2025 SecurityDesk Инструкция

пользователя

[SECURITYDESK АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ]

Инструкция по использованию 1.42

Оглавление

Введе	ение	2
Приня	ятые сокращения и определения	2
Основ	зные объекты системы	2
Работа	а пользователя в системе	4
1.	Вход в систему	4
2.	Главная панель мониторинга состояния безопасности	4
3.	Управление Активами	5
4.	Регистрация Инцидентов	6
5.	Регистрация Уязвимости	8
6.	Регистрация Уязвимости по результатам сканирования	9
7.	Регистрация Задач	10
8.	Мониторинг и управление Инцидентами	11
9.	Мониторинг и управление Уязвимостями	14
10.	Мониторинг и управление Задачами	16
11.	Панель стандартизованных диаграмм	17
12.	Аналитическая панель диаграмм	19
13.	Аналитическая панель отчетов	20
Интег	рация со сторонними системами	21
1.	Коннектор для передачи инцидентов в АСОИ ФинЦЕРТ	21
2.	Коннектор с RuSIEM	22
3.	Коннектор с Positive Technologies MaxPatrol SIEM	22
4.	Коннектор для DLP InfoWatch Traffic Monitor	22

Введение

Автоматизированная система управления безопасностью «SecurityDesk» представляет собой WEBприложение, поэтому для работы с системой достаточно иметь персональный компьютер с установленным браузером Google Chrome, Microsoft Edge.

Принятые сокращения и определения

Инцидент	-	Любое непредвиденное или нежелательное событие, которое
		может нарушить деятельность или требуемое состояние
		безопасности актива, 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
		управления безопасностью 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 него 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 субъекты, которые могут служить
		источником или объектом воздействия событий безопасности.

Основные объекты системы

Деятельность подразделений, обеспечивающих безопасность компании в основном основана на обнаружении инцидентов, проведении анализа причин их возникновения, а также выработки мер по их дальнейшему предотвращению. Основным объектом управления безопасностью в Системе является **Инцидент**.

Инциденты классифицируются по категории безопасности (в базовом варианте установки Система включает в себя три категории безопасности: информационная, физическая или экономическая, но набор категорий может быть легко расширен Администратором Системы), по критичности, месту возникновения (подразделению), кроме того **Инцидент** классифицируется по качественной и количественной оценке ущерба.

Тем не мене управление безопасностью не может осуществляться с помощью одних только инцидентов, необходимо выявлять уязвимости, планировать и осуществлять работы направленные на снижение возможности возникновения инцидентов, а также работы по разбору произошедших инцидентов, профилактике возникновения их в будущем. Управление работами реализуется с помощью функционала объекта - **Задача**. С помощью **Задач** планируются планово-

предупредительные профилактические мероприятия, а также работы, проводимые в рамках выявленных инцидентов или уязвимостей.

Схематично взаимосвязь Инцидентов, Задач и Уязвимостей представлена на рисунке - Рисунок 1. Как изображено на рисунке может существовать множество Задач в рамках одного Инцидента или Уязвимости. Функционал Системы также позволяет работать с Инцидентами и Уязвимостями без создания Задач, если они не требуются. Уязвимость в свою очередь может быть связана с Инцидентами, а также Задачами. Задачи делятся на четыре типа: по инциденту (доступны только в рамках инцидента), по уязвимости (доступны только в рамках уязвимости), плановые и внеплановые.



Рисунок 1. Взаимосвязь объектов системы типа Инцидентов и Задача.

Стадии жизненного цикла **Инцидентов, Уязвимостей** и **Задач** задаются администратором системы с помощью редактора схемы рабочих процедур, пояснения и возможные переходы между типовыми состояниями отображены в таблице - Таблица 1.

Состояние	Возможные	Пояснение
	переходы	
Зарегистрировано	В работе	Начальное состояние объекта, работы на данном
		этапе не выполняются
В работе	Выполнено,	В данном состоянии выполняются основные
	Отменено	работы по объекту Системы
Выполнено	Закрыто, В работе	Все работы завершены, но возможно перевести в
	Отменено	статус «Отменено» или вернуть «В работу» объект,
		в случае необходимости
Закрыто	Переход невозможен	Объект закрыт для редактирования, изменение
		невозможно
Отменено	Переход невозможен	Объект закрыт для редактирования, проведение
		работы отменено

Таблица 1. Стадии жизненного цикла типовой схемы для Инцидентов, Уязвимостей и Задач.

В случае создания Задач с привязкой к Инциденту или Уязвимости состояние Инцидента или Уязвимости устанавливается системой в состояние Закрыто, в случае установки всех связанных Задач переходят в состояние Закрыто, т.е. состояние Инцидента или Уязвимости будет определяться состоянием связанными Задачами.

Переход в архивное состояние **Закрыто** из состояния **Выполнено** может переводиться Системой автоматически с помощью заданных настроек, период ожидания до перевода Системой в состояние **Закрыто** устанавливается в настройках, в разделе «**Администрирование**».

Работа пользователя в системе

1. Вход в систему

Для входа в Систему откройте в браузере ссылку на вход в Систему, которую предоставит вам Администратор. В открывшемся окне браузера - Рисунок 2 выберите в поле домен подключение, через которое вы будете проходить аутентификацию или оставьте локальную, если входите под локальной учетной записью.

Secu	irity	Des	k
------	-------	-----	---

~

Рисунок 2. Окно входа пользователя в Систему.

2. Главная панель мониторинга состояния безопасности

После прохождения процедуры аутентификации пользователю открывается «Главная панель мониторинга», предназначенная для отображения актуальных событий безопасности – незавершенных Инцидентов, существующих Уязвимостях и назначенных пользователю Задач – Рисунок 3.

Отображение информации на главной панели мониторинга зависит от уровня привилегий пользователя:

- В случае минимальных привилегий пользователю отображаются только зарегистрированные не него **Инциденты** или назначенные ему **Задачи**.
- Уязвимости отображаются независимо от уровня доступа пользователя.
- В случае вхождения пользователя в привилегированные группы (встроенные профили с полным доступом, администраторы) Система будет отображать информацию по всем Инцидентам и Задачам за указанный период.

SecurityDe	esk ®Главная ≜Мониторинг≁ ⊘Регистра	рия + :≣Активы + ⊙Ана.							тепь 💄 admin 🔂 🔂 Бър
ы Инц	иденты	🗲 Уязвимости		ଙ	Задачи		ШАктив	ы	
Bcero a	активных: 164	Всего активных:		11 B	сего активных:		Всего име	ется:	
	рированные: 161	Зарегистрированные:		9 3a			Компьютерь		
В работе Выполне		В работе: Выполненные:		2 B 0 Bt	работе: «полненные:		Персонал:		
		Инциденты заре	гистрированные	е за последние 10 дней	для пользователя '	С полным доступом			
Номер	Наименование	Категория	Уровень	Состояние	Подразделение	Владелец	Дата регистрации	Дата обнаружения	Дата возникновения
2274	Вирусное заражение 🖉 🏢	Информационная	Низкий	В работе		admin	18-11-2021 18:21	18-11-2021 18:21	18-11-2021 18:21
2321	Взлом корпоративного сайта 🗲	Информационная	Низкий	Зарегистрировано	Клиент	user	27-11-2021 12:05	27-11-2021 12:05	27-11-2021 12:05
		Уязвимости заре	гистрированны	е за последние 10 дней	для пользователя '	"С полным доступом			
Номер	Наименование	Категория	Уровень	Состояние	Вектор атаки	Владелец	Дата регистрации	Дата обн	аружения
2022	Некорректная цепочка сертификатов 🧮 👌	Информационная	Средний	Зарегистрировано	Удаленная	user	27-11-2021 10:50	13-12-201	9 14:46
2023	Стандартный паропь пользователя SYSDBA 🗮	Информационная	Критический	Зарегистрировано	Удаленная	user	27-11-2021 10:50	13-12-201	9 14:46
2024	XSPIDER ID:7006 Устаревший сертификат 🗹	Информационная	Средний	В работе	Удаленная	user	27-11-2021 10:50	13-12-201	9 14: <mark>4</mark> 6
Страница	а 1 из 3 (Всего элементов: 8) Предыдущая 1 2	3 Следующая							
		Задачи зареги	стрированные з	а последние 10 дней д	пя пользователя "С	полным доступом"			
Номер	Наименование	Категория	Тип задачи	Состояние	Подразделение	Исполнитель	Дата регистрации	Дата начала испо	Срок исполнения
2054	По Инциденту ОБС	ФинЦерт-операция БС	По инциденту	Зарегистрировано	Клиент	admin	23-11-2021 22:52	25-07-2021 15:38	25-07-2021 15:38
2085	Заменить сертификат	Информационная	По уязвимости	Зарегистрировано		admin	28-11-2021 12:59	28-11-2021 12:58	28-11-2021 12:58

Версия для внутреннего некоммерческого использовани Текущая дата: 28.11.2021 12:59.00 Автоматизированная система управления безопасностью SecurityDesk. Все права защищены. Версия 1.34.1

Рисунок 3. Главная панель мониторинга.

