



Контроль съемных устройств с помощью технологий Dr.Web Enterprise Security Suite 12.0



Dr.Web Enterprise Security Suite 12.0

Контроль съемных устройств с помощью технологий Dr.Web Enterprise Security Suite 12.0

Внимание! Перед началом процедуры обновления рекомендуется изучить соответствующие разделы документации по продукту Dr.Web Enterprise Security Suite 12.

Содержание

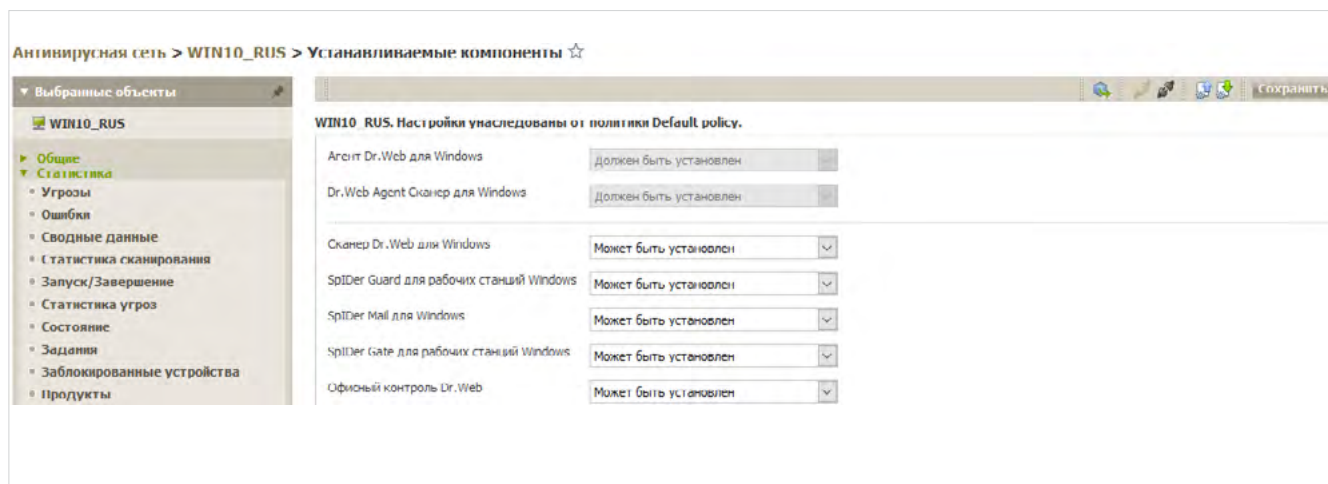
1.	Возможности Dr.Web Enterprise Security Suite 12.0.....	3
1.1.	Контроль доступа к сменным носителям с помощью Центра управления Dr.Web Enterprise Security Suite 12.0.....	3
1.2.	Отображение статистики заблокированных устройств в Центре управления Dr.Web Enterprise Security Suite 12.0.....	11
1.3.	Контроль доступа к сменным носителям на станциях, не управляемых из Центра управления Dr.Web Enterprise Security Suite 12.0.....	11

1. Возможности Dr.Web Enterprise Security Suite 12.0

Используя возможности Центра управления, администратор сети может удаленно настроить права доступа пользователя защищаемого компьютера или устройства к оборудованию рабочей станции, подключаемым сменным носителям, проводить антивирусную проверку сменных носителей, а также контролировать попытки доступа к сменным носителям с помощью раздела статистики. Что позволяет снизить риск распространения вредоносных программ через сменные носители и выявить попытки нарушения политики компании в области сменных носителей.

1.1. Контроль доступа к сменным носителям с помощью Центра управления Dr.Web Enterprise Security Suite 12.0

Контроль доступа к сменным носителям осуществляется с помощью модуля **Офисный контроль**. Чтобы проверить, установлен ли данный модуль на станции и должен ли он устанавливаться, можно, выберите пункт **Антивирусная сеть** в главном меню Центра управления, далее в открывшемся окне в иерархическом списке выберите станцию или группу и затем в открывшемся окне выберите пункт **Устанавливаемые компоненты**.



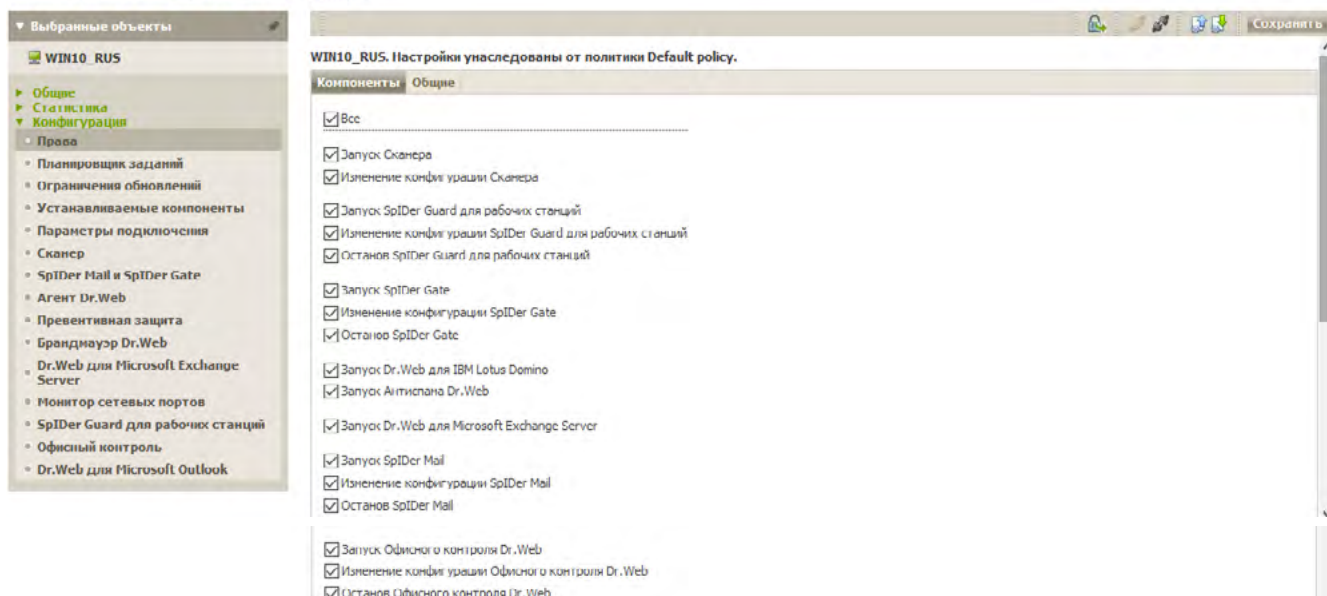
Для того чтобы модуль устанавливался на станции, выберите в выпадающем списке один из вариантов:

- **Должен быть установлен** — задает обязательное наличие компонента на станции. При задании значения **Должен быть установлен** для уже существующей станции компонент будет добавлен в состав имеющегося антивирусного пакета.
- **Может быть установлен**. Решение об установке принимает пользователь при установке Агента.

Для того чтобы разрешить пользователю редактировать настройки модуля Офисного контроля, выберите пункт **Антивирусная сеть** в главном меню Центра управления,

далее в открывшемся окне в иерархическом списке выберите станцию или группу и в открывшемся окне выберите пункт **Права**.

Антивирусная сеть > WIN10_RUS > Права ☆

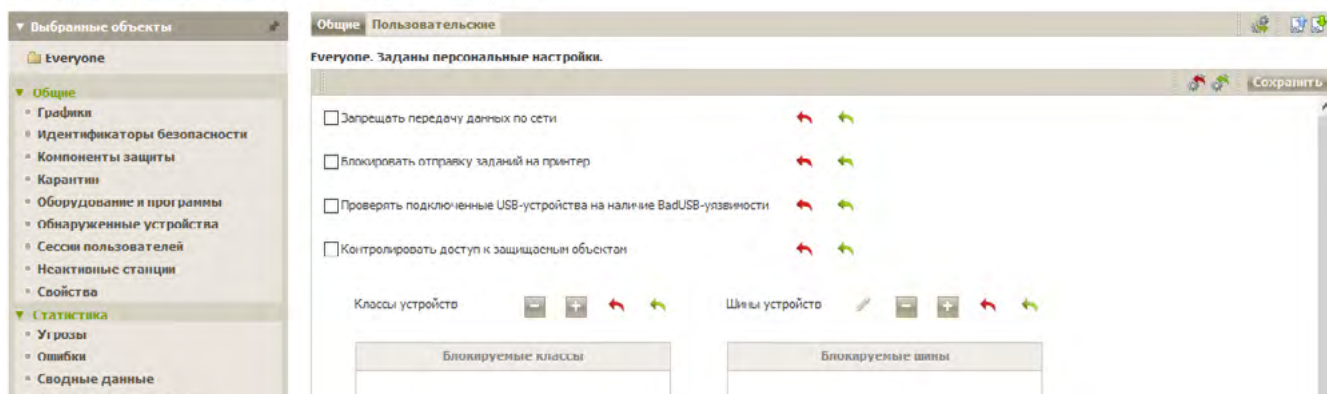


Для того чтобы пользователь имел права изменения конфигурации модуля, отметьте пункт **Изменение конфигурации...**

Для открытия окна редактирования настроек выберите пункт **Антивирусная сеть** главного меню Центра управления, в открывшемся окне в иерархическом списке нажмите на название станции или группы и затем выберите пункт **Конфигурация** → **Windows** → **Офисный контроль** и настройте нужные типы защиты — например, отметив **Контролировать доступ к защищаемым объектам**, вручную добавив шины и классы устройств, доступ к которым необходимо заблокировать. Эти параметры задаются для рабочей станции или группы в целом и находятся на вкладке **Общие**.

По умолчанию для всех учетных записей разрешен неограниченный доступ к ресурсам сети Интернет и к локальным ресурсам, ограничения по времени отсутствуют.

Антивирусная сеть > Everyone > Windows > Офисный контроль ☆



Внимание! Ограничения Офисного контроля распространяются одновременно на всех пользователей компьютера, на котором установлен Dr.Web для ОС Windows.

На вкладке **Общие** вы можете настроить доступ к ресурсам локальной файловой системы и ограничить их использование.

- Включите опцию **Блокировать отправку заданий на принтер**, чтобы запретить передачу на принтер задания на печать.
- Включите опцию **Проверять подключенные USB-устройства на наличие BadUSB-**

уязвимости, чтобы проверить, действительно ли подключаемое USB-устройство является клавиатурой.

- Включите опцию **Контролировать доступ к защищаемым объектам**, чтобы получить возможность ограничить доступ к определенным шинам и классам устройств, а также настроить белый список устройств.

Внимание! При включении следующих опций станции не смогут подключиться к Серверу Dr.Web:

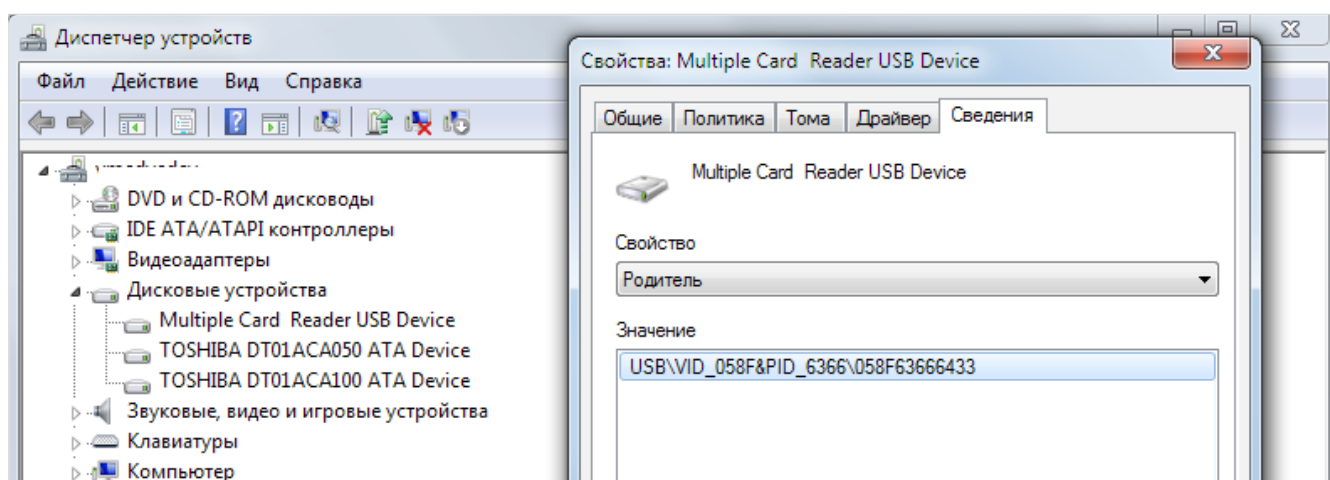
- Запрещать передачу данных по сети.**
- Контролировать доступ к следующим объектам → Классы устройств → Сетевые адаптеры.**

Данные опции запрещают всё сетевое взаимодействие для станции. При этом любое удаленное изменение настроек через Центр управления также невозможно.

