2025

SecurityDesk
Инструкция
пользователя

[SECURITYDESK АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ]

Инструкция по использованию 1.42

Оглавление

Введение

Автоматизированная система управления безопасностью «SecurityDesk» представляет собой WEB-приложение, 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*.

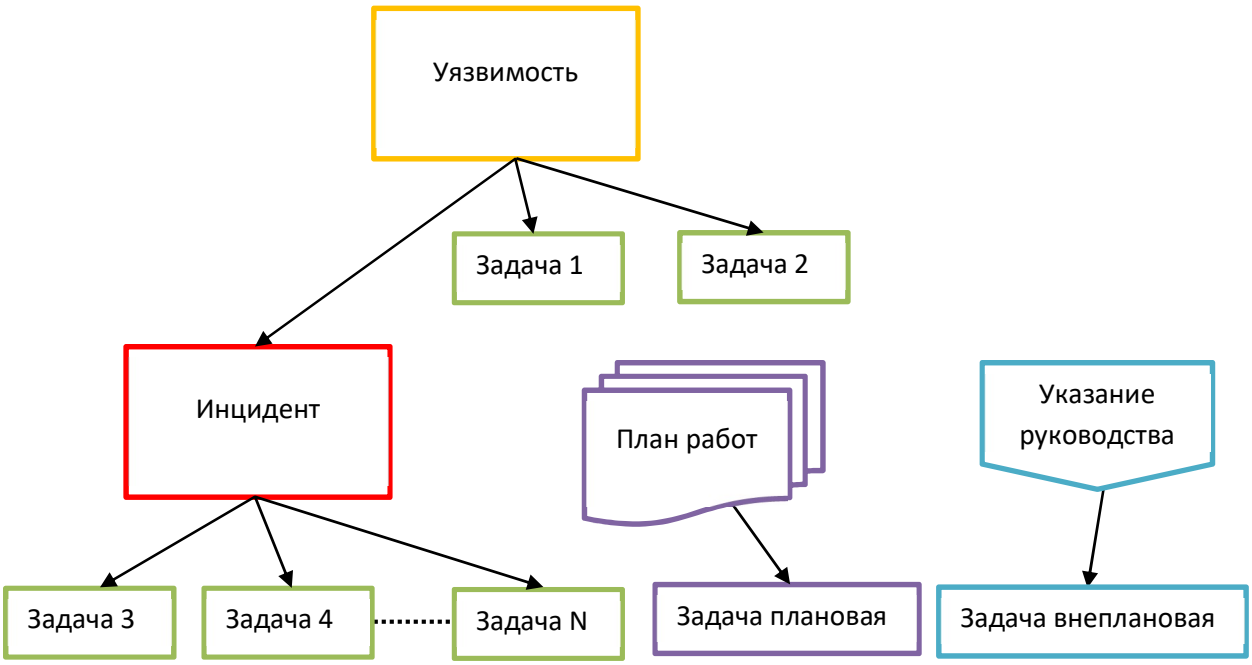


Рисунок 1. Взаимосвязь объектов системы типа Инцидентов и Задача.

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.

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

Состояние	Возможные переходы	Пояснение
Зарегистрировано	**В работе**	Начальное состояние объекта, работы на данном этапе не выполняются
В работе	**Выполнено, Отменено**	В данном состоянии выполняются основные работы по объекту Системы
Выполнено	**Закрыто, В работе Отменено**	Все работы завершены, но возможно перевести в 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

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.

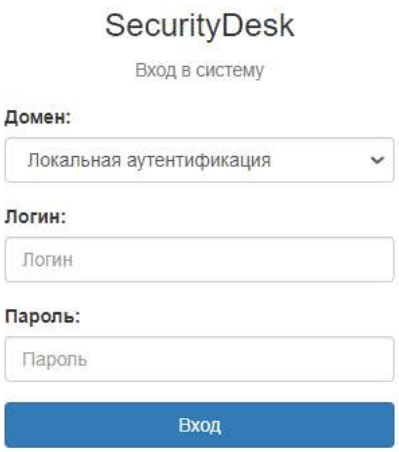


Рисунок 2. Окно входа пользователя в Систему.

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.

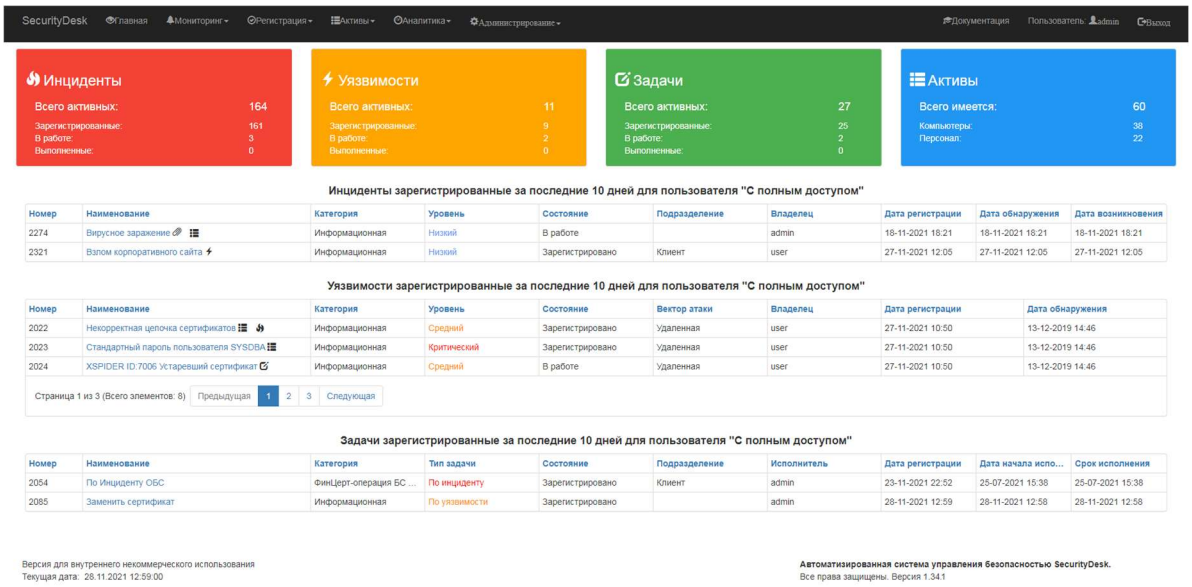
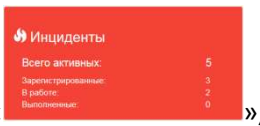
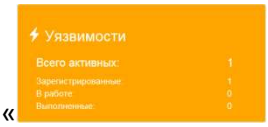


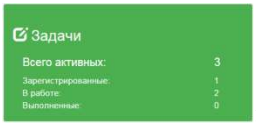
Рисунок 3. Главная панель мониторинга.

