Программное обеспечение «Базис.Virtual Security». Руководство по установке

RU.НРФЛ.00002-02 93 01

Москва

08/11/2023

Содержание

Аннотация

Настоящее руководство содержит описание действий по установке и настройке программного обеспечения ПО (далее Система, BVS).

Идентификационные данные

В руководстве по установке программного обеспечения «Базис.Virtual Security», кодовое обозначение RU.НРФЛ.00002-02, приводятся сведения об установке, настройке и обновлении программных модулей «Базис.Virtual Security», которые представлены в виде 3-х частей к настоящему руководству и имеют следующие идентификационные данные:

Идентификационные данные ПО	**Программное обеспечение «Базис.Virtual Security». Руководство по установке**
Название документа	Программное обеспечение «Базис.Virtual Security». Руководство по установке
Обозначение документа	RU.НРФЛ.00002-02 93 01
Название документа	Программное обеспечение «Базис.Virtual Security». Руководство по установке. Часть 1. Программный модуль «Базис.Virtual Security»
Обозначение документа	RU.НРФЛ.00002-02 93 01 Ч1
Название документа	Программное обеспечение «Базис.Virtual Security». Руководство по установке. Часть 2. Программный модуль «Базис.DynamiX»
Обозначение документа	RU.НРФЛ.00002-02 93 01 Ч2
Название документа	Программное обеспечение «Базис.Virtual Security». Руководство по установке. Часть 3. Программный модуль «Базис.vCore»
Обозначение документа	RU.НРФЛ.00002-02 93 01 Ч3
Автор документа	ООО «БАЗИС»

Общие сведения

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.

Требования к квалификации персонала

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»

Системные требования

ПО «Базис.Virtual Security» функционирует на компьютерах, имеющих следующие конфигурации вычислительной среды:

Требования к оборудованию программного модуля «Базис.DynamiX»

К аппаратному и программному обеспечению, которые используются для функционирования программного модуля «Базис.DynamiX», предъявляются требования, изложенные в таблице.

Таблица – Минимальные требования к программному и аппаратному обеспечению

Элемент	Параметр
Узлы вычисления среды виртуализации	
Операционная система	• Astra Linux Special Edition сертификат № 2557 (выдан ФСТЭК России 30.01.2012, действителен до 27.01.2026); • Альт 8 СП (релиз 10) сертификат № 3866 (выдан ФСТЭК России 10.08.2018, действителен до 10.08.2028).

Гипервизоры 1 типа	• Базис.vCore (для исполнения И1)
Библиотеки	• Libvirt 9.5; • qemu 7.2.
Процессор	• Процессор с тактовой частотой от 2.2 ГГц; • 8 ядер (для тестового и демонстрационного использования); • 10 ядер и больше (промышленного использования); • Поддерживаются процессоры двух типов: AMD64 и Intel64. Процессоры должны иметь поддержку аппаратной виртуализации AMD-V или Intel VT. Также необходимо наличие атрибута NX bit; • Поддерживаемые модели процессоров: • AMD: Семейство процессоров EPYC с микроархитектурой Zen и выше; • Intel: Семейство процессоров Xeon (5 и 6-го поколения) и выше.
Оперативная память	• 32 Гб (ECC) DDR4 2133 МГц (тестового и демонстрационного использования); • 256 Гб (ECC) DDR4 2133 МГц (для промышленного использования).
Жесткий диск	• Не менее двух SSD-дисков по 256 Гб.
Сетевой адаптер	• Не менее двух Ethernet-адаптеров 10 Гбит/сек (для тестового использования); • Для промышленного использования пропускная способность сети выбирается исходя из профиля сетевой нагрузки.
Контроллер управления	
Операционная система	• Astra Linux Special Edition сертификат № 2557 (выдан ФСТЭК России 30.01.2012, действителен до 27.01.2026); • Альт 8 СП (релиз 10) сертификат № 3866 (выдан ФСТЭК России 10.08.2018, действителен до 10.08.2028).

Процессор	• Процессор 8 ядер серверного класса и тактовой частотой от 2.2 ГГц;
	• Требования по архитектуре процессора: x86_64;
	• Поддерживаемые модели:
	  • AMD: с микроархитектурой Zen и выше;
	  • Intel: 5 и 6-го поколения.

