

InfoWatch Data Discovery. Руководство пользователя

18/01/2024

© АО "ИнфоВотч"

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1	Аудитория	5
2	Комплект документов	6
3	Техническая поддержка пользователей	
4	Функциональные возможности Data Discovery	8
5	Интерфейс Data Discovery	9
5.1	Разделы Data Discovery	10
5.2	Раздел "Задачи"	10
	I. Действия, доступные в разделе	
	2 Задача сканирования	
	Сканирование ресурсов	
	Событие Traffic Monitor	13
5.2.3	3 Создание, настройка и запуск задачи	15
	Создание задачи	15
	Запуск задачи сканирования	15
	Настройки задачи	16
	Добавление и настройка хостов	29
	Добавление путей сканирования	36
	Примеры настроек задачи, хоста и добавления путей сканирования	37
5.2.4	4 Редактирование задачи и хоста	43
5.2.5	5 Копирование задачи	44
5.2.6	5 Удаление задачи, хостов и путей сканирования	44
5.2.7	7 Статистика выполнения задач	46
	Статистика по задачам	46
	Статистика по хостам	47
	Статистика по путям сканирования	49
5.3	Раздел "Информация о файлах"	50
5.3.1	L Таблица с информацией о файлах	51
	Добавление записей в таблицу в рамках задачи	51
	Структура таблицы с информацией о файлах	51
	Идентификация персон и групп	54
	Действия с файлами	55
5.3.2	2 Настройка отображения таблицы	56
5.3.3	3 Поиск дубликатов	56
	Поиск по образцу	56
	Сброс результатов поиска	57

5.3.4	Выгрузка информации о файлах	57
5.3.5	БПример работы с таблицей	57
	Настройка фильтров	58
	Результаты фильтрации	59
5.4	Раздел "Досье"	61
5.4.1	. Просмотр досье персоны	62
5.4.2	Вкладка "Персональная информация"	63
5.4.3	Вкладки Владелец файлов и Доступные файлы	64
5.4.4	Создание, редактирование и удаление досье	64
5.4.5	Добавление контактов персоны	65
5.4.6	З Изменение руководителя персоны	66
5.4.7	7 Объединение досье	66
5.5	Единый фильтр	66
5.5.1	. Фильтры	67
5.5.2	. Переход в другие продукты Платформы	69
5.5.3	В Работа с Единым фильтром	69
	Добавление и удаление фильтров	69
	Значения фильтров	69
	Сохранение и загрузка наборов фильтров	72
6	Пользовательское лицензионное соглашение	73
7	Глоссарий	78

В настоящем руководстве вы сможете найти сведения по работе в InfoWatch Data Discovery (далее Система или Data Discovery) – программном обеспечении, предназначенном для поиска конфиденциальной информации на общих сетевых ресурсах, рабочих станциях, серверах и в хранилищах документов.

Веб-консоль управления (далее также Консоль управления) имеет интуитивно понятный интерфейс, поэтому настоящее руководство содержит только общую информацию и ряд примеров, представляющих функциональность Системы.

1 Аудитория

Информация, содержащаяся в руководстве, предназначена для пользователей, работающих с Системой (выполняющих настройку конфигурации, анализ информационных ресурсов и т. п.). Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Linux и СУБД PostgreSQL.

2 Комплект документов

В документацию входят:

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

Сопутствующая документация по системе InfoWatch Traffic Monitor включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание установки, настройки, обновления и удаления 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, подготовка 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 Системы, 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.

Часы работы Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: www.infowatch.ru/services/support.

4 Функциональные возможности Data Discovery

Система Data Discovery предназначена для поиска конфиденциальной информации на общих сетевых ресурсах, рабочих станциях, серверах и в хранилищах документов. Система работает следующим образом:

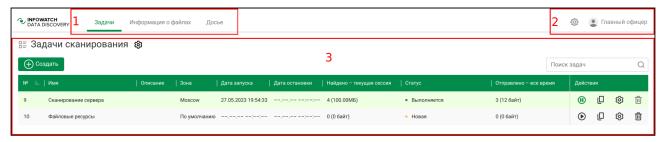
- Система подключается к различным ресурсам.
- Система сканирует файлы на ресурсах и собирает метаданные файлов.
- Система отправляет данные в Traffic Monitor для анализа, если отправка настроена в задаче сканирования.
- Система отображает метаданные просканированных файлов.

Используя Data Discovery, вы можете:

- подключаться к общим сетевым ресурсам и к распределенным файловым системам (DFS) по протоколу SMB:
 - подключаться к SMB-ресурсам, созданным на хостах под управлением MS Windows;
 - подключаться к SMB-ресурсам, созданным на хостах под управлением Linux;
- подключаться к рабочим станциям и серверам под управлением Linux по протоколу SSH;
- подключаться к библиотекам документов в SharePoint Server 2016 по протоколу HTTPS;
- подключаться к файловым ресурсам по протоколу FTP;
- подключаться к хранилищу данных Nextcloud по протоколу WebDAV;
- сканировать файлы на ресурсах:
 - обнаруживать новые и измененные файлы;
 - собирать метаданные файлов;
 - создавать копии файлов для анализа в Traffic Monitor;
- отправлять данные на сервер Traffic Monitor для анализа;
- просматривать статистику о выполнении задач сканирования;
- просматривать информацию о файлах;
- выгружать информацию о файлах;
- искать дубликаты файлов.

5 Интерфейс Data Discovery

Работа с Data Discovery ведется в Консоли управления:



Элементы интерфейса Data Discovery:

Номер на схеме	Элемент	Назначение элемента
1	Панель навигации	Выбор рабочего раздела Data Discovery: Задачи, Информация о файлах, Досье
2	Настройки	В разделе доступны: настройки пользователей и ролей; общие настройки Системы; настройки интеграций; управление лицензиями; настройки зон и серверов.
	Отчеты	В этом разделе вы можете скачать файлы отчетов. Подробнее см. "Выгрузка информации о файлах"
	Меню пользователя	В Меню пользователя вы можете: отредактировать свою учетную запись; сменить пароль своей учетной записи; поменять язык интерфейса; ознакомиться с Руководством пользователя; просмотреть информацию о Системе и узнать контактные данные компании InfoWatch и службы поддержки; выйти из Системы.
3	Рабочая область	Отображение элементов выбранного раздела Data Discovery

Система может быть установлена совместно с другими продуктами Платформы. Чтобы перейти в интерфейс другого продукта Платформы, нажмите в левом верхнем углу и выберите продукт.

5.1 Разделы Data Discovery

Работа с Data Discovery ведется в следующих разделах:

Раздел	Описание
Задачи	Раздел содержит список задач сканирования и подробную информацию о каждой из них
Информация о файлах	В разделе отображается информация о файлах, которые были просканированы в рамках задач. Доступна фильтрация данных в разделе с помощью Единого фильтра (см. "Единый фильтр")
Досье	Раздел содержит справочник персон компании, а также позволяет просмотреть, какими файлами владеет и к каким файлам имеет доступ конкретная персона

5.2 Раздел "Задачи"

Раздел содержит список задач сканирования и подробную информацию о каждой из них.

О работе задач сканирования см. "Задача сканирования".

5.2.1 Действия, доступные в разделе

Следующие основные действия доступны при работе с разделом:

- Создание, настройка и запуск задачи (см. "Создание, настройка и запуск задачи"):
 - Добавление и настройка хостов (см. "Добавление и настройка хостов")
 - Добавление путей сканирования (см. "Добавление путей сканирования")
- Редактирование задачи и хоста (см. "Редактирование задачи и хоста")
- Копирование задачи (см. "Копирование задачи")
- Удаление задачи, хостов и путей сканирования (см. "Удаление задачи, хостов и путей сканирования")
- Просмотр статистики и информации о задачах (см. "Статистика выполнения задач")

5.2.2 Задача сканирования

Задача сканирования – операция проверки ресурсов (путей сканирования) на наличие конфиденциальных данных. Доступны два режима выполнения задачи (см. "Создание, настройка и запуск задачи", параметр Выполнение задачи):

• Непрерывное выполнение – Система циклично сканирует ресурсы, пока пользователь не остановит задачу вручную или пока она не будет остановлена автоматически по расписанию.

• Разовое выполнение – задача останавливается автоматически, если был выполнен один проход по каждому ресурсу.

При повторном запуске задачи не осуществляется полное повторное сканирование - обработка ресурсов продолжается с того места, где она закончилась в предыдущем сканировании.

Хост - рабочая станция или сервер, к которому осуществляется подключение для сканирования файлов. Хост содержит список ресурсов, которые называются Пути сканирования. При создании задачи сканирования в задачу необходимо добавить хосты, для каждого хоста необходимо добавить пути сканирования (подробнее про создание и настройку задачи см. "Создание, настройка и запуск задачи").

Проход - полное сканирование одного ресурса. Проход может состоять из нескольких сессий.

Сессия - подключение к ресурсу в рамках прохода.

Подробнее об обработке ресурсов см. "Сканирование ресурсов". О событиях, которые Система отправляет в Traffic Monitor см. "Событие Traffic Monitor".

Сканирование ресурсов

Типы ресурсов

Создав задачу, вы можете сканировать:

- общие сетевые ресурсы и распределенные файловые системы (DFS) по протоколу SMB:
 - SMB-ресурсы на хостах под управлением MS Windows;
 - SMB-ресурсы на хостах под управлением Linux;
- файловые системы серверов и рабочих станций под управлением Linux по протоколу SSH;
- библиотеки документов в SharePoint Server 2016 по протоколу HTTPS;
- файловые ресурсы по протоколу FTP;
- хранилища Nextcloud по протоколу WebDAV.

примечание:

Система не проверяет подлинность сертификата сервера при подключении к SharePoint.

Поддерживается сканирование Nextcloud версии 25 и более новых.

Подключение по протоколу WebDAV проходит без проверки TLS/SSL-сертификатов.

Учетная запись для сканирования

Учетная запись, которую Система использует для сканирования ресурсов, должна иметь следующие права:

- Право на чтение общего сетевого ресурса (при SMB-подключении);
- Право на чтение директорий;
- Право на вывод списка содержимого директорий;
- Право на чтение файлов.

Значения параметров для учетной записи указываются в настройках задачи и в настройках хоста (подробнее см. "Создание, настройка и запуск задачи").

Обработка файлов в рамках задачи

В рамках первого прохода по ресурсу Data Discovery выполняет следующие действия со всеми файлами на ресурсе:

- Собирает метаданные файла и добавляет их в таблицу с информацией о файлах (см. Раздел "Информация о файлах").
- Если параметр Собирать только информацию о файлах не включен:
 - Скачивает файл с ресурса в хранилище задачи.
 - Отправляет событие на сервер Traffic Monitor для анализа. Событие состоит из копии файла и информации о файле.



Примечание:

Если размер файла превышает 4 ГБ, Система не скачивает его и не отправляет событие в Traffic Monitor.

При последующих сессиях Система обрабатывает только новые и измененные файлы. Чтобы определить измененные файлы, Система проверяет метаданные файлов на изменения:

- Путь к файлу;
- Имя файла;
- Размер файла;
- Дата и время изменения файла;
- Владелец файла;
- Пользователи/группы, которые имеют доступ к файлу.



Важно!

Проверка следующих метаданных на изменения поддерживается только при сканировании SMB-ресурсов на хостах под управлением ОС семейства Windows:

- Владелец файла
- Пользователи/группы, которые имеют доступ к файлу

Если файл является новым или измененным, то Система:

- Добавляет метаданные файла в таблицу с информацией о файлах (см. Раздел "Информация о файлах").
- Если параметр Собирать только информацию о файлах не включен:
 - Скачивает файл с ресурса в хранилище задачи.
 - Отправляет событие на сервер Traffic Monitor для анализа.



Примечание:

Если в настройках задачи включен параметр Дополнительно проверять неизмененные файлы, то при каждом проходе по ресурсу Data Discovery скачивает файл и проверяет содержимое файла на наличие изменений (подробнее про параметр см. "Создание, настройка и запуск задачи"). Если содержимое файла изменилось, то файл отправляется в составе события в Traffic Monitor.

Если размер файла превышает 4 ГБ, Система не скачивает его и не отправляет событие в Traffic Monitor.

Ошибки при сканировании

При сканировании могут возникать ошибки, например:

- Система не может подключиться к ресурсу;
- у Системы недостаточно прав для обработки директории/файла.

Если Система не может подключиться к ресурсу, то Система перейдет к обработке другого ресурса. В рамках задачи Система будет периодически пытаться подключиться к ресурсу, к которому не удалось подключиться ранее.

Если Система не может обработать директорию/файл, то Система пропустит директорию/файл. Система попытается обработать директорию/файл повторно при следующем подключении к ресурсу.

Событие Traffic Monitor

Data Discovery отправляет в Traffic Monitor события, которые содержат информацию о файлах. В каждом событии копия файла является вложением.

примечание:

Тип события и перехватчик, указанные в событии в Traffic Monitor, зависят от версии Traffic Monitor:

- Для Traffic Monitor версии 7.3 и ниже: тип события Краулер, перехватчик Crawler;
- Для Traffic Monitor версии выше 7.3: тип события Data Discovery, перехватчик Data Discovery.

Атрибуты события, которое формирует Data Discovery для отправки в Traffic Monitor:

Атрибут события	Описание
Отправители	Data Discovery отправляет SID владельца файла, например: S-1-5-21-1922741149-3613679056-2300624754-1 000 Система получает значение из файловой системы ресурса. Примечание: Traffic Monitor может идентифицировать персону по полученному SID.

