

Содержание

1	Защита	4
1.1	Техника безопасности при эксплуатации	4
1.2	Правила техники безопасности данных	4
2	Введение	5
3	Обзор системы	6
4	Первый вход в систему и настройка системы	7
4.1	Выбор режима работы	8
4.1.1	Работа в режиме полнофункциональной системы записи и управления видеоданными	8
4.1.2	Работа системы в режиме только видеозаписи	9
4.1.3	Работа в качестве расширения хранилища iSCSI	9
5	Расширение функциональных возможностей и обновление ПО	11
6	Удаленное подключение к системе	12
6.1	Защита системы от несанкционированного доступа	12
6.2	Настройка перенаправления портов	12
6.3	Выбор подходящего клиента	12
6.3.1	Удаленное подключение к Operator Client	12
6.3.2	Удаленное подключение к приложению Video Security	12
6.4	Установка Enterprise Management Server	13
7	Обслуживание	14
7.1	Мониторинг системы	14
7.2	Восстановление настроек устройства	14
8	Дополнительная информация	16
8.1	Дополнительная документация и клиентское программное обеспечение	16
8.2	Услуги поддержки и Bosch Academy	16

1 Защита

Ознакомьтесь с правилами техники безопасности в этом разделе.

1.1 Техника безопасности при эксплуатации

Устанавливать устройство должны только профессиональные специалисты. Устройство не предназначено для личного и домашнего применения. Никаких ограничений на использование устройства в коммерческих и промышленных целях нет, за исключением описанных в разделе «Сведения по технике безопасности».



Замечание!

Данное изделие является изделием **класса А**. При использовании в жилых помещениях данное изделие может являться причиной радиопомех; в этом случае от пользователя может потребоваться принятие соответствующих мер.



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 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.

2 Введение

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).

DIVAR IP Software Center

DIVAR IP Software Center — это центральный пользовательский интерфейс для установки, обновления и выбора режима работы программного обеспечения.

После установки ПО DIVAR IP Software Center необходимо выбрать режим работы для настройки системы.

С помощью DIVAR IP Software Center также можно обновить установленное программное обеспечение и расширить его функциональные возможности.

Последнюю версию программного обеспечения и доступные пакеты обновления можно найти в **разделе загрузок** Bosch Security and Safety Systems на странице:

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

3 Обзор системы

Системы DIVAR IP all-in-one 7000 работают с операционной системой Microsoft Windows Server IoT 2019 for Storage Standard. Операционная система 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 настроен для обеспечения оптимальной производительности подключенного к сети хранилища данных. Операционная система Microsoft Windows Server IoT 2019 for Storage Standard предоставляет значительные улучшения в отношении сценариев управления хранением, а также интеграции компонентов управления и функциональных возможностей устройств хранения данных.

Замечание!

Данная глава относится к моделям DIVAR IP all-in-one 7000, которые поставляются с предварительно установленными жесткими дисками.

Операционная система на пустых устройствах, в которые загружены жесткие диски сторонних производителей, запускается в обычном режиме. Однако дополнительные жесткие диски нужно настроить с помощью утилиты RAID перед первоначальной установкой программного обеспечения.

Для получения дополнительной информации см. руководство по установке.



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: задается при первом входе в систему.

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 Первый вход в систему и настройка системы



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.



Замечание!

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

Чтобы настроить систему, выполните следующие действия:

