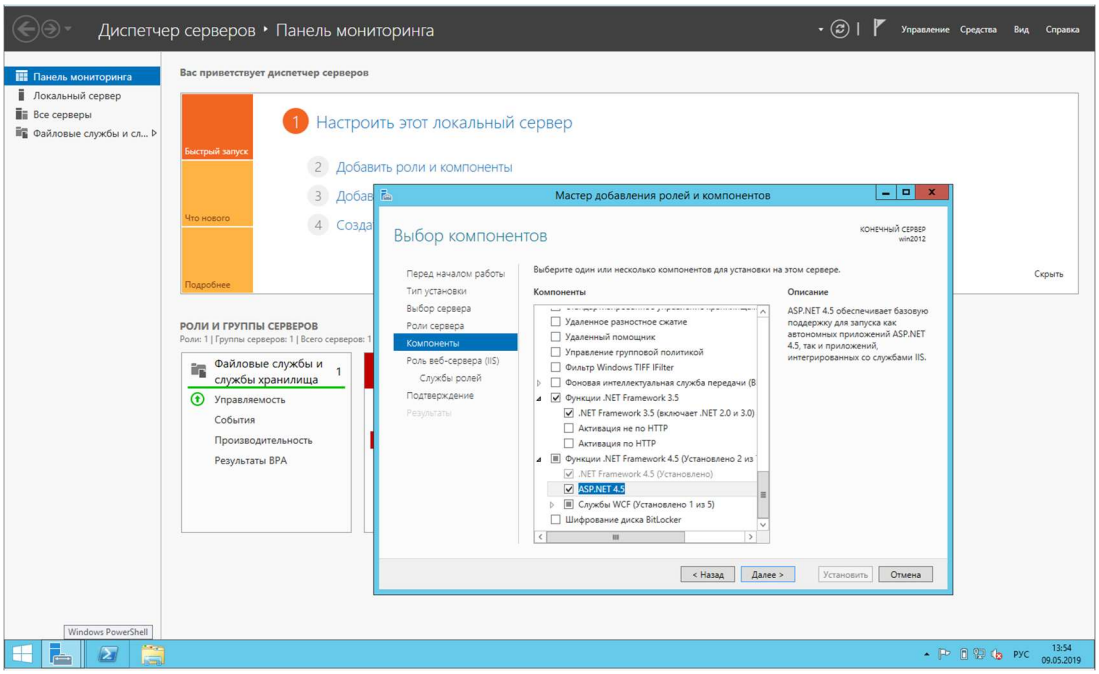


Рисунок 6. Выбор компонентов.

На открывшемся окне выбора служб ролей сервера выберите параметры как указано на рисунке (Рисунок 7) и нажмите кнопку «Далее».

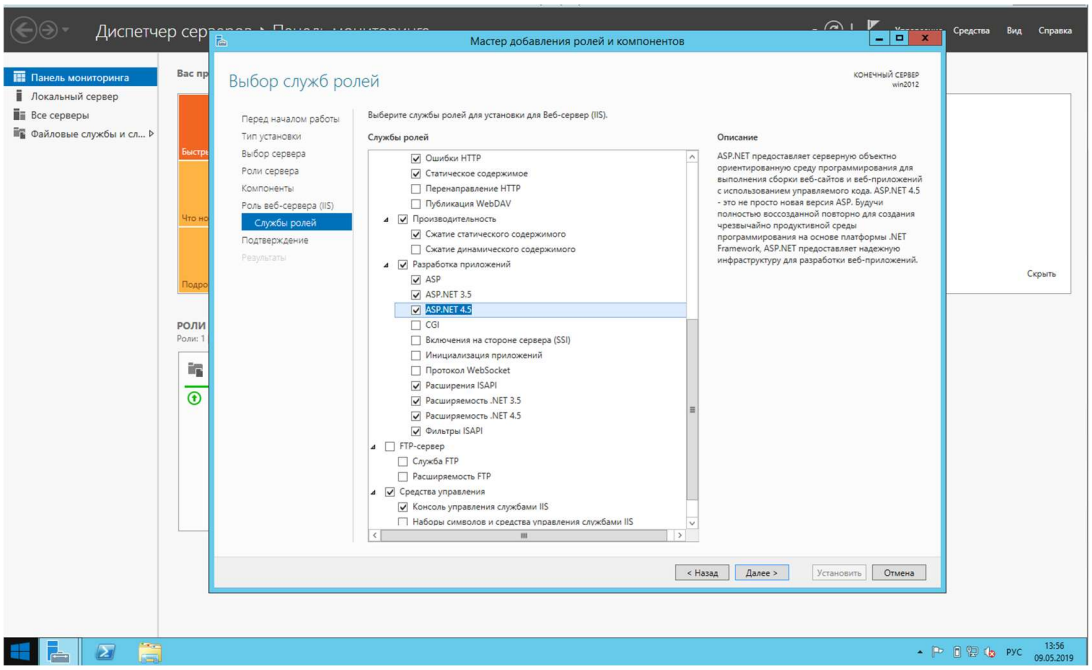


Рисунок 7. Выбор служб ролей сервера.

В новом открывшемся окне мастера отобразиться окончательный перечень устанавливаемых ролей и компонентов. Проверьте, что все роли и компоненты указаны как на рисунке (Рисунок 8) и нажмите кнопку «Установить».

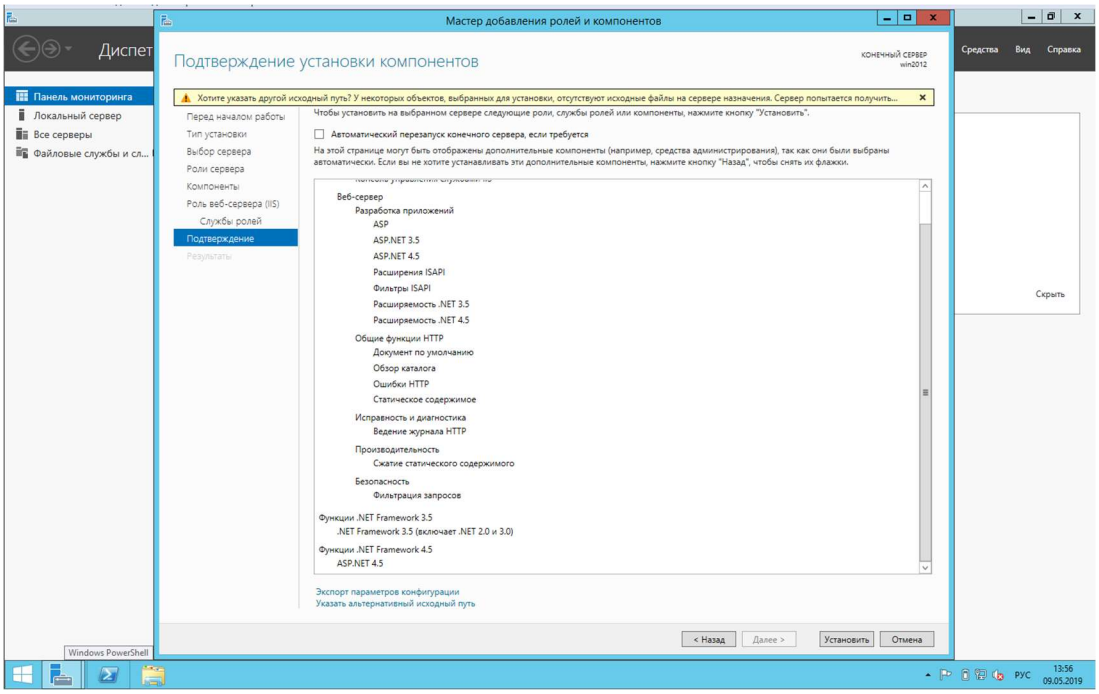


Рисунок 8. Подтверждение установки компонентов.

После нажатия кнопки «Установить» начнется процесс установки новых компонентов – Рисунок 9, по окончанию которого можно переходить к установке СУБД Microsoft SQL Server – подпункт 2.2 данного руководства.

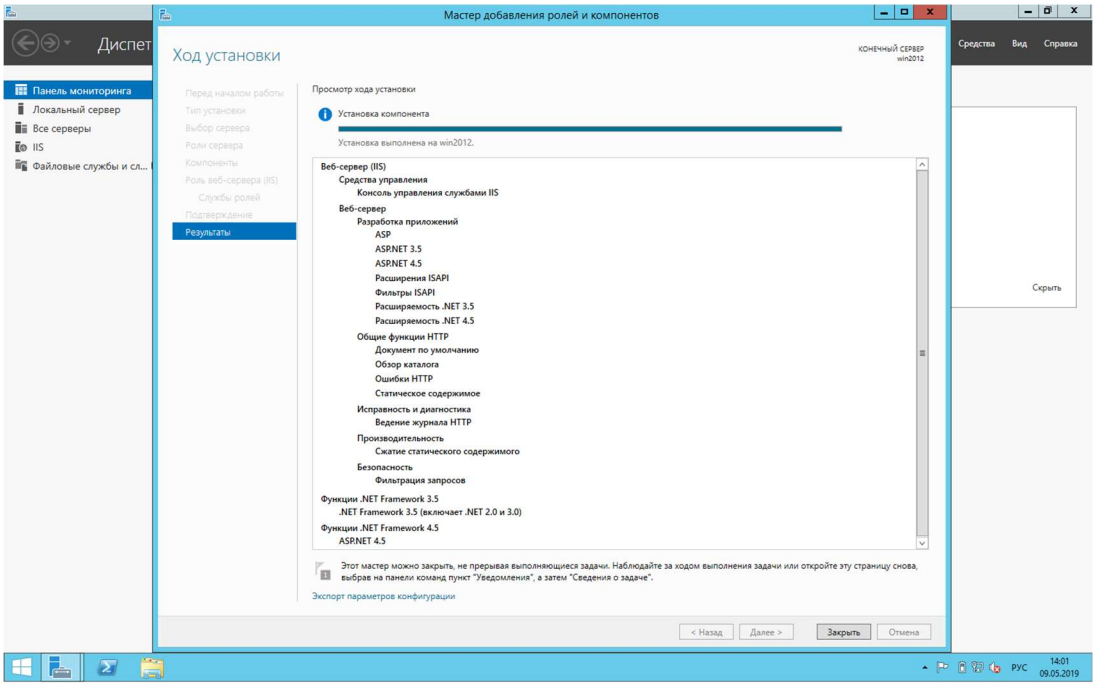


Рисунок 9. Процесс установки компонентов.

## 2.2 Установка СУБД Microsoft SQL Server

Запустите дистрибутив СУБД Microsoft SQL Server и проконтролируйте, что все указанные компоненты сервера СУБД выбраны, как показано на рисунке (Рисунок 10) и нажмите кнопку «Далее».

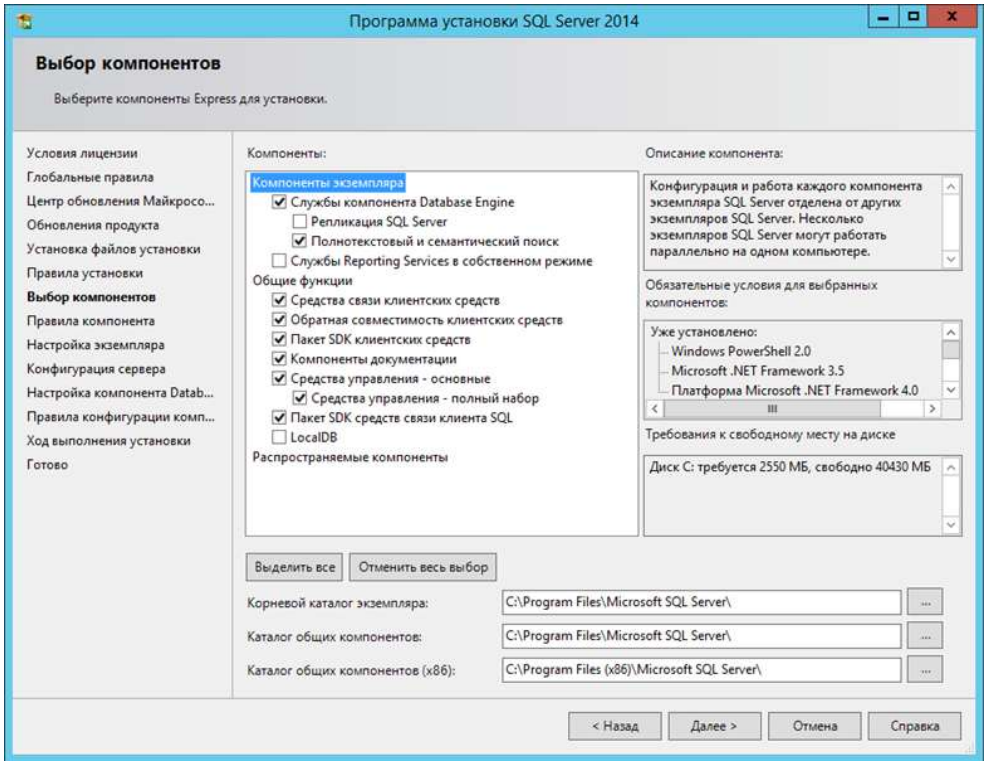


Рисунок 10. Выбор компонентов.

В следующем окне мастера установки СУБД выберите вариант «Экземпляр по умолчанию» и нажмите кнопку «Далее» - Рисунок 11.

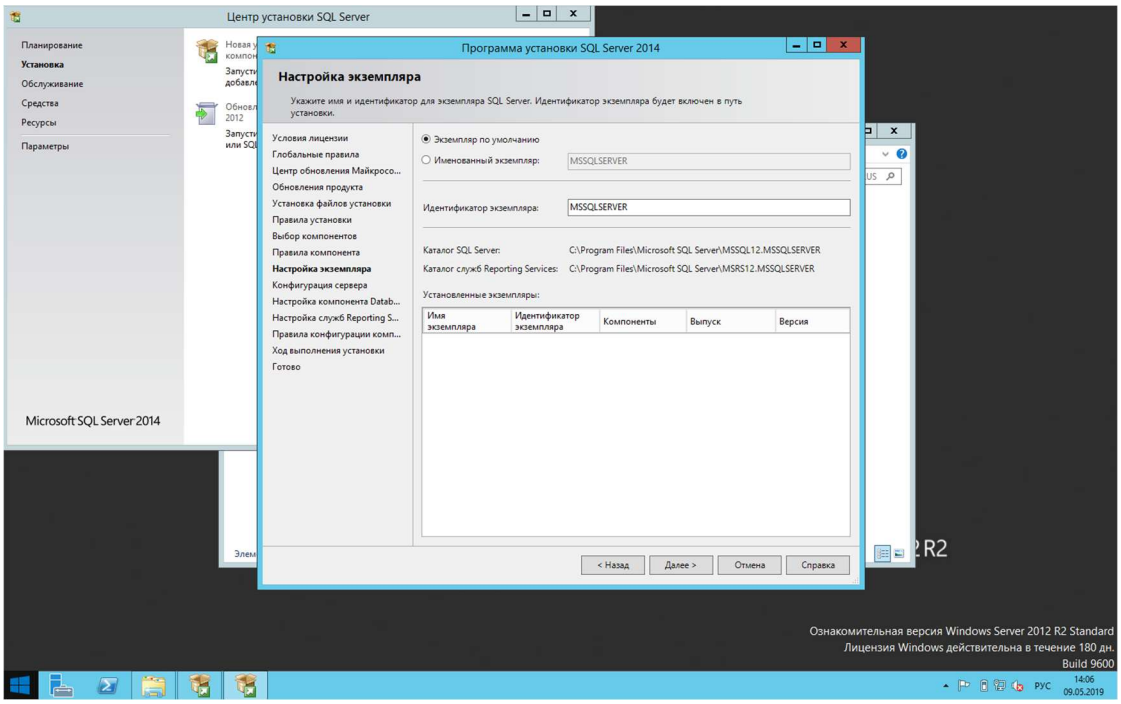


Рисунок 11. Настройка экземпляра.

В следующем окне установите тип запуска служб сервера, как показано на рисунке (Рисунок 12) и нажмите кнопку «Далее».

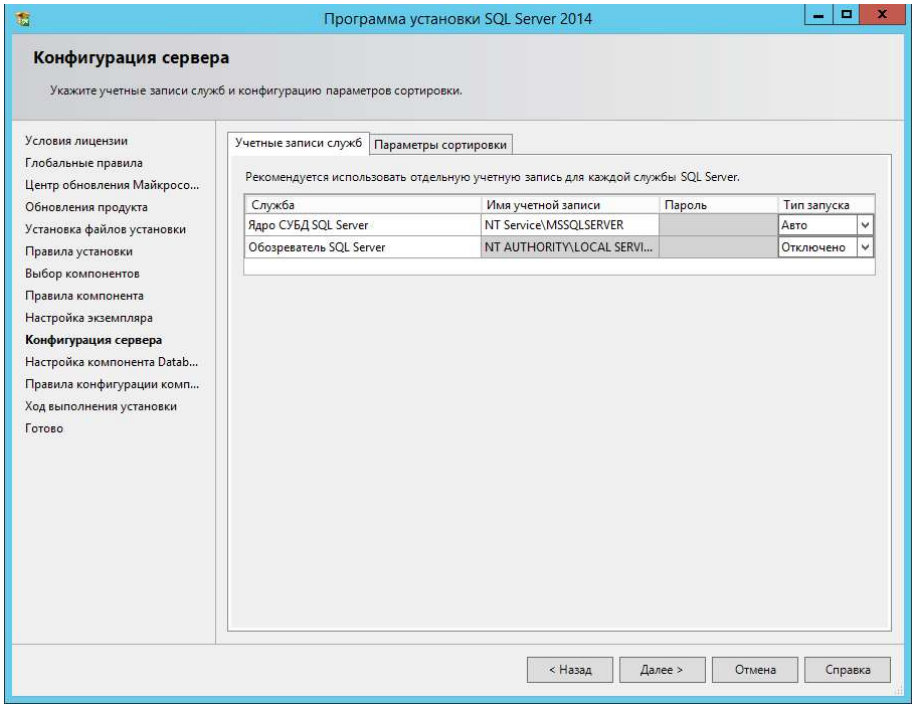


Рисунок 12. Конфигурация служб сервера.

В следующем окне мастера, настройки типа авторизации пользователей оставьте «Режим проверки подлинности Windows» или выберите «Смешанный режим» и укажите пароль для пользователя «sa» и нажмите кнопку «Далее». – Рисунок 13. В зависимости от режима проверки подлинности дальнейшая настройка системы будет отличаться.

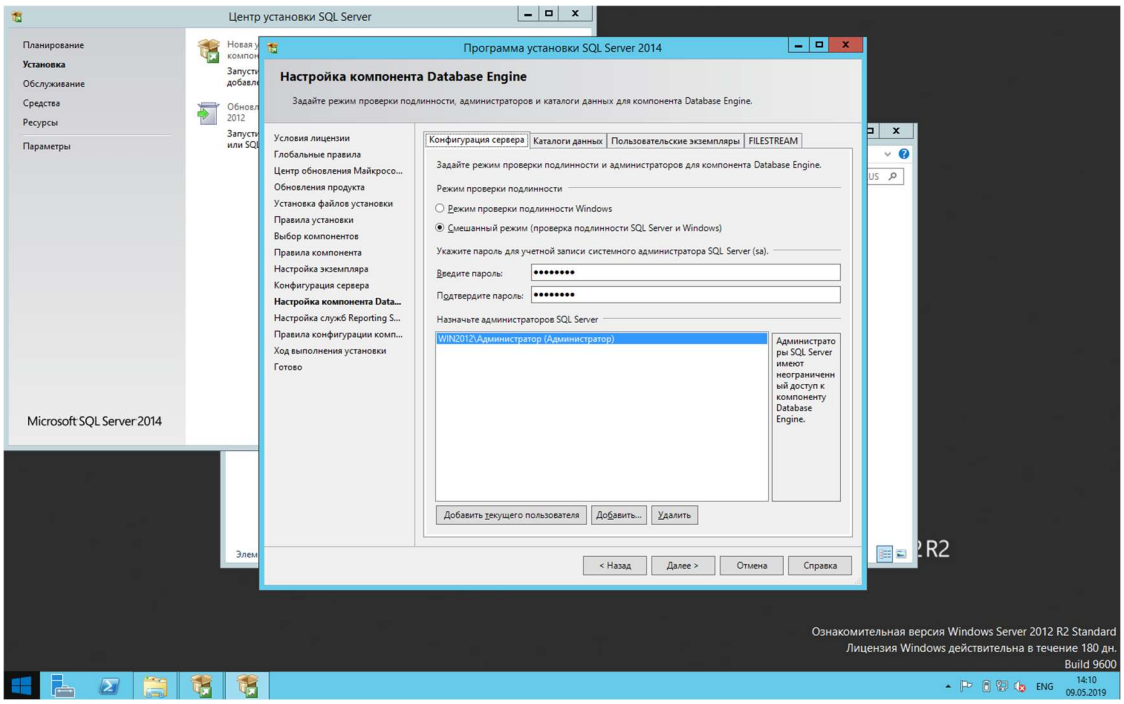


Рисунок 13. Настройка типа авторизации пользователей.

Нажмите кнопку «Далее», которая начнет установку дистрибутива СУБД Microsoft SQL Server – Рисунок 14.

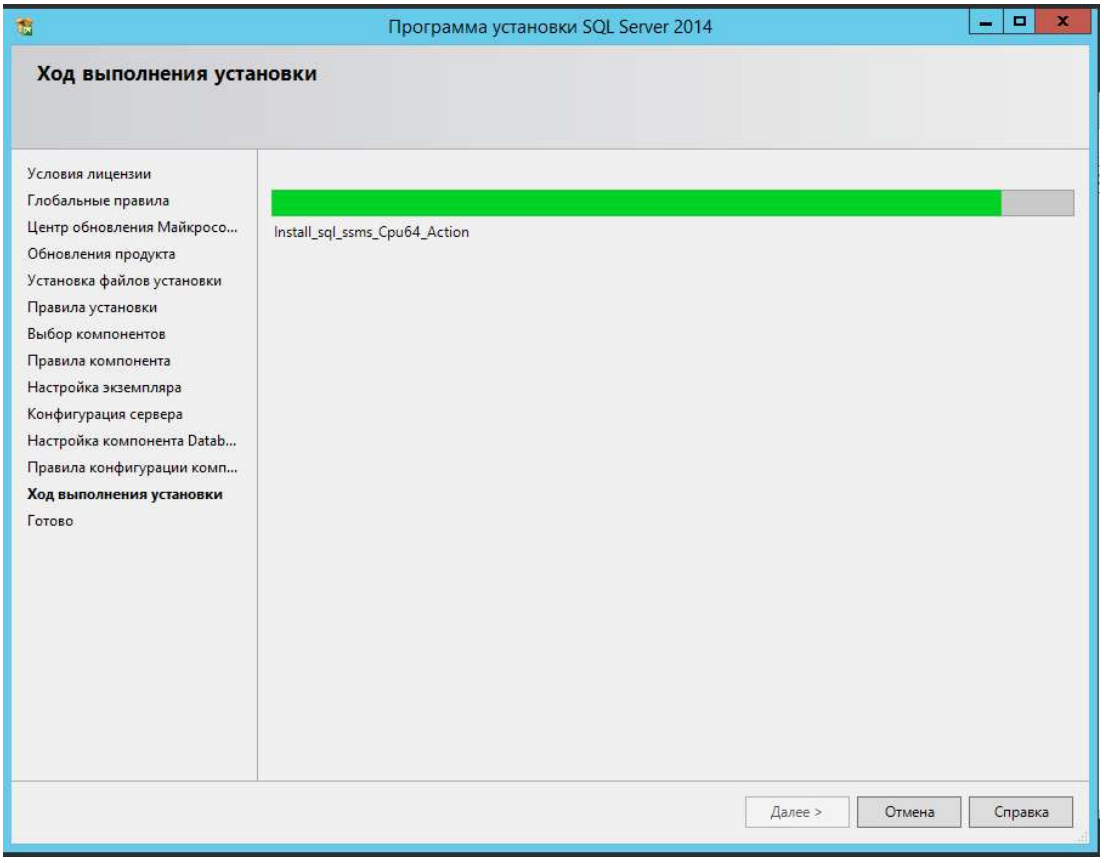


Рисунок 14. Процесс установки СУБД.

По завершению установки появится результирующее окно – Рисунок 15, в котором можно проконтролировать итоги установки, и в случае необходимости провести установку повторно.

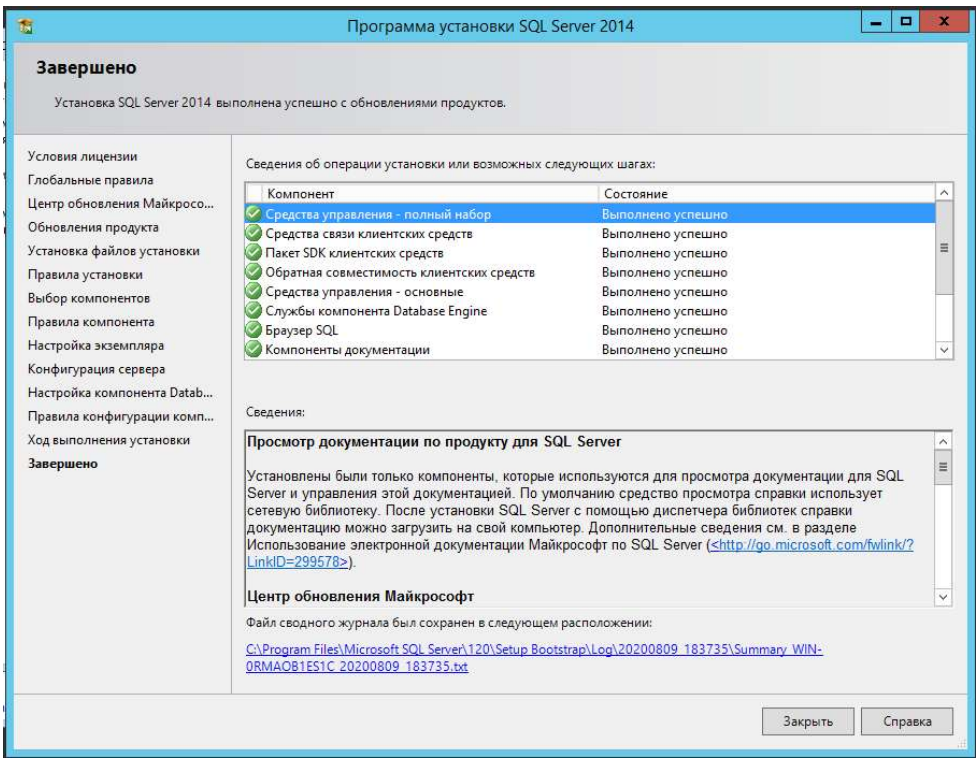


Рисунок 15. Окончание установки СУБД.

В случае успешного завершения установки СУБД можно переходить к установке непосредственно Системы на сервер – раздел 2.3.

## 2.3 Установка Системы

Скопируйте установочные файлы дистрибутивов Системы (SecurityDesk-System-1.*.exe) и сервисов (SecurityDesk-Services-1.*.exe) на сервер и запустите установку Системы (SecurityDesk-System-1.*.exe) с правами администратора сервера – Рисунок 16.

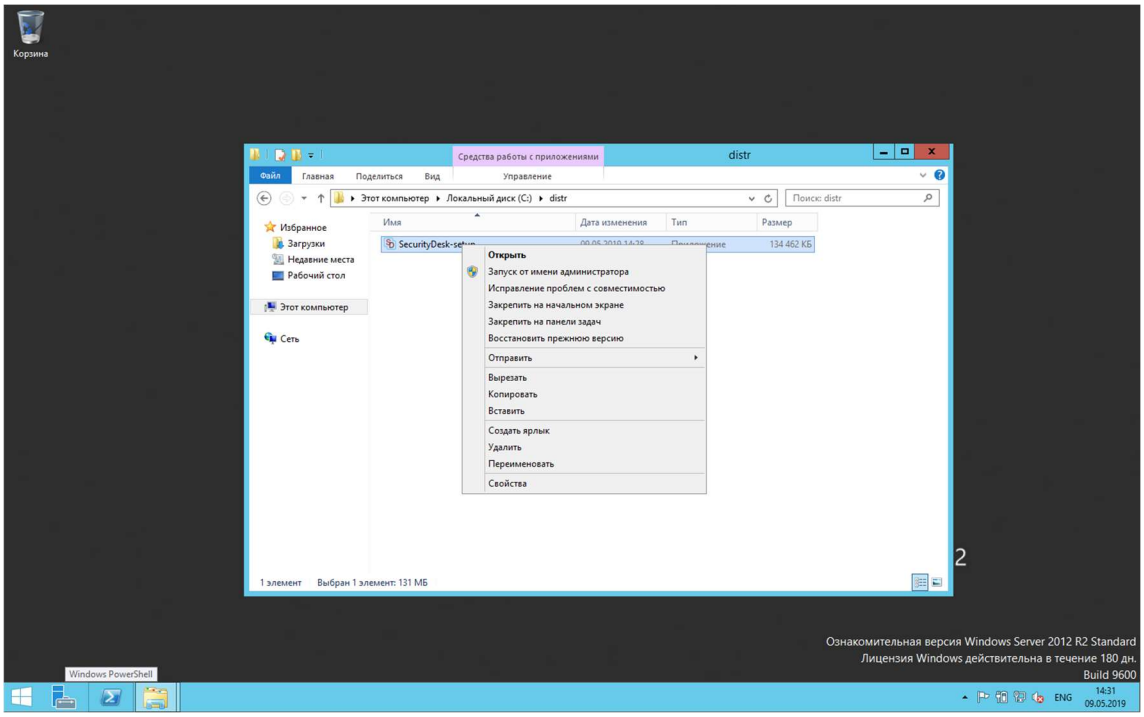


Рисунок 16. Запуск установочного файла системы.

После запуска установочного файла Системы необходимо ознакомится с лицензионным соглашением, и в случае принятия условий соглашений продолжить установку, нажав кнопку «Далее» - Рисунок 17.

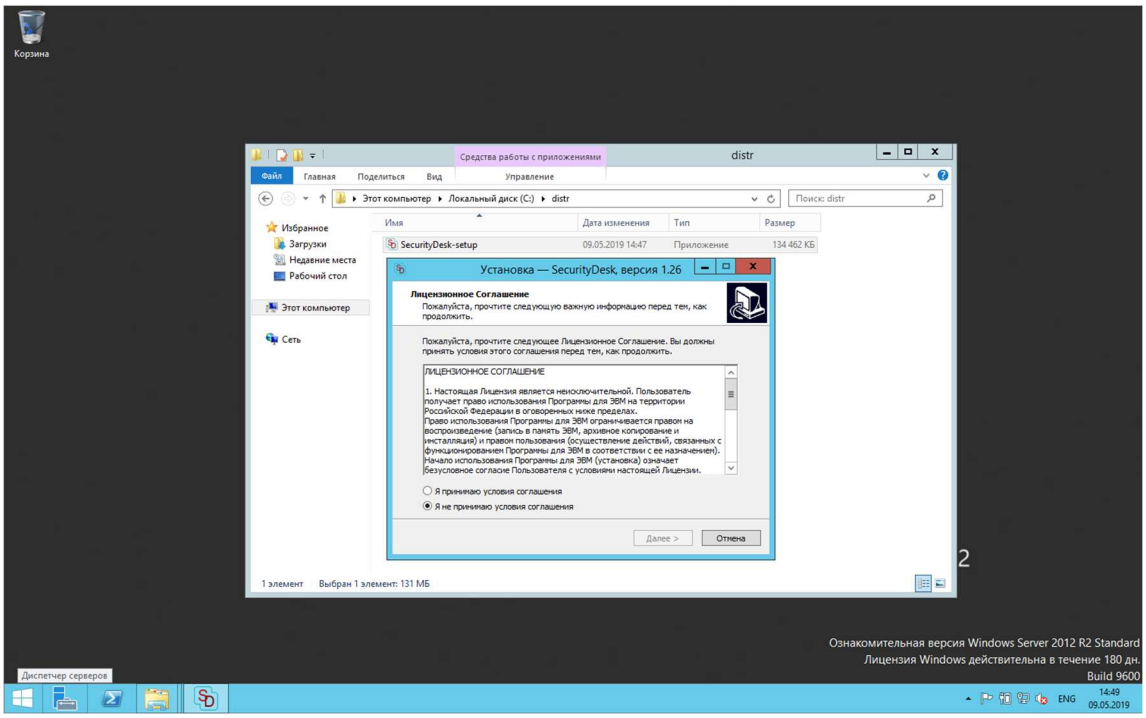


Рисунок 17. Окно лицензионного соглашения.

На следующем шаге инсталлятор проверит наличие установленного дистрибутива .NET Framework и в случае его отсутствия запустит его установку в сценарии установки системы – Рисунок 18.

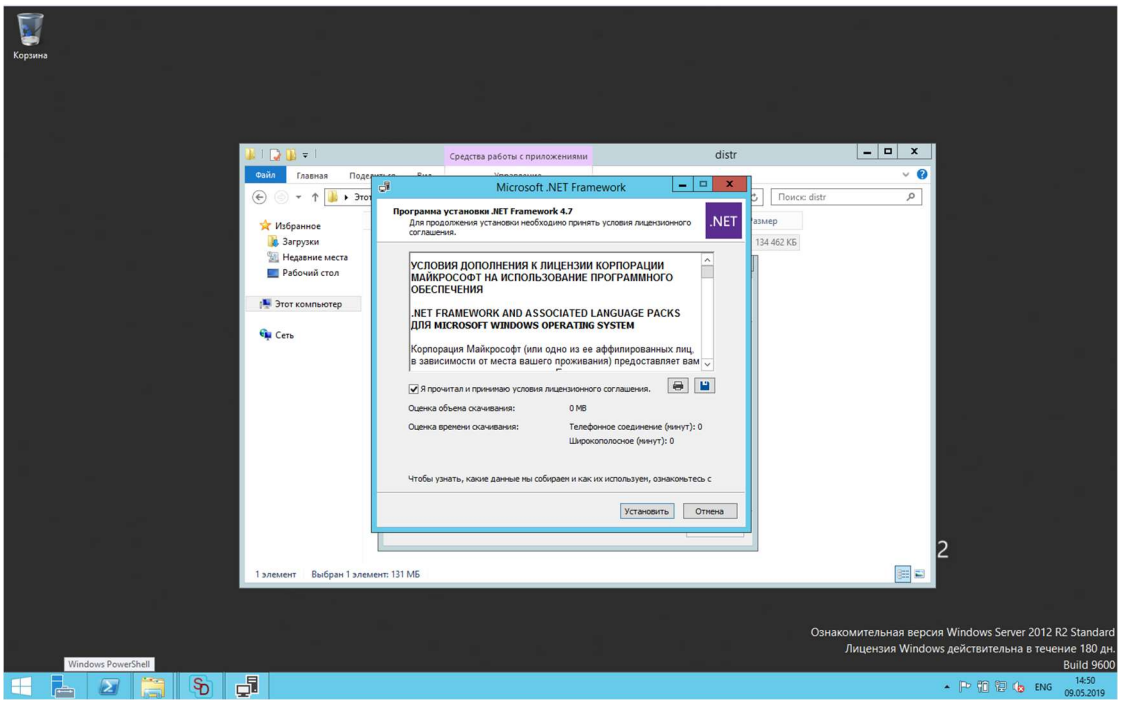


Рисунок 18. Окно установки .NET Framework.

