# Программное обеспечение «Базис.WorkPlace Security»

# Руководство пользователя

RU.НРФЛ.00003-01.94.01

Москва

18.07.2023

# Содержание

# Термины и определения

Ниже приведены термины, используемые в документе, и их определения:

**Администратор**: пользователь ПО «Базис.WorkPlace Security», уполномоченный выполнять некоторые действия по администрированию «Базис.WorkPlace Security» (имеющий административные полномочия) в соответствии с установленной ролью и имеющимися привилегиями в «Базис.WorkPlace Security» на выполнение этих действий. В данном документе не различаются понятия "администратор" и "пользователь с ролью «Администратор».

**Администратор безопасности:** пользователь с ролью «Администратор», на которого возложена ответственность за обеспечение требований безопасности при функционировании системы, в которой установлено ПО «Базис.WorkPlace Security».

**Аудитор:** пользователь с ролью «Администратор», имеющий ограниченные административные полномочия, которые позволяют ему запускать Сервис управления и администрирования и работать с журналами регистрации ПО «Базис.WorkPlace Security».

**Аутентификационная информация [информация аутентификации]:** информация, используемая для установления подлинности (верификации) субъекта доступа.

**Аутентификация:** проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа).

**Виртуальная машина:** вычислительная система, эмулируемая с помощью технологии виртуализации, в которой установлена гостевая операционная система и обеспечивается выполнение прикладного программного обеспечения.

**Временный файл:** файл, создаваемый операционной системой или иным программным обеспечением для сохранения промежуточных результатов в процессе функционирования или передачи данных другому программному обеспечению.

**Гостевая операционная система:** операционная система, установленная на виртуальной машине.

**Идентификатор:** представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа.

**Идентификация:** присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

**Информационная система:** совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**Компонент программного обеспечения:** составная часть программного обеспечения, выполняющая определенную функцию.

**Контейнер (контуры безопасности):** изолированные друг от друга среды ПО «Базис.WorkPlace Security», в каждой из которой могут независимо выполняться системные процессы и процессы пользователей «Базис.WorkPlace Security».

**Локальный доступ:** доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети).

**Многофакторная аутентификация:** аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации.

**Непривилегированная учетная запись:** учетная запись пользователя (процесса, выполняемого от его имени).

**Непривилегированный субъект доступа:** процесс, порождаемый пользователем.

**Неуполномоченный субъект доступа:** процесс, порождаемый лицами, не являющимися пользователями «Базис.WorkPlace Security», при попытке несанкционированного доступа.

**Объект доступа:** единица информационного ресурса (файл, каталог, том, устройство и (или) иные), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

**Пароль:** конфиденциальный набор символов, используемый субъектом доступа для аутентификации в системе.

**Пользователь:** пользователь «Базис.WorkPlace Security», не имеющий административных полномочий.

**Пользователь «Базис.WorkPlace Security»:** лицо (администратор, пользователь), которому разрешено выполнять некоторые действия (операции) по администрированию «Базис.WorkPlace Security» или обработке информации в «Базис.WorkPlace Security».

**Привилегированная учетная запись:** учетная запись администратора.

**Привилегированный субъект доступа:** процесс, порождаемый администратором или от имени служебной учетной записи «Базис.WorkPlace Security».

**Рабочий стол:** основное окно графической среды пользователя, реализуемое «Базис.WorkPlace Security» (в т.ч. - гостевой «Базис.WorkPlace Security» виртуальной машины).

**Роль:** предопределенная совокупность правил, устанавливающих допустимое взаимодействие с «Базис.WorkPlace Security».

**Субъект доступа:** процесс, порождаемый пользователем «Базис.WorkPlace Security» (пользователем или администратором).

**Терминал (терминальная станция):** идентифицированное аппаратное обеспечение средства вычислительной техники, на котором выполняется компонент «Базис.WorkPlace Security» «Базис - Терминал».

**Техническое средство:** аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации.

**Удаленный доступ:** процесс получения доступа (через внешнюю сеть) к объектам доступа из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

**Уполномоченный непривилегированный субъект доступа:** процесс, порождаемый пользователем в соответствии с правами доступа к объекту доступа.

**Уполномоченный привилегированный субъект доступа**: процесс, порождаемый администратором или от имени служебной учетной записи в соответствии с ролью.

**Управление доступом:** ограничение и контроль доступа субъектов доступа к объектам доступа в соответствии с установленными правилами разграничения доступа.

**Целостность информации:** свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

# Перечень сокращений

В документе использованы следующие сокращения:

| | | |
|---|---|---|
| АРМ | – | автоматизированное рабочее место |
| «Базис.WorkPlace Security» | – | программное обеспечение «Базис.WorkPlace Security» |
| ВМ | – | виртуальная машина |
| ИС | – | информационная система |
| ИТ | – | информационная технология |
| НСД | – | несанкционированный доступ |
| ОС | – | операционная система |
| ПЗ | – | профиль защиты |
| ПК | – | программный компонент (основная часть «Базис.WorkPlace Security») |
| ПО | – | программное обеспечение |
| ПРД | – | правила разграничения доступа |
| ПО | – | программное обеспечение |
| РД | – | руководящий документ |
| СВТ | – | средства вычислительной техники |
| СЗИ | – | средство защиты информации |
| ТУ | – | технические условия RU.НРФЛ.00003-01 90 01 |
| ЦОД | – | центр обработки данных |
| ACL | – | Access Control List или ACL, список управления доступом |
| RDP | – | Remote Desktop Protocol, протокол удалённого рабочего стола. |

# Введение

Идентификационные данные программного обеспечения (ПО):

| **Идентификационные данные ПО** | **Программа для ЭВМ «Базис.WorkPlace Security»** |
|---|---|
| Название документа | Программное обеспечение «Базис.WorkPlace Security». Руководство пользователя |
| Версия документа | 2.0 |
| Обозначение документа | RU.НРФЛ.00003-01.94.01 |
| Автор документа | ООО «БАЗИС» |
| Уровень доверия | ПО «Базис.WorkPlace Security» соответствует 4 уровню доверия в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденными приказом ФСТЭК России от 2 июня 2020 г. № 76. |

# Общие сведения

Программное обеспечение «Базис.WorkPlace Security» предназначено для защиты информации от несанкционированного доступа (НСД) в вычислительных сетях и информационных системах посредством создания распределенной безопасной среды терминального доступа к рабочим столам гостевых операционных систем, выполняющихся на виртуальных машинах (ВМ) в центре обработки данных (ЦОД).

«Базис.WorkPlace Security» является средством защиты информации, не содержащей сведений, составляющих государственную тайну.

Документ предназначен для непривилегированных пользователей ПО «Базис.WorkPlace Security» и содержит базовые инструкции по работе пользователей с компонентом «Базис - Терминал» на автоматизированном рабочем месте (терминале).

# Назначение, состав и функциональные возможности программного обеспечения

«Базис.WorkPlace Security» представляет собой программное обеспечение, которое выполняет функции защищенной системы терминального доступа к рабочим столам клиентских операционных систем, поддерживающих протокол RDP.

«Базис.WorkPlace Security» предназначено для функционирования на физических или виртуальных серверах и рабочих станциях в составе вычислительной сети. Целью использования «Базис.WorkPlace Security» является создание эффективной территориально распределенной безопасной инфраструктуры рабочих мест пользователей компании.

ПО «Базис.WorkPlace Security» состоит из следующих основных частей – программных компонентов (ПК):

- программный компонент «Базис - Сервер безопасности» (выполняется на сервере ЦОД);
- программный компонент «Базис - Терминал» (выполняется на автоматизированном рабочем месте (терминале) пользователя).

ПО «Базис.WorkPlace Security» имеет следующие базовые функциональные возможности:

- подключение автоматизированного рабочего места (АРМ) пользователя к платформе виртуализации вычислительных ресурсов с использованием терминального доступа к рабочим столам гостевых операционных систем, поддерживающих протокол RDP (установление VDI-сессии);
- реализация возможности работы пользователя АРМ с локальными приложениями, разработанными и предназначенными для функционирования в операционных системах семейства Linux;
- реализация возможности работы пользователя АРМ в различных контурах безопасности - изолированных друг от друга программных средах, в каждой из которой могут независимо выполняться процессы пользователей на АРМ, и имеющих возможность подключения к различным сегментам вычислительной сети, отличающимися политиками безопасности. Изолированность подразумевает невозможность передачи информации между контурами;
- централизованное управление (администрирование) пользователями и АРМ.

ПО «Базис.WorkPlace Security» имеет следующие базовые функции безопасности:

- идентификация и аутентификация пользователей и терминалов;
- управление доступом к объектам доступа;
- фильтрация сетевого потока на основе определения параметров сетевых интерфейсов, разрешенных для взаимодействия по сетевому интерфейсу;
- контроль целостности программного обеспечения;
- регистрация событий безопасности;
- обеспечение безопасности при работе пользователя в различных контурах безопасности;
- обеспечение безопасности при работе с периферийными устройствами и съемными носителями.

# Программный компонент «Базис - Терминал»

ПК «Базис - Терминал» представляет собой программное обеспечение, устанавливаемое на АРМ пользователя, в качестве которого может выступать персональный компьютер или терминальная станция, и не требующее для своего функционирования дополнительного программного обеспечения.

ПК «Базис - Терминал» управляет работой АРМ пользователя, обеспечивает работу его локальных приложений (программного обеспечения, разработанного для семейства ОС Linux) и работу удаленных виртуальных рабочих столов (клиента терминального доступа).

ПК «Базис - Терминал» реализует следующие функции:

- идентификация и аутентификация пользователей и АРМ;
- запуск локальных приложений и/или установление VDI-сессии с виртуальной инфраструктурой ЦОД;
- формирование пользовательского окружения;
- поддержка работы независимых изолированных контуров безопасности, обмен информацией между которыми невозможен;
- контроль целостности программных модулей компонента;
- управление доступом субъектов доступа к объектам доступа.

# Программный компонент «Базис - Сервер безопасности»

ПК «Базис - Сервер безопасности» представляет собой программное обеспечение, устанавливаемое на физический или виртуальный сервер ЦОД, и не требующее для своего функционирования дополнительного программного обеспечения.

ПК «Базис - Сервер безопасности» управляет доступом пользователей к рабочим столам гостевых операционных систем виртуальных машин ЦОД и обеспечивает централизованное управление инфраструктурой пользовательских АРМ.

ПК «Базис - Сервер безопасности» реализует следующие функции:

- аутентификация и идентификация пользователей, АРМ и контуров безопасности;
- настройка и хранение учетных записей пользователей, АРМ и других ресурсов в единой базе учетных данных;
- управление подключением АРМ пользователей к рабочим столам гостевых операционных систем;
- администрирование пользователей, АРМ и управление их работой, в том числе управление доступом пользователей к АРМ, контурам безопасности и другим ресурсам;
- сбор и обработка журналов регистрации событий безопасности.

# Работа пользователя на АРМ (терминале)

Условия выполнения программы, технические требования к аппаратным средствам АРМ (терминала), процедура установки и настройки ПО «Базис.WorkPlace Security» на технические средства рассмотрены в документе «ПО «Базис.WorkPlace Security». Руководство по установке. RU.НРФЛ.00003-01 96 01». В данном документе рассмотрена только работа пользователя на АРМ (терминале).

## Вход в систему

Для входа в систему пользователь должен выполнить следующие действия:

- подключить персональный идентификатор (токен) к АРМ (при его наличии);
- включить АРМ, дождаться окончания загрузки ПК «Базис - Терминал» и появления запроса данных для входа в систему. Если на экране появилось сообщение «Не удалось установить соединение с сервером», то необходимо обратиться к Администратору безопасности и следовать его указаниям;
- ввести Имя пользователя и Пароль в соответствующие поля формы и нажать ОК (Рисунок 1);

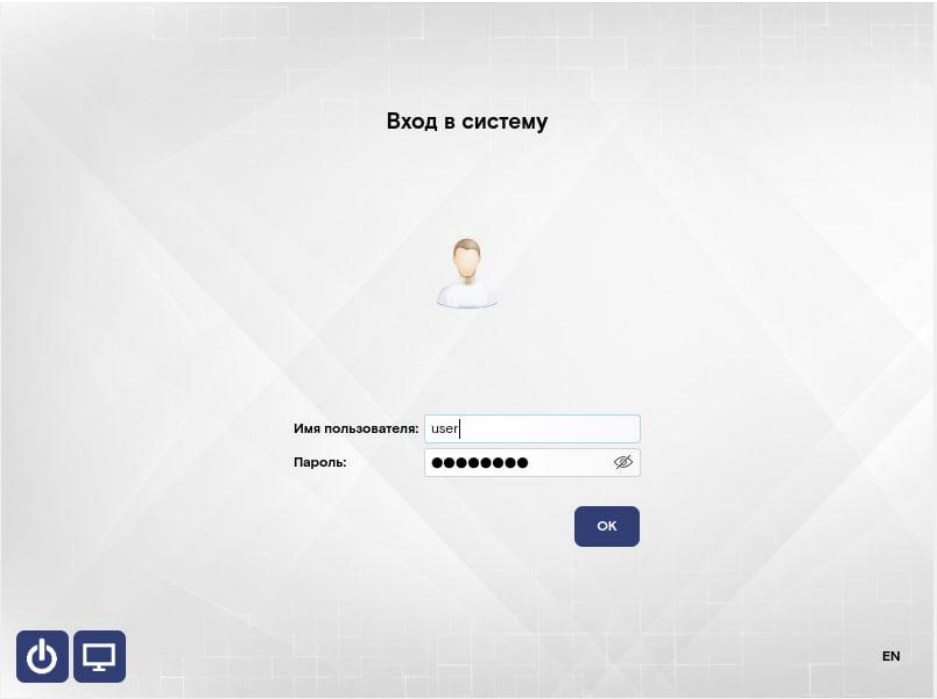



Рисунок 1. Форма входа в систему

- если пин-код для токена отличается от пароля пользователя, то ввести пин-код в Конфигурации терминала;

Если Имя пользователя и Пароль были введены неверно, то появится сообщение «Ошибка аутентификации пользователя. Проверьте логин и пароль". Для повторной попытки аутентификации необходимо нажать на кнопку ОК.

После корректного ввода Имени пользователя и Пароля происходит вход в систему (Рисунок 2).


Рисунок 2. Успешный вход в систему

# Работа с контурами безопасности и приложениями

После того, как пользователь выполнит успешный вход в систему, на мониторе отобразится Панель управления со списком контуров безопасности (вкладка «Контуры»), доступных для данного пользователя (Рисунок 3).

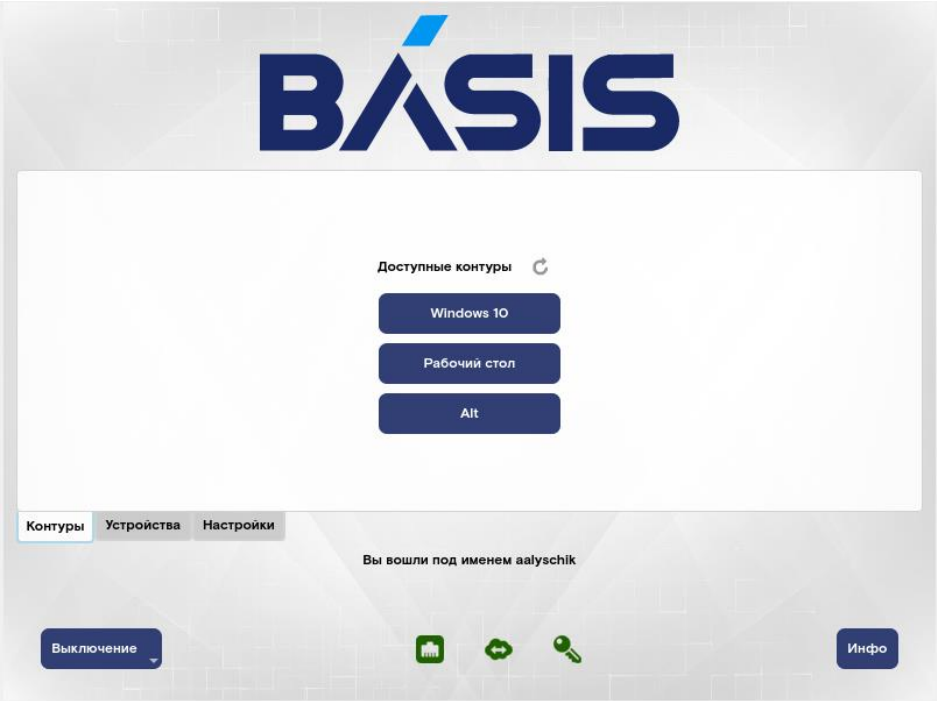



Рисунок 3. Панель управления со списком контуров безопасности

В данной форме пользователь может выбрать любой доступный ему контур, при этом на экране отобразится рабочий стол с приложениями, доступными ему в данном контуре.

Кроме переключения между контурами, данная форма Панели управления позволяет:

- наблюдать сетевой статус АРМ;
- управлять работой подключенных к АРМ устройств (вкладка «Устройства»);
- изменять масштаб изображения экрана (вкладка «Настройка»);
- завершать, перезагружать или блокировать работу АРМ (кнопка «Выключение» в нижней части формы).

Панель управления может быть вызвана при работе пользователя в активном контуре (при активном рабочем столе клиентской ОС), для этого необходимо одновременно нажать комбинацию клавиш: **Ctrl+Alt+0** и выбрать в нижней части экрана кнопку «Меню» (Рисунок 6). Также доступен вызов Панели управления по нажатию **Ctrl+Alt+Click** в нижней части экрана (2 нижних пикселя).

## Индикация сетевого статуса АРМ

В нижней части Панели управления отображается индикация сетевого статуса АРМ (Рисунок 4):

| | |
|---|---|
| | наличие подключения к сети; |
| | наличие соединения с серверами; |
| | наличие актуального сессионного ключа. |

Рисунок 4. Индикация сетевого статуса

В случае, если сервис не работает, соответствующая пиктограмма будет окрашена в красный цвет, если сервис работает – в зеленый, если отсутствует – в серый.

## Работа с приложениями

В Панели управления (вкладка «Контуры») пользователь может выбрать любой доступный ему контур, при этом на экране отобразится рабочий стол с приложениями, доступными ему в данном контуре.

Конкретный вид рабочего стола зависит от операционной системы, которая функционирует на удаленной ЭВМ (физической или виртуальной), и к которой подключен данный контур (клиентская ОС). Видом рабочего стола и составом доступных пользователю приложений в рамках работы с данным контуром управляет Администратор безопасности. На рабочем столе пользователя публикуются ярлыки приложений, к которым разрешен доступ. Запуск, работа, закрытие приложений осуществляется так же, как и в клиентской ОС, рабочий стол которой отображается на терминале.

Например, если выбранный контур ассоциирован с удаленной ЭВМ с клиентской ОС на базе Windows, то пользователю отобразится рабочий стол следующего вида (Рисунок 5):


Рисунок 5. Рабочий стол пользователя Windows

Если Администратор безопасности разрешил пользователю доступ к локальному контуру безопасности, то работа происходит с локальными приложениями, установленными администратором на АРМ (терминале) пользователя. В противном случае выбор контура означает доступ пользователя к приложениям, которые выполняются на удаленной ЭВМ в ЦОД, к которой пользователь обращается в терминальном режиме работы (работа приложений и обработка информации осуществляется на удаленной ЭВМ, на АРМ пользователя информация не хранится и не обрабатывается).

## Быстрая смена активного контура

Для перехода между контурами безопасности можно использовать Навигационную панель в нижней части экрана, которая вызывается нажатием комбинаций клавиш: **Ctrl+Alt+0** (Рисунок 6).

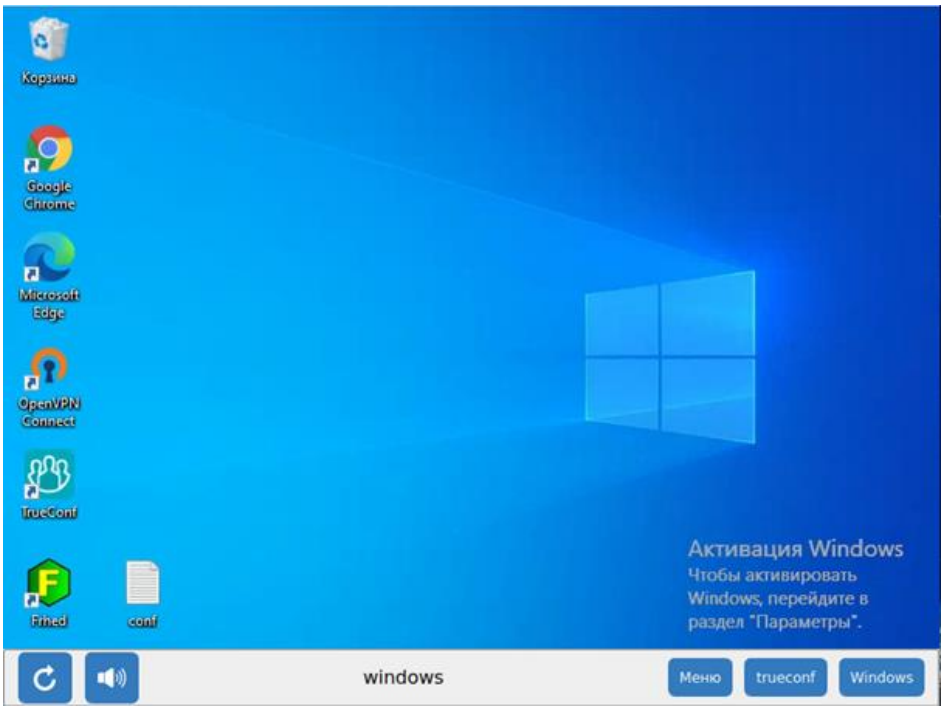



Рисунок 6. Навигационная панель. Выбор активного контура

В Навигационной панели можно либо быстро переключиться (сделать активным) на один из доступных контуров, либо вызвать форму управления контурами безопасности (кнопка «Меню»).

# Управление устройствами, подключенными к АРМ

Для управления устройствами, подключенными к АРМ, необходимо в Панели управления выбрать вкладку «Устройства».

В зависимости от установленных политик безопасности, пользователю может быть предоставлено право для подключения, отключения и работы с устройствами (Рисунок 7).

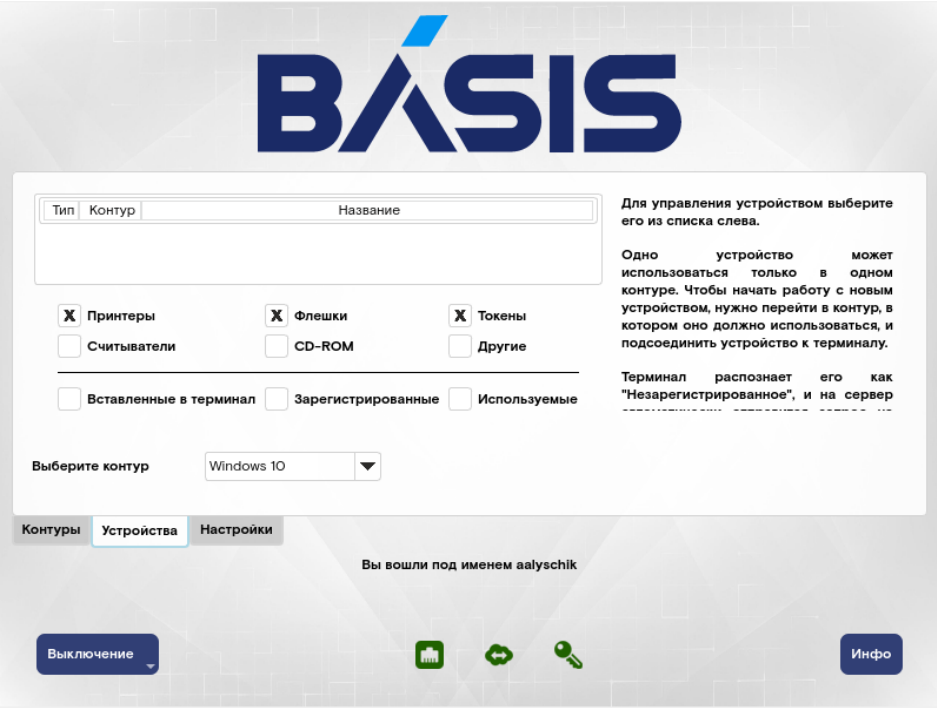



Рисунок 7. Управление устройствами

## Подключение устройства к контуру

Для того, чтобы физически подключенное к АРМ пользователя устройство было доступно для работы, его необходимо логически подключить к соответствующему контуру безопасности (удаленному рабочему столу). Подключение и работа с устройством на АРМ невозможны, если:

- клиентская ОС на удаленной ЭВМ запрещает подключение устройства (запрещен «проброс устройств»);
- подключение устройства запрещено политиками «Базис.WorkPlace Security».

Для того, чтобы логически подключить устройство к контуру безопасности, необходимо выполнить следующие действия:

- физически подключить устройство к АРМ;
- перейти во вкладку «Устройства» Панели управления (Рисунок 7);
- выделить строку с нужным устройством;
- выбрать требуемый контур (по умолчанию определен тот контур, в котором пользователь в данный момент находится). При необходимости, в данной форме можно использовать фильтр устройств (см. следующий раздел);
- Нажать кнопку «Подключить».

В некоторых случаях в процессе подключения устройства может возникнуть необходимость регистрации устройства в системе. В этом случае в Панели управления появится сообщение: «Устройство (Имя) готово к подключению», которое появится в панели управления.

## Фильтрация устройств

Для удобства работы со списком устройств во вкладке «Устройства» Панели управления предусмотрена возможность формирования перечня устройств с фильтрацией по разным признакам.

Первым признаком фильтрации является тип устройств, подключенных к АРМ:

- **принтеры** – все принтеры, доступные в данном контуре;
- **флэшки** – все флэш-накопители, доступные в данном контуре;
- **токены** – все токены, доступные в данном контуре;
- **считыватели** − отображает подсоединенные считыватели, например iButton;
- **другое** – отображает устройства, не вошедшие в предыдущие категории.

Вторым признаком является статус подключения устройства:

- **вставленные в терминал** – все устройства, подключенные к АРМ;
- **зарегистрированные** – все устройства, зарегистрированные в данном контуре;
- **используемые** – все используемые в данном контуре устройства.

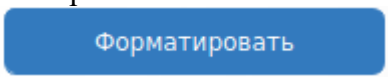
## Особенности использования USB-накопителей

Система поддерживает возможность сохранения информации непосредственно на USB-накопитель. Для этого необходимо выбрать функцию сохранения в приложении и указать путь к каталогу на USB накопителе, в котором будет размещен файл.

Запуск файлов непосредственно с USB накопителя запрещен.

Пользователю предоставляется возможность уничтожения (стирания) информации на машинных носителях (USB-накопителях) путем многократной полной перезаписи информации на носителе специальными битовыми последовательностями.

Необходимо обратить внимание, на то, что процедура форматирования может занять значительное время (от 30 минут и более). Длительность форматирования зависит от емкости USB-накопителя. Во время процедуры форматирования нельзя производить никаких действий с форматируемым USB-накопителем. Не рекомендуется извлекать USB-накопитель до окончания процедуры форматирования, так как извлеченный в ходе форматирования накопитель может иметь испорченную внутреннюю структуру.

Для форматирования USB-накопителя нужно выбрать подключенный накопитель и нажать кнопку 

. Далее появится предупреждающая форма, в которой необходимо подтвердить начало форматирования нажатием кнопки «Да» (Рисунок 8).

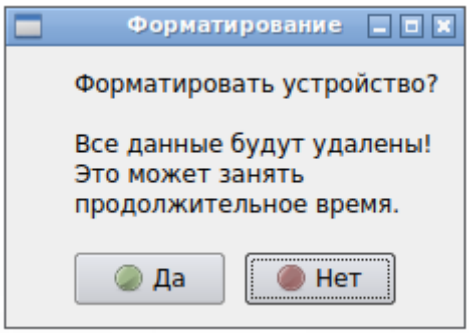



Рисунок 8. Форма подтверждения начала форматирования.

Статус процесса форматирования можно отслеживать в окне, находящемся справа от списка устройств.

После успешного окончания процедуры форматирования появляется форма, показанная на рисунке (Рисунок 9). Необходимо нажать кнопку «ОК», после чего становятся доступны другие действия над USB-накопителем.

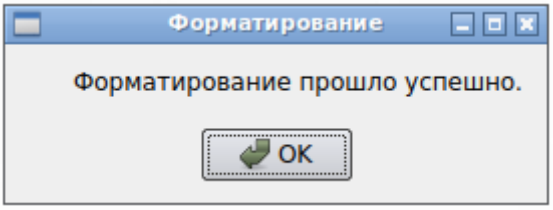



Рисунок 9. Форма успешного завершения процедуры форматирования.

## Удаление устройства из контура

Для того, чтобы прекратить использование подключенного к контуру устройства, его необходимо логически удалить. Для этого необходимо выполнить следующие действия:

- перейти во вкладку «Устройства» Панели управления (Рисунок 7);
- выделить строку с нужным устройством;
- Нажать кнопку «Удалить».

# Смена масштаба изображения экрана

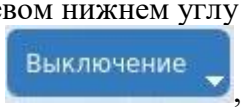
Во вкладке «Настройка» Панели управления можно выбрать масштаб, с которым будут отображаться удаленные рабочие столы. Данная возможность позволяет оптимально отображать информацию на мониторах с различным разрешением.

Вид формы для управления масштабом изображения показан на рисунке (Рисунок 10):


Рисунок 10. Вкладка «Настройка» Панели управления.

# Выключение, блокировка и перезагрузка АРМ пользователя

Необходимо отметить, что выключение, блокировка или перезагрузка АРМ пользователя не влияет на работу открытых сессий, работающих в рамках активных контуров безопасности (за исключением локального контура безопасности). Для завершения работы таких сессий необходимо использовать штатные средства клиентских ОС, работающих на удаленных ЭВМ, к которым осуществляется терминальный доступ.

Выключение, блокировка и перезагрузка АРМ пользователя возможна либо по нажатию кнопки  , расположенной в левом нижнем углу начального экрана входа в систему (Рисунок 1), либо нажатием кнопки 

, расположенной в левом нижнем углу Панели управления.

После нажатия одной из этих кнопок появится окно со списком возможных действий: Выключить, Перезагрузить, Заблокировать. Необходимо выбрать нужное действие, после чего АРМ пользователя будет выключен, перезагружен или заблокирован.

## Автоматическая блокировка работы АРМ пользователя

Кроме принудительной блокировки АРМ по команде пользователя возможна автоматическая блокировка работы АРМ, если пользователь не был активен в течение установленного администратором времени.

Для разблокировки АРМ пользователя необходимо ввести Пароль на экране входа в систему.

# Действия пользователя в случае нештатных ситуаций

## Не удается выполнить процедуру входа в систему

В случае, если пользователю не удается выполнить вход в систему, необходимо:

- убедиться в том, что вводятся верные идентификационные и аутентификационные данные;
- убедиться в том, что использован корректный токен (в случае двухфакторной аутентификации);
- убедиться в том, что сетевое подключение активно.

Если указанные действия не привели к решению проблемы, то следует обратиться к Администратору безопасности «Базис.WorkPlace Security».

## Несанкционированное вмешательство в работу ПО

При обнаружении несанкционированного вмешательства в работу «Базис.WorkPlace Security», нарушении целостности его контрольных сумм, подозрении на компрометацию аутентификационной информации, а также в случае некорректного выполнения функций ПО пользователь обязан незамедлительно проинформировать Администратора безопасности «Базис.WorkPlace Security» о случившемся событии. Работа пользователя до выяснения причин произошедшего запрещается.