



SecurityDesk Инструкция администратора

[SECURITYDESK АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ]

Инструкция администратора 1.42

Оглавление

В	ЗведениеЗ							
Π	ринять	ые сокращения и определения	3					
1.	Ми	нимальные системные требования	3					
2.	Уста	ановка и настройка	4					
	2.1	Подготовка операционной системы	4					
	2.2	Установка СУБД Microsoft SQL Server	8					
	2.3	Установка Системы	11					
	2.4	Установка базы данных и параметров подключения к СУБД Microsoft SQL Server	14					
	2.5	Настройка компонентов Системы	19					
	2.5.1	Частройка основного конфигурационного файла	24					
	2.5.2	/становка лицензионного ключа	25					
	2.5.3	Настройка продолжительности сессии пользователей	26					
	2.5.4	Частройка сервиса электронной почты	26					
	2.5.5	Настройка сервиса выполнения периодических операций	27					
	2.5.6	Обеспечение безопасности настроек подключения с проверкой подлинности SQL Serve	r					
			28					
	2.5.7	Настойка подключения к серверу бизнес-процессов	28					
3.	Ади	линистрирование	29					
	3.1 Пе	рвоначальная настройка	29					
	3.2 Ha	стройка справочников	33					
	3.3 Уп	равление состояниями объектов	34					
	3.4 Уп	равление пользователями и ролями	36					
	3.5 Ko	нструктор аналитических диаграмм	40					
	3.6 Ko	нструктор аналитических отчетов	41					
	3.7 Пр	едоставление доступа пользователей к аналитическим панелям отчетов и диаграмма	м					
	•••••		42					
	3.8 По	одключение к внешним источникам	43					
	3.9 Ил	лпорт активов	45					
	3.10 3	аполнение справочника нормативных документов	48					
	3.11 ⊦	астройка сценариев автоматизации	48					
	3.12 ⊦	астройка создания объектов через коннектор с электронной почтой	53					
	3.13 J	ополнительные параметры	55					
	3.14 L	Цаблоны автоматического заполнения	57					
	3.15 P	езервное копирование и восстановление	59					
4.	Инт	еграция с сторонними системами по rest api	60					

4.1 Общие настройки	60
4.2 Интеграция с системой сбора событий информационной безопасности RuSIEM	61
4.3 Интеграция с системой сбора событий информационной безопасности Positive	
Technologies MaxPatrol SIEM	67
4.4 Правила взаимодействия	72

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.

🕞 🗸 Диспетче	ер серверов • Панель мони	торинга		• 🕝 🚩 Управление	Средства Вид Справка
🎹 Панель мониторинга	Вас приветствует диспетчер серверов				
 Покальный сервер Все серверы Файловые службы и сл ▷ 	1 Настрои Бестрий запуск 2 Добави	ить этот локальный (ить роли и компоненты	сервер		
	3 Добав	ř.	Мастер добавления ролей и компонентов	X	
	Что нового 4 Созда	Выбор целевого	сервера	КОНЕЧНЫЙ СЕРВЕР win2012	
	Подробнее	Перед началом работы Тип установки Выбор соороор	Выберите сервер или виртуальный жесткий диск, на котором будут ус компоненты. Выберите сервер из пула серверов	становлены роли и	Скрыть
	РОЛИ И ГРУППЫ СЕРВЕРОВ Роли: 1 Группы серверов: 1 Всего серверов: 1 Файловые службы и	Роли сервера Компоненты Подтверждение	Выберите виртуальный жесткий диск Пул серверов Фильтр:		
	 службы хранилища Управляемость События 	Результаты	Има IP-адрес Операционная система win2012 10.02.15 Майкрософт Ознакомит	з тельная версия Windows Serve	
	Производительность Результаты ВРА		Каланиетеров: 1 Найдено компьютеров: 1 На этой странице показаны серверы под управлением Windows Serve добавлены с похощью команды. "Добавле серверы" в дистетчере се автонокличе серверы и добавленные новые серверы, данных с котор получены.	> sr 2012, которые были еревров. Не выводятся ных пока полностью не	
			< Hasag Danee >	Установить Отмена	
				*	Рус 13:50 09.05.2019

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».

💮 т Диспетче	ер серверов • Панель монит	оринга		- 🗊 🚩 Управление	Средства Вид Справка
Панель мониторинга	Вас приветствует диспетчер серверов				
 Покальный сервер Все серверы Файловые службы и сл ▷ 	1 Настрои	ть этот локальный	сервер		
	2 Добави	ть роли и компоненты	Мастер добавления ролей и компонентов	_ □ X	
	Что нового (4) Созда	Выбор компонен	НТОВ	КОНЕЧНЫЙ СЕРВЕР win2012	
	Падобнее РОЛИ И ГРУППЫ СЕРВЕРОВ Роли: Группи серверов: Вего серверов: Файловые службы и 1 Фулравлеемость События Производительность. Результаты ВРА	Перед началом работы Тил установон Выбор серевра Роли серевра Компонента Роль веб-серевра (II) Служби ролей Подтверхдение Рерукстви	Виберите один или несколько компонентов для установси т Компоненты Удаленное разностное скатие Удаленное разностное скатие Одаленной помицика Одаленной помицика Одаленной помиккой Онлатр Windows THF Filter D Онлатр Windows THF Filter D Oncease интерастраная служба передин (8 Odanugur ANET Framework 3.5 (колночет NET 2.0 и 3.0) Астивация не по HTTP Астивация по HTTP Астивация не по HTTP Оdanue ALE Framework 4.5 (установлено 2 из MET Framework 4.5 (установлено 1 из 5) ME Oppode Wet Radio Radi	на этом сервере. Описание АSP.RT 4.5 обеспечивает базовую подадержу для запуска как автомочники приложений ASP.NET 4.5, так и прокожений, интеррированных со службании IIS.	Copens
			< Назад Далее	е > Установить Отмена	
Windows PowerShell					
				• 🖻	Pyc 13:54 09.05.2019

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».

Выберите компоненты Екргезз для установки. Условия лицензии Глобальные правила Центр обковления Майкросс Обновления продукта Установка файлов установки Правила установки Выбор компонента Настройка экземпляра Конфигурация и работа каждого компонента Пакет SOK компонента Database Engine ○ Сружбы компонента Database Engine ○ Средства сван клиентских средств ○ Средства управления - полный набор Пакет SOK компоненты 20L селова управлия и сковбодноми месту на диске Диск С: требуется 2550 M5, свободно 40430 M5 Выделить все Выделить все Отменить все Выбор Корневой каталог экземпляра	3	Программа устан	овки SQL Server 201	14			
Условия лицензии Глобальные правила Центр обновления Майкросо Обновления продукта Установка файлов установки Правила установки Выбор компонента Выбор каталог экземпляра: С:\Program Files\Microsoft SQL Server\	Выбор компонентов Выберите компоненты Expre	ss для установки.					
Выделить все Отменить весь выбор Корневой каталог экземпляра: С:\Program Files\Microsoft SQL Server\	Условия лицензии Глобальные правила Центр обновления Майкросо Обновления продукта Установка файлов установки Правила установки Выбор компонентов Правила компонента Настройка компонента Datab Правила конфигурации комп Ход выполнения установки Готово	Компоненты: Службы компонента Database Er Службы компонента Database Er Службы Reporting Services в соб Обще функции Службы Reporting Services в соб Обще функции Средства связи клиентских средств Обдите функции Средства управления - основны Средства управления - основны	ngine еский поиск ственном режиме ств тских средств е ый набор I SQL	Описание компонента: Конфигурация и работа каждого компон экземпларов SQL Server отделена от другю экземпларов SQL Server иогут работать параллельные условия для выбранных компонентов: Уже установлено: 	ента « 4.0 > 30 МБ		
Каталог общих компонентов: C:\Program Files\Microsoft SQL Server\ Каталог общих компонентов (x86): C:\Program Files (x86)\Microsoft SQL Server\		Выделить все Отменить весь выбор Корневой каталог экземпляра: Каталог общих компонентов: Каталог общих компонентов (x86):	C:\Program Files\Mic C:\Program Files\Mic C:\Program Files (x86	Files\Microsoft SQL Server\ Files\Microsoft SQL Server\ Files (x86)\Microsoft SQL Server\			

Рисунок 10. Выбор компонентов.

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

1		Центр	установки SQL Server			×									
Планирование Установка Обслуживание Средства	1	Hoi Kon Jar Aot	Новая у компон Запусти добавля	Новая у компон Запусти добавля	Настройка экземпляр Укажите имя и идентификато установки.	Програ ра пр для экземпляра SC	имма установ L Server. Иденти	<mark>іки SQL</mark> фикатор	L Server 2014 р экземпляра будет	зключен в путь	_ D X				
Ресурсы Параметры		Запусти или SQL	Условия лицензии Глобальные правила Центр обновления Майкросо	 Экземпляр по у Именованный 	молчанию кземпляр:	MSSQL	SERVER			× 2	_		-		
			Основнити родити Установка файлов установки Правила установки Выбор компонентов Паравила компонента Настройка эзосемиляра Конфигурация сервера	Идентификатор эн Каталог SQL Serve Каталог служб Rep Установленные эк	земпляра: : orting Services: земпляры:	MSSQL C:\Prog C:\Prog	.SERVER gram Files\Microsoft 9 gram Files\Microsoft 9	iQL Server\MSSQL12 iQL Server\MSRS12.1	MSSQLSERVER MSSQLSERVER]					
Mirrosoft SQL Server 2014			Настройка служб Reporting S Правила конфигурации комп Ход выполнения установки Готово	Имя экземпляра	Идентифика экземпляра	тор	Компоненты	Выпуск	Версия						
											רס		-		
		Элем					< Назад Дал	ee > Otmer	а Справка		L KZ		-		
				-					Ознако Г	мительная в Іицензия Wi	ерсия Windows ndows действите	Server 2012 R2 ельна в течен	2 Standard ие 180 дн. Build 9600		
											• 🏱 📋	🗐 🍓 РУС	09.05.2019		

Рисунок 11. Настройка экземпляра.

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

5	Программа у	становки SQL Server 2014		_ 0	3
Конфигурация сервер Укажите учетные записи служи	а б и конфигурацию параметров сорт	ировки.			
Условия лицензии Глобальные правила Центр обновления Майкросо	Учетные записи служб Параме Рекомендуется использовать о	тры сортировки тдельную учетную запись для каждой слуз	кбы SQL Server.	:	
Обновления продукта	Служба	Имя учетной записи	Пароль	Тип запуска	
Установка файлов установки	лдро СУБД SQL Server	NT Service/MSSQLSERVER		Авто	ř
Правила компонента Настройка экземпляра Конфигурация сервера Настройка компонента Datab Правила конфигурации комп Ход выполнения установки Готово					
		< Назад Да	лее > С	Отмена Спра	вка

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.

1		Центр	установки SQL Server		- • ×			
Планирование Установка Обслужавание Средства Ресурсы Параметры		Центр Новая у компон Запусти добавля Обновл 2012 Запусти или SQI	установки SQL Server	Программи а Database Engin линности, администратор Конфигурация сервер Задайте режим про Режим проверки по,	а установки SQL Server 2014 е обб и каталоги данных для компонента Datal а Каталоги данных Пользовательские эки а Каталоги данных Пользовательские эки доминистраторов для и даминисти	base Engine. емпляры FILESTREAM сомпонента Database Engine.		
Microsoft SQL Server 2014			Установка файлов установки Правила установки Выбор компонентов Правила компонента Настройка засемляра Конфилурация сервера Настройка компонента Data. Правила конфилурация комп Хода выполнения установски Готово	 Веким проверки и Среданный реки Среданный реки Ужалте парола: Податверчите парола: Податверчите парола: Колосов дининстр Колосов Даринистр 	падлинности Windows M (проверка падлинности SQL Server и Wind учетной записи системного администратора (******* # arropole SQL Server	оха) SQL Server (sa). — раз SQL Server эры SQL Server имееот ий доступ к разонаниту разволе водолениту разволе		
		Элем		Добавить Текущего	о пользователя Добдантъ Уданитъ К Назад Далее >	Отмена Справи	акомительная версия V	Vindows Server 2012 R2 Standar
	1	1					Лицензия Windows д	ействительна в течение 180 дн Build 9600 P 🕜 💱 🐚 ENG 14:10 09.05.2019

Рисунок 13. Настройка типа авторизации пользователей.

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

1	Программа установки SQL Server 2014	- • ×
Ход выполнения уста	новки	
Условия лицензии Глобальные правила Центр обновления Майкросо Обновления продукта Установка файлов установки Правила установки Выбор компонентов Правила компонента Настройка экземпляра Конфигурация сервера Настройка компонента Datab Правила конфигурации комп Ход выполнения установки Готово	Install_sql_ssms_Cpu64_Action	
	Далее > Отмена	Справка

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.

1	Программа установки SQL Se	rver 2014 📃 🗖 🗙
Завершено Установка SQL Server 2014 вы	яполнена успешно с обновлениями продуктов.	
Условия лицензии	Сведения об операции установки или возможных сле	дующих шагах:
Глобальные правила	Компонент	Состояние
Центр обновления Маикросо	🖉 Средства управления - полный набор	Выполнено успешно
Обновления продукта	Средства связи клиентских средств	Выполнено успешно
Установка файлов установки	Пакет SDK клиентских средств	Выполнено успешно
Правила установки	Обратная совместимость клиентских средств	Выполнено успешно
Выбор компонентов	Средства управления - основные	Выполнено успешно
	🕝 Службы компонента Database Engine	Выполнено успешно
Правила компонента	🖉 Браузер SQL	Выполнено успешно
Настройка экземпляра	Компоненты документации	Выполнено успешно
Настройка компонента Datab Правила конфигурации комп	Сведения:	
Ход выполнения установки	Просмотр документации по продукту для SQI	_ Server ^
Завершено	Установлены были только компоненты, которые и Server и управления этой документацией. По умо сетевую библиотеку. После установки SQL Serve документацию можно загрузить на свой компьют Использование электронной документации Майкр LinkID=299578>). Центр обновления Майкрософт	спользуются для просмотра документации для SQL пчанию средство просмотра справки использует с помощью диспетчера библиотек справки ер. Дополнительные седения см. в разделе юсофт по SQL Server (< <u>http://go.microsoft.com/fwlink/?</u>
	Файл сводного журнала был сохранен в следующем р	асположении:
	C\Program Files\Microsoft SQL Server\120\Setup Bootst 0RMAOB1ESTC 20200809 183735.txt	rap\Log\20200809_183735\Summary_WIN-
	1	Закрыть Справка

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.

Бар Корзина									-
			👪 l 💽 👪 = 1		Средства работы с приложениями		distr	_ _ X	
			Файл Главная По,	делиться Вид	Управление			~ 0	
			(e) (e) + ↑ () (b) + 3n	от компьютер 🕨 Л	Іокальный диск (C:) 🕨 distr		🗸 🖒 Поиск: distr	٩	
			🔆 Избранное	Имя	Д ата	изменения Тип	Размер		
			i Sarpyson Si Hagamus Mecta Pasouni cron I Stor commortep I Stor commortep	5 SecurityDesk-	опол. Загуск от имееня администр Загуск от имееня администр Справление проблема с со загусетия ть ваназлиноза загустиять на панели задач Вырезать Вставить Создатя врлык Удалить Переименовать Свойства	2010.14/30 Пачина разде затора вместимостью ране >ссию	: 134 462 КБ		
								2	
_			1 элемент Выбран 1 эл	емент: 131 МБ					
	Windows Pow	verShell				2	Ознак	омительная версия Wind Лицензия Windows дейс	ows Server 2012 R2 Standard гвительна в течение 180 дн. Build 9600
	- 2							• P	14:31 ENG 09.05.2019

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.

