InfoWatch Data Explorer. Руководство пользователя

28/04/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 4

2 Комплект документов 5

3 Техническая поддержка пользователей 6

4 Обзор 7

5 Интерфейс Центра расследований 8

6 Единый фильтр 11

6.1 Фильтры 11

6.1.1 Фильтры в разделе Кластеризация 11

6.2 Работа с Единым фильтром 15

6.2.1 Добавление и удаление фильтров 15

6.2.2 Значения фильтров 16

Условие с несколькими фильтрами 16

Тип значения "поиск по шаблону" 16

Включение и исключение значений фильтра 17

Сброс значений фильтра 19

6.2.3 Сохранение и загрузка наборов фильтров 19

7 Раздел "Кластеризация" 21

7.1 Вкладка "Файлы" 21

7.1.1 Просмотр содержимого кластеров 22

7.1.2 Действия с файлами 24

7.1.3 Облако тегов 25

7.2 Вкладка "Карта кластеров" 25

8 ПОЛЬЗОВАТЕЛЬСКОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ 28

9 Глоссарий 33

В настоящем руководстве вы можете найти сведения по работе в InfoWatch Data Explorer.
InfoWatch Data Explorer (далее Модуль/Система или Data Explorer) это – модуль, позволяющий автоматически систематизировать документы, найденные с помощью InfoWatch Data Discovery. Для работы Data Explorer необходим InfoWatch Data Analysis Service.

1 Аудитория

Данное руководство предназначено для пользователей, работающих с Модулем.

Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Linux и MS Windows.

2 Комплект документов

В документацию по InfoWatch Data Explorer входят:

- *InfoWatch Data Explorer. Руководство по установке*. Содержит описание установки и удаления Модуля;
- *InfoWatch Data Explorer. Руководство администратора*. Документ содержит информацию по настройке Модуля.
- *InfoWatch Data Explorer. Руководство пользователя*. Содержит описание работы с Модулем.

Сопутствующая документация по продукту InfoWatch Data Discovery включает в себя:

- *InfoWatch Data Discovery. Руководство по установке*. Документ содержит описание процесса установки, обновления и удаления Data Discovery.
- *InfoWatch Data Discovery. Руководство администратора*. Документ содержит информацию по настройке Data Discovery.
- *InfoWatch Data Discovery. Руководство пользователя*. Содержит описание работы с задачами сканирования.

Сопутствующая документация по сервису InfoWatch Data Analysis Service включает в себя:

- *InfoWatch Data Analysis Service. Руководство по установке, конфигурированию и администрированию*. Содержит описание установки, обновления, удаления и настройки Data Analysis Service.

Сопутствующая документация по продукту InfoWatch Traffic Monitor включает в себя:

- *InfoWatch Traffic Monitor. Руководство по установке*. Содержит описание установки, настройки и удаления системы InfoWatch Traffic Monitor;
- *InfoWatch Traffic Monitor. Руководство администратора*. Содержит информацию по администрированию InfoWatch Traffic Monitor (база данных, серверная часть);
- *InfoWatch Traffic Monitor. Руководство пользователя*. Содержит описание работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, составление политик для обработки объектов);
- *InfoWatch Traffic Monitor. Справочник по конфигурационным файлам*. Содержит пояснения к часто используемым конфигурационным файлам.

3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Модуля, вы можете обратиться в службу технической поддержки:

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера;
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Вы также можете посетить раздел технической поддержки на нашем сайте: https://www.infowatch.ru/services/support.

4 Обзор

Центр расследований представляет собой веб-интерфейс для работы с продуктами InfoWatch. У пользователя есть возможность установить как один, так и несколько продуктов. Весь набор установленных продуктов позволяет получать наиболее полную информацию о нарушениях, персонах, рисках и т.д.

Data Explorer – это модуль, который используется совместно с продуктом InfoWatch Data Discovery и помогает проводить аудит файловых хранилищ и рабочих станций.

Принцип работы Data Explorer:

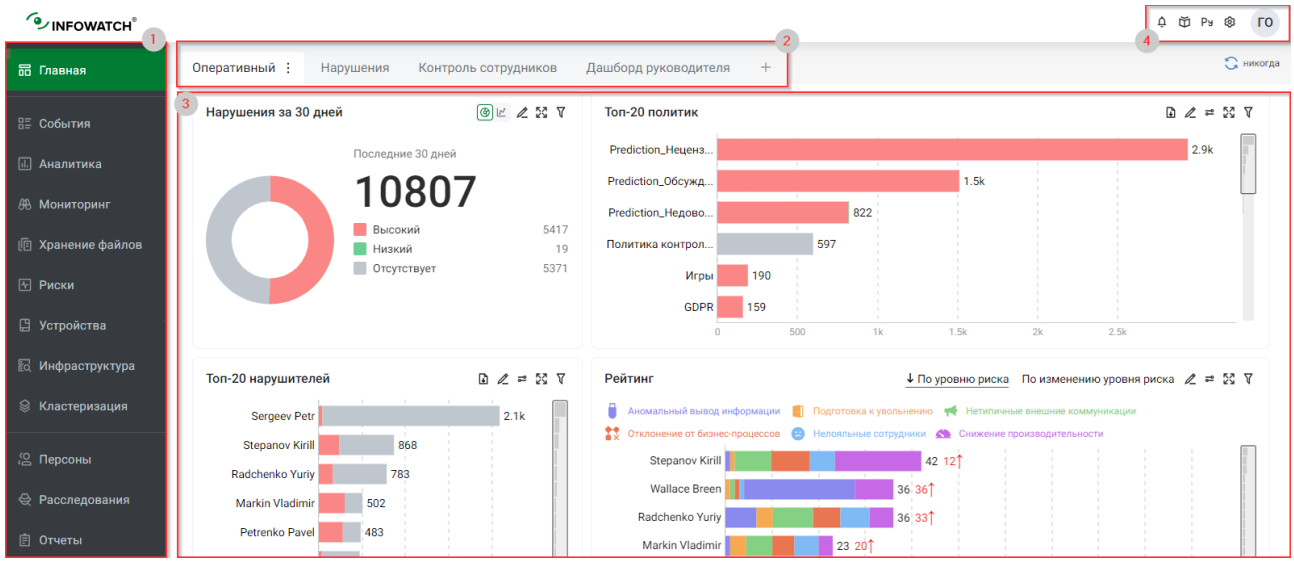
1. Data Discovery сканирует сетевые ресурсы, рабочие станции, серверы и хранилища документов. В процессе сканирования он извлекает из копий файлов текстовые контенты, в том числе текст с изображений с помощью OCR, и уведомляет Data Analysis Service о наличии данных для анализа.
2. Data Analysis Service автоматически определяет для каждого файла набор тегов, по которым можно понять тематику и примерное содержание документа, а затем сортирует полученные файлы в зависимости от терминологии и объединяет похожие в группы – кластеры. Каждый кластер содержит файлы с одинаковым набором тегов.
3. Data Explorer отображает данные об обработанных документах и кластерах в удобной для пользователя форме. Это позволяет:
    - провести аудит документов, хранящихся на рабочих станциях, серверах и других хранилищах компании. Например, можно проанализировать, где хранятся документы, содержащие конфиденциальную информацию, или какие-либо посторонние документы.
    - провести расследование, что хранится на рабочей станции конкретного сотрудника.
    - собрать образцы документов для формирования политик DLP, не разбираясь предварительно в тематике документооборота компании.

5 Интерфейс Центра расследований

Для работы с Data Explorer используйте веб-консоль Центра расследований InfoWatch.

Центр расследований представляет собой единую графическую среду, в которой могут быть представлены и проанализированы данные установленных продуктов InfoWatch.

В интерфейсе Центра расследований можно выделить несколько областей. На изображении ниже представлена **Главная** страница.