При установке файлов Системы рекомендуется выбрать путь установке, как показано на Рисунок 19 – папка для установки WEB-приложений  IIS.

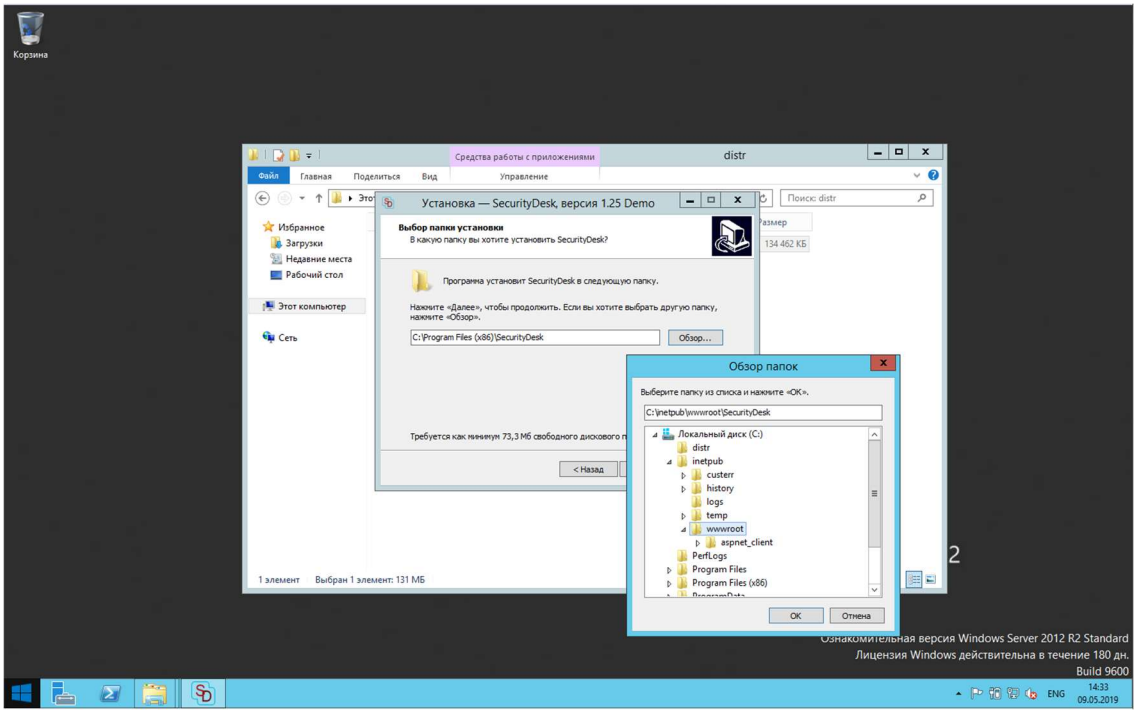


Рисунок 19. Выбор пути установки системы.

После выбора пути установки нажмите на кнопку «Установить» - Рисунок 20 и Система будет установлена на сервер, о чем будет оповещено установщиком, как показано на Рисунок 21.

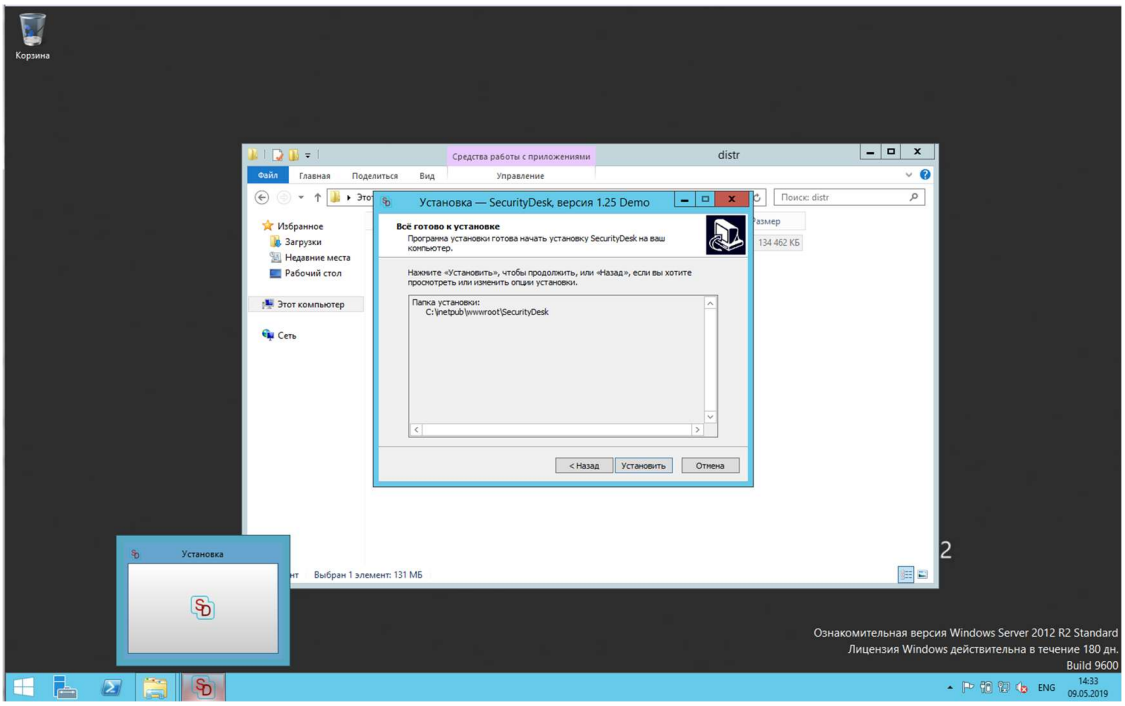


Рисунок 20. Установка системы.

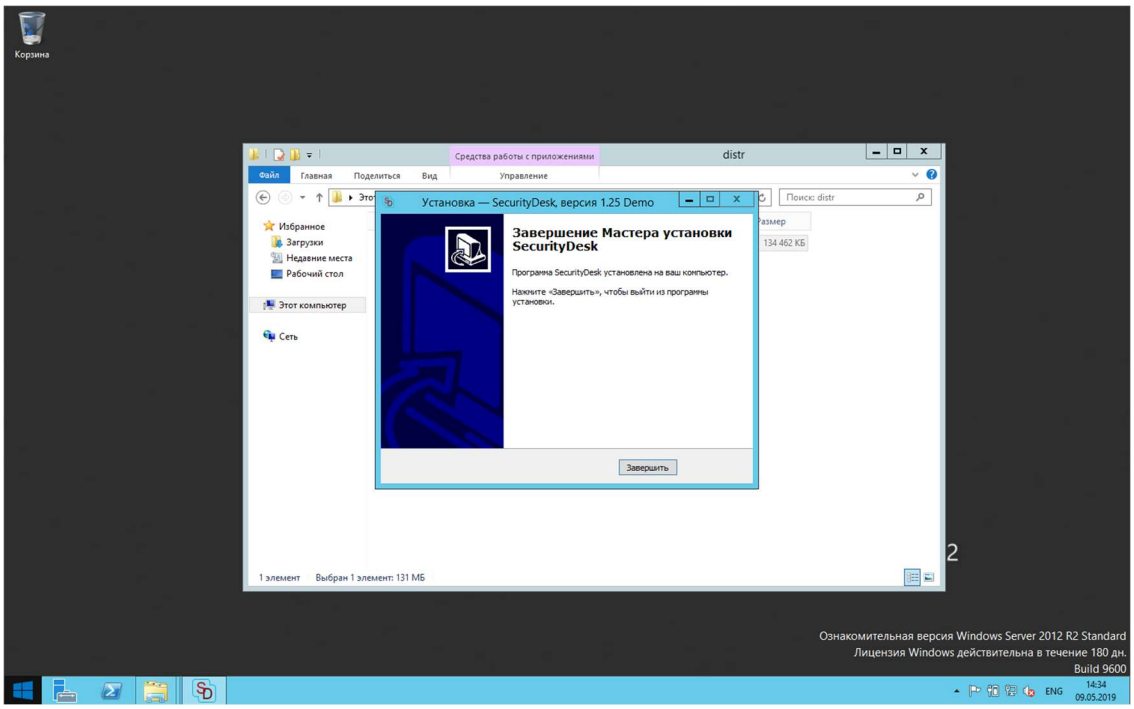


Рисунок 21. Завершение установки системы.

После установки Системы запустите дистрибутив с сервисами (SecurityDesk-Services-1.*.exe). Установка дистрибутива сервисов полностью аналогична установке Системы, за исключением пути установки. В качестве пути установки сервисов рекомендуется выбирать папку «C:\Program Files\SecurityDesk».

## 2.4 Установка базы данных и параметров подключения к СУБД Microsoft SQL Server

Для установки и настройки базы данных Системы откройте установленное средство управления СУБД Microsoft SQL Server Management Studio - Рисунок 22 и подключитесь к Microsoft SQL Server - нажав кнопку «Соединить».

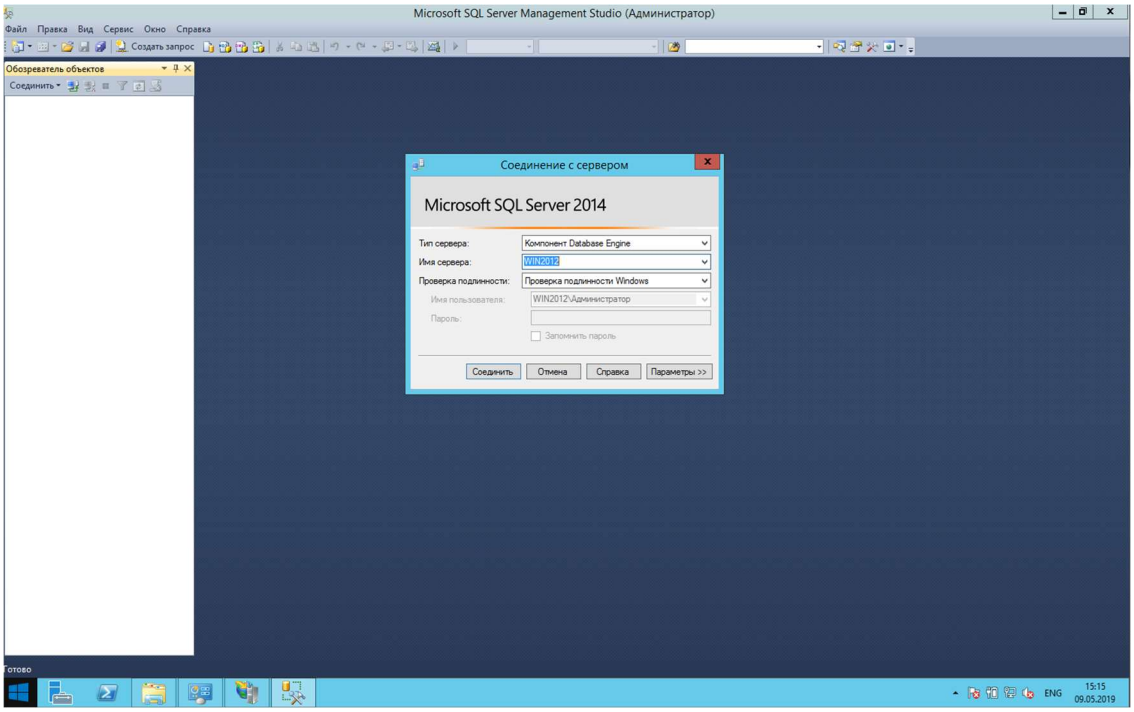


Рисунок 22. Подключение к СУБД Microsoft SQL Server.

Подключившись к SQL Server убедитесь, нажав правой кнопкой мыши на пиктограмме сервера в левой части окна и выбрав из контекстного меню параметр «Свойства» во вкладке «Безопасность», что переключатель «Серверная проверка подлинности» установлен в необходимый режим проверки подлинности «Проверка подлинности Windows» или «Проверка подлинности SQL Server и Windows» - Рисунок 23.

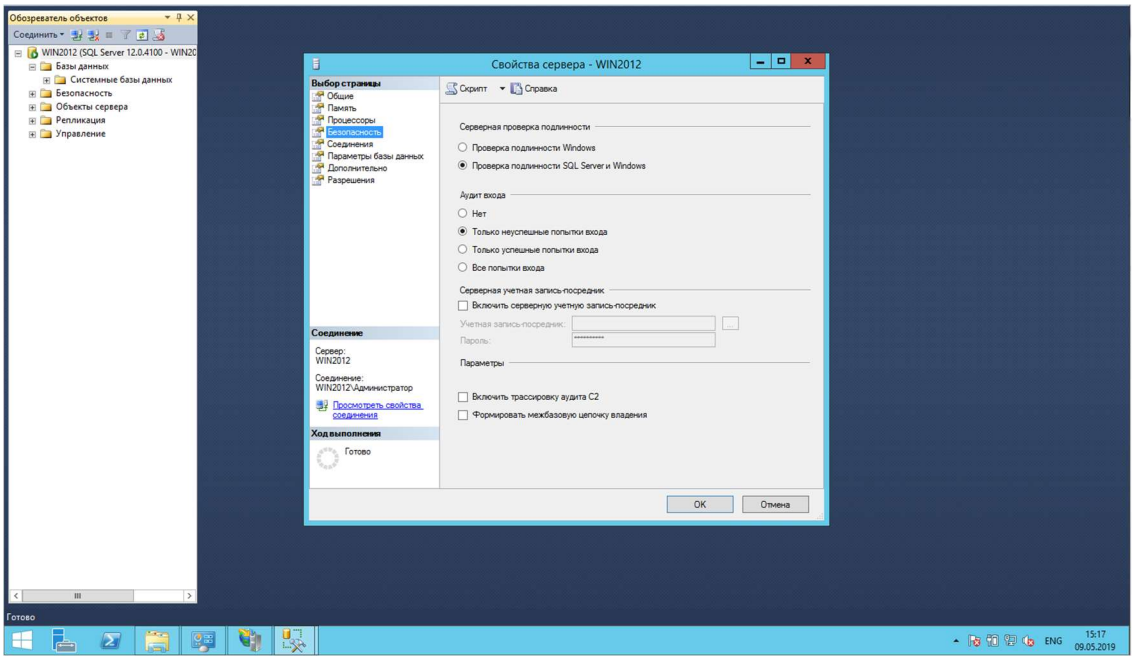


Рисунок 23.Проверка параметров проверки подлинности.

В левой части окна выберите папку «Базы данных», правой кнопкой мыши вызовите контекстное меню выберите в меню параметр «Восстановить базу данных» - Рисунок 24.

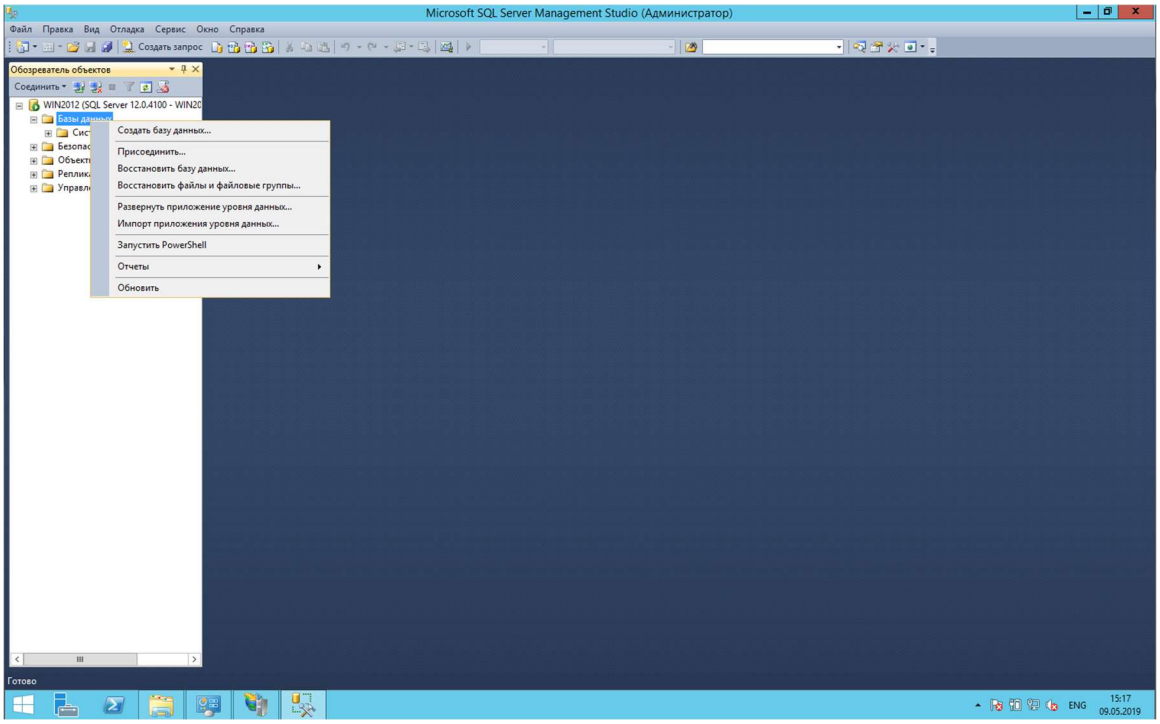


Рисунок 24. Установка новой базы данных.

В качестве источника восстановления в появившемся окне установите переключатель в положение «Устройство», далее нажав на кнопку «…» выберите тип устройства резервного копирования «Файл», нажмите кнопку «Добавить» и найдите резервную копию базы SecurityDB.bak по пути установки Системы, в подпапке «Docs» – Рисунок 25, после чего нажмите кнопку «ОК».

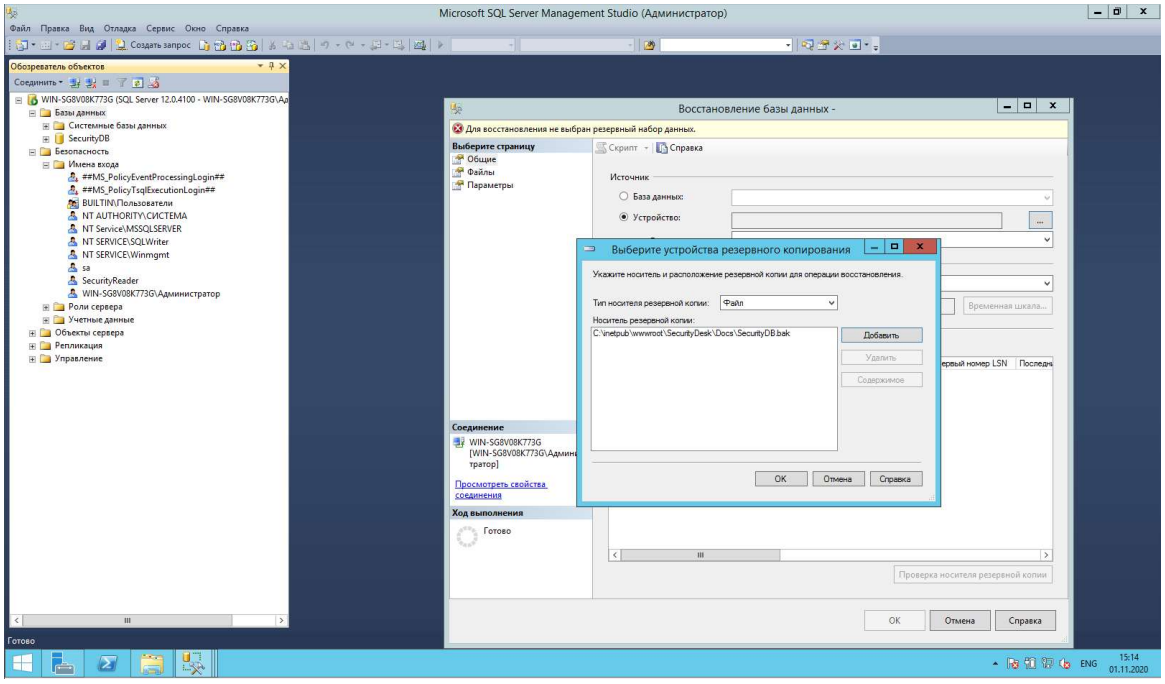


Рисунок 25. Выбор источника восстановления базы данных.

Поле выбора источника восстановления нажмите кнопку «Ок», на окне восстановления базы данных, чтобы запустить процесс восстановления – Рисунок 26.

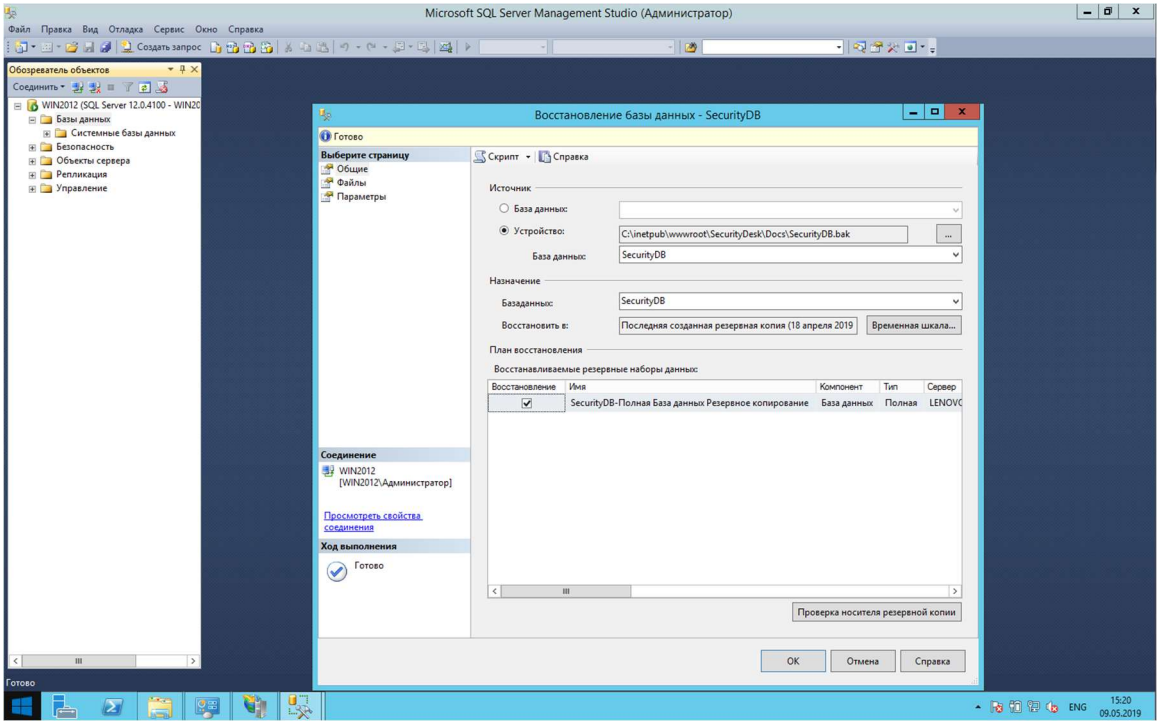


Рисунок 26. Выбранный источник восстановления базы данных.

В случае успешного восстановления базы данных из выбранного источника SQL Server оповестит вас соответствующим сообщением – Рисунок 27, а в перечне баз данных, доступных на сервере появится база данных «SecurityDB».

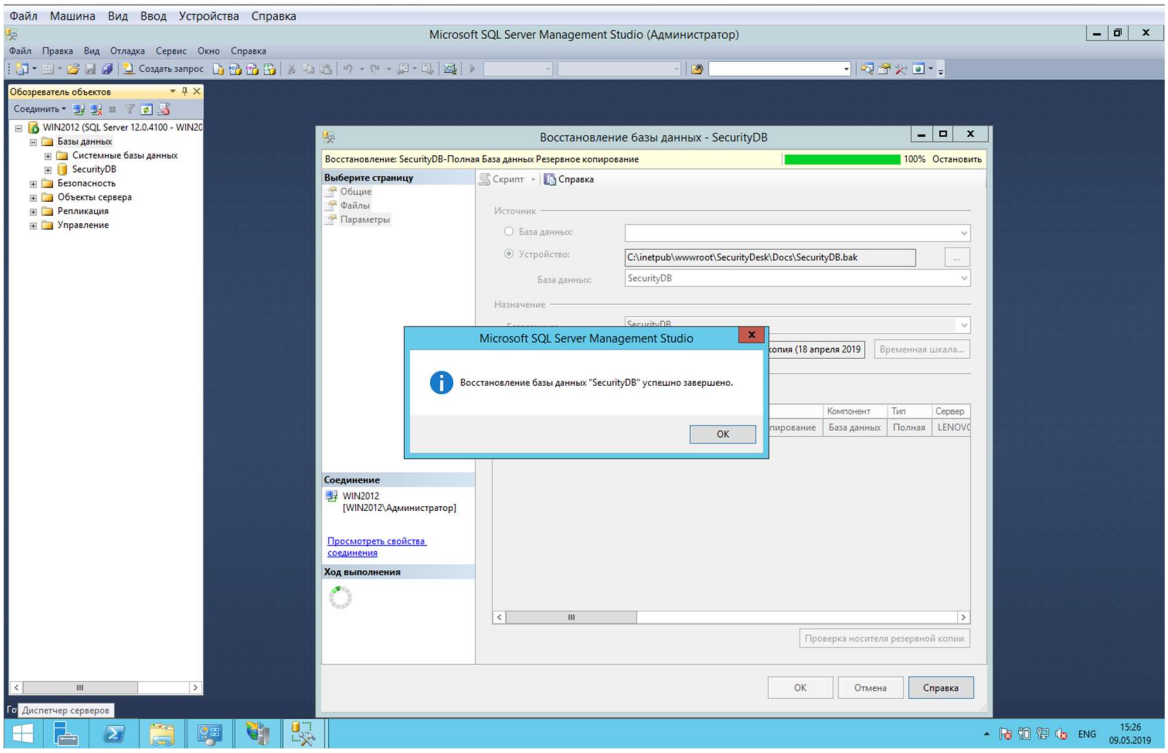


Рисунок 27. Процесс восстановления базы данных.

После успешного создания базы данных Системы необходимо добавить (в случае проверки пользователя **Windows**) или создать пользователя (в случае проверки подлинности **SQL Server**), с помощью которого Система будет осуществлять доступ к базе данных:

- Для добавления пользователя Windows (предварительно обратитесь к администратору Windows для создания специальной учетной записи пользователя Windows, для доступа к базе данных Системы) в левой части окна Microsoft SQL Server Management Studio откройте папку «Безопасность», «Имена входа», далее нажав правой кнопкой мыши и выбрав контекстное меню, выберите пункт «Создать имя входа». В появившемся окне создания имени входа убедитесь, что переключатель «Имя входа» установлено в положение «Проверка подлинности Windows». Нажмите кнопку «Найти» и в появившемся окне выбора пользователей введите требуемое имя сервисной учетной записи Windows, с помощью которой будет предоставляться доступ Системе к базе данных - Рисунок 28. Далее нажмите кнопку «Проверить имена», чтобы удостовериться в правильности введенного имени учетной записи Windows, и в случае успешной проверки нажмите кнопку «ОК». Выберите базу данных по умолчанию «SecurityDB» и язык по умолчанию «Russian».

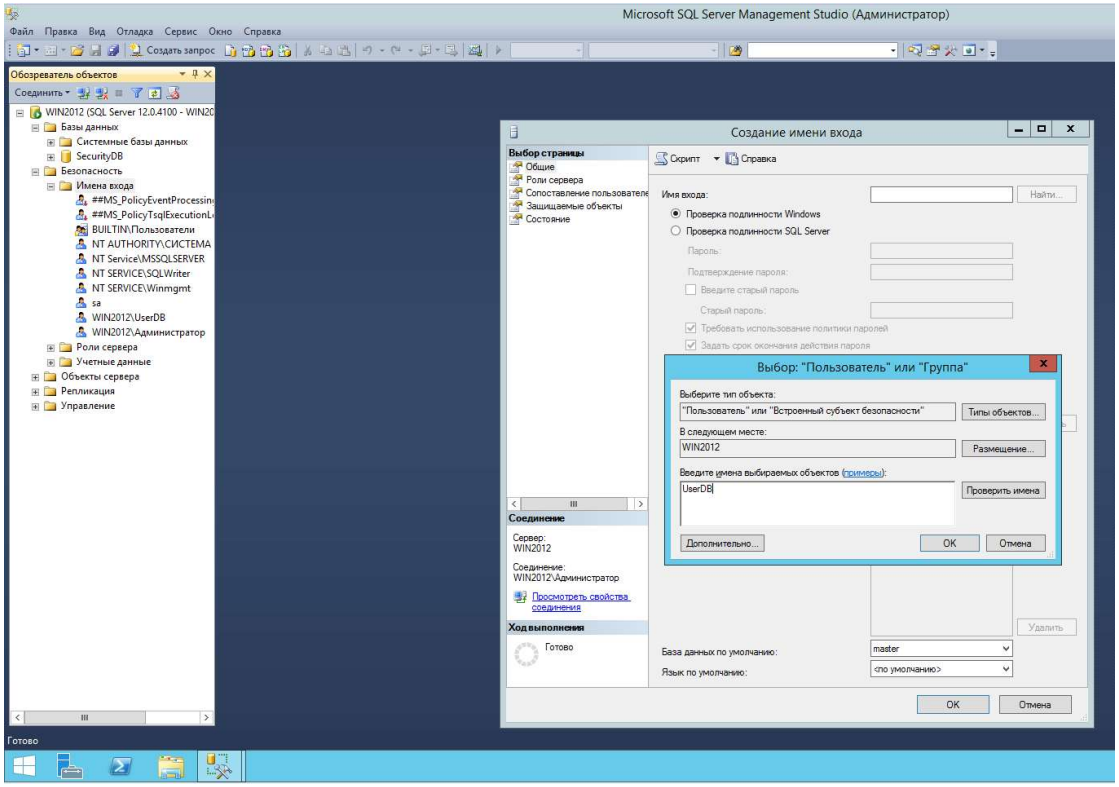


Рисунок 28. Настройка доступа к базе данных пользователю Windows.

- Для создания нового пользователя в режиме проверки SQL Server в левой части окна Microsoft SQL Server Management Studio откройте папку «Безопасность», «Имена входа», далее нажав правой кнопкой мыши и выбрав контекстное меню, выберите пункт «Создать имя входа». В появившемся окне создания имени входа задайте имя пользователя в окне «Имя входа», выберите «Проверка подлинности SQL Server», введите пароль, снимите флаг «Задать срок окончания действия пароля», выберите базу данных по умолчанию «SecurityDB» и язык по умолчанию «Russian» - Рисунок 29.

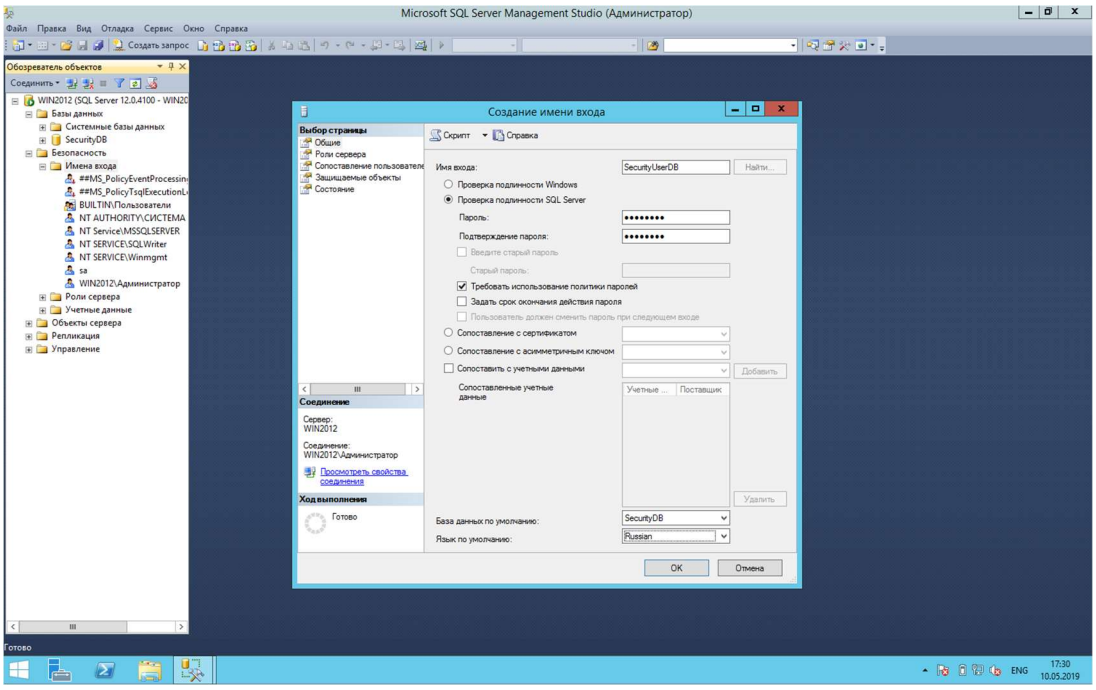


Рисунок 29. Создание пользователя в SQL Server для доступа к базе данных.

