INFOWATCH®

InfoWatch Data Access Tracker

Руководство администратора

INFOWATCH DATA ACCESS TRACKER

Руководство администратора

Тел. +7 (495) 229-00-22 • Факс +7 (495) 229-00-22
http://www.infowatch.ru

Дата редакции: июль 2021 года

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящем руководстве содержатся сведения о развертывании InfoWatch DAT, об особенностях интерфейса веб-консоли, сборе информации и о возможностях анализа данных, которые предоставляет InfoWatch DAT.

Документ предназначен для администраторов системы аудита и управления информационными активами InfoWatch DAT.

InfoWatch DAT – это инструмент сбора и анализа информации об объектах и событиях корпоративной сети. InfoWatch DAT состоит из веб-консоли, программной части и базы данных.

АНАЛИЗ ОБЪЕКТОВ КОРПОРАТИВНОЙ СЕТИ

Администрирование корпоративных сетей, даже небольших, является непростой задачей. Необходимость постоянного анализа состояния объектов корпоративной инфраструктуры, таких как компьютеры, почтовые ящики, пользователи и события приводит к естественному выводу о необходимости автоматизированного решения для обработки и анализа потока данных.

InfoWatch DAT предоставляет интерфейс, в котором вы можете обрабатывать и анализировать не только количественные и качественные показатели объектов корпоративной инфраструктуры. С помощью InfoWatch DAT вы можете анализировать и оценивать риски для пар объектов, например, пользователи и файлы, пользователи и почтовые ящики.

ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

InfoWatch DAT обладает следующими функциональными характеристиками:

Управление инцидентами:

- Сбор и хранение инцидентов из разных источников.
- Управление инцидентами.
  - Установка сроков решения инцидентов.
  - Приоритизация инцидентов.
  - Установка статусов решения инцидентов.
  - Возможность комментировать инциденты.
  - Категоризация инцидентов.
  - Назначение сценариев реагирования.
  - Назначение ответственных за решение инцидентов.
  - Добавление наблюдателей.
- Просмотр сводной информации об инцидентах.
- Автоматизация реагирования на инциденты с применением файлов скриптов.
- Получение уведомлений об инцидентах.
- Импорт и экспорт инцидентов.

Анализ данных:

- Сбор данных о следующих событиях:
  - Изменения файлов и папок.
  - Изменения в составе и параметрах пользователей, компьютеров и групп.
  - События Event Log.
- Аудит структуры данных и прав доступа к ним.
- Сбор и просмотр статистики об объектах и событиях.
- Анализ зависимостей групп объектов:
  - Пользователи – файлы.
  - Файлы – пользователи.
  - Пользователи – почтовые ящики.
  - Приложения – компьютер.
- Выявление риск-факторов.
- Автоматизация реагирования на риск-факторы с применением скриптов.
- Выявление текстовых файлов, регулируемых стандартами.
- Автоматизация сбора данных с помощью агентов сбора данных.
- Создание задач сбора данных заданного типа.

ПРОГРАММНО-АППАРАТНЫЕ ТРЕБОВАНИЯ

Аппаратные требования

- Процессор Intel Core i5
- Оперативная память (ОЗУ): 8 GB
- Свободное место на жестком диске: 10 GB

Программные требования

Поддерживаемые операционные системы:

- Windows 10
- Windows Server 2016
- Windows Server 2019

Дополнительное программное обеспечение:

- Браузер Chrome.

> **Внимание!** Для работы InfoWatch DAT требуется доступ в интернет.

НЕОБХОДИМЫЕ ПРАВА

Для работы сервиса:

Требуется сервисная учетная запись с правами:

- Локального администратора
- Запуска Powershell скриптов (ExecutionPolicy Bypass)

Для аудита Active Directory:

Требуется учетная запись с правом чтения всех свойств всех аудируемых объектов в Active Directory.

Для аудита изменений в Active Directory:

Требуется учетная запись с правами (Группа Event Log Readers и отдельные права на журнал security (см. Event log access rights в Базе знаний IW DAT). Назначение привилегий на журнал безопасность осуществляется из реестра.

Для аудита файловых ресурсов:

Требуется учетная запись с правами и доступ на исследуемый файловый ресурс (Read and Execute).

Для аудита действий на файловых ресурсах:

Требуется учетная запись с правами и доступ на чтение журналов событий на исследуемых контроллерах домена и файловом сервере (в том числе журнал Security). Группа Event Log Readers и отдельные права на журнал security (см. Event log access rights в Базе знаний IW DAT).

Для аудита MS Exchange

Требуется учетная запись с правами MS Exchange Администраторов, входящих в группы ролей управления организацией с правами только на просмотр.

Для аудита действий в MS Exchange

Требуется учетная запись с правами MS Exchange Администраторов, входящих в группы ролей управления организацией с правами только на просмотр.

Для работы продукта необходимо настроить сам аудит

- Для Active Directory см. Active Directory policy auditing в Базе знаний IW DAT.
- Для общедоступных хранилищ см. Objects auditing в Базе знаний IW DAT.
- Для почты см. Mailbox audit logging в Базе знаний IW DAT.

> **Внимание!** Powershell скрипты могут изменяться во время эксплуатации, поэтому, если их необходимо подписывать, то подписывать потребуется при каждом их изменении.

Для большего понимания в **Приложении 2** вы можете найти схему взаимодействия модулей Системы.

РАЗВЕРТЫВАНИЕ INFOWATCH DAT В КОРПОРАТИВНОЙ СЕТИ

Установка на ОС Microsoft Windows из MSI-файла

> **Внимание!** Установка из MSI-файла может быть выполнена как на физической, так и на виртуальной машине.

1. Установите СУБД PostgreSQL версии 9.6 x64 или выше.
2. Установите средство администрирования pgAdmin.
3. Запустите pgAdmin и создайте пустую базу данных в СУБД PostgreSQL.
4. Двойным щелчком мыши запустите файл InfoWatch-DAT.msi из комплекта поставки.

   В список служб Windows будет добавлена служба InfopWatch DAT Service. Служба будет запущена автоматически.
5. Измените параметры подключения к СУБД PostgreSQL в конфигурационном файле config.json в папке установки программы.

   Путь к папке установки: <Название системного диска>:\Program Files (x86)\ InfoWatch-DAT(на примере Windows 10).

> **Внимание!** Редактирование файла config.json следует выполнять от имени администратора.

Пример параметров подключения:

```
"orm": {
   "host": "127.0.0.1",
   "pwd": "test",
   "user": "postgres",
   "dbname": "iw_admin"
}
```

6. Перезапустите службу.

Удаление приложения, установленного из MSI-файла

1. Откройте список приложений, установленных в вашей операционной системе.
2. Выберите приложение InfoWatch DAT и нажмите на кнопку **Удалить**.

ИНТЕРФЕЙС ВЕБ-КОНСОЛИ

Интерфейс веб-консоли (см. Изображение 1) состоит из следующих элементов:

- **Основное меню**. Плавающее меню, которое содержит основные разделы веб-консоли. Может быть свернуто или перемещено в панель инструментов. По умолчанию расположено в левой части экрана.
- **Рабочая область**. Область, изменяющаяся в зависимости от выбранного раздела. В рабочей области могут отображаться сводка зарегистрированных инцидентах и добавленных объектах, окна регистрации новых инцидентов и добавления объектов и другие инструменты. Рабочая область занимает большую часть экрана.
- **Панель инструментов**. Панель, которая содержит дополнительные инструменты для управления инцидентами и объектами, включая поиск, оповещение о новых и назначенных инцидентах, а также средства переключения учетных записей и языка системы. Панель расположена в верхней части экрана.
- **Панель управления видом консоли**. Панель содержит инструменты управления основным меню и темой веб-консоли.

Изменение положения основного меню

1. Нажмите на кнопку  в левом нижнем углу.
2. Выполните одно из следующих действий:
    a. Переведите переключатель **Свернутое меню** в положение **ВКЛ** или **ВЫКЛ**, чтобы свернуть или развернуть основное меню.
    b. Переведите переключатель **Меню сверху** в положении **ВКЛ** или **ВЫКЛ**, чтобы переместить основное меню в верхнюю часть экрана или вернуть меню в левую часть экрана.

> **Внимание!** Если переключатель **Меню сверху** включен, основное меню нельзя свернуть.

ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Этот раздел содержит информацию о том, как регистрировать инциденты ИБ в веб-консоли и управлять зарегистрированными инцидентами. Кроме того, в этом разделе содержится информация о создании категорий, статусов, сценариев обработки инцидентов и меток для инцидентов.

Регистрация инцидентов

Вы можете регистрировать инциденты вручную или импортировать из существующей базы данных инцидентов, используя запросы REST API.

Регистрация инцидента

1. В боковом меню выберите пункт **Инциденты** -> **Список**.
2. В правом верхнем углу рабочей области нажмите на кнопку **Зарегистрировать**.

   Откроется окно, в котором вы можете зарегистрировать новый инцидент.
3. В раскрывающемся списке **Категория** выберите категорию инцидента.
4. В раскрывающемся списке **Сценарий** выберите сценарий обработки инцидента.

> **Внимание!** При выборе категории и сценария в инциденте автоматически появится назначенная инструкция по обработке инцидента.

5. В раскрывающемся списке **Приоритет** выберите приоритет инцидента.
6. В раскрывающемся списке **Статус** выберите статус инцидента.
7. В раскрывающемся списке **Ответственный** выберите лицо, ответственное за решение инцидента.
8. В поле **Тема** введите краткую информацию об инциденте.
9. В поле **Описание** добавьте подробную информацию об инциденте.
10. Нажмите на кнопку **Создать**.

Инцидент будет зарегистрирован в базе данных.

Импорт инцидентов из базы данных

Вы можете использовать запрос со следующим синтаксисом:

```
POST /incident/ HTTP/1.1
Host: localhost:8000
Content-Type: application/json
Authorization: Basic YWRtaW46YWRtaW4=
```

```
cache-control: no-cache
Postman-Token: 66c89571-101d-4247-b3b1-2d50e43b6d0b
{
    "assignee": "test_admin@gmail.com",
    "body": "<p>Текст</p>",
    "category": "8",
    "playbook": "0",
    "priority": "3",
    "state": "3",
    "title": "Вирус"
```

Управление зарегистрированными инцидентами

В этом разделе дается информация о том, как просматривать сводные данные о зарегистрированных инцидентах, а также о том, как изменять параметры, просматривать историю и добавлять комментарии в зарегистрированные инциденты.

Просмотр сводной информации об инцидентах

В боковом меню выберите пункт **Инциденты** -> **Сводка**.

Откроется окно с краткой информацией об инцидентах, зарегистрированных в базе данных.

В этом окне вы сможете найти следующие данные об инцидентах:

- Общее количество инцидентов в системе.
- Количество инцидентов, решение которых назначено текущей учетной записи.
- Количество инцидентов, созданных с текущей учетной записи.
- Общее количество инцидентов, которые не были рассмотрены текущей учетной записью.
- Количество нерассмотренных инцидентов, решение которых назначено текущей учетной записи.
- Количество не просмотренных инцидентов, созданных с текущей учетной записи.
- Общее количество открытых инцидентов.
- Количество открытых инцидентов, решение которых назначено текущей учетной записи.
- Количество открытых инцидентов, созданных с текущей учетной записи.
- Графики по статусам, категориям, меткам, приоритету и лицам, ответственным за решение, для всех инцидентов, зарегистрированных в базе данных.

Просмотр инцидентов в виде списка

1. В боковом меню выберите пункт Инциденты > Список.

   Откроется список инцидентов, имеющихся в базе данных.

2. Выполните следующие действия:

- Нажмите на кнопку **Назначено мне**, чтобы просмотреть все инциденты, назначенные текущей учетной записи.
- Нажмите на кнопку **Создано мной**, чтобы просмотреть все инциденты, созданные текущей учетной записью.
- Нажмите на кнопку **Открытые**, чтобы просмотреть все открытые инциденты.
- В раскрывающемся списке **Важность** выберите один из типов приоритета, чтобы просмотреть все инциденты, которые относятся к этому типу.
- В раскрывающемся списке **Статус** выберите одно из состояний инцидента, чтобы просмотреть все инциденты, которые относятся к этому состоянию.
- В раскрывающемся списке **Метка** выберите одну из меток, чтобы просмотреть все инциденты, которые помечены этой меткой.

