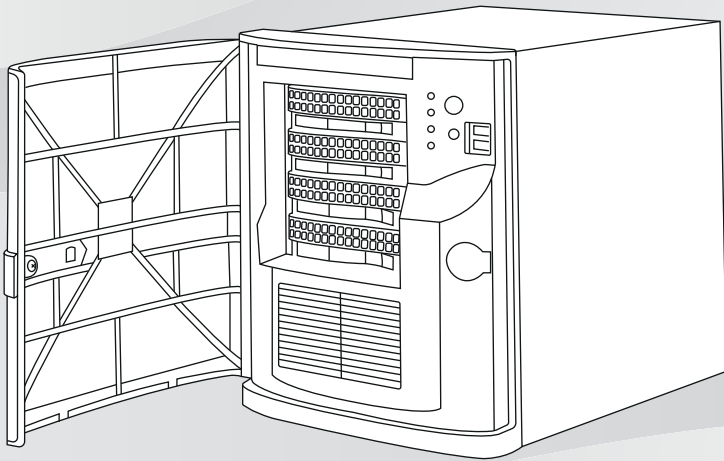




BOSCH

DIVAR IP all-in-one 5000

DIP-5240IG-00N | DIP-5244IG-4HD | DIP-5248IG-4HD |
DIP-524CIG-4HD | DIP-5240GP-00N | DIP-5244GP-4HD |
DIP-5248GP-4HD | DIP-524CGP-4HD



ru

Руководство по установке

Содержание

1	Правила техники безопасности	5
1.1	Общие правила техники безопасности	5
1.2	Правила электробезопасности	8
1.3	Меры предотвращения электростатических разрядов	9
1.4	Техника безопасности при эксплуатации	11
1.5	Правила техники безопасности данных	11
2	Введение	12
2.1	Комплектация	12
2.2	Регистрация продукта	13
3	Обзор системы	13
3.1	Внешний вид устройства	14
3.2	Элементы панели управления	17
4	Установка жесткого диска	19
4.1	Извлечение контейнера диска из отсека для жестких дисков	20
4.2	Установка жесткого диска в контейнер	21
4.3	Установка контейнера жесткого диска в отсек для жестких дисков	23
5	Настройка системы	23
5.1	Параметры по умолчанию	23
5.2	Необходимые условия	24
5.3	Режимы работы	24
5.4	Подготовка жестких дисков к видеозаписи	25
5.5	Запуск приложения	26
5.5.1	Работа в режиме полнофункциональной системы записи и управления видеоданными	28
5.5.2	Работа системы в режиме только видеозаписи	28
5.5.3	Работа в качестве расширения хранилища iSCSI	28
5.6	Использование BVMS Config Wizard	29
5.7	Добавление дополнительных лицензий	30
5.8	Использование BVMS Operator Client	31
6	Удаленное подключение к системе	32
6.1	Защита системы от несанкционированного доступа	32
6.2	Настройка перенаправления портов	33

6.3	Выбор подходящего клиента	33
6.3.1	Удаленное подключение к Operator Client	34
6.3.2	Удаленное подключение к приложению Video Security	34
7	Обслуживание	35
7.1	Мониторинг системы	35
7.2	Восстановление настроек устройства	35
7.3	Обслуживание и ремонт	37
8	Дополнительная информация	37
8.1	Дополнительная документация и клиентское программное обеспечение	37
8.2	Услуги поддержки и Bosch Academy	37

1 Правила техники безопасности

Ознакомьтесь с правилами техники безопасности в этом разделе.

1.1 Общие правила техники безопасности

Для обеспечения общей безопасности следуйте данным ниже правилам:

- Пространство вокруг системы должно быть чистым и незагромождено посторонними предметами.
- При снятии верхней крышки шасси или другой детали системы отложите ее в сторону или положите на стол, чтобы случайно не наступить на нее.
- При работе с системой не следует надевать свободную одежду, такую как галстуки и рубашки с расстегнутыми рукавами. Такая одежда может соприкоснуться с электрическими схемами или быть затянутой в охлаждающий вентилятор.
- Необходимо снять с себя все ювелирные изделия или металлические предметы, которые, являясь превосходными проводниками, могут вызвать короткое замыкание и нанести вред в случае контакта с печатными платами или элементами, находящимися под напряжением.

Предупреждение!

Отключение электропитания

Напряжение подается сразу после включения вилки кабеля питания в электророзетку.



Но если в устройстве имеется выключатель питания, устройство готово к работе, только когда выключатель питания включен (находится в положении ВКЛ.). Когда вилка кабеля питания вынута из розетки, подача питания на устройство полностью прекращается.

Предупреждение!

Снятие корпуса

Во избежание поражения электрическим током демонтаж корпуса должен производиться только квалифицированным сервисным специалистом.



Перед снятием корпуса вилка кабеля питания должна быть вынута из розетки и не должна включаться, пока корпус снят. Обслуживание должно выполняться только квалифицированным сервисным специалистом. Никакие виды ремонта пользователем не выполняются.

Предупреждение!

Шнур питания и адаптер переменного тока

При установке этого продукта используйте предоставленные или указанные соединительные кабели, шнуры питания и адаптеры переменного тока. Использование любых других кабелей или адаптеров может привести к неисправности или возгоранию. Закон об электроприборах и паспорте безопасности запрещает использование кабелей, сертифицированных по стандартам UL или CSA (которые имеют обозначение UL/CSA в коде) для любых других электрических устройств.

**Предупреждение!**

Литиевая батарея

Неправильно вставленные батареи могут взорваться. Всегда заменяйте разряженные батареи батареями того же типа или аналогичного, рекомендованного производителем.



С использованными батареями следует обращаться осторожно. Не допускайте повреждения батареи.

Повреждение батареи может привести к попаданию в окружающую среду вредных веществ.

Утилизируйте разряженные батареи в соответствии с инструкциями производителя или региональным законодательством.

