Программное обеспечение «Базис.Virtual Security». Руководство администратора

RU.НРФЛ.00002-02 95 01

Москва

08/11/2023

Содержание

Введение ... 3
Назначение ... 5
Структура ПО «Базис.Virtual Security» ... 7
Требования к административно-техническому персоналу ... 9
Действия по реализации функций безопасности среды функционирования ... 10
Действия по приемке, установке и настройке ПО Базис.Virtual Security ... 21
Действия после сбоев и ошибок эксплуатации ПО Базис.Virtual Security ... 22
Часть 1. Программный модуль «Базис.Virtual Security» ... 23
Часть 2. Программный модуль «Базис.DynamiX» ... 24
Часть 3. Программный модуль «Базис.vCore» ... 25

Введение

Настоящий документ представляет собой Руководство администратора программного обеспечения «Базис.Virtual Security» (далее – ПО, Изделие) и составлен в соответствии с «Требованиями по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утв. приказом ФСТЭК России от 02 июня 2020 г. № 76) к средствам, соответствующими 4 уровню доверия.

Требования к разработке средств, соответствующих 4 уровню доверия, включают категорию требований к «разработке руководства администратора средства», в соответствии с которыми, Разработка руководства администратора средства должна предусматривать:

- описание действий по безопасной приемке поставленного ПО;
- описание действий по реализации функций безопасности среды функционирования ПО.

В руководстве администратора ПО «Базис.Virtual Security» приводятся сведения о программном обеспечении «Базис.Virtual Security», кодовое обозначение RU.НРФЛ.00002-02, и его программных модулях, которые представлены в виде 3-х частей к настоящему руководству и имеют следующие идентификационные данные:

Идентификационные данные	**Программное обеспечение «Базис.Virtual Security»**
Версия документа	2.0
Название документа	Программное обеспечение «Базис.Virtual Security». Руководство администратора»
Обозначение документа	RU.НРФЛ.00002-02 95 01
Название документа	«Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security»
Обозначение документа	RU.НРФЛ.00002-02 95 01 Ч1
Название документа	«Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 2. Программный модуль «Базис.DynamiX»
Обозначение документа	RU.НРФЛ.00002-02 95 01 Ч2
Название документа	«Программное обеспечение «Базис.Virtual Security». Программный модуль «Базис.DynamiX». Приложение 1. Руководство администратора по использованию API
Обозначение документа	RU.НРФЛ.00002-02 95 01 Ч2-01
Название документа	«Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 3. Программный модуль «Базис.vCore»
Обозначение документа	RU.НРФЛ.00002-02 95 01 Ч3
Автор документа	ООО «БАЗИС»

Разработчиком и изготовителем является Общество с ограниченной ответственностью «БАЗИС» (ООО «БАЗИС»), адрес местонахождения: 109316, г. Москва, вн. тер. г. Муниципальный округ Текстильщики, пр-д Остаповский, д. 22, стр. 16, эт. 2, ком. 52, адрес места осуществления деятельности: 117485, г. Москва, ул. Бутлерова, д.7, лицензия на деятельность по разработке и производству средств защиты конфиденциальной информации (регистрационный номер Л050-00107-00/00578916, выдана ФСТЭК России 12.12.2019, действует бессрочно).

Настоящий документ предназначен для инженерно-технических специалистов, осуществляющих эксплуатацию, поддержку и сопровождение программного обеспечения требования, к которым приведены в разделе "Требования к административно-техническому персоналу" настоящего руководства.

Назначение

Программное обеспечение (далее – ПО) «Базис.Virtual Security» является программным средством, обеспечивающим безопасное создание и функционирование изолированных программных сред, состоящих из виртуального оборудования, гостевых операционных систем и прикладного программного обеспечения (далее – виртуальные машины), в информационной (автоматизированной) системе (далее – средства виртуализации). ПО обеспечивает выполнение следующих функций безопасности (ФБ):

- доверенная загрузка виртуальных машин средством виртуализации;
- контроль целостности в средстве виртуализации;
- регистрация событий безопасности в средстве виртуализации;
- управление доступом в средстве виртуализации;
- резервное копирование в средстве виртуализации;
- управление потоками информации в средстве виртуализации;
- защита памяти;
- ограничение программной среды;
- идентификация и аутентификация пользователей в средстве виртуализации;
- централизованное управление образами виртуальных машин и виртуальными машинами.