Просмотр инцидентов в виде таблицы

1. В боковом меню выберите пункт Инциденты > Список.

   Откроется список инцидентов, имеющихся в базе данных.

2. В верхнем правом углу нажмите на кнопку  .

Кнопка изменится на  и список инцидентов будет отображен в виде таблицы. Чтобы вернуться к виду по умолчанию, нажмите на кнопку еще раз.

Просмотр и изменение информации об инциденте

1. В боковом меню выберите пункт Инциденты > Список.

   Откроется список инцидентов, имеющихся в базе данных.

2. Нажмите на инцидент в списке.

   Откроется окно изменения инцидента.

3. Выполните следующие действия:

- Перейдите на закладку **Описание**, чтобы просмотреть или изменить информацию об инциденте, предоставленную лицом, зарегистрировавшим инцидент.
- Перейдите на закладку **Комментарий**, чтобы просмотреть комментарии лиц, ответственных за решение инцидента, или добавить свой комментарий.
- Перейдите на закладку **Активность**, чтобы просмотреть историю работы с инцидентом.
- Перейдите на закладку **Файлы**, чтобы добавить или загрузить файлы, прикрепленные к инциденту.
- Перейдите на закладку **Объекты**, чтобы добавить пользователя, компьютер, файл или событие, связанные с инцидентом.
- Перейдите на закладку **Инструкции**, чтобы ознакомиться с действиями, которые необходимо выполнить для решения инцидента.

Установка сроков решения инцидента

Вы можете указать время, в течение которого инцидент должен быть решен.

Установка сроков решения инцидента

1. В боковом меню выберите пункт **Инциденты** -> **Список**.

   Откроется список инцидентов, имеющихся в базе данных.

2. Нажмите на инцидент в списке.

   Откроется окно изменения инцидента.

3. Нажмите на кнопку  в строке **Решить до**.

   Откроется диалоговое окно, в котором вы можете выбрать дату и время, когда инцидент должен быть решен.

4. Установите дату и время и нажмите на кнопку **Применить**.

Добавление и удаление наблюдателей

Вы можете установить наблюдателей, которые будут следить за ходом решения инцидента.

Добавление наблюдателей в зарегистрированном инциденте

1. В боковом меню выберите пункт **Инциденты** -> **Список**.

   Откроется список инцидентов, имеющихся в базе данных.

2. Нажмите на инцидент в списке.

   Откроется окно изменения инцидента.

3. В строке **Наблюдатели** нажмите на кнопку  .

   Откроется окно выбора наблюдателей.

4. Выберите наблюдателя из списка.

   Наблюдатель будет получать уведомления о ходе решения инцидента по электронной почте.

Удаление наблюдателей в зарегистрированном инциденте

1. В боковом меню выберите пункт **Инциденты** -> **Список**.

   Откроется список инцидентов, имеющихся в базе данных.

2. Нажмите на инцидент в списке.

   Откроется окно изменения инцидента.

3. В строке **Наблюдатели** нажмите на кнопку  напротив имени наблюдателя, которого вы хотите удалить.

Добавление файлов к зарегистрированному инциденту

При работе с инцидентом может возникнуть необходимость добавить файлы. Это могут быть доказательства (например, объяснительные) или дополнительная информация об инциденте (например, правила прокси-сервера для блокировки атаки).

Добавление файлов в зарегистрированный инцидент

1. В боковом меню выберите пункт **Инциденты** -> **Список**.

   Откроется список инцидентов, имеющихся в базе данных.
2. Нажмите на инцидент в списке.
3. На закладке **Файлы** перетащите файл в область загрузки или нажмите на нее, чтобы выбрать файл в системном окне проводника.

   Файл будет добавлен к инциденту.

Удаление файла из инцидента

1. В боковом меню выберите пункт **Инциденты** -> **Список**.

   Откроется список инцидентов, имеющихся в базе данных.
2. Нажмите на инцидент в списке.
3. На закладке **Файлы** нажмите на кнопку  напротив файла, который требуется удалить.

Добавление объектов к зарегистрированному инциденту

Вы можете добавить к зарегистрированному инциденту объекты, собранные с помощью скриптов сбора данных (пользователей, компьютеры, файлы или события). После добавления объекта к инциденту этот инцидент будет также отображаться в информации пользователя.

Добавление объекта к инциденту

1. В боковом меню выберите пункт **Инциденты** -> **Список**.

   Откроется список инцидентов, имеющихся в базе данных.
2. Нажмите на инцидент в списке.
3. На закладке **Объекты** нажмите на кнопку **Добавить объекты**.

   Откроется окно, в котором вы можете выбрать объекты, добавляемые к инциденту.
4. Нажмите на объект, который требуется добавить к инциденту.

   Объект будет добавлен к инциденту.

Удаление объекта из инцидента

1. В боковом меню выберите пункт **Инциденты** -> **Список**.

   Откроется список инцидентов, имеющихся в базе данных.
2. Нажмите на инцидент в списке.

3. На закладке **Объекты** нажмите на кнопку  напротив объекта, который вы хотите удалить из инцидента.

Настройки инцидентов

В комплекте поставки InfoWatch DAT присутствует файл settings.json с настройками по умолчанию. При первоначальном развертывании платформы рекомендуется загрузить настройки по умолчанию из этого файла.

Загрузка файла settings.json с настройками по умолчанию

1. В боковом меню выберите пункт **Данные** -> **Загрузка**.
2. Выполните одно из следующих действий:
3. Перетащите файл settings.json в поле **Загрузить файлы с данными**.
4. Нажмите на кнопку **Загрузить** и выберите файл settings.json.
5. Настройки по умолчанию будут применены.

О статусах инцидентов

Статусы инцидентов предназначены для отслеживания текущего этапа работ по разрешению инцидента. Вы можете добавлять свои статусы, чтобы детализировать процесс, и фильтровать инциденты по текущему состоянию. Например, вы можете добавить статусы Зарегистрирован, В работе, Работа завершена.

Создание статусов инцидентов

1. В боковом меню выберите пункт **Настройки** -> **Инциденты** > **Статусы**.

   Откроется список статусов, которые можно присвоить инциденту. По умолчанию список пуст.

2. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.

   Откроется окно, в котором вы можете добавить детали нового статуса.

3. Выполните следующие действия:
   c. В поле **Имя** введите название статуса.
   d. В поле **Описание** добавьте описание статуса.
   e. В списке **Цвет** выберите цвет, который будет соответствовать статусу.
   f. Установите флажок **Конец обработки**, если этот статус означает, что инцидент закрыт.
4. Нажмите на кнопку **Создать**.

Статус будет добавлен в список статусов, а также станет доступен при создании и изменении инцидентов.

Изменение статуса инцидента

1. В боковом меню выберите пункт **Инциденты** -> **Список**.

Откроется список инцидентов, имеющихся в базе данных.

2. Нажмите на инцидент в списке.

   Откроется окно изменения инцидента.

3. В списке **Статус** выберите статус, который вы хотите установить инциденту.

О категориях инцидентов

Категории инцидентов служат для разделения группы инцидентов по общему признаку.

Добавление категорий инцидентов

1. В боковом меню выберите пункт **Настройки** -> **Инциденты** -> **Категории**.

   Откроется список категорий, которые можно присвоить инциденту. По умолчанию список пуст.

2. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.

   Откроется окно, в котором вы можете добавить детали новой категории.

3. Выполните следующие действия:

   g. В поле **Имя** введите название категории.

   h. В поле **Описание** добавьте краткую информацию о категории.

   i. В списке **Приоритет по умолчанию** выберите приоритет, который будет автоматически присваиваться инциденту при выборе категории.

   j. В списке **Ответственный по умолчанию** выберите лицо, ответственное за решение инцидента, которое будет автоматически назначено при выборе категории.

   k. В поле **Инструкции** добавьте список действий, который нужно выполнить ответственному лицу для решения инцидента. При необходимости использовать язык гипертекстовой разметки установите флажок **Редактировать как HTML**.

4. Нажмите на кнопку **Создать**.

   Категория будет добавлена в список категорий, а также станет доступна при создании и изменении инцидентов.

О сценариях реагирования

Сценарии реагирования – это набор инструкций, которые должен выполнить ответственный за решение инцидента.

Вы можете создавать сценарии реагирования и назначать их инцидентам.

Создание сценария реагирования

1. В боковом меню выберите пункт **Настройки** -> **Инциденты** -> **Сценарии реагирования**.

   Откроется список сценариев реагирования на инциденты. По умолчанию список пуст.

2. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.
3. Откроется окно, в котором вы можете добавить детали нового сценария.
4. Выполните следующие действия:
    l. В поле **Имя** введите название сценария реагирования.
    m. В поле **Описание** добавьте краткую информацию о сценарии реагирования.
    n. В списке **Действие** выберите действие, которое необходимо выполнить в сценарии реагирования.
    o. В списке **Поля** выберите поля, которые соответствуют сценарию реагирования.
    p. В списке **Для категории** выберите категорию, при выборе которой сценарий реагирования будет автоматически назначен инциденту.
    q. В поле **Инструкции** добавьте информацию о действиях, которые необходимо выполнить для решения инцидента. При необходимости использовать язык гипертекстовой разметки установите флажок **Редактировать как HTML**.
5. Нажмите на кнопку **Создать**.

Сценарий реагирования будет добавлен в список сценариев, а также станет доступен при изменении существующих инцидентов.

О метках

Для дифференциации зарегистрированных инцидентов вы можете добавлять метки. Метки – это дополнительный инструмент для быстрого добавления и получения информации об инциденте. Метки выглядят как разноцветные области с поясняющим текстом и отображаются в списке инцидентов.

Вы можете создать набор меток (например, Под контролем СИБ, Под контролем генерального директора) разных цветов.

Создание меток

1. В боковом меню выберите пункт **Настройки** -> **Метки**.

    Откроется список меток. По умолчанию список пуст.
2. Нажмите на кнопку **Создать**.

    Откроется окно, в котором вы можете добавить детали новой метки.
3. В поле **Имя** введите название новой метки.
4. В поле **Описание** добавьте информацию о метке.
5. В списке **Цвет** выберите цвет метки.
6. Нажмите на кнопку **Создать**.

Метка будет добавлена в список меток, а также станет доступна при изменении инцидентов.

Вы можете добавлять метки существующим инцидентам.

Добавление меток для инцидента

1. В боковом меню выберите пункт **Инциденты** -> **Список**.
2. Нажмите на инцидент в списке.

   Откроется окно изменения инцидента.
3. Нажмите на кнопку **Установить метки**  .

   Откроется диалоговое окно со список меток.
4. Установите флажок рядом с нужными метками.
5. Закройте диалоговое окно нажатием на любую часть рабочей области.
6. Чтобы добавить или удалить метки, в окне изменения инцидента нажмите на кнопку  и установите/снимите флажки рядом с имеющимися метками.

Добавленные метки отображаются в списке инцидентов.

О полях

Вы можете добавлять поля, которые необходимо заполнить при выполнении инструкций сценария реагирования.

Добавление поля

1. В боковом меню выберите пункт **Настройки** -> **Поля**.

   Откроется окно со списком полей.
2. Нажмите на кнопку **Создать**.

   Откроется окно, в котором вы можете добавить новый скрипт.
3. В поле **Имя** введите название поля.
4. В поле **Описание** добавьте подробную информацию о поле.
5. В поле **Ключ** укажите значение, которое будет использовано при формировании запросов.
6. В раскрывающемся списке **Тип** выберите один из доступных форматов полей.
7. Вы можете указать текстовый (**Строка**) или числовой (**Число**) формат.