1. Подключите устройство DIVAR IP all-in-one 7000 и камеры к сети.
2. Включите устройство.
Будут выполнены процедуры установки Microsoft Windows Server IoT 2019 for Storage Standard. Это может занять некоторое время. 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 Microsoft Software License Terms и EULA (лицензионное соглашение с конечным пользователем).
4. Нажмите кнопку **«Принять»**, чтобы принять условия лицензионного соглашения и дождитесь перезапуска Windows. Это может занять некоторое время. Не выключайте систему.
После перезапуска отобразится страница входа в систему Windows.
5. Установите новый пароль учетной записи администратора **BVRAdmini** подтвердите его (примечание: минимальная длина пароля составляет 14 символов). Нажмите клавишу ВВОД.
Отобразится страница **выбора ПО**.
6. Щелкните файл установки DIVAR IP Software Center.
Начнется процесс установки DIVAR IP Software Center. По завершении установки Windows перезапустится и вы будете перенаправлены на страницу входа в Windows.
Примечание. Если файл установки DIVAR IP Software Center не хранится на локальном диске, вставьте носитель данных (USB-устройство флэш-памяти, DVD-диск) с файлом установки.
Будет выполнен автоматический поиск файла установки DIVAR IP Software Center на носителе данных, после чего он будет отображен на странице **выбора ПО**.
7. Войдите в систему с учетной записью администратора.
Автоматически запустится браузер Microsoft Edge.
8. Введите имя пользователя и пароль администратора и нажмите **Войти**.
Запустится DIVAR IP Software Center и произойдет загрузка пакетов программного обеспечения.
Примечание. Если пакеты программного обеспечения для требуемого режима работы недоступны на локальном диске, вставьте носитель данных с пакетами программного

обеспечения для продолжения настройки системы.

Последнюю версию программного обеспечения и доступные пакеты обновления можно найти в **разделе загрузок** Bosch Security and Safety Systems на странице: <https://downloadstore.boschsecurity.com/>