**Предупреждение!**

Обработка материалов со свинцовым припоем, используемая в этом продукте, может подвергнуть вас воздействию свинца, известному в штате Калифорния как химическому элементу, вызывающему врожденные пороки и наносящие другой вред репродуктивной системе.

**Замечание!**

Устройство, чувствительное к электростатическому напряжению

Чтобы избежать электростатических разрядов, необходимо предпринять необходимые меры защиты КМОП/МОП-ПТ. При работе с печатными платами, чувствительными к электростатическому разряду, необходимо надевать заземленные антистатические манжеты и соблюдать соответствующие меры предосторожности.

**Замечание!**

Установка должна выполняться только квалифицированным сервисным специалистом в соответствии с действующими электротехническими нормами.

**Замечание!**

Операционная система включает в себя новейшие исправления безопасности Windows, доступные на момент создания ПО. Рекомендуется регулярно устанавливать обновленные исправления безопасности с помощью функции обновления Windows.

**Утилизация**

Данное изделие производства Bosch разработано и изготовлено с использованием высококачественных материалов и компонентов, которые можно использовать повторно.

Этот символ означает, что электронные и электрические устройства, отслужившие свой срок, должны утилизироваться отдельно от домашнего мусора.

В ЕС уже имеются системы раздельного сбора для использованных электрических и электронных изделий. Утилизируйте такие устройства в местном пункте сбора и переработки отходов.

1.2 Правила электробезопасности

Выполняйте следующие базовые правила электробезопасности, чтобы избежать получения травм и повреждения оборудования:

- Выясните, где на шасси расположен выключатель питания, а также где в помещении находится кнопка аварийного выключения, главный выключатель или электрическая розетка. Это позволяет в случае электротравмы быстро отключить питание от системы.
- Не работайте с находящимися под высоким напряжением компонентами в одиночку.
- Отсоедините кабели питания перед установкой или снятием каких-либо компонентов компьютера, включая объединительную панель.
- При отключении питания сначала выключается система, а затем отсоединяются шнуры питания от всех модулей источника питания системы.
- При работе с открытыми электрическими цепями необходимо, чтобы поблизости находился еще один человек, знающий расположение выключателей, чтобы при необходимости отключить питание.
- Для работы с включенным электрическим оборудованием следует использовать одну руку. Это позволяет избежать образования замкнутого контура, который может вызвать поражение электрическим током. С особой осторожностью следует использовать

металлические инструменты, которые при контакте легко могут повредить любые электрические компоненты или печатные платы.

- Вилки кабелей питания и электрические розетки должны быть заземлены. Устройство имеет несколько кабелей питания. Перед началом обслуживания отсоедините оба кабеля питания, чтобы избежать поражения электрическим током.
- Заменяемые впаянные предохранители системной платы: замена самовосстанавливающихся РТС (с положительным температурным коэффициентом) предохранителей системной платы должна производиться только квалифицированным специалистом по обслуживанию. Для замены следует использовать такие же или аналогичные предохранители. Для получения подробной информации и поддержки обратитесь в службу технической поддержки.

Внимание!



Элемент питания системной платы. Существует опасность взрыва, если элемент питания установлен в перевернутом положении (что приводит к изменению полярности). Для замены следует использовать только такие же или аналогичные элементы питания, рекомендованные производителем (CR2032). Использованные элементы питания следует утилизировать в соответствии с инструкциями производителя.

1.3 Меры предотвращения электростатических разрядов

Электростатический разряд (ESD) генерируется двумя вступающими в контакт объектами с различными электрическими зарядами. Электрический разряд направлен на выравнивание разности зарядов и может вызывать повреждение электронных компонентов и печатных плат. Для

нейтрализации разности зарядов до возникновения контакта и защиты оборудования от ESD обычно достаточно соблюдать следующие меры предосторожности:

- В качестве защиты от поражения электрическим током нельзя использовать коврики, предназначенные для уменьшения электростатического разряда. Вместо этого следует использовать резиновые коврики, которые специально созданы, чтобы служить электрическим изолятором.
- Рекомендуется использовать антистатический браслет, предназначенный для предотвращения статического разряда.
- Храните все компоненты и печатные платы (PCB) в антистатических пакетах до момента монтажа.
- Перед извлечением платы из антистатического пакета коснитесь заземленного металлического объекта.
- Следите, чтобы компоненты или печатные платы не касались вашей одежды, так как она может сохранять заряд, даже если вы надели антистатический браслет.
- Плату следует держать только за края. Не прикасайтесь к ее компонентам, периферийным микросхемам, модулям памяти и контактам.
- При обращении с микросхемами или модулями не следует касаться их контактов.
- Если системная плата и периферийные микросхемы не используются, поместите их обратно в антистатические пакеты.
- Для обеспечения заземления убедитесь, что шасси компьютера обеспечивает хорошую проводимость между источником питания, корпусом, креплениями и системной платой.

1.4 Техника безопасности при эксплуатации

Замечание!



Для обеспечения правильного охлаждения необходимо, чтобы во время работы системы крышка шасси была закрыта.

Несоблюдение этих мер может стать причиной негарантийного случая повреждения системы.

Замечание!



С использованными батареями следует обращаться осторожно. Не допускайте повреждения батареи.

Повреждение батареи может привести к попаданию в окружающую среду вредных веществ. Не выбрасывайте использованную батарею вместе с обычным мусором или на мусорные свалки. При утилизации батареи следуйте нормам, установленным отделом обработки опасных отходов в вашем регионе.

Предупреждение!



Соблюдайте осторожность при проведении обслуживания и работе с объединительной панелью. При эксплуатации системы на объединительной панели присутствует опасный уровень напряжения или энергии. Не прикасайтесь к объединительной панели никакими металлическими объектами и убедитесь, что плоские кабели не касаются панели.

1.5 Правила техники безопасности данных

В целях обеспечения безопасности данных необходимо соблюдать следующие правила.