Поля, имеющиеся в базе данных, становятся доступны при создании сценария реагирования.

О скриптах

Вы можете добавлять скрипты, которые будут автоматически выполняться при решении инцидентов. InfoWatch DAT позволяет выполнять скрипты, написанные на JavaScript, Python, Bash, PowerShell.

Добавление скрипта

1. В боковом меню выберите пункт **Настройки** -> **Скрипты**.

   Откроется окно со списком скриптов.
2. Нажмите на кнопку **Создать**.

Откроется окно, в котором вы можете добавить новый скрипт.

3. Выполните следующие действия:
4. В поле **Имя** укажите название скрипта.
5. В поле **Описание** добавьте подробную информацию о скрипте.
6. В раскрывающемся списке **Язык скрипта** выберите синтаксис кода скрипта.
7. В раскрывающемся списке **Применяется** для выберите объект, при появлении которого применяется скрипт.

   Вы можете добавить скрипты для следующих объектов: пользователь, компьютер, группа, файл или событие.
8. В поле **Содержание** добавьте код скрипта.

ОБЪЕКТЫ

InfoWatch DAT позволяет анализировать данные о пользователях, файлах компьютерах и событиях в корпоративной сети.

Сбор данных с помощью скриптов

Данные, которые требуется загрузить в базу данных InfoWatch DAT для дальнейшего анализа, могут быть загружены в виде файлов JSON или в виде файлов журналов в формате EVTX.

Добавление файлов JSON или EVTX в базу данных

1. В боковом меню выберите пункт **Данные** -> **Загрузка**.
2. Выполните одно из следующих действий:
   - Перетащите файл с данными в поле **Загрузить файлы с данными**.
   - Нажмите на кнопку **Загрузить** и выберите нужный файл.

   Данные будут загружены в базу данных InfoWatch DAT.

Для сбора данных требуется использовать скрипты Microsoft PowerShell, предоставляемые с продуктом InfoWatch DAT.

> **Внимание!** Рекомендуется включить аудит файловой системы и событий на компьютерах корпоративной сети для дальнейшей интеграции с SIEM-системами.

Настройка сбора данных по расписанию с помощью Планировщика заданий

Вы можете настроить расписание сбора данных с помощью скриптов и выполнять эту операцию автоматически. Для этого необходимо настроить запуск скриптов по расписанию с помощью Планировщика задач, встроенного в операционные системы Windows.

Настройка запуска скриптов для сбора данных по расписанию

1. Запустите планировщик задач одним из следующих способов:
   - Откройте системное меню **Средства администрирования** -> **Планировщик задач**.
   - Нажмите сочетание клавиш Windows + R и введите в открывшемся диалоговом окне Выполнить команду taskschd.msc.
2. В меню **Действия** выберите пункт Создать задачу.
3. На закладке **Общие** выполните следующие действия:

- В поле **Имя** укажите название задачи.
- В поле **Описание** добавьте описание задачи.
- В поле **При выполнении задачи использовать следующую учетную запись пользователя** укажите пользователя, от чьего имени будет запускаться задача.
- Укажите, будет ли задача выполняться для всех пользователей или только для тех, кто вошел в систему.
- Установите флажок **Выполнить с наивысшими правами** при необходимости повышения привилегий для выполнения задачи.

4. На закладке Триггеры нажмите на кнопку **Создать** и в открывшемся окне выполните следующие действия:
   - В раскрывающемся списке **Начать задачу** выберите пункт По расписанию.
   - В поле **Старт** укажите дату и время начала выполнения задачи.
   - В блоке **Параметры** выберите режим запуска задачи.
   - При необходимости настройте дополнительные условия запуска задачи в блоке Дополнительные параметры. Вы можете задать произвольную задержку выполнения задачи, временные рамки для повтора задачи, срок действия задачи.
5. На закладке Действия выполните следующие действия:
   - В раскрывающемся списке **Действие** выберите пункт Запуск программы.
   - В поле **Программа** или сценарий укажите значение powershell.exe.
   - В поле **Добавить аргументы** перечислите дополнительные параметры выполнения скрипта.

Дополнительные параметры	
-File	Расположение файла скрипта.
-Command	Запуск исполняемого файла.
-ExecutionPolicy	Политика выполнения скриптов для текущего сеанса. Может принимать значения Unrestricted, RemoteSigned, AllSigned и Restricted.
-WindowStyle	Запуск PowerShell в скрытом режиме.
-NonInteractive	Отключение вывода интерактивных запросов к пользователю.
-NoProfile	Запрет на загрузку профилей. Может быть использован для ускорения выполнения скрипта.

6. Подтвердите создание задачи, нажав на кнопку **OK** в окне Создание задачи.

Экспорт пользователей, групп пользователей и компьютеров из Active Directory

Требования для использования:

- Windows 7 или более поздние версии.
- Windows Server 2012 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.
- Remote Server Administration Tools для соответствующей версии ОС.

> **Внимание!** Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1.

Пример запуска команды:

```
powershell.exe -ExecutionPolicy Bypass -Command "./export-ad.ps1" -base DC=acme``,DC=local -server dc.acme.local -outfilename export-ad
```

Параметры		
Название параметра	**Обязателен**	**Назначение**
base	Да	Корневое подразделение (Organizational unit) в Active Directory, из которого будут экспортированы данные о пользователях, группах и компьютерах.
server	Да	Имя контроллера домена.
user	Нет	Пользователь, от чьего имени выполняется запрос.
pwd	Нет	Пароль пользователя, от чьего имени выполняется запрос.
outfilename	Да	Файл, в который будут записаны полученные данные.
dat_url	Да	Адрес сервера InfoWatch DAT, на который будет отправлена информация. Необходимо указать URL-адрес, например, http://10.0.0.10:8000.
dat_user	Да	Пользователь InfoWatch DAT, от чьего имени выполняется операция.
dat_pwd	Да	Пароль пользователя InfoWatch

		DAT.

Если параметр user не задан, после запуска команды появится окно с запросом учетных данных для доступа к контроллеру домена. Для корректной работы команды пользователь, чьи учетные данные используются при выполнении запроса, должен иметь права на чтение данных из Active Directory.

Сбор данных о файлах в папке

Требования для использования:

- Windows 7 или более поздние версии.
- Windows Server 2012 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.
- Remote Server Administration Tools для соответствующей версии ОС.
- Для индексирования файлов Microsoft Office и файлов в формате PDF необходимо установить на рабочие станции следующие пакеты:
  - Пакеты Filter Packs для Microsoft Office 2010
    Дополнительная информация: https://www.microsoft.com/en-ie/download/details.aspx?id=17062
  - PDF iFilter 64 11.0.01
    Дополнительная информация:
    https://supportdownloads.adobe.com/detail.jsp?ftpID=5542

> **Внимание!** Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1.

Пример запуска команды без выделения текста:

```
powershell.exe -ExecutionPolicy Bypass -Command "./explore-folder.ps1" -folder "c:\\work\test" -outfilename folder_test
```

Пример запуска команды с выделением текста:

```
powershell.exe -ExecutionPolicy Bypass -Command "./explore-folder.ps1" -folder "c:\\work\\test" -outfilename folder_test -extract
```

Пример запуска команды для сбора данных обо всех папках общего доступа с компьютеров, зарегистрированных в указанном подразделении (OU) без выделения текста:

```
powershell.exe -ExecutionPolicy Bypass -Command "./explore-folder.ps1" -base DC=acme``,DC=local -server dc.acme.local -outfilename folder_test
```

Параметры		
Название параметра	**Обязателен**	**Назначение**
folder	Нет	Локальная или сетевая папка для сбора данных.
base	Нет	Корневое подразделение (Organizational unit) в Active Directory для получения списка компьютеров, с которых будут собраны файлы.
server	Нет	Имя контроллера домена для получения списка компьютеров Active Directory, с которых будут собраны файлы.
user	Нет	Пользователь, от чьего имени выполняется запрос.
pwd	Нет	Пароль пользователя, от чьего имени выполняется запрос.
outfilename	Да	Файл, в который будут записаны полученные данные.
extract	Нет	Извлечение текста из файлов DOC, DOCX, XLS, XSLX.
compliance	Нет	Проверка текста на соответствие стандартам.
no_hash	Нет	Запрет на вычисление хэша файлов.
dat_url	Да	Адрес сервера InfoWatch DAT, на который будет отправлена информация. Необходимо указать URL-адрес, например, http://10.0.0.10:8000.
dat_user	Да	Пользователя InfoWatch DAT, от чьего имени выполняется операция.
dat_pwd	Да	Пароль пользователя InfoWatch DAT.
start	Нет	Временная точка, начиная с которой собирается информация об изменениях файлов. Формат: yyyyMMddHHmmss.
startfn	Нет	Файл, в который будет записана метка времени.

Если параметр user не задан, после запуска команды появится окно с запросом учетных данных для доступа к контроллеру домена. Для корректной работы команды пользова-

тель, чьи учетные данные используются при выполнении запроса, должен иметь права на чтение инспектируемых файлов и папок и на чтение данных из Active Directory.

Мониторинг папки с файлами журнала событий Windows (Event Log) на удаленных рабочих компьютерах

Функциональность

С помощью этого скрипта вы можете настроить автоматический мониторинг папки с файлами журнала событий Windows (Event Log) и передачу собранных данных по протоколу HTTP/HTTPS в базу данных InfoWatch DAT для анализа.

Требования для использования:

- Windows 7 x64 или более поздние версии.
- Windows Server 2012 x64 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.

> **Внимание!** Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1.

Пример запуска с передачей данных по протоколу HTTP:

```
powershell.exe -ExecutionPolicy Bypass -Command "./folder-evtx-monitor.ps1"
-dat_url "http://10.0.0.10:8000" -dat_user admin -dat_pwd admin
```

Параметры	
Название параметра	**Назначение**
folder	Имя папки с файлами журнала событий Windows. По-умолчанию C:\Windows\System32\winevt\Logs.
dat_url	Адрес сервера, на который будет отправлена информация. Необходимо указать URL-адрес, например, http://10.0.0.10:8000.
dat_user	Пользователь, от чьего имени выполняется операция.
dat_pwd	Пароль пользователя.

Мониторинг файлов в заданной папке

Функциональность

С помощью этого скрипта вы можете настроить автоматический мониторинг файлов в выбранной папке. Агент будет отслеживать изменения файлов и отправлять информацию об этих событиях по протоколу HTTP/HTTPS в базу данных InfoWatch DAT для анализа.

Требования для использования:

- Windows 7 x64 или более поздние версии.
- Windows Server 2012 x64 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.

> **Внимание!** Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1.

Пример запуска с передачей данных по протоколу HTTP:

```
powershell.exe -ExecutionPolicy Bypass -Command "./folder-monitor.ps1" -folder c:\work -dat_url "http://10.0.0.10:8000" -dat_user admin -dat_pwd admin
```

Параметры	
Название параметра	**Назначение**
folder	Имя папки.
no_hash	Запрет на вычисление хэша файлов.
extract	Извлечение текста из файлов DOC, DOCX, XLS, XSLX.
dat_url	Адрес сервера, на который будет отправлена информация. Необходимо указать URL-адрес, например, http://10.0.0.10:8000.
dat_user	Пользователь, от чьего имени выполняется операция.
dat_pwd	Пароль пользователя.

Мониторинг действий пользователя

Функциональность

С помощью этого скрипта вы можете настроить автоматическую съемку снимков экрана, определение смены активного окна или его заголовка, журналирование клавиатурного ввода. Агент будет отправлять данные об этих событиях по протоколу HTTP/HTTPS в базу данных InfoWatch DAT для анализа.

Требования для использования:

- Windows 7 x64 или более поздние версии.
- Windows Server 2012 x64 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.

> **Внимание!** Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1.

Пример запуска с передачей данных по протоколу HTTP:

```
powershell.exe -ExecutionPolicy Bypass -Command "./user-agent.ps1" -dat_url "http://10.0.0.10:8000" -dat_user admin -dat_pwd admin
```

Параметры	
Название параметра	**Назначение**
dat_url	Адрес сервера, на который будет отправлена информация. Необходимо указать URL-адрес, например, http://10.0.0.10:8000.
dat_user	Пользователь, от чьего имени выполняется операция.
dat_pwd	Пароль пользователя.