Используя на закрепленном вверху меню команд всегда можно вернуться на главную панель нажав в меню ссылку «Главная» 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 «Регистрация»,
- просмотру стандартизованных диаграмм, аналитических панелей, генерации аналитических отчетов - раздел «Аналитика».

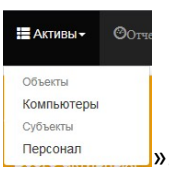
Отображаемые на главной панели цветные блоки « 

», « 

» и « 

» 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

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.

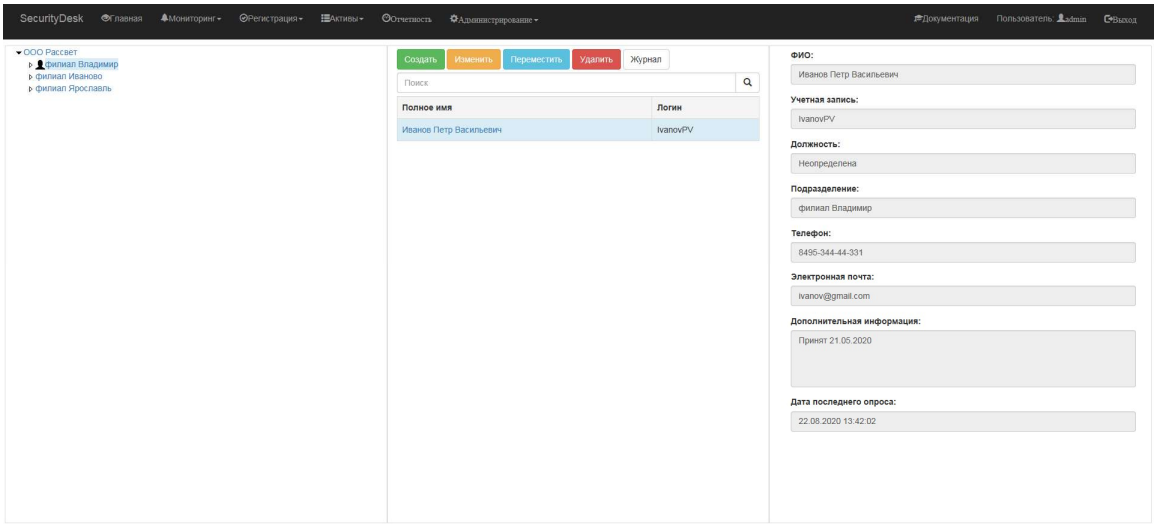


Рисунок 4. Форма управления Активами.

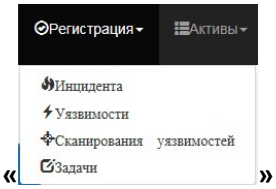
Для регистрации нового актива, изменения существующего, удаления или перемещения нажмите на соответствующую кнопку «  ». При нажатии кнопки «  » отобразится окно с журналом изменения параметров актива.

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 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).

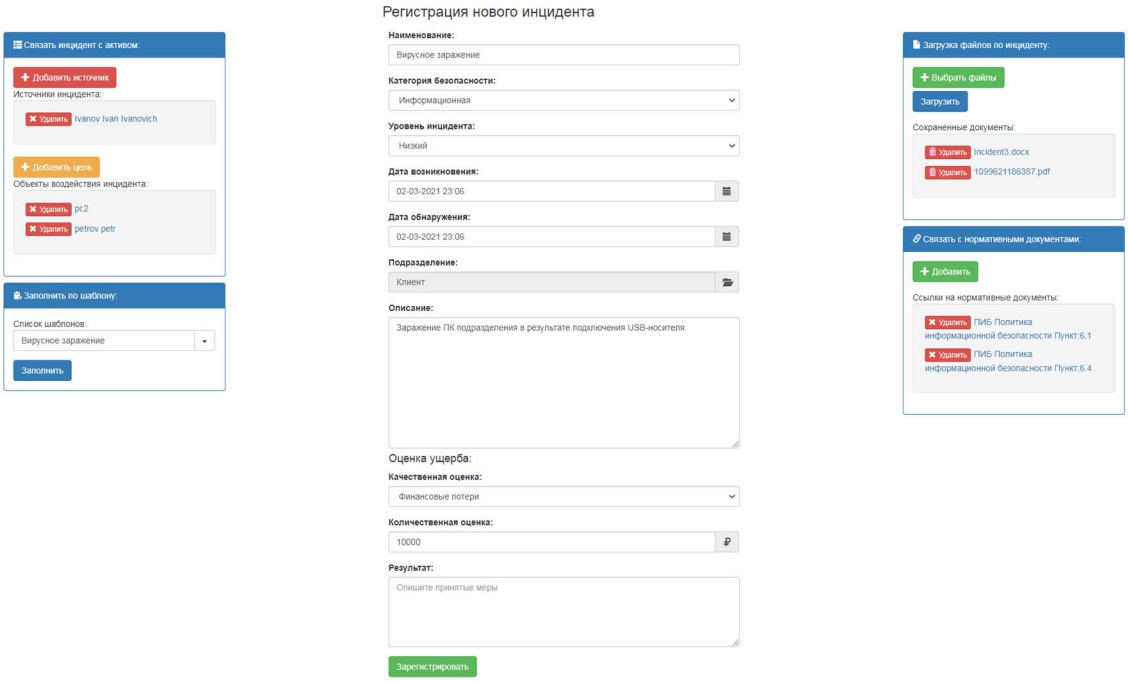


Рисунок 5. Форма регистрации Инцидента безопасности.

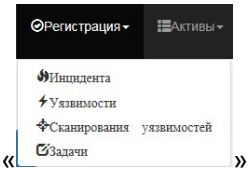
Как показано на рисунке, кроме заполнения данных в полях карточки к **Инциденту** можно прикрепить дополнительные материалы в виде файлов – окно «Загрузка файлов по инциденту:». **Помните!** – все загружаемые файлы увеличивают размер базы данных, поэтому для оптимального расходования размера жесткого диска сервера и скорости работы системы прикладывайте только необходимые файлы, а в случае сканированных документов обращайте внимание на настройки сканирующего оборудования и выходной размер скан-копий документов.