Элементы интерфейса:

Номер на схеме	Элемент окна	Описание элемента
1	Панель навигации	Рабочие разделы Центра расследований
2	Панель дашбордов	Список предустановленных дашбордов
3	Рабочая область	Отображение виджетов продуктов InfoWatch и работа с ними
4	Меню пользователя	Пользовательское меню, в котором вы можете: • отредактировать свою учетную запись; • сменить пароль; • включить использование горячих клавиш; • узнать контактные данные компании InfoWatch и службы поддержки; • выйти из Системы

Номер на схеме	Элемент окна	Описание элемента
	 Настройки	Раздел настроек (подробнее см. *Data Explorer. Руководство администратора*)
	 Уведомления	Папка уведомлений, в которую попадают сообщения Системы пользователю (подробнее см. *Data Explorer. Руководство администратора.* *Системные уведомления*.)
	 Смена языка	Выбор языка интерфейса: *Русский* или *Английский*
	 Справочник	Справочник Центра расследований

Работа в Центре расследований ведется в тематических разделах:

Раздел	Описание
Главная	Основной раздел, в котором размещены предустановленные дашборды с наборами виджетов, позволяющие быстро получить и отобразить информацию о нарушениях и нарушителях на каждом из них с учетом фильтров. Вы также можете создавать собственные дашборды с желаемым набором виджетов.
События	Список событий, согласно установленным фильтрам
Аналитика	Статистическая информация о нарушениях/нарушителях, согласно установленным фильтрам, отображаемая на: • виджетах, содержащих графики, диаграммы и таблицы; • графе связей с визуализацией событий. Вкладка *Статистика нарушений* доступна всем продуктам. На вкладке *Граф связей* представлена функциональность продукта *InfoWatch Vision* (см. *InfoWatch Vision. Руководство пользователя*). На вкладке *Статистика активности* представлена функциональность продукта *InfoWatch Activity Monitor* (см. *InfoWatch Activity Monitor. Руководство пользователя*)
Мониторинг	Мониторинг активности сотрудников, а также наблюдение за рабочими станциями сотрудников в режиме онлайн. Раздел продукта *InfoWatch Activity Monitor* (см. *InfoWatch Activity Monitor. Руководство пользователя*)
Хранение файлов	Создание и запуск задач сканирования сетевых ресурсов, просмотр и анализ детальной информации о файлах, включая владельцев, поиск дубликатов и похожих файлов.

Раздел	Описание
	Раздел продукта *InfoWatch Data Discovery* (см. *InfoWatch Data Discovery. Руководство пользователя*)
Риски	Расчет рейтинга сотрудников для прогнозирования рисков информационной безопасности. Раздел продукта *InfoWatch Prediction* (см. *InfoWatch Prediction. Руководство пользователя*)
Устройства	Контроль внешних устройств хранения Раздел продукта *InfoWatch Device Control* (см. *InfoWatch Device Control. Руководство пользователя*)
Инфраструктура	Автоматический аудит службы каталогов и доступа к почтовым ящикам; отслеживание изменений прав доступа к папкам и файлам Раздел продукта *InfoWatch Data Access Tracker* (см. *InfoWatch Data Access Tracker. Руководство пользователя*)
Кластеризация	Просмотр и анализ документов, найденных InfoWatch Data Discovery, систематизированных и сгруппированных в кластеры. Раздел модуля *InfoWatch Data Explorer*
Персоны	Справочник персон компании, а также справочник внешних контактов
Расследования	Проведение расследований с использованием накопленных данных по нарушениям
Отчеты	Работа с шаблонами отчетов и задачами на регулярную отправку почтовых отчетов, выгрузка созданных отчетов

6 Единый фильтр

Единый фильтр – универсальный инструмент, позволяющий управлять поиском и отображением данных в Центре расследований InfoWatch.

В разных разделах Центра расследований представлены различные наборы фильтров.

Также на доступность фильтра влияют настройки Роли пользователя.

С помощью Единого фильтра вы можете:

- управлять отображением записей о кластеризованных файлах:
  - выбирать конкретные записи для отображения;
  - исключать лишние записи;
- сохранять настройки фильтрации, чтобы быстро получать необходимую информацию.

Важно!

При работе с единым фильтром учитывайте:

- все настройки Единого фильтра распространяются только в рамках одной вкладки в браузере;
- при перемещении на шаг назад или вперед (кнопка **Назад**/**Вперед** браузера) фильтр возвращается в то состояние, в каком он был на этом шаге;
- при выходе из Системы все атрибуты фильтра сбрасываются в исходное состояние.

6.1 Фильтры

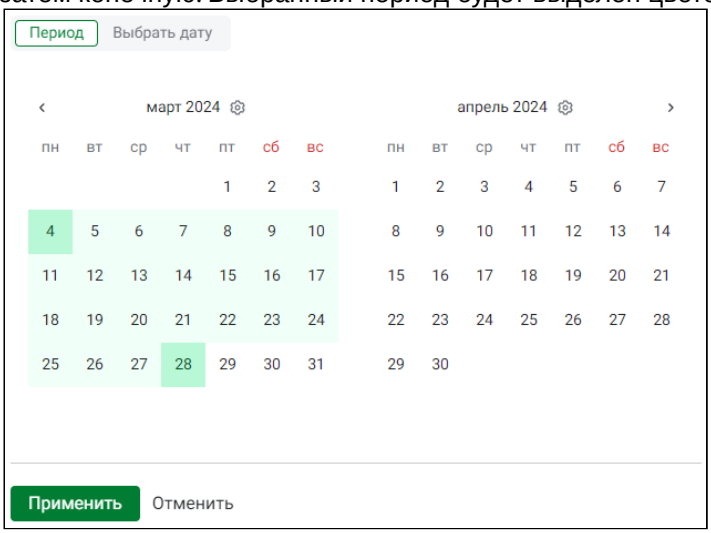
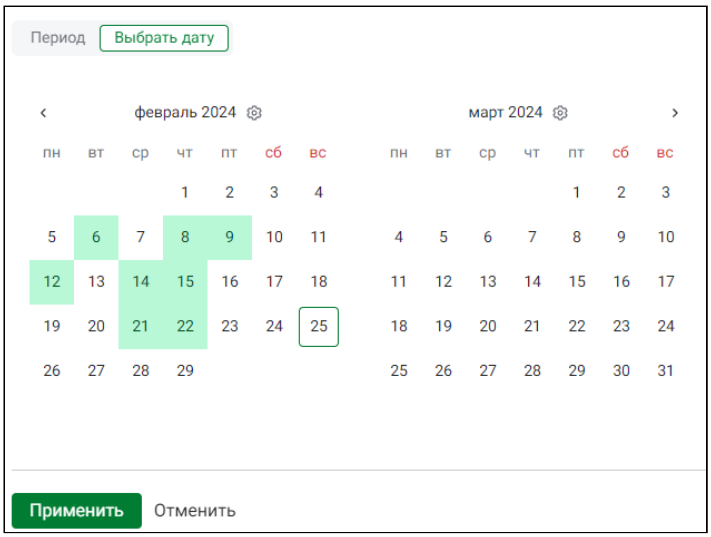
Единый фильтр – панель, которая содержит группу фильтров.

6.1.1 Фильтры в разделе **Кластеризация**

Примечание:

Фильтры **Теги**, **Дата создания кластера** и **Дата изменения кластера** уникальны для Data Explorer и работают только в разделе **Кластеризация**. Их значения не переносятся при переходе в другие разделы и влияют только на фильтрацию данных Data Explorer.
Все остальные фильтры относятся к Data Discovery и переносятся при переходах между разделом **Кластеризация** и разделами Data Discovery. Подробнее см. *InfoWatch Data Discovery. Руководство пользователя. Единый фильтр*.