Под классами устройств понимаются устройства, выполняющие одинаковые функции, например устройства для печати. Под шинами — подсистемы передачи данных между функциональными блоками компьютера, например шина USB. Можно заблокировать один или несколько классов устройств на всех шинах или заблокировать все устройства, подключенные к одной или нескольким шинам.

Определить, к какому классу относится устройство и на какой шине расположен определенный класс устройств, можно, например, с помощью **Диспетчера устройств Windows**.

- В Диспетчере устройств Windows найдите нужное устройство. При необходимости раскройте пункты указанных типов устройств. Пункт, к которому относится устройство, является классом устройства (например, флеш-накопитель относится к классу **Дисковые устройства**).
- Выберите это устройство, вызовите контекстное меню и нажмите **Свойства**.
- На вкладке **Сведения** в выпадающем списке **Свойство** выберите **Родитель**.



- В поле **Значение** будет указана строка вида *Шина\UID устройства*. Например, для флеш-накопителя будет указана строка *USB\VID_1EAB&PID_0501\03421*, где USB — это шина, на которой расположен класс устройства.

Чтобы настроить список заблокированных классов устройств:

- Убедитесь, что опция **Контролировать доступ к защищаемым объектам** включена.
- В разделе **Классы устройств** нажмите **+**, чтобы добавить устройство в список **Блокируемых классов**.


3. В открывшемся окне выберите те классы устройств, доступ к которым должен быть заблокирован. Для этого установите опцию **Запрещать** напротив соответствующего класса в приведенном списке.

Блокируемые классы	Запрещать
Адаптеры SCSI	<input type="checkbox"/>
Аудио входы и выходы	<input type="checkbox"/>
Биометрические устройства	<input type="checkbox"/>
Датчики	<input type="checkbox"/>
Дисководы гибких дисков	<input type="checkbox"/>
Дисковые устройства	<input type="checkbox"/>
Звуковые устройства	<input type="checkbox"/>
Клавиатуры	<input type="checkbox"/>
Ленточные накопители	<input type="checkbox"/>
Модемы	<input type="checkbox"/>
Мультимедийные устройства	<input type="checkbox"/>
Мыши и иные указывающие устройства	<input type="checkbox"/>
Переносные устройства Windows	<input type="checkbox"/>

4. Нажмите **Сохранить**.



5. Чтобы удалить устройство из списка, выберите его в списке и нажмите .

Чтобы настроить список заблокированных шин устройств:

1. Убедитесь, что опция **Контролировать доступ к защищаемым объектам** включена.
2. В разделе **Шины устройств** нажмите , чтобы добавить устройство в список **Блокируемых шин**.
3. В открывшемся окне выберите из выпадающего списка те шины устройств, доступ к которым должен быть заблокирован.
4. Выберите классы, которые будут заблокированы этой шине. Чтобы заблокировать шину целиком, выберите все классы.

Выберите классы, которые будут заблокированы на этой шине. Чтобы заблокировать шину целиком, выберите все классы.

Класс	<input type="checkbox"/>
Адаптеры SCSI	<input type="checkbox"/>
Аудио входы и выходы	<input type="checkbox"/>
Биометрические устройства	<input type="checkbox"/>
Датчики	<input type="checkbox"/>
Дисководы гибких дисков	<input type="checkbox"/>
Дисковые устройства	<input checked="" type="checkbox"/>
Звуковые устройства	<input type="checkbox"/>
Клавиатуры	<input type="checkbox"/>
Ленточные накопители	<input type="checkbox"/>
Модемы	<input type="checkbox"/>
Мультимедийные устройства	<input type="checkbox"/>

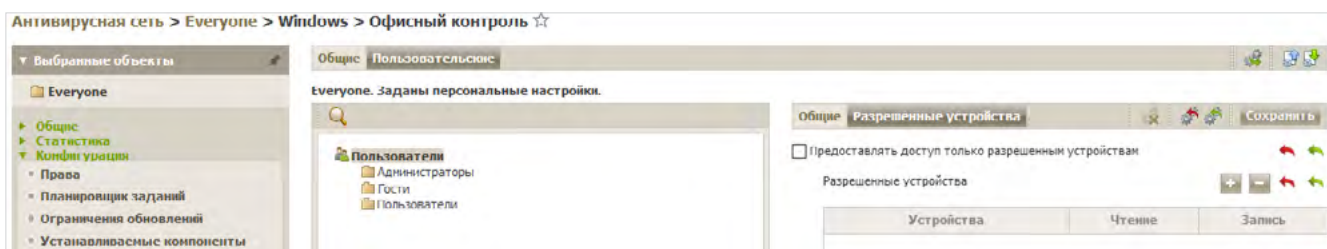
5. Нажмите **Сохранить**.
6. Чтобы удалить устройство из списка, выберите его в списке и нажмите .
7. Чтобы отредактировать список классов, заблокированных на данной шине, выберите ее в списке блокируемых шин и нажмите .

Если необходимо разрешить доступ к определенному устройству, добавьте его в белый список. В список можно добавлять любые типы устройств, в том числе устройства на съемных носителях (USB флеш-накопителях, дискетах, CD/DVD приводах, ZIP-дисках и т. п.), клавиатуры, принтеры, сетевые адаптеры и др. Также в список разрешенных можно добавить конкретное устройство, чтобы не проверять его на наличие BadUSB-уязвимости.

Можно задать правила доступа к устройствам для всех пользователей, для групп пользователей или для отдельных пользователей.

Чтобы составить общий список разрешенных устройств

1. В настройках Офисного контроля перейдите на закладку **Пользовательские**.



2. Выберите корневую группу **Пользователи**.
3. Включите опцию **Предоставлять доступ только разрешенным устройствам**. Доступ к разрешенным устройствам из общего списка предоставляется всем пользователям компьютеров, на которых установлен Dr.Web для ОС Windows.




Внимание! Опция доступна только для корневой группы **Пользователи**.

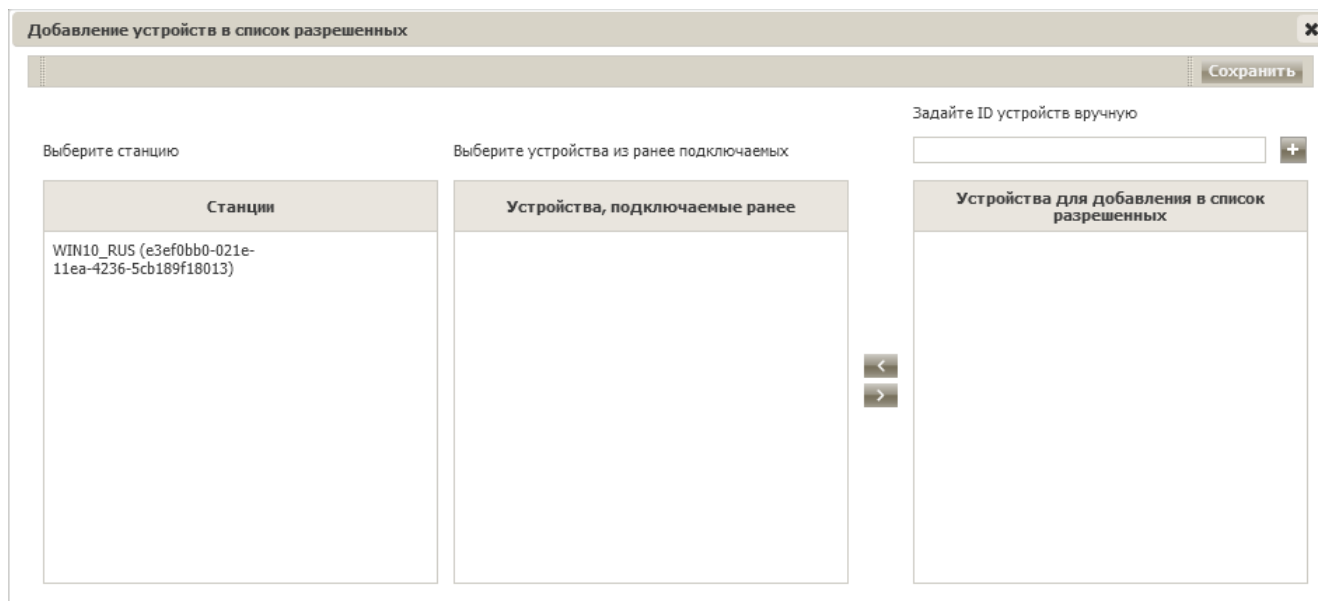
Если доступ к разрешенным устройствам предоставлен, вы можете настроить пользовательские списки разрешенных устройств.

Внимание! Добавление и удаление устройств из списка разрешенных осуществляется в настройках корневой группы **Пользователи**. При выборе членов группы Пользователи (Администраторы, Гости, Пользователи) и попытке настройки списка разрешенных устройств будет показана надпись «Добавление и удаление устройств из списка разрешенных осуществляется в настройках корневой группы Пользователи».

4. Чтобы составить пользовательские списки разрешенных устройств
 - a. Выберите соответствующую группу пользователей, пользователя, политику.
 - b. Перейдите в раздел **Разрешенные устройства**.
 - c. Если на открывшейся странице имеется надпись «Пользовательские настройки не заданы», отметьте Задать настройки.

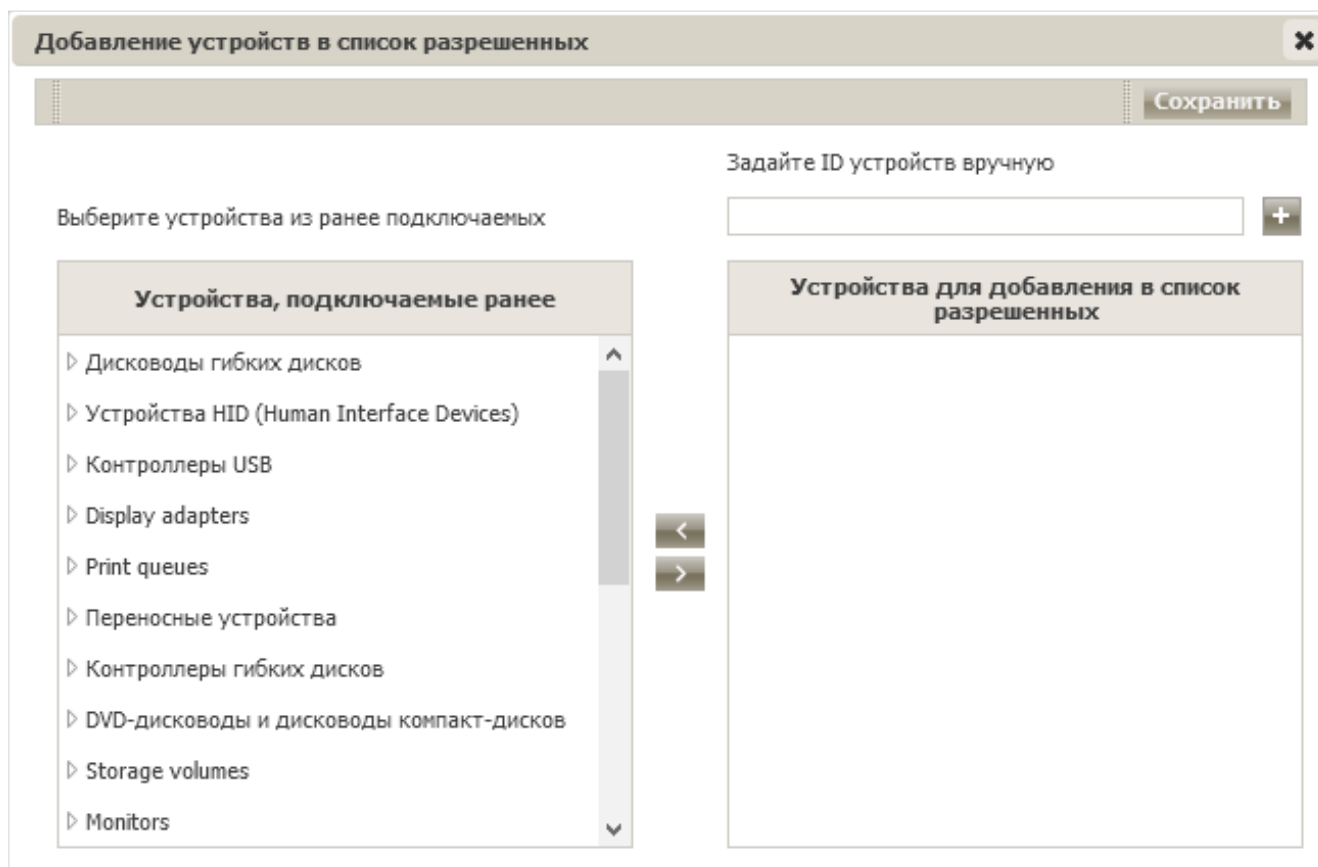


d. Нажмите кнопку , чтобы добавить устройство в список.
Если вы настраиваете разрешения для группы, то окно будет выглядеть следующим образом.