- Физический доступ к системе должен быть предоставлен строго уполномоченному персоналу. Настоятельно рекомендуется поместить систему в охраняемую зону с контролем доступа во избежание физического вмешательства в работу системы.
-

- Для установки обновлений функций безопасности операционной системы можно использовать функции онлайн-обновления Windows или соответствующие ежемесячные накопительные пакеты исправлений для автономной установки.
- Настоятельно рекомендуется предоставлять доступ к локальной сети исключительно доверенным устройствам. Подробные сведения содержатся в техническом примечании Проверка подлинности в сети 802.1X и в Руководстве Bosch по безопасности IP-видео и данных, доступных в нашем веб-каталоге продукции.
- Для доступа через открытые сети используйте только защищенные (зашифрованные) каналы связи.

См.

- *Удаленное подключение к системе, Страница 32*

2 Введение

Перед началом установки прочитайте инструкции по безопасности и следуйте им.

2.1 Комплектация

Убедитесь в наличии всех компонентов и отсутствии повреждений. Если упаковка или какие-либо компоненты повреждены, свяжитесь со своим грузоотправителем. Если какие-либо компоненты отсутствуют, уведомите об этом торгового представителя Bosch Security Systems или представителя службы обслуживания заказчиков.

Количество	Компонент
1	DIVAR IP all-in-one 5000
1	Руководство по установке
1	Кабель питания, для Европы

Количество	Компонент
1	Кабель питания, для США
2	Ключи

2.2 Регистрация продукта

Зарегистрируйте свой продукт:

<https://www.boschsecurity.com/product-registration/>



3 Обзор системы

Устройство DIVAR IP all-in-one 5000 — это простая в использовании комплексная система записи, просмотра и управления для сетевых систем видеонаблюдения. DIVAR IP all-in-one 5000 — это интеллектуальное IP-устройство хранения, оснащенное комплексным решением BVMS (BVMS) и программным обеспечением Bosch Video Recording Manager (VRM), включая Bosch Video Streaming Gateway (VSG) для интеграции камер сторонних производителей, которое устраняет необходимость в отдельном сервере NVR (сетевом видеорегистраторе) и устройствах хранения. BVMS управляет всеми IP- и цифровыми видео- и аудиоданными, а также всеми данными безопасности, передаваемыми по IP-сети. Она эффективно объединяет IP-

камеры и кодеры, обеспечивает управление событиями и предупреждениями на уровне системы, мониторинг работоспособности системы, а также управление пользователями и приоритетами.

DIVAR IP all-in-one 5000 — это блок с 4 отсеками в корпусе «minitower», оснащенный жесткими дисками SATA с возможностью быстрой замены через переднюю панель. Простая установка и эксплуатация. Все системное программное обеспечение предварительно установлено; это устройство управления видеонаблюдением готово к немедленному использованию.

В устройствах DIVAR IP all-in-one 5000 используется операционная система Windows Storage Server 2016.

3.1 Внешний вид устройства

Система DIVAR IP all-in-one 5000 имеет компактное шасси типа «minitower». Передняя крышка на петлях закрывает жесткие диски и панель управления.

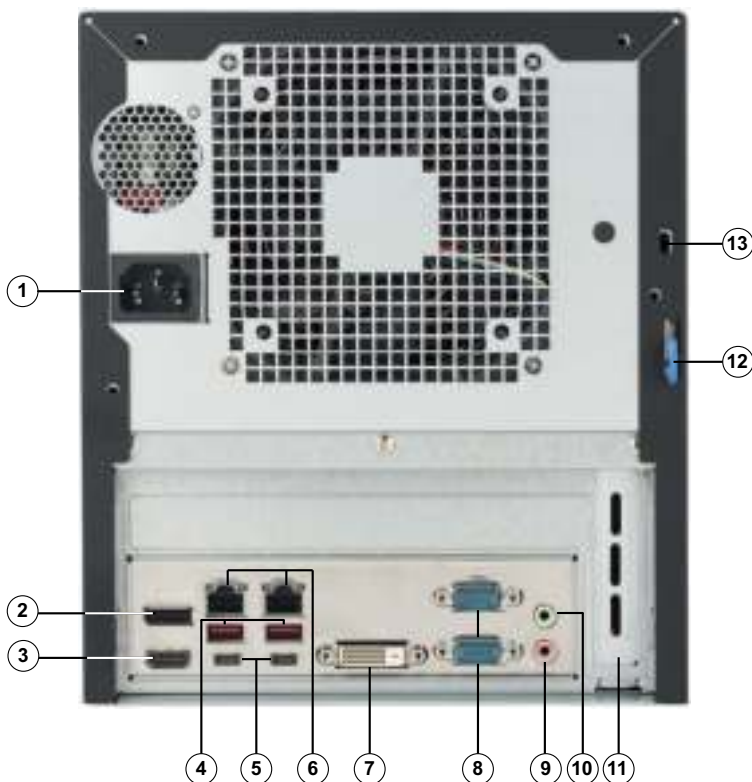
Панель управления расположена спереди и оснащена кнопками питания и светодиодными индикаторами состояния.

На задней панели размещены различные порты ввода-вывода.

Вид спереди

1	Передняя крышка	2	Замок передней крышки
3	4 порта для жестких дисков (3,5")	4	Впускной фильтр
5	Индикатор питания	6	Индикатор жесткого диска (не используется)
7	Индикатор сети	8	Индикатор информации
9	Кнопка сброса	10	2 порта USB 2.0
11	Кнопка включения / выключения питания		

Вид сзади




1	Подключение к сети электропитания	2	Порт DisplayPort
3	Порт HDMI 2.0	4	2 порта USB 3.1 (тип А)
5	2 порта USB 3.1 (тип С)	6	2 порта LAN (RJ-45), объединены Примечание: режим объединения отключать не следует!
7	Порт DVI-D	8	2 порта COM
9	Аудиовход MIC IN	10	Линейный аудиовыход


11	<p>Дополнительная видеокарта с 4 портами Mini DisplayPort (в этом случае для подключения монитора следует использовать порты Mini DisplayPort).</p> <p>Примечание: доступно только для DIP-5240GP-00N, DIP-5244GP-4HD, DIP-5248GP-4HD и DIP-524CGP-4HD.</p>	12	<p>Накладка заднего шасси (совместима с различными распространенными типами замков).</p> <p>Примечание: замки не входят в комплект.</p>
13	<p>Кенсингтонский разъем (для стандартного Кенсингтонского замка).</p> <p>Примечание: Кенсингтонский замок не входит в комплект.</p>		

3.2 Элементы панели управления





Панель управления расположена в передней части шасси и оснащена кнопками питания и светодиодными индикаторами состояния.