ПО «Базис.Virtual Security» также обеспечивает:

- реализацию технологии единой точки доступа (Single Sign On, SSO) к информационным системам, поддерживающим протоколы OpenID Connect и LDAP;
- управление взаимодействием с внешними информационными системами, поддерживающими протоколы OpenID Connect и LDAP;
- аутентификацию по токену сессии, выданному в соответствии со стандартом OpenID Connect, при удалённом или локальном доступе систем, обращающихся к СУБД Postgres Pro от имени ранее аутентифицированных пользователей;
- управление доступом к API-интерфейсам защищаемых информационных и автоматизированных систем.

В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, введенными в действие приказом ФСТЭК России № 17 от 11 февраля 2013 г. (далее – приказ ФСТЭК России № 17), Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, введенными в действие приказом ФСТЭК России № 21 от 18 февраля 2013 г. (далее – приказ ФСТЭК России № 21), Требованиями к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критических важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, введенными в действие приказом ФСТЭК России № 31 от 14 марта 2014 г. (далее - приказ ФСТЭК России № 31), и Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, введенными в действие приказом ФСТЭК России № 239 от 25 декабря 2017 г. (далее - приказ ФСТЭК России № 239), изделие, соответствующее 4 классу защиты и 4 уровню доверия, при выполнении указаний по эксплуатации может использоваться:

- для создания государственных информационных систем до 1 класса защищенности включительно в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17 с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 № 27;
- для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных до 1 уровня защищенности, в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» введенным в действие приказом ФСТЭК России № 21 от 18 февраля 2013 г. (далее – приказ ФСТЭК России № 21).
- в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности в соответствии с документом «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», утвержденным приказом ФСТЭК России от 14 марта.2014 № 31 с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 № 49 и приказом ФСТЭК России от 9 августа 2018 г. № 138;
- в информационных и автоматизированных системах управления, информационно-телекоммуникационные сети, которые отнесены к значимым объектам критической информационной инфраструктуры до 1 категории значимости, в соответствии с документом «Требования по обеспечению безопасности значимых объектов критической информационной

инфраструктуры Российской Федерации», введенным в действие приказом ФСТЭК России № 239 от 25 декабря 2017 г. (далее - приказ ФСТЭК России № 239)

- в информационных системах общего пользования II класса, в соответствии с документом «Требования по защите информации, содержащейся в информационных системах общего пользования», введенным в действие приказом ФСТЭК России №489 от от 31 августа 2010.

Структура ПО «Базис.Virtual Security»

ПО «Базис.Virtual Security» состоит из следующих программных модулей:

- «Базис.Virtual Security» – программный модуль, отвечающий за аутентификацию и авторизацию в других программных модулях программного обеспечения и во внешних информационных системах, а также за защиту информации, обрабатываемой с использованием средств виртуализации;
- «Базис.DynamiX» – программный модуль, отвечающий за обеспечение централизованного управления созданием и функционированием изолированных программных сред, состоящих из виртуального оборудования, гостевых операционных систем и прикладного программного обеспечения (виртуальных машин), в средстве виртуализации;
- «Базис.vCore» – гипервизор 1 типа, являющийся программным модулем виртуализации, обеспечивающим создание и функционирование изолированных программных сред, состоящих из виртуального оборудования, гостевых операционных систем и прикладного программного обеспечения (виртуальных машин).

В ПО «Базис.Virtual Security» предусмотрен вариант исполнения функции средства виртуализации сертифицированной ОС, соответствующей требованиям по безопасности к средствам виртуализации.

