Программное обеспечение «Базис.WorkPlace Security»

Руководство по эксплуатации

RU.НРФЛ.00003-01.97.01

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 по эксплуатации
Версия документа	2.0
Обозначение документа	RU.НРФЛ.00003-01.97.01
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 администраторов, отвечающих за эксплуатацию «Базис.WorkPlace Security», в т.ч. администраторов безопасности.

Данный документ содержит описание применения «Базис.WorkPlace Security», системные требования и условия его безопасной работы. Дополнительно к настоящему документу администраторы должны использовать следующие документы:

- «ПО «Базис.WorkPlace Security». Руководство по установке. RU.НРФЛ.00003-01 96 01;
- «ПО «Базис.WorkPlace Security». Руководство администратора RU.НРФЛ.00003-01 95 01.

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;
- интеграция с внешними LDAP-серверами;
- резервное сохранение и восстановление информации;
- сбор и обработка журналов регистрации событий безопасности.

Условия применения

Программный компонент «Базис - Сервер безопасности», технические требования

ПК «Базис - Сервер безопасности» может быть установлен на виртуальную или аппаратную платформу сервера безопасности, удовлетворяющую минимальным требованиям, указанным в таблице ниже (Таблица 1).

Таблица 1. Среда функционирования ПК «Базис - Сервер безопасности»

Характеристика	Минимальное значение	Рекомендуемое значение
Процессор	Процессор архитектуры x86-64 с тактовой частотой 2.0 GHz, 4 ядра (или эквивалент)	Рекомендуется добавлять одно ядро на каждые 100 активных соединений (или эквивалент)
Память	16 GB RAM	Зависит от числа пользователей «Базис.WorkPlace Security», рекомендуется добавлять 4 GB на 100 активных соединений
Сетевой интерфейс	100 Мбит/с	1000 Мбит/с
Дисковая подсистема	80 GB HDD/SDD	Зависит от числа пользователей «Базис.WorkPlace Security», рекомендуется добавлять 0,5GB на 1 пользователя
USB-интерфейс для подключения флеш-накопителя	USB 2.0	USB 3.0

Программный компонент «Базис – Терминал», технические требования

ПК «Базис - Терминал» может использовать специализированные устройства, а также персональные компьютеры, отвечающие минимальным требованиям, указанным в таблице ниже (Таблица 2).

Таблица 2. Среда функционирования ПК «Базис - Терминал»

Характеристика	Минимальное значение	Рекомендуемое значение
Процессор	Процессор архитектуры x86-32 или x86-64 с тактовой частотой 1,0 GHz	Процессор архитектуры x86-32 или x86-64 с 4 ядрами 1,6 GHz
Память	4 GB RAM	8 GB RAM
Сетевой интерфейс	10 Мбит/с	100 Мбит/с
Дисковая подсистема	16GB HDD/SDD	32GB HDD/SDD
USB-интерфейс для подключения флеш-накопителя	USB 2.0	USB 3.0

Рабочее место пользователя должно включать следующее оборудование:

- Системный блок (терминал).
- Устройства ввода/вывода (клавиатура, мышь).
- Монитор.

Описание применения

Функциональные задачи администратора системы

В задачи администратора (администраторов) по настройке управлению работой «Базис.WorkPlace Security» системы входят следующие действия:

- управление политиками безопасности в системе;
- управление учетными записями пользователей;
- управление доступом к ресурсам системы;
- мониторинг событий безопасности;
- настройка системы.

Состав дистрибутива «Базис.WorkPlace Security»

Дистрибутив ПО «Базис.WorkPlace Security» представляет собой записанные на машинный носитель информации файлы «Basis WPS Terminal.iso» и «Basis WPS Server.iso», которые включают установочные образы программных компонентов ПО «Базис.WorkPlace Security»:

- «Базис - Сервер безопасности» (устанавливается на сервере ЦОД);
- «Базис - Терминал» (устанавливается на АРМ пользователей).

Архитектура «Базис.WorkPlace Security»

Пример типовой схемы архитектуры применения «Базис.WorkPlace Security» приведен на рисунке ниже (Рисунок 1):

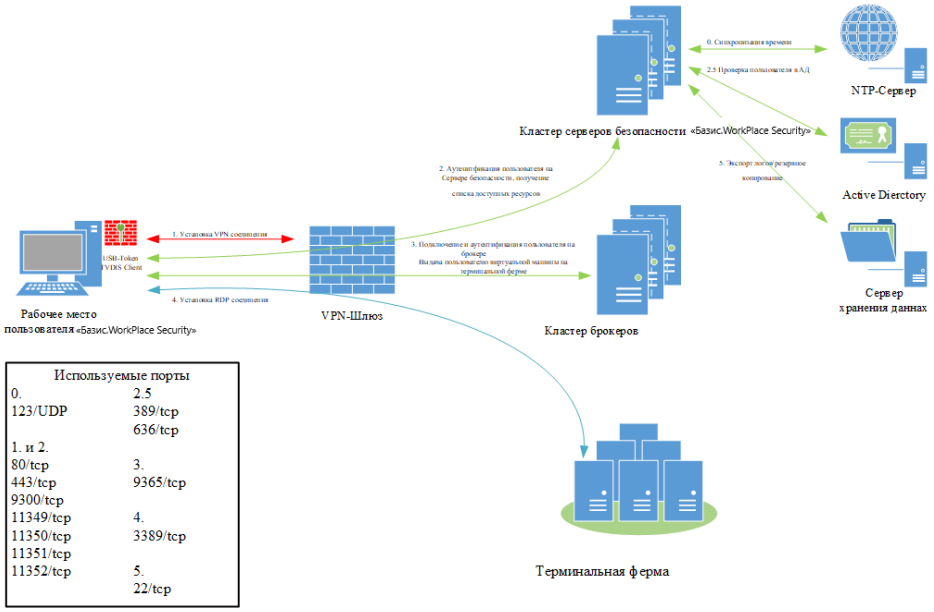

Рисунок 1. Пример типовой схемы архитектуры применения «Базис.WorkPlace Security»

«Базис.WorkPlace Security» поддерживает работу с криптошлюзом Ngate. Также возможна поддержка иных криптошлюзов.

«Базис.WorkPlace Security» использует следующие программные модули, входящие в его состав:

- ОС на основе Debian 11;
- База данных ElasticSearch;
- Web-сервер Nginx

«Базис.WorkPlace Security» использует следующие протоколы:

- Протоколы общения между компонентами системы: TLS;
- Протоколы удаленного доступа: RDP, SPICE, X2GO, BLAST, ICA и другие стандартные протоколы.

Установка «Базис.WorkPlace Security»

Установка ПО «Базис.WorkPlace Security» осуществляется согласно документу «ПО «Базис.WorkPlace Security». Руководство по установке. RU.НРФЛ.00003-01 96 01».

Настройка «Базис.WorkPlace Security»

Настройка ПО «Базис.WorkPlace Security» осуществляется согласно документу «ПО «Базис.WorkPlace Security». Руководство администратора. RU.НРФЛ.00003-01 95 01».

Перед началом эксплуатации Администратор безопасности должен настроить правила управления (разграничения) доступом для объектов и субъектов доступа.

Список объектов доступа, субъектов доступа и допустимых операций представлен в таблице ниже (Таблица 3).

Таблица 3. Список объектов доступа, субъектов доступа и допустимых операций

Объекты доступа	**Идентификация объекта доступа**	**Допустимые субъекты доступа**	**Допустимые операции**
Файлы и каталоги	Полное квалифицированное имя файла и/или каталога, содержащего файл	Процессы	Чтение Запись (включая удаление, создание и модификацию)
Контейнеры	Уникальное имя контейнера, заданное администратором	Пользователь «Базис.WorkPlace Security»	Запуск Создание
Выполняемые файлы	Полное квалифицированное имя файла (приложения)	Процессы, контейнер	Запуск (включая чтение выполняемого файла)

Объекты доступа	**Идентификация объекта доступа**	**Допустимые субъекты доступа**	**Допустимые операции**
Сервис управления и администрирования	Наименование сервиса (обращение к сервису производится по IP-адресу ПК «Базис - Сервер безопасности»	Администратор (полный доступ) Аудитор (доступ к журналам регистрации)	Полный доступ к Сервису Доступ к функциям работы с регистрационными журналами
Терминал	Уникальное имя терминала, заданное администратором	Пользователь «Базис.WorkPlace Security»	Аутентификация пользователя «Базис.WorkPlace Security» (запуск сессии в ПК «Базис - Терминал» на заданном терминале)
Сетевые интерфейсы (на терминале)	Полное квалифицированное имя устройства (драйвера)	Администратор (определение сетевых параметров) Контейнер (сетевой обмен)	Определение сетевых параметров Сетевой обмен (передача и прием сетевого трафика через интерфейс)
USB-накопители (подключаемые к терминалу)	Уникальное имя накопителя, определяемое при инициализации	Пользователь «Базис.WorkPlace Security»	Чтение и запись информации
Устройства (драйверы устройств)	Полное квалифицированное имя ссылки на драйвер устройства	Процессы пользователя	Чтение и запись информации
Принтеры (подключаемые к терминалу и принт-серверы)	Полное квалифицированное имя устройства	Пользователь, контейнер	Печать

Настройка прав доступа осуществляется Администратором безопасности либо с использованием Сервиса управления и администрирования, входящего в состав ПК «Базис - Сервер безопасности», либо (для файлов, каталогов, выполняемых файлов, устройств) с помощью определения атрибутов доступа для соответствующего объекта средствами и командами, аналогичными стандартным средствам и командам UNIX-подобных систем.

Работа пользователей с «Базис.WorkPlace Security»

Работа пользователей с ПО «Базис.WorkPlace Security» осуществляется на АРМ (терминалах) согласно документу «ПО «Базис.WorkPlace Security». Руководство пользователя. RU.НРФЛ.00003-01 94 01».

Восстановление после сбоя

В случае возникновения сбоя в системе, возникшего в случае внештатной ситуации или неполадок в работе оборудования, который привел к перезагрузке системы, «Базис.WorkPlace Security» автоматически восстанавливает свою работоспособность после перезагрузки.

Условия безопасной работы

Перед эксплуатацией «Базис.WorkPlace Security» необходимо внимательно ознакомиться с эксплуатационной документацией.

Перед вводом в эксплуатацию «Базис.WorkPlace Security» должен быть назначен Администратор безопасности, отвечающий за соблюдение мер безопасности при эксплуатации «Базис.WorkPlace Security».

При эксплуатации «Базис.WorkPlace Security» Администратор безопасности должен обеспечить следующие условия для его безопасной работы:

- должна быть обеспечена защита аппаратных средств, на которых функционирует «Базис.WorkPlace Security», от несанкционированного физического доступа (например, путем установки замков и/или защитных наклеек);
- технические средства вычислительной сети (включая каналы связи), в составе которой функционирует «Базис.WorkPlace Security», должны быть защищены от несанкционированного доступа организационно-техническими мероприятиями и/или применением сертифицированных средств криптографической защиты информации;
- должны быть обеспечены организационно-технические меры, исключающие возможность несанкционированной модификации программных компонент «Базис.WorkPlace Security»;
- должны быть разработаны нормативные документы, определяющие порядок допуска пользователей к «Базис.WorkPlace Security» и назначения их полномочий;
- должен быть разработан порядок установки и изменения прикладных программных средств, функционирующих в изделии;
- должны быть разработаны инструкции для пользователей, определяющие обязанности по обеспечению сохранности персональных идентификаторов и паролей, порядок работы на компьютерах, оснащенных «Базис.WorkPlace Security»;
- должно быть обеспечено сохранение конфиденциальности паролей пользователей;
- при каждой установке «Базис.WorkPlace Security» должен быть изменен предустановленный пароль администратора;
- должна производиться периодическая смена паролей пользователей «Базис.WorkPlace Security»;
- должно выполняться периодическое тестирование защитных функций и контроля целостности «Базис.WorkPlace Security» согласно эксплуатационной документации;
- должна соблюдаться установленная предприятием-изготовителем процедура обновления «Базис.WorkPlace Security» в случае выпуска обновлений, исправлений (патчей) «Базис.WorkPlace Security»;
- при применении «Базис.WorkPlace Security» следует использовать комплекс мероприятий антивирусной защиты с применением сертифицированных средств антивирусной защиты;
- на средствах вычислительной техники, на которых установлено «Базис.WorkPlace Security», должны быть реализованы меры, исключающие возможность использования средств разработки и отладки ПО, средств для редактирования кода и оперативной памяти, используемой «Базис.WorkPlace Security»;
- должны быть приняты меры по исключению возможности изменения пользователями настроек BIOS;
- должна быть исключена загрузка на средствах вычислительной техники иных программных средств, кроме компонент «Базис.WorkPlace Security».