Атрибут события	Описание
Получатели	Data Discovery отправляет список SID пользователей и групп, которые имеют доступ к файлам.
	Система получает значение из файловой системы ресурса.
	Примечание: Traffic Monitor может идентифицировать персону или группу по полученному SID.
Компьютер	IP-адрес хоста или доменное имя хоста, на котором был найден файл.
	Примечание: Traffic Monitor может идентифицировать рабочую станцию по полученной информации о хосте.
Название задачи	Название задачи сканирования в Data Discovery, в рамках которой файл был скачан с ресурса.
Дата запуска задачи	Дата и время начала сессии, в рамках которой файл был скачан с ресурса
Дата создания файла	Дата и время создания файла на хосте.
	Система получает значение из файловой системы ресурса.
	Примечание: Определение даты создания файла не поддерживается в следующих случаях:
	• при сканировании SMB-ресурсов на хостах под управлением Linux;
	 при сканировании хостов под управлением Linux по протоколу SSH.
	В этих случаях атрибут заполняется значением атрибута события Дата изменения файла.
Дата изменения файла	Дата и время изменения файла на хосте.
	Система получает значение из файловой системы ресурса.
Путь к файлу или адрес приемника	Полный путь к файлу на хосте
	Примечание: Полный путь включает в себя путь сканирования ресурса. Для файлов с SharePoint-хостов полный путь также включает в себя путь к сайту.
Дата перехвата	Дата и время, когда файл был скачан Системой
Сервер перехвата	Сервер Data Discovery, который обрабатывал ресурс

∆ Важно!

Получение SID владельца файла и SID пользователей/групп, которые имеют доступ к файлу, поддерживается для:

- SMB-ресурсов на хостах под управлением ОС семейства Windows;
- библиотек документов в SharePoint Server 2016.

Возможно некорректное заполнение атрибутов Отправители и Получатели, если:

- Производится сканирование SMB-ресурса на хосте под управлением Linux;
- Производится сканирование SMB-ресурса, созданного на сервере SMB, который не поддерживает файловые атрибуты для определения владельца файла и пользователей/групп, которые имеют доступ к файлу;
- Производится сканирование SMB-ресурса, созданного в файловой системе, которая не поддерживает файловые атрибуты для определения владельца файла и пользователей/групп, которые имеют доступ к файлу.

Получение SID владельца файла и SID пользователей/групп, которые имеют доступ к файлу, не поддерживается при сканировании хостов:

- под управлением Linux по протоколу SSH;
- по протоколу FTP;
- по протоколу WebDAV.

В этом случае атрибуты Отправители и Получатели имеют значение "iw data discovery".

5.2.3 Создание, настройка и запуск задачи

Создание задачи

Чтобы создать новую задачу сканирования:

- 1. Нажмите на раздел Задачи, чтобы перейти к списку задач сканирования.
- 2. В левом верхнем углу нажмите 🕀 Создать.
- 3. В открывшемся окне настройте задачу и нажмите Сохранить (см. "Настройки задачи").
- 4. Добавьте в задачу хосты (см. "Добавление и настройка хостов").
- 5. Для хостов добавьте пути сканирования (см. "Добавление путей сканирования").



Важно!

Вы не можете запустить задачу, если в задаче нет путей сканирования.

См. также "Примеры настроек задачи, хоста и добавления путей сканирования".

Запуск задачи сканирования

Новая задача имеет статус:

• Новая, если для задачи не был настроен автоматический запуск по расписанию;

Для запуска задачи нажмите в столбце Действия в списке задач сканирования. При этом статус
задачи изменится на Выполняется, а кнопка запуска задачи изменится на
остановить задачу.

• Ожидает запуск по расписанию, если для задачи был настроен автоматический



Важно!

запуск по расписанию.

Вы можете запустить задачу сканирования, только если в Системе есть активная лицензия (см. "InfoWatch Data Discovery. Руководство администратора", "Лицензирование").

Подробнее о запущенной задаче можно узнать, просмотрев статистику (см. "Статистика выполнения задач").

Настройки задачи



примечание:

Поля, обязательные к заполнению, отмечены в интерфейсе значком $\stackrel{\bigstar}{\blacksquare}$.

Доступны следующие настройки:

1. Вкладка **Общие**:

а. Основные настройки задачи:

Параметр	Описание
Название	Название задачи
Описание	Краткое описание задачи

Параметр	Описание
Выполнение задачи	Режим выполнения задачи. Непрерывное: • Система циклично сканирует ресурсы, пока пользователь не остановит задачу вручную или пока она не будет остановлена автоматически по расписанию. • При повторном запуске задачи не осуществляется полное повторное сканирование – обработка ресурсов продолжается с того места, где она закончилась в предыдущем сканировании. Разовое:
	 Система выполняет один проход по каждому ресурсу, после чего задача считается завершенной. Задача автоматически останавливается и получает статус Завершена. Если запустить задачу, которая имеет статус Завершена, то Система: обработает новые и измененные файлы на каждом ресурсе; остановит задачу и установит статус Завершена. задача получает статус Завершена, если был выполнен проход по каждому доступному ресурсу. Задача со статусом Завершена может содержать ресурсы со статусом Ошибка, которые Система не смогла обработать. Если параметр Собирать только информацию о файлах отключен, то задача получит статус Завершена, только когда все данные будут отправлены в Traffic Monitor. задача может запускаться и останавливаться по расписанию. Задача остановится, если Система выполнила один проход по каждому ресурсу или если наступило время автоматической остановки по расписанию. Важно: В обоих случаях задача получит статус Ожидает запуск по расписанию.
Собирать только информацию о файлах	В рамках задачи сканирования Система собирает метаданные файла и добавляет их в таблицу с информацией о файлах. Информация о файлах,

Параметр	Описание
	включая метаданные файлов, доступна для просмотра в разделе Информация о файлах.
	• Если параметр включен (), то Система собирает только метаданные файлов, но не скачивает файлы и не отправляет события в Traffic Monitor.
	• Если параметр отключен(), то Система не только собирает метаданные файлов, но и скачивает файлы, после чего отправляет события в Traffic Monitor. Вы можете отключить параметр, если в зоне задачи настроен экспорт данных (см. "InfoWatch Data Discovery. Руководство администратора", "Зоны и серверы").

b. Секция **Авторизация для доступа к ресурсам**:

Параметр	Описание
Группа SMB	Домен или группа. Параметр используется для хостов с SMB-подключением.
Логин	Имя пользователя Важно: Для подключения к SharePoint необходимо указать значение в формате: domain\user
Пароль	Пароль

примечание:

Если значения параметров авторизации не указаны, то по умолчанию для подключения к SMB-хостам в рамках задачи будет использоваться анонимный доступ.

Чтобы ускорить сканирование хранилища Nextcloud, для подключения используйте пароль приложения (подробнее см. примечание в пункте Сторонние клиенты WebDAV из официальной документации Nextcloud).

- 2. Вкладка Фильтры файлов фильтры по размеру и именам файлов:
 - а. Фильтр Размер позволяет установить ограничения на размер файла. Если размер файла подходит под условие, установленное в фильтре, то файл будет просканирован.
 - В поле От укажите минимальный размер файла. Вы не можете указать значение больше 4 ГБ.

- В поле **До** укажите максимальный размер файла. Вы не можете указать значение больше 4 ГБ.
- Справа от каждого из указанных полей фильтра отображается текущая единица измерения. Чтобы изменить единицу измерения для поля, нажмите на единицу измерения и выберите требуемое значение в раскрывающемся списке.

примечание:

Если указан только минимальный размер файла, то будут просканированы файлы, чей размер больше или равен минимальному размеру. Если указан только максимальный размер файла, то будут просканированы файлы, чей размер не превышает максимальный размер.

примечание:

Если размер файла превышает 4 ГБ, то Система не скачивает файл и не отправляет событие в Traffic Monitor. Запись о файле добавляется в таблицу с информацией о файлах (см. "Таблица с информацией о файлах").

- b. Список добавленных масок содержит маски имен файлов:
 - Система сканирует файл, если имя файла подходит под условие маски.

Важно!

Если не указать ни одну маску, Система будет сканировать файлы с любыми именами, включая системные файлы. Отправка большого количества файлов на сервер Traffic Monitor может значительно повысить нагрузку на Traffic Monitor.

- Действия с масками:
 - Чтобы добавить маску:
 - i. Нажмите на поле **Добавьте маску файла**. В открывшемся списке отображаются предустановленные категории файлов и маски для форматов.
 - іі. Выполните одно из действий:
 - Выберите маски/категории в списке. Для поиска начните вводить маску или имя категории в поле.
 - Введите маску в поле и выберите эту маску в списке.
 - ііі. Щелкните вне списка.

 - Чтобы экспортировать список масок в файл, нажмите
 - Вы можете импортировать список масок из файла. Требуется файл с расширением .txt, каждая маска должна быть указана на отдельной строке.

Чтобы импортировать список масок:

- і. Нажмите
- іі. В открывшемся окне выберите файл.

примечание:

В результате импорта в задаче останутся только маски, указанные в файле, остальные будут удалены.

- Формат для масок имен файлов:
 - Для составления маски имени используйте следующие символы:
 - символ "*" означает любую последовательность символов, в том числе отсутствие символов;
 - символ "?" означает один любой символ.

Примеры масок

- *.doc файлы, имена которых оканчиваются на '.doc' (example.doc, отчет.doc)
- *отчет* файлы, имена которых включают 'отчет' (новый_отчет.txt, отчетность.pdf)

отчет????.pdf - файлы с именами вида: 'отчет' + 4 символа + '.pdf' (отчет2012.pdf, отчеты_22.pdf)

file.txt - файлы, у которых имя 'file.txt'

- Фильтр по именам файлов не учитывает регистр.
- 3. Вкладка Фильтры папок:
 - Чтобы исключить директорию и все ее поддиректории из сканирования, введите полный путь к этой директории в поле Исключить и нажмите 🖭. Путь к директории будет добавлен в Список исключенных папок.

примечание:

По умолчанию Список исключенных папок содержит системные директории для административных ресурсов Windows.

- Чтобы включить директорию и все ее поддиректории в сканирование, введите полный путь к этой директории в поле Включить и нажмите 🖭. Путь к директории будет добавлен в Список включенных папок. Если в Список включенных папок не добавлена ни одна директория, то будут просканированы все директории, кроме исключенных из сканирования.
- Чтобы удалить директорию из списка включенных/исключенных папок, нажмите справа от директории в списке.



Важно!

Исключение директорий из сканирования имеет более высокий приоритет, чем включение директорий в сканирование. Например, если исключить директорию share/documents/folder и включить директорию share/documents/folder/example, то директория share/documents/folder/example обработана не будет.

• Формат пути к директории:

- Полный путь к директории последовательность из имен директорий, разделенных символом "/", которая указывает на расположение директории в файловой системе.
- Для **SMB**-ресурсов полный путь к директории должен включать в себя имя ресурса. Полный путь к директории не должен начинаться с символа "/".
- Для **SSH**-ресурсов полный путь к директории должен включать в себя путь сканирования. Полный путь к директории должен начинаться с символа "/".
- Для **SharePoint**-ресурсов полный путь к директории должен включать в себя имя библиотеки документов. Полный путь к директории не должен начинаться с символа "/".
- Для **FTP**-ресурсов полный путь к директории должен включать в себя путь сканирования. Полный путь к директории должен начинаться с символа "/".
- Для хранилищ Nextcloud по протоколу WebDAV полный путь к директории должен включать в себя путь сканирования. Полный путь к директории должен начинаться с символа "/".
- Фильтры по директориям не учитывают регистр. Примеры путей к директориям

Для SMB-хоста:

• Если необходимо просканировать директорию /folder/example и все ее поддиректории на общем сетевом ресурсе share, то добавьте в Список включенных папок путь

share/folder/example

• Если необходимо исключить из сканирования директорию /system/
files и все ее поддиректории на общем сетевом ресурсе
resource, то добавьте в Список исключенных
папок путь resource/system/files

Для SSH-хоста:

• Если в качестве пути сканирования на SSH-хосте указан путь /home/folder

и необходимо просканировать директорию / home/folder/example и все ее поддиректории, то добавьте в Список включенных папок путь

/home/folder/example

• Если в качестве пути сканирования на SSH-хосте указан путь /home/documents и необходимо исключить из сканирования директорию /home/documents/old_files и все ее поддиректории, то добавьте в

Список исключенных папок путь

/home/documents/old_files

Для протоколов FTP и WebDAV формат указания путей к директориям аналогичен SSH.

Для SharePoint-хоста:

• Если необходимо просканировать директорию /folder/example и все ее поддиректории в библиотеке library, то добавьте в Список включенных папок путь

library /folder/example

• Если необходимо исключить из сканирования директорию / outdated/reports и все ее поддиректории в библиотеке documents, то добавьте в Список исключенных папок путь documents/outdated/reports

• Маски для имен директорий:

Имя каждой директории в полном пути к директории можно указать в формате маски. Для составления маски имени используйте следующие символы:

- символ "*" означает любую последовательность символов, в том числе отсутствие символов;
- символ "?" означает один любой символ.

•

Важно!