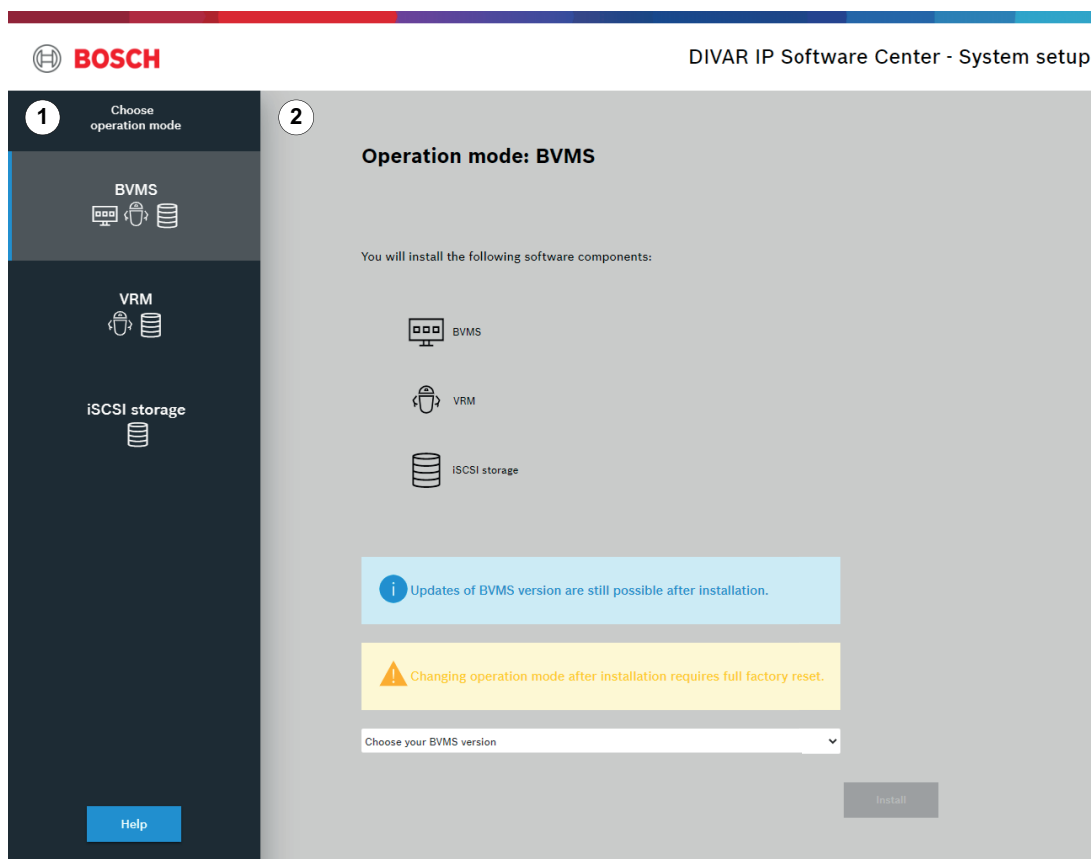
4.1 Выбор режима работы

В приложении DIVAR IP Software Center необходимо выбрать требуемый режим работы для настройки системы DIVAR IP all-in-one 7000.



Замечание!

Изменение режима работы после установки требует полного восстановления заводских настроек.



1	Окно выбора
2	Главное окно

См.

– Режимы работы, Страница 5

4.1.1 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. В окне выбора нажмите **BVMS**.
В главном окне отобразятся программные компоненты, которые будут установлены.

2. Выберите нужную версию BVMS из списка и нажмите кнопку **Установить** (Установить).
Откроется диалоговое окно **Установка BVMS** (Установка BVMS) с указанием пакетов программного обеспечения, которые будут установлены.
3. Нажмите **Установить** (Установить), чтобы продолжить.
Начнется установка пакета программного обеспечения. Это может занять некоторое время. Не выключайте систему и не отсоединяйте устройство хранения.
Примечание. Если во время установки возникнет ошибка, нажмите **Готово** (Завершить). Произойдет перезапуск системы. После перезапуска обновите соответствующие программные пакеты и продолжите установку.
4. После успешного завершения установки всех пакетов нажмите **Готово** (Завершить). Затем произойдет перезапуск системы. После перезапуска откроется рабочий стол BVMS.
5. На рабочем столе BVMS нажмите требуемое приложение для настройки системы.

**Замечание!**

Для получения дополнительной информации см. документацию BVMS.

4.1.2

Работа системы в режиме только видеозаписи

Для работы системы DIVAR IP в режиме только видеозаписи выполните следующие действия:

1. В окне выбора нажмите **VRM**.
В главном окне отобразятся программные компоненты, которые будут установлены.
2. Выберите нужную версию VRM из списка и нажмите кнопку **Установить** (Установить).
Откроется диалоговое окно **Установка VRM** (Установка VRM) с указанием пакетов программного обеспечения, которые будут установлены.
3. Нажмите **Установить** (Установить), чтобы продолжить.
Начнется установка пакета программного обеспечения. Это может занять некоторое время. Не выключайте систему и не отсоединяйте устройство хранения.
Примечание. Если во время установки возникнет ошибка, нажмите **Готово** (Завершить). Произойдет перезапуск системы. После перезапуска обновите соответствующие программные пакеты и продолжите установку.
4. После успешного завершения установки всех пакетов нажмите **Готово** (Завершить). Затем произойдет перезапуск системы. После перезапуска появится экран входа в Windows.

**Замечание!**

Для получения дополнительной информации см. документацию VRM.

4.1.3

Работа в качестве расширения хранилища iSCSI

Для работы системы DIVAR IP в качестве расширения хранилища iSCSI выполните следующие действия:

1. В окне выбора нажмите **iSCSI-хранилище** (Хранилище iSCSI).
В главном окне отобразятся программные компоненты, которые будут установлены.
2. Выберите нужные компоненты из списка и нажмите кнопку **Установить** (Установить).
Откроется диалоговое окно **Установка iSCSI-хранилища** (Установка хранилища iSCSI) с указанием пакетов программного обеспечения, которые будут установлены.