Мониторинг изменения параметров пользователей, групп и компьютеров из Active Directory

Требования для использования:

- Windows 7 x64 или более поздние версии.
- Windows Server 2012 x64 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.
- Remote Server Administration Tools для соответствующей версии ОС.

> **Внимание!** Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1.

Пример запуска скрипта:

```
powershell.exe -ExecutionPolicy Bypass -Command "./ad-monitor.ps1" -base DC=acme``,DC=local -server dc.acme.local
```

Параметры		
Название параметра	**Обязателен**	**Назначение**
base	Да	Корневое подразделение (OU) для экспорта.
server	Да	Имя контроллера домена.
user	Нет	Пользователь, от чьего имени выполняется запрос.
pwd	Нет	Пароль пользователя, от чьего имени выполняется запрос.
start	Да	Время, начиная с которого отслеживаются изменения.
startfn	Нет	Файл, в который будет записана метка времени.
outfilename	Нет	Имя файла, в который записываются результаты выполнения скрипта. Если параметр не задан, то изменения параметров в файл не записываются.
dat_url	Да	Адрес сервера InfoWatch DAT, на который будет отправлена информация. Необходимо указать URL-адрес, например, http://10.0.0.10:8000.

dat_user	Да	Пользователь InfoWatch DAT, от чьего имени выполняется операция.
dat_pwd	Да	Пароль пользователя InfoWatch DAT.

Если параметр user не задан, после запуска команды появится окно с запросом учетных данных для доступа к контроллеру домена. Для корректной работы команды пользователь, чьи учетные данные используются при выполнении запроса, должен иметь права на чтение данных из Active Directory.

Сбор событий из журналов событий Windows (Event Log) с удаленных рабочих компьютеров

Требования для использования:

- Windows 7 или более поздние версии.
- Windows Server 2012 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.
- Remote Server Administration Tools для соответствующей версии ОС.

> **Внимание!** Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1.

Пример запуска команды для сбора всех типов событий с компьютера dc.acme.local:

```
powershell.exe –ExecutionPolicy Bypass -Command "./export-events.ps1" -Computers dc.acme.local
```

Пример запуска команды для сбора событий типа Logon с компьютера dc.acme.local:

```
powershell.exe -ExecutionPolicy Bypass -Command "./export-events.ps1" -Computers dc.acme.local –Target Logon
```

Параметры		
Название параметра	**Обязателен**	**Назначение**
computers	Да	Список компьютеров, с которых будут собраны записи журналов событий.
target	Да	Типы собираемых событий.

outfilename	Нет	Файл, в который будут записаны полученные данные.
user	Нет	Пользователь, от чьего имени выполняется запрос.
pwd	Нет	Пароль пользователя, от чьего имени выполняется запрос.
fwd	Нет	Имя журнала, использованного при форвардинге.
dat_url	Да	Адрес сервера InfoWatch DAT, на который будет отправлена информация. Необходимо указать URL-адрес, например, http://10.0.0.10:8000.
dat_user	Да	Пользователь InfoWatch DAT, от чьего имени выполняется операция.
dat_pwd	Да	Пароль пользователя InfoWatch DAT.
start	Нет	Временная точка, начиная с которой собираются события. Формат: yyyyMMddHHmmss
startfn	Нет	Файл, в который будет записана метка времени.
count	Да	Количество собираемых событий. По умолчанию собирается 3000 событий.

Типы событий	
Название параметра	**Тип**
All	Все возможные типы событий.
Logon	События, возникающие при попытке аутентификации.
Service	События, возникающие при управлении службами.
User	События, возникающие при управлении учетными данными пользователей.
Computer	События, возникающие при управлении учетными данными компьютеров.

Clean	События, возникающие при очистке журналов.
File	События, возникающие при обращении пользователей к файлам.
MSSQL	События, возникающие при работе Microsoft SQL Server.
RAS	События, возникающие при удаленном подключении пользователей.
USB	События, возникающие при работе с USB-устройствами.
Sysmon	События, возникающие при функционировании System Monitor.
TS	События, возникающие при работе Windows Terminal Services.

Если параметр user не задан, после запуска команды появится окно с запросом учетных данных для доступа к контроллеру домена. Для корректной работы команды пользователь, чьи учетные данные используются при выполнении запроса, должен иметь права чтения журналов событий Event Log.

Экспорт списка почтовых ящиков из Microsoft Exchange

Требования для использования:

Запуск команды следует осуществлять из Windows PowerShell ISE с включенным Exchange Management Shell.

Пример запуска команды для экспорта списка почтовых ящиков:

```
"./export_mb_folders.ps1" -outfile mailboxes
```

Параметры		
Название параметра	**Обязателен**	**Назначение**
outfile	Да	Файл, в который будут записаны полученные данные.

Мониторинг почтового трафика Microsoft Exchange

Требования для использования:

- Exchange Management Shell
- Microsoft Exchange Web Services Managed API

- Для проверки тела и темы сообщений на соответствие стандартам необходимо установить на рабочие станции следующие пакеты:
  - Пакеты Filter Packs для Microsoft Office 2010

    Дополнительная информация: https://www.microsoft.com/en-ie/download/details.aspx?id=17062
  - PDF iFilter 64 11.0.01

    Дополнительная информация: https://supportdownloads.adobe.com/detail.jsp?ftpID=5542

Запуск команды следует осуществлять из Windows PowerShell ISE с включенным Exchange Management Shell.

Пример запуска команды для экспорта почтовых сообщений:

```
./export-exchange-messages.ps1 -outfilename export-exchange-messages
```

Параметры		
Название параметра	**Обязателен**	**Назначение**
outfilename	Да	Файл, в который будут записаны полученные данные
user	Да	Пользователь, от чьего имени выполняется запрос.
domain	Да	Домен пользователя, от чьего имени выполняется запрос.
pwd	Да	Пароль пользователя, от чьего имени выполняется запрос.
save_body	Нет	Сохранение тела почтового сообщения.
compliance	Нет	Проверка текста на соответствие стандартам.
start	Нет	Временная точка, начиная с которой собирается информация об изменениях объектов. Формат: yyyyMMddHHmmss.
startfn	Нет	Файл, в который будет записана метка времени.
dat_url	Да	Адрес сервера InfoWatch DAT, на который будет отправлена информация. Необходимо указать URL-адрес, например, http://10.0.0.10:8000.
dat_user	Да	Пользователь InfoWatch DAT, от

		чьего имени выполняется операция.
dat_pwd	Да	Пароль пользователя InfoWatch DAT.

Экспорт записей в журналах отслеживания сообщений Microsoft Exchange

Требования для использования:

Запуск команды следует осуществлять из Windows PowerShell ISE с включенным Exchange Management Shell.

Пример запуска команды для экспорта записей в журналах отслеживания сообщений:

```
./export-message-tracks.ps1 -outfilename mamessage-tracks
```

Параметры		
Название параметра	**Обязателен**	**Назначение**
outfilename	Да	Файл, в который будут записаны полученные данные
start	Нет	Временная точка, начиная с которой собирается информация о последнем прохождении аудита. Формат: yyyyMMddHHmmss.
startfn	Нет	Файл, в который будет записана метка времени.
dat_url	Да	Адрес сервера InfoWatch DAT, на который будет отправлена информация. Необходимо указать URL-адрес, например, http://10.0.0.10:8000.
dat_user	Да	Пользователь InfoWatch DAT, от чьего имени выполняется операция.
dat_pwd	Да	Пароль пользователя InfoWatch DAT.

Экспорт событий из базы данных RusGuard

Требования для использования:

- Windows 7 или более поздние версии.
- Windows Server 2012 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.

> **Внимание!** Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1.

Пример запуска для сохранения данных в файл:

```
powershell.exe -ExecutionPolicy Bypass -Command "./mssql-rusguard.ps1" -outfilename rusguard
```

Пример запуска с передачей данных на сервер InfoWatch DAT:

```
powershell.exe -ExecutionPolicy Bypass -Command "./mssql-rusguard.ps1" -dat_url http://192.168.0.77:8000
```

Параметры		
Название параметра	**Обязателен**	**Назначение**
connection	Да	Строка с информацией для соединения с базой данных. Например, server=localhost;user id=sa;password=pwd
outfilename	Да	Файл, в который будут записаны полученные данные
start	Нет	Временная точка, начиная с которой собирается информация о последнем прохождении аудита. Формат: yyyyMMddHHmmss.
startfn	Нет	Файл, в который будет записана метка времени.
dat_url	Да	Адрес сервера InfoWatch DAT, на который будет отправлена информация.

		Необходимо указать URL-адрес, например, http://10.0.0.10:8000.
dat_user	Да	Пользователь InfoWatch DAT, от чьего имени выполняется операция.
dat_pwd	Да	Пароль пользователя InfoWatch DAT.

Сбор информации о папках с помощью InfoWatch DAT -агента

Требования для использования:

- Windows 7 x64 или более поздние версии.
- Windows Server 2012 x64 или более поздние версии.

> **Внимание!** Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1.

- Права на чтение файлов из инспектируемых файлов и папок

Пример запуска:

```
dat-agent.exe load_folder <folder> <output_file>
```

Пример запуска без выделения текста из папки:

```
dat-agent.exe load_folder //<folder> <output_file>
```

Пример запуска без выделения текста из папки общего доступа:

```
dat-agent.exe load_folder //server/share files.json
```

Пример запуска без выделения текста из всех папок общего доступа указанного компьютера:

```
dat-agent.exe load_folder //server files.json
```

Пример запуска без выделения текста из нескольких папок общего доступа:

```
dat-agent.exe load_folder //server/share;//server2/share files.json
```

Параметры	
Название параметра	**Назначение**

folder	Корневая папка (локальная или сетевая) или компьютер для сбора данных
output_file	Имя файла результатов (обязательно использование формата JSON).

Управление агентами сбора данных

Добавление агентов сбора данных в InfoWatch DAT

Вы можете добавить в InfoWatch DAT агентов сбора данных.

Агенты сбора данных автоматизируют процесс сбора с одного или более компьютеров в корпоративной сети. Агенты позволяют собрать данные выбранного типа (например, информацию об изменении файлов в сетевой папке или события Active Directory) и централизованно загрузить их в базу данных InfoWatch DAT.

В этом разделе вы найдете информацию о добавлении агентов в InfoWatch DAT, о создании и запуске задач для агентов.

Добавление агента сбора данных в InfoWatch DAT

1. В боковом меню выберите **Данные** -> **Агенты**.

   Откроется окно со списком агентов.

2. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.

   Откроется окно, в котором вы можете добавить информацию об агенте.

3. В раскрывающемся списке **Тип** выберите тип агента:

   - **Сервис**. При выборе этого типа агент сможет отправлять запросы на сбор данных и отслеживать прогресс выполнения запроса.
   - **Передатчик**. При выборе этого типа агент сможет только принимать данные, собранные PowerShell скриптами.

4. Вид следующего поля зависит от выбора в раскрывающемся списке тип:

   - Если вы выбрали тип **Сервис**, в поле **Доступ к агенту по URL** укажите URL сервера, на котором расположен агент. Необходимо указать IP-адрес и порт, например, http://10.0.0.10:8000.
   - Если вы выбрали тип **Передатчик**, в поле **Маска IP-адресов агентов** укажите маску IP-адресов серверов, на которых будут выполнены PowerShell скрипты.

5. В поле **Описание** добавьте краткую информацию об агенте.

6. Нажмите на кнопку **Зарегистрировать**.

   Новый агент появится в списке агентов.

Изменение информации об агенте сбора данных

1. В боковом меню выберите **Данные** -> **Агенты**.

Откроется окно со списком агентов.

2. Нажмите на кнопку  напротив агента, информацию о котором вы хотите изменить.