Программный модуль «Базис.Virtual Security» состоит из следующих компонентов:

- ядро управления – основной компонент, реализующий бизнес-логику и обеспечивающий интеграцию между подсистемами программного модуля;
- веб-интерфейс – программный компонент, предоставляющий графический интерфейс администратору для централизованного управления программным модулем и различными функциями безопасности, которые данный программный модуль реализует;
- сервис аутентификации, отвечающий за реализацию функций безопасности, связанных с идентификацией, аутентификацией пользователей в средстве виртуализации и в других внешних системах с использованием протоколов OpenID Connect (OIDC), SAML 2.0, Kerberos, LDAP/Active Directory;
- LDAP-сервис, обеспечивающий реализацию протокола легковесного доступа к каталогам (LDAP, Lightweight Directory Access Protocol) и позволяющий выполнять операции создания, хранения, изменения и удаления различных записей в указанных каталогах, в том числе управлять жизненным циклом учётных записей пользователей;
- сервис-агент – программный компонент, функционирующий в составе гипервизора 1 типа Базис.vCore или в составе сертифицированной хостовой операционной системы, и выполняющий функции безопасности, связанные с контролем жизненного цикла виртуальных машин, вычислительных сетей и узлов виртуализации, а также с контролем целостности и доверенной загрузкой;
- сервис проксирования, отвечающий за управление доступом к API-интерфейсам защищаемых информационных и автоматизированных систем;
- шина обмена сообщениями, выполняющая транспортные функции в программном модуле и гарантирующая доставку различных управляющих сигналов между программными компонентами серверной части и сервисом-агентом, который функционирует на вычислительных узлах;
- балансировщик нагрузки – сервис, реализующий распределение запросов между нескольким узлами кластера управления программного модуля «Базис.Virtual Security»;
- сервис сбора логов, выполняющий функции сбора и обработки журналов событий программного обеспечения «Базис.Virtual Security» и других внешних систем.

Программный модуль «Базис.DynamiX» состоит из следующих компонентов:

- подсистема управления, реализующая основные функции централизованного управления виртуальными машинами, виртуализированным оборудованием и другими сущностями среды виртуализации с использованием различных интерфейсов администрирования;
- подсистема взаимодействия с базой данных, предоставляющая унифицированные механизмы взаимодействия с системой управления базами данных для обеспечения постоянного хранения данных подсистемы управления;
- подсистема взаимодействия с агентами, реализующая программные интерфейсы взаимодействия для передачи служебной информации между подсистемой управления и различными сервис-агентами, функционирующими на гипервизорах 1 типа vCore или сертифицированных хостовых операционных системах, которые могут выступать средствами виртуализации;
- вспомогательная подсистема, отвечающая за отслеживание состояния вычислительных узлов и мониторинг основных служб, необходимых для корректного функционирования средства виртуализации;
- сервис-агент (JSagent), обеспечивающий информационный обмен между внутренними подсистемами средства виртуализации на базе сертифицированной операционной системы и подсистемой управления. Применяется в исполнении Изделия (И2).

Программный модуль «Базис.vCore» состоит из следующих компонентов:

- ядро гипервизора, реализующее основные функции виртуализации и обеспечивающее функционирование других подсистем гипервизора 1 типа;
- подсистема виртуализации, в которую входят: библиотека для программной интеграции функций виртуализации; эмулятор аппаратных платформ и виртуализированного оборудования;
- конфигуратор гипервизора, предоставляющий графический интерфейс администратору для управления настройками подсистем гипервизора;
- сетевая подсистема, обеспечивающая реализацию функций сетевого обмена в среде виртуализации, а также сегментации сетевого трафика на уровнях вычислительных узлов и виртуальных машин;
- дисковая подсистема, которая должна отвечать за взаимодействие средства виртуализации с локальными и внешними системами хранения данных;
- компонент управления, обеспечивающий выполнение транспортных функций в программном модуле и гарантирующий доставку различных управляющих сигналов между программными компонентами серверной части и сервисом-агентом vCore, который функционирует на вычислительных узлах, а также предоставляет другие интерфейсы централизованного управления гипервизорами 1 типа «Базис.vCore»;
- сервис-агент, обеспечивающий информационный обмен между внутренними подсистемами гипервизора и программным модулем, который отвечает за централизованное управление виртуальной инфраструктурой.