Символы "*" и "?" используются только в рамках имени одной директории. Например, путь share/folder/example не подходит под условие маски share/*/example, но подходит под условие маски share/*/example

Примеры путей с использованием масок

Тип хоста	Пример пути	Описание	Директории, подходящие под условие
	*/Example	Директория Example и все ее поддиректории, если Example находится в корневом каталоге ресурса	C\$/Example share/example
SMB	*/*/*/Example	Директория Example и все ее поддиректории, если Example находится на три уровня ниже	mvshare/path/to/ Example

Тип хоста	Пример пути	Описание	Директории, подходящие под условие
		корневой директории ресурса	
	share/Doc*	Директория и все ее поддиректории, если директория находится в корневом каталоге ресурса share и ее имя начинается с " Doc "	share/Doc share/documents
	?\$/Users/*/ Documents	Директория Documents и все ее поддиректории у каждого пользователя на скрытом ресурсе	C\$/Users/Ivanov/ Documents D\$/Users/Petrov/ Documents
	share/documents/*/*	Все поддиректории для директории documents на ресурсе share , но не сама директория documents . Пути такого вида поддерживаются только для включающего фильтра (Список включенных папок)	share/documents/ reports share/documents/ templates
Share Point	*/Example	Директория Example и все ее поддиректории, если Example находится в корневом каталоге библиотеки документов	my_library/example
	//Example	Директория Example и все ее поддиректории, если Example находится на три уровня ниже корневой директории библиотеки документов	documents/2021/ folder/Example
	Library/Doc*	Директория и все ее поддиректории, если директория находится в корневом каталоге библиотеки Library и имя директории начинается с " Doc "	Library/Documents

Тип хоста	Пример пути	Описание	Директории, подходящие под условие
	storage/documents/ */*	Все поддиректории для директории documents в	storage/documents/ reports
		библиотеке storage, но не сама директория documents. Пути такого вида поддерживаются только для включающего фильтра (Список включенных папок)	storage/documents/ templates
SSH, FTP, WebD	/home*	Директория и все ее поддиректории, если директория находится в корневом каталоге и ее имя начинается с "home"	/home /HomeFolder
AV	/home/*/*/Example	Директория Example и все ее поддиректории, если Example находится на 3 уровня ниже папки home	/home/path/to/ Example
	/home/*/Documents	Директория Documents и все ее поддиректории у каждого пользователя на рабочей станции под управлением Linux (для SSH-хоста)	/home/ivanov/ Documents
	/home/*/*	Все поддиректории для	/home/username
		директории home, но не сама директория home. Пути такого вида поддерживаются только для включающего фильтра (Список включенных папок)	/home/folder

4. Вкладка Расписание – настройки для автоматического запуска и остановки задачи:

∆ Важно!

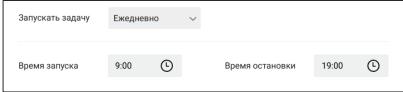
Задача не будет запущена автоматически, если в Системе отсутствует активная лицензия (см. "InfoWatch Data Discovery. Руководство администратора", "Лицензирование").

• Если задачу не требуется запускать и останавливать автоматически, в поле Запускать задачу выберите Вручную.

• Если задачу требуется запускать и останавливать автоматически каждый день в одно и то же время, в поле Запускать задачу выберите Ежедневно. В поле Время запуска и в поле Время остановки укажите время в формате H:mm или HH:mm.

Примеры ежедневного расписания

1) Задача автоматически запускается каждый день в 9:00 и останавливается в 19:00:

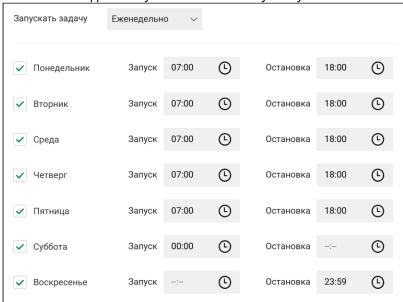


2) Задача автоматически запускается каждый день в 18:00 и останавливается в 7:00 следующего дня:

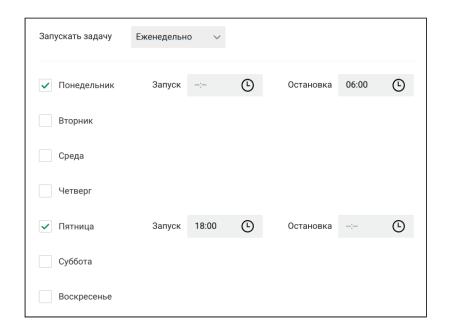
Запускать задачу	Ежеднев	но	~			
Время запуска	18:00	(Время остановки	7:00	©

• Если задачу требуется запускать и останавливать автоматически в различные дни недели, в поле Запускать задачу выберите Еженедельно. Установите флажок слева от того дня недели, в который требуется запускать или останавливать задачу. В поле Запуск и/или в поле Остановка справа от выбранного дня укажите время в формате H:mm или HH:mm. Примеры еженедельного расписания

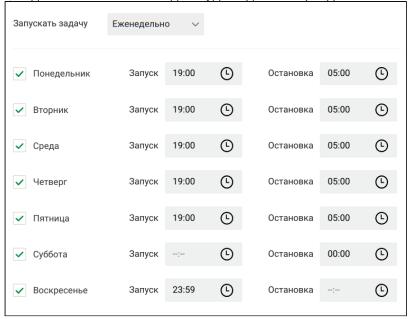
1) Задача автоматически запускается каждый будний день в 07:00 и останавливается в 18:00. Также задача запускается в 00:00 в субботу и останавливается в 23:59 в воскресенье:



2) Задача автоматически запускается в пятницу в 18:00 и останавливается в понедельник в 06:00:



3) Задача выполняется каждый будний день в периоды 00:00 – 05:00 и 19:00 – 23:59:



примечание:

При сохранении расписания указанное время добавляется в Систему в часовом поясе рабочей станции, с которой осуществляется подключение к веб-интерфейсу.

При просмотре расписания время отображается в часовом поясе рабочей станции, с которой осуществляется подключение к веб-интерфейсу.

(i) Примечание:

Если для задачи настроено расписание, ее можно также запускать и останавливать вручную. При этом автоматический запуск и остановка задачи будут выполняться по расписанию.

5. Вкладка **Расширенные настройки** – настройка задачи с учетом особенностей инфраструктуры:

Параметр	Описание
Число сканеров	Количество сканеров (экземпляров сервиса Puller). Сканеры используются для сканирования ресурсов задачи и загрузки файлов с ресурсов.
	Если указано значение 0 , то Система:
	 не сканирует файлы и не скачивает новые файлы в хранилища; отправляет файлы из хранилищ в Traffic Monitor. Примечание: Для сканирования одного хоста в рамках задачи используется только один сканер. Не рекомендуется указывать число сканеров, которое превышает число хостов в задаче.
	Если у хоста большое количество путей сканирования, то рекомендуется распределить пути сканирования по разным задачам. Для этого:
	 а. Создайте несколько задач. b. В каждую задачу добавьте хост. c. В каждой задаче для хоста укажите несколько путей сканирования. Каждый путь сканирования хоста должен быть указан только в одной из задач. Если хост указан в нескольких задачах, то хост будет обрабатываться несколькими сканерами. В этом случае может значительно увеличиться нагрузка на хост во время сканирования.
Нисло передатчик	Количество передатчиков (экземпляров сервиса Sender). Передатчики используются для отправки данных в Traffic Monitor.
OB	Рекомендуется указать значение, которое больше или равно количеству серверов Data Discovery в зоне задачи.
	Параметр не используется, если параметр Собирать только информацию о файлах включен.
Интервал обработки (в секундах)	Пауза после завершения прохода по ресурсу. Система повторно просканирует ресурс, только если указанный интервал закончился и очередь вновь дошла до ресурса. Параметр позволяет уменьшить нагрузку на ресурсы
	Tapamer production small building that programs
Глубина обработки (в днях)	Размер окна сканирования ресурса. Если дата изменения файла не попадает в окно сканирования, то файл не будет обработан в текущую сессию. Параметр используется для равномерного сканирования ресурсов. Чем ниже значение, тем чаще сканер будет переключаться между ресурсами.

Параметр	Описание
	Параметр не используется, если параметр Собирать только информацию о файлах включен.
	В первой сессии сканирования в рамках прохода по ресурсу в качестве окна сканирования устанавливается период от <i>Newest</i> до <i>Newest – Depth</i> , где:
	 Newest – самая поздняя дата изменения у файлов на ресурсе; Depth – количество дней, указанное в параметре. В каждой следующей сессии в качестве окна сканирования устанавливается период от Last до Last – Depth, где:
	 Last – самая ранняя дата изменения у файлов, обработанных в предыдущую сессию; Depth – количество дней, указанное в параметре. Новые и измененные файлы обрабатываются в каждой сессии.
	Пример использования параметра
	На ресурсе находятся 4 файла:
	 Файл А, дата изменения которого – 28.05.2021; Файл В, дата изменения которого – 03.05.2021; Файл С, дата изменения которого – 15.04.2021; Файл D, дата изменения которого – 19.03.2021. Если значение параметра равно 30 дням, то:
	 а. В первой сессии в рамках прохода в качестве окна сканирования устанавливается период 28.05.2021 – 28.04.2021. Обрабатывается файл А и файл В. Сканер переключается на другой ресурс. b. Во второй сессии в качестве окна сканирования устанавливается период 02.05.2021 – 02.04.2021. Обрабатывается файл С. Сканер переключается на другой ресурс. с. В третьей сессии в качестве окна сканирования устанавливается
	период 14.04.2021 – 15.03.2021. Обрабатывается файл D. Проход по ресурсу завершается.
Длительнос ть обработки (в минутах)	Максимальная длительность сессии. Сессия включает в себя получение списка файлов, хранящихся на ресурсе, и обработку файлов. По истечении времени, указанного в параметре, обработка ресурса будет приостановлена, сканер начнет обработку следующего ресурса.
	Параметр используется для равномерного сканирования ресурсов. Чем ниже значение, тем чаще сканер будет переключаться между ресурсами.
	Примечание: Когда сканер повторно дойдет до ресурса, обработка которого была приостановлена по истечении максимального времени, обработка продолжится с того места, где она была приостановлена в предыдущую сессию.
	Важно: При каждом подключении к ресурсу сканер получает список файлов, хранящихся на ресурсе. Во время получения списка файлов ресурс имеет

Параметр	Описание
	статус Сбор информации . Обработка ресурса начинается после получения списка файлов.
	Если на ресурсе находится большое количество файлов, то получение списка файлов может занять некоторое время. В некоторых случаях получение списка файлов может занимать все время, отведенное на одну сессию обработки ресурса. В этих случаях файлы на ресурсе не будут обрабатываться. Рекомендуется увеличить значение параметра Длительность обработки при сканировании ресурсов, которые имеют большое количество файлов.
Зона	Зона задачи.
	 Сервисы задачи запускаются на серверах, которые добавлены в зону.
	 Система скачивает файлы в хранилища серверов зоны. Задача использует настройки зоны для экспорта данных в Traffic Monitor.
	Вы можете изменить зону задачи, только если задача имеет статус Новая . Чтобы изменить зону в других случаях:
	 i. В настройках задачи на вкладке Расписание в поле Запускать задачу выберите Вручную и сохраните настройки. ii. Скопируйте задачу.
	ііі. Измените зону у копии задачи.Подробнее о зонах и серверах см. "InfoWatch Data Discovery. Руководство администратора", "Зоны и серверы".
Дополнител ьно проверять	По умолчанию для файлов, которые были скачаны во время предыдущих проходов по ресурсу, сканер проверяет только метаданные. Если метаданные файла не изменились, то файл не будет обработан повторно.
неизмененн ые файлы	Если параметр включен (), то при каждом проходе по ресурсу сканер будет скачивать файл и проверять содержимое файла на наличие изменений. Это позволяет выявить файлы, у которых изменилось содержимое, но не изменились метаданные. Если содержимое файла изменилось, то файл отправляется в составе события в Traffic Monitor.
	Параметр не используется, если параметр Собирать только информацию о файлах включен.
	Важно: Если параметр включен (), то увеличится объем трафика и время, требуемое для повторной обработки ресурса.

Добавление и настройка хостов



Важно!

Добавление хостов из LDAP-каталогов и импорт списка хостов доступны только для хостов с SMB-подключением. При добавлении для всех хостов в параметре Тип подключения по умолчанию указывается **SMB**. Изменение значения данного параметра недоступно при редактировании добавленных хостов.

Для всех хостов по умолчанию параметр Наследовать из задачи включен.

Чтобы добавить хосты в задачу:

- 1. Нажмите на задачу, чтобы перейти к списку хостов.
- 2. Выполните одно из следующих действий:
 - Нажмите , чтобы добавить один хост и указать его адрес вручную. В открывшемся окне настройте хост и нажмите Сохранить (см. Настройки хоста).
 - Нажмите 🗐, чтобы добавить хосты из LDAP-каталога. В открывшемся окне отображаются данные из LDAP-каталогов, полученные Системой в результате синхронизаций с Active Directory. Если удалить интеграцию, то данные этой интеграции не будут отображаться в окне. Подробнее о добавлении данных в Систему см. "InfoWatch Data Discovery. Руководство администратора", "Интеграции".

примечание:

Если Система установлена совместно с другими продуктами Платформы, в окне также могут отображаться данные, полученные в результате синхронизаций с Traffic Monitor.

Данные в окне представлены в виде дерева. Для элементов LDAP-каталога используются следующие обозначения:

- контейнер;
- компьютер.

Чтобы раскрыть элемент дерева, нажмите слева от элемента. Чтобы искать элементы по имени, введите текст в поисковую строку.



Важно!

Поиск осуществляется только по данным, которые отображаются в окне. Перед поиском рекомендуется раскрыть элементы дерева и убедиться, что элементы загрузились и отображаются в окне.

Чтобы добавить компьютеры из каталога в задачу:

- а. Выберите в дереве компьютеры и/или элементы, которые включают в себя компьютеры;
- b. Нажмите **Добавить**.

При добавлении компьютера в качестве хоста в задачу, в параметре Адрес у хоста автоматически указывается полное доменное имя компьютера.

• Нажмите 进, чтобы добавить хосты из файла. В открывшемся окне выберите файл, который содержит список адресов хостов. Требуется файл с расширением .txt, в котором адрес каждого хоста указан на отдельной строке. Адрес может быть представлен в формате IP-адреса или как полное доменное имя (FQDN).

В результате добавленные хосты отображаются в списке хостов.

В верхней части экрана со списком хостов доступно управление задачей. Нажмите 🔄, чтобы вернуться к списку задач.

Настройки хоста:

примечание:

Поля, обязательные к заполнению, отмечены в интерфейсе значком 🖹.