Также для полной классификации нарушений регламентных документов по безопасности, в карточке Инцидента присутствует механизм привязки ссылок нормативных документов к **Инциденту** – окно «Связать с нормативными документами:». Заполнение справочника нормативными документами осуществляется через административные настройки Системы пользователем с уровнем доступа **Администратор**.

Для получения аналитики в разрезе активов прикрепите соответствующие активы – окно «Связать инцидент с активом:» с **Инцидентом**. Для ускорения заполнения информации по типовым инцидентам 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 **Инцидент** сохраняется в Системе по нажатию кнопки Зарегистрировать и переходит в начальное состояние «**Зарегистрировано**».

5. Регистрация Уязвимости

Уязвимости регистрируются в системе аналогично Инцидентам через меню « 

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

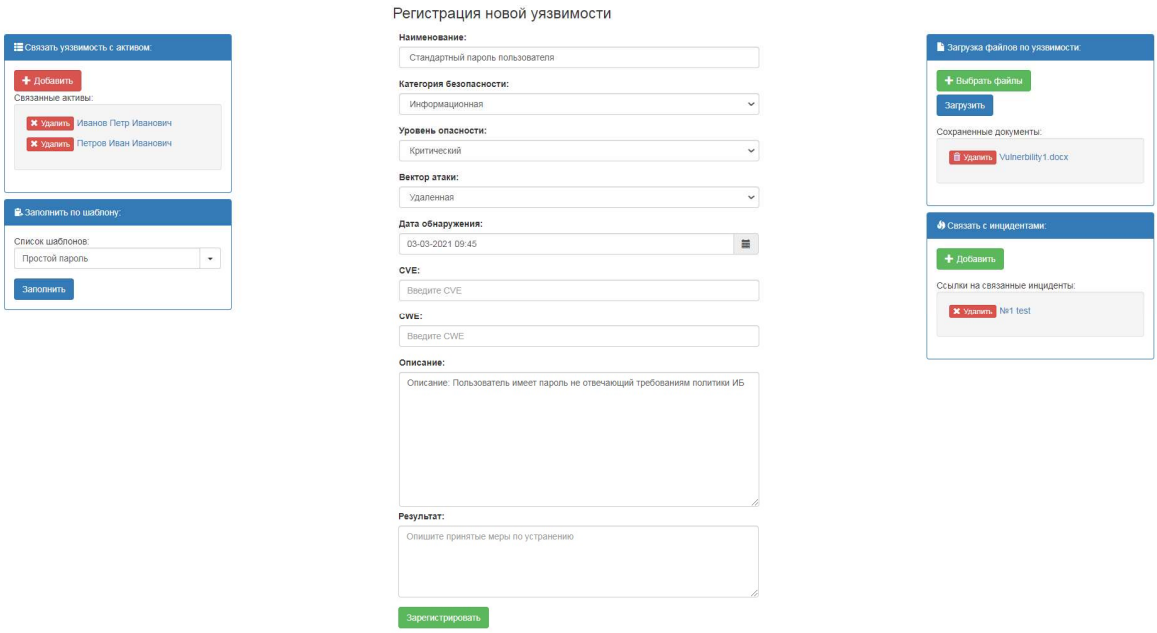
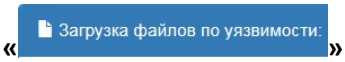
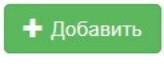


Рисунок 6. Форма регистрации Уязвимости.

Как показано на рисунке, кроме самих данных уязвимости к карточке можно прикрепить дополнительные материалы в виде файлов – окно **«** 

».

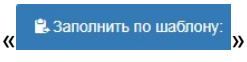
Помните! – все загружаемые файлы увеличивают размер базы данных, поэтому для оптимального расходования размера жесткого диска сервера и скорости работы системы прикладывайте только необходимые файлы, а в случае сканированных документов обращайте внимание на настройки сканирующего оборудования и выходной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

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

» в окне « 

». 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 « 

» к **Уязвимости**. Для ускорения заполнения информации по типовым уязвимостям в карточке присутствует функционал заполнения данных из шаблона.

Для применения шаблона выберите из окна « 

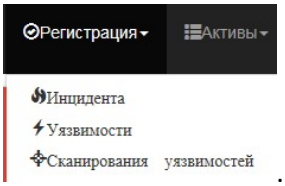
» необходимый шаблон и нажмите кнопку «Заполнить». Создавать, изменять и удалять шаблоны могут пользователи, имеющие роль Администратор системы.

После занесения всех необходимых данных **Уязвимость** сохраняется в системе по нажатию кнопки 

и переходит в начальное состояние «Зарегистрировано».

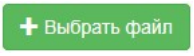
6. Регистрация Уязвимости по результатам сканирования

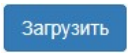
В Системе доступна регистрация Уязвимостей на основе результатов сканирования, выполненных с помощью специализированных сканеров проверки защищенности. В настоящий момент присутствует возможность загружать результаты сканирования в виде файлов и создавать на их основе карточки уязвимости. Для перехода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



. 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 « 

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

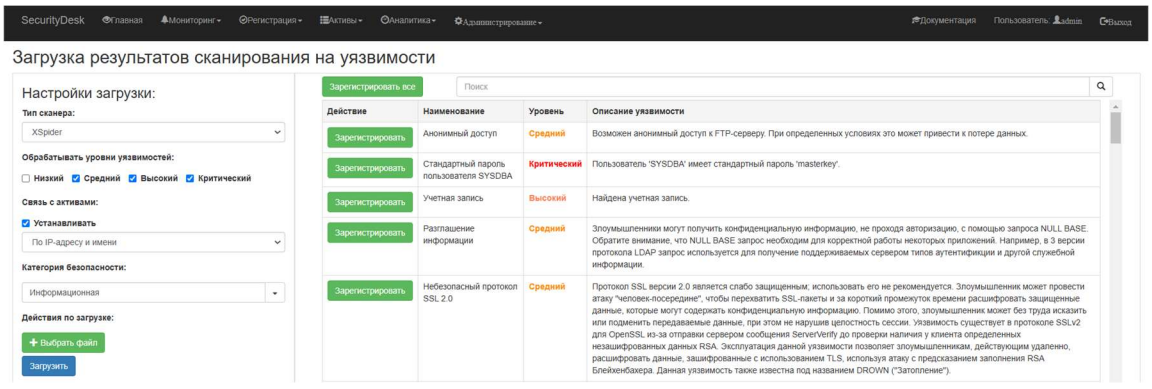
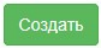


Рисунок 7. Форма регистрации Уязвимостей на основе результатов сканирования.