Удаление агента сбора данных из InfoWatch DAT

1. В боковом меню выберите **Данные** -> **Агенты**.

   Откроется окно со списком агентов.

2. Нажмите на кнопку  напротив агента, которого вы хотите удалить.

Создание и запуск задач для агентов сбора данных

Вы можете создавать задачи сбора данных, которые агенты будут выполнять при ручном запуске, по расписанию или постоянно по мере появления изменений, которые требуется зафиксировать и проанализировать.

InfoWatch DAT позволяет создать следующие типы задач сбора данных.

- Инспекция файлов
- Инспекция EVTX-файлов
- Инспекция Event Log
- Инспекция Active Directory
- Инспекция LDAP
- Инспекция Exchange

Создание задачи инспекции файлов

1. В боковом меню выберите **Данные** -> **Агенты**.

   Откроется окно со списком агентов.

2. Нажмите на агента, для которого вы хотите создать задачу.
3. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.
4. В раскрывающемся списке **Тип** выберите пункт Инспекция файлов.
5. В поле **Папка** укажите локальную или сетевую папку, которая содержит инспектируемые файлы.
6. В раскрывающемся списке режим выберите один из следующих вариантов:
   - **PowerShell** для сбора данных с помощью скриптов PowerShell.
   - **Агент** InfoWatch DAT для сбора данных с помощью агента, поставляемого с программой.
7. В поле **Имя пользователя** введите имя доменного пользователя, от имени которого будет производиться сбор данных.

   Если имя пользователя не задано, отправка данных будет произведена от имени пользователя, запустившего агента.

8. В поле **Пароль** введите пароль доменного пользователя.

9. В раскрывающемся списке Тип сбора данных выберите один из следующих вариантов:
    - **Вручную**. Задача не будет выполняться в автоматическом режиме.
    - **Через заданный интервал времени**. Задача будет выполняться в автоматическом режиме по истечению заданного промежутка времени. При выборе этого варианта в появившемся поле **Период, мин** необходимо указать интервал, через который будет выполняться задача.
    - **Постоянная работа и загрузка изменений**. Задача выполняется постоянно все время жизни агента, отслеживая изменения в инспектируемой папке или Active Directory.
10. Нажмите на кнопку **Создать**.

Создание задачи инспекции EVTX-файлов

1. В боковом меню выберите **Данные** -> **Агенты**.

   Откроется окно со списком агентов.
2. Нажмите на агента, для которого вы хотите создать задачу.
3. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.
4. В раскрывающемся списке **Тип** выберите пункт **Инспекция EVTX-файлов**.
5. В поле **Папка** укажите локальную или сетевую папку, которая содержит инспектируемые файлы.
6. В раскрывающемся списке режим выберите один из следующих вариантов:
    - **PowerShell** для сбора данных с помощью скриптов PowerShell.
    - **Агент** InfoWatch DAT для сбора данных с помощью агента, поставляемого с программой.
7. В поле **Имя пользователя** введите имя доменного пользователя, от имени которого будет производиться сбор данных.

   Если имя пользователя не задано, отправка данных будет произведена от имени пользователя, запустившего агента.
8. В поле **Пароль** введите пароль доменного пользователя.
9. В раскрывающемся списке Тип сбора данных выберите один из следующих вариантов:
    - **Вручную**. Задача не будет выполняться в автоматическом режиме.
    - **Через заданный интервал времени**. Задача будет выполняться в автоматическом режиме по истечению заданного промежутка времени. При выборе этого варианта в появившемся поле Период, мин необходимо указать интервал, через который будет выполняться задача.
    - **Постоянная работа и загрузка изменений**. Задача выполняется постоянно все время жизни агента, отслеживая изменения в инспектируемой папке или в Active Directory.
10. Нажмите на кнопку **Создать**.

Создание задачи инспекции Event Log

1. В боковом меню выберите **Данные** -> **Агенты**.

   Откроется окно со списком агентов.

2. Нажмите на агента, для которого вы хотите создать задачу.
3. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.
4. В раскрывающемся списке **Тип** выберите пункт **Инспекция Event Log**.
5. В поле **Адрес компьютера** укажите адрес компьютера, из Event Log которого будет собрана информация.
6. В раскрывающемся списке режим выберите один из следующих вариантов:
   - **PowerShell** для сбора данных с помощью скриптов PowerShell.
   - **Агент** InfoWatch DAT для сбора данных с помощью агента, поставляемого с программой.
7. В поле **Имя пользователя** введите имя доменного пользователя, от имени которого будет производиться сбор данных.

   Если имя пользователя не задано, отправка данных будет произведена от имени пользователя, запустившего агента.

8. В поле **Пароль** введите пароль доменного пользователя.
9. В раскрывающемся списке **Тип сбора данных** выберите один из следующих вариантов:
   - **Вручную**. Задача не будет выполняться в автоматическом режиме.
   - **Через заданный интервал времени**. Задача будет выполняться в автоматическом режиме по истечению заданного промежутка времени. При выборе этого варианта в появившемся поле Период, мин необходимо указать интервал, через который будет выполняться задача.
   - **Постоянная работа и загрузка изменений**. Задача выполняется постоянно все время жизни агента, отслеживая изменения в инспектируемой папке или в Active Directory.
10. Нажмите на кнопку **Создать**.

Создание задачи Инспекция Active Directory

1. В боковом меню выберите **Данные** -> **Агенты**.

   Откроется окно со списком агентов.

2. Нажмите на агента, для которого вы хотите создать задачу.
3. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.
4. В раскрывающемся списке **Тип** выберите пункт **Инспекция Active Directory**.
5. В поле **Контроллер домена** введите имя или IP-адрес контроллера домена. Информация о событиях в Active Directory с этого контроллера будет отправляться в базу данных InfoWatch DAT.
6. В поле **Корневая организационная единица** введите имя корневого подразделения LDAP, для которого собираются данные.

7. В раскрывающемся списке режим выберите один из следующих вариантов:
    - **PowerShell** для сбора данных с помощью скриптов PowerShell.
    - **Агент** InfoWatch DAT для сбора данных с помощью агента, поставляемого с программой.
8. В поле **Имя пользователя** введите имя доменного пользователя, от имени которого будет производиться сбор данных.

    Если имя пользователя не задано, отправка данных будет произведена от имени пользователя, запустившего агента.
9. В поле **Пароль** введите пароль доменного пользователя.
10. В раскрывающемся списке Тип сбора данных выберите один из следующих вариантов:
    - **Вручную**. Задача не будет выполняться в автоматическом режиме.
    - **Через заданный интервал времени**. Задача будет выполняться в автоматическом режиме по истечению заданного промежутка времени. При выборе этого варианта в появившемся поле Период, мин необходимо указать интервал, через который будет выполняться задача.
    - **Постоянная работа и загрузка изменений**. Задача выполняется постоянно все время жизни агента, отслеживая изменения в инспектируемой папке или в Active Directory.
11. Нажмите на кнопку **Создать**.

Создание задачи Инспекция LDAP

1. В боковом меню выберите **Данные** -> **Агенты**.

    Откроется окно со списком агентов.
2. Нажмите на агента, для которого вы хотите создать задачу.
3. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.
4. В раскрывающемся списке **Тип** выберите пункт **Инспекция LDAP**.
5. В поле **Контроллер домена** введите имя или IP-адрес контроллера домена. Информация о событиях служб с поддержкой LDAP с этого контроллера будет отправляться в базу данных InfoWatch DAT.
6. В поле **Корневая организационная единица** введите имя корневого подразделения LDAP, для которого собираются данные.
7. В раскрывающемся списке режим выберите один из следующих вариантов:
    - **PowerShell** для сбора данных с помощью скриптов PowerShell.
    - **Агент** InfoWatch DAT для сбора данных с помощью агента, поставляемого с программой.
8. В поле **Имя пользователя** введите имя доменного пользователя, от имени которого будет производиться сбор данных.

    Если имя пользователя не задано, отправка данных будет произведена от имени пользователя, запустившего агента.
9. В поле **Пароль** введите пароль доменного пользователя.

10. В раскрывающемся списке **Тип сбора данных** выберите один из следующих вариантов:
    - **Вручную**. Задача не будет выполняться в автоматическом режиме.
    - **Через заданный интервал времени**. Задача будет выполняться в автоматическом режиме по истечению заданного промежутка времени. При выборе этого варианта в появившемся поле Период, мин необходимо указать интервал, через который будет выполняться задача.
    - **Постоянная работа и загрузка изменений**. Задача выполняется постоянно все время жизни агента, отслеживая изменения в инспектируемой папке или в Active Directory.
11. Нажмите на кнопку Создать.

Создание задачи Инспекция Exchange

1. В боковом меню выберите **Данные** -> **Агенты**.

   Откроется окно со списком агентов.
2. Нажмите на агента, для которого вы хотите создать задачу.
3. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.
4. В раскрывающемся списке **Тип** выберите пункт **Инспекция Exchange**.
5. В поле **Имя пользователя** введите имя доменного пользователя, от имени которого будет производиться сбор данных.
6. В поле **Пароль** введите пароль доменного пользователя.
7. В раскрывающемся списке Тип сбора данных выберите один из следующих вариантов:
    - **Вручную**. Задача не будет выполняться в автоматическом режиме.
    - **Через заданный интервал времени**. Задача будет выполняться в автоматическом режиме по истечению заданного промежутка времени. При выборе этого варианта в появившемся поле Период, мин необходимо указать интервал, через который будет выполняться задача.
    - **Постоянная работа и загрузка изменений**. Задача выполняется постоянно все время жизни агента, отслеживая изменения в инспектируемой папке или в Active Directory.
8. Нажмите на кнопку **Создать**.

Запуск задачи для агента сбора данных

1. В боковом меню выберите **Данные** -> **Агенты**.

   Откроется окно со списком агентов.
2. Нажмите на агента, для которого требуется запустить задачу.
3. Нажмите на кнопку  рядом с названием задачи, которую требуется запустить.

Обработка данных

Анализ пользователей

Вы можете просмотреть информацию о пользователях, собранную с помощью скрипта export-ad.ps1, выбрав пункт бокового меню Объекты > Пользователи.

В верхней части рабочей области представлена сводная информация об общем количестве пользователей, включая отключенных и неактивных, о количестве групп пользователей и возможных рисках, которые обнаружены в результате анализа.

В нижней части рабочей области представлен список пользователей в виде таблицы.

В столбцах таблицы вы можете найти следующую информацию:

- **Аватар** – фотография пользователя.
- **Имя** – идентификатор пользователя в домене.
- **Домен** – название домена, с которого получена информация о пользователе.
- **E-Mail** – почтовый адрес пользователя.

  Риск-фактор – информация о потенциальных рисках, которые InfoWatch DAT обнаружила при анализе пользователя.

  В этом столбце может появиться следующая информация:

  - Пользователь с паролем, у которого нет срока истечения.
  - Пользователь без пароля.
  - Пользователь, у которого истек срок действия пароля, но пароль не был изменен.
  - Пользователь, который не выполнял авторизацию в домене в течение двух месяцев.
  - Пользователь, который не изменял пароль в течение 40 дней.
  - Пользователь, который не изменял пароль в течение 60 дней.
  - Пользователь без Kerberos-авторизации.
  - Пользователь, который был импортирован из другого домена.
  - Пустая группа пользователей и компьютеров.
- **Метки** – текстово-графические метки, установленные для объекта.
- **Телефон** – контактный номер телефона.
- **Аккаунт** – имя пользователя учетной записи, которое закреплено за пользователем в домене.
- **Принципал** – уникальное имя пользователя для аутентификации в домене.
- **NT-имя** – имя пользователя в NT-домене.
- **Последний логон** – время последнего входа пользователя в учетную запись.
- **Количество входов** – сколько раз пользователь входил в учетную запись.
- **Время создания** – время создания пользователя в домене.
- **Время последнего изменения** – время последнего изменения данных пользователя в домене.
- **Пароль действителен до** – дата истечения срока действия пароля.
- **Неверный пароль введен** – время последней попытки ввести неверный пароль.