Кнопки панели управления

Кнопка	Описание
 <p>Питание</p>	<p>Кнопка питания используется для включения или отключения подачи питания от источника питания к системе.</p> <p>Примечание. При отключении питания системы с помощью этой кнопки основное питание отключается, но к системе продолжает подаваться резервное питание.</p>

Кнопка	Описание
	Для полного отключения питания отсоедините систему от электросети, прежде чем выполнять задачи техобслуживания.
 Сброс	Кнопка сброса используется для перезагрузки системы.

Светодиодные индикаторы на панели управления

Светодиоды	Описание	
 Питание	Этот светодиодный индикатор указывает на подачу питания к модулям источника питания системы. Во время работы системы данный индикатор должен гореть.	
 Жесткий диск	Данный индикатор не используется.	
 Сеть	Мигающий индикатор указывает на сетевую активность.	
 Информация	Состояние системы	Описание
	Непрерывно горит красным	Возникло состояние перегрева. (это может быть вызвано перегрузкой кабеля).

Светодиоды	Описание	
	Мигает красным (1 Гц)	Сбой вентилятора: проверьте работоспособность вентиляторов.
	Мигает красным (0,25 Гц)	Сбой питания: проверьте работоспособность источников питания.
	Постоянно горит синим	Активирован локальный UID. Используйте эту функцию для выбора устройства в стойке.
	Мигает синим (300 мс)	Активирован удаленный UID. Используйте эту функцию для выбора удаленного устройства.

4 Установка жесткого диска

Система DIVAR IP all-in-one 5000 оснащена четырьмя жесткими дисками с возможностью горячей замены. Жесткие диски устанавливаются в контейнерах жестких дисков, чтобы упростить их установку и извлечение из шасси. Эти контейнеры также помогают обеспечить правильное движение воздушного потока вокруг отсеков для жестких дисков.

Процедура

Для установки жесткого диска необходимо выполнить следующие действия.

1. *Извлечение контейнера диска из отсека для жестких дисков, Страница 20*
2. *Установка жесткого диска в контейнер, Страница 21*

3. *Установка контейнера жесткого диска в отсек для жестких дисков, Страница 23*

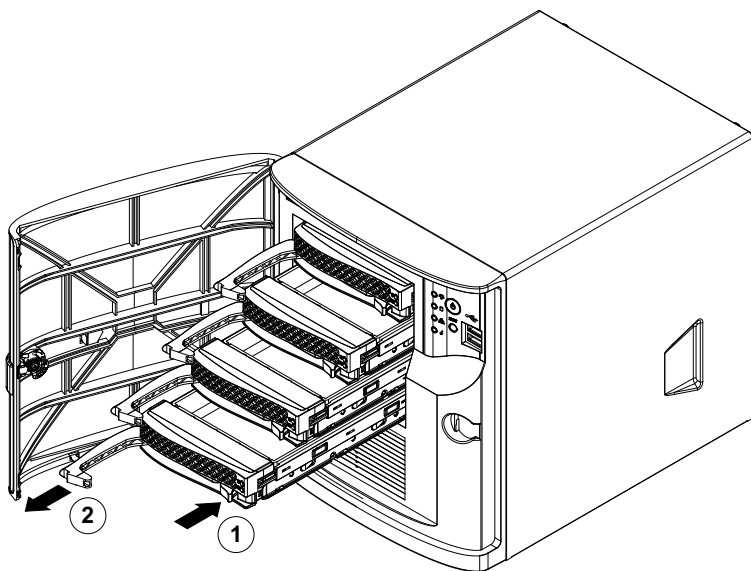
**Замечание!**

Перед работой с шасси просмотрите предупреждения и меры предосторожности, перечисленные в данном руководстве.

4.1 Извлечение контейнера диска из отсека для жестких дисков

Для извлечения контейнера диска из отсека для жестких дисков выполните следующие действия.

1. Разблокируйте переднюю крышку и откройте ее.
2. Нажмите кнопку разблокировки справа от контейнера жесткого диска. В результате выдвигается ручка контейнера жесткого диска.
3. Взявшись за ручку, извлеките корпус жесткого диска из шасси.



1	Кнопка разблокировки	2	Ручка контейнера жесткого диска
---	----------------------	---	---------------------------------

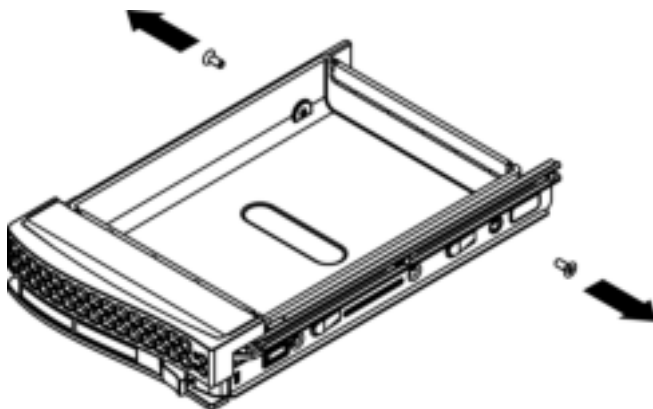
**Замечание!**

Не используйте устройство, когда контейнеры жестких дисков извлечены из отсеков.