Хранение данных серверной части программных модулей ПО «Базис.Virtual Security» осуществляется с применением реляционных баз данных.

Информация о структуре ПО «Базис.Virtual Security» приведена на рисунке.

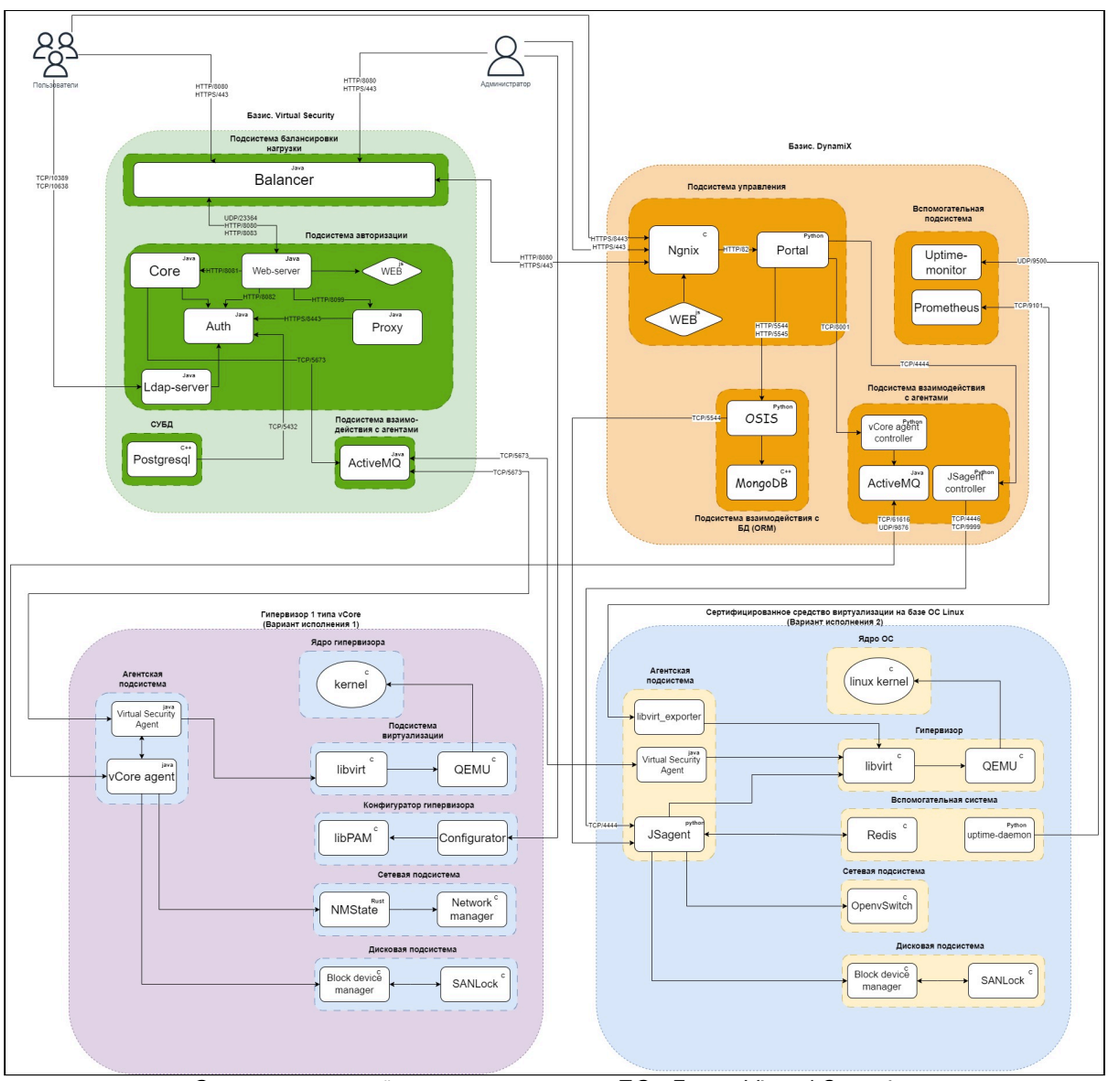

Схема взаимодействия компонентов ПО «Базис.Virtual Security»