Бар Корзина				.
-				
	🎉 l 🕞 🚯 = 1	Средства работы с приложениями	distr	
	Файл Главная Подел	иться Вид Управление		 Ø
	💮 💿 👻 🛉 🎉 🔸 Это	8 Установка — SecurityDesk, версия 1.25	Demo – 🗆 🗙 🖒 Поиск: distr	
	🔆 Избранное	Выбор папки установки В какую папку вы хотите установить SecurityDesk?	Размер 134 462 КБ	
	Рабочий стол	Программа установит SecurityDesk в следующу	io nanky.	
	1 Этот компьютер	Нажните «Далее», чтобы продолжить. Если вы хотите нажните «Обзор».	выбрать другую папку,	
	🙀 Сеть	C:\Program Files (x86)\SecurityDesk	Обзор	
			Обзор папок	x
		Требуется как ненятум 73,3 Мб свободного диокаеого Казад	Bu66pure nancy is crusca in Haxistre -OKs. (c:/inetpub/jivivivroot/SecurityDesk	
			↓ logs ↓ temp ↓ ↓ aspnet_client ↓ ↓ aspnet_client ↓ PerfLogs	2
-	1 элемент Выбран 1 элем	ент: 131 МБ	Program Files Program Files (x86) Program Data	*
			ОК ОТ	мена
			U3Hdk	омительная версия Windows Server 2012 R2 Standard Лицензия Windows действительна в течение 180 дн. Build 9600
🕂 🛃 🖉 🎇 🥎				▲ P ² 10 10 10 ENG 14:33 09.05.2019

Рисунок 19. Выбор пути установки системы.

Корзина Корзина					
	🚨 l 🔁 🚯 = 1	Средства работы с приложениями	distr	X	
	Сойл Главная Поделиться E	Вид Управление	– с х с Поиск: distr	<u>د</u>	
	 № Избранное	Установка — эсеситку/чек, версия н.2.3 bemo утака установка траня установка вите «Установить», чтобы прадоленть, иля «Казаа», если вы к онгрет «Установить», чтобы прадоленить, иля «Казаа», если вы к онгрет и чистика биды установки. получествори: Стумерай (инитект) Бесилтурсак Стумерай (инитект) Бесилтурсак	Vasaep 134 462 KS		
% Установка				2	
B	нт Выбран Тэлемент: 131 МБ		Ознак	Омительная версия Windows Server 2012 R2 Лицензия Windows действительна в течени в а с с с с с с с с с с с с с с с с с с	Standard e 180 дн. uild 9600
🗄 占 🖉 🚊 🔊				• 🖻 🔞 🕲 🌜 ENG 💦	14:33 9.05.2019

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.

Г Корзина						
	👪 l 💽 🚯 🗢 l	Средства работы с приложениями	distr		_ D X	
	Файл Главная Поделиться	я Вид Управление			~ 🕐	
	🛞 💿 🔹 🕯 🕨 🏵	Установка — SecurityDesk, верси	a 1.25 Demo 😑 💷 🗙	🖒 Поиск: distr	Q	
	 ✓ Избранное № Наранное № Нарание мскта № Рабоший стол № Этот компьютер № Этот компьютер € Cers 	Сорональство и политика и п Политика и политика и по	е Мастера установки к к установлена на ваш колтнотер. н, чтобы выйти на програмы	¹ 23мер 134 462 КБ		
_			Завершить			
					2	
	1 элемент Выбран 1 элемент: 1	131 MB				
				Ознако	омительная версия Win Лицензия Windows дей	dows Server 2012 R2 Standard ствительна в течение 180 дн. Build 9600
📫 🛃 📜 🗞					• F	▷ 🔞 😭 🌘 ENG 14:34 09.05.2019

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».

'突	Microsoft SQL Server	r Management Studio (Ад	министратор)		
Файл Правка Вид Сервис Окно Справка					
🖓 • 🖂 • 🎽 📓 🥔 🔔 Создать запрос 🕞 🔧 🚱 🍰 🐇 🖓 🖄 / М 🖉 / О • С • 💭 • С		-	- 12	• I 🗠 🕾 💥 🖬 • 🖕	
Обозреватель объектов 🔹 👎 🐥					
Соединить - 🛃 🕄 🗉 🍸 🛃 📓					
	-l Co	елинение с сервером	x		
and an and a subscription of a subscription of the subscription of					
	Microsoft CO	1 Com/or 2014			
	witcrosoft SQ	L Server 2014			
	Тип сервера:	Komnoheht Database Engine			
	Имя сервера:	WIN2012			
	Проверка подлинности:	Проверка подлинности Window	vs V		
	Имя пользователя:	WIN2012\Administratiop			
	Пароль:				
		Запомнить пароль			
	Continents	Опиена Спозвиа			
	Cocpeterio		Traparioripor 22		
Готово					
					Do 200 (00 c) and 15:15
					 ING 100 100 ENG 09.05.2019

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 SQL Server и Windows» - Рисунок 23.

- 1 ×				
Обозреватель объектов				
Соединить - 🛃 🛃 💷 🍸 🛃 🎿				
WIN2012 (SQL Server 12.0.4100 - WIN20	8			
🖃 🧰 Базы данных	0	Своиства сервера - WIN2012		
Ш Системные сазы данных	Выбор страницы	🕄 Скрипт 👻 🎼 Справка		
	Общие			
н 🦕 Соссина сереро	Процессоры			
🗉 🧰 Управление	Безопасность	Серверная проверка подлинности		
	Соединения	O Проверка подлинности Windows		
	Параметры базы данных	Проверка подлинности SQL Server и Windows		
	Разрешения			
		Аудит входа		
		O Her		
		 Transmission and an annual 		
		• Только неуспешные попытки входа		
		О Только успешные попытки входа		
		 Все попытки входа 		
		Серверная учетная запись-посредник		
		Включить серверную учетную запись-посредник		
	Соединение			
	Сервер:	Tapons.		
	WIN2012	Параметры		
	Соединение:			
	winzuiz\ядминистратор	Включить трассировку аудита C2		
	Соединения	Формировать межбазовую целочку врадения		
	V			
	ход выполнения			
	Готово			
	~45°			
		ОК Отм	ена	
< III >				
Готово				
				▲ 😼 🔞 💬 🈘 ENG 15:17

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 «OK».



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.

ų.	Microso	ft SQL Server Management	Studio (Администратор)		_ 0 ×			
Файл Правка Вид Отладка Сервис Окно Справка								
🗄 🔂 🔹 🖂 🥔 🎒 🤰 Cоздать запрос 🛛 🔒 😘 🏠	メロ語 9-0-5-512	× -	- 20	• 🔍 🕾 🗶 🖬 •	-			
Обозреватель объектов 🔹 д 🗙					_			
Соединить - 🕄 🕄 🔳 🍸 🛃 🔀								
= 6 WIN2012 (SQL Server 12.0.4100 - WIN20								
на Базы данных		Восстановле	ние базы данных - SecurityDB	_				
🛞 🚞 Системные базы данных	Протово							
🗉 🚞 Безопасность	Выберите страници	Courses a 173 Courses						
П Объекты сервера	Общие	Скринт • Ссправка						
н Стравление	🔗 Файлы	Истонник						
· · · · · · · · · · · · · · · · · · ·	🚰 Параметры	O -						
		🔾 База данных:						
		Устройство:	C:\inetpub\wwwroot\SecurityDesk\Docs\Secur	ityDB.bak				
		База данных	SecurityDB		▼			
		Назначение						
			Securit-DR					
		Базаданных	a (a	2010				
		Восстановить в:	Последняя созданная резервная копия (18 ап	временная ц	кала			
		План восстановления —						
		Восстанавливаемые резер	овные наборы данных:					
		Восстановление Имя		Компонент Тип	Сервер			
		Security	DB-Полная База данных Резервное копирование	База данных Полная	LENOVC			
		Conservation and the second						
	Соединение							
	3 WIN2012							
	[WIN2012\Администратор]							
	Contract of Concentration							
	Просмотреть свойства							
	Xee a second							
	ход выполнения							
	О Готово							
		< 111			>			
			Пе	оверка носителя резервной	копии			
			100					
< 111 >			ОК	Отмена Сп	равка			
Готово								
					• Re 印 空 Ch ENG 15:20			
	in X .				09.05.2019			

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 «OK». Выберите базу данных по умолчанию «SecurityDB» и язык по умолчанию «Russian».

<u>k</u>	Micro	osoft SQL Server Management Studio (Адм	инистратор)
Файл Правка Вид Отладка Сервис Окно Справка		- 28	- ST - ST -
Cocquerants deterros ▼ # × Cocquerants 9 2 = 7 2 3 Gotto deterros 1 2 2 = 7 2 3			
🗏 🛅 Базы данных	8	Создание имени входа	X
е ⊒ Системные базы данных ⊛ <mark> </mark> SecurityDB в ⊒ Безопасность	Выбор страницы Общие	🛒 Скрипт 🔻 📳 Справка	
Marea studie A staff, Policy CreatProcessin A staff, Policy CreatProcessin BULTINTOn-subservent Morea studie BULTINTOn-subservent Morea staff, Policy CreatProcessin Morea staff, Po	 Роли сереера Сопоставление опъзватели пользователи Защищаемые объекты Состояние Состояние 	Иня входа: Проверка подлинности Windows Проверка подлинности SQL Server Перопь: Партверхдение пароля: Веверите старый пароль: Старый пароль: Старый пароль: Таребавать соло конснечае действия пароля Задать соло конснечае действия пароля Выборя: "Пользователь" сил. "Воловенны субъект безо Вользование месть: Тальзование месть:	Нали
	<	WIN2012 Вердите умена выбираемых объектов (солология) ЦвегоВ Дополнительно	Размещение Гроверить имена ОК Отмена авсег V то умолчанию V
			d
🗄 🛓 🗷 🚔 🖳			

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.

₩ • • • • • • • • • • •	Micro	osoft SQL Server Management Studio (A	дминистратор)		_ 0 X
Файл Правка вид Отладка Сервис Окно Спј	paska na mil v na na lun u nu u tri u tri uni				
: [] · · [] [] [] [] Cospare sample: [] []					
Обозреватель объектов — Ф ×					
Соединить • 🛃 🛃 🗉 🍸 😰 🍇					
WIN2012 (SQL Server 12.0.4100 - WIN20		Contraction of the second seco			
🗏 🧰 Базы данных		Создание имени входа	L		
	Выбор страняцы	🛒 Скрипт 👻 🚺 Справка			
П Безопасность					
🖃 🧰 Имена входа	Сопоставление пользователя	Имя входа:	SecurityUserDB	Наяти	
A ##MS_PolicyEventProcessing	Защищаемые объекты	Проверка подличности Windows			
A ##MS_PolicyTsqlExecutionL	Состояние	Проверка подлинности SQL Server			
BUILTIN/TIO/IBOBATE/		Damage -		1	
A NT Service\MSSQLSERVER					
A NT SERVICE\SQLWriter		Подтверждение пароля:	•••••		
A NT SERVICE\Winmgmt		Введите старый пароль			
🟯 sa		Старый пароль:			
📇 WIN2012\Администратор		Требовать использование политики па	ролей	the size according to the second	
Поли сервера		Задать срок окончания действия парол	R		
🕀 🧰 Объекты сервера	and a second second	Пользователь должен сменить пароль	при следующем входе	the set of the second second second	
🛞 🧰 Репликация		 Сопоставление с сертификатом 	~		
🛞 🧰 Управление		О Сопоставление с асимметричным ключом	×		
		Сопоставить с учетными данными	×	Добавить	
	< III >	Сопоставленные учетные	Учетные Поставщик		
	Соединение	данные			
	Cepsep: WIN2012				
	Соединение: WIN2012\Администратор				
	💷 Просмотреть свойства				
	соединения				
	Ход выполнения			Удалить	
	Готово	База данных по умолчанию:	SecurityDB ¥		
		Язык по умолчанию:	Russian 🗸 🗸		
			OK	Отмена	
c III >					
Готово					
🗧 占 🛛 📋 🕵					▲ 😼 🗊 🕼 🕼 ENG 17:30 10.05.2019

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.

1 6	Micro	soft SQL Server Managem	ent Studio (Админис	тратор)		- 0 ×
Файл Правка Вид Отладка Сервис Окно Справка	4月19-0-月-日国	• •	- 2	9	- 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	
Обозреватель объектов • • • • × Соединить • • • • • • • • • • • • • • • • • • •						
П Базы данных	H	Создание им	ени входа			
 В Системные базы данных В 3 SecurityDB Безопасность 	Выбор страницы Сбщие Роли сервера	🛒 Скрипт 🔹 🌇 Справка				
🖃 🦳 Имена входа	Сопоставление пользователя	Пользователи, сопоставленные	с этим именем входа:			
 ▲ ++MS_2*Reis/Stellin Rocksmin ▲ +MS_2*Reis/Stellin Rocksmin ▲ BULTINNINOnascerenn ▲ NT Service/MSSGLSRVER ▲ NT Service/SSGLVitter ▲ NT SERVICE/SQLWitter ▲ NT SERVICE/SQLWitter 	Состояние	basa ga+esx master model msdb SecuntyDB tempdb	SecurityUserDB	Cxema no ymonvaniio		
 За № №2012-Администратор № Опи серевоа № Учетные данные № Очетных серевра № Пелликация № Управление 		Учетная запись гостя, вклю	ченная для: SecurityDB		_	
	< ш > Ссединске Серенске ШN2012 Сседински ШN2012 Адинонастратор ☐ <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински</u> <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински</u> <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински</u> <u>Сседински</u> <u>Сседински <u>Сседински</u> <u>Сседински <u>Сседински</u> <u>Сседински <u>Сседински</u> <u>Сседински <u>Сседински</u> <u>Сседински <u>Сседински</u> <u>Сседински <u>Сседински <u>Сседински</u> <u>Сседински <u>Сседински <u>Сседински <u>Сседински</u> <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински</u> <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински <u>Сседински</u></u> <u>Сседински</u> <u>Сседински</u> </u> <u>Сседински</u> <u>Сседински</u> </u> <u>Сседински</u> <u>Сседински</u> </u> <u>Сседински</u> <u>Сседински</u> </u> <u>Сседински</u> </u> <u>Сседински</u> <u>Сседински</u> </u> <u>Сседински</u> </u> <u>С</u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u></u>	Vinercimo e pons Gasta jatietes y espret. Roles, BasicAccess aspret. Roles, ReliAccess aspret. Roles, FellAccess db_accessadimi db_backupperator db_dstareader db_dstareader db_dstareader db_dstareader	ss securityDB	^		
	Готово	☐ db_denydatawrter ✔ db_owner ☐ db_securtyadmin ✔ public		ОК Отмена		
C III D						
- 📥 🛛 🚞 💭 🐫 🖁						No 15:30

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.

