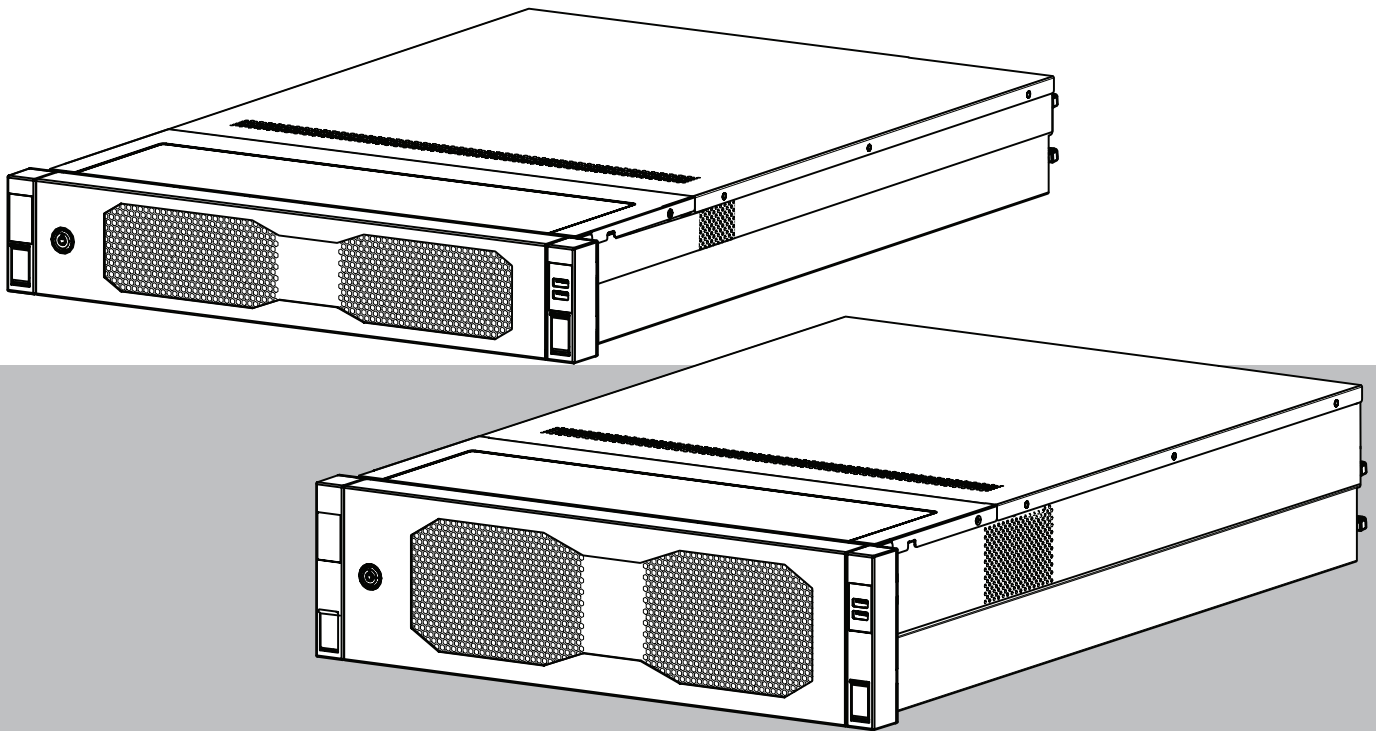


DIVAR IP all-in-one 7000 2U | DIVAR IP all-in-one 7000 3U

DIP-74C0-00N | DIP-74C4-8HD | DIP-74C8-8HD | DIP-74CI-8HD |
DIP-74CI-12HD | DIP-74G0-00N | DIP-74GI-16HD



Содержание

1	Обеспечение безопасности	4
1.1	Техника безопасности при эксплуатации	4
1.2	Правила техники кибербезопасности	5
1.3	Меры предосторожности при использовании программного обеспечения	6
1.3.1	Используйте самую актуальную версию ПО	6
1.3.2	Информация OSS	7
2	Введение	8
3	Общие сведения о системе	9
4	Настройка системы	10
4.1	Параметры по умолчанию	10
4.2	Необходимые условия	10
4.3	Первый вход в систему и первоначальная настройка системы	10
4.3.1	Выбор работы в режиме BVMS	12
4.3.2	Выбор работы в режиме VRM	13
4.3.3	Выбор работы в режиме iSCSI-хранилища	13
5	Обновление программного обеспечения	15
5.1	Обновление DIVAR IP System Manager	15
5.2	Обновление программного обеспечения с помощью DIVAR IP System Manager	15
6	Удаленное подключение к системе	18
6.1	Защита системы от несанкционированного доступа	18
6.2	Настройка перенаправления портов	18
6.3	Выбор подходящего клиента	18
6.3.1	Удаленное подключение с BVMS Operator Client	18
6.3.2	Удаленное подключение к приложению Video Security	19
6.4	Подключение к Enterprise Management Server	19
6.5	Подключение к Remote Portal	19
6.5.1	Создание учетной записи Remote Portal	20
6.5.2	Регистрация устройств DIVAR IP all-in-one на Remote Portal	20
6.5.3	Отмена регистрации устройств DIVAR IP all-in-one с Remote Portal	20
7	Обслуживание	21
7.1	Вход в систему под учетной записью администратора	21
7.2	Мониторинг системы	21
7.2.1	Мониторинг системы с помощью приложения ASUS Inband Tool	21
7.2.2	Мониторинг системы с помощью веб-интерфейса BMC	22
7.3	Замена неисправного жесткого диска и настройка нового жесткого диска	23
7.3.1	Замена неисправного жесткого диска	23
7.3.2	Восстановление RAID5 с использованием нового жесткого диска	23
7.4	Сбор файлов журналов DIVAR IP System Manager	24
7.5	Восстановление настроек устройства	24
8	Дополнительная информация	26
8.1	Дополнительная документация и клиентское программное обеспечение	26
8.2	Услуги поддержки и Bosch Academy	26

1 Обеспечение безопасности

Ознакомьтесь с правилами техники безопасности в этом разделе.