Используя на закрепленном вверху меню команд всегда можно вернуться на главную панель нажав в меню ссылку « Оглавная или наименование системы « SecurityDesk ». Также закрепленное меню позволяет перейти к:

- просмотру всех зарегистрированных в системе Инцидентов, Уязвимостей и Задач раздел «Мониторинг»,
- регистрации новых Инцидентов, Уязвимостей и Задач раздел « ^{Орегистрация -} »,
- просмотру стандартизованных диаграмм, аналитических панелей, генерации аналитических отчетов раздел « [©]Аналитика ».

Отображаемые на главной панели цветные блоки



отображают

независимо от временного периода все находящиеся в активном (незакрытом) состоянии Инциденты, Уязвимости и Задачи, назначенные пользователю. Нажатие по блокам приводит к переходу в соответствующий раздел мониторинга Инцидентов, Уязвимостей или Задач.

Выведенные под цветными блоками таблицы имеют активные ссылки, нажав на которые открываются отдельные карточки с детальной информацией по интересующему объекту.

3. Управление Активами

📕 Активы -	Отче	
Объекты		
Компьютеры		
Субъекты		
Персонал		»

Для управления активами используется функционал, доступный в меню « 🖵 🖻

В данных разделах возможно создание, изменение информации по вычислительной технике и персоналу. Далее активы доступны для прикрепления в карточках **Инцидентов -** Рисунок 5, **Уязвимостей -** Рисунок 6 и **Задач -** Рисунок 9.

Для того чтобы создать новый, изменить существующий актив выберите из меню соответствующий пункт. После этого откроется форма управления в левой части, которой отображается дерево подразделений, а в правой список доступных активов в данном подразделении – Рисунок 4.

SecurityDesk ФГлавная ФМониторинг - @Регистрация - ШАктивы - (л≢Документация Пользователь: ≜ заяті С•Выход
 ООО Рассвет ▶финиал Владимир 	Создать Изменить Переместить Удалить Жу	онал		ФИО:
 филиал Иваново филиал Ярославль 	Поиск		Q	иванов нетр васильевич
	Полное имя	Логин		Учетная запись:
	Иванов Петр Васильевич	IvanovPV		IvanovPV
				Должность:
				Неопределена
				Подразделение:
				филиал Владимир
				Телефон:
				8495-344-44-331
				Электронная почта:
				lvanov@gmail.com
				Дополнительная информация:
				Принят 21.05.2020
				дата последнего опроса:
				22.08.2020 13:42:02

Рисунок 4. Форма управления Активами.

Для регистрации нового актива, изменения существующего, удаления или перемещения

нажмите на соответствующую кнопку « Создать ». При журнал » отобразится окно с журналом изменения параметров актива. нажатии кнопки « Кнопки управления активами доступны только тем пользователям, которые входят в роль

«ActiveManagers» в Системе.

Для упрощения поиска активов в дереве подразделений у подразделения, в котором находятся активы отображается соответствующая пиктограмма.

Также активы могут автоматически загружаться из каталогов Active Directory или FreeIPA и csv-файлов, например, из системы инвентаризации. Настройку автоматического импорта активов осуществляет Администратор системы.

4. Регистрация Инцидентов

Для регистрации Инцидента в системе необходимо через основное меню выбрать

ØРегистрация -	 Активы -	
Э Инцидента		
4 Уязвимости		
ФСканирования	уязвимостей	
С Задачи		>

регистрацию Инцидента – «

» после чего откроется форма регистрации нового Инцидента – Рисунок 5.

Для регистрации нового Инцидента обязательным полем является поле «Наименование», остальные поля могут заполняться/уточняться, по мере необходимости.

Для оценки ущерба от **Инцидента** доступна количественная и качественная оценка. Качественная оценка осуществляется с помощью справочника системы, который может быть дополнен через административные настройки системы пользователем с уровнем доступа Администратор. Количественная оценка подразумевает экспертный ввод потерь от Инцидента, выраженный в деньгах или иных единицах измерения. В зависимости от методологии, которую вы применяете для количественной оценки потерь от инцидентов, возможен ввод как положительных, так и отрицательных значений, например, Инциденты повлекшие ущерб – положительные, предотвращенные Инциденты – отрицательные (или наоборот).

	Регистрация нового инцидента		
Связать иншидент с активом:	Наименование:		Заггузка файлов по иншиленту:
	Вирусное заражение		
+ добавить источник	Категория безопасности:		+ Выбрать файлы
Источники инцидента:	Информационная	~	Загрузить
X Yganime Ivanov Ivan Ivanovich	Уровень инцидента:		Сохраненные документы:
	Низкий	~	🛱 Veaners, Incident3 docx
+ добавить цель	Дата возникновения:		🖀 Удалить 1099621186387.pdf
Объекты воздействия инцидента:	02-03-2021 23:06	=	
ж удалить рс2	Дата обнаружения:		
X Yganimis petrov petr	02-03-2021 23:06	=	Связать с нормативными документами:
	Подразделение:		
	Клиент	-	+ Досавить
😫 Заполнить по шаблону:	Описание:		Ссылки на нормативные документы:
Спих си цаблонов: Вирусное заражение • Заплотингъ	Заракение ПК подразделения в результате подолочени	n USB неситеря	★ Здачть ТИБ Полнтика информационой безоласности Пункт.6.1 ★ здачть ТИА Полнтика информационной безоласности Пункт.6.4
	Оценка ущерба:		
	Качественная оценка:		
	Финансовые потери	~	
	Количественная оценка:		
	10000	₽	
	Результат:		
	Описанте принятые меры		
	Зарегистрировать		

Рисунок 5. Форма регистрации Инцидента безопасности.

Как показано на рисунке, кроме заполнения данных в полях карточки к Инциденту можно Загрузка файлов по инциденту: прикрепить дополнительные материалы в виде файлов – окно «

Помните! – все загружаемые файлы увеличивают размер базы данных, поэтому для оптимального расходования размера жесткого диска сервера и скорости работы системы прикладывайте только необходимые файлы, а в случае сканированных документов обращайте внимание на настройки сканирующего оборудования и выходной размер сканкопий документов.

Также для полной классификации нарушений регламентных документов по безопасности, в карточке Инцидента присутствует механизм привязки ссылок нормативных документов к

Е Связать с нормативными документами Инциденту окно Заполнение справочника нормативными документами осуществляется через административные настройки Системы пользователем с уровнем доступа Администратор.

Для получения аналитики в разрезе активов прикрепите соответствующие активы – окно

Е Связать инцидент с активом: » с Инцидентом. Для ускорения заполнения информации по типовым инцидентам в карточке присутствует функционал заполнения данных из шаблона. Для 😢 Заполнить по шаблону: » необходимый шаблон и применения шаблона выберите из окна « нажмите кнопку «Заполнить». Создавать, изменять и удалять шаблоны могут пользователи, имеющие роль Администратор системы.

После занесения всех необходимых данных Инцидент сохраняется в Системе по нажатию кнопки

и переходит в начальное состояние «Зарегистрировано».