6				Диспетче	р служб IIS	5					_ 0 ×
											₩ ≈ 4 @
Файл Режим Справка											
Подключения	🗐 Начальная	страница WIN-SG	3V08K773G								Действия
Начальная страница	Фильтры:	• 🐨 Перейти - 🖓 По	жазать все Сгруппирс	вать по: Облас	ть	• 📰 •					Управление сервером
а тинч завиок//за (инч завиок//за — 20 Пулы приложений а ща сайты а ща SecurityDesk	ASP.NET	٤	R	8.		404	ab	2	•	^	 Перезапустить Запустить Остановить
▷ - Actives ▷ - Administration	Глобализ Ключ .NET машины	Компиляция Параметры Г .NET приложения	Іоставщики Правила авторизац.	Состояние сеанса	Страницы и элементы	Страницы ошибок	Строки подключе	Уровни довер	Электронная почта (SM		Просмотреть пулы приложений Просмотреть сайты
þ bin þ css þ Docs	IIS	æ	H		-	2		A	-	^ ^	Изменить версию .NET Framework Получить новые компоненты веб-платформы
⊳-000 fonts ⊳-000 Images ⊳-000 js	Ведение Документ по журнала умолчанию	Заголовки Кэширова ответов выводимы	Модули Ограниче ISAPI и CG	. Проверка Подлинно	Просмотр каталога	Рабочие процессы	Сертификат ы сервера	Сжатие	Сопостав обработч	Страницы ошибок	😧 Справка
⊳ Templates ⊳ Upload	Типы МІМЕ Фильтрация запросов	Фильтры ISAPI									
	Управление									^	
	Делегиро Общая компонента конфигур	Редактор конфигур									
< III >	Просмотр возможностей	👔 Просмотр содержимо	ro								
Готовность											6
🗧 ⊾ 🛛 📋 🛛	🦻 🚺 🌔										▲ 😼 🔞 🕲 😓 ENG 01.11.2020

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».

Файл Режим Справка							
Подключения	Constant						Действия
S	Сертифика	ты сервера					Импортировать
Чачальная страница ▲ Чачальная страница В Чачальная страни страница В Чачальна В Чачальная страница	Используйте эту функцик	одля запроса и обработки сертифика	тов, которые веб-сервер мож	ет использовать с веб-сі	айтами, где настроено использ	ование SSL.	Создать запрос сертификата Запрос установки сертификатов
- 👔 Пулы приложений	Фильтры:	• 🦉 Перейти - 🦙 Показать в	се Сгруппировать по: Без	группирования	•		Создать сертификат домена
a 😜 SecurityDesk	ИМЯ	Получатель сертификата	Поставщик	дата окончания	хэш сертификата	Аранилище серти	Создать самозаверенный сертификат
 Actives Administration 							Включить автоматическую повторную привязку обновленных сертификатов
in in Gs Gs Gs Gs Gradie	Просмотр величениет						Crysson
Готовность Проводник							6
	ş 🖣 🏉						▲ 😼 🖗 💯 🍁 ENG 16:07 01.11.2020

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.

G j		Диспетчер служб IIS	_ 0 ×
€ () ♥ WIN-SG8V08K773G >			🖼 🖂 🚱 •
Файл Режим Справка			
Подключения	Contuburot	1. 5000000	Действия
🔍 • 🗟 🚈 🕏	Сертификат	ы сервера	Импортировать
Начальная страница	Используйте эту функцию	аля запроса и обработки сертификатов, которые веб-сервер может использовать с веб-сайтами, где настроено использование SSL.	Создать запрос сертификата
- 2 Пулы приложений	Фильтры:	• 🍸 Перейти - 🥁 Показать все Сгруппировать по: Без группирования 🔹	Запрос установки сертификатов
⊿- <u>ії</u> сайты	Имя	Получатель сертификата Поставщик Дата окончания Хэш сертификата Хранилище серти	Создать сертификат домена
 SecurityDesk Actives 		Созвршие самозавелениого селтификата ? Х	Создать самозаверенный сертификат Включить автоматическую повторную привязку
b- bin		создание самозаверенного сертификата	обновленных сертификатов
p-mini css p-mini Docs b-mini fants		Понятное имя	😢 Справка
 b - in impacts b - in products b - in Templetes b - in Uplead 		Усавите лики фийки для вапросе сертификата. Следующие данные могут быть отосланы центру сертификации: Понятое има сертификата: SecurityOest] Выбрать пранилище сертификатов для нового сертификата: Личный v	
		OK Onwere	
2 III 1	Просмотр возможностей	Просмотр содержимого	
Готовность	Cont 1		1 ноября 2020 г. воскресенье
	a 🐘 🗡		- Do PT PT /b FMC 16:17
			- No 10 18 (0 ENG 01.11.2020

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.

8)	Диспетчер служб IIS	_ 0 ×
	айты → SecurityDesk →	😐 🔤 🖓 i 😢 •
Organical Construction Organic Construction Organiconstruction Organical Construction	Диспениер служб IIS айты > SecurityDesk >	Constant and a c
5 11 5	Радатор: жонфитур:. Просмотр томкожноства одержимиете	
Готовность		6
	🥦 📢 🕼 🕒	▲ 16:29 ▲ 16:29 ▲ ENG 01.11.2020

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».

Предыдущи	е версии	Настройка		Pa	2 KE						
Общие	Доступ	Безопасно		Pa	14 KF		nu "Hala	ad"	x		
Имя объекта: С: Группы или польз	\inetpub\www.root\S юватели:	ecurityDesk\Upload	Безопас	ность	шения д	ля груп	пы оріс	au			
СОЗДАТЕЛЬ СИСТЕМА	-ВЛАДЕЛЕЦ		Имп.об	LAYTS	С.\inetoub\w Выбо	р: "Пол	curityDeck\) b30BaTeJ	и" или "	Группь	"Ic	
К Администрат Пользовател <	оры (WIN2012\Адм MUN2012\Пользе III	инистраторы)	Выбе	рите тиг	объекта:				1		
Чтобы изменить ; нажмите кнопку "	разрешения, Изменить",	Измен	Всле	њзовате едующем	ли, труппы	ы или Вс	троенные с	уоъекты ое	зопасне	Типы обт	Бектов
Разрешения для г "СОЗДАТЕЛЬ-ВЛ	руппы АДЕЛЕЦ''	Разрешить Запр	WIN	2012						Размеш	цение
Полный доступ			Введ	ите <u>и</u> мен	на выбираем	ых объек	гов (пример	ы):		la.	
Изменение Чтение и выпол	пнение		IIS A	ppPool\S	SecurityDesk					Проверит	љ имен
Список содерж Чтение Запись	имого папки		Дог	толнител	ьно				ОК		тмена
Чтобы задать осо параметры, нажм "Дополнительно"	бые разрешения из ите кнопку	и Дополни	чтен Спис Чтен	ие и вып ок содер ие	олнение жимого пап	ки	N N N		~		
	ОК	Отмена Пр									

Рисунок 37. Настройка доступа пула приложения.

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

000011001100110				
Имя объекта	C:\inetpub\www.roo	t\SecurityDesk\I	Jpload	
Группы или п	ользователи:			
용 Админис	траторы (WIN2012\/4	дминистраторы	4)	^
용 Пользов	атели (WIN2012\Пол	ьзователи)		
IIS_IUSR	S (WIN2012\IIS_IUS	RS)		=
Converter C	staller			_
Security L	esk		1 12	~
1				
<	ш		>	-
<		Добавить	Удалит	2
Разрешения и	ш 1ЛЯ ГОУППЫ	Добавить	Удалит	>
< Разрешения л "SecurityDesk	ш лля группы	Добавить]	Удалит Запрети	ъ
Paspeшeния / "SecurityDesk Полный дол	ш иля группы "	Добавить [Разрешить	Удалит Запрети	ть
Разрешения и "SecurityDeskПолный дог Изменение	ш иля группы ступ	Добавить [Разрешить 	Удалит Запрети	Б
Разрешения / "SecurityDeskПолный доИзменениеЧтение и в	ш лля группы этуп ыполнение	Добавить Г Разрешить Г	Удалит Запрети	ь ть П
Разрешения /"SecurityDeskПолный долИзменениеЧтение и выСписок сод	ш аля группы этуп ыполнение ержимого папки	Добавить	Удалитт Запрети	ъ
Разрешения // "SecurityDeskПолный доИзменениеЧтение и віСписок содЧтение	ш для группы " ступ ыполнение ержимого папки	Добавить	Удалит Запрети	ь ть < Ш

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.

	1			
Файл Режим Справка				
Сирекка Сирекка Соказаная страница • Пулы приложений • МИК202 (СИКО212-Админис • МИК202 (СИКО212-Админис • МИК202 сайты	Typbi приложен Tracepanua nosenaet просматр забочна процесом, содержито, Фильтры: MRT v20 Classic MRT v20 Classic MRT v45 Classic Classic NRT AppPool DefaultAppPool DefaultAppPool SecurityDesk	ий шиать и изменять список пулов при и или несколько приложений и № Перейли • Состоль Версия ср. Работа v2.0 Работа v2.0 Работа v4.0 Работа v4.0 Работа v4.0 Работа v4.0	ложений, существующих на сервере. Кахдый пул приложений связан с беспечивает изоляцию приложений друг от друга. "пултикровать по: Без группирования "Ремм упра Хостоверение Приложения Сероения АројсаtionPoold0 АројсаtionPoold0 АројсаtionPoold0 АројсаtionPooldentity Исполняемый файл Удостоверение АројсаtionPooldentity © Собав учетная записы: АројсаtionPooldentity © Отменая Исполняемый файл Удостоверение АројсаtionPooldentity © Отменая учетная записы: Исполняемый файл Удостоверение СК. Отмена Приложения Качетие СК. Отмена Приложения властве сврооней учетной записа, а именою сах удостоверение пула приложений (рекоменаучетной записа, а именою сах удостоверения пула приложений (рекоменаучетной), ствеой службы, л	Ск. Стмена Ск. Стмена Ск. Стмена Ск. Стмена Ск. Стмена

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.

l 🔁 🚺 = 1				Sec	curityDesk			0 ×
Файл Главная По,	делиться Вид							~
🔄 🔄 🔹 🕇 📕 भ अ	тот компьютер 🕨 Локальный диск (і	C:) ▶ inetpub ▶ wwwroot ▶ S	ecurityDesk 🕨			~ C	Поиск: SecurityDesk	م
🔆 Избранное	Имя	Дата изменения	Тип		Размер			
🚺 Загрузки	fonts	09.05.2019 15:11	Папка с фа	йлам	и			
🔄 Недавние места	Images	09.05.2019 15:11	Папка с фа	йлам	M.			
Рабочий стол	is is	09.05.2019 15:11	Папка с фа	йлам	И			
	Templates	09.05.2019 15:11	Папка с фа	йлам	ы			
📜 Этот компьютер	Upload	09.05.2019 15:11	Папка с фа	йлам	и			
	Default.aspx	29.03.2019 1:08	ASP.NET Ser	rver P	a 16 KE			
📬 Сеть	ErrorPage.aspx	28.02.2019 20:20	ASP.NET Se	rver P	а 2 КБ			
	ErrorSecurity.aspx	28.02.2019 20:20	ASP.NET Ser	ver P	2 КБ			
	S favicon.ico	09.03.2019 13:38	Файл "ІСО"		2 KE			
	GetDocumentHandler.ashx	17.06.2017 15:45	ASP.NET Ge	neric	1 KE			
	Incident.aspx	03.04.2019 23:02	ASP.NET Se	rver P	а 33 КБ			
	Incidents.aspx	04.02.2019 22:29	ASP.NET Ser	rver P	а 7 КБ			
	IncidentView.aspx	18.04.2019 0:24	ASP.NET Se	iver P	25 КБ			
	🛅 Login.aspx	28.02.2019 20:20	ASP.NET Ser	rver P	а 2 КБ			
	E Reports.aspx	Открыть		er P	Pa 51 KE			
	🛅 Site.Master	Изменить		ter	Р 11 КБ			
	Task.aspx	Открыть с помощью	•	00	Microsoft Visual Studio 2010			
	🛅 Tasks.aspx	Восстановить прежнюю в	рсию		Блокнот			
	TaskView.aspx	Отправить	•		Выбрать программу			
	TestForm.aspx	Вырезать		Terr				
	unins000.dat	Копировать			25 Kb			
	Contraction of the second	Canada and w		Ē.,	1 210 KB			
	UploadHandler.asnx	Создать ярлык		eric	IND SVE			
	Vulnerabilities.aspx	Удалить		er P	a 0 ND			
	Wulnershilth diaw serve	Переименовать			20 KB			
	web config	Свойства		IG"	7 KE			
Desusarias 22 Pulinau	1 a nouver 6 02 KE	10.03.2019 10:21	Wann CON	10	/ ND			Ree I
элементов: 52 Выбран	Т ЭЛЕМЕНТ: 0,95 ND							11.40
							🔺 🗄 🔁 👍 РУС	11:48

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 />

<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear />
<clear //
<

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.

cconnectionStrings>
cclear/s
cclear/s
cadd name="tocalSglServer" connectionString="data source=.\SQLEXPRESS;Integrated Security=SSPI;AttachDBFilename=[DataDirectory|aspnetdb.mdf;User Instance=true"
providerName="System_Stata_SglCient" />
cadd name="bataDirectory" connectionString=" roviderName="" />
cadd name="bataDirectory" connectionString=" roviderName=" />
cadd rame="bataDirectory" connectionString=" roviderName=" /

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.

configurations	
<appset (figs)<="" td=""><td></td></appset>	
C:\TempImageFiles\;	
<add key="ChartImageHandler" value="storage=file;timeout=20;dir=~/Upload/;"></add>	
<add key="ValidationSettings:UnobtrusiveValidationMode" value="None"></add>	
<add key="<u>clientKey" value="11111111-AAAA-BBBB-CCCC-DDDDDDDDDD"></add>	
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.



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.