1.1 Техника безопасности при эксплуатации

**Замечание!**

Назначение

Этот продукт предназначен только для профессионального использования. Он не предназначен для установки в общественных местах, доступных для широкой публики.

**Замечание!**

Не используйте этот продукт в сырых или влажных помещениях.

**Замечание!**

Примите меры по защите устройства от коммутационных и грозовых перенапряжений.

**Замечание!**

Содержите пространство вокруг устройства в чистоте и не загромождайте его.

**Замечание!**

Отверстия в корпусе

Не закрывайте и не блокируйте отверстия. Все отверстия в корпусе предназначены для вентиляции. Эти отверстия предотвращают перегрев и обеспечивают надежную работу.

**Замечание!**

Не открывайте и не снимайте крышку устройства. Открытие или снятие крышки может привести к повреждению системы и аннулирует гарантию.

**Замечание!**

Не допускайте попадания жидкостей на устройство.

**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.

**Замечание!**

Отсоедините продукт от сети перед его перемещением. Перемещайте продукт с осторожностью. Избыточные усилия или сотрясения могут привести к повреждению продукта и жестких дисков.

**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!**

Поскольку потеря видеосигнала является сопутствующим явлением для цифровой видеозаписи, компания Bosch Security Systems не несет какой-либо ответственности за ущерб, причиненный потерей видеоинформации в архиве.

Для уменьшения риска потери информации рекомендуется использовать несколько резервных систем записи, а также резервное копирование всей цифровой и аналоговой информации.

1.2**Правила техники кибербезопасности**

В целях обеспечения кибербезопасности необходимо соблюдать следующие правила.

- Убедитесь, что физический доступ к системе предоставляется только уполномоченному персоналу. Поместите систему в охраняемую зону с контролем доступа во избежание физического вмешательства в ее работу.
- Для предотвращения несанкционированного снятия жестких дисков заблокируйте лицевую панель. Всегда извлекайте ключ из замка и храните его в надежном месте.
- Используйте функцию «Датчик проникновения в шасси» для обнаружения несанкционированного физического доступа внутрь устройства.
- Операционная система включает в себя новейшие исправления безопасности Windows, доступные на момент создания ПО. Для установки обновлений функций безопасности операционной системы используйте функции онлайн-обновления Windows или соответствующие ежемесячные накопительные пакеты исправлений для автономной установки.
- Всегда используйте актуальную версию браузера, чтобы обеспечить его безопасность и правильную работу.
- Не выключайте Защитник Windows и брандмауэр Windows и регулярно обновляйте их. Не устанавливайте дополнительное антивирусное программное обеспечение, которое может нарушить конфигурацию системы безопасности.
- Не предоставляйте системную информацию и конфиденциальные данные незнакомым вам людям, если вы не уверены в их полномочиях.
- Не отправляйте конфиденциальную информацию через Интернет до проверки безопасности сайта.
- Разрешите доступ к локальной сети только доверенным устройствам. Подробные сведения приведены в следующих документах, которые доступны в интернет-каталоге продуктов:
 - *Проверка подлинности сети 802.1X*
 - *Руководство по кибербезопасности для IP-видеосистем Bosch*
- Учетная запись администратора предоставляет полные административные привилегии и неограниченный доступ к системе. Права администратора позволяют пользователям устанавливать, обновлять или удалять программное обеспечение, а также изменять параметры конфигурации. Более того, права администратора позволяют пользователям напрямую получать доступ к ключам реестра и изменять

их, обходя централизованное управление и настройки безопасности. Пользователи, вошедшие в систему с учетной записью администратора, могут обходить брандмауэры и удалять антивирусное программное обеспечение, что подвергает систему риску вирусов и кибератак. Это может создать серьезную угрозу для системы и безопасности данных.

Чтобы минимизировать риски кибербезопасности, соблюдайте следующие правила.

- Убедитесь, что учетная запись администратора защищена сложным паролем в соответствии с правилами использования паролей.
- Убедитесь, что доступ к учетной записи администратора имеет только ограниченное число доверенных пользователей.
- В связи с требованиями эксплуатации системный диск не должен быть зашифрован. Без шифрования к данным, хранящимся на этом диске, можно легко получить доступ и удалить их. Чтобы избежать кражи или случайной потери данных, убедитесь, что доступ к системе и учетной записи администратора имеют только уполномоченные лица.
- Для установки и обновления программного обеспечения, а также для восстановления системы может потребоваться использование USB-устройств. Поэтому USB-порты вашей системы не должны быть отключены. Однако подключение USB-устройств к системе создает риск заражения вредоносным ПО. Чтобы избежать атак с использованием вредоносного ПО, убедитесь, что к системе не подключены зараженные USB-устройства.
- Не изменяйте настройки BIOS UEFI. Изменение настроек BIOS UEFI может нарушить безопасность системы или даже привести к ее неисправности.
- Систему BMC нельзя подключать к общедоступной сети.

1.3 Меры предосторожности при использовании программного обеспечения

1.3.1 Используйте самую актуальную версию ПО

Перед первым использованием устройства установите самую актуальную версию ПО. Для обеспечения оптимальных функциональных возможностей, совместимости, производительности и безопасности регулярно обновляйте ПО в течение всего срока эксплуатации устройства. Следуйте инструкциям в документации к продукту в отношении обновлений ПО.

Более подробную информацию можно получить по следующим ссылкам:

- общие сведения: <https://www.boschsecurity.com/xc/en/support/product-security/>
- рекомендации по безопасности, а именно список обнаруженных уязвимых мест и предлагаемых решений: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>
- Информацию о безопасности с описанием возможных последствий уязвимостей третьих сторон см. по адресу <https://www.boschsecurity.com/us/en/support/product-security/security-information.html>

Для получения новых рекомендаций по безопасности подписывайтесь на RSS-каналы на странице рекомендаций по безопасности Bosch Security and Safety Systems по адресу <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Компания Bosch не берет на себя никакой ответственности за какой-либо ущерб, вызванный эксплуатацией ее продуктов при использовании устаревшего ПО.