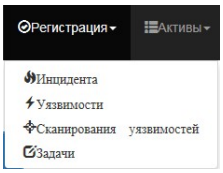
Для списка загруженных уязвимостей доступны следующие элементы управления – кнопка « 

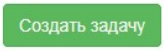
», нажав на которую в Системе будут созданы карточки по всем обнаруженным уязвимостям и кнопка « 

» напротив каждой уязвимости, позволяющая выборочно регистрировать только необходимые уязвимости.

7. Регистрация Задач

Задачи регистрируются в системе двумя способами:

- С помощью основного меню 

необходимо выбрать регистрацию **Задачи**. Для такого способа регистрации существует возможность создать задачу 2х типов: *плановую* и *внеплановую*.
- С помощью кнопки 

в карточке **Инцидента** или **Уязвимости** (Рисунок 8). В данном случае создается **Задача**, привязанная к **Инциденту** или **Уязвимости**, из карточки которой она создавалась.

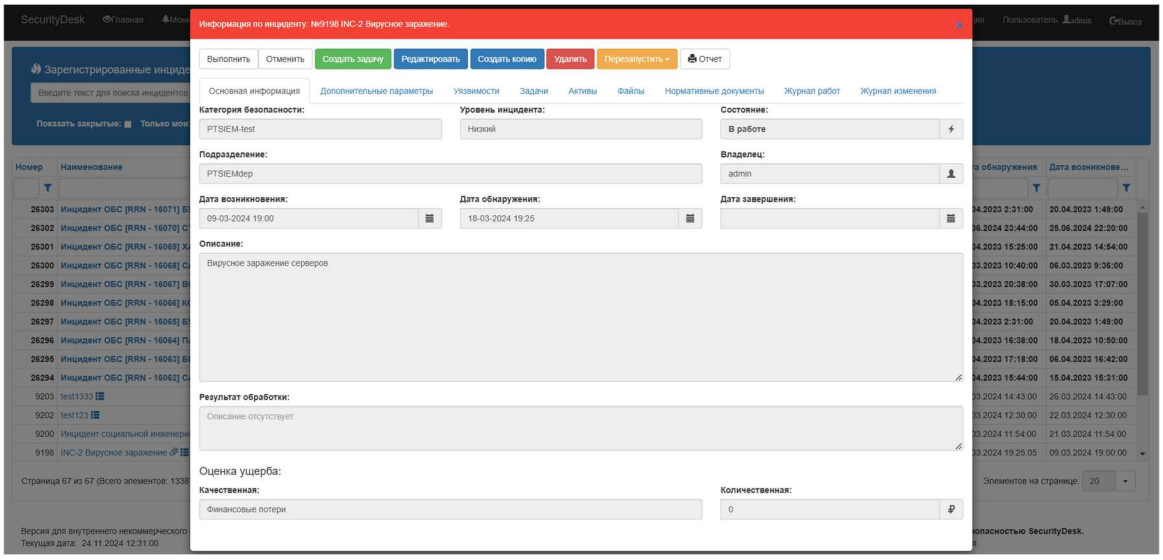


Рисунок 8. Карточка просмотра Инцидента.

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.

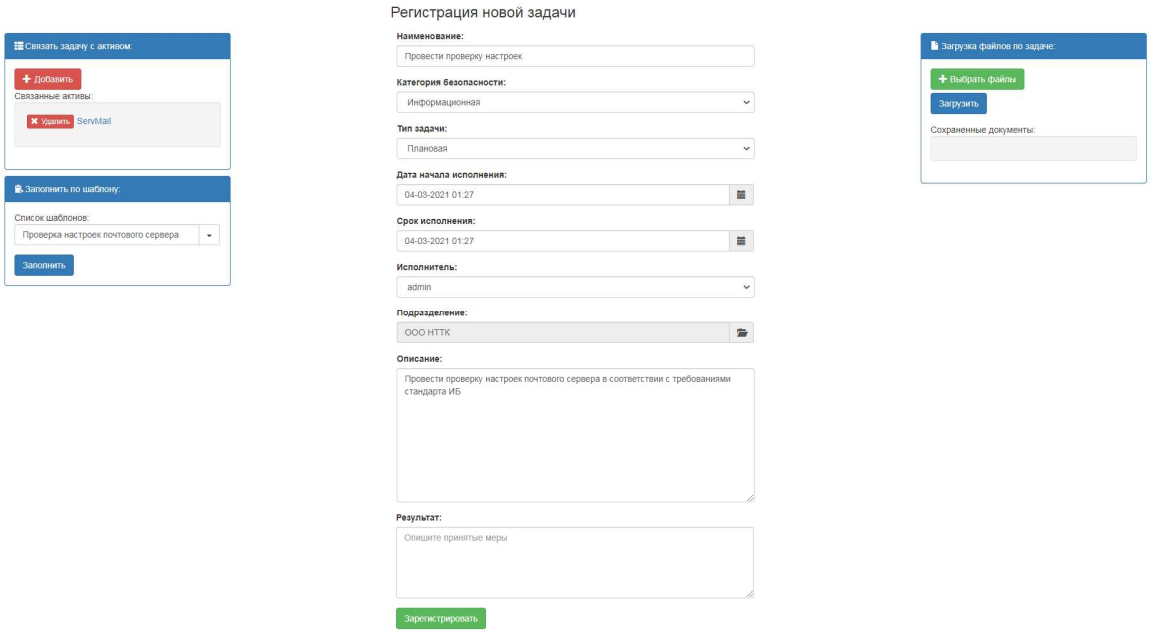
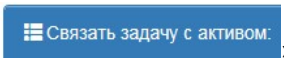


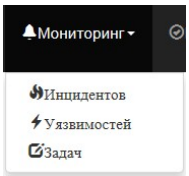
Рисунок 9. Форма регистрации Задачи.

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 «  » 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  и переходит в начальное состояние «Зарегистрировано».

8. Мониторинг и управление Инцидентами



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.