🔉 l 💽 🚺 🕈 l			t	vin		-	0 X
Файл Главная Г	Тоделиться Вид				1.		~ 0
⊕ ⊚ • ↑ 🎩 •	Этот компьютер 🕨 Локальный ди	іск (C:) 🕨 inetpub 🕨 и	wwwroot + SecurityDesk + bin		 С Поиска 	bin	Q
🔆 Избранное	Имя	Дата	изменения Тип	Размер			
〕 Загрузки	🕲 l 🗋 = l			Службы		-	
🔛 Недавние места	Файл Главная Подели	Файл Действие В	Зид Справка				
Рабочий стол	🕒 🕘 – ↑ 🔁 🕨 Пане.						
🌉 Этот компьютер		🎑 Службы (локалы	Службы (локальные)	-			
	Загрузки		MailService	Имя	Описание	Состояние	Тип за 🔨
🙀 Сеть	П Недавние места			ASP.NET State Service	Provides support for out-of-process sessi		Вручн
	Рабочий стол		Остановить службу	G DHCP-клиент	Регистрирует и обновляет IP-адреса и	Выполняется	Автом -
	-			ок UNS-клиент	Служба DINS-клиента (dnscacne) кэши	выполняется	ABTOM-
	🏴 Этот компьютер		Описание	MailService	SecurityDesk mail service	Выполняется	Автом
			SecurityDesk mail service	NetTcpPortSharing	Предоставляет возможность совместн		Отклю
	🗣 Сеть			Relig and Play	Позволяет компьютеру распознавать и	Выполняется	Вручну
	^			SMP дисковых пространств (Майкрософт)	Служба узла для поставщика управлен		Вручн
				SQL Full-text Filter Daemon Launcher (MSS	Служба запустит процесс управляюще	Выполняется	Вручн
				SQL Server (MSSQLSERVER)	Осуществляет хранение и обработку д	Выполняется	Автом
				SQL Server, службы синхронизации контр	. Предоставляет интерфейс для резервн	Выполняется	Автом
				G Superfetch	Поддерживает и улучшает производит		Вручн
				WITCohod Jac Canica	Manages VM runtime information, time	Выполняется	ABTOM
				Windows Audio	SecurityDesk workFlow Scheduler Service		Вручн
				Windows Driver Foundation - User-mode D	Создает процессы драйверов пользова		Вручн
				Arent SQL Server (MSSQLSERVER)	Выполняет задания, наблюдает за SQL		Отклю
				🖓 Агент защиты сетевого доступа	Агент службы защиты доступа к сети с		Вручну
				🕞 Агент политики IPsec	Безопасность протокола IP (IPsec) подд		Вручн
				🏟 Адаптер производительности WMI	Предоставляет сведения библиотеки п		Вручн
				G Брандмауэр Windows	Брандмауэр Windows помогает предот	Выполняется	ABTOM Y
		<	Расширенный (Стандартный /				
200100000000000000000000000000000000000	Элементов: 24 Выбран 1 эл						
SHEMICIDE 22							20-27
	/ 🔚 🔌 🖊				• R D	🔁 🌆 ENG	11.05.2019

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.

G.		Слу	ужбы	= 🗆 X
Файл Действие	Вид Справка			
4-41000 00 0				
🥋 Службы (локалы	🔍 Службы (локальные)			
	MailService	Имя	Описание Состояние Тип запуска Вход от имени	^
		ASP.NET State Service	Provides s Вручную Сетевая служба	
	Запустить службу	🖏 DHCP-клиент	Регистрир Выполняется Автоматиче Локальная служба	
		🔅 DNS-клиент	Служба D Выполняется Автоматиче Сетевая служба	
	Описание:	🌼 KtmRm для координатора распределенных транзакц	. Координи Вручную (ак Сетевая служба	
	SecurityDesk mail service	🐫 MailService	SecurityDe Автоматиче\UserDB	=
		🖏 NetTcpPortSharing	Преда Свойства: MailSenrice (Локальный компьютер) 🗙	
		🔍 Plug and Play	Позво	
		SMP дисковых пространств (Майкрософт)	Служе Общие Вход в систему Восстановление Зависимости	
		SQL Full-text Filter Daemon Launcher (MSSQLSERVER)	Служе Вход в систему:	
		SQL Server (MSSQLSERVER)	Осущи	
		😘 SQL Server, службы синхронизации контроля версий	Предо	
		🔍 Superfetch	Подде	
		VirtualBox Guest Additions Service	Manag 💿 С учетной записью: .\UserDB Обзор	
		S WFSchedulerService	Securit	
		😪 Windows Audio	Управ. Пароль.	
		Windows Driver Foundation - User-mode Driver Frame	Создан Подтверждение:	
		Arent SQL Server (MSSQLSERVER)	Buno/	
		🥋 Агент защиты сетевого доступа	Агент	
		🧠 Агент политики IPsec	Beson:	x
		🖓 Адаптер производительности WMI	Предо Выбор: Пользователь	
		😘 Брандмауэр Windows	Бранд Выберите тип объекта:	
		😘 Браузер компьютеров	Обслу "Пользователь" или "Встровный сибъект безопасности"	
		😘 Брокер системных событий	Коорд	
		👒 Быстрая проверка	Прове В следующем месте:	_
		👒 Виртуальный диск	Предо WIN2012 Размещение	
		😪 Вспомогательная служба IP	Обесп Ввелите имена выбираемых объектов (примеры):	
		Вторичный вход в систему		at l
		🧠 Готовность приложений	Подго	4
		😪 Диспетчер автоматических подключений удаленног	. Созда	
		😪 Диспетчер локальных сеансов	Основ	
		Диспетчер настройки устройств	Включени ОК Отмена	
		😪 Диспетчер печати	Эта служб Вы	
		🤤 Диспетчер подключений Windows	Принимае Выполняется Автоматиче Локальная служба	
		Диспетчер подключений удаленного доступа	Управляет Вручную Локальная система	
		😪 Диспетчер учетных данных	Обеспечи Вручную Локальная система	
		Диспетчер учетных записей безопасности	Запуск это Выполняется Автоматиче Локальная система	
		🗤 Доступ к HID-устройствам	Активируе Вручную (ак Локальная система	
		🦋 Журнал событий Windows	Эта служб Выполняется Автоматиче Локальная служба	~
< III >	Расширенный (Стандартный /	THE XUMPTER IN ORDER HER REALIZED AND REALIZED OF THE	т покрази: Воллыми Покальвая сложба	
	(

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 конфигурационном файле в «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 «-pef» на «-pdf».
- 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 бизнеспроцессов 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:

 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 бизнеспроцессов (смотри инструкцию по настройке сервера бизнес-процессов).

Наименование:	Тип подключения:
sdservice	Обобщенное подключение 🗸
	Таймаут подключения (сек.):
Соединение активно: 🗹	10
Адрес сервера:	Порт:
Имя сервера или ІР-адрес	8000
Пользователь:	
sdservice	
Пароль:	
•••••	
Описание:	
sd wexflow	
	,

Рисунок 47. Создание обобщенного подключения.

 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.

SecurityDesk ФГлавная & Мониторинг	• ©Регистрация • ШАктивы • ©Аналитика • Ф _{Алмин}				ментация Попьзователь: Ladmin	
Общие Электронная почта Подключен	ие к внешним источникам Настройка импорта активов					
Общие настройки систе	МЫ					
Наименование системы:	URL-путь к приложению:	Сервер бизнес- процессов	Режим отладки сервера бизнес-	URL-путь к серверу бизнес-процессов:	Имя подключения:	
SecurityDesk	http://localhost.30092	0		http://localhost:8000	wexflowservice	

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.

SecurityDesk	
Вход в систему	
домен:	
Локальная аутентификация	~
Погин:	
Логин	
Тароль:	
Пародь	

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.

SecurityDe	sk ©Главная	≜ Мониторинг -	⊘Регистрация -	₩Активы -	⊙Аналитика •	Адлянистрирование -			j e j	Јокументация Попьзо	затель: 🌡 admin 🔂 Вых
У Инциденты Всего активных: 0 Зареть прородиные: 0 в работе: 0 выполнетвые: 0		0 0 0 0	Уязвил Всего акти Зарегистрирс В работе: Выполненный	ЮСТИ ВНЫХ: ванные: 2	Настройки и можноринг работы системы Основные настройки Обработка входящих сообщений Редактор сценариев Редактор сценариев Дополнительные параметры Списки параметров Журнал работы	адачи о активных: истрированные: оте: пненные:	1 1 0 0	На Акти Всего и Компьют Персона	ИВЫ имеется: еры: п:	8 5 3	
	Инциденты за		азарегистрирс	Управление доступом Управление пользователями Управление уровнем доступа	я пользователя " там отсутствует	С полным доступо	м"				
				Уязвимости	а зарегистриро	Управление пользовательскими ролями Управление аналитическими панелями	я пользователя "	С полным доступо	м"		
Номер	Наименование				Категор	Управление аналитическими отчетами Справочники	Состояние	Вектор атаки	Регистратор	Дата регистрации	Дата обнаружения
2	XSPIDER ID: 1057	Стандартный парс	иль пользователя S'	YSDBA	Информа	Подразделений Лолжностей	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
3	XSPIDER ID:7034	Некорректная цеп	очка сертификатов		Информ	Типов компьютеров	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
4	XSPIDER ID:1024	Анонимный достуг	1		Информ	Категорий безопасности	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
5	XSPIDER ID: 1079	Учетная запись			Информа	Типов качественной оценки ущерба	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	1 <mark>3-12-2019 14</mark> :41
6	XSPIDER ID:1119	Разглашение инфо	ормации		Информа	документация Инструкция администратора	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
7	XSPIDER ID:1147	Поиск пользовател	тей		Информа	Нормативные документы Хранилище файлов	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41

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.

аименование си	стемы:	URL-путь к прило	жению:	Включить взаимо	одействие с сервером	Режим отладки взаимодействия с	URL-путь к серверу бизнес-процессов:	Имя подключения:	
SecurityDesk		http://127.0.0.1:80	080	бизнес-процессо	B:	сервером оизнес-процессов:	http://127.0.0.1:8000	wexflowservice	
	HOME HEUTED	изавимости за	уязвимостей	задачи за	задач на странице:				
нциденты за	инцидентов	(munit):	US OTRAUMUA!		CIDONNIUC.				
нциденты за аней): 20	инцидентов на странице: 10	(дней): 20	на странице:	20	10				

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.

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

Таблица 1. Основные настройки – вкладка «Общие».

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

	дключение к внешним	источникам настройка импорта активо	интеграция с RuSIEM				
астройка отправкі	и сообщени	ий через сервер эле	ктронной почты по г	протоколу SMTP			
Сервер отправки сообщений:	Порт:	Имя пользователя:	Пароль:	Использовать		Отправить тестовое письмо:	
smtp.test.ru	25	test@test.ru			Проверить	Введите почтовый адрес для отправки	Отправить
ервер приема сообщений:	Порт:	Имя пользователя:	Пароль:	Использовать			
Зервер приема сообщений: pop.test.ru	Порт: 995	Имя пользователя: test@test.ru	Пароль:	Использовать SSL:	Проверить		
Сервер приема сообщений: pop.test.ru	Порт: 995	Имя пользователя: test@test.ru	Пароль:	Использовать SSL: M	Проверить		
Сервер приема сообщений: pop.test.ru ассылка уведомле	порт: 995 ЭНИЙ ПО ЭЛЕ	Имя пользователя: test@test.ru	Пароль:	Kenon⊾somat⊾ SSL: ⊄	Проверить		
Сервер приема сообщений: popitestru ассылка уведомле	порт: 995 РНИЙ ПО ЭЛЕ	имя пользователя: tesi@test.ru	Пароль:	Использовать 58L: 2	Проверить		
ереер приема сообщений: pop test ru ассылка уведомле ведомлять о экополенных (часов): с рассыллюй в	перт: 995 ЭНИЙ ПО ЭЛС	имя пользователя:	Параль:	Kononadatu SSL: C	Проверить		

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.

Та	аблица 2.	Основные	настройки –	вклад	дка «Элек	гронная почта».	,
							_

Поле	Пояснение
	Время, за которое Система будет напоминать
	пользователям о неисполненных задачах,
уведомлять о неисполненных за	инцидентах или не закрытых уязвимостях.
	При установленном значении «0» Система не будет
	осуществлять рассылку.
	Время рассылки напоминаний пользователям о
с рассылкой в:	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 АРІ.

ityDesk ФГлавная ≜Мониторинг⊸ ⊘Регис	трация • 🖽 Активы • ООтчетность ФАдминистрирование •		¢≢Документация	Пользователь: 👤 admin 🕞 В
ие Электронная почта Подключение к внешним	источникам Настройка импорта активов			
аключение к внешним исто	чникам			
оздать Изменить Удалить Проверить				
енование	Тип подключения	Использовать для аутентификации	Описание	Соединение активно
PA	LDAP FreeIPA	2	FreeIPA connect	2

Рисунок 53. Настройка внешних источников.

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

SecurityDesk	⊘Главная ≜Мони		трация • 🛛 📰 Активы •			Пользователь: 💄 admin	
общие элек Для наст Список дос	пронная почта Под РОЙКИ ИМПО ТУПНЫХ ПОДКЛН	ключение к внешним рта актив очений:	источникам Настройка ов выберите	а импорта активов требуемое подк Общие Персонал	илючение из списка Компьютеры		
Наименование	Тип подключения	Соединение активно	Автоматический импорт активов включен	Общие настройк	и импорта активов		
FreeIPA	LDAP FreeIPA	8		Влончить загозатический импорт активов:⊡	Bianonama awapter xaxatae (accos): 0		
Сохранить							

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.

SecurityD	esk ФГлавная	Мониторинг -	ØРегистрация -	⊞ Активы +	ØАналитика -	ФАдолинистрирование -	-		হে,	Документация Пользов	saтепь: 💄admin 🕻 С+Выхо;
 Унциденты Всего активных: О здети: продовже: в работе: В ваботе: В ваботе: В ваботе: О 		0 0 0 0	УЯЗВИМ Всего акти Зарегистриро В работе: Выполненный	IOCTU BHUX: cannue: ::	Настройки и измитерние работы системы Основные настройки Обработа воходицик сообщений Редактор сценарике Редактор сценарике Дополнительные параметры Списко параметров Журнап работы	адачи о активных: истрированные: оте: пненные:	1 1 0 0	На Акти Всего Компьют Персона	ИВЫ имеется: repы: in:	8 5 3	
				Инциденть	зарегистриро	Управление доступом Управление пользователями	я пользователя "	С полным доступом	e"		
						Управление уровнем доступа	там отсутствует				
				Уязвимости	зарегистриро	Управление пользовательскими ролями Управление аналитическими панелями	я пользователя '	С полным доступо	a"		
Номер	Наименование				Категори	Управление аналитическими отчетами Справочники	Состояние	Вектор атаки	Регистратор	Дата регистрации	Дата обнаружения
2	XSPIDER ID: 105	7 Стандартный пар	оль пользователя S1	/SDBA	Информа	Подразделений Должностей	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
3	XSPIDER ID:703	4 Некорректная цег	почка сертификатов		Информа	Типов компьютеров	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
4	XSPIDER ID:102	4 Анонимный досту	n		Информа	Категорий безопасности	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
5	XSPIDER ID:107	9 Учетная запись			Информа	Типов качественной оценки ущеров	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
6	XSPIDER ID:111	9 Разглашение инф	ормации		Информа	Инструкция администратора	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
7	XSPIDER ID:114	7 Поиск пользовате	лей		Информа	Нормативные документы Хранилище файлов	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41

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.

иинистрирование справочника подразделений	
Kalanina Hammana Yazamana	
inflatforenee	
- Внешиние контранеты ь 000 "Закупка"	
▶ 000 Tesepa2 MRoCropificrans ▶ Person-the congraduatewee Morea	
 Ремонтное подразделение Навосийциск Ремонтное подразделение Савит-Петорбург 	
b Celarichem dynitrian (vrl.) - Crinag Moreas - Kylsiwia - Crinag Moreas - Kylsiwia	
y Qurnian Boponex b Qurnian Estroponétypr Volman Manan Manan Manan	
ο Φυντικαι ή Τουργογία Ο Φυντικαι ή Τουργογία Ο Φυντικαι ή Τουργογία αυτοφεί για το τουργία το τουργία το τουργία το τουργία το τουργία του τουργία του τουργ	
ի Փилиан Роспон-ա-Дону - Φилиан Самиара - Φилиан Самиан Пепевбияг	
b Ovrnan Zašapostx b Ovrnan Henrismex	
ρ Φνήκατη «γιτα φ Φνηκικα Αροοπαστι» L. Центральный απαίρατ	

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.