Требования к административно-техническому персоналу

Основными обязанностями администратора являются:

- установка, настройка и мониторинг работоспособности ПО;
- установка и настройка параметров программного обеспечения систем управления базами данных (СУБД);
- оптимизация функционирования баз данных по времени отклика и скорости доступа к данным;
- резервное копирование и аварийное восстановление данных;
- управление и реализация эффективной политики доступа к информации, которая хранится в базах данных;
- ввод и поддержание в актуальном состоянии классификаторов баз данных;
- администрирование платформы виртуализации;
- владение в полном объеме информацией предоставляемой в комплекте документов к ПО.

Администратор ПО должен обладать высоким уровнем квалификации и практическим опытом по установке и настройке, администрированию программных компонентов, которые применяются в программных модулях ПО «Базис.Virtual Security», а так же:

- иметь профессиональные знания и практические навыки по системному администрированию;
- обладать опытом настройки взаимодействия с LDAP каталогами;
- иметь представление о работе виртуализации на базе QEMU-KVM;
- иметь знания по установке и администрированию серверных операционных систем семейства Astra Linux;
- иметь высокий уровень квалификации и практический опыт по администрированию СУБД (MongoDB и Postgresql), применяемых в программных модулях;
- иметь опыт работы с хранилищами NFS, ISCSI, FC;
- иметь навыки настроек сетевой инфраструктуры на базовом уровне (DHCP, LACP, PXE, VLAN и т.д.);
- иметь знания основных типов виртуализации: аппаратная и программная виртуализации, а также иметь представление об уровнях виртуализации, уметь грамотно настраивать и обслуживать виртуальные системы, в случае критических сбоев оперативно возвращать их в работу.

Дополнительно к настоящему документу технические администраторы должны использовать документ RU.НРФЛ.00002-02 96 01 «Программное обеспечение «Базис.Virtual Security». Руководство по установке»

Действия по реализации функций безопасности среды функционирования

Действия по реализации функций безопасности среды функционирования ПО «Базис.Virtual Security» приведены в приложениях 1, 2 и 3 настоящего руководства.

В таблице 1 приведены наименования разделов в документации, где расположена информация о реализации функций безопасности в интерфейсе программных модулей.

Таблица 1.

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
1	Доверенная загрузка виртуальных машин	Блокировка запуска виртуальной машины при выявлении нарушения целостности конфигурации виртуального оборудования данной виртуальной машины	Базис.Virtual Security	Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Виртуализация Базис.Virtual Security >> Виртуальные машины
		Блокировка запуска виртуальной машины при выявлении нарушения целостности файлов виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины) и (или) исполняемых файлов гостевой операционной системы		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Виртуализация Базис.Virtual Security >> Виртуальные машины
2	Контроль целостности	Контроль целостности в процессе загрузки и динамически в процессе функционирования средства виртуализации объектов контроля самостоятельно или с применением сертифицированной хостовой операционной системы или средства доверенной загрузки	Базис.Virtual Security	Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Виртуализация Базис.Virtual Security >> Политики целостности
		Информирование администратора безопасности средства виртуализации о нарушении целостности объектов - контроля		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Виртуализация >> Витруальные машины Функционал Базис.Virtual Security >> Управление событиями Базис.Virtual Security

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
		Контроль целостности конфигурации виртуального оборудования виртуальных машин		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Виртуализация Базис.Virtual Security >> Виртуальные машины Функционал Базис.Virtual Security >> Виртуализация Базис.Virtual Security >> Политики целостности
3	Регистрация событий безопасности	Обеспечение регистрации событий безопасности, связанных с функционированием средства виртуализации	Базис.Virtual Security	Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Управление событиями Базис.Virtual Security
		Оповещение администратора безопасности средства виртуализации о событиях безопасности		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Оповещения пользователя Функционал Базис.Virtual Security >> Управление событиями Базис.Virtual Security
		Выполнение действия, являющегося реакцией на события безопасности самостоятельно или с применением - сертифицированных средств защиты информации		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Управление событиями Базис.Virtual Security
		Осуществление сбора и хранения записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Управление событиями