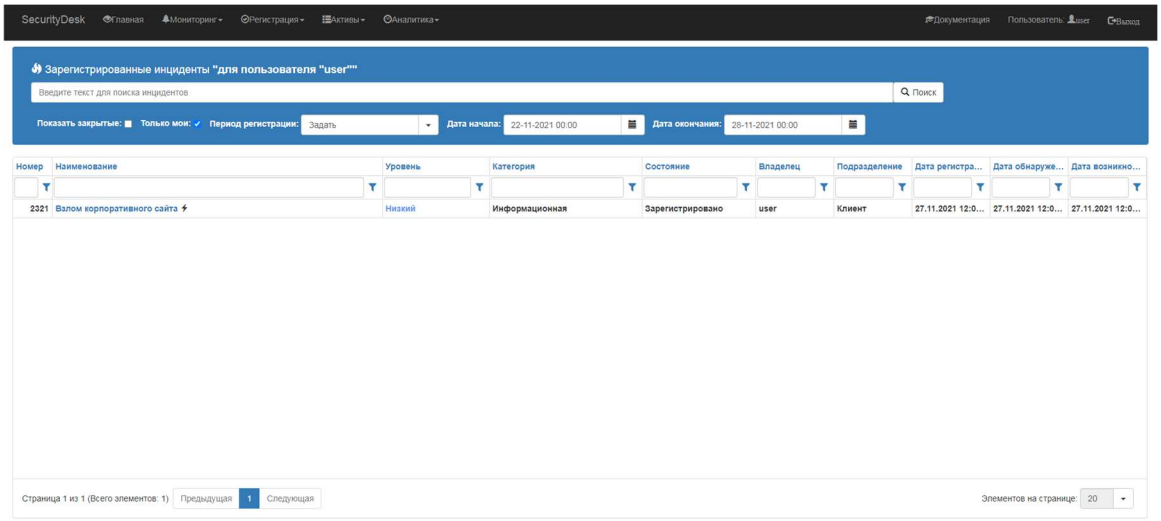


Рисунок 10. Форма просмотра зарегистрированных инцидентов в системе.

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.

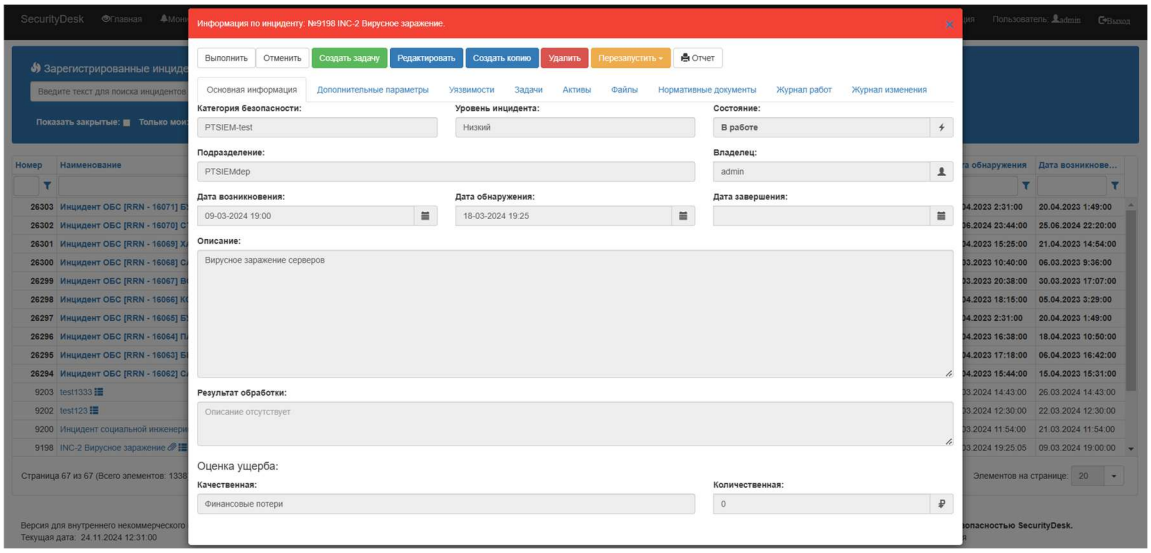


Рисунок 11. Карточка просмотра Инцидента.

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

управления состоянием **Инцидента** и созданием подчиненных **Задач** 

. Остальные вкладки содержат перечень 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 №1

"Взлом почтовой системы"

Владелец: admin (Главный пользователь системы, пароль по умолчанию 123456)
Состояние: Зарегистрировано

Параметры инцидента:
Категория безопасности: Информационная
Уровень: Высокий
Подразделение: филиал Владимир

Временные параметры:
Дата возникновения: 22-08-2020 14:11
Дата обнаружения: 22-08-2020 14:11
Дата завершения:

Общее описание:
Взлом почтового сервера компании.

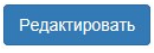
Результат обработки:

Оценка ущерба:
Качественная: Финансовые потери
Количественная:100000

Связанные активы:

Направление	Тип	Наименование	Подразделение	Дополнительная информация
Источник	Персонал	Иванов Петр Васильевич	филиал Владимир	Login=IvanovPV, Должность=Неопределена, 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 

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 имеет прикрепленные Задачи,** состояние инцидента в состоянии «**Закрыто**» контролируется состоянием связанных Задач.

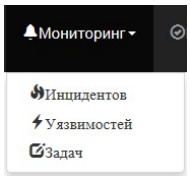
Кроме представленных кнопок управления администратору системы доступна дополнительная кнопка 

, позволяющая полностью удалить Инцидент из Системы и

кнопка 

, 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



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.

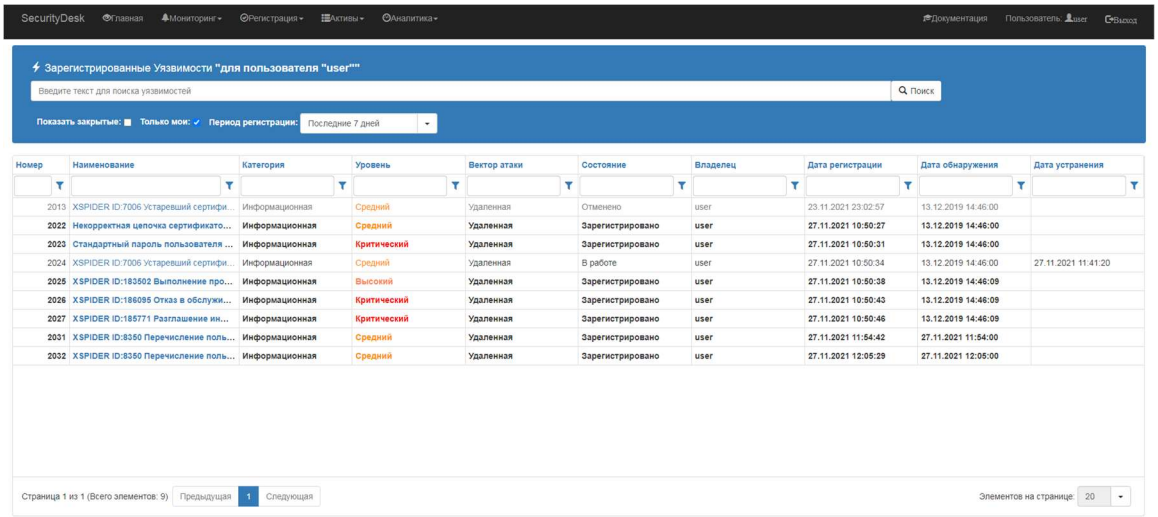


Рисунок 13. Форма просмотра зарегистрированных Уязвимостей.