Название фильтра	Описание	Установка значений
Теги	Ключевые термины, определенные в процессе кластеризации	Выберите значения из списка. Для поиска в списке введите значение в строку поиска. Отображение элементов в списке не зависит от условий, установленных в других фильтрах. Для выбора доступны все теги, которые Data Analysis Service присвоил файлам. Теги дополняются в процессе взаимодействия Data Discovery и Data Analysis Service. Вы можете выбирать ✓ и исключать ✗ теги. Отмеченные теги объединяются в условие фильтрации **по логическому "И"**. **Пример**: если выбраны ✓ теги *Документ* и *Закон*, а исключены ✗ теги *Выплата* и *Штраф*, в списке останутся кластеры с тегами *Документ* и *Закон*, в которых **нет одновременно** тегов *Выплата* и *Штраф*. В списке могут остаться кластеры с тегами *Выплата* или *Штраф*, так как исключены именно одновременные вхождения обоих тегов.
Дата создания кластера	Период, в который впервые был создан кластер	Выберите период времени: • *Последние сутки* – последние 24 часа; • *Текущий день* – от 0:00 до текущего времени; • *Последние 3 дня;* • *Последние 7 дней;* • *Последние 30 дней;* • *Текущий месяц;* • *Прошлый месяц;* • *Произвольный период* (можно выбрать даты начала и окончания периода либо список произвольных дат): **Чтобы указать интересующий период времени:**

Название фильтра	Описание	Установка значений
Дата изменения кластера	Период, в который новые файлы были добавлены в кластер	1. Выберите указателем мыши начальную дату в календаре, а затем конечную. Выбранный период будет выделен цветом:  2. Нажмите **Применить**. **Чтобы указать одну или несколько произвольных дат:** 1. Выберите указателем мыши одну или несколько дат в календаре. Выбранные даты будут выделены цветом:  2. Нажмите **Применить**. Значение по умолчанию: **Любая дата**
Обнаружен	Период, в который файл был просканирован Data Discovery	
Создан	Период времени, в который файл был создан	
Изменен	Период времени, в который файл был изменен	

Название фильтра	Описание	Установка значений
Задача	Название задачи сканирования Data Discovery	Чтобы выбрать значение, выполните одно из действий: • Выберите значение из списка. Для поиска в списке введите значение в строку поиска. Отображение элементов в списке не зависит от условий, установленных в других фильтрах. • Введите значение в строку поиска и выберите значение типа "поиск по шаблону". Значение по умолчанию: **Все**
Хост	Имя или IP-адрес хоста	
Расположение	Полный путь к директории	
Имя файла	Имя Файла	
Владелец	Персона или группа, которая является владельцем файла	В списке отображаются имена персон и групп, идентифицированных по SID. Вы можете фильтровать записи одновременно и по группам, и по персонам. Персоны и группы выбираются отдельно, для этого в фильтре используйте переключатель **Персона**/**Группа**. Все выбранные значения объединяются с помощью логического "ИЛИ". Чтобы выбрать значение, выполните одно из действий: • Выберите персону из списка. Для поиска в списке введите имя персоны или SID в строку поиска. • Выберите группу из дерева Active Directory. Для поиска по дереву введите имя группы в строку поиска. Подробнее об идентификации персон и групп в таблице см. *Data Discovery. Руководство пользователя. Таблица с информацией о файлах*. Значение по умолчанию: **Все** Опция **Искать по правам, назначенным персоне напрямую** определяет, должен ли фильтр учитывать вхождение персоны в группы, а также вложенность групп. Если доступ к файлу имеет группа, а не конкретная персона, с включенной опцией поиск по персоне, входящей в группу, не даст результатов. Аналогично действие и для вложенных групп: с включенной опцией поиск по дочерней группе не выведет в результатах файлы, если владение/доступ к ним назначен родительской группе. Если опция выключена, в результатах будут выведены и файлы, владение/доступ к которым назначен персоне или группе напрямую, и файлы, владение/доступ к которым имеет родительская группа.

Название фильтра	Описание	Установка значений
Доступен для	Персоны и группы, которые имеют доступ к файлу	**Примечание:** В фильтре отображаются все группы, добавленные при интеграции с Active Directory. Если у группы нет SID, ее невозможно выбрать в фильтре
Размер	Ограничения на размер файла	В поле **от** укажите минимальный размер файла. В поле **до** укажите максимальный размер файла. Выберите единицу измерения. Значение по умолчанию: **Все** **Примечание**: Если указан только минимальный размер файла, то будут отображаться файлы, чей размер больше или равен минимальному размеру. Если указан только максимальный размер файла, то будут отображаться файлы, чей размер не превышает максимальный размер.
Тип подключения	Тип подключения хоста	Выберите значение из списка. Значение по умолчанию: **Все**
Объект защиты	Наличие в просканированных файлах объектов защиты из конфигурации Traffic Monitor, загруженных в результате интеграции	Доступны следующие значения: • *События без ОЗ* • *События с ОЗ* Для значения *События с ОЗ* **доступен выбор конкретных объектов защиты**. Доступен поиск по объектам защиты. Значение по умолчанию: **Все** - в таблице отображаются все файлы, с объекты защиты и без них.

Подробнее про настройку панели фильтров см. *Работа с Единым фильтром*.

6.2 Работа с Единым фильтром

6.2.1 Добавление и удаление фильтров

В панели фильтров можно использовать один или несколько фильтров.

Чтобы добавить фильтр на панель фильтров:

1. Нажмите ;
2. В открывшемся окне выберите нужный фильтр из списка.

3. Щелкните вне окна со списком фильтров.

Фильтр будет добавлен на панель фильтров.

Чтобы удалить фильтр с панели фильтров:

1. Нажмите ;
2. Снимите флажок с фильтра в списке.
3. Щелкните вне окна со списком фильтров.

Фильтр будет удален с панели фильтров.

Чтобы переместить фильтр на другое место на панели, зажмите  у выбранного фильтра перетащите на любое другое место.

Чтобы скрыть панель Единого фильтра, нажмите .

6.2.2 Значения фильтров

В фильтре необходимо выбрать минимум одно значение. Если не выбрано ни одно значение, то используется значение по умолчанию.

Важно!

При выходе из Системы сбрасываются значения фильтров. Рекомендуется сохранить фильтры перед выходом из Системы (см. "Сохранение и загрузка наборов фильтров").

Условие с несколькими фильтрами

Если заданы значения для нескольких фильтров, то условия нескольких фильтров объединяются с помощью логического "И".

Пример:

Укажите значение для нескольких фильтров:

- в фильтре **Теги** укажите значение: **договор**
- в фильтре **Дата изменения кластера** укажите текущий месяц
- в фильтре **Размер** укажите в поле **до** значение **2** и выберите единицу измерения **МБ**

В результате настройки отобразятся кластеры, имеющие тег "договор" и в которые в текущем месяце были добавлены новые файлы. При просмотре содержимого кластеров будут показаны только файлы размером не более 2 мегабайт.

Тип значения "поиск по шаблону"

Тип значения "поиск по шаблону" доступен для следующих фильтров:

- Задача;
- Хост;
- Расположение;
- Имя файла;
- Владелец;
- Доступен для.

Чтобы использовать значение типа "поиск по шаблону", введите значение в строку поиска и выберите значение типа "поиск по шаблону".

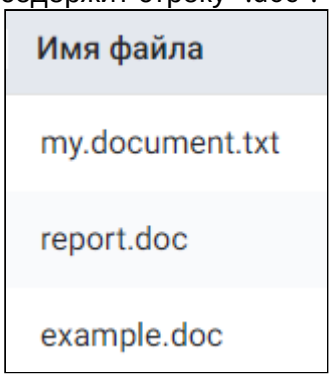
При фильтрации Система проверяет, входит ли значение из строки поиска в полное значение поля записи о файле. Для значений типа "поиск по шаблону" не учитывается регистр.

Пример:

1. Для фильтра **Имя файла** включите значение поиска по шаблону ".doc":



2. В результате фильтрации в таблице отображаются только те файлы, имя которых содержит строку ".doc":



Включение и исключение значений фильтра

В разделе **Кластеризация** несколько состояний доступны для значений следующих фильтров:

- Теги;
- Задача;
- Хост;
- Расположение;
- Имя файла;
- Владелец;
- Доступен для;
- Тип подключения.

Доступные состояния для значений вышеуказанных фильтров:

- – значение не выбрано (состояние по умолчанию);
- – значение включено;
- – значение исключено.

Чтобы изменить состояние значения, щелкните по флажку состояния.

Вы можете включить и/или исключить несколько значений, при этом:

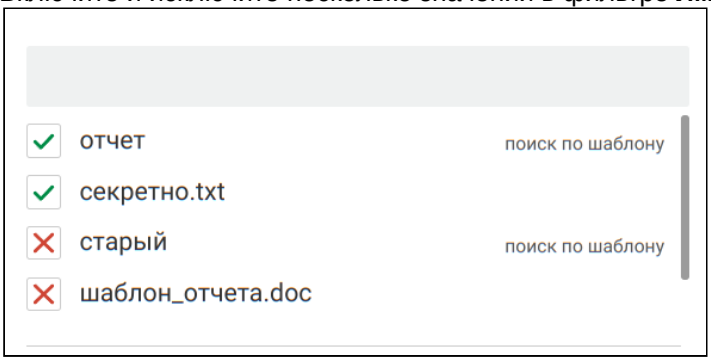
- Несколько включенных значений объединяются с помощью логического "ИЛИ";
- Несколько исключенных значений объединяются с помощью логического "ИЛИ";
- Условие из нескольких включенных значений и условие из нескольких исключенных значений объединяются с помощью логического "И".