Последнюю версию программного обеспечения и доступные пакеты обновления можно найти в центре загрузки Bosch Security and Safety Systems по адресу:

<https://downloadstore.boschsecurity.com/>

1.3.2

Информация OSS

Компания Bosch использует в продуктах DIVAR IP all-in-one программное обеспечение с открытым исходным кодом.

Лицензии на используемые компоненты программного обеспечения с открытым исходным кодом можно найти на системном диске в каталоге:

```
C:\license txt\
```

Лицензии на компоненты программного обеспечения с открытым исходным кодом, используемые в любом другом программном обеспечении, которое установлено в вашей системе, хранятся в папке установки соответствующего программного обеспечения, например в папке:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-  
commander\[version]\License
```

или в папке:

```
C:\Program Files\Bosch\SysMgmService\apps\sysmgm-executor\[version]\License
```

2 Введение

DIVAR IP all-in-one 7000 – это недорогое, удобное в использовании комплексное решение для записи, просмотра и управления видео для сетевых систем видеонаблюдения с поддержкой до 256 каналов (8 каналов имеют предустановленную лицензию).

DIVAR IP all-in-one 7000 2U/3U представляет собой блок 2U/3U для монтажа в стойку. В этом экономичном, удобном для установки и эксплуатации устройстве видеозаписи объединены передовые функции и современные технологии управления записью Bosch Video Management System. Решение предназначено для клиентов, ориентированных на внедрение ИТ-технологий.

Модель DIVAR IP all-in-one 7000 имеет интегрированную конструкцию с базовыми компонентами и работает на основе операционной системы Microsoft Windows Server IoT 2022 for Storage Standard. Устройство оснащается жесткими дисками SATA корпоративного класса с возможностью «горячей» замены, при этом общая емкость хранилища может достигать 216/288 ТБ.

3

Общие сведения о системе

Операционная система

Операционная система Microsoft Windows Server IoT 2022 for Storage Standard предоставляет интерфейс пользователя для исходной настройки сервера и обеспечивает централизованное управление устройствами хранения, простоту установки и управления устройствами хранения, а также поддержку Microsoft iSCSI Software Target. Она специально настроена для обеспечения оптимальной производительности подключенного к сети хранилища данных. Операционная система Microsoft Windows Server IoT 2022 for Storage Standard предоставляет значительные улучшения в отношении сценариев управления хранением, а также интеграции компонентов управления и функциональных возможностей устройств хранения данных.

DIVAR IP System Manager

Приложение DIVAR IP System Manager представляет собой центральный пользовательский интерфейс, с помощью которого можно легко выполнять настройку системы, конфигурирование и обновление программного обеспечения.

Режимы работы

Системы DIVAR IP all-in-one 7000 могут работать в трех разных режимах.

- Полнофункциональная система записи и управления видео с использованием базовых компонентов и сервисов BVMS и Video Recording Manager. Этот режим позволяет реализовать передовое IP-решение для видеонаблюдения, обеспечивающее непрерывное управление цифровым видео, аудио и данными по IP-сети. В нем эффективно объединяются IP-камеры и кодеры, обеспечивается управление событиями и сигналами тревоги на уровне системы, мониторинг работоспособности системы, а также управление пользователями и приоритетами. В этом режиме применяется лучшая система управления видео для устройств видеонаблюдения Bosch, в которой используются уникальные возможности камер и решений для записи от Bosch. Эта система включает компоненты Video Streaming Gateway для интеграции камер сторонних производителей.
- Передовое решение для видеозаписи для системы BVMS, в котором используются базовые компоненты и службы Video Recording Manager, а также уникальные возможности камер и решений для записи от Bosch. В систему BVMS, работающую на устройстве DIVAR IP all-in-one, можно добавить до двух серверов Video Recording Manager.
- Расширение хранилища iSCSI для системы BVMS, работающей на другом оборудовании. В систему BVMS, работающую на устройстве DIVAR IP all-in-one 7000, можно добавить до четырех таких расширений хранилища iSCSI.

При настройке системы в приложении DIVAR IP System Manager необходимо выбрать требуемый режим работы для настройки системы.

С помощью приложения DIVAR IP System Manager также можно обновить установленное программное обеспечение.

Последнюю версию программного обеспечения и доступные пакеты обновления можно найти в центре загрузки Bosch Security and Safety Systems по адресу:

<https://downloadstore.boschsecurity.com/>



Замечание!

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

4 Настройка системы

4.1 Параметры по умолчанию

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

- Имя пользователя: **BVRAdmin**
- Пароль: задается при первом входе в систему.
Требования к паролю:
 - не менее 14 символов;
 - Пароль должен содержать символы из четырех категорий:
 - Не менее одной буквы в верхнем регистре.
 - Не менее одной буквы в нижнем регистре.
 - Не менее одной цифры.
 - Не менее одного специального символа.

4.2 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.

4.3 Первый вход в систему и первоначальная настройка системы



Замечание!

Не меняйте какие-либо параметры операционной системы. Изменение параметров операционной системы может привести к ее сбою.



Замечание!

Для выполнения административных задач необходимо войти в учетную запись администратора.



Замечание!

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





Замечание!

В целях безопасности будут отображаться диалоговые окна контроля учетных записей (УАС), запрашивающие подтверждение вносимых в систему изменений. Продолжить настройку можно только после соответствующего подтверждения.

Чтобы настроить систему, выполните следующие действия:

1. Подключите устройство DIVAR IP all-in-one и камеры к сети.
2. Включите устройство.
Дождитесь появления экрана BIOS и завершения процедур настройки Microsoft Windows Server IoT 2022 for Storage Standard. Этот процесс может занять несколько минут. Не выключайте систему.
По завершении процесса будет отображен экран выбора языка Windows.