В левой части окна создания имени входа «Выбор страницы» нажмите на пункт «Сопоставление пользователей» базы данных – Рисунок 30. Поставьте галочку в колонке «Схема» напротив базы данных «SecurityDB» и галочку в поле «Членство в роли базы данных: SecurityDB» напротив роли «**db_owner**», после чего нажмите «ОК» и в СУБД будет создан новый пользователь.

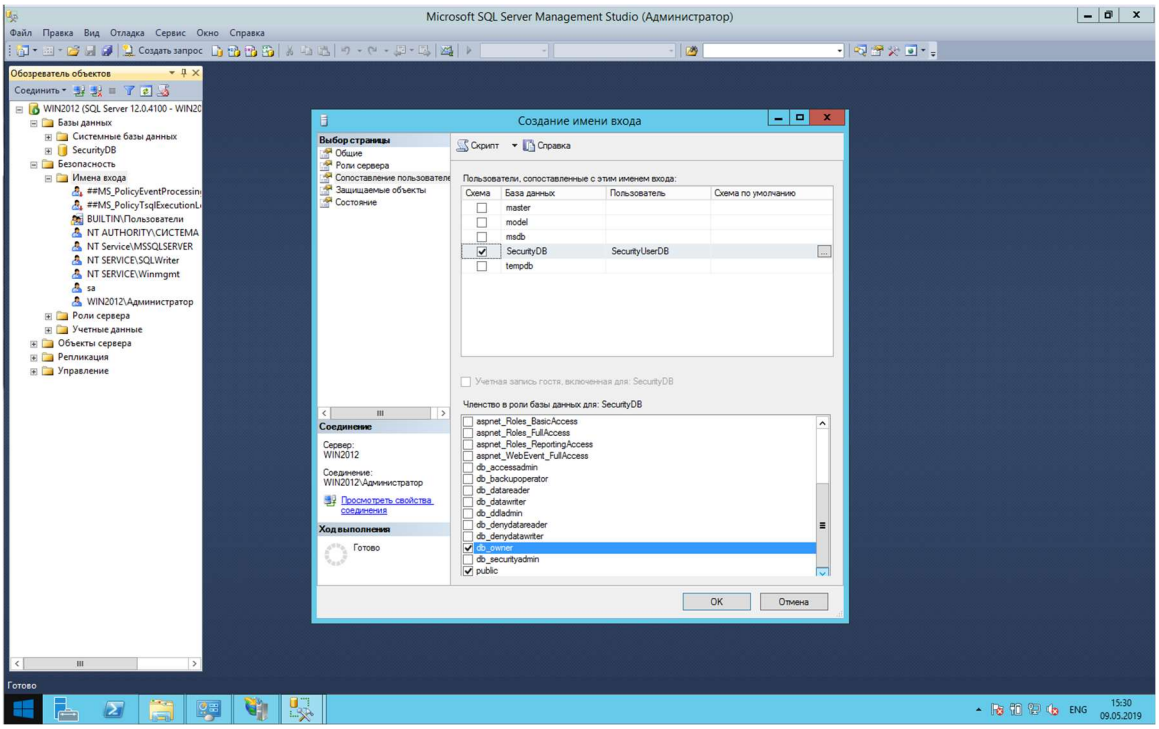


Рисунок 30. Настройка доступа к базе данных.

Работа по настройке Microsoft SQL Server закончена, закройте приложение Microsoft SQL Server Management Studio и переходите к пункту 2.5.

## 2.5 Настройка компонентов Системы

Настройка Web-сервера Системы производится через «Диспетчер служб IIS», который находится в разделе «Администрирование». Для работы Системы необходимо удалить (или остановить) сайт, созданный по умолчанию, далее в папке «сайты» создайте через контекстное меню новый сайт, задав имя сайта «**SecurityDesk**», выбрав физический путь установки дистрибутива (рекомендуется «**C:\inetpub\wwwroot\SecurityDesk**»), остальные параметры можно оставить по умолчанию - Рисунок 31.

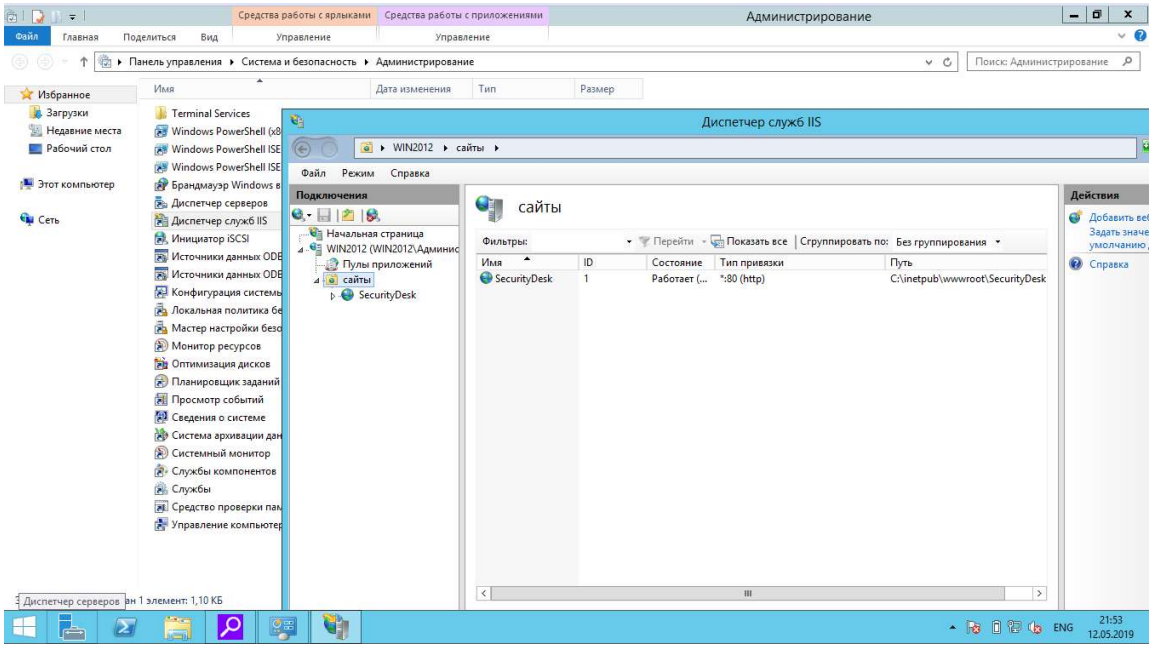


Рисунок 31. Настройка web-сервера.

Внимание! Чтобы исключить возможность перехвата передаваемых данных на web-сервер рекомендуется настроить соединение по протоколу https - расширение протокола http, поддерживающее шифрование. Для настройки доступа по https перейдите в IIS на узел web-сервера и дважды щелкните по пиктограмме «Сертификаты сервера» - Рисунок 32.

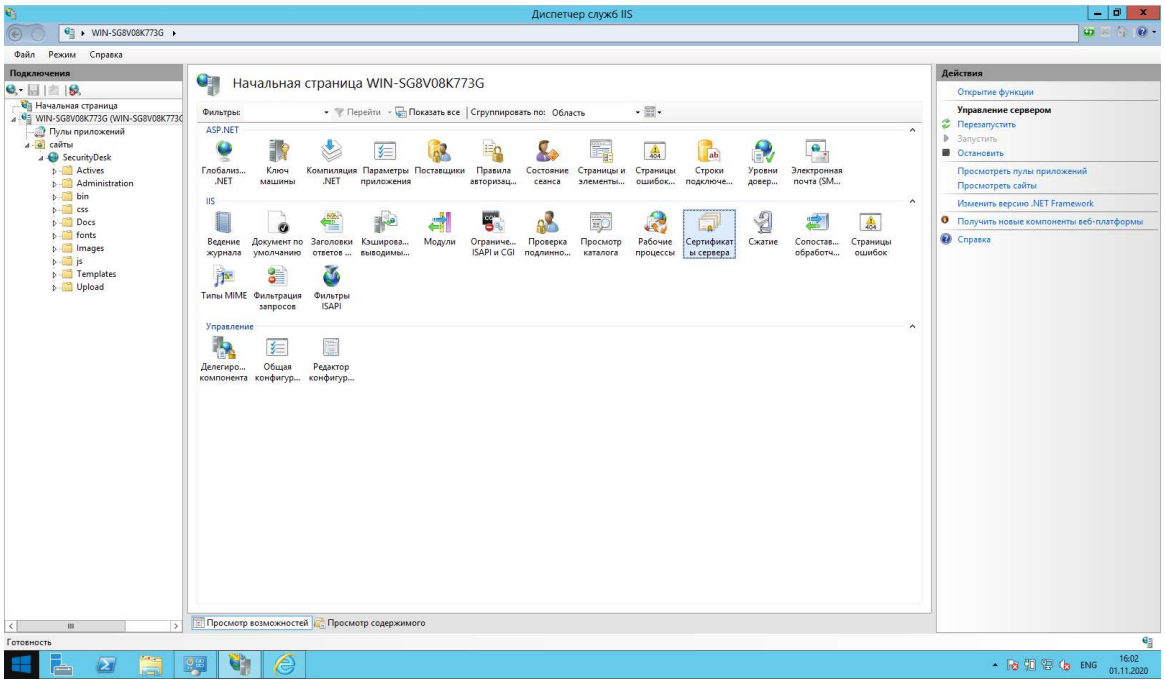


Рисунок 32. Настройка сертификата на web-сервере.

Перейдя в раздел сертификаты - Рисунок 33 в разделе «**Действия**» (правая часть экрана) импортируйте сертификат, полученный от администратора сервера сертификатов с помощью ссылки **«Импортировать»** или в более простом варианте можно сгенерировать и установить «самоподписанный» сертификат – ссылка «**Создать самозаверенный сертификат**».

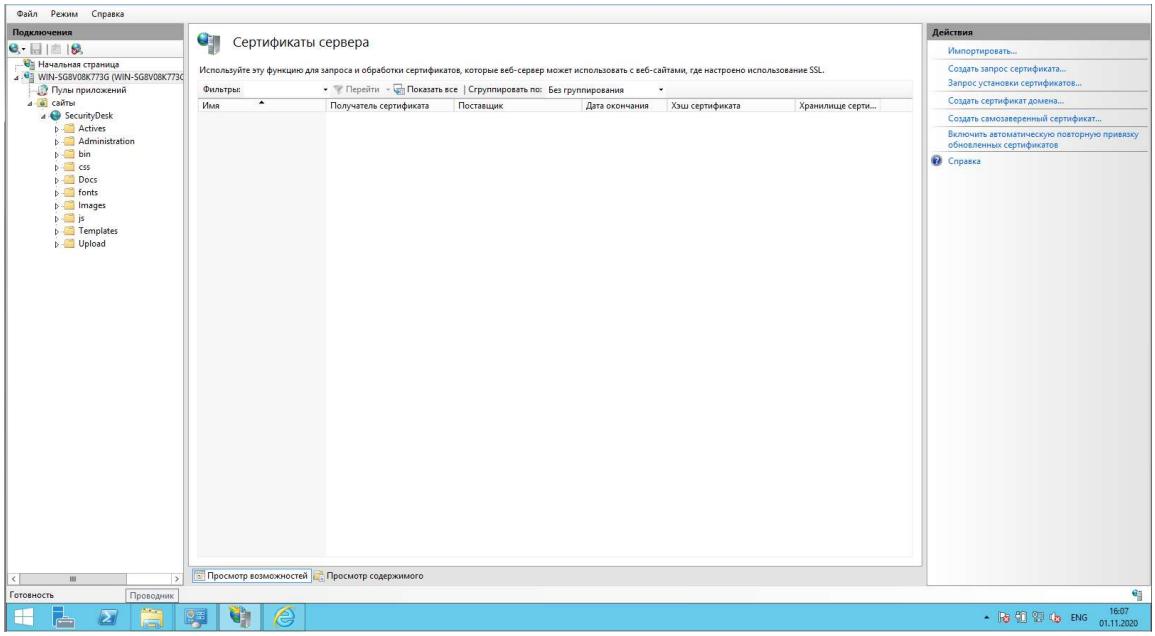


Рисунок 33. Раздел сертификатов.

Чтобы создать «самоподписанный» сертификат перейдите по ссылке «**Создать самозаверенный сертификат**» и в открывшемся окне введите название сертификата в поле «**Понятное имя сертификата**» - Рисунок 34 и нажмите «Ок», после чего в списке сертификатов сервера - Рисунок 33 появится новый сертификат.

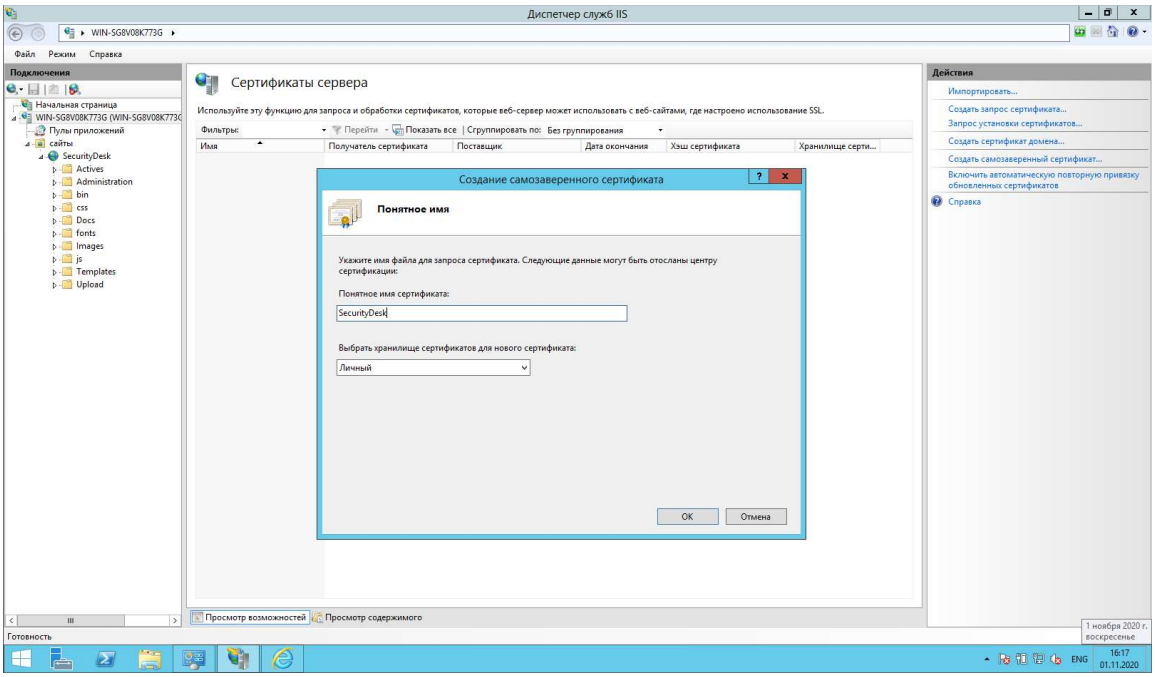


Рисунок 34. Создание самоподписанного сертификата.

После того как сертификат создан (импортирован) перейдите в узел web-приложения в Диспетчере служб IIS-сервера и выберите ссылку «**Привязки**» в разделе «**Действия**» (правая часть экрана) – Рисунок 35.

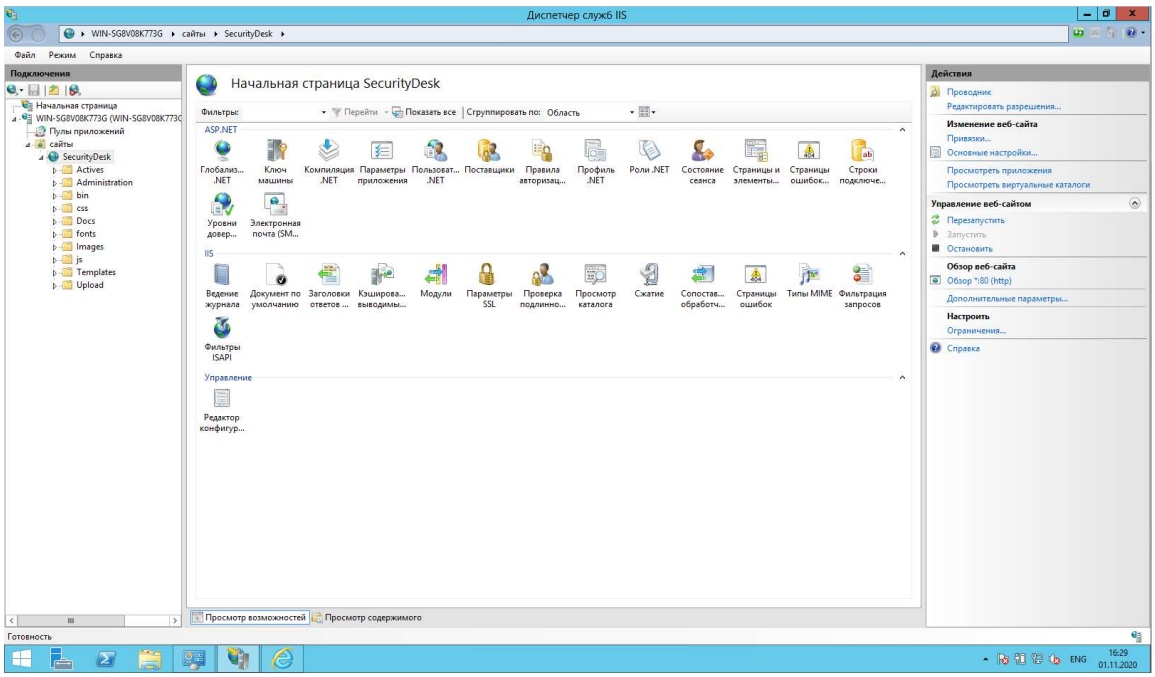


Рисунок 35. Настройка привязки сертификата к web-сайту.

В открывшемся окне привязки сайта нажмите кнопку «**Добавить**» и в окне «**Добавление привязки сайта**» выберите тип **https**, а в выпадающем списке созданный/импортированный SSL-сертификат и нажмите «Ок» - Рисунок 36. Доступ к сайту по протоколу https настроен, в окне привязок сайта можно удалить соединение по протоколу http.

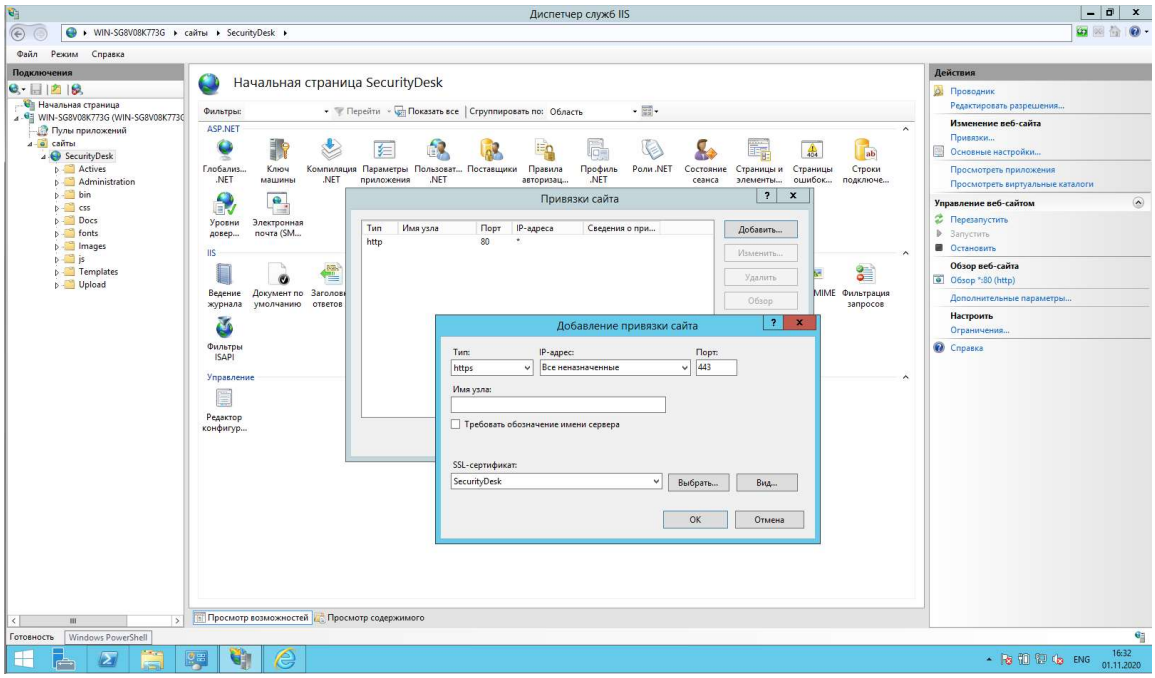


Рисунок 36. Установка сертификата.

Внимание! Для корректного формирования системой отчетов из карточек Инцидентов, Задач и Уязвимостей, и возможности загрузки журналов сканирования в систему необходимо после установки дистрибутива Системы предоставить возможность пулу приложения IIS право записи на подпапку «Upload» Системы. Делается это через

контекстное меню, вызвав его на папке Upload правой клавишей мыши. Вкладка «Безопасность», кнопка «Изменить», в окне разрешений кнопка «Добавить». В появившемся окне ввести «**IIS AppPool\[Имя пула]»** - Рисунок 37, нажмите кнопку «Проверить имя» и в случае если операционная система отобразит требуемый пул приложения нажмите кнопку «ОК».

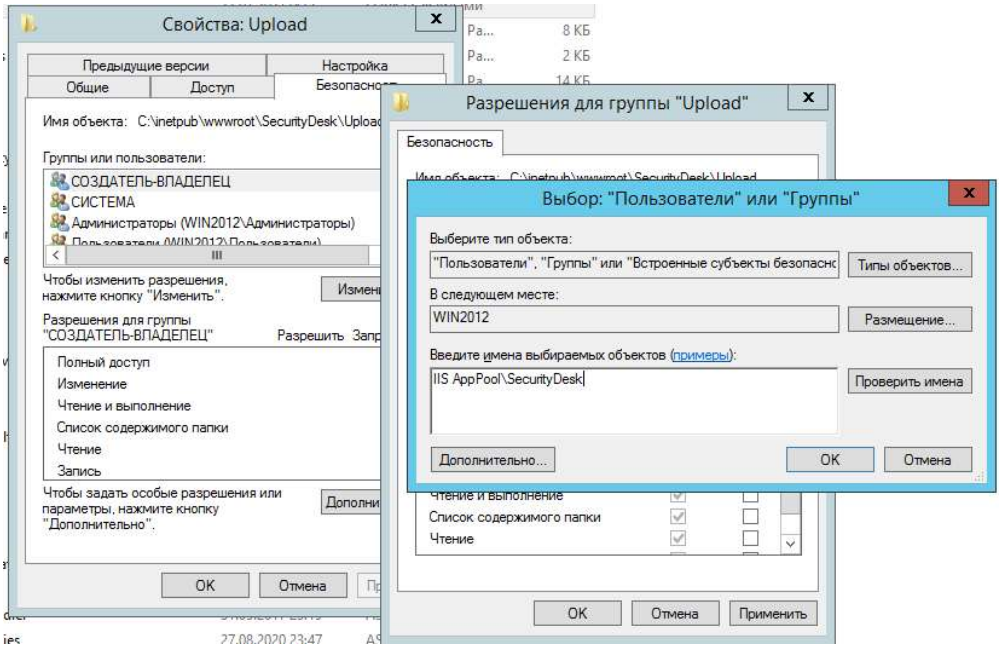


Рисунок 37. Настройка доступа пула приложения.

Добавьте для пула приложения возможность изменения содержимого в папке с помощью соответствующей галочки – Рисунок 38.

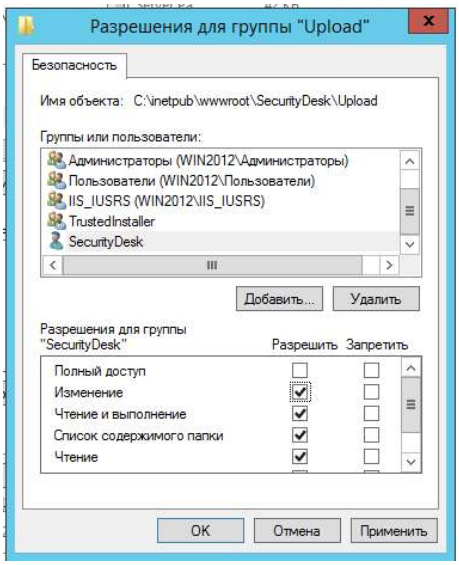


Рисунок 38. Добавление разрешения записи в папку Upload.

В случае использования доступа к базе данных проверки подлинности Windows необходимо дополнительно настроить пул web-приложения - Рисунок 39. Для настройки перейдите в оснастку управления IIS, в левой части окна выберите пункт «Пулы приложений». В центральной части оснастки найдите пул приложения системы

«SecurityDesk» и в правой части оснастки IIS выберите пункт «Дополнительные параметры». В открывшемся окне дополнительных параметров пула приложения найдите пункт «Удостоверение», выбрав данный пункт, нажмите на кнопку с изображением «…». В появившемся окне «Удостоверение пула приложений» установите переключатель в положение «Особая учетная запись» и нажмите кнопку «Установить», далее в окне «Задание учетных данных» введите имя и пароль учетной записи пользователя Windows, которому предоставлен доступ к базе данных, согласно п.2.4.

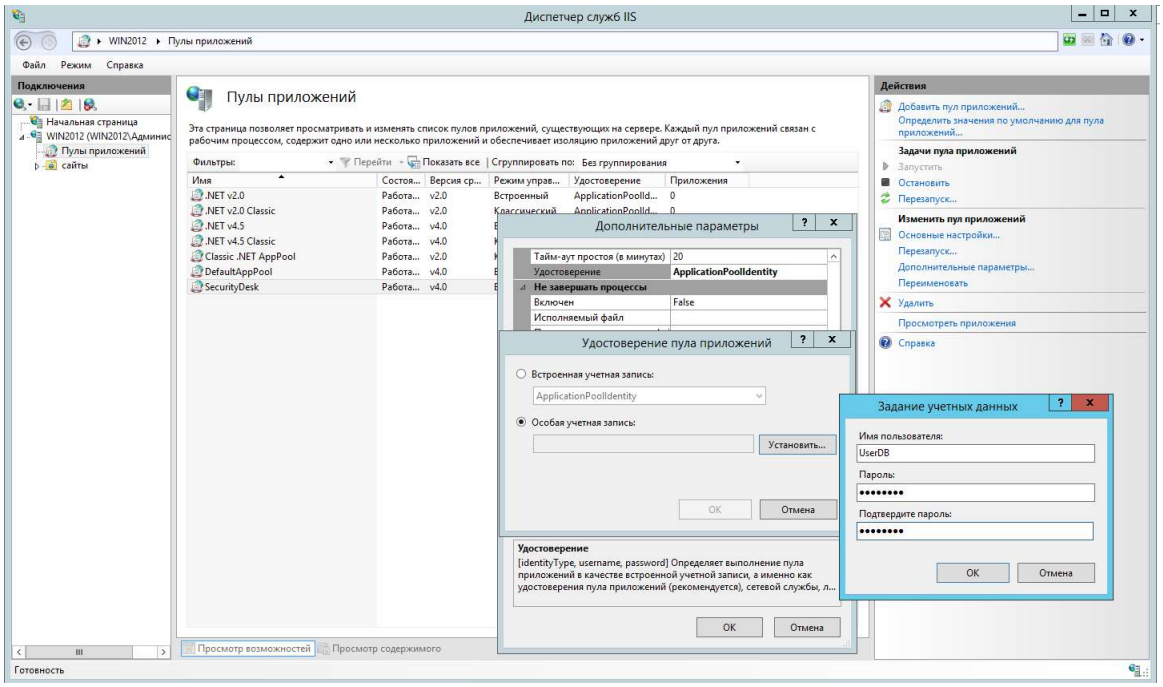


Рисунок 39. Настройка пула приложения.

### 2.5.1 Настройка основного конфигурационного файла

Для настройки подключения Системы к базе данных откройте с помощью блокнота Notepad конфигурационный файл «web.config», который расположен в корне директории с установленной системой – Рисунок 40.

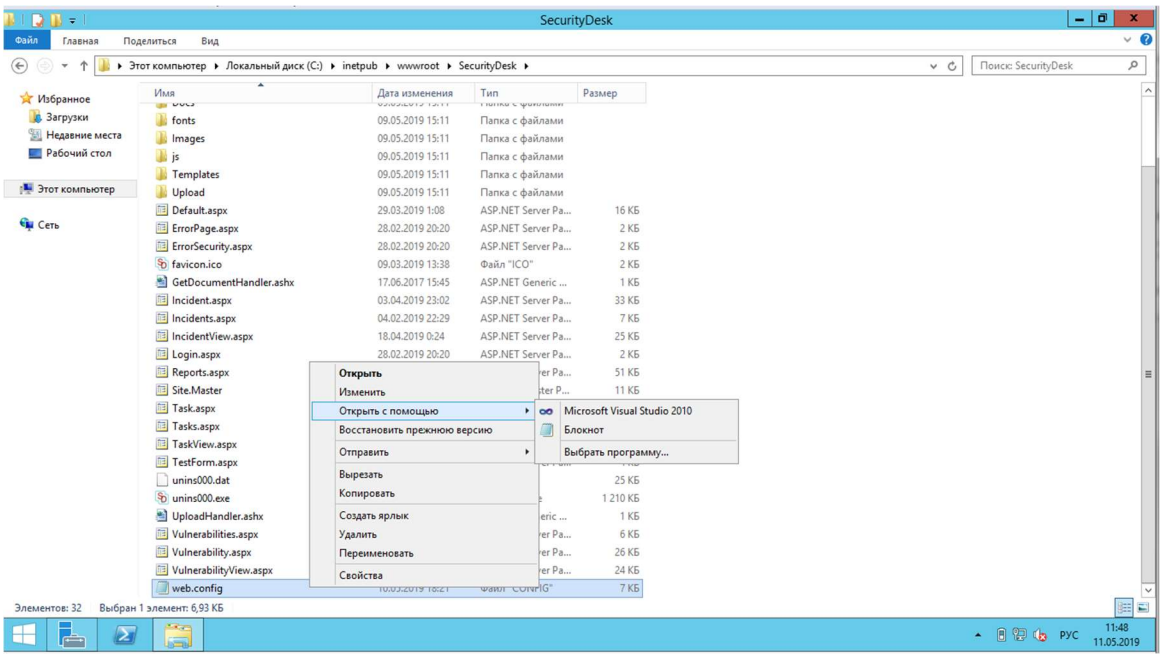


Рисунок 40. Настройка конфигурационного файла.

В зависимости от того какой режим проверки подлинности в SQL Server был выбран настройка строки подключения будет отличаться:

- При настройке доступа к базе данных с помощью проверки подлинности Windows строка подключения должна выглядеть следующим образом – Рисунок 41. В конфигурационном файле найдите раздел «ConnectionStrings», в строке «DatabaseConnection» заполняются данные по адресу SQL Server и имени базы данных.

```
<connectionStrings>
  <clear />
  <add name="LocalSqlServer" connectionString="data source=.\SQLEXPRESS;Integrated Security=SSPI;AttachDBFilename=|DataDirectory|a
  <add name="OraAspNetConString" connectionString=" " providerName="" />
  <add name="DatabaseConnection" connectionString="Data Source=localhost;Initial Catalog=SecurityDB;Integrated Security=SSPI"/>
</connectionStrings>
```

Рисунок 41.Настройка подключения к базе данных при проверке подлинности Windows.

- При настройке доступа к базе данных с помощью проверки подлинности SQL Server в конфигурационном файле найдите раздел «ConnectionStrings» - Рисунок 42, и отредактируйте его, задав имена пользователей «User ID» и пароль «Password», которые создавались в предыдущем пункте. В строке «DatabaseConnection» В случае если база данных устанавливалась на другом сервере, отредактируйте также поле «Data Source», задав имя сервера или его IP-адрес, а также имя базы данных, в случае восстановления ее с другим именем.

```
<connectionStrings>
  <clear />
  <add name="LocalSqlServer" connectionString="data source=.\SQLEXPRESS;Integrated Security=SSPI;AttachDBFilename=|DataDirectory|aspnetdb.mdf;User Instance=true"
providerName="System.Data.SqlClient" />
  <add name="OraAspNetConString" connectionString=" " providerName="" />
  <add name="DatabaseConnection" connectionString="Data Source=localhost;Initial Catalog=SecurityDB;Integrated Security=False;User
ID=UserDB;Password=P@ssw0rd;Connect Timeout=15;Encrypt=False;TrustServerCertificate=True;ApplicationIntent=ReadWrite;MultiSubnetFailover=False" providerName="" />
</connectionStrings>
```

Рисунок 42. Настройка подключения к базе данных при проверке подлинности SQL Server.

### 2.5.2 Установка лицензионного ключа

После настройки доступа Системы к базе данных, согласно пункта 2.5.1 в файл «web.config» также необходимо ввести лицензионный ключ, поставляемый в комплекте с дистрибутивами Системы. Для записи лицензионного ключа откройте файл «web.config» и

найдите раздел <Configuration> <appSettings>…. </appSettings></Configuration> и введите ключ – Рисунок 43.

```
<configuration>
  <appSettings>
    <!-- c:\TempImageFiles\; -->
    <add key="ChartImageHandler" value="storage=file;timeout=20;dir=~/Upload/;" />
    <add key="ValidationSettings:UnobtrusiveValidationMode" value="None"/>
    <add key="ClientKey" value="11111111-AAAA-BBBB-CCCC-DDDDDDDDD" />
    <!-- Лицензионный ключ  -->
```

Рисунок 43. Редактирование параметров конфигурационного файла.

### 2.5.3 Настройка продолжительности сессии пользователей

При первоначальной установке Системы время жизни сессии пользователя установлено в 8 часов. Для изменения данного параметра отредактируйте файл «web.config» в разделе `<system.web>…</system.web>` в параметрах <sessionState> и <forms> - Рисунок 44.

```
<system.web>
        <!-- Таймаут сессии в минутах-->
        <sessionState mode="InProc" timeout="480"></sessionState>

        <authentication mode="Forms">
                <!-- Таймаут сессии в минутах-->
                <forms timeout="480"></forms>
        </authentication>
```

Рисунок 44. Настройка продолжительности сессии пользователей.