Пример:

Среди обнаруженных есть 5 файлов со следующими значениями в поле **Имя файла**:

- отчет_2021.docx
- старый_отчет.doc
- новый_отчет.pdf
- секретно.txt
- шаблон_отчета.doc

Включите и исключите несколько значений в фильтре **Имя файла**:



В результате будут отображаться записи о файлах, у которых значение поля **Имя файла** соответствует одновременно двум условиям:

- **Условие по включенным значениям**:
  Условие выполняется, если: имя файла содержит в себе подстроку **отчет** ИЛИ именем файла является **секретно.txt**
- **Условие по исключенным значениям**:
  Условие НЕ выполняется, если: имя файла содержит подстроку **старый** ИЛИ именем файла является **шаблон_отчета.doc**

В результате будут отображены записи со следующими значениями в поле **Имя файла**:

- отчет_2021.docx
- новый_отчет.pdf
- секретно.txt

Сброс значений фильтра

Чтобы сбросить значения фильтра, нажмите на панели фильтра . Для фильтра будет установлено значение по умолчанию.

Чтобы сбросить значения для всех фильтров, нажмите .

6.2.3 Сохранение и загрузка наборов фильтров

Чтобы использовать заданные значения фильтров в дальнейшем, вы можете сохранить их в каталоги одного из типов:

- *Личные* – каталоги и их содержимое доступны только создавшему их пользователю;
- *Общие* – каталоги и их содержимое доступны всем пользователям Системы.

Чтобы сохранить фильтр:

1. Установите требуемые значения фильтров и нажмите .
2. В окне **Сохранить фильтр** задайте имя нового фильтра.
3. Выберите тип каталога, в который Система сохранит фильтр: *Личный* или *Общий*.
4. Выберите каталог, в котором следует сохранить фильтр, или создайте новый. Если каталогов много, используйте поиск по названию.

   > **Примечание:**
   >
   > Если не выбрать каталог, Система сохранит фильтр в корневой директории указанного типа каталогов.

5. Нажмите **Сохранить**.

Чтобы воспользоваться ранее созданным фильтром:

1. В области Единого фильтра нажмите **Сохраненные фильтры**.
2. Откройте каталог, который содержит интересующий фильтр.
3. Нажмите на фильтр, чтобы его активировать.

Чтобы отредактировать каталоги и фильтры:

1. В области Единого фильтра нажмите **Сохраненные фильтры** или на имя примененного фильтра.
2. Нажмите  над списком с фильтрами.
3. В окне **Настройка фильтров и каталогов** вы можете:
   - изменить иерархию каталогов путем перетаскивания;
   - в строке типа каталога:
     -  создать каталог;
   - при наведении курсора на каталог:
     -  переименовать каталог;
     -  создать дочерний каталог;
     -  удалить каталог;

- перемещать фильтры внутри каталогов и между каталогами;
- при наведении курсора на имя фильтра:
    -  переименовать фильтр;
    -  записать текущий фильтр, т.е. сохранить с этим названием примененные на данный момент значения фильтров;
    -  удалить фильтр.

При этом Главный офицер может редактировать и удалять личные и общие каталоги и/или их содержимое. Другие офицеры безопасности могут редактировать и удалять только личные каталоги и/или фильтры.

7 Раздел "Кластеризация"

Раздел **Кластеризация** содержит функциональность InfoWatch Data Explorer. В нем пользователь может искать и просматривать файлы, отсканированные Data Discovery и сгруппированные в кластеры. Для удобства поиска используются теги и карта кластеров.

Для отображения результатов кластеризации:

- В одном кластере с Data Explorer должны быть установлены:
  - Data Discovery
  - Data Analysis Service
- В Data Analysis Service должна быть включена функция протокластеризации;
- Data Analysis Service должен быть настроен на обработку ноды, на которой установлен Data Discovery;
- В задачах сканирования Data Discovery обязательно должен быть выбран режим обработки **Определять похожие файлы**.

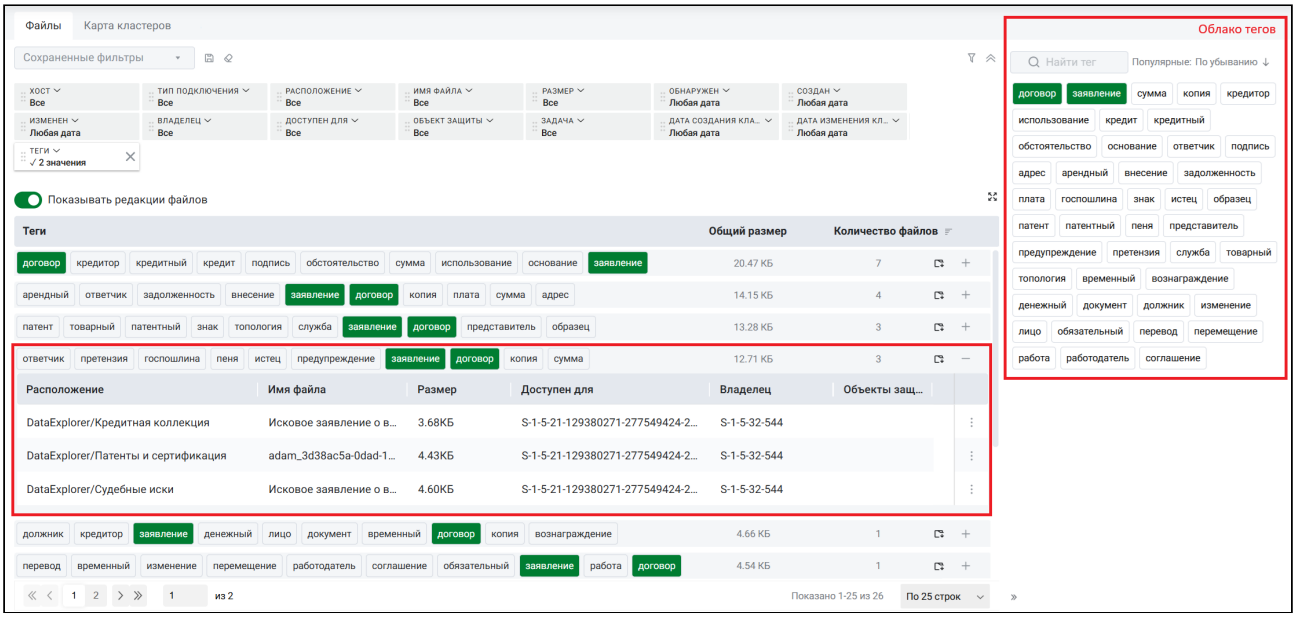
> **Примечание:**
>
> Data Analysis Service осуществляет обработку извлеченных **текстовых контентов** размером **не менее 200 Байт**.
>
> Из одного файла может быть извлечено несколько текстовых контентов, но для анализа и отображения они будут объединены в один.
>
> **Пример**: если экстрактор обрабатывает файл-архив, содержащий несколько документов, из каждого может быть извлечен текстовый контент, но в итоге они будут объединены в один общий, относящийся к файлу-архиву.

В разделе представлены вкладки:

- Файлы – отображение кластеров в виде табличного списка;
- Карта кластеров – отображение кластеров в виде карты.

7.1 Вкладка "Файлы"

На вкладке **Файлы** вы можете видеть список кластеров. Кластер – это тематическая группа файлов, которые близки по смыслу и имеют один и тот же набор тегов. Каждый кластер представлен на данной вкладке в виде таблицы с информацией о файлах, входящих в него.



В результате анализа контентов могут быть выделены кластеры, состоящие из одного файла. Это означает, что среди обработанных не обнаружено файлов, похожих по смыслу. Подобная уникальность также может иметь значение для Офицера безопасности при анализе тематики файлов.

Для каждого кластера указаны:

- **теги**, наиболее точно **определяющие общий смысл** документов;
- общий размер кластера;
- количество файлов в кластере.

Чтобы отфильтровать кластеры по тегам:

- Нажмите на любой тег в списке кластеров в центральной области или в облаке тегов справа, чтобы добавить его в фильтр.
  или
- Используйте фильтр **Теги** (подробнее см. *Единый фильтр*). В фильтре вы можете выбирать ✓ и исключать ✗ теги. Отмеченные теги объединяются в условие фильтрации **по логическому И**.