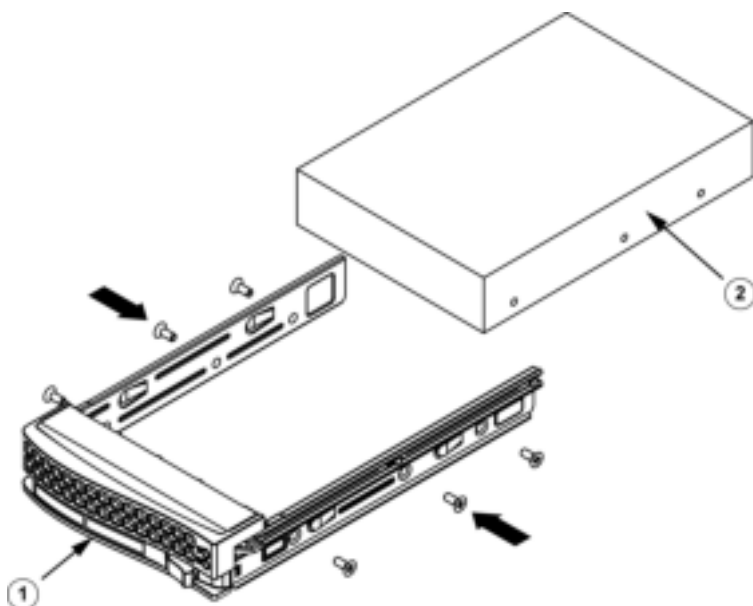
4.2 Установка жесткого диска в контейнер

Чтобы установить жесткий диск в контейнер, выполните следующие действия.

1. Извлеките винты, закрепляющие диск-заглушку в контейнере.



2. Извлеките диск-заглушку из контейнера и поместите контейнер жесткого диска на плоскую поверхность.
3. Вставьте новый жесткий диск в контейнер платой вниз.
4. Совместите монтажные отверстия контейнера с монтажными отверстиями жесткого диска.
5. Зафиксируйте жесткий диск в контейнере с помощью шести винтов.



1	Контейнер жесткого диска	2	Жесткий диск SATA
---	--------------------------	---	-------------------

Замечание!

Bosch рекомендует использовать соответствующие жесткие диски Bosch. Жесткий диск как один из критически важных компонентов тщательно выбирается Bosch на основе доступных процентов сбоя. Жесткие диски других производителей не поддерживаются.

Дополнительные сведения о поддерживаемых жестких дисках см. в таблице данных в веб-каталоге продуктов Bosch по адресу:

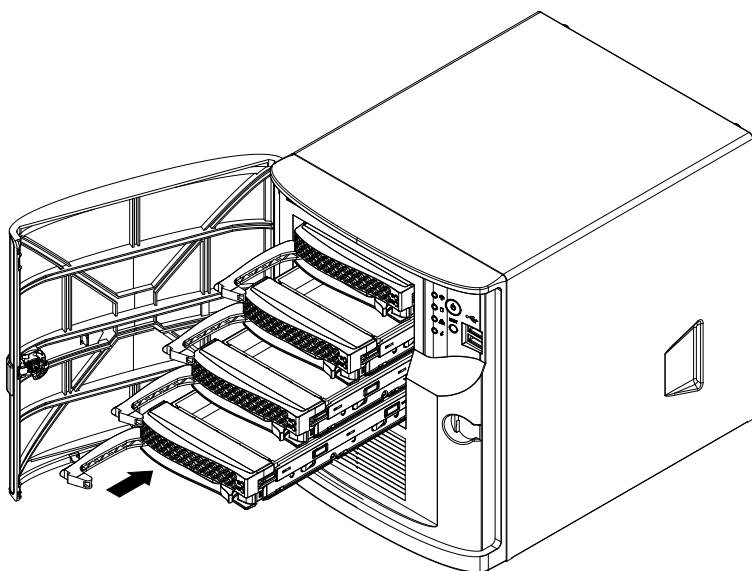
www.boschsecurity.com



4.3 Установка контейнера жесткого диска в отсек для жестких дисков

Чтобы установить контейнер жесткого диска в отсек для жестких дисков, выполните следующие действия.

1. Вставьте контейнер жесткого диска по горизонтали в отсек для жестких дисков, расположив контейнер жесткого диска так, чтобы кнопка разблокировки была справа.
2. Вставляйте контейнер жесткого диска в отсек до тех пор, пока не сложится ручка и контейнер не зафиксируется со щелчком.
3. Закройте и заблокируйте переднюю крышку.



5 Настройка системы

5.1 Параметры по умолчанию

Системы DIVAR IP поставляются с уже установленным на заводе мастером конфигурации.

Во всех системах DIVAR IP предварительно настроены IP-адрес и параметры iSCSI по умолчанию.

- IP-адрес назначается автоматически с помощью DHCP (резервный IP-адрес: 192.168.0.200).
- Маска подсети автоматически назначается с помощью DHCP (резервная маска подсети: 255.255.255.0).

Настройки пользователя по умолчанию для учетной записи администратора

- Пользователь: BVRAdmin
- Пароль: WSS4Bosch

5.2 Необходимые условия

Соблюдайте следующие правила:

- DIVAR IP требуется активное сетевое соединение во время установки. Убедитесь, что включен сетевой коммутатор, к которому вы подключаетесь.
- IP-адрес по умолчанию не должен быть занят другими устройствами в сети. Перед добавлением еще одной системы DIVAR IP убедитесь, что IP-адреса по умолчанию существующих в сети систем DIVAR IP изменены.
- Определите, проходит ли первоначальная установка в сети DHCP. Если нет, необходимо присвоить видеоустройствам действительные IP-адреса. Чтобы получить действительные IP-адреса, которые можно использовать с DIVAR IP и связанными устройствами, свяжитесь с ИТ-администратором сети.
- Параметры iSCSI по умолчанию можно оптимизировать с помощью VRM.