- **Количество ввода неверного пароля** – количество попыток ввести пароль для авторизации на домене, закончившихся неудачей.
- **Количество элементов** – количество пользователей в группе.

Вы можете открыть меню пользователя, чтобы посмотреть информацию о файлах, которые ему доступны, выполнить какое-либо действие с помощью предустановленных скриптов или экспортировать данные о пользователе.

Переход в дополнительное меню пользователя или группы пользователей

1. В боковом меню выберите пункт **Объекты** -> **Пользователи**.

   Откроется список пользователей и групп пользователей, полученных с помощью скриптов сбора данных.

2. Двойным щелчком по имени пользователя откройте меню пользователя.
3. При необходимости выполните следующие действия:
   - На закладке **Файлы** просмотрите список файлов, к которым у пользователя есть доступ. Список представлен в виде таблицы со следующими данными:
     - **Каталог** – папка, в которой расположен файл.
     - **Имя** – имя файла.
     - **Чтение** – маркер, показывающий, доступен ли файл пользователю в режиме чтения.
     - **Запись** – маркер, показывающий, доступен ли файл пользователю в режиме записи.
   - На закладке **Скрипты** выберите один из предустановленных скриптов (например, вы можете инициировать смену пароля на компьютере пользователя).

   Если вы открываете меню группы пользователей, вы также можете посмотреть список пользователей, которые состоят в группе на закладке **Состав группы**.

Статистика по пользователям

Вы можете просмотреть сводную статистику по данным пользователей и групп, собранным с помощью скрипта export-ad.ps1, в виде диаграмм и графиков.

Просмотр сводной статистики пользователей и групп

1. В боковом меню выберите пункт **Объекты** -> **Пользователи**.
2. В правом верхнем углу рабочей области нажмите на кнопку **Статистика**.

   Откроется окно **Статистика по пользователям**.

В окне **Статистика по пользователям** доступна следующая информация:

- Статистика по пользователям – линейная диаграмма процентного соотношения пользователей по риск-факторам и другим параметрам (например, соотношение заблокированных и активных пользователей).

- График статистики по последнему входу пользователей на инспектируемые рабочие станции, по показателям количество пользователей (ось y) и временной интервал (ось x).
- Диаграмма по меткам, установленным на записи о пользователях.
- Столбчатая диаграмма, показывающая количество пользователей, зарегистрированных в различных доменах.
- Круговая диаграмма, показывающая количество рисков, обнаруженных при анализе пользователей.
- Таблица по аномальным скачкам количества событий, произошедших в течение часа. В таблице вы можете найти следующую информацию:
    - **Время** – дата и время, начиная с которого был зафиксировано аномальное количество событий.
    - **Кто** – количество профилей пользователей, на которых были зафиксировано аномальное количество событий за часовой период.
    - **Количество** – общее и среднее количество событий, зафиксированных за часовой период.

Анализ компьютеров

Вы можете просмотреть информацию о компьютерах, собранную с помощью скрипта export-ad.ps1, выбрав пункт бокового меню **Объекты** -> **Компьютеры**.

В верхней части рабочей области представлена сводная информация об общем количестве компьютеров, включая отключенные и неактивные, о количестве групп компьютеров и возможных рисках, которые обнаружены в результате анализа.

В нижней части рабочей области представлен список компьютеров в виде таблицы.

В столбцах таблицы вы можете найти следующую информацию:

- **Домен** – название домена, к которому принадлежит компьютер.
- **Имя** – имя компьютера в домене.
- **Операционная система** – операционная система, установленная на компьютере.
- **Версия ОС** – версия операционной системы, установленной на компьютере.
- **Риск-фактор** - информация о потенциальных рисках, которые InfoWatch DAT обнаружила при анализе компьютера.

  В этом столбце может появиться следующая информация:

    - На компьютере установлена устаревшая операционная система, подвергающая риску остальные компьютеры корпоративной сети (например, компьютер с ОС Windows XP, Windows Server 2003).
    - На компьютере ни разу не вводился пароль.
    - Пустая группа компьютеров.
    - Домен не содержит группы Power Users.
- **Метки** – текстово-графические метки, установленные для объекта.
- **Аккаунт** – учетная запись компьютера,
- **Количество общих файлов** – количество файлов, к которым разрешен сетевой доступ.
- **Размер общих файлов** – общий размер всех файлов, к которым разрешен сетевой доступ.

- **Количество входов** – количество входов в учетные записи компьютера.
- **Количество вводов неверного пароля** – количество попыток ввести неверный пароль при входе в учетные записи компьютера.
- **Время создания** – дата и время регистрации компьютера в домене или создания группы.
- **Время последнего изменения** – дата и время последнего изменения данных компьютера или группы.
- **Количество приложений** – количество приложений, установленных на компьютере пользователя.
- **Количество лицензий** – количество программ с лицензией.
- **Количество профилей** – количество профилей пользователя на компьютере.
- **Количество элементов** – количество компьютеров в группе.

Вы можете открыть меню компьютера, чтобы посмотреть информацию о папках общего доступа, выполнить предустановленные скрипты, посмотреть подробную информацию о лицензиях, приложениях или профилях.

Переход в дополнительное меню компьютера или группы компьютеров

1. В боковом меню выберите пункт **Объекты** -> **Компьютеры**.

   Откроется список компьютеров и групп компьютеров, полученных с помощью скрипта сбора данных.

2. Двойным щелчком по названию компьютера откройте меню компьютера.
3. При необходимости выполните следующие действия:
   - На закладке **Папки общего доступа** просмотрите список папок общего доступа, которые есть на компьютере.
   - На закладке **Скрипты** выберите один из предустановленных скриптов (например, вы можете перезагрузить компьютер).
   - На закладке **Лицензии** просмотрите подробную информацию о лицензиях, обнаруженных с помощью скрипта сбора данных о компьютере.
   - На закладке **Профили** просмотрите информацию о пользователях и корневых папках, существующих на компьютере.

   Если вы открываете меню группы компьютеров, вы также можете просмотреть список компьютеров, которые входят в группу на закладке **Состав группы**.

Вы также можете подключиться к компьютеру через службу Подключение к удаленному рабочему столу.

Подключение к компьютеру через службу Подключение к удаленному рабочему столу

1. В боковом меню выберите пункт **Объекты** -> **Компьютеры**.

   Откроется список компьютеров и групп компьютеров, полученных с помощью скрипта сбора данных.

2. Двойным щелчком по названию компьютера откройте меню компьютера.

3. Нажмите на кнопку **Соединиться по RDP**.

Статистика по компьютерам

Вы можете просмотреть сводную статистику по данным компьютеров, собранным с помощью скрипта export-ad.ps1, в виде диаграмм.

Просмотр сводной статистики компьютеров

1. В боковом меню выберите пункт **Объекты** -> **Компьютеры**.
2. В правом верхнем углу рабочей области нажмите на кнопку **Статистика**.

   Откроется окно **Статистика по компьютерам**.

В окне **Статистика по компьютерам** доступна следующая информация:

- Столбчатая диаграмма, показывающая соотношение операционных систем, установленных на компьютерах в корпоративной сети.
- Столбчатая диаграмма, показывающая соотношение количества событий на компьютерах в корпоративной сети.

Анализ файлов

Вы можете просмотреть информацию о файлах, собранную с помощью скрипта explore-folder.ps1, выбрав пункт бокового меню **Объекты** -> **Файлы**.

В верхней части рабочей области представлена сводная информация об общем количестве и размере файлов, о количестве файлов дубликатов и информация о файлах, регулируемых стандартом.

В нижней части рабочей области представлен список файлов в виде таблицы.

В столбцах таблицы вы можете найти следующую информацию:

- **Тип** – тип файла.
- **Компьютер** – компьютер, на котором расположен файл.
- **Каталог** – папка, в которой расположен файл.
- **Имя** – имя файла.
- **Время изменения** – время последнего изменения файла.
- **Время доступа** – время последней обращения к файлу.
- **Тип документа** – тип документа.
- **Размер** – размер файла.
- **Риск-фактор** - информация о потенциальных рисках, которые InfoWatch DAT обнаружила при анализе файла.

  В этом столбце может появиться следующая информация:

  - Файл соответствует стандарту.
  - Файл является текстовым (DOC, DOCX, XLS, XLSX, PDF и TXT).
  - В Access Control List (ACL) есть группа Everyone, Domain Users, Autentificated Users.
  - ACL содержит не наследуемые Access Control Entries (ACE).
- **Метки** – текстово-графические метки, установленные для объекта.

- **Регулируется стандартом** – информация о стандартах, которым соответствует файл.

  InfoWatch DAT автоматически определяет наличие данных, регулируемых стандартами, в файлах формата DOC, DOCX, XLS, XLSX, PDF и TXT. Вы можете узнать больше о стандартах, по которым проводится исследование файла в **Приложении 1 О файловых стандартах**.
- **Доступ** – пользователи и группы, которые имеют доступ к файлу.
- **Дубликаты** – количество копий файлов.

Вы также можете просмотреть информацию о файлах и папках в режиме дерева файлов.

> **Внимание!** Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1.

Переключение списка файлов и папок в вид дерева файлов

В правом верхнем углу нажмите на кнопку  .

Для возврата в вид таблицы в правом верхнем углу нажмите

на кнопку  .

В режиме дерева файлов доступна фильтрация списка файлов и папок по текстовому содержимому столбца таблицы.

Фильтрация списка файлов в режиме дерева файлов

Начните печатать в поле **Фильтр…** над столбцом таблицы, по которому вы хотите отфильтровать файлы.

В списке файлов останутся только те результаты, которые соответствуют вашему вводу.

Вы также можете открыть меню файла или папки, чтобы просмотреть информацию о пользователях и группах, которые имеют к ним доступ, выполнить предустановленные скрипты или просмотреть содержимое файла.

Переход в дополнительное меню файла

1. В боковом меню выберите пункт **Объекты** -> **Файлы**.

   Откроется список файлов, полученных с помощью скрипта сбора данных.
2. Двойным щелчком по имени файла откройте меню файла.
3. При необходимости выполните следующие действия:
   - На закладке **Доступ** просмотрите список пользователей и групп пользователей, которые имеют доступ на чтение и запись файла.
   - На закладке **Скрипты** выберите один из предустановленных скриптов (например, удаление папки или файла).

Если вы открываете меню папки, вы также можете просмотреть файлы в этой папке на закладке **Содержание**.

Статистика по файлам

Вы можете просмотреть сводную статистику по данным о файлах, собранным с помощью скрипта explore-folder.ps1, в виде диаграмм и графиков.

Просмотр сводной статистики файлов

1. В боковом меню выберите пункт **Объекты** -> **Файлы**.
2. В правом верхнем углу рабочей области нажмите на кнопку **Статистика**.

   Откроется окно **Статистика по файлам**.

В окне **Статистика по файлам** доступна следующая информация:

- Столбчатая диаграмма, показывающее соотношение файлов по типам, а также соотношение их дубликатов.
- Столбчатая диаграмма, показывающая соотношение файлов по стандартам, которыми регулируются файлы.
- Столбчатая диаграмма, показывающее соотношение количества файлов на компьютерах корпоративной сети.
- График статистики по времени создания файлов, по показателям количество файлов (ось y) и временной интервал (ось x).
- График статистики по времени изменения файлов, по показателям количество файлов (ось y) и временной интервал (ось x).
- График статистики по времени изменения файлов, по показателям количество файлов (ось y) и временной интервал (ось x).

Анализ почтовых ящиков

Вы можете просмотреть информацию о пользователях, собранную с помощью скрипта export-mb-folders.ps1, выбрав пункт бокового меню **Объекты** -> **Почтовые ящики**.

В верхней части рабочей области представлена сводная информация об общем количестве почтовых ящиков в домене, о количестве папок, заведенных пользователя, а также информация о количестве и размере элементов в почтовых ящиках.

В нижней части рабочей области представлен список почтовых ящиков в виде таблицы.

В столбцах таблицы вы можете найти следующую информацию:

- **Имя** – имя пользователя, которое используется в почтовом адресе.
- **Alias** – имя пользователя для контроллера домена.
- **Риск-фактор** - информация о потенциальных рисках, которые InfoWatch DAT обнаружила при анализе почтового ящика.

  В этом столбце может появиться информация о том, что к почтовому ящику имеет доступ дополнительный пользователь.
- **Дружественное имя** – псевдоним пользователя.
- **Метки** – текстово-графические метки, установленные для объекта.
- **Имя сервера** – название сервера, на котором используется имя пользователя.

- **Количество папок** – количество папок в почтовом ящике.
- **Количество элементов** – количество элементов в почтовом ящике.
- **Размер** – общий размер всех элементов в почтовом ящике.

Вы можете открыть меню почтового ящика, чтобы просмотреть информацию о доступах и папках почтового ящика, а также выполнить предустановленные скрипты.

Переход в дополнительное меню почтового ящика

1. В боковом меню выберите пункт **Объекты** > **Почтовые ящики**.

   Откроется список почтовых ящиков, полученных с помощью скрипта сбора данных.

2. Двойным щелчком по имени почтового ящика откройте его меню.
3. При необходимости выполните следующие действия:
   - На закладке **Доступ** просмотрите список пользователей и групп пользователей, которые имеют доступ на чтение, запись, изменение владельца и изменение прав на доступ к почтовому ящику.
   - На закладке **Скрипты** выберите один из предустановленных скриптов (например, удаление папки).

Анализ событий

Вы можете просмотреть информацию о событиях, собранную с помощью скрипта export-events.ps1, выбрав пункт бокового меню **Объекты** > **События**.

В верхней части рабочей области представлена сводная информация об общем количестве событий.

В нижней части рабочей области представлен список файлов в виде таблицы.

В столбцах таблицы вы можете найти следующую информацию:

- **Время** – время регистрации события в журнале событий.
- **Категория** – категория события в журнале событий.
- **ID-события** – уникальный номер события.
- **Важность** – индикатор важности события.
- **Действие** – действие, которое было выполнено во время события.
- **Кто** – пользователь, который инициировал событие.
- **Что** – тип события.
- **Где** – расположение компьютера, на котором произошло событие.
- **Компьютер** – название компьютера, на котором произошло событие.
- **Пользователь** – пользователь, на чьей учетной записи произошло событие.
- **Домен** – домен, в котором произошло событие.

Вы можете открыть меню события, чтобы просмотреть подробную информацию о событии или выполнить предустановленные скрипты.

Переход в дополнительное меню события

1. В боковом меню выберите пункт **Объекты** -> **События**.

   Откроется список событий, полученных с помощью скрипта сбора данных.

2. Двойным щелчком по событию откройте меню события.
3. При необходимости выполните следующие действия:
   - На закладке **Информация** просмотрите подробную информацию о событии.
   - На закладке **Скрипты** выберите один из предустановленных скриптов.

Статистика по событиям

Вы можете просмотреть сводную статистику по данным о событиях, собранным с помощью скрипта export-events.ps1, в виде диаграмм и графиков.

Просмотр сводной статистики событий

1. В боковом меню выберите пункт **Объекты** -> **События**.
2. В правом верхнем углу рабочей области нажмите на кнопку **Статистика**.

   Откроется окно **Статистика по событиям**.

В окне **Статистика по событиям** доступна следующая информация:

- Столбчатая диаграмма, показывающая соотношение событий по типу выполненного действия.
- Круговая диаграмма распределения событий по важности.
- Столбчатая диаграмма, показывающая распределение событий по компьютерам.
- Столбчатая диаграмма, показывающая распределение событий по пользователям.
- Столбчатая диаграмма, показывающая распределение событий по контролирующим стандартам.
- График статистики по событиям на временной отрезок (день), по показателям количество событий (ось y) и дата события (ось x).
- График статистики по событиям на временной отрезок (час), по показателям количество событий (ось y), а также дата и время события (ось x).
- Таблица по аномальным скачкам количества событий, произошедших в течение часа. В таблице вы можете найти следующую информацию:
  - **Время** – дата и время, начиная с которого был зафиксировано аномальное количество событий.
  - **Количество** – общее и среднее количество событий, зафиксированных за часовой период.

О сводной статистике по рискам

В InfoWatch DAT вы можете посмотреть сводную статистику по рискам объектов в следующих категориях объектов:

- Пользователи и группы пользователей
- Компьютеры
- Файлы и папки
- Почтовые ящики
- События

Для каждой группы объектов в сводной статистике приводится значение по количеству рисков незначительного, среднего и критического приоритета, а также среднее значение в виде текстово-графического индикатора:

- Зеленый – низкий уровень риска.
- Оранжевый – средний уровень риска.
- Красный – высокий уровень риска.

Кроме того, для каждой группы перечислены некоторые числовые показатели.

Пользователи

- Количество доменов – количество доменов, к которым принадлежат пользователи, проанализированные платформой.
- Количество пользователей – количество пользователей, проанализированных платформой.
- Количество групп – количество групп пользователей, проанализированных платформой.

При наличии риск-факторов эта информация будет отображена в виде круговых диаграмм, показывающих соотношение пользователей с соответствующим риском-фактором и пользователей без риск-факторов.

Компьютеры

- Количество доменов – количество доменов, к которым принадлежат компьютеры, проанализированные платформой.
- Количество пользователей – количество профилей пользователей на компьютерах, проанализированных платформой.
- Количество групп – количество групп пользователей на компьютерах, проанализированных платформой.

При наличии риск-факторов эта информация будет отображена в виде круговых диаграмм, показывающих соотношение компьютеров с соответствующим риском-фактором и компьютеров без риск-факторов.

Файлы

- Количество файлов – количество файлов корпоративной сети, проанализированных платформой.
- Количество папок – количество папок корпоративной сети, проанализированных платформой.

При наличии файлов, не открывавшихся или не измененных в течение последних двух месяцев, а также файлов-дубликатов, эта информация будет отражена в виде круговой диаграммы, показывающей отношение таких файлов к остальным.

При наличии файлов, регулируемых стандартом, будет дополнительно указано количество таких файлов, а также будет перечислен список стандартов, которыми регулируются файлы.

Почтовые

- Количество ящиков – количество почтовых ящиков на сервере Microsoft Exchange, проанализированных платформой.
- Количество папок – количество папок в почтовых ящиках, проанализированных платформой.
- Количество писем – количество писем в почтовых ящиках, проанализированных системой.
- Общий размер ящиков – общий размер почтовых ящиков на сервере Microsoft Exchange, проанализированных системой.

О метках

Для дифференциации проанализированных объектов вы можете добавлять *метки*. Метки – это дополнительный инструмент для быстрого добавления и получения информации об объекте. Метки выглядят как разноцветные области с поясняющим текстом и отображаются в списках объектов.

Вы можете создать набор меток (например, *Проинформировать СИБ, Проинформировать генерального директора*) разных цветов.

Создание меток

1. В боковом меню выберите пункт **Настройки** -> **Метки**.

   Откроется список меток. По умолчанию список пуст.

2. Нажмите на кнопку **Создать**.

   Откроется окно, в котором вы можете добавить детали новой метки.

3. В поле **Имя** введите название новой метки.
4. В поле **Описание** добавьте информацию о метке.
5. В списке **Цвет** выберите цвет метки.
6. Нажмите на кнопку **Создать**.

   Метка будет добавлена в список меток, а также станет доступна при работе с объектами.

Вы можете добавлять метки существующим объектам.

Добавление меток для инцидента

1. В боковом меню выберите пункт **Объекты** -> **<Тип объекта>**.
2. Нажмите на объект в открывшемся списке.

   Откроется дополнительно меню объекта.

3. В правом верхнем углу рабочей области нажмите на кнопку **Меню**.

   Откроется диалоговое окно со список меток.

4. Установите флажок рядом с нужными метками.
5. Закройте диалоговое окно нажатием на любую часть рабочей области.

Добавленные метки отображаются в списке соответствующих объектов.

О фильтрации объектов

Вы можете использовать фильтры по свойствам объектов в базе данных, чтобы упростить поиск объектов, информацию о которых вы хотите просмотреть в списке объектов.

Фильтрация объектов по предустановленному условию

1. В боковом меню выберите пункт **Объекты** > **<Тип объекта>**.
2. В центральной части рабочей области нажмите на кнопку **Добавить фильтр**.
3. Выберите одно из предустановленных условий для фильтрации списка объектов.

Об экспорте объектов

Вы можете экспортировать сводную информацию о собранных объектах в файлы формата CSV.

Экспорт сводной информации об объектах

1. В боковом меню выберите пункт **Объекты** > **<Тип объекта>**.

   Откроется список объектов, полученных с помощью скриптов сбора данных.
2. В правой верхней части рабочей области нажмите на кнопку **Меню**.
3. Выберите пункт раскрывающегося списка **Экспорт в CSV**.

   Сводная информация об объекте будет экспортирована в файл CSV.

Информация об отдельных объектах может быть экспортирована в файл формата PDF.

Экспорт информации об отдельных объектах

1. В боковом меню выберите пункт **Объекты** > **<Тип объекта>**.

   Откроется список объектов, полученных с помощью скриптов сбора данных.
2. Двойным щелчком по объекту в списке откройте дополнительное меню объекта.
3. В правой верхней части рабочей области нажмите на кнопку **Меню**.
4. Выберите пункт раскрывающегося списка **Экспорт PDF**.

   Информация об объекте будет экспортирована в файл формата PDF.

УЧЕТНЫЕ ЗАПИСИ И ОПОВЕЩЕНИЯ

В веб-консоли предусмотрено автоматическое оповещение учетных записей, ответственных за решение инцидента, а также учетных записей, назначенных наблюдателями инцидентов.

Добавление учетных записей ответственных лиц в InfoWatch DAT

1. В боковом меню выберите пункт **Настройки** -> **Аккаунты**.

   Откроется список учетных записей ответственных лиц.

2. Нажмите на кнопку **Создать**.

   Откроется окно, в котором вы можете добавить новую учетную запись.

3. Выполните следующие действия:

   r. В поле **Имя** укажите имя учетной записи.

   s. В поле **Полной имя** укажите полное имя ответственного лица.

   t. В поле **Аватар** нажмите на кнопку **Выберите файл** и выберите изображение, которое будет отображаться для этой учетной записи.

   u. В поле **Описание** добавьте информацию об ответственном лице.

   v. В поле **Почта** укажите адрес электронной почты ответственного лица.

   w. В поле **Пароль** укажите пароль учетной записи.

   x. В поле **Подтвердить** укажите пароль учетной записи еще раз.

   y. Установите флажок **Права администратор**, если требуется предоставить учетной записи права администратора.

   z. Установите флажок **Права инспектора**, если требуется предоставить учетной записи права инспектора.

Учетные записи с правами администратора и инспектора могут изменять настройки платформы и добавлять объекты.

Добавление ответственного лица при создании инцидента

1. В боковом меню выберите пункт **Инциденты** -> **Список**.

   Откроется окно со списком инцидентов.

2. Нажмите на кнопку **Зарегистрировать**.

   Откроется окно создания инцидента.

3. В раскрывающемся списке **Ответственный** выберите учетную запись лица, ответственного за решение инцидента.

4. Заполните остальные поля и нажмите на кнопку **Создать**.

Лицу, назначенному ответственным за решение инцидента, будет отправлено оповещение о новом инциденте.

Добавление наблюдателя

1. В боковом меню выберите пункт **Инциденты** -> **Список**.

   Откроется окно со списком инцидентов.

2. Нажмите на инцидент в списке.

   Откроется окно создания инцидента.

3. В раскрывающемся списке **Наблюдатели не установлены** выберите учетную запись, которая будет наблюдателем.

Лицу, назначенному наблюдателем инцидента, будет отправлено оповещение о новом инциденте.

ОПОВЕЩЕНИЯ

Если у вас есть необходимость отслеживать ситуации, в которых определенные объекты подвергают корпоративную сеть риску заражения вирусами, утечки конфиденциальных данных и другим рискам, вы можете настроить оповещения о таких ситуациях.

Создание и настройка правил оповещений о рисках

1. В боковом меню выберите **Настройки** > **Объекты** > **Оповещения**.
2. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.
3. Откроется окно, в котором вы сможете добавить детальную информацию о риске и задать условия появления оповещения.
4. В поле **Имя** введите имя риска, оповещения о котором вы хотите получать.
5. В поле **Описание** введите краткую информацию о риске.
6. В поле **Риск** укажите произвольный числовой идентификатор риска.
7. Нажмите на кнопку **Добавить условие**, чтобы добавить строку в таблице со списком условий.
8. В раскрывающемся списке столбца **Поле** выберите одно из следующих значений:
   - Категория – категория события.
   - ID-события - уникальный номер события.
   - Важность – индикатор важности события.
   - Действие - действие, которое было выполнено во время события.
   - Кто – пользователь, который инициировал событие.
   - Что – тип события.
   - Где - расположение компьютера, на котором произошло событие.
   - Регулируется стандартом – индикатор, показывающий, регулируется ли файл стандартом.
   - Компьютер – компьютер, на котором обнаружен файл, папка или событие, ведущее к рискам.
   - Пользователь – пользователь, на компьютере которого хранится файл или на учетной записи которого запущено событие.
   - Домен – домен, в котором расположен компьютер, где хранится файл или произошло событие, ведущее к рискам.
   - Тип объекта – тип файла.
   - Источник – создатель файла.
   - Содержимое – текстовое содержимое файла.
9. В раскрывающемся списке столбца **Оператор** выберите одно из следующих значений:
   - Содержит – указанное значение присутствует в выбранном столбце таблицы с информацией об объекте.
   - Не содержит - указанное значение отсутствует в выбранном столбце таблицы с информацией об объекте.

- Равно - указанное значение соответствует значению в выбранном столбце таблицы с информацией об объекте.
- Не равно - указанное значение не соответствует значению в выбранном столбце таблицы с информацией об объекте.

10. В поле столбца **Значение** укажите значение, при обнаружении которого будет создано оповещение.
11. При необходимости добавить еще дополнительно условие, нажмите кнопку **Добавить условие** еще раз и повторите последовательность действий в шагах 7-9.
12. В блоке **Отправлять уведомления по почте** выполните следующие действия:
    - В поле ввода **Получатели** укажите адреса электронной почты, на которые будет отправлено оповещение при появлении соответствующего риска.
    - В поле ввода **Тема** укажите тему сообщения электронной почты.
    - В поле ввода **Тело** укажите текст сообщения, который будет отправлен на адрес электронной почты.

> **Внимание!** В тексте сообщения вы можете вставлять переменные из раскрывающегося списка **Поле** в формате {{.Who}}. При отправке уведомления в тексте будет автоматически проставлено соответствующее значение. Вы можете использовать следующие переменные: Who, Where, What, Time, Priority, Category, Source.

13. Нажмите на кнопку **Создать**, чтобы сохранить новое правило.

Когда анализ объектов покажет, что риски, для которых были настроены оповещения, обнаружены в корпоративной сети, в панели оповещений появится соответствующая информация.

Как открыть панель оповещений

В боковом меню выберите **Объекты** > **Оповещения**.

РАССЫЛКА ПОЧТОВЫХ УВЕДОМЛЕНИЙ

Вы можете настроить рассылку почтовых уведомлений об изменении состояния инцидентов, зарегистрированных в InfoWatch DAT. В качестве адресатов данных уведомлений будут фигурировать все лица, связанные с инцидентами.

Создание рассылки

1. В боковом меню выберите **Настройки** -> **Почтовые уведомления**.
2. В поле **SMTP-сервер** введите адрес SMTP-сервера, с которого будут рассылаться почтовые уведомления, например, smtp.gmail.com:587.
3. В поле **Отправитель** введите имя отправителя почтовых уведомлений.
4. В поле **Имя пользователя** введите имя пользователя, авторизованного для подключения к SMTP-серверу.
5. В поле **Пароль** введите пароль пользователя, авторизованного для подключения к SMTP-серверу.
6. Нажмите на кнопку **Сохранить**.

СОЗДАНИЕ БАЗЫ ЗНАНИЙ

При работе с инцидентами информационной безопасности и объектами компьютерной инфраструктуры может появиться необходимость зафиксировать в открытом виде дополнительную информацию (например, подробную информацию о зловредных утилитах, особенности обработки специфических объектов, списки сотрудников), с помощью которой сотрудники ИБ и другие причастные лица смогут принимать решения или обрабатывать данные.

Для этих целей в InfoWatch DAT предусмотрена возможность создать базу знаний. *База знаний* состоит из текстовые статей, которые вы добавляете в веб-консоли InfoWatch DAT.

Как открыть базу знаний

В боковом меню выберите пункт **База знаний**.

Откроется список существующих разделов и статей.

Для более удобной организации материалов вы можете создавать разделы и подразделы, в которых будут располагаться близкие по содержанию статьи.

Создание разделов и подразделов

1. В боковом меню выберите пункт **База знаний**.
2. В правом верхнем углу рабочей области нажмите на кнопку **Создать раздел**.
3. В появившемся диалоговом окне в поле **Имя раздела** введите название раздела и нажмите на кнопку **Создать раздел**.

   Новый раздел появится в рабочей области.
4. Чтобы создать подраздел, нажмите на название основного раздела.
5. В открывшемся списке выполните действия 2 и 3 из этой инструкции еще раз.

Добавление статьи в базу знаний

1. В боковом меню выберите пункт **База знаний**.
2. Выберите раздел, в котором требуется создать статью.
3. В верхнем правом угле рабочей области нажмите на кнопку **Создать страницу**.
4. В появившемся диалоговом окне в поле **Имя страницы** введите название статьи и нажмите на кнопку **Создать страницу**.

   Будет создана пустая статья. Вы можете выбрать тип разметки новой страницы, HTML или Markdown, нажав на раскрывающееся меню **HTML** в верхнем правом углу рабочей области. По умолчанию установлен тип разметки HTML.
5. Нажмите на кнопку **Изменить текст**.

   Откроется окно текстового редактора.
6. Добавьте необходимую информацию и нажмите на кнопку **Сохранить текст**.

При необходимости перенести базу знаний или создать архив статей, вы можете экспортировать информацию из базы.

Экспорт статей из базы знаний

1. В боковом меню выберите пункт **База знаний**.
2. В верхнем правом углу нажмите на кнопку **Меню**.
3. Выберите пункт **Экспорт**.

   База знаний будет выгружена в файл формата JSON.

Импорт статей в базу знаний

1. В боковом меню выберите пункт **База знаний**.
2. В верхнем правом углу нажмите на кнопку **Меню**.
3. Выберите пункт **Импорт**.

   Откроется окно загрузки данных.
4. Перетащите файл формата JSON в квадратную область загрузки или нажмите на кнопку **Загрузить**, чтобы выбрать файл на вашем компьютере.

   Статьи из файла будут добавлены в базу знаний.

Вы можете добавлять в базу знаний файлы.

Добавление файла в базу знаний

1. В боковом меню выберите пункт **База знаний**.
2. В верхнем правом углу рабочей области нажмите на кнопку **Загрузить файл**.

   Откроется окно **Загрузить файл**.
3. Перетащите файл в область загрузки или нажмите на нее, чтобы выбрать файл в системном окне проводника.

   Файл будет загружен в базу знаний.

ПРИЛОЖЕНИЕ 1 О ФАЙЛОВЫХ СТАНДАРТАХ

InfoWatch DAT определяет в файлах наличие данных, регулируемых следующими стандартами:

- Федеральный закон "О персональных данных" 152-ФЗ

  Закон регулирует обращение с персональными данными физических лиц в целях реализации конституционных прав человека, в том числе права на неприкосновенность частной жизни, личную и семейную тайну.

- Personal Health Information Protection Act (PHIPA)

  Стандарт устанавливает правила сбора, использования и предоставления информации о состоянии здоровья частного лица.

- General Data Protection Regulation (GDPR)

  Стандарт устанавливает правила сбора, использования и предоставления данных частных лиц в пределах Европейского союза.

- Health Insurance Portability and Accountability Act (HIPAA)

  Акт (закон) о мобильности и подотчётности медицинского страхования.

- Personally identifiable information (PII)

  Свод правил для защиты идентифицирующей персональной информации в рамках ISO/IEC 27000.

- Financial Records

  Стандарт устанавливает правила использования финансовой информации.

  Payment Card Industry Data Security Standard (PCI DSS)

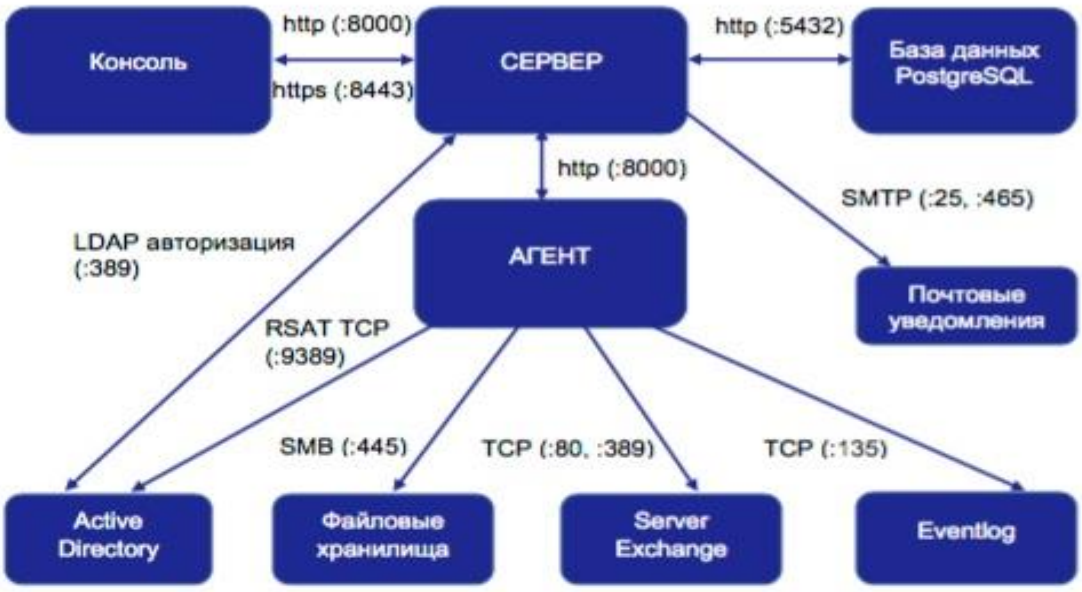
  Стандарт безопасности данных, используемых в индустрии платежных карт.

- Gramm-Leach-Bliley Act (GLB Act or GLBA)

  Стандарт, регулирующий правила обращения с финансовыми данными покупателей.

ПРИЛОЖЕНИЕ 2 СХЕМА ВЗАИМОДЕЙСТВИЯ МОДУЛЕЙ

Схема взаимодействия модулей InfoWatch Data Access Tracker



Взаимодействие	Протокол	Порт	Назначение
Сервер - Консоль	http	8000	Веб-интерфейс
Сервер - Консоль	http	8443	Веб-интерфейс
Сервер – База данных	http	5432	Хранение данных
Сервер – почтовые уведомления	smtp	25, 465	Отправка уведомлений по почте
Сервер – LDAP авторизация	TCP	389	Авторизация доменных юзеров в веб-интерфейсе
Агент – Active Directory (RSAT)	TCP	9389	Сбор данных из Active Directory
Агент - файловые хранилища (SMB)	TCP	445	Сбор данных о директориях и файлах
Агент – сервер Exchange	TCP	80, 389	Сбор данных о почтовых ящиках и событий
Агент – Eventlog	TCP	135	Сбор событий с контроллеров домена и файловых серверов.