Оперативная память	• 32 Гб (ECC) DDR4 2133 МГц (рекомендовано 64 ГБ для промышленной эксплуатации).
Жесткий диск	• Не менее двух SSD 960 Гб.
Сетевой адаптер	• Ethernet 10 Гбит/сек * 2 (для тестового использования); • Для промышленного использования пропускная способность сети выбирается исходя из профиля сетевой нагрузки.
Клиент	
Браузер	• Из состава ОС.

Сетевой адаптер	• Ethernet 100 Мбит/сек.
Монитор	• Диагональ от 17"; • Разрешение от 1280x1024 (4:3), от 1440x900 (16:9).
Периферийное оборудование	• Клавиатура; • Манипулятор типа мышь.

Требования к оборудованию программного модуля«Базис.vCore»

К аппаратному и программному обеспечению, которые используются для функционирования программного модуля «Базис.vCore», предъявляются требования, изложенные в таблице.

Таблица – Минимальные требования к программному и аппаратному обеспечению

Элемент	**Параметр**
Гипервизор 1 типа «Базис.vCore»	
Жесткий диск	• 100 ГБ и более (SSD серверного уровня); • Диск необходим, если требуется полноценная установка гипервизора на вычислительный узел и для локального сохранения конфигурации ВУ.
Оперативная память	• 32 ГБ (ECC) DDR4 2133 МГц и выше (рекомендовано 64 ГБ и более для промышленной эксплуатации).

Процессор	• Процессор с тактовой частотой от 2.0 ГГц:
	• 8 ядер ЦП (для тестового и демонстрационного использования);
	• 16 ядер и больше (для промышленного использования).
	• Поддерживаются процессоры двух типов: AMD64 и Intel64. Процессоры должны иметь поддержку аппаратной виртуализации AMD-V или Intel VT. Также необходимо наличие атрибута NX bit;
	• Поддерживаемые модели процессоров:
	  • AMD: Семейство процессоров EPYC с микроархитектурой Zen и выше;
	  • Intel: Семейство процессоров Xeon с микроархитектурой Skylake (6-го поколения) и выше.

Сетевой адаптер	• Ethernet 1 Гбит/сек. (для тестового использования); • Ethernet 10 Гбит/сек. (для промышленного использования).
Компонент управления	
Операционная система	• Astra Linux Special Edition сертификат № 2557 (выдан ФСТЭК России 27.01.2012, действителен до 27.01.2026); • Альт 8 СП (релиз 10) сертификат № 3866 (выдан ФСТЭК России 10.08.2018, действителен до 10.08.2028).

Процессор	• Процессор с тактовой частотой от 2.0 ГГц:
	• 8 ядер ЦП (для тестового и демонстрационного использования);
	• 16 ядер и больше (промышленного использования).
	• Требования по архитектуре процессора: x86_64;
	• Поддерживаемые модели:
	  • AMD: с микроархитектурой Zen и выше;
	  • Intel: с микроархитектурой Skylake (6-го поколения) и выше.

Оперативная память	• 16 ГБ (ECC), DDR4 2133 МГц и выше (рекомендовано 24 ГБ и более для промышленной эксплуатации).
Жесткий диск	• 2 x 100 ГБ в режиме RAID1 (SSD серверного уровня).
Сетевой адаптер	• Ethernet 1 Гбит/сек. (для тестового использования); • Ethernet 10 Гбит/сек. (для промышленного использования).
Клиент	
Браузер	• Из состава ОС.
Сетевой адаптер	• Ethernet 100 Мбит/сек.
Монитор	• Диагональ от 17"; • Разрешение от 1280x1024 (4:3), от 1440x900 (16:9).
Периферийное оборудование	• Клавиатура; • Манипулятор типа мышь.

Требования к оборудованию программного модуля«Базис.Virtual Security»

К аппаратному и программному обеспечению, которые используются для функционирования «Базис.Virtual Security», предъявляются требования, изложенные в таблице.