5. Регистрация Уязвимости

Уязвимости регистрируются в системе аналогично Инцидентам через меню

	⊘Регистрация -	📕 Активы –
	Э Инцидента	
	Уязвимости ▲	×
«	ФСканирования С Задачи	уязвимостен

« Задачи ». Для регистрации новой **Уязвимости** единственным обязательным полем является только поле **«Наименование»**, остальные поля могут заполняться/уточняться, по мере необходимости – Рисунок 6.

Связанные активы:	
X Удалить Иванов Петр Ив	анович
× удалить Петров Иван Ив	анович
🕏 Заполнить по шаблону:	
 Заполнить по шаблону: Список шаблонов: 	

Than the Holean Ho	e:	
Стандартны	й пароль пользователя	
Категория без	зопасности:	
Информацио	онная	
Уровень <mark>о</mark> паси	ности:	
Критический	1	
Вектор атаки:		
Удаленная		
Дата обнаруж	ения:	
03-03-2021 0	9:45	=
CVE:		
Введите CVE		
CWE:		
Введите CWE	E	
Описание:		
Результат:		



Рисунок 6. Форма регистрации Уязвимости.

Как показано на рисунке, кроме самих данных уязвимости к карточке можно прикрепить

дополнительные материалы в виде файлов – окно «

Помните! — все загружаемые файлы увеличивают размер базы данных, поэтому для оптимального расходования размера жесткого диска сервера и скорости работы системы прикладывайте только необходимые файлы, а в случае сканированных документов обращайте внимание на настройки сканирующего оборудования и выходной размер сканов документов.

Кроме ввода информации по Уязвимости, также возможно установить ее связь с Инцидентами, зарегистрированными в Системе, список которых можно вызвать через

кнопку « Добавить » в окне « Связать с инцидентами: ». В окне выбора инцидентов будут отображаться только те инциденты, которые пользователю позволяет его уровень доступа. Для получения аналитики в разрезе активов прикрепите соответствующие активы – окно

« Ваполнить по шаблоны могут пользователи, имеющие роль Администратор системы. Для ускорения заполнения информации по типовым уязвимостям в карточке присутствует функционал заполнения данных из шаблона. Для применения шаблона выберите из окна « Заполнить по шаблону: » необходимый шаблон и нажмите кнопку «Заполнить». Создавать, изменять и удалять шаблоны могут пользователи, имеющие роль Администратор системы. После занесения всех необходимых данных Уязвимость сохраняется в системе по нажатию

кнопки Зарегистрировать и переходит в начальное состояние «Зарегистрировано».

6. Регистрация Уязвимости по результатам сканирования

В Системе доступна регистрация Уязвимостей на основе результатов сканирования, выполненных с помощью специализированных сканеров проверки защищенности. В настоящий момент присутствует возможность загружать результаты сканирования в виде файлов и создавать на их основе карточки уязвимости. Для перехода к регистрации уязвимостей перейдите в меню **Регистрация** и соответственно **Сканирования уязвимостей**

⊘Регистрация -	Нактивы ◄
ы Инцидента	
ФСканирования	уязвимостей

. Как показано на рисунке - Рисунок 7 в левой части формы загрузки выполняются следующие настройки:

- Тип сканера уязвимости;
- Уровни уязвимости данная настройка позволяет загружать только необходимые уровни, что упрощает работу со списком обнаруженных уязвимостей;
- Установка связей с активами данная настройка позволяет автоматически связывать активы-компьютеры, содержащиеся в базе Системы с компьютерами, на которых были обнаружены уязвимости. Настройка позволяет связывать по имени компьютера или по IP-адресу при помощи выпадающего списка.

Для загрузки журнала сканирования нажмите сначала кнопку «

», а затем

кнопку «^{Загрузить}». После загрузки файла на сервер будет проведена проверка корректности его формата, и в случае успеха на левой части формы отобразится список найденных уязвимостей.

SecurityDesk ФГлавная ФМониторинг- ФРегистра	ия + ⊞Активы + ⊘Ан	алитика - Фдранинстриров	nnie +	🕫 Документация Пользователь: 💄 sdmin	С•Выход
Загрузка результатов сканирова	ния на уязвим	ости			
Настройки загрузки:	Зарегистрировать	Поиск			۹
Тип сканера:	Действие	Наименование	Уровень	Описание уязвимости	-
XSpider 👻	Зарегистрироват	Анонимный доступ	Средний	Возможен анонимный доступ к FTP-серверу. При определенных условиях это может привести к потере данных.	
Обрабатывать уровни уязвимостей: П Низкий 🗹 Средний 💆 Высокий 🗹 Критический	Зарегистрироват	стандартный пароль пользователя SYSDBA	Критический	Пользователь 'SYSDBA' имеет стандарлный пароль 'masterkey'.	
Связь с активами:	Зарегистрироват	Учетная запись	Высокий	Найдена учетная запись.	
Устанавливать	2	Разглашение	Средний	Зпоумышленники могут получить конфиденциальную информацию, не проходя авторизацию, с помощью запроса NULL BASE	
По IP-адресу и имени 🗸	Saperine (pulpoda)	информации		Обратите внимание, что NULL BASE запрос необходим для корректной работы некоторых приложений. Например, в 3 версии протокола LDAP запрос используется для получение поддерживаемых сервером типое аутентификции и другой служебной информации:	
Категория безопасности: Информационная -	Зарегистрироват	ть Небезопасный протокол SSL 2.0	Средний	по-ролиции. Протокол SSL версии 2.0 является слабо защищенным, использовать его не рекомендуется. Злоумышленник может провести атаку человек-посередине", чтобы перехватить SSL-пакеты и за короткий промежуток времени расшифровать защищенные	
Действия по загрузке: + Выбрать файл Загрузить				данные, клюрые когут содераль конфоденциалиро информацию. Почико этото, злоукашиенных консе без трада ксазалть иля подменть передавание, данные, прат отие нарушие ворсстисться сессок. Экакисьтся существет а протохов 65.4/2 для Сорект51, из-за отправая содерерои сообщения Белечбеній до провери наличия у илиента определенных назацифодаваных данных. Так и сложитарии данной узакисисти позологат эпохимитенных дана. Констрания дана и сложители позологат эпохимитенных закиствето расшифодовать, данные, закимфорованные с использованием ПОЗИ ("Долимитенных данной узакимитенных распестрания узакимите така и всехота на и сложители водокать с использованием ПОЗИ ("Долимитенных данной узакимитенных ПОЗИ") Пелемберовара, данные, закимформанные с использованием ПОЗИ ("Долимитенных данных узакимитенных распестрания узакимите така и всехота по данных водоку ("Долимитенных данной узакимитенных ПОЗИ") Пелемберовара, данные узакимите така и всехота по данная то познота то познотат эпохотельной така.	b

Рисунок 7. Форма регистрации Уязвимостей на основе результатов сканирования.

Для списка загруженных уязвимостей доступны следующие элементы управления – кнопка « Создать все », нажав на которую в Системе будут созданы карточки по всем обнаруженным уязвимостям и кнопка « Создать » напротив каждой уязвимости, позволяющая выборочно регистрировать только необходимые уязвимости.

7. Регистрация Задач

Задачи регистрируются в системе двумя способами:



- С помощью основного меню Задачи необходимо выбрать регистрацию
 Задачи. Для такого способа регистрации существует возможность создать задачу 2х типов: плановую и внеплановую.
- С помощью кнопки ^{Создать задачу} в карточке **Инцидента** или **Уязвимости** (Рисунок 8). В данном случае создается **Задача**, привязанная к **Инциденту** или **Уязвимости**, из карточки которой она создавалась.