Администрирование справочника типов качественной оценки ущерба

Добавить И	Ізменить Удалить	
Типы качести	энной оценки ущерба:	
Выбор	Номер	Наименование типа
Выбор	1	Ущерб коммерческим интересам партнеров и третык лиц
Выбор	2	Санкции со стороны правоокранительных и регулирующих органов (штрафы, административная, уголовная ответственность)
Выбор	3	Ущерб коммерческим интересам организации
Выбор	4	бинансовые потери
Выбор	5	Ущерб репутации организации
Выбор	6	Дезорганизация деятельности, ухудшение морального климата в коллектиев, снижение производительности труда

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.

SecurityDesk ФГлавная Амониторинг• @Регистрация• ШАктивы• ФАналитика•				ФАдминистрирование -				🕫 Дохументация Пользователь: 💄 admin 🕻 🕒 Выхо			
 Инциденты Вего активных: заропестриованные в работе: Вилотехники: 		10 10 0 0	Уязвимости Всего активных: зврегистроровные: в работе выполнетные:		Настройки и монитории работы системы Основные настройки Обработка входящих сообщений Редактор сценариев Редактор сценариев Дополнительные параметры Списки параметров Редактор сием рабоних процедур	наначение вдачи то активных: истрированные: оте: пненные:	на вас задржи 22 0 0	На Активы Всего имеется: Комплатеры Персонат:		1) 7 5	2
Инциденты зарегистрир					Журнал работы Управление доступом Управление пользователями	ля пользователя "С полным доступом"					
				ия							
Уязвимости зарегистри				Управление уровнем доступа Управление пользовательскими ролями Управление аналитическими панелями	пя пользователя "С полным доступом"						
				Управление аналитическими отчетами	аравление аналитическими отчетами ия						
Задачи зарегистриров					Справочники Подразделений Поличностий	пользователя "С полным доступом"					
Номер	Наименование		Категория	Тип зад	Типов компьютеров	Подразделение	Исполнитель	Дата регистрации	Дата начала испо	Срок исполнен	кия
167	По задаче по регистрации		Информационная	я Внепла	Операционных систем Категорий безопасности Тилов качественной оценки ущерба		admin	26-06-2022 11:12	26-06-2022 11:12	28-06-2022 11:1	2
166	test tats		Информационная	я Планов		Рога и копыта	admin	26-06-2022 11:12	26-06-2022 11:12	26-06-2022 11:1	2
160	По задаче по регистрации		Информационная	я Внепла			admin	25-06-2022 16:46	25-06-2022 16:46	27-06-2022 16:4	6
Страниц	а 1 из 2 (Всего элементов: 5) Предыду	ущая 1 2 (Следующая		Документация Инструкция администратора Нормативные документы Хранилище файлов						

Версия для внутреннего некоммерческого использо Текущая дата: 26.06.2022 22:49:34 Автоматизированная система управления безопасностью SecurityDesk. Эсе поава защищены Велсия 1.35

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.
Secu	rityDesk Фглавная Фмониторин	Header				×	жумент	ация Пользователь	Ladmin CoBasson
+	Зарегистрированные Уязвимости	Выполнить Создать задачу Редактировать	Создать копию Удалить	Перезапустить - 🚔 Отчет	1				
8	едите текст для поиска уязвимостей	Основная информация Дополнительные пара	метры Инциденты Задач	по текущей рабочей процедур	енения				
		Категория безопасности:	Уровень уязвимости:	по новой активной рабочей пр	юцедуре ние:				
		Информационная	Высокий		В работе	4			
Houan	Изиманование	Вектор атаки:			Владелец:		a la		
	T	Удаленная			iuser	1	-	T	T
	4 Tect II	Дата обнаружения:	Дата регистрации:		Дата завершения:		14.44	12 12 2021 15:14:00	12 12 2021 15:15:32
	3 XSPIDER ID: 184168 Использование по	03-04-2019 17:59	12-12-2021 14:40	=		≡	40:24	03.04.2019 17:59:36	
	1 XSPIDER ID:8183 Выполнение произ	CVE:		CWE:			40:14	03.04.2019 17:59:36	
	CVE-2015-0231								
		Описание:							
Cinicower Microsobasiwe nonce coordiocqueres 8 gyneure process, nested, data s existandardivar, unsertalizer s PHP notaconer tranyouunenewsaw, gencretoreure y panews, benchmen spokesmenuel rog (pm notecup chequanelo dopumposawero buscea unsentate; spinegaujers / terespectrine) događorne operatoreuro en transverse province provincence en electropumposawero buscea unsentate; spinegaujers / terespectrine) događorne operatoreuro electropumposawero buscea unsentate; spinegaujers / terespectrine) događorne operatoreu electropumposawero buscea unsentate; spinegaujers / terespectrine) događorne operatoreu electropumposawero buscea unsentate; spinegaujers / terespectrine) događorne operatoreu electropumposawero programa / terespectrine) događorne operatoreu electropumposawero programa, constericitajouje vicinitarije programa / terespectrine) događorne operatoreu electropumposawero programa, constericitajouje vicinitarije programa / terespectrine) događorne operatoreu electropumposawero programa / terespectropumposawero programa / terespectropumposawero programa / terespectropumposawero programa / terespectropumposawero / terespec									
		Результат обработки:							
		Описание отсутствует							
Стран	ица 1 из 1 (Всего элементов: 3) Предыд					11		Элементов на стра	нице: 20 🔹
Верси Текущ	а для внутреннего некоммерческого испол ая дата: 26.06.2022 23:25:33		_	_	Все права защищены. Верс	AR 1.35 a2	ения б	езопасностью Securit	yDesk.

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.

-			-								
SecurityDe		ф Мониторинг ~		Ш Активы -		Администрирование -					атель: 💄 admin 🕞 Выхос
У Инци Всего ал Зарегистр В работе: Выполнен	Уинциденты // Уязвимост Всего активных: 0 зарект: просвязен: 0 врайле: 0 виколеенные: 0			ИОСТИ ІВНЫХ: разільна: е:	Настройки и комперии работы системы Основные настройки Обработка входящих сообщений Редактор сценариев Редактор сценариев Дополнительные параметры Дополнительные параметры Списки параметров Журнал работы	адачи то активных: истрированные: оте: пненные:	1 1 0 0	₩ Акт Всего Компью Персона	₩АКТИВЫ Всего имеется: Конколтри Персона:		
	Инциденты зар			і зарегистриро	Управление доступом Управление пользователями Управление уровнем доступа	я пользователя " там отсутствует	С полным доступом	л''			
				Уязвимости	и зарегистриро	управление пользовательскими ролями Управление аналитическими панелями	я пользователя "	С полным доступо	и"		
Номер	Наименование				Категор	Управление аналитическими отчетами Справочники	Состояние	Вектор атаки	Регистратор	Дата регистрации	Дата обнаружения
2	XSPIDER ID: 1057	Стандартный парс	оль пользователя SY	SDBA	Информ	Подразделений Лопжностей	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
3	XSPIDER ID:7034	Некорректная цеп	очка сертификатов		Информ	Типов компьютеров	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
4	XSPIDER ID:1024	Анонимный достуг	1		Информ	Категорий безопасности	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
5	XSPIDER ID:1079	Учетная запись			Информ	Типов качественной оценки ущерба	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
6	XSPIDER ID:1119	Разглашение инфо	ормации		Информ	инструкция администратора	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
7	XSPIDER ID:1147	Поиск пользовател	тей		Информ	Нормативные документы Хранилище файлов	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41

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.

SecurityDesk	🔊 павная 🛔 Мониторі	ihr• ⊘Pe	егистрация +	Ш Активы -	ØАналитика÷	Ф Администрирование →			<i>1</i> €Документ	ация Пользователь: 👤 admin	С•Вылюд
Показать пользи Создать Добав	ователей имеющих р ить Изменить Раз	юль: Все	Удалить	~							
Пользователь	Полное имя	Email	Дополнитель	ная информ	ция		Последняя дата входа	Дата смены пароля	Заблокирован	Внешняя аутентификация	
admin	Имя не указано		Главный поль:	зователь сист	емы, пароль по ум	лчанию 123456	14.07.2024 14:34:06	11.04.2017 20:06:45			

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.

Логин	
Логин	
Пароль	
Пароль	
Повторите пароль	
Пароль	
E-mail	
E-mail	
Полное имя	
Фамиля Имя Отчество	
Категория безопасности по умолчанию:	
Информационная	~
Подразделение по умолчанию:	
	~
Дополнительная информация	

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.

ж учетных записей:						
імя подключения:		Фильтр поиска пользова	телей:			
FreeIPA	~	uld=*			Поиск	Q. Загрузить Вернуться
	Логин	Фамилия	Имя	Отчество	Email	Дополнительная информация
Создать	admin	Administrator				
Создать	valentin	Алексеев	Валентин		valentin@ipa.example.org	
Создать	gedroyts	Гедройц	Дмитрий		gedroyts@ipa.example.org	
Создать	kalininms	Калинин	Михаил Сергеевич		kalininms@ipa.example.org	
Создать	mininds	Минин	Денис Степанович		mininds@ipa.example.org	

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.

SecurityDe	sk 👁Главная 🐥 Мониторинг		• 🗮 Активы •		Администрирование -					атель 💄 admin 🛛 🔂 выхор
У Инці Всего а Зарегистр В работе: Выполнен	УИНЦИДЕНТЫ Всего активных: зарикт просавинае: вылотиченике: вылотиченике: выполненике: выпо				Настройни и мониторни работы системы. Основные настройки Обработка входящих сообщений Редактор синариев Редактор шаблонов Дополнительные парамятры Слиски параметров Журнал работы	адачи ю активных: истрированные: оте: пнеяные:	1ВЫ імеется: пры: п;	8 5 3		
			Инциденты	зарегистрир	Управление доступом Управление пользователями Управление уровнем доступа	я пользователя " там отсутствует	С полным доступом			
			Уязвимости	зарегистрир	Управление пользовательскими ролями Управление аналитическими панелями	я пользователя "	С полным доступом			
Номер	Наименование			Категор	Управление аналитическими отчетами Споавочники	Состояние	Вектор атаки	Регистратор	Дата регистрации	Дата обнаружения
2	XSPIDER ID: 1057 Стандартный па	роль пользователя \$	SYSDBA	Информ	Подразделений Допжностей	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
3	XSPIDER ID:7034 Некорректная це	епочка сертификато	8	Информ	Типов компьютеров	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
4	XSPIDER ID: 1024 Анонимный дост	yn		Информ	Категорий безопасности	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
5	XSPIDER ID: 1079 Учетная запись			Информ	Типов качественной оценки ущерба	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
6	XSPIDER ID:1119 Разглашение ини	формации		Информ	инструкция администратора	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
7	XSPIDER ID: 1147 Поиск пользоват	елей		Информ	Нормативные документы Хранилище файлов	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41

Рисунок 65. Управление уровнем доступа пользователей в Системе.

В Системе присутствуют 4 неизменяемые системные роли:

- <u>Пользователь</u> 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.
- <u>Менеджер активов</u> (ActiveManagers) пользователям, обладающим данной ролью предоставлена возможность создавать, редактировать, перемещать, удалять активы в Системе через раздел «Активы».
- <u>Руководитель</u> (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**».

Іеречень ролей с	истемы	Список пользователей для	роли: Administrators	
Наименование	Описание	Добавить		
ActiveManagers	Роль дает возможность создавать, редактировать, перемещать, удалять активы	Управление	Пользователи	
Administrators	Ропь для управления разделом администрирования системы. Пользователи данной роли имеют полный доступ	Удалить	admin	
PowerUsers	Роль предоставляет полный доступ ко всем объектам системы за исключением раздела администрирования управления активами			
ИБ_редактирование	Информационная безопасность_редактирование Мосстройпоставка			
ИБ_Чтение	роль для чтения ИБ в ЦА			
ФБ чтение	ца			
ЭБ Чтение				

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.

SecurityDe	esk ®Главная	≜ Мониторинг ~	⊘Регистрация -	⊞Активы +	ØАналитика÷	Адрикинстрирование - Настройки и мониторинг работы системы				е Документация	Пользов	атель L admin	GBaccor
У Инци Всего а Зарегистр В работе: Выполнен	Э́ Инциденты Всего активных: 3арект пропознание: Влаботе: Влаботе: 0 Варабо			УЯЗВИМ Всего актия Зарегистриров В работе: Выполненные	ОСТИ зных: каные:	Основные настройки Обработка входящих сообщений Редактор синакриев Редактор шаблонов Долопнительные параметры Сликси параметров Журнал работы	адачи ю активных: истрированные: оте: пненные:	1 1 0 0		Всего имеется: Компьютеры: Персонал:			8 5 3
	Инциденты зарегистри Уязвимости зарегистри					Управление доступом Управление пользователями Управление уровнем доступа Управление пользовательскими ролями Управление значлитивескими пранями	я пользователя " там отсутствует	С полным доступом	4" 4"				
Номер	Наименование			7 ASBRINGET	Категори	Управление аналитическими отчетами	Состояние	Вектор атаки	Регистр	ратор Дата	трации	Дата	9
2	XSPIDER ID: 1057	Стандартный паро	оль пользователя S'	/SDBA	Информа	Справочники Подразделений Подразделений	Зарегистрировано	Удаленная	admin	02-03-	2021 13:02	13-12-2019 14	4:41
3	XSPIDER ID:7034	Некорректная цепо	очка сертификатов		Информа	Типов компьютеров	Зарегистрировано	Удаленная	admin	02-03-	2021 13:02	13-12-2019 14	4:41
4	XSPIDER ID: 1024	Анонимный доступ	1		Информа	Сперационных систем Категорий безопасности	Зарегистрировано	Удаленная	admin	02-03-	2021 13:02	13-12-2019 14	4:41
5	XSPIDER ID: 1079	Учетная запись			Информа	Типов качественной оценки ущерба	Зарегистрировано	Удаленная	admin	02-03-	2021 13:02	13-12-2019 14	4:41
6	XSPIDER ID: 1119	Разглашение инфо	ормации		Информа	Документация Инструкция администратора	Зарегистрировано	Удаленная	admin	02-03-	2021 13:02	13-12-2019 14	4:41
7	XSPIDER ID:1147	Поиск пользовател	лей		Информа	Нормативные документы Хранилище файлов	Зарегистрировано	Удаленная	admin	02-03-	2021 13:02	13-12-2019 14	4:41

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.