Таблица – Минимальные требования к программному и аппаратному обеспечению

Элемент	**Параметр**
Узлы вычисления среды виртуализации, на которых функционирует агентская часть программного модуля «Базис.Virtual Security»	
Операционная система	• Astra Linux Special Edition сертификат № 2557 (выдан ФСТЭК России 27.01.2012, действителен до 27.01.2026); • Альт 8 СП (релиз 10) сертификат № 3866 (выдан ФСТЭК России 10.08.2018, действителен до 10.08.2028).
Библиотеки	• Libvirt из состава ОС; • qemu из состава ОС.
Процессор	• В соответствии с требованиями ОС, установленной в среде виртуализации.
Оперативная память	• В соответствии с требованиями ОС, установленной в среде виртуализации и 512 МБ дополнительно.
Жесткий диск	• 1 ГБ.
Сетевой адаптер	• Ethernet 1 Гбит/сек.
СУБД	• Система управления базами данных «Postgres Pro» сертификат № 3637 (выдан ФСТЭК России 05.10.2016, действителен до 05.10.2024); • Система управления базами данных Postgres Pro Enterprise сертификат № 4063 (выдан ФСТЭК России 16.01.2019, действителен до 16.01.2029);

Процессор	• Процессор 4 ядра серверного класса с поддержкой виртуализации и тактовой частотой от 2.0 ГГц.
Оперативная память	• 16 ГБ.
Жесткий диск	• 10 ГБ.
Сетевой адаптер	• Ethernet 1 Гбит/сек.
Программный модуль «Базис.Virtual Security» для аутентификации в PostgreSQL	
СУБД	• Система управления базами данных «Postgres Pro» сертификат № 3637 (выдан ФСТЭК России 05.10.2016, действителен до 05.10.2024); • Система управления базами данных Postgres Pro Enterprise сертификат № 4063 (выдан ФСТЭК России 16.01.2019, действителен до 16.01.2029);
Операционная система	• Astra Linux Special Edition сертификат № 2557 (выдан ФСТЭК России 27.01.2012, действителен до 27.01.2026); • Альт 8 СП (релиз 10) сертификат № 3866 (выдан ФСТЭК России 10.08.2018, действителен до 10.08.2028);
Процессор	• x86_64.
Оперативная память	• 4 ГБ.
Жесткий диск	• 1 ГБ.
Клиент	
Браузер	• Из состава ОС
Сетевой адаптер	• Ethernet 100 Мбит/сек.
Монитор	• Диагональ от 17"; • Разрешение от 1280x1024 (4:3), от 1440x900 (16:9).
Периферийное оборудование	• Клавиатура; • Манипулятор типа мышь.
Программный модуль управления безопасностью API	
Операционная система	• Альт 8 СП (релиз 10) сертификат № 3866 (выдан ФСТЭК России 10.08.2018, действителен до 10.08.2028);
Процессор	• Процессор 4 ядра серверного класса с поддержкой виртуализации и тактовой частотой от 2.0 ГГц.
Оперативная память	• 8 ГБ.
Жесткий диск	• 10 ГБ.
Сетевой адаптер	• Ethernet 1 Гбит/сек.

Этапы установки

Установка программных модулей

Перед началом работы с ПО "Базис. Virtual Security" необходимо провести установку программных модулей и настройку интеграции ПО.

Установка модулей производится в произвольном порядке. Ознакомиться с инструкциями по установке программных модулей можно в следующих руководствах:

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

Процесс настройки интеграции ПО описан в разделе "Настройка провайдера аутентификации" настоящего руководства.

Настройка провайдера аутентификации

Для настройки интеграции выполните следующие действия:

1. Осуществить вход в программный модуль "Базис.Virtual Security (далее BVS) под учетной записью администратора.

2. В разделе домены выбрать домен "dynamix".

3. Перейти в раздел "Безопасность" → "Клиентские системы".

4. Создать клиентскую систему.