3. Нажмите **Установить** (Установить), чтобы продолжить.
Начнется установка пакета программного обеспечения. Это может занять некоторое время. Не выключайте систему и не отсоединяйте устройство хранения.
Примечание. Если во время установки возникнет ошибка, нажмите **Готово** (Завершить). Произойдет перезапуск системы. После перезапуска обновите соответствующие программные пакеты и продолжите установку.
4. После успешного завершения установки всех пакетов нажмите **Готово** (Завершить). Затем произойдет перезапуск системы. После перезапуска появится экран входа в Windows.
5. 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 Расширение функциональных возможностей и обновление ПО

С помощью DIVAR IP Software Center можно обновить установленное программное обеспечение и расширить его функциональные возможности.

Последнюю версию программного обеспечения и доступные пакеты обновления можно найти в **разделе загрузок** Bosch Security and Safety Systems на странице:

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

Расширение возможностей программного обеспечения

Для расширения возможностей установленного программного обеспечения выполните следующие действия:

1. Загрузите необходимые пакеты программного обеспечения из **раздела загрузки** и сохраните их на локальном диске или на носителе данных. Затем подключите носитель данных к системе.
2. Запустите DIVAR IP Software Center.
Откроется страница **Установленное ПО** (Установленное ПО).
3. В разделе **Обновления** (Улучшения) отображаются доступные улучшения. Нажмите **Обновить** (Обновить) для улучшения выбранного программного обеспечения. Откроется диалоговое окно **Обновление** (Улучшение), в котором отображаются программные пакеты, включенные в улучшение.
Примечание. Будут сохранены все ваши настройки, обновлено программное обеспечение и произведен перезапуск системы.
4. Нажмите **Установить**, чтобы продолжить.
Начнется установка пакетов программного обеспечения. Это может занять некоторое время. Не выключайте систему и не отсоединяйте устройство хранения.
По завершении установки произойдет перезапуск системы.

Обновление программного обеспечения

Чтобы обновить установленное программное обеспечение:

1. Загрузите необходимые пакеты программного обеспечения из **раздела загрузки** и сохраните их на локальном диске или на носителе данных. Затем подключите носитель данных к системе.
2. Запустите DIVAR IP Software Center.
Откроется страница **Установленное ПО** (Установленное ПО).
3. В разделе **Обновления** (Обновления) отображаются доступные обновления. Нажмите **Обновить все** (Обновить все) для установки обновленной версии всех программных пакетов.
Откроется диалоговое окно **Обновление** (Обновление) с указанием пакетов программного обеспечения, которые будут обновлены.
Примечание. Будут сохранены все ваши настройки, обновлено программное обеспечение и произведен перезапуск системы.
4. Нажмите **Установить**, чтобы продолжить.
Начнется установка пакетов программного обеспечения. Это может занять некоторое время. Не выключайте систему и не отсоединяйте устройство хранения.
По завершении установки произойдет перезапуск системы.

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 12.*
- *Удаленное подключение к приложению Video Security, Страница 12.*



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

6.4 Установка Enterprise Management Server

Для централизованного управления несколькими системами можно установить Bosch VMS Enterprise Management Server на отдельном сервере.

Установка Bosch VMS Enterprise Management Server на отдельном сервере:

1. Загрузите установщик BVMS со страницы продукта.
2. Скопируйте **установщик** BVMS на сервер, который должен работать как Enterprise Management Server.
3. Дважды щелкните программу установки и подтвердите сообщение безопасности.
4. В диалоговом окне **приветствия** снимите все флажки, кроме **Enterprise Management Server** и **Configuration Client**.
5. Следуйте инструкциям по установке.
6. По завершении установки запустите Configuration Client с помощью ярлыка на рабочем столе.



Замечание!

Сведения о конфигурации Enterprise Management Server см. в документации BVMS.

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 системы (в зависимости от выбранного режима работы это может быть рабочий стол BVMS или экран входа в систему Windows) нажмите сочетание клавиш 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: DivaripSD5
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.

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.

Последнюю версию программного обеспечения и доступные пакеты обновления можно найти в **разделе загрузок** Bosch Security and Safety Systems на странице:

<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 Security and Safety Systems предоставляет поддержку в следующих областях:

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



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

Нидерланды

www.boschsecurity.com

© Bosch Security Systems B.V., 2020