### 2.5.4 Настройка сервиса электронной почты

При установке дистрибутива сервисов Системы для отправки и получения сообщений электронной почты устанавливается специализированный сервис с именем «**MailService**» - Рисунок 45.

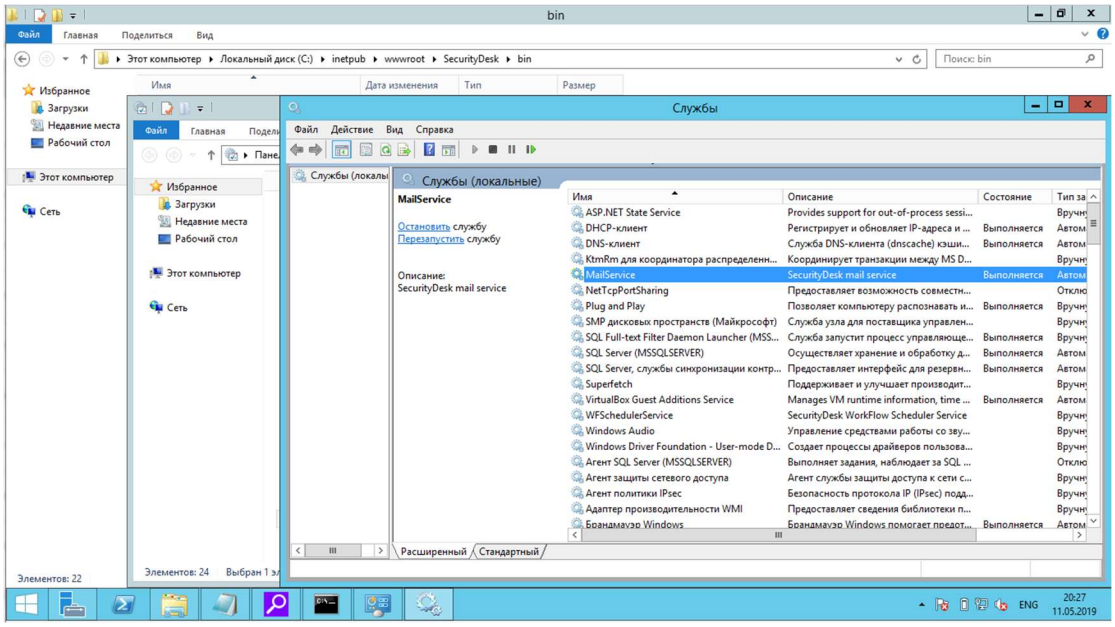


Рисунок 45. Установленные сервисы Системы.

Конфигурационный файл «**MailService.exe.config**» сервиса «**MailService**» находится в папке «**C:\Program Files\SecurityDesk**». Аналогично тому, как выполнялась настройка файла в пункте 2.5.1 найдите раздел «ConnectionStrings», и отредактируйте его:

- При настройке  доступа к базе данных с помощью проверки подлинности Windows, аналогично тому, как показано на  Рисунок 41. Сам сервис необходимо запустить от

имени пользователя Windows, которому был предоставлен доступ к базе данных. Для этого в списке Служб найдите необходимый сервис «**MailService**» и щелчком правой кнопки мыши выберите пункт «Свойства», далее в открывшемся окне свойств перейдите на вкладку «Вход в систему» и установите переключатель в положение «С учетной записью» и нажмите кнопку «Обзор», появившемся окне выберите необходимого пользователя - Рисунок 46.

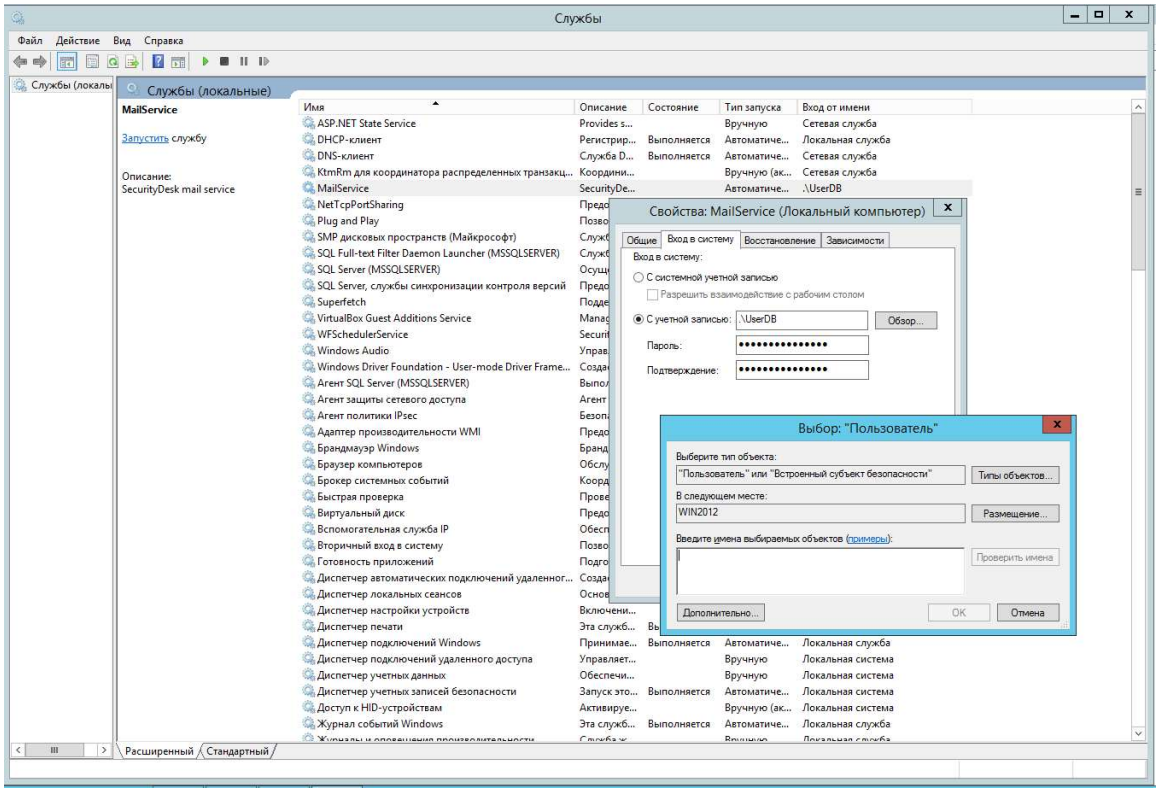


Рисунок 46. Настройка доступа сервиса к базе данных.

- При настройке доступа к базе данных с помощью проверки подлинности SQL Server, аналогично тому, как показано на Рисунок 42 задав имя пользователя «User ID» и пароль «Password», которые создавались в предыдущем пункте. В случае если база данных устанавливалась на другом сервере, отредактируйте также поле «Data Source», задав имя сервера или его IP-адрес, а также имя базы данных, в случае восстановления ее с другим именем.

Мониторинг работы сервиса можно производить в «Журнале Windows» - подраздел «Приложение» и в разделе «**Журнал работы**», в разделе «**Администрирование**» Системы.

### 2.5.5 Настройка сервиса выполнения периодических операций

При установке дистрибутива Системы для выполнения заданий по расписанию в Системе на сервер устанавливается специализированный сервис «**WFSchedulerService**» - Рисунок 45. Настройка его аналогична настройке сервиса «**MailService**» и заключается в настройке строки подключения к базе данных в конфигурационном файле «**WFSchedulerService.exe.config**», который находится в папке «**C:\Program Files\SecurityDesk**». В случае если база данных устанавливалась на другом сервере отредактируйте также поле «Data Source», задав имя сервера или его IP-адрес, а также имя базы данных, в случае восстановления ее с другим именем.

Мониторинг работы сервиса можно производить в «Журнале Windows» - подраздел «Приложение» и в разделе «**Журнал работы**», в разделе «**Администрирование**» Системы.

### 2.5.6 Обеспечение безопасности настроек подключения с проверкой подлинности SQL Server

Внимание! Для обеспечения безопасности хранения параметров подключения к базе данных в режиме проверки подлинности SQL Server рекомендуется выполнить шифрование строк подключения, выполнив следующие действия:

- Откройте папку «**C:\inetpub\wwwroot\SecurityDesk\bin**».
- Найдите и запустите файл «**encription.bat**» от имени администратора, при необходимости изменив пути расположения файлов конфигурации системы.
- Удалите, переместите «**encription.bat**» с сервера.

Для обратной расшифровки строк подключения:

- Поместите файл «**encription.bat**» в папку «C:\inetpub\wwwroot\SecurityDesk\bin».
- Отредактируйте файл, заменив ключ «-p**e**f» на «-p**d**f».
- Запустите файл «**encription.bat**» от имени администратора.

### 2.5.7 Настойка подключения к серверу бизнес-процессов

В случае необходимости использования более широкого функционала автоматизации Системы можно использовать специализированный сервер автоматизации бизнес-процессов Системы. Саму установку и настройку сервера бизнес-процессов смотрите в инструкции администратора сервера бизнес-процессов.

Для подключения Системы к серверу бизнес-процессов выполните следующие настройки:

1. В разделе «**Администрирование**» - «**Подключение к внешним источникам**» создайте новое подключение типа «**Обобщенное подключение**», в котором укажите логин **sdservice** и пароль, используемые для доступа к серверу бизнес-процессов (смотри инструкцию по настройке сервера бизнес-процессов).

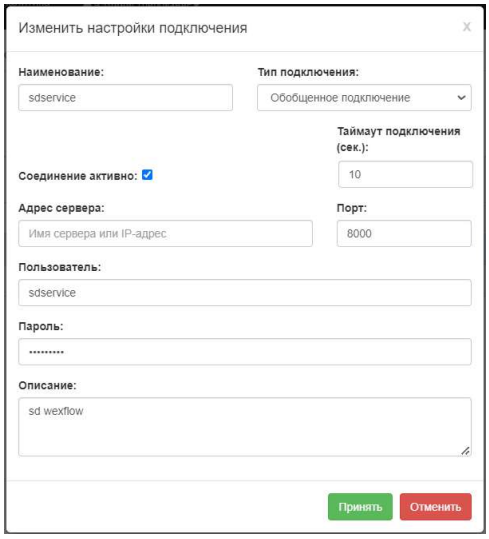


Рисунок 47. Создание обобщенного подключения.

2. В разделе «**Администрирование**» - «**Общие**» Рисунок 48 активируйте подключение к серверу бизнес-процессов, введите URL-ссылку для подключения к серверу (http://[IP-сервера БП]:8000) и выберите в выпадающем меню «**Имя подключения**» учетную запись для подключения, созданную в соответствии с п.1.

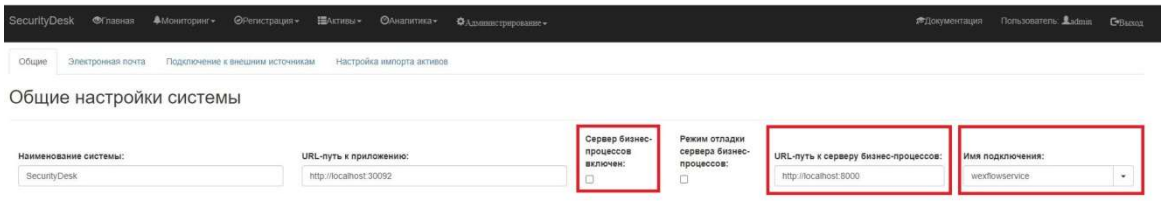


Рисунок 48. Настройка подключения к серверу бизнес-процессов.

3. Активируйте соединение с серером бизнес-процессов соответсвующим чекбоксом.

# 3. Администрирование

## 3.1 Первоначальная настройка

После установки дистрибутива Системы необходимо выполнить ее первоначальную настройку в разделе «**Администрирование**». Для перехода в раздел «**Администрирование**» войдите в систему от имени Администратора системы, для чего откройте web-браузер по ссылке установки системы. В web-браузере появится окно приглашения входа – Рисунок 49.

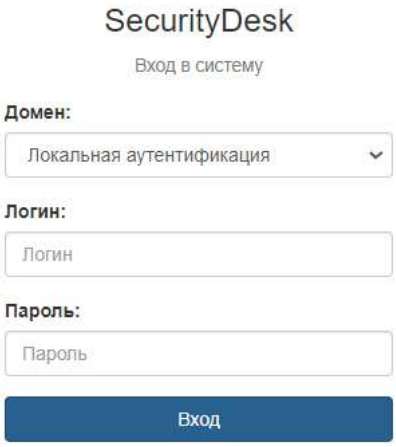


Рисунок 49. Окно входа пользователя Системы.

Введите в качестве логина пользователя имя **admin**, пароль по умолчанию **123456**. Данный пользователь входит в роль Администратора Системы, т.е. имеет полный доступ к настройкам Системы (подробнее об управлении пользователями и ролями смотрите раздел 3.3). ! Рекомендуется сменить пароль по умолчанию на стойкий, также указать электронную почту и полное ФИО администратора системы (учетная запись admin).

При успешной аутентификации вы будете перенаправлены системой на главную страницу. Для настроек основных параметров системы перейдите в параметр «**Основные настройки**» вкладки «**Администрирование**» раздела «**Настройки и мониторинг работы системы**» - Рисунок 50.

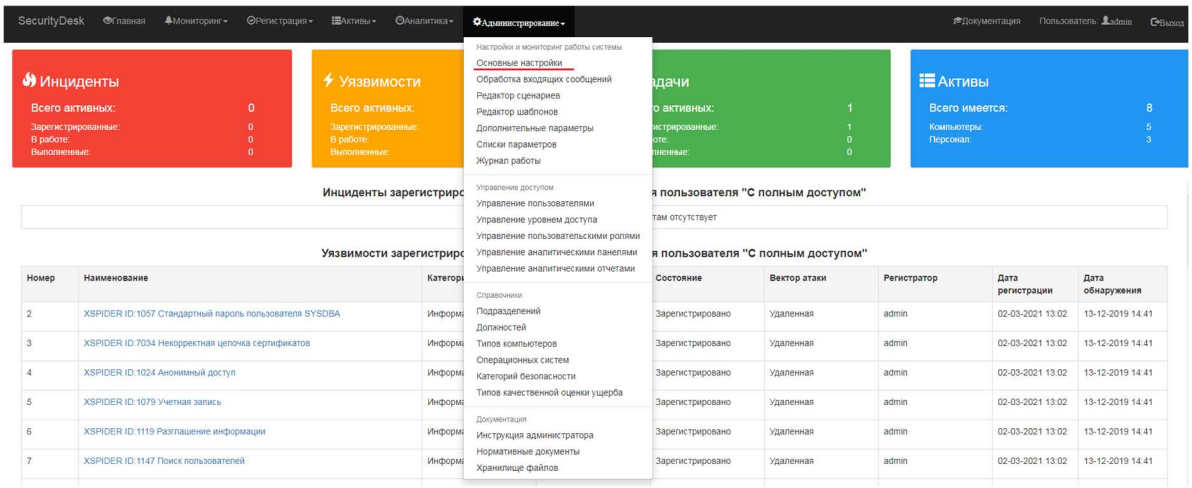


Рисунок 50. Переход к основным настройкам Системы.

В окне появившихся настроек представлено 5 вкладок: «Общие», «Электронная почта», «Подключение к внешним источникам», «Настройка импорта активов» и «Интеграция с RuSIEM» - Рисунок 51.

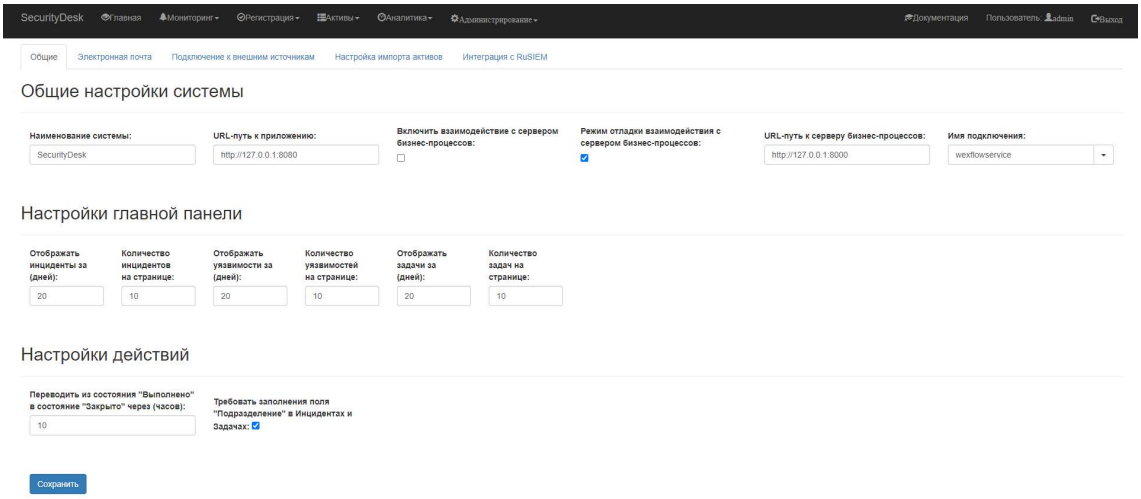


Рисунок 51. Основные настройки системы.

После выполнения необходимых настроек на вкладке «Общие», с учетом пояснений - Таблица 1 нажмите кнопку «Сохранить» и переходите к вкладке «Электронная почта» - Рисунок 52.

Таблица 1. Основные настройки – вкладка «Общие».

| **Поле** | **Пояснение** |
|---|---|
| Наименование системы | изменение наименование системы, для отображения в интерфейсе. |
| URL-путь к приложению | настройка используется для формирования корректной ссылки на объекты системы в почтовых рассылках пользователям. |
| Отображать инциденты за (дней) | Период в днях, за который отображаются на главном экране инциденты. |
| Отображать уязвимости за (дней) | Период в днях, за который отображаются на главном экране уязвимости. |

| | |
|---|---|
| Отображать задачи за (дней) | Период в днях, за который отображаются на главном экране задачи. |
| Переводить из состояния "Выполнено" в состояние "Закрыто" через (часов) | Количество часов, через которое Система будет автоматически переводить задачи, инциденты или уязвимости в состояние «**Закрыто**» при их установке пользователями в состояние «**Выполнено»** |
| Требовать заполнения поля "Подразделение" в Инцидентах и Задачах | Установка данного флага вводит обязательное для заполнение поле «**Подразделение**» в инцидентах и задачах Системы. |

Создайте на своем сервере электронной почты технологический почтовый ящик и выполните настройки подключения к серверу электронной почты по протоколам SMTP, POP3 в соответствующих разделах - Рисунок 52. Внимание! Не указывайте в качестве почтового ящика системы адрес электронной почты одного из пользователей Системы – это может привести к зацикливанию работы ее процессов!

Также установите параметры рассылки уведомлений, согласно пояснениям - Таблица 2.

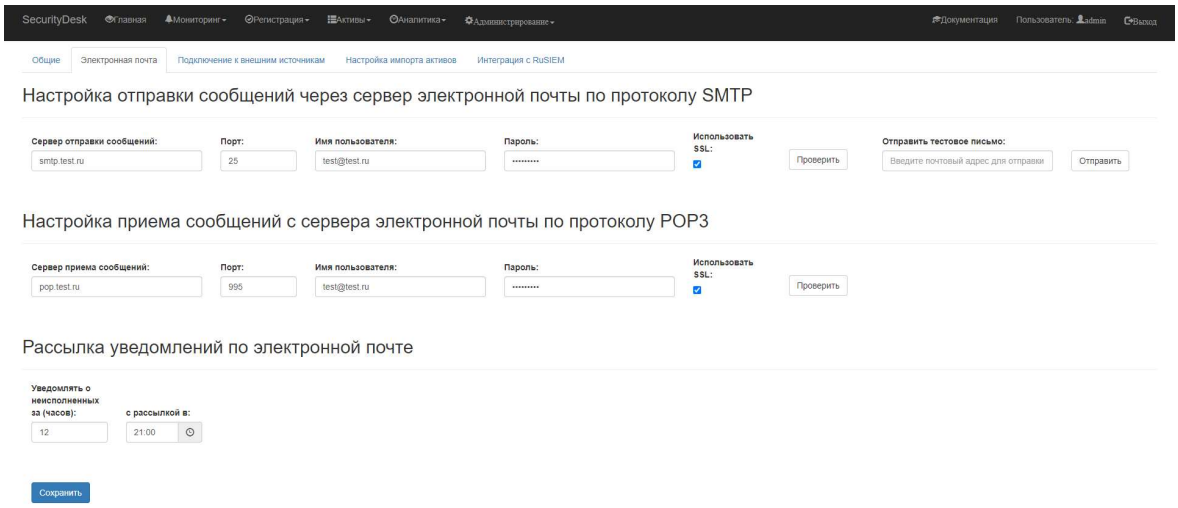


Рисунок 52. Настройка электронной почты.

После установки настроек проверьте возможность подключения к сервисам отправки и получения электронной почты с помощью соответствующей кнопки «**Проверить**», также можно поместить в очередь отправки тестовое сообщение на указанный ящик пользователя в поле «**Отправить тестовое письмо**» с помощью кнопки «**Отправить**». По окончанию настроек нажмите кнопку «**Сохранить**» для сохранения настроек.

Таблица 2. Основные настройки – вкладка «Электронная почта».

| Поле | Пояснение |
|---|---|
| Уведомлять о неисполненных за (часов): | Время, за которое Система будет напоминать пользователям о неисполненных задачах, инцидентах или не закрытых уязвимостях.<br>При установленном значении «0» Система не будет осуществлять рассылку. |
| с рассылкой в: | Время рассылки напоминаний пользователям о неисполненных задачах, инцидентах или не закрытых уязвимостях. |

На вкладке «**Подключение к внешним источникам**» выполняются настройки для подключения внешней аутентификации пользователей и импорта активов. Для подключения доступны следующие типы:

- FTP-импорт активов csv – импорт активов из csv-файлов;
- LDAP Active Directory – используется для импорта активов и внешней аутентификации в инфраструктуре Microsoft;
- LDAP FreeIPA - используется для импорта активов и внешней аутентификации в инфраструктуре Linux;
- Обобщенное подключение – используется для доступа к различным сервисам по API.

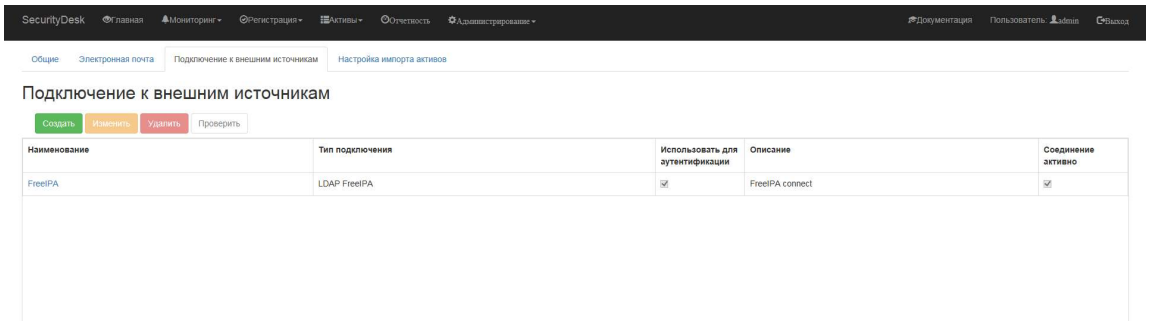


Рисунок 53. Настройка внешних источников.

На вкладке «Настройка импорта активов» настраиваются правила импорта активов от внешних источников - Рисунок 54.

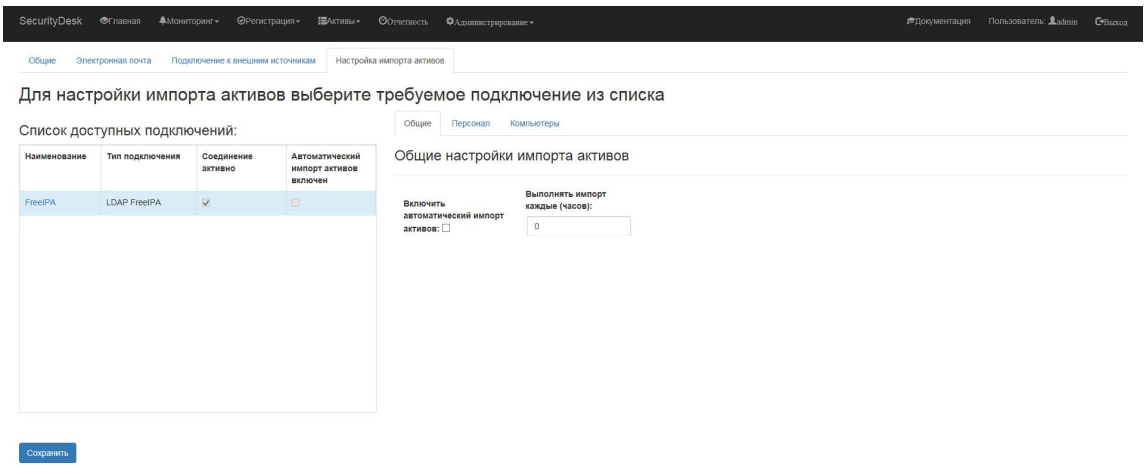


Рисунок 54. Настройка импорта активов.

Более подробно о подключении внешних источников и настройке импорта активов смотрите раздел - 3.8.

## 3.2 Настройка справочников

Для заполнения справочных данных, применяемых в Системе, используется раздел «**Справочники**» во вкладке «**Администрирование**» - Рисунок 55.

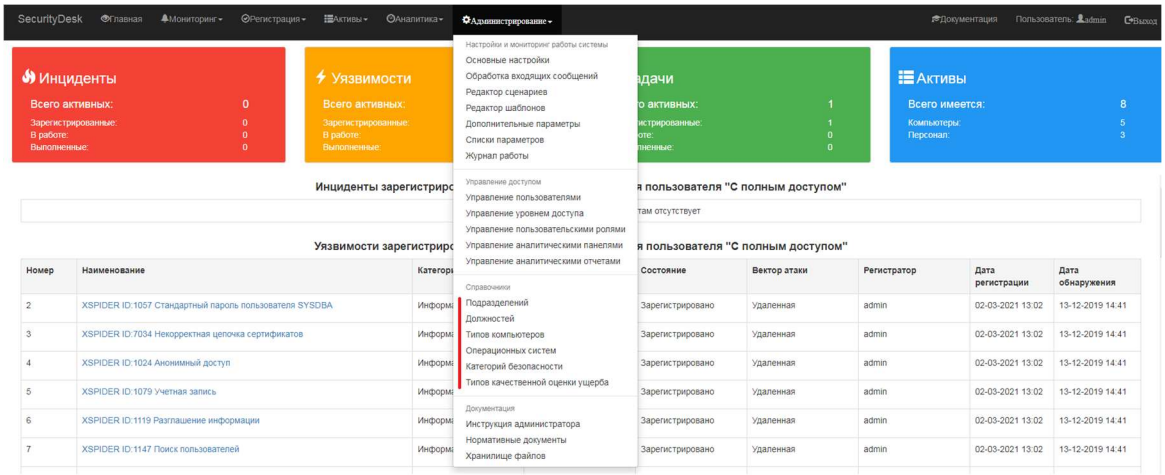


Рисунок 55. Раздел настроек справочников Системы.

Справочник «**Подразделений**» представляет собой справочник с иерархической структурой - Рисунок 56 и позволяет определить структуру предприятия, а также создать отдельные ветви для размещения, например внешних активов. Данный справочник используется в карточках инцидентов и задач, размещения активов, распределения полномочий в пользовательских ролях.


Рисунок 56. Настройка справочника «Подразделений».

Справочники «**Должностей**», «**Типов компьютеров**», «**Операционных систем**» представляют собой таблицы, используемые для заполнения параметров карточек активов Системы.

Справочники «**Категорий безопасности**», «**Типов качественной оценки ущерба**» - Рисунок 57 и представляют собой таблицы, которые используются в карточках инцидентов, задач, уязвимостей, а также для предоставления доступа пользовательским ролям.

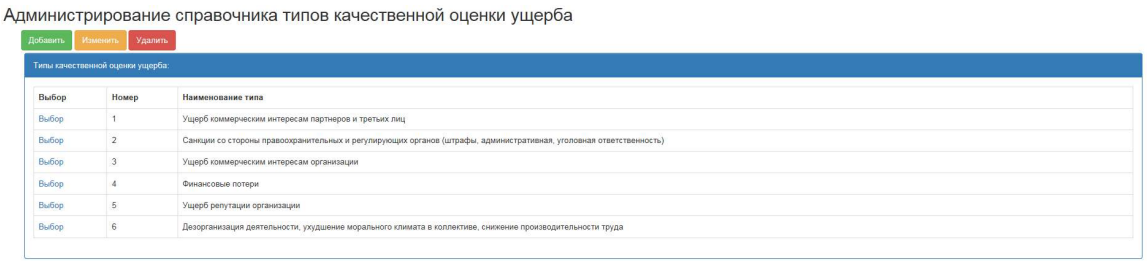


Рисунок 57. Настройка справочника типов качественной оценки ущерба.

## 3.3 Управление состояниями объектов

При первоначальном вводе в работу системы необходимо настроить схему изменения состояний с помощью специального редактора рабочих процедур. Для создания новой схемы рабочей процедуры перейдите во вкладку «**Администрирование**» и выберите параметр «**Редактор схем рабочих процедур**» - Рисунок 58.

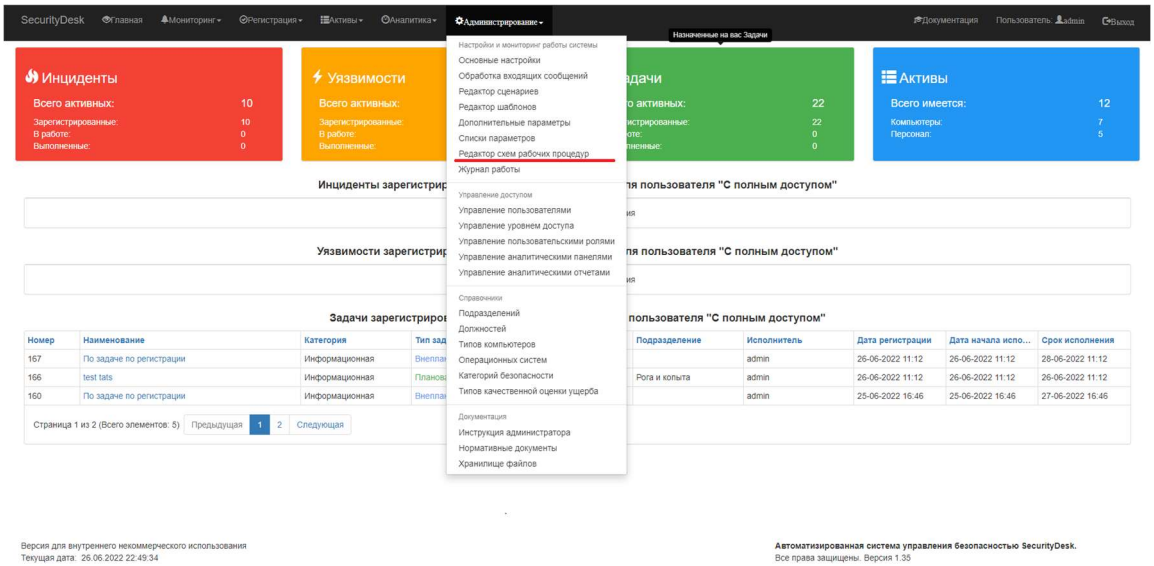


Рисунок 58. Управление схемами рабочих процедур.

В открывшемся редакторе схем выберите в выпадающих меню тип объекта (Инцидент, Уязвимость, Задача) для которого необходимо добавить схему и требуемую категорию безопасности - Рисунок 59.

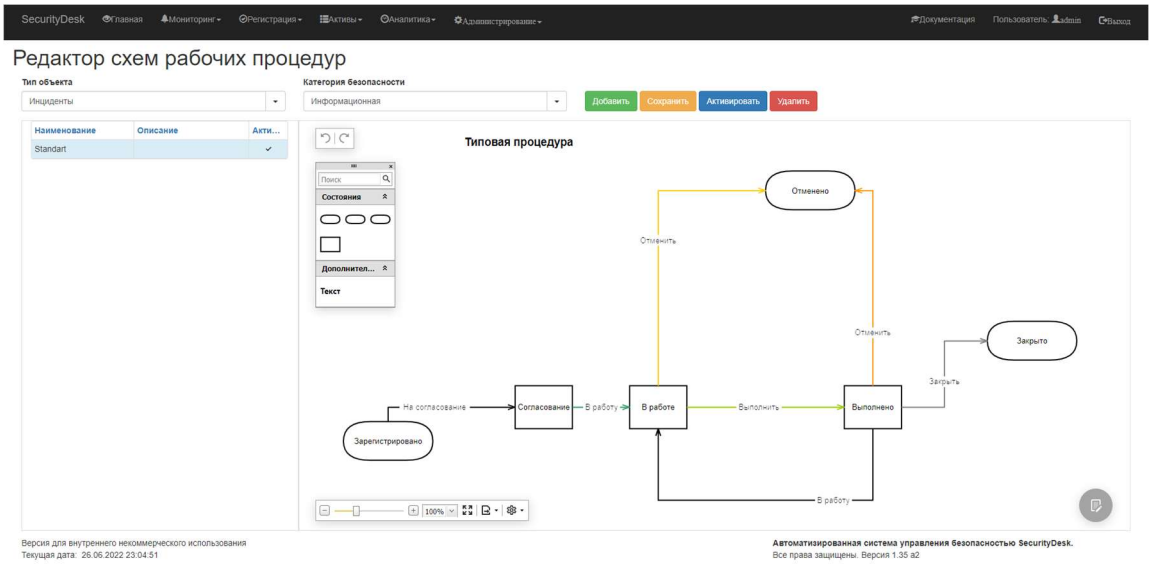


Рисунок 59. Редактор схем рабочих процедур.

Для добавления новой схемы нажмите кнопку «**Добавить**» и введите название процедуры и ее описание, в случае установленного параметра «**Добавить типовую процедуру из шаблона**» в процедуру будет автоматически добавлена типовая схема, имеющая состояния «**Зарегистрировано**», «**В работе**», «**Выполнено**», «**Закрыто**», «**Отменено**». Также возможно использовать любые другие состояния, а также соединения в любой последовательности. Обязательным для схемы являются только состояния «**Зарегистрировано**» и «**Закрыто**». Для корректности работы системы связи между состояниями должны быть подписаны, данные подписи отображаются системой на кнопках перехода между состояниями. После редактирования схему необходимо сохранить с помощью кнопки «**Сохранить**», и нажать кнопку «**Активировать**» - Система проверит выполненную схему на корректность, и в случае успеха будет использовать ее при создании объектов данного типа и категории.

