InfoWatch Device Control. Руководство пользователя

27/01/2025

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Аудитория 4

2 Комплект документов 5

3 Техническая поддержка пользователей 6

4 Обзор 7

5 Интерфейс Центра расследований 8

5.1 Раздел "Устройства" 9

5.1.1 Вкладка "События использования" 9

Вердикты 11

Панель фильтров 12

Работа с фильтрами 13

5.1.2 Вкладка "Правила" 16

Действия с правилами 17

Действия с группами правил 21

Эффективная политика 22

5.1.3 Вкладка "Группы устройств" 23

6 Пользовательское лицензионное соглашение 26

7 Глоссарий 31

Настоящее руководство содержит сведения по работе в InfoWatch Device Control (далее также Система или Device Control) - программном обеспечении, позволяющем управлять правами доступа к съемным устройствам.

1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, работающих с Системой.

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

2 Комплект документов

В комплект документации по InfoWatch Device Control входят:

- «InfoWatch Device Control. Руководство по установке». Содержит описание установки, обновления и удаления InfoWatch Device Control.
- «InfoWatch Device Control. Руководство администратора». Содержит информацию по настройке и подготовке к работе InfoWatch Device Control.
- «InfoWatch Device Control. Руководство пользователя». Содержит описание работы с InfoWatch Device Control.

Сопутствующая документация по модулю InfoWatch Device Monitor for Linux включает в себя:

- «InfoWatch Device Monitor for Linux. Руководство по установке». Содержит описание установки, обновления и удаления модуля InfoWatch Device Monitor for Linux.
- «InfoWatch Device Monitor for Linux. Руководство пользователя». Содержит описание работы с InfoWatch Device Monitor for Linux.

3 Техническая поддержка пользователей

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

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

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

4 Обзор

InfoWatch Device Control – это программный продукт, позволяющий предотвращать утечки данных с корпоративных компьютеров на внешние устройства хранения (карты памяти, жесткие диски, MTP-устройства, принтеры и др.).

Device Control реализован на базе модуля InfoWatch Device Monitor for Linux. Для защиты от утечек непосредственно на пользовательских компьютерах используются Агенты Device Monitor.

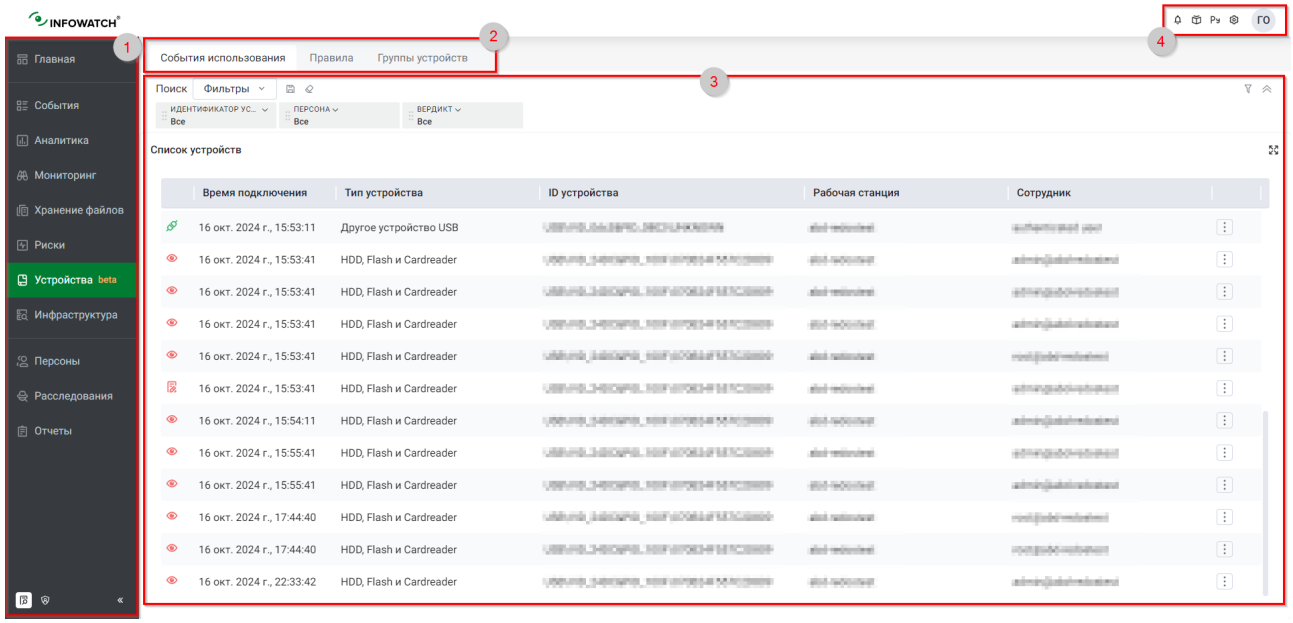
Device Control работает следующим образом:

1. В интерфейсе Device Control вы создаете правила доступа к внешним носителям информации для сотрудников и компьютеров.
2. С помощью сервера Device Monitor созданные правила распространяются на Агенты Device Monitor.
3. В соответствии с правилами Агенты на рабочих станциях осуществляют контроль доступа к внешним устройствам.

5 Интерфейс Центра расследований

Для работы с Device Control используйте веб-консоль Центра расследований InfoWatch.

В интерфейсе Центра расследований можно выделить несколько областей. На изображении ниже представлен раздел **Устройства**.