Вы можете сортировать кластеры по значениям столбцов:

- **Общий размер**;
- **Количество файлов**.

Для этого нажмите на заголовок столбца. Список кластеров будет отсортирован по возрастанию/убыванию значений выбранного столбца.

Чтобы развернуть список кластеров на весь экран, справа над списком нажмите ⛶.

Навигация по страницам списка кластеров осуществляется с помощью панели в нижней части экрана.

7.1.1 Просмотр содержимого кластеров

Чтобы просмотреть содержимое кластера, нажмите справа от него +.

В раскрывшейся таблице для каждого файла указана следующая информация, полученная из Data Discovery:

Поле	Описание
Расположение *	Расположение файла – полный путь к директории, в которой был обнаружен файл.
Имя файла	Имя файла. Data Discovery получает значение из файловой системы сканируемого ресурса.
Размер	Размер файла. Data Discovery получает значение из файловой системы сканируемого ресурса.
Доступен для	В поле **Доступен для** указывается список имен персон и групп, которые имеют доступ к файлу. В поле **Владелец** указывается имя персоны или группы, которая является владельцем файла. Персоны и группы идентифицируются Data Discovery по SID, значения которых он получает из файловой системы сканируемого ресурса. Data Discovery определяет имена по SID на основе данных из Active Directory (Подробнее об идентификации персон и групп см. *InfoWatch Data Discovery. Руководство пользователя. Таблица с информацией о файлах*). Если данные для идентификации персоны или группы отсутствуют, вместо имени будет указан SID. Например: `S-1-5-21-1922741149-3613679056-2300624754-1000`
Владелец	
Объекты защиты	Объекты защиты, которые Data Discovery детектировал в этом файле с помощью модуля контентного анализа (подробнее см. *InfoWatch Data Discovery. Руководство пользователя.*).
* Если содержимое какого-либо поля превышает размеры ячейки таблицы и не видно полностью, для просмотра наведите курсор на это поле. Информация будет отображена во всплывающем окне, где вы также можете скопировать ее в буфер, нажав . Скопированное значение поля **Расположение** при этом будет начинаться с адреса хоста.	

По умолчанию Data Explorer показывает все файлы в кластере, в том числе копии одного и того же файла. Но вы можете скрыть те файлы, которые минимально отличаются друг от друга. Для этого выключите опцию **Показывать редакции файла** над списком кластеров. Из каждого набора таких почти одинаковых файлов будет показан один случайный.

Чтобы скачать архив со всеми контентами, которые входят в кластер, нажмите .

Чтобы изменить порядок сортировки записей о файлах в таблице, нажмите на заголовок столбца, по которому нужно выполнить сортировку. Все записи таблицы будут отсортированы по возрастанию/убыванию значений выбранного столбца.

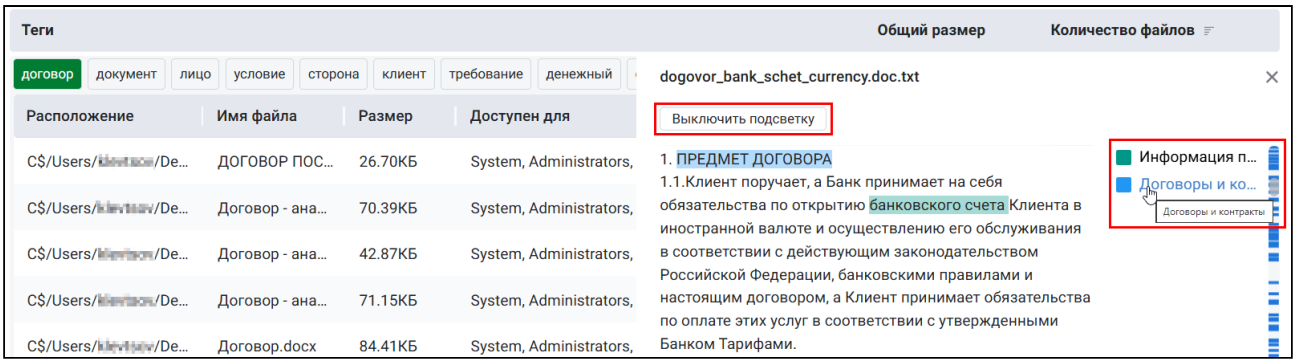
Чтобы переместить столбец, нажмите на заголовок столбца и перетащите его вдоль строки заголовков.

Чтобы изменить ширину столбца, нажмите на правую границу заголовка столбца и, не отпуская, перемещайте границу столбца.

7.1.2 Действия с файлами

Чтобы просмотреть извлеченные из файла текстовые данные, выберите строку в таблице. Справа откроется окно с содержимым файла. Если из файла не извлечены текстовые данные, окно будет содержать только имя файла.

Если модуль контентного анализа Data Discovery обнаружил в текстовом контенте объекты защиты, то относящиеся к ним фрагменты будут выделены цветом.

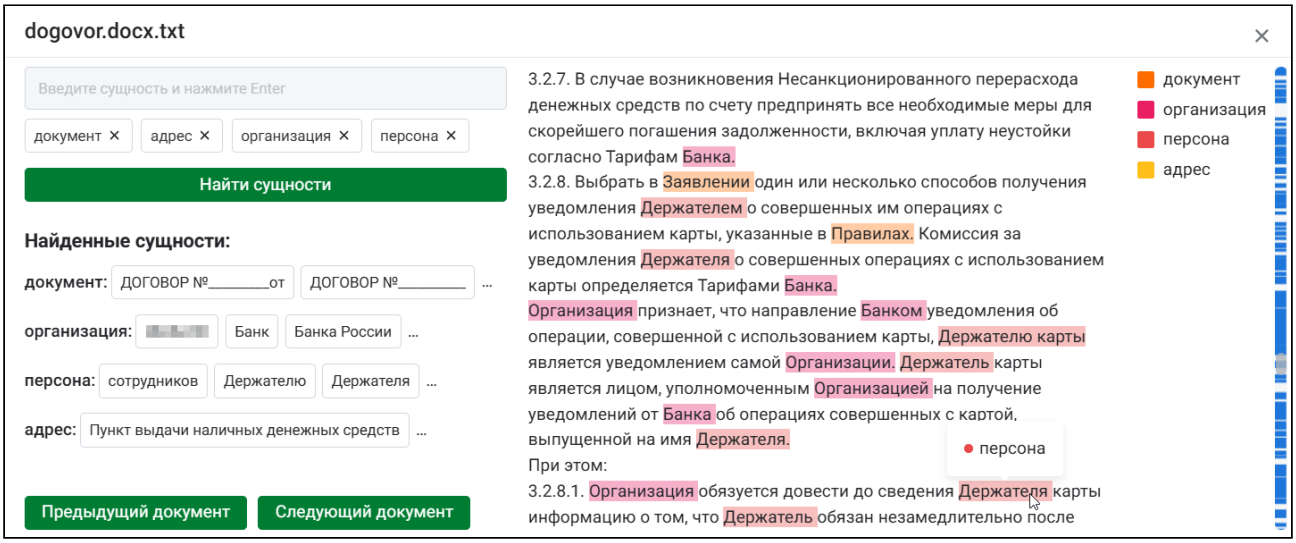


На легенде справа от текстовых данных будут перечислены названия обнаруженных объектов защиты. Чтобы выключить/включить подсветку фрагментов, относящихся к конкретному объекту защиты, нажмите на его название в легенде. Если навести курсор на выделенный цветом текстовый фрагмент, отобразится подсказка с именем объекта защиты.
Вы можете убрать все выделение цветом с помощью кнопки **Выключить подсветку** над содержимым.

Справа от каждого файла кластера вы можете нажать ⋮ и выбрать одно из доступных действий с файлом:

- **Копировать ссылку на файл**;
- **Подробно** – открыть содержимое файла для просмотра на весь экран.
  В этом режиме вы можете выполнить **поиск сущностей** в тексте.