3. Выберите страну или регион, язык операционной системы и раскладку клавиатуры из списка, а затем нажмите кнопку **Далее**.
Будут отображены условия лицензирования программного обеспечения Microsoft.
4. Нажмите кнопку **«Принять»**, чтобы принять условия лицензионного соглашения и дождитесь перезапуска Windows. Это может занять несколько минут. Не выключайте систему.
После перезапуска отобразится страница входа в Windows.
5. Задайте новый пароль для учетной записи администратора **BVRAdmin** и подтвердите его.
Требования к паролю:
 - не менее 14 символов;
 - Пароль должен содержать символы из четырех категорий:
 - Не менее одной буквы в верхнем регистре.
 - Не менее одной буквы в нижнем регистре.
 - не менее одной цифры.
 - Не менее одного специального символа.Нажмите клавишу Enter.
Отобразится страница **Software Selection**.
6. Система автоматически сканирует локальный диск и любые подключенные внешние носители на наличие установочного файла DIVAR IP System Manager (**SystemManager_x64_[software version].exe**), расположенного в папке по следующему пути: `Drive root\BoschAppliance\`.
Сканирование может занять некоторое время. Дождитесь его завершения.
7. После того как система обнаружит установочный файл, он отобразится на странице **Software Selection**. Нажмите на строку, в которой отображается файл установки, чтобы начать установку.
Примечание. Убедитесь, что установлена последняя версия DIVAR IP System Manager. Последнюю версию программного обеспечения и доступные пакеты обновления можно найти в центре загрузки Bosch Security and Safety Systems по адресу: <https://downloadstore.boschsecurity.com/>.
8. Если во время процесса сканирования файл установки не найден, выполните следующие действия.
 - Перейдите по адресу <https://downloadstore.boschsecurity.com/>.
 - На вкладке **Software** выберите **BVMS Appliances** из списка, а затем нажмите **Select**.
Отобразится список всех доступных пакетов программного обеспечения.
 - Найдите ZIP-файл **SystemManager_[software version].zip** и сохраните его на USB-накопитель или другой аналогичный носитель.
 - Распакуйте файл на носителе так, чтобы папка **BoschAppliance** находилась в корневом каталоге носителя.

- Подключите носитель к своей системе DIVAR IP all-in-one. Система автоматически просканирует носитель на наличие установочного файла. Сканирование может занять некоторое время. Дождитесь его завершения.
 - После обнаружения файла установки он будет отображен на странице **Software Selection**. Нажмите на строку, в которой отображается файл установки, чтобы начать установку.
Примечание. Чтобы установочный файл мог быть обнаружен автоматически, он должен находиться в папке со следующим путем: Drive root\BoschAppliance\
(например: F:\BoschAppliance\).
Если установочный файл находится в другом месте, которое не соответствует
- 
- указанной выше структуре папок, нажмите , чтобы перейти к соответствующему местоположению. Затем нажмите установочный файл, чтобы начать установку.
9. Перед началом установки отображается диалоговое окно **End User License Agreement (EULA)**. Прочитайте условия лицензионного соглашения и нажмите **Ассент** чтобы продолжить.
 10. В следующих диалоговых окнах контроля учетных записей нажимайте **Yes** чтобы продолжить. Начнется установка.
 11. После завершения установки система перезапустится и откроется страница входа в Windows. Выполните вход под учетной записью администратора.
 12. Откроется браузер Microsoft Edge и отобразится страница **DIVAR IP - Настройка системы**. На странице отображается тип устройства и его серийный номер, а также три режима работы и доступные версии программного обеспечения для каждого режима работы.
Для настройки системы DIVAR IP all-in-one необходимо выбрать требуемый режим работы и нужную версию программного обеспечения.
Примечание Если нужная версия программного обеспечения для соответствующего режима работы отсутствует на локальном диске, выполните следующее:
 - Перейдите по адресу <https://downloadstore.boschsecurity.com/>.
 - На вкладке **Software** выберите **BVMS Appliances** из списка, а затем нажмите **Select**.
Отобразится список всех доступных пакетов программного обеспечения.
 - Найдите ZIP-файлы нужных пакетов программного обеспечения (например, **BVMS_[BVMS version]_SystemManager_package_[package version].zip**) и сохраните их на USB-накопитель или другой аналогичный носитель.
 - Распакуйте файлы на носителе, не изменяя структуру содержащих их папок.
 - Подключите носитель к своей системе DIVAR IP all-in-one.

**Замечание!**

Изменение режима работы после установки требует полного восстановления заводских настроек.

4.3.1**Выбор работы в режиме BVMS**

Для эксплуатации системы DIVAR IP all-in-one в качестве полнофункциональной системы видеозаписи и управления видео выполните следующее:

1. На странице **DIVAR IP - Настройка системы** выберите режим работы **BVMS** и версию BVMS, которую нужно установить, а затем нажмите **Установить режим работы**.
Отобразится лицензионное соглашение BVMS.
2. Прочитайте и примите лицензионное соглашение, а затем нажмите **Да, установить** для продолжения.
Начнется установка, и в диалоговом окне будет показан ход установки. В процессе установки не выключайте систему и не извлекайте носитель информации.
3. После успешной установки всех пакетов программного обеспечения система перезапустится. После перезапуска откроется рабочий стол BVMS.
4. На рабочем столе BVMS нажмите требуемое приложение для настройки системы.

**Замечание!**

Дополнительные сведения можно найти в соответствующем онлайн-тренинге по DIVAR IP all-in-one и в документации BVMS.

Онлайн-тренинг доступен по адресу www.boschsecurity.com/xc/en/support/training/.

4.3.2**Выбор работы в режиме VRM**

Для эксплуатации системы DIVAR IP all-in-one в качестве только системы видеозаписи выполните следующее:

1. На странице **DIVAR IP - Настройка системы** выберите режим работы **VRM** и версию VRM, которую нужно установить, а затем нажмите **Установить режим работы**.
Отобразится лицензионное соглашение для VRM.
2. Прочитайте и примите лицензионное соглашение, а затем нажмите **Да, установить** для продолжения.
Начнется установка, и в диалоговом окне будет показан ход установки. В процессе установки не выключайте систему и не извлекайте носитель информации.