Security		Информация по инциденту: №9198 INC-						ия Пользоват		
() 3a	регистрированные инциде	Выполнить Отменить Создать	задачу Редактирова	ть Создать копию Удалить	Перезапустить • 📄 Отч	ет				٦
Введ	ите текст для поиска инцидентов	Основная информация Дополнит	гельные параметры	Уязвимости Задачи Активы	Файлы Нормативны	е документы Журнал работ Журнал изменени	R			
		Категория безопасности:		Уровень инцидента:		Состояние:				
Пока	зать закрытые: 📕 Только мои:	PTSIEM-test		Низкий		В работе	+			
		Подразделение:				Владелец:		_		
Номер	Наименование	PTSIEMdep				admin	1	а обнаружения	Дата возникнове	
T							-	٣	T	
26303	Инцидент ОБС [RRN - 16071] 5	Дата возникновения:		Дата обнаружения:		Дата завершения:		04.2023 2:31:00	20.04.2023 1:49:00	-
26302	Инцидент ОБС [RRN - 16070] С	09-03-2024 19:00	=	18-03-2024 19:25				06.2024 23:44:00	25.06.2024 22:20:00	
26301	Инцидент ОБС [RRN - 16069] X	Описание:						04.2023 15:25:00	21.04.2023 14:54:00	
26300	Инцидент ОБС [RRN - 16068] С.	Вирусное заражение серверов						03.2023 10:40:00	06.03.2023 9:36:00	
26299	Инцидент ОБС [RRN - 16067] В							03.2023 20:38:00	30.03.2023 17:07:00	
26298	Инцидент ОБС [RRN - 16066] КС							04.2023 18:15:00	05.04.2023 3:29:00	
26297	Инцидент ОБС [RRN - 16065] Б							04.2023 2:31:00	20.04.2023 1:49:00	
26296	Инцидент ОБС [RRN - 16064] П.							04.2023 16:38:00	18.04.2023 10:50:00	
26295	Инцидент ОБС [RRN - 16063] Б							04.2023 17:18:00	06.04.2023 16:42:00	
26294	Инцидент ОБС [RRN - 16062] С.						1.	04.2023 15:44:00	15.04.2023 15:31:00	
9203	test1333 📰	Результат обработки:						03.2024 14:43:00	26.03.2024 14:43:00	
9202	test123 📰	Описание отсутствует						03.2024 12:30:00	22.03.2024 12:30:00	
9200	Инцидент социальной инженери							03.2024 11:54:00	21.03.2024 11:54:00	
9198	INC-2 Вирусное заражение Ø 🔳						le	03.2024 19:25:05	09.03.2024 19:00:00	¥
Страница	а 67 из 67 (Всего элементов: 1338	Оценка ущерба: Качественная:				Количественная:		Элементов на с	странице: 20 👻	
		Финансовые потери				0	₽			
Версия д Текущая	ля внутреннего некоммерческого дата: 24.11.2024 12:31:00							опасностью Sec	urityDesk.	

Рисунок 8. Карточка просмотра Инцидента.

Количество привязанных к инциденту или уязвимости Задач не лимитировано, т.е. может создаваться в любом количестве.

Карточка создания Задачи - Рисунок 9 имеет более простую форму заполнения по сравнению с Инцидентом или Уязвимостью. Для регистрации новой Задачи единственным обязательным полем является только поле «Наименование», остальные поля могут заполняться/уточняться, по мере необходимости.

and the second second	авить		
Связанны	ые активы:		
🗙 Удр	anim Servi	fail	
😫 Заполн	нить по шаб		
Список ш	заблонов:		

Наименование:	
Провести проверку настроек	
Категория безопасности:	
Информационная	
Тип задачи:	
Плановая	
Дата начала исполнения:	
04-03-2021 01:27	
Срок исполнения:	
04-03-2021 01:27	=
Исполнитель:	
admin	
Подразделение:	
OOO HTTK	-
Описание:	
Провести проведку настроек почтового сервера в соответст стандарта ИБ	вии с требованиями
Результат:	
Опишите принятые меры	



Рисунок 9. Форма регистрации Задачи.

Как показано на рисунке, кроме ввода данных к Задаче можно прикрепить дополнительные

материалы в виде файлов – окно « », а также связать задачу с активами

— ОКНО «

Помните! — все загружаемые файлы увеличивают размер базы данных, поэтому для оптимального расходования размера жесткого диска сервера и скорости работы системы прикладывайте только необходимые файлы, а в случае сканированных документов обращайте внимание на настройки сканирующего оборудования и выходной размер сканов документов. Для ускорения заполнения информации по типовым задачам в карточке присутствует функционал заполнения данных по шаблону. Для применения шаблона

выберите из окна « ^{В Заполнить по шаблону:} » необходимый шаблон задачи и нажмите кнопку «Заполнить». Создавать, изменять и удалять шаблоны могут пользователи, имеющие роль Администратор системы.

После занесения всех необходимых данных **Задача** сохраняется в системе по нажатию кнопки ^{Зарегистрировать} и переходит в начальное состояние «Зарегистрировано».

8. Мониторинг и управление Инцидентами

▲Мониторинг -	0
Э Инцидентов	
4 Уязвимостей	
С Задач	

Для просмотра всех зарегистрированных Инцидентов в основном меню

необходимо выбрать соответственно мониторинг **Инцидентов**, в результате чего откроется форма просмотра списка **Инцидентов**, доступных пользователю — Рисунок 10. Форма позволяет осуществлять полнотекстовый поиск инцидентов, по ключевым словам, содержащимся:

- в карточке инцидентов и их дополнительных параметрах;
- связанных с инцидентами активах;

- связанных с инцидентами нормативных документах;
- связанных с инцидентами задачах и их дополнительных параметрах.

Для поиска по слову необходимо ввести его в поле поиска и нажать кнопку «Поиск». Для поиска инцидента по маске слова используйте знак * и двойные кавычки (например, "Безопасн*"). Также возможно осуществлять поиск по фразе, заключая ее слова в двойные кавычки. Допускается поиск по нескольким словам с использованием ключевых слов AND, OR и NOT. Возможно применение фильтров, расположенных над столбцами для большего удобства работы. Все незавершенные **Инциденты** подсвечиваются жирным шрифтом. Наличие связей с задачами, уязвимостями и документами отображаются соответствующими пиктограммами.

SecurityDesk Ф/павная Амониторинг- ОРегистрация- ШАлтивы-	©Аналитика +									<i>≢</i> Документация	Пользовате	16: Luser	С•Выход
Э Зарегистрированные инциденты "для пользователя "user"" Введите текст для поиска инцидентов									0	. Поиск			
Показать закрытые: 📕 Только мои: 🧹 Период регистрации: Задать	🗸 Дата	начал	na: 22-11-2021 00:00		Дата окончания: 28-11-	-2021	00:00	=					
Номер Наименование	Уровень		Категория	с	Состояние	Вла,	делец	Подразде	пение	Дата регистра	Дата обнаруже	Дата воз	никно
T		T	T		T		۲		۲	T		T	۲
2321 Валом корпоративного саита 🕈	Низкии		Информационная	3	Зарегистрировано	user	r	Клиент		27.11.2021 12:0	27.11.2021 12:0	27.11.202	1 12:0
Страница 1 из 1 (Всего элементов: 1) Предыдущая 1 Следующая										э	пементов на стра	нице: 20	•

Рисунок 10. Форма просмотра зарегистрированных инцидентов в системе.

Для вызова детальной информации по **Инциденту**, изменения его состояния, а также перехода в редактирование содержащейся в нем информации необходимо перейти по ссылке поля «Наименование», после чего откроется карточка инцидента – Рисунок 11.