Элементы интерфейса:

Номер на схеме	Элемент окна	Описание элемента
1	Панель навигации	Содержит: • Рабочие разделы Центра расследований. Для работы с Device Control используется только раздел **Устройства**. • Кнопки переключения между Центром расследований и Центром администрирования. Центр администрирования используется для работы с InfoWatch Device Monitor.
2	Панель вкладок	Список вкладок раздела
3	Рабочая область	Отображение виджетов Device Control и работа с ними
4	Меню пользователя	Пользовательское меню, в котором вы можете: • отредактировать свою учетную запись;

Номер на схеме	Элемент окна	Описание элемента
		• сменить пароль; • включить использование горячих клавиш; • узнать контактные данные компании InfoWatch и службы поддержки; • выйти из Системы
	 Настройки	Раздел настроек (подробнее см. "*InfoWatch Device Control. Руководство администратора*")
	 Уведомления	Папка уведомлений, в которую попадают сообщения Системы пользователю (подробнее см. "*InfoWatch Device Control. Руководство администратора*" статью "*Уведомления*")
	 Смена языка	Выбор языка интерфейса: *Русский* или *Английский*
	 Справочник	Справочник Центра расследований. В данной версии Device Control не доступен.

5.1 Раздел "Устройства"

Функциональность Device Control представлена в Центре Расследований в разделе **Устройства**. В нем пользователь может просматривать события использования устройства, создавать правила контроля внешних устройств и группировать устройства.

> **Важно!**
>
> В разделе может работать только пользователь, которому разрешен доступ согласно роли. Подробнее см. "*InfoWatch Device Control. Руководство администратора → Настройки → Роли*".

В разделе представлены вкладки:

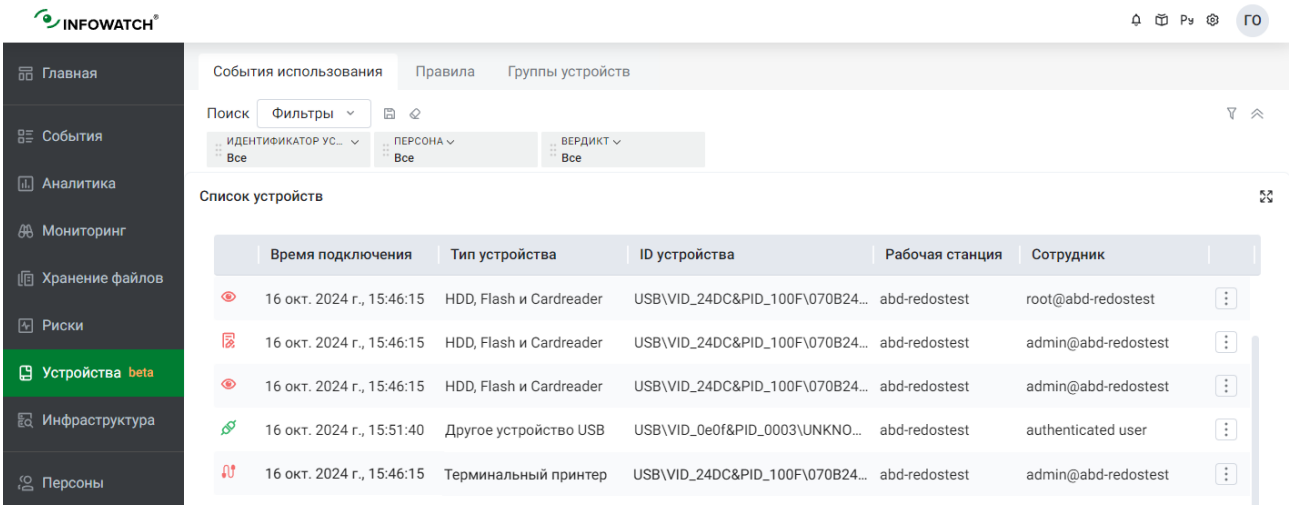
- События использования
- Правила
- Группы устройств

5.1.1 Вкладка "События использования"

Вкладка содержит данные событий использования устройств на рабочих станциях компании.

Важно!

Для получения и просмотра событий, настройте правила, ограничивающие доступ к устройствам на вкладке **Правила** .



События представлены в виде таблицы. Каждая запись таблицы содержит следующие поля:

Параметр	Описание
Вердикт	Факт события и вердикт системы после того, как сотрудник инициировал действие с внешним устройством. События, зарегистрированные Системой, могут быть двух типов в зависимости от совершенного действия и иметь следующие вердикты: 1. **События подключения** внешних устройств. Вердикты: • Подключение разрешено  - устройство было подключено и по крайней мере чтение с устройства разрешено; • Подключение запрещено  - устройство было подключено и любые дальнейшие операции с ним будут запрещены; 2. **События запрета взаимодействия** с ранее подключенными внешними устройствами. Вердикты: • Чтение запрещено  - Система заблокировала попытку чтения с устройства; • Запись запрещена  - Система заблокировала попытку записи на устройство; • Использование запрещено  - Система заблокировала попытку использования устройства. Подробнее механизм вынесения вердиктов описан ниже.

Параметр	Описание
Время подключения	Дата и время события
Тип устройства	Наименование типа устройства: флоппи-дисковод, USB-накопитель и т.д.
ID устройства *	Идентификатор устройства в формате: (VID) + серийный номер экземпляра (PID) применяемого внешнего устройства или принтера, используемого в операции Например: FDC\GENERIC_FLOPPY_DRIVE\6&2BC13940&0&0
Рабочая станция	Рабочая станция, где произошло событие с устройством
Сотрудник *	Персона-инициатор события

* Для Агентов Device Monitor под управлением ОС Astra Linux 1.7, РЕД ОС и ОС Альт при подключении/использовании внешних устройств через USB:

- может отсутствовать идентификатор устройства, если он не задан в этом устройстве производителем;
- может не определяться имя учетной записи пользователя, которым было подключено устройство.