5.3 Режимы работы

Режимы работы

Системы DIVAR IP all-in-one могут работать в трех разных режимах.

- Полнофункциональная система записи и управления видеоданными с использованием базовых компонентов и служб BVMS и VRM: данный режим включает дополнительные функции управления видеоданными, такие как обработка событий и сигналов тревоги.
- Только система видеозаписи с использованием основных компонентов и служб VRM.
- Расширение хранилища iSCSI для системы BVMS или VRM, установленных на другом оборудовании.

**Замечание!**

Записанные видеопотоки должны быть настроены так, чтобы не превышалась максимальная полоса пропускания (основной системы BVMS/VRM, а также расширения хранилища iSCSI).

5.4 Подготовка жестких дисков к видеозаписи

Системы, предварительно оснащенные заводскими жесткими дисками, готовы к записи сразу после распаковки. Жесткие диски, которые были добавлены к пустой системе, необходимо подготовить (отформатировать), прежде чем использовать их для видеозаписи.

Доступны следующие способы форматирования жесткого диска.

- Выполнение первоначальной заводской настройки: см. *Восстановление настроек устройства, Страница 35.*
- Выполнение сценария форматирования.

Выполнение сценария форматирования

Чтобы выполнить сценарий форматирования, необходимо войти в учетную запись администратора (BVRAdmin).

1. Запустите систему.
2. На экране BVMS по умолчанию нажмите клавиши CTRL +ALT+DEL.

3. Удерживайте клавишу SHIFT, нажмите **сменить пользователя** и продолжайте удерживать SHIFT в течение примерно пяти секунд.
4. Введите имя пользователя и пароль администратора.
5. На рабочем столе в папке **Инструменты** нажмите правой кнопкой мыши сценарий **Format_data_hard_drives** и выберите **Запуск от имени администратора**.
6. Следуйте инструкциям.
7. После завершения форматирования можно добавить хранилище в конфигурацию управления видеоданными.

**Замечание!**

При форматировании жесткого диска с него удаляются все существующие данные.

5.5 Запуск приложения

Это приложение представляет собой простое в установке и использовании решение для сетевых систем видеонаблюдения.

Запуск приложения.

1. Подключите устройство и камеры к сети.
2. Включите устройство.
Запускается процесс настройки Windows Storage Server 2016.
3. Выберите подходящий язык для установки и нажмите кнопку **Далее**.
4. В списках **Страна или регион**, **Формат времени и денежных единиц** и **Раскладка клавиатуры** выберите нужные настройки и нажмите кнопку **Далее**.
На экране появятся Microsoft Software License Terms и EULA (лицензионное соглашение с конечным пользователем).
5. Подтвердите принятие условий лицензионного соглашения и нажмите кнопку **Пуск**. Windows перезагрузится.

6. После перезагрузки, нажмите сочетание клавиш CTR+ALT+DELETE. Откроется экран входа в систему Windows.
7. Введите пароль по умолчанию **WSS4Bosch**.
8. После ввода пароля появится сообщение о необходимости сменить пароль перед первым входом в систему. Для подтверждения нажмите кнопку **OK**.
9. Измените пароль.
Набор скриптов выполнит важные задачи по настройке. Это может занять некоторое время. Не выключайте компьютер.
Откроется экран BVMS по умолчанию.
Теперь вы можете решить, какой режим работы системы подходит вам.
 - *Работа в режиме полнофункциональной системы записи и управления видеоданными, Страница 28*
 - *Работа системы в режиме только видеозаписи, Страница 28*
 - *Работа в качестве расширения хранилища iSCSI, Страница 28*

**Замечание!**

Если вы забыли пароль, восстановление системы осуществляется в соответствии с руководством по установке. Конфигурация осуществляется с нуля или импортируется.

**Замечание!**



Настоятельно рекомендуется не изменять параметры операционной системы. Изменение параметров операционной системы может привести к ее сбою.

**Замечание!**

Для выполнения административных задач необходимо войти в учетную запись администратора.

5.5.1 Работа в режиме полнофункциональной системы записи и управления видеоданными

Для работы системы DIVAR IP в режиме полнофункциональной системы записи и управления видеоданными выполните следующие действия.

1. На экране BVMS по умолчанию дважды щелкните значок  BVMSConfig Wizard () для запуска Config Wizard. Отобразится страница **Welcome**.
2. Настройте систему с помощью Config Wizard.

См.

– *Использование BVMS Config Wizard, Страница 29*

5.5.2 Работа системы в режиме только видеозаписи

Для работы системы DIVAR IP в режиме только видеозаписи необходимо войти в учетную запись администратора (BVRAAdmin) и внести следующие изменения в конфигурацию.

1. На экране BVMS по умолчанию нажмите клавиши CTRL +ALT+DEL.
2. Удерживайте клавишу SHIFT, нажмите **сменить пользователя** и продолжайте удерживать SHIFT в течение примерно пяти секунд.
3. Введите имя пользователя и пароль администратора.
4. На рабочем столе в папке **Инструменты** нажмите правой кнопкой мыши сценарий **Disable_BVMS** и нажмите кнопку **Запуск от имени администратора**.
5. Настройте Video Recording Manager (VRM) с внешней системы с помощью BVMSConfiguration Client или Configuration Manager.

5.5.3 Работа в качестве расширения хранилища iSCSI

Для работы DIVAR IP системы как расширения хранилища iSCSI необходимо войти в учетную запись администратора (BVRAAdmin) и внести следующие изменения в конфигурацию.

1. На экране BVMS по умолчанию нажмите клавиши CTRL +ALT+DEL.
2. Удерживайте клавишу SHIFT, нажмите **сменить пользователя** и продолжайте удерживать SHIFT в течение примерно пяти секунд.
3. Введите имя пользователя и пароль администратора.
4. На рабочем столе в папке **Инструменты** нажмите правой кнопкой мыши сценарий **Disable_BVMS_and_VRM** и нажмите кнопку **Запуск от имени администратора**.
5. Добавьте систему в качестве расширения хранилища iSCSI к внешнему серверу BVMS или VRM с помощью BVMSConfiguration Client или Configuration Manager.