SecurityDesk Фглавная &Мон	Информация по инциденту. №9198 INC-2 Вирусное заражение			×	ия Пользоват	
Эарегистрированные инцида	Выполнить Отменить Создать задаму Редактиров	ать Создать колию Удалить Перезапустить •	Отчет			
Введите текст для поиска инцидентов	Основная информация Дополнительные параметры	Уязвимости Задачи Активы Файлы Нормат	изные документы Журнал работ Журнал изменения			
	Категория безопасности:	Уровень инцидента:	Состояние:			
Показать закрытые: 🔳 Только мои	PTSIEM-test	Низкий	В работе	+		
	Подразделение:		Владелец:			
Номер Наименование	PTSIEMdep		admin	1	а обнаружения	Дата возникнове
T		a 19	-	-	٣	T
26303 Инцидент ОБС [RRN - 16071] Б	Дата возникновения:	Дата обнаружения:	Дата завершения:		4.2023 2:31:00	20.04.2023 1:49:00
26302 Инцидент ОБС [RRN - 16070] С	09-03-2024 19:00	18-03-2024 19:25		-	06.2024 23:44:00	25.06.2024 22:20:00
26301 Инцидент ОБС [RRN - 16069] X	Описание:				04.2023 15:25:00	21.04.2023 14:54:00
26300 Инцидент ОБС [RRN - 16068] С	Вирусное заражение серверов				33.2023 10:40:00	06.03.2023 9:36:00
26299 Инцидент ОБС [RRN - 16067] В					33.2023 20:38:00	30.03.2023 17:07:00
26298 Инцидент ОБС [RRN - 16066] К					04.2023 18:15:00	05.04.2023 3:29:00
26297 Инцидент ОБС [RRN - 16065] E					04.2023 2:31:00	20.04.2023 1:49:00
26296 Инцидент ОБС [RRN - 16064] П					4.2023 16:38:00	18.04.2023 10:50:00
26295 Инцидент ОБС [RRN - 16063] E					04.2023 17:18:00	06.04.2023 16:42:00
26294 Инцидент ОБС [RRN - 16062] С				1.	04.2023 15:44:00	15.04.2023 15:31:00
9203 test1333 🔚	Результат обработки:				03.2024 14:43:00	26.03.2024 14:43:00
9202 test123 🗮	Описание отсутствует				3.2024 12:30:00	22.03.2024 12:30:00
9200 Инцидент социальной инженери					03.2024 11:54:00	21.03.2024 11:54:00
9198 INC-2 Вирусное заражение 🖉				11	03.2024 19:25:05	09.03.2024 19:00.00 👻
Crosumus C7 us C7 (Repro sequentos 1930	Оценка ущерба:				Onauton un d	20 -
Crpaninga of ita of (acero anementos, race	Качественная:		Количественная:		Shementoo na c	ipaninge. 20
	Финансовые потери		0	₽		
Версия для внутреннего некоммерческого Текущая дата: 24.11.2024 12.31.00					опасностью Seci	urityDesk.

Рисунок 11. Карточка просмотра Инцидента.

Карточка **Инцидента** имеет несколько вкладок. На первой вкладке выведена основная информация, состояние, качественная и количественная оценка ущерба, а также панель



связанных с Инцидентом Уязвимостей и Задач с их текущим состоянием, ссылки на нормативные документы, а также журнал изменения информации в карточке Инцидента. Кнопки изменения состояния Инцидента выводятся системой в соответствии со схемой

рабочей процедуры инцидента данной категории безопасности. По кнопке из карточки инцидента Система сформирует отчет в формате MS Word – Рисунок 12. В отчет автоматически добавляется вся информация из карточки инцидента, а также связанных с ним активов, задач, пунктов нормативных документов.

		Отчет по	ИНЦИДЕНТУ	
Инцидент М	191			
"Взлом поч	товой систе	емы"		
Владелец: ad Состояние: За	min (Главный арегистриров	і пользователь си ано	стемы, пароль по	умолчанию 123456)
Параметры и Категория бе: Уровень: Выс Подразделен I Временные г Дата возникн Дата обнаруж Дата заверше Общее описа Взлом почтов Результат обј Оценка ущер	нцидента: зопасности: И окий нараметры: нараметры: овения: 22-08-2 ения: ения: эения: ого сервера н работки: оба:	Інформационная ладимир 8-2020 14:11 2020 14:11 компании.		
Количественн	ная:100000			
Направление	Тип	Наименование	Подразделение	Дополнительная информация
Источник	Персонал	Иванов Петр Васильевич	филиал Владимир	Login=IvanovPV, Должность=Heonpedeneta E-mail=ivanov@gmail.com, Телефон=8495-344-44-331, Дополнительная информация=Принят 21.05.2020

Рисунок 12. Сформированный отчет по инциденту.

При нажатии кнопки Редактировать Инцидент переводится в режим редактирования, форма режима которого полностью идентична форме регистрации инцидента - Рисунок 5. Данная возможность доступна пользователю только в состояниях **«Зарегистрировано»**, **«В работе»**. В состояниях **«Выполнено»**, **«Отменено»** и **«Закрыто»** редактирование информации по **Инциденту** блокируется системой.

В случае если **Инцидент** <u>имеет прикрепленные</u> **Задачи,** состояние инцидента в состоянии «**Закрыто**» контролируется состоянием связанных Задач.

Кроме представленных кнопок управления администратору системы доступна дополнительная кнопка удалить, позволяющая полностью удалить Инцидент из Системы и

кнопка (перезапустить), которая позволяет перезапустить текущую рабочую процедуру привязанную к инциденту или выполнить перезапуск по новой процедуре введенной в работу администратором - Рисунок 11.

9. Мониторинг и управление Уязвимостями

Мониторинг **У**Инцидентов Уязвимостей **С**Залач

Для просмотра всех зарегистрированных Уязвимостей в основном меню

необходимо выбрать соответственно мониторинг **Уязвимостей**, после чего откроется форма просмотра списка **Уязвимостей** – Рисунок 13. Форма позволяет осуществлять полнотекстовый поиск уязвимостей, по ключевым словам, содержащимся:

- в карточках уязвимостей и их дополнительных параметрах;
- связанных с уязвимостями активах;
- связанных с уязвимостями задачах и их дополнительных параметрах.

Для поиска по слову необходимо ввести его в поле поиска и нажать кнопку «Поиск». Для поиска инцидента по маске слова используйте знак * и двойные кавычки (например, "Безопасн*"). Также возможно осуществлять поиск по фразе, заключая ее слова в двойные кавычки. Допускается поиск по нескольким словам с использованием ключевых слов AND, OR и NOT. Возможно применение фильтров, расположенных над столбцами для большего удобства работы. Все актуальные **Уязвимости** - не находящиеся в состоянии «**Завершено**» или «**Отменено**» выделяются жирным шрифтом. Наличие связей с задачами, инцидентами, активами и документами отображаются соответствующими пиктограммами.

Mep	Наименование	Категория		Уровень	Вектор атаки	Состовние		Владелец	Лата регистрации		Дата обнаружения		Дата устранения
T	T		T	T		T T	T	T		T		T	
2013	XSPIDER ID:7006 Устаревший сертифи.	Информационная		Средний	Удаленная	Отменено		user	23.11.2021 23:02:57		13.12.2019 14:46:00		
2022	Некорректная цепочка сертификато	Информационная		Средний	Удаленная	Зарегистрировано		user	27.11.2021 10:50:27		13.12.2019 14:46:00		
2023	Стандартный пароль пользователя	Информационная		Критический	Удаленная	Зарегистрировано		user	27.11.2021 10:50:31		13.12.2019 14:46:00		
2024	XSPIDER ID:7006 Устаревший сертифи	Информационная		Средний	Удаленная	В работе		user	27.11.2021 10:50:34		13.12.2019 14:46:00		27.11.2021 11:41:20
2025	XSPIDER ID:183502 Выполнение про	Информационная		Высокий	Удаленная	Зарегистрировано		user	27.11.2021 10:50:38		13.12.2019 14:46:09		
2026	XSPIDER ID:186095 Отказ в обслужи	Информационная		Критический	Удаленная	Зарегистрировано		user	27.11.2021 10:50:43		13.12.2019 14:46:09		
2027	XSPIDER ID:185771 Разглашение ин	Информационная		Критический	Удаленная	Зарегистрировано		user	27.11.2021 10:50:46		13.12.2019 14:46:09		
2031	XSPIDER ID:8350 Перечисление поль	Информационная		Средний	Удаленная	Зарегистрировано		user	27.11.2021 11:54:42		27.11.2021 11:54:00		
2032	XSPIDER ID:8350 Перечисление поль	Информационная		Средний	Удаленная	Зарегистрировано		user	27.11.2021 12:05:29		27.11.2021 12:05:00		

Рисунок 13. Форма просмотра зарегистрированных Уязвимостей.

Для вызова детальной информации по **Уязвимости**, изменения ее состояния, а также редактирования содержащейся в ней информации необходимо перейти по ссылке в поле «Наименование», в результате чего откроется карточка уязвимости – Рисунок 14.