SecurityDesk ФГлавная	а ♠Мониторинг+ ⊘Регистрация+	ШАктивы + ⊙отчетность	Ф Администрирование •		,© Документация	Пользователь: 💄 admin	С•Выход					
Создать Изменить С	ньских ролей Сохранить Удалить			Установка доступа по подразделениям Внешние контрагнеты								
Наименование	Описание			▶ Шклиента								
ИБ_редактирование	Информационная безопасность_редакти	рование Мосстройпоставка		 Компьютеры AD Пользователи AD 	• Скомпьютеры AD							
ИБ_Чтение	роль для чтения ИБ в ЦА			 Премонтное подразделение Москва 								
ФБ чтение	ЦА			▶ □Open								
ЭБ Чтение				 Ремонтное подразделение Новосибирск Ремонтное подразделение Санкт-Петербург 								
Разрешения для катего	рий безопасности			Elsonag Mocean - Pythesia Elsonag Mocean - Pythesia Elsonag Mocean - Pythesia Elsonare Espenses Elsonare Esurementy Elsonare Hosein-Hosein-Hoseiny Elsonare Hosein-Hoseiny Elsonare Hosein-Hoseiny Elsonare Personanose-Calavarcovi Elsonare Englisheria.								
Наименование		Уровень доступа к объек	там	▶ □Филиал Санкт-Петербург								
Физическая		 Запрещено Чтение Редактирование 										
Информационная		 Запрещено Чтение Редактирование 										
Экономическая		 Запрещено Чтение 		,								

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.

SecurityDe	esk ФГлавная ≜Мониторинг∽	ØРегистрация -	⊞Активы - ⊘Анал	итика - ФАдолинистр	прование •				# Документация	Пользователь: 🗴	ladmin G +Baco
У Инці Всего а Зарегист В работе Вылолнен	иденты ктивных: имес	4 4 0 0	Диягра УЯЗВИМ Акали Всего акти Зарене трирскани с Выполисные:	ины артизированные тические панели тические отчеты	2 2 0 0	С Задачи Всего активных: зарегистрированные: В раболе: Выполненные:		2	Активы Всего имеется: Компьютеры: Персонал:		2 1 1
Номер	Наименование		Инциденты зарег	истрированные за тегория	а последние 30 д Уровень инцидента	ней для пользовател Состояние	я "С полным достуг Подразделение	ПОМ" Рагистратор	Дата регистрации	Дата обнаружения	Дата возникновения
23	Инцидент ФинЦЕРТ		Φι	нЦерт-инцидент	Низкий	Зарегистрировано	Клинет	admin	17-10-2020 22:53	17-10-2020 22:53	17-10-2020 22:53
26	Инцидент ОТН		Фи ИН ОО	инЦЕРТ- формационный мен	Низкий	Зарегистрировано	Клинет	admin	20-10-2020 20:39	18-10-2020 16:30	20-10-2020 20:34
			Уязвимости зарег	истрированные з	а последние 30 д	ней для пользовател	я "С полным досту	пом"			
				За указанны	й период информация	Уязвимостям отсутствует					
			Задачи зарегис	трированные за п	оследние 30 дне	й для пользователя '	С полным доступо	м"			
Номер	Наименование		1	Категория	Тип задачи	Состояние	Подразделение	Исполните	ль Дата регистра	Дата ции начала исполнени	Срок исполнения я
30	По инциденту № 23 Инцидент ФинЦЕР	זי		ФинЦерт-операция БС ФЛ Карта-Неизвестный получатель	По инциденту	Зарегистрировано	Клинет	admin	17-10-202 22:57	0 17-10-2020 22:56	17-10-2020 22:56

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).
- 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.
- 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.

SecurityDe	sk ©Главная	Мониторинг -	ØРегистрация -	⊞Активы •	©Аналитика -	Ф Администрирование •			ŧ	Документация Пользов	arens 💵 admin 🛛 🔂 Bacoura
У Инци Всего ал Зарегистр В работе: Выполнен	 Унциденты Уязвимости Всего активных: Всего активных: Вработе: Вработе: Волоте: Вилотиенные: Вилотиенные: Вилотиенные: 				настройки и конклории работы системы Основные настойки Обработае входицик сообщений Редактор сценариев Редактор сценариев Дополнительные параметры Списко параметров Журнал работы	адачи о активных: истрированные: оте: пненные:	1 1 0 0	III Акт Всего Компью Персон	Наличина Всего имеется: Компьютеры Персоная		
				Инциденть	і зарегистрирс	Управление доступом Управление пользователями Управление уровнем доступа Управление пользовательскими ролями	я пользователя " там отсутствует	С полным доступо	«"		
Номер	Наименование			уязвимости	Категори	Управление аналитическими отчетами	Состояние	Вектор атаки	Регистратор	Дата регистрации	Дата обнаружения
2	XSPIDER ID:1057	Стандартный паро	ль пользователя SY	SDBA	Информа	Подразделений	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
3	XSPIDER ID:7034	Некорректная цепо	очка сертификатов		Информа	Типов компьютеров	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
4	XSPIDER ID:1024	Анонимный доступ	c .		Информа	Операционных систем Категорий безопасности	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
5	XSPIDER ID:1079	Учетная запись			Информа	Типов качественной оценки ущерба	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
6	XSPIDER ID:1119	Разглашение инфо	рмации		Информа	Документация Инструкция администратора	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
7	XSPIDER ID:1147	Поиск пользовател	ей		Информа	Нормативные документы Хранилище файлов	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41

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.

SecurityDesk Фглавная филониторинг- ©Регистрация- ШАктиеы- Флиалитика- Фланконстраров	анис -			г ≢Документация	Пользователь: 💄 admin	С•Выход
Перечень аналитических панелей	1	Теречень пользователей для і	выбранной анал <mark>итическо</mark>	ой панели Инциденты		
Наименование		Добавить				
Инциденты		Управление	Пол	тьзователь		
Очередь почтовых сообщений		Удалить	user	r		
Уязвимости		Удалить	use	rt		

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.

SacurityDask Ф/гланая Амонгорин- @Репктрация- ШАктивы- Остистають ФАдиманстрарование- 🗚 рокументация Попьзователь 🗴									
Общие Электронная почта Подключение к внешн	ним источникам Настройка импорта активов								
Подключение к внешним источникам									
Содать Изменить Уданны Проверить									
Наименование	Тип подключения	Использовать для аутентификации	Описание		Соединени активно	e			
FreeIPA	LDAP FreeIPA	2	FreeIPA соединение		1				
TEST.RU	LDAP Active Directory		Active Directory соединение		1				
Computers import	FTP-импорт активов csv		Импорт компьютеров		2				
Personal import	FTP-импорт активов csv	0.	Импорт персонала		2				

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.

		Наименование:		Тип подключе	ния:		
одключение к вне	ешним источникам	Nord.ru		LDAP Active	Directory V		
Создать Изменить Удалит	Проверить				Таймаут подключения (сек.):		
аименование	Тип подключения	Соединение активно: 🗹			10		Соединение
	LDAR FreeIRA	Адрес сервера:			Порт:		
	LUAPTICOPA	10.1.1.100			389		
	LDAP Active Directory	Пользователь:				динение	×
omputers import	FTP-импорт активов csv	Idapuser				08	X
ersonal import	FTP-импорт активов csv	Пароль:				2	
		•••••					
		Manage same and	AuthType:				
		аутентификации: 🗹	Ntim	~	Использовать SSL: 🗌		
		Домен:					
		NORD.RU					
		Путь:					
		DC=NORD,DC=RU					
		Описание:					
		АD авторизация					

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 активо	B 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	Продолжать обработку файла при ошибке
не найденные поля	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 <u>Менеджер активов</u> (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.

Наименование Тип подключения создинение актевно инпорт активов иллоческий иллоческий инпорт активов иллоческий инпорт активов иллоческий иллоческий инпорт активов иллоческий илл					очений:	тупных подкли	Список дос
FreeIPA LDAP FreeIPA 📝 🗹 🗹 Включить Выполнять каждые (часов):		импорта активов	Общие настройки	Автоматический импорт активов включен	Соединение активно	Тип подключения	Наименование
		Выполнять импорт каждые (часов):	Включить	V	2	LDAP FreeIPA	FreeIPA
TEST RU LDAP Active Directory 2 articol S 0		0	автоматический импорт активов: 🗹		1	LDAP Active Directory	TEST.RU
Computes FTP-wanoptracmees V III					N.	FTP-импорт активов csv	Computers import
Personal Import TPP-MunopTactiveos VI					×	FTP-импорт активов csv	Personal import

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.

цля наст Список дос	роики импор тупных подклю	рта активо очений:	выоерите	Общие Персонал Ко	омпьютеры		
Наименование	Тип подключения	Соединение активно	Автоматический импорт активов включен	Настройка импорта	персонала		
FreeIPA	LDAP FreeIPA	×	8	Включить импорт персонала:	Обновлять информацию у существующего персонала: 🗌	Импортировать персонал	
TEST.RU	LDAP Active Directory	×.	-	Фильтр поиска:	Путь:	Munorrangerste a possigerenautor	
Computers mport	FTP-импорт активов csv	×		uid=*	Путь для импорта	OOO Pacceet	·]
Personal Import	FTP-импорт активов csv	~					
				Атрибуты импорта г	терсонала		
				Учетная запись:	Фамилия:	Имя:	Отчество:
				1	3	2	4
				Должность:	Телефон:	Электронная почта:	Дополнительная информация
				5	6	7	8

Рисунок 77. Настройка импорта персонала.

Таблица 4. Параметры импорта персонала.

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

писок дос	тупных подклю	очений:		Общие Персонал Компьютерь	4		
Наименование	Тип подключения	Соединение активно	Автоматический импорт активов включен	Настройка импорта компь	ютеров		
FreeIPA	LDAP FreeIPA	×	×	Включить импорт компьютеров:	Обновлять информацию у существующих компьютеров:	Импортировать компьютеры	
TEST.RU	LDAP Active Directory	M		Фильтр поиска:	Путь:	Импортировать в подразделение:	
Computers Import	FTP-импорт активов csv	V		fqdn=*	Путь для импорта	OOO Pacceet V	
Personal Import	FTP-импорт активов csv	×	11				
				Атрибуты импорта компьн	отеров		
				Наименование:	Manage same DNC	IP-agpec:	Тип компьютера:
				serverHostName	для получения IP-адреса:	info	nsHardwarePlatform
				ARTONISTINACIU ASRCENET	Операционная система:	Дополнительная информация:	
				ABIOMATH TOOLN SATURINE	Commence and the second	Concernations -	

Рисунок 78. Настройка импорта компьютеров.

Таблица 5. Параметры импорта компьютеров.

Параметры	Пояснение
BURNNET MARONT VOMELIOTODOR	Включение автоматического импорта компьютеров
включитв импорт компьютеров	по расписанию
	В случае если при импорте компьютеров актив уже
	импортирован в систему, осуществляется только
у существующих компьютеров	обновление его параметров
	Используется для избирательного импорта активов
Фильтр поиска	через LDAP-подключение
Путь	Путь в LDAP-каталоге
	Подразделение, в которое импортируются новые
импортировать в подразделение	активы
Использовать DNS	При включенном параметре система автоматически
для получения IP-адреса	выполняет поиск IP-адреса по его сетевому имени
	В случае если при импорте компьютера
Автоматически заполнять	операционная система не содержится в
справочник операционных систем	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
<pre>(&(objectCategory=user)(objectClass=user)(userPrincipalNam e=*))</pre>	Все пользователи
objectCategory=person)(objectClass=user)(!useraccountcontr	Все пользователи, кроме
ol:1.2.840.113556.1.4.803:=2)	отключенных
(&(objectCategory=user)(objectClass=user)(ltitle=*))	Пользователи, у которых не
	заполнено поле должность
(objectCategory=computer)	Все компьютеры
(objectCategory=computer)(operatingSystem=Windows 10*)	Все компьютеры Windows 10
	Все SQL серверы, с любой
(objectCategory=computer)(servicePrincipalName=MSSQLSvc	ОС, у которых
)(operatingSystem=Windows Server)	зарегистрирован
	servicePrincipalName
(objectCategory=computer)(servicePrincipalName=exchange	Bce Exchange censent
MDB*)(operatingSystem=Windows Server*)	все скланде 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.

№ Инциденты Уязвимости Основне настойни конторне работи систими Основне настойни конторне работи систими Основне настойни конторне работи систими 1 Е Активы Всего активных: 0 Всего активных: 0 Всего активных: 0 Всего инчестся:	
Зарепистрированные: В риботе: В риботе:	8 5 3
Инциденты зарегистриор Управление пользователянии Управление пользователяния от там отсутствует	
Управление пользовательскими ролями Уязвимости зарегистрирс Управление аналитическими панелями в пользователя "С полным доступом"	
Номер Наименование Категор упредление индигинескими отчетами Остовоннии Состояние Вектор атаки Регистратор Дата регистрации	Дата обнаружения
2 XSPIDER ID:1057 Стандартный пароль пользователя SYSDBA Информи Подразделений Зарегистрировано Удаленная аdmin 02-03-2021 13 Подразделений Подразделений Зарегистрировано Удаленная admin 02-03-2021 13	J2 13-12-2019 14:41
3 XSPIDER ID 7034 Некорректная целочка сертификатов Информ Типов компьютеров Зарегистрировано Удаленкая admin 02-03-2021 13	J2 13-12-2019 14:41
4 XSPIDER ID:1024 Анжимлый доступ Информи Категорий дезопасности Зарегистрировано Удаленная admin 02-03-2021 13	32 13-12-2019 14:41
5 XSPIDER ID:1079 Учеткая запись Информи Типов качественной оценки ущерба зарегистрировано Удаленная admin 02-03-2021 13	02 13-12-2019 14:41
6 XSPIDER ID:1119 Разглашение информации Информ Инструкция администратора Зарегистрировано Удаленная admin 02-03-2021 13	02 13-12-2019 14:41
7 XSPIDER ID:1147 Поиск пользователей Информативные документы Хранилище файлов Зарегистрировано Удаленная admin 02-03-2021 13	32 13-12-2019 14:41

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.

Администрирование нормативных документов	OB	
--	----	--

					-	
Нормати	вный документ:					
Выберит	е нормативный ;	зокумент				
Полит	ика информацио	нной безопасности				
Поиск						
Добав	ить Изменит	ъ Удалить				
Содержа	ние нормативно	го документа				
	Код документа	Раздел	Пункт	Формулировка	Теги	ID
Выбор	ПИБ-2019	Требование	6.3.1.1	Запрещается использовать ПЗВМ в целях не относящихся к производственной деятельности	тмп	1
Выбор	ПИБ-2019	Требование	6.5.1.1	Пароль должен иметь не менее 8 симаолов, включая строчные и прописные бухвы, цифры и спецсимаолы.	нсд	10
Выбор	ПИБ-2019	Рекомендация	8.1.1	Рекомендуется изменять пароль не реже чем одного раза в 30 дней	тмп кт	11
Выбор	ПИБ-2019	Требование	8.1.2	На всех устройствах, подверженных вирусному заражению при подилючении их к корпоративной сети необходимо установить антивирусное ПО с актуальными базами, а также проверку устройства на наличени вирусов	ВИРУС	39
Выбор	ПИБ-2019	Требование	8.2.2	Запрещается записывать и хранить пароли рядом с ПЗВМ.	нсд	40
Выбор	ПИБ-2019	Нормативный	9.1.1	Проверка на уязвимости выполняется администратором безопасности не реже 1 раза в месяц на серверном комплексе.		41

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.