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.

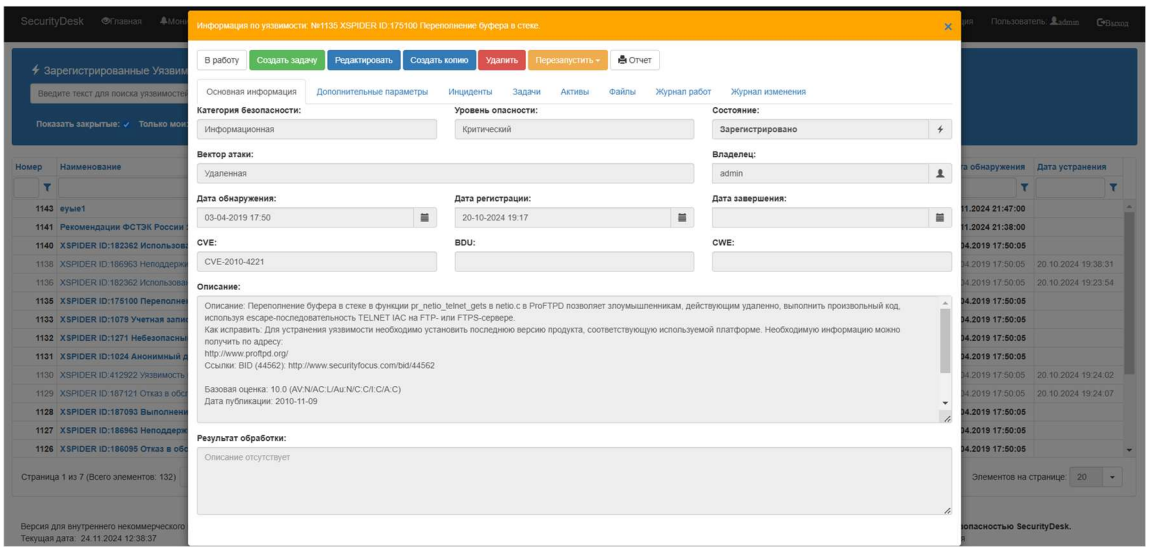
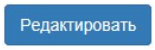


Рисунок 14. Карточка Уязвимости.

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

. 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 

из карточки 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 имеет прикрепленные 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.

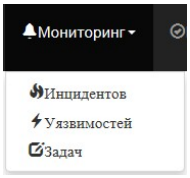
Кроме представленных на рисунке кнопок управления администратору системы доступна дополнительная кнопка 

, позволяющая полностью удалить Уязвимость из Системы и кнопка 

, 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.

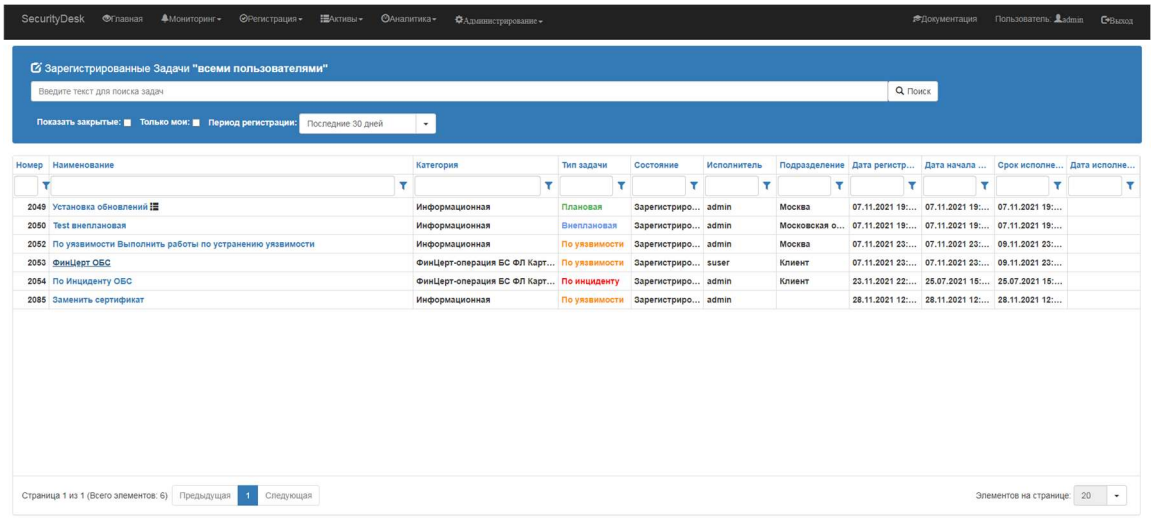


Рисунок 15. Форма просмотра зарегистрированных Задач в системе.

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.

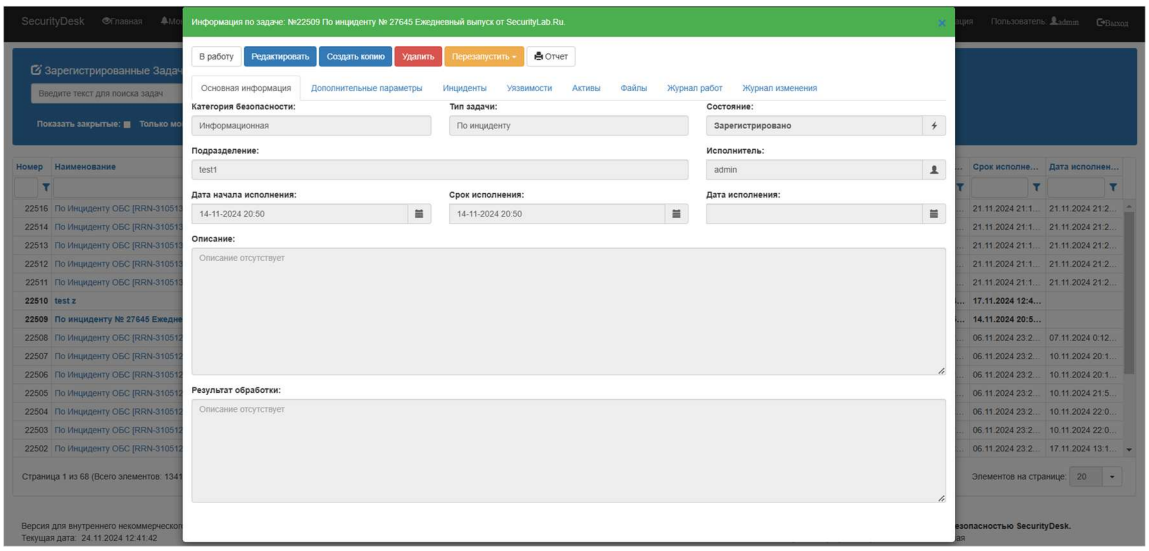
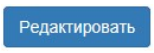


Рисунок 16. Карточка задачи.