Security	rDesk ®Главная ≜Мони	Информация по уязвимости: №1135 XSPIDER ID:175100	Переполнение буфера в стеке.			×	рия Пользоват	eris Ladmin 🕞 Barcoa
4 3a	регистрированные Уязвим	В работу Создать задачу Редактировать Си	оздать копию Удалить Перезапуст	ить -				
Веед	ите текст для поиска уязвимостей	Основная информация Дополнительные парамет	ры Инциденты Задачи Акти	зы Файлы Журнал раб	бот Журнал изменения			
		Категория безопасности:	Уровень опасности:		Состояние:			
	зать закрытые: 🗸 🛛 Только мон	Информационная	Критический		Зарегистрировано	+		
		Вектор атаки:			Владелец:			
Номер	Наименование	Удаленная			admin	1	а обнаружения	Дата устранения
T		Data of Hadilyaning					τ	τ.
1143	еуые1	02 04 2019 17:50	20 10 2024 19 17	=	Auto suseptionna.	=	11.2024 21:47:00	
1141	Рекомендации ФСТЭК России	03-04-2013 17:30	20-10-2024 15.17	-			11.2024 21:38:00	
1140	XSPIDER ID:182362 Использов	CVE:	BDU:		CWE:		04.2019 17:50:05	
1138	XSPIDER ID: 186963 Неподдержи	CVE-2010-4221					04.2019 17:50:05	20.10.2024 19:38:31
1136	XSPIDER ID: 182362 Использова	Описание:					04.2019 17:50:05	20.10.2024 19:23:54
1135	XSPIDER ID:175100 Переполне	Описание: Переполнение буфера в стеке в функции рг	netio_telnet_gets s netio.c s ProFTPD nos	воляет злоумышленникам, дей	ствующим удаленно, выполнить произвольный код,		04.2019 17:50:05	
1133	XSPIDER ID:1079 Учетная запи	используя escape-последовательность TELNET IAC на	FTP- или FTPS-сервере.				04.2019 17:50:05	
1132	XSPIDER ID:1271 Небезопасны	как исправить: для устранения уязвимости неооходим получить по адресу:	о установить последнюю версию продукта	а, соответствующую используе	мои платформе: неооходимую информацию можно	- 1	04.2019 17:50:05	
1131	XSPIDER ID:1024 Анонимный д	http://www.proftpd.org/	4500			- 1	04.2019 17:50:05	
1130	XSPIDER ID:412922 Уязвимость	CCBINK, BID (44062). http://www.securityiocus.com/bid/44	4002				04.2019 17:50:05	20.10.2024 19:24:02
1129	XSPIDER ID 187121 OTKas & offer	Базовая оценка: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C) Лата публикации: 2010-11-09					04.2019 17:50:05	20.10.2024 19.24.07
1128	XSPIDER ID:187093 Выполнени					4	04.2019 17:50:05	
1127	XSPIDER ID:186963 Henoggepa	Результат обработки:					04.2019 17:50:05	
1126	X SPIDER ID:186095 OTKas B 060	Описание отсутствует					04.2019 17:50:05	
Страница	а 1 из 7 (Всего элементов: 132)	Concerne of Charges					Элементов на о	транице: 20 👻
Версия д Текущая,	пя внутреннего некоммерческого дата: 24.11.2024.12.38.37					11	иопасностью Sec	urityDesk.

Рисунок 14. Карточка Уязвимости.

Карточка **Уязвимости** имеет несколько вкладок. На первой вкладке выведена основная информация, а также панель управления состоянием **Уязвимости** и созданием

подчиненных Задач В работу Создать задачу Редактировать Создать копию. Остальные вкладки содержат перечень связанных с Уязвимостью Инцидентов и Задач с их текущим состоянием, описание результата обработки Уязвимости, а также журнал изменения информации в карточке Уязвимости. Кнопки изменения состояния Уязвимости выводятся

системой в соответствии со схемой рабочей процедуры. По кнопке уязвимости Система сформирует отчет в формате MS Word аналогичный отчету по инциденту – Рисунок 12. В отчет автоматически добавляется вся информация из карточки уязвимости, а также связанных с ней Инцидентов, Активов, Задач.

При нажатии кнопку **Уязвимость** переводится в режим редактирования, форма режима которого полностью идентична форме регистрации уязвимости - Рисунок 6. Возможность редактирования доступна пользователю только в состояниях «Зарегистрировано», «В работе» и т.п., а в состояниях «Выполнено», «Отменено» и «Закрыто» редактирование информации по Инциденту будет заблокировано системой.

В случае если **Уязвимость** <u>имеет прикрепленные</u> **Задачи,** состояние ее будет контролироваться состоянием прикрепленных **Задач**. При переходе всех связанных задач в состояние «**Закрыто**», уязвимость также будет переведена в состояние «**Закрыто**».

Связанные с Уязвимостью Инциденты своим состоянием не определяют состояние Уязвимости, равно, как и Уязвимость не определяет своим состоянием состояние связанных Инцидентов.

Кроме представленных на рисунке кнопок управления администратору системы доступна

дополнительная кнопка Удалить, позволяющая полностью удалить Уязвимость из Системы

и кнопка Перезапустить, которая позволяет перезапустить текущую рабочую процедуру, привязанную к уязвимости или выполнить перезапуск по новой процедуре, введенной в работу администратором.

10. Мониторинг и управление Задачами

Для просмотра всех зарегистрированных Задач в системе выберите в основном меню



соответственно мониторинг **Задач**, в результате чего откроется форма просмотра **Задач**, назначенных пользователю – Рисунок 15.

мер Наименование		Категория	Тип задачи	Состояние	Исполнитель	Подразделение	Дата регистр	Дата начала	Срок исполне	Дата испол
T	T	T	τ 🗌	۲		T T	7	•	T	
2049 Установка обновлений 🔚		Информационная	Плановая	Зарегистриро	admin	Москва	07.11.2021 19:	07.11.2021 19:	07.11.2021 19:	
2050 Теst внеплановая		Информационная	Внеплановая	Зарегистриро	admin	Московская о	07.11.2021 19:	07.11.2021 19:	07.11.2021 19:	
2052 По уязвимости Выполнить работы по устранению уязвимости		Информационная	По уязвимости	Зарегистриро	admin	Москва	07.11.2021 23:	07.11.2021 23:	09.11.2021 23:	
2053 ФинЦерт ОБС		ФинЦерт-операция БС ФЛ Карт	По уязвимости	Зарегистриро	suser	Клиент	07.11.2021 23:	07.11.2021 23:	09.11.2021 23:	
2054 По Инциденту ОБС		ФинЦерт-операция БС ФЛ Карт	По инциденту	Зарегистриро	admin	Клиент	23.11.2021 22:	25.07.2021 15:	25.07.2021 15:	
2085 Заменить сертификат		Информационная	По уязвимости	Зарегистриро	admin		28.11.2021 12:	28.11.2021 12:	28.11.2021 12:	
Заменить сертификат		Информационная	По уязвимости	Зарегистриро	admin		28.11.2021 12:	28.11.2021 12:	28.11.2021 12:	

Рисунок 15. Форма просмотра зарегистрированных Задач в системе.

Форма позволяет осуществлять полнотекстовый поиск в задачах по ключевым словам содержащимся:

- в карточках задач и их дополнительных параметрах;
- связанных с задачами активах.

Для поиска по слову необходимо ввести его в поле поиска и нажать кнопку «Поиск». Для поиска задаче по маске слова используйте знак * и двойные кавычки (например, "Безопасн*"). Также возможно осуществлять поиск по фразе, заключая ее слова в двойные кавычки. Допускается поиск по нескольким словам с использованием ключевых слов AND, OR и NOT. Возможно применение фильтров, расположенных над столбцами для большего удобства работы. Все незавершенные **Задачи** подсвечиваются системой жирным шрифтом. Наличие связей с инцидентами, уязвимостями и документами отображаются соответствующими пиктограммами. Для вызова детальной информации по **Задаче**, изменения ее состояния, а также редактирования содержащейся в ней информации необходимо перейти по ссылке в поле «Наименование», после чего откроется карточка **Задачи** – Рисунок 16.