3. После успешной установки всех пакетов программного обеспечения система перезапустится. После перезапуска отобразится экран входа в Windows.

**Замечание!**

Для получения дополнительной информации см. документацию VRM.

4.3.3**Выбор работы в режиме iSCSI-хранилища**

Для работы системы DIVAR IP all-in-one в качестве расширения хранилища iSCSI выполните следующие действия:

1. На странице **DIVAR IP - Настройка системы** выберите режим работы **Хранилище iSCSI** и версию хранилища iSCSI, которую нужно установить, а затем нажмите **Установить режим работы**.
Отобразится диалоговое окно установки.
2. В диалоговом окне установки нажмите **Да, установить** для продолжения.
Начнется установка, и в диалоговом окне будет показан ход установки. В процессе установки не выключайте систему и не извлекайте носитель информации.
3. После успешной установки всех пакетов программного обеспечения система перезапустится. После перезапуска отобразится экран входа в Windows.
4. Добавьте систему в качестве расширения хранилища iSCSI к внешнему серверу BVMS или VRM с помощью BVMS Configuration Client или Configuration Manager.



Замечание!

Для получения дополнительной информации см. документацию BVMS или Configuration Manager.

5 Обновление программного обеспечения

Убедитесь, что обновляете DIVAR IP System Manager до последней версии.

5.1 Обновление DIVAR IP System Manager

1. Перейдите по адресу <https://downloadstore.boschsecurity.com/>.
2. На вкладке **Software** выберите **BVMS Appliances** из списка, а затем нажмите **Select**. Отобразится список всех доступных пакетов программного обеспечения.
3. Найдите ZIP-файл **SystemManager_[Версия ПО 2.3.0 или выше].zip** и сохраните его на носителе данных, например на USB-накопителе.
4. Распакуйте файл на носителе,
5. Подключите носитель данных к своему устройству DIVAR IP all-in-one.
6. Запустите DIVAR IP System Manager:
 - если вы вошли в Windows под учетной записью администратора **BVRAdmin**, дважды нажмите значок DIVAR IP System Manager на рабочем столе Windows. Запустится DIVAR IP System Manager.
 - Если система работает в режиме BVMS, нажмите значок DIVAR IP System Manager на рабочем столе BVMS и выполните вход в учетную запись администратора BVRAdmin. DIVAR IP System Manager откроет полноэкранное диалоговое окно (чтобы закрыть диалоговое окно, нажмите Alt+ F4).
7. Откроется страница **Программные пакеты**. Выберите пакет программного обеспечения DIVAR IP System Manager и нажмите **Установить пакет** для продолжения. Отобразится диалоговое окно установки.
8. В диалоговом окне установки нажмите **Да, установить** для продолжения. Начнется установка. Процесс установки может занять несколько минут. Не выключайте систему и не извлекайте информационный носитель во время установки. Следите за уведомлениями в верхней части страницы.

5.2 Обновление программного обеспечения с помощью DIVAR IP System Manager

С помощью приложения DIVAR IP System Manager установленное в вашей системе программное обеспечение можно обновить до более поздней версии.

Последнюю версию программного обеспечения и доступные пакеты обновления можно найти в центре загрузки Bosch Security and Safety Systems по адресу:

<https://downloadstore.boschsecurity.com/>





Замечание!

Понижение версии установленного программного обеспечения не поддерживается.

Для расширения возможностей установленного программного обеспечения выполните следующие действия:

1. Перейдите по адресу <https://downloadstore.boschsecurity.com/>.
2. На вкладке **Software** выберите **BVMS Appliances** из списка, а затем нажмите **Select**. Отобразится список всех доступных пакетов программного обеспечения.

3. Найдите ZIP-файлы нужных пакетов программного обеспечения (например, **BVMS_[BVMS version]_SystemManager_package_[package version].zip**) и сохраните их на USB-накопитель или другой аналогичный носитель.
4. Распакуйте файлы на носителе, не изменяя структуру содержащих их папок.
5. Запустите DIVAR IP System Manager:
 - если вы вошли в Windows под учетной записью администратора **BVRAdmin**, дважды нажмите значок DIVAR IP System Manager на рабочем столе Windows. Запустится DIVAR IP System Manager.
 - Если система работает в режиме BVMS, нажмите значок DIVAR IP System Manager на рабочем столе BVMS и выполните вход в учетную запись администратора BVRAdmin. DIVAR IP System Manager откроет полноэкранное диалоговое окно (чтобы закрыть диалоговое окно, нажмите Alt+ F4).
6. Отобразится страница **Программные пакеты**, в верхней части которой будут указаны тип устройства и его серийный номер.
 - В столбце **Имя пакета ПО** перечисляются все программные приложения DIVAR IP System Manager, уже установленные в системе, а также любые другие программные приложения DIVAR IP System Manager, которые были обнаружены системой на диске **Images** или на каком-либо подключенном носителе.
 - В столбце **Установленная версия** отображается версия программного приложения, установленная в системе в настоящее время.
 - В столбце **Статус** указывается состояние соответствующего программного приложения:
 - Значок  означает, что система не обнаружила более поздние версии установленного программного приложения на диске **Images** или на носителе. **Примечание.** Чтобы убедиться в том, что используется последняя версия программного обеспечения, проверьте все доступные версии программного обеспечения в центре загрузки Bosch Security and Safety Systems по адресу: <https://downloadstore.boschsecurity.com/>
 - Значок  означает, что система обнаружила более поздние версии установленного программного приложения на диске **Images** или на носителе. Этот значок также отображается, если система обнаружила программное приложение, которое еще не установлено в системе.
 - В столбце **Доступная версия** можно видеть более поздние версии установленных программных приложений. Это версии, которые были обнаружены системой на диске **Images** или на подключенном носителе. В столбце также отображаются доступные версии обнаруженных программных приложений, которые еще не установлены в системе. **Примечание.** Отображаются только более поздние версии установленных программных приложений. Понижение версии программного приложения не поддерживается.