1. Вкладка **Общие**:

а. Основные настройки хоста:

Описание
Доменное имя или IP-адрес.
Система получает IP-адреса для всех доменных имен:
• при запуске задачи;
 регулярно во время выполнения задачи: через 30 секунд после того, как все адреса были получены.
Примечание: Для подключения к SharePoint необходимо указать адрес, по которому доступно веб-приложение SharePoint. В некоторых случаях вебприложение SharePoint может быть доступно, только если адрес указан в формате доменного имени.
Порт подключения. Если порт подключения не указан, то используется значение по умолчанию:
• для SMB-подключения – 445;
 для SSH-подключения – 22;
FTP-подключения - 21;WebDAV-подключения - 8080.
Для SharePoint-подключения поле обязательно для заполнения.
Доступные значения:
 SMB – для сканирования общих сетевых ресурсов; SSH – для сканирования серверов и рабочих станций под управлением Linux;

Пара метр	Описание
	 SharePoint – для сканирования библиотек документов в SharePoint Server 2016 по протоколу HTTPS; FTP - для сканирования файловых ресурсов по протоколу FTP; WebDAV (Nextcloud) - для сканирования хранилищ данных Nextcloud по протоколу WebDAV. Изменение значения данного параметра недоступно при редактировании хоста.
Пут ь к	Путь внутри SharePoint к сайту. Сайт должен содержать библиотеки документов, которые требуется просканировать.
caŭm y	Параметр доступен, если для хоста выбрано SharePoint-подключение. Пример: Адрес библиотеки documents – sp.example.com/my_path/site/documents.В этом случае путь к сайту – my_path/site
Про токо л	Доступные значения: • HTTPS • HTTP Параметр доступен, если для хоста выбран тип подключения WebDAV (Nextcloud).
Пут ь подк люче ния	Для подключения к Nextcloud по протоколу WebDAV в поле <i>Путь подключения</i> необходимо вставить часть ссылки из хранилища (подробнее см. "Получение ссылки для подключения к Nextcloud"). Параметр доступен, если для хоста выбран тип подключения WebDAV (Nextcloud).
Опис ание	Краткое описание хоста

примечание:

Подключение по протоколу WebDAV проходит без проверки TLS/SSL-сертификатов.

b. Секция **Параметры авторизации**:

Парамет р	Описание	
Наследо вать из задачи	Если параметр включен (), то для подключения к хосту используются значения параметров авторизации, указанные в настройках задачи.	

Парамет р	Описание
	Чтобы ввести значения, отличные от указанных в настройках задачи, отключите параметр. При добавлении хоста параметр включен по умолчанию.
Группа SMB	Домен или группа. Параметр доступен, если для хоста выбрано SMB-подключение.
Логин	Имя пользователя Важно: Для подключения к SharePoint необходимо указать значение в формате: domain\user
Пароль	Пароль

(i) Примечание:

При подключении к SMB-хосту используется анонимный доступ в следующих случаях:

- Если параметр **Наследовать из задачи** выключен и значения параметров авторизации для хоста не указаны;
- Если параметр **Наследовать из задачи** включен и в настройках задачи значения параметров авторизации не указаны.

2. Вкладка Расширенные настройки:

	•
Параметр	Описание
Таймаут (мс)	Время ожидания при подключении к хосту. Для SharePoint-хостов не рекомендуется указывать значение меньше 60000 (60 секунд). Если при сканировании ресурса возникают ошибки вида "Connection timed out / Connection timeout", рекомендуется увеличить значение параметра. Подробнее о статусах ресурсов см. "Статистика выполнения задач".
Попыток повторени я	Максимальное количество попыток соединения
Уровень отладки	Параметр контролирует представление отладочной информации. Для SMB-подключения: Для изучения возникающих проблем рекомендуется использовать значение 2 . Подробнее см. документацию smbclient (параметр debuglevel).

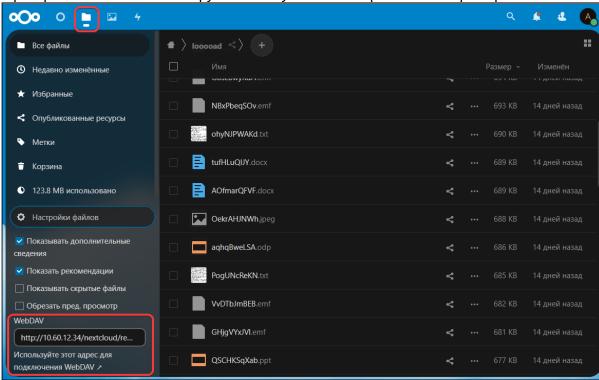
Параметр	Описание
	 Для SSH-подключения: Для изучения возникающих проблем рекомендуется использовать следующие значения: 8 – информация об аутентификации; 64 – отладочная информация протокола SFTP; 128 – информация об ошибках; 512 – информация о работе с сокетами. Для получения отладочной информации одновременно по нескольким значениям, введите сумму значений. Например, чтобы одновременно получить отладочную информацию протокола SFTP (значение параметра: 64) и информацию об ошибках (значение параметра: 128), укажите в поле Уровень отладки значение 192 (64+128).
	Подробнее см. документацию libssh2.
	Для SharePoint-подключения: Для изучения возникающих проблем рекомендуется использовать следующие значения:
	 1 – информация сокетах; 2 – информация о запросах и ответах по HTTP; 8 – информация об HTTP-аутентификации; 16 – информация об HTTP-аутентификации (plaintext); 128 – информация о теле HTTP-ответов; 256 – информация об SSL/TLS. Для получения отладочной информации одновременно по нескольким значениям, введите сумму значений. Например, чтобы одновременно получить информацию об аутентификации (значения параметра: 8 и 16) и информацию об SSL/TLS (значение параметра: 256), укажите в поле Уровень отладки значение 280 (8+16+256).
	Для FTP- или WebDAV-подключения : Для изучения возникающих проблем рекомендуется использовать следующие значения:
	 0 - общая информация о выполнении запросов и ошибках при выполнении запросов; 1 - дополнительные данные, полученные от хоста; 2 - дополнительные данные, отправленные хосту; 3 - данные от выполненных запросов. Если использовалось шифрование, будут представлены в нерасшифрованном виде; 4 - данные для запросов, отправленных к хосту; 5 - данные по SSL/TLS, отправленные хосту; 6 - данные по SSL/TLS, полученные от хоста.
	Для FTP и WebDAV поддерживается получение отладочной информации одновременно только по одному значению.
Пауза до повтора (сек)	Временной интервал между попытками соединения

Параметр	Описание
Размер чанка (байт)	Размер фрагмента передаваемых данных

Получение ссылки для подключения к Nextcloud

Чтобы Data Discovery подключился к хранилищу Nextcloud по протоколу WebDAV:

- 1. Откройте веб-интерфейс хранилища Nextcloud.
- 2. Авторизуйтесь под учетной записью, от имени которой будет подключаться Data Discovery.
- 3. На верхней панели выберите вкладку Файлы.
- 4. В левом нижнем углу нажмите на Настройки файлов.
- 5. В раскрывшемся меню скопируйте ссылку как на изображении из примера:



- 6. Из скопированной ссылки в окне добавления хоста:
 - а. В поле Адрес укажите ір-адрес хранилища.
 - В нашем примере: 10.60.12.34
 - b. В поле **Протокол** укажите протокол передачи.
 - В нашем примере: http
 - с. В поле Путь подключения укажите оставшуюся часть ссылки.

Пример ссылки для подключения к Nextcloud:
/nextcloud/remote.php/dav/files/admin/

Ссылка ведет в корневой каталог хранилища, доступного этому пользователю. Для этого хоста вы будете указывать пути сканирования относительно корневого каталога.

Добавление путей сканирования

Чтобы добавить путь сканирования:

- 1. Нажмите на хост, чтобы перейти к списку путей сканирования.
- 2. В поле в левом верхнем углу укажите путь сканирования:
 - Для хоста с SMB-подключением укажите имя общего сетевого ресурса, например:

share

Примечание:

Для хостов с SMB-подключением не поддерживается возможность указать поддиректорию сетевого ресурса (например: share/folder) в качестве пути сканирования.

Чтобы сканировать поддиректорию SMB-ресурса, настройте фильтры для директорий на вкладке Фильтры папок в настройках задачи.

 Для хоста с SSH-, FTP- или WebDAV-подключением укажите полный путь к директории, например:

/home/username/Documents

примечание:

Для типа подключения WebDAV указывайте пути сканирования относительно корневого каталога, указанного в поле Путь подключения при описании хоста.

- Для хоста с SharePoint-подключением вы можете указать значение в следующих форматах:
 - имя библиотеки документов, например: Shared Documents
 - путь к директории внутри библиотеки, например: Shared Documents/ folder/example
- 3. Нажмите Добавить.

В результате добавленный путь сканирования отображается в списке.

В верхней части экрана со списком путей сканирования доступно управление задачей и хостом.

, чтобы вернуться к списку хостов.



Важно!

Определение путей сканирования поддерживается только для хостов с SMB-подключением. Определение путей сканирования проводится для тех хостов, у которых не указан ни один путь сканирования.

Чтобы автоматически определить пути сканирования:

- 1. Перейдите в список хостов.
- 2. Выберите хосты. Если требуется выбрать все хосты на текущей странице, установите напротив заголовка столбца Хост.



Примечание:

Если вы не выберете ни один хост, то Система будет искать пути сканирования для всех хостов в задаче.

- 3. Нажмите (действие доступно, если задача не выполняется).
- 4. Нажмите Запустить.

примечание:

Вы также можете запустить определение путей сканирования для одного хоста со страницы со списком путей:

- 1. Нажмите на хост, чтобы перейти к списку путей сканирования.
- 2. Нажмите (действие доступно только для SMB-хостов, у которых не указаны пути).

Система определит и добавит доступные пути сканирования для хостов. Если вы определяете пути для большого количества хостов, то процесс определения путей сканирования может занять некоторое время. В этом случае задача будет иметь статус Определение путей сканирования. Вы не можете запустить задачу, если проводится определение путей сканирования.

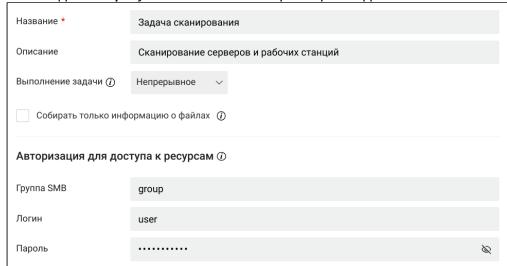


примечание:

Если наступило время автоматического запуска задачи по расписанию и задача имеет статус Определение путей сканирования, то запуск не будет произведен. Рекомендуется запустить задачу вручную, когда завершится процесс определения путей сканирования.

Примеры настроек задачи, хоста и добавления путей сканирования Настройте задачу:

1. На вкладке Общие укажите значения параметров задачи:



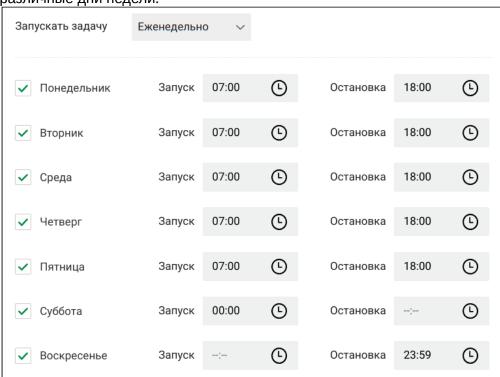
2. На вкладке Фильтры файлов установите ограничение на размер для каждого файла и настройте фильтр по именам файлов:



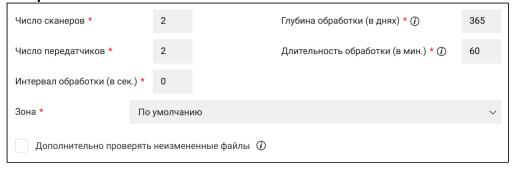
3. На вкладке Фильтры папок настройте фильтры по директориям:



4. На вкладке **Расписание** настройте автоматический запуск и остановку задачи в различные дни недели:



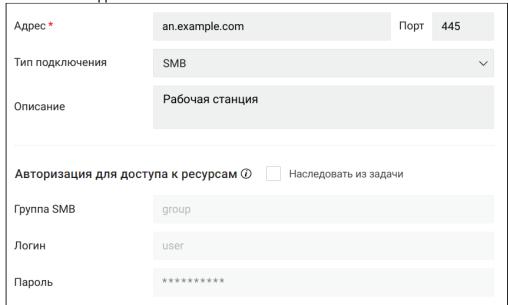
5. При необходимости измените значения параметров на вкладке **Расширенные настройки**:



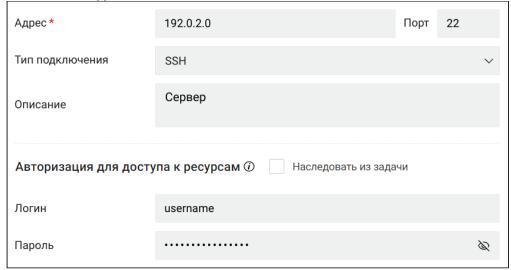
Настройте хост:

1. На вкладке Общие укажите значения параметров для подключения к хосту:

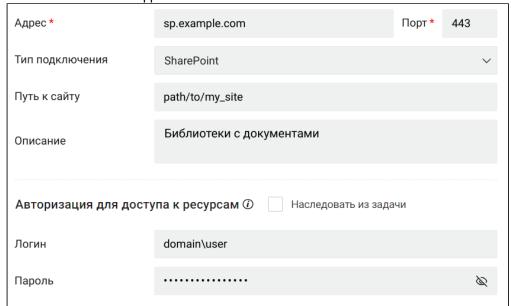
• Хост с **SMB**-подключением:



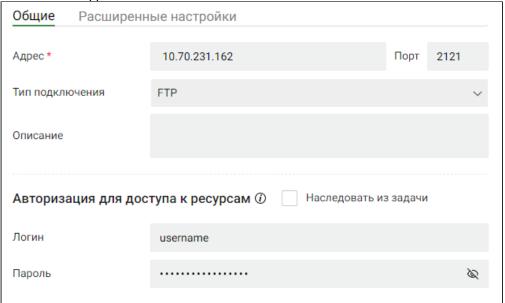
• Хост с **SSH**-подключением:



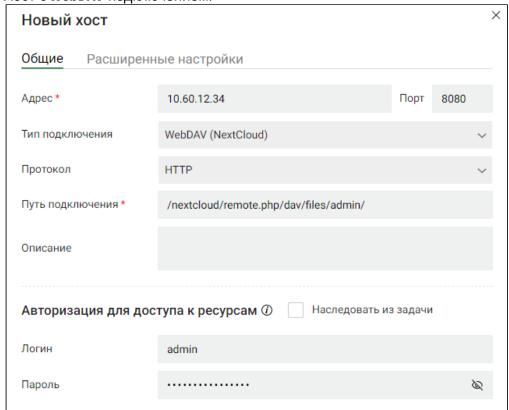
• Хост с SharePoint-подключением:



• Хост с **FTP**-подключением:



• Хост с **WebDAV**-подключением:

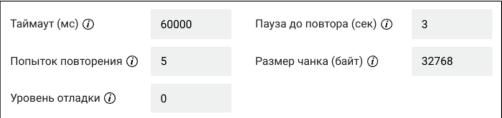


(i) Примечание:

Чтобы ускорить сканирование хранилища Nextcloud, для подключения используйте пароль приложения (подробнее см. примечание в пункте Сторонние клиенты WebDAV из официальной документации Nextcloud).