5.6 Использование BVMS Config Wizard

Config Wizard предназначен для быстрой и легкой настройки конфигурации небольших систем. Config Wizard помогает настроить конфигурацию системы, включая VRM, систему iSCSI, камеры, профили записи и группы пользователей. Группы пользователей и их разрешения настраиваются автоматически. Можно добавлять или удалять пользователей и задавать пароли.

Config Wizard может получить доступ к Management Server только на локальном компьютере.

Активированную конфигурацию можно сохранить для последующего резервного копирования и импортировать эту конфигурацию позднее. После импорта импортированную конфигурацию можно изменить.

Config Wizard автоматически добавляет локальный VRM.

Ограничения

С помощью Config Wizard нельзя выполнить следующие задачи. В этих случаях следует использовать BVMS Configuration Client.

- корректировка расписаний;
- настройка систем без (или с несколькими) Video Recording Manager;

- настройка внешних устройств хранения;
- добавление Video Streaming Gateway;
- все дополнительные компоненты конфигурации помимо основной настройки (например, карты или тревоги).

Быстрое изменение конфигурации с помощью Config Wizard.

1. На экране BVMS по умолчанию дважды нажмите значок Config Wizard. Откроется страница **Welcome**.
2. Следуйте инструкциям мастера на экране.



Замечание!

Информацию о задачах, которые не могут быть выполнены с помощью Config Wizard, а также подробные сведения о Config Wizard, см. в руководстве BVMS, доступном в веб-каталоге продукции.

См.

- *Дополнительная документация и клиентское программное обеспечение, Страница 37*

5.7 Добавление дополнительных лицензий

Дополнительные лицензии можно добавить с помощью Configuration Client.

Чтобы активировать программное обеспечение:


1. Запустите Configuration Client.
2. В меню **Сервис** выберите пункт **Диспетчер лицензий....** Откроется диалоговое окно **Диспетчер лицензий**.
3. Установите флажки напротив программного обеспечения, функций и расширений, которые следует активировать. Для расширений введите количество лицензий.
Если вы получили информационный файл Bundle Information, нажмите **Импортировать пакетную информацию**, чтобы импортировать его.

4. Нажмите **Активировать**.
Откроется диалоговое окно **Лицензионное соглашение Активация**.
5. Запишите цифровую подпись компьютера или скопируйте ее в текстовый файл.
6. На компьютере с доступом в Интернет введите в браузер следующий URL-адрес:
`https://activation.boschsecurity.com`
Если у вас нет учетной записи для доступа в центр активации лицензий Bosch, можно создать новую запись (рекомендуется) или нажать ссылку для активации новой лицензии, не выполняя вход в систему. Если создается учетная запись и выполняется вход в систему до активации, License Manager сохраняет активации. Вы можете повторить это действие в любое время. Следуйте инструкциям для получения ключа активации лицензии.
7. Вернитесь к программе BVMS. В диалоговом окне **Лицензионное соглашение Активация** введите ключ активации лицензии, полученный от License Manager, и нажмите кнопку **Активировать**.
Пакет программного обеспечения активирован.

5.8 Использование BVMS Operator Client

BVMS Operator Client используется для проверки функций просмотра в реальном времени, записи и воспроизведения DIVAR IP.

Проверка функции просмотра изображения в реальном времени в Operator Client

1. На экране BVMS по умолчанию дважды нажмите значок Operator Client . Приложение запустится.

2. Введите следующие сведения и нажмите кнопку **ОК**.
Имя пользователя: admin
Пароль: пароль не требуется (если он не задан с помощью мастера)
Соединение: 127.0.0.1
3. Щелкните значок изображения в режиме реального времени. Откроется логическое дерево камер.
4. Выберите камеру и перетащите ее в окно изображения. Изображение камеры появляется, если камера назначена правильно.

Примечание.

Камеры в окне изображений, обозначенные красной точкой на значке камеры, отображаются в режиме реального времени.

Проверка функции записи в Operator Client

- ▶ Камеры, обозначенные в логическом дереве красной точкой на значке камеры, ведут запись.

Проверка функции воспроизведения в Operator Client

- ▶ Если камера просматривается в режиме воспроизведения, временная шкала перемещается.

Информацию о других функциях см. в руководстве BVMS, доступном в веб-каталоге продукции.

6 Удаленное подключение к системе

В данном разделе описываются действия, необходимые для доступа к системе DIVAR IP из сети Интернет.

6.1 Защита системы от несанкционированного доступа

Чтобы защитить систему от несанкционированного доступа, до ее подключения к Интернету рекомендуется установить надежный пароль. Чем сильнее пароль, тем надежнее ваша система будет защищена от несанкционированного доступа лиц и вредоносного ПО.

6.2 Настройка перенаправления портов

Чтобы получить доступ к системе DIVAR IP из сети Интернет через маршрутизатор с поддержкой NAT/PAT, в системе DIVAR IP и на маршрутизаторе необходимо настроить перенаправление портов.

Чтобы настроить перенаправление портов, выполните следующие действия.

- ▶ Введите следующие правила портов в настройках перенаправления портов на вашем Интернет-маршрутизаторе.
 - порт 5322 для доступа через тоннель SSH с помощью BVMSOperator Client.
 - порт 443 для HTTPS-доступа к VRM с помощью Video Security Client или Video Security App.
- Теперь система DIVAR IP доступна из сети Интернет.

6.3 Выбор подходящего клиента

В данном разделе описаны способы установки удаленного подключения к системе DIVAR IP через Интернет.

Существует 2 способа установления удаленного подключения.

- *Удаленное подключение к Operator Client, Страница 34.*
- *Удаленное подключение к приложению Video Security, Страница 34.*




Замечание!