7. В столбце **Имя пакета ПО** нажмите соответствующий переключатель для выбора программного приложения, которое нужно обновить или установить.
8. В столбце **Доступная версия** выберите нужную версию, до которой нужно обновить программное приложение или которую необходимо установить, а затем нажмите **Установить пакет**.

Отобразится диалоговое окно лицензионного соглашения (если это применимо).

9. Прочитайте и примите лицензионное соглашение, а затем нажмите **Да, установить**, чтобы продолжить.
Начнется установка, и в диалоговом окне установки будет отображаться ход ее выполнения. В процессе установки не выключайте систему и не извлекайте носитель.
10. После того как все пакеты программного обеспечения будут успешно установлены, вы получите подтверждение об успешной установке.
11. Если установка не увенчалась успехом, вы получите соответствующее сообщение, информирующее вас о том, как поступить в этом случае.

6 Удаленное подключение к системе

К системе DIVAR IP all-in-one можно подключиться удаленно и получать к ней доступ через Интернет.

Для создания удаленного подключения необходимо выполнить следующее:

1. *Защита системы от несанкционированного доступа, Страница 18.*
2. *Настройка перенаправления портов, Страница 18.*
3. *Выбор подходящего клиента, Страница 18.*

Можно подключиться к DIVAR IP all-in-one через Bosch Remote Portal и использовать текущие и последующие функциональные возможности, доступные на Remote Portal. Дополнительную информацию см. в разделе *Подключение к Remote Portal, Страница 19.*

6.1 Защита системы от несанкционированного доступа

Чтобы защитить систему от несанкционированного доступа, перед подключением системы к Интернету следует 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 all-in-one из сети Интернет через маршрутизатор с поддержкой NAT/PAT, в системе DIVAR IP all-in-one и в 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 BVMS Operator Client.
Примечание. Это подключение применимо только при работе в режиме BVMS.
- порт 443 для HTTPS-доступа к VRM с помощью Video Security Client или Video Security App.
Примечание. Это подключение применимо только при работе в режиме BVMS или VRM.

Теперь к DIVAR IP all-in-one можно получать доступ через Интернет.

6.3 Выбор подходящего клиента

Возможны два варианта удаленного подключения к системе DIVAR IP all-in-one:

- *Удаленное подключение с BVMS Operator Client, Страница 18.*
- *Удаленное подключение к приложению Video Security, Страница 19.*



Замечание!

Совместимость версий BVMS Operator Client или Video Security App определяется версиями программного обеспечения BVMS или VRM, установленного в DIVAR IP. Подробную информацию можно найти в документации и учебным материалам по соответствующему программному обеспечению.

6.3.1 Удаленное подключение с BVMS Operator Client



Замечание!

Это подключение применимо только при работе в режиме BVMS.

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 указанную ниже информацию, а затем нажмите **ОК**.

Имя пользователя: admin (или другое имя пользователя, если оно настроено)

Пароль: пароль пользователя

Подключение: ssh://[общедоступный-IP-адрес-DIVAR-IP_all-in-one]:5322

6.3.2

Удаленное подключение к приложению Video Security



Замечание!

Это подключение применимо только при работе в режиме BVMS или VRM.

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 следующую информацию:

Имя пользователя: admin (или другое имя пользователя, если оно настроено)

Пароль: пароль пользователя

6.4

Подключение к Enterprise Management Server

Для централизованного управления несколькими системами DIVAR IP all-in-one, работающими в режиме BVMS, можно использовать BVMS Enterprise Management Server, установленный на отдельном сервере.

Подробные сведения о настройке и эксплуатации BVMS Enterprise System можно найти в документации и учебных материалах по BVMS.

6.5

Подключение к Remote Portal

Вы можете подключиться к устройству DIVAR IP all-in-one через Bosch Remote Portal и использовать текущие и будущие функции, такие как служба Bosch Remote System Management, доступная через Remote Portal.

Подробную информацию о службе Remote System Management можно найти в документации и учебным материалам по Remote System Management.

Необходимые условия

Подключение Remote Portal

Для подключения устройств DIVAR IP all-in-one к Remote Portal обеспечьте соблюдение следующих условий:

- На устройстве должен быть установлен DIVAR IP System Manager 2.3.0 (или выше).
- Должна быть создана учетная запись Remote Portal.

Канал связи Remote Portal

Требования к подключению для связи с Remote Portal.

Примечание: Все подключения исходящие.

HTTPS (порт 443)

- <https://api.remote.boschsecurity.com/rest/iot/devices>
- <https://sw-repo-remote.s3.eu-central-1.amazonaws.com>

MQTTS (Port 8883)

- [tls://a1j83emmuys8gs-ats.iot.eu-central-1.amazonaws.com:8883](https://a1j83emmuys8gs-ats.iot.eu-central-1.amazonaws.com:8883)

6.5.1

Создание учетной записи Remote Portal

Чтобы создать учетную запись Remote Portal:

1. Откройте <https://remote.boschsecurity.com/login>.
2. Нажмите **Sign up**.
3. Введите имя своей компании и свою электронную почту.
4. Выберите регион своей компании.
5. Прочитайте условия соглашения и уведомление о защите данных, затем поставьте галочку, что принимаете их.
6. Нажмите Чтобы создать учетную запись, **Sign up**.

6.5.2

Регистрация устройств DIVAR IP all-in-one на Remote Portal

Чтобы зарегистрировать устройство DIVAR IP all-in-one на Remote Portal:

1. Запустите DIVAR IP System Manager.
2. Перейдите на вкладку **Подключение к Remote Portal**.
3. Если у вас есть учетная запись Remote Portal, введите свой адрес электронной почты и пароль, затем нажмите **Register**, чтобы зарегистрировать устройство DIVAR IP all-in-one на Remote Portal.
4. Если ваш адрес электронной почты назначен нескольким учетным записям компании с правами администратора, отобразится диалог выбора соответствующих учетных записей компании.

В диалоговом окне выберите учетную запись компании, на которую вы хотите зарегистрировать устройство DIVAR IP all-in-one.

Замечание!

SingleKey ID

Bosch предлагает SingleKey ID в качестве поставщика удостоверения (IdP), чтобы обеспечить возможность централизованного входа для всех приложений, сервисов и платформ Bosch.