Вердикты

При подключении внешнего устройства Система формирует **событие подключения** с разрешающим или запрещающим вердиктом. Далее при нарушении политики контроля внешних устройств формируются **события запрета взаимодействия** с этим устройством в зависимости от его типа.
Для устройств с возможностью чтения/записи файла в случае запрета взаимодействия Система назначает вердикты "Чтение запрещено " или "Запись запрещена ". К этим устройствам относятся следующие типы:

- HDD, Flash и Cardreader
- MTP-устройство
- CD/DVD
- Флоппи-диск
- Терминальное устройство хранения

Для таких устройств любое действие, модифицирующее их содержимое, считается записью. Все остальные действия - чтением.
Для устройств всех остальных типов, в случае запрета взаимодействия с ними, Device Control назначает вердикт "Использование запрещено ".

Важно!

На компьютерах под управлением ОС семейства Linux настройка доступа и контроль поддерживаются только для устройств с возможностью чтения/записи файла.
При этом события подключения устройств всегда будут иметь вердикт "Подключение разрешено ". При запрете использования устройств они будут отображаться в операционной системе, но будут недоступны для взаимодействия.

Вердикты событий, формируемых Системой:

Тип устройства	Устройства с возможностью чтения/записи файла			Другие устройства	
Вердикт при подключении устройства	Подключение разрешено 	Подключение запрещено 		Подключение разрешено 	Подключение запрещено 
Вердикт при последующем нарушении политики	Запись запрещена 	Запись запрещена 	Чтение запрещено 	-	Использование запрещено 

Пример 1:

Сотрудник подключает к рабочей станции MTP-устройство, доступ к которому ему запрещен согласно правилу. После чего пытается каким-либо способом просмотреть содержимое устройства.

Device Control создает событие подключения с вердиктом "Подключение запрещено ". При последующих попытках сотрудника просмотреть содержимое Система блокирует это действие и создает события с вердиктом "Чтение запрещено ".

Пример 2:

Сотрудник подключает к рабочей станции USB-Flash-накопитель, и ему разрешено только чтение с этого устройства. Он пытается каким-либо способом изменить содержимое накопителя.

Device Control создает событие подключения с вердиктом "Подключение разрешено ". При последующих попытках сотрудника изменить содержимое Система блокирует это действие и создает события "Запись запрещена ".

Панель фильтров

В верхней части рабочей области находится панель фильтров. С ее помощью вы можете:

- управлять отображением событий использования устройств:

    - выбирать конкретные события для отображения;
    - исключать лишние события из таблицы;
- сохранять настройки фильтрации, чтобы быстро получать необходимую информацию.

На вкладке доступны следующие фильтры:

Название фильтра	Соответствует столбцу в таблице с событиями	Выбор значения
Идентификатор устройства	ID устройства	Чтобы выбрать значение, выполните одно из действий: • Выберите значение из списка. Для поиска в списке введите значение в строку поиска. Отображение элементов в списке не зависит от условий, установленных в других фильтрах. • Введите значение в строку поиска и выберите значение типа "поиск по шаблону". Значение по умолчанию: **Все**
Персона	Сотрудник	
Вердикт	Вердикт	Выберите значение из списка. Значение по умолчанию: **Все**

Подробнее о действиях с фильтрами см. статью "Работа с фильтрами".

Также на вкладке **События использования** вы можете:

- **Переместить столбец**. Для этого нажмите на заголовок столбца и, не отпуская, перемещайте заголовок вдоль строки заголовков.
- **Изменить ширину столбца**. Для этого нажмите на правую границу заголовка столбца и, не отпуская, перемещайте границу столбца.
- **Скопировать адрес электронной почты пользователя** в столбце **Сотрудник**. Для этого:
    1. Наведите курсор на содержимое ячейки.
    2. Во всплывающем окне поместите курсор на строку с содержимым.
    3. Нажмите на появившуюся кнопку  **Копировать**.
- **Скопировать ID устройства**. Для этого:
    1. Нажмите  в крайнем правом столбце напротив выбранного события.
    2. Во всплывающем окне нажмите 

.
- **Открыть таблицу с событиями на весь экран**. Для этого в правом верхнем углу таблицы нажмите .

Работа с фильтрами

Добавление и удаление фильтров

В панели фильтров можно использовать один или несколько фильтров.

Чтобы добавить фильтр на панель фильтров:

1. В правом верхнем углу рабочей области нажмите .
2. В открывшемся окне выберите нужный фильтр из списка.
3. Щелкните вне окна со списком фильтров.

Фильтр будет добавлен на панель фильтров.

Чтобы удалить фильтр с панели фильтров:

1. В правом верхнем углу рабочей области нажмите .
2. Снимите флажок с фильтра в списке.
3. Щелкните вне окна со списком фильтров.

Фильтр будет удален с панели фильтров.

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

Чтобы скрыть панель фильтров, нажмите .

Значения фильтров

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

Если изменить значение фильтра, то автоматически обновится таблица с событиями использования устройств. В таблице отображаются только те события, которые соответствуют условиям фильтров.

Важно!

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

Условие с несколькими фильтрами

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

Пример:

Укажите значение для нескольких фильтров:

- в фильтре **Персона** выберите сотрудника, например, **Иванова И.И.**
- в фильтре **Вердикт** выберите опцию **Запись запрещена**

В результате отобразятся только те события, которые одновременно соответствуют всем вышеуказанным условиям, а именно, события, в которых сотруднику **Иванову И.И.** была **запрещена запись** на внешнее устройство.

Тип значения "поиск по шаблону"

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

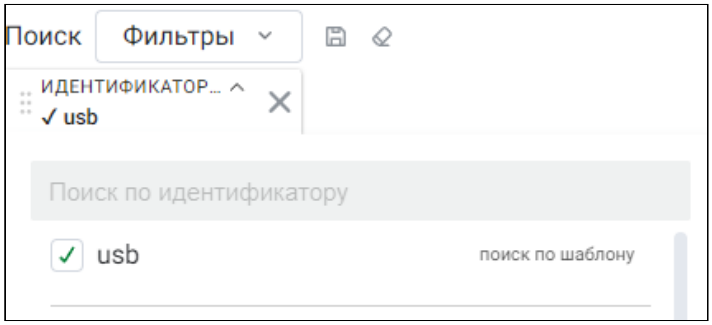
- Идентификатор устройства;
- Персона.