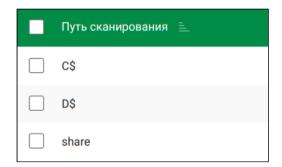
Подключение по протоколу WebDAV проходит без проверки TLS/SSL-сертификатов.

2. При необходимости измените значения параметров на вкладке **Расширенные настройки**:



Добавьте пути сканирования:

• Для хоста с **SMB**-подключением в качестве путей сканирования укажите имена сетевых ресурсов:

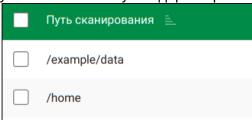


примечание:

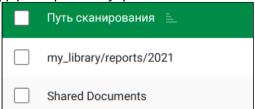
Не поддерживается возможность указать поддиректорию сетевого ресурса (например: share/folder) в качестве пути сканирования.

Чтобы сканировать поддиректорию SMB-ресурса, настройте фильтры для директорий на вкладке **Фильтры папок** в настройках задачи.

• Для хоста с **SSH**-, **FTP**- или **WebDAV**-подключением в качестве путей сканирования укажите полные пути к директориям:



• Для хоста с **SharePoint**-подключением укажите имена библиотек и/или пути к директориям внутри библиотек:



5.2.4 Редактирование задачи и хоста

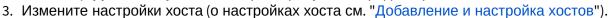
Редактирование настроек задачи и хостов доступно только для задач со статусами **Новая**, **Ожидает запуск по расписанию**, **Остановлена**, **Завершена**. Вы можете нажать , чтобы просмотреть текущие настройки задачи/хоста, даже если редактирование недоступно.

Чтобы отредактировать задачу:

- 1. Нажмите на раздел Задачи, чтобы перейти к списку задач сканирования.
- 2. В столбце **Действия** у задачи, которую требуется отредактировать, нажмите
- 3. Измените настройки задачи (о настройках задачи см. "Создание, настройка и запуск задачи").
- 4. Нажмите Сохранить.

Чтобы отредактировать хост в задаче:

- 1. Нажмите на задачу, чтобы перейти к списку хостов.
- 2. В столбце **Действия** у хоста, который требуется отредактировать, нажмите



4. Нажмите Сохранить.

5.2.5 Копирование задачи

Чтобы скопировать задачу:

- 1. Нажмите на раздел Задачи, чтобы перейти к списку задач сканирования.
- 2. Нажмите в столбце **Действия** у задачи, копия которой вам нужна.

В списке задач отобразится новая задача. Название новой задачи состоит из названия оригинальной задачи и слова "Копия". Новая задача имеет те же настройки, хосты и пути сканирования.

4

Важно!

Файлы задачи и метаданные файлов не будут скопированы.

В рамках новой задачи Система полностью повторно просканирует ресурсы.

5.2.6 Удаление задачи, хостов и путей сканирования

Удаление задачи, хостов и путей сканирования доступно только для задач со статусами **Новая**, **Ожидает запуск по расписанию**, **Остановлена**, **Завершена**.

Чтобы удалить задачу:

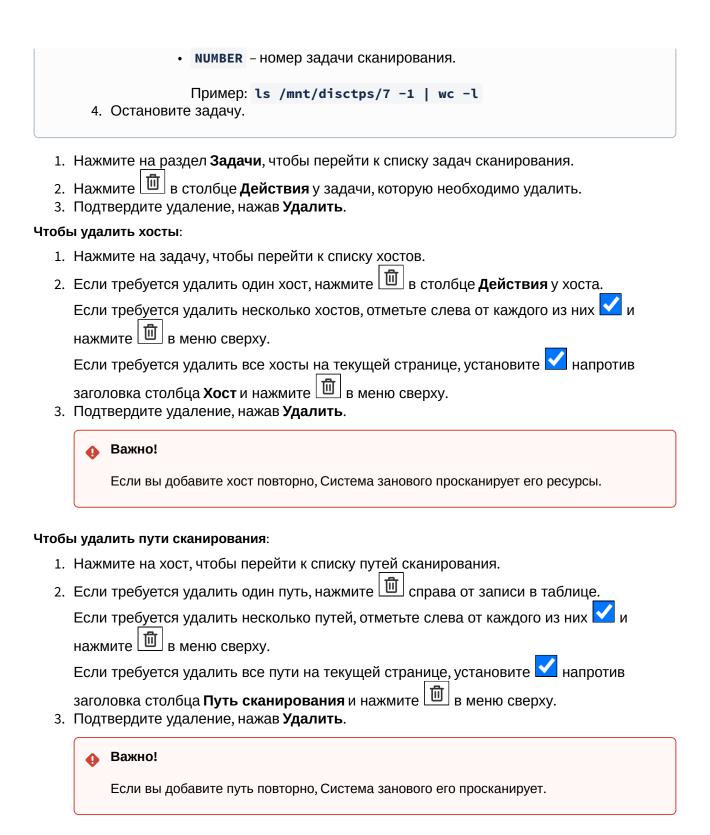
(i)

Примечание:

Если вы удалите задачу, файлы задачи будут удалены из хранилищ зоны. Эти файлы не будут отправлены в Traffic Monitor.

Рекомендуется отправить файлы в Traffic Monitor перед удалением задачи:

- 1. В настройках задачи:
 - Отключите параметр Собирать только информацию о файлах.
 - Укажите следующие значения:
 - 0 для параметра Число сканеров.
 - **N** для параметра **Число передатчиков**, где **N** больше или равно количеству серверов Data Discovery в зоне задачи.
- 2. Запустите задачу. Система отправляет файлы в Traffic Monitor и удаляет их из хранилищ, но не скачивает новые файлы в хранилища зоны.
- 3. Дождитесь, когда в хранилищах зоны не останется файлов задачи. Чтобы получить количество файлов задачи на сервере Data Discovery:
 - а. Подключитесь к ssh-консоли сервера.
 - b. Выполните команду ls PATH/NUMBER -1 | wc -l, где:
 - PATH путь к хранилищу сервера, по умолчанию: /mnt/disctps;



5.2.7 Статистика выполнения задач

Статистика по задачам

В Системе представлена статистика – информация о выполнении каждой задачи сканирования. Статистика доступна в разделе **Задачи**. Навигация по страницам списка задач осуществляется с помощью панели, расположенной внизу экрана. Статистика по задачам включает в себя следующие данные:

Параметр	Описание					
Nº	Номер задачи. Номер является уникальным					
Римя	Название задачи					
Описание	Краткое описание задачи сканирования					
Зона	Зона задачи					
Дата запуска	Дата и время запуска задачи, значение отображается в формате dd.MM.yyyy HH:mm:ss					
Дата остановки	Дата и время остановки задачи, значение отображается в формате dd.MM.yyyy HH:mm:ss. Для задачи в статусе Выполняется данные отсутствуют					
Найдено – текущая сессия	Число и общий объем файлов, найденных на всех ресурсах задачи с учетом фильтров. Система получает число файлов на ресурсе при каждом подключении (в каждой сессии). Число найденных файлов может уменьшиться, если с ресурса удалили файлы или если изменились настройки фильтров в задаче					
Статус	 Текущий статус задачи: Новая Ожидает запуск по расписанию Запускается Выполняется Останавливается Остановлена Определение путей сканирования Завершена Если возникла ошибка при работе с ресурсом, рядом со статусом отображается Чтобы просмотреть информацию об ошибке, наведите курсор на 					

Параметр	Описание
Отправлено – все время	Число и общий объем файлов, отправленных в Traffic Monitor за все время выполнения задачи

Работа со списком задач

Сортировка задач возможна по следующим столбцам: №, Имя, Дата запуска, Дата остановки, Статус. Чтобы изменить порядок сортировки строк в списке задач, щелкните левой клавишей мыши по заголовку того столбца, по которому нужно выполнить сортировку.

Чтобы искать задачи по имени, введите первые символы имени в поле **Поиск задач**, расположенное в правом верхнем углу экрана. В списке отображаются задачи, имя которых начинается с символов, введенных в поле **Поиск задач**. Поиск осуществляется без учета регистра.

Чтобы переместить столбец, нажмите левой клавишей мыши на заголовок столбца и, не отпуская клавишу, перемещайте заголовок вдоль строки заголовков. Отпустите левую клавишу мыши, столбец будет перемещен на указанное место.

Чтобы изменить ширину столбца, нажмите левой клавишей мыши на правую границу заголовка столбца и, не отпуская клавишу, перемещайте границу столбца. Отпустите левую клавишу мыши, ширина столбца будет изменена.

Статистика по хостам

Нажмите на задачу, чтобы перейти к списку хостов. Навигация по страницам списка хостов осуществляется с помощью панели навигации, расположенной внизу экрана. Статистика содержит следующую информацию:

Параметр	Описание
Хост	Адрес хоста
Тип	Тип подключения хоста
Описание	Описание хоста
Найдено - текущая сессия	Число и общий объем файлов, найденных на ресурсах хоста с учетом фильтров. Система получает число файлов на ресурсе при каждом подключении (в каждой сессии). Число найденных файлов может уменьшиться, если с ресурса удалили файлы или если изменились настройки фильтров в задаче
Просканировано – текущая сессия	Число и общий объем просканированных файлов на ресурсах хоста. Система учитывает только файлы, найденные на ресурсах в текущих сессиях. В большинстве случаев число просканированных файлов возрастает с каждой сессией. В конце прохода по ресурсу число файлов сбрасывается, в следующем проходе сканер проверяет файлы и обрабатывает новые

Параметр	Описание				
Прогресс сканирования	Общий объем просканированных файлов / общий объем найденных файлов				
Статус	Примечание: Статус хоста зависит от статусов ресурсов хоста. Текущий статус хоста: •				
Отправлено - все время	Число и общий объем файлов хоста, отправленных в Traffic Monitor за все время выполнения задачи				

Работа со списком хостов

Сортировка хостов возможна по столбцам: Хост, Тип. Чтобы изменить порядок сортировки строк в списке хостов, щелкните левой клавишей мыши по заголовку того столбца, по которому нужно выполнить сортировку.

Чтобы искать хосты по адресу, введите первые символы IP-адреса/доменного имени в поле Поиск хостов, расположенное в правом верхнем углу экрана. В списке отображаются хосты, адрес которых начинается с символов, введенных в поле Поиск хоста. Поиск осуществляется без учета регистра.



примечание:

Поиск хостов по адресу осуществляется по значениям, указанным при создании/ редактировании хоста. Например, если при создании/редактировании хоста адрес был указан в виде доменного имени, то хост не будет найден по IP-адресу.

Чтобы переместить столбец, нажмите левой клавишей мыши на заголовок столбца и, не отпуская клавишу, перемещайте заголовок вдоль строки заголовков. Отпустите левую клавишу мыши, столбец будет перемещен на указанное место.

Чтобы изменить ширину столбца, нажмите левой клавишей мыши на правую границу заголовка столбца и, не отпуская клавишу, перемещайте границу столбца. Отпустите левую клавишу мыши, ширина столбца будет изменена.