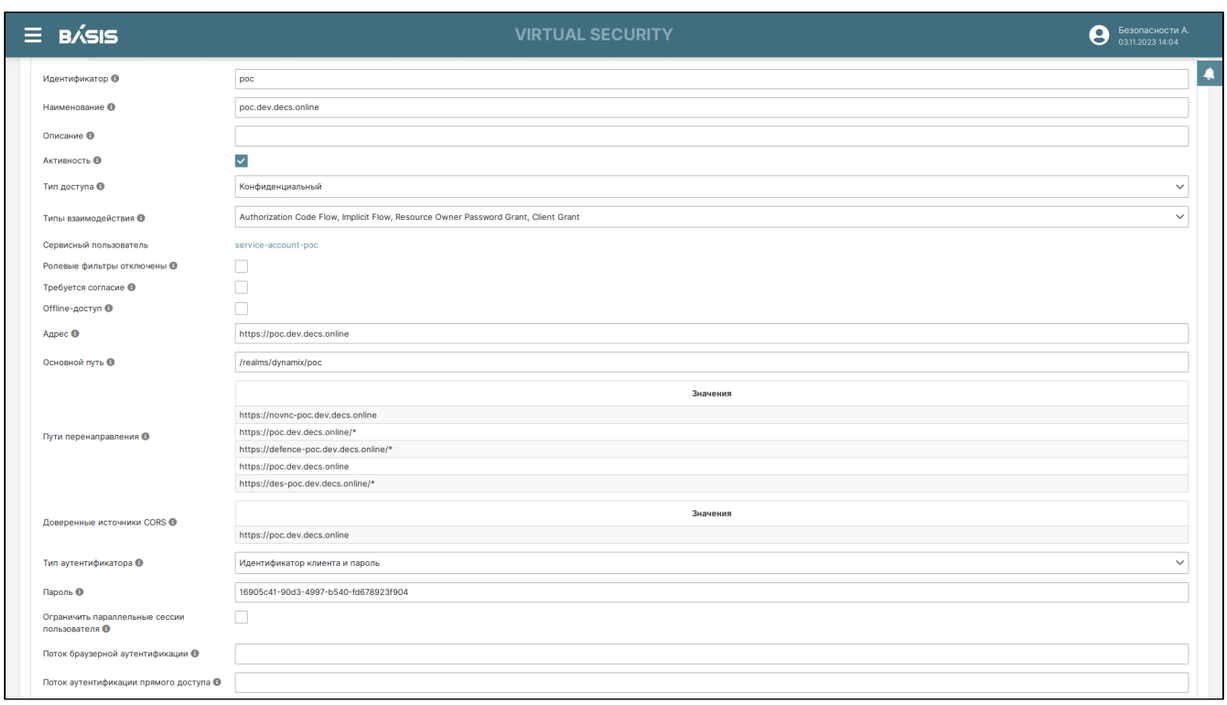

Рисунок 1 - Пример настройки клиентской системы

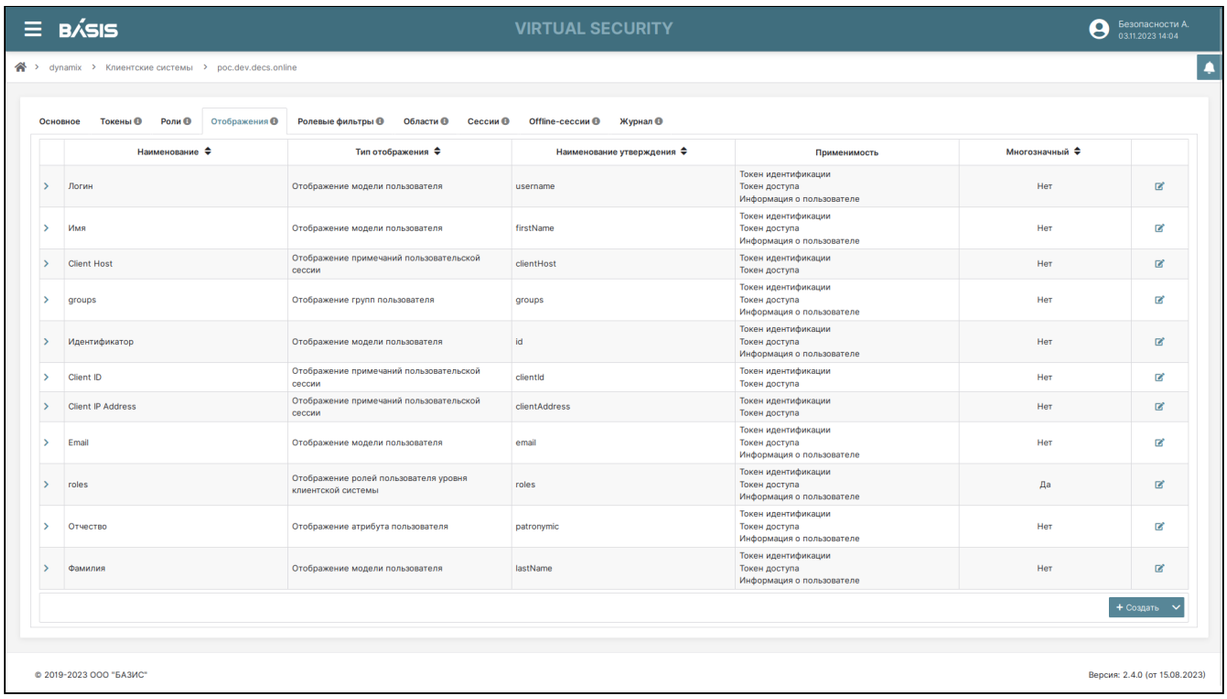

Рисунок 2 - Пример настройки отображений

5. Настроить DynamiX:

- если сертификат самоподписанный необходимо добавить его в доверенные на каждом управляющем узле и затем однократно перезапустить pod portal:

```
cp /root/tvs_one.pem /usr/local/share/ca-certificates/tvs_one.crt; update-ca-certificates

kubectl delete pod portal-*
```

- если отсутствует запись DNS, указывающая на имя bvs, и оно прописано только локально в директории /etc/hosts необходимо:
  - добавить имя и ip-адрес в kubectl edit deployment portal и перезапустить портал:

```
hostAliases:
 - hostnames:
 - bvs.d.gtp
   ip: 10.2.2.2
 - hostnames:
 - sso-portal.d.gtp
   ip: 10.1.1.1
```

- добавить в конфигурационный файл SYSTEM CONFIG новую секцию "bvs":

```
  "bvs":
      "bvsIp": |-
        <BVS IP>, i.e: 10.16.230.6
      "bvsServer": |-
        <BVS URL>, i.e: https://bvs-poc.dev.decs.online
```

```
      "bvsPort": |-
        <BVS PORT>, i.e: 8443
      "realmName": |-
        <BVS REALM NAME>, i.e: dynamix
      "clientId": |-
        <BVS CLIENT ID>, i.e: poc
      "clientSecret": |-
        <BVS_CLIENT SECRET>, i.e: 16905c41-90d3-4997
      "matchRoles": !!bool |-
        true/false - обозначаем, брать ли роли из информации о пользователе, в которых он состоит, для корректного добавления пользовательских групп apiaccess в портале
      "matchGroups": !!bool |-
        true/false - обозначаем, брать ли группы из информации о пользователе, в которых он состоит, для корректного добавления пользовательских групп apiaccess в портале
      "useOnlyBvsRules": !!bool |-