Для изменения схемы рабочей процедуры существующего объекта администратору доступна возможность перезапуска по новой активной схеме. Для того, чтобы перезапустить схему на любом объекте откройте его карточку и в выпадающем меню кнопки «**Перезапустить**» выберите вариант «**по новой активной рабочей процедуре**» - Рисунок 60.

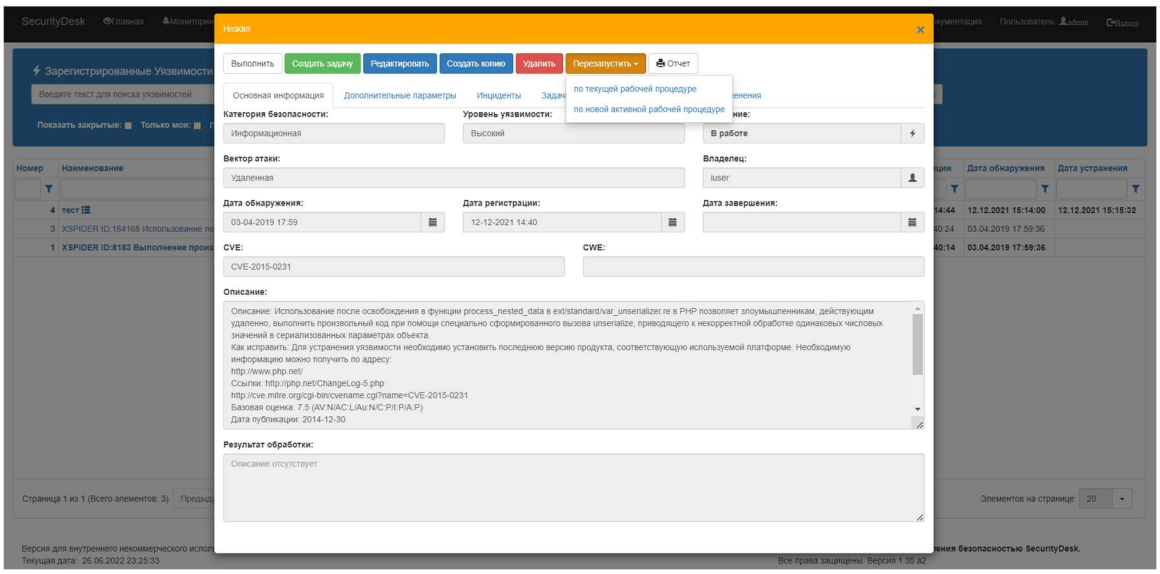


Рисунок 60. Перезапуск схемы рабочей процедуры.

Внимание! Перед запуском в эксплуатацию системы необходимо подготовить для всех категорий безопасности свои схемы рабочих процедур, в противном случае изменение состояния объектов будет невозможно!

## 3.4 Управление пользователями и ролями

Для создания нового пользователя или изменения существующего откройте вкладку «**Администрирование**» и выберите параметр «**Управление пользователями**» в разделе «**Управление доступом**» - Рисунок 61.

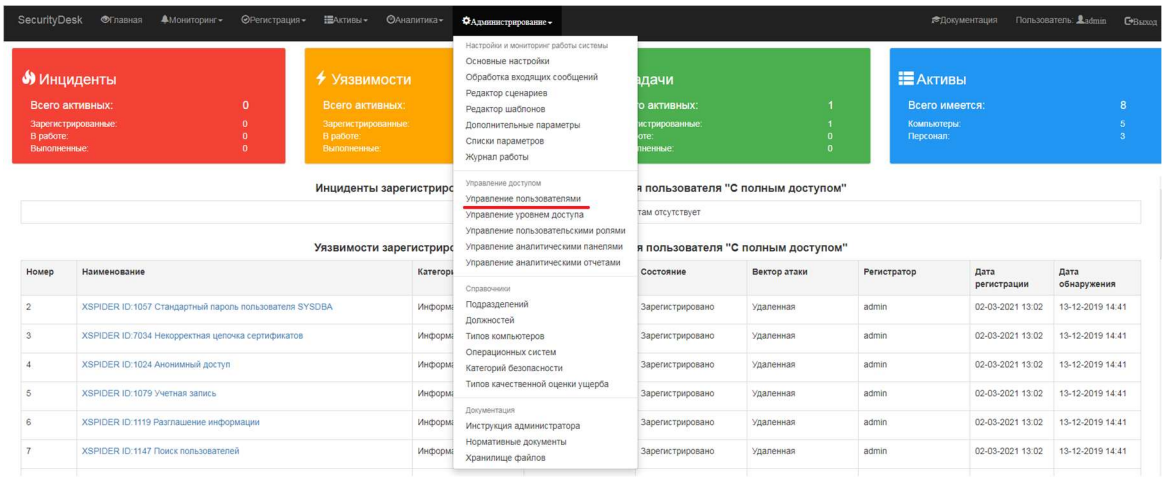


Рисунок 61. Управление пользователями Системы.

Система позволяет создавать как локальные учетные записи пользователей (содержащиеся непосредственно в базе данных Системы), так и предоставлять доступ пользователям Active Directory и Linux FreeIPA по протоколу LDAP.

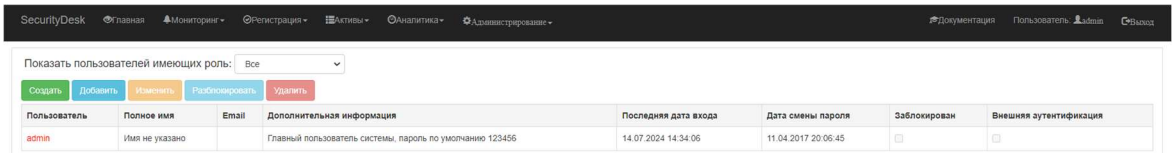


Рисунок 62. Панель управления пользователями

Для создания пользователей с локальной аутентификацией используйте кнопку «**Создать**», которая выведет форму регистрации нового пользователя Системы – Рисунок 62. В появившейся форме создания нового пользователя заполните необходимые поля пользователя - Рисунок 63. Для упрощения работы пользователя установите необходимые значения категории безопасности и подразделение по умолчанию (подразделения создаются в подразделе «**Справочники**» - «**Подразделений**» раздела «**Администрирование**»). Нажмите кнопку «**Зарегистрировать**», для создания пользователя в Системе.

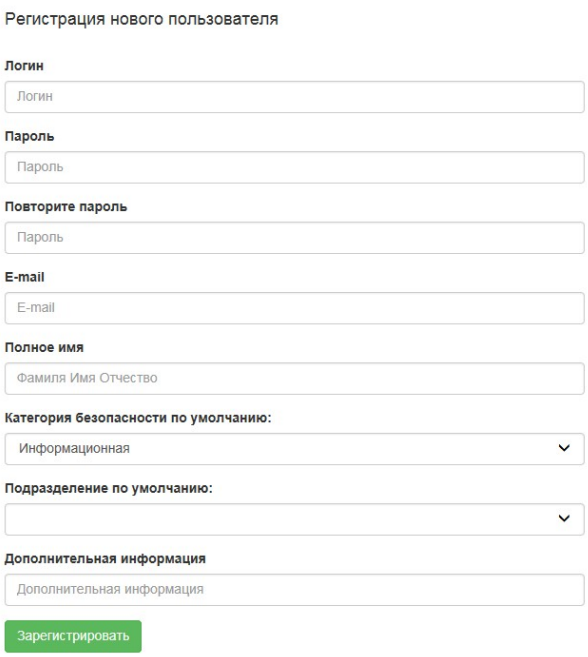


Рисунок 63. Регистрация нового пользователя Системы.

Для добавления пользователей из Active Directory или FreeIPA необходимо нажать кнопку «**Добавить**» в панели управления пользователями - Рисунок 62.

Внимание! Перед добавлением новых пользователей из Active Directory или FreeIPA необходимо настроить подключение внешнего источника в разделе «**Администрирование**» - «**Основные настройки**» - вкладка «**Подключение к внешним источникам**».

В появившейся форме импорта пользователей необходимо выполнить их первоначальную загрузку, для чего выберите требуемое имя подключения и нажмите кнопку «**Загрузить**», далее из полученного списка добавьте необходимых пользователей в Систему с помощью кнопки «**Создать**» - Рисунок 64.

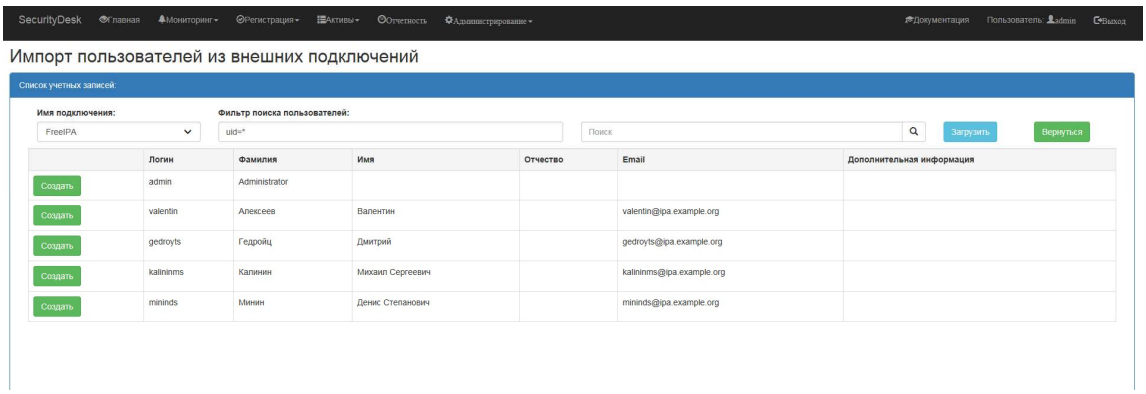


Рисунок 64. Импорт пользователей из внешних подключений.

Первоначально при создании учетных записей пользователей (за исключением учетной записи admin) им присваивается по умолчанию встроенная роль «**Пользователь**».

Для более точного управления привилегиями пользователей перейдите в раздел «**Управление уровнем доступа**» - Рисунок 65.

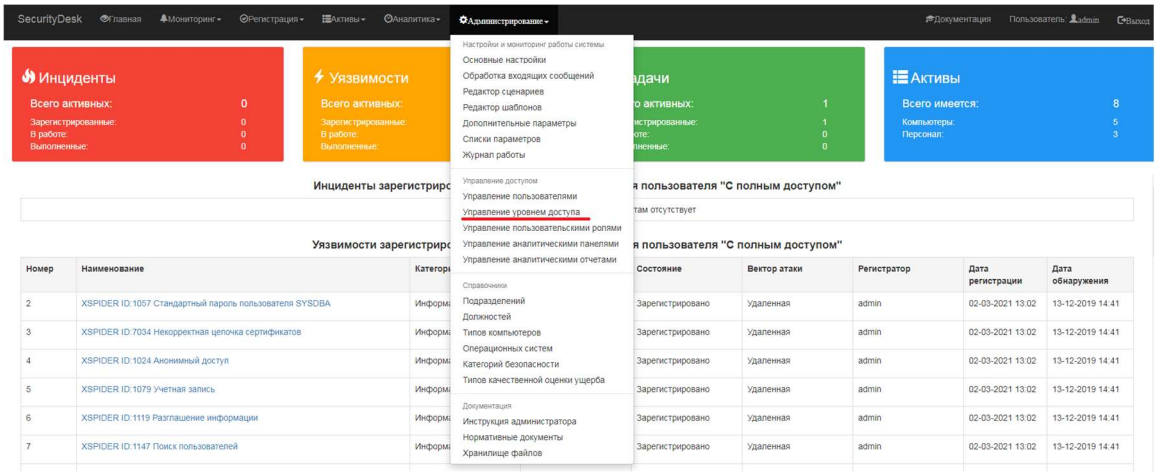


Рисунок 65. Управление уровнем доступа пользователей в Системе.

В Системе присутствуют 4 неизменяемые системные роли:

- **Пользователь** – роль предоставляется по умолчанию всем пользователям системы, и позволяет создавать, управлять своими объектами Системы. Пользователям предоставляется доступ только к Объектам (задачам, инцидентам, уязвимостям), владельцами которых они являются или к тем, по которым на них были назначены подчиненные задачи.
- **Пользователь с расширенными правами** (**ExtendedUserRights**) – роль наделяющая пользователя расширенными правами – возможностью удаления инцидентов, к которым пользователь имеет доступ, а также возможностью изменять их владельцев.
- **Менеджер активов** **(ActiveManagers)** – пользователям, обладающим данной ролью предоставлена возможность создавать, редактировать, перемещать, удалять активы в Системе через раздел «**Активы**».
- **Руководитель** (**PowerUsers**) – имеющую данную роль пользователи Системы могут просматривать и изменять состояние Объектов системы без ограничения. Данному типу пользователей не предоставляется доступ к разделу «**Администрирование**».

- **<u>Администратор</u> (Administrators)** – данный пользователь имеет возможность не только просматривать и управлять всеми объектами системы, но и возможность изменять настройки в разделе «**Администрирование**», а также удалять карточки Объектов в Системе.

В окне управления уровнем доступа системные роли отображаются красным цветом, пользовательские роли - синим цветом - Рисунок 66. Для перемещения пользователя в необходимую роль, выберите данную роль из списка и нажмите кнопку «**Добавить**», после чего во всплывающем окне выберите соответствующего пользователя и нажмите кнопку «**Принять**».

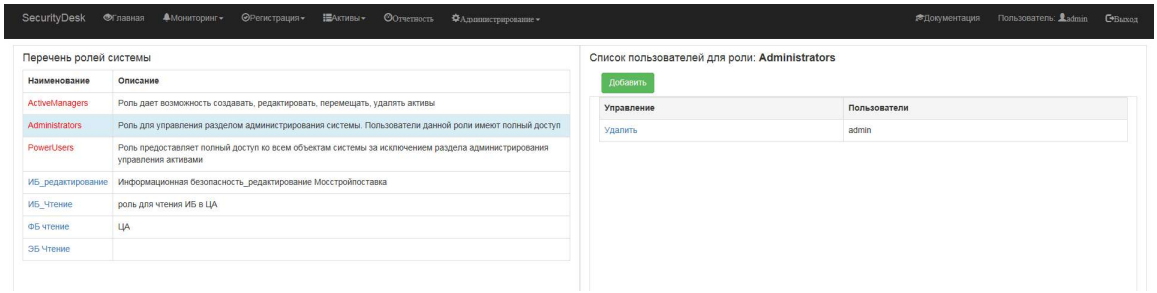


Рисунок 66. Добавление пользователя к роли.

Для более гибкого управления уровнем доступа пользователей в Системе помимо системных ролей существует возможность создавать пользовательские роли. Для создания пользовательских ролей перейдите в раздел «**Управление пользовательскими ролями**» - Рисунок 67.

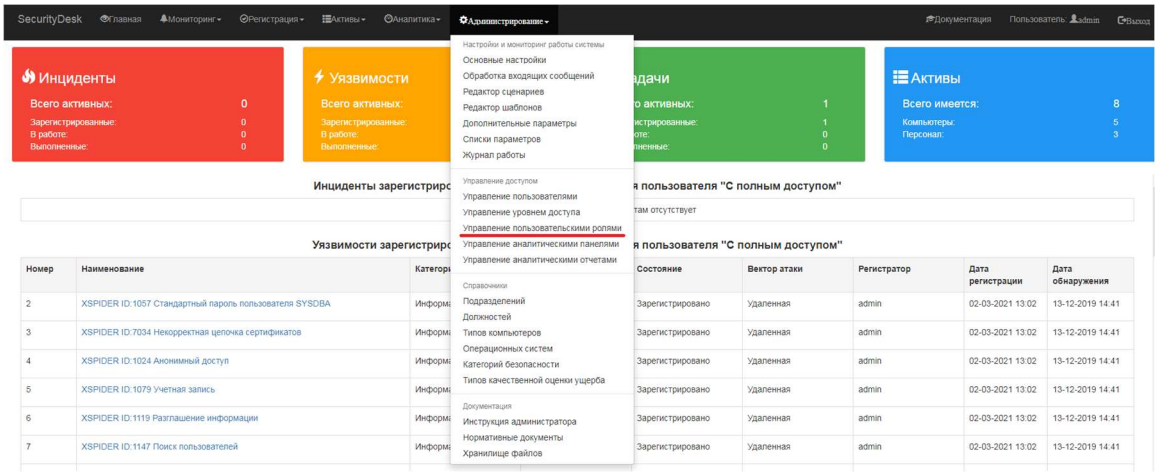


Рисунок 67. Управление пользовательскими ролями.

В панели «**Управление пользовательскими ролями**» необходимо выбрать существующую роль из списка или создать новую пользовательскую роль с помощью кнопки «**Создать**» - Рисунок 68. Для выбранной роли необходимо указать уровень доступа для категорий безопасности, а также уровень доступа к объектам Системы на основе принадлежности к подразделению.

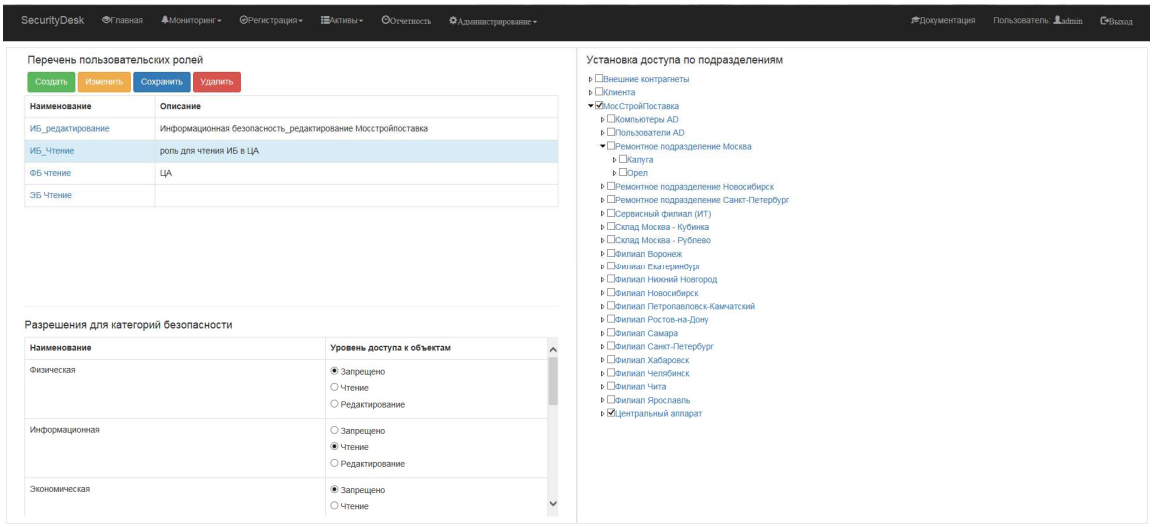


Рисунок 68. Администрирование пользовательских ролей.

Внимание! Для зарегистрированных уязвимостей уровень доступа будет контролироваться только по принадлежности к той или иной категории безопасности.

Внимание! В случае если инциденту или задаче не назначено подразделение, то к таким объектам доступ будет предоставляться всем пользователям, входящим в роль с соответствующим уровнем доступа к категории безопасности.

## 3.5 Конструктор аналитических диаграмм

Кроме стандартизованных аналитических диаграмм (настроенных и доступных в Системе сразу) Система позволяет создавать собственные диаграммы с помощью встроенного конструктора. Для перехода к конструктору диаграмм перейдите в меню «**Аналитика**» - «**Аналитические панели**» - Рисунок 69.

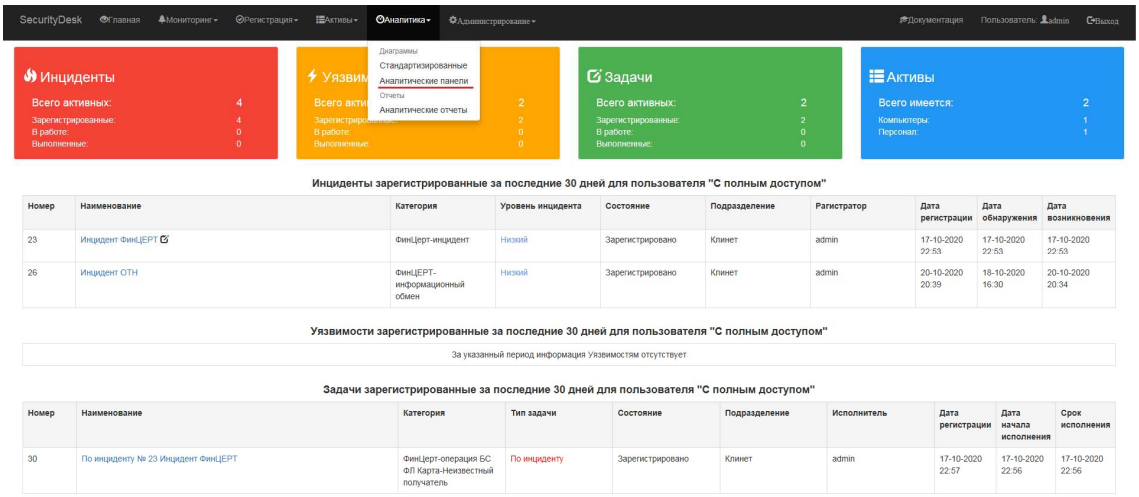


Рисунок 69. Переход к конструктору аналитических диаграмм.

Доступ к конструктору диаграмм - Рисунок 70 предоставляется только пользователям, имеющим роль **Администратор**. Для остальных пользователей будет предоставляться доступ только к аналитической панели с диаграммами, доступ к которым им предоставил Администратор.

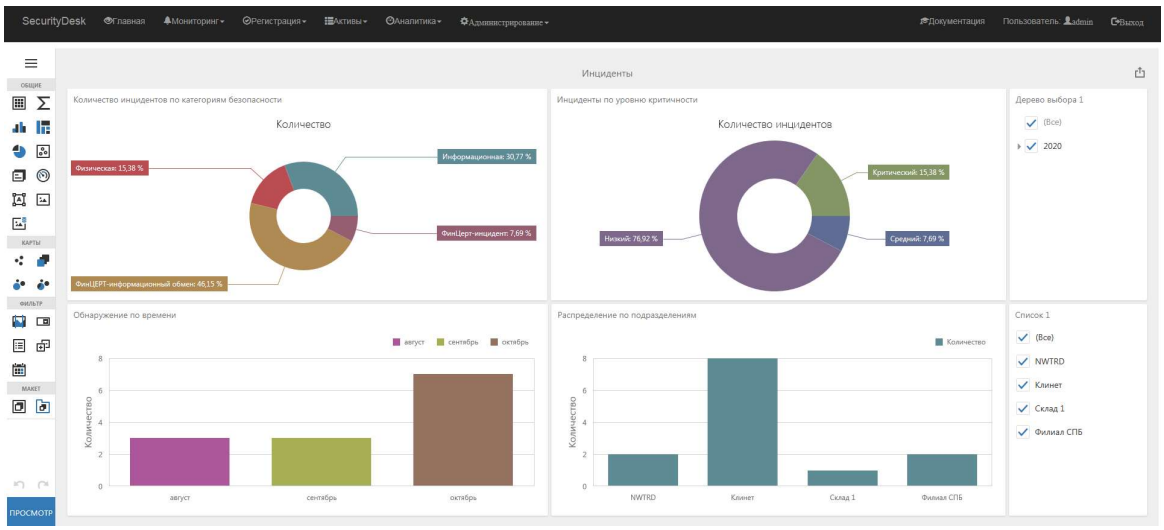


Рисунок 70. Конструктор аналитических диаграмм.

Построение панели аналитических диаграмм выполняется в следующей последовательности:

1. Создается набор данных, на основе которых будет выполняться построение диаграмм (набор данных может создаваться из выборки таблиц базы данных, представлений, специализированных SQL-запросов, хранимых процедур).
2. На аналитической панели располагаются требуемые типы диаграмм и графиков (в конструкторе доступны круговые диаграммы, графики, древовидные диаграммы, индикаторы, точечные диаграммы, таблицы, сводные таблицы, точечные картограммы, пузырьковые картограммы и др.) к которым применяются наборы данных.
3. Для возможности фильтрации данных на панели располагают элементы фильтрации (доступна фильтрация по диапазону, в виде дерева, выпадающего списка, обычного списка, ввода даты).

## 3.6 Конструктор аналитических отчетов

С помощью конструктора аналитических отчетов возможно разработать любой собственный отчет, вывести его на печать или выгрузить в файл форматов docx, xlsx, pdf, rtf, html и др. Для доступа к конструктору отчетов перейдите в меню «**Аналитика**» - «**Аналитические отчеты**» - Рисунок 69. Доступ к конструктору отчетов - Рисунок 71 предоставляется только пользователям, имеющим роль **Администратор**. Для остальных пользователей будет предоставляться доступ только к аналитической панели с перечнем отчетов, доступ к которым им предоставил Администратор.

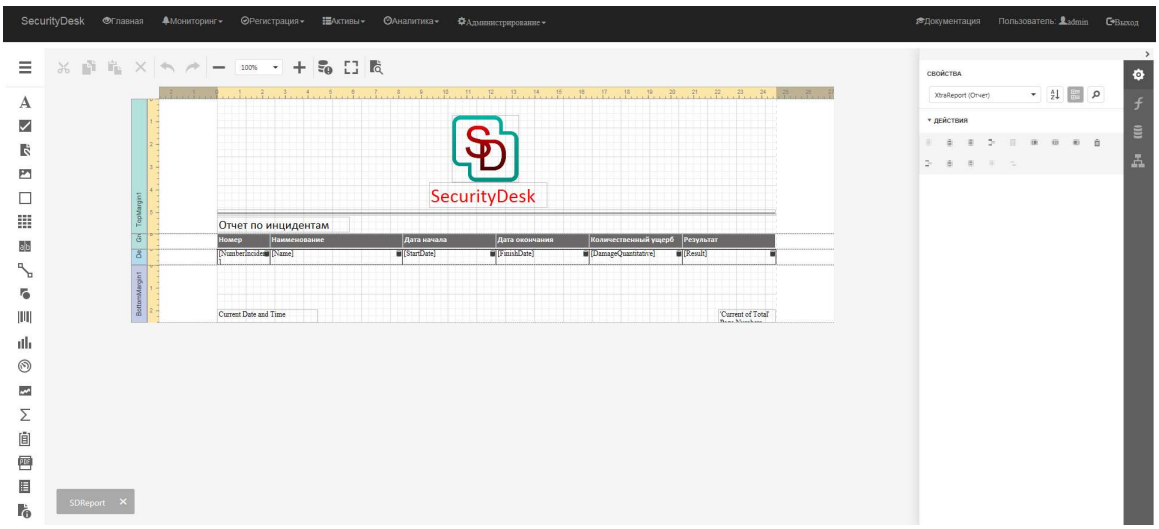


Рисунок 71. Конструктор аналитических отчетов.

Создание отчета выполняется в следующей последовательности:

1. С помощью мастера выбирается макет отчета (отчет может формироваться в вертикальном или горизонтальном направлении).
2. Создается набор данных, на основе которых будет выполняться построение отчета (набор данных может создаваться из связанных таблиц базы данных, представлений, специализированных SQL-запросов, хранимых процедур). Если отчет выполняется с помощью хранимой процедуры необходимо предоставить доступ учетной записи сервера баз данных, созданной для чтения возможность выполнения хранимой процедуры.
3. В области верхнего колонтитула (TopMargin1) создается «заголовок» отчета с необходимым количеством столбцов и их названиями.
4. В области данных (Detail1) создаются элементы: таблицы, диаграммы, графики и прочие элементы с панели элементов (левая часть экрана).
5. При необходимости заполняется нижний колонтитул (BottomMargin1).
6. Для элементов отчета устанавливаются необходимые стили (правая часть экрана).
7. В элементы области данных назначаются наборы (столбцы) из набора данных (правая часть экрана – список полей).

## 3.7 Предоставление доступа пользователей к аналитическим панелям отчетов и диаграммам

Настройка доступа к аналитическим панелям диаграмм и отчетов назначается через раздел «**Администрирование**» - «**Управление аналитическими панелями**» и «**Управление аналитическими отчетами**» соответственно - Рисунок 72.

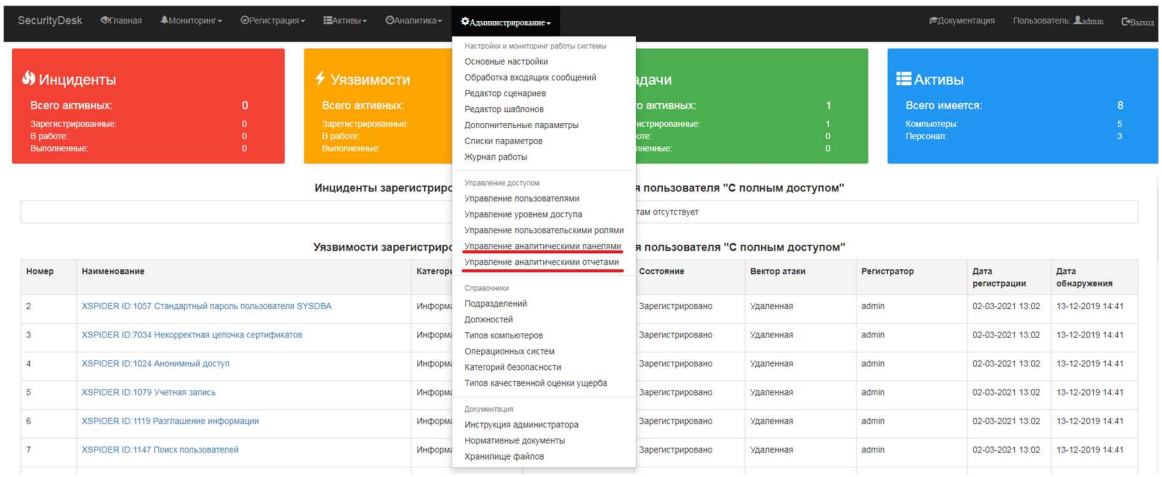


Рисунок 72. Настройка доступа к аналитическим панелям и отчетам.

Для назначения доступа к аналитической панели или отчету перейдите в соответствующий раздел, в левой части раскрывшейся формы выберите необходимую панель или отчет, предоставьте доступ необходимому пользователю с помощью кнопки «**Добавить**» - Рисунок 73.

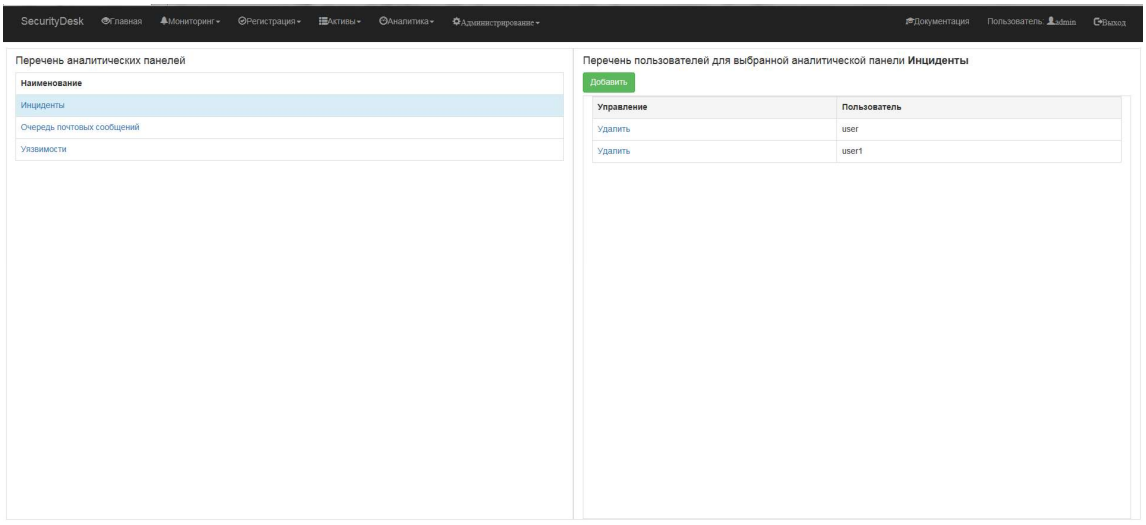


Рисунок 73. Назначение доступа к аналитической панели.

## 3.8 Подключение к внешним источникам

Система позволяет подключать внешние источники данных для осуществления аутентификации внешних пользователей, автоматического импорта активов и других внешних подключений. Чтобы создать новое подключение перейдите в раздел «**Администрирование**» - «**Основные настройки**» и выберите вкладку «**Подключение к внешним источникам**» - Рисунок 74.

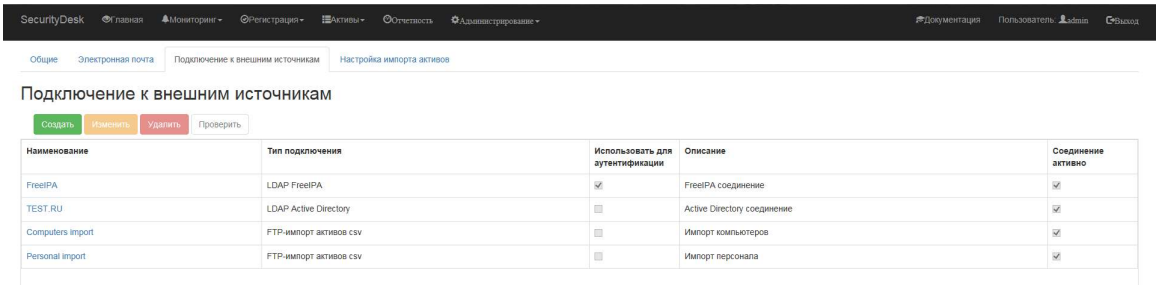


Рисунок 74. Панель подключения к внешним источникам

Для создания нового источника данных нажмите кнопку «**Создать**», в появившемся окне выберите тип подключения и заполните соответствующие параметры подключения - Рисунок 75. Таблица 3 содержит пояснения к параметрам подключения. Если все настройки выполнены верно, то при нажатии на кнопку «**Проверить**» Система сообщит об успешности подсоединения к серверу.