Чтобы подключить устройство к Remote Portal с помощью SingleKey ID, следуйте инструкциям на экране.



5. Если у вас еще не учетной записи Remote Portal, нажмите **Create account** и создайте учетную запись Remote Portal. См. .

6.5.3

Отмена регистрации устройств DIVAR IP all-in-one с Remote Portal

Чтобы отменить регистрацию устройства DIVAR IP all-in-one с Remote Portal:

1. Запустите DIVAR IP System Manager.
2. Нажмите Вкладка **Remote Portal connection**.
3. Нажмите **Unregister**, чтобы отменить регистрацию устройства DIVAR IP all-in-one с Remote Portal.

Примечание: Отмена регистрации устройства на Remote Portal не приводит к удалению настроек устройства с Remote Portal. Чтобы удалить конфигурацию устройства, войдите в соответствующую учетную запись Remote Portal.

7 Обслуживание

7.1 Вход в систему под учетной записью администратора

Вход в учетную запись администратора для работы в режиме BVMS

Чтобы войти в учетную запись администратора для работы в режиме BVMS, выполните следующее:

1. На рабочем столе BVMS нажмите Ctrl+Alt+Del.
2. Нажмите **Сменить пользователя**, после чего сразу же нажмите и удерживайте левую клавишу Shift.
3. Еще раз нажмите Ctrl+Alt+Del.
4. Выберите пользователя **BVRAdmin** и введите пароль, который был установлен во время настройки системы. Затем нажмите Enter.

Примечание. Чтобы вернуться к рабочему столу BVMS, нажмите Ctrl+Alt+Del, а затем нажмите **Сменить пользователя** или **Выход**. Система автоматически вернется к рабочему столу BVMS без перезапуска системы.

Вход в учетную запись администратора для работы в режиме VRM или iSCSI

Чтобы войти в учетную запись администратора для работы в режиме VRM или iSCSI, выполните следующее:

- ▶ На экране входа в Windows нажмите Ctrl+Alt+Del и введите пароль **BVRAdmin**.

7.2 Мониторинг системы

7.2.1 Мониторинг системы с помощью приложения ASUS Inband Tool

Системы DIVAR IP all-in-one поставляются с предустановленным приложением **ASUS Inband Tool**, которое можно использовать для мониторинга системы.

Служба приложения активирована по умолчанию.

Чтобы запустить приложение, выполните следующие действия.

1. Войдите в систему под учетной записью администратора (см. *Вход в систему под учетной записью администратора*, Страница 21).
2. Откройте на рабочем столе папку **Tools** и дважды нажмите ярлык ASUS Inband Tool. Приложение запустится.
3. Войдите в систему со следующими учетными данными по умолчанию:
 - Учетная запись: **admin**
 - Пароль: **admin**
4. После первого входа в систему вам будет предложено поменять исходный пароль. Введите новый пароль и подтвердите его. Храните новый пароль в надежном месте. Пароль должен соответствовать требованиям:
 - Пароль должен содержать не менее 14 символов.
 - Пароль должен содержать не менее одной буквы в верхнем регистре.
 - Пароль должен содержать не менее одной буквы в нижнем регистре.
 - Пароль должен содержать не менее одного специального символа.
 - Пароль должен содержать не менее одной цифры.
5. После подтверждения нового пароля отобразится страница **Dashboard**, отображающая общее состояние системы.
6. В левой панели **MENU** можно выбрать соответствующие страницы для получения подробной информации о состоянии системы.
7. В пункте меню **SNMP** можно настроить пользователей SNMP и назначения SMMP.
8. На странице **Report** можно создать отчет, содержащий выбранную информацию.

7.2.2

Мониторинг системы с помощью веб-интерфейса BMC

Устройство DIVAR IP all-in-one 7000 имеет специальный порт BMC на задней панели. Каждое устройство DIVAR IP all-in-one 7000 поставляется с именем пользователя BMC по умолчанию **admin** и исходным паролем BMC. Исходный пароль BMC уникален для каждого устройства. Его можно найти на табличке на задней панели устройства, под портом BMC.

После первого входа в веб-интерфейс BMC вам будет предложено поменять исходный пароль. Храните новый пароль в надежном месте.

Пароль должен соответствовать требованиям:

- Пароль должен содержать не менее 14 символов.
- Пароль должен содержать не менее одной буквы в верхнем регистре.
- Пароль должен содержать не менее одной буквы в нижнем регистре.
- Пароль должен содержать не менее одного специального символа.
- Пароль должен содержать не менее одной цифры.



Замечание!

Из соображений безопасности не подключайте устройство к общедоступным сетям через порт BMC.

Настройка параметров BMC

Чтобы настроить параметры BMC, выполните следующие действия.

1. Включите устройство и нажмите клавишу Del для входа в программу настройки BIOS.



Замечание!

Пароль BIOS

Исходный пароль BIOS уникален для каждого устройства. Его можно найти на табличке на задней панели устройства. Компания Bosch настоятельно рекомендует изменить этот исходный пароль. Храните новый пароль в надежном месте.

Пароль должен соответствовать требованиям:

- Пароль должен содержать не менее 14 символов.
- Пароль должен содержать не менее одной буквы в верхнем регистре.
- Пароль должен содержать не менее одной буквы в нижнем регистре.
- Пароли должны содержать не менее одного специального символа.
- Пароль должен содержать не менее одной цифры.

2. В настройках BIOS перейдите на вкладку **Server Mgmt.**
3. Выберите параметр **BMC Network Configuration** и нажмите клавишу Enter.
4. В следующем диалоговом окне выберите параметр **Configuration Address source** и нажмите Enter.
Отобразится диалоговое окно **Configuration Address source.**
5. В диалоговом окне **Configuration Address source** выберите нужный вариант настройки адреса BMC и нажмите Enter.
6. Задайте необходимые параметры конфигурации сети.
7. Нажмите клавиши F4 и Enter для сохранения и выхода.
Устройство DIVAR IP all-in-one 7000 перезапустится.

Работа в удаленном режиме с использованием интерфейса BMC iKVM

По умолчанию устройства DIVAR IP all-in-one 7000 предназначены для работы с одним или двумя локальными мониторами, подключенными к интерфейсам HDMI на задней панели устройства.

Если к интерфейсам HDMI не подключены локальные мониторы, устройством можно удаленно управлять с помощью интерфейса BMC iKVM.

Чтобы разрешить системе дистанционное управление:

1. Убедитесь, что к системе не подключен локальный монитор HDMI.
2. Войдите в веб-интерфейс BMC.