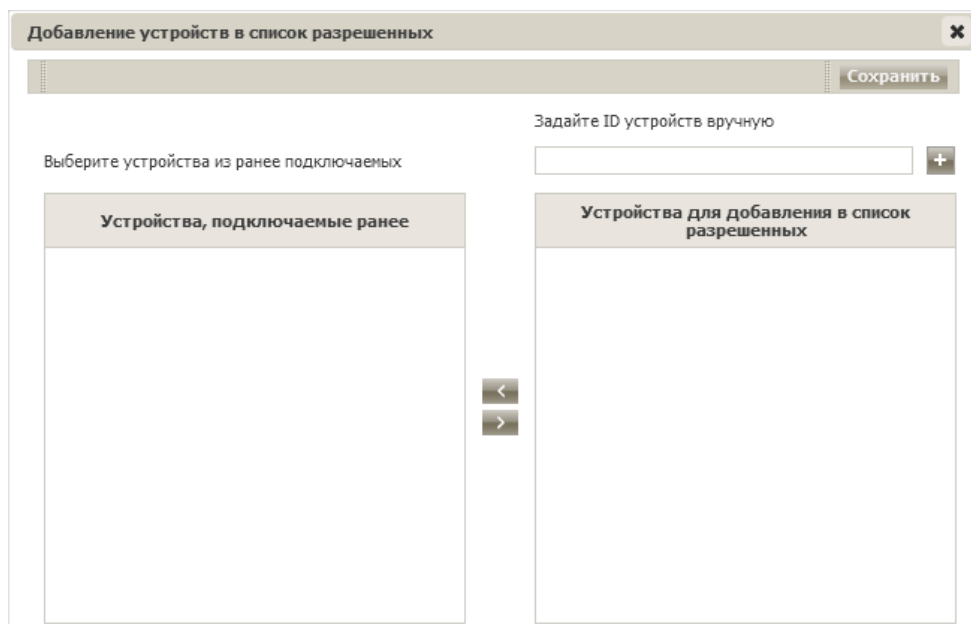
После того как будет выбрана станция группы, таблица **Устройства, подключаемые ранее** примет вид, аналогичный показанному для этой таблицы на скриншоте ниже.

Если вы настраиваете ограничения для отдельной станции, то окно будет выглядеть следующим образом.



Внимание! Список устройств, подключенных ранее, доступен только для отдельных пользователей.

Если вы настраиваете ограничения для политики, то окно будет выглядеть следующим образом.

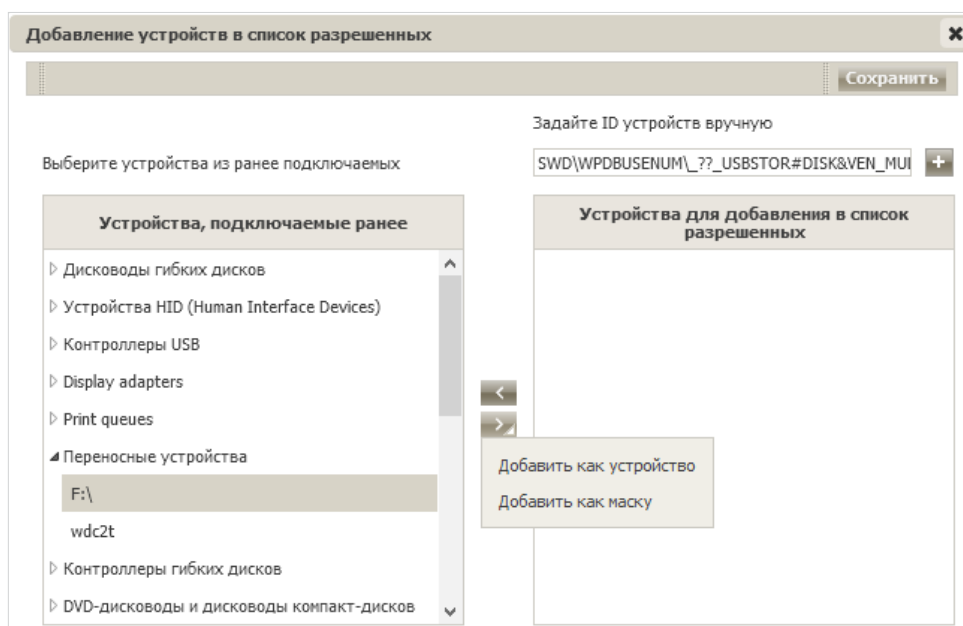



е. В окне **Добавление устройств в список разрешенных** выберите станцию, если вы настраиваете группу для получения списка подключенных ранее устройств.

Внимание! Список устройств, подключенных ранее, становится доступен после подключения станции к Серверу.

ф. Выберите устройство в поле **Устройства, подключаемые ранее**. Идентификатор устройства появится в поле **Задайте ID устройства вручную**.

С помощью стрелочки перенесите устройство в поле **Устройства для добавления в список разрешенных**. Выбранный элемент можно добавить в поле **Устройства для добавления в список разрешенных** как устройство или как маску. Маска позволяет исключить из проверки устройство, которое генерирует новый ID при каждом подключении к станции.



Вы также можете задать ID устройства вручную в соответствующем поле и нажать  для добавления его в поле **Устройства для добавления в список разрешенных**.

г. Нажмите **Сохранить**.



h. По окончании настройки нажмите на кнопку **Сохранить**. Настройки вступят в силу после подтверждения новой конфигурации станции.

i. Чтобы задать правила обращения к устройствам с собственной файловой системой, включите опцию **Чтение** для просмотра устройств и **Запись** для их изменения. Правила обращения к устройствам с собственной файловой системой можно задать только для отдельных пользователей и групп пользователей.

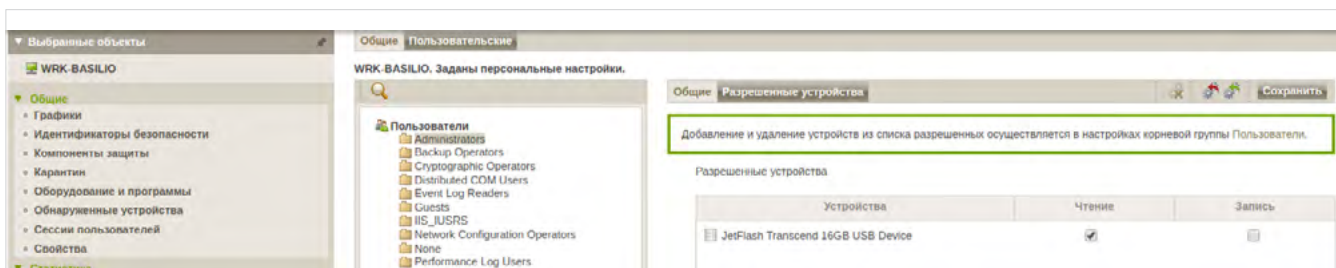
ii. Выберите пользователей в корневой группе Пользователи

iii. Перейдите в раздел **Разрешенные устройства**.


iv. Если на открывшейся странице имеется надпись «Пользовательские настройки не заданы», отметьте **Задать настройки**.



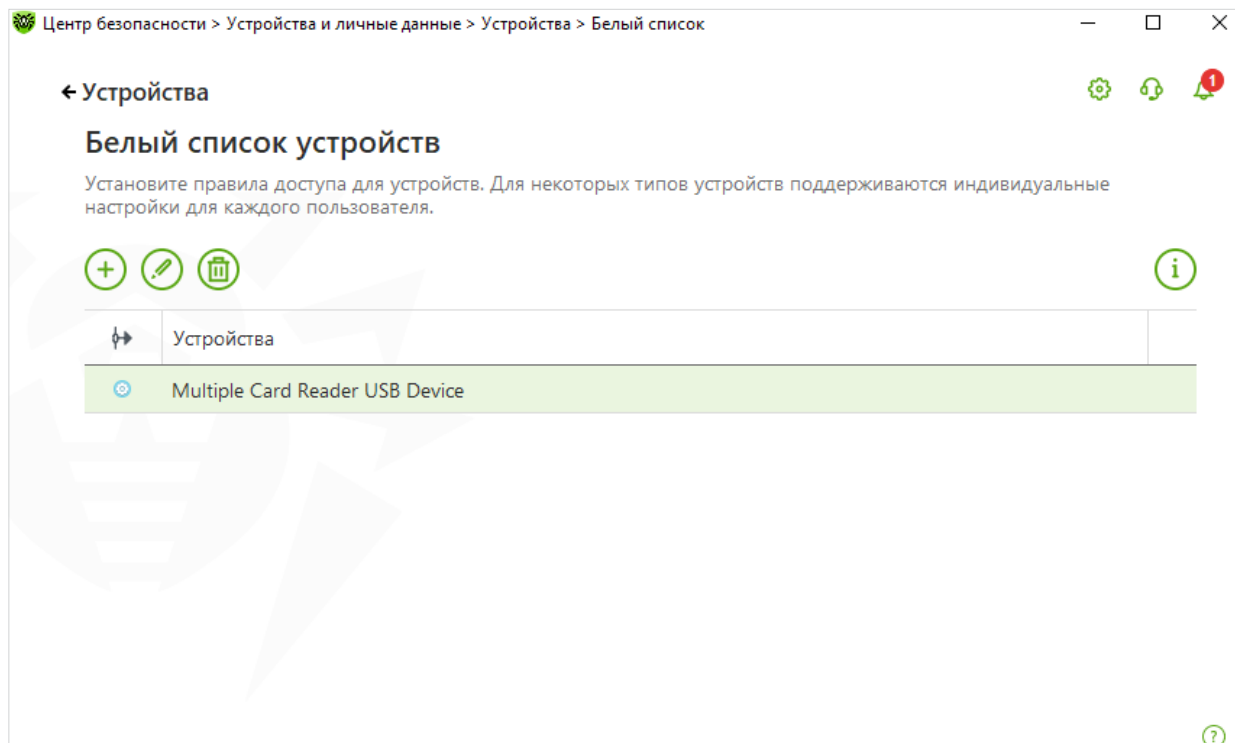
iv. Отметьте в столбцах **Чтение** и **Запись** наличие нужных прав.



v. По окончании настройки нажмите на кнопку **Сохранить**.