> **Примечание:**
>
> Для поиска сущностей необходимо, чтобы в Data Analysis Service был включен модуль распознавания именованных сущностей. Подробнее см. *Data Analysis Service. Руководство по установке, конфигурированию и администрированию.*



Чтобы найти сущности:

1. Добавьте тип сущностей. Для этого введите его в строку поиска и нажмите **Enter**. Например, если указать тип сущностей "персона", то в тексте могут быть найдены такие сущности, как "Иванов Иван", "директор", "учредитель", "клиент" и т.п.
2. По аналогии с первым шагом добавьте другие типы сущностей, если необходимо.
3. Нажмите **Найти сущности**.
4. Дождитесь завершения поиска.
   Результаты будут выведены в левой части окна. А в тексте файла найденные сущности будут выделены цветом.

Для переключения между документами кластера не выходя из режима, используйте кнопки **Предыдущий документ** и **Следующий документ**.

7.1.3 Облако тегов

Чтобы просмотреть облако тегов, нажмите справа « **Развернуть**. В открывшейся области отобразятся теги, которые относятся к кластерам, удовлетворяющим условиям Единого фильтра в текущий момент.

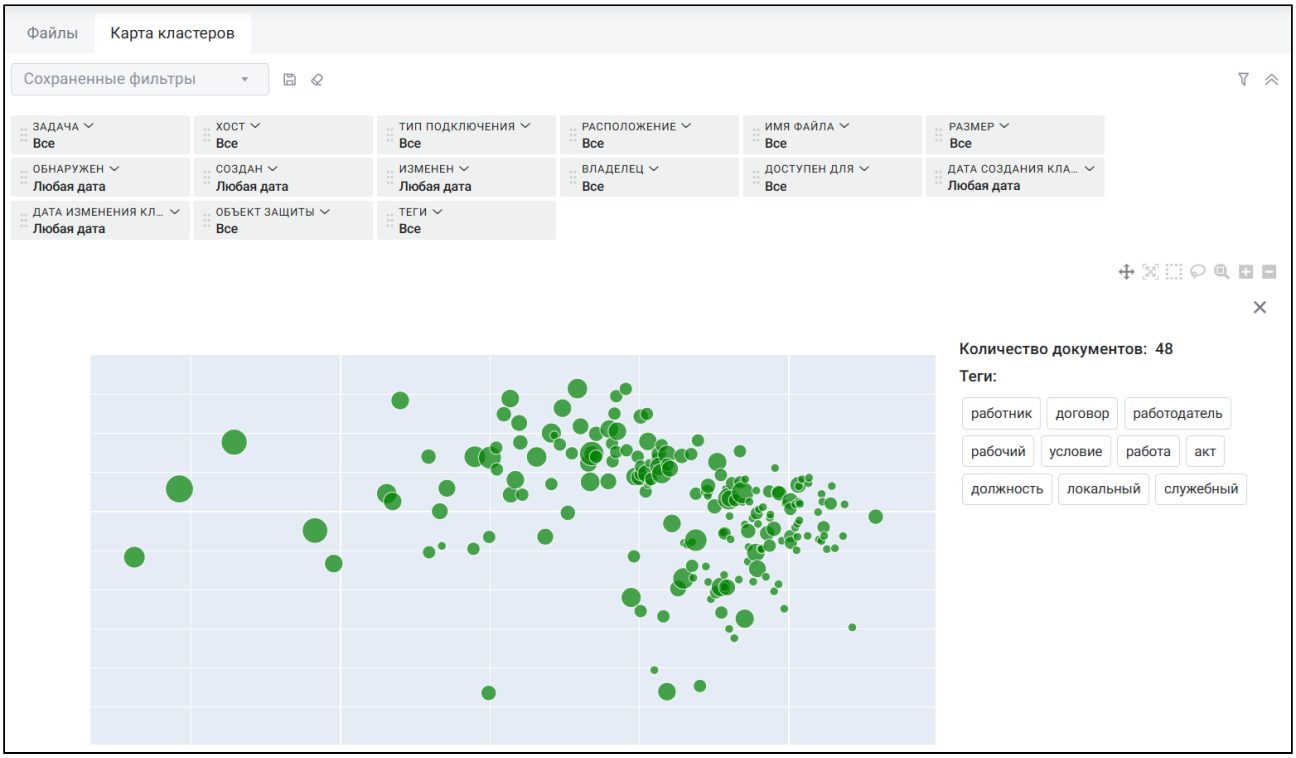
Вы можете отсортировать теги по убыванию или возрастанию частоты их встречаемости.

Выберите самые популярные теги, чтобы найти типовые документы для вашей компании и их примеры. Их можно использовать в работе с базой технологий для настройки политик InfoWatch Traffic Monitor (например, для обучения технологии Автолингвист).

Выбор редких тегов позволит обнаружить аномальные документы, хранящиеся на рабочих станциях сотрудников и других хранилищах.

7.2 Вкладка "Карта кластеров"

На данной вкладке каждый кластер изображен в виде круга на карте. Чем больше круг, тем больше файлов входит в кластер. Чем ближе круги друг к другу, тем ближе по смыслу документы в этих кластерах.



Справа находится панель инструментов для взаимодействия с картой. Для использования какого-либо инструмента, кликните на его значок на панели:

Обозначение	Действие
	Перетаскивайте карту, зажав левую или среднюю кнопку мыши в произвольном месте карты. Щелкните по кластеру на карте, чтобы справа увидеть информацию о нем: количество документов и теги этого кластера. Теги интерактивны: их можно выбирать, чтобы отфильтровать кластеры.
	Нажмите на значок, чтобы автоматически отмасштабировать карту.
 	Инструменты для выделения кластеров. С помощью прямоугольника или лассо обведите область, в которой находятся интересующие вас кластеры. Чтобы изучить их подробнее, после этого вы можете перейти на вкладку **Файлы**.
	Обведите область, которую хотите увеличить.
	Нажмите на значок, чтобы увеличить масштаб.

Обозначение	Действие
	Нажмите на значок, чтобы уменьшить масштаб.

Вы можете перемещаться между вкладками **Файлы** и **Карта кластеров** для анализа кластеров. Все параметры, выбранные на одной вкладке, сохраняются при этом перемещении.
Например, вы можете выбрать интересующие вас теги на вкладке **Файлы** и перейти на вкладку **Карта кластеров**. На карте будут показаны только те кластеры, которые содержат выбранные теги. Затем можно выделить на карте несколько кластеров, которые сильно отстоят от основной массы, и вернуться на вкладку **Файлы** для их подробного исследования.

Чтобы отменить выделение на карте кластеров, находясь на любой вкладке, нажмите **Отменить выделение**.

8 ПОЛЬЗОВАТЕЛЬСКОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями настоящего Лицензионного соглашения с конечным пользователем (далее – «Соглашение») перед началом работы с программным обеспечением. Установка и/или использование программного обеспечения означает ваше полное и безоговорочное согласие со всеми условиями настоящего Соглашения.

Если вы не согласны с условиями настоящего Соглашения, или если вы заключаете настоящее Соглашение от имени юридического лица, но у вас нет таких полномочий, вы должны прервать установку и/или прекратить использование программного обеспечения и удалить его копии.

1. Предоставление лицензии

1.1. Настоящее Лицензионное соглашение с конечным пользователем является договором присоединения, заключаемым между вами и ООО «Лаборатория ИнфоВотч», ИНН 7734583888 (далее – «Правообладатель»).

1.2. По настоящему Соглашению вам на условиях личной, не подлежащей передаче неисключительной лицензии предоставляются права на использование программного обеспечения Правообладателя (далее — «ПО»), а именно права загрузки, установки, резервного копирования и использования программного обеспечения по функциональному назначению в соответствии с условиями, указанными в Документации к ПО (Руководстве Пользователя, Руководстве Администратора, Руководстве по установке), настоящем Соглашении и Договоре, заключенном между вами и вашим лицензиаром. Документация к ПО признается частью настоящего Соглашения.

1.3. ПО предназначено только для использования в вашей текущей операционной деятельности. В случае если вы получили, загрузили и/или установили ПО, предназначенное для ознакомительных целей, вы имеете право использовать ПО только в целях ознакомления и только в течение ознакомительного периода. Любое использование ПО для других целей или по завершении ознакомительного периода запрещено.

1.4. Если вы используете ПО разных версий или версии ПО для разных языков, если вы получили ПО на нескольких носителях, если вы иным способом получили несколько копий ПО или получили ПО в составе пакета другого программного обеспечения, то общее число используемых вами лицензий не должно превышать их количества, определенного Договором между вами и вашим лицензиаром.