3. В области меню слева выберите страницу **Remot Control**.
4. Нажмите кнопку **Launch H5Viewer**.

Откроется окно с выводом монитора DIVAR IP all-in-one 7000 и возможностью управления мышью и клавиатурой удаленного компьютера.

7.3 Замена неисправного жесткого диска и настройка нового жесткого диска



Замечание!

Компания Bosch не несет ответственности за потерю или повреждение данных, а также за системные сбои устройств, оснащенных жесткими дисками, которые поставлены сторонними организациями. Компания Bosch не может предоставить поддержку, если причиной проблемы являются жесткие диски, не поставляемые компанией Bosch. Для устранения возможных проблем с оборудованием компания Bosch потребует установить жесткие диски, которые поставляет сама.

7.3.1 Замена неисправного жесткого диска


Для замены неисправного жесткого диска выполните следующее:

- ▶ Извлеките неисправный жесткий диск из устройства и установите новый жесткий диск.

См. главу *Установка жесткого диска SATA* в руководстве по установке.

7.3.2 Восстановление RAID5 с использованием нового жесткого диска

Автоматическое восстановление RAID5

1. На рабочем столе DIVAR IP all-in-one дважды щелкните ярлык **Launch LSA**. Запустится приложение **LSI Storage Authority** и откроется страница **Remote Server Discovery**.
2. Войдите, используя учетные данные учетной записи администратора **BVRAdmin**. Отобразится диалоговое окно, сообщающее, что есть контроллер, в котором имеется серьезная проблема.
3. В верхней части страницы нажмите **Select Controller**, а затем нажмите панель **Controller ID:**, чтобы открыть параметры контроллера.
 - Если неисправный жесткий диск еще не удален, он будет отображаться в разделе **Drives > Foreign Drives > Unconfigured Drives**.
 - После того как вы удалите неисправный жесткий диск и установите новый жесткий диск, система автоматически запустит восстановление RAID5 с использованием нового жесткого диска и на индикаторе выполнения будет отображаться ход выполнения восстановления.
4. После успешного завершения восстановления отобразится значок .

Восстановление RAID5 вручную

Если после установки нового жесткого диска восстановление RAID5 не начинается автоматически, выполните следующее:

1. В диалоговом окне настройки контроллера в разделе **Drives > Foreign Drives > Unconfigured Drives** выберите жесткий диск с состоянием **Unconfigured Bad**, а затем в области справа выберите **Make Unconfigured Good**.
Отобразится диалоговое окно.
2. Установите флажок **Confirm**, а затем нажмите **Yes, Make Unconfigured Good**, чтобы продолжить.
Система приступит к восстановлению RAID5 с использованием нового жесткого диска.



3. После успешного завершения восстановления отобразится значок .

7.4

Сбор файлов журналов DIVAR IP System Manager

Приложение DIVAR IP System Manager включает специальный сценарий, который упрощает сбор файлов журналов.

Чтобы собрать файлы журналов DIVAR IP System Manager, выполните следующее:

1. Войдите в систему под учетной записью администратора (см. Вход в систему под учетной записью администратора).
2. В меню **Пуск** в Windows щелкните правой кнопкой мыши **Export System Manager Logs** и запустите сценарий от имени администратора.
Сценарий экспортирует файлы журналов в папку `Documents\Bosch` и создаст ZIP-файл с именем со следующей структурой: `SysMgrLogs-[date]_[time]`.
Этот ZIP-файл можно прикрепить к подробному описанию ошибки.

7.5

Восстановление настроек устройства

Для восстановления устройства выполните следующие действия.

1. Включит устройство и нажимайте клавишу F7 во время самотестирования BIOS при включении питания, чтобы выполнить вход в Windows PE.
Появится диалоговое окно **System Management Utility**.
2. Выберите один из следующих параметров.
 - **System factory default:** этот параметр позволяет форматировать разделы видеоданных и восстанавливать разделы ОС с использованием заводского образа по умолчанию.
Этот процесс займет несколько минут.
 - **Full data overwrite and system factory default:** этот параметр позволяет форматировать разделы видеозаписей, полностью перезаписывать существующие данные, а также восстанавливать раздел ОС с использованием заводского образа по умолчанию.
Примечание. Этот процесс может занять несколько дней.
 - **OS system recovery only:** этот параметр восстанавливает раздел ОС с использованием заводского образа по умолчанию и импортирует существующие виртуальные жесткие диски из существующих разделов видеоданных.
Этот процесс займет несколько минут.

Примечание.

Параметр **OS system recovery only** не удаляет видеозаписи, хранящиеся на жестких дисках данных. Однако он заменит раздел операционной системы (включая параметры системы управления видео) на конфигурацию по умолчанию. Чтобы получить доступ к существующим видеоматериалам после восстановления, конфигурацию системы управления видео 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. Подтвердите выбор параметра.
Система запустит процесс форматирования и восстановления образа.
4. После завершения процесса восстановления подтвердите перезапуск системы.
Система перезапустится и будут выполнены процедуры настройки.
5. После завершения процесса отобразится экран выбора языка Windows.
6. Перейдите к первоначальной настройке системы.

8 Дополнительная информация

8.1 Дополнительная документация и клиентское программное обеспечение

Для получения дополнительной информации, а также скачивания программного обеспечения и документации перейдите на страницу соответствующего продукта в каталоге продуктов:

<http://www.boschsecurity.com>

Последнюю версию программного обеспечения и доступные пакеты обновления можно найти в центре загрузки Bosch Security and Safety Systems по адресу:

<https://downloadstore.boschsecurity.com/>

8.2 Услуги поддержки и Bosch Academy



Поддержка

Получить **услуги поддержки** можно по адресу www.boschsecurity.com/xc/en/support/.



Bosch Building Technologies Academy

Посетите сайт Bosch Building Technologies Academy для доступа к **учебным курсам**, **видеоучебникам** и **документам**: www.boschsecurity.com/xc/en/support/training/

Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2024

Решения в сфере управления зданиями для улучшения качества жизни

202404171736