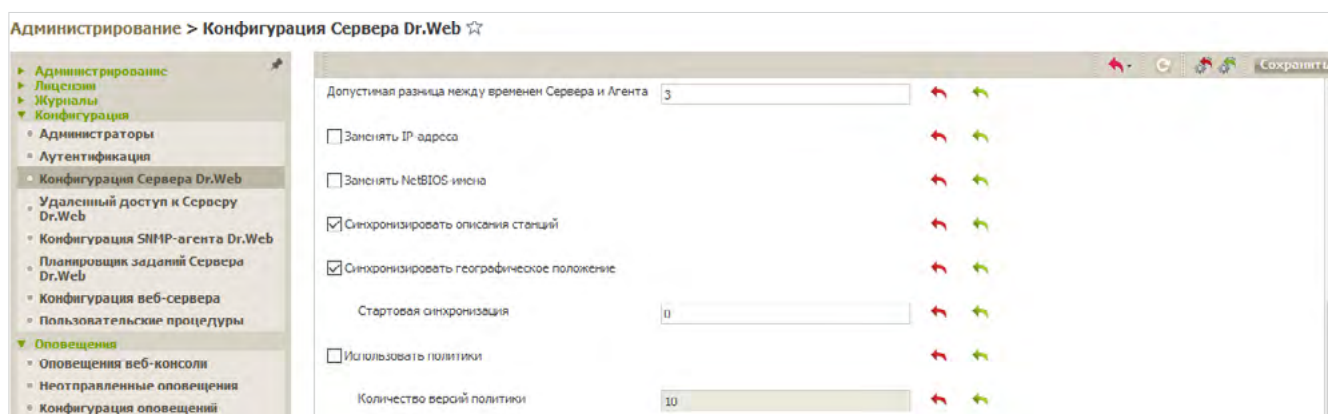
Чтобы удалить устройство из списка, выберите его в списке и нажмите  .

В случае наличия прав на изменение настроек Офисного контроля, пользователь может в дальнейшем переопределить сделанные для него настройки.



1.2. Отображение статистики заблокированных устройств в Центре управления Dr.Web Enterprise Security Suite 12.0

Для отображения информации о заблокированных устройствах последовательно перейдите **Администрирование** → **Конфигурация Сервера Dr.Web** → **Статистика** и отметьте опцию **Заблокированные устройства**. Это разрешает мониторинг информации об устройствах, заблокированных компонентом Офисный контроль, и запись информации в базу данных.



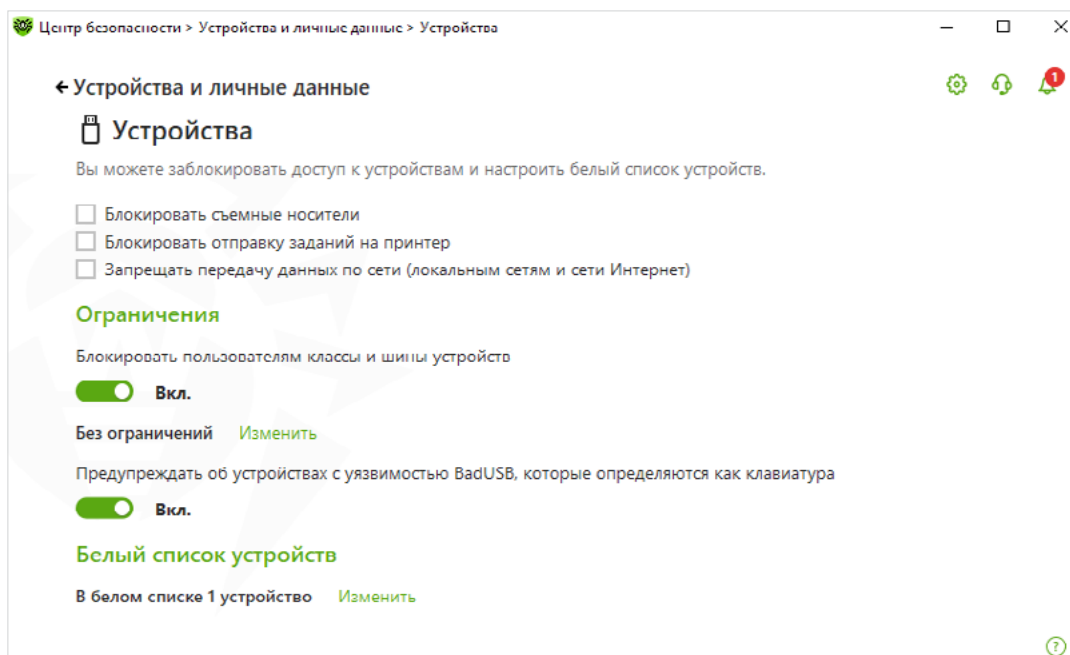
Показ информации о заблокированных устройствах осуществляется в окне **Статистика** → **Заблокированные устройства**.

1.3. Контроль доступа к сменным носителям на станциях, не управляемых из Центра управления Dr.Web Enterprise Security Suite 12.0

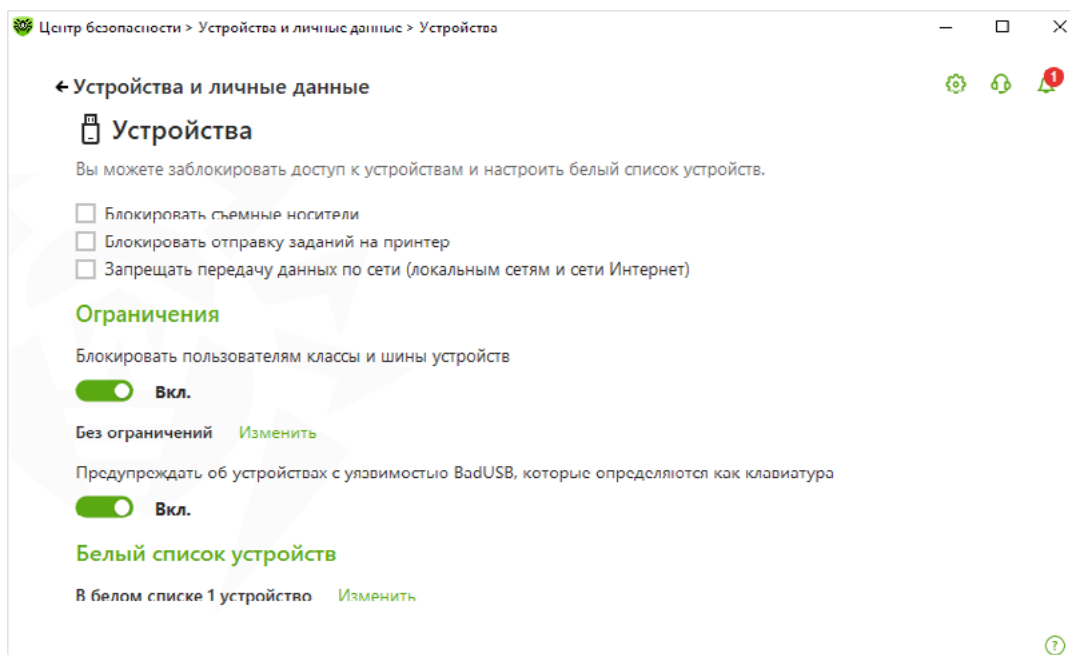
По умолчанию **Родительский контроль** включен для каждой учетной записи и работает в режиме **Без ограничений**. Для настройки модуля:

1. Кликните в трее на иконку и выберите пункт **Центр безопасности**.

2. В открывшемся окне выберите раздел **Устройства и личные данные**.



3. Для разблокировки доступа к настройкам нажмите на , значок изменит вид на .



4. Нажмите плитку **Устройства**. В окне **Устройства** вы можете ограничить доступ к определенным устройствам или шинам устройств и настроить черный и белый списки.

Класс устройства — специальный код, передаваемый устройством операционной системе, позволяющий операционной системе выбрать правильный драйвер и определить перечень функционала, предоставляемый устройством (аудиоустройства ввода/вывода, биометрические устройства, дисковые устройства, DVD/CD-ROM, дисководы, устройства GPS, камеры/фотоаппараты, инфракрасные устройства, клавиатуры, мыши и иные подобные устройства, модемы, сетевые карты, принтеры и т. д.).

Шина устройства — способ подключения к компьютеру (Bluetooth, IEEE 1394, USB, последовательный/параллельный порт, устройства чтения смарт-карт, PCMCIA, шина PCI и т. д.).

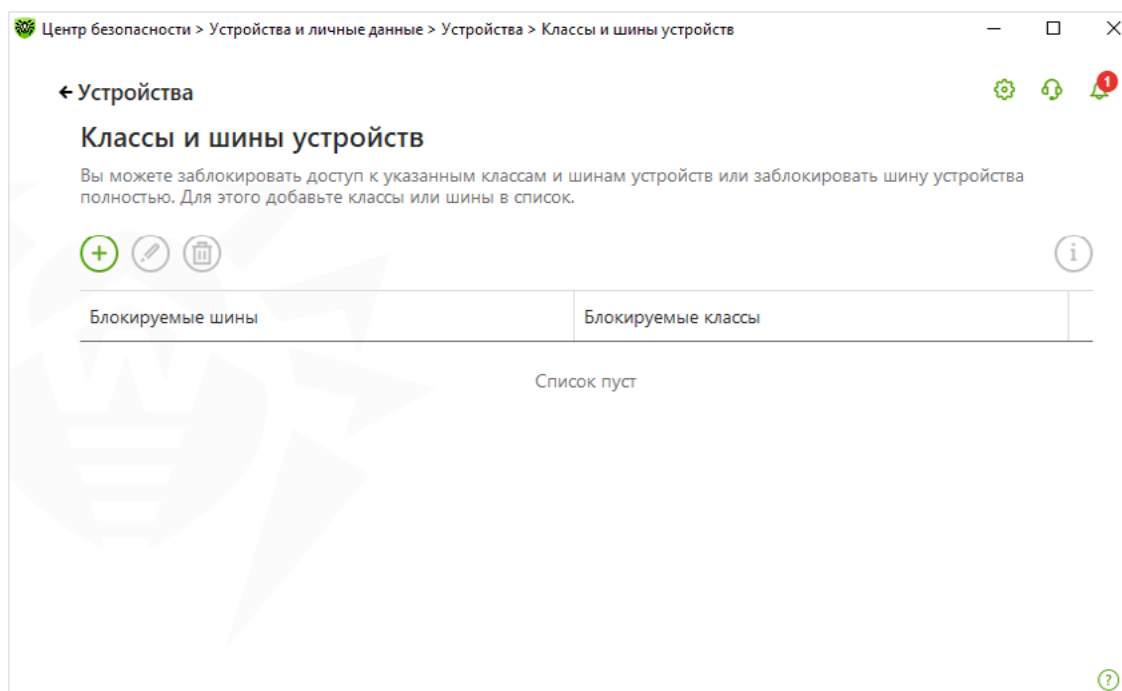
Внимание! Параметры доступа устанавливаются сразу для всех учетных записей Windows. Вы можете запретить пользователям использование всех видов сетей, установив флажок **Запрещать передачу данных по сети**, и использование принтеров флажком **Блокировать отправку заданий на принтер**.

Флажок **Блокировать сменные носители** запрещает доступ к любым типам накопителей, подключенным к портам USB. При этом если подключается мобильное устройство, то работа с ним будет возможна, но если при подключении указать его как съемный накопитель — доступ будет заблокирован.


Внимание! Большинство смартфонов, многие MP3-проигрыватели и некоторые другие устройства подключаются к компьютеру не по протоколу сменных носителей, а по протоколу MTP и, соответственно, не блокируются как сменные носители. Для блокировки таких устройств нужно в параметрах **Классов устройств** отметить флажком пункт **Переносные устройства Windows**.