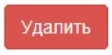
Карточка **Задачи** имеет несколько вкладок. На первой вкладке выведена основная информация, состояние, а также панель управления состоянием Задачи 

. 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 

из карточки задачи Система сформирует отчет в 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 

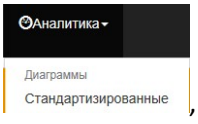
Задача переводится в режим редактирования, форма которой полностью идентична форме регистрации **Задачи** - Рисунок 9. Данная возможность доступна пользователю только в состояниях «**Зарегистрировано**», «**В работе**», а в состояниях «**Выполнено**», **«Отменено»** и **«Закрыто» редактирование** информации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

Кроме представленных на рисунке кнопок управления, Администратору системы доступна дополнительная кнопка 

, позволяющая полностью удалить Задачу из системы и кнопка 

, 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**» 

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

При нажатии на кнопки выгрузки 

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.

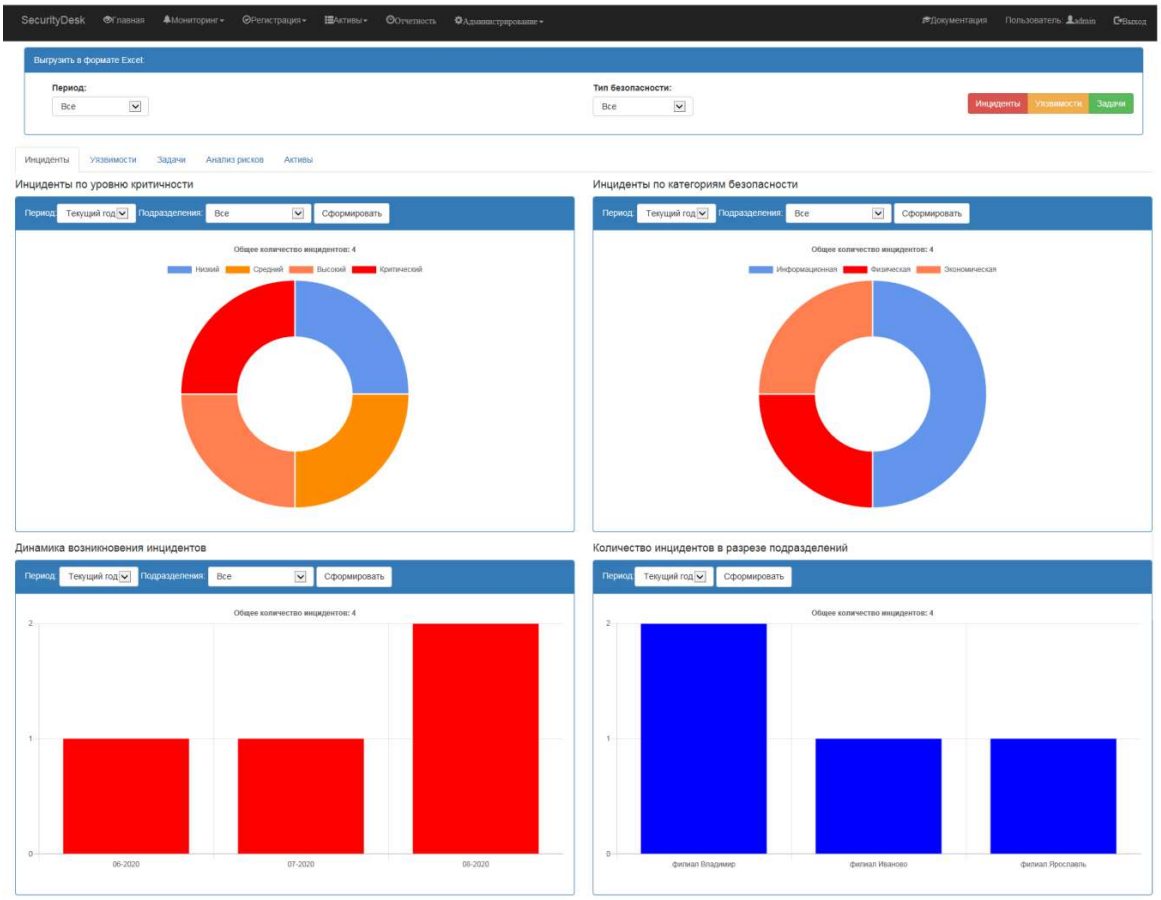


Рисунок 17. Панель диаграмм статистики.

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.

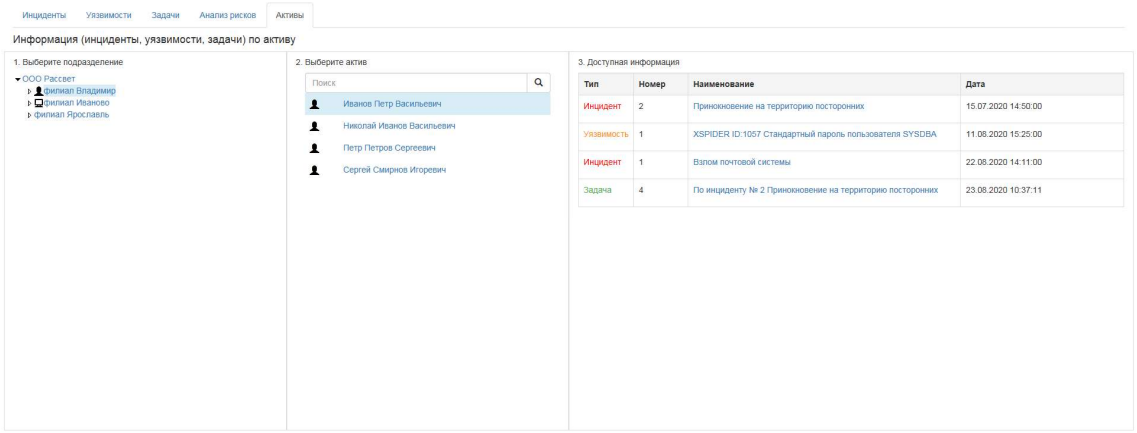
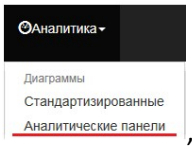


Рисунок 19. Панель анализа в разрезе активов

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**» - 

, 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.