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
		Реализация перечня событий, необходимых для регистрации и учета для каждой функции безопасности		
		Регистрация номера (уникального идентификатора) события, даты, времени, типа события безопасности для регистрируемых событий безопасности в каждой записи журнала событий безопасности		
		Журнал событий безопасности средства виртуализации доступен только для чтения		
		Осуществление архивирования журнала с последующей очисткой высвобождаемой области памяти при исчерпании области памяти, отведенной под журнал событий безопасности средства виртуализации		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Управление событиями >> Настройки событий
		Обеспечение минимального перечня событий безопасности: • успешные и неуспешные попытки аутентификации пользователей средства виртуализации; • доступ пользователей средства виртуализации к виртуальным машинам; • создание и удаление виртуальных машин; • запуск и остановка средства виртуализации с указанием причины остановки; • запуск и остановка виртуальных машин с указанием причины остановки; • изменение ролевой модели; • изменение конфигурации средства виртуализации; • изменение конфигураций виртуальных машин; • факты нарушения целостности объектов контроля		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Управление событиями

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
		Регистрация описания события безопасности, включающее сведения о его важности, в каждой записи журнала событий безопасности		
4	Управление доступом	Реализация ролевого метода управления доступом с четырьмя ролями пользователей: • разработчик виртуальной машины; • администратор безопасности средства виртуализации; • администратор средства виртуализации; • администратор виртуальной машины	Базис.Virtual Security	Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Управление параметрами безопасности >> Роли Базис.Virtual Security Функционал Базис.Virtual Security >> Управление параметрами безопасности >> Пользователи Базис.Virtual Security Функционал Базис.Virtual Security >> Управление параметрами безопасности >> Группы Базис.Virtual Security
		Роль разработчика виртуальной машины позволяет: • создавать виртуальные машины; • изменять конфигурации виртуальных машин.	Базис .DynamiX ›	Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 2. Программный модуль «Базис.DynamiX» >> Действия по реализации функций безопасности программного модуля Базис.DynamiX>> Разделение обязанностей полномочий (ролей), администраторов и лиц, обеспечивающих функционирование информационной системы Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 2. Программный модуль «Базис.DynamiX» >> Доступ>>Управление доступом
		Роль администратора безопасности средства виртуализации позволяет: • осуществлять доступ на чтение к журналу событий безопасности средства виртуализации; • формировать отчеты с учетом заданных критериев отбора, выгрузки (экспорт) данных из журнала событий безопасности средства виртуализации.		

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
		Роль администратора средства виртуализации позволяет: • создавать учетные записи пользователей средства виртуализации; • управлять учетными записями пользователей средства виртуализации; • назначать права доступа пользователям средства виртуализации к виртуальным машинам; • создавать и удалять виртуальное оборудование средства виртуализации; • изменять конфигурации виртуального оборудования средства виртуализации; • управлять доступом виртуальных машин к физическому и виртуальному оборудованию; • управлять квотами доступа виртуальных машин к физическому и виртуальному оборудованию; • управлять перемещением виртуальных машин; • удалять виртуальные машины; • запускать и останавливать виртуальные машины; • создавать снимки состояния виртуальных машин, включающих файл конфигурации виртуальной машины, образа виртуальной машины и образа памяти виртуальной машины		
		Роль администратора виртуальной машины должна позволять осуществлять доступ пользователя средства виртуализации к виртуальной машине посредством интерфейса средства виртуализации		
		Обеспечение возможности определения полномочий для пользователей средства виртуализации в пределах назначенных им ролей		