5. Чтобы заблокировать доступ к выбранным классам и шинам устройств

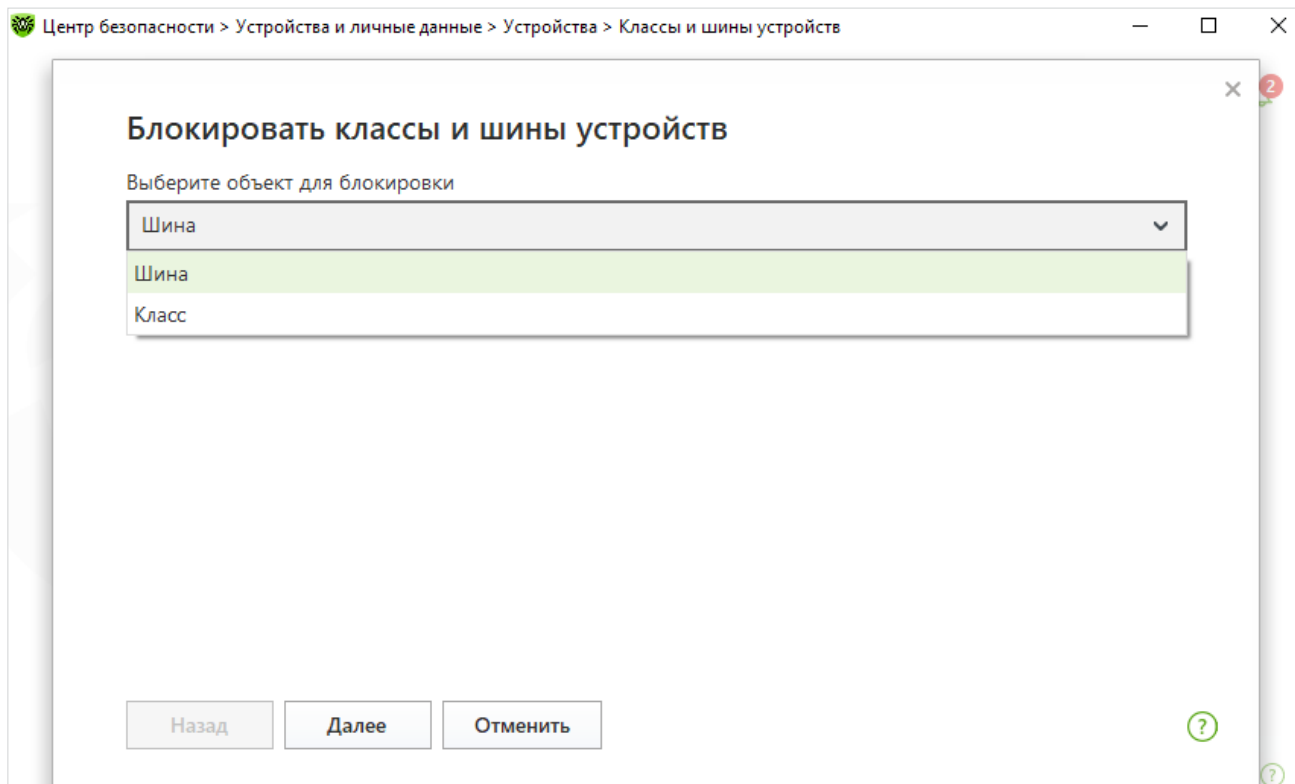
- a. Включите опцию **Блокировать пользователям классы и шины устройств** при помощи соответствующего переключателя.
- b. Нажмите кнопку **Изменить**. В открывшемся окне вы можете выбрать классы или шины устройств, доступ к которым хотите заблокировать.



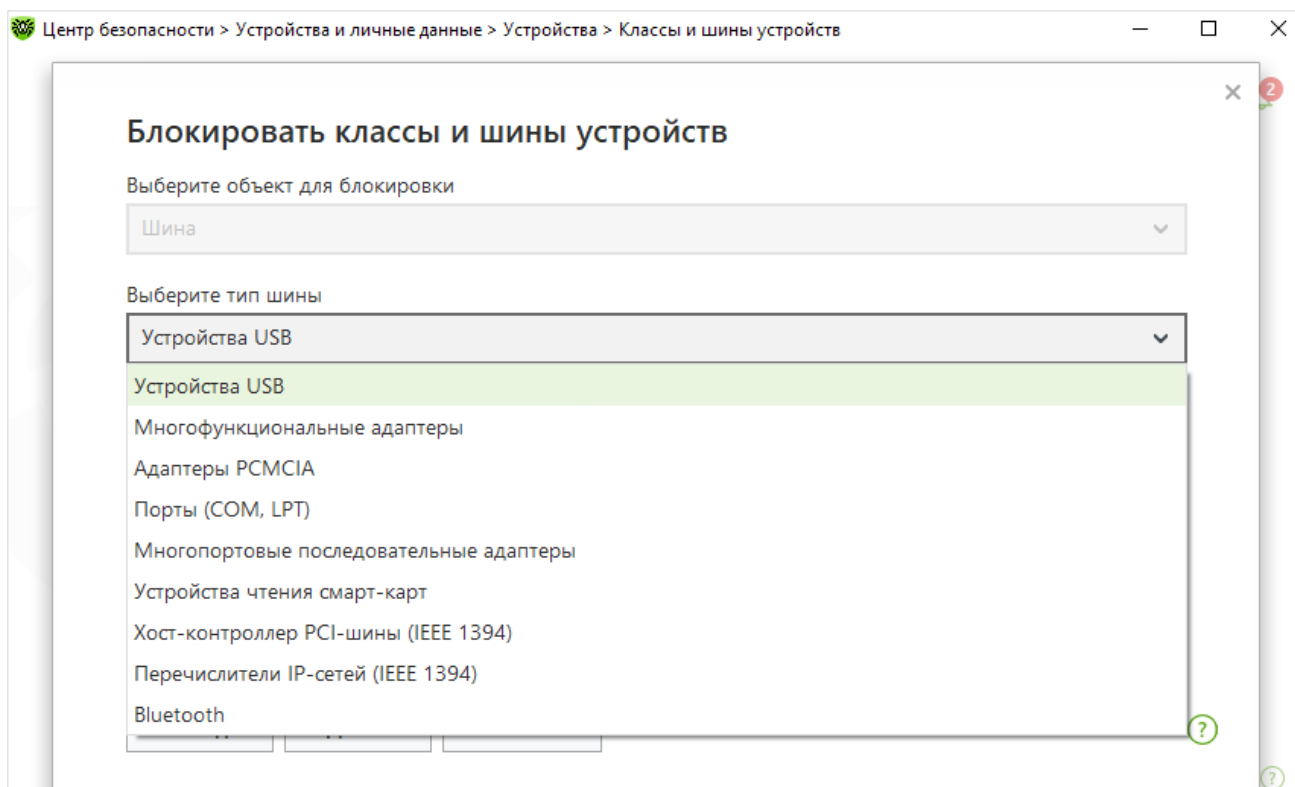
Внимание! Правила ограничения доступа классу устройств являются более приоритетными, чем отдельные правила для конкретных устройств данного типа. Например, если вы запретите доступ ко всем сменным носителям, то добавленное ранее правило для определенного флеш-накопителя перестанет действовать.

- c. Для добавления шины полностью или некоторого устройства на определенной шине в список используйте .

Если вы хотите заблокировать шину, то из выпадающего списка выберите **Шина** и нажмите **Далее**.

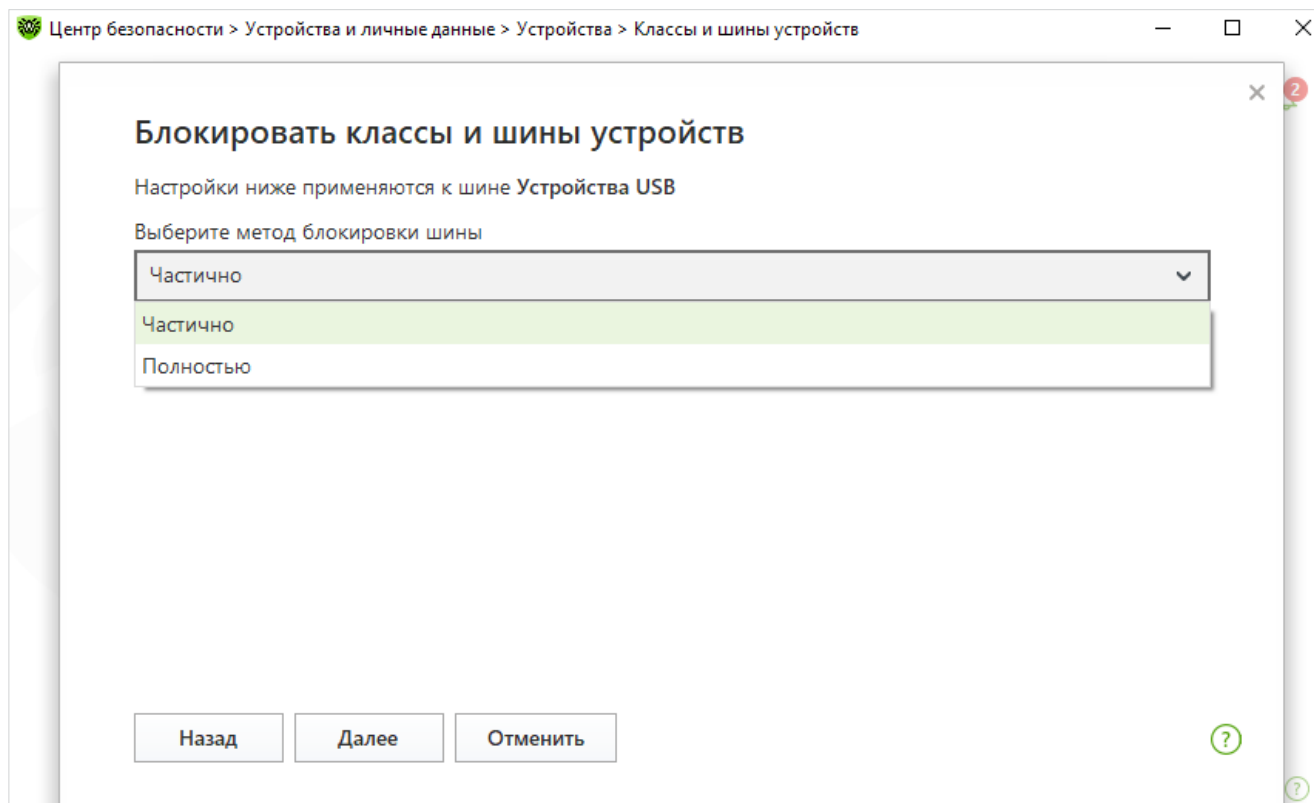


Выберите тип шины и нажмите **Далее**.

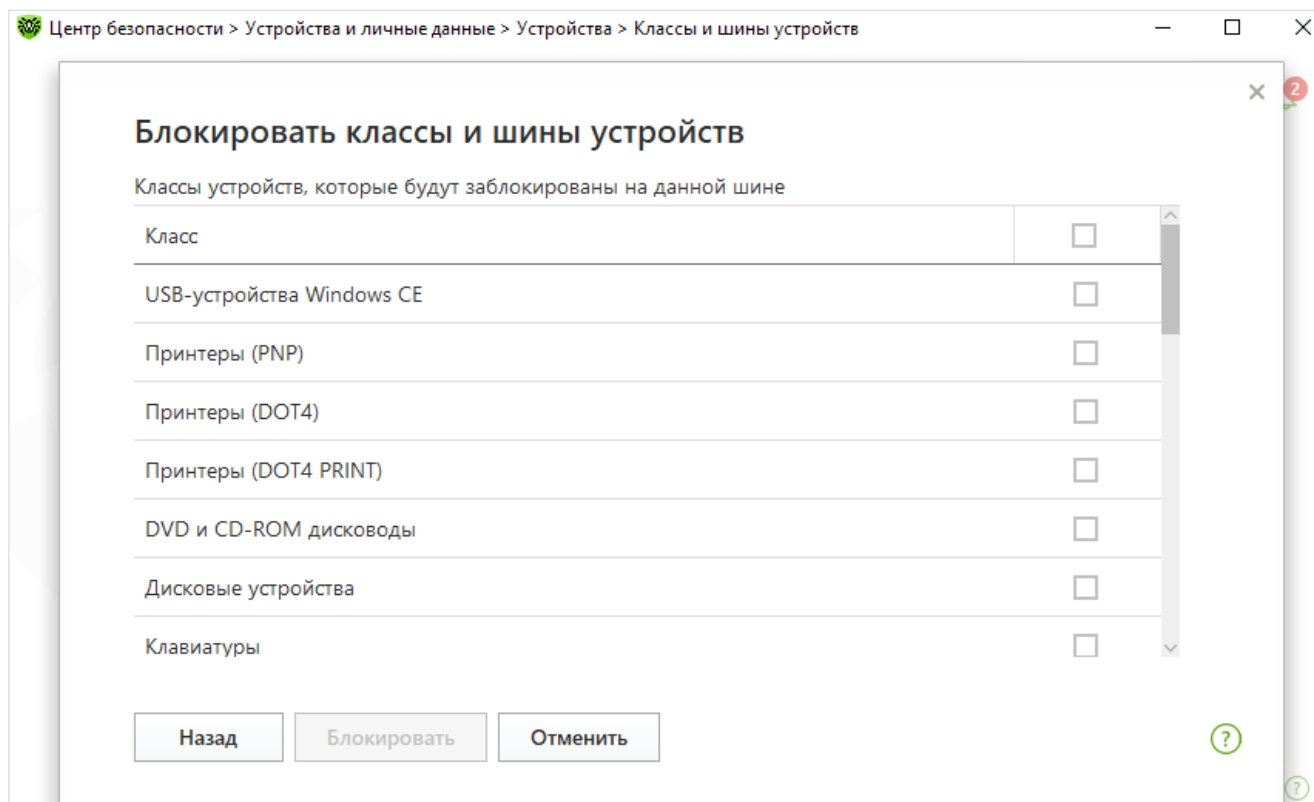


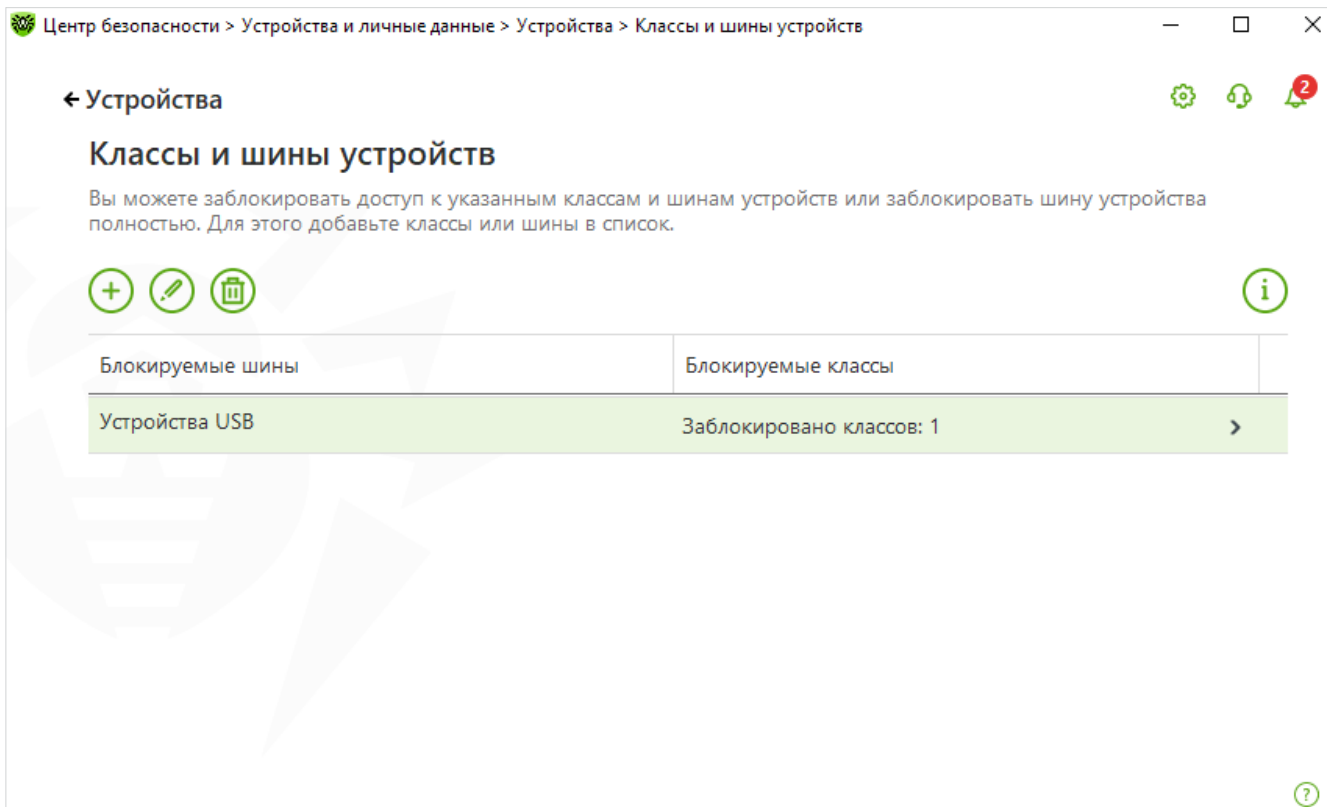
Выберите тип блокировки (**Полностью** — будут заблокированы все классы устройств

на данной шине или **Частично** — откроется окно выбора классов устройств для блокировки на данной шине) и нажмите **Далее**.




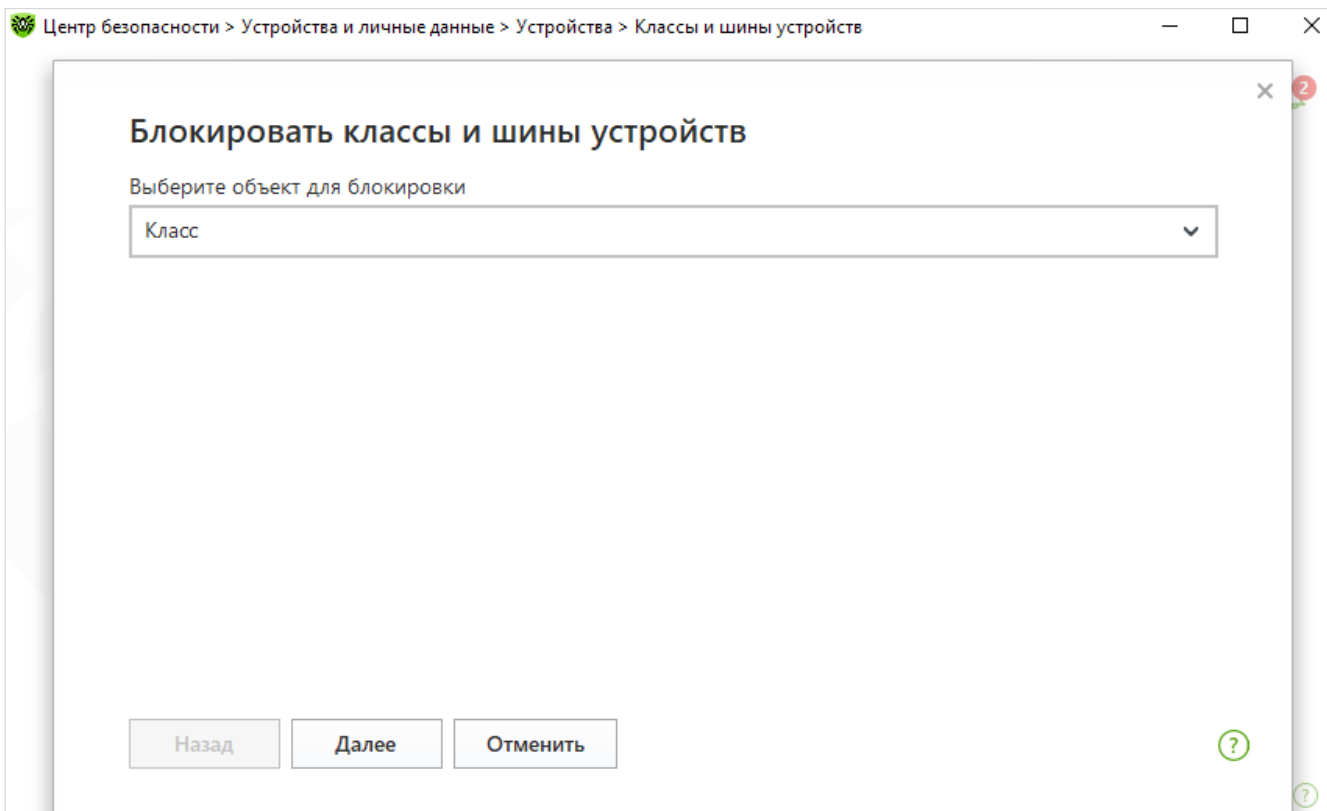
Отметьте классы из списка, которые вы хотите заблокировать. Нажмите **Блокировать**.



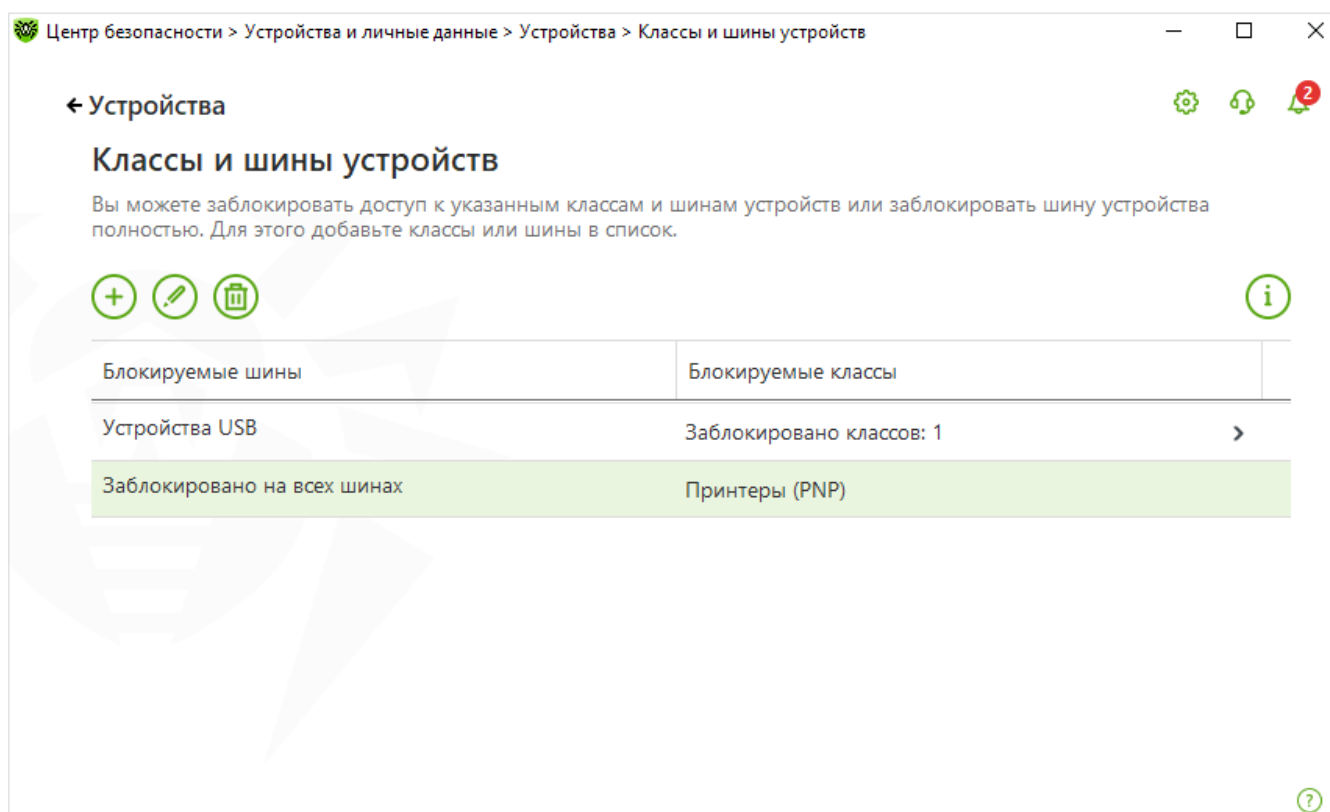
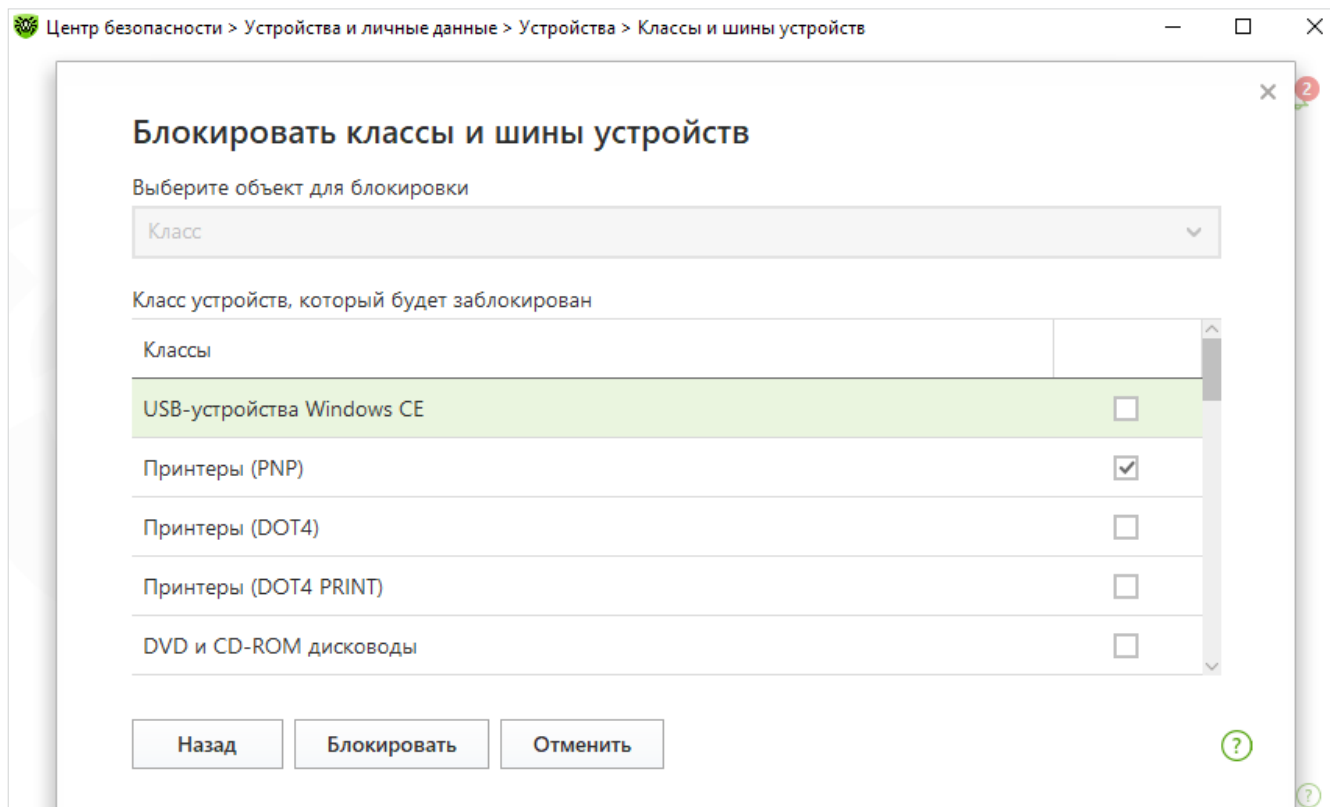


Внимание! При блокировке шины USB-клавиатура и мышь вносятся в исключения.

Чтобы заблокировать один или несколько классов устройств, нажмите кнопку . В открывшемся окне из выпадающего списка выберите **Класс** и нажмите **Далее**.

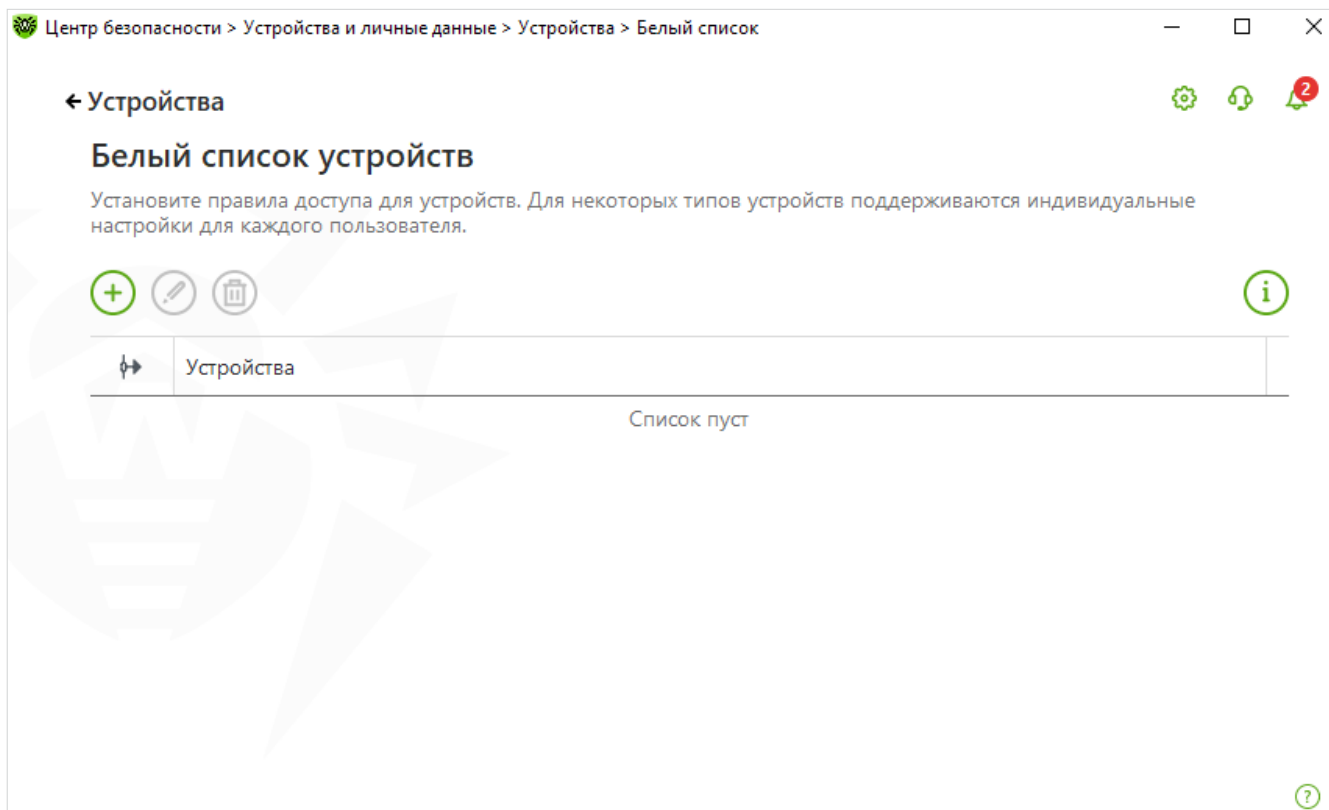


Отметьте те классы из списка, которые вы хотите заблокировать. Нажмите **Блокировать**.



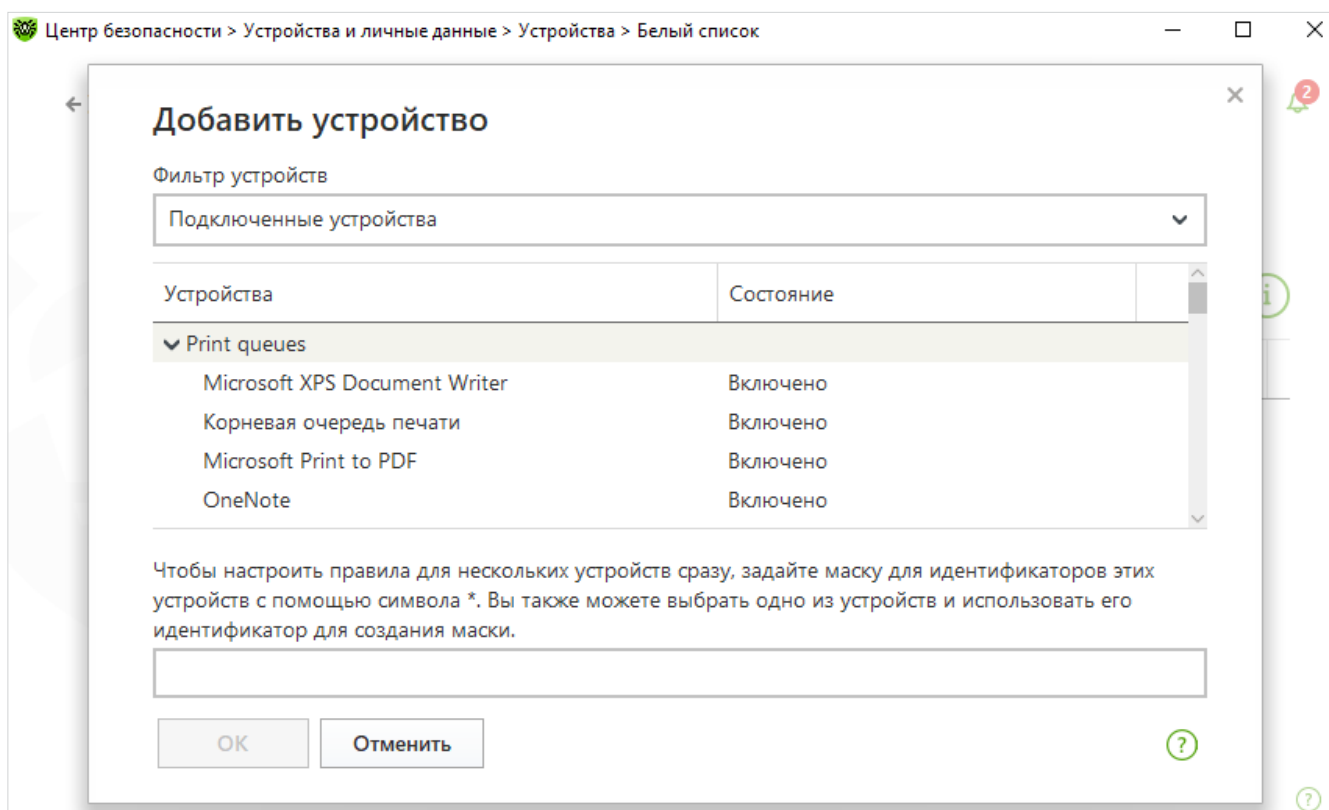
Внимание! При активации блокировки уже подключенного устройства требуется либо подключить устройство заново, либо перезагрузить компьютер. Блокировка работает только для устройств, подключенных после активации функции.

Для формирования белого списка устройств в группе настроек **Белый список устройств** нажмите кнопку **Изменить**.

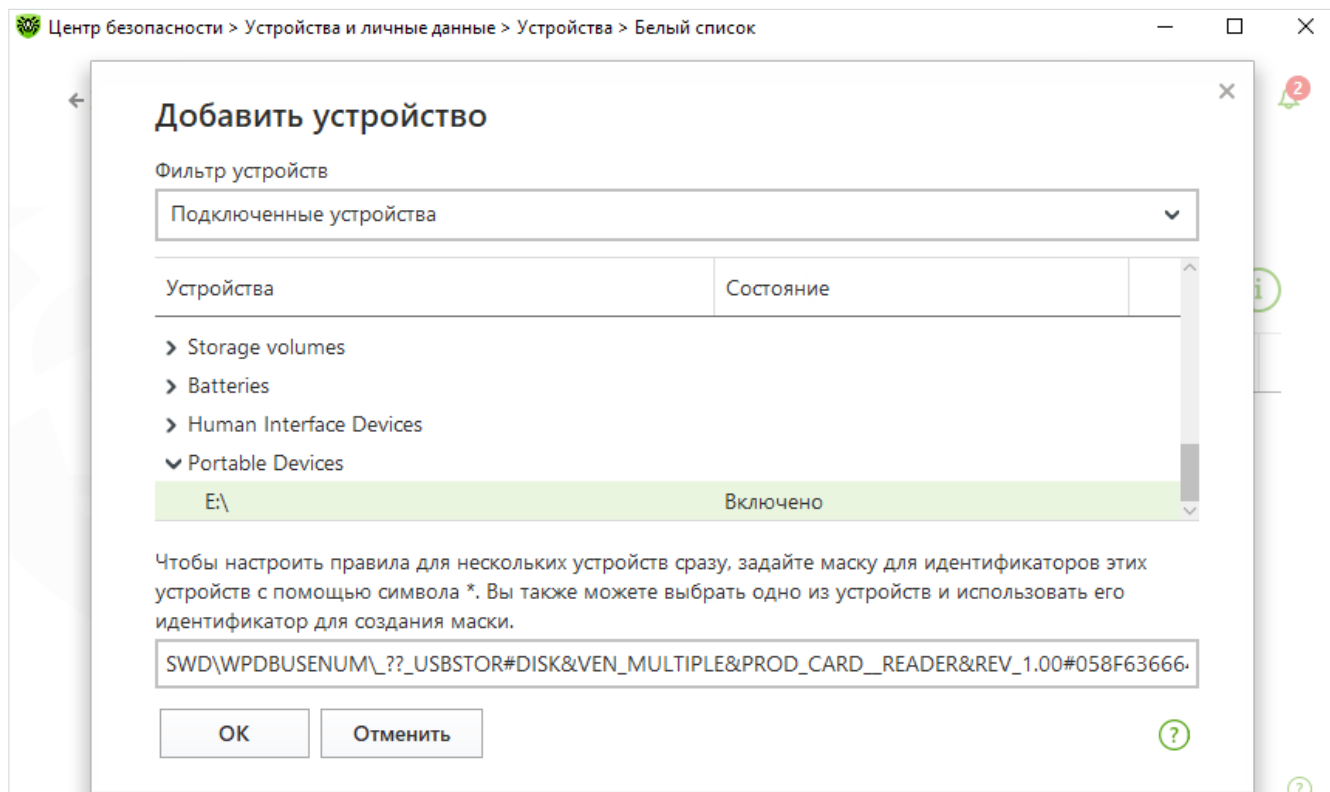


Окно **Белый список устройств** содержит информацию обо всех устройствах, добавленных в белый список.

Для добавления устройства в белый список подключите его к компьютеру и нажмите **+**.



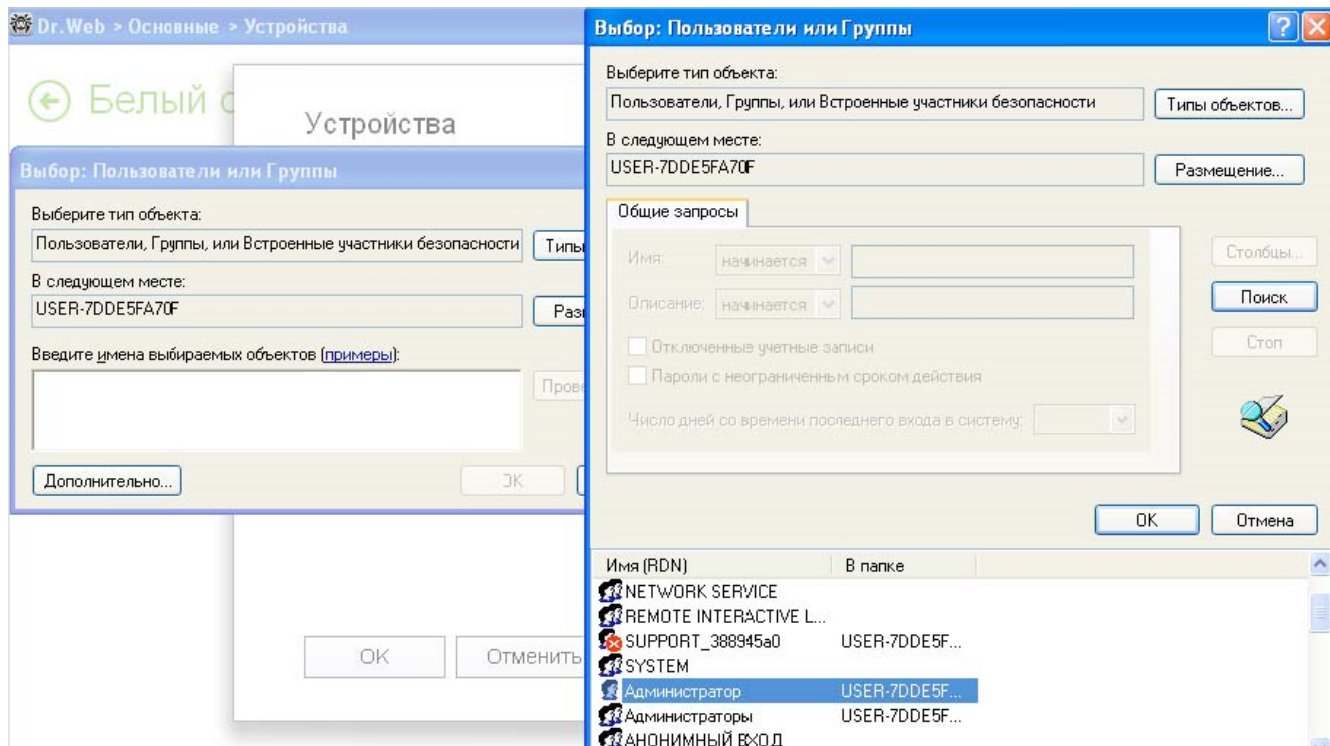
В открывшемся окне нажмите кнопку **Обзор** и выберите нужное устройство. В выпадающем списке выберите показ только подключенных или только отключенных устройств.

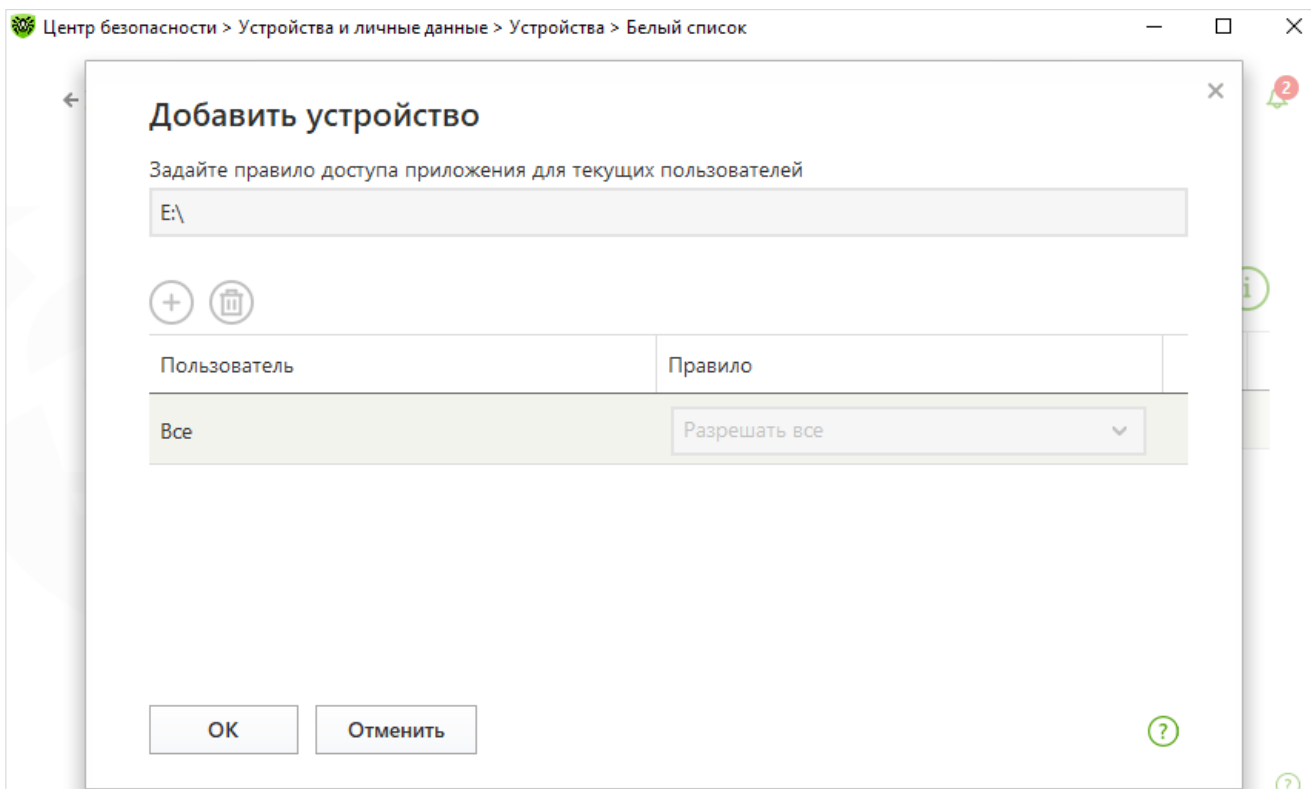


Нажмите кнопку **OK**.

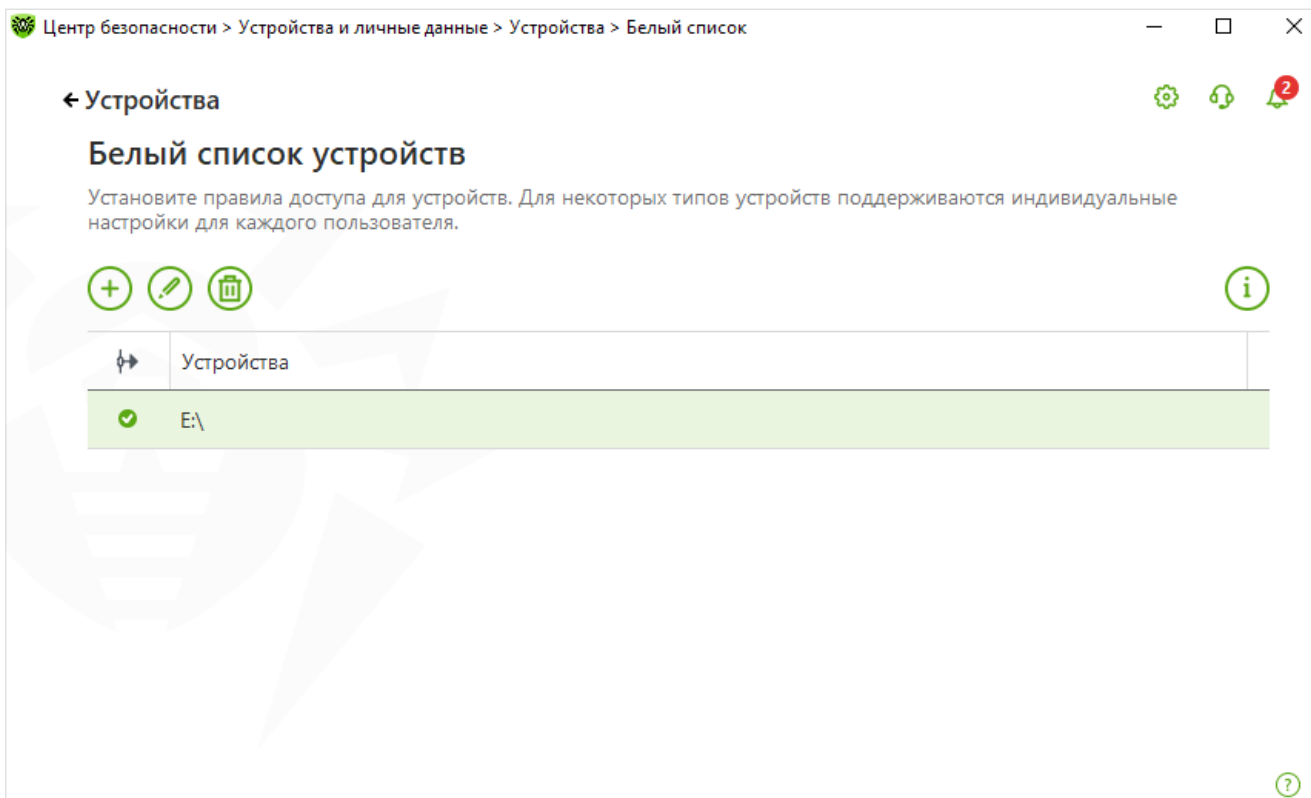
Для устройств с файловой системой вы можете настроить правила доступа. Для этого в столбце **Правило** выберите один из режимов: **Разрешать все** или **Только чтение**.

Чтобы добавить новое правило для конкретного пользователя, нажмите **+**, **Поиск** и выберите необходимого пользователя.





Нажмите кнопку **OK**.



О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании.

Вот только некоторые клиенты Dr.Web: <https://customers.drweb.com>.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

«Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.

Dr.Web сертифицирован на отсутствие недеklarированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.

Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).

Использование ПО Dr.Web позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:

- информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);
- отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	Сертификаты Минобороны России	Сертификаты ФСБ России	Все сертификаты и товарные знаки
--	---	--	--

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.



© ООО «Доктор Веб»,
2003–2019

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 495 789–45–87 (многоканальный)
Факс: +7 495 789–45–97

<https://антивирус.рф> | <https://www.drweb.ru> | <https://curenet.drweb.ru> | <https://free.drweb.ru>