SecurityDesk ФГлавная 🌲	Информация по задаче: №22509 По инциденту № 27645 Ежеди	невный выпуск от SecurityLab.Ru.	×	ация Пользователь: <u>&admin</u> С о Выход
Зарегистрированные Зад Введите текст для поиска задач	В работу Редактировать Создать колино Удалить З ^а Основная информация Дополнительные параметры	Перезапустить - 🖻 Отчет Инциденты Уязвимости Активы Файлы Журні	ал работ Журнал изменения	
	Категория безопасности:	Тип задачи:	Состояние:	
Показать закрытые: 🔳 Только	Мо Информационная	По инциденту	Зарегистрировано 4	
	Подразделение:		Исполнитель:	
Номер Наименование	test1		admin 1	Срок исполне Дата исполнен
т	Дата начала исполнения:	Срок исполнения:	Дата исполнения:	τ τ τ
22516 По Инциденту ОБС [RRN-310	14-11-2024 20:50	14-11-2024 20:50		21.11.2024 21:1 21.11.2024 21:2 🔔
22514 По Инциденту ОБС [RRN-310	513			21.11.2024 21:1 21.11.2024 21:2
22513 По Инциденту ОБС (RRN-310	513 Описание:			21.11.2024 21:1 21.11.2024 21:2
22512 По Инциденту ОБС [RRN-310	Описание отсутствует			21.11.2024 21:1 21.11.2024 21.2
22511 По Инциденту ОБС [RRN-310	513			21.11.2024 21.1 21.11.2024 21.2
22510 test z				17.11.2024 12:4
22509 По инциденту № 27645 Еже,	the state of the s			14.11.2024 20:5
22508 По Инциденту ОБС (RRN-310	512			06.11.2024 23.2 07.11.2024 0:12
22507 По Инциденту ОБС [RRN-310	512			06.11.2024 23:2 10.11.2024 20:1
22506 По Инциденту ОБС (RRN-310	512		li li	06.11.2024 23.2 10.11.2024 20.1
22505 По Инциденту ОБС [RRN-310	Результат обработки:			06.11.2024 23:2 10.11.2024 21:5
22504 По Инциденту ОБС (RRN-310	описание отсутствует			06.11.2024 23.2 10.11.2024 22.0
22503 По Инциденту ОБС [RRN-310	512			06.11.2024 23.2 10.11.2024 22.0
22502 По Инциденту ОБС [RRN-310	512			06.11.2024 23:2 17.11.2024 13:1 👻
Страница 1 из 68 (Всего элементов 1	341			Элементов на странице: 20 -
Версия для внутреннего некоммерчес Текущая дата: 24.11.2024 12.41.42	xon			езопасностью SecurityDesk. ая

Рисунок 16. Карточка задачи.

Карточка Задачи имеет несколько вкладок. На первой вкладке выведена основная информация, состояние. а также панель управления состоянием Задачи Выполнить Отменить Редактировать Создать копию . Остальные вкладки содержат привязанный к Задаче Инцидент или Уязвимость, а также журнал изменения информации в карточке Задачи. Кнопки изменения состояния Задачи выводятся системой в соответствии со схемой

рабочей процедуры. По кнопке формате MS Word аналогичный отчету по инциденту – Рисунок 12. В отчет добавится вся информация из карточки Задачи, а также связанных с ней активов.

При нажатии кнопки Редактировать Задача переводится в режим редактирования, форма которой полностью идентична форме регистрации Задачи - Рисунок 9. Данная возможность доступна пользователю только в состояниях «Зарегистрировано», «В работе», а в состояниях «Выполнено», «Отменено» и «Закрыто» редактирование информации по Задаче блокируется системой.

Кроме представленных на рисунке кнопок управления, Администратору системы доступна

дополнительная кнопка Удалить, позволяющая полностью удалить Задачу из системы и кнопка Перезапустить , которая позволяет перезапустить текущую рабочую процедуру, привязанную к уязвимости или выполнить перезапуск по новой процедуре, введенной в работу администратором.

11. Панель стандартизованных диаграмм

Для просмотра стандартизованных (типовых) аналитических диаграмм и выгрузки зарегистрированных **Инцидентов, Уязвимостей** и **Задач** в формате Microsoft Excel перейдите в основное меню системы по ссылке «Аналитика» - «Стандартизованные» [©]Аналитика-

Диаграммы Стандартизировани

Стандартизированные , после чего откроется страница диаграмм и блок с с настройками и кнопками возможных выгрузок данных в файл – Рисунок 17.

При нажатии на кнопки выгрузки

Инциденты Уязвимости Задачи

информация будет выгружена

пользователю с учетом того уровня привилегий, которые предоставлены ему в рамках его учетной записи.

Графические диаграммы доступны всем пользователям системы в полном объеме, без учета уровня привилегий.



Рисунок 17. Панель диаграмм статистики.

На панели представлены вкладки «Инциденты», «Уязвимости» и «Задачи», отображающие аналитику в различных разрезах по объектам Системы. Вкладка «Анализ рисков» формирует диаграммы по качественному и количественному ущербу от уязвимостей и инцидентов – Рисунок 18.

Вкладка «Активы» - Рисунок 19 предназначена для получения аналитики в разрезе интересуемого актива. Выбрав в левой части дерева подразделение и в средней интересующий актив Система отобразит все Инциденты, Уязвимости и Задачи с которыми он связан.



Рисунок 18. Панель анализа рисков.

ов Петр Васильевич олай Иезинов Васильевич о Петров Сергеевич гей Смирнов Игоревич	Тип Инцидент Уязвимость Инцидент	Номер 2 1	Наименование Приновновение на территорию посторонних XSPIDER ID:10:07 Стандартный пароль попьзователя SYSDBA	Дата 15.07.2020 14:50:00 11.08.2020 15:25:00
нов Петр Васильевич алай Иванов Васильевич о Петров Сергеевич гей Смирнов Игоревич	Инцидент Уязвимость Инцидент	2	Приновновение на территорию посторонних XSPIDER ID:1057 Стандартный пароль пользователя SYSDBA	15.07.2020 14:50:00
р Петров Сергеевич гей Смирнов Игоревич	Инцидент	1		
		*	Валом почтовой системы	22.08.2020 14:11:00

Рисунок 19. Панель анализа в разрезе активов

12. Аналитическая панель диаграмм

Кроме стандартизованных диаграмм возможно создание собственных наборов диаграмм с помощью специального встроенного конструктора, размещая их на аналитических панелях. Для доступа к аналитическим панелям с диаграммами перейдите в меню по ссылке



«Аналитика» - «Аналитические панели» - Аналитические панели, в результате чего откроется форма с доступными пользователю панелями — Рисунок 20. В левой части формы пользователю будет сформирован перечень аналитических панелей, к которым ему предоставил доступ Администратор системы. Режим конструктора диаграмм включается в данном разделе только для пользователей имеющих роль Администратор.



Рисунок 20. Аналитические панели диаграмм.

13. Аналитическая панель отчетов

Для формирования собственных отчетов и вывода их на печать или в файлы различных форматов перейдите в меню по ссылке «Аналитика» - «Аналитические отчеты» -

ОАналитика -
Диаграммы
Стандартизированные
Аналитические панели
Отчеты

<u>Аналитические отчеты</u>, после чего откроется форма с доступными пользователю отчетами -Рисунок 21. В левой части формы пользователю будет сформирован перечень отчетов, к которым ему предоставил доступ Администратор системы. Функционал конструктора отчетов доступен в данном разделе только пользователям, имеющим роль Администратор.