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
		Применение средства криптографической защиты информации, прошедшее процедуру оценки соответствия в соответствии с законодательством Российской Федерации, в целях обеспечения удаленного доступа пользователей с использованием сетей связи общего пользования к средству виртуализации		
5	Резервное копирование	Обеспечение резервного копирования образов виртуальных машин и конфигурации виртуального оборудования виртуальных машин самостоятельно или с применением хостовой операционной системы или сертифицированных средств резервного копирования	Базис.Virtual Security	Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал >> Виртуализация>>Виртуальные машины Базис.Virtual Security>>Конфигурация
		Обеспечение резервного копирования параметров настройки средства виртуализации		Программное обеспечение «Базис.Virtual Security». Руководство по установке. Часть 3. Программный модуль «Базис.vCore» Обновление «Базис.vCore»
		Обеспечение резервного копирования сведений о событиях безопасности		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал Базис.Virtual Security >> Управление событиями >> События

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
6	Ограничение программной среды в средстве виртуализации	Осуществление контроля за запуском компонентов программного обеспечения, обеспечивающего выявление и блокировку запуска компонентов программного обеспечения, не включенных в перечень (список) компонентов, разрешенных для запуска	Базис.Virtual Security Базис.vCore	Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал >>Виртуализация>>Политики целостности Руководство администратора программного модуля Базис.Virtual Security. Часть 3. Программный модуль Базис.vCore >> Функциональность Базис.vCore>>Гипервизор Базис.vCore>>Защита памяти
		Осуществление контроля за запуском компонентов программного обеспечения, обеспечивающий: • выявление и блокировку запуска компонентов программного обеспечения, целостность которого нарушена; • блокировку запуска компонентов программного обеспечения, не прошедших аутентификацию с использованием свидетельств подлинности модулей (в том числе цифровых сигнатур производителя или иных свидетельств подлинности модулей)		
7	Управление потоками информации	Обеспечение управления потоками информации между виртуальными машинами и информационными (автоматизированными) системами на канальном и сетевом уровнях самостоятельно или с применением сертифицированных средств управления потоками информации (коммутаторов, маршрутизаторов) и (или) межсетевых экранов, а также контроль взаимодействия виртуальных машин между собой	Базис.Virtual Security	Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Виртуализация>>Сетевые фильтры Базис.Virtual Security

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
8	Защита памяти	Очищение остаточной информации в памяти средства вычислительной техники при ее освобождении (распределении) или блокировании доступа субъектов к остаточной информации	Базис.vCore	Руководство администратора программного модуля Базис.Virtual Security. Часть 3. Программный модуль Базис.vCore >> Функциональность Базис.vCore>>Гипервизор Базис.vCore>>Защита памяти
		Удаление объектов файловой системы, используемых средством виртуализации, путем перезаписи уничтожаемых (стираемых) объектов файловой системы случайной битовой последовательностью		
		Размещение кода средства виртуализации в области памяти, не доступной одновременно для записи и исполнения		
		Изоляция области памяти виртуальных машин		
9	Идентификация и аутентификация пользователей	Осуществление первичной идентификации пользователей средства виртуализации администратором средства виртуализации	Базис.Virtual Security	Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал >> Управление доменами>>Вкладка "Безопасность">>Параметры входа Функционал >>Управление параметрами безопасности >>Пользователи>>Создание пользователя
		Блокировка доступа пользователей в средстве виртуализации в случае неуспешной идентификации и аутентификации		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал >> Управление доменами>>Вкладка "Безопасность">>Параметры обнаружения перебора паролей

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
		Осуществление аутентификации пользователей при предъявлении идентификатора и пароля пользователя		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал >> Управление доменами>>Вкладка "Безопасность">>Параметры входа Функционал >>Управление параметрами безопасности >>Пользователи>>Создание пользователя
		Обеспечение возможности смены установленного администратором средства виртуализации пароля пользователя средства виртуализации после его первичной аутентификации		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал >> Управление доменами>>Вкладка "Безопасность">>Параметры входа
		Обеспечение невозможности установления одинаковых идентификаторов и паролей для разных пользователей		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал >>Аутентификация>>Политика паролей
		Вывод сообщения с приглашением ввести правильный идентификатор и пароль еще раз при попытке ввода неправильного значения идентификатора или пароля пользователя		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал >> Аутентификация >> Вход в систему