Статистика по путям сканирования

Нажмите на хост, чтобы перейти к списку путей сканирования. Навигация по страницам списка путей сканирования осуществляется с помощью панели навигации, расположенной внизу экрана. Для пути сканирования статистика содержит следующую информацию:

Параметр	Описание			
Путь сканирования	Путь сканирования хоста (ресурс)			
Дата последнего сканирования	Дата и время последнего подключения к ресурсу, значение отображается в формате dd.MM.yyyy HH:mm:ss			
Найдено – текущая сессия	Число и общий объем файлов, найденных на ресурсе с учетом фильтров.			
	Система получает число файлов на ресурсе при каждом подключении (в каждой сессии). Число найденных файлов может уменьшиться, если с ресурса удалили файлы или если изменились настройки фильтров в задаче			
Просканировано – текущая сессия	Число и общий объем просканированных файлов на ресурсе. Система учитывает только файлы, найденные на ресурсе в текущей сессии.			
	В большинстве случаев число просканированных файлов возрастает с каждой сессией. В конце прохода по ресурсу число файлов сбрасывается, в следующем проходе сканер проверяет файлы и обрабатывает новые			
Прогресс сканирования	Общий объем просканированных файлов / общий объем найденных файлов			
Статус	 Ожидает сканирования - подключение к ресурсу еще не осуществлялось в рамках задачи Подключение - осуществляется подключение к ресурсу Сбор информации - Система получает список файлов и информацию о файлах Обработка файлов - Система сохраняет информацию о файлах и загружает копии файлов в хранилище Остановлено - завершилась сессия сканирования ресурса или была остановлена задача сканирования 			

Параметр	Описание		
	 Выполнено – завершился проход по ресурсу, были обработаны все файлы, находящиеся на ресурсе Ошибка – произошла ошибка при работе с ресурсом (чтобы просмотреть информацию об ошибке, наведите курсор на статус ресурса) Примеры ошибок 		
	В некоторых случаях сообщения об ошибке содержат следующий текст:		
	 Operation not permitted Permission denied Authentication failed Ошибки такого вида могут означать, что используются неверные параметры авторизации или у учетной записи недостаточно прав доступа для сканирования ресурса. 		
Отправлено - все время	Число и общий объем файлов ресурса, отправленных в Traffic Monitor		

Работа со списком путей сканирования

Сортировка путей сканирования возможна по столбцу **Путь сканирования**. Чтобы изменить порядок сортировки строк в списке путей сканирования, щелкните левой клавишей мыши по заголовку столбца **Путь сканирования**.

Чтобы искать пути сканирования, введите первые символы пути в поле **Поиск путей сканирования**, расположенное в правом верхнем углу экрана. В списке отображаются пути, которые начинаются с символов, введенных в поле **Поиск путей сканирования**. Поиск осуществляется без учета регистра.

Чтобы переместить столбец, нажмите левой клавишей мыши на заголовок столбца и, не отпуская клавишу, перемещайте заголовок вдоль строки заголовков. Отпустите левую клавишу мыши, столбец будет перемещен на указанное место.

Чтобы изменить ширину столбца, нажмите левой клавишей мыши на правую границу заголовка столбца и, не отпуская клавишу, перемещайте границу столбца. Отпустите левую клавишу мыши, ширина столбца будет изменена.

5.3 Раздел "Информация о файлах"

В разделе отображается информация о файлах, которые были просканированы в рамках задач. Информация о файлах представлена в виде таблицы:

- о составе таблицы и о том, как записи добавляются в таблицу, см. "Таблица с информацией о файлах";
- о настройке отображения записей в таблице см. "Настройка отображения таблицы";
- о фильтрации записей в таблице см. "Единый фильтр";
- о поиске дубликатов для файлов см. "Поиск дубликатов";

• о выгрузке данных из таблицы см. "Выгрузка информации о файлах".

Также см. "Пример работы с таблицей".

5.3.1 Таблица с информацией о файлах

Информация о файлах представлена в виде таблицы. В конце каждой сессии обработки ресурса в таблицу добавляется информация о просканированных за эту сессию файлах.

Добавление записей в таблицу в рамках задачи

Проход - полное сканирование одного ресурса. Проход может состоять из нескольких сессий.

Сессия - подключение к ресурсу в рамках прохода.

В рамках первого прохода по ресурсу Data Discovery собирает метаданные всех файлов на ресурсе и добавляет для каждого файла запись в таблицу.

При последующих сессиях Система обрабатывает только новые и измененные файлы. Чтобы определить измененные файлы, Система проверяет метаданные файлов на изменения:

- Путь к файлу;
- Имя файла;
- Размер файла;
- Дата и время изменения файла;
- Владелец файла;
- Пользователи/группы, которые имеют доступ к файлу.

4

Важно!

Проверка следующих метаданных на изменения поддерживается только при сканировании SMB-ресурсов на хостах под управлением ОС семейства Windows:

- Владелец файла
- Пользователи/группы, которые имеют доступ к файлу

Если файл является новым или измененным, то Система в конце сессии добавляет новую запись в таблицу.

Структура таблицы с информацией о файлах

Каждая запись таблицы содержит информацию об одном просканированном файле. Каждая запись содержит следующие поля:

Поле	Описание	
Обнаружен	Дата и время, когда файл впервые был обнаружен на ресурсе Системой в рамках задачи сканирования. Дата и время указываются в формате dd.MM.yyyy HH:mm:ss	
	Примечание: Если неизмененный файл обнаружен повторно в следующих сессиях в рамках задачи, то:	
	• в таблицу не добавляются новые записи;	

Поле	Описание
	• значение поля Обнаружен в записи о файле не обновляется.
Задача	Название задачи сканирования, в рамках которой файл был обнаружен на ресурсе
	Примечание: Если файл на ресурсе обнаружен в рамках нескольких задач сканирования, то в таблицу добавляется запись о файле для каждой такой задачи
Хост	Доменное имя хоста, на котором был обнаружен файл
IP-адрес хоста	IP-адрес хоста, на котором был обнаружен файл.
	Если адрес для SharePoint-хоста указан в формате доменного имени в настройках хоста, то поле не заполняется.
Расположение	Расположение файла – полный путь к директории, в которой был обнаружен файл.
	Примечание: Полный путь включает в себя путь сканирования ресурса. Для файлов с SharePoint-хостов полный путь также включает в себя путь к сайту.
Имя файла	Имя файла.
	Система получает значение из файловой системы ресурса.
Размер	Размер файла.
	Система получает значение из файловой системы ресурса.
Создан	Дата и время создания файла. Дата и время указываются в формате dd.MM.yyyy HH:mm:ss
	Система получает значение из файловой системы ресурса.
	Примечание: Определение даты создания файла не поддерживается в следующих случаях:
	• при сканировании SMB-ресурсов на хостах под управлением Linux;
	 при сканировании хостов под управлением Linux по протоколу SSH.
	В этих случаях поле Создан заполняется значением поля Изменен .
Изменен	Дата и время изменения файла. Дата и время указываются в формате dd.MM.yyyy HH:mm:ss
	Система получает значение из файловой системы ресурса.

Поле	Описание				
	Примечание: Дата и время изменения файла в поле указывают на следующие изменения: При сканировании SMB-ресурсов на хостах под управлением ОС семейства Windows: последнее изменение содержимого файла; последнее изменение имени файла; последнее изменение пути к файлу; последнее изменение владельца файла или списка пользователей и групп, которые имеют доступ к файлу; При сканировании SMB-ресурсов на хостах под управлением Linux / хостов под управлением Linux по протоколу SSH: последнее изменение содержимого файла; При сканировании библиотек документов в SharePoint Server 2016:				
Не обнаружен	• последнее изменение имени файла. Дата и время окончания прохода в рамках задачи, если файл не был обнаружен повторно на ресурсе по результатам прохода. Дата и время указываются для первого прохода, в который файл не был обнаружен. Дата и время указываются в формате dd.MM.yyyy HH:mm:ss				
	 Система не обнаружит файл повторно в рамках задачи, если: Файл был удален с ресурса. У файла изменились метаданные. В этом случае в таблицу добавляется новая запись. В настройках задачи были изменены фильтры файлов/директорий и при повторном сканировании файл не соответствовал условиям фильтров. 				
Владелец	В поле Владелец указывается SID владельца файла, например: S-1-5-21-1922741149-3613679056-2300624754-1000				
Доступен для	В поле Доступен для указывается список SID пользователей и групп, которые имеют доступ к файлу.				
	Система получает значения из файловой системы ресурса. Система может идентифицировать персон и группы по SID (см. "Идентификация персон и групп").				



Важно!

Получение SID владельца файла и SID пользователей/групп, которые имеют доступ к файлу, поддерживается для:

- SMB-ресурсов на хостах под управлением ОС семейства Windows;
- библиотек документов в SharePoint Server 2016.

Возможно некорректное заполнение полей Владелец и Доступен для, если:

- Производится сканирование SMB-ресурса на хосте под управлением Linux;
- Производится сканирование SMB-ресурса, созданного на сервере SMB, который не поддерживает файловые атрибуты для определения владельца файла и пользователей/групп, которые имеют доступ к файлу;
- Производится сканирование SMB-ресурса, созданного в файловой системе, которая не поддерживает файловые атрибуты для определения владельца файла и пользователей/групп, которые имеют доступ к файлу.

Получение SID владельца файла и SID пользователей/групп, которые имеют доступ к файлу, не поддерживается при сканировании хостов:

- под управлением Linux по протоколу SSH;
- по протоколу FTP;
- по протоколу WebDAV.

В этом случае атрибуты Отправители и Получатели имеют значение "iw data discovery".



примечание:

Дата и время в полях Обнаружен, Изменен, Создан, Не обнаружен отображается в часовом поясе рабочей станции, с которой осуществляется подключение к веб-интерфейсу Data Discovery.

Идентификация персон и групп

Система может идентифицировать персон и группы по SID.

В случае успешной идентификации:

- вместо SID **персоны** в полях **Владелец** и **Доступен для** Системы отобразит имя, указанное в досье;
- вместо SID **группы** в поле **Доступен для** Система отобразит название группы, полученное из Active Directory.

Идентификация учетных записей ОС Windows по известным (well-known) SID

Система идентифицирует следующие учетные записи ОС Windows (подробнее об известных SID см. документацию Microsoft Windows):

SID	Учетная запись	Описание	
S-1-5-18	System	Учетная запись, которую использует операционная система	
S-1-1-0	Everyone	Все пользователи	

Данные об указанных SID по умолчанию добавлены в Систему. Система производит идентификацию во всех записях таблицы.

Идентификация персон и групп из Active Directory

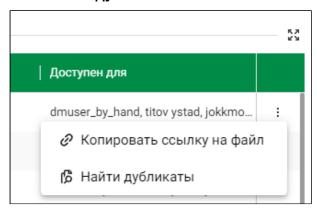
Все персоны, добавленные в Систему результате синхронизации с Active Directory имеют тип контакта SID, что позволяет идентифицировать их. Если группы из Active Directory имеют SID, они будут идентифицированы. Подробнее о добавлении данных о персонах и группах в Систему см. "InfoWatch Data Discovery. Руководство администратора", "Интеграции".

Система идентифицирует персон и группы во всех записях таблицы по актуальным данным каждой интеграции. Идентификация по данным последней синхронизации может занять некоторое время – до 15 минут с момента завершения синхронизации.

Действия с файлами

Справа от каждой записи вы можете нажать кнопку :, чтобы выбрать одно из доступных действий с файлом:

- Копировать ссылку на файл;
- Найти дубликаты.



Найти дубликаты - действие аналогично Поиску дубликатов по образцу, но в качестве образца будет использован файл из таблицы.

Примечание:

Поиск дубликатов по файлу из таблицы будет недоступен при выполнении любого из условий:

- размер файла превышает 4 ГБ;
- в настройках задачи сканирования включена опция Собирать только информацию о файлах.

Если файлы были просканированы Data Discovery версии **ниже 1.8**, информация об их содержимом отсутствует. Поиск по таким файлам не осуществляется. В этом случае:

- 1. Скопируйте задачу, в которой были просканированы файлы.
- 2. Повторно просканируйте файлы в новой задаче.

5.3.2 Настройка отображения таблицы

Чтобы изменить порядок сортировки записей о файлах в таблице, щелкните левой клавишей мыши по заголовку того столбца, по которому нужно выполнить сортировку. Все записи таблицы будут отсортированы по возрастанию/убыванию значений выбранного столбца.

Чтобы переместить столбец, нажмите левой клавишей мыши на заголовок столбца и, не отпуская клавишу, перемещайте заголовок вдоль строки заголовков. Отпустите левую клавишу мыши, столбец будет перемещен на указанное место.

Чтобы изменить ширину столбца, нажмите левой клавишей мыши на правую границу заголовка столбца и, не отпуская клавишу, перемещайте границу столбца. Отпустите левую клавишу мыши, ширина столбца будет изменена.

Навигация по страницам таблицы осуществляется с помощью панели, расположенной внизу экрана.

5.3.3 Поиск дубликатов

Вы можете искать дубликаты файлов. Файлы считаются дубликатами, если файлы имеют одинаковое содержимое.

Система получает информацию о содержимом файлов в рамках задачи сканирования, если параметр Собирать только информацию о файлах отключен.



Примечание:

Поиск дубликатов будет недоступен, если размер просканированного файла превышает 4 ГБ.

Поиск по образцу

Чтобы искать дубликаты:

- 1. Нажмите Поиск дубликатов по образцу.
- 2. В открывшемся окне загрузите файл.
- 3. Нажмите Найти дубликаты.
- 4. Дождитесь окончания поиска.

В таблице отображаются записи о файлах, которые являются дубликатами загруженного файла. К записям применяются условия Единого фильтра (см. "Единый фильтр").



Важно!

Если файлы были просканированы Системой версии 1.7 или ниже, информация об их содержимом отсутствует. Поиск по таким файлам не осуществляется.

В этом случае:

- 1. Скопируйте задачу, в которой были просканированы файлы.
- 2. Повторно просканируйте файлы в новой задаче.

Сброс результатов поиска

Чтобы сбросить результаты поиска, нажмите права от имени загруженного образца.

5.3.4 Выгрузка информации о файлах

Вы можете выгрузить информацию о файлах из таблицы в отчет. Формат файла отчета - XLSX.

Чтобы выгрузить данные:

1. Настройте фильтр (см. "Единый фильтр") и сортировку записей (см. "Настройка отображения таблицы").



Важно!

Если после фильтрации таблица содержит более 10 000 записей, то в отчет добавляются только первые 10 000 записей.