SecurityDesk	©Главная	Монитори	нг∗ ⊘Регистрация∗	Ш Активы -	Фана	титика v						1⁸⁵Документация	Пользователь: 🚨 🛚 🕮 ст	С• Выход
отчеты Инциденты		_	≪ ≪ <u>1se1</u>	• > >	00	Стран	usue • + 🗄 🖶	品間・ス) []					¢
Отчет 0403203								Security	yDesk					Q
						Отчет по и	нцидентам	1						
						Номер	Hanssencesene	Дата начала 18109-0000924500	Дата окончания 19.09200001331419	Количественный умерб 0	Peryanter			
						2	1447	03.08.2020.13.4500	12.09.202013-1400	0	информация отсутствует Разультите/жили			
						10	Increase protocologic as	12.09.202017/2000		5000	информация отсутствуют			
						11	территорию	10.00.00017.5400		100000				
						12	Somer Thint securyarapyer Oday-	11.08.2020 20:30:00	22.10.2020 9:51:45	10000	1800 MT			
						23	улиниется в наршрутнаторах Tenda	17 10 2020 22:5300		100000				
						24	Hammer SOI	18.10.2020 14:30:00	27.10.2020 12:53:30	0	test			
						25	Vanauxeer LST	20.10.2020 20:29:00	24.10.202013:2019	0	Результат не указан			
						26	Hampinger OTH	20.10.2020 20:34:00		0	normorgerence: admin			
						27	Henneser LST 2	22.10.2020 9:52:00	22.10.2020 10:32:55	0	ok			
						28	Henneser LST 3	22.10.2020 10:33:00	22.10.202010.3644	0	Репультат не ухазан			
						29	Hannasar LST3	11.08.2020.21.25:00	24.10.202013:19:50	0	Репультат не указан			
						1015	test incident	20.10.2020 21:10:00	02:11:2020 1:22:12	10000	Регультирующая протокал			
						4 monfips 2020	Г.	1			1/1			I

Рисунок 21. Аналитические отчеты.

Выбранный отчет можно отправить на печать, сохранить в форматах pdf, word, excel и т.д.

Интеграция со сторонними системами

Для облегчения ввода информации по инцидентам в «SecurityDesk» из других систем безопасности имеется возможность интеграции. Так как большинство систем или устройств безопасности могут формировать почтовые сообщения при обнаружении инцидентов в «SecurityDesk» встроена возможность интеграции с ними через «Универсальный коннектор» электронной почты, настройка данного коннектора выполняется Администратором Системы.

Для полноценного информационного обмена между Системой и RuSIEM имеется встроенный Систему специальный коннектор.

Дополнительно для интеграции возможна разработка специализированных программных модулей – коннекторов.

1. Коннектор для передачи инцидентов в АСОИ ФинЦЕРТ

Для передачи информации по операциям без согласия в АСОИ ФинЦЕРТ Администратору Системы необходимо настроить на сервере специальную службу-коннектор в соответствии с инструкцией. Коннектор позволяет автоматически передавать инциденты, зарегистрированные в Системе в ФинЦЕРТ по АРІ.

Управление ходом передачи данных осуществляется с помощью дополнительных параметров:

- «Отправить в АСОИ» установленный флаг в данном поле сигнализирует коннектору о готовности инцидента к передаче. В случае не успешности передачи коннектор снимает данный флаг для возможности корректировки передаваемой информации пользователем и повторной отправки;
- «Версия отправки в АСОИ» номер версии инцидента, переданного в АСОИ. Используется при повторной передаче инцидента, ранее уже зарегистрированного в АСОИ.

Для контроля в карточке инцидента используются следующие дополнительные параметры:

- «Результат отправки в АСОИ» в параметр автоматически заносятся результаты успешности передачи инцидента в АСОИ;
- «Номер АСОИ» в параметре отображается номер инцидента, выданного АСОИ в случае его успешной регистрации;
- «Идентификатор запроса в АСОИ» в параметре отображается идентификатор инцидента, выданного АСОИ в случае его успешной регистрации;
- «Идентификатор вложения в АСОИ» в параметре отображается идентификатор вложения сообщения, выданного АСОИ в случае его успешной регистрации инцидента.

Также результаты передачи инцидентов в АСОИ сохраняются в «Журнале работы» Системы, в карточке инцидента в вкладке «Журнал изменения».

Информация по инциденту:№ 6									
Наименование:	Состояние:								
Инцидент ОБС [RRN - 0492052	12315] Сидоров С.С.	Выполнено	+						
Информация по инциденту	Дополнительные параметры Файлы Уязви	мости Задачи Активы Нормативные документы Результат обработки Журнал изменения							
Журнал изменения	инцидента:								
Дата	Пользователь	Действие							
20.03.2022 18:41:03	system	Создание инцидента							
20.03.2022 18:53:20	system	Инцидент 61 успешно зарегистрирован! Номер в АСОИ=REQ-20220320-16	Инцидент 61 успешно зарегистрировані Номер в АСОИ=REQ-20220320-16						
20.03.2022 18:53:20	system	Состояние изменено на "Выполнено"							

Рисунок 22. Результат регистрации инцидента в АСОИ.

Кроме автоматизированной передачи инцидентов в Системе присутствует функционал выгрузки информации в формате JSON, позволяющей в дальнейшем загружать инцидент через личный кабинет в АСОИ. Чтобы выполнить выгрузку инцидента в формате JSON

откройте соответствующую карточку инцидента и нажмите на кнопку « состраните сформированный Системой файл на жесткий диск своего компьютера.

2. Коннектор с RuSIEM

Прием и обработка инцидентов от RuSIEM ничем не отличается от работы с другими инцидентами в Системе. Для возможности приема инцидентов в Системе и изменения состояния инцидентов в RuSIEM Администраторам Системы и RuSIEM необходимо выполнить настройки интеграции в соответствии с инструкцией Администратора Системы. Для отправки изменения состояний в RuSIEM потребуется использование отдельно стоящего сервера бизнес-процессов.

3. Коннектор с Positive Technologies MaxPatrol SIEM

Прием и обработка инцидентов от Positive Technologies MaxPatrol SIEM (далее PTSIEM) ничем не отличается от работы с другими инцидентами в Системе. Для возможности приема инцидентов в Системе и изменения их состояния в PTSIEM Администраторам Системы и PTSIEM необходимо выполнить настройки интеграции в соответствии с инструкцией Администратора Системы. Для отправки изменения состояний в PTSIEM потребуется использование сервера бизнес-процессов, который устанавливается отдельно.

4. Коннектор для DLP InfoWatch Traffic Monitor

Для передачи информации из системы защиты от утечек конфиденциальной информации InfoWatch Traffic Monitor в редакции Enterprise, использующей в своей работе СУБД Oracle разработан специальный модуль интеграции. Коннектор необходимо установить и настроить Администратору Системы.

Для регистрации события из системы «InfoWatch» в систему «SecurityDesk» в качестве инцидента на событии необходимо в интерфейсе DLP-системы поставить соответствующий тэг, предварительно настроенный Администратором Системы. После простановки тега в соответствии с расписанием синхронизации Системы данные будут переданы в систему «SecurityDesk» и в перечне инцидентов появятся советующие карточки Инцидентов – Рисунок 23 название инцидентов будет начинаться со слов «Инцидент IWTM №».

4321	Инцидент IWTM: 101 Канал перехвата: Print Устройство Xerox WorkCentre 3325 Учетная зались отправителя: sb-test1	Информационная	Критический	Закрыто	Центральный аппарат	system	14.04.2018 16:42:25	06.04.2018 9:19:59	06.04.2018 9:16:39
4322	Инцидент IWTM: 2123 Канал перехвата: Print Устройство Xerox WorkCentre 3325 Учетная запись отправителя: sb-test1	Информационная	Критический	Выполнено	Центральный аппарат	system	14.04.2018 16:43:11	13.04.2018 8:26:23	13.04.2018 8:21:48
4323	Инцидент IWTM: 2117 Канал перехвата: Web message Учетная запись отправителя: sb-testl 🖉	Информационная	Критический	В работе	Центральный аппарат	admin	14.04.2018 16:43:55	13.04.2018 8:22:43	13.04.2018 8:22:24

Рисунок 23. Инциденты, полученные из системы InfoWatch Traffic Monitor.

В случае удаления администратором данных **Инцидентов** из системы «SecurityDesk», при следующей синхронизации системы данные **Инциденты** будут зарегистрированы повторно, если в системе InfoWatch Traffic Monitor соответствующий тэг синхронизации не будет снят с события.