1.5. Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей или для замены правомерно приобретенного экземпляра в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Такая копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.

1.6. Вы самостоятельно несете ответственность и обеспечиваете соблюдение применимого экспортного и импортного законодательства, а также применимых торговых санкций и эмбарго в отношении передачи прав и использования ПО.

2. Условия использования

2.1. Программное обеспечение предназначено исключительно для использования в целях анализа и контроля информационных потоков в корпоративной среде, в том числе, для выявления и предотвращения случаев несанкционированного использования конфиденциальных данных.

2.2. Вы обязаны использовать ПО исключительно в соответствии с применимыми к вам требованиями законодательства Российской Федерации и иных стран, которые, не ограничиваясь, могут включать:

- законодательство о персональных данных;
- законодательство о коммерческой тайне;
- законодательство о противодействии неправомерному использованию инсайдерской информации;

- законодательство о противодействии коррупции;
- законодательство о критической информационной инфраструктуре;
- законодательство о государственных информационных системах;
- законодательство о защите данных в Национальной платежной системе;
- нормы Трудового кодекса РФ;
- а также иные применимые источники права.

2.3. Вы не вправе использовать ПО для любых целей или любым способом, нарушающим применимое законодательство, настоящее Соглашение и/или права третьих лиц. Правообладатель не несет ответственность за нарушение вами условий настоящего пункта.

2.4. Если вы не являетесь резидентом РФ, вы обязаны использовать ПО в соответствии с применимым правом, включая законы и нормативные акты, регламентирующие защиту персональных данных и коммерческой тайны.

2.5. Во избежание нарушения вами статей 138, 138.1 УК РФ, статьи 23 Конституции РФ и иных правовых норм перед началом использования программного обеспечения вам рекомендовано письменно проинформировать сотрудников о том, что:

- на рабочей станции используется данное ПО, о функциональности данного ПО и о данных, которые могут быть получены в результате применения данного ПО;
- рабочая станция и используемые каналы связи (электронная почта, локальная корпоративная сеть, телефония и IP-телефония и прочее) являются вашей собственностью и передаются им во временное пользование для выполнения служебных обязанностей;
- вся информация, созданная на рабочей станции, является вашей собственностью и подлежит контролю и логированию на законных основаниях.

2.6. Обращаем ваше внимание, что вам необходимо получить согласие лиц, данные которых будут обрабатываться при использовании ПО, на соответствующий сбор, хранение, использование, обработку, распространение и иную обработку указанных данных.

2.7. Напоминаем, что установка программы на компьютере другого лица без его ведома, получение личной информации третьих лиц без их ведома, нарушение неприкосновенности частной жизни, нарушение тайны переписки, телефонных переговоров, телеграфных и иных видов сообщений является уголовно наказуемым деянием и преследуется в соответствии с действующим законодательством Российской Федерации.

2.8. Правообладатель не имеет доступа к данным, созданным и/или полученным в рамках использования вами ПО. Вы имеете исключительный доступ к указанным данным. С учетом этого Правообладатель не осуществляет сбор, хранение, использование и распространение указанных данных.

2.9. Вы самостоятельно несете риск того, что данные, созданные и/или полученные в рамках использования вами ПО, могут содержать данные неэтического и/или противоправного характера, компьютерные вирусы или программы (или ссылки на них), способные прервать или нарушить нормальную функциональность компьютерного оборудования, программного обеспечения или средств телекоммуникации любых лиц.

2.10. Вам не разрешается:

- целиком или частично редактировать, изменять, адаптировать, переводить, декомпилировать, дизассемблировать, осуществлять инженерный анализ, создавать или воссоздавать исходный код, модернизировать, исправлять явные ошибки, модифицировать ПО и/или его компоненты, осуществлять попытки предпринять аналогичные действия в отношении ПО и/или его компонентов, а также создавать производные работы, основанные на ПО и/или Документации;
- использовать ПО сверх лицензируемого количества учетных записей, предусмотренных договором с вашим непосредственным лицензиаром;

- осуществлять интеграцию ПО в сторонние сайты и программные продукты, за исключением случаев, когда такая интеграция прямо разрешена Правообладателем и правообладателем сторонних сайтов и программных продуктов. Допускается интеграция ПО в сторонние программные продукты посредством встроенного модуля API в рамках функциональных возможностей указанного модуля;
- удалять или изменять уведомления об авторских правах, правах собственности на ПО и/или его элементы;
- использовать ПО с целью извлечения прибыли, сдавать ПО в аренду, прокат или во временное пользование, предоставлять подписку на ПО, предоставлять услуги аутсорсинга с использованием ПО, сублицензировать, распространять или иным образом предоставлять любому физическому или юридическому лицу любые права в отношении ПО и/или Документации, разглашать результаты стендовых испытаний ПО, за исключением случаев, прямо разрешенных настоящим Соглашением либо письменным согласием Правообладателя;
- передавать и предоставлять ссылку на дистрибутив и/или доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения и Договора, заключенного между вами и вашим лицензиаром;
- использовать ПО с целью создания данных или кода, предназначенных для использования другими программными продуктами;
- самостоятельно устанавливать дополнительные приложения к ПО, заменять компоненты ПО;
- осуществлять незаконный сбор, систематизацию, хранение и распространение конфиденциальной и/или персональной информации;
- использовать ПО для несанкционированного удаленного доступа к компьютерам третьих лиц, а также изменения конфигурации компьютера так, чтобы такие возможности могли появиться у стороннего ПО;
- собирать, хранить, использовать, обрабатывать и распространять с помощью ПО любые информационные данные, которые нарушают применимое законодательство, права и законные интересы третьих лиц.

2.11. Лицензионный ключ является конфиденциальной информацией, его несанкционированная передача третьим лицам запрещена. Правообладатель оставляет за собой право использовать средства для проверки подлинности установленного у вас лицензионного ключа.

3. Ограничение гарантий и ответственности Правообладателя

3.1. Программное обеспечение предоставляется «КАК ЕСТЬ» («AS IS») в соответствии с общепринятым в международной практике обычаем делового оборота. За проблемы, возникающие в процессе эксплуатации ПО, в том числе: проблемы совместимости с другими программными продуктами (пакетами, драйверами и др.), проблемы, возникающие из-за неоднозначного толкования Документации в отношении ПО, несоответствия результатов использования ПО вашим ожиданиям и т.п.) и иные, Правообладатель ответственности не несет.

3.2. Вы подтверждаете, что вам известны функциональные свойства ПО, в отношении которых предоставляется право использования, и самостоятельно несете риск соответствия ПО своим индивидуальным пожеланиям и потребностям, а также за результаты, полученные с его помощью.

3.3. Правообладатель не предоставляет никаких гарантий, выраженных или подразумеваемых, и настоящим отказывается от всех гарантий.

Правообладатель не гарантирует, что ПО не содержит ошибок, будет работать непрерывно, быстро, без неточностей, и не несет никакой ответственности за прямые или косвенные последствия использования ПО, в том числе возникшие из-за возможных ошибок в ПО или опечаток в ПО и/или прилагаемой или переданной позднее Документации.

Правообладатель не дает никаких гарантий и не несет никакой ответственности перед вами в случае любых изменений в программном обеспечении третьих лиц, произошедшее после установки/ внедрения ПО и повлекшее потерю функциональности ПО (включая, но не ограничиваясь, изменением протокола передачи данных, формата хранения данных, логике работы стороннего программного обеспечения, обновлением программного обеспечения, которое перестает поддерживать работу с ПО). Правообладатель не дает никаких гарантий, условий, представлений или положений (выражаемых в явной или в подразумеваемой форме) на все, включая без ограничений нарушения прав третьих лиц, коммерческое качество, интеграцию или пригодность для определенных целей.

3.4. Данные, которые становятся доступными при использовании ПО, включая файлы, ссылки, изображения и текст, являются исключительной ответственностью физического или юридического лица, от которого они были получены, и являются собственностью соответствующего лица. Настоящее Соглашение не дает никаких прав на такие данные. Вы принимаете на себя ответственность за возможные последствия, риски безопасности и любые убытки, вызванные такими данными, просмотренными или полученными Вами с помощью ПО.