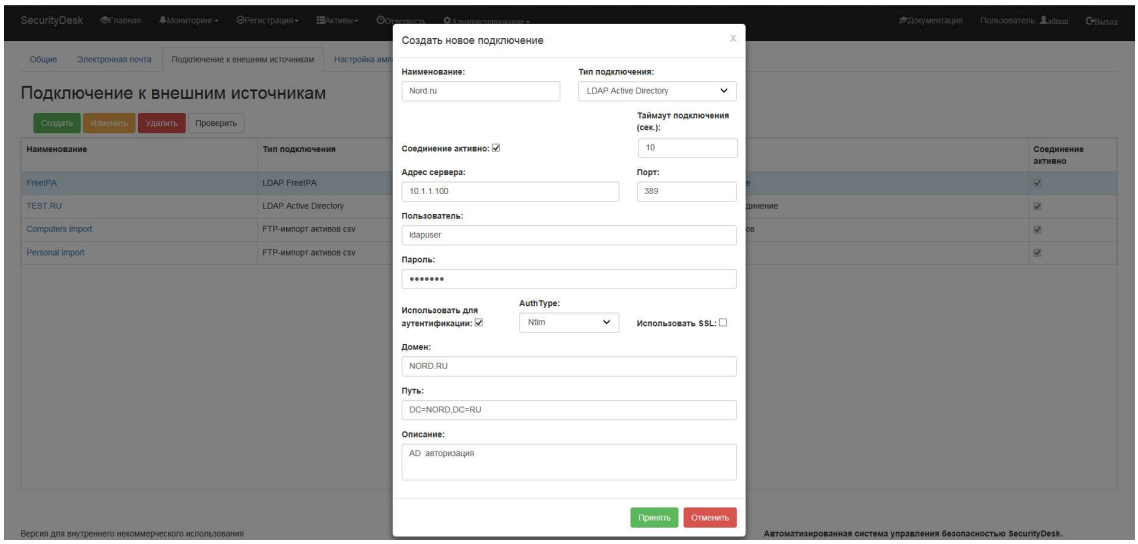


Рисунок 75. Создание нового подключения.

Таблица 3. Параметры подключения.

| **Поле** | **Пояснение** |
|---|---|
| Наименование | Уникальное название подключение |
| Тип подключения | Перечень доступных типов подключений |
| Соединение активно | Активирует подключение |
| Таймаут подключения (сек.): | Максимально время доступности при подключении |
| Адрес сервера | IP-адрес или сетевое имя сервера подключения |
| Порт | Порт подключения к серверу |
| Пользователь | Имя учетной записи для подключения |
| Пароль | Пароль учетной записи для подключения |
| Описание | Любая дополнительная информация |
| **Соединение LDAP Active Directory/FreeIPA** | |
| Использовать для аутентификации | Разрешает использовать соединение для аутентификации пользователей |
| AuthType | Тип аутентификации |
| Использовать SSL | Использование протокола SSL для подключения |
| Домен | Имя домена |
| Путь | Путь подключения |
| **Соединение FTP-импорт активов csv** | |

| | |
|---|---|
| Путь и файл импорта | Путь расположения файла csv |
| Удалять файл после загрузки | Установить если после каждого импорта необходимо удалять файл |
| С заголовком | Установить если файл содержит заголовок столбцов |
| Игнорировать не найденные поля | Продолжать обработку файла при ошибке обработке информации |
| Разделитель | Символ разделителя столбцов в файле |
| Кодировка | Тип кодировки текста файла |

## 3.9 Импорт активов

Активы могут создаваться вручную через меню «**Активы**», если у пользователя есть роль **Менеджер активов (ActiveManagers)** или импортироваться из внешних источников по расписанию.

Предварительно для настройки автоматического импорта активов необходимо настроить внешний источник подключения в соответствии с разделом 3.8. Настройка импорта активов производится во вкладке «**Настройка импорта активов**» меню «**Администрирование**» - «**Основные настройки**» - Рисунок 76.

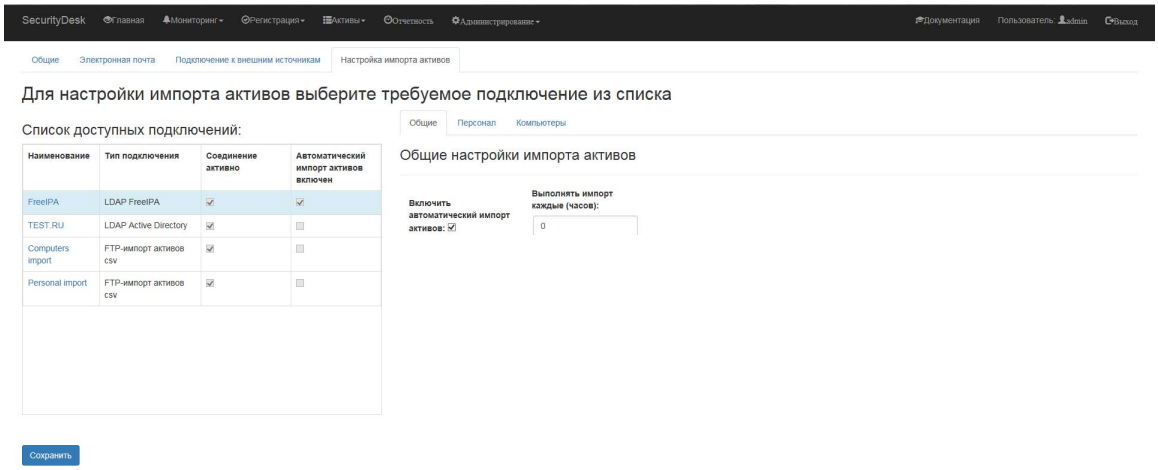


Рисунок 76. Настройка автоматического импорта активов

Для настройки импорта выберите необходимое подключение в левой части панели. На появившейся справа вкладке «**Общие**» установите периодичность импорта в часах и включите автоматический импорт после настройки импорта персонала и компьютеров в соответствующих вкладках.

Для настройки импорта персонала заполните параметры на вкладке «**Персонал**» - Рисунок 77 и установите флаг «**Включить импорт персонала**». Описание полей и атрибутов для импорта персонала - Таблица 4. Параметры импорта персонала.

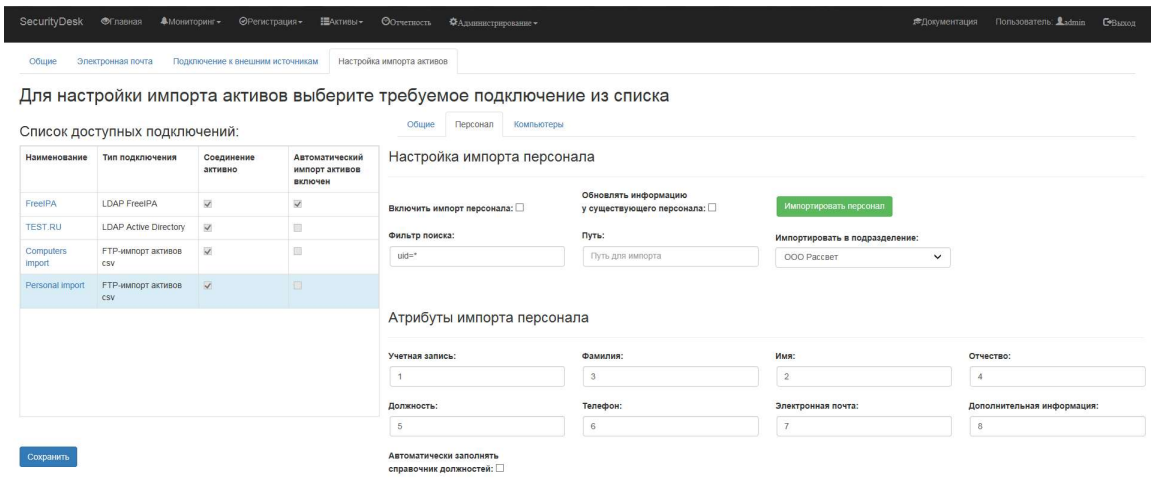


Рисунок 77. Настройка импорта персонала.

Таблица 4. Параметры импорта персонала.

| **Параметры** | **Пояснение** |
|---|---|
| Включить импорт персонала | Включение автоматического импорта персонала по расписанию |
| Обновлять информацию у существующего персонала | В случае если при импорте персонала актив уже импортирован в систему, осуществляется только обновление его информации |
| Фильтр поиска | Используется избирательного для импорта активов через LDAP-подключение |
| Путь | Путь в LDAP-каталоге |
| Импортировать в подразделение | Подразделение, в которое будут импортироваться новые активы |
| Автоматически заполнять справочник должностей | При включенном параметре система автоматически заполняет справочник должностей в случае отсутствия найденной при импорте должности |

Для настройки импорта компьютеров заполните параметры на вкладке «**Компьютеры**» - Рисунок 78. Пояснение назначения параметров на вкладке представлено в таблице - Таблица 5.

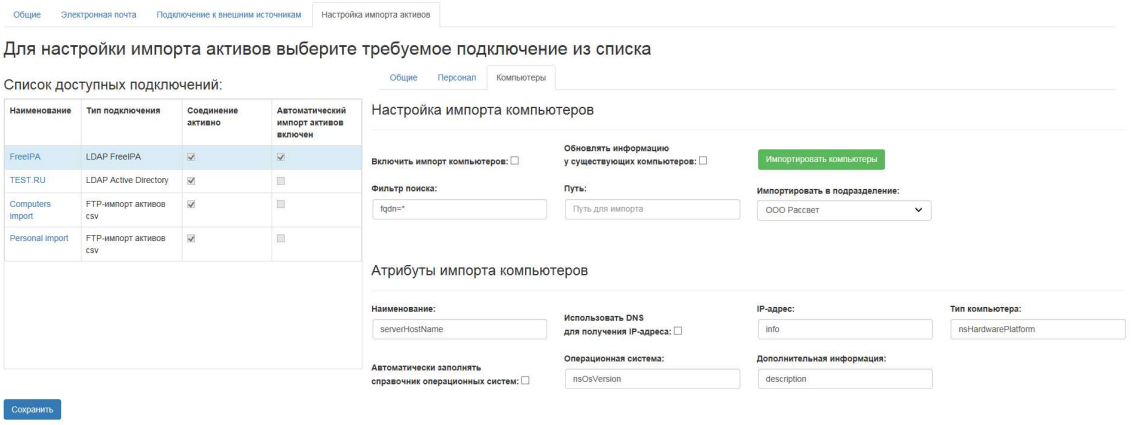


Рисунок 78. Настройка импорта компьютеров.

Таблица 5. Параметры импорта компьютеров.

| Параметры | Пояснение |
|---|---|
| Включить импорт компьютеров | Включение автоматического импорта компьютеров по расписанию |
| Обновлять информацию у существующих компьютеров | В случае если при импорте компьютеров актив уже импортирован в систему, осуществляется только обновление его параметров |
| Фильтр поиска | Используется для избирательного импорта активов через LDAP-подключение |
| Путь | Путь в LDAP-каталоге |
| Импортировать в подразделение | Подразделение, в которое импортируются новые активы |
| Использовать DNS для получения IP-адреса | При включенном параметре система автоматически выполняет поиск IP-адреса по его сетевому имени |
| Автоматически заполнять справочник операционных систем | В случае если при импорте компьютера операционная система не содержится в справочнике системы, то она автоматически в него добавляется |

Фильтры поиска учетных записей для компьютеров и пользователей необходимы для ускорения загрузки активов в систему и фильтрации только требуемых активов. Фильтры поиска можно получить, например, из оснастки MMC «**Active Directory Users and Computers**», создав в разделе оснастки поисковый запрос. Основные запросы, которые могут понадобиться для настройки импорта активов сведены в таблицу - Таблица 6.

Для атрибутов импорта доступны две кнопки «**Импортировать пользователей**» и «**Импортировать компьютеры**» данные кнопки предназначены для ручной загрузки активов в Систему.

Таблица 6. Фильтры поиска учетных записей в каталоге LDAP.

| Фильтр поиска | Описание |
|---|---|
| (&(objectCategory=user)(objectClass=user)(userPrincipalName=*)) | Все пользователи |
| objectCategory=person)(objectClass=user)(!useraccountcontrol:1.2.840.113556.1.4.803:=2) | Все пользователи, кроме отключенных |
| (&(objectCategory=user)(objectClass=user)(!title=*)) | Пользователи, у которых не заполнено поле должность |
| (objectCategory=computer) | Все компьютеры |
| (objectCategory=computer)(operatingSystem=Windows 10*) | Все компьютеры Windows 10 |
| (objectCategory=computer)(servicePrincipalName=MSSQLSvc*)(operatingSystem=Windows Server*) | Все SQL серверы, с любой ОС, у которых зарегистрирован servicePrincipalName |
| (objectCategory=computer)(servicePrincipalName=exchangeMDB*)(operatingSystem=Windows Server*) | Все Exchange серверы |

После выполнения сохранения настроек всех разделов нажмите кнопку «**Сохранить**» и перезапустить установленные службы Системы (MailService, WFShedulerService, ConnectorRuSIEM, ConnectorFinCERT т.д.)

## 3.10 Заполнение справочника нормативных документов

Для категорирования инцидентов в Системе, в соответствии с регламентирующими документами первоначально требуется заполнить соответствующий справочник, который находится в разделе «**Документация**» вкладки «**Администрирование**» – Рисунок 79.

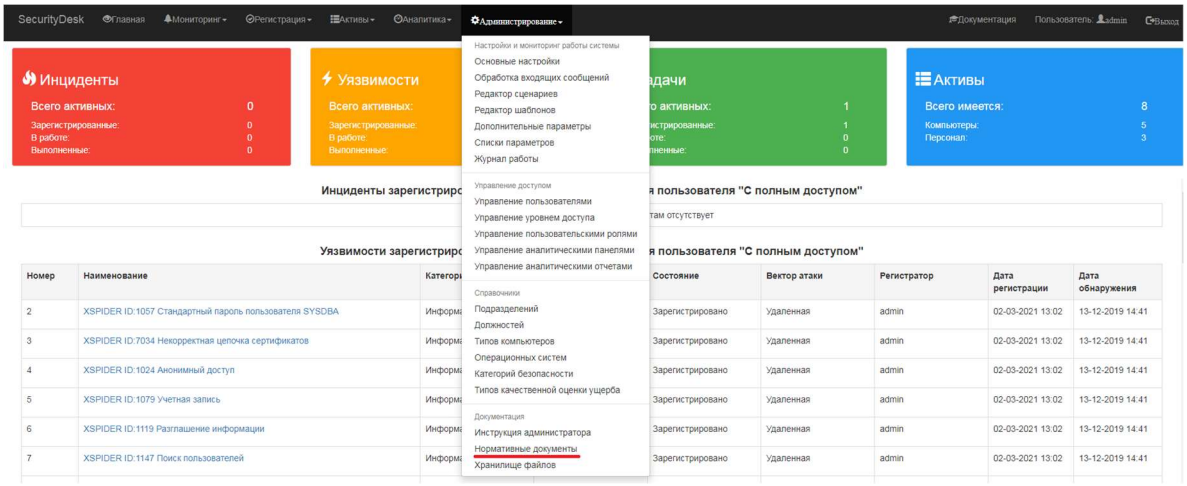


Рисунок 79. Раздел настройки нормативных документов.

Данный справочник представляет собой два уровня:

- 1-й уровень - Наименование нормативного документа;
- 2-й уровень - Содержание нормативного документа.

На первом уровне вводится наименование документа, например, «Политика информационной безопасности», а также буквенный код документа. На втором уровне вводятся пункты выбранного на 1-м уровне регламентирующего документа, их формулировка, номер, тег (для использования быстрого поиска) – Рисунок 80.

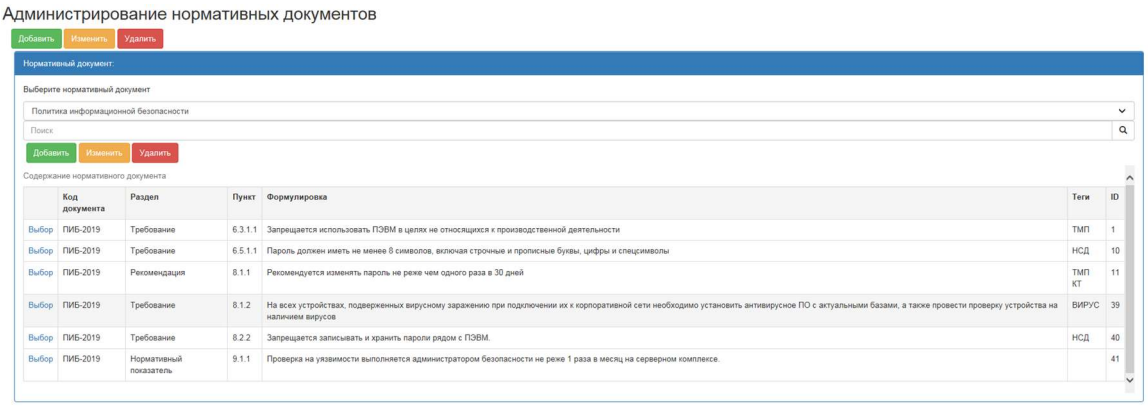


Рисунок 80. Настройка нормативных документов.

## 3.11 Настройка сценариев автоматизации

С помощью «сценариев автоматизации» возможно автоматизированное создание связанных, подчиненных задач для появляющихся в Системе инцидентов, уязвимостей или создаваемых задач.

Внимание! В случае использования сервера бизнес-процессов не рекомендуется использовать данный функционал в целях исключения дублирования. Настройку

автоматизации с использованием сервера бизнес-процесса смотрите в соответствующей инструкции.

Доступ к редактору сценариев осуществляется через раздел «**Настройки и мониторинг работы системы**» - «**Редактор сценариев**», вкладки «**Администрирование**» – Рисунок 81.

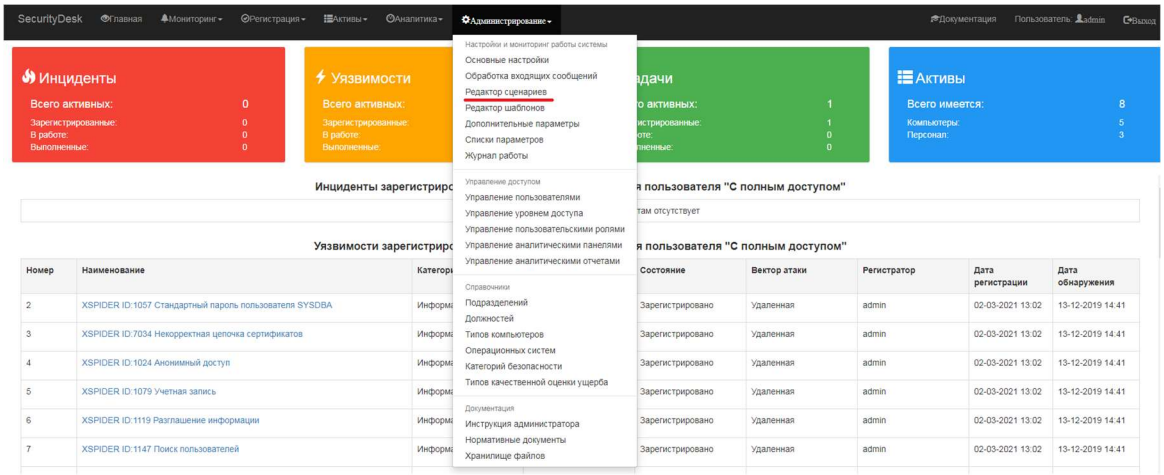


Рисунок 81. Доступ к сценариям автоматизации.

Для создания нового сценария необходимо выбрать тип родительского объекта, в качестве которого может выступать инцидент, уязвимость или задача. Также необходимо выбрать категорию безопасности, для которой сценарий будет действовать, затем нажать кнопку «**Добавить**» - Рисунок 82.

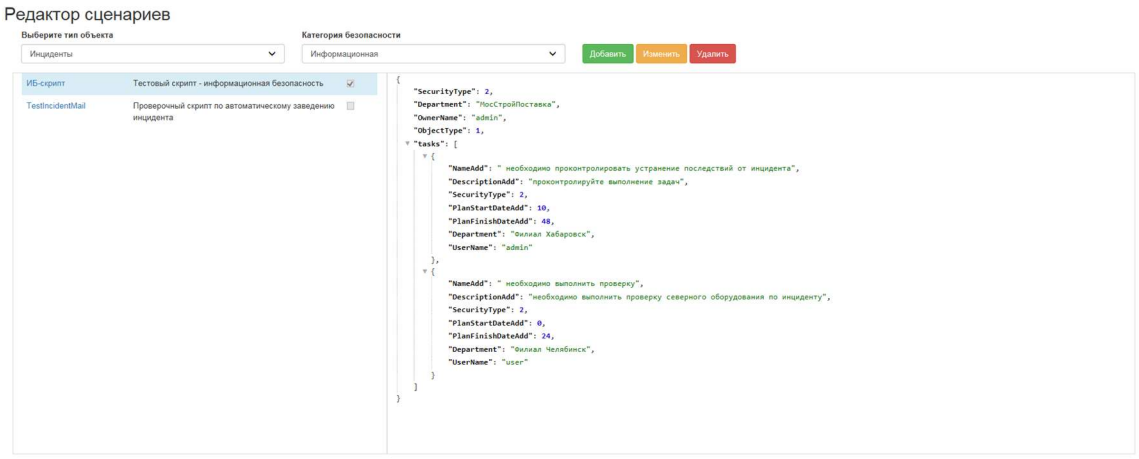


Рисунок 82. Редактор сценариев автоматизации.

В появившемся диалоговом окне введите наименование сценария, дополнительную информацию, а также установить параметр включения в работу сценария – «**Включить**» и флаг создания шаблона сценария «**Добавить шаблон сценария**» – Рисунок 83.

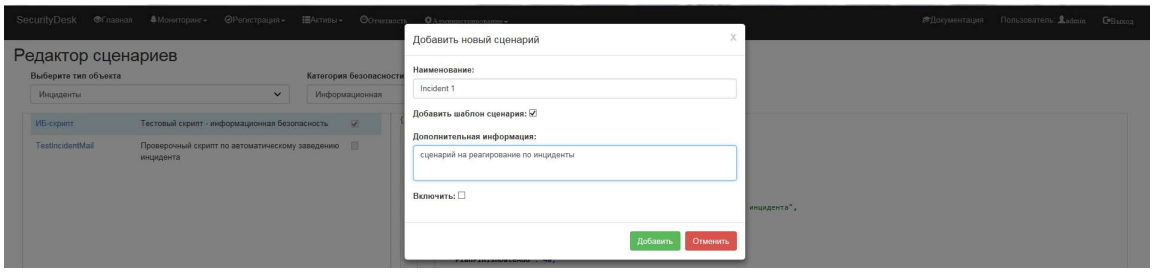


Рисунок 83. Создание нового сценария.

Далее в панели, на основе выбранного шаблона появится новый сценарий автоматизации, с шаблонными параметрами родительского объекта и одной подчиненной задачей. Требования к заполнению полей родительского объекта и подчиненных задач указаны в таблицах - Таблица 7 для Инцидентов, Таблица 8 для Уязвимостей, Таблица 9 для Задач. Допускается добавление множества Задач к одному родительскому объекту, дополнительные подчиненные задачи указываются через запятую, в фигурных скобках – Рисунок 82.

Таблица 7. Требования к заполнению полей сценария автоматизации для Инцидента.

| **Наименование поля** | **Тип данных** | **Пояснение** | **Примечание** |
|---|---|---|---|
| **Родительский объект - Инцидент** | | | |
| SecurityType | Целое | Категория безопасности | Нельзя изменять |
| Department | Строка | Наименование подразделения - срабатывает при совпадении | При пустом значении не учитывается |
| OwnerName | Строка | Имя владельца инцидента - срабатывает при совпадении | При пустом значении не учитывается |
| Name | Строка | Подстрока в названии инцидента - срабатывает при совпадении | При пустом значении не учитывается |
| Status | Строка | Наименование состояния, при котором срабатывает сценарий | Обязательно к заполнению |
| ObjectType | Целое | Тип объекта | Нельзя изменять |
| **Подчиненные объекты – Задачи** `"task": { … }` | | | |
| Name | Строка | Добавляется к названию задачи | |
| Description | Строка | Добавляется к описанию задачи | |
| SecurityType | Целое | Категория безопасности задачи | Номер категории указан в справочнике |
| PlanStartDateAdd | Целое | Количество часов к плановому началу выполнения задачи от текущего времени | |

| | | | |
|---|---|---|---|
| PlanFinishDateAdd | Целое | Количество часов к плановому завершению выполнения задачи от текущего времени | |
| Department | Строка | Наименование подразделения для задачи | Обязательно для заполнения! |
| UserName | Строка | Имя пользователя для задачи | Обязательно для заполнения! |
| ObjectType | Целое | Тип объекта | 0 - Нельзя изменять |
| tasks | структура | Подчиненные задачи | null - Нельзя изменять |

Таблица 8. Требования к заполнению полей сценария автоматизации для Уязвимости.

| **Наименование поля** | **Тип данных** | **Пояснение** | **Примечание** |
|---|---|---|---|
| **Родительский объект - Уязвимость** | | | |
| SecurityType | Целое | Категория безопасности | Нельзя изменять |
| DangerLevel | Целое | 1- Низкий<br>4 - Критический | При 0 – не учитывается |
| OwnerName | Строка | Имя владельца инцидента - срабатывает при совпадении | При пустом значении не учитывается |
| Name | Строка | Подстрока в названии инцидента - срабатывает при совпадении | При пустом значении не учитывается |
| Status | Строка | Наименование состояния, при котором срабатывает сценарий | Обязательно к заполнению |
| ObjectType | Целое | Тип объекта | Нельзя изменять |
| **Подчиненные объекты – Задачи** `"task": { … }` | | | |
| Name | Строка | Добавляется к названию задачи | |
| Description | Строка | Добавляется к описанию задачи | |
| SecurityType | Целое | Категория безопасности задачи | Номер категории указан в справочнике |
| PlanStartDateAdd | Целое | Количество часов к плановому началу выполнения задачи от текущего времени | |
| PlanFinishDateAdd | Целое | Количество часов к плановому завершению выполнения задачи от текущего времени | |
| Department | Строка | Наименование подразделения для задачи | Обязательно для заполнения! |
| UserName | Строка | Имя пользователя для задачи | Обязательно для заполнения! |
| ObjectType | Целое | Тип объекта | 0 - Нельзя изменять |

| | | | |
|---|---|---|---|
| tasks | структура | Подчиненные задачи | null - Нельзя изменять |

Таблица 9. Требования к заполнению полей сценария автоматизации для Задачи.

| Наименование поля | Тип данных | Пояснение | Примечание |
|---|---|---|---|
| **Родительский объект - Задача** | | | |
| Name | Строка | Подстрока в названии инцидента - срабатывает при совпадении | При пустом значении не учитывается |
| Description | Строка | Не используется | |
| SecurityType | Целое | Категория безопасности | Нельзя изменять |
| PlanStartDateAdd | Целое | Не используется | |
| PlanFinishDateAdd | Целое | Не используется | |
| Department | Строка | Наименование подразделения - срабатывает при совпадении | При пустом значении не учитывается |
| UserName | Строка | Имя владельца инцидента - срабатывает при совпадении | При пустом значении не учитывается |
| Status | Строка | Наименование состояния, при котором срабатывает сценарий | Обязательно к заполнению |
| ObjectType | Целое | Тип объекта | Нельзя изменять |
| **Подчиненные объекты – Задачи** `"task": { … }` | | | |
| Name | Строка | Добавляется к названию задачи | |
| Description | Строка | Добавляется к описанию задачи | |
| SecurityType | Целое | Категория безопасности задачи | Номер категории указан в справочнике |
| PlanStartDateAdd | Целое | Количество часов к плановому началу выполнения задачи от текущего времени | |
| PlanFinishDateAdd | Целое | Количество часов к плановому завершению выполнения задачи от текущего времени | |
| Department | Строка | Наименование подразделения для задачи | Обязательно для заполнения! |
| UserName | Строка | Имя пользователя для задачи | Обязательно для заполнения! |
| ObjectType | Целое | Тип объекта | 0 - Нельзя изменять |
| tasks | структура | Подчиненные задачи | null - Нельзя изменять |

После окончания редактирования сценария нажмите кнопку «**Изменить**», после чего Система проверит корректность синтаксиса сценария и в случае успеха проверки выведет окно для подтверждения изменения.

### 3.12 Настройка создания объектов через коннектор с электронной почтой

Так как большинство устройств и систем безопасности позволяет информировать о событиях посредством сообщений по электронной почте, то с помощью коннектора электронной почты, встроенного в Систему возможно настроить интеграцию со сторонними системами - автоматизированное создание инцидентов, задач или уязвимостей на основе входящих почтовых сообщений. Также можно организовать процесс реагирования на рассылку уязвимостей, настроив подписку с сайтов новостей и обрабатывая их почтовые сообщения в системе. Доступ к настройкам обработки электронной почты осуществляется через пункт «**Обработка входящих сообщений**» в разделе «**Настройки и мониторинг работы системы**», вкладки «**Администрирование**» – Рисунок 84.

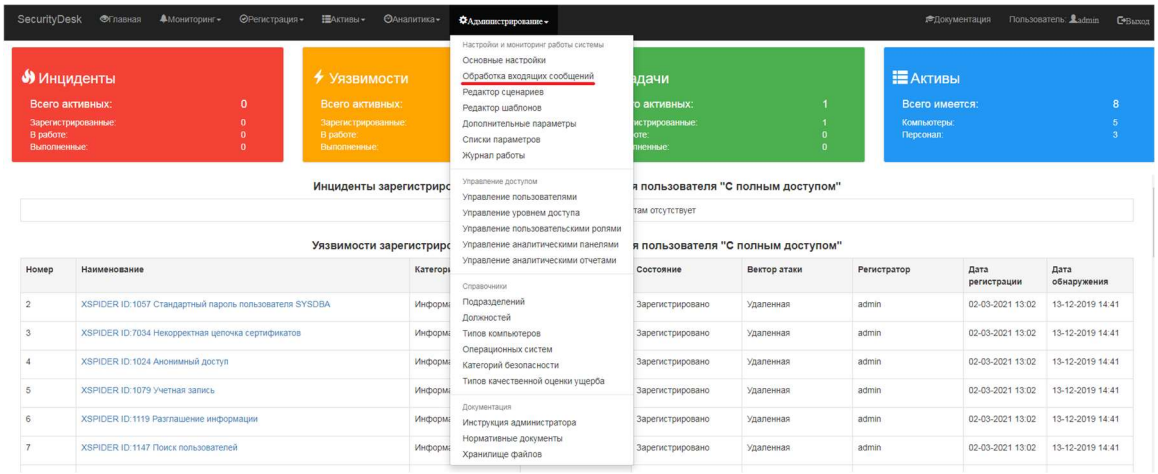


Рисунок 84. Доступ к редактору создания объектов по сообщениям электронной почты.

Для создания нового правила нажмите кнопку «**Создать**», в появившемся окне создания правила введите: Наименование правила, признак создания шаблона правила, Тип шаблона – т.е. какой объект будет создаваться по входящему почтовому сообщению (инцидент, уязвимость или задача), Дополнительную информацию, а также установите параметры очистки HTML-кода (целесообразно, когда электронное письмо содержит много HTML-конструкций) и включения в работу правила. Описание требований к атрибутам заполнения структуры правил представлены в таблице - Таблица 10.

Таблица 10. Требования к атрибутам правил создания объектов.

| **Наименование поля** | **Тип данных** | **Пояснение** | **Примечание** |
|---|---|---|---|
| **Родительский объект – Электронное сообщение** | | | |
| MailSubject | Строка | Срабатывает при совпадении темы письма с регулярным выражением | Для любых значений укажите \\w* |
| MailBody | Строка | Срабатывает при совпадении содержания письма с регулярным выражением | Для любых значений укажите \\w* |
| MailAddress | Строка | Адрес отправителя сообщения - | При пустом значении не учитывается |

| | | | |
|---|---|---|---|
| | | срабатывает при совпадении | |
| SaveAttachments | bool | Сохранять вложения сообщения в карточку объекта | true – сохранять вложение |
| SearchActives | bool | Искать во вложении активы и привязывать к объекту | true – искать активы во вложении |
| ObjectType | Целое | Тип объекта | 0 - Нельзя изменять |
| **Подчиненный объект – Инцидент** `"incident": { … }` | | | |
| Name | Строка | Добавляется к наименованию инцидента | |
| Description | Строка | Добавляется к описанию инцидента | |
| level | Целое | Уровень инцидента | Обязательно для заполнения! |
| Department | Строка | Наименование подразделения для задачи | |
| OwnerName | Строка | Имя пользователя для инцидента | Обязательно для заполнения! |
| ObjectType | Целое | Тип объекта | 0 - Нельзя изменять |
| tasks | структура | Подчиненные задачи | null - Нельзя изменять |
| **Подчиненный объект – Уязвимость** `"vulnerability": { … }` | | | |
| Name | Строка | Добавляется к наименованию уязвимости | |
| Description | Строка | Добавляется к описанию уязвимости | |
| SecurityType | Целое | Категория безопасности задачи | Номер категории указан в справочнике |
| OwnerName | Строка | Имя владельца инцидента - срабатывает при совпадении | Обязательно для заполнения! |
| DangerLevel | Строка | 1 - Низкий<br>4 - Критический | Обязательно для заполнения! |
| ObjectType | Целое | Тип объекта | 0 - Нельзя изменять |
| tasks | структура | Подчиненные задачи | null - Нельзя изменять |
| **Подчиненный объект – Задача** `"task": { … }` | | | |
| Name | Строка | Добавляется к названию задачи | |
| Description | Строка | Добавляется к описанию задачи | |
| SecurityType | Целое | Категория безопасности задачи | Номер категории указан в справочнике |
| PlanStartDateAdd | Целое | Количество часов к плановому началу выполнения задачи от текущего времени | |
| PlanFinishDateAdd | Целое | Количество часов к плановому завершению | |

| | | | |
|---|---|---|---|
| | | выполнения задачи от текущего времени | |
| Department | Строка | Наименование подразделения для задачи | |
| UserName | Строка | Имя пользователя для задачи | Обязательно для заполнения! |
| ObjectType | Целое | Тип объекта | 0 - Нельзя изменять |
| tasks | структура | Подчиненные задачи | null - Нельзя изменять |
| **Подчиненный объект – Параметры** `"parameters":[{…},{…}]` | | | |
| Name | Строка | Наименование дополнительного параметра | |
| Value | Строка/Число | Значение дополнительного параметра | Для числовых параметров используйте число, для остальных – строчное представление. Причем для чекбокса значения будут «True» «False», для даты формат «дд.мм.гггг чч:мм» |

Правила создания на основе почтовых сообщений объектов можно комбинировать со сценариями автоматизации. Выполняться такая комбинация будет в последовательности: **Правило обработки сообщения электронной почты –> сценарий автоматизации**.