- 2. Нажмите ப на панели Единого фильтра.
- 3. В открывшемся окне:
 - а. В списке Состав выгрузки выберите Информация о файлах.
 - b. Чтобы добавить лист с дополнительной информацией в отчет, выберите в списке **Дополнительная информация**. Лист содержит:
 - дату и время формирования отчета;
 - настройки фильтров;
 - ссылку для перехода в Консоль управления.
 - с. Нажмите Сохранить.
- 4. Дождитесь уведомления о том, что отчет был сохранен.
- 5. Нажмите 🛅 в правом верхнем углу экрана.
- 6. В открывшемся окне нажмите на название отчета. Файл с отчетом будет сохранен на ваш компьютер.

5.3.5 Пример работы с таблицей

В таблице содержится информация о файлах, просканированных на различных ресурсах в рамках нескольких задач сканирования.

Необходимо определить:

- на каких рабочих станциях располагался файл с информацией о доходах;
- в какой временной период файл располагался на рабочих станциях.

О файле с информацией о доходах известно, что:

- имя файла включает в себя строку "доход";
- файл был создан в текущем месяце;
- размер файла не превышает 5 мегабайт.

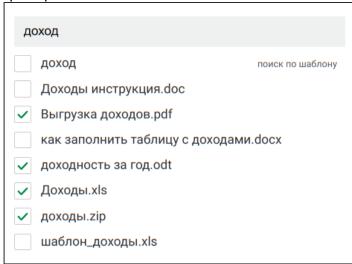
Настройка фильтров

Настройте фильтрацию для записей в таблице:

1. В фильтре **Задача** выберите из списка имя задачи, в рамках которой были просканированы рабочие станции. В нашем примере:

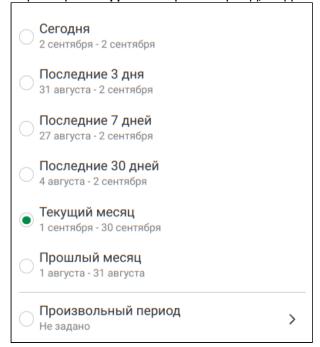
Сканирование сервера
Файловое хранилище
 Сканирование рабочих станций
Linux-сервер

- 2. Выберите значения для фильтра Имя файла:
 - а. В фильтре введите в строку поиска "доход";
 - b. Выберите интересующие имена файлов из предложенных в списке. В нашем примере:



(i) Примечание:

Отображение элементов в списке не зависит от условий других фильтров. Например, в списке могут присутствовать файлы из той задачи сканирования, которая не подходит под условие фильтра **Задача**. 3. В фильтре Создан выберите период, когда был создан файл. В нашем примере:



4. В фильтре Размер установите ограничение на размер файла. В нашем примере:



Результаты фильтрации

В таблице с информацией о файлах отображаются только записи, которые соответствуют одновременно всем указанным условиям:

- имя задачи сканирования, в которой был обнаружен файл "Сканирование рабочих станций";
- имя файла "Выгрузка доходов.pdf", "доходность за год.odt", "Доходы.xls" или "доходы.zip";
- файл был создан в текущем месяце;
- размер файла не превышает 5 мегабайт.

Выполните сортировку в таблице по столбцу Хост:

Обнаружен	Задача	Xoct ≧	Имя файла	Размер	Создан	Изменен	Не обнаружен
02.09.2022 15:22:17	Сканирование рабочих станций	user1.example.com	доходы.xls	4.21 MB	02.09.2022 15:15:17	02.09.2022 15:15:17	,,;;
04.09.2022 11:22:17	Сканирование рабочих станций	user2.example.com	доходы.xls	4.21 MB	04.09.2022 11:07:38	04.09.2022 11:07:38	04.09.2022 14:59:10
04.09.2022 13:52:11	Сканирование рабочих станций	user2.example.com	Выгрузка доходов.pdf	2.34МБ	04.09.2022 13:42:36	04.09.2022 13:42:36	,,;;
05.09.2022 18:01:29	Сканирование рабочих станций	user3.example.com	доходы.xls	4.21 MB	05.09.2022 17:59:20	05.09.2022 17:59:20	06.09.2022 13:01:29
06.09.2022 13:01:15	Сканирование рабочих станций	user3.example.com	доходы.xls	4.17Mb	05.09.2022 17:59:20	06.09.2022 13:00:01	,,

Файлы, соответствующие условиям, были найдены на 3 рабочих станциях:

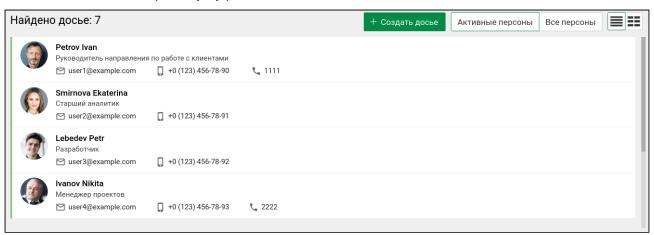
Имя рабочей станции	Описание записей о файлах
user1.example.com	Система обнаружила на хосте файл доходы.xls . Файл был впервые обнаружен 02.09.2022 в 15:22:17.
	Поле Не обнаружен не заполнено, что возможно в следующих случаях:
	 Неизмененный файл доходы.xls еще находится на ресурсе. Файл был изменен/удален, но повторное сканирование ресурса после изменения/удаления файла не проводилось.
user2.example.com	 Система обнаружила на хосте файл доходы.xls. Файл был впервые обнаружен 04.09.2022 в 11:22:17. Поле Не обнаружен заполнено – Система не обнаружила файл при повторном сканировании, что возможно в следующих случаях: Файл был удален с ресурса. Файл был изменен. Если после изменения файл соответствует условиям фильтров в настройках задачи, то при повторном сканировании в таблицу добавляется новая запись о измененном файле. Примечание: Запись о измененном файле может не отображаться в таблице, если файл не подходит под текущие условия фильтров таблицы. Условия фильтров в настройках задачи были изменены и при повторном сканировании файл не соответствовал новым условиям. Система обнаружила на хосте файл Выгрузка доходов.pdf. Файл был впервые обнаружен о4.09.2022 в 13:52:11. Поле Не обнаружен не заполнено.
user3.example.com	 Система обнаружила на хосте файл доходы.xls. Файл был впервые обнаружен 05.09.2022 в 18:01:29. Поле Не обнаружен заполнено. Система обнаружила на хосте файл доходы.xls. Файл был впервые обнаружен 06.09.2022 в 13:01:15. Поле Не обнаружен не заполнено.
	Дата создания и имя файла в обеих записях одинаковые. В записях различаются размер файла и дата изменения файла. Файл доходы.xls мог быть отредактирован на хосте, после чего при повторном сканировании:
	а. Был обнаружен измененный файл доходы.xls , в таблицу была добавлена новая запись.

Имя рабочей станции	Описание записей о файлах
	b. Не был обнаружен файл доходы.xls с неизмененными метаданными, у существующей записи Система заполнила дату и время, когда файл не был обнаружен.

5.4 Раздел "Досье"

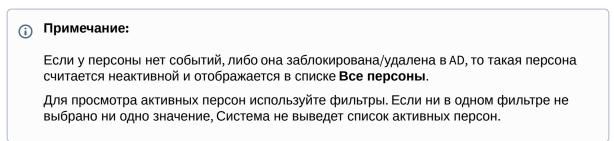
Раздел содержит справочник персон, данные которых загружены в Систему при синхронизации с Active Directory или Traffic Monitor, и персон, данные которых внесены вручную.

Для просмотра досье персоны, выберите ее левой кнопкой мыши. Для возврата к списку персон нажмите в левом верхнем углу рабочей области.



В списке персон отображаются только персоны, удовлетворяющие условиям единого фильтра. Для настройки отображения досье используйте кнопки в правой части рабочей области:

• **Активные персоны** – отобразить досье только сотрудников с активной учетной записью в Active Directory и хотя бы одним событием;



- **Все персоны** отобразить досье всех персон, включая когда-либо работавших в компании;
- 📕 отображать в виде таблицы;
- 🔢 отображать в виде плитки.

В этом разделе также доступны следующие действия:

- Просмотр досье персоны
- Просмотр и настройка виджетов персональной информации

- Просмотр информации о файлах, которыми владеет персона и к которыми имеет доступ
- Создание, редактирование и удаление досье
- Добавление контактов персоны
- Изменение руководителя персоны
- Объединение досье

5.4.1 Просмотр досье персоны

Досье содержит информацию о конкретном сотруднике в организации.

В Досье персоны отображается:

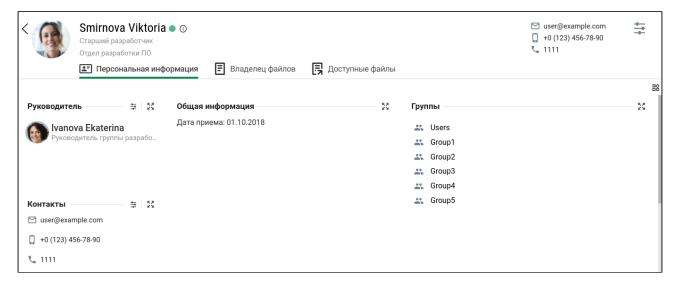
- ФИО сотрудника;
- Должность;
- Отдел;
- Контакты: учетная запись из Active Directory вида *login @company.com*, личные или рабочие контакты персоны, включая адрес электронной почты, номер телефона, номер мобильного телефона.

примечание:

Все персоны, добавленные при интеграции с Active Directory, имеют тип контакта SID, используемый для их идентификации.

Важно!

Не создавайте персон с одинаковым значением контакта SID. Наличие в Системе двух и более персон с одинаковыми SID приведет к некорректному определению владельца файла



Справа от имени персоны отображается цветовой индикатор статуса:

- 🔲 сотрудники, отключенные в AD или имеющие неопределенный статус.

Нажмите на иконку 🔘 справа от имени персоны, чтобы увидеть:

- дату создания досье;
- дату обновления досье;
- владельца досье Система или Офицер безопасности (если досье было добавлено вручную).

Чтобы изменить данные в досье, используйте кнопку в правой части рабочей области (подробнее см. "Создание, редактирование и удаление досье").

Информация в досье персоны представлена на вкладках:

- Персональная информация содержит виджеты досье, специфичные для персоны: Общая информация, Руководитель, Контакты, Группы, Описание (см. "Вкладка "Персональная информация"");
- Владелец файлов содержит таблицу с файлами, для которых персона определена владельцем (см. "Вкладки Владелец файлов и Доступные файлы");
- Доступные файлы содержит таблицу с файлами, к которым персона имеет доступ (см. "Вкладки Владелец файлов и Доступные файлы").

Чтобы вернуться к списку персон, нажмите 🔼 в верхнем левом углу рабочей области.

5.4.2 Вкладка "Персональная информация"

Виджеты на вкладке **Персональная информация** позволяют Офицеру безопасности просмотреть все данные по персоне, хранящиеся в Системе.

Название виджета	Описание
Руководитель	Отображает список руководителей персоны, а также позволяет задать руководителя вручную
Контакты	Позволяет управлять контактами персоны, а также отображает контакты, загруженные из подключенных источников
Общая информация	Отображает состояние персоны в различных источниках: дата приема, стаж работы, рабочее место, дата увольнения
Группы	Отображает список групп из ActiveDirectory или InfoWatch Traffic Monitor, в которые входит персона

Название виджета	Описание
Описание	Отображает описание персоны, позволяет задавать и редактировать его вручную

Чтобы развернуть виджет на весь экран, нажмите 🔄.

Чтобы отредактировать данные на виджете, нажмите 🚖.

5.4.3 Вкладки Владелец файлов и Доступные файлы

На вкладках **Владелец файлов** и **Доступные файлы** структура таблиц с файлами аналогична разделу **Информация о файлах** (подробнее см. "Таблица с информацией о файлах"), но все записи относятся к выбранной персоне. О фильтрации записей в таблицах см. "Единый фильтр".

Поиск дубликатов файлов доступен только в разделе Информация о файлах.

Вы также можете выгрузить отчет с представленными данными в формате XLSX (подробнее см. "Выгрузка информации о файлах").



Важно!

Владельца файлов и возможность доступа персоны к файлам Data Discovery определяет с помощью идентификатора безопасности SID. Если в контактах персоны отсутствует SID, на вкладках **Владелец файлов** и **Доступные файлы** информация будет недоступна.

Персоны, добавленные в результате интеграции с Active Directory (см. "InfoWatch Data Discovery. Руководство администратора", "Интеграция с Active Directory") имеют контакт типа SID.

Если персона добавлена вручную, чтобы Data Discovery мог определять ее как владельца файлов или определять наличие у нее доступа к файлам, добавьте персоне контакт типа SID (см. "Добавление контактов персоны").

5.4.4 Создание, редактирование и удаление досье

Чтобы создать досье новой персоны или дополнительное досье существующей в Системе персоны:

- 1. Перейдите в раздел Досье.
- 2. Нажмите **+ Создать досье**.
- 3. Заполните персональные данные:

Поле	Описание
Имя персоны	Имя персоны
Должность	Должность в организации
Отдел	Отдел, где работает персона
Описание	Дополнительное описание

4. Добавьте фотографию.

- 5. Добавьте контактные данные персоны: личный или рабочий номер телефона, адрес электронной почты, аккаунты в социальных сетях.
- 6. Нажмите Создать досье. Новое досье будет доступно в списке досье сотрудников.

Чтобы внести изменения в досье:

- 1. Откройте нужное досье.
- 2. Нажмите 🔄 и выберите Редактировать.
- 3. Внесите изменения и нажмите Сохранить.

Чтобы удалить досье:

- 1. Откройте нужное досье.
- 2. Нажмите 🔄 и выберите Удалить.
- 3. Нажмите ОК. Досье будет удалено без возможности восстановления.

Важно!

Если вы удалите досье с контактом типа SID, при идентификации персоны по этому SID в полях Владелец и Доступен для будет отображаться имя персоны из удаленного досье. Чтобы это исправить, создайте новое досье и добавьте ему этот SID.

Чтобы обновить значения полей Владелец и Доступен для выполните повторное сканирование.