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
		Блокировка с возможностью разблокировки администратором средства виртуализации или с возможностью автоматической разблокировки по истечении временного интервала, устанавливаемого администратором средства виртуализации при исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетной записи пользователя средства виртуализации		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал >> Управление доменами>>Вкладка "Безопасность">>Параметры обнаружения перебора паролей
		Обеспечение защиты пароля пользователя средства виртуализации при его вводе за счет отображения вводимых символов условными знаками		Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» >> Функционал >> Управление доменами>>Вкладка "Безопасность">>Параметры входа
		Обеспечение хранения аутентификационной информации пользователя средства виртуализации в защищенном формате или в защищенном хранилище		Хранение аутентификационной информации пользователя осуществляется в базе данных программного модуля «Базис.Virtual Security» в зашифрованном виде без доступа для непривилегированных пользователей.
10	Централизованное управление образами виртуальных машин и виртуальными машинами	Средство виртуализации позволяет: • создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе; • обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности средства виртуализации	Базис .DynamiX	Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 2. Программный модуль «Базис.DynamiX» >> Действия по реализации функций безопасности программного модуля «Базис.DynamiX>> Централизованное управление образами виртуальных машин

№	Требования к средствам виртуализации	Реализация функций безопасности	Наименование выполняющего ФТ программного модуля	Расположение информации о реализации ФБ в РА программных модулей
		Обеспечение управления размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.		

Действия по приемке, установке и настройке ПО Базис.Virtual Security

Перед установкой ПО «Базис.Virtual Security» необходимо убедиться, что:

1. Комплектность Изделия соответствует комплектности поставки, указанной в Формуляре RU.НРФЛ.00002-02 30 01
2. На носителях информации, входящих в состав поставки, отсутствуют сколы, царапины, целостность этикеток и пломб не нарушены.
3. Контрольные суммы дистрибутива соответствуют заявленным в Формуляре RU.НРФЛ.00002-02 30 01

Действия по установке и настройке ПО «Базис.Virtual Security» приведены в руководстве по установке ПО «Базис.Virtual Security» RU.НРФЛ.00002-02 93 01 состоящий из трех частей:

- Программное обеспечение «Базис.Virtual Security». Руководство по установке. Часть 1. Программный модуль «Базис.Virtual Security» RU.НРФЛ.00002-02 93 01 Ч1;
- Программное обеспечение «Базис.Virtual Security». Руководство по установке. Часть 2. Программный модуль «Базис.DynamiX» RU.НРФЛ.00002-02 93 01 Ч2;
- Программное обеспечение «Базис.Virtual Security». Руководство по установке. Часть 3. Программный модуль «Базис.vCore» RU.НРФЛ.00002-02 93 01 Ч3.

Действия после сбоев и ошибок эксплуатации ПО Базис.Virtual Security

В случае возникновения ошибок в процессе эксплуатации ПО «Базис.Virtual Security» следует проинформировать предприятие-изготовителя путем отправки сообщения на электронную почту или посредством отправки запроса через службу технической поддержки организации по телефону 7 (495) 645-68-89 и электронной почте: support@basistech.ru[1], info@basistech.ru[2].

1 mailto:support@basistech.ru
2 mailto:info@basistech.ru

Часть 1. Программный модуль «Базис.Virtual Security»

Описание работы с программным модулем «Базис.Virtual Security» приведено в документе RU.НРФЛ.00002-02 95 01 Ч1 «Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 1. Программный модуль «Базис.Virtual Security» и прилагается к настоящему документу.

Часть 2. Программный модуль «Базис.DynamiX»

Описание работы с программным модулем «Базис.DynamiX» приведено в документе RU.НРФЛ.00002-02 95 01 Ч2 «Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 2. Программный модуль «Базис.DynamiX» и прилагается к настоящему документу.

Часть 3. Программный модуль «Базис.vCore»

Описание работы с программным модулем «Базис.vCore» приведено в документе RU.НРФЛ.00002-02 95 01 Ч3 «Программное обеспечение «Базис.Virtual Security». Руководство администратора. Часть 3. Программный модуль «Базис.vCore» и прилагается к настоящему документу.