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

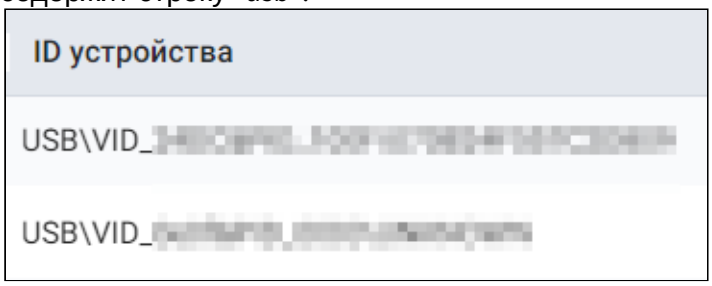
При фильтрации Система проверяет, входит ли значение из строки поиска в полное значение поля записи о файле. Для значений типа "поиск по шаблону" не учитывается регистр.

Пример:

1. Для фильтра **Идентификатор устройства** включите значение поиска по шаблону "usb":



2. В результате фильтрации отображаются только те события, в которых ID устройства содержит строку "usb":



Включение и исключение значений фильтра

На вкладке **События использования** несколько состояний доступны для значений следующих фильтров:

- Идентификатор устройства
- Персона;
- Вердикт.

Доступные состояния для значений вышеуказанных фильтров:

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

Чтобы изменить состояние значения, щелкните по флажку состояния.

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

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

Важно!

В фильтре **Идентификатор устройства** использование типа значения "поиск по шаблону" при включении/исключении нескольких значений не поддерживается.

Сброс значений фильтра

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

Чтобы сбросить значения для всех фильтров, нажмите .

Сохранение и загрузка наборов фильтров

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

1. Установите нужные значения фильтров и нажмите .
2. В открывшемся окне задайте имя нового фильтра.
3. Выберите тип фильтра:
   - *Личный* - при этом фильтр будет доступен только создавшему его пользователю;
   - *Общий* - фильтр будет доступен всем пользователям Системы.
4. Нажмите **Сохранить**.

Чтобы воспользоваться ранее созданным фильтром:

1. На панели фильтров нажмите **Фильтры**.
2. Нажмите на интересующий фильтр, чтобы его активировать. При этом Главный офицер может:
   -  - редактировать личные и общие фильтры;
   -  - удалять личные и общие фильтры.

Другие офицеры безопасности могут редактировать и удалять только личные фильтры.

5.1.2 Вкладка "Правила"

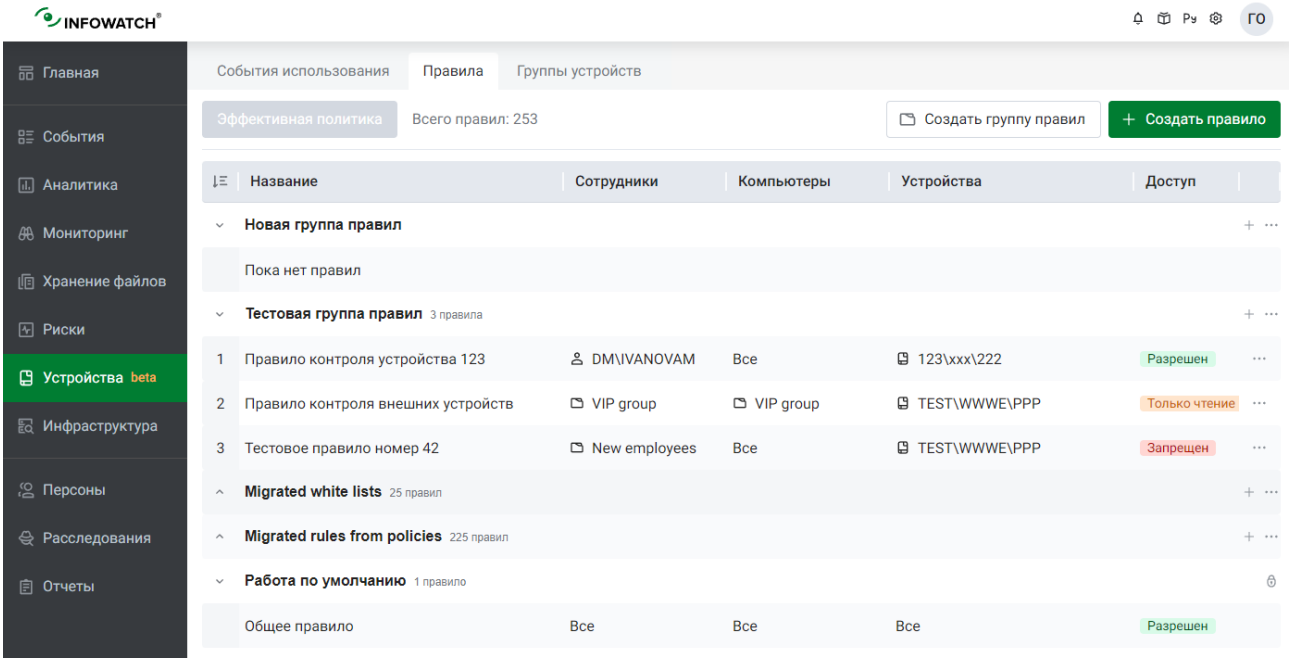
Правила позволяют контролировать доступ и использование съемных устройств хранения.

На вкладке **Правила** вы можете работать с правилами и группами правил - создавать их и изменять. А с помощью инструмента **Эффективная политика** - просмотреть, какие правила действуют для выбранных компьютеров, сотрудников и устройств.