        true/false - обозначаем, если True. то при каждом входе пользователя его apiaccess группы будут строиться на основе roles и/или groups из BVS. (если matchRoles и matchGroups - False, то данное поле вне зависимости от написанного должно быть False, т.к. иначе при входе у пользователя при каждом входе не будут отсутствовать права)
      "ssh_port": !!int |-
        7022 - резервная опция под расширение поддержки zero-access на учётки bvs, оставляем 7022 для всех клиентов
```

- перезапустить поды/поды portal:

```
    "ssh_port": !!int |-
      7022
  "bvs":
    "bvsIp": |-
      10.16.230.6
    "bvsServer": |-
      https://bvs-poc.dev.decs.online
    "bvsPort": |-
      8443
    "realmName": |-
      dynamix
    "clientId": |-
      poc
    "clientSecret": |-
      16905c41-90d3-4997-b540-fd678923f904
    "matchRoles": !!bool |-
      true
    "matchGroups": !!bool |-
      true
    "useOnlyBvsRules": !!bool |-
      true
    "ssh_port": !!int |-
      7022
  "docker_registry":
    "password": |-
      password
    "server": |-
      registry-1:5000
    "username": |-
      username
  "environment":
```


Рисунок 3 - Перезапуск подов

6. Если все шаги выполнены правильно, то при аутентификации появится дополнительная кнопка "Login with BVS".

Обновление ПО

Обновление ПО (далее Система) производится обновлением программных модулей в произвольном порядке.

По окончании обновлений программных модулей производится общая настройка Системы.

Детальное описание обновления программных модулей представлено в следующих документах:

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

Процесс детальной настройки Системы описан в разделе "Настройка провайдера аутентификации" настоящего руководства.