## 3.13 Дополнительные параметры

В системе предусмотрена возможность расширить карточки Инцидентов, Уязвимостей и Задач добавив дополнительные параметры. Данная возможность позволяет гибко настроить карточки объектов под свои нужды и использовать данные параметры в отчетности наравне с основными параметрами. Для добавления параметра перейдите в раздел «**Администрирование**»- «**Дополнительные параметры**» - Рисунок 85.

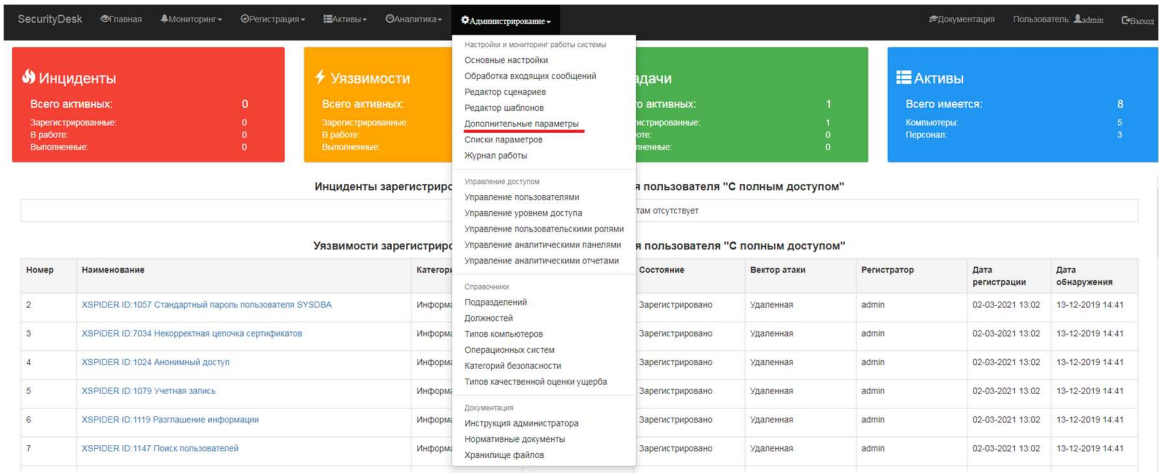


Рисунок 85. Переход к настройкам дополнительных параметров.

В форме редактора дополнительных параметров из выпадающего меню необходимо выбрать тип объекта и категорию безопасности – Рисунок 86. Далее с помощью кнопок к

объекту данной категории можно добавить параметр, удалить или отредактировать существующий.

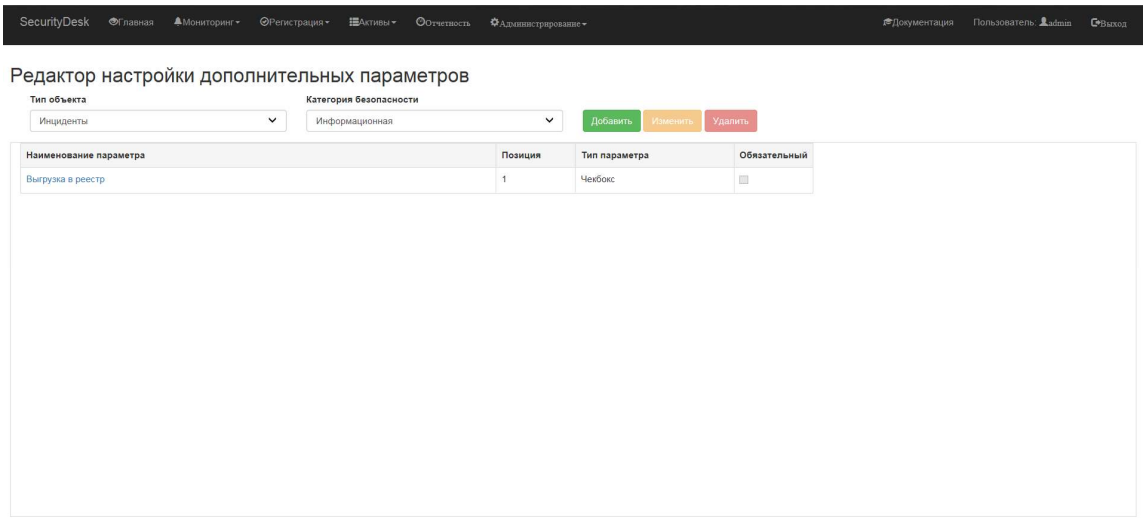


Рисунок 86. Редактор дополнительных параметров.

Для добавления нового параметра нажмите кнопку «**Добавить**», введите в поле «**Наименование**» - имя, с которым параметр будет отображаться на карточке, в поле «**Позиция**» указывается порядок положения параметра в списке дополнительных параметров, «**Тип параметра**» - соответственно формат параметра, параметр «**Обязательный**» - признак, требующий от пользователя обязательного заполнения данного параметра на карточке объекта при сохранении – Рисунок 87.

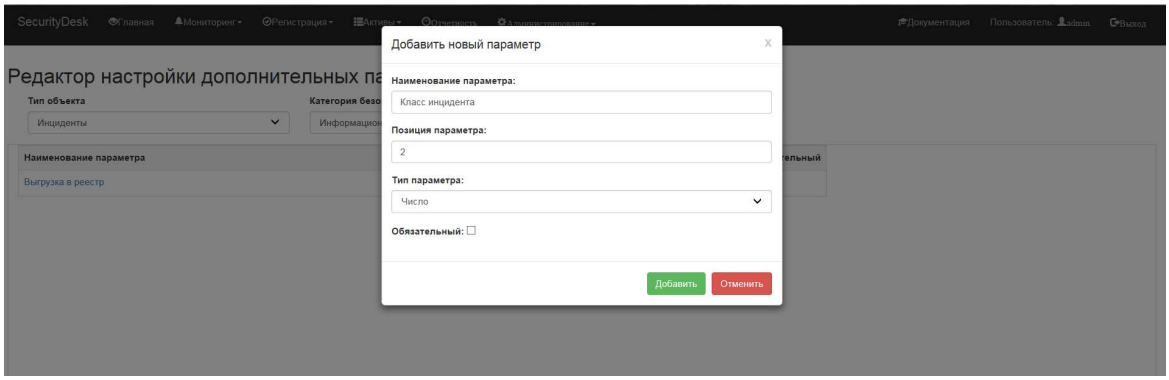


Рисунок 87. Создание дополнительного параметра.

При появлении хотя-бы одного дополнительного параметра в карточке объекта, ниже поля «Результат» появится раздел «**Дополнительные параметры**» в котором будут сгруппированы параметры, которые были добавлены для данного объекта – Рисунок 88. Также дополнительные параметры будут выводиться в карточках просмотра объектов во вкладке «**Дополнительные параметры**» и будут выгружаться в таблицу Excel из раздела «**Аналитика**» - «**Стандартизованные диаграммы**».

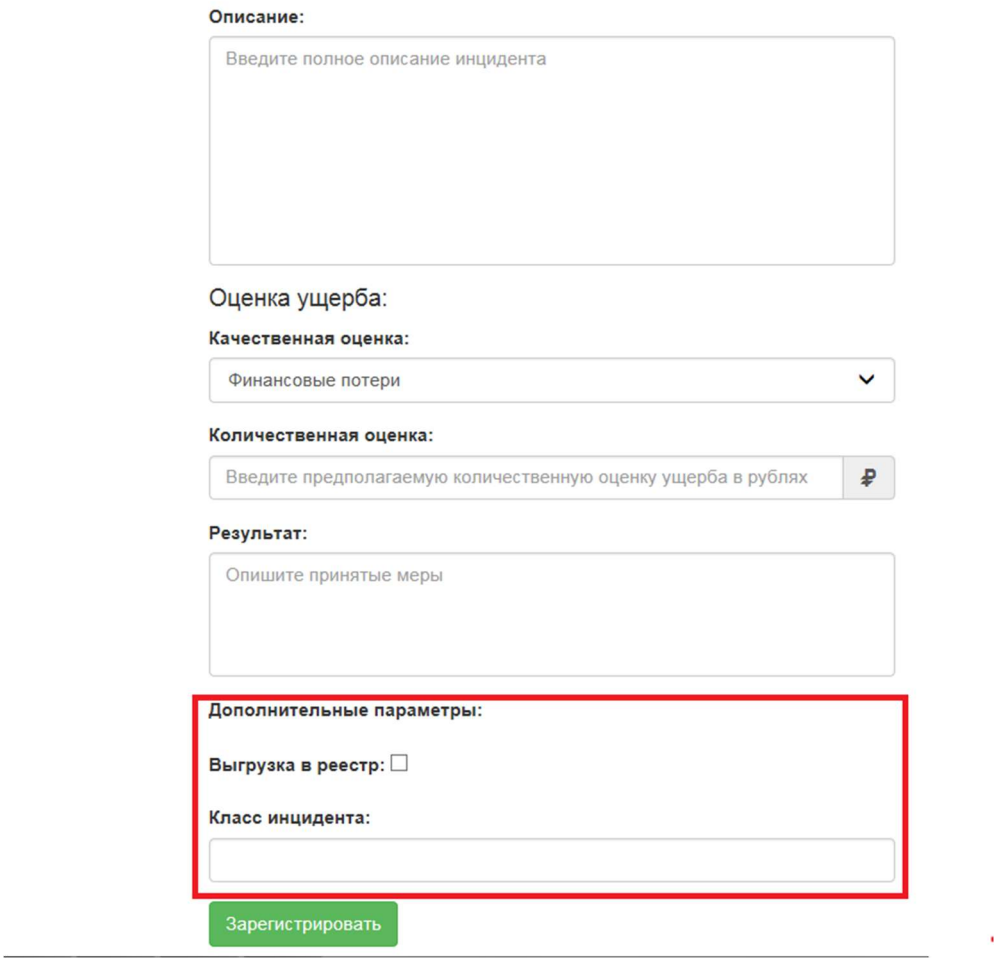


Рисунок 88. Дополнительные параметры на форме регистрации инцидента.

### 3.14 Шаблоны автоматического заполнения

Функционал шаблонов автоматического заполнения позволяет быстро заполнять поля для типовых инцидентов, уязвимостей и задач, существенно увеличивая производительность пользователей Системы. Возможность создания шаблонов предоставляется только пользователям, имеющим роль Администратор Системы. Применение шаблонов предоставляется всем пользователям без ограничения. Для создания шаблона перейдите в карточку инцидента, уязвимости или задачи для которого необходимо создать шаблон - Рисунок 89, заполните поля карточки и нажмите на кнопку «Сохранить» в блоке «Заполнить по шаблону», в появившемся окне введите имя шаблона и нажмите кнопку «Добавить».

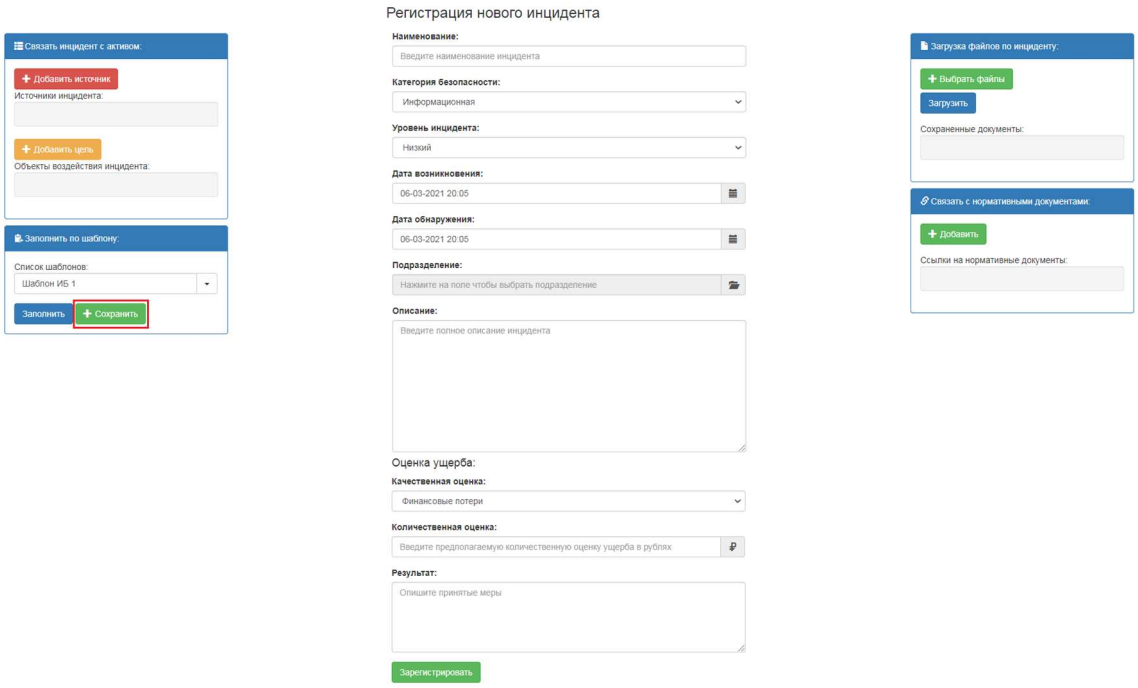


Рисунок 89. Создание шаблона заполнения.

Изменение и удаление шаблонов выполняется в соответствующем разделе администрирования – Рисунок 90.

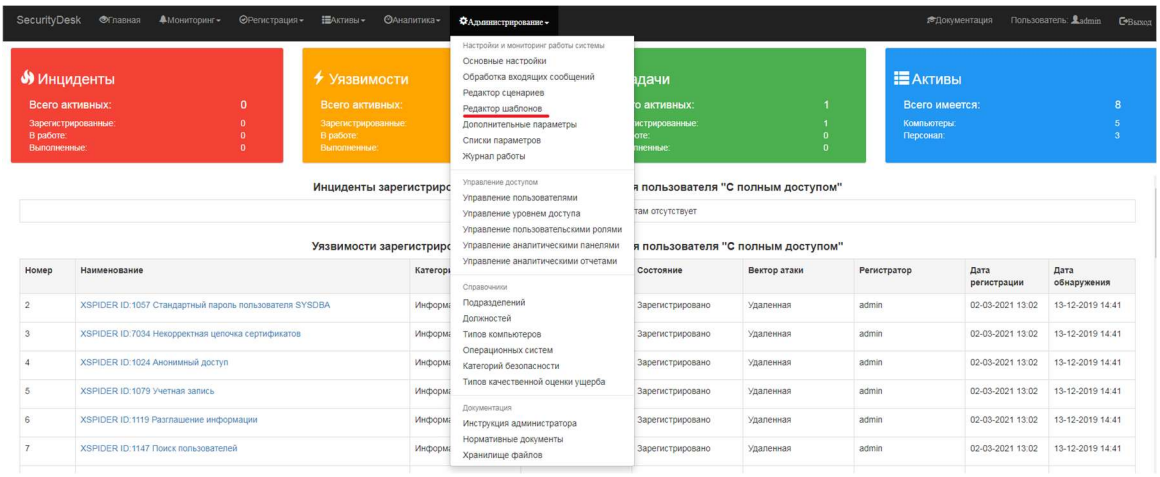


Рисунок 90. Управление шаблонами заполнения.

В открывшейся панели управления шаблонами - Рисунок 91 выберите необходимый тип объекта и категорию безопасности, после чего в левой части панели появится список доступных шаблонов. При нажатии на имя шаблона в правой части отобразится его структура в формате JSON - структуры. Для изменения шаблона отредактируйте параметры в JSON и нажмите кнопку «**Изменить**». Для удаления шаблона используйте кнопку «**Удалить**».

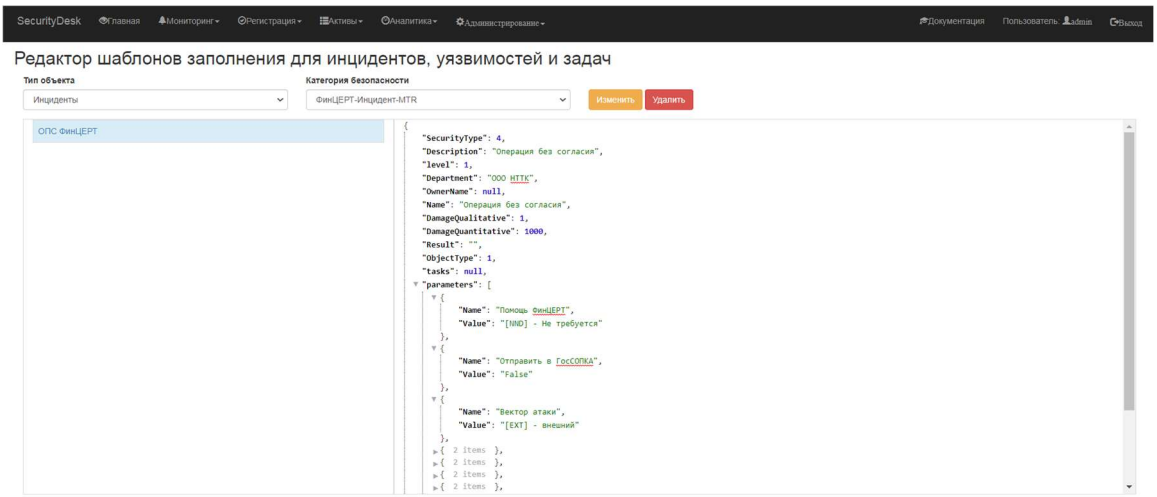


Рисунок 91. Панель управления шаблонами.

### 3.15 Резервное копирование и восстановление

Для резервного копирования Системы достаточно выполнять резервное копирование базы данных Microsoft SQL Server через средство управление **Microsoft SQL Server Management Studio**. Предварительно перед выполнением резервного копирования необходимо остановить WEB-сервер Системы через оснастку IIS – Рисунок 31, а также сервисы «**MailService**» и «**WFSchedulerService**» через средство управления службами - Рисунок 45. Далее откройте средство управление **Microsoft SQL Server Management Studio** выберите базу данных **SecurityDB** и через контекстное меню «**Задачи**» выбрав пункт «**Создать резервную копию …**» - Рисунок 92.

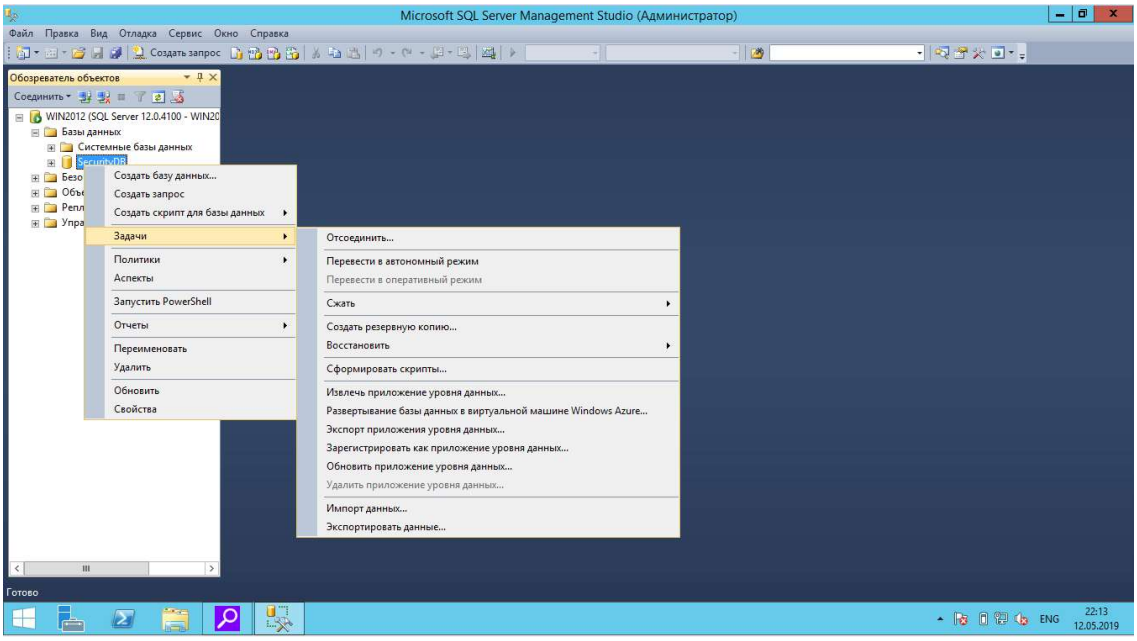


Рисунок 92. Создание резервной копии.

В окне укажите тип резервной копии, путь создания резервной копии и нажмите кнопку «**Ок**» после чего по указанному пути будет создана резервная копия базы данных Системы – Рисунок 93.

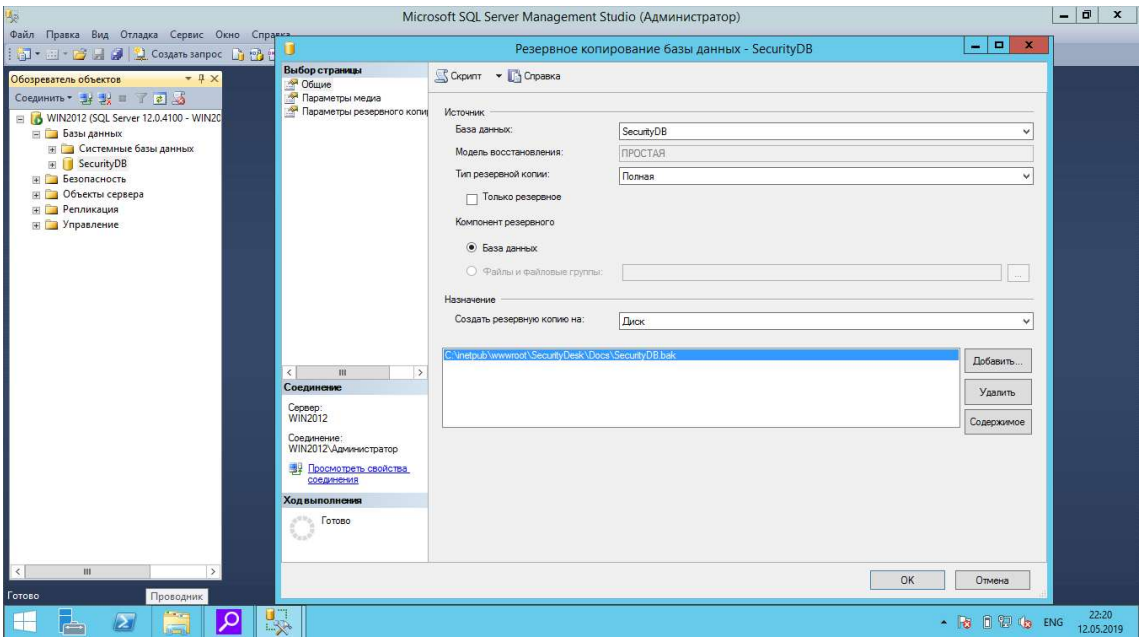


Рисунок 93. Окно резервного копирования.

Восстановление Системы производится аналогично тому, как описано в разделе 2.4 настоящего руководства.

# 4. Интеграция с сторонними системами по rest api

## 4.1 Общие настройки

Системой поддерживается функционал взаимодействия с внешними системами по API на основе REST-архитектуры. Для того чтобы осуществлять взаимодействие с WEB-сервисами системы по протоколу http, на основе REST-архитектуры необходимо выполнить следующие общие настройки:

- **Проверить наличие следующего раздела в файле настроек Web.config.**

```
<!--настройка авторизации для доступа по web api-->
  <location path="api">
    <system.web>
      <authorization>
        <allow users ="*" />
      </authorization>
    </system.web>

  </location>
```

Данная настройка отключает перенаправление пользователей на страницу авторизации, осуществляющих подключение по маршруту **[имя сервера]/api/…/…**. так как для проверки доступа к WEB-сервисам системой используется другой механизм авторизации.

- **Создать пользователя с необходимыми правами для взаимодействия**

Для доступа к объектам системы необходимо создать локального пользователя, имеющего необходимые привилегии доступа. Процесс создания пользователя не отличается от создания обычного локального пользователя.

### 4.2 Интеграция с системой сбора событий информационной безопасности RuSIEM

В Систему встроен специализированный коннектор для подключения системы сбора событий информационной безопасности RuSIEM. Для его включения необходимо выполнить настройки как в RuSIEM, так и в Системе.

- Для выполнения необходимых настроек в Системе перейдите в разделе «**Администрирование**» - «**Основные настройки**» во вкладку «**Интеграция с RuSIEM**» - Рисунок 94:

1. Введите/создайте с помощью кнопки «  » токен авторизации, который будет использоваться для передачи инцидентов в Систему из RuSIEM.
2. Выберите подразделение, имя пользователя под которым будут регистрироваться инциденты, поступающие из RuSIEM в Систему.
3. Для интеграции с активами (компьютерами и персоналом), зарегистрированными в Системе сделайте необходимые установки в разделе Настройки регистрации инцидентов.
4. Так как информация по инциденту из RuSIEM периодически обогащается за счет новых событий, Система позволяет сохранять всю хронологию поступающих обновлений из RuSIEM в файл JSON-формата. Для хранения обновлений включите соответствующий параметр «**Сохранять в инциденте raw-файл**».
5. Инциденты, находящиеся в RuSIEM в закрытом состоянии при получении новых данных могут повторно открываться. Для автоматического повторного открытия в Системе таких инцидентов включите соответствующий параметр «**Переоткрывать при возврате в RuSIEM**».
6. Параметр «**Сохранять в описании основные данные инцидента**» добавляет в описание инцидента основные параметры инцидента RuSIEM по форме: «**RuSIEM id='33046', fqdn='pc-vs078115.sd.ru', status='Зарегистрирован'**….»
7. Параметр «**Сохранять в описании инцидента метаданные**» добавляет в описание инцидента метаданные из раздела «rusiem_metadata_array» RuSIEM в виде «**Метаданные инцидента: 'symptoms.id':'Kaspersky: Virus detected'; 'hostname': 'pc-vs078115.sd.ru';»**
8. Параметр «**Сохранять в описании инцидента объекты группировки**» добавляет в описание инцидента метаданные из раздела «group_by_fields_array» RuSIEM в виде «**Объекты группировки: 'src.hostname':'PC-VS078115';»**

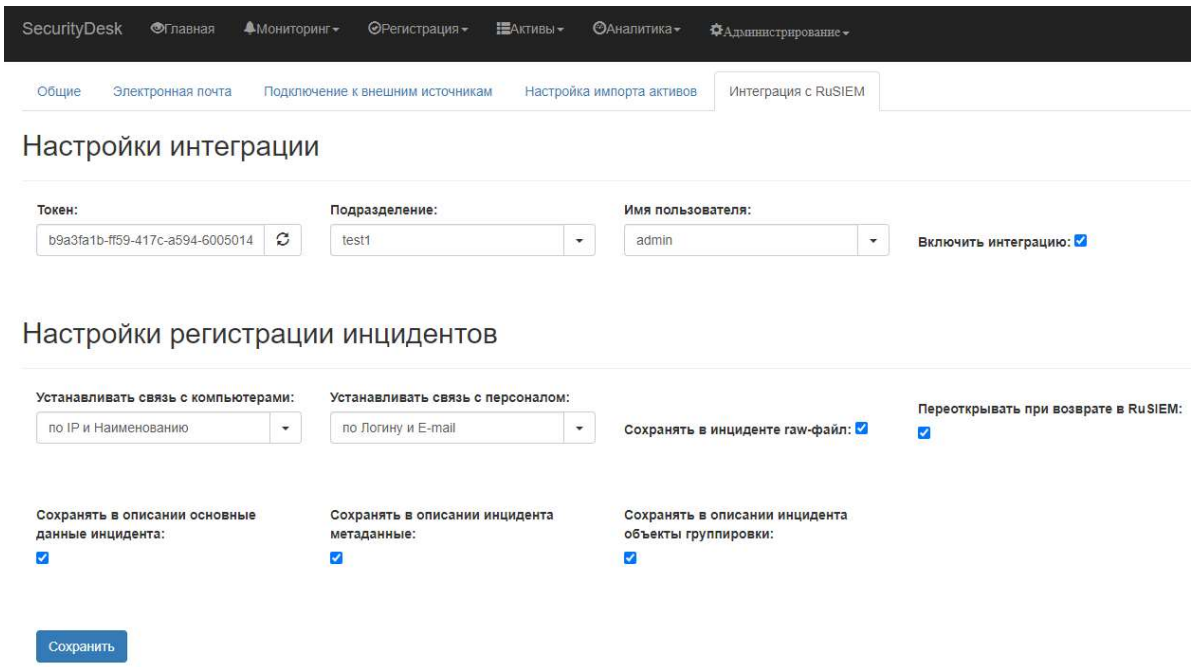


Рисунок 94. Настройка интеграции с RuSIEM.

- Добавьте в Системе к карточке инцидента и требуемой категории безопасности дополнительные параметры - Таблица 11. Для этого перейдите в раздел «**Администрирование**» - «**Дополнительные параметры**» Рисунок 85.

Таблица 11. Дополнительные параметры инцидента.

| **Наименование параметра** | **Тип параметра** |
|---|---|
| rusiem_id | Число |
| rusiem_category | Строка |
| system_updated_at | Строка |
| incident_link | Строка |
| IP | Строка |
| IP_TARGET | Строка |
| IP_SOURCE | Строка |
| fqdn | Строка |
| email | Строка |
| priority | Число |
| hash | Строка |
| login | Строка |
| soc_db_id | Строка |

| | |
|---|---|
| uri | Строка |
| web_domain | Строка |

- Для обеспечения изменения состояний инцидентов в RuSIEM, обработанных в Системе необходимо задействовать в работе сервер бизнес-процессов. Изменение состояния инцидента в RuSIEM осуществляется в workflow-схеме обработки инцидента на сервере бизнес-процессов с помощью специального компонента интеграции **SDRuSIEMChangeStatus**:
  1. Установите сервер бизнес-процессов и подключите к нему Систему, создайте workflow-схемы для соответствующих состояний Системы, в которых планируется изменять состояния инцидентов в RuSIEM.
  2. Откройте workflow-схему для обработки требуемого состояния инцидента.
  3. Для возможности отправки в сторону RuSIEM нового состояния сохраните номер инцидента в переменную «**rusiem_id**» используя блок установки новой переменной **SDsetVariable** Рисунок 95. Код сохранения номера в переменную «**rusiem_id**» на языке Lua может быть следующим:

```
lcnt=entity.Parameters.Count
for i=0, lcnt-1 do
 if(entity.Parameters[i]['Name']=='rusiem_id') then
    return entity.Parameters[i]['Value']
   end
end
return 0
```

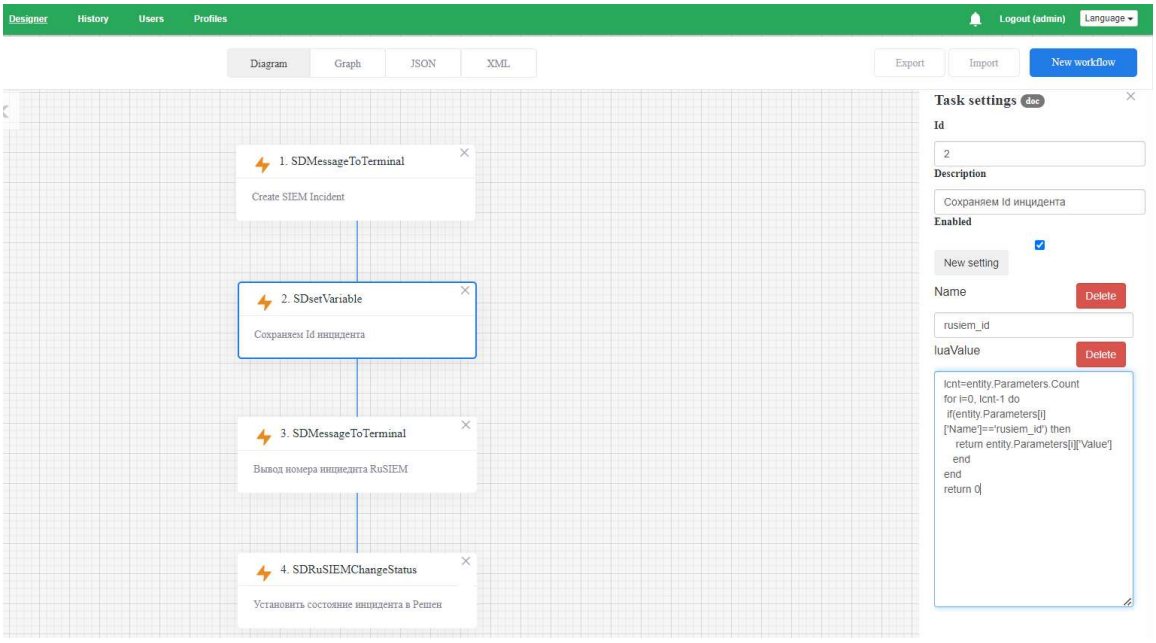


Рисунок 95. Сохранение номера инцидента RuSIEM в переменную.

4. Добавьте в workflow-схему блок изменения состояния **SDRuSIEMChangeStatus** Рисунок 96 и выполните его настройки:
   - Поле токена пользователя RuSIEM «**api_key**» – полученный токен учетной записи пользователя в RuSIEM (смотри далее раздел настроек интеграции в RuSIEM), от которой будут выполняться изменения состояний.