Используйте только версии BVMSOperator Client или Video Security App, соответствующие DIVAR IP. Другие клиенты или приложения могут работать, но не поддерживаются.

6.3.1 Удаленное подключение к Operator Client

Для удаленного подключения к BVMSOperator Client выполните следующие действия.

1. Установите BVMSOperator Client на рабочей станции клиента.
2. По завершении установки запустите Operator Client с помощью настольного ярлыка .
3. Введите следующие данные, а затем нажмите **ОК**.
Имя пользователя: admin (или другой пользователь, если это предусмотрено настройками)
Пароль: введите пароль пользователя
Подключение: ssh://[public-IP-address-of-DIVAR-IP_all-in-one]:5322

6.3.2 Удаленное подключение к приложению Video Security

Для удаленного подключения к Video Security App выполните следующие действия.

1. В App Store компании Apple найдите BoschVideo Security.
2. Установите приложение Video Security на ваше устройство iOS.
3. Запустите приложение Video Security.
4. Выберите **Добавить**.
5. Введите общедоступный IP-адрес или имя dynDNS.
6. Убедитесь, что функция Secure Connection (SSL) активирована.
7. Выберите **Добавить**.
8. Введите следующие данные:
имя пользователя: admin (или другой пользователь, если это предусмотрено настройками)
Пароль: введите пароль пользователя

7 Обслуживание

7.1 Мониторинг системы

Система оснащена инструментами мониторинга ее работоспособности.

Для активации функции мониторинга войдите в учетную запись администратора (BVRAdmin).

1. На экране BVMS по умолчанию нажмите клавиши CTRL + ALT + DEL.
2. Удерживайте клавишу SHIFT, нажмите **сменить пользователя** и продолжайте удерживать SHIFT в течение примерно пяти секунд.
3. Введите имя пользователя и пароль.
4. На рабочем столе в папке **Инструменты** нажмите правой кнопкой мыши сценарий **Enable_SuperDoctor_5_Service** и выберите **Запуск от имени администратора**.
5. Дважды нажмите значок **SuperDoctor 5 Web** в той же папке.
6. Войдите в веб-интерфейс с помощью следующих учетных данных по умолчанию:
имя пользователя: ADMIN
пароль: ADMIN
7. Щелкните вкладку **Конфигурация**, а затем нажмите **Настройки пароля** и измените пароль по умолчанию.
8. Щелкните вкладку **Конфигурация**, а затем нажмите **Конфигурация тревог**.
9. Активируйте функцию **Запрос SNMP** и укажите IP-адрес приемника запросов SNMP.

7.2 Восстановление настроек устройства

Ниже описывается порядок восстановления образа устройства по умолчанию.

Восстановление образа устройства по умолчанию.

1. Запустите устройство и нажимайте клавишу **F7** во время самотестирования BIOS при включении питания. Появится меню восстановления настроек.
2. Выберите один из следующих параметров:
 - **Первоначальные заводские настройки:** восстановление образа устройства по умолчанию и удаление всех данных с жестких дисков.
или
 - **Восстановление системы (возврат к заводским настройкам):** восстановление образа устройства по умолчанию; данные с жестких дисков не будут удалены.

Примечание.

Функция **Восстановление системы** не подразумевает удаление видеоматериалов, хранящихся на жестких дисках, однако заменяет все данные операционной системы (включая настройки VMS) конфигурацией по умолчанию. Чтобы получить доступ к существующим видеоматериалам после восстановления, конфигурацию VRM необходимо экспортировать до восстановления системы и вновь импортировать после восстановления.

**Замечание!**

Не выключайте устройство, пока операция не будет завершена. Это может повредить носитель для восстановления устройства.

3. Устройство запускается с носителя для восстановления. В случае успешного выполнения настройки нажмите **Yes** для перезагрузки системы.
4. Windows выполнит первоначальную настройку операционной системы. После завершения настройки устройство перезагрузится.
5. После перезагрузки устройства вступят в силу настройки по умолчанию.

7.3 Обслуживание и ремонт

На систему хранения предоставляется трехлетняя гарантия. Претензии рассматриваются в соответствии с инструкциями по обслуживанию и технической поддержке Bosch. Устройства хранения поставляются с соглашением об обслуживании и поддержке исходного производителя. В случае неисправности устройства необходимо обращаться в службу технической поддержки Bosch, но обязательства по обслуживанию и технической поддержке исполняются производителями или партнерами. Чтобы организация производителя, ответственная за обслуживание и техническую поддержку, могла обеспечить указанный уровень обслуживания, систему необходимо зарегистрировать повторно. В противном случае будет обеспечиваться не указанный уровень обслуживания, а только максимально возможный. Список необходимой информации и сведения о том, куда ее отправить, можно найти в печатной документации, которая поставляется с каждым комплектом оборудования. Кроме того, эти данные можно найти в электронном формате в интернет-каталоге продукции Bosch.

8 Дополнительная информация

8.1 Дополнительная документация и клиентское программное обеспечение

Для получения дополнительной информации, загрузки программного обеспечения и документации посетите веб-сайт <http://www.boschsecurity.com> и перейдите на страницу соответствующего продукта в каталоге продуктов.

8.2 Услуги поддержки и Bosch Academy



Поддержка

Наша **служба поддержки** доступна по адресу <https://www.boschsecurity.com/xc/en/support/>.

Bosch Security and Safety Systems предоставляет поддержку по следующим направлениям:

- [Приложения и инструменты](#)
- [Информационное моделирование здания](#)
- [Ввод в эксплуатацию](#)
- [Гарантия](#)
- [Устранение неисправностей](#)
- [Ремонт и замена](#)
- [Безопасность продуктов](#)



Bosch Building Technologies Academy

Посетите веб-сайт академии Bosch Building Technologies Academy и получите доступ к **учебным курсам, видеоучебникам и документам**: <https://www.boschsecurity.com/xc/en/support/training/>



Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Нидерланды

www.boschsecurity.com

© Bosch Security Systems B.V., 2020