5.4.5 Добавление контактов персоны

При синхронизации с Active Directory и InfoWatch Traffic Monitor становятся доступны контакты персон: номера телефона, адреса электронной почты, аккаунты в социальных сетях (при синхронизации с ТМ) и прочее. При этом пользователь может добавить дополнительные контакты вручную. Для этого:

- 1. Перейдите в досье персоны.
- 2. На вкладке Персональная информация на виджете Контакты нажмите 🚖.
- 3. В открывшемся окне будут отображены все автоматически добавленные при интеграции из других систем контакты персоны. При этом по умолчанию показаны по одному контакту типа: логин в домене, телефон, электронная почта, мобильный телефон.

Нажмите Добавить контакт.

4. Укажите тип контакта (например, личный номер телефона) и введите его значение. Возможно добавить несколько позиций и оставить комментарий к контакту, для этого нажмите 🗐



примечание:

Для идентификации персоны, владеющей файлом или имеющей доступ к файлу, добавьте ей контакт типа SID.

4

Важно!

Не создавайте персон с одинаковым значением контакта типа SID. Наличие в Системе двух и более персон с одинаковыми SID приведет к некорректному определению владельца файла.

5. Нажмите **Сохранить**. Новый контакт доступен в досье. Наличие комментария к контакту отмечается значком ①. Чтобы прочитать комментарий, нажмите на него.

5.4.6 Изменение руководителя персоны

На вкладке **Персональная информация** на виджете **Руководитель** указан руководитель персоны. Данная информация добавляется при синхронизации с Active Directory и InfoWatch Traffic Monitor.

Офицер безопасности может изменить руководителя персоны, который был добавлен вручную. Руководитель персоны, загруженный из системы-источника, не редактируется. Для изменения руководителя:

- 1. На виджете нажмите 🗐
- 2. В открывшемся окне **Изменение руководителя** в поле *Добавлено вручную* введите имя нового руководителя из числа персон, зарегистрированных в Системе. Допускается добавить несколько имен.
- 3. Нажмите **Сохранить**. На виджете **Руководитель** отображаются указанные руководители.

Для перехода в досье руководителя щелкните левой клавишей мыши на его имени на виджете **Руководитель**.

5.4.7 Объединение досье

Вы можете объединить два или несколько досье в одно. При этом новое досье будет содержать всю информацию из досье, существовавших до объединения. Для этого:

- 1. Откройте досье, которое требуется объединить с другими.
- 2. Нажмите 🔄 и выберите Объединить досье.
- 3. В открывшемся окне в поле **Объединить с** выберите для объединения одно или несколько досье из списка.
- 4. Нажмите Объединить.

5.5 Единый фильтр

Единый фильтр – инструмент, позволяющий управлять отображением данных, которые хранятся в Системе.

Единый фильтр доступен в разделе Информация о файлах.

С помощью Единого фильтра вы можете:

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

5.5.1 Фильтры



Важно!

Фильтры **Владелец** и **Доступен для** могут работать некорректно после обновления Системы. Отредактируйте или пересоздайте все наборы фильтров (**Запросы**), которые включают эти фильтры.

Единый фильтр – панель, которая содержит несколько фильтров. Фильтры соответствуют полям таблицы с информацией о файлах.

Название фильтра	Описание	Установка значений
Обнаружен	Период времени, в который файл был впервые обнаружен	Выберите период времени: • Сегодня;
Создан	Период времени, в который файл был создан	Последние 3 дня;Последние 7 дней;Последние 30 дней;
Изменен	Период времени, в который файл был изменен	 Текущий месяц; Прошлый месяц; Произвольный период: Период (укажите даты начала и конца периода); Выбрать дату (укажите одну или несколько дат). Значение по умолчанию: Любая дата
Задача	Название задачи сканирования	Чтобы выбрать значение, выполните одно из действий:
Хост	Имя хоста	 Выберите значение из списка. Для поиска в списке введите значение в строку поиска.
ІР-адрес хоста	ІР-адрес хоста	Отображение элементов в списке не зависит от условий,
Расположение	Полный путь к директории	установленных в других фильтрах.
Имя файла	Имя Файла	 Введите значение в строку поиска и выберите значение типа "поиск по шаблону".
		Значение по умолчанию: Все
Владелец	Персона, которая является владельцем файла	В списке отображаются имена персон и групп, идентифицированных по SID. Вы можете фильтровать записи одновременно и по группам, и по

Название фильтра	Описание	Установка значений
Доступен для	Персоны и группы, которые имеют доступ к файлу	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. "Таблица с информацией о файлах".
		Значение по умолчанию: Все
		Примечание: Если доступ к файлу имеет именно группа, а не конкретные персоны, поиск по персонам, входящим в группу не даст результатов. 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

5.5.2 Переход в другие продукты Платформы

При переходе в интерфейс другого продукта Платформы набор фильтров меняется на специфичный набор этого продукта.

Сохраняются значения следующих фильтров:

- при переходе в Infowatch Activity Monitor:
 - Обнаружен;
 - Расположение;
 - Имя файла;
 - Размер;
- при переходе в Infowatch Vision:
 - Обнаружен.

5.5.3 Работа с Единым фильтром

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.

Значения фильтров

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

Если изменить значение фильтра, то автоматически обновится таблица в разделе **Информация о** файлах. В таблице отображаются только те записи, которые соответствуют условиям фильтров.



Важно!

При выходе из Системы сбрасываются значения фильтров. Рекомендуется сохранить фильтры перед выходом из Системы (см. "Сохранение и загрузка 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 Имя файла укажите значение: отчет .doc
- в фильтре Задача укажите значение: Сканирование сетевых ресурсов
- в фильтре Размер укажите в поле до значение 2 и выберите единицу измерения МБ

В результате настройки в таблице с информацией о файлах отображаются только записи, которые одновременно соответствуют всем вышеуказанным условиям.

В таблице отображаются записи о файлах с именем **отчет.doc** из задачи **Сканирование сетевых ресурсов**, если размер файла не превышает 2 мегабайта.

Тип значения "поиск по шаблону"

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

- Задача;
- Xoct;
- ІР-адрес хоста;
- 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":

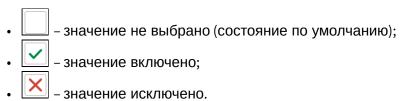


Включение и исключение значений фильтра

Доступны несколько состояний для значений следующих фильтров:

- Задача;
- XOCT;
- ІР-адрес хоста;
- Расположение;
- Имя файла;
- Владелец;
- Доступен для;
- Тип подключения.

Доступные состояния для значений вышеуказанных фильтров:



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:

В таблице находятся 5 записей 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 таблице 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 в таблице отображаются 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 $\stackrel{\textstyle |\times|}{\times}$. Для фильтра будет установлено значение по умолчанию.

Чтобы сбросить значения для всех фильтров, нажмите Очистить фильтры.

Сохранение и загрузка наборов фильтров

Чтобы использовать заданные значения фильтров в дальнейшем, вы можете сохранить фильтры. Для этого:

- 1. На панели фильтров выберите Сохранить.
- 2. В открывшемся окне укажите имя набора фильтров.
- 3. Выберите тип:
 - **Личный** фильтры будет доступны только пользователю, который сохранил фильтры;
 - Общий фильтры будет доступны всем пользователям Системы.
- 4. Нажмите Сохранить.

Чтобы воспользоваться ранее сохраненным набором фильтров:

- 1. На панели фильтров выберите Запросы.
- 2. Нажмите на имя набора, чтобы активировать фильтры.

6 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. 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, модифицировать ПО, осуществлять попытки предпринять аналогичные действия в отношении ПО, а также создавать производные работы, основанные на ПО и/или Документации;
- 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;
- сдавать ПО в аренду, прокат или во временное пользование, сублицензировать, распространять или иным образом предоставлять любому физическому или юридическому лицу любые права в отношении ПО и/или Документации, а также разглашать результаты стендовых испытаний ПО, за исключением случаев, прямо разрешенных настоящим Соглашением;
- передавать и предоставлять доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения и Договора, заключенного между вами и вашим лицензиаром;
- 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. 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, 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 license.inf (license.info), распространяемом с ПО в составе дистрибутива.

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 какоголибо 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

7 Глоссарий

Термин	Определение
Администратор	Администратор – пользователь Системы, выполняющий установку, настройку и поддерживающий работу Системы. См. также: Офицер безопасности, Пользователь
Группа SMB	Параметр, позволяющий использовать Систему как часть определенной рабочей группы для сетевого управления папками, расположенными на рабочих станциях, терминальных серверах, файловых хранилищах и т.д. (например, домен)
Задача сканирования	Операция проверки ресурсов (путей сканирования) на наличие конфиденциальных данных. Задача содержит описание ресурсов сканирования, загрузки и передачи файлов с них в Traffic Monitor. Включает в себя список хостов, список путей сканирования, фильтр по именам сканируемых файлов, фильтр по размеру сканируемых файлов, фильтр по директориям и расписание для автоматического запуска и остановки задачи
Зона	Группа серверов Data Discovery. В зону могут входить несколько серверов из кластера Системы. Каждая зона имеет отдельные настройки для экспорта данных в Traffic Monitor
Интерфейс пользователя	Совокупность средств и методов, при помощи которых пользователь взаимодействует с Системой
Информация о файле	Информация о файле включает в себя метаданные файла и данные о сканировании файла/ресурса. К данным о сканировании файла/ресурса относятся: название задачи; дата обнаружения файла; IP-адрес хоста и др. См. также: Метаданные файла
Консоль управления	Графический интерфейс пользователя, предназначенный для управления системой Data Discovery (администрирование и настройка Системы, работа с задачами сканирования)
Лицензия	Право на использование Системы. Получается при приобретении Системы и определяет допустимые действия с Системой

Термин	Определение
Маска	Шаблон поиска – метод описания поискового запроса с использованием метасимволов. Маски используются для фильтра по именам сканируемых файлов и для фильтра по директориям
Метаданные файла	Данные о файле, которые Data Discovery получает из файловой системы ресурса:
	 Полный путь к файлу; Имя файла; Размер файла; Дата и время создания файла; Дата и время изменения файла; Владелец файла; Пользователи/группы, которые имеют доступ к файлу.
	См. также: Информация о файле
Офицер безопасности	Основной пользователь Консоли управления. Также – предустановленная роль пользователя Консоли управления, имеющая привилегии на все действия в Системе, за исключением административных
План выполнения задачи	Формируемый сервисом Execution Controller порядок действий для сервиса сканера (Puller). Определяет последовательность обработки ресурсов
Пользователь	Пользователь системы Data Discovery - администратор, офицер безопасности и др. См. также: Администратор, Офицер безопасности
Продуктовая 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
Проход	Полное сканирование одного ресурса (т.е. все файлы на ресурсе должны быть обработаны сервисом сканера (Puller)). Проход может состоять из нескольких сессий
Рабочая станция/Компьютер	В терминах Системы подразумевается контролируемая рабочая станция или терминальное устройство
Расписание	Расписание для автоматического запуска и остановки задачи. Доступно ежедневное и еженедельное расписание

Термин	Определение
Pecypc (Resource)	Ресурс хоста, который содержит файлы. Система сканирует файлы на ресурсах и загружает файлы в хранилище. Для подключения к ресурсу необходимо указать путь сканирования хоста
Сессия	Подключение к ресурсу в рамках прохода. Длительность сессии сканирования (параметр Длительность обработки) задается в расширенных настройках задачи
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 продукте Data Discovery для хранения настроек и конфигураций задач, а также статистики о задачах. Компонент продуктовой Платформы
Фильтры папок	Набор условий для обработки директорий на ресурсах. Представляет из себя список директорий, включенных в обработку, и список директорий, исключенных из обработки
Фильтры файлов	Набор условий в настройках задачи для сканирования и загрузки файлов с ресурсов. Представляет из себя список масок для фильтрации по именам файлов, а также фильтры по максимальному и минимальному размеру файлов
XOCT (Host)	Рабочая станция или сервер, к которому осуществляется подключение для сканирования файлов и загрузки с него файлов для дальнейшего анализа. Содержит список ресурсов для сканирования
Хранилище (Storage)	Временное место хранения скачанных файлов. Файл хранится здесь до отправки в Traffic Monitor
Экспорт данных в Traffic Monitor	Описание подключения к Traffic Monitor для отправки скачанных с ресурсов файлов и их дальнейшего анализа. Указывает на конкретную инсталляцию Traffic Monitor, требуется токен авторизации и список адресов XAPI. В меню Консоли управления Системы относится к разделу Зоны и серверы
Discoperator	Сервис представляет из себя бэкенд и используется для работы Консоли управления.
FTP	Протокол передачи данных по сети

Термин	Определение
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
Nextcloud	Набор клиент-серверных программ для создания и использования хранилища данных
Puller	Сервис для сканирования ресурсов и загрузки файлов с них. Экземпляры сервиса Puller – сканеры. Сканеры собирают метаданные файлов и загружают файлы с ресурсов в хранилище
Sender	Сервис для отправки загруженных файлов в Traffic Monitor. Экземпляры сервиса Sender – передатчики. Передатчики отправляют файлы из хранилища в Traffic Monitor для анализа. После отправки файла в Traffic Monitor передатчик удаляет файл из хранилища
SMB (Server Message Block)	Сетевой протокол для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SSH (Secure Shell)	Сетевой протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов)
Task Execution Controller	Сервис для управления выполнением задачи. Контролирует работу над задачей всех остальных сервисов
TPS Agent	Сервис для мониторинга состояния хранилища. Помогает работе с хранилищем сервисам Puller и Sender, предоставляет статистику по хранилищу
WebDAV	Расширение протокола HTTP, позволяющее пользователям управлять файлами, хранящимися на удаленных серверах
XAPI	Приватный API для передачи файлов в Traffic Monitor