- Поле «host» - адрес сервера RuSIEM.
- Поле «status» - состояние, в которое требуется установить инцидент в RuSIEM.
- Поле «luaSolution» - скрипт на языке Lua, результат которого заносится в поле решения инцидента в RuSIEM.

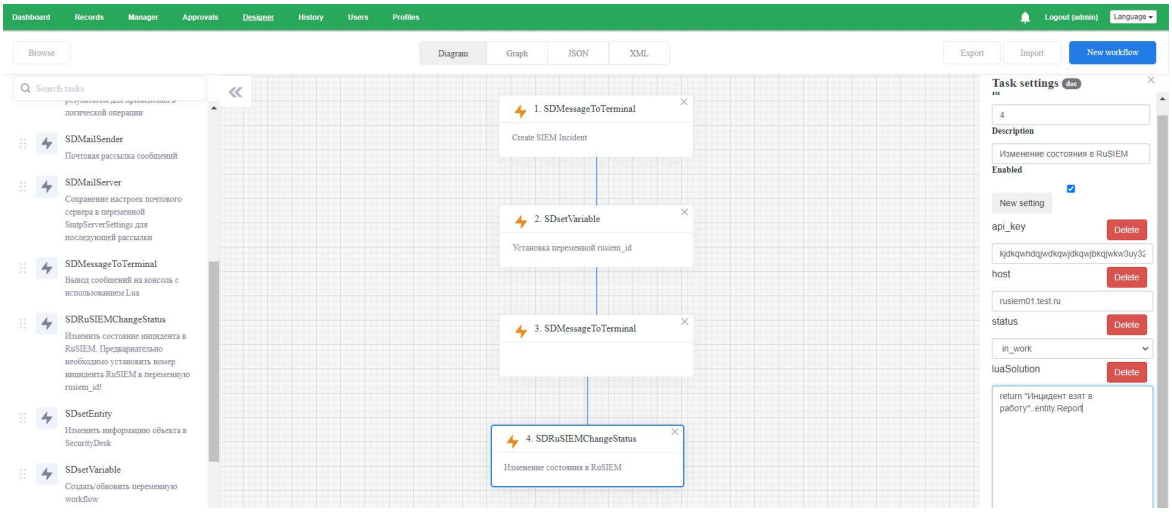


Рисунок 96. Настройка изменения состояния инцидента RuSIEM на сервере бизнес-процессов.

- Выполните настройки интеграции в RuSIEM:
  1. Создайте в системе новую пользовательскую роль, для этого перейдите в RuSIEM в раздел меню «**Настройки**» вкладка «**Роли**».

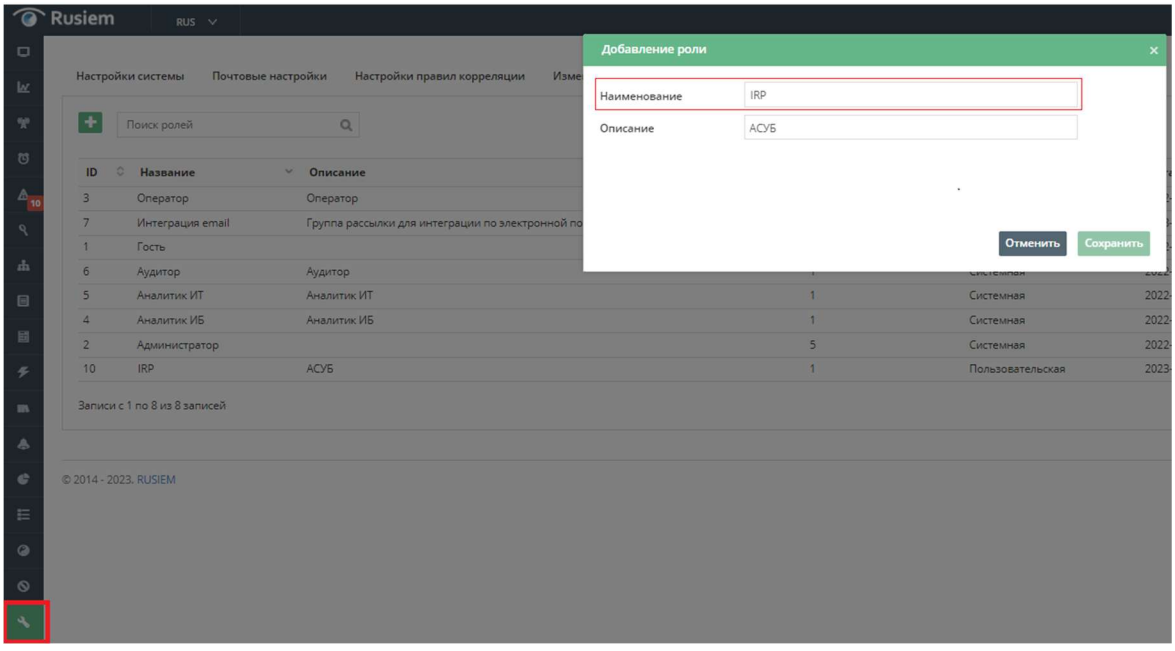


Рисунок 97. Создание новой роли.

  2. Перейдите в раздел «**Настройки**» - «**Интеграции**» и на вкладке «R-Vision» Рисунок 98 настройте параметры:
     - В поле «**Хост R-Vision**» введите адрес Системы.

- В поле «**Токен авторизации**» пропишите токен, созданный при настройке интеграции в Системе Рисунок 94.
- В качестве «**Группы для отправки инцидентов**» выберите созданную в предыдущем пункте роль.
- Включите параметры «**Интеграция активна**» и «**Синхронизация статусов**».
- В поле «**Категория по умолчанию**» заполните категорию безопасности. Системы, на которую будут регистрироваться инциденты из RuSIEM.
- Сохраните настройки кнопкой «**Сохранить**» и проверьте успешность подключения кнопкой «**Проверка подключения**».

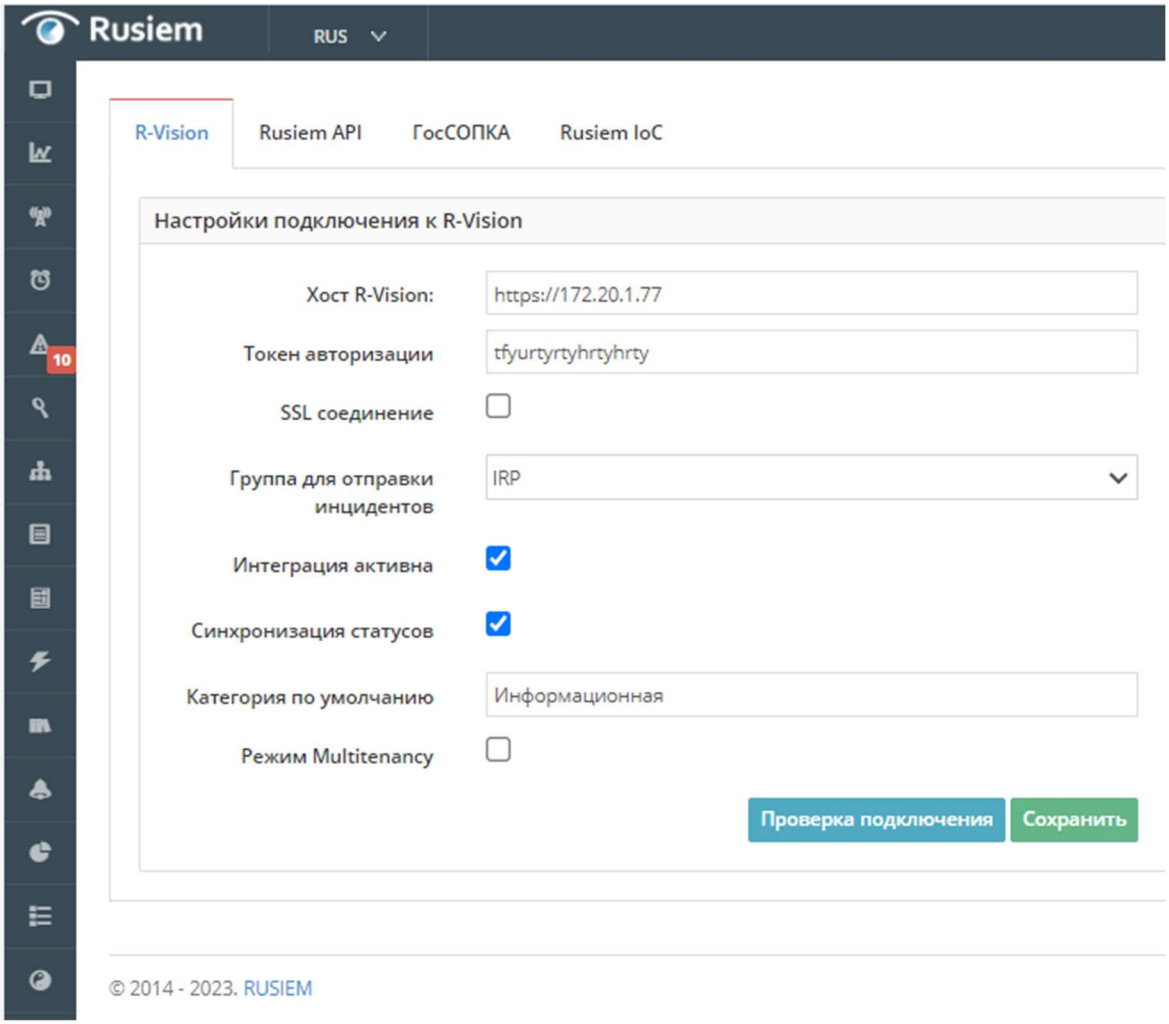


Рисунок 98. Настройка интеграции с Системой.

3. Создайте нового пользователя в RuSIEM Рисунок 99, от имени которого Система будет проводить изменения состояний в RuSIEM. Для этого в RuSIEM перейдите в раздел «**Настройки**» вкладка «**Пользователи**» и создайте пользователя как показано ниже.

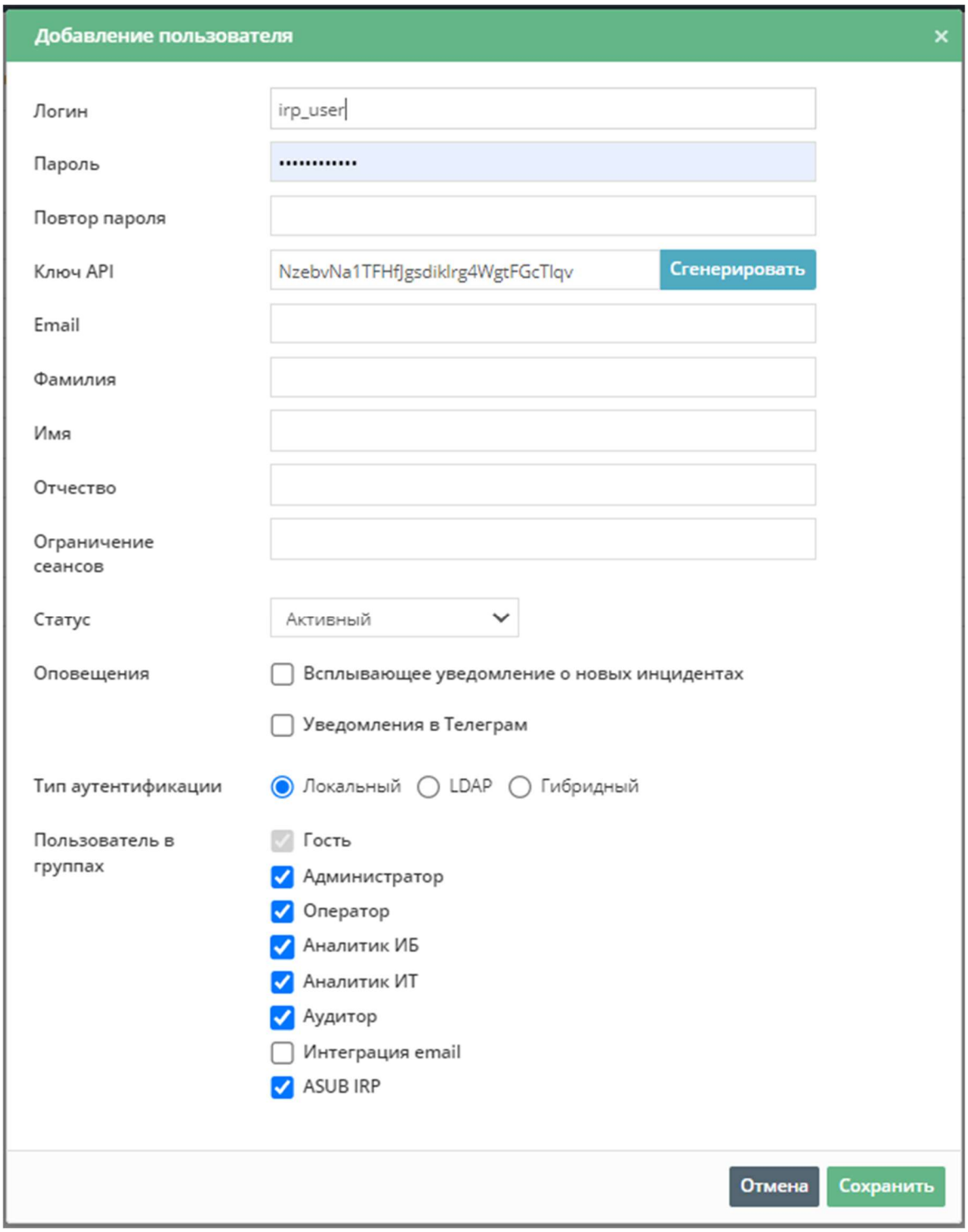


Рисунок 99. Создание нового пользователя в RuSIEM

Сгенерированный для пользователя «**Ключ API**» необходимо будет использовать в блоке **SDRuSIEMChangeStatus** сервера бизнес-процессов Системы в поле «**api_key**» - Рисунок 96.

4. Перейдите в раздел RuSIEM «**Корреллляция**», найдите необходимую корреляцию, инциденты по которой необходимо отправлять в Систему и скопируйте ее кнопкой  - Рисунок 100.

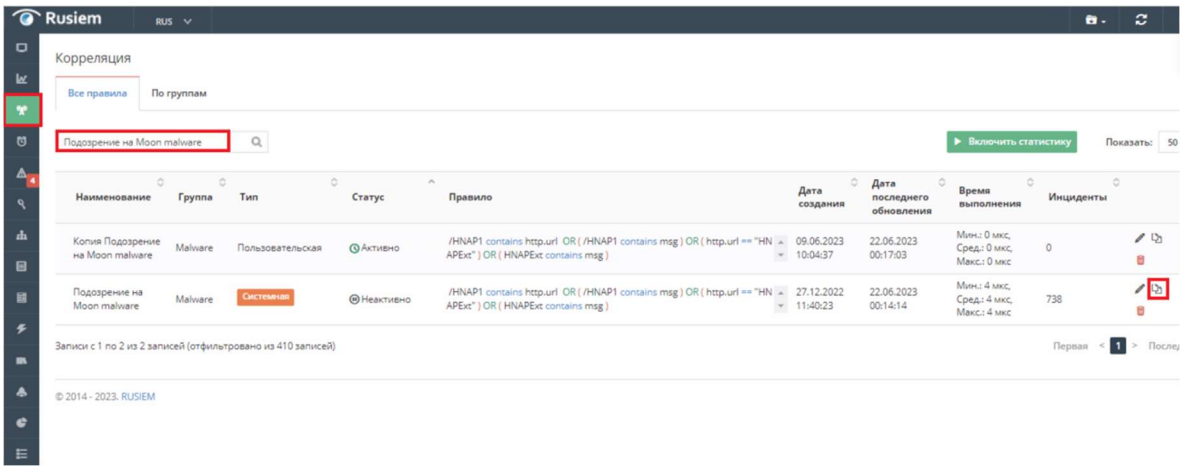


Рисунок 100. Создание пользовательской корреляции.

Перейдите в режим редактирования созданной пользовательской корреляции с помощью кнопки  . Выполните активацию скопированной корреляции Рисунок 101 и в группы назначения добавьте в группу, созданную ранее роль - Рисунок 97. Одновременно с активацией пользовательской корреляции, для исключения дублирования срабатываний, выполните деактивацию аналогичной системной корреляции, для этого перейдите в режим ее редактирования и снимите флаг с параметра «**Активно**».

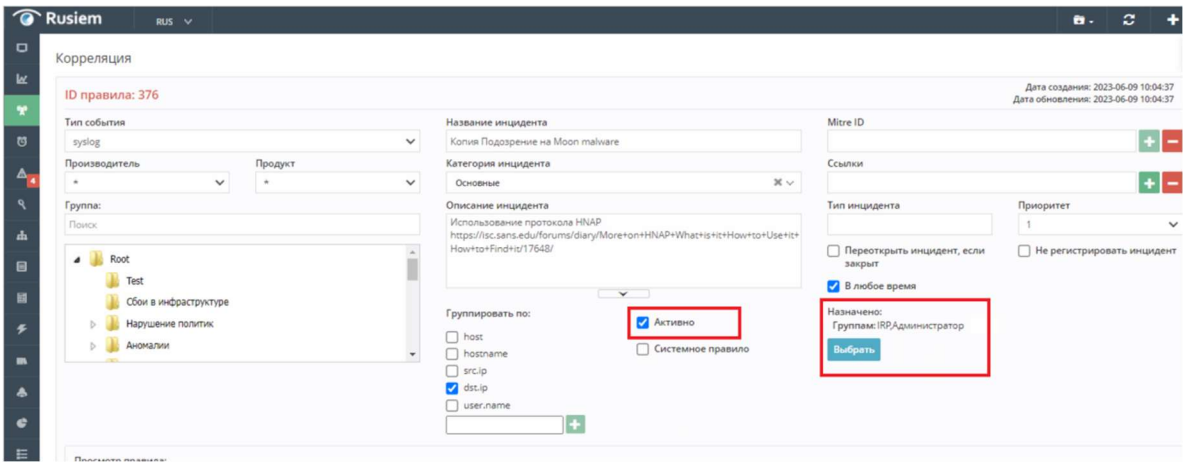


Рисунок 101. Редактирование пользовательской корреляции.

В случае правильно выполненных настроек интеграции в Системе будут регистрироваться инциденты RuSIEM. Карточка инцидента, полученного по интеграции RuSIEM будет содержать заполненные параметры инцидента. В случае установленных параметров интеграции во вкладке «**Активы**» будут находиться активы, задействованные в инциденте, а во вкладке «**Файлы**» будут сохранятся обновления инцидента в JSON-формате.

### 4.3 Интеграция с системой сбора событий информационной безопасности Positive Technologies MaxPatrol SIEM

В дистрибутиве с Системой поставляется специализированный коннектор-служба для подключения по API к системе сбора событий информационной безопасности Positive Technologies MaxPatrol SIEM

(далее PTSIEM). Для его подключения необходимо зарегистрировать службу ConnectorPTSIEM.exe, которая находится в дистрибутиве SecurityDesk-Services-[версия] с помощью команды:

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319\installutil.exe "C:\Program Files (x86)\
SecurityDesk\ConnectorPTSIEM.exe"
```

Настройте параметры подключения в конфигурационном файле **ConnectorPTSIEM.exe.config** службы:

Таблица 12. Настройки службы ConnectorPTSIEM.

| **Наименование параметра** | **Тип данных** | **Пояснение** | **Пример** |
|---|---|---|---|
| **Раздел appSettings** | | | |
| ConnectionTimeInterval | Число | Периодичность проверки появления инцидентов в PTSIEM (1000 - 1 секунда) | 1500 |
| DebugMode | bool | Включение режима отладки для подробного журналирования работы в Системе | false |
| SaveRaw | bool | Прикреплять данные инцидента PTSIEM в JSON-формате в карточку Инцидента Системы | true |
| CheckDays | Число | Глубина проверки инцидентов в PTSIEM за последние количество дней | 7 |
| SecurityType | Число | Идентификатор категории безопасности в которую будут сохраняться инциденты | 2 |
| AccountPTSIEM | Строка | Имя обобщённого подключения, используемого для доступа к PTSIEM | ptservice |
| client_id | Строка | Идентификатор подключения к PTSIEM | mpx |
| client_secret | Строка | Ключ подключения к PTSIEM смотрите: grep ClientSecret /var/lib/deployer /role_instances/ Core/params.yaml | **5c2327d2-15a1-4b8b-9b75-b8808167d0a8** |
| response_type | Строка | Тип ответа от PTSIEM на запрос аутентификации | code id_token |
| scope | Строка | Область – смотри документацию к PTSIEM | offline_access mpx.api ptkb.api |
| tokenRequestLink | Строка | Адрес сервиса для запроса токена аутентификации | https://[**IP**]:3334/connect/token |
| incidentListLink | Строка | Адрес сервиса для запроса списка инцидентов | https://[**IP**]/api/v2/incidents |
| incidentLink | Строка | Адрес сервиса для запроса конкретного инцидента | https://[**IP**]/api/incidents ReadModel/incidents |
| assignedUserEmail | Строка | Импорт инцидентов назначенных на пользователя в PTSIEM с email (значок * для загрузки всех инцидентов) | irp@securitydesk.ru |

| | | | |
|---|---|---|---|
| sdUser | Строка | Логин пользователя на которого регистрируется инциденты в SecurityDesk полученные из PTSIEM (для доменного пользователя укажите [домен]\[имя пользователя]) | admin |
| sdDepartment | Строка | Подразделение, на которое регистрируются инциденты в SecurityDesk | ptSIEMdep |
| ConnectActives | bool | Связывать инцидент PTSIEM с активами в SecurityDesk | true |

Запуск службы настройте от имени учетной записи, которой предоставлен доступ на запись в СУБД Системы и укажите подключения в конфигурационном файле **ConnectorPTSIEM.exe.config** раздела connectionStrings в строке подключения DatabaseConnection.

Для корректной регистрации инцидентов из PTSIEM дополните настройки инцидента соответствующей категории безопасности в Системе:

- Для категории безопасности, в которой будут регистрироваться инциденты, в карточку инцидента добавьте дополнительные параметры, согласно таблице 13 Дополнительные параметры инцидента PTSIEM.

Таблица 13. Дополнительные параметры инцидента PTSIEM.

| **Наименование параметра** | **Тип параметра** |
|---|---|
| key | Строка |
| source | Строка |
| isConfirmed | Чекбокс |
| measures | Строка |
| category | Строка |
| type | Строка |
| Influence | Строка |
| modified_date | Строка |

- В разделе «**Администрирование**» - «**Подключение к внешним источникам**» в Системе создайте обобщенное подключение **ptservice**, с логином и паролем пользователя, для которого предоставлены полномочия работы с инцидентами в PTSIEM.
- Убедитесь, что подразделение (sdDepartment) и пользователь (sdUser), указанные в конфигурационном файле **ConnectorPTSIEM.exe.config** присутствуют в Системе.

- Запустите службу **ConnectorPTSIEM.exe** от имени учетной записи windows, которой предоставлен доступ к СУБД SecurityDesk. Если настройки выполнены корректно инциденты из PTSIEM начнут загружаться в Систему, а в папке logs появится журнал работы службы.

Для изменения состояний инцидентов в PTSIEM, обработанных в Системе необходимо использовать в работе специальный компонент **SDPTSIEMChangeStatus** в workflow-схеме обработки инцидента на сервере бизнес-процессов (подключение сервера бизнес-процессов смотрите в разделе 2.5.7). Предварительно необходимо установить переменную **«id»** в workflow-схеме, сохранив в нее идентификатор инцидента с помощью компонента **SDsetVariable** – без установленной переменной **«id»** изменение состояния выполняться не будет. В блоке **SDsetVariable** установите параметры **Name: id, luaValue: return entity.Id -** Рисунок 102**.**

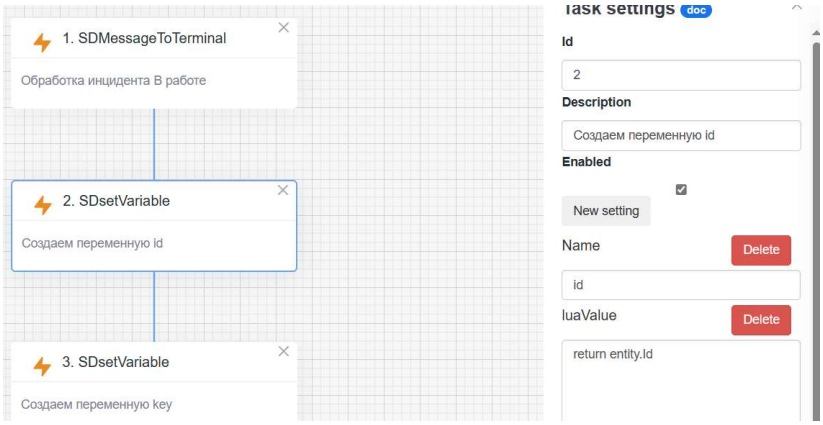


Рисунок 102. Установка переменной id.

Также предварительно необходимо использовать компонент SDsetVariable для создания и установки новой переменной «**key**» в workflow-схеме обработки состояний инцидента. На основании значения переменной «**key**» серверу бизнес-процессов необходимо будет принимать решение о том, является ли данный инцидент в системе инцидентом PTSIEM или нет.

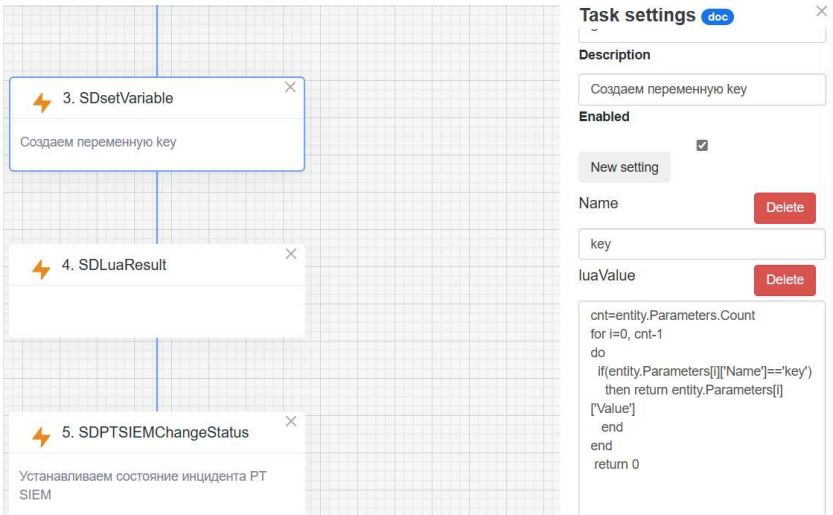


Рисунок 103. Установка переменной key.

Для сохранения значения в переменную «**key**» используйте следующий LUA-скрипт:

```
cnt=entity.Parameters.Count
for i=0, cnt-1
```

```
do
  if(entity.Parameters[i]['Name']=='key')
    then return entity.Parameters[i]['Value']
   end
end
 return 0
```

Далее, с помощью блока **SDLuaResult**, проверьте наличие данных в переменной «**key**» - Рисунок 104.

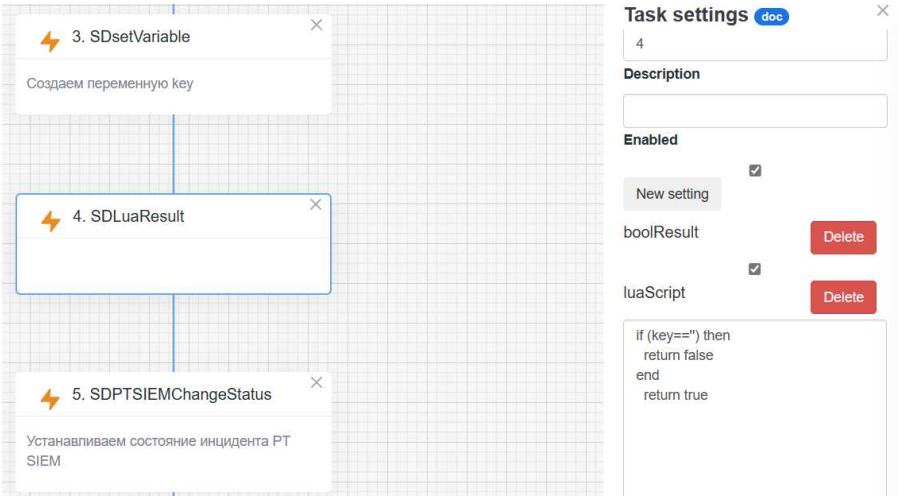


Рисунок 104. Проверка переменной key.

LUA-скрипт для проверки данных в переменной «**key**» может выглядеть следующим образом:

```
if (key=='') then
  return false
end
  return true
```

В случае положительного результата с помощью блока **SDPTSIEMChangeStatus** установите новое состояние инцидента в PTSIEM.

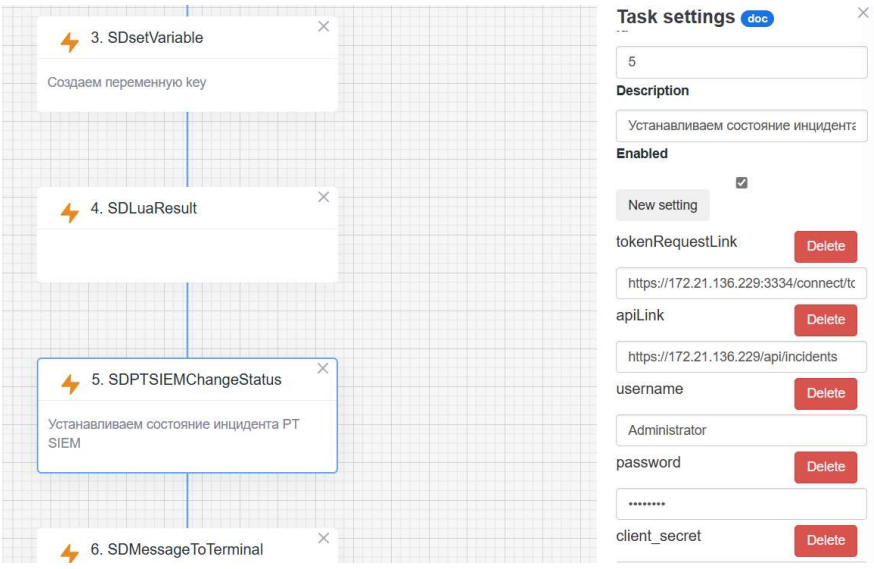


Рисунок 105. Установка нового состояния в PTSIEM.

Параметры установки **SDPTSIEMChangeStatus** смотрите в таблице 18 инструкция администратора сервера бизнес-процессов.

Внимание! При установке нового состояния необходимо соблюдать схему возможных переходов состояний инцидента в PTSIEM, указанных на рисунке 23 инструкции администратора сервера бизнес-процессов.

### 4.4 Правила взаимодействия

Для взаимодействия по API с внешними системами поддерживаются следующие http-глаголы для создания, изменения, удаления и чтения объектов системы в формате JSON:

**GET** – используется для чтения объектов;
**POST** - создание нового объекта;
**PUT** – изменение существующего объекта;
**DELETE** – удаление объекта.

Таблица 14 содержит возможные варианты запросов. Для создания/изменения объектов системы в теле запроса необходимо передавать данные в следующем JSON-формате:

- для инцидентов

```
incident = {
          name: "Наименование",
          securityType: 1, <!–Тип безопасности-->
          level: 1, <!–Уровень-->
          registrationDate: null,
          detectionDate: "Дата обнаружения",
          startDate: "Дата возникновения",
          department: "Идентификатор подразделения",
          owner: "имя учетной записи",
          status: "Состояние",
          description: "Полное описание",
          damageQualitative: 1, <!–Качественная оценка ущерба-->
          damageQuantitative: 1000, <!–Количественная оценка ущерба-->
          result:"Результат обработки инцидента"

     };
```

- для уязвимостей

```
vulnerability = {
          name: "Наименование",
          securityType: 1, <!–Тип безопасности-->
          level: 1, <!–Уровень-->
          registrationDate: null,
          publicDate: "Дата публикации",
          closeDate: null,
          owner: " имя учетной записи ",
          status: "Состояние",
          description: "Полное описание",
          impact: null,
          result:"Результат обработки уязвимости",
          attackVector: 1,
```

```
            cve: null, <!—Вектор атаки-->
            cwe:null

        };
```

- для задач

```
task = {
            name: "Наименование",
            securityType: 1, <!—Тип безопасности-->
            taskType: 2, <!—Уровень-->
            registrationDate: null,
            startDate: "21.12.2019 13:45",
            planFinishDate: "29.12.2020 00:25",
            realFinishDate: null,
            department: "Идентификатор подразделения",
            owner: " имя учетной записи ",
            status: "Состояние",
            description: "Полное описание",
            result: "результат обработки задачи"

        };
```

Таблица 14. Перечень http-запросов

| № | http-глагол | Шаблон запроса | Описание |
|---|---|---|---|
| 1 | GET | /api/Incidents | Получение полного списка инцидентов системы |
| 2 | GET | /api/Vulnerabilities | Получение полного списка уязвимостей системы |
| 3 | GET | /api/Tasks | Получение полного списка задач системы |
| 4 | GET | /api/Incidents/Id | Получение детальной информации по инциденту с номером Id |
| 5 | GET | /api/ Vulnerabilities /Id | Получение детальной информации по уязвимости с номером Id |
| 6 | GET | /api/ Tasks /Id | Получение детальной информации по задаче с номером Id |
| 7 | POST | /api/Incidents | Создание нового инцидента, параметры передаются в теле запроса |
| **8** | POST | /api/ Vulnerabilities | Создание новой уязвимости, параметры передаются в теле запроса |
| **9** | POST | /api/ Tasks | Создание новой задачи, параметры передаются в теле запроса |
| **10** | PUT | /api/Incidents/Id | Изменение существующего инцидента с номером Id, параметры передаются в теле запроса |
| **11** | PUT | /api/Vulnerabilities /Id | Изменение существующей уязвимости с номером Id, параметры передаются в теле запроса |
| **12** | PUT | /api/Tasks /Id | Изменение существующей задачи с номером Id, параметры передаются в теле запроса |
| **13** | DELETE | /api/Incidents/Id | Удаление существующего инцидента с номером Id |
| **14** | DELETE | /api/Vulnerabilities /Id | Удаление существующей уязвимости с номером Id |
| **15** | DELETE | /api/Tasks /Id | Удаление существующей задачи с номером Id |