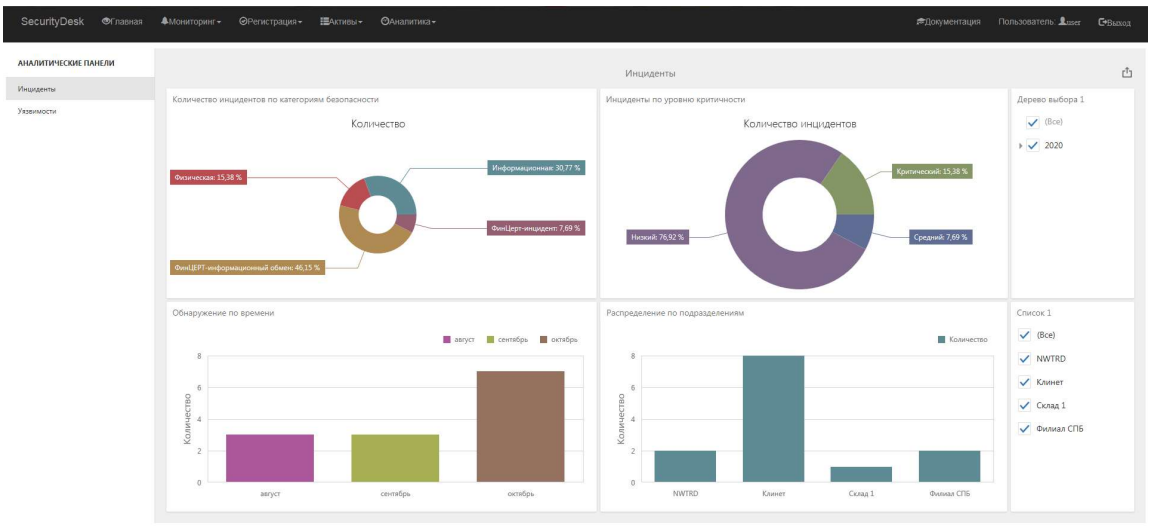
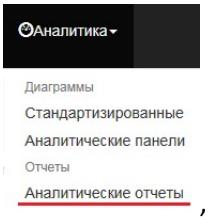


Рисунок 20. Аналитические панели диаграмм.

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**» -



, 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.

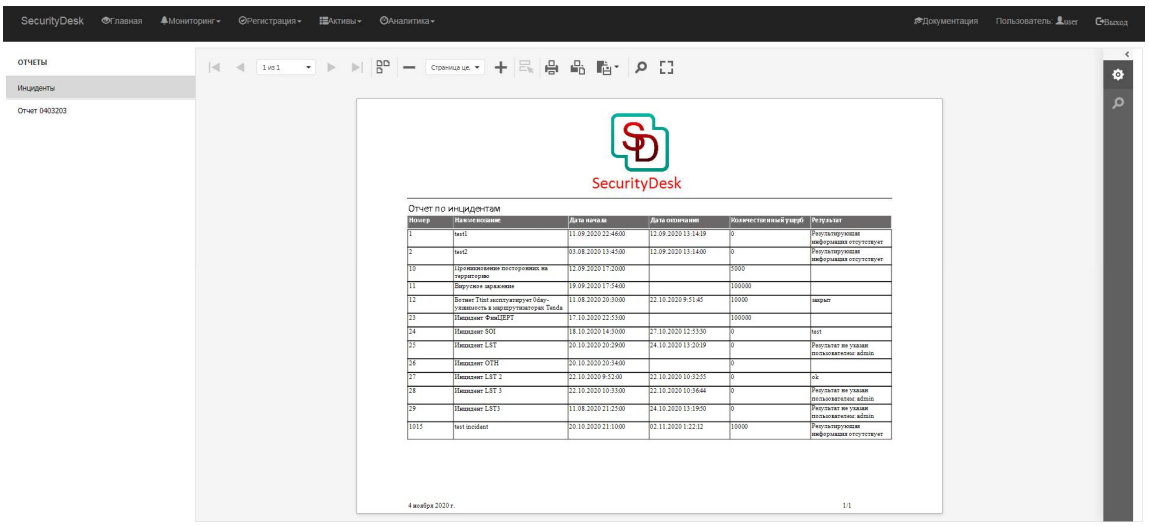


Рисунок 21. Аналитические отчеты.

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 API.

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».

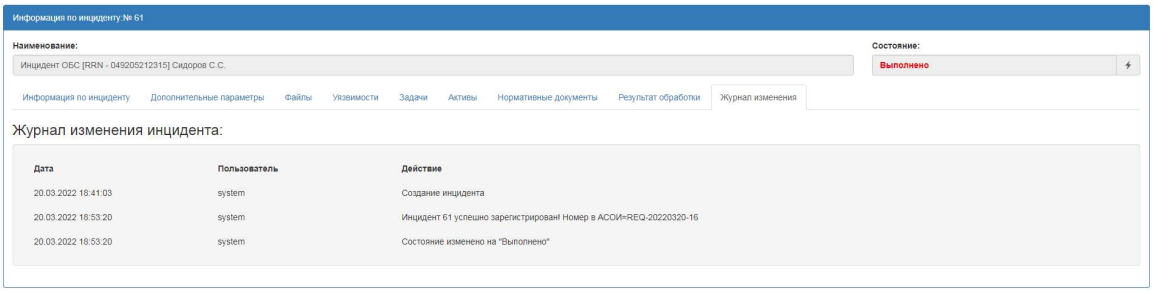


Рисунок 22. Результат регистрации инцидента в АСОИ.

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 «ФинЦЕРТ JSON» и сохраните 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.

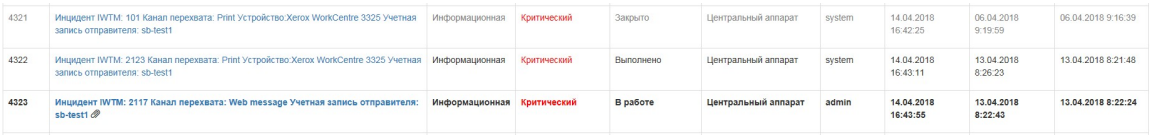
3. Коннектор с Positive Technologies MaxPatrol SIEM

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 запись 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-test1**	**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.