SecurityDe	esk ®Главная ≜Мониторинг≁ ⊘Регистра	ция • 🖽 Активы • С		Администрирование -	-				атель: 🎗 admin 🛛 🔂 Быхо
У Инци Всего а Зарегистр В работе: Выполнен	ИДЕНТЫ КТИВНЫС: О мрозаники: О екке: О	УЯЗВИМОС Всего активны Зарегистрировани в работе: Вылолисивные:	CTM IXC NMC	настройн и изингорин раблы системи Основши настройни Обработав хорадицих сообщений Редактор сценариев Редактор цейпариев Дополнительные параметры Списки параметров Журнал работы	адачи о активных: истрированные: оте: тненные:	1 1 0 0	Всего и Компьюте Персонал	IBЫ меется: ::	8 5 3
		Инциденты за Уязвимости за	регистрирс регистрирс	Управление доступом Управление пользователями Управление уровнем доступа Управление пользовательскими ролями Управление аналитическими панелями	я пользователя " там отсутствует я пользователя "	С полным доступом" С полным доступом"			
Номер	Наименование		Категори	Управление аналитическими отчетами	Состояние	Вектор атаки	Регистратор	Дата регистрации	Дата обнаружения
2	XSPIDER ID:1057 Стандартный пароль пользовате	ля SYSDBA	Информа	Подразделений Полжностей	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
3	XSPIDER ID:7034 Некорректная цепочка сертифии	атов	Информа	Типов компьютеров	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
4	XSPIDER ID: 1024 Анонимный доступ		Информа	Сперационных систем Категорий безопасности	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
5	XSPIDER ID: 1079 Учетная запись		Информа	Типов качественной оценки ущерба	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
6	XSPIDER ID:1119 Разглашение информации		Информа	документация Инструкция администратора	Зарегистрировано	удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
7	XSPIDER ID:1147 Поиск пользователей		Информа	Нормативные документы Хранилище файлов	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41

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.

ыоерите тип объекта		категория оезопасност		
Инциденты	~	Информационная	~	Добавить Изменить Удалить
MS-cqpwnr Teu TeuthocidentMai Dp же	стовый скритт - информационная безопа оверочный скритт по автоматическому з цировита	сность 🧭	<pre>{ "scurityType": 2, Toppartemt": "MocCrashormans", Tomertame: "india", TodyCetType": 1, " "tasks": [" "maschdd": "mooccrashormans", "maschdd": "mooccrashormans", " "maschdd": "mooccrashormans", " "maschdd": "mooccrashormans", " "maschdd": "mooccrashormans, Toppartemt": "moncana, Xalog " "usertame": "admin" ", " "maschdd": "mooccrashormans, " "maschdd": "mooccrashormans, " "maschdd": "mooccrashormans, " "maschdd": "mooccrashormans, " "maschdd": "mooccrashorman, " "mooccrashorman, " "maschdd": "mooccrashorman, " "mooccrashorman, "</pre>	акантралировать устранение последствий от инцидента", ролкруйте вимолитие задач", полнить проверсу", имо вилолить проверсу ссеедного оборудования по инциденту", белеск",

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.

S	ecurityDesk ©Главна	я Ф Мониторинг+ @Репистрация+	ШАктивы - Остчетност			д © Документация	Пользователь: 🚨 admin	Бязыход
Ρ	едактор сцен	ариев		Добавить новый сценарий ×				
	Выберите тип объекта		Категория безопасности	Наименование:				
	Инциденты	~	Информационная	Incident 1				
	ИБ-скрипт	Тестовый скрипт - информационная Безон	асность 😥 🤇	Добавить шаблон сценария: 🗹				
	TestIncidentMail	Проверочный скрипт по автоматическому : инцидента	заведению	Дополнительная информация: сценарий на реапирование по инциденты				
				Вилючить: 🗆	инцидента",			
				Добавить Отменить	J			

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.

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

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

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

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

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

Наименование	Тип данных	Пояснение	Примечание
поля			
Родительский объе	ект - Задача	1 -	1_
Name	Строка	Подстрока в названии	При пустом значении не
		инцидента -	учитывается
		срабатывает при	
		совпадении	
Description	Строка	Не используется	
SecurityType	Целое	Категория безопасности	Нельзя изменять
PlanStartDateAdd	Целое	Не используется	
PlanFinishDateAdd	Целое	Не используется	
Department	Строка	Наименование	При пустом значении не
		подразделения -	учитывается
		срабатывает при	
		совпадении	
UserName	Строка	Имя владельца	При пустом значении не
		инцидента -	учитывается
		срабатывает при	
		совпадении	
Status	Строка	Наименование	Обязательно к
		состояния, при котором	заполнению
		срабатывает сценарий	
ObjectType	Целое	Тип объекта	Нельзя изменять
Подчиненные объ	екты – Задачи "	task": { }	
Name	Строка	Добавляется к	
		названию задачи	
Description	Строка	Добавляется к	
		описанию задачи	
SecurityType	Целое	Категория безопасности	Номер категории указан
		задачи	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	Обязательно для
		подразделения для	заполнения!
		задачи	
UserName	Строка	Имя пользователя для	Обязательно для
	-	задачи	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.

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

Таблица 10. Требования к атрибутам правил создания объектов.

		срабатывает при	
		совпадении	
SaveAttachments	bool	Сохранять вложения	true – сохранять
		сообщения в карточку	вложение
		объекта	
SearchActives	bool	Искать во вложении	true – искать активы во
		активы и привязывать к	вложении
		объекту	
ObjectType	Целое	Тип объекта	0 - Нельзя изменять
Подчиненный объ	ект – 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	Обязательно для
		инцидента	заполнения!
ObjectType	Целое	Тип объекта	0 - Нельзя изменять
tasks	структура	Подчиненные задачи	null - Нельзя изменять
Подчиненный объ	ект – Уязвимость	<pre>vulnerability": { }</pre>	
Name	Строка	Добавляется к	
		наименованию	
		уязвимости	
Description	Строка	Добавляется к	
		описанию уязвимости	
SecurityType	Целое	Категория безопасности	Номер категории указан
		задачи	в справочнике
OwnerName	Строка	Имя владельца	Обязательно для
		инцидента -	заполнения!
		срабатывает при	
		совпадении	
DangerLevel	Строка	1 - Низкий	Обязательно для
		4 - Критический	заполнения!
ObjectType	Целое	Тип объекта	0 - Нельзя изменять
tasks	структура	Подчиненные задачи	null - Нельзя изменять
Подчиненный объ	е кт – Задача "ta:	sk": { }	
Name	Строка	Добавляется к	
		названию задачи	
Description	Строка	Добавляется к	
		описанию задачи	
SecurityType	Целое	Категория безопасности	Номер категории указан
		задачи	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	Обязательно для
		задачи	заполнения!
ObjectType	Целое	Тип объекта	0 - Нельзя изменять
tasks	структура	Подчиненные задачи	null - Нельзя изменять
Подчиненный объе	ект – Параметры	<pre>"parameters":[{},{}]</pre>	
Name	Строка	Наименование	
		дополнительного	
		параметра	
Value	Строка/Число	Значение	Для числовых
		дополнительного	параметров используйте
		параметра	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.

SecurityDe	esk ©Главная	▲Мониторинг -	ØРегистрация	+ ⊞Активы.+	©Аналитика -	Администрирование -			¢;	Документация Пользоі	атель: 💄 admin 🛛 🔂 Ва
У Инци Всего ал Зарегистр В работе: Выполнен	Инциденты Всего активных: 0 Зарепастрирование: 0 В работе 0 Выполнетные: 0		Уязвим Всего актив Заренстриров В работе: Выполненные Инциденты	ОСТИ аных: анные: зарегистриро	настрои и монтронг забот астими Основные настойки Обработка входящих сообщений Редактор цайонов Дополнительные параметры Списи параметро Журная даботы Управление пользователями	адачи о активных: мстрированные: оте: пненные: а пользователя "	1 1 0 0 С полным доступом	E AKTI Bcero I Koamaot Nepcona	ИВЫ имеется: ерм: л.	8 5 3	
				Уязвимости	зарегистриро	управление уровнем доступа Управление пользовательскими ролями Управление аналитическими панелями	я пользователя "	С полным доступо	n "		
Номер	Наименование				Категор	Управление аналитическими отчетами Справочники	Состояние	Вектор атаки	Регистратор	Дата регистрации	Дата обнаружения
2	XSPIDER ID:1057	/ Стандартный пар	оль пользователя	SYSDBA	Информ	Подразделений Должностей	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
3	XSPIDER ID:703	И Некорректная це	почка сертификато	8	Информ	Типов компьютеров	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
4	XSPIDER ID: 1024	Анонимный дост	γn		Информ	Категорий безопасности	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
5	XSPIDER ID: 107	Э Учетная запись			Информ	Типов качественной оценки ущерба	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
6	XSPIDER ID: 1119	Разглашение инф	оормации		Информ	документация Инструкция администратора	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
7	XSPIDER ID:1147	Поиск пользовате	алей		Информ	Нормативные документы Хранилище файлов	Зарегистрировано	удаленная	admin	02-03-2021 13:02	13-12-2019 14:41

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.

Позиция 1	Тип параметра Чекбокс	Обязательный	
1	Чекбокс		

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.

SecurityDesk ФГлавная Амониторинг - ФРегистрация -	ШАхтивы = — Фотчетность Фальнинстинование -	-	¢ [©] Документация	Пользователь: 🔔 admin	С •Выход
	Добавить новый параметр ×				
Редактор настройки дополнительны	КПЕ Наименование параметра:				
Тип объекта Категори	я безо Класс инцидента				
Инциденты У Инфор	Позиция параметра:				
Наименование параметра	2	тельный			
Выгрузка в реестр	Тип параметра:				
2	Число 🗸				
	Обязательный: \Box				
	Добавить Отменить				

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».

Эценка ущерба: сачественная оценка: Финансовые потери Соличественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры сополнительные параметры: тасс инцидента:	ведите полное описание инцидента	
Оценка ущерба: Зачественная оценка: Финансовые потери Золичественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры ополнительные параметры: ыгрузка в реестр: ласс инцидента:		
Оценка ущерба: ачественная оценка: Финансовые потери ✓ соличественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры ополнительные параметры: ыгрузка в реестр: □ ласс инцидента:		
Оценка ущерба: ачественная оценка: Финансовые потери ✓ соличественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры сополнительные параметры: кыгрузка в реестр: □ ласс инцидента:		
Оценка ущерба: ачественная оценка: Финансовые потери ✓ Соличественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры Сополнительные параметры: сыгрузка в реестр: □ ласс инцидента:		
Оценка ущерба: Качественная оценка: Финансовые потери ✓ Количественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры Кополнительные параметры: Кыгрузка в реестр: □ ласс инцидента:		
Оценка ущерба: Качественная оценка: Финансовые потери ✓ Количественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры Кополнительные параметры: Кыгрузка в реестр: □ ласс инцидента:		
ачественная оценка: Финансовые потери ✓ Соличественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры Сополнительные параметры: Кыгрузка в реестр: □ ласс инцидента:	енка ушерба:	
Финансовые потери ✓ Количественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры Ополнительные параметры: ыгрузка в реестр: □ ласс инцидента:	ественная оценка:	
Финансовые потери ✓ Количественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры Сополнительные параметры: Кыгрузка в реестр: □ ласс инцидента:		
Соличественная оценка: Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры Сополнительные параметры: сыгрузка в реестр: □ ласс инцидента:	инансовые потери	×
Введите предполагаемую количественную оценку ущерба в рублях Результат: Опишите принятые меры ополнительные параметры: ыгрузка в реестр: ласс инцидента:	ичественная оценка:	
Результат: Опишите принятые меры ополнительные параметры: выгрузка в реестр: ласс инцидента:	ведите предполагаемую количественную оценку ущерба в рублях	₽
Результат: Опишите принятые меры Сополнительные параметры: Сыгрузка в реестр: ласс инцидента:		
Опишите принятые меры ополнительные параметры: выгрузка в реестр: ласс инцидента:	ультат:	
ополнительные параметры: Ъыгрузка в реестр: □ ласс инцидента:	пишите принятые меры	
ополнительные параметры: Зыгрузка в реестр: □ ласс инцидента:		
lополнительные параметры: выгрузка в реестр: □ ласс инцидента:		
lополнительные параметры: выгрузка в реестр: □ ласс инцидента:		
Зыгрузка в реестр: 🗆 ласс инцидента:	олнительные параметры:	
Зыгрузка в реестр: ⊔ ласс инцидента:	_	
ласс инцидента:	грузка в реестр: 🗌	
	асс инцидента:	
		_

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».

+ Добавить источник	
Источники инцидента:	
+ Добавить цель	
Объекты воздействия инциде	ента:
🖹 Заполнить по шаблону:	
📽 Заполнить по шаблону: Список шаблонов:	

Регистрация нового инцидента Наименование: Категория безопа Marth ровень ини нта Дата возникновения 06-03-2021 20:05 = Дата обнаружения 06-03-2021 20:05 ≡ Подразделение Оценка <mark>у</mark>щерба Качественная оценка Количественная оценка: ₽ Зарепистрировать



Рисунок 89. Создание шаблона заполнения.

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

SecurityDe	sk ⊗Главная ≜Мониторинг÷		- 📕 Активы -		Адолнистрирование -	-			ЭДокументация Пользов	атель: 👤 admin 🛛 С+Выхор
У Инци Всего ак Зарегистри В работе: Вылолиени	ДЕНТЫ тивных: еме:	0 0 0 0	УЯЗВИЛ Всего акти Зарегистриро в работе: Выполненные	ЮСТИ ВНЫХ: ванные: ::	настройи и изынгорые работы системи Основные настройки Редактор сценариев Редактор сценариев Дополнительные параметры Списки параметров Журнал работы	адачи ю активных: истрированные: оте: пненные:	1 1 0 0	Ecerc Komis Report	ГИВЫ • имеется: отеры: нал:	8 5 3
			Инциденты	зарегистриро	Управление доступом. Управление пользователями	я пользователя "	С полным доступом	(¹¹		
					Управление уровнем доступа	там отсутствует				
			Уязвимости	зарегистриро	Управление аналитическими панелями	я пользователя "	С полным доступо	n''		
Номер	Наименование			Категори	Управление аналитическими отчетами Споавочники	Состояние	Вектор атаки	Регистратор	Дата регистрации	Дата обнаружения
2	XSPIDER ID:1057 Стандартный паро	пь пользователя \$	YSDBA	Информа	Подразделений Должностей	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
3	XSPIDER ID:7034 Некорректная целя	очка сертификато		Информа	Типов компьютеров	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
4	XSPIDER ID: 1024 Анонимный доступ			Информа	Категорий безопасности	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
5	XSPIDER ID:1079 Учетная запись			Информа	гилов качественной оценки ущерба	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
6	XSPIDER ID:1119 Разглашение инфо	рмации		Информа	Инструкция администратора	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41
7	XSPIDER ID:1147 Поиск пользовател	ей		Информа	Нормативные документы Хранилище файлов	Зарегистрировано	Удаленная	admin	02-03-2021 13:02	13-12-2019 14:41

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».