3.5. Правообладатель не несет ответственности за какие-либо убытки, ущерб, независимо от причин его возникновения (включая, но не ограничиваясь прямым или косвенным ущербом, убытками связанными с недополученной прибылью, прерыванием коммерческой или производственной деятельности, утратой деловой информации, небрежностью, или какими-либо иными убытками), возникшие вследствие использования или невозможности использования ПО, даже если Правообладатель был уведомлен о возможных убытках. При любых обстоятельствах ответственность Правообладателя ограничена возмещением документально подтвержденного реального ущерба, ограниченного 3 000 (тремя тысячами) рублей, и возлагается на него при наличии в его действиях вины.

4. Права на объекты интеллектуальной собственности

4.1. Вы соглашаетесь с тем, что исключительные права на любые объекты интеллектуальной собственности, воплощенные в ПО и /или любой предоставленной вам документации, принадлежат Правообладателю. По настоящему Соглашению ПО не передается в собственность, не продается, а предоставляются права его использования на условиях ограниченной неисключительной лицензии. Ничто в данном Соглашении не предоставляет вам никаких прав на указанные объекты интеллектуальной собственности иные, чем предоставленные вам по Договору, заключенному между вами и вашим лицензиаром.

4.2. Вы соглашаетесь с тем, что исходный код, лицензионный ключ для ПО являются собственностью Правообладателя.

5. Права на информацию, доступ к которой получен вами в рамках осуществления настоящего Соглашения

5.1. Вы соглашаетесь с тем, что вам не принадлежат никакие права на любую информацию, не являющуюся объектом интеллектуальной собственности в соответствии с разделом 4, доступ к которой получен вами в рамках осуществления настоящего Соглашения.

5.2. К указанной информации, включая, но не ограничиваясь, относятся системы, методы работы, иная информация.

5.3. Указанная выше информация будет использоваться Вами только в целях осуществления прав на ПО, предоставленных вам по настоящему Соглашению и Договору с лицензиаром, без права использования указанной информации в собственных интересах и за пределами Соглашения и Договора, заключенного между вами и вашим лицензиаром.

6. Открытое программное обеспечение

Вы проинформированы **о том, что ПО содержит открытое программное обеспечение, распространяемое под определенными лицензиями, с которыми вы можете ознакомиться в файле licenses.inf (license.info), распространяемом с ПО в составе дистрибутива.**

Вы соглашаетесь с тем, что входящие в состав ПО программные компоненты внешних поставщиков предоставляются без гарантий доступа к обновленным версиям компонент и к иным программам, оборудованию, сертификатам на обучение или услугам внешних поставщиков.

7. Заключительные положения

7.1. Настоящее Соглашение вступает в силу с начала установки ПО и действует на протяжении всего периода использования.

7.2. В случае нарушения вами какого-либо из условий Соглашения и/или Договора, заключенного между вами и вашим лицензиаром, или в случае, если исполнение Соглашения или Договора, заключенного между вами и вашим лицензиаром будет нарушать или нарушает применимое право, Правообладатель вправе отказаться от исполнения Соглашения и расторгнуть его (включая, но не ограничиваясь, путем блокировки лицензионного ключа, прекращения предоставления прав) в любое время без уведомления вас. В указанном в настоящем пункте случае стоимость ПО/размер вознаграждения за права на ПО, а также возможные убытки по настоящему Соглашению и/или Договору, заключенному между вами и вашим лицензиаром, вам не возмещаются.

7.3. При расторжении или прекращении Соглашения Пользователь обязан уничтожить все копии установленного ПО.

7.4. Вы настоящим уведомляетесь о том, что при включении в ПО функции сбора статистики использования, ПО может осуществлять сбор и запись информации в обезличенном виде:

а) об аппаратном обеспечении, об операционной системе устройства, на котором установлено и эксплуатируется ПО, а также иная техническая информация, содержащая сведения об использовании аппаратных средств, нагрузке на аппаратные средства и быстродействии ПО;

б) данные о действиях конечного пользователя в пользовательском интерфейсе ПО.

Правообладатель вправе использовать указанные данные для принятия решений о развитии функциональности и улучшении эксплуатационных характеристик ПО.

Правообладатель обязуется обеспечить конфиденциальность полученных данных, не разглашать и не передавать их третьим лицам.

7.5. Настоящее Соглашение, а также любые споры, возникающие из или в связи с настоящим Соглашением, регулируются и истолковываются в соответствии с законодательством Российской Федерации.

7.6. Все споры и разногласия, возникающие в процессе исполнения Соглашения, будут по возможности разрешаться путем переговоров. В случае недостижения согласия, споры будут рассматриваться в судебном порядке в Арбитражном суде г. Москвы.

7.7. Настоящее Соглашение может быть изменено Правообладателем в любой момент без какого-либо уведомления. Новая редакция Соглашения вступает в силу с момента ее размещения по указанному в настоящем пункте адресу. С условиями действующей редакции Соглашения вы всегда можете ознакомиться по адресу https://kb.infowatch.com/display/EULA/. При этом продолжение использования ПО после внесения изменений и/или дополнений в настоящее Соглашение означает согласие с такими изменениями и/или дополнениями. В случае несогласия с условиями такого измененного Соглашения, вы обязаны немедленно отказаться от дальнейшего использования ПО.

8. Контактная информация Правообладателя

Тел./факс: +7(495)229-00-22

Коммерческий департамент: sales@infowatch.com

Служба технической поддержки: support@infowatch.com

Веб-сайт: www.infowatch.ru

9 Глоссарий

Термин	Определение
Администратор	Пользователь Системы, выполняющий установку, настройку и поддерживающий работу Системы. См. также: Офицер безопасности, Пользователь
Документ	Оригинальный документ сотрудника организации. Документ может содержать не только текст, но и изображение, видео, звук. Data Explorer кластеризует только текстовые контенты оригинальных документов. См. также: контент
Задача сканирования	Операция проверки ресурсов (путей сканирования) на наличие конфиденциальных данных, выполняемая Data Discovery
Интерфейс пользователя	Совокупность средств и методов, при помощи которых пользователь взаимодействует с Системой
Консоль управления	Графический интерфейс пользователя, предназначенный для работы с модулем Data Explorer
Контент	Фрагмент оригинального документа. Из документа может быть извлечено более одного контента. Текстовый контент содержит только текст, в нем не сохранены форматирование и структура оригинального документа
Лицензия	Право на использование Системы. Получается при приобретении Системы и определяет допустимые действия с Системой
Офицер безопасности	Основной пользователь Консоли управления. Также – предустановленная роль пользователя Консоли управления, имеющая привилегии на все действия в Системе, за исключением административных. См. также: Администратор, Пользователь
Пользователь	Пользователь модуля Data Explorer – администратор, офицер безопасности и др. См. также: Администратор, Офицер безопасности
Платформа	Принципиальная конструкция продукта – комплекс частей, подсистем, интерфейсов и производственных процессов. Продуктовая Платформа выступает в качестве базы для развертывания семейства продуктов и сборки готовых изделий из стандартизированных компонентов
Рабочая станция/ Компьютер	В терминах Системы подразумевается контролируемая рабочая станция или терминальное устройство

Термин	Определение
Сервис ClickHouse	Распределенная аналитическая столбцовая СУБД, предназначенная для проведения анализа по хранящимся данным в реальном времени. Компонент продуктовой Платформы
Сервис PostgreSQL	СУБД, которая используется в модуле Data Explorer для хранения настроек и данных. Компонент продуктовой Платформы
Хост (Host)	Рабочая станция или сервер, к которому Data Discovery подключается для сканирования файлов и загрузки с него файлов для дальнейшего анализа
Active Directory (AD)	LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT
InfoWatch Data Analysis Service	Data Analysis Service предназначен для потоковой постобработки и анализа данных, предоставляемых продуктами компании InfoWatch. Для Data Explorer используются модуль протокластеризации текстовых данных и модуль распознавания именованных сущностей
InfoWatch Data Discovery	Data Discovery предназначен для поиска конфиденциальной информации на общих сетевых ресурсах, рабочих станциях, серверах и в хранилищах документов
InfoWatch Traffic Monitor	Traffic Monitor – программный комплекс, предназначенный для контроля различных видов трафика (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) и теневых копий данных, копируемых на съемные носители и отправляемых на печать
Kubernetes	Программное обеспечение для оркестрации контейнеризированных приложений – автоматизации их развертывания, масштабирования и координации в условиях кластера
NATS	Система обмена сообщениями для компонентов
SSH (Secure Shell)	Сетевой протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов)