Программное обеспечение «Базис.WorkPlace Security»

Руководство по установке

RU.НРФЛ.00003-01.96.01

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 установке
Версия документа	2.0
Обозначение документа	RU.НРФЛ.00003-01.96.01
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 безопасности, которые выполняют первоначальную установку и обновление ПО «Базис.WorkPlace Security».

Данный документ содержит:

- условия применения (системные требования) для установки ПО «Базис.WorkPlace Security»;
- описание процесса установки ПО «Базис.WorkPlace Security».

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.

Порядок установки программного обеспечения «Базис.WorkPlace Security»

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).

Создание загрузочных носителей для программных компонент «Базис.WorkPlace Security»

Установка ПК «Базис - Сервер безопасности» на Сервер безопасности и ПК «Базис - Терминал» на АРМ пользователей осуществляется с заранее подготовленных загрузочных носителей, которые формируются из файлов дистрибутива «Базис.WorkPlace Security».

Формирование загрузочных носителей может осуществляться на компьютере с установленной операционной системой семейства Windows (с использованием дополнительного бесплатного ПО с открытым кодом) или с установленной операционной системой семейства Linux.

В качестве носителей загрузочных образов могут использоваться стандартные USB-накопители или аппаратный токен (RuToken, JaCarta или аналогичные) с дополнительной флеш-памятью.

Использование ОС Windows

В операционной системе Windows для создания загрузочных образов ПК «Базис - Сервер безопасности» и ПК «Базис - Терминал» на съемных носителях информации (токенах) используется бесплатное ПО Rufus версии 3.6.

Необходимо подключить к компьютеру машинный носитель информации, содержащий файлы дистрибутива «Базис.WorkPlace Security», и запустить программу Rufus (Рисунок 1):

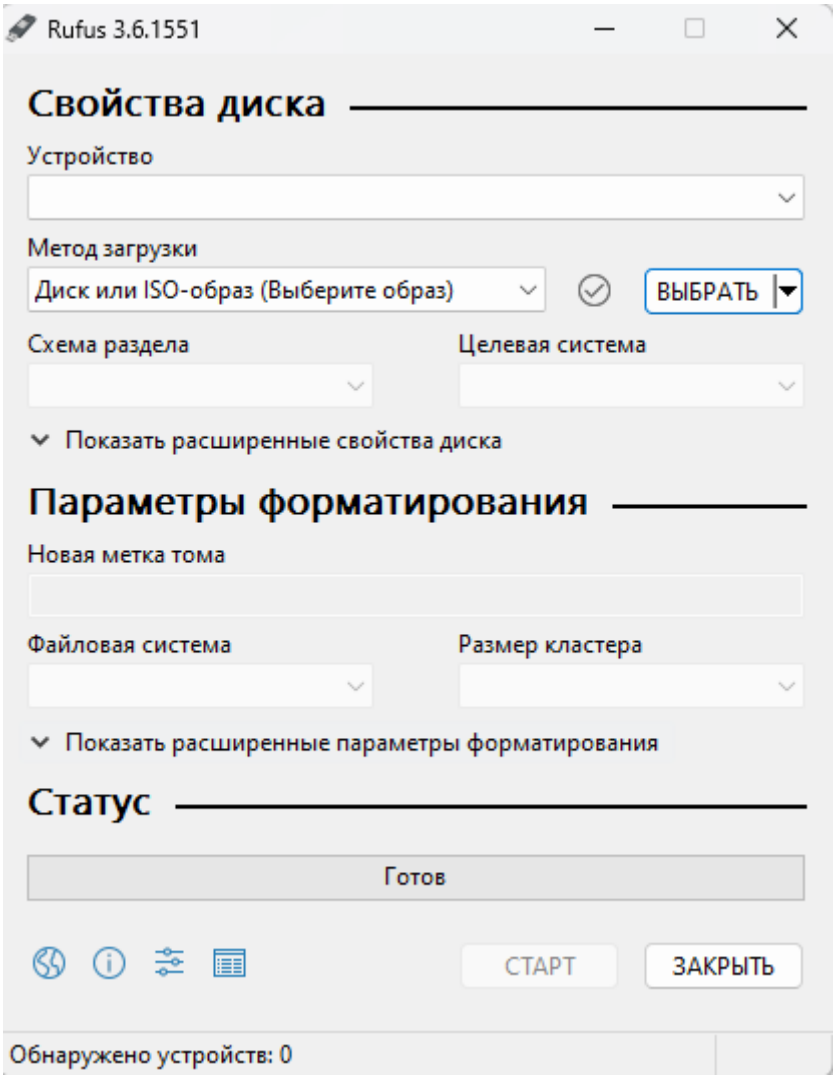

Рисунок 1. Пользовательский интерфейс программы Rufus 3.6

Затем следует выбрать в строке «Устройство» накопитель, на котором будет создан загрузочный образ, нажать кнопку «Выбрать» и в выпадающем меню найти на носителе с дистрибутивом нужный файл с расширением .iso из состава дистрибутива «Базис.WorkPlace Security» (Рисунок 2):

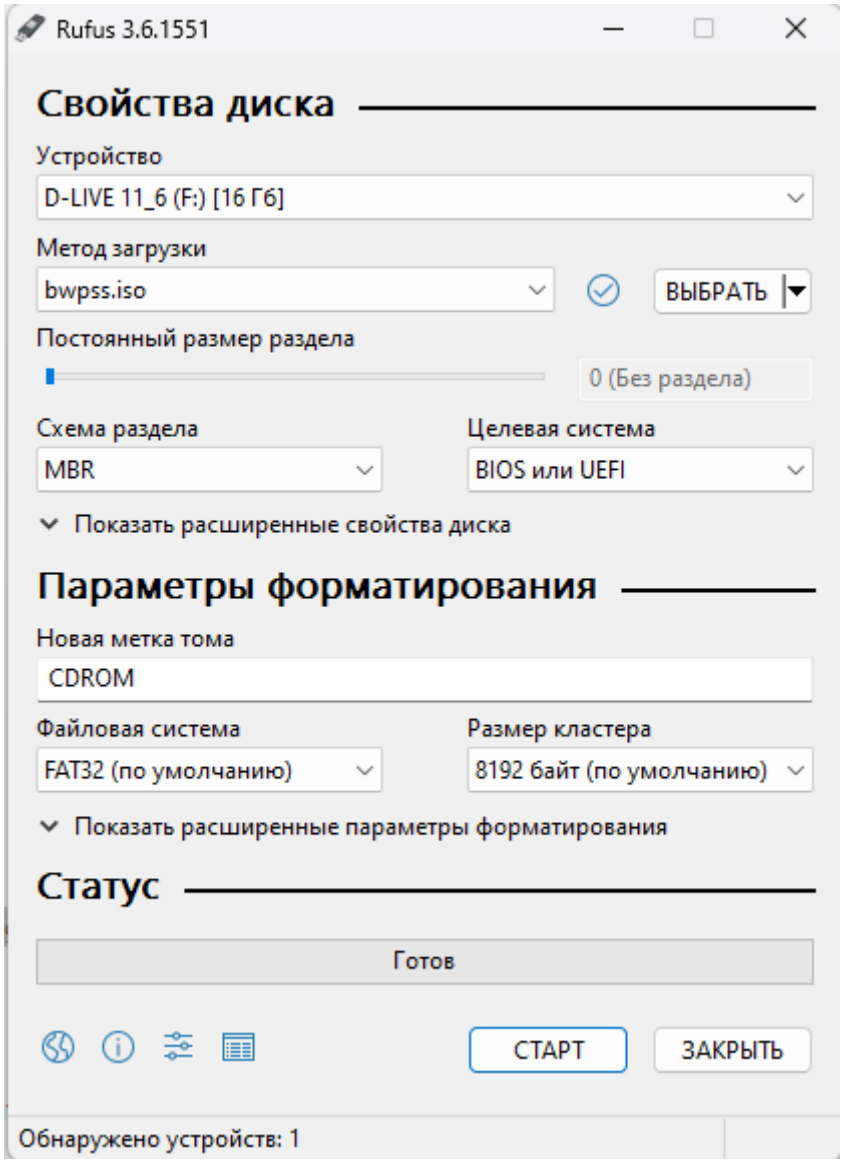

Рисунок 2. Выбор файла с расширением .iso

После этого необходимо запустить создание на носителе соответствующего загрузочного образа, нажав кнопку «Старт».

После успешного создания загрузочного образа появится зеленый индикатор и сообщение «Готов» (Рисунок 3). В случае ошибки появляется красный индикатор и сообщение «Сбой», тогда требуется повторить процесс записи с начала, устранив выявленные ошибки.

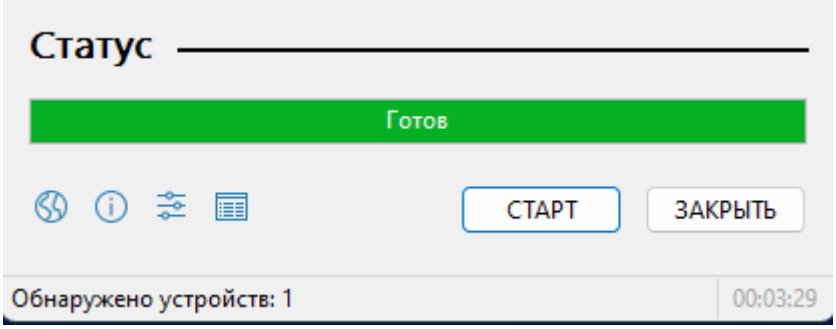

Рисунок 3. Образ записан

Использование ОС Linux

В операционной системе Linux для создания загрузочных образов ПК «Базис - Сервер безопасности» и ПК «Базис - Терминал» на съемных носителях информации (токенах) необходимо:

- подключить к компьютеру и смонтировать дистрибутивный носитель «Базис.WorkPlace Security»;
- подключить к компьютеру съемный носитель информации для создания загрузочного образа;
- выполнить в командной строке команду:
    - sudo dd of=<имя_устройства_с_носителем> if=<файл_ISO> status=progress

где:

- <имя_устройства_с_носителем> - имя устройства в формате Linux (например, /dev/sda), к которому подключен съемный носитель информации для создания загрузочного образа;
- <файл_ISO> - полный путь до файла ISO, находящегося на дистрибутивном носителе.

Например, если носитель был подключен к устройству /dev/sda, а дистрибутив смонтирован по адресу «/distr», то команда создания загрузочного образа для АРМ должна выглядеть следующим образом:

- sudo dd of=/dev/sda ”if=/distr/Basis WPS Terminal.iso” status=progress

Работы по установке Сервера безопасности

Первоначальная установка «Базис.WorkPlace Security» на Сервер безопасности

Для установки «Базис.WorkPlace Security» на Сервер безопасности необходимо подключить к виртуальному или физическому серверу носитель, на который записан загрузочный образ ПК «Базис - Сервер безопасности» («Basis WPS Server.iso»), настроить сервер на загрузку с указанного носителя и произвести начальную загрузку.

Установка ПК «Базис - Сервер безопасности» происходит в автоматическом режиме. Если в локальной вычислительной сети, к которой подключен Сервер безопасности, отсутствует сервер DHCP, то мастер установки предложит добавить вручную сетевые настройки, необходимые для функционирования сервера.

После установки компонента на Сервер безопасности использованный носитель с загрузочным образом можно отключить.

В случае установки компонента на виртуальный Сервер безопасности рекомендуется сделать снап-шот виртуальной машины средствами используемой системы виртуализации для возможности быстрого восстановления в случае необходимости.

После окончания установки «Базис.WorkPlace Security» необходимо перезагрузить Сервер безопасности, затем выполнить вход в операционную систему со стандартным именем «root» и стандартным паролем «wauj5ii0Ca]z». После первого входа Администратор безопасности должен сменить стандартный пароль пользователя «root» на уникальный для данной установки, для этого необходимо ввести команду:

- passwd

Измененный пароль должен соответствовать политикам безопасности, и его необходимо сохранять в тайне. Дальнейшие действия по настройке Сервера безопасности выполняются в командной строке от имени пользователя «root».

Кластеризация Сервера безопасности

Данный раздел руководства выполняется только в том случае, если администратор принял решение об установке Сервера безопасности на кластер ЭВМ. Если выбрана обычная (без кластеризации) установка, то настройка кластеризации в процессе эксплуатации «Базис.WorkPlace Security» невозможна.

Кластеризация Сервера безопасности заключается в организации распределенной работы используемой в Сервере безопасности базы данных (БД) Elasticsearch на нескольких ЭВМ, объединенных в единый кластер. Для настройки кластеризации администратор должен обладать знаниями по настройке и управлению БД Elasticsearch, а также навыками работы в текстовом редакторе «nano». В данном разделе приводится содержимое настроечных файлов, которое формируется администратором с помощью редактора «nano», который запускается в командной строке следующей командой:

- nano <имя файла>

Далее приведено описание процесса настройки на примере трех узлов. Названия узлов приводятся в виде «es-c**N**», где **N** – порядковый номер узла.

На каждом узле необходимо обеспечить доступность узла по его имени, введя в файл «/etc/hosts» каждого узла строчки следующего вида:

- <IP-адрес узла 1> es-c1
- <IP-адрес узла 2> es-c2
- <IP-адрес узла 3> es-c3

Далее, на каждом узле необходимо отредактировать файл «/etc/elasticsearch/elasticsearch.yml» следующим образом (пример приведен для узла es-c1):

- path.data: /data/elastic/data
- path.logs: /data/elastic/logs
- network.host: 0.0.0.0
- http.port: 11111
- #Название кластера:
- cluster.name: cluster-tvdis
- #Название узла:
- network.publish_host: es-c1
- #Название узла

- node.name: es-c1
- #
- node.master: true
- #
- node.data: true
- #Минимальное количество узлов
- discovery.zen.minimum_master_nodes: 2
- # Указываем названия всех нод (узлов) которые будут объединены в кластер
- discovery.zen.ping.unicast.hosts: ["es-c1", "es-c2", "es-c3"]

Затем на каждом узле выполняется команда:

- service elasticsearch restart

Далее необходимо развернуть базу через tvdisa-init, действуя по инструкции как для одиночной инсталяции ПО «Базис.WorkPlace Security», например, начиная с "init data.json" в Build, install and configure BWPS.

Предварительная настройка Сервера безопасности

Для настройки Сервера безопасности необходимо после установки компонента «Базис - Сервер безопасности» в сеансе работы пользователя «root» выполнить следующие команды:

- cd /usr/sbin/
- sudo config.sh
- sudo initialize.sh

В процессе выполнения этих команд на экране будет отображаться информация следующего вида (Рисунок 4):

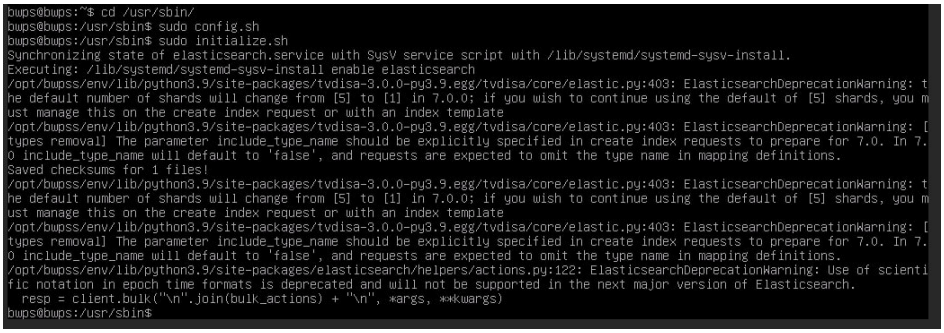

Рисунок 4. Вывод информации на экран

После предварительной настройки дальнейшая настройка Сервера безопасности может осуществляться через WEB-сервер, который входит в состав Сервера безопасности, согласно документу «ПО «Базис.WorkPlace Security». Руководство администратора RU.НРФЛ.00003-01 95 01». Для обращения к интерфейсу администратора через WEB-сервер необходимо на любом компьютере, имеющим сетевой доступ к Серверу безопасности, открыть WEB-браузер и перейти по следующему адресу:

- https://IP_адрес_Сервера_безопасности

В случае успешной установки и предварительной настройки Сервера безопасности в браузере отобразится окно, показанное на рисунке ниже (Рисунок 5):

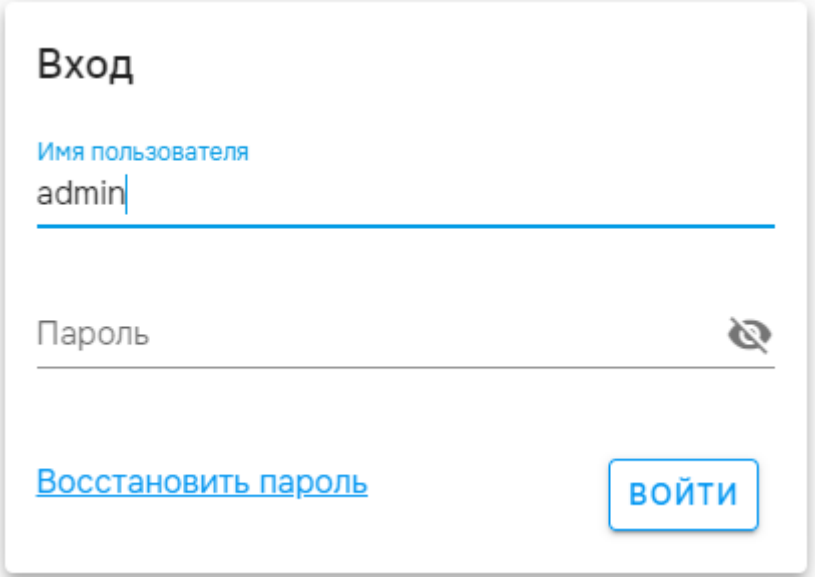

Рисунок 5. WEB-интерфейс администратора

В поле «Пароль» необходимо указать стандартный пароль «wauj5ii0Ca]z». После первого входа необходимо сменить стандартный пароль пользователя «admin» на уникальный для данной установки, согласно документу «ПО «Базис.WorkPlace Security». Руководство администратора RU.НРФЛ.00003-01 95 01».

Работы по установке АРМ (терминала) пользователя

Первоначальная установка «Базис.WorkPlace Security» на АРМ пользователя

Для установки «Базис.WorkPlace Security» на АРМ (терминал) пользователя необходимо подключить к АРМ носитель, на который записан загрузочный образ ПК «Базис - Терминал» («Basis WPS Terminal.iso»), настроить АРМ на загрузку с указанного носителя и произвести начальную загрузку.

Установка ПК «Базис - Терминал» происходит в автоматическом режиме.

Предварительная настройка АРМ пользователя после установки «Базис.WorkPlace Security»

После успешной установки ПК «Базис - Терминал» на АРМ пользователя необходимо выполнить перезагрузку АРМ. После перезагрузки на экране появится окно настройки конфигурации АРМ:

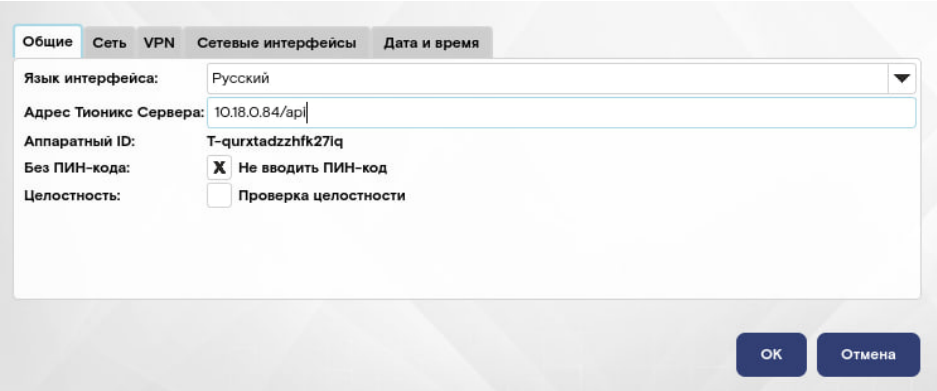

Рисунок 6. Конфигурация терминала – вкладка общих настроек

В данном окне необходимо указать IP-адрес ранее установленного Сервера безопасности. Если в локальной вычислительной сети, в которой функционирует АРМ, не используется сервер DHCP, необходимо вручную настроить сетевую конфигурацию, заполнив требуемые поля. Также можно выбрать дополнительные уровни защиты – запрос ПИН-кода и проверка целостности.

Во вкладке «Сетевые интерфейсы» (Рисунок 7) из выпадающего списка необходимо выбрать тип интерфейса: eth*, если для подключения к сети Интернет используется сетевой кабель, и wlan* –при подключении к Wi-Fi сети.

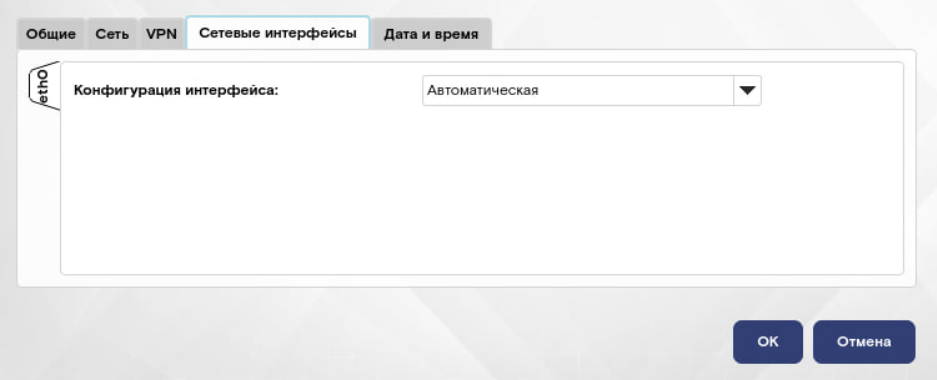

Рисунок 7. Конфигурация терминала – вкладка сетевых настроек

В поле «Профиль VPN» из выпадающего меню выбрать требуемый профиль.

После завершения начальной настройки конфигурации АРМ пользователя необходимо нажать на кнопку «ОК». В случае правильности настройки АРМ подключится к Серверу безопасности.

Далее на экране АРМ появится приглашение, показанное на рисунке ниже.

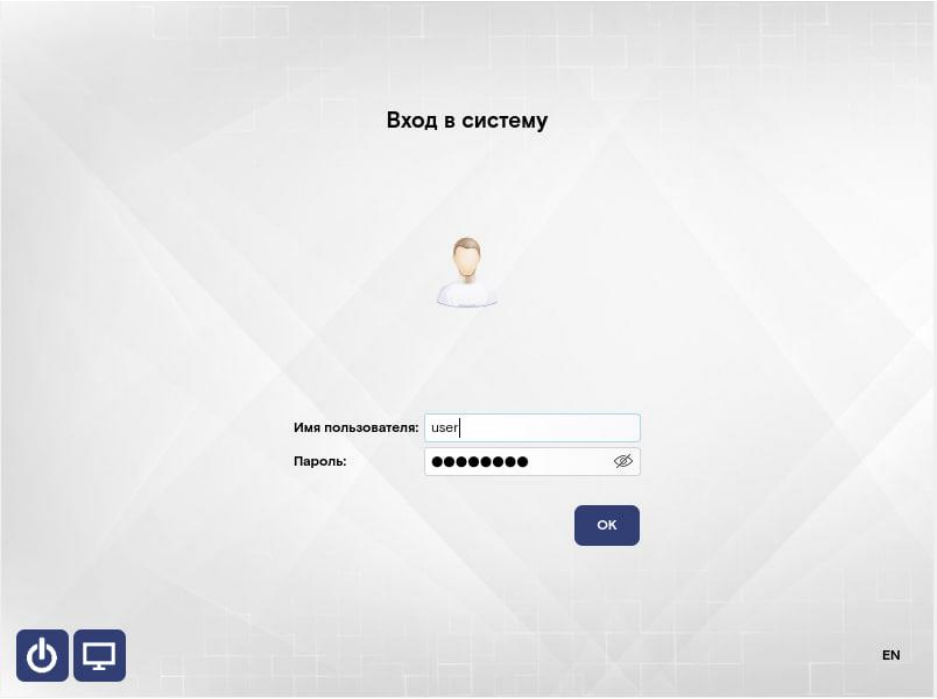

Рисунок 8. Экран АРМ пользователя после подключения к Серверу безопасности