Правила представлены в виде таблицы и расположены в ней в порядке убывания их приоритета, вверху списка – правило с наивысшим приоритетом. Таблица содержит:

- Созданные вами правила;
- Правило по умолчанию, которое всегда располагается внизу списка и разрешает доступ для всех сотрудников, компьютеров и устройств;
- Правила контроля внешних устройств и белые списки, мигрированные из Device Monitor.

> **Примечание:**
>
> Белые списки предназначены для управления устройствами, доступ к которым безусловно разрешен (сотруднику, группе сотрудников, компьютеру или группе компьютеров).



В этом разделе:

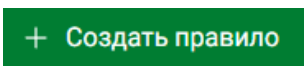
- Действия с правилами
- Действия с группами правил
- Эффективная политика

Действия с правилами

Доступные действия с правилами:

- создание правила;
- редактирование правила;
- перемещение правила в списке;
- удаление правила.

Чтобы создать правило:

1. На вкладке **Правила** в правом верхнем углу нажмите 

.
2. В открывшемся окне в области **Правило**:
   - Выберите группу правил, в которую входит данное правило (группа по умолчанию недоступна для выбора).
   - Введите название правила.
3. В области **Устройства**:
   a. Отметьте необходимый вариант ограничения доступа на использование устройства. Вы можете:

- полностью запретить доступ к устройству:
  - на компьютерах под управлением ОС Windows – для типов **HDD, Flash и Cardreader**, **CD/DVD**, **Флоппи-диск** и **MTP-устройство**;
  - на компьютерах под управлением ОС семейства Linux – только для типов **HDD, Flash и Cardreader** и **MTP-устройство**;
- разрешить только чтение (доступно только для типов **HDD, Flash и Cardreader**, **CD/DVD**, **Флоппи-диск**, **MTP-устройство** и **Терминальное устройство хранения**);

  > **Примечание:**
  >
  > Контроль подключения через MTP-протокол осуществляется для устройств на платформах: Android, iOS, Windows Phone/10 Mobile; Blackberry 10.

- разрешить доступ к устройству.

b. Выберите устройства, входящие в правило:
   i. По умолчанию выбраны все устройства. Чтобы выбрать только нужные устройства, отключите настройку  **Выбрать все типы**. Затем нажмите **Выбрать устройства**.
   В открывшемся диалоговом окне в области слева отобразится список типов устройств и обнаруженные устройства каждого типа (при наличии) из числа ранее зарегистрированных в Системе.
   ii. Выберите из списка **Устройства**, **Группы устройств** и/или **Типы устройств** контролируемые данным правилом:
   Хранение информации:
   - HDD, Flash и Cardreader
   - MTP-устройство
   - CD/DVD
   - Флоппи-диск
   - Ленточное устройство
   - PDA

   Порты и адаптеры:
   - Параллельный порт
   - Последовательный порт
   - Другое устройство USB
   - Считыватель смарт-карт
   - IrDA устройство
   - FireWire
   - Многофункциональное устройство
   - PCMCIA устройство

   Сетевые:
   - Модем
   - Сетевой адаптер USB
   - Bluetooth устройство

   Принтеры и сканеры:
   - Локальный принтер
   - Сетевой принтер
   - Устройство работы с изображениями (камера, сканер)

Терминальные:

- Терминальное устройство хранения
- Терминальный порт
- Терминальное самонастраиваемое устройство
- Терминальный принтер

> **Важно!**
>
> На рабочих станциях под управлением ОС семейства Linux поддерживается контроль только следующих типов устройств:
>
> - HDD, Flash и Cardreader;
> - MTP-устройство;
> - CD/DVD;
> - Флоппи-диск.

Чтобы развернуть или свернуть список, используйте .
Для добавления типа, группы устройств или отдельного устройства, наведите на него курсор и нажмите , тип/группа/устройство появится справа в области **Выбрано**. В области слева, напротив добавленных устройств, групп и типов устройств, появится значок .

> **Примечание:**
>
> Создавать группы устройств можно на вкладке **Группы устройств**.

Чтобы исключить, нажмите .
Также добавить или исключить тип/группу/устройство можно **двойным щелчком мыши**.

> **Важно!**
>
> Если какое-либо устройство подключалось на разных рабочих станциях, то в Системе могут возникнуть дублирующие записи этого устройства. Если вы добавите в правило любую запись этого устройства, то дублирующая запись также будет добавлена.

По окончании выбора устройств нажмите **Применить**.

iii. Чтобы выбрать сразу все устройства, нажмите кнопку  **Выбрать все типы**.

4. В области **Сотрудники:**
   По умолчанию выбраны все сотрудники. Чтобы выбрать только нужных сотрудников:
   a. Отключите настройку  **Выбрать все**
   b. Нажмите 

      .

c. Выберите сотрудников и/или группы сотрудников, контролируемые данным правилом.
d. Нажмите **Применить**.

5. В области **Компьютеры:**
   По умолчанию выбраны все компьютеры. Чтобы выбрать только нужные компьютеры:
   - Отключите настройку  **Выбрать все**.
   - Нажмите 

.
   - Выберите компьютеры и/или группы компьютеров, контролируемые данным правилом.
   - Нажмите **Применить**.
6. После заполнения всех полей, нажмите **Создать правило**.

> **Примечание:**
>
> Если в правило входит тип устройств, группа устройств, группа сотрудников или группа компьютеров, то правило действует на все входящие подгруппы и элементы вне зависимости от глубины вложенности.

Вы также можете создать правило непосредственно в нужной группе правил, см. "Действия с группами правил".

> **Примечание:**
>
> Новое правило автоматически размещается вверху списка правил.

Особенности применения правил:

1. После обновления Агента Device Monitor для поддержки запрета доступа к MTP-устройствам необходимо перезагрузить рабочую станцию. При чистой установке перезагрузка не требуется.
2. Мобильные устройства на платформе BlackBerry 10 при включенной настройке "Режим USB-накопителя" определяются как два устройства разных типов: **MTP-устройство** и **HDD, Flash и Cardreader**. Чтобы запретить копирование данных на устройство, необходимо установить запрет для типа **HDD, Flash и Cardreader**.