SecurityDesk ФГлавная &Монитор	инг • 🛛 🕬 Регистрация • 📰	ативы •	🕫 Документация Пользователь: 💵 admin 🕞 Выск
Редактор шаблонов за тип объекта Инциденты	аполнения для I катего У Фин	НЦИДЕНТОВ, УЯЗВИМОСТЕЙ И ЗАДАЧ рия базопасности ЦЕРГ-Илецидент-ИПК ✓ Изменень Удалить	
OTC GWLEPT		<pre>{ "SecurityType": 4, "Description": "Despate for cornacus", "Ineel": i, "Despate for cornacus", "Tealse" "Ornpaters is for cornacus", "Tealse", "{ "Tealse", "for cornacus", "Tealse", ", 2 lices], 4 (2 lices],</pre>	

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.

ц _ю		Microsoft SQL Server Management Studio (Ar	цминистратор)	_ 0 ×
Файл Правка Ви	д Отладка Сервис Окно Справка			
i 🚰 • 🖂 • 😂 🔒	🦼 🔔 Создать запрос <table-cell> 📸 📸 🏠</table-cell>	※ 12 22 ウ・マ・第・12 22 ト -	- 🙆	- 🔩 🕾 🏷 💽 - 📮
Обозреватель объе	ктов 👻 🕂 🗙			
Соединить -	k = 7 2 💰			
🖃 🐻 WIN2012 (SC	QL Server 12.0.4100 - WIN20			
🖃 🧰 Базы дан	ных			
н 📔 Сист	емные базы данных			
🗄 🧀 Безо	Создать базу данных			
🖽 🧰 Объс	Создать запрос			
	Создать скрипт для базы данных 🔸			
10 July - 1 J	Задачи 🔸	Отсоединить		
	Политики	Перевести в автономный режим		
	Аспекты	Перевести в оперативный режим		
	Запустить PowerShell	Сжать	•	
	Отчеты +	Создать резервную копию		
	Переименовать	Восстановить	•	
	Удалить	Сформировать скрипты		
	Обновить	Извлечь приложение уровня данных		
	Свойства	Развертывание базы данных в виртуальной машине Windows Azure		
		Экспорт приложения уровня данных		
		Зарегистрировать как приложение уровня данных		
		Обновить приложение уровня данных		
		Удалить приложение уровня данных		
		Импорт данных		
		Экспортировать данные		
< 111	>			
Готово				
E 14				▲ 😼 🗊 🖓 😘 ENG 22:13 12.05.2019

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.

4.	Micro	osoft SQL Server Management S	udio (Администратор)		- 0 X
Файл Правка Вид Отладка Сервис Окно Спра	J	Резервное копи	рование базы данных - SecurityDB	_ D X	
Обозреватель объектов 🔷 🕂 🕂 🗙	Выбор страницы Рбщие	🔄 Скрипт 👻 🚺 Справка			
Соединит • • • • • • • • • • • • • • • • • • •	Паранетры медла Параметры резереного коли, Сосдинето Сосдинето Сосание МИ2012 Сосание МИ2012 Сосание МИ2012 Сосание МИ2012 Сосание Сосание МИ2012 Сосание Сосание Сосание МИ2012 Сосание Сосание МИ2012 Сосание Сосани Сосани Сосание Сосание Сосани	Источник База данных: База данных: Тит резервной колии: Только резервное Компоннит резервного @ База данных @ Файлы и Файловые группы: Назначение Создать резервную колию на:	SecuriyOB IRPOCTAR Tomes Deve SecuriyOB bak	v v Добампь Удалль Содерженое	
< III >				ОК Отмена	
Проводник					22:20
🛨 📥 🖉 📑 🖊 片	Ś.			- 😼 🖯 😳 🕼 E	NG 12.05.2019

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]/арі/.../.... 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.
 - 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».
 - 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».
 - 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'....»
 - 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': 'pcvs078115.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';»

Общие Электронная почта	Подключ	иние к внешним источникам	Настройка и	Аналитика - Фдлиннстри ипорта активов Интеграци	ирование - Iя с RuSIEM	
токен:	иции	Подразделение:		Имя пользователя:		
	C	test1	-	admin	-	Включить интеграцию: 🗹
астройки регист	раци	и инцидентов				
вразтать-пор-417с-аор4-6005014	рами:	И ИНЦИДЕНТОВ Устанавливать связь с перс	оналом:			
вразтать-лър-417с-ар94-6005014 АСТРОЙКИ РЕГИСТ Устанавливать связь с компьютер по IP и Наименованию	раци	И ИНЦИДЕНТОВ Устанавливать связь с перс по Логину и E-mail	оналом:	Сохранять в инциденте г	аw-файл: 🗹	Переоткрывать при возврате в RuSi
Вразтать-пор-417с-аор4-6005014 Состройки регистр и связь с компьютер по IP и Наименованию Сохранять в описании основные данные инцидента:	раци	И ИНЦИДЕНТОВ Устанавливать связь с перс по Логину и E-mail Сохранять в описании инци, метаданные:	оналом:	Сохранять в инциденте г Сохранять в описании ин объекты группировки:	аw-файл: 🗹 ицидента	Переоткрывать при возврате в RuS ☑

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.

|--|

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.
 - 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
```

<u>Designer</u>	History	Users	Profiles		🔔 Logout (admin) Language 🗸
				Diagram Graph JSON XML.	Export Import New workflow
¢					Task settings (dos) ×
				✓ 1. SDMessageToTerminal ×	2 Description
				Create SIEM Incident	Сохраняем Id инцидента Enabled
					✓ New setting
			1	✓ 2. SDsetVariable ×	Name Delete
				Сохраняем Ід инпидента	rusiem_id luaValue Delete
				↓ 3. SDMessageToTerminal	Icnt=entity.Parameters.Count for i=0, Icnt-1 do if(entity.Parameters[i] [Name]==rusiem_id') then return entity.Parameters[i][Value]
				Выпод номера инциедита RuSIEM	end return 0
				4. SDRuSIEMChangeStatus X Yeranonurs.cocronnine munucentra a Pennen	

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.

Dashi	board	Records Manager Approv	vals <u>Designer</u> History	Users Profiles		🔔 Logout (admin) Language 🗸
E	lrowse			Diagram	Graph JSON XML	Export Import New workflow
Q	Searc	h tasks	«			Task settings 📾 🗡
		логической операции	*		✓ 1. SDMessageToTerminal	4
	4	SDMailSender			Create SIEM Incident	Description
	7	Почтовая рассылка сообщений			and the second sec	Изменение состояния в RuSIEM
		SDMailSamar				Enabled
	4	Сохранение настроек почтового сервера в переменной			×	New setting
	SmtpServerSettings для			4 2. SDsetVariable	api_key Delete	
					Установка переменной rusiem_id	kjdkqwhdqjwdkqwjdkqwjbkqjwkw3uy32
	4	SDMessageToTerminal Baison coofinemiñ na soncons c				host Delete
		нспользованием Lua				rusiem01.test.ru
	4	SDRuSIEMChangeStatus			✓ 3. SDMessageToTerminal ×	status Delete
		RuSIEM. Предварнательно				in_work 🗸
	необходимо установить номер инцидента RuSIEM в переменную				luaSolution Delete	
	4	rusiem_id! SDsetEntity				return "Инцидент ваят в paбory"entity.Report
	-4	Изменнть информацию объекта в SecurityDesk			4. SDRuSIEMChangeStatus	
	4	SDsetVariable Создать/обновить переменную			Изменение состояния в RuSIEM	
		workflow				

Рисунок 96. Настройка изменения состояния инцидента RuSIEM на сервере бизнеспроцессов.

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

0	Rusiem	l RUS ∨					
•				Добавление роли			×
w.	Настро	ойки системы Почтовые н	астройки Настройки правил корреляции Изме		100		1
				Наименование	IRP		
×	<u> </u>	Поиск ролей	٩	Описание	АСУБ		
Ø	ID	Название	 Описание 				
A 10	3	Оператор	Оператор				
9	7	Интеграция email	Группа рассылки для интеграции по электронной по				
	1	Гость				Отменить	Сохранить
ф	6	Аудитор	Аудитор	,	<u>,</u>	CICICMIDA	2022
8	5	Аналитик ИТ	Аналитик ИТ		1	Системная	2022-
_	4	Аналитик ИБ	Аналитик ИБ		1	Системная	2022-
B	2	Администратор			5	Системная	2022-
÷	10	IRP	ACY6		1	Пользовательская	2023-
	Записи	и с 1 по 8 из 8 записей					
٨							
e	© 2014 - 2	023. RUSIEM					
⊨							
9							
0							
4							

Рисунок 97. Создание новой роли.

- 2. Перейдите в раздел «Настройки» «Интеграции» и на вкладке «R-Vision» Рисунок 98 настройте параметры:
 - В поле «Xoct 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».

🕜 R	Rusiem Rus 🗸	
D		
k	R-Vision Rusiem API FocCo	ΟΠΚΑ Rusiem loC
W)	Настройки подключения к R-	Vision
ଞ	Хост R-Vision:	https://172.20.1.77
▲ 10	Токен авторизации	tfyurtyrtyhrtyhrty
٩	SSL соединение	
ф	Группа для отправки	IRP 🗸
	Интеграция активна	
	Синхронизация статусов	
~	Категория по умолчанию	Информационная
	Режим Multitenancy	
•		Проверка подключения Сохранить
¢		
E		
0	© 2014 - 2023. RUSIEM	

Рисунок 98. Настройка интеграции с Системой.

 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.

Добавление пользователя

Логин	irp_user
Пароль	
Повтор пароля	
Ключ АРІ	NzebvNa1TFHfJgsdiklrg4WgtFGcTlqv Сгенерировать
Email	
Фамилия	
Имя	
Отчество	
Ограничение сеансов	
Статус	Активный 🗸
Оповещения	Всплывающее уведомление о новых инцидентах
	Уведомления в Телеграм
Тип аутентификации	🔵 Локальный 🔘 LDAP 🔘 Гибридный
Пользователь в	🗸 Гость
группах	🗹 Администратор
	🗸 Оператор
	🗸 Аналитик ИБ
	🗸 Аналитик ИТ
	🗸 Аудитор
	🗌 Интеграция email
	ASUB IRP
	Отмена

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.

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

The R	usiem RU	is v								I		3
	Корреляция Все правила По	группам										
U	Подозрение на Мооп п	malware	Q						Включить ст	атистику	Пока	зать: 50
۵ ۹	О	С Группа	Тип	Статус	Правило	Д c) ата оздания	Дата последнего обновления	Время выполнения	0 Инциден	О	
њ 8	Копия Подозрение на Moon malware	Malware	Пользовательская	Активно	/HNAP1 contains http.url OR (/HNAP1 contains msg) OR (http.url == "HI APExt") OR (HNAPExt contains msg)		9.06.2023 0:04:37	22.06.2023 00:17:03	Мин.: 0 мкс, Сред.: 0 мкс, Макс.: 0 мкс	0		/ U2 8
8	Подозрение на Moon malware	Malware	Системная	Неактивно	/HNAP1 contains http:// OR (/HNAP1 contains msg) OR (http:// == "HI APExt") OR (HNAPExt contains msg)	÷ 21	7.12.2022 1:40:23	22.06.2023 00:14:14	Мин.: 4 мкс, Сред.: 4 мкс, Макс.: 4 мкс	738		/ b
۶ m	Записи с 1 по 2 из 2 запи	исей (отфильт	ровано из 410 записей)						Первая	< 1	> После,
*	© 2014 - 2023. RUSIEM											
=												

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».

орреляция						
ID правила: 376					Дата создания: 2023-0 Дата обновления: 2023-0	06-09 10:04:37 06-09 10:04:37
Тип события		Название инцидента		Mitre ID		
syslog	~	Копия Подозрение на Moon malware				+ -
Производитель Продук	т	Категория инцидента		Ссылки		
* *	~	Основные	$H \sim$			+ -
Группа:		Описание инцидента		Тип инцидента	Приоритет	
Noxox		Использование протокола НИАР https://ics.san.sdu/forums/diany/More+on+HNAP+What+is+ic+How+to+Use+ic+ How+to+Find+ic/17648/			1	~
				Переоткрыть инцидент, если закрыт	Не регистрирова	іть инцидент
 Сбои в инфраструктуре Нарушение политик Аномалии 		Группировать по: Z Активно	справило	Назначено: Группам: IRP,Администратор		
~		rscip ✓ dscip User.name				

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:

Наименование	Тип	Пояснение	Пример
параметра	данных		
Раздел appSettings			
ConnectionTimeInterval	Число	Периодичность проверки	1500
		появления инцидентов в PTSIEM	
		(1000 - 1 секунда)	
DebugMode	bool	Включение режима отладки для	false
		подробного журналирования	
CoveDov	haal	работы в Системе	
Saveraw	1000	Прикреплять данные инцидента	true
		РТЗЕМ В ЈЗОМ-формате в карточку	
CheckDays	Число	Глубица проверки иниидентов в	7
CHECKDays	число	ПЛУОИНА ПРОВЕРКИ ИНЦИДЕНТОВ В DTSIEM 23 последние колицество	7
		лней	
SecurityType	Число	Илентификатор категории	2
		безопасности в которую будут	-
		сохраняться инциденты	
AccountPTSIEM	Строка	Имя обобщённого подключения,	ptservice
		используемого для доступа к	•
		PTSIEM	
client_id	Строка	Идентификатор подключения к	mpx
		PTSIEM	
client_secret	Строка	Ключ подключения к PTSIEM	5c2327d2-15a1-4b8b-
		смотрите: grep ClientSecret	9b75-b8808167d0a8
		/var/lib/deployer /role_instances/	
	6	Core/params.yaml	1
response_type	Строка	Тип ответа от РТЅІЕМ на запрос	code id_token
		аутентификации	
scope	Строка	Область – смотри документацию к	offline_access_mpx_api
	e.pena	PTSIEM	ptkb.api
tokenRequestLink	Строка	Адрес сервиса для запроса токена	https://[IP]:3334/connec
		аутентификации	t/token
incidentListLink	Строка	Адрес сервиса для запроса списка	https://[IP]/api/v2/incide
		инцидентов	nts
incidentLink	Строка	Адрес сервиса для запроса	https://[IP]/api/incidents
		конкретного инцидента	ReadModel/incidents
assignedUserEmail	Строка	Импорт инцидентов назначенных	irp@securitydesk.ru
		на пользователя в PTSIEM с email	
		(значок * для загрузки всех	
		инцидентов)	

Таблица 12. Настройки службы ConnectorPTSIEM.

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.

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

Таблица 13. Дополнительные параметры инцидента PTSIEM.

- 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** <u>– без установленной переменной «id» изменение состояния выполняться не будет</u>. 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 кеу.

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 кеу.

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



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

NՉ	http-	Шаблон запроса	Описание
	глагол		
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
			ld, параметры передаются в теле запроса
11	PUT	/api/Vulnerabilities /Id	Изменение существующей уязвимости с номером
			ld, 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