Чтобы отредактировать правило:

1. На вкладке **Правила** выберите правило.
2. Нажмите  **Действия с правилом** и выберите **Редактировать**.
3. Внесите изменения и нажмите **Сохранить**.

Чтобы переместить правило в списке:

1. На плитке правила нажмите  **Действия с правилом**.
2. Выберите, где необходимо разместить правило: **Наверх**, **Вниз**, **Выше**, **Ниже**.

или

1. На плитке правила, которое необходимо переместить, наведите курсор на порядковый номер правила в левом столбце.

   Вместо номера отобразится значок .
2. Нажмите на значок и удерживая его, переместите правило выше или ниже в списке.

Наивысший приоритет имеет правило, которое находится вверху списка, наименьший приоритет – правило внизу списка.

> **Примечание:**
>
> Перемещение недоступно при выбранном параметре эффективной политики.

Чтобы удалить правило:

1. На плитке правила нажмите  **Действия с правилом** и выберите **Удалить**.
2. Нажмите **Подтвердить**.

Действия с группами правил

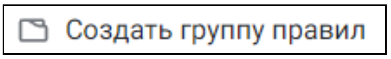
По умолчанию при первом входе в Систему на вкладке отображаются две группы правил:

- **Группа по умолчанию**, которая всегда имеет наименьший приоритет и не доступна для редактирования. Группа содержит правило, разрешающее доступ для всех сотрудников, компьютеров и устройств.
- **Новая группа**, которая не содержит ни одного правила.

Доступные действия с группами:

- создание группы (вы также можете создать группу выше или ниже в существующем списке);
- изменение наименования группы;
- добавление правила в группу;
- перемещение группы в списке;
- удаление группы.

Чтобы создать группу правил:

1. На панели вверху нажмите 

.
2. Введите наименование группы.
3. Нажмите **Сохранить**.

> **Примечание:**
>
> Новая группа правил автоматически размещается вверху списка групп, если при ее создании не было задано место в списке.

Чтобы создать группу правил в определенном месте списка:

1. На плитке существующей группы правил в списке нажмите  **Действия с группой**.
2. Выберите **Создать группу выше** или **Создать группу ниже**.
3. Нажмите **Сохранить**.

Чтобы изменить наименование группы:

1. На плитке группы правил нажмите  **Действия с группой**.
2. Выберите **Редактировать**.
3. Введите наименование группы.
4. Нажмите **Сохранить**.

Чтобы добавить правило в группу:

1. На плитке группы правил нажмите  **Добавить правило в группу**.
2. В открывшемся окне создания правила задайте параметры правила (поле группа заполняется автоматически). Подробнее см. "Действия с правилами".
3. В правой верхней части рабочей области нажмите **Создать правило**.

Чтобы переместить группу в списке:

1. На плитке группы правил нажмите  **Действия с группой**.
2. Выберите, куда необходимо переместить группу: **Наверх**, **Вниз**, **Выше**, **Ниже**.

Чтобы удалить группу:

1. На плитке группы правил нажмите  **Действия с группой**.
2. Выберите **Удалить**.
3. Нажмите **Подтвердить**.

Эффективная политика

Эффективная политика – это перечень правил, представленных в порядке убывания приоритета их применения. С помощью данного инструмента вы можете проверить, какие правила действуют для выбранных компьютеров, сотрудников и устройств. Для этого:

1. Слева вверху на панели нажмите кнопку 

.
2. Нажмите кнопку **Выберите столбец**, и выберите нужный столбец из списка:
   - **Компьютеры**;
   - **Сотрудники**;
   - **Устройства**.
3. В открывшемся окне выберите значение для одного параметра. Например, в столбце **Компьютеры** – **Компьютеры** или **Группы**.
4. Чтобы добавить следующий столбец, нажмите .
5. Нажмите **Применить**. В результате система отобразит список правил, удовлетворяющих выбранным параметрам, а также общее количество этих правил. При этом, правила расположены в порядке убывания их приоритета, вверху списка – правило с наивысшим приоритетом. Правило по умолчанию не учитывается в подсчете и всегда располагается внизу списка.

Пример

Заданы следующие параметры:

- *Устройства*: Устройство 1.
- *Компьютеры*: Группа компьютеров 1.
- *Сотрудники*: Сотрудник 1.

В результате будут отображены правила, содержащие:

- [Устройство 1 *ИЛИ* Группу устройств 1 *ИЛИ* Тип устройств 1 *ИЛИ* *Все* устройства]

и

- [Группу компьютеров 1 *ИЛИ* группу компьютеров, содержащую в себе Группу компьютеров 1 *ИЛИ* *Все* компьютеры]

и

- [Сотрудника 1 *ИЛИ* Группу сотрудников, имеющую в составе Сотрудника 1 *ИЛИ* *Всех* сотрудников]

Примечание:

При выбранном параметре эффективной политики, недоступно создание группы правил в определенном месте списка, а также изменение приоритета правил и групп правил (перемещение в списке).

5.1.3 Вкладка "Группы устройств"

На вкладке **Группы устройств** вы можете работать с группами устройств.

Слева располагается область **Группы**, где отображаются все группы устройств в иерархическом порядке в соответствии с типами устройств.
Каждый тип устройств содержит:

- группу **Обнаруженные**, которая включает в себя все устройства данного типа, зарегистрированные в Системе. Регистрация происходит при их первом подключении к рабочей станции с Агентом Device Monitor.
- созданные вами группы.

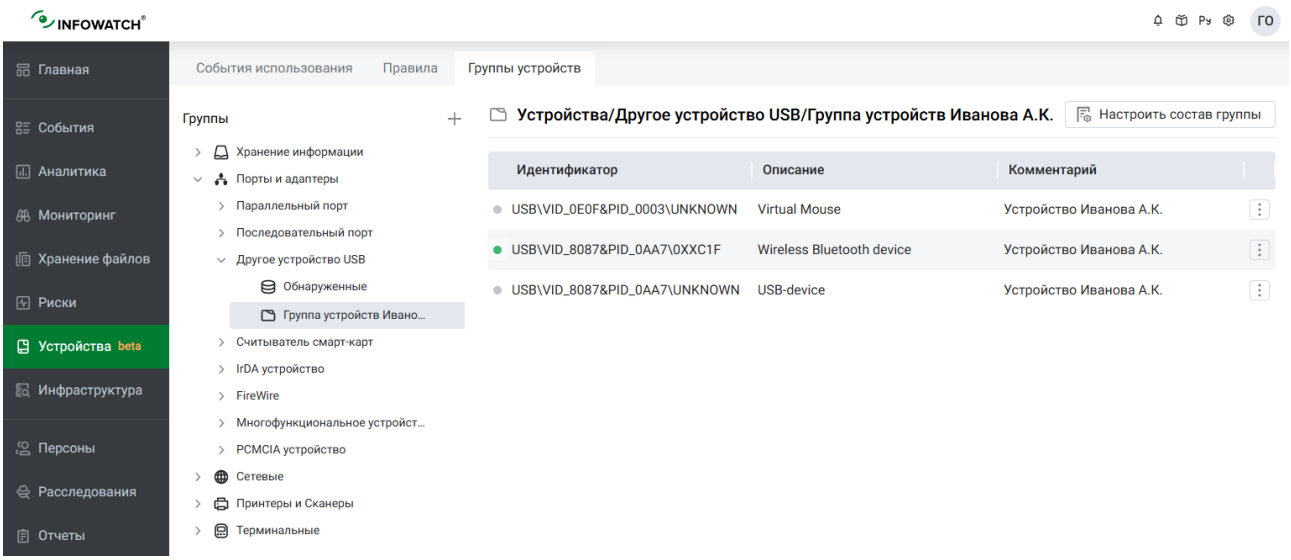
Чтобы просмотреть все входящие в группу устройства, выберите группу левой кнопкой мыши. Устройства будут отображены в центральной части рабочей области.

Слева от каждого устройства отображается индикатор активности:

-  - если устройство в данный момент подключено к какой-либо рабочей станции;
-  - если устройство в данный момент не подключено ни к одной рабочей станции.

Важно!

Если устройство подключалось на разных рабочих станциях, то в Системе могут возникнуть дублирующие записи этого устройства с разными индикаторами. В таком случае рекомендуется добавлять в группу устройство по идентификатору.



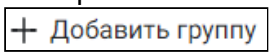
Доступные действия с группами:

- создание;
- переименование;
- настройка состава;
- удаление.

Чтобы создать группу устройств:

1. В верхней части области **Группы** нажмите  **Создать**.
2. Введите наименование и выберите тип устройства группы.
3. Нажмите **Добавить**.

или

1. Наведите курсор на тип устройства создаваемой группы.
2. Нажмите  справа от названия типа.
3. Нажмите 

.
4. Введите наименование группы.
5. Нажмите **Добавить**.

Чтобы переименовать группу устройств:

1. Наведите курсор на группу устройств.
2. Нажмите  справа от названия группы.
3. Выберите **Редактировать группу**.
4. Внесите изменения.
5. Нажмите **Добавить**.

Настройка состава группы устройств

Вы можете настроить состав группы по протоколу устройств или добавить устройство по его идентификатору.

Чтобы настроить состав группы по протоколу устройств:

1. Выберите необходимую группу.

2. В правом верхнем углу рабочей области нажмите Настроить состав группы и выберите способ настройки **По протоколу устройств**.
   или

   Напротив названия группы нажмите ⋮ и выберите **Настроить состав группы**.
   В открывшемся диалоговом окне в области слева отобразится список групп устройств и обнаруженные устройства (при наличии) выбранного типа. Чтобы развернуть или свернуть какую-либо группу, используйте ⌄.
3. Для добавления устройства наведите на него курсор и нажмите →, устройство появится справа в области **Выбрано**. В области слева, напротив добавленного устройства появится значок ✓.

   Аналогично вы можете добавить все устройства из какой-либо группы, нажав → напротив нее.

   Чтобы исключить устройство, нажмите ←.
4. По окончании выбора устройств нажмите **Применить**.

Чтобы добавить в группу устройство по идентификатору:

1. Выберите необходимую группу.
2. В правом верхнем углу рабочей области нажмите Настроить состав группы и выберите способ настройки **По идентификатору устройства**.
3. В открывшемся диалоговом окне заполните поля:
   - параметры идентификатора в одном из форматов:
     - тип устройства (например, USB)\Vendor ID\Product ID
     - тип устройства\Vendor ID.
   - описание и комментарий (если требуется).
4. Нажмите **Добавить**.

Чтобы удалить группу устройств:

1. Наведите курсор на группу устройств.
2. Нажмите ⋮ справа от названия группы.
3. Выберите **Удалить**.
4. Нажмите **Подтвердить**.

6 Пользовательское лицензионное соглашение

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

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

1. Предоставление лицензии

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

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

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

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

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

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

2. Условия использования

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

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

- законодательство о персональных данных;
- законодательство о коммерческой тайне;
- законодательство о противодействии неправомерному использованию инсайдерской информации;
- законодательство о противодействии коррупции;
- законодательство о критической информационной инфраструктуре;
- законодательство о государственных информационных системах;

- законодательство о защите данных в Национальной платежной системе;
- нормы Трудового кодекса РФ;
- а также иные применимые источники права.

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

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

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

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

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

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

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

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

2.10. Вам не разрешается:

- целиком или частично редактировать, изменять, адаптировать, переводить, декомпилировать, дизассемблировать, осуществлять инженерный анализ, создавать или воссоздавать исходный код, модифицировать ПО, осуществлять попытки предпринять аналогичные действия в отношении ПО, а также создавать производные работы, основанные на ПО и/или Документации;
- осуществлять интеграцию ПО в сторонние сайты и программные продукты, за исключением случаев, когда такая интеграция прямо разрешена Правообладателем и правообладателем сторонних сайтов и программных продуктов. Допускается интеграция ПО в сторонние программные продукты посредством встроенного модуля API в рамках функциональных возможностей указанного модуля;

- удалять или изменять уведомления об авторских правах, правах собственности на ПО и/или его элементы;
- сдавать ПО в аренду, прокат или во временное пользование, сублицензировать, распространять или иным образом предоставлять любому физическому или юридическому лицу любые права в отношении ПО и/или Документации, а также разглашать результаты стендовых испытаний ПО, за исключением случаев, прямо разрешенных настоящим Соглашением;
- передавать и предоставлять доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения и Договора, заключенного между вами и вашим лицензиаром;
- осуществлять незаконный сбор, систематизацию, хранение и распространение конфиденциальной и/или персональной информации;
- использовать ПО для несанкционированного удаленного доступа к компьютерам третьих лиц, а также изменения конфигурации компьютера так, чтобы такие возможности могли появиться у стороннего ПО;
- собирать, хранить, использовать, обрабатывать и распространять с помощью ПО любые информационные данные, которые нарушают применимое законодательство, права и законные интересы третьих лиц.

2.11. Лицензионный ключ является конфиденциальной информацией. Правообладатель оставляет за собой право использовать средства для проверки подлинности установленного у вас лицензионного ключа.

3. Ограничение гарантий и ответственности Правообладателя

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

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

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

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

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

3.4. Данные, которые становятся доступными при использовании ПО, включая файлы, ссылки, изображения и текст, являются исключительной ответственностью физического или юридического лица, от которого они были получены, и являются собственностью соответствующего лица. Настоящее Соглашение не дает никаких прав на такие данные. Вы принимаете на себя ответственность за

возможные последствия, риски безопасности и любые убытки, вызванные такими данными, просмотренными или полученными Вами с помощью ПО.

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

4. Права на объекты интеллектуальной собственности

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

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

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

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

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

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

6. Открытое программное обеспечение

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

7. Заключительные положения

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

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

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

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

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

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

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

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

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

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

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

8. Контактная информация Правообладателя

Тел./факс: +7(495)229-00-22

Коммерческий департамент: sales@infowatch.com

Служба технической поддержки: support@infowatch.com

Веб-сайт: www.infowatch.ru

7 Глоссарий

Термин	Определение
Администратор	Администратор – пользователь Системы, выполняющий установку, настройку и поддерживающий работу Системы. См. Главный офицер безопасности, Пользователь
Главный офицер безопасности	Предустановленная роль пользователя Консоли управления, имеющая привилегии на все действия в Системе См. Офицер безопасности, Пользователь
Интерфейс пользователя	Совокупность средств и методов, при помощи которых пользователь взаимодействует с Системой
Кластер	Совокупность серверов, объединенных для выполнения общих задач и представляющихся пользователю единой системой. См. Нода
Веб-консоль	Графический интерфейс пользователя, предназначенный для управления системой Device Control (администрирование и настройка Системы, просмотр событий использования устройств)
Лицензия	Право на использование Системы. Получается при приобретении Системы и определяет допустимые действия с Системой
Нода	Сервер, объединенный с другими серверами в общий кластер. См. Кластер
Объект службы каталогов	Отдельная сущность службы каталогов, например, пользователь или компьютер. См. Служба каталогов, Active Directory
Офицер безопасности	Основной пользователь Консоли управления. Также предустановленная роль пользователя Консоли управления, имеющая привилегии на все действия в Системе, за исключением административных
Персона	Учетная запись сотрудника организации или внешнего контакта, содержащаяся в справочнике Системы и позволяющая обрабатывать данные, принадлежащие этой учетной записи, как единое целое, а также отображать

Термин	Определение
	события, относящиеся к ней, в удобном для пользователя виде.
Платформа	Принципиальная конструкция продукта – комплекс частей, подсистем, интерфейсов и производственных процессов. Продуктовая Платформа выступает в качестве базы для развертывания семейства продуктов и сборки готовых изделий из стандартизированных компонентов.
Пользователь	Пользователь системы Device Control – администратор, Офицер безопасности и др. См. Администратор, Офицер безопасности
Рабочая станция / Компьютер	В терминах Системы подразумевается контролируемая рабочая станция или терминальное устройство
Сервис ClickHouse	Распределенная аналитическая столбцовая СУБД, предназначенная для проведения анализа по хранящимся данным в реальном времени. Компонент продуктовой Платформы
Сервис PostgreSQL	СУБД, которая используется в продукте Device Control для хранения событий использования устройств, правил и информации об устройствах. Компонент продуктовой Платформы
Active Directory (AD)	LDAP-совместимая реализация интеллектуальной службы каталогов корпорации Microsoft для операционных систем семейства Windows NT
InfoWatch Device Monitor	Device Monitor: модуль системы InfoWatch Traffic Monitor, позволяющий контролировать обмен данными на рабочих станциях сотрудников.
InfoWatch Traffic Monitor	Traffic Monitor: программный комплекс, предназначенный для контроля различных видов трафика (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) и теневых копий данных, копируемых на съемные носители и отправляемых на печать
Kubernetes	Программное обеспечение для оркестрации контейнеризированных приложений – автоматизации их развертывания, масштабирования и координации в условиях кластера См. POD
NATS	Система обмена сообщениями для компонентов

Термин	Определение
POD	Базовая сущность для построения приложений, работающих на платформе Kubernetes. См. Kubernetes
SSH (Secure